IBM QRadar

DSM Configuration Guide
March 2024

Note

Before using this information and the product that it supports, read the information in “Notices” on page 1663.

Contents

About this DSM Configuration Guide..... xxxv

Part 1. QRadar DSM installation and log source management.....1

Chapter 1. Event collection from third-party devices..... 3
Adding a DSM..... 4

Chapter 2. Introduction to log source management..... 5
Adding a log source..... 5
Adding a log source by using the **Log Sources** icon..... 7
Adding bulk log sources..... 8
Adding bulk log sources by using the Log Sources icon..... 9
Editing bulk log sources..... 10
Editing bulk log sources by using the Log Sources icon..... 11
Adding a log source parsing order..... 11
QRadar DSM installations and log source management FAQ..... 12
Testing log sources..... 12
Protocols available for testing..... 12
Log source groups..... 13
Creating a log source group..... 13
Copying and removing log sources..... 14
Removing a log source group..... 14

Chapter 3. Gateway log source..... 15
Log source identifier pattern..... 16

Chapter 4. Log source extensions..... 19
Examples of log source extensions on QRadar Support Forums..... 19
Patterns in log source extension documents..... 20
Match groups..... 20
Matcher (matcher)..... 21
JSON matcher (json-matcher)..... 26
LEEF matcher (leef-matcher)..... 30
CEF matcher (cef-matcher)..... 31
Name Value Pair matcher (namevaluepair-matcher)..... 31
Generic List matcher (genericlist-matcher)..... 33
XML Matcher (xml-matcher)..... 34
Multi-event modifier (`event-match-multiple`)..... 35
Single-event modifier (`event-match-single`)..... 35
Extension document template..... 36
Creating a log source extensions document to get data into QRadar..... 38
Common regular expressions..... 39
Building regular expression patterns..... 40
Uploading extension documents to QRadar..... 42
Examples of parsing issues..... 42

Chapter 5. Manage log source extensions..... 45
Adding a log source extension..... 45

Chapter 6. Threat use cases by log source type..... 47

Chapter 7. Troubleshooting DSMs....59

Part 2. QRadar protocol configuration....63

Chapter 8. Undocumented protocols....65
Configuring an undocumented protocol....65

Chapter 9. Protocol configuration options....67
Akamai Kona REST API protocol configuration options....67
Alibaba Cloud Object Storage protocol configuration options....69
Alibaba Cloud Simple Log Service protocol configuration options....71
Alibaba Cloud Simple Log Service protocol workflow....73
Amazon AWS S3 REST API protocol configuration options....75
Amazon Web Services protocol configuration options....83
Apache Kafka protocol configuration options....96
Configuring Apache Kafka to enable Client Authentication....102
Configuring Apache Kafka to enable SASL Authentication....105
Troubleshooting Apache Kafka....107
Blue Coat Web Security Service REST API protocol configuration options....108
Centrify Redrock REST API protocol configuration options....108
Cisco Duo protocol configuration options....110
Cisco Duo protocol workflow....112
Cisco Firepower eStreamer protocol configuration options....114
Cisco NSEL protocol configuration options....116
EMC VMware protocol configuration options....116
Forwarded protocol configuration options....117
Google Cloud Pub/Sub protocol configuration options....117
Configuring Google Cloud Pub/Sub to integrate with QRadar....120
Adding a Google Cloud Pub/Sub log source in QRadar....121
Google G Suite Activity Reports REST API protocol options....122
Google G Suite Activity Reports REST API protocol FAQ....123
HCL BigFix SOAP protocol configuration options (formerly known as IBM BigFix)....124
HTTP Receiver protocol configuration options....125
Setting up certificate-based authentication for HTTP Receiver....130
IBM Cloud Object Storage protocol configuration options....131
IBM Fiberlink REST API protocol configuration options....134
IBM Security Randori REST API protocol configuration options....136
IBM Security Randori REST API protocol workflow....138
IBM Security QRadar EDR REST API protocol configuration options....141
IBM Security QRadar EDR REST API protocol workflow....143
IBM Security Verify Event Service protocol configuration options....144
JDBC protocol configuration options....147
JDBC - SiteProtector protocol configuration options....152
Juniper Networks NSM protocol configuration options....154
Juniper Security Binary Log Collector protocol configuration options....154
Log File protocol configuration options....155
Microsoft Azure Event Hubs protocol configuration options....159
Configuring Microsoft Azure Event Hubs to communicate with QRadar....164
Configuring VNet Flow Logs on the Microsoft Azure portal....166
Troubleshooting Microsoft Azure Event Hubs protocol....167
Microsoft Defender for Endpoint SIEM REST API protocol configuration options....174
Microsoft DHCP protocol configuration options....177
Microsoft Exchange protocol configuration options....179
Microsoft Graph Security API protocol configuration options....182
Configuring Microsoft Graph Security API to communicate with QRadar....185

Migrating Microsoft Defender for Endpoint REST API log sources to Microsoft Graph Security API log sources ... 186
Microsoft IIS protocol configuration options ... 187
Microsoft Security Event Log protocol configuration options ... 189
Microsoft Security Event Log over MSRPC Protocol ... 189
MQ protocol configuration options ... 192
Office 365 Message Trace REST API protocol configuration options ... 193
Troubleshooting the Office 365 Message Trace REST API protocol ... 196
Office 365 REST API protocol configuration options ... 199
Okta REST API protocol configuration options ... 200
OPSEC/LEA protocol configuration options ... 201
Oracle Database Listener protocol configuration options ... 203
PCAP Syslog Combination protocol configuration options ... 204
RabbitMQ protocol configuration options ... 206
Copy the server certificate ... 208
SDEE protocol configuration options ... 208
Seculert Protection REST API protocol configuration options ... 208
Seculert Protection REST API protocol workflow ... 211
SMB Tail protocol configuration options ... 214
SNMPv2 protocol configuration options ... 216
SNMPv3 protocol configuration options ... 217
Sophos Enterprise Console JDBC protocol configuration options ... 218
Sourcefire Defense Center eStreamer protocol options ... 220
Syslog Redirect protocol overview ... 220
TCP Multiline Syslog protocol configuration options ... 222
TLS Syslog protocol configuration options ... 227
Multiple log sources over TLS Syslog ... 233
UDP multiline syslog protocol configuration options ... 233
VMware vCloud Director protocol configuration options ... 236

Chapter 10. Universal Cloud REST API protocol ... 239
Workflow ... 241
Workflow Parameter Values ... 242
State ... 242
Actions ... 243
Abort ... 243
Add ... 244
CallEndpoint ... 244
ClearStatus ... 250
Copy ... 250
Create JWTAccessToken ... 250
Delete ... 251
DoWhile ... 252
ForEach ... 252
FormatDate ... 253
GenerateHMAC ... 253
If/ElseIf/Else ... 254
Initialize ... 255
Log ... 256
Merge ... 256
ParseDate ... 257
PostEvent ... 257
PostEvents ... 258
RegexCapture ... 259
Set ... 260
SetStatus ... 260
Sleep ... 260
Split ... 261

While... 261
XPathQuery... 262
JPath... 263
Basic selection... 263
Query... 264
Arithmetic operations in JSON elements... 265
Functions in JPath expressions... 266
Command line testing tool... 267

Chapter 11. Protocols that support Certificate Management... 269

Part 3. DSMs... 271

Chapter 12. 3Com Switch 8800... 273
Configuring your 3COM Switch 8800... 274

Chapter 13. AhnLab Policy Center... 275

Chapter 14. Akamai Kona... 277
Configure an Akamai Kona log source by using the HTTP Receiver protocol... 277
Configure an Akamai Kona log source by using the Akamai Kona REST API protocol... 278
Configuring Akamai Kona to communicate with QRadar... 280
Creating an event map for Akamai Kona events... 280
Modifying the event map for Akamai Kona... 281
Akamai Kona sample event messages... 282

Chapter 15. Alibaba ActionTrail... 285
Alibaba ActionTrail sample event message... 285

Chapter 16. Amazon... 287
Amazon AWS Application Load Balancer Access Logs... 287
Amazon AWS Application Load Balancer Access Logs DSM specifications... 287
Publishing flow logs to an S3 bucket... 288
Create an SQS queue and configure S3 ObjectCreated notifications... 288
Amazon AWS S3 REST API log source parameters for Amazon AWS Application Load Balancer Access Logs... 298
Amazon AWS Application Load Balancer Access Logs sample event message... 299
Amazon AWS CloudTrail... 299
Configuring an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol... 301
Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol... 320
Configuring an Amazon AWS CloudTrail log source that uses Amazon Security Lake... 333
Amazon AWS CloudTrail sample event messages... 333
AWS Config... 334
Enabling AWS Config logs... 335
Configuring an Amazon AWS Config log source by using the Amazon AWS S3 REST API protocol... 336
Amazon AWS Elastic Kubernetes Service... 353
Amazon AWS Elastic Kubernetes Service DSM specifications... 354
Configuring Amazon Elastic Kubernetes Service to communicate with QRadar... 354
Configuring security credentials for your AWS user account... 355
Amazon Web Services log source parameters for Amazon AWS Elastic Kubernetes Service... 355
Amazon AWS Elastic Kubernetes Service sample event messages... 358
Amazon AWS Network Firewall... 360
Amazon AWS Network Firewall DSM specifications... 360
Create an SQS queue and configure S3 ObjectCreated notifications... 361

Amazon AWS S3 REST API log source parameters for Amazon AWS Network Firewall..... 369
AWS Network Firewall sample event messages.....370
Amazon AWS Route 53..... 371
Amazon AWS Route 53 DSM specifications.....371
Configuring an Amazon AWS Route 53 log source by using the Amazon Web Services protocol and CloudWatch logs..... 372
Configuring an Amazon AWS Route 53 log source by using an S3 bucket with an SQS queue..380
Configuring an Amazon AWS Route 53 log source by using an S3 bucket with a directory prefix..... 393
Configuring an Amazon Route 53 log source that uses Amazon Security Lake.....399
Amazon AWS Route 53 sample event messages..... 400
Amazon AWS Security Hub..... 401
Amazon AWS Security Hub DSM specifications.....402
Creating an EventBridge rule for sending events..... 402
Creating an Identity and Access (IAM) user in the AWS Management Console.....403
Amazon Web Services log source parameters for Amazon AWS Security Hub..... 403
Amazon AWS Security Hub sample event message..... 403
Amazon AWS WAF.....404
Amazon AWS WAF DSM specifications..... 404
Configuring Amazon AWS WAF to communicate with QRadar.....405
Configuring security credentials for your AWS user account..... 406
Amazon AWS S3 REST API log source parameters for Amazon AWS WAF..... 406
Amazon AWS WAF sample event messages.....407
Amazon CloudFront.....408
Configuring an Amazon CloudFront log source by using the Amazon Web Services protocol... 409
Amazon CloudFront sample event message.....415
Configuring security credentials for your AWS user account..... 415
Amazon GuardDuty..... 416
Configuring an Amazon GuardDuty log source by using the Amazon Web Services protocol....416
Creating an EventBridge rule for sending events..... 419
Creating an Identity and Access (IAM) user in the AWS Management Console.....420
Configuring an Amazon GuardDuty log source by using the Amazon AWS S3 REST API protocol.....420
Configuring an Amazon GuardDuty log source that uses Amazon Security Lake..... 423
Create an SQS queue and configure S3 ObjectCreated notifications..... 424
Configuring Amazon GuardDuty to forward events to an AWS S3 Bucket.....433
Adding an Amazon GuardDuty log source on the QRadar Console using an SQS queue..... 433
Amazon GuardDuty sample event messages..... 437
Amazon VPC Flow Logs.....439
Amazon VPC Flow Logs specifications.....443
Publishing flow logs to an S3 bucket..... 443
Create the SQS queue that is used to receive ObjectCreated notifications.....444
Configuring security credentials for your AWS user account..... 444
AWS Verified Access..... 444
AWS Verified Access DSM specifications.....445
Configuring an AWS Verified Access log source by using the Amazon AWS S3 REST API protocol.....445

Chapter 17. Ambiron TrustWave ipAngel 465

Chapter 18. APC UPS.....467
Configuring your APC UPS to forward syslog events.....468
APC UPS sample event messages..... 468

Chapter 19. Apache HTTP Server..... 469
Configuring Apache HTTP Server with syslog..... 469
Syslog log source parameters for Apache HTTP Server..... 470
Configuring Apache HTTP Server with syslog-ng.....470

Syslog log source parameters for Apache HTTP Server 471
Apache HTTP Server sample event messages 472

Chapter 20. Apple Mac OS X 473
Apple Mac OS X DSM specifications 473
Syslog log source parameters for Apple Mac OS X 473
Configuring syslog on your Apple Mac OS X 474
Apple Mac OS X sample event message 476

Chapter 21. Application Security DbProtect 477
Installing the DbProtect LEEF Relay Module 478
Configuring the DbProtect LEEF Relay 478
Configuring DbProtect alerts 479

Chapter 22. Arbor Networks 481
Arbor Networks Peakflow SP 481
Supported event types for Arbor Networks Peakflow SP 482
Configuring a remote syslog in Arbor Networks Peakflow SP 482
Configuring global notifications settings for alerts in Arbor Networks Peakflow SP 482
Configuring alert notification rules in Arbor Networks Peakflow SP 483
Syslog log source parameters for Arbor Networks Peakflow SP 483
Arbor Networks Pravail 484
Configuring your Arbor Networks Pravail system to send events to IBM QRadar 485
Arbor Networks Pravail sample event message 486

Chapter 23. Arpeggio SIFT-IT 487
Configuring a SIFT-IT agent 487
Syslog log source parameters for Arpeggio SIFT-IT 488
Additional information 488

Chapter 24. Array Networks SSL VPN 491
Syslog log source parameters for Array Networks SSL VPN 491

Chapter 25. Aruba Networks 493
Aruba ClearPass Policy Manager 493
Configuring Aruba ClearPass Policy Manager to communicate with QRadar 494
TCP Multiline Syslog log source parameters for Aruba ClearPass Policy Manager 503
Aruba ClearPass Policy Manager sample event message 505
Aruba Introspect 505
Configuring Aruba Introspect to communicate with QRadar 507
Aruba Mobility Controllers 508
Configuring your Aruba Mobility Controller 508
Syslog log source parameters for Aruba Mobility Controllers 509
Aruba Mobility Controllers sample event messages 509

Chapter 26. Avaya VPN Gateway 511
Avaya VPN Gateway DSM integration process 511
Configuring your Avaya VPN Gateway system for communication with IBM QRadar 512
Syslog log source parameters for Avaya VPN Gateway 512
Avaya VPN Gateway sample event messages 512

Chapter 27. BalaBit IT Security 515
BalaBit IT Security for Microsoft Windows Events 515
Configuring the Syslog-ng Agent event source 515
Configuring a syslog destination 516
Restarting the Syslog-ng Agent service 517
Syslog log source parameters for BalaBit IT Security for Microsoft Windows Events 517
BalaBit IT Security for Microsoft ISA or TMG Events 517

Configure the BalaBit Syslog-ng Agent ... 518
Configuring the BalaBit Syslog-ng Agent file source ... 518
Configuring a BalaBit Syslog-ng Agent syslog destination ... 519
Filtering the log file for comment lines ... 519
Configuring a BalaBit Syslog-ng PE Relay ... 520
Syslog log source parameters for BalaBit IT Security for Microsoft ISA or TMG Events ... 521

Chapter 28. Barracuda ... 523
Barracuda Spam & Virus Firewall ... 523
Configuring syslog event forwarding ... 523
Syslog log source parameters for Barracuda Spam Firewall ... 523
Barracuda Spam and Virus Firewall sample event messages ... 524
Barracuda Web Application Firewall ... 525
Configuring Barracuda Web Application Firewall to send syslog events to QRadar ... 526
Configuring Barracuda Web Application Firewall to send syslog events to QRadar for devices that do not support LEEF ... 526
Barracuda Web Filter ... 527
Configuring syslog event forwarding ... 528
Syslog log source parameters for Barracuda Web Filter ... 528
Barracuda Web Filter sample event message ... 528

Chapter 29. BeyondTrust PowerBroker ... 531
Syslog log source parameters for BeyondTrust PowerBroker ... 531
TLS Syslog log source parameters for BeyondTrust PowerBroker ... 532
Configuring BeyondTrust PowerBroker to communicate with QRadar ... 532
BeyondTrust PowerBroker DSM specifications ... 534
BeyondTrust PowerBroker sample event message ... 534

Chapter 30. BlueCat Networks Adonis ... 537
Supported event types ... 537
Event type format ... 537
Configuring BlueCat Adonis ... 537
Syslog log source parameters for BlueCat Networks Adonis ... 538

Chapter 31. Blue Coat ... 539
Blue Coat SG ... 539
Creating a custom event format ... 540
Creating a log facility ... 541
Enabling access logging ... 541
Configuring Blue Coat SG for FTP uploads ... 541
Syslog log source parameters for Blue Coat SG ... 542
Log File log source parameters for Blue Coat SG ... 543
Configuring Blue Coat SG for syslog ... 546
Creating extra custom format key-value pairs ... 546
Blue Coat SG sample event messages ... 547
Blue Coat Web Security Service ... 547
Configuring Blue Coat Web Security Service to communicate with QRadar ... 549
Blue Coat Web Security Service sample event message ... 549

Chapter 32. Box ... 551
Configuring Box to communicate with QRadar ... 552
Box sample event messages ... 554

Chapter 33. Bridgewater ... 557
Configuring Syslog for your Bridgewater Systems Device ... 557
Syslog log source parameters for Bridgewater Systems ... 557

Chapter 34. Broadcom ... 559

Broadcom CA ACF2 ... 559
Create a log source for near real-time event feed ... 560
Log File log source parameter ... 560
Integrate Broadcom CA ACF2 with IBM QRadar by using audit scripts ... 564
Configuring Broadcom CA ACF2 that uses audit scripts to integrate with IBM QRadar ... 565
Broadcom CA Top Secret ... 568
Log File log source parameter ... 569
Create a log source for near real-time event feed ... 573
Integrate Broadcom CA Top Secret with IBM QRadar by using audit scripts ... 573
Configuring Broadcom CA Top Secret that uses audit scripts to integrate with IBM QRadar ... 574
Broadcom Symantec SiteMinder ... 577
Broadcom Symantec SiteMinder DSM specifications ... 577
Syslog log source parameters for Broadcom Symantec SiteMinder ... 578
Configuring syslog-ng for Broadcom Symantec SiteMinder ... 579
Broadcom Symantec SiteMinder sample event messages ... 580

Chapter 35. Brocade Fabric OS ... 581
Configuring syslog for Brocade Fabric OS appliances ... 581
Brocade Fabric OS sample event messages ... 581

Chapter 36. Carbon Black ... 583
Carbon Black ... 583
Configuring Carbon Black to communicate with QRadar ... 584
Carbon Black sample event messages ... 585
Carbon Black Bit9 Parity ... 585
Syslog log source parameters for Carbon Black Bit9 Parity ... 586
Bit9 Security Platform ... 586
Configuring Carbon Black Bit9 Security Platform to communicate with QRadar ... 587

Chapter 37. Centrify Infrastructure Services ... 589
Configuring WinCollect agent to collect event logs from Centrify Infrastructure Services ... 590
Configuring Centrify Infrastructure Services on a UNIX or Linux device to communicate with QRadar ... 592
Centrify Infrastructure Services sample event messages ... 593

Chapter 38. Check Point ... 597
Integrate Check Point by using syslog ... 597
Syslog log source parameters for Check Point ... 598
Syslog sample event messages for Check Point ... 599
Integrate Check Point by using OPSEC ... 600
Adding a Check Point Host ... 600
Creating an OPSEC Application Object ... 600
Locating the log source SIC ... 601
OPSEC/LEA log source parameters for Check Point ... 602
Edit your OPSEC communications configuration ... 602
Changing the default port for OPSEC LEA communication ... 603
Configuring OPSEC LEA for unencrypted communications ... 603
Integrating Check Point by using TLS Syslog ... 604
TLS syslog log source parameters for Check Point ... 605
Syslog Redirect log source parameters for Check Point ... 606
Configuring Check Point to forward LEEF events to QRadar ... 607
Configuring QRadar to receive LEEF events from Check Point ... 609
Integration of Check Point Firewall events ... 609
Check Point Multi-Domain Management (Provider-1) ... 609
Integrating syslog for Check Point Multi-Domain Management (Provider-1) ... 610
Configuring OPSEC for Check Point Multi-Domain Management (Provider-1) ... 611
Check Point Multi-Domain Management (Provider-1) sample event messages ... 612

Chapter 39. Cilasoft QJRN/400....613
Configuring Cilasoft QJRN/400....613
Syslog log source parameters for Cilasoft QJRN/400....614

Chapter 40. Cisco....617
Cisco ACE Firewall....617
Configuring Cisco ACE Firewall....617
Syslog log source parameters for Cisco ACE Firewall....617
Cisco ACS....618
Configuring Syslog for Cisco ACS v5.x....618
Creating a Remote Log Target....618
Configuring global logging categories....619
Syslog log source parameters for Cisco ACS v5.x....619
Configuring Syslog for Cisco ACS v4.x....620
Configuring syslog forwarding for Cisco ACS v4.x....620
Syslog log source parameters for Cisco ACS v4.x....621
UDP Multiline Syslog log source parameters for Cisco ACS....621
Cisco ACS sample event messages....622
Cisco Aironet....623
Syslog log source parameters for Cisco Aironet....624
Cisco ASA....624
Integrate Cisco ASA Using Syslog....624
Configuring syslog forwarding....625
Syslog log source parameters for Cisco ASA....625
Integrate Cisco ASA for NetFlow by using NSEL....626
Configuring NetFlow Using NSEL....626
Cisco NSEL log source parameters for Cisco ASA....627
Removing leading domain names from usernames when Cisco ASA events are processed....628
Collecting IP addresses for Cisco ASA Teardown TCP connection events....628
Cisco ASA sample event message....628
Cisco AMP....629
Cisco AMP DSM specifications....630
Creating a Cisco AMP Client ID and API key for event queues....630
Creating a Cisco AMP event stream....631
Cisco AMP event stream configuration....633
Cisco AMP sample event message....635
Cisco CallManager....635
Configuring syslog forwarding....635
Syslog log source parameters for Cisco CallManager....636
Cisco CallManager sample event message....636
Cisco CatOS for Catalyst Switches....637
Configuring syslog forwarding for Cisco CatOS devices....637
Syslog log source parameters for Cisco CatOS for Catalyst Switches....637
Cisco CatOS for Catalyst Switches sample event messages....638
Cisco Cloud Web Security....639
Configuring Cloud Web Security to communicate with QRadar....641
Cisco CSA....642
Configuring Cisco CSA to send events to IBM QRadar....642
Syslog log source parameters for Cisco CSA....642
SNMPv1 log source parameters for Cisco CSA....643
SNMPv2 log source parameters for Cisco CSA....644
Cisco Duo....644
Cisco Duo DSM specifications....645
Configuring Cisco Duo to communicate with QRadar....645
Cisco Duo protocol log source parameters for Cisco Duo....646
Cisco Duo sample event messages....646
Cisco Firepower Management Center....647

Creating Cisco Firepower Management Center 5.x, 6.x, and 7.x certificates..... 650
Importing a Cisco Firepower Management Center certificate in QRadar..... 651
Cisco Firepower Management Center log source parameters..... 652
Cisco Firepower Threat Defense.....653
Cisco Firepower Threat Defense DSM specifications..... 653
Configuring Cisco Firepower Threat Defense to communicate with QRadar.....654
Configuring QRadar to use previous connection event processing for Cisco Firepower Threat Defense 654
Cisco Firepower Threat Defense sample event message.....655
Cisco FWSM..... 655
Configuring Cisco FWSM to forward syslog events.....656
Syslog log source parameters for Cisco FWSM.....656
Cisco Identity Services Engine.....656
Configuring a remote logging target in Cisco ISE.....659
Configuring logging categories in Cisco ISE.....659
Cisco Identity Services Engine sample event message..... 660
Cisco IDS/IPS..... 661
SDEE log source parameters for Cisco IDS/IPS.....661
Cisco IOS..... 663
Configuring Cisco IOS to forward events..... 663
Syslog log source parameters for Cisco IOS.....664
Cisco IOS sample event messages..... 664
Cisco IronPort.....665
Cisco IronPort DSM specifications..... 666
Configuring Cisco IronPort appliances to communicate with QRadar..... 666
Configuring a Cisco IronPort and Cisco ESA log source by using the log file protocol..... 667
Configuring a Cisco IronPort and Cisco WSA log source by using the Syslog protocol..... 670
Cisco IronPort sample event message..... 670
Cisco Meraki..... 671
Cisco Meraki DSM specifications.....672
Configure Cisco Meraki to communicate with IBM QRadar 672
Cisco Meraki sample event messages..... 673
Cisco NAC..... 674
Configuring Cisco NAC to forward events..... 674
Syslog log source parameters for Cisco NAC.....674
Cisco Nexus..... 675
Configuring Cisco Nexus to forward events..... 675
Syslog log source parameters for Cisco Nexus.....675
Cisco Nexus sample event message..... 676
Cisco Pix..... 676
Configuring Cisco Pix to forward events..... 676
Syslog log source parameters for Cisco Pix..... 677
Cisco Secure Workload..... 677
Cisco Secure Workload DSM specifications.....678
Configure Cisco Secure Workload to communicate with IBM QRadar 678
Cisco Secure Workload sample event message..... 679
Cisco Stealthwatch.....679
Configuring Cisco Stealthwatch to communicate with QRadar.....680
Cisco Stealthwatch sample event messages.....681
Cisco Umbrella..... 682
Configure Cisco Umbrella to communicate with QRadar..... 684
Cisco Umbrella DSM specifications.....684
Cisco Umbrella sample event messages..... 684
Cisco VPN 3000 Concentrator 685
Syslog log source parameters for Cisco VPN 3000 Concentrator.....686
Cisco Wireless LAN Controllers..... 686
Configuring syslog for Cisco Wireless LAN Controller..... 686
Syslog log source parameters for Cisco Wireless LAN Controllers..... 687

Configuring SNMPv2 for Cisco Wireless LAN Controller....688
Configuring a trap receiver for Cisco Wireless LAN Controller....689
SNMPv2 log source parameters for Cisco Wireless LAN Controllers....689
Cisco Wireless Services Module....690
Configuring Cisco WiSM to forward events....691
Syslog log source parameters for Cisco WiSM....692

Chapter 41. Citrix....695
Citrix Access Gateway....695
Syslog log source parameters for Citrix Access Gateway....695
Citrix NetScaler....696
Syslog log source parameters for Citrix NetScaler....697
Citrix NetScaler sample event message....697

Chapter 42. Cloudera Navigator....699
Configuring Cloudera Navigator to communicate with QRadar....700

Chapter 43. Cloudflare Logs....701
Cloudflare Logs DSM specifications....701
Configure Cloudflare to send events to IBM QRadar when you use the HTTP Receiver protocol....702
Configuring Cloudflare Logs to send events to IBM QRadar when you use the Amazon S3 REST API protocol....703
Create an SQS queue and configure S3 ObjectCreated notifications....703
Finding the S3 bucket that contains the data that you want to collect....704
Creating the SQS queue that is used to receive ObjectCreated notifications....704
Setting up SQS queue permissions....705
Creating ObjectCreated notifications....706
Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge....712
Configuring security credentials for your AWS user account....713
HTTP Receiver log source parameters for Cloudflare Logs....713
Amazon AWS S3 REST API log source parameters for Cloudflare Logs....714
Cloudflare Logs sample event messages....715

Chapter 44. CloudPassage Halo....719
Configuring CloudPassage Halo for communication with QRadar....719
Syslog log source parameters for CloudPassage Halo....721
Log File log source parameters for CloudPassage Halo....721

Chapter 45. CloudLock Cloud Security Fabric....723
Configuring CloudLock Cloud Security Fabric to communicate with QRadar....724

Chapter 46. Correlog Agent for IBM z/OS....725
Configuring your CorreLog Agent system for communication with QRadar....726

Chapter 47. CrowdStrike Falcon....727
CrowdStrike Falcon DSM specifications....727
Configuring CrowdStrike Falcon to communicate with QRadar....728
Syslog log source parameters for CrowdStrike Falcon....731
CrowdStrike Falcon Host sample event message....731

Chapter 48. CrowdStrike Falcon Data Replicator....733
CrowdStrike Falcon Data Replicator DSM specifications....733
Configuring CrowdStrike Falcon Data Replicator to communicate with IBM QRadar....734
Amazon AWS S3 REST API parameters for CrowdStrike Falcon Data Replicator log source....734
CrowdStrike Falcon Data Replicator sample event message....734

Chapter 49. CRYPTOCard CRYPTO-Shield....737
Configuring syslog for CRYPTOCard CRYPTO-Shield....737

Syslog log source parameters for CRYPTOCard CRYPTO-Shield....737

Chapter 50. CyberArk....739
CyberArk Identity....739
CyberArk Identity DSM specifications....739
Configuring CyberArk Identity to communicate with QRadar....740
CyberArk Identity sample event message....741
CyberArk Privileged Threat Analytics....741
Configuring CyberArk Privileged Threat Analytics to communicate with QRadar....742
CyberArk Vault....743
Configuring syslog for CyberArk Vault....743
Syslog log source parameters for CyberArk Vault....744

Chapter 51. CyberGuard Firewall/VPN Appliance....745
Configuring syslog events....745
Syslog log source parameters for CyberGuard....745

Chapter 52. Damballa Failsafe....747
Configuring syslog for Damballa Failsafe....747
Syslog log source parameters for Damballa Failsafe....747

Chapter 53. DG Technology MEAS....749
Configuring your DG Technology MEAS system for communication with QRadar....749

Chapter 54. Digital China Networks (DCN)....751
Configuring a DCN DCS/DCRS Series Switch....751
Syslog log source parameters for DCN DCS/DCRS Series switches....752

Chapter 55. Enterprise-IT-Security.com SF-Sherlock....753
Configuring Enterprise-IT-Security.com SF-Sherlock to communicate with QRadar....754

Chapter 56. Epic SIEM....755
Configuring Epic SIEM 2014 to communicate with QRadar....756
Configuring Epic SIEM 2015 to communicate with QRadar....756
Configuring Epic SIEM 2017 to communicate with QRadar....758
Configuring Epic SIEM 2022 to communicate with QRadar....760

Chapter 57. ESET Remote Administrator....761
Configuring ESET Remote Administrator to communicate with QRadar....762

Chapter 58. Exabeam....763
Configuring Exabeam to communicate with QRadar....763
Exabeam sample event message....764

Chapter 59. Extreme....765
Extreme 800-Series Switch....765
Configuring your Extreme 800-Series Switch....765
Syslog log source parameters for Extreme 800-Series Switches....765
Extreme Dragon....766
Creating a Policy for Syslog....766
Syslog log source parameters for Extreme Dragon....768
Configure the EMS to forward syslog messages....768
Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later....768
Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier....769
Extreme HiGuard Wireless IPS....769
Configuring Enterasys HiGuard....770
Syslog log source parameters for Extreme HiGuard....770
Extreme HiPath Wireless Controller....771

Configuring your HiPath Wireless Controller ... 771
Syslog log source parameters for Extreme HiPath ... 771
Extreme Matrix Router ... 772
Extreme Matrix K/N/S Series Switch ... 773
Extreme NetSight Automatic Security Manager ... 774
Extreme NAC ... 774
Syslog log source parameters for Extreme NAC ... 775
Extreme stackable and stand-alone switches ... 775
Extreme Networks ExtremeWare ... 776
Syslog log source parameters for Extreme Networks ExtremeWare ... 777
Extreme XSR Security Router ... 777
Syslog log source parameters for Extreme XSR Security Router ... 778

Chapter 60. F5 Networks ... 779
F5 Networks BIG-IP AFM ... 779
Configuring a logging pool ... 779
Creating a high-speed log destination ... 780
Creating a formatted log destination ... 780
Creating a log publisher ... 780
Creating a logging profile ... 781
Associating the profile to a virtual server ... 781
Syslog log source parameters for F5 Networks BIG-IP AFM ... 782
F5 Networks BIG-IP AFM sample event message ... 782
F5 Networks BIG-IP APM ... 783
Configuring Remote Syslog for F5 BIG-IP APM V11.x to V14.x ... 783
Configuring a Remote Syslog for F5 BIG-IP APM 10.x ... 783
Syslog log source parameters for F5 Networks BIG-IP APM ... 784
F5 Networks BIG-IP APM sample event message ... 784
F5 Networks BIG-IP ASM ... 785
Syslog log source parameters for F5 Networks BIG-IP ASM ... 785
F5 Networks BIG-IP ASM sample event messages ... 786
F5 Networks BIG-IP LTM ... 788
F5 Networks BIG-IP LTM DSM specifications ... 789
Syslog log source parameters for F5 Networks BIG-IP LTM ... 789
Configuring syslog forwarding in BIG-IP LTM ... 790
Configuring Remote Syslog for F5 BIG-IP LTM V11.x to V14.x ... 790
Configuring Remote Syslog for F5 BIG-IP LTM V10.x ... 790
Configuring Remote Syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8 ... 791
F5 Networks BIG-IP LTM sample event messages ... 791
F5 Networks FirePass ... 792
Configuring syslog forwarding for F5 FirePass ... 792
Syslog log source parameters for F5 Networks FirePass ... 793

Chapter 61. Fair Warning ... 795
Log File log source parameters for Fair Warning ... 795
Fair Warning sample event messages ... 795

Chapter 62. Fasoo Enterprise DRM ... 797
Configuring Fasoo Enterprise DRM to communicate with QRadar ... 802

Chapter 63. Fidelis XPS ... 803
Configuring Fidelis XPS ... 803
Syslog log source parameters for Fidelis XPS ... 804
Fidelis XPS sample event messages ... 804

Chapter 64. FireEye ... 807
Configuring your FireEye system for communication with QRadar ... 809
Configuring your FireEye HX system for communication with QRadar ... 809

Configuring a FireEye log source in QRadar ... 810
FireEye sample event message ... 810

Chapter 65. Forcepoint ... 813
Forcepoint Stonesoft Management Center ... 813
Configuring FORCEPOINT Stonesoft Management Center to communicate with QRadar ... 814
Configuring a syslog traffic rule for FORCEPOINT Stonesoft Management Center ... 815
Forcepoint Sidewinder ... 816
Forcepoint Sidewinder DSM specifications ... 817
Configure Forcepoint Sidewinder to communicate with QRadar ... 817
Forcepoint Sidewinder sample event message ... 817
Forcepoint TRITON ... 818
Configuring syslog for Forcepoint TRITON ... 819
Syslog log source parameters for Forcepoint TRITON ... 819
Forcepoint V-Series Data Security Suite ... 820
Configuring syslog for Forcepoint V-Series Data Security Suite ... 820
Syslog log source parameters for Forcepoint V-Series Data Security Suite ... 820
Forcepoint V-Series Data Security Suite sample event message ... 821
Forcepoint V-Series Content Gateway ... 821
Configure syslog for Forcepoint V-Series Content Gateway ... 822
Configuring the Management Console for Forcepoint V-Series Content Gateway ... 822
Enabling Event Logging for Forcepoint V-Series Content Gateway ... 823
Syslog log source parameters for Forcepoint V-Series Content Gateway ... 823
Log file protocol for Forcepoint V-Series Content Gateway ... 823
Forcepoint V-Series Content Gateway sample event messages ... 825

Chapter 66. ForeScout CounterACT ... 827
Syslog log source parameters for ForeScout CounterACT ... 827
Configuring the ForeScout CounterACT Plug-in ... 827
Configuring ForeScout CounterACT Policies ... 828
ForeScout CounterACT sample event messages ... 829

Chapter 67. Fortinet FortiGate Security Gateway ... 831
Configuring a syslog destination on your Fortinet FortiGate Security Gateway device ... 832
Configuring a syslog destination on your Fortinet FortiAnalyzer device ... 833
Fortinet FortiGate Security Gateway sample event messages ... 833
Configuring QRadar to categorize App Ctrl events for Fortinet Fortigate Security Gateway ... 835

Chapter 68. Foundry FastIron ... 837
Configuring syslog for Foundry FastIron ... 837
Syslog log source parameters for Foundry FastIron ... 837

Chapter 69. FreeRADIUS ... 839
Configuring your FreeRADIUS device to communicate with QRadar ... 839

Chapter 70. Generic ... 841
Generic authorization Server ... 841
Configuring event properties for authorization events ... 841
Syslog log source parameters for generic authorization server ... 843
Generic firewall ... 844
Configuring event properties for generic firewall events ... 844
Syslog log source parameters for generic firewall ... 846

Chapter 71. genua genugate ... 849
Configuring genua genugate to send events to QRadar ... 850
genua genugate sample event messages ... 850

Chapter 72. Google ... 853

Google Cloud Audit Logs....853
Google Cloud Audit Logs DSM specifications....853
Configuring Google Cloud Audit Logs to communicate with QRadar....854
Google Cloud Pub/Sub protocol log source parameters for Google Cloud Audit Logs....854
Google Cloud Audit Logs sample event messages....855
Google Cloud Platform - Cloud DNS....857
Google Cloud Platform - Cloud DNS DSM specifications....857
Configuring Google Cloud Platform - Cloud DNS to communicate with QRadar....858
Google Cloud Pub/Sub protocol log source parameters for Google Cloud Platform - Cloud DNS....858
Google Cloud Platform - Cloud DNS sample event message....859
Google Cloud Platform Firewall....859
Google Cloud Platform Firewall DSM specifications....860
Configuring Google Cloud Platform Firewall to communicate with QRadar....860
Google Cloud Pub/Sub log source parameters for Google Cloud Platform Firewall....861
Sample event message....861
Google G Suite Activity Reports....862
Google G Suite Activity Reports DSM specifications....862
Configuring Google G Suite Activity Reports to communicate with QRadar....863
Assigning a role to a user....863
Creating a service account with viewer access....865
Granting API client access to a service account....865
Google G Suite Activity Reports log source parameters....866
Google G Suite Activity Reports sample event messages....866
Troubleshooting Google G Suite Activity Reports....867

Chapter 73. Great Bay Beacon....873
Configuring syslog for Great Bay Beacon....873
Syslog log source parameters for Great Bay Beacon....873

Chapter 74. H3C Technologies....875
H3C Comware Platform....875
Configuring H3C Comware Platform to communicate with QRadar....876

Chapter 75. HBGary Active Defense....877
Configuring HBGary Active Defense....877
Syslog log source parameters for HBGary Active Defense....877

Chapter 76. HCL BigFix (formerly known as IBM BigFix)....879

Chapter 77. Honeycomb Lexicon File Integrity Monitor (FIM)....881
Supported Honeycomb FIM event types logged by QRadar....881
Configuring the Lexicon mesh service....881
Syslog log source parameters for Honeycomb Lexicon File Integrity Monitor....882

Chapter 78. Hewlett Packard Enterprise....885
HPE Network Automation....885
Configuring HPE Network Automation Software to communicate with QRadar....886
HPE ProCurve....887
Syslog log source parameters for HPE ProCurve....888
HPE Tandem....888
HPE Tandem sample event message....889
Hewlett Packard Enterprise UniX (HPE-UX)....890
Syslog log source parameters for Hewlett Packard Enterprise UniX (HPE-UX)....890

Chapter 79. Huawei....893
Huawei AR Series Router....893
Syslog log source parameters for Huawei AR Series Router....893

Configuring Your Huawei AR Series Router....894
Huawei S Series Switch....894
Syslog log source parameters for Huawei S Series Switch....895
Configuring Your Huawei S Series Switch....895
Huawei S Series Switch sample event message....896

Chapter 80. HyTrust CloudControl....897
Configuring HyTrust CloudControl to communicate with QRadar....898

Chapter 81. IBM....899
IBM AIX....899
IBM AIX Server DSM overview....899
IBM AIX Audit DSM overview....901
IBM BigFix Detect....905
IBM CICS....906
Create a log source for near real-time event feed....907
Log File log source parameter....907
IBM Cloud Activity Tracker....911
IBM Cloud Activity Tracker DSM specifications....912
Configuring IBM Cloud Activity Tracker to communicate with QRadar....912
Apache Kafka log source parameters for IBM Cloud Activity Tracker....913
IBM Cloud Activity Tracker sample event messages....914
IBM Cloud Platform (formerly known as IBM Bluemix Platform)....917
Configuring IBM Cloud Platform to communicate with QRadar....918
IBM DataPower....920
Configuring IBM DataPower to communicate with QRadar....921
IBM DB2....921
Create a log source for near real-time event feed....922
Log File log source parameter....923
Integrating IBM DB2 Audit Events....927
Extracting audit data for DB2 v8.x to v9.4....928
Extracting audit data for DB2 v9.5....928
IBM DB2 sample event messages....929
IBM DLC Metrics....929
IBM DLC Metrics DSM specifications....930
Configuring IBM Disconnected Log Collector to communicate with QRadar....930
Forwarded Log source parameters for IBM DLC Metrics....931
IBM DLC Metrics sample event message....932
IBM Federated Directory Server....932
Configuring IBM Federated Directory Server to monitor security events....933
IBM Guardium....934
Creating a syslog destination for events....934
Configuring policies to generate syslog events....935
Installing an IBM Guardium Policy....936
Syslog log source parameters for IBM Guardium....936
Creating an event map for IBM Guardium events....936
Modifying the event map....937
IBM Guardium sample event messages....938
IBM i....939
Configuring IBM i to integrate with IBM QRadar....940
Manually extracting journal entries for IBM i....942
Pulling Data when you use the Log File Protocol....943
Configuring Townsend Security Alliance LogAgent to integrate with QRadar....944
IBM i sample event message....944
IBM IMS....945
Configuring IBM IMS....945
Log File log source parameters for IBM IMS....948
IBM Informix Audit....948

IBM Lotus Domino....949
Setting Up SNMP Services....949
Setting up SNMP in AIX....949
Starting the Domino Server Add-in Tasks....950
Configuring SNMP Services....950
SNMPv2 log source parameters for IBM Lotus Domino....951
IBM Lotus Domino sample event messages....951
IBM MaaS360 Security....952
IBM Fiberlink REST API log source parameters for IBM MaaS360 Security....952
IBM MaaS360 Security sample event message....953
IBM Manage Virtual Server....954
IBM Manage Virtual Server DSM specifications....954
Syslog log source parameters for IBM Manage Virtual Server....954
IBM Manage Virtual Server sample event message....955
IBM Privileged Session Recorder....956
Configuring IBM Privileged Session Recorder to communicate with QRadar....957
JDBC log source parameters for IBM Privileged Session Recorder....958
IBM Proventia....958
IBM Proventia Management SiteProtector....958
JDBC log source parameters for IBM Proventia Management SiteProtector....959
IBM ISS Proventia....960
IBM QRadar Packet Capture....960
Configuring IBM QRadar Packet Capture to communicate with QRadar....962
Configuring IBM QRadar Network Packet Capture to communicate with QRadar....963
IBM QRadar Network Security XGS....963
Configuring IBM QRadar Network Security XGS Alerts....964
Syslog log source parameters for IBM QRadar Network Security XGS....965
IBM RACF....965
Log File log source parameter....966
Create a log source for near real-time event feed....970
Integrate IBM RACF with IBM QRadar by using audit scripts....971
Configuring IBM RACF that uses audit scripts to integrate with IBM QRadar....971
IBM Red Hat OpenShift....973
IBM Red Hat OpenShift DSM specifications....974
Configuring Red Hat OpenShift to communicate with QRadar....974
IBM Red Hat OpenShift Syslog log source parameters....974
IBM Red Hat OpenShift sample event messages....975
IBM SAN Volume Controller....976
Configuring IBM SAN Volume Controller to communicate with QRadar....977
IBM Security Access Manager for Enterprise Single Sign-On....978
Configuring a log server type....978
Configuring syslog forwarding....979
Syslog log source parameters for IBM Security Access Manager for Enterprise Single Sign-On....979
IBM Security Access Manager for Mobile....980
Configuring IBM Security Access Manager for Mobile to communicate with QRadar....982
Configuring IBM IDaaS Platform to communicate with QRadar....983
Configuring an IBM IDaaS console to communicate with QRadar....983
IBM Security Verify Directory....983
IBM Security Verify Directory DSM specifications....984
Configuring IBM Security Verify Directory to communicate with QRadar....984
Syslog log source parameters for IBM Security Verify Directory....986
IBM Security Guardium Insights....986
IBM Security Guardium Insights DSM specifications....987
Syslog log source parameters for IBM Security Guardium Insights....987
Creating an event map for IBM Guardium events....988
Modifying the event map....989
IBM Security Guardium Insights sample event messages....989

IBM Security Identity Governance ... 990
JDBC log source parameters for IBM Security Identity Governance ... 993
IBM Security Identity Manager ... 994
IBM Security Identity Manager JDBC log source parameters for IBM Security Identity Manager ... 994
IBM Security Network IPS (GX) ... 998
Configuring your IBM Security Network IPS (GX) appliance for communication with QRadar ... 999
Syslog log source parameters for IBM Security Network IPS (GX) ... 1000
IBM Security Privileged Identity Manager ... 1000
Configuring IBM Security Privileged Identity Manager to communicate with QRadar ... 1003
IBM Security Privileged Identity Manager sample event message ... 1004
IBM Security QRadar EDR ... 1004
QRadar EDR DSM specifications ... 1005
Configuring QRadar EDR to communicate with QRadar ... 1006
IBM Security QRadar EDR REST API data source parameters for QRadar EDR ... 1006
Configuring QRadar to collect only the first username from the alert ... 1007
QRadar EDR sample event messages ... 1007
IBM Security Randori Recon ... 1008
IBM Security Randori Recon DSM specifications ... 1009
IBM Security Randori REST API protocol log source parameters ... 1009
IBM Security Randori Recon sample event messages ... 1010
IBM Security Trusteer ... 1011
IBM Security Trusteer DSM specifications ... 1011
HTTP Receiver log source parameters for IBM Security Trusteer ... 1012
IBM Security Trusteer sample event messages ... 1012
IBM Security Trusteer Apex Advanced Malware Protection ... 1014
Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar ... 1018
Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar ... 1019
Configuring a Flat File Feed service ... 1021
IBM Security Trusteer Apex Local Event Aggregator ... 1022
Configuring syslog for Trusteer Apex Local Event Aggregator ... 1022
IBM Security Verify (formerly known as IBM Cloud Identity) ... 1023
IBM Security Verify DSM Specifications ... 1023
Configuring QRadar to pull events from IBM Security Verify ... 1024
IBM Security Verify Event Service log source parameters for IBM Security Verify ... 1025
IBM Security Verify sample event messages ... 1025
IBM Sense ... 1029
Configuring IBM Sense to communicate with QRadar ... 1030
IBM SmartCloud Orchestrator ... 1030
Installing IBM SmartCloud Orchestrator ... 1031
IBM SmartCloud Orchestrator log source parameters ... 1031
IBM Tivoli Access Manager for e-business ... 1032
Configuring Tivoli Access Manager for e-business ... 1032
Syslog log source parameters for IBM Tivoli Access Manager for e-business ... 1033
IBM Tivoli Access Manager for e-business sample event message ... 1034
IBM Tivoli Endpoint Manager ... 1034
IBM WebSphere Application Server ... 1034
Configuring IBM WebSphere ... 1034
Customizing the Logging Option ... 1035
Log File log source parameters for IBM WebSphere ... 1035
IBM WebSphere sample event message ... 1039
IBM WebSphere DataPower ... 1039
IBM z/OS ... 1039
Create a log source for near real-time event feed ... 1040
Log File log source parameter ... 1041
IBM zOS sample event message ... 1045

IBM zSecure Alert ... 1045
Syslog log source parameters for IBM zSecure Alert ... 1046

Chapter 82. ISC BIND ... 1047
ISC BIND DSM specifications ... 1048
Syslog log source parameters for ISC BIND ... 1049
ISC BIND sample event message ... 1049

Chapter 83. Illumio Adaptive Security Platform ... 1051
Configuring Illumio Adaptive Security Platform to communicate with QRadar ... 1052
Configuring Exporting Events to Syslog for Illumio PCE ... 1053
Configuring Syslog Forwarding for Illumio PCE ... 1053

Chapter 84. Imperva Incapsula ... 1055
Configuring Imperva Incapsula to communicate with QRadar ... 1056

Chapter 85. Imperva SecureSphere ... 1059
Configuring an alert action for Imperva SecureSphere ... 1060
Configuring a system event action for Imperva SecureSphere ... 1061
Configuring Imperva SecureSphere V11.0 to V13 to send database audit records to QRadar ... 1063

Chapter 86. Infoblox NIOS ... 1065
Infoblox NIOS DSM specifications ... 1065
Infoblox NIOS sample event message ... 1066

Chapter 87. iT-CUBE agileSI ... 1067
Configuring agileSI to forward events ... 1067
SMB Tail log source parameters for iT-CUBE agileSI ... 1068

Chapter 88. Itron Smart Meter ... 1069
Syslog log source parameters for Itron Smart Meter ... 1069

Chapter 89. Juniper Networks ... 1071
Juniper Networks AVT ... 1071
JDBC log source parameters for Juniper Networks AVT ... 1071
Juniper Networks DDoS Secure ... 1072
Juniper Networks DX Application Acceleration Platform ... 1073
Configuring IBM QRadar to receive events from a Juniper DX Application Acceleration Platform ... 1073
Juniper Networks EX Series Ethernet Switch ... 1073
Configuring IBM QRadar to receive events from a Juniper EX Series Ethernet Switch ... 1075
Juniper Networks IDP ... 1075
Configure a log source ... 1075
Juniper Networks Infranet Controller ... 1076
Juniper Networks Firewall and VPN ... 1076
Configuring IBM QRadar to receive events ... 1076
Juniper Networks Firewall sample event message ... 1077
Juniper Networks Junos OS ... 1077
Syslog log source parameters for Juniper Junos OS ... 1079
Configure the PCAP Protocol ... 1079
PCAP Syslog Combination log source parameters for Juniper SRX Series ... 1080
Juniper Junos OS sample event message ... 1080
Juniper Networks Network and Security Manager ... 1080
Configuring Juniper Networks NSM to export logs to syslog ... 1081
Juniper NSM log source parameters for Juniper Networks Network and Security Manager ... 1081
Juniper Networks Secure Access ... 1082
Juniper Networks Security Binary Log Collector ... 1082
Configuring the Juniper Networks Binary Log Format ... 1082

Juniper Security Binary Log Collector log source parameters for Juniper Networks Security Binary Log Collector ... 1083
Juniper Networks Steel-Belted Radius ... 1084
Juniper Networks Steel-Belted Radius DSM specifications ... 1085
Configure Juniper Networks Steel-Belted Radius to forward Windows events to QRadar ... 1086
Configuring Juniper Networks Steel-Belted Radius to forward Syslog events to QRadar ... 1087
Configuring a Juniper Steel-Belted Radius log source by using the Syslog protocol ... 1087
Configuring a Juniper Networks Steel-Belted Radius log source by using the TLS syslog protocol ... 1088
Configuring a Juniper Steel-Belted Radius log source by using the Log File protocol ... 1089
Juniper Steel Belted Radius sample event message ... 1090
Juniper Networks vGW Virtual Gateway ... 1090
Juniper Networks Junos WebApp Secure ... 1091
Configuring syslog forwarding ... 1092
Configuring event logging ... 1092
Syslog log source parameters for Juniper Networks Junos WebApp Secure ... 1094
Juniper Junos WebApp Secure sample event message ... 1094
Juniper Networks WLC Series Wireless LAN Controller ... 1094
Configuring a syslog server from the Juniper WLC user interface ... 1095
Configuring a syslog server with the command-line interface for Juniper WLC ... 1095

Chapter 90. Kisco Information Systems SafeNet/i ... 1097
Configuring Kisco Information Systems SafeNet/i to communicate with QRadar ... 1098

Chapter 91. Kubernetes Auditing ... 1101
Kubernetes Auditing DSM specifications ... 1101
Configuring Kubernetes Auditing to communicate with QRadar ... 1102
Kubernetes Auditing log source parameters ... 1103
Kubernetes Auditing sample event message ... 1103

Chapter 92. Lastline Enterprise ... 1105
Configuring Lastline Enterprise to communicate with QRadar ... 1106

Chapter 93. Lieberman Random Password Manager ... 1107

Chapter 94. LightCyber Magna ... 1109
Configuring LightCyber Magna to communicate with QRadar ... 1110

Chapter 95. Linux ... 1113
Linux DHCP Server ... 1113
Linux DHCP Server DSM specifications ... 1113
Syslog log source parameters for Linux DHCP ... 1114
Linux DHCP Server sample event message ... 1114
Linux IPtables ... 1114
Configuring IPtables ... 1115
Syslog log source parameters for Linux IPtables ... 1116
Linux OS ... 1116
Configuring syslog on Linux OS ... 1117
Configuring syslog-ng on Linux OS ... 1117
Configuring Linux OS to send audit logs ... 1118
Linux OS Sample event messages ... 1119

Chapter 96. LOGbinder ... 1121
LOGbinder EX event collection from Microsoft Exchange Server ... 1121
Configuring your LOGbinder EX system to send Microsoft Exchange event logs to QRadar ... 1122
LOGbinder SP event collection from Microsoft SharePoint ... 1122
Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar ... 1123
LOGbinder SQL event collection from Microsoft SQL Server ... 1124

Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar 1125

Chapter 97. McAfee 1127
JDBC log source parameters for McAfee Application/Change Control 1127
McAfee ePolicy Orchestrator 1128
Configuring SNMP notifications on McAfee ePolicy Orchestrator 1131
Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator 1132
Installing the Java Cryptography Extension on QRadar 1133
McAfee ePolicy Orchestrator sample event messages 1133
McAfee MVISION Cloud (formerly known as Skyhigh Networks Cloud Security Platform) 1134
Configuring McAfee MVISION Cloud to communicate with QRadar 1135
McAfee MVISION Cloud sample event messages 1136
McAfee Network Security Platform (formerly known as McAfee Intrushield) 1136
McAfee Network Security Platform DSM specifications 1137
Configuring alert events for McAfee Network Security Platform 2.x - 5.x 1138
Configuring alert events for McAfee Network Security Platform 6.x - 7.x 1139
Configuring alert events for McAfee Network Security Platform 8.x - 10.x 1141
Configuring fault notification events for McAfee Network Security Platform 6.x - 7.x 1143
Configuring fault notification events for McAfee Network Security Platform 8.x - 10.x 1144
McAfee Network Security Platform sample event messages 1145
McAfee Web Gateway 1146
McAfee Web Gateway DSM integration process 1147
Configuring McAfee Web Gateway to communicate with QRadar (syslog) 1147
Importing the Syslog Log Handler 1148
Configuring McAfee Web Gateway to communicate with IBM QRadar (log file protocol) 1148
Pulling data by using the log file protocol 1149
Creation of an event map for McAfee Web Gateway events 1150
Discovering unknown events 1150
Modifying the event map 1150
McAfee Web Gateway sample event message 1151

Chapter 98. MetaInfo MetaIP 1153

Chapter 99. Microsoft 1155
Microsoft 365 Defender 1155
Microsoft 365 Defender DSM Specifications 1156
Microsoft Defender for Endpoint SIEM REST API log source parameters 1158
Microsoft Azure Event Hubs log source parameters 1159
Microsoft Graph Security API log source parameters 1159
Microsoft 365 Defender sample event messages 1160
Microsoft Entra ID 1163
Microsoft Entra ID DSM specifications 1164
Microsoft Entra ID log source parameters 1164
Microsoft Entra ID sample event messages 1165
Microsoft Azure Platform 1166
Microsoft Azure Platform DSM specifications 1167
Microsoft Azure log source parameters for Microsoft Azure Event Hubs 1167
Microsoft Azure Platform sample event messages 1168
Microsoft Defender for Cloud 1170
Microsoft Defender for Cloud DSM specifications 1171
Microsoft Graph Security API protocol log source parameters for Microsoft Defender for Cloud 1171
Microsoft Azure Event Hubs protocol log source parameters for Microsoft Defender for Cloud 1172
Microsoft Defender for Cloud sample event message 1173
Microsoft DHCP Server 1176
Microsoft DHCP Server sample event message 1177
Microsoft DNS Debug 1178

Enabling DNS debugging on Windows Server... 1178
Microsoft DNS Debug sample event message... 1179
Microsoft Endpoint Protection... 1179
Creating a database view... 1180
JDBC log source parameters for predefined database queries... 1181
Microsoft Exchange Server... 1184
Configuring Microsoft Exchange Server to communicate with QRadar... 1184
Microsoft Exchange Server log source parameters for Microsoft Exchange... 1187
Microsoft Exchange Server sample event message... 1189
Microsoft Hyper-V... 1190
Microsoft Hyper-V DSM integration process... 1191
WinCollect log source parameters for Microsoft Hyper-V... 1191
Microsoft IAS Server... 1192
Microsoft IIS Server... 1192
Configuring Microsoft IIS by using the IIS Protocol... 1193
Microsoft IIS log source parameters for Microsoft IIS Server... 1194
Syslog log source parameters for Microsoft IIS Server... 1194
Microsoft IIS Server sample event messages... 1195
Microsoft ISA... 1196
Microsoft Office 365... 1196
Configuring a Microsoft Office 365 account in Microsoft Azure Active Directory... 1199
Microsoft Office 365 sample event messages... 1200
Microsoft Office 365 Message Trace... 1201
Microsoft Office 365 Message Trace DSM specifications... 1202
Microsoft Office Message Trace REST API log source parameters for Microsoft Office Message Trace... 1202
Microsoft Office 365 Message Trace sample event message... 1203
JDBC log source parameters for Microsoft Operations Manager... 1204
Microsoft SharePoint... 1205
Configuring Microsoft SharePoint audit events... 1205
Creating a database view for Microsoft SharePoint... 1206
Creating read-only permissions for Microsoft SharePoint database users... 1206
JDBC log source parameters for Microsoft Share Point... 1207
JDBC log source parameters for Microsoft SharePoint with predefined database queries... 1208
Microsoft SQL Server... 1210
Microsoft SQL Server preparation for communication with QRadar... 1211
JDBC log source parameters for Microsoft SQL Server... 1213
Microsoft SQL Server sample event message... 1214
JDBC log source parameters for Microsoft System Center Operations Manager... 1214
Microsoft Windows Security Event Log... 1216
Installing the MSRPC protocol on the QRadar Console... 1216
MSRPC parameters on Windows hosts... 1217
WMI parameters on Windows hosts... 1220
Installing Winlogbeat and Logstash on a Windows host... 1220
Configuring which usernames QRadar considers to be system users in events that are collected... 1222
Configuring IBM QRadar to parse XML level tag for application events... 1223
Microsoft Windows Security Event Log sample event messages... 1223

Chapter 100. Motorola Symbol AP... 1227
Syslog log source parameters for Motorola SymbolAP... 1227
Configure syslog events for Motorola Symbol AP... 1227

Chapter 101. Name Value Pair... 1229

Chapter 102. NCC Group DDoS Secure... 1233
Configuring NCC Group DDoS Secure to communicate with QRadar... 1234

Chapter 103. NetApp Data ONTAP 1235

Chapter 104. Netgate pfSense 1237
Netgate pfSense DSM specifications 1237
Configuring Netgate pfSense to communicate with QRadar 1238
Syslog log source parameters for Netgate pfSense 1239
Netgate pfSense sample event messages 1239

Chapter 105. Netskope Active 1241
Netskope Active REST API log source parameters for Netskope Active 1242
Netskope Active sample event messages 1242

Chapter 106. NGINX HTTP Server 1245
NGINX HTTP Server DSM specifications 1245
Configuring NGINX HTTP Server to communicate with QRadar 1246
NGINX HTTP Server sample event messages 1246

Chapter 107. Niksun 1249

Chapter 108. Nokia Firewall 1251
Integration with a Nokia Firewall by using syslog 1251
Configuring IPtables 1251
Configuring syslog 1252
Configuring the logged events custom script 1252
Syslog log source parameters for Nokia Firewall 1252
Integration with a Nokia Firewall by using OPSEC 1253
Configuring a Nokia Firewall for OPSEC 1253
OPSEC/LEA log source parameters for Nokia FireWall 1254

Chapter 109. Nominum Vantio 1255

Chapter 110. Nortel Networks 1257
Nortel Multiprotocol Router 1257
Nortel Application Switch 1259
Nortel Contivity 1260
Nortel Ethernet Routing Switch 2500/4500/5500 1261
Nortel Ethernet Routing Switch 8300/8600 1261
Nortel Secure Router 1262
Nortel Secure Network Access Switch 1264
Nortel Switched Firewall 5100 1264
Integrating Nortel Switched Firewall by using syslog 1264
Integrate Nortel Switched Firewall by using OPSEC 1265
Configuring a log source 1265
Nortel Switched Firewall 6000 1266
Configuring syslog for Nortel Switched Firewalls 1266
Configuring OPSEC for Nortel Switched Firewalls 1267
Reconfiguring the Check Point SmartCenter Server 1267
Nortel Threat Protection System (TPS) 1268
Nortel VPN Gateway 1268

Chapter 111. Novell eDirectory 1271
Configuring XDASv2 to forward events 1271
Loading the XDASv2 Module 1272
Loading the XDASv2 on a Linux Operating System 1272
Loading the XDASv2 on a Windows Operating System 1273
Configuring event auditing using Novell iManager 1273
Configuring a log source 1274

Novell eDirectory sample event message....1274

Chapter 112. Observe IT JDBC....1277

Chapter 113. Okta....1283

Chapter 114. Onapsis Security Platform....1287
Configuring Onapsis Security Platform to communicate with QRadar....1288

Chapter 115. OpenBSD....1289
Syslog log source parameters for OpenBSD....1289
Configuring syslog for OpenBSD....1289

Chapter 116. Open LDAP....1291
UDP Multiline Syslog log source parameters for Open LDAP....1291
Configuring IPtables for UDP Multiline Syslog events....1292
Configuring event forwarding for Open LDAP....1294
Configuring QRadar for users to use OP code instead of connection number....1294

Chapter 117. Open Source SNORT....1295
Configuring Open Source SNORT....1295
Syslog log source parameters for Open Source SNORT....1296

Chapter 118. OpenStack....1297
Configuring OpenStack to communicate with QRadar....1299

Chapter 119. Oracle....1301
Oracle Acme Packet Session Border Controller....1301
Supported Oracle Acme Packet event types that are logged by IBM QRadar....1301
Syslog log source parameters for Oracle Acme Packet SBC....1301
Configuring SNMP to syslog conversion on Oracle Acme Packet SBC....1302
Enabling syslog settings on the media manager object....1302
Oracle Audit Vault....1303
Configuring Oracle Audit Vault to communicate with QRadar....1307
Oracle BEA WebLogic....1307
Enabling event logs....1307
Configuring domain logging....1308
Configuring application logging....1308
Configuring an audit provider....1308
Log file log source parameters for Oracle BEA WebLogic....1309
Oracle BEA WebLogic sample event messages....1309
Oracle RDBMS Audit Record....1310
Enabling Unified Auditing in Oracle 12c....1316
Configuring an Oracle database server to send audit logs to QRadar....1316
Oracle DB Listener....1318
Oracle Database Listener log source parameters....1318
Collecting Oracle database events by using Perl....1318
Configuring the Oracle Database Listener within QRadar....1320
Oracle Directory Server overview....1321
Oracle Enterprise Manager....1321
Oracle Fine Grained Auditing....1323
JDBC log source parameters for Oracle Fine Grained Auditing....1323
Oracle RDBMS OS Audit Record....1324
Oracle RDBMS OS Audit Record DSM specifications....1325
Configuring Oracle RDBMS OS Audit Record to communicate with QRadar....1325
Syslog log source parameters for Oracle RDBMS OS Audit Record....1327
Log File log source parameters for Oracle RDBMS OS Audit Record....1328
Sample event message....1328

Chapter 120. osquery....1331
osquery DSM specifications....1332
Configuring rsyslog on your Linux system....1332
Configuring osquery on your Linux system....1333
osquery log source parameters....1334
osquery sample event message....1334

Chapter 121. OSSEC....1337
Configuring OSSEC....1337
Syslog log source parameters for OSSEC....1337

Chapter 122. Palo Alto Networks....1339
Palo Alto Endpoint Security Manager....1339
Configuring Palo Alto Endpoint Security Manager to communicate with QRadar....1340
Palo Alto Networks PA Series....1341
Palo Alto PA DSM specifications....1341
Configuring Syslog or LEEF formatted events on your Palo Alto PA Series device....1342
Forwarding Palo Alto Cortex Data Lake (Next Generation Firewall) LEEF events to IBM QRadar....1352
Creating a forwarding policy on your Palo Alto PA Series device....1352
Configuring Palo Alto Networks firewall to send ArcSight CEF formatted Syslog events....1353
TLS Syslog log source parameters for Palo Alto PA Series....1354
Palo Alto PA Series Sample event message....1355

Chapter 123. PingFederate....1359
PingFederate DSM specifications....1359
Configuring PingFederate to communicate with IBM QRadar....1359
Syslog log source parameters for PingFederate....1360
PingFederate sample event message....1360

Chapter 124. Pirean Access: One....1363
JDBC log source parameters for Pirean Access: One....1363

Chapter 125. PostFix Mail Transfer Agent....1367
Configuring syslog for PostFix Mail Transfer Agent....1367
UDP Multiline Syslog log source parameters for PostFix MTA....1367
Configuring IPtables for multiline UDP syslog events....1369
PostFix Mail Transfer Agent sample event messages....1369

Chapter 126. ProFTPd....1373
Configuring ProFTPd....1373
Syslog log source parameters for ProFTPd....1373

Chapter 127. Proofpoint Enterprise Protection and Enterprise Privacy....1375
Configuring Proofpoint Enterprise Protection and Enterprise Privacy DSM to communicate with IBM QRadar....1376
Syslog log source parameters for Proofpoint Enterprise Protection and Enterprise Privacy....1376
Proofpoint Enterprise Protection and Enterprise Privacy sample event messages....1377

Chapter 128. Pulse Secure....1379
Pulse Secure Infranet Controller....1379
Syslog log source parameters for Pulse Secure Infranet Controller....1379
Pulse Secure Pulse Connect Secure....1379
Configuring a Pulse Secure Pulse Connect Secure device to send WebTrends Enhanced Log File (WELF) events to IBM QRadar....1381
Configuring a Pulse Secure Pulse Connect Secure device to send syslog events to QRadar....1382
Pulse Secure Pulse Connect Secure sample event message....1382

Chapter 129. Radware ... 1385
Radware AppWall ... 1385
Configuring Radware AppWall to communicate with QRadar ... 1386
Increasing the maximum TCP Syslog payload length for Radware AppWall ... 1387
Radware AppWall sample event messages ... 1387
Radware DefensePro ... 1388
Syslog log source parameters for Radware DefensePro ... 1388

Chapter 130. Raz-Lee iSecurity ... 1389
Configuring Raz-Lee iSecurity to communicate with QRadar ... 1389
Syslog log source parameters for Raz-Lee iSecurity ... 1391

Chapter 131. Redback ASE ... 1393
Configuring Redback ASE ... 1393
Syslog log source parameters for Redback ASE ... 1393

Chapter 132. Red Hat Advanced Cluster Security for Kubernetes ... 1395
Red Hat Advanced Cluster Security for Kubernetes DSM specifications ... 1395
Configuring Red Hat Advanced Cluster Security for Kubernetes to communicate with QRadar ... 1396
HTTP Receiver log source parameters for Red Hat Advanced Cluster Security for Kubernetes ... 1396
Red Hat Advanced Cluster Security for Kubernetes sample event messages ... 1397

Chapter 133. Resolution1 CyberSecurity ... 1399
Configuring your Resolution1 CyberSecurity device to communicate with QRadar ... 1400
Log file log source parameters for Resolution1 CyberSecurity ... 1400

Chapter 134. Riverbed ... 1401
Riverbed SteelCentral NetProfiler (Cascade Profiler) Audit ... 1401
Creating a Riverbed SteelCentral NetProfiler report template and generating an audit file ... 1402
Riverbed SteelCentral NetProfiler (Cascade Profiler) Alert ... 1403
Configuring your Riverbed SteelCentral NetProfiler system to enable communication with QRadar ... 1405

Chapter 135. RSA Authentication Manager ... 1407
Configuration of syslog for RSA Authentication Manager 6.x, 7.x and 8.x ... 1407
Configuring Linux ... 1407
Configuring Windows ... 1408
Configuring the log file protocol for RSA Authentication Manager 6.x and 7.x ... 1408
Log File log source parameters for RSA Authentication Manager ... 1409
Configuring RSA Authentication Manager 6.x ... 1409
Configuring RSA Authentication Manager 7.x ... 1410

Chapter 136. SafeNet DataSecure ... 1411
Configuring SafeNet DataSecure to communicate with QRadar ... 1411

Chapter 137. Salesforce ... 1413
Salesforce Security ... 1413
Configuring the Salesforce Security Monitoring server to communicate with QRadar ... 1414
Salesforce REST API log source parameters for Salesforce Security ... 1414
Salesforce Security Auditing ... 1415
Downloading the Salesforce audit trail file ... 1416
Log File log source parameters for Salesforce Security Auditing ... 1416

Chapter 138. Samhain Labs ... 1419
Configuring syslog to collect Samhain events ... 1419
JDBC log source parameters for Samhain ... 1420
JDBC protocol configuration options ... 1421

Chapter 139. SAP Enterprise Threat Detection....1427
SAP Enterprise Threat Detection DSM specifications....1427
SAP Enterprise Threat Detection Alert API log source parameters for SAP Enterprise Threat Detection....1428
Creating a pattern filter on the SAP server....1429
Troubleshooting the SAP Enterprise Threat Detection Alert API....1430
SAP Enterprise Threat Detection V1.0 SP6 sample event messages....1431
SAP Enterprise Threat Detection V2.0 SP5 sample event messages....1440

Chapter 140. Seculert....1445

Chapter 141. Sentrigo Hedgehog....1447

Chapter 142. Snowflake....1449
Snowflake DSM specifications....1449
Snowflake sample event message....1449

Chapter 143. SolarWinds Orion....1453
Configuring SolarWinds Orion to communicate with QRadar....1454
SNMP log source parameters for SolarWinds Orion....1456
Installing the Java Cryptography Extension on QRadar....1457
Solar Winds Orion sample event message....1457

Chapter 144. SonicWALL....1459
Configuring SonicWALL to forward syslog events....1459
Syslog log source parameters for SonicWALL....1459
SonicWALL sample event messages....1460

Chapter 145. Sophos....1461
Sophos Enterprise Console....1461
Sophos Enterprise Console DSM specifications....1461
Configuring the database view for Sophos Enterprise Console....1462
Sophos Enterprise Console JDBC log source parameters for Sophos Enterprise Console....1462
JDBC log source parameters for Sophos Enterprise Console....1463
Sophos PureMessage....1464
Integrating QRadar with Sophos PureMessage for Microsoft Exchange....1464
JDBC log source parameters for Sophos PureMessage....1464
Integrating QRadar with Sophos PureMessage for Linux....1465
JDBC log source parameters for Sophos PureMessage for Microsoft Exchange....1466
Sophos Astaro Security Gateway....1467
Sophos Astaro Security Gateway sample event messages....1468
Sophos Web Security Appliance....1469

Chapter 146. Sourcefire Intrusion Sensor....1471
Configuring Sourcefire Intrusion Sensor....1471
Syslog log source parameters for Sourcefire Intrusion Sensor....1471

Chapter 147. Splunk....1473
Collecting Windows events that are forwarded from Splunk....1473
TCP Multiline Syslog log source parameters for Splunk....1473

Chapter 148. Squid Web Proxy....1475
Configuring syslog forwarding....1475
Syslog log source parameters for Squid Web Proxy....1476
Squid Web Proxy sample event messages....1476

Chapter 149. SSH CryptoAuditor....1479

Configuring an SSH CryptoAuditor appliance to communicate with QRadar....1480

Chapter 150. Starent Networks....1481

Chapter 151. STEALTHbits....1485
STEALTHbits StealthINTERCEPT....1485
Syslog log source parameters for STEALTHbits StealthINTERCEPT....1485
Configuring your STEALTHbits StealthINTERCEPT to communicate with QRadar....1486
Configuring your STEALTHbits File Activity Monitor to communicate with QRadar....1486
Syslog log source parameters for STEALTHbits File Activity Monitor....1487
STEALTHbits StealthINTERCEPT Alerts....1487
Collecting alerts logs from STEALTHbits StealthINTERCEPT....1488
STEALTHbits StealthINTERCEPT Analytics....1488
Collecting analytics logs from STEALTHbits StealthINTERCEPT....1489

Chapter 152. Sun....1491
Sun ONE LDAP....1491
Enabling the event log for Sun ONE Directory Server....1491
Log File log source parameters for Sun ONE LDAP....1492
UDP Multiline Syslog log source parameters for Sun ONE LDAP....1495
Configuring IPtables for UDP Multiline Syslog events....1495
Sun Solaris Basic Security Mode (BSM)....1497
Enabling Basic Security Mode in Solaris 10....1497
Enabling Basic Security Mode in Solaris 11....1498
Converting Sun Solaris BSM audit logs....1498
Creating a cron job....1499
Log File log source parameters for Sun Solaris BSM....1499
Sun Solaris DHCP....1502
Syslog log source parameters for Sun Solaris DHCP....1503
Configuring Sun Solaris DHCP to communicate with QRadar....1503
Sun Solaris OS....1504
Sun Solaris OS DSM specifications....1504
Configuring Sun Solaris OS to communicate with QRadar....1505
Syslog log source parameters for Sun Solaris OS....1505
Sun Solaris OS sample event messages....1506
Sun Solaris Sendmail....1507
Syslog log source parameters for Sun Solaris Sendmail....1507

Chapter 153. Suricata....1509
Suricata DSM specifications....1509
Configuring Suricata to communicate with QRadar....1510
Syslog log source parameters for Suricata....1510
TLS Syslog log source parameters for Suricata....1511
Suricata sample event message....1511

Chapter 154. Sybase ASE....1513
JDBC log source parameters for Sybase ASE....1513

Chapter 155. Symantec....1517
Symantec Critical System Protection....1517
Symantec Data Loss Prevention (DLP)....1520
Creating an SMTP response rule....1521
Creating a None Of SMTP response rule....1521
Configuring a log source....1522
Event map creation for Symantec DLP events....1523
Discovering unknown events....1523
Modifying the event map....1523
Symantec Endpoint Protection....1524

Configuring Symantec Endpoint Protection to Communicate with QRadar ... 1525
Symantec Endpoint Protection sample event messages ... 1526
Symantec Encryption Management Server ... 1527
Configuring Symantec Encryption Management Server to communicate with QRadar ... 1527
Syslog log source parameters for Symantec Encryption Management Servers ... 1528
Symantec SGS ... 1528
Syslog log source parameters for Symantec SGS ... 1528
Symantec System Center ... 1529
Configuring a database view for Symantec System Center ... 1529
JDBC log source parameters for Symantec System Center ... 1530

Chapter 156. SysFlow ... 1533
SysFlow DSM specifications ... 1533
Configuring SysFlow agent to communicate with QRadar ... 1534
Syslog log source parameters for SysFlow ... 1534
SysFlow sample event message ... 1535

Chapter 157. ThreatGRID Malware Threat Intelligence Platform ... 1537
Supported event collection protocols for ThreatGRID Malware Threat Intelligence ... 1537
ThreatGRID Malware Threat Intelligence configuration overview ... 1537
Syslog log source parameters for ThreatGRID Malware Threat Intelligence Platform ... 1537
Log File log source parameters for ThreatGRID Malware Threat Intelligence Platform ... 1539

Chapter 158. TippingPoint ... 1543
TippingPoint Intrusion Prevention System ... 1543
Configuring remote syslog for SMS ... 1543
Configuring notification contacts for LSM ... 1544
Configuring an Action Set for LSM ... 1544
TippingPoint X505/X506 Device ... 1545
Configuring your TippingPoint X506/X506 device to communicate with QRadar ... 1545
TippingPoint Intrusion Prevention System sample event message ... 1546

Chapter 159. Top Layer IPS ... 1547

Chapter 160. Townsend Security LogAgent ... 1549
Configuring Raz-Lee iSecurity ... 1549
Syslog log source parameters for Raz-Lee i Security ... 1549

Chapter 161. Trend Micro ... 1551
Trend Micro Apex Central ... 1551
Trend Micro Apex Central DSM specifications ... 1551
Configuring Trend Micro Apex Central to communicate with QRadar ... 1552
Syslog log source parameters for Trend Micro Apex Central ... 1553
TLS Syslog log source parameters for Trend Micro Apex Central ... 1554
Trend Micro Apex Central sample event messages ... 1554
Trend Micro Apex One ... 1555
Integrating with Trend Micro Apex One 8.x ... 1555
Integrating with Trend Micro Apex One 10.x ... 1556
Integrating with Trend Micro Apex One XG ... 1558
Changing the date format in QRadar to match the date format for your Trend Micro Apex One device ... 1559
SNMPv2 log source parameters for Trend Micro Apex One ... 1560
Trend Micro Control Manager ... 1561
SNMPv1 log source parameters for Trend Micro Control Manager ... 1561
SNMPv2 log source parameters for Trend Micro Control Manager ... 1561
SNMPv3 log source parameters for Trend Micro Control Manager ... 1562
Configuring SNMP traps ... 1563
Trend Micro Deep Discovery Analyzer ... 1563

Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar....1564
Trend Micro Deep Discovery Director....1565
Trend Micro Deep Discovery Director DSM specifications....1566
Configuring Trend Micro Deep Discovery Director to communicate with QRadar....1566
Trend Micro Deep Discovery Director sample event messages....1567
Trend Micro Deep Discovery Email Inspector....1568
Configuring Trend Micro Deep Discovery Email Inspector to communicate with QRadar....1569
Trend Micro Deep Discovery Inspector....1570
Configuring Trend Micro Deep Discovery Inspector V3.0 to send events to QRadar....1571
Configuring Trend Micro Deep Discovery Inspector V3.8, V5.0 and V5.1 to send events to QRadar....1572
Trend Micro Deep Security....1572
Configuring Trend Micro Deep Security to communicate with QRadar....1573
Trend Micro Deep Security sample event message....1574

Chapter 162. Tripwire....1575

Chapter 163. Tropos Control....1577

Chapter 164. Universal CEF....1579
Configuring event mapping for Universal CEF events....1579

Chapter 165. Universal LEEF....1581
Syslog protocol log source parameters for Universal LEEF....1581
Forwarding events to IBM QRadar....1581
Universal LEEF event map creation....1582
Discovering unknown events....1582
Modifying an event map....1582

Chapter 166. Vectra Networks Vectra....1585
Configuring Vectra Networks Vectra to communicate with QRadar....1586
Vectra Networks Vectra sample event messages....1586

Chapter 167. Venustech Venusense....1589
Venusense configuration overview....1589
Configuring a Venusense syslog server....1589
Configuring Venusense event filtering....1589
Syslog log source parameters for Venustech Venusense....1590

Chapter 168. Verdasys Digital Guardian....1591
Configuring IPtables....1592
Configuring a data export....1593
Syslog log source parameters for Verdasys Digital Guardian....1594

Chapter 169. Vericept Content 360 DSM....1595

Chapter 170. VMware....1597
VMware AppDefense....1597
VMware AppDefense DSM specifications....1597
Configuring VMware AppDefense to communicate with QRadar....1598
VMWare AppDefense API log source parameters for VMware AppDefense....1598
VMware AppDefense sample event messages....1599
VMware Carbon Black App Control (formerly known as Carbon Black Protection)....1601
VMware Carbon Black App Control DSM specifications....1602
Configuring VMware Carbon Black App Control to communicate with QRadar....1602
Syslog log source parameters for VMware Carbon Black App Control....1603
VMware Carbon Black App Control sample event messages....1603

VMware ESX and ESXi....1604
Configuring syslog on VMware ESX and ESXi servers....1605
Enabling syslog firewall settings on vSphere Clients....1605
Syslog log source parameters for VMware ESX or ESXi....1606
Configuring the EMC VMWare protocol for ESX or ESXi servers....1607
Creating an account for QRadar in ESX....1607
Configuring read-only account permissions....1608
EMC VMWare log source parameters for VMware ESX or ESXi....1608
EMC VMWare sample event messages....1609
VMware vCenter....1610
EMC VMWare log source parameters for VMware vCenter....1610
VMware vCenter sample event message....1611
VMware vCloud Director....1611
Configuring the vCloud REST API public address....1612
Supported VMware vCloud Director event types logged by IBM QRadar....1612
VMware vCloud Director log source parameters for VMware vCloud Director....1612
VMware vShield....1613
VMware vShield DSM integration process....1614
Configuring your VMware vShield system for communication with IBM QRadar....1614
Syslog log source parameters for VMware vShield....1615

Chapter 171. Vormetric Data Security....1617
Vormetric Data Security DSM integration process....1617
Configuring your Vormetric Data Security systems for communication with IBM QRadar....1618
Configuring Vormetric Data Firewall FS Agents to bypass Vormetric Data Security Manager....1618
Syslog log source parameters for Vormetric Data Security....1619

Chapter 172. WatchGuard Fireware OS....1621
Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar....1622
Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar....1622
Syslog log source parameters for WatchGuard Fireware OS....1623

Chapter 173. Websense....1625

Chapter 174. Zscaler Nanolog Streaming Service....1627
Zscaler NSS DSM specifications....1628
Syslog log source parameters for Zscaler NSS....1628
HTTP Receiver log source parameters for Zscaler NSS....1629
Zscaler NSS sample event messages....1630

Chapter 175. Zscaler Private Access....1633
Zscaler Private Access DSM specifications....1633
Configuring Zscaler Private Access to send events to QRadar....1634
Syslog log source parameters for Zscaler Private Access....1635
Zscaler Private Access sample event messages....1635

Chapter 176. QRadar supported DSMs....1637

Chapter 177. DSMs supported by third-party vendors....1657

Notices....1663
Trademarks....1664
Terms and conditions for product documentation....1664
IBM Online Privacy Statement....1665
General Data Protection Regulation....1665

Privacy policy considerations 1666
Glossary..... 1667
A..... 1667
B..... 1667
C..... 1668
D..... 1668
E..... 1669
F..... 1669
G..... 1669
H..... 1669
I..... 1670
K..... 1670
L..... 1670
M..... 1671
N..... 1671
O..... 1672
P..... 1672
Q..... 1672
R..... 1672
S..... 1673
T..... 1674
V..... 1674
W..... 1674

About this DSM Configuration Guide

The DSM Configuration guide provides instructions about how to collect data from your third-party devices, also known as log sources.

You can configure IBM® QRadar® to accept event logs from log sources that are on your network. A *log source* is a data source that creates an event log.

Note: This guide describes the Device Support Modules (DSMs) that are produced by IBM. Third-party DSMs are available on the IBM App Exchange, but are not documented here.

Intended audience

System administrators must have QRadar access, knowledge of the corporate network security concepts and device configurations.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport).

Contacting customer support

For information about contacting customer support, see QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Part 1. QRadar DSM installation and log source management

Chapter 1. Event collection from third-party devices

To configure event collection from third-party devices, you need to complete configuration tasks on the third-party device, and your QRadar Console, Event Collector, or Event Processor. The key components that work together to collect events from third-party devices are log sources, DSMs, and automatic updates.

Log sources

A *log source* is any external device, system, or cloud service that is configured to either send events to your IBM QRadar system or be collected by your QRadar system. QRadar shows events from log sources in the **Log Activity** tab.

To receive raw events from log sources, QRadar supports several protocols, including syslog from OS, applications, firewalls, IPS/IDS, SNMP, SOAP, JDBC for data from database tables and views. QRadar also supports proprietary vendor-specific protocols such as OPSEC/LEA from Checkpoint.

DSMs

A *Device Support Module (DSM)* is a code module that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output. Each type of log source has a corresponding DSM. For example, the IBM Fiberlink MaaS360 DSM parses and normalizes events from an IBM Fiberlink MaaS360 log source.

Automatic Updates

QRadar provides daily and weekly automatic updates on a recurring schedule. The weekly automatic update includes new DSM releases, corrections to parsing issues, and protocol updates. For more information about automatic updates, see the *IBM QRadar Administration Guide*.

Third-party device installation process

To collect events from third-party device, you must complete installation and configuration steps on both the log source device and your QRadar system. For some third-party devices, extra configuration steps are needed, such as configuring a certificate to enable communication between that device and QRadar.

The following steps represent a typical installation process:

1. Read the specific instructions for how to integrate your third-party device.
2. Download and install the RPM for your third-party device. RPMs are available for download from the IBM support website (http://www.ibm.com/support).

   Tip: If your QRadar system is configured to accept automatic updates, this step might not be required.
3. Configure the third-party device to send events to QRadar.

   After some events are received, QRadar automatically detects some third-party devices and creates a log source configuration. The log source is listed on the Log Sources list and contains default information. You can customize the information.
4. If QRadar does not automatically detect the log source, manually add a log source. The list of supported DSMs and the device-specific topics indicate which third-party devices are not automatically detected.
5. Deploy the configuration changes and restart your web services.

Custom log source types for unsupported third-party log sources

After the events are collected and before the correlation can begin, individual events from your devices must be properly normalized. *Normalization* means to map information to common field names, such

as event name, IP addresses, protocol, and ports. If an enterprise network has one or more network or security devices that QRadar does not provide a corresponding DSM, you can use a custom log source type. QRadar can integrate with most devices and any common protocol sources by using a custom log source type.

For more information, see the *IBM QRadar Administration Guide*.

Adding a DSM

If your Device Support Module (DSM) is not automatically discovered, manually install a DSM.

Each type of log source has a corresponding DSM that parses and normalizes events from the log source.

Procedure

1. Download the DSM RPM file from the IBM support website (http://www.ibm.com/support).
2. Copy the RPM file to QRadar.
3. Using SSH, log in to the QRadar host as the root user.
4. Go to the directory that includes the downloaded file.
5. Type the following command:

   `yum -y install <rpm_filename>`

   Note: The `rpm -Uvh <rpm_filename>` command line to install was replaced with the `yum -y install <rpm_filename>` command.
6. Log in to QRadar.
7. On the **Admin** tab, click **Deploy Changes**.

   Restriction: Uninstalling a Device Support Module (DSM) is not supported in QRadar.

Chapter 2. Introduction to log source management

You can configure IBM QRadar to accept event logs from log sources that are on your network. A *log source* is a data source that creates an event log.

For example, a firewall or intrusion protection system (IPS) logs security-based events, and switches or routers logs network-based events.

To receive raw events from log sources, QRadar supports many protocols. *Passive protocols* listen for events on specific ports. *Active protocols* use APIs or other communication methods to connect to external systems that poll and retrieve events.

Depending on your license limits, QRadar can read and interpret events from more than 300 log sources.

To configure a log source for QRadar, you must do the following tasks:

1. Download and install a device support module (DSM) that supports the log source. A *DSM* is software application that contains the event patterns that are required to identify and parse events from the original format of the event log to the format that QRadar can use.
2. If automatic discovery is supported for the DSM, wait for QRadar to automatically add the log source to your list of configured log sources.
3. If automatic discovery is not supported for the DSM, manually create the log source configuration.

Related tasks

"Adding a log source" on page 5
"Adding bulk log sources" on page 8
"Adding a log source parsing order" on page 11
You can assign a priority order for when the events are parsed by the target event collector.
"Adding a DSM" on page 4

Adding a log source

If the log source is not automatically discovered, manually add it by using the QRadar Log Source Management app so that you can receive events from your network devices or appliances.

If you are using QRadar 7.3.1 to 7.5.0 Update Package 3, you can also add a log source by using the Log Sources icon. In QRadar 7.5.0 Update Package 4 and later, when you click the **Log Sources** icon, the QRadar Log Source Management app opens.

Before you begin

Ensure that the QRadar Log Source Management app is installed on your QRadar Console. For more information about installing the app, see Installing the QRadar Log Source Management app.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. To open the app, click the **QRadar Log Source Management** app icon.
4. Click **New Log Source** > **Single Log Source**.
5. On the **Select a Log Source Type** page, select a log source type, and click **Select Protocol Type**.
6. On the **Select a Protocol Type** page, select a protocol, and click **Configure Log Source Parameters**.
7. On the **Configure the Log Source parameters** page, configure the log source parameters, and click **Configure Protocol Parameters**.

   The following table describes the common log source parameters for all log source types:

Table 1. Common log source parameters	
Parameter	**Description**
Enabled	When this option is not enabled, the log source does not collect events.
Credibility	Credibility represents the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events and can be adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Specifies the QRadar host where the log source's protocol runs. Outbound protocols initiate connections to remote systems from this host, and inbound protocols initialize their port listeners on this host to receive event data sent by remote systems. This parameter is not specifically used for assigning a log source to an Event Collector appliance. Because the Event Collector component exists on the following hosts, the protocols can be assigned to any of these hosts: • Event Collectors • Event Processors • Data Gateways (QRadar on Cloud only) • The QRadar Console **Tip:** All QRadar hosts that can collect events have an active syslog listener on port 514, whether they have any syslog log sources that are assigned or not. The **Target Event Collector** parameter is not used for log sources with the Syslog protocol.
Coalescing Events	When multiple events with the same **QID**, **Username**, **Source IP**, **Destination IP**, **Destination Port**, **Domain**, and **Log Source** occur within a short time interval (10 seconds), they are coalesced (bundled) together. Because the events are bundled together, the number of events that are stored is decreased, which reduces the storage cost of events. Coalescing events might lead to loss of information, including raw payloads or event properties. The default is enabled. For more information, see How does coalescing work in QRadar?

8. On the **Configure the protocol parameters** page, configure the protocol-specific parameters.
   - If your configuration can be tested, click **Test Protocol Parameters**.

- If your configuration cannot be tested, click **Finish**.

9. In the **Test protocol parameters** window, click **Start Test**.
10. To fix any errors, click **Configure Protocol Parameters**. Configure the parameters and click **Test Protocol Parameters**.
11. Click **Finish**.

Adding a log source by using the Log Sources icon

If the log source is not automatically discovered, manually add a log source for QRadar to receive events from your network devices or appliances.

If you are using QRadar 7.3.0 or earlier, you can add a log source in QRadar only by using the **Log Sources** icon.

If you are using QRadar 7.3.1 and later, you can add a log source by using the QRadar Log Source Management app.

Procedure

1. Log on to QRadar.
2. Click the **Admin** tab.
3. Click the **Log Sources** icon.
4. Click **Add**.
5. Configure the common parameters for your log source.
6. Configure the protocol-specific parameters for your log source.

   The following table describes the common log source parameters for all log source types:

Table 2. Common log source parameters

Parameter	Description
Enabled	When this option is not enabled, the log source does not collect events.
Credibility	Credibility represents the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events and can be adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.

Table 2. Common log source parameters (continued)	
Parameter	**Description**
Target Event Collector	Specifies the QRadar host where the log source's protocol runs. Outbound protocols initiate connections to remote systems from this host, and inbound protocols initialize their port listeners on this host to receive event data sent by remote systems. This parameter is not specifically used for assigning a log source to an Event Collector appliance. Because the Event Collector component exists on the following hosts, the protocols can be assigned to any of these hosts: • Event Collectors • Event Processors • Data Gateways (QRadar on Cloud only) • The QRadar Console **Tip:** All QRadar hosts that can collect events have an active syslog listener on port 514, whether they have any syslog log sources that are assigned or not. The **Target Event Collector** parameter is not used for log sources with the Syslog protocol.
Coalescing Events	When multiple events with the same **QID**, **Username**, **Source IP**, **Destination IP**, **Destination Port**, **Domain**, and **Log Source** occur within a short time interval (10 seconds), they are coalesced (bundled) together. Because the events are bundled together, the number of events that are stored is decreased, which reduces the storage cost of events. Coalescing events might lead to loss of information, including raw payloads or event properties. The default is enabled. For more information, see How does coalescing work in QRadar?

7. Click **Save**.
8. On the **Admin** tab, click **Deploy Changes**.

Adding bulk log sources

Use the QRadar Log Source Management app to add multiple log sources to IBM QRadar at the same time. You can add as many log sources as you want.

If you are using QRadar V7.3.0 or earlier, you can add a log source in QRadar only by using the Log Sources icon.

In QRadar 7.5.0 Update Package 4 and later, when you click the **Log Sources** icon, the QRadar Log Source Management app opens.

Procedure

1. In the QRadar Log Source Management app, click **+ New Log Source** and then click **Multiple Log Sources**.
2. On the **Select a Log Source type** page, select a log source type and click **Select Protocol Type**.
3. On the **Select a protocol type** page, select a protocol type and click **Configure Common Log Source Parameters**.
4. On the **Configure the common Log Source parameters** page, configure the parameters that you want to set for all of the log sources.
5. If you have log sources that have different log source parameter values, clear the relevant check boxes, and then click **Configure Common Protocol Parameters**.
6. On the **Configure the common protocol parameters** page, configure the protocol-specific parameters that you want to set for all of the log sources.
7. If you have log sources that have different protocol parameter values, clear the relevant check boxes, and then click **Configure Individual Parameters**.
8. On the **Configure the individual parameters** page, upload a CSV file that contains the individual log source parameter values, and click **Add**.

   A log source is created for each line of this file, except for empty lines and comment lines that begin with a hashtag (*#*). Each line must contain the comma-separated list of parameter values for the **Log Source Identifier** field, and any other deferred parameters, in the order shown in the deferred parameters table.
9. Click **Bulk Template** to download the file template and add the parameters that you want to configure, in order.

   For example, if you deferred the **Enabled** and **Groups** parameters, the CSV file must contain the following values:

   ```
   Enabled, Groups, Log Source Identifier
   ```

   If you include a comma in a parameter, enclose the value in double quotation marks.
10. If you do not upload a CSV file:
    a) Click **Manual** to specify the values for the parameters that you deferred.
    b) Enter a **Log Source Identifier** for each new log source and click **Add**.
11. Click **Finish**.

What to do next

Test your log sources. For more information, see "Testing log sources" on page 12

Adding bulk log sources by using the Log Sources icon

You can add up to 500 log sources at one time. When you add multiple log sources at one time, you add a bulk log source in QRadar. Bulk log sources must share a common configuration.

If you are using QRadar V7.3.0 or earlier, you can add a log source in QRadar only by using the **Log Sources** icon.

If you are using QRadar V7.3.1 to V7.3.3, you can also add a log source by using the QRadar Log Source Management app.

Procedure

1. On the **Admin** tab, click **Log Sources**.
2. From the **Bulk Actions** list, select **Bulk Add**.
3. In the **Bulk Log Sources** window, configure the parameters for the bulk log source.
4. Select the **Enabled** check box to enable the log source. By default, this check box is selected.

5. Select the **Coalescing Events** check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value that is configured in the **Coalescing Events** list in the **System Settings** window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar *Administration Guide*.
6. Select the **Store Event Payload** check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** list in the **System Settings** window on the **Admin** tab. When you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar *Administration Guide*.
7. Upload the log sources by choosing one of the following methods:
   - File Upload - Upload a text file that has one host name or IP per line.

     The text file must contain one IP address or host name per line. Extra characters after an IP address or host names longer than 255 characters can result in a value being bypassed from the text file. The file upload lists a summary of all IP address or host names that were added as the bulk log source.
   - Manual - Enter the host name or IP of the host that you want to add.
8. Click **Add** > **Save**.

   Note: By default, a check box is selected for each log source in the host list. Clear the check box if you want the log source to be ignored. Duplicate host names or IP addresses are ignored.
9. Click **Continue** to add the log sources.
10. On the **Admin** tab, click **Deploy Changes**.

Editing bulk log sources

In the QRadar Log Source Management app, view and edit a number of log sources at the same time. You can edit the parameters of up to 1000 log sources at one time. Edit multiple log sources when the log sources have similar parameters that you want to change, instead of editing each log source individually.

If you are using QRadar V7.3.1 to V7.3.3, you can also edit bulk log sources by using the Log Sources icon.

In QRadar 7.5.0 Update Package 4 and later, when you click the **Log Sources** icon, the QRadar Log Source Management app opens.

Before you begin

Ensure that the QRadar Log Source Management app is installed on your QRadar Console. For more information about installing the app, see Installing the QRadar Log Source Management app.

Procedure

1. In the QRadar Log Source Management app, select the relevant log sources that you want to edit.
2. Click **Edit**.
3. In the **Log Source Summary** pane, select and edit the parameters and click **Save**.

   Restriction: The **Log Source Identifier**, **Log Source Type** and **Protocol Configuration** parameters cannot be edited in bulk in the QRadar Log Source Management app. To edit the **Log Source Type** parameter in bulk by using the API, see QRadar: How to change log source type in bulk by using the QRadar API.
4. In the **Name Template** and **Description Template** fields, use the available variables to create the names and descriptions of the selected log sources.
5. Click the **Protocol** tab to edit the protocol parameters for the selected log sources. The selected log sources must share a protocol.

6. Click **Save**.

Editing bulk log sources by using the Log Sources icon

You can edit log sources in bulk to update the configuration parameters for log sources that were added as part of a bulk log source.

Restriction: The **Log Source Identifier**, **Log Source Type** and **Protocol Configuration** parameters cannot be edited in bulk by using the **Log Sources** icon. To edit the **Log Source Type** parameter in bulk by using the API, see QRadar: How to change log source type in bulk by using the QRadar API.

If you are using QRadar V7.3.0 or earlier, you can edit multiple log sources in QRadar only by using the **Log Sources** icon.

If you are using QRadar V7.3.1 to V7.3.3, you can also edit multiple log sources by using the QRadar Log Source Management app.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click the **Log Sources** icon.
3. Select the log sources that you want to edit, and from the **Bulk Actions** list, select **Bulk Edit**.
4. Modify the relevant parameters.
5. The list of log sources is for display purposes only. The check boxes are only used during the workflow for adding log sources to QRadar.
6. Click **Save** to update your log source configuration.
7. Click **Continue** to add the log sources.
8. On the **Admin** tab, click **Deploy Changes** if you added an IP address or host name to your bulk log source.

Results

The bulk log source is updated.

Adding a log source parsing order

You can assign a priority order for when the events are parsed by the target event collector.

About this task

You can order the importance of the log sources by defining the parsing order for log sources that share a common IP address or host name. Defining the parsing order for log sources ensures that certain log sources are parsed in a specific order, regardless of changes to the log source configuration. The parsing order ensures that system performance is not affected by changes to log source configuration by preventing unnecessary parsing. The parsing order ensures that low-level event sources are not parsed for events before more important log source.

Procedure

1. Click the **Admin** tab.
2. Click the **Log Source Parsing Ordering** icon.
3. Select a log source.
4. Optional: From the **Selected Event Collector** list, select the Event Collector to define the log source parsing order.
5. Optional: From the **Log Source Host** list, select a log source.
6. Prioritize the log source parsing order.

7. Click **Save**.

QRadar DSM installations and log source management FAQ

Learn about installing DSMs on QRadar.

How do I configure automatic updates for DSMs and protocols?

How do I manually install a DSM or protocol?

Testing log sources

In IBM QRadar V7.3.2. Fix Pack 3 or later, test your log source configuration in the QRadar Log Source Management app to ensure that the parameters that you used are correct. The test runs from the host that you specify in the **Target Event Collector** setting, and can collect sample event data from the target system. The target system is the source of your event data.

Restriction: If the **Test** tab doesn't appear for your log source, you can't test the configuration. In QRadar V7.3.2. Fix Pack 3 and QRadar Log Source Management app v5.0.0, only a few protocols are updated to include test capabilities. Ensure that you install the latest version of your protocols to get the testing capability when it is available.

To download a Fix Pack, go to Fix Central (https://www-945.ibm.com/support/fixcentral/).

Procedure

1. In the QRadar Log Source Management app, select a log source.
2. On the **Log Source Summary** pane, click the **Test** tab, then click **Start Test**.

   If there is high network latency between the QRadar Console and the log source's **Target Event Collector**, it might take a moment for the results to appear.

   When the test is successful, checkmarks are displayed next to each of the results and sample event information is generated. If the test is not successful, an **X** is displayed next to the result that failed, and no sample event information is generated. When one result fails, the test of the other results is canceled.
3. Optional: If the test is not successful, click **Edit** to configure the parameter that caused the test to fail and test your log source again.

   Click the drop-down arrow next to the failed result for more information about the error.
4. Optional: Click the **Settings** icon to edit the **Target Event Collector** settings.
5. Optional: Click the **Download** icon to view the test results in a `.txt` file.
6. Click **Close**.

Related reference

"Protocols available for testing" on page 12
In QRadar and QRadar Log Source Management app 5.0.0 or later, some protocols are updated to include test capabilities. Ensure that you install the latest version of your protocols to get the testing capability when it is available.

Protocols available for testing

In QRadar and QRadar Log Source Management app 5.0.0 or later, some protocols are updated to include test capabilities. Ensure that you install the latest version of your protocols to get the testing capability when it is available.

The following table lists the protocols available to be tested in the QRadar Log Source Management app.

Protocol	Fix Central link
Amazon AWS S3 REST API	Download Amazon AWS S3 REST API protocol

Protocol	Fix Central link
Amazon Web Services	Download Amazon Web Services protocol
Cisco Firepower eStreamer	Download Cisco eStreamer protocol
Google Cloud Pub Sub	Download Google Cloud Pub Sub protocol
Google G Suite Activity Reports REST API	Download Google G Suite Activity Reports REST API protocol
HTTP Receiver	Download HTTP receiver protocol
IBM Cloud Identity	Download IBM Cloud Identity protocol
JDBC	Download JDBC protocol
Log File	Download Log File protocol
Microsoft Azure Event Hubs	Download Microsoft Azure Event Hubs protocol
Microsoft DHCP	Download Microsoft DHCP protocol
Microsoft Exchange	Download Microsoft Exchange protocol
Microsoft Graph Security API	Download Microsoft Graph Security API protocol
Microsoft IIS	Download Microsoft IIS protocol
Microsoft Office 365	Download Microsoft Office 365 protocol
MQ JMS	Download MQ JMS protocol
Office 365 Message Trace REST API	Download Office 365 Message Trace REST API protocol
Okta REST API	Download Okta REST API protocol
Oracle Database Listener	Download Oracle Database Listener protocol
SMB Tail	Download SMB Tail protocol
TLS Syslog	Download TLS Syslog protocol
VMware VCloud Director	Download VMware VCloud Director protocol

Log source groups

You can categorize your log sources into groups to efficiently view and track your log sources. For example, you might group your log sources by functional purpose, physical location, or business unit association.

You can also use log source groups in searches and rules, instead of listing the log sources to which the search or rule applies.

You must have administrative access to create, edit, or delete groups. For more information about user roles, see the *IBM QRadar Administration Guide*.

Creating a log source group

When you create log source groups, you can drag groups in the navigation tree to change the organization of the tree items.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click **Log Source Groups**.

3. From the navigation tree, select the group where you want to create a new group, and then click **New Group**.
4. In the **Group Properties** window, enter a name and description. The name can be up to 255 characters in length and is case-sensitive. The description can be up to 255 characters in length.
5. Click **OK**.
6. To change the location of the new group, click the group and drag the folder to your chosen location in the navigation tree.
7. To edit the group name or description, select the log source group and then click **Edit**.

Copying and removing log sources

You can copy a log source to one or more groups to suit your organizational needs. When you no longer need a log source in a particular group, you can remove it. Removing a log source from a group does not delete the log source from IBM QRadar.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click **Log Source Groups**.
3. From the navigation tree, select the relevant log source group.
4. To copy the log source, complete the following steps:
   a) In the **Group Content** window, select the relevant log source and click **Copy**.
   b) In the **Choose Group** window, select the group that you want to copy the log source to, and click **Assign Groups**.
5. To remove the log source, complete the following steps:
   a) In the **Group Content** window, select the relevant log source and click **Remove**.
   b) In the **Confirmation** window, click **OK**.

Removing a log source group

You can remove a log source group that contains log sources. If any content, such as rules or saved searches, depends on the log source group it cannot be deleted.

About this task

Removing a log source group does not delete the log sources from IBM QRadar.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click **Log Source Groups**.
3. From the navigation tree, select the group that contains the group you want to remove.
4. In the **Group Content** window, select the group and click **Remove**.
5. If the log source group has no dependents, in the **Confirm Deletion** window, click **Delete**.
6. If the log source group has dependents, complete the following steps:
   a) In the **Found Dependents** window, click **View**.
   b) Delete or edit the dependents so that they do not reference the log source group. Perform these actions in the relevant areas of QRadar.
   c) In the **Unable to delete one or more items** window, click **Cancel**.
   d) Return to step 4.

Chapter 3. Gateway log source

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

Before you configure your gateway log source, you must understand the difference between protocols, DSMs, and log sources.

Protocol
Protocols provide the capability of collecting a set of data files by using various connection options. These connections pull the data back, or passively receive data, into the event pipeline in QRadar. Then, the corresponding DSM parses and normalizes the data.

DSM
A DSM is a code module that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as output. Each type of log source has a corresponding DSM.

Log source
A log source is a data source that creates an event log. For more information, see Chapter 2, "Introduction to log source management," on page 5.

Gateway log sources support the following protocols:

- Amazon AWS S3 REST
- Amazon AWS Web Services
- Google Cloud Pub Sub
- HTTP Receiver
- Kafka
- Microsoft Azure Event Hubs
- TCPMutilineSyslog
- TLS Syslog
- UDPMutilineSyslog

Tip: To provide the best fit for the generic data, use the Universal DSM when you configure your gateway log source.

A gateway log source does not use a DSM. It delegates the DSM parsing to stand-alone Syslog log sources that have an appropriate identifier and DSM. These log sources are a collector log source (the gateway) and a parser log source. Parser log sources match data that comes in from the gateway and do not actively collect the events themselves.

Before you create your gateway log source, you must know what types of data you expect to collect from the data gateway. Data gateways can collect many data types and QRadar does not support all data types by default. To parse the data correctly, a DSM must exist that can handle the events that you are collecting. Even if QRadar supports the event's source, if the gateway returns it in an unexpected format, the DSM might not parse it. For example, if the data gateway returns an event in a JSON format, but the DSM expects a LEEF format, you might need a custom DSM to parse the data.

A gateway log source works in the same way as other log sources by using its selected protocol to reach out and collect events. The difference between a gateway log source and other log sources occurs when the collected events are ready to be posted. A normal log source attempts to force the events to be parsed by the selected DSM. A gateway log source sends the events as a Syslog payload with a default identifier set to either 0.0.0.0 or to the connected Services IP address.

When an event is posted to the event pipeline as a Syslog payload, the events are handled by log source auto detection. If an existing dummy log source with the provided identifier exists, the event is handled

by that log source, regardless of whether the event parses with that DSM. If no existing dummy log source exists, the event is parsed by DSMs that support auto detection. If the event correctly parses with a DSM, then it updates the identifier to “IP or Host @ DSM” and creates a log source.

Log sources that are automatically created do not have their identifier set by the protocol. These log sources identifiers are in the “IP or Host @ DSM Type” format. To match to an automatically created dummy log source, the Syslog payload must have an identifier that is the same IP or Host, and the selected DSM must be able to parse it. The default identifier is sent as **[IP or Host]**, not “IP or Host @ DSM Type”. For the identifier to be updated with the DSM Type, it must parse with that DSM Type. If you use the default settings, events that cannot be parsed are sent directly to sim-generic.

Tip:

Manually created log sources that have an identifier that matches the identifier of the Syslog payload are used even if the DSM of the log source fails to parse the event.

To configure a gateway log source, enable the **Use As A Gateway Log Source** option for the selected protocol. If you enable this option, the events are sent to the event pipeline and are autodetected. To get the maximum value from this feature, use the “Log source identifier pattern” on page 16.

Related concepts

“Introduction to log source management” on page 5
You can configure IBM QRadar to accept event logs from log sources that are on your network. A *log source* is a data source that creates an event log.

Log source identifier pattern

Use the log source identifier pattern to customize the identifier that is sent with payloads when an event is posted. You can choose identifiers for your event formats and event types.

Important:

To use the full capabilities of the log source identifier pattern, you must have a basic understanding of regular expressions (regex) and how to use them.

The log source identifier pattern accepts a list of key-value pairs. A key is an identifier that is represented as a regex. The value is a regex that matches to event data. When the regex matches to the data within the event, then it posts the event with the identifier that is associated with that value.

Basic example

Key1 = `value1`

Key2 = `value2`

Key3 = `value3`

In this example, if an event contains a value of “value1”, the identifier for that event is key1. If an event contains a value of “value2”, the identifier is Key2. If an event contains both “value1” and “value2”, the first identifier, Key1, is matched.

In this example, you must manually create three Syslog log sources, one for each of the identifier options.

Regex example

Key1 = `value1`

Key2 = `\d\d\d` (where `\d\d\d` is a regex that matches to three consecutive digits.)

`\1= \d(\d)` (where `\d(\d)` is a regex that matches to two consecutive digits and captures the second digit. `\1` references the first captured value in the value field.)

In this example, the following statements are true:

- `\d` represents a "digit".

- If an event contains a value of “value1”, the identifier for that event is Key1.
- If an event contains “111” or “652” or any three consecutive digits, the identifier would be Key2.
- If an event contains two consecutive digits such as “11’, “73”, and “24”, the identifier is \1. The regex saves the second value (“1”, “3” and “4” in the examples) for future use with the parentheses. The value that is saved by the regex is used later as the identifier. If you set the key to “\1”, the key matches to the first saved value in the regex. In this case, the identifier is not a hardcoded value, but instead it can be ten values (0 - 9.) Three identifiers are in the sample events (“1”, “3” and “4”.)

You must create a log source with the identifiers Key1 and Key2, and a log source for each possible Key1 value. In this example, for the events to go to the correct log source, you must create three Syslog log sources. For the log sources, one has the identifier set to “1”, one has the identifier set to “3” and one has the identifier set to “4”. To capture all of the possible identifiers, you need ten Syslog log sources. Each log source corresponds to a single digit.

Tips for using the log source identifier pattern

It is important to know what type of data you are receiving and how granular you need your log sources to be. Each QRadar environment is unique. The following tips can help you to configure the log source identifier pattern.

Keep the data separated at the source

Most gateway supported services, such as Microsoft Azure Event Hubs and Google Pub Sub, offer ways to separate the data at the source. Keep your data in separate sources to reduce the complexity on the QRadar side. For example, if you want to collect Windows Logs, Linux® Logs and Audit Logs, use three separate gateway log sources to simplify the configuration. If you collect all of those logs in one source, QRadar must identify the events and associate them with the correct log source.

Hardcode the regex if possible

If you hardcode the key, all of the events that match the value’s regex are collected by a single log source. This action requires less effort to create and maintain log sources, and they are easier to monitor.

Use online regex testers

Before you save and enable your log source, use online tools to test the regex.

Use the Event Retriever to determine the identifier

Use the Event Retriever to display the assigned log source identifier in QRadar. You can also use it to test that your regex and identifier are matching correctly.

Chapter 4. Log source extensions

An extension document can extend or modify how the elements of a particular log source are parsed. You can use the extension document to correct a parsing issue or override the default parsing for an event from an existing DSM.

An extension document can also provide event support when a DSM does not exist to parse events for an appliance or security device in your network.

An extension document is an Extensible Markup Language (XML) formatted document that you can create or edit one by using any common text, code or markup editor. You can create multiple extension documents but a log source can have only one applied to it.

The XML format requires that all regular expression (regex) patterns be contained in character data (CDATA) sections to prevent the special characters that are required by regular expressions from interfering with the markup format. For example, the following code shows the regex for finding protocols:

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns=""> <![CDATA[(TCP|UDP|ICMP|GRE)]]></
pattern>
```

`(TCP|UDP|ICMP|GRE)` is the regular expression pattern.

The log sources extension configuration consists of the following sections:

Pattern
Regular expressions patterns that you associate with a particular field name. Patterns are referenced multiple times within the log source extension file.

Match groups
An entity within a match group that is parsed, for example, EventName, and is paired with the appropriate pattern and group for parsing. Any number of match groups can appear in the extension document.

Examples of log source extensions on QRadar Support Forums

You can create log source extensions (LSX) for log sources that don't have a supported DSM. To help you create your own log source extensions (also known as DSM extensions), you modify existing ones that were created.

The IBM QRadar Support Forum is an online discussion site where users and subject matter experts collaborate and share information.

You can find examples and answers to administration or troubleshooting questions that are related to the DSM Editor, log source extensions, and custom parsing issues on IBM QRadar Support Forum (https://www.ibm.com/mysupport/s/forumsproduct?language=en_US&name=qradar-dsm-editor&id=0TO0z000000R0iKGAS).

Optionally, for administration or troubleshooting questions that are related to the DSM Editor, log source extensions, and custom parsing issues, you can go to IBM QRadar FORUMS 101 (https://www.ibm.com/community/qradar/home/forums/). From the **Category** list, select *Events and Log Sources*, and from the **Tag** list, select *qradar-dsm-editor*.

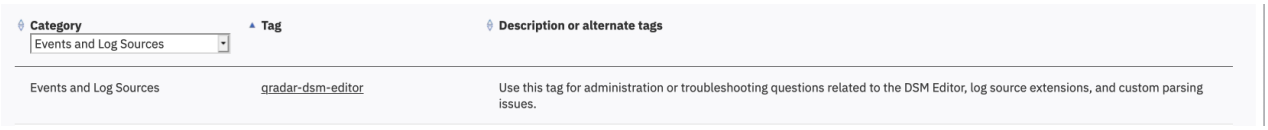


Figure 1. IBM QRadar Forums 101

Related concepts
Creating a log source extensions document to get data into QRadar

You create log source extensions (LSX) when log sources don't have a supported DSM, or to repair an event that has missing or incorrect information, or to parse an event when the associated DSM fails to produce a result.

Patterns in log source extension documents

Rather than associating a regular expression directly with a particular field name, patterns (`patterns`) are declared separately at the top of the extension document. These regex patterns can be then referenced multiple times within the log source extension file.

All characters between the start tag <pattern> and end tag </pattern> are considered part of the pattern. Do not use extra spaces or hard returns inside or around your pattern or <CDATA> expression. Extra characters or spaces can prevent the DSM extension from matching your intended pattern.

Table 3. Description of pattern parameters

Pattern	Type	Description
`id` (Required)	String	A regular string that is unique within the extension document.
`case-insensitive` (Optional)	Boolean	If true, the character case is ignored. For example, `abc` is the same as `ABC`. If not specified, this parameter defaults to false.
`trim-whitespace` (Optional)	Boolean	If true, whitespace and carriage returns are ignored. If the CDATA sections are split onto different lines, any extra spaces and carriage returns are not interpreted as part of the pattern. If not specified, this parameter defaults to false.
`use-default-pattern` (Optional)	Boolean	If true, the system uses Java Patterns for the Log Source Extension, instead of the more effective Adaptive Patterns. Set this option to true if Adaptive Patterns are providing inconsistent matching. If not specified, this parameter defaults to false.

Match groups

A *match group* (`match-group`) is a set of patterns that are used for parsing or modifying one or more types of events.

A *matcher* is an entity within a match group that is parsed, for example, EventName, and is paired with the appropriate pattern and group for parsing. Any number of match groups can appear in the extension document.

Table 4. Description of match group parameters	
Parameter	**Description**
`order` (Required)	An integer greater than zero that defines the order in which the match groups are executed. It must be unique within the extension document.
`description` (Optional)	A description for the match group, which can be any string. This information can appear in the logs. If not specified, this parameter defaults to empty.
`device-type-id-override` (Optional)	Define a different device ID to override the QID. Allows the particular match group to search in the specified device for the event type. It must be a valid log source type ID, represented as an integer. If not specified, this parameter defaults to the log source type of the log source to which the extension is attached.

Match groups can have these entities:

- “Matcher (matcher)” on page 21
- “Single-event modifier (event-match-single)” on page 35
- “Multi-event modifier (event-match-multiple)” on page 35

Matcher (matcher)

A matcher entity is a field that is parsed, for example, EventName, and is paired with the appropriate pattern and group for parsing.

Matchers have an associated order. If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found or a failure occurs.

Table 5. Description of matcher parameters	
Parameter	**Description**
`field` (Required)	The field to which you want the pattern to apply, for example, EventName, or SourceIp. You can use any of the field names that are listed in the List of valid matcher field names table.
`pattern-id` (Required)	The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of the pattern that is previously defined in a pattern ID parameter (Table 3 on page 20).
`order` (Required)	The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the EventName field, the one with the lowest order is attempted first.

Table 5. Description of matcher parameters (continued)	
Parameter	**Description**
`capture-group` (Optional)	Referenced in the regular expression inside parenthesis ( ). These captures are indexed starting at one and processed from left to right in the pattern. The `capture-group` field must be a positive integer less than or equal to the number of capture groups that are contained in the pattern. The default value is zero, which is the entire match. For example, you can define a single pattern for a source IP address and port; where the SourceIp matcher can use a capture group of 1, and the SourcePort matcher can use a capture group of 2, but only one pattern needs to be defined. This field has a dual purpose when combined with the `enable-substitutions` parameter. To see an example, review the extension document example.
`enable-substitutions` (Optional)	Boolean When you set to `true`, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. This parameter changes the meaning of the `capture-group` parameter. The `capture-group` parameter creates the new value, and group substitutions are specified by using `\x` where x is a group number, 1 - 9. You can use groups multiple times, and any free-form text can also be inserted into the value. For example, to form a value out of group 1, followed by an underscore, followed by group 2, an @, and then group 1 again, the appropriate capture-group syntax is shown in the following code: `capture-group="\1_\2@\1"` In another example, a MAC address is separated by colons, but in QRadar, MAC addresses are usually hyphen-separated. The syntax to parse and capture the individual portions is shown in the following example: `capture-group="\1:\2:\3:\4:\5:\6"` If no groups are specified in the capture-group when substitutions are enabled, a direct text replacement occurs. Default is false.

Table 5. Description of matcher parameters (continued)	
Parameter	**Description**
`ext-data` (Optional)	An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the List of valid matcher field names.

The following table lists valid matcher field names.

Table 6. List of valid matcher field names	
Field name	**Description**
EventName (Required)	The event name to be retrieved from the QID to identify the event. **Note:** This parameter doesn't appear as a field in the **Log Activity** tab.
EventCategory cat (LEEF)	An event category for any event with a category not handled by an event-match-single entity or an event-match-multiple entity. Combined with EventName, EventCategory is used to search for the event in the QID. The fields that are used for QIDmap lookups require an override flag to be set when the devices are already known to QRadar, for example, `<event-match-single event-name= "Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity= "OverrideAndNeverSend" />` The `force-qidmap-lookup-on-fixup="true"` is the flag override. **Note:** This parameter doesn't appear as a field in the **Log Activity** tab.
SourceIp src (LEEF)	The source IP address for the message.
SourcePort srcPort (LEEF)	The source port for the message.

Table 6. List of valid matcher field names (continued)	
Field name	**Description**
SourceIpPreNAT srcPreNAT (LEEF)	The source IP address for the message before Network Address Translation (NAT) occurs.
SourceIpPostNAT srcPostNAT (LEEF)	The source IP address for the message after NAT occurs.
SourceMAC srcMAC (LEEF)	The source MAC address for the message.
SourcePortPreNAT srcPreNATPort (LEEF)	The source port for the message before NAT occurs.
SourcePortPostNAT srcPostNATPort (LEEF)	The source port for the message after NAT occurs.
DestinationIp dst (LEEF)	The destination IP address for the message.
DestinationPort dstPort (LEEF)	The destination port for the message.
DestinationIpPreNAT dstPreNAT (LEEF)	The destination IP address for the message before NAT occurs.
DestinationIpPostNAT dstPostNAT (LEEF)	The destination IP address for the message after NAT occurs.
DestinationPortPreNAT dstPreNATPort (LEEF)	The destination port for the message before NAT occurs.
DestinationPortPostNAT dstPostNATPort (LEEF)	The destination port for the message after NAT occurs.
DestinationMAC dstMAC (LEEF)	The destination MAC address for the message.

Table 6. List of valid matcher field names (continued)

Field name	Description
DeviceTime devTime (LEEF)	The time and format that is used by the device. This date and time stamp represent the time that the event was sent, according to the device. This parameter doesn't represent the time that the event arrived. The `DeviceTime` field supports the ability to use a custom date and time stamp for the event by using the ext-data Matcher attribute. The following list contains examples of date and time stamp formats that you can use in the `DeviceTime` field: • ext-data="dd/MMM/YYYY:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd YYYY / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/YYYY" 05:26:00:11/Mar/2015 For more information about the possible values for the data and time stamp format, see the Joda-Time web page (http://www.joda.org/joda-time/key_format.html). DeviceTime is the only event field that uses the ext-data optional parameter.
Protocol proto (LEEF)	The protocol for the message; for example, TCP, UDP, or ICMP.
UserName	The user name for the message.
HostName identHostName (LEEF)	The host name for the message. Typically, this field is associated with identity events.
GroupName identGrpName (LEEF)	The group name for the message. Typically, this field is associated with identity events.
IdentityIp	The identity IP address for the message.
IdentityMac identMAC (LEEF)	The identity MAC address for the message.
IdentityIpv6	The IPv6 identity IP address for the message.
NetBIOSName identNetBios (LEEF)	The NetBIOS name for the message. Typically, this field is associated with identity events.
ExtraIdentityData	Any user-specific data for the message. Typically, this field is associated with identity events.

Table 6. List of valid matcher field names (continued)	
Field name	**Description**
SourceIpv6	The IPv6 source IP address for the message.
DestinationIpv6	The IPv6 destination IP address for the message.

JSON matcher (json-matcher)

A JSON-matcher (json-matcher) entity is a field that is parsed and is paired with the appropriate pattern and group for parsing. This entity is new in IBM QRadar V7.3.1.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

Table 7. Description of JSON matcher parameters	
Parameter	**Description**
`field` (Required)	The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the List of valid matcher field names table.
`pattern-id` (Required)	The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 3 on page 20)
`order` (Required)	The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the **EventName** field, the one with the lowest order is attempted first. The regular regex matchers and JSON matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.
`enable-substitutions` (Optional)	Boolean When set to `true`, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Wherever the pattern is in the form of a multi-keypath, set the **`enable-subtitutions`** value to '=true' so that each keypath in the pattern and expression is replaced with the value that is found by the payload. For example, if the JSON payload contains the **`first_name`** and **`last_name`** fields, but no **`full_name`** field, you can define an expression that contains multiple keypaths, such as `{/"last_name"}, {/"first_name"}`. The captured value for this expression is smith, john. Default is false.

Table 7. Description of JSON matcher parameters (continued)	
Parameter	**Description**
`ext-data` (Optional)	An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the List of valid JSON matcher field names.

The following table lists valid **JSON matcher** field names.

*Table 8. List of valid **JSON matcher** field names*	
Field name	**Description**
EventName (Required)	The event name to be retrieved from the QID to identify the event. **Note:** This parameter doesn't appear as a field in the **Log Activity** tab.
EventCategory	An event category for any event with a category that is not handled by an event-match-single entity or an event-match-multiple entity. Combined with EventName, EventCategory is used to search for the event in the QID. The fields that are used for QIDmap lookups require an override flag to be set when the devices are already known to the QRadar system, for example: `<event-match-single event-name="Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity="OverrideAndNeverSend" />` The `force-qidmap-lookup-on-fixup="true"` is the flag override. **Note:** This parameter doesn't appear as a field in the **Log Activity** tab.
SourceIp	The source IP address for the message.
SourcePort	The source port for the message.
SourceIpPreNAT	The source IP address for the message before Network Address Translation (NAT) occurs.

*Table 8. List of valid **JSON matcher** field names (continued)*	
Field name	**Description**
SourceIpPostNAT	The source IP address for the message after NAT occurs.
SourceMAC	The source MAC address for the message.
SourcePortPreNAT	The source port for the message before NAT occurs.
SourcePortPostNAT	The source port for the message after NAT occurs.
DestinationIp	The destination IP address for the message.
DestinationPort	The destination port for the message.
DestinationIpPreNAT	The destination IP address for the message before NAT occurs.
DestinationIpPostNAT	The destination IP address for the message after NAT occurs.
DestinationPortPreNAT	The destination port for the message before NAT occurs.
DestinationPortPostNAT	The destination port for the message after NAT occurs.
DestinationMAC	The destination MAC address for the message.

*Table 8. List of valid **JSON matcher** field names (continued)*

Field name	Description
DeviceTime	The time and format that is used by the device. This date and time stamp represent the time that the event was sent, according to the device. This parameter doesn't represent the time that the event arrived. The `DeviceTime` field supports the ability to use a custom date and time stamp for the event by using the ext-data Matcher attribute. The following list contains examples of date and time stamp formats that you can use in the `DeviceTime` field: • ext-data="dd/MMM/YYYY:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd YYYY / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/YYYY" 05:26:00:11/Mar/2015 For more information about the possible values for the data and time stamp format, see the Java SimpleDateFormat web page (https://docs.oracle.com/javase/8/docs/api/java/text/SimpleDateFormat.html). DeviceTime is the only event field that uses the ext-data parameter.
Protocol	The protocol for the message; for example, TCP, UDP, or ICMP.
UserName	The user name for the message.
HostName	The host name for the message. Typically, this field is associated with identity events.
GroupName	The group name for the message. Typically, this field is associated with identity events.
IdentityIp	The identity IP address for the message.
IdentityMac	The identity MAC address for the message.
IdentityIpv6	The IPv6 identity IP address for the message.
NetBIOSName	The NetBIOS name for the message. Typically, this field is associated with identity events.
ExtraIdentityData	Any user-specific data for the message. Typically, this field is associated with identity events.
SourceIpv6	The IPv6 source IP address for the message.

Table 8. List of valid ***JSON matcher*** *field names (continued)*	
Field name	**Description**
DestinationIpv6	The IPv6 destination IP address for the message.

LEEF matcher (leef-matcher)

A LEEF-matcher (leef-matcher) entity is a field that is parsed and is paired with the appropriate pattern of type 'LeefKey' for parsing. This entity is new in IBM QRadar V7.3.2.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

Table 9. Description of LEEF matcher parameters	
Parameter	**Description**
`field` (Required)	The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the Table 6 on page 23table.
`pattern-id` (Required)	The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 3 on page 20)
`order` (Required)	The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the **EventName** field, the one with the lowest order is attempted first. The regular regex, JSON, LEEF, and CEF matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.
`enable-substitutions` (Optional)	Boolean When set to `true`, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Default is false.
`ext-data` (Optional)	An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the Table 6 on page 23.

CEF matcher (cef-matcher)

A CEF-matcher (cef-matcher) entity is a field that is parsed and is paired with the appropriate pattern of type 'CefKey' for parsing. This entity is new in IBM QRadar V7.3.2.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

Table 10. Description of CEF matcher parameters

Parameter	Description
`field` (Required)	The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the Table 6 on page 23table.
`pattern-id` (Required)	The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 3 on page 20)
`order` (Required)	The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the **EventName** field, the one with the lowest order is attempted first. The regular regex, JSON, LEEF, and CEF matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.
`enable-substitutions` (Optional)	Boolean When set to `true`, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Default is false.
`ext-data` (Optional)	An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the Table 6 on page 23.

Name Value Pair matcher (namevaluepair-matcher)

A Name Value Pair-matcher (namevaluepair-matcher) entity is a field that is parsed and is paired with the appropriate pattern of type 'NameValuePairKey' for parsing. This entity is new in IBM QRadar V7.3.3.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

Table 11. Description of Name Value Pair matcher parameters	
Parameter	**Description**
`field` (Required)	The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the Table 6 on page 23.
`pattern-id` (Required)	The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 3 on page 20)
`order` (Required)	The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the **EventName** field, the one with the lowest order is attempted first. The regular regex, JSON, LEEF, and CEF matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.
`enable-substitutions` (Optional)	Boolean When set to `true`, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Default is false.
`ext-data` (Optional)	An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the Table 6 on page 23.
`delimiter-pair` (Optional)	The delimiter between each value in a NameValuePair payload.
`delimiter-namevalue` (Optional)	The delimiter between the name and value in each pair.

Example

In the following example, the delimiter-pair is a comma (,) and the delimiter-namevalue is an equal sign (=).

```
key1=value1,key2=value2,key3=value3
```

Generic List matcher (genericlist-matcher)

A Generic List-matcher (genericlist-matcher) entity is a field that is parsed and is paired with the appropriate pattern of type ''GenericListKey'' for parsing. This entity is new in IBM QRadar V7.3.3.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

Table 12. Description of Generic List matcher parameters

Parameter	Description
`field` (Required)	The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the Table 6 on page 23.
`pattern-id` (Required)	The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 3 on page 20)
`order` (Required)	The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the **EventName** field, the one with the lowest order is attempted first. The regular regex, JSON, LEEF, and CEF matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.
`enable-substitutions` (Optional)	Boolean When set to `true`, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Default is false.
`ext-data` (Optional)	An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the Table 6 on page 23.
`delimiter` (Optional)	The delimiter between each value in a GenericList payload.

Example

In the following example, the delimiter is a comma (,).

```
value1,value2,value3
```

XML Matcher (xml-matcher)

A XML-matcher (xml-matcher) entity is a field that is parsed and is paired with the appropriate pattern of type 'XmlKey' for parsing.

If multiple matchers are specified for the same field name, the matchers are run in the order that is presented until a successful parse is found.

Table 13. Description of XML matcher parameters

Parameter	Description
`field` (Required)	The field to which you want the pattern to apply; for example, EventName or SourceIp. You can use any of the field names that are listed in the Table 6 on page 23table.
`pattern-id` (Required)	The pattern that you want to use when the field is parsed from the payload. This value must match (including case) the ID parameter of an already defined pattern. (Table 3 on page 20)
`order` (Required)	The order that you want this pattern to attempt among matchers that are assigned to the same field. If two matchers are assigned to the **EventName** field, the one with the lowest order is attempted first. The regular regex, JSON, LEEF, and CEF matchers are combined into one list. The different types of matchers are attempted based on their orders, and the process stops when one of the matchers is able to parse out data from the payload.
`enable-substitutions` (Optional)	Boolean When set to `true`, a field cannot be adequately represented with a straight group capture. You can combine multiple groups with extra text to form a value. Default is false.
`ext-data` (Optional)	An extra-data parameter that defines any extra field information or formatting that a matcher field can provide in the extension. The only field that currently uses this parameter is DeviceTime. For example, you might have a device that sends events by using a unique time stamp, but you want the event to be reformatted to a standard device time. Use the ext-data parameter included with the DeviceTime field to reformat the date and time stamp of the event. For more information, see the Table 6 on page 23.

Multi-event modifier (`event-match-multiple`)

The multi-event modifier (`event-match-multiple`) matches a range of event types and then modifies them as specified by the `pattern-id` parameter and the `capture-group-index` parameter.

This match is not done against the payload, but is done against the results of the EventName matcher previously parsed out of the payload.

This entity allows mutation of successful events by changing the device event category, severity, or the method the event uses to send identity events. The `capture-group-index` must be an integer value (substitutions are not supported) and pattern-ID must reference an existing pattern entity. All other properties are identical to their counterparts in the single-event modifier.

Single-event modifier (`event-match-single`)

Single-event modifier (`event-match-single`) matches and then modifies exactly one type of event, as specified by the required, case-sensitive EventName parameter.

This entity allows mutation of successful events by changing the device event category, severity, or the method for sending identity events.

When events that match this event name are parsed, the device category, severity, and identity properties are imposed upon the resulting event.

You must set an `event-name` attribute and this attribute value matches the value of the **EventName** field. In addition, an event-match-single entity consists of these optional properties:

Table 14. Description of single-event parameters

Parameter	Description
`device-event-category`	A new category for searching for a QID for the event. This parameter is an optimizing parameter because some devices have the same category for all events.
`severity`	The severity of the event. This parameter must be an integer value 1 - 10. If a severity of less than 1 or greater than 10 is specified, the system defaults to 5. If not specified, the default is whatever is found in the QID.

Table 14. Description of single-event parameters (continued)	
Parameter	**Description**
send-identity	Specifies the sending of identity change information from the event. Choose one of the following options: • UseDSMResults If the DSM returns an identity event, the event is passed on. If the DSM does not return an identity event, the extension does not create or modify the identity information. This option is the default value if no value is specified. • SendIfAbsent If the DSM creates identity information, the identity event is passed through unaffected. If no identity event is produced by the DSM, but there is enough information in the event to create an identity event, an event is generated with all the relevant fields set. • OverrideAndAlwaysSend Ignores any identity event that is returned by the DSM and creates a new identity event, if there is enough information. • OverrideAndNeverSend Suppress any identity information that is returned by the DSM. Suggested option unless you are processing events that you want to go into asset updates.

Extension document template

The example of an extension document provides information about how to parse one particular type of Cisco FWSM so that events are not sent with an incorrect event name.

For example, if you want to resolve the word session, which is embedded in the middle of the event name:

```
Nov 17 09:28:26 192.0.2.1 %FWSM-session-0-302015: Built UDP connection for faddr
<IP_address1>/80 gaddr <IP_address2>/31696 laddr <IP_address3>/2157 duration 0:00:00 bytes
57498 (TCP FINs)
```

This condition causes the DSM to not recognize any events and all the events are unparsed and associated with the generic logger.

Although only a portion of the text string (302015) is used for the QID search, the entire text string (%FWSM-session-0-302015) identifies the event as coming from a Cisco FWSM. Since the entire text string is not valid, the DSM assumes that the event is not valid.

Extension document example for parsing one event type

An FWSM device has many event types and many with unique formats. The following extension document example indicates how to parse one event type.

Note: The pattern IDs do not have to match the field names that they are parsing. Although the following example duplicates the pattern, the SourceIp field and the SourceIpPreNAT field cab use the exact same pattern in this case. This situation might not be true in all FWSM events.

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
```

```
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
      <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1"/>
      <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />
      <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2"/>
      <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />
      <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />
      <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />
      <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />
      <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
      <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="2" />
      <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />
      <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true/>
      <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
   </match-group>
</device-extension>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<!-- Do not remove the "allEventNames" value -->
<pattern id="EventName-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceIp-Fakeware_Pattern" xmlns=""><![CDATA[]]</pattern>
<pattern id="SourcePort-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationPort" order="1" pattern-id="SDestinationPort-Fakeware_Pattern" capture-group="1" />
   <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
   <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
</match-group>
</device-extension>
```

Parsing basics

The preceding extension document example demonstrates some of the basic aspects of parsing:

- IP addresses
- Ports
- Protocol
- Multiple fields that use the same pattern with different groups

This example parses all FWSM events that follow the specified pattern. The fields that are parsed might not be present in those events when the events include different content.

The information that was necessary to create this configuration that was not available from the event:

- The event name is only the last 6 digits (`302015`) of the `%FWSM-session-0-302015` portion of the event.
- The FWSM has a hardcoded device event category of `Cisco Firewall`.
- The FWSM DSM uses the Cisco Pix QIDmap and therefore includes the `device-type-id-override="6"` parameter in the match group. The Pix firewall log source type ID is 6.

Note: If the QID information is not specified or is unavailable, you can modify the event mapping. For more information, see the Modifying Event Mapping section in the *IBM QRadar User Guide*.

Event name and device event category

An event name and a device event category are required when the QIDmap is searched. This device event category is a grouping parameter within the database that helps define like events within a device. The `event-match-multiple` at the end of the match group includes hardcoding of the category. The `event-match-multiple` uses the EventNameId pattern on the parsed event name to match up to 6 digits. This pattern is not run against the full payload, just that portion parsed as the EventName field.

The EventName pattern references the `%FWSM` portion of the events; all Cisco FWSM events contain the `%FWSM` portion. The pattern in the example matches `%FWSM` followed by any number (zero or more) of

letters and dashes. This pattern match resolves the word `session` that is embedded in the middle of the event name that needs to be removed. The event severity (according to Cisco), followed by a dash and then the true event name as expected by QRadar. The `(\d{6})` string is the only string within the EventNameFWSM pattern that has a capture group.

The IP addresses and ports for the event all follow the same basic pattern: an IP address followed by a colon followed by the port number. This pattern parses two pieces of data (the IP address and the port), and specifies different capture groups in the matcher section.

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\] </pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
       capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username" capture-group="1"/>
</match-group>
</device-extension>
```

IP address and port patterns

The IP address and port patterns are four sets of one to three digits, separated by periods followed by a colon and the port number. The IP address section is in a group, as is the port number, but not the colon. The matcher sections for these fields reference the same pattern name, but a different capture group (the IP address is group 1 and the port is group 2).

The protocol is a common pattern that searches the payload for the first instance of TCP, UDP, ICMP, or GRE. The pattern is marked with the case-insensitive parameter so that any occurrence matches.

Although a second protocol pattern does not occur in the event that is used in the example, there is a second protocol pattern that is defined with an order of two. If the lowest-ordered protocol pattern does not match, the next one is attempted, and so on. The second protocol pattern also demonstrates direct substitution; there are no match groups in the pattern, but with the enable-substitutions parameter enabled, the text TCP can be used in place of protocol=6.

Creating a log source extensions document to get data into QRadar

You create log source extensions (LSX) when log sources don't have a supported DSM, or to repair an event that has missing or incorrect information, or to parse an event when the associated DSM fails to produce a result.

When to create a log source extension

For log sources that don't have an official DSM, use a custom log source type to integrate log sources. A log source extension (also known as a device extension) is then applied to the custom log source type to provide the logic for parsing the logs. The LSX is based on Java™ regular expressions and can be used against any protocol type, such as syslog, JDBC, and Log File. Values can be extracted from the logs and mapped to all common fields within IBM QRadar.

When you use log source extensions to repair missing or incorrect content, any new events that are produced by the log source extensions are associated to the log source that failed to parse the original payload. Creating an extension prevents unknown or uncategorized events from being stored as unknown in QRadar.

Using the DSM Editor to quickly create a log source extension

For IBM QRadar V7.2.8 and later, you can use the DSM Editor to create log source extensions. The DSM Editor provides real-time feedback so that you know whether the log source extension that you are creating has problems. Use the DSM Editor to extract fields, define custom properties, categorize events,

define new QID definitions, and define your own log source type. For more information about the DSM Editor, see the *IBM QRadar Administration Guide*.

Process for manually creating a log source extension

Alternatively, to manually create a log source extension, complete the following steps:

1. Ensure that a log source is created in QRadar.

   Use a custom log source type to collect events from a source when the log source type is not listed as a QRadar supported DSM.

   Use the DSM Editor to create the new log source type, and then manually create the log source. You can attach an LSX to a supported log source type, such as Windows, Bluecoat, Cisco, and others that are listed as QRadar supported DSMs.
2. To determine what fields are available, use the **Log Activity** tab to export the logs for evaluation.
3. Use the extension document example template to determine the fields that you can use.

   It is not necessary to use all of the fields in the template. Determine the values in the log source that can be mapped to the fields in extension document template.
4. Remove any unused fields and their corresponding Pattern IDs from the log source extension document.
5. Upload the extension document and apply the extension to the log source.
6. Map the events to their equivalents in the QIDmap.

   This manual action on the **Log Activity** tab is used to map unknown log source events to known QRadar events so that they can be categorized and processed.

Related concepts

Examples of log source extensions on QRadar Support Forums
You can create log source extensions (LSX) for log sources that don't have a supported DSM. To help you create your own log source extensions (also known as DSM extensions), you modify existing ones that were created.

“Extension document template” on page 36
The example of an extension document provides information about how to parse one particular type of Cisco FWSM so that events are not sent with an incorrect event name.

Related information

r_supported_dsm_list.dita

Common regular expressions

Use regular expressions to match patterns of text in the log source file. You can scan messages for patterns of letters, numbers, or a combination of both. For example, you can create regular expressions that match source and destination IP addresses, ports, MAC addresses, and more.

The following codes show several common regular expressions:

```
\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3} \d{1,5} (?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2} (TCP|UDP|ICMP|
GRE) \w{3}\s\d{2}\s\d{2}:\d{2}:\d{2} \s \t .*?
```

The escape character, or "\", is used to denote a literal character. For example, "." character means "any single character" and matches A, B, 1, X, and so on. To match the "." characters, a literal match, you must use "\."

Table 15. Common regex expressions

Type	Expression
IP Address	\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}

Table 15. Common regex expressions (continued)	
Type	**Expression**
MAC Address	(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}
Port Number	\d{1,5}
Protocol	(TCP|UDP|ICMP|GRE)
Device Time	\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
Whitespace	\s
Tab	\t
Match Anything	.*?

Tip: To ensure that you don't accidentally match another characters, escape any non-digit or non-alpha character.

Building regular expression patterns

To create a log source extension, you use regular expressions (regex) to match strings of text from the unsupported log source.

About this task

The following example shows a log entry that is referenced in the steps.

```
May 20 17:24:59 kernel: DROP MAC=<MAC_address>
SRC=<Source_IP_address> DST=<Destination_IP_address> LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
May 20 17:24:59 kernel: PASS MAC=<MAC_address>
SRC=<Source_IP_address> DST=<Destination_IP_address> LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
May 20 17:24:59 kernel: REJECT
MAC=<MAC_address>  SRC=<Source_IP_address> DST=<Destination_IP_address> LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

Procedure

1. Visually analyze the unsupported log source to identify unique patterns.

   These patterns are later translated into regular expressions.
2. Find the text strings to match.

   Tip: To provide basic error checking, include characters before and after the values to prevent similar values from being unintentionally matched. You can later isolate the actual value from the extra characters.
3. Develop pseudo-code for matching patterns and include the space character to denote the beginning and end of a pattern.

   You can ignore the quotes. In the example log entry, the event names are DROP, PASS, and REJECT. The following list shows the usable event fields.

   - EventName: " kernel: VALUE "
   - SourceMAC: " MAC=VALUE "
   - SourceIp: " SRC=VALUE "
   - DestinationIp: " DST=VALUE "
   - Protocol: " PROTO=VALUE "
   - SourcePort: " SPT=VALUE "

- DestinationPort: " DPT=VALUE "

4. Substitute a space with the \s regular expression.

   You must use an escape character for non-digit or non-alpha characters. For example, = becomes \= and : becomes \:.

5. Translate the pseudo-code to a regular expression.

Table 16. Translating pseudo-code to regular expressions

Field	Pseudo-code	Regular expression
EventName	" kernel: VALUE "	\skernel\:\s.*?\s
SourceMAC	" MAC=VALUE "	\sMAC\=(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}\s
SourceIP	" SRC=VALUE "	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
DestinationIp	" DST=VALUE "	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
Protocol	" PROTO=VALUE "	\sPROTO\=(TCP|UDP|ICMP|GRE)\s
SourcePort	" SPT=VALUE "	\sSPT\=\d{1,5}\s
DestinationPort	" DPT=VALUE "	\sDPT\=\d{1,5}\s

6. Specify capture groups.

   A capture group isolates a certain value in the regular expression.

   For example, in the SourcePort pattern in the previous example, you can't pass the entire value since it includes spaces and SRC=<code>. Instead, you specify only the port number by using a capture group. The value in the capture group is what is passed to the relevant field in IBM QRadar.

   Insert parenthesis around the values you that you want capture:

Table 17. Mapping regular expressions to capture groups for event fields

Field	Regular expression	Capture group
EventName	\skernel\:\s.*?\s	\skernel\:\s(.*?)\s
SourceMAC	\sMAC\=(?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2}\s	\sMAC\=((?:[0-9a-fA- F]{2}\:){5}[0-9a-fA-F]{2})\s
SourceIP	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sSRC\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s
Destination IP	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sDST\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\s
Protocol	\sPROTO\=(TCP|UDP|ICMP|GRE)\s	\sPROTO\=((TCP|UDP|ICMP|GRE))\s
SourcePort	\sSPT\=\d{1,5}\s	\sSPT\=(\d{1,5})\s
DestinationPort	\sDPT\=\d{1,5}\s	\sDPT\=(\d{1,5})\s

7. Migrate the patterns and capture groups into the log source extensions document.

   The following code snippet shows part of the document that you use.

```
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-]*\d-(\d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
```

```
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
```

Uploading extension documents to QRadar

You can create multiple extension documents and then upload them and associated them to various log source types. The logic from the log source extension (LSX) is then used to parse the logs from the unsupported log source.

Extension documents can be stored anywhere before you upload to IBM QRadar.

Procedure

1. On the **Admin** tab, click **Log Source Extensions**.
2. Click **Add**.
3. Assign a name.
4. If you want to apply this log source extension to more than one instance of a log source type, select the log source type from the available **Log Source Type** list and click the add arrow to set it as the default.

   Setting the default log source type applies the log source extension to all events of a log source type, including those log sources that are automatically discovered.

   Ensure that you test the extension for the log source type first to ensure that the events are parsed correctly.
5. Click **Browse** to locate the LSX that you saved and then click **Upload**.

   QRadar validates the document against the internal XSD and verifies the validity of the document before the extension document is uploaded to the system.
6. Click **Save** and close the window.
7. Associate the log source extension to a log source.
   a) From the **Admin** tab, click **Data Sources** > **Log Sources**.
   b) Double-click the log source type that you created the extension document for.
   c) From the **Log Source Extension** list, select the document that you created.
   d) Click **Save** and close the window.

Examples of parsing issues

When you create a log source extension, you might encounter some parsing issues. Use these XML examples to resolving specific parsing issues.

Converting a protocol

The following example shows a typical protocol conversion that searches for TCP, UDP, ICMP, or GRE anywhere in the payload. The search pattern is surrounded by any word boundary, for example, tab, space, end of line. Also, the character case is ignored:

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[\b(TCP|UDP|ICMP|GRE)\b]]>
</pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol" capture-group="1" />
```

Making a single substitution

The following example shows a substitution that parses the source IP address, and then overrides the result and sets the IP address to 192.0.2.1, ignoring the IP address in the payload.

This example assumes that the source IP address matches something similar to SrcAddress=203.0.113.1 followed by a comma:

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}),]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK"
capture-group="192.0.2.1" enable-substitutions="true"/>
```

Generating a colon-separated MAC address

QRadar detects MAC addresses in a colon-separated form. Because all devices might not use this form, the following example shows how to correct that situation:

```
<pattern id="SourceMACWithDashes" xmlns="">
    <![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-
    ([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})]]>
</pattern>
 <matcher field="SourceMAC" order="1" pattern-id="
    SourceMACWithDashes" capture-group="\1:\2:\3:\4:\5:\6" />
```

In the preceding example, SourceMAC=12-34-1a-2b-3c-4d is converted to a MAC address of 12:34:1a:2b:3c:4d.

If the dashes are removed from the pattern, the pattern converts a MAC address and has no separators. If spaces are inserted, the pattern converts a space-separated MAC address.

Combining IP address and port

Typically an IP address and port are combined into one field, which is separated by a colon.

The following example uses multiple capture groups with one pattern:

```
pattern id="SourceIPColonPort" xmlns="">
<! [CDATA[Source=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([\d]{1,5})]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1" pattern-id="SourceIPColonPort" capture-group="2" />
```

Modifying an Event Category

A device event category can be hardcoded, or the severity can be adjusted.

The following example adjusts the severity for a single event type:

```
<event-match-single event-name="TheEvent" device-event-category="Actual
Category" severity="6" send-identity="UseDSMResults" />
```

Suppressing identity change events

A DSM might unnecessarily send identity change events.

The following examples show how to suppress identity change events from being sent from a single event type and a group of events.

```
// Never send identity for the event with an EventName of Authen OK
<event-match-single event-name="Authen OK" device-event-category="ACS"
severity="6" send-identity="OverrideAndNeverSend" />

// Never send any identity for an event with an event name starting with 7,
followed by one to five other digits:
<pattern id="EventNameId" xmlns=""><![CDATA[(7\d{1,5})]]>
</pattern>

<event-match-multiple pattern-id="EventNameId" capture-group-index="1"
```

```
device-event-category="Cisco Firewall" severity="7"
send-identity="OverrideAndNeverSend"/>
```

Formatting event dates and time stamps

A log source extension can detect several different date and time stamp formats on events.

Because device manufacturers do not conform to a standard date and time stamp format, the ext-data optional parameter is included in the log source extension to allow the DeviceTime to be reformatted. The following example shows how an event can be reformatted to correct the date and time stamp formatting:

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\]</pattern>
<pattern id="Username">(TLSv1)</pattern>

<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1_Pattern" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1_Pattern"
   capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username_Pattern" capture-group="1"/>
</match-group>
</device-extension>
```

Multiple Log Formats in a Single Log Source

Occasionally, multiple log formats are included in a single log source.

```
May 20 17:15:50 kernel: DROP IN=vlan2 OUT= MAC= SRC=<Source_IP_address>
DST=<Destination_IP_address> PROTO=UDP SPT=1900 DPT=1900
May 20 17:16:26 <server>[22331]: password auth succeeded for 'root' from <IP_address>
May 20 17:16:28 <server>[22331]: exit after auth (root): Exited normally </br>
May 20 17:16:14 <server>[22331]: bad password attempt for 'root' from <IP_address>:3364
```

For example, there are 2 log formats: one for firewall events, and one for authentication events. You must write multiple patterns for parsing the events. You can specify the order to be parsed. Typically, the more frequent events are parsed first, followed by the less frequent events. You can have as many patterns as required to parse all of the events. The order variable determines what order the patterns are matched in.

The following example shows multiple formats for the following fields EventName and UserName

Separate patterns are written to parse each unique log type. Both of the patterns are referenced when you assign the value to the normalized fields.

```
<pattern id="EventName-DDWRT-FW_Pattern" xmlns=""><![CDATA[kernel\:\s(.*?)\s]]></pattern>
<pattern id="EventName-DDWRT-Auth_Pattern" xmlns=""><![CDATA[sdrophear\[\d{1,5}\]|:\s(.*?\s.*?)\s]]>
</pattern>

<pattern id="UserName_DDWRT-Auth1__Pattern" xmlns=""><![CDATA[\sfor\s\'(.*?)\'s]]></pattern>
<pattern id="UserName_DDWRT-Auth2__Pattern" xmlns=""><![CDATA[\safter\sauth\s\((.*?)\)\:]]></pattern>

<match-group order="1" description="DD-WRT Device Extensions xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-DDWRT-FW_Pattern" capture-group="1"/>
   <matcher field="EventName" order="2" pattern-id="EventName-DDWRT-Auth_Pattern" capture-group="1"/>

   <matcher field="UserName" order="1" pattern-id="UserName-DDWRT-Auth1_Pattern" capture-group="1"/>
   <matcher field="UserName" order="2" pattern-id="UserName-DDWRT-Auth2_Pattern" capture-group="1"/>
```

Parsing a CSV log format

To parse a log file that is in CSV format, use the Generic List expression type that is available in the DSM Editor. For more information , see Expressions in Generic List format for structured data (https://www.ibm.com/docs/en/qsip/7.5?topic=editor-expressions-in-generic-list-format-structured-data).

```
Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,<Username>,<Source_IP_address>,1024,<Destination_IP_address>,22
Successful Login,<Username>,<Source_IP_address>,1743,<Destination_IP_address>,110
Privilege Escalation,<Username>,<Source_IP_address>,1028,<Destination_IP_address>,23
```

Chapter 5. Log source extension management

You can create log source extensions to extend or modify the parsing routines of specific devices.

A *log source extension* is an XML file that includes all of the regular expression patterns that are required to identify and categorize events from the event payload. Extension files can be used to parse events when you must correct a parsing issue or you must override the default parsing for an event from a DSM. When a DSM does not exist to parse events for an appliance or security device in your network, an extension can provide event support. The **Log Activity** tab identifies log source events in these basic types:

- Log sources that properly parse the event. Properly parsed events are assigned to the correct log source type and category. In this case, no intervention or extension is required.
- Log sources that parse events, but have a value **Unknown** in the **Log Source** parameter. Unknown events are log source events where the log source type is identified, but the payload information cannot be understood by the DSM. The system cannot determine an event identifier from the available information to properly categorize the event. In this case, the event can be mapped to a category or a log source extension can be written to repair the event parsing for unknown events.
- Log sources that cannot identify the log source type and have a value of **Stored** event in the **Log Source** parameter. Stored events require you to update your DSM files or write a log source extension to properly parse the event. After the event parses, you can then map the events.

Before you can add a log source extension, you must create the extension document. The extension document is an XML document that you can create with any common word processing or text editing application. Multiple extension documents can be created, uploaded, and associated with various log source types. The format of the extension document must conform to a standard XML schema document (XSD). To develop an extension document, knowledge of and experience with XML coding is required.

Adding a log source extension

You can add a log source extension to extend or modify the parsing routines of specific devices.

Procedure

1. Click the **Admin** tab.
2. Click the **Log Source Extensions** icon.
3. Click **Add**.
4. From the **Log Source Types** list, select one of the following options:

Option	Description
Available	Select this option when the device support module (DSM) correctly parses most fields for the log source. The incorrectly parsed field values are enhanced with the new XML values.
Set to default for	Select log sources to add or remove from the extension parsing. You can add or remove extensions from a log source. When a log source extension is **Set to default for** a log source, new log sources of the same **Log Source Type** use the assigned log source extension.

5. Click **Browse** to locate your log source extension XML document.

6. Click **Upload**. The contents of the log source extension is displayed to ensure that the proper extension file is uploaded. The extension file is evaluated against the XSD for errors when the file is uploaded.
7. Click **Save**.

Results

If the extension file does not contain any errors, the new log source extension is created and enabled. It is possible to upload a log source extension without applying the extension to a log source. Any change to the status of an extension is applied immediately and managed hosts or Consoles enforce the new event parsing parameters in the log source extension.

What to do next

On the **Log Activity** tab, verify that the parsing patterns for events is applied correctly. If the log source categorizes events as **Stored**, the parsing pattern in the log source extension requires adjustment. You can review the extension file against log source events to locate any event parsing issues.

Chapter 6. Threat use cases by log source type

External log sources feed raw events to the QRadar system that provide different perspectives about your network, such as audit, monitoring, and security. It's critical that you collect all types of log sources so that QRadar can provide the information that you need to protect your organization and environment from external and internal threats. For example, if your organization adopts cloud services and begins to onboard Amazon Web Services (AWS), or Azure cloud services, or Microsoft Office 365, add the log sources to QRadar so that you continue to have visibility into all malicious activity and compliance breaches.

Click a check mark in the following matrix to go to the log source that you're most interested in. For each log source, the relevant ATT&CK framework categories are listed. The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework was developed by Mitre Corp. The public knowledge base of threat tactics and techniques helps your security analysts to understand hacker threats and how to prevent adversarial attacks from happening to your organization's networks. These tactics can become your weaknesses if you're not collecting that type of log source.

Table 18. Log sources in QRadar with use cases

Log sources	Advanced Persistent Threat	Insider Threat	Securing the Cloud	Critical Data Protection	Incident Response	Compliance	Risk and Vulnerability Management
Firewall/Router	√		√	√	√	√	√
IDS/IPS (Intrusion Detection System/Intrusion Protection System)	√			√	√		√
Web Proxy	√	√	√	√		√	
VPN	√						
DNS	√	√					√
DHCP	√	√			√		
Mail Logs	√	√		√			
DLP (Data Loss Prevention)	√	√		√		√	
Endpoint	√	√		√		√	√
Identity/ Authentication (LDAP/AD/Radius)	√	√	√		√		
Anti Virus	√			√	√	√	√
QRadar Network Insights/Netflow	√	√	√	√	√	√	√
Database Logs	√	√	√	√	√	√	
EDR	√				√		√

Table 18. Log sources in QRadar with use cases (continued)							
Log sources	**Advanced Persistent Threat**	**Insider Threat**	**Securing the Cloud**	**Critical Data Protection**	**Incident Response**	**Compliance**	**Risk and Vulnerability Management**
Cloud Infrastructure/ Audit (AWS CloudTrail, Azure Event Hubs)	√	√	√	√		√	
Office 365			√		√	√	

Firewall/Router

The following table provides examples of use cases that are affected by firewall/router log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Discovery
- Command and Control
- Exfiltration

Table 19. Firewall/Router log source and use case examples	
Use case	**Examples**
Advanced Persistent Threat	Firewall data helps detect command control issues. Use it for external recon and prevent malicious IP communications from entering your environment.
Securing the Cloud	Identify risky internet service provider connections, such as connections to TOR.
Critical Data Protection	Discover and protect against abnormal database connection attempts.
Incident Response	See which hosts communicated with an infected host so that you can stop the spread of data infection.
Compliance	Monitor for unauthorized or unexpected firewall configuration changes to allow access to critical business assets. For example, PCI requires all critical assets that contain “banking information” to communicate through an internal DMZ with no direct access to the outside world.
Risk and Vulnerability Management	Discover assets that are actively communicating on vulnerable ports.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Intrusion detection system (IDS)/Intrusion protection system (IPS)

The following table provides examples of use cases that are affected by IDS/IPS log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Persistence Mechanism
- Discovery
- Command and Control

Table 20. IDS/IPS log source and use case examples

Use case	Examples
Advanced Persistent Threat	Correlate threat events with vulnerabilities, and then escalate those threat events. Perform more acute offense detection.
Critical Data Protection	SQL, XSS Injection
Incident Response	See which hosts are infected and watch for potential epidemics so that you can stop the spread of data infection.
Risk and Vulnerability Management	Validate and assess threats to prioritize by correlating with asset and vulnerability data.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Web proxy

The following table provides examples of use cases that are affected by web proxy log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Persistence Mechanism
- Data Exfiltration
- Command and Control
- Privilege Escalation
- Credential Access

Table 21. Web proxy log source and use case examples

Use case	Examples
Advanced Persistent Threat	Monitor for malicious domain communication, data exfiltration, and command and control activities. Detect attempts to bypass normal user restrictions by surfing with a service account.
Insider Threat	Track malicious activity such as crypto mining that uses corporate resources.

Table 21. Web proxy log source and use case examples (continued)	
Use case	**Examples**
Securing the Cloud	Detect shadow IT, unapproved cloud service usage, and potential data exfiltration from corporate environments.
Critical Data Protection	Monitor for unauthorized data exfiltration.
Compliance	Monitor for critical asset communication with the outside world.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

VPN

The following table provides examples of use cases that are affected by VPN log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Credential Access
- Lateral Movement

Table 22. VPN log source and use case example	
Use case	**Examples**
Advanced Persistent Threat	Monitor for logins from suspicious locations.
Insider Threat	Detect the use of VPN for users outside of normal usage patterns or from abnormal geographical areas.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

DNS

The following table provides examples of use cases that are affected by DNS log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Defense Evasion
- Persistence Mechanism
- Command and Control
- Exfiltration
- Credential Access (note: Technique T1171)

Table 23. DNS log source and use case examples	
Use case	**Examples**
Advanced Persistent Threat	Monitor for malicious DNS usages such as domain name generation, tunneling, and squatting.
Insider Threat	Detect tunneling of traffic through DNS records.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

DHCP

The following table provides examples of use cases that are affected by DHCP log sources. Data from this type of log source is important for detecting adversarial the techniques in the Defense Evasion ATT&CK category.

Table 24. DHCP log source and use case example

Use case	Examples
Advanced Persistent Threat	Detection of rogue access points or other unexpected device presence on corporate network.
Insider Threat	Detection of rogue access points or other unexpected device presence on corporate network.
Incident Response	Identification of which host had a specific IP address at the time of an incident.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Mail logs

The following table provides examples of use cases that are affected by mail log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Execution
- Initial Access
- Collection

Table 25. Mail log source and use case examples

Use case	Examples
Advanced Persistent Threat	Monitor for phishing and spam.
Insider threat	Phishing
Critical Data Protection	Phishing, data exfiltration by email

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

DLP (data loss prevention)

The following table provides examples of use cases that are affected by DLP log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Data Exfiltration
- Collection

Table 26. DLP log source and use case examples	
Use case	**Examples**
Advanced Persistent Threat	Data can be exfiltrated through many methods. Identify and track suspicious files such as: • DNS abnormalities • Sensitive content • Aberrant connections • Aliases
Insider Threat	Data can be exfiltrated through many methods. Identify and track suspicious files such as: • DNS abnormalities • Sensitive content • Aberrant connections • Aliases
Critical Data Protection	Data can be exfiltrated through many methods. Identify and track suspicious files such as: • DNS abnormalities • Sensitive content • Aberrant connections • Aliases
Compliance	Data can be exfiltrated through many methods. Identify and track suspicious files such as: • DNS abnormalities • Sensitive content • Aberrant connections • Aliases

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Endpoint

The following table provides examples of use cases that are affected by Endpoint log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Privilege Escalation
- Initial Access
- Execution
- Persistence
- Credential Access
- Defense Evasion
- Discovery

- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Table 27. Endpoint log source and use case examples	
Use case	**Examples**
Advanced Persistent Threat	Monitor for malicious hashes, suspicious PowerShell activity, process abuse, or other suspicious endpoint activities.
Insider Threat	Detection of persistent malware by using host resources (for example, crypto mining)
Critical Data Protection	Data can be exfiltrated through many methods. Identify and track suspicious files such as: • DNS abnormalities • Sensitive content • Aberrant connections • Aliases
Compliance	Monitor for adherence to corporate company policy (for example, unapproved software use).
Risk and Vulnerability Management	Assess and manage risk through vulnerability.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Identity/Authentication (LDAP/AD/Radius)

The following table provides examples of use cases that are affected by LDAP/AD/Radius log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Privilege Escalation
- Credential Access
- Initial Access

Note: You can also track privilege abuse (for example, surf with a super account, privileges that are given to users).

Table 28. LDAP/AD/Radius log source and use case examples	
Use case	**Examples**
Advanced Persistent Threat	Monitor for activities such as brute force login by malware, lateral movement through the network, or suspicious logins.
Insider Threat	Account takeover by malware
Securing the Cloud	Provide user-to-IP association to help identify cloud users from data that has only IP source address.

Table 28. LDAP/AD/Radius log source and use case examples (continued)	
Use case	**Examples**
Incident Response	Visibility into where a user logged in during the IR process.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Anti-virus

The following table provides examples of use cases that are affected by anti-virus log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Persistence
- Initial Access
- Defense Evasion

Table 29. Anti-virus log source and use case examples	
Use case	**Examples**
Advanced Persistent Threat	Monitor for activities such as: • Endpoint infection by anti-virus • Virus that is not cleaned • Reinforcement of other suspicious endpoint behavior
Critical Data Protection	Detection of virus outbreak to prevent movement to servers that contain critical business data.
Incident Response	Visibility into where a specific virus signature was seen.
Compliance	Ensuring up-to-date AV definitions on critical hosts/servers.
Risk and Vulnerability Management	Malicious WWW domain connections indication of a vulnerable host that is compromised.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

QRadar Network Insights/Netflow

The following table provides examples of use cases that are affected by QRadar Network Insights/Netflow log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Lateral Movement
- Discovery
- Persistence Mechanism
- Defense Evasion

- Data Exfiltration
- Credential Access
- Command and Control

Table 30. QRadar Network Insights/Netflow log source and use case examples

Use case	Examples
Advanced Persistent Threat	Monitor for activities such as: • Recon • Malicious download • Lateral movement • Phishing
Insider Threat	Phishing detection
Securing the Cloud	Monitor for activities such as: • Data exfiltration • Expired WWW certificates • Self-signed WWW certificates • Phishing • Risky WWW domain connections
Critical Data Protection	Data can be exfiltrated through many methods. Identify and track suspicious files such as: • DNS abnormalities • Sensitive content • Aberrant connections • Aliases
Incident Response	Provides a huge pool of investigative data to determine the spread of an attack from domain communication, hashes that are downloaded, IP addresses that are communicated with, file names, data volumes transferred.
Compliance	Monitor for critical asset communications (for example, crown jewel communicate to the open internet).
Risk and vulnerability management	Prioritize host vulnerability remediation based upon the level of risk that hosts are communicated with.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Database logs

The following table provides examples of use cases that are affected by database log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Credential Access
- Collection
- Initial Access
- Discovery
- Data Exfiltration
- Privilege Escalation

Table 31. Database log source and use case examples

Use case	Examples
Insider Threat	Detect unauthorized database access and data theft.
Critical Data Protection	Databases often include sensitive corporate information and require monitoring for most compliance standards. Monitor for unauthorized user permission changes.
Incident Response	Evidence of what data was accessed, and by whom, during a breach.
Compliance	Databases often include sensitive corporate information and require monitoring for most compliance standards.
Risk and Vulnerability Management	Prioritize vulnerabilities on hosts with active databases that potentially contain critical data. Detect default accounts and passwords that are enabled.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

EDR (endpoint detection and response)

The following table provides examples of use cases that are affected by EDR log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Credential Access
- Privilege Escalation
- Discovery

Table 32. EDR log source and use case examples

Use case	Examples
Advanced Persistent Threat	Monitor for activities such as: • Compromised endpoints • Suspicious endpoint behavior
Incident Response	Rapidly determine existence of IOCs at endpoints, including hashes and file names.
Risk and Vulnerability Management	Correlate vulnerability information with endpoint data.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Cloud Infrastructure/Audit (AWS Cloudtrail, Azure Event Hubs)

The following table provides examples of use cases that are affected by Cloud Infrastructure/Audit log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Credential Access
- Privilege Escalation

Table 33. Cloud Infrastructure/Audit log source and use case examples

Use case	Examples
Advanced Persistent Threat	Multi-vector attacks that impact multiple cloud environments, crypto jacking (Hijacking cloud properties/computing resources for crypto currency mining).
Insider Threat	Detection of compromised cloud accounts, escalated role/user privilege, altering network security group access policies.
Securing the Cloud	Monitor for activities such as: • Misconfiguration of S3 buckets and user policies • Visibility into cloud environments • Enforcing best cloud security practices • Continuous monitoring of network interface traffic
Critical Data Protection	Lock down and isolation of sensitive data repositories.
Compliance	Retention of cloud audit trail logs and ensuring log integrity

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Microsoft Office 365

The following table provides examples of use cases that are affected by Microsoft Office 365 log sources. Data from this type of log source is important for detecting adversarial techniques in the following ATT&CK categories:

- Initial Access
- Execution
- Persistence

Table 34. Office 365 log source and use case examples	
Use case	**Examples**
Securing the Cloud	Monitor for activities such as: • Brute force logins • Suspicious logins from multiple locations • Blocklisted countries and locations • Excessive file access attempts
Incident Response	Evidence of what data was accessed during a breach.
Compliance	Continuous monitoring of file activity and user access.

Find out more about each technique and tactic: ATT&CK Technique matrix (https://attack.mitre.org/wiki/Technique_Matrix)

(Back to top)

Related information

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)

See how QRadar Advisor with Watson 2.0.1 analyzes several MITRE ATT&CK techniques

A Basic Model to Measure SIEM Maturity

Chapter 7. Troubleshooting DSMs

If you come across a problem with your DSM, you can troubleshoot the following issues.

What happens when events, which are parsed, are collected with unofficial DSMs?

Not having an official DSM doesn't mean that the events aren't collected. It indicates that the event that is received by IBM QRadar might be identified as "**Unknown**" on the Log Activity tab of QRadar. "**Unknown**" means that IBM QRadar collected the event, but was unable to parse the event format to categorize the event. However, some unique events in unofficial DSMs cannot be parsed or identified if they don't follow an event format that is expected. When an event cannot be understood by the system, they are categorized as "**Unknown**".

What is the difference between an unknown event and a stored event?

Events comprise three different categories:

Parsed events
QRadar collects, parses, and categorizes the event to the proper log source.

Unknown events
The event is collected and parsed, but cannot be mapped or categorized to a specific log source. The **Event Name** and the **Low-Level Category** are set as **Unknown**. Log sources that aren't automatically discovered are typically identified as **Unknown Event Log** until a log source is manually created in the system. When an event cannot be associated to a log source, the event is assigned to a generic log source. You can identify these events by searching for events that are associated with the `SIM Generic` log source or by using the `Event is Unparsed` filter.

Stored events
The event cannot be understood or parsed by QRadar. When QRadar cannot parse an event, it writes the event to disk and categorize the event as **Stored**.

How can you find these events in the Log Activity tab?

To find events specific to your device, you can search in QRadar for the source IP address of your device. You can also select a unique value from the event payload and search for `Payload Contains`. One of these searches might locate your event, and it is likely either categorized as **Unknown** or **Stored**.

The easiest way to locate unknown or stored events is to add a search filter for `Event in Unparsed`. This search filter locates all events that either cannot be parsed (stored) or events that might not be associated with a log source or auto discovered (Unknown Log Event).

For more information about officially supported DSMs, see QRadar supported DSMs.

What do you do if you have an unknown event log from a log source that is not auto discovered?

The Event Collection Service (ECS) contains a traffic analysis process that automatically discovers and creates new log sources from events. Traffic analysis tries to identify the log source by analyzing the event payloads. At minimum, 25 events are required to identify a log source. If the log source cannot be identified by traffic analysis after 1,000 events, then QRadar abandons the auto discovery process. When a log source cannot be identified by the event payload and reaches the maximum threshold for traffic analysis, then QRadar generates a notification that specifies the IP address of the log source. QRadar generates the following notification:

```
Unable to automatically detect the associated log source for IP address <IP>
```

QRadar then categorizes the log source as SIM Generic and labels the events as **Unknown Event Log**.

QRadar can auto discover certain log sources, but some supported log sources cannot be detected. Common causes of this notification are:

- The device is a newer version than the DSM that QRadar supports to parse events.
- The device type does not support automatic log source discovery. Review the documentation for your DSM to see whether it is automatically discovered.
- The logs might not follow an expected format. A customizable event format or required field might be missing.
- The device might be creating an event format due to an incorrect configuration.
- The logs are coming from a device that is not an officially supported DSM in QRadar.

To resolve the unknown event log:

- Review the IP address to determine which device is sending unparsed events. After you identify the device, you can manually create a log source by using the IBM QRadar Log Source Management app.
- Review any log sources that forward events at a low rate. Log sources with low event rates are a common cause of this notification.
- Ensure that auto update downloads the latest DSMs to properly parse events for your QRadar system.
- Review any log sources that provide events through a central log server. Logs that are provided from central log servers or management consoles might require their log sources to be created manually.
- Review the **Log Activity** tab to determine the appliance type from the IP address in the notification message and manually create a log source in QRadar.

What do you do if the product version or device you have is not listed in the DSM Configuration Guide?

Sometimes a version of a vendor product or a device is not listed as supported. If the product or device is not listed, follow these guidelines:

Version not listed

If the DSM for your product is officially supported by QRadar, but your product version is not listed in the *IBM QRadar DSM Configuration Guide*, you have the following options:

- Try the DSM to see whether it works. The product versions that are listed in the guide are tested by IBM, but newer untested versions can also work.
- If you tried the DSM and it didn't work, open a support ticket for a review of the log source to troubleshoot and rule out any potential issues.

  Tip: In most cases, no changes are necessary, or perhaps a minor update to the IBM QRadar Identifier (QID) Map might be all that is required. Software updates by vendors might on rare occasions add or change event formats that break the DSM, requiring an RFE for the development of a new integration. This is the only scenario where an RFE is required.

Device not listed

When a device is not officially supported, you have the following options:

- Open a request for enhancement (RFE) to have your device become officially supported.
  - Go to the QRadar SIEM RFE page (https://ibm.biz/BdRPx5).
  - Log in to the support portal page.
  - Click the **Submit** tab and type the necessary information.

    Tip: If you have event logs from a device, attach the event information and include the product version of the device that generated the event log.
- Write a log source extension to parse events for your device. For more information, see Chapter 4, "Log source extensions," on page 19 and the DSM Editor.

- You can use content extensions for sending events to QRadar that are provided by some third-party vendors. They can be found on the IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub/). These third-party DSM integrations are supported by the vendor, not by IBM. For a list of available third-party DSMs, see Chapter 177, "DSMs supported by third-party vendors," on page 1657.

Part 2. QRadar protocol configuration

Chapter 8. Undocumented protocols

When you configure a log source, the set of available protocol type options is limited by the selected log source type. Not all log source types support all protocol types.

The *DSM Configuration Guide* describes how to configure log sources of a particular type, with each of the protocol types that IBM fully supports for that log source type. Any protocol type that has configuration documentation for a particular log source type is considered a "documented" protocol for that log source type. By default, only these documented protocols are displayed in the **Protocol Configuration** list in the **Log Sources** window.

As an open platform, QRadar collects and processes event data through other integration methods (protocol types). Some protocol types can be configured for a particular log source type but are marked as *undocumented*. However, the *DSM Configuration Guide* doesn't contain instructions on how to set up event collection for undocumented protocols. IBM does not provide support with the configuration of log sources that use undocumented protocols because they are not internally tested and documented. Users are responsible for determining how to get the event data into QRadar.

For example, the JDBC protocol is the documented configuration for getting events from a system that stores its event data in a database. However, it is possible to collect the same event data through a third-party product and then forward it to QRadar through Syslog. Configure the log source to use the undocumented protocol type "Syslog". QRadar accepts the events and routes them to the appropriate log source.

You must configure the third-party product to retrieve the event data from the database and to send this data to QRadar through Syslog because this configuration is not the documented collection method.

Important: Collecting and processing event data through undocumented protocols might result in data that is formatted differently from what a documented DSM log source type expects. As a result, parsing might not work for the DSM if it’s receiving events from an undocumented protocol. For example, a JDBC protocol creates event payloads that consist of a series of space-separated key and value pairs. In the target database table, the key is a column name and the value is the column for the table row that the event represents. The DSM for a supported log source type that uses the JDBC protocol expects this event format. If the event data forwarded from a third-party product through the syslog protocol is in a different format, the DSM is unable to parse it. It might be necessary to use the DSM Editor to adjust the parsing of a DSM so that it can handle these events.

Related tasks

“Configuring an undocumented protocol” on page 65

As an open platform, QRadar collects and processes event data through multiple integration methods (protocol types). Some protocol types can be configured for a particular log source type but are marked as "undocumented". The *DSM Configuration Guide* doesn't contain instructions on how to set up event collection for undocumented protocols. IBM does not offer support with the configuration of log sources that use undocumented protocols because they are not internally tested and documented.

Configuring an undocumented protocol

As an open platform, QRadar collects and processes event data through multiple integration methods (protocol types). Some protocol types can be configured for a particular log source type but are marked as "undocumented". The *DSM Configuration Guide* doesn't contain instructions on how to set up event collection for undocumented protocols. IBM does not offer support with the configuration of log sources that use undocumented protocols because they are not internally tested and documented.

Procedure

1. Use SSH to log in to your QRadar Console appliance as a root user.
2. Edit the following file: `/store/configservices/staging/globalconfig/nva.conf`

3. Set the **EXPOSE_UNDOCUMENTED_PROTOCOLS** property value to true.
4. Save the file.
5. To close the SSH session type `exit`.
6. Log in to the QRadar Console.
7. Click the **Admin** tab.
8. Click **Deploy Changes**.

   Undocumented protocol options appear in the **Protocol Configuration** list in the log source **Add/Edit** window.

Related concepts

"Undocumented protocols" on page 65

Chapter 9. Protocol configuration options

Protocols in IBM QRadar provide the capability of collecting a set of data files by using various connection options. These connections pull the data back or passively receive data into the event pipeline in QRadar. Then, the corresponding Device Support Module (DSM) parses and normalizes the data.

The following standard connection options pull data into the event pipeline:

- JDBC
- FTP
- SFTP
- SCP

The following standard connection options receive data into the event pipeline:

- Syslog
- HTTP Receiver
- SNMP

QRadar also supports proprietary vendor-specific protocol API calls, such as Amazon Web Services.

Related information

Adding a log source

Akamai Kona REST API protocol configuration options

To receive events from your Akamai Kona Platform, configure a log source to use the Akamai Kona REST API protocol.

The Akamai Kona REST API protocol is an outbound/active protocol that queries the Akamai Kona Platform and sends events to the QRadar Console.

The following table describes the parameters that require specific values for Akamai KONA DSM event collection.

Table 35. Akamai KONA DSM log source parameters

Parameter	Value
Log Source Type	Akamai KONA
Protocol Configuration	Akamai Kona REST API
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Akamai KONA DSM log source, ensure that you give each one a unique name.
Host	The **Host** value is provided during the SIEM OPEN API provisioning in the Akamai Luna Control Center. The **Host** is a unique base URL that contains information about the appropriate rights to query the security events. This parameter is a password field because part of the value contains secret client information.

Table 35. Akamai KONA DSM log source parameters (continued)	
Parameter	**Value**
Client Token	**Client Token** is one of the two security parameters. This token is paired with **Client Secret** to make the client credentials. This token can be found after you provision the Akamai SIEM OPEN API.
Client Secret	**Client Secret** is one of the two security parameters. This secret is paired with **Client Token** to make the client credentials. This token can be found after you provision the Akamai SIEM OPEN API.
Access Token	**Access Token** is a security parameter that is used with client credentials to authorize API client access for retrieving the security events. This token can be found after you provision the Akamai SIEM OPEN API.
Security Configuration ID	**Security Configuration ID** is the ID for each security configuration that you want to retrieve security events for. This ID can be found in the SIEM Integration section of your Akamai Luna portal. You can specify multiple configuration IDs in a comma-separated list. For example, `configID1,configID2`.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
Automatically Acquire Server Certificate	Select **Yes** for QRadar to automatically download the server certificate and begin trusting the target server.
Recurrence	The time interval between log source queries to the Akamai SIEM API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 1 minute.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Alibaba Cloud Object Storage protocol configuration options

The Alibaba Cloud Object Storage protocol for IBM QRadar is an active outbound protocol that collects logs that are contained in objects from Alibaba Cloud Object Storage buckets.

Important: Before you configure the Alibaba Cloud Object Storage protocol, configure user access roles and service credentials to access the Alibaba Cloud Object Storage buckets.

- Grant permissions to another Alibaba Cloud account or to specific users, so they can access or manage resources in a bucket. For more information about user access roles and permissions, see Bucket policy overview (https://www.alibabacloud.com/help/en/oss/user-guide/overview).
- Create service credentials. For more information, see Obtain an AccessKey pair (https://www.alibabacloud.com/help/en/beginner-guide/latest/obtain-an-accesskey-pair).

Table 36. Alibaba Cloud Object Storage protocol common log source parameters

Parameter	Description
Protocol Configuration	Alibaba Cloud Object Storage Service
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Alibaba Cloud Object Storage log source, ensure that you give each one a unique name.
Access Key ID	The Access Key ID generates when you configure the service credentials.
Secret Access Key	The Secret Access Key generates when you configure the service credentials.
Endpoint	The public endpoint on the bucket configuration page. For more information, see Regions and endpoints (https://www.alibabacloud.com/help/en/oss/user-guide/regions-and-endpoints).
Bucket Name	The name of the bucket that logs are stored in.
Prefix	The prefix filter value to limit collecting objects or file keys that begin with the prefix. To pull all files from the bucket, use a forward slash (/). **Important:** Changing the **Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. If the **Prefix** file path is used to specify folders, you must not begin the file path with a forward slash. For example, use `folder1/folder2` instead.
Event Format	The following event formats are supported: **ActionTrail** Raw log files that contain an array of records. You can use `.gz` files for compression. **LINEBYLINE** Raw log files that contain one record per line. You can use either `.gz`, `.gzip`, or `.zip` files for compression.

Table 36. Alibaba Cloud Object Storage protocol common log source parameters (continued)

Parameter	Description
Use As A Gateway Log Source	If you do not want to define a custom log source identifier for events, clear the checkbox. If you don't select **Use As A Gateway Log Source** and you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources.
Log Source Identifier Pattern	If you select **Use As A Gateway Log Source**, you can define a custom log source identifier. Use this option for events that are being processed and for log sources that are automatically discovered. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom log source identifier. The key is the identifier format string, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom log source identifier is displayed. The following examples show multiple key-value pair functions: `Patterns VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` `Events` `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` `Resulting custom log source identifier VPC-ACCEPT-OK`
Show Advanced Options	To configure the advanced options for event collection, set this option to **On**.
File Pattern	Type a regex for the file pattern that matches the files that you want to pull, such as `.*?\.json\.gz`. This option is available when you set **Show Advanced Options** to **On**.
Local Directory	The local directory on the Target Event Collector. The directory must exist before the protocol attempts to retrieve events. This option is available when you set **Show Advanced Options** to **On**.

Table 36. Alibaba Cloud Object Storage protocol common log source parameters (continued)	
Parameter	**Description**
Use Proxy	If QRadar accesses Alibaba Cloud Object Storage by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** parameters. If the proxy does not require authentication, leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Type a time interval to determine how frequently the protocol polls for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds. The minimum value is 1M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Alibaba Cloud Simple Log Service protocol configuration options

The Alibaba Cloud Simple Log Service protocol for IBM QRadar is an outbound or active protocol that collects logs from a specific Log Store available in the Alibaba Cloud Log application.

Important: Before you configure the Alibaba Cloud Simple Log Service protocol, configure the user access roles and the service credentials to access the Alibaba Cloud Log application.

- To access logs from the Log Store, create Log Store in the Log application. For more information, see Manage a Logstore.
- Create service credentials. For more information, see AccessKey Pair.

Table 37. Alibaba Cloud Simple Log Service protocol common log source parameters	
Parameter	**Description**
Protocol Configuration	Alibaba Cloud Simple Log Service
Log Source Identifier	Type a unique name for the log source. The log source identifier does not need to reference a specific server, and it can be the same value as the **Log Source Name**.
Access Key ID	The Access Key ID is generated when you configure the service credentials.
Secret Access Key	The Secret Access Key generates when you configure the service credentials.

Table 37. Alibaba Cloud Simple Log Service protocol common log source parameters (continued)	
Parameter	**Description**
Log Store Public Endpoint	The Log Store Public Endpoint on the Alibaba Cloud Log Application section. For more information, see Regions and endpoints.
Log Store Project Name	The Log Store Project Name on the Alibaba Cloud Log Application.
Log Store Name	The Log Store Name on the Alibaba Cloud Log Application's Log Store section.
Use Proxy	If QRadar accesses Alibaba Cloud Simple Log Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** parameters. If the proxy does not require authentication, leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Type a time interval to determine how frequently the protocol polls for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, **2H** = 2 hours, **15M** = 15 minutes, **30** = seconds. The minimum value is **60** (seconds) or **1M**.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Enable Advanced Options	Select this checkbox to enable the following configuration options: • **Allow Untrusted** • **Override Workflow**
Allow Untrusted	Enable this parameter for the protocol to accept self-signed and otherwise untrusted certificates that are located within the /opt/qradar/conf/trusted_certificates/ directory. If you disable the parameter, the scanner trusts only certificates that are signed by a trusted signer. The certificates must be in PEM or RED-encoded binary format and saved as a *.crt* or *.cert* file. Your workflow can override this setting. For more information about this process, see IBM Documentation.

Table 37. Alibaba Cloud Simple Log Service protocol common log source parameters (continued)	
Parameter	**Description**
Override Workflow	Enable this option to customize the workflow. When you enable this option, the **Workflow** and **Workflow Parameters** parameters appear.
Workflow	The XML document that defines how the protocol instance collects events from the target API. For more information on the default workflow, see “Alibaba Cloud Simple Log Service protocol workflow” on page 73.
Workflow Parameters	The XML document that contains the parameter values used directly by the workflow. For more information on the default workflow parameters, see “Alibaba Cloud Simple Log Service protocol workflow” on page 73.

Alibaba Cloud Simple Log Service protocol workflow

You can customize your workflow and workflow parameters based on the default workflow.

A workflow is an XML document that describes the event retrieval process. The workflow defines one or more parameters. These parameters can either be explicitly assigned values in the workflow XML or can derive values from the 'workflow parameter values XML' document. The workflow consists of multiple actions that run sequentially.

The default workflow and workflow parameter XML files are available on GitHub. For more information, see Alibaba Simple Log Service.

Alibaba Cloud Simple Log Service default workflow

The following example shows the default Alibaba Cloud Simple Log Service workflow:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--
AliCloud Workflow
-->
<Workflow name="AliCloudLogstore" version="1.0" minimumRecurrence="360" xmlns="http://
qradar.ibm.com/UniversalCloudRESTAPI/Workflow/V2">

    <Parameters>
        <Parameter name="host" label="Host" required="true" />
        <Parameter name="logstore_name" label="The name of the logstore we are pulling from"
required="true" />
        <Parameter name="access_key_id" label="Access Key" required="true" />
        <Parameter name="secret_key" label="Secret Key" required="true" secret="true" />
    </Parameters>

    <Actions>

        <!--
            ////////////////////////////////
            Get data from AliCloud Logstore
            ////////////////////////////////
        -->

        <!-- Get epoch from 10 minutes ago for "from" -->
        <Initialize path="/AliCloudLogstore/from" value="${(time() / 1000) - (60 * 15)}" />
        <!-- 15 minutes. Gets updated at end of workflow to current time to prepare for next
run, which queries to cover the time since last run. -->

        <!-- Get epoch for current time for "to" -->
        <Set path="/AliCloudLogstore/to" value="${time() / 1000}" />

        <!-- get ISO822 time for Date fields -->
```

```
        <FormatDate pattern="E, dd MMM yyyy HH:mm:ss z" timeZone="GMT" time="${/
AliCloudLogstore/to * 1000}" savePath="/AliCloudLogstore/current_time_formatted" />

        <!-- Header Definitions -->
        <Set path="/AliCloudLogstore/headers/apiVersion"   value="0.6.0" />
        <Set path="/AliCloudLogstore/headers/signatureMethod" value="hmac-sha1"/>

        <!--
            Parameters we can work with:
            https://www.alibabacloud.com/help/en/sls/developer-reference/api-getlogs?
spm=a2c63.p38356.0.0.56474d49f4kUvz#parameters

            Generating an HMAC-SHA1 Signature:
            https://www.alibabacloud.com/help/en/sls/developer-reference/request-signatures?
spm=a2c63.p38356.0.0.61b554d4UEl1ik#section-8e1-lk0-m0z
        -->

        <Set path="/AliCloudLogstore/offset" value="0"/>
        <Set path="/AliCloudLogstore/line" value="100"/> <!-- Page size to use, 100 is maximum
size. -->

        <SetStatus type="INFO" message="Querying for events..." />

        <!-- Set the endpoint once, as it does not change -->
        <Initialize path="/AliCloudLogstore/endpoint" value="/logstores/${/logstore_name}" />
        <Set path="/AliCloudLogstore/totalCount" value="0" />

        <DoWhile condition="/AliCloudLogstore/eventCount = /AliCloudLogstore/line"> <!-- If the
count of events received is not the full page size, then we have received them all.-->

            <!-- Build sorted parameter string (alphabetical) -->
            <Set path="/AliCloudLogstore/
params" value="?from=${/AliCloudLogstore/from}&amp;line=${/AliCloudLogstore/line}&amp;offset=${/
AliCloudLogstore/offset}&amp;to=${/AliCloudLogstore/to}&amp;type=log" />

            <!-- Build the signing string according to the documented requirements -->
            <Set path="/
AliCloudLogstore/signString" value="GET&#xA;&#xA;&#xA;${/AliCloudLogstore/
current_time_formatted}&#xA;x-log-apiversion:${/AliCloudLogstore/headers/apiVersion}&#xA;x-log-
bodyrawsize:0&#xA;x-log-signaturemethod:${/AliCloudLogstore/headers/signatureMethod}&#xA;${/
AliCloudLogstore/endpoint}${/AliCloudLogstore/params}"/>

            <!-- Create the signature -->
            <GenerateHMAC algorithm="SHA1" secretKey="${/secret_key}" message="${/
AliCloudLogstore/signString}" saveFormat="BASE64" savePath="/AliCloudLogstore/signature" />

            <!-- Create the authorization string -->
            <Set path="/AliCloudLogstore/authorization" value="LOG ${/access_key_id}:${/
AliCloudLogstore/signature}" />

            <!-- Fetch the Events - Parameters and headers need to be in
the same order as HMAC or signature will fail to pass. Alphabetical order
for each set, but Auth at the bottom of headers.-->
            <CallEndpoint url="https://${/host}${/AliCloudLogstore/endpoint}${/AliCloudLogstore/
params}" method="GET" savePath="/AliCloudLogstore/logs/response">

                <QueryParameter name="from" value="${/AliCloudLogstore/from}" />
                <QueryParameter name="line" value="${/AliCloudLogstore/line}" />
                <QueryParameter name="offset" value="${/AliCloudLogstore/offset}" />
                <QueryParameter name="to" value="${/AliCloudLogstore/to}" />
                <QueryParameter name="type" value="log" />

                <RequestHeader name="Date" value="${/AliCloudLogstore/
current_time_formatted}" />
                <RequestHeader name="Host" value="${/host}" />
                <RequestHeader name="x-log-apiversion" value="${/AliCloudLogstore/headers/
apiVersion}" />
                <RequestHeader name="x-log-bodyrawsize" value="0" />
                <RequestHeader name="x-log-signaturemethod" value="${/AliCloudLogstore/headers/
signatureMethod}" />
                <RequestHeader name="Authorization" value="${/AliCloudLogstore/
authorization}" />

            </CallEndpoint>

            <!-- Handle Errors -->
            <If condition="/AliCloudLogstore/logs/response/status_code != 200">
                <Abort reason="${/AliCloudLogstore/logs/response/body/errorCode}: ${/
AliCloudLogstore/logs/response/body/errorMessage}" />
            </If>

            <Set path="/AliCloudLogstore/eventCount" value="${count(/AliCloudLogstore/logs/
```

```
response/body)}" />
            <Log type="DEBUG" message="We received a total of ${/AliCloudLogstore/
eventCount} Events." />

            <!-- Post the Events -->
            <PostEvents path="/AliCloudLogstore/logs/response/body" source="${/host}" />

            <Set path="/AliCloudLogstore/totalCount" value="${/AliCloudLogstore/totalCount
+ /AliCloudLogstore/eventCount}" />

            <If condition="/AliCloudLogstore/eventCount = /AliCloudLogstore/line">
                <Set path="/AliCloudLogstore/offset" value="${/AliCloudLogstore/offset + /
AliCloudLogstore/line}" />
                <Log type="DEBUG" message="Full page received, continuing to loop
with offset of [${/AliCloudLogstore/offset}]" />
            </If>
            <Else>
                <Log type="DEBUG" message="The current iteration event count [$
{/AliCloudLogstore/eventCount}] was less that our  page size of [${/AliCloudLogstore/
line}], so we will exit the loop." />
                <Log type="DEBUG" message="Total events received in this iteration
is [${/AliCloudLogstore/totalCount}]." />
            </Else>

        </DoWhile>

        <SetStatus type="INFO" message="Successfully queried for events." />

        <!-- Set the next recurrence to begin immediately after the last end
time, increment 1 millisecond -->
        <Set path="/AliCloudLogstore/from" value="${/AliCloudLogstore/to + 1}"/>

    </Actions>

    <Tests>
        <DNSResolutionTest host="${/host}" />
        <TCPConnectionTest host="${/host}" />
        <SSLHandshakeTest host="${/host}" />
        <HTTPConnectionThroughProxyTest url="https://${/host}" />
    </Tests>

</Workflow>
```

Alibaba Cloud Simple Log Service default workflow parameters

The following example shows the default Alibaba Cloud Simple Log Service workflow parameters:

```
<?xml version="1.0" encoding="UTF-8" ?>
<WorkflowParameterValues xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
WorkflowParameterValues/V2">
    <!--
        Refer to https://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/
download%2Fpdf%2F29006%2FAPI_Reference_intl_en-US.pdf for URLs:

        The value of the Host parameter consists of a project name and a Log Service endpoint.
You must specify a project in the Host
        parameter when you call this API operation.

        See page 11 for different endpoints to use with your project.
    -->
    <Value name="host"  value="" />
    <Value name="logstore_name" value="" />
    <Value name="access_key_id" value="" />
    <Value name="secret_key"    value="" />
</WorkflowParameterValues>
```

Amazon AWS S3 REST API protocol configuration options

The Amazon AWS S3 REST API protocol is an active outbound protocol that collects AWS CloudTrail logs from Amazon S3 buckets.

Note: It's important to ensure that no data is missing when you collect logs from Amazon S3 to use with a custom DSM or other unsupported integrations. Because of the way that the S3 APIs return the data, all files must be in an alphabetically increasing order when the full path is listed. Make sure that the full path

name includes a full date and time in ISO9660 format (leading zeros in all fields and a YYYY-MM-DD date format).

Consider the following file path:

```
<Name>test-bucket</Name><Prefix>MyLogs/</Prefix><Marker>MyLogs/
2018-8-9/2018-08-09T23-5925.955097.log.g</Marker><MaxKeys>1000</
MaxKeys><IsTruncated>false</IsTruncated></ListBucketResult>
```

The full name of the file in the marker is `MyLogs/2018-8-9/2018-08-09T23-59-25.955097.log.gz` and the folder name is written as `2018-8-9` instead of `2018-08-09`. This date format causes an issue when data for the 10 September 2018 is presented. When sorted, the date displays as `2018-8-10` and the files are not sorted chronologically:

```
2018-10-1

2018-11-1

2018-12-31

2018-8-10

2018-8-9

2018-9-1
```

After data for 9 August 2018 comes in to IBM QRadar, you won't see data again until 1 September 2018 because leading zeros were not used in the date format. After September, you won't see data again until 2019. Leading zeros are used in the date (ISO 9660) so this issue does not occur.

By using leading zeros, files and folders are sorted chronologically:

```
2018-08-09

2018-08-10

2018-09-01

2018-10-01

2018-11-01

2018-12-01

2018-12-31
```

Restriction:

A log source can retrieve data from only one region, so use a different log source for each region. Include the region folder name in the file path for the **`Directory Prefix`** value when you use the Directory Prefix event collection method to configure the log source.

The following table describes the common parameter values to collect audit events by using the Directory Prefix collection method or the SQS event collection method. These collection methods use the Amazon AWS S3 REST API protocol.

Table 38. Amazon AWS S3 REST API protocol common log source parameters with the Directory Prefix method or the SQS method

Parameter	Description
Protocol Configuration	**Amazon AWS S3 REST API**

Table 38. Amazon AWS S3 REST API protocol common log source parameters with the Directory Prefix method or the SQS method (continued)

Parameter	Description
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one configured log source per DSM, ensure that you give each one a unique name.
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see Configuring security credentials for your AWS user account. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.
Assume an IAM Role	Enable this option by authenticating with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "`arn:`" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.

Table 38. Amazon AWS S3 REST API protocol common log source parameters with the Directory Prefix method or the SQS method (continued)

Parameter	Description
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This parameter can contain only upper and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.
Assume Role External ID	An identifier that you might need to assume a role in another account. You get this value from the administrator of the account that the role belongs to. This value can be any string, such as a passphrase, GUID, or account number. For more information, see How to use an external ID when granting access to your AWS resources to a third party (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html). If you enabled **Assume an IAM Role**, the **Assume Role External ID** parameter is displayed.
S3 Collection Method	**SQS Event Notifications** Poll an SQS Queue that contains ObjectCreated notifications that are configured on the S3 folders of your choice. Then, download and process the files that are referenced in the notification from the S3 bucket. You can use either a single queue or separate queues to cover multiple buckets and accounts. This decision depends on your configuration. For more information, see Table 40 on page 83. **Use a Specific Prefix** Logs within the specified folder are processed. For CloudTrail log sources, the prefix must be for a single account or region only. For other log sources, the prefix must point to a single directory that contains files with ISO8601 timestamps at the beginning of each file name. The timestamp in each file name ensures that the protocol collects new events with this method. For more information, see Table 39 on page 82.

Table 38. Amazon AWS S3 REST API protocol common log source parameters with the Directory Prefix method or the SQS method (continued)

Parameter	Description
Region Name	The region that the SQS Queue or the AWS S3 bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Event Format	Choose the format of the events that are contained in the files. **AWS CloudTrail JSON** Files that contain JSON formatted events for Amazon Cloud Trail (`.json.gz` files only). **LINEBYLINE** Raw log files that contain one record per line. Compression with gzip (`.gz` or `.gzip`), and zip (`.zip`) is supported. **AWS VPC Flow Logs** Files that contain AWS native/OCSF VPC Flow logs (`.txt.gz` or `gz.parquet` files only). This option sends flows to the **Network Activity** tab in QRadar. The configured log source doesn't show a **Last Event Seen Time** because the output is flow data. **AWS Network Firewall Logs** Files that contain AWS Network Firewall Alert or Flow logs. This option sends flow logs to the **Network Activity** tab and sends alert logs as events to the **Log Activity** tab in QRadar. The Amazon AWS Network Firewall DSM parses the logs. **Tip:** If your system is not licensed for flows, use the **LINEBYLINE** processor so that the DSM can parse the AWS Network Firewall logs. **W3C** For use with the Cisco Cloud Web Services DSM (`.gz` files only). **Cisco Umbrella CSV** For use with the Cisco Umbrella DSM (`.gz` files only). **Apache Parquet** Choose this option to convert Apache Parquet files into JSON events (`.gz.parquet` and `.parquet` files only).
Flow Destination Hostname	The flow processor hostname where the VPC Flow or AWS Network Firewall flow logs are sent. If you select **AWS VPC Flow Logs** or **AWS Network Firewall** in the **Event Format** parameter, you can configure this parameter.

Table 38. Amazon AWS S3 REST API protocol common log source parameters with the Directory Prefix method or the SQS method (continued)

Parameter	Description
Flow Destination Port	The flow processor port where the VPC Flow or AWS Network Firewall flow logs are sent. If you select **AWS VPC Flow Logs** or **AWS Network Firewall** in the **Event Format** parameter, you can configure this parameter.
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events that are being processed.
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK

Table 38. Amazon AWS S3 REST API protocol common log source parameters with the Directory Prefix method or the SQS method (continued)

Parameter	Description
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`.
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API protocol attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS S3 REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is `https://s3.amazonaws.com`.
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.

Table 38. Amazon AWS S3 REST API protocol common log source parameters with the Directory Prefix method or the SQS method (continued)	
Parameter	**Description**
Recurrence	How often a poll is made to scan for new data. If you are using the SQS event collection method, **SQS Event Notifications** can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, **Use a Specific Prefix** has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

The following table describes the specific parameter values to collect audit events by using the Directory Prefix event collection method:

Table 39. Amazon AWS S3 REST API protocol log source-specific parameters with the Directory Prefix method	
Parameter	**Description**
S3 Collection Method	Select **Use a Specific Prefix**.
Bucket Name	The name of the AWS S3 bucket where the log files are stored.

Table 39. Amazon AWS S3 REST API protocol log source-specific parameters with the Directory Prefix method (continued)	
Parameter	**Description**
Directory Prefix	The root directory location on the AWS S3 bucket from where the CloudTrail logs are retrieved; for example, `AWSLogs/<AccountNumber>/CloudTrail/<RegionName>/`. To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path. **Note:** • Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. • The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket. • If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use `folder1/folder2` instead).

The following table describes the parameters that require specific values to collect audit events by using the SQS event collection method:

Table 40. Amazon AWS S3 REST API protocol log source-specific parameters with the SQS method	
Parameter	**Description**
S3 Collection Method	Select **SQS Event Notifications**.
SQS Queue URL	The full URL that begins with `https://`, for the SQS Queue that is set up to receive notifications for ObjectCreated events from S3.

Related concepts

"Gateway log source" on page 15

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

Related information

Adding a log source

Configuring security credentials for your AWS user account

Creating an Identity and Access Management (IAM) user in the AWS Management Console

Amazon Web Services protocol configuration options

The Amazon Web Services (AWS) protocol is an outbound/active protocol for IBM QRadar that collects AWS CloudWatch Logs, Amazon Kinesis Data Streams, and Amazon Simple Queue Service (SQS) messages.

Important: The Amazon Web Services protocol requires QRadar 7.3.1 or later, and the IBM QRadar Log Source Management app.

You can use the Amazon Web Services protocol with either “Amazon Kinesis Data Streams” on page 84, “AWS CloudWatch Logs” on page 88, or “Amazon Simple Queue Service (SQS)” on page 92.

Amazon Kinesis Data Streams

The following table describes the protocol-specific parameters for collecting Amazon Kinesis Data Streams with the Amazon Web Services protocol:

Table 41. Amazon Web Services log source parameters for Amazon Kinesis Data Streams

Parameter	Description
Protocol Configuration	Select **Amazon Web Services** from the Protocol Configuration list.
Authentication Method	**Access Key ID/Secret Key** Standard authentication that can be used from anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.
Assume an IAM Role	Enable this option to authenticate with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "`arn:`" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This parameter can contain only upper and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.
Assume Role External ID	**Assume Role External ID** is an optional identifier that is required to assume a role in a different account. If the account administrator, to which the role belongs, provides you with an external ID, then insert that value in the **Assume Role External ID** parameter. This value can either be a string, a passphrase, a GUID, or an account number. For more information, see AWS documentation Using an external ID for third-party access.

Table 41. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Regions	Toggle each region that is associated with the Amazon Web Service that you want to collect logs from.
AWS Service	From the **AWS Service** list, select **Kinesis Data Streams**.
Kinesis Data Stream	The Kinesis Data Stream from which to consume data.
Enable Kinesis Advanced Options	Enable the following optional advanced configuration values. Advanced option values are only used when this option is chosen; otherwise, the default values are used. **Initial Position in Stream** This option controls which data to pull on a newly configured log source. Select **Latest** to pull the latest data that is available. Select **Trim Horizon** to pull the oldest data that is available. **Kinesis Worker Thread Count** The number of worker threads to use for Kinesis Data Stream processing. Each worker thread can process approximately 10000 - 20000 events per second depending on record size and system load. If your log source is not able to process the new data in the stream, you can increase the number of threads here to a maximum of 16. The allowed range is 1 - 16. The default value is 2. **Checkpoint Interval** The interval (in seconds) at which to checkpoint data sequence numbers. Each record from a shard in a Kinesis Data Stream has a sequence number. Checkpointing your position allows this shard to resume processing at the same point if processing fails or a service restarts. A more frequent interval reduces data duplication but increases Amazon Dynamo DB usage. The allowed range is 1 - 3600 seconds. The default is 10 seconds. **Kinesis Application** Leave this option blank to have this log source consume data from all available shards in the Kinesis Data Stream. To have multiple log sources on multiple event processors scale log consumption without loss or duplication, use a common Kinesis Application across those log sources (Example: ProdKinesisConsumers). **Partition** Select this option to collect data from a specific partition in the Kinesis Data Stream by specifying a partition name.

Table 41. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Extract Original Event	Forwards only the original event that was added to the Kinesis Data Stream. Kinesis logs wrap the events that they receive with extra metadata. Select this option if you want only the original event that was sent to AWS without the additional stream metadata through Kinesis. The original event is the value for the message key that is extracted from the Kinesis log. The following Kinesis logs event example shows the original event that is extracted from the Kinesis log in highlighted text: `{"owner":"123456789012","subscriptionFilters":["allEvents"], "logEvents": [{"id":"35093963143971327215510178578576502306458824699048362100", "message":"{\"eventVersion\":\"1.05\",\"userIdentity\": {\"type\":\"AssumedRole\", \"principalId\":\"ARO1GH58EM3ESYDW3XHP6:test_session\",\"arn\":\"arn:aws:sts::123456789012:assumed-role\/CVDevABRoleToBeAssumed\/test_visibility_session\", \"accountId\":\"123456789012\",\"accessKeyId\":\"ASIAXXXXXXXXXXXXXXX\",\"sessionContext\":{\"sessionIssuer\": {\"type\":\"Role\",\"principalId\":\"AROAXXXXXXXXXXXXXXX\", \"arn\":\"arn:aws:iam::123456789012:role\/CVDevABRoleToBeAssumed\",\"accountId\":\"123456789012\", \"userName\":\"CVDevABRoleToBeAssumed\"},\"webIdFederationData\": {},\"attributes\":{\"mfaAuthenticated\":\"false\", \"creationDate\":\"2019-11-13T17:01:54Z\"}}},\"eventTime\":\"2019-11-13T17:43:18Z\",\"eventSource\":\"cloudtrail.amazonaws.com\", \"eventName\":\"DescribeTrails\",\"awsRegion\":\"ap-northeast-1\",\"sourceIPAddress\":\"192.0.2.1\",\"requestParameters\": null,\"responseElements\":null, \"requestID\":\"41e62e80-b15d-4e3f-9b7e-b309084dc092\",\"eventID\":\"904b3fda-8e48-46c0-a923-f1bb2b7a2f2a\",\"readOnly\":true,\"eventType\":\"AwsApiCall\", \"recipientAccountId\":\"123456789012\"}","timestamp":1573667733143}], "messageType":"DATA_MESSAGE","logGroup":"CloudTrail\/DefaultLogGroup","logStream":"123456789012_CloudTrail_us-east-2_2"}` (highlighted text: `{\"eventVersion\":\"1.05\",\"userIdentity\": {\"type\":\"AssumedRole\", \"principalId\":\"ARO1GH58EM3ESYDW3XHP6:test_session\",\"arn\":\"arn:aws:sts::123456789012:assumed-role\/CVDevABRoleToBeAssumed\/test_visibility_session\", \"accountId\":\"123456789012\",\"accessKeyId\":\"ASIAXXXXXXXXXXXXXXX\",\"sessionContext\":{\"sessionIssuer\": {\"type\":\"Role\",\"principalId\":\"AROAXXXXXXXXXXXXXXX\", \"arn\":\"arn:aws:iam::123456789012:role\/CVDevABRoleToBeAssumed\",\"accountId\":\"123456789012\", \"userName\":\"CVDevABRoleToBeAssumed\"},\"webIdFederationData\": {},\"attributes\":{\"mfaAuthenticated\":\"false\", \"creationDate\":\"2019-11-13T17:01:54Z\"}}},\"eventTime\":\"2019-11-13T17:43:18Z\",\"eventSource\":\"cloudtrail.amazonaws.com\", \"eventName\":\"DescribeTrails\",\"awsRegion\":\"ap-northeast-1\",\"sourceIPAddress\":\"192.0.2.1\",\"requestParameters\": null,\"responseElements\":null, \"requestID\":\"41e62e80-b15d-4e3f-9b7e-b309084dc092\",\"eventID\":\"904b3fda-8e48-46c0-a923-f1bb2b7a2f2a\",\"readOnly\":true,\"eventType\":\"AwsApiCall\", \"recipientAccountId\":\"123456789012\"}`)
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events that are being processed.

Table 41. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

AWS CloudWatch Logs

The following table describes the protocol-specific parameters for collecting AWS CloudWatch Logs with the Amazon Web Services protocol:

Table 42. Amazon Web Services log source parameters for AWS CloudWatch Logs

Parameter	Description
Protocol Configuration	Select **Amazon Web Services** from the Protocol Configuration list.
Authentication Method	**Access Key ID/Secret Key** Standard authentication that can be used from anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.
Assume an IAM Role	Enable this option by authenticating with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "`arn:`" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This parameter can contain only upper and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.

Table 42. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)

Parameter	Description
Assume Role External ID	**Assume Role External ID** is an optional identifier that is required to assume a role in a different account. If the account administrator, to which the role belongs, provides you with an external ID, then insert that value in the **Assume Role External ID** parameter. This value can either be a string, a passphrase, a GUID, or an account number. For more information, see AWS documentation Using an external ID for third-party access.
Regions	Toggle each region that is associated with the Amazon Web Service that you want to collect logs from.
AWS Service	From the **AWS Service** list, select **CloudWatch Logs**.
Log Group	The name of the log group in Amazon CloudWatch where you want to collect logs from. **Tip:** A single log source collects CloudWatch Logs from one log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group.
Enable CloudWatch Advanced Options	Enable the following optional advanced configuration values. Advanced option values are only used when this option is chosen; otherwise, the default values are used. **Log Stream** The name of the log stream within a log group. If you want to collect logs from all log streams within a log group, leave this field blank. **Filter Pattern** Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specified are collected from CloudWatch Logs. If you type ACCEPT as the Filter Pattern value, only the events that contain the word ACCEPT are collected, as shown in the following example. `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Event Delay** Delay in seconds for collecting data. **Other Region(s)** Deprecated. Use **Regions** instead.

Table 42. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)

Parameter	Description
Extract Original Event	Forwards only the original event that was added to the CloudWatch Logs. CloudWatch logs wrap the events that they receive with extra metadata. Select this option if you want to collect only the original event that was sent to AWS without the additional stream metadata through CloudWatch Logs. The original event is the value for the message key that is extracted from the CloudWatch log. The following CloudWatch Logs event example shows the original event that is extracted from CloudWatch Logs in highlighted text: `{LogStreamName: 123456786_CloudTrail_us-east-2,` `Timestamp: 1505744407363, Message:` **`{"eventVersion":"1.05","userIdentity":`** **`{"type":`** **`"IAMUser","principalId":"AAAABBBCCCDDDBBBCCC"`** **`,`** **`"arn":"arn:aws:iam::1234567890:user/`** **`<username>",`** **`"accountId":"1234567890","accessKeyId":`** **`"AAAABBBBCCCCDDDD","userName":"User-Name",`** **`"sessionContext":{"attributes":`** **`{"mfaAuthenticated":"false","creationDate":`** **`"2017-09-18T13:22:10Z"}},"invokedBy":`** **`"signin.amazonaws.com"},"eventTime":`** **`"2017-09-18T14:10:15Z","eventSource":`** **`"cloudtrail.amazonaws.com","eventName":`** **`"DescribeTrails","awsRegion":"us-east-1",`** **`"sourceIPAddress":"192.0.2.1","userAgent":`** **`"signin.amazonaws.com","requestParameters":`** **`{"includeShadowTrails":false,"trailNameList":`** **`[]},"responseElements":null,"requestID":`** **`"11b1a00-7a7a-11a1-1a11-44a4aaa1a","eventID":`** **`"a4914e00-1111-491d-bbbb-a0dd3845b302",`** **`"eventType":"AwsApiCall","recipientAccountId"`** **`:`** **`"1234567890"}`**`,IngestionTime: 1505744407506,` `EventId:` `335792223611111122479126672222222513333}`
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events that are being processed.

Table 42. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)

Parameter	Description
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.

Table 42. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)	
Parameter	**Description**
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Amazon Simple Queue Service (SQS)

The following table describes the protocol-specific parameters for collecting Amazon SQS log sources with the Amazon Web Services protocol:

Table 43. Amazon Web Services log source parameters for Amazon SQS	
Parameter	**Description**
Protocol Configuration	Select **Amazon Web Services** from the Protocol Configuration list.
Authentication Method	**Access Key ID/Secret Key** Standard authentication that can be used from anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.

Table 43. Amazon Web Services log source parameters for Amazon SQS (continued)	
Parameter	**Description**
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.
Assume an IAM Role	Enable this option by authenticating with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "`arn:`" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This name can contain only uppercase and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.
Assume Role External ID	**Assume Role External ID** is an optional identifier that is required to assume a role in a different account. If the account administrator, to which the role belongs, provides you with an external ID, then insert that value in the **Assume Role External ID** parameter. This value can either be a string, a passphrase, a GUID, or an account number. For more information, see AWS documentation Using an external ID for third-party access.
Regions	Toggle each region that is associated with the Amazon Web Service that you want to collect logs from.
AWS Service	From the **AWS Service** list, select **SQS Queue**.
SQS Queue URL	The full URL of the SQS queue to pull data from, starting with `https://`, such as `https://sqs.us-east-2.amazonaws.com/1234567890123/CloudTrail_SQS_QRadar`. For more information, see Amazon S3 Event Notifications (https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html).

Table 43. Amazon Web Services log source parameters for Amazon SQS (continued)

Parameter	Description
Extract Original Event	Forwards only the original event that was added to the SQS queue to QRadar, select this option.
Original Event JSON Element	When you use this option to extract original event with SQS, the original event might be in a specific JSON element. If so, you must specify the name of the top-level JSON element that contains the original event. This option also unescapes any data that is contained within that element. For example, when the `Message` element is used, it takes that root element and unescapes the nested JSON if necessary: `{ "Type" : "Notification", "MessageId" : "6d11936e-2361-5dc1-a689-c590f69c73da", "Subject" : "Test Notification", "Message" : "{\"eventVersion\":\"2.1\", \"eventSource\":\"aws:s3\", \"awsRegion\":\"us-east-1\", \"eventTime\":\"2020-04-01T17:47:39.107Z\"}" }` The unescaped data then appears as this extracted original event: `{"eventVersion":"2.1", "eventSource":"aws:s3", "awsRegion":"us-east-1", "eventTime":"2020-04-01T17:47:39.107Z"}`
Use As A Gateway Log Source	If you do not want to define a custom log source identifier for events, clear the checkbox. If you don't select **Use As A Gateway Log Source** and you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources.

Table 43. Amazon Web Services log source parameters for Amazon SQS (continued)

Parameter	Description
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier. This option can be defined for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.

Table 43. Amazon Web Services log source parameters for Amazon SQS (continued)	
Parameter	**Description**
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Related concepts

"Gateway log source" on page 15

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

Related information

Adding a log source

Apache Kafka protocol configuration options

IBM QRadar uses the Apache Kafka protocol to read streams of event data from topics in a Kafka cluster that uses the Consumer API. A topic is a category or feed name in Kafka where messages are stored and published. The Apache Kafka protocol is an outbound or active protocol, and can be used as a gateway log source by using a custom log source type.

The Apache Kafka protocol supports topics of almost any scale. You can configure multiple QRadar collection hosts (EP/ECs) to collect from a single topic; for example, all firewalls. For more information, see the Kafka Documentation (http://kafka.apache.org/documentation/).

The following table describes the protocol-specific parameters for the Apache Kafka protocol:

Table 44. Apache Kafka protocol parameters	
Parameter	**Description**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Apache Kafka log source, ensure that you give each one a unique name.

Table 44. Apache Kafka protocol parameters (continued)	
Parameter	**Description**
Bootstrap Server List	The *<hostname/ip>:<port>* of the bootstrap server (or servers). Multiple servers can be specified in a comma-separated list, such as in this example: *hostname1:9092,1.1.1.1:9092*.
Consumer Group	A unique string or label that identifies the consumer group that this log source belongs to. Each record that is published to a Kafka topic is delivered to one consumer instance within each subscribing consumer group. Kafka uses these labels to load balance the records over all consumer instances in a group.
Topic Subscription Method	The method that is used for subscribing to Kafka topics. Use the **List Topics** option to specify a specific list of topics. Use the **Regex Pattern Matching** option to specify a regular expression to match against available topics.
Topic List	A list of topic names to subscribe to. The list must be comma-separated; for example: `Topic1,Topic2,Topic3` This option is only displayed when **List Topics** is selected for the **Topic Subscription Method** option.
Topic Filter Pattern	A regular expression to match the topics to subscribe to. This option is only displayed when **Regex Pattern Matching** is selected for the **Topic Subscription Method** option.
Use SASL Authentication	This option displays SASL authentication configuration options. When used without client authentication, you must place a copy of the server certificate in the `/opt/qradar/conf/trusted_certificates/` directory.
SASL Mechanism	Select the SASL mechanism that is compatible with your Kafka configuration: • `PLAIN` • `SCRAM-SHA-256` • `SCRAM-SHA-512`
SASL Username	The username that is used for SASL authentication.
SASL Password	The password that is used for SASL authentication.
Use SSL	Select this option to enable SSL (TLS) encryption if your Kafka configuration supports or requires it.

Table 44. Apache Kafka protocol parameters (continued)

Parameter	Description
Use Client Authentication	Displays the client authentication configuration options. You can enable this option only if you enable the **Use SSL** parameter and use SSL (TLS) for authentication and data transfer.
Key Store/Trust Store Type	The archive file format for your keystore and truststore type. The following options are available for the archive file format: • JKS • PKCS12
Trust Store Filename	The name of the truststore file. The truststore must be placed in `/opt/qradar/conf/trusted_certificates/kafka/`. The file contains the username and password.
Key Store Filename	The name of the keystore file. The keystore must be placed in `/opt/qradar/conf/trusted_certificates/kafka/`. The file contains the username and password.
Use As A Gateway Log Source	This option enables collected events to go through the QRadar Traffic Analysis engine and to automatically detect the appropriate log sources.

Table 44. Apache Kafka protocol parameters (continued)

Parameter	Description
Log Source Identifier Pattern	Defines a custom Log Source Identifier for events that are being processed, if the **Use As A Gateway Log Source** checkbox is selected. Key-value pairs are used to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Multiple key-value pairs are defined by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Show Advanced Options	Show optional advanced options for the Kafka configuration. The advanced option values are in effect whether they are shown or not.
Use Payload Extraction	Enable this parameter to extract the payload and send it to the event pipeline. This parameter identifies the specified payload if it is somewhere within the Kafka log records. Multiple regular expressions can be defined by entering each pattern on a new line. When multiple Payload Extraction patterns are used, they are evaluated in order until a match is found and an extracted payload can be returned. This payload extraction occurs before any character replacements.
Payload Extraction Regular Expression	A regular expression that identifies the specified payload within the Kafka log records so it can be sent to QRadar. This expression must include a capture group and uses the first capture group as the new payload.

Table 44. Apache Kafka protocol parameters (continued)

Parameter	Description
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns and extracts payloads from events without running the regex for every event, which increases the parsing speed. In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Character Sequence Replacement	Replaces specific literal character sequences that are in the event payload with actual characters. One or more of the following options are available: • **Newline(CR LF) Character (\r\n)** • **Line Feed Character (\n)** • **Carriage Return Character (\r)** • **Tab Character (\t)** • **Space Character (\s)** • **Unescape JSON Data** **Tip:** Select this option if you want the entire payload to be JSON unescaped after any payload extraction. When you unescape JSON messages, any character that prevents parsing is removed from the message. Enable this option when you want to extract JSON messages that are embedded in JSON objects.

Table 44. Apache Kafka protocol parameters (continued)

Parameter	Description
Kafka Consumer Properties Override	A list of `key=value` pairs that can be used to provide specific configuration properties to the Kafka Consumer. The list uses one pair per line. For example, the `key=value` pair `session.timeout.ms=10000` configures the session timeout in milliseconds. For a list of available `key=value` pairs, see the Kafka Consumer Configuration documentation (https://ibm.biz/kafkaconsumerconfigs). Any parameters that are entered in this field override any previous ones set during the configuration phase of the log source. These parameters include, but are not limited to, the following examples: • `fetch.max.bytes` • `group.id` • `ssl.enabled.protocols` You cannot enter any password-type properties with secret values in this field. These properties include, but are not limited to, the following examples: • `ssl.key.password` • `ssl.key.password` • `ssl.keystore.password` • `ssl.truststore.password` • `sasl.jaas.config` • `ssl.truststore.certificates` • `ssl.keystore.certificate.chain` • `ssl.keystore.key` Use the **Private Key Password**, **Trust Store Password**, **Key Store Password**, **Private Key Password**, or **SASL Password** fields to enter password-type Kafka consumer properties.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.

Related concepts

"Gateway log source" on page 15

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

Related information

Adding a log source

Configuring Apache Kafka to enable Client Authentication

This task discusses how to enable Client Authentication with Apache Kafka.

Before you begin

1. Ensure that the ports that are used by the Kafka server are not blocked by a firewall.
2. To enable client authentication between the Kafka consumers (QRadar) and a Kafka brokers, a key and certificate for each broker and client in the cluster must be generated. The certificates also need to be signed by a certificate authority (CA).

About this task

In the following steps, you generate a CA, sign the client and broker certificates with it, and add it to the client and broker truststores. You also generate the keys and certificates by using the Java keytool and OpenSSL. Alternatively, an external CA can be used along with multiple CAs, one for signing broker certificates and another for client certificates.

Procedure

1. Generate the truststore, keystore, private key, and CA certificate.

   Note: Replace PASSWORD, VALIDITY, SERVER_ALIAS and CLIENT_ALIAS in the following commands with appropriate values.

   a) Generate Server keystore.

   Note:

   The common name (CN) of the broker certificates must match the fully qualified domain name (FQDN) of the server/host. The Kafka Consumer client that is used by QRadar compares the CN with the DNS domain name to ensure that it is connecting to the correct broker instead of a malicious one. Make sure to enter the FQDN for the *CN*/*First and Last name* value when you generate the Server keystore.

   ```
   keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS
    -validity VALIDITY -genkey
   ```

   Example

   ```
   keytool -keystore kafka.server.keystore.jks -alias server.hostname
    -validity 365 -genkey
   ```

   b) Generate CA Certificate.

   Note:

   This CA certificate can be used to sign all broker and client certificates.

   ```
   openssl req -new -x509 -keyout ca-key -out ca-cert -days VALIDITY
   ```

   Example

   ```
   openssl req -new -x509 -keyout ca-key -out ca-cert -days 365
   ```

   c) Create Server truststore and import CA Certificate.

```
keytool -keystore kafka.server.truststore.jks -alias CARoot
 -import -file ca-cert
```

d) Create Client truststore and import CA Certificate.

```
keytool -keystore kafka.client.truststore.jks -alias CARoot
 -import -file ca-cert
```

e) Generate a Server Certificate and sign it using the CA.

```
keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS
 -certreq -file cert-file
```

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out
 cert-signed -days VALIDITY -CAcreateserial
```

Example

```
keytool -keystore kafka.server.keystore.jks -alias server.hostname
-certreq -file cert-file
```

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out
 cert-signed -days 365 -CAcreateserial
```

f) Import CA Certificate into the Server keystore.

```
keytool -keystore kafka.server.keystore.jks -alias CARoot
 -import -file ca-cert
```

g) Import Signed Server Certificate to the Server keystore.

```
keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -import
 -file cert-signed
```

Example

```
keytool -keystore kafka.server.keystore.jks -alias server.hostname
 -import -file cert-signed
```

h) Export the Server Certificate into the binary DER file.

Note: The `keytool -exportcert` command uses the DER format by default. Place the certificate in the `trusted_certificates/` directory of any EP that communicates with Kafka. You need the server certificate for every bootstrap server that you use in the configuration. Otherwise, QRadar rejects the TLS handshake with the server.

```
keytool -exportcert -keystore kafka.server.keystore.jks -alias
 SERVER_ALIAS -file SEVER_ALIAS.der
```

Example

```
keytool -exportcert -keystore kafka.server.keystore.jks -alias
 server.hostname -file server.hostname.der
```

i) Generate a Client keystore.

```
keytool -keystore kafka.client.keystore.jks -alias CLIENT_ALIAS
 -validity VALIDITY -genkey
```

Example

```
keytool -keystore kafka.client.keystore.jks -alias client.hostname
 -validity 365 -genkey
```

j) Generate a Client Certificate and sign it using the CA.

```
keytool -keystore kafka.client.keystore.jks -alias CLIENT_ALIAS
 -certreq -file client-cert-file
```

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in client-cert-file -out
 client-cert-signed -days VALIDITY -CAcreateserial
```

Example

```
keytool -keystore kafka.client.keystore.jks -alias client.hostname
 -certreq -file client-cert-file
```

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in client-cert-file
 -out client-cert-signed -days 365 -CAcreateserial
```

k) Import CA Certificate into the Client keystore.

```
keytool -keystore kafka.client.keystore.jks -alias CARoot
 -import -file ca-cert
```

l) Import Signed Client Certificate to the Client keystore.

```
keytool -keystore kafka.client.keystore.jks -alias CLIENT_ALIAS
 -import -file client-cert-signed
```

Example

```
keytool -keystore kafka.client.keystore.jks -alias client.hostname
 -import -file client-cert-signed
```

m) Copy Client keystore and truststore and to QRadar.

i) Copy the `kafka.client.keystore.jks` and `kafka.client.truststore.jks` to `/opt/qradar/conf/trusted_certificates/kafka/` on each of the Event processors that the log source is configured for.

ii) Copy the server certificates `<filename>.der` that were generated for each broker to `/opt/qradar/conf/trusted_certificates/`.

2. Configure Kafka brokers for Client Authentication.

a) Find the **Socket Server Settings** section.

b) Complete 1 of the following options:

- If you are not using SASL Authentication, change `listeners=PLAINTEXT://:<port>` to `listeners=SSL://:<PORT>` and add `security.inter.broker.protocol=SSL`.
- If you are using SASL Authentication, change `listeners=PLAINTEXT://:<port>` to `listeners=SASL_SSL://:<PORT>` and add `security.inter.broker.protocol=SASL_SSL`.

c) Add the following properties to force encrypted communication between brokers and between the brokers and clients. Adjust the paths, file names, and passwords as you need them. These properties are the truststore and keystore of the **server**:

```
security.inter.broker.protocol=SSL

ssl.client.auth=required

ssl.keystore.location=/somefolder/kafka.server.keystore.jks

ssl.keystore.password=test1234

ssl.key.password=test1234

ssl.truststore.location=/somefolder/kafka.server.truststore.jks

ssl.truststore.password=test1234
```

Important: Since the passwords are stored in plain text in the `server.properties`, it is advised that access to the file is restricted by way of file system permissions.

d) Restart the Kafka brokers that had their `server.properties` modified.

Configuring Apache Kafka to enable SASL Authentication

This task discusses how to enable SASL Authentication with Apache Kafka without SSL Client Authentication.

Before you begin

If you are using SASL Authentication with Client Authentication enabled, see "Configuring Apache Kafka to enable Client Authentication" on page 102.

1. Ensure that the ports that are used by the Kafka server are not blocked by a firewall.
2. To enable client authentication between the Kafka consumers (QRadar) and a Kafka brokers, a key and certificate for each broker and client in the cluster must be generated. The certificates also need to be signed by a certificate authority (CA).

About this task

In the following steps, you generate a CA, sign the client and broker certificates with it, and add it to the broker truststores. You also generate the keys and certificates by using the Java keytool and OpenSSL. Alternatively, an external CA can be used along with multiple CAs, one for signing broker certificates and another for client certificates.

Procedure

1. Generate the truststore, keystore, private key, and CA certificate.

   Note: Replace PASSWORD, VALIDITY, SERVER_ALIAS and CLIENT_ALIAS in the following commands with appropriate values.

   a) Generate Server keystore.

   Note:

   The common name (CN) of the broker certificates must match the fully qualified domain name (FQDN) of the server/host. The Kafka Consumer client that is used by QRadar compares the CN with the DNS domain name to ensure that it is connecting to the correct broker instead of a malicious one. Make sure to enter the FQDN for the *CN*/*First and Last name* value when you generate the Server keystore.

   ```
   keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS
    -validity VALIDITY -genkey
   ```

   Example

   ```
   keytool -keystore kafka.server.keystore.jks -alias server.hostname
    -validity 365 -genkey
   ```

   b) Generate CA Certificate.

   Note:

   This CA certificate can be used to sign all broker and client certificates.

   ```
   openssl req -new -x509 -keyout ca-key -out ca-cert -days VALIDITY
   ```

   Example

   ```
   openssl req -new -x509 -keyout ca-key -out ca-cert -days 365
   ```

c) Create Server truststore and import CA Certificate.

```
keytool -keystore kafka.server.truststore.jks -alias CARoot
 -import -file ca-cert
```

d) Generate a Server Certificate and sign it using the CA.

```
keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS
 -certreq -file cert-file
```

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out
 cert-signed -days VALIDITY -CAcreateserial
```

Example

```
keytool -keystore kafka.server.keystore.jks -alias server.hostname
-certreq -file cert-file
```

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out
 cert-signed -days 365 -CAcreateserial
```

e) Import CA Certificate into the Server keystore.

```
keytool -keystore kafka.server.keystore.jks -alias CARoot
 -import -file ca-cert
```

f) Import Signed Server Certificate to the Server keystore.

```
keytool -keystore kafka.server.keystore.jks -alias SERVER_ALIAS -import
 -file cert-signed
```

Example

```
keytool -keystore kafka.server.keystore.jks -alias server.hostname
 -import -file cert-signed
```

g) Export the Server Certificate into the binary DER file.

Note: The `keytool -exportcert` command uses the DER format by default. Place the certificate in the `trusted_certificates/` directory of any EP that communicates with Kafka. You need the server certificate for every bootstrap server that you use in the configuration. Otherwise, QRadar rejects the TLS handshake with the server.

```
keytool -exportcert -keystore kafka.server.keystore.jks -alias
 SERVER_ALIAS -file SEVER_ALIAS.der
```

Example

```
keytool -exportcert -keystore kafka.server.keystore.jks -alias
 server.hostname -file server.hostname.der
```

2. Configure Kafka brokers for Client Authentication.

a) Find the **Socket Server Settings** section and then change `listeners=PLAINTEXT://:<port>` to `listeners=SSL://:<PORT>`.

b) Add the following properties to force encrypted communication between brokers and between the brokers and clients. Adjust the paths, file names, and passwords as you need them. These properties are the truststore and keystore of the **server**:

`security.inter.broker.protocol=SASL_SSL`

`ssl.client.auth=none`

`ssl.keystore.location=/somefolder/kafka.server.keystore.jks`

`ssl.keystore.password=test1234`

```
ssl.key.password=test1234
ssl.truststore.location=/somefolder/kafka.server.truststore.jks
ssl.truststore.password=test1234
```

Note:

Since the passwords are stored in plain text in the `server.properties`, it is advised that access to the file is restricted by way of file system permissions.

c) Restart the Kafka brokers that had their `server.properties` modified.

Troubleshooting Apache Kafka

This reference provides troubleshooting options for configuring Apache Kafka to enable Client Authentication.

Apache Kafka

Table 45. Troubleshooting for Apache Kafka Client Authentication

Issue	Solution
The **Use As A Gateway Log Source** option is selected in the log source configuration, but log sources are not being automatically detected.	Events being streamed from Kafka must contain a valid Syslog RFC3164 or RFC5424 compliant header, so QRadar can correctly determine the log source identifier of each event.
No events are being received and the following error is displayed in the log source configuration form: "`Encountered an error while attempting to fetch topic metadata... Please verify the configuration information.`"	Verify that the bootstrap server and port details that are entered into the configuration are valid. If Client Authentication is enabled, verify the following things: • The passwords that are entered are correct. • The client truststore and keystore files are present in `/opt/qradar/conf/trusted_certificates/kafka/` folder and the file names specified match. • The server certificates (`<filename>.der`) are present in `/opt/qradar/conf/trusted_certificates/` folder.
No events are being received and the following error is displayed in the log source configuration form: "`The user specified list of topics did not contain any topics that exists in the Kafka cluster. Please verify the topic list.`"	When you use the **List Topics** options to subscribe to topics, QRadar attempts to verify the topics available in the Kafka cluster to the specified topics when the log source is initially started. If no topics match between what was entered in the configuration and what is available on the cluster, you are presented with this message. Verify the topic names that are entered in the configuration; also, consider the use of the **Regex Pattern Matching** option for subscribing to topics.
When any parameter value in the property file on the Kafka server is changed, expected results are not received.	Disable, then re-enable the Kafka log source.

Blue Coat Web Security Service REST API protocol configuration options

To receive events from Blue Coat Web Security Service, configure a log source to use the Blue Coat Web Security Service REST API protocol.

The Blue Coat Web Security Service REST API protocol is an outbound/active protocol that queries the Blue Coat Web Security Service Sync API and retrieves recently hardened log data from the cloud.

The following table describes the protocol-specific parameters for the Blue Coat Web Security Service REST API protocol:

Table 46. Blue Coat Web Security Service REST API protocol parameters

Parameter	Description
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Blue Coat Web Security Service REST API log source, ensure that you give each one a unique name.
API Username	The API user name that is used for authenticating with the Blue Coat Web Security Service. The API user name is configured through the Blue Coat Threat Pulse Portal.
Password	The password that is used for authenticating with the Blue Coat Web Security Service.
Confirm Password	Confirmation of the **Password** field.
Use Proxy	When you configure a proxy, all traffic for the log source travels through the proxy for QRadar to access the Blue Coat Web Security Service. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	You can specify when the log collects data. The format is M/H/D for Months/Hours/Days. The default is 5 M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Centrify Redrock REST API protocol configuration options

The Centrify Redrock REST API protocol is an outbound/active protocol for IBM Security QRadar that collects events from Centrify Identity Platform.

The Centrify Redrock REST API protocol supports Centrify Identity Platform and CyberArk Identity Security Platform.

The following parameters require specific values to collect events from Centrify Identity Platform:

Table 47. Centrify Redrock REST API protocol log source parameters	
Parameter	**Value**
Log Source type	Centrify Identity Platform
Protocol Configuration	Centrify Redrock REST API
Log Source Identifier	A unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the **Log Source Name**. If you have more than one Centrify Identity Platform log source that is configured, you might want to identify the first log source as *centrify1*, the second log source as *centrify2*, and the third log source as *centrify3*.
Tenant ID	The Centrify assigned unique customer or tenant ID.
Tenant URL	Automatically generated tenant URL for the specified tenant ID. For example, `tenantId.my.centrify.com`
Username	The user name that is associated with the Cloud service for Centrify Identity Platform.
Password	The password that is associated with the Centrify Identity Platform user name.
Event Logging Filter	Select the logging level of the events that you want to retrieve. **Info**, **Warning** and **Error** are selectable. At least one filter must be selected.
Allow Untrusted Certificates	Enable this option to allow self-signed, untrusted certificates. Do not enable this option for SaaS hosted tenants. However, if required, you can enable this option for other tenant configurations. The certificate must be downloaded in PEM or DER encoded binary format and then placed in the `/opt/qradar/conf/trusted_certificates/` directory with a `.cert` or `.crt` file extension.
Use Proxy	When a proxy is configured, all traffic from the Centrify Redrock REST API travels through the proxy. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.

Table 47. Centrify Redrock REST API protocol log source parameters (continued)	
Parameter	**Value**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Recurrence	The time interval can be in hours (H), minutes (M) or days (D). The default is 5 minutes (5M).

Related information

Adding a log source

Cisco Duo protocol configuration options

To receive authentication events from Cisco Duo, configure a log source to use the Cisco Duo protocol.

The Cisco Duo protocol is an active outbound protocol that collects authentication logs from the Cisco Duo Admin API, and sends authentication events to IBM QRadar.

Important: Before you configure a log source to use the Cisco Duo protocol, you must obtain your keys from the Cisco Duo admin portal.

1. Log in to the Cisco Duo admin portal (https://admin.duosecurity.com/).
2. From the dashboard, go to the **Applications** tab, and then click **Protect an Application**.
3. Navigate to the **Admin API** application, and then click **Protect**.
4. In the Permissions menu, select **Grant read log** so that Cisco can collect other authentication logs from the Admin API.
5. Copy the values for **Integration key**, **Secret key**, and **API hostname**. You need these values when you configure the Cisco Duo protocol parameters.

Important: Because Cisco Duo has rate limits on API calls, you can create only one log source per customer account.

The following table describes the protocol-specific parameters for the Cisco Duo protocol:

Table 48. Cisco Duo protocol parameters	
Parameter	**Description**
Log Source Type	**Cisco Duo**
Protocol Configuration	**Cisco Duo**
Log Source Identifier	Type a unique name for the log source as an identifier for events from Cisco Duo. The value of the **Log Source Identifier** parameter must match the **Host** parameter when you are using the Cisco Duo default workflow. If the Cisco Duo default workflow is modified, then the **Log Source Identifier** must match the **Source** value - `source="${/host}"` that is used under the `PostEvents` section. For more information, see Cisco Duo protocol workflow.

Table 48. Cisco Duo protocol parameters (continued)	
Parameter	**Description**
Host	The API hostname in the Cisco Duo portal that is used to authenticate with the Cisco Duo Admin API. Review the preceding procedure for obtaining this information from Cisco Duo.
Integration Key	The integration key that is used to authenticate with the Cisco Duo Admin API. Review the preceding procedure for obtaining this information from Cisco Duo.
Secret Key	The secret key that is used to authenticate with the Cisco Duo Admin API. Review the preceding procedure for obtaining this information from Cisco Duo.
Use Proxy	If the API is accessed by using a proxy, select this checkbox. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Specify how often the log collects data. The format is M/H/D for Minutes/Hours/Days. The default is 5 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Enable Advanced Options	Select this checkbox to enable the following configuration options: **Allow Untrusted Certificates**, **Override Workflow**, **Workflow**, and **Workflow Parameters**. These parameters are only visible if you select this checkbox.
Allow Untrusted	If you enable this parameter, the protocol can accept self-signed and otherwise untrusted certificates that are located within the `/opt/qradar/conf/trusted_certificates/` directory. If you disable the parameter, the scanner trusts only certificates that are signed by a trusted signer. The certificates must be in PEM or RED-encoded binary format and saved as a `.crt` or `.cert` file. If you modify the workflow to include a hardcoded value for the **Allow Untrusted Certificates** parameter, the workflow overrides your selection in the UI. If you do not include this parameter in your workflow, then your selection in the UI is used.
Override Work Flow	Enable this option to customize the workflow. When you enable this option, the **Workflow** and **Workflow Parameters** fields appear.
Workflow	The XML document that defines how the protocol instance collects events from the target API. For more information about the default workflow, see “Cisco Duo protocol workflow” on page 112.

Table 48. Cisco Duo protocol parameters (continued)	
Parameter	**Description**
Workflow Parameters	The XML document that contains the parameter values used directly by the workflow. For more information about the default workflow parameters, see "Cisco Duo protocol workflow" on page 112.
Enabled	By default, the checkbox is selected to enable the log source to communicate with QRadar.
Credibility	Select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this checkbox to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this checkbox to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Cisco Duo protocol workflow

You can customize your workflow and workflow parameters based on the default workflow.

A workflow is an XML document that describes the event retrieval process. The workflow defines one or more parameters, which can be explicitly assigned values in the workflow XML or can derive values from the workflow parameter values XML document. The workflow consists of multiple actions that run sequentially.

The default workflow and workflow parameter XML files are available on GitHub. For more information, see Cisco Duo (https://github.com/IBM/IBM-QRadar-Universal-Cloud-REST-API/tree/master/IBM%20Verified/Cisco%20Duo).

Cisco Duo default workflow

Important: The value of the **Log Source Identifier** parameter must match the **Host** parameter when you are using the Cisco Duo default workflow. If the Cisco Duo default workflow is modified, then the **Log Source Identifier** must match the **Source** value - `source="${/host}"` that is used under the `PostEvents` section.

The following example shows the default Cisco Duo workflow:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!--
  Duo Admin API
  https://duo.com/docs/adminapi
  Duo Admin Panel
  https://admin.duosecurity.com/
  To obtain an 'Integration Key' and 'Secret Key':
  - Log on to the Duo Admin Panel
  - Navigate to "Applications"
  - Select the application to be monitored.
  - The "Integration Key" and "Secret Key" should be visible on the application page.
-->
<Workflow name="Duo" version="1.0" xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/Workflow/
V1">
    <Parameters>
        <Parameter name="host"              label="Host"           required="true" />
        <Parameter name="integration_key"   label="Integration Key" required="true" />
        <Parameter name="secret_key"        label="Secret Key"      required="true"
secret="true" />
    </Parameters>
    <Actions>
      <!--
      ////////////////////////
      // Authentication Logs //
      ////////////////////////
    -->
        <!-- Initialize the Bookmarks - mintime and maxtime -->
        <Initialize path="/auth_logs/mintime" value="${time() - 60000 * 60 * 24 * 30}" />
        <Set path="/auth_logs/maxtime" value="${time() - 60000 * 2}" />
        <!-- Log events are ranging from the last 30 days up to as recently as two minutes
before the API request -->
        <Set path="/method" value="GET" />
        <Set path="/endpoint" value="/admin/v2/logs/authentication" />

        <!--
      Generate the HTTP Password as an HMAC signature of the request https://duo.com/docs/
adminapi#authentication
        - Date enumerated as RFC 2822 format [Tue, 21 Aug 2012 17:29:18 -0000]
        - Method [GET, POST, etc.]
        - API Hostname [api-xxxxxxxx.duosecurity.com]
        - API method's path [/admin/v2/logs/]
        - Parameters [mintime=xxxxxx&maxtime=xxxxxx&limit=1000&next_offset=xxxxxx]
    -->
    <FormatDate pattern="EEE, dd MMM yyyy HH:mm:ss Z" timeZone="UTC" savePath="/auth_logs/
date" />
    <If condition="/auth_logs/response/body/response/metadata/next_offset != null">
      <Set path="/value" value="$
{/auth_logs/date}&#xA;${/method}&#xA;${/host}&#xA;${/endpoint}&#xA;limit=1000&amp;maxtime=${/
auth_logs/maxtime}&amp;mintime=${/auth_logs/mintime}&amp;next_offset=${url_encode(/auth_logs/
offset)}" />
            <GenerateHMAC algorithm="SHA1" secretKey="${/secret_key}" message="${/value}"
saveFormat="HEX" savePath="/signature" />
    </If>
    <Else>
      <Set path="/value" value="${/auth_logs/date}&#xA;${/method}&#xA;${/host}&#xA;${/
endpoint}&#xA;limit=1000&amp;maxtime=${/auth_logs/maxtime}&amp;mintime=${/auth_logs/mintime}" />
            <GenerateHMAC algorithm="SHA1" secretKey="${/secret_key}" message="${/value}"
saveFormat="HEX" savePath="/signature" />
    </Else>

        <CallEndpoint url="https://${/host}${/endpoint}" method="${/method}" savePath="/
auth_logs/response">
            <BasicAuthentication username="${/integration_key}" password="${/signature}" />
            <QueryParameter name="limit" value="1000" />
            <QueryParameter name="maxtime" value="${/auth_logs/maxtime}" />
            <QueryParameter name="mintime" value="${/auth_logs/mintime}" />
            <QueryParameter name="next_offset" value="${/auth_logs/offset}" omitIfEmpty="true"/>
            <RequestHeader name="Date" value="${/auth_logs/date}" />
        </CallEndpoint>
        <Delete path="/auth_logs/offset" />
    <!--
      RESPONSE FORMAT:
      {
        "stat":"OK",
        "response":
        {
          "authlogs":[...], <- logs are stored in this array /auth_logs/response/authlogs
          "metadata":
          {
            "next_offset":[
              "1532951895000",
```

```
              "af0ba235-0b33-23c8-bc23-a31aa0231de8"
            ],
            "total_objects":0
          }
        }
      }
    -->
        <If condition="/auth_logs/response/status_code != 429">
            <!-- Handle Errors -->
            <If condition="/auth_logs/response/status_code != 200">
                <!-- Event retriever thread is a bit slow to kill error'd out
provider threads, this prevents duplicate errors. -->
                <Sleep duration="2000" />
                <Log type="ERROR" message="Received error from Cisco Duo Protocol: $
{/auth_logs/response/body/code}: ${/auth_logs/response/body/message}. Abort polling events
until next recurrence time" />
                <Abort reason="${/auth_logs/response/body/code}: ${/auth_logs/response/body/
message}" />
            </If>
            <!-- Post the Events -->
            <PostEvents path="/auth_logs/response/body/response/authlogs" source="${/host}" />
            <!-- Set the offset -->
            <If condition="/auth_logs/response/body/response/metadata/next_offset != null">
                <Set path="/auth_logs/offset" value="${/auth_logs/response/body/response/
metadata/next_offset[0]},${/auth_logs/response/body/response/metadata/next_offset[1]}" />
                <Log type="DEBUG" message="An offset value of [${/auth_logs/offset}]
was found. A request with the offset value will be send in the next recurrence." />
            </If>
            <Else>
                <Log type="DEBUG" message="No offset value detected in response." />
                <!-- Update the Bookmark for the next iteration. Set the current
maxtime + 1 as next poll's mintime. -->
                <Set path="/auth_logs/mintime" value="${/auth_logs/maxtime + 1}" />
                <Log type="DEBUG" message="Done posting events for this recurrence.
Updating bookmark to begin at ${/auth_logs/maxtime + 1}." />
            </Else>
        </If>
        <Else>
            <Log type="WARN" message="Received warning from Cisco Duo: ${/auth_logs/response/
body/code}: ${/auth_logs/response/body/message}." />
        </Else>
    </Actions>
    <Tests>
        <DNSResolutionTest host="${/host}" />
        <TCPConnectionTest host="${/host}" />
        <SSLHandshakeTest host="${/host}" />
        <HTTPConnectionThroughProxyTest url="https://${/host}" />
    </Tests>
</Workflow>
```

Cisco Duo default workflow parameters

The following example shows the default workflow parameters for Cisco Duo:

```
<?xml version="1.0" encoding="UTF-8" ?>
<WorkflowParameterValues xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
WorkflowParameterValues/V1">
    <Value name="host"              value="" />
    <Value name="integration_key"   value="" />
    <Value name="secret_key"        value="" />
</WorkflowParameterValues>
```

Cisco Firepower eStreamer protocol configuration options

To collect events in IBM QRadar from a Cisco Firepower eStreamer (Event Streamer) service, configure a log source to use the Cisco Firepower eStreamer protocol.

The Cisco Firepower eStreamer protocol is formerly known as Sourcefire Defense Center eStreamer protocol.

The Cisco Firepower eStreamer protocol is a passive outbound protocol. For more information about how this protocol streams events, see Understanding the eStreamer Application Protocol (https://www.cisco.com/c/en/us/td/docs/security/firepower/670/api/eStreamer/EventStreamerIntegrationGuide/Protocol.html).

Events are streamed to QRadar to be processed after the Cisco Firepower Management Center DSM is configured.

The following table describes the protocol-specific parameters for the Cisco Firepower eStreamer protocol:

Table 49. Cisco Firepower eStreamer protocol parameters

Parameter	Description
Protocol Configuration	**Cisco Firepower eStreamer**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Cisco Firepower eStreamer log source, ensure that you give each one a unique name.
Server Port	The port number that the Cisco Firepower eStreamer services is configured to accept connection requests on. The default port that QRadar uses for Cisco Firepower eStreamer is 8302.
Keystore Filename	The directory path and file name for the keystore private key and associated certificate. By default, the import script creates the keystore file in the following directory: `/opt/qradar/conf/estreamer.keystore`
Truststore Filename	The directory path and file name for the truststore files. The truststore file contains the certificates that are trusted by the client. By default, the import script creates the truststore file in the following directory: `/opt/qradar/conf/estreamer.truststore`
Request Extra Data	Select this option to request intrusion event extra data from Cisco Firepower Management Center. For example, extra data includes the original IP address of an event.
Domain	**Important:** Domain Streaming Requests are supported for eStreamer version 6.x and later. Leave the **Domain** field blank for eStreamer version 5.x. The domain where the events are streamed from. The value in the **Domain** field must be a fully qualified domain. Therefore, all ancestors of the desired domain must be listed starting with the top-level domain and ending with the leaf domain that you want to request events from. Example: Global is the top-level domain, B is a second-level domain that is a subdomain of Global, and C is a third-level domain and a leaf domain that is a subdomain of B. To request events from C, type the following value for the **Domain** parameter: `Global \ B \ C`

Cisco NSEL protocol configuration options

To monitor NetFlow packet flows from a Cisco Adaptive Security Appliance (ASA), configure the Cisco Network Security Event Logging (NSEL) protocol source.

The Cisco NSEL protocol is an inbound/passive protocol. To integrate Cisco NSEL with QRadar, you must manually create a log source to receive NetFlow events. QRadar does not automatically discover or create log sources for syslog events from Cisco NSEL.

The following table describes the protocol-specific parameters for the Cisco NSEL protocol:

Table 50. Cisco NSEL protocol parameters

Parameter	Description
Protocol Configuration	**Cisco NSEL**
Log Source Identifier	If the network contains devices that are attached to a management console, you can specify the IP address of the individual device that created the event. A unique identifier for each, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.
Collector Port	The UDP port number that Cisco ASA uses to forward NSEL events. QRadar uses port 2055 for flow data on QRadar QFlow Collectors. You must assign a different UDP port on the Cisco Adaptive Security Appliance for NetFlow.

Related information

Adding a log source

EMC VMware protocol configuration options

To receive event data from the VMWare web service for virtual environments, configure a log source to use the EMC VMware protocol.

The EMC VMware protocol is an outbound/active protocol.

IBM QRadar supports the following event types for the EMC VMware protocol:

- Account Information
- Notice
- Warning
- Error
- System Informational
- System Configuration
- System Error
- User Login
- Misc Suspicious Event
- Access Denied
- Information
- Authentication
- Session Tracking

The following table describes the protocol-specific parameters for the EMC VMware protocol:

Table 51. EMC VMware protocol parameters	
Parameter	**Description**
Protocol Configuration	**EMC VMware**
Log Source Identifier	The value for this parameter must match the **VMware IP** parameter.
VMware IP	The IP address of the VMWare ESXi server. The VMware protocol appends the IP address of your VMware ESXi server with HTTPS before the protocol requests event data.

Forwarded protocol configuration options

To receive events from another Console in your deployment, configure a log source to use the Forwarded protocol.

The Forwarded protocol is an inbound/passive protocol that is typically used to forward events to another QRadar Console. For example, Console A has Console B configured as an off-site target. Data from automatically discovered log sources is forwarded to Console B. Manually created log sources on Console A must also be added as a log source to Console B with the forwarded protocol.

Google Cloud Pub/Sub protocol configuration options

The Google Cloud Pub/Sub protocol is an outbound/active protocol for IBM QRadar that collects Google Cloud Platform (GCP) logs.

If automatic updates are not enabled, download the GoogleCloudPubSub protocol RPM from the IBM support website.

Important: Google Cloud Pub/Sub protocol is supported on QRadar 7.3.2.6, build number 20191022133252 or later.

The following table describes the protocol-specific parameters for collecting Google Cloud Pub/Sub logs with the Google Cloud Pub/Sub protocol:

Table 52. Google Cloud Pub/Sub log source parameters for Google Cloud Pub/Sub	
Parameter	**Description**
`Service Account Credential Type`	Specify where the required Service Account Credentials are coming from. Ensure that the associated service account has the **Pub/Sub Subscriber** role or the more specific **pubsub.subscriptions.consume** permission on the configured **Subscription Name** in GCP. **User Managed Key** Provided in the **Service Account Key** field by inputting the full JSON text from a downloaded Service Account Key. **GCP Managed Key** Ensure that the QRadar managed host is running in a GCP Compute instance and the Cloud API access scopes include Cloud Pub/Sub.

Table 52. Google Cloud Pub/Sub log source parameters for Google Cloud Pub/Sub (continued)

Parameter	Description
Service Account Key	The full text from the JSON file that was downloaded when you created a **User Managed Key** for a service account in the **IAM & admin** > **Service accounts** section in Google Cloud Platform (GCP). **Example:** `{` `  "type": "service_account",` `  "project_id": "qradar-test-123456",` `  "private_key_id": "453422aa6efb1c2de189f12d725c417c8346033b",` `  "private_key": "-----BEGIN PRIVATE KEY-----\\n<MULTILINE PRIVATE KEY DATA>\\n-----END PRIVATE KEY-----\\n",` `  "client_email": "pubsubtest@qradar-test-123456.iam.gserviceaccount.com",` `  "client_id": "526344196064252652671",` `  "auth_uri": "https://accounts.google.com/o/oauth2/auth",` `  "token_uri": "https://oauth2.googleapis.com/token",` `  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",` `  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/pubsubtest%40qradar-test-123456.iam.gserviceaccount.com"` `}`
Subscription Name	The full name of the Cloud Pub/Sub subscription. For example, `projects/my-project/subscriptions/my-subscription`.
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events being processed.

Table 52. Google Cloud Pub/Sub log source parameters for Google Cloud Pub/Sub (continued)	
Parameter	**Description**
Log Source Identifier Pattern	When the **Use As A Gateway Log Source** option is selected, use this option to define a custom log source identifier for events that are processed. If the **Log Source Identifier Pattern** is not configured, QRadar receives events as unknown generic log sources. The **Log Source Identifier Pattern** field accepts key-value pairs, such as **key**=value, to define the custom Log Source Identifier for events that are being processed and for log sources to be automatically discovered when applicable. **Key** is the Identifier Format String which is the resulting source or origin value. Value is the associated regex pattern that is used to evaluate the current payload. The value (regex pattern) also supports capture groups which can be used to further customize the key (Identifier Format String). Multiple key-value pairs can be defined by typing each pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found. When a match is found, a custom Log Source Identifier displays. The following examples show the multiple key-value pair functionality: **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Use Proxy	Select this option for QRadar to connect to the GCP by using a proxy. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Proxy IP or Hostname	The IP or host name of the proxy server.
Proxy Port	The port number that is used to communicate with the proxy server. The default is 8080.
Proxy Username	Required only when the proxy requires authentication.
Proxy Password	Required only when the proxy requires authentication.

Table 52. Google Cloud Pub/Sub log source parameters for Google Cloud Pub/Sub (continued)	
Parameter	**Description**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Convert Google VPC Flow Logs to IPFIX	This option converts Google VPC Flow Logs to IPFIX that is then sent to the flow processor.
Flow Destination Hostname	The flow processor hostname where the Google VPC Flow logs are sent. **Note:** Enable **Convert Google VPC Flow Logs to IPFIX** to configure this parameter.
Flow Destination Port	The flow processor port where the Google VPC Flow logs are sent. **Note:** Enable **Convert Google VPC Flow Logs to IPFIX** to configure this parameter.

Related concepts

"Gateway log source" on page 15
Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

Related tasks

"Configuring Google Cloud Pub/Sub to integrate with QRadar" on page 120
Before you can add a log source in IBM QRadar, you must create a Pub/Sub Topic and Subscription, create a service account to access the Pub/Sub Subscription, and then populate the Pub/Sub topic with data.

"Adding a Google Cloud Pub/Sub log source in QRadar" on page 121
Set up a log source in IBM QRadar to use a custom log source type or an IBM log source type that supports the Google Cloud Pub/Sub protocol.

Configuring Google Cloud Pub/Sub to integrate with QRadar

Before you can add a log source in IBM QRadar, you must create a Pub/Sub Topic and Subscription, create a service account to access the Pub/Sub Subscription, and then populate the Pub/Sub topic with data.

Procedure

1. Create a topic in the Pub/Sub tab on the Google Cloud Platform (https://console.cloud.google.com).

   For more information about creating topics, see Managing topics and subscriptions (https://cloud.google.com/pubsub/docs/admin).
2. Create a subscription

   For more information about creating subscriptions, see Managing topics and subscriptions (https://cloud.google.com/pubsub/docs/admin).

   Important: The following parameters need specific configuration to work with QRadar:

   - For the **Delivery Type** parameter, enable the **Pull** option.
   - To ensure that messages are processed only once, set the **Acknowledgement Deadline** to 60 seconds, and deselect the **Retain acknowledged messages** option.

3. Create a service account on the **IAM & admin** menu.

   For more information about service accounts, see Creating and managing service accounts (https://cloud.google.com/iam/docs/creating-managing-service-accounts).

   Tip: You do not need to make a service account if any of the following conditions apply to you:

   - You already have an account that you want to use.
   - You use **GCP Managed Key** as the **Service Account Type** option on your QRadar All-in-One appliance or QRadar Event Collector that collects events from a Google Cloud Platform Compute instance.

   If you use the **User Managed Key** option for the **Service Account Key** parameter when you configure a log source in QRadar, you must create a service account key. For more information, see Creating and managing service account keys (https://cloud.google.com/iam/docs/creating-managing-service-account-keys).
4. Assign permissions to your service account.

   For more information about service account permissions, see Manage access to service accounts (https://cloud.google.com/iam/docs/manage-access-service-accounts).

   Tip: You do not need to assign the permissions for the service account if any of the conditions from step 3 apply to you.
5. Populate the Pub/Sub topic with data by creating a Logging Sink.

   For more information about creating a Logging Sink, see Configure and manage sinks (https://cloud.google.com/logging/docs/export/configure_export_v2).

What to do next

Add a Google Cloud Pub/Sub log source on the QRadar Console by using the Google Cloud Pub/Sub protocol. For more information, see "Adding a Google Cloud Pub/Sub log source in QRadar" on page 121.

Adding a Google Cloud Pub/Sub log source in QRadar

Set up a log source in IBM QRadar to use a custom log source type or an IBM log source type that supports the Google Cloud Pub/Sub protocol.

Before you begin

You can use the Google Cloud Pub/Sub protocol to retrieve any type of event from the Google Cloud Pub/Sub service. IBM provides DSMs for some Google Cloud services. Any services that don't have a DSM can be handled by using a custom log source type.

If you want to use an existing DSM to parse data, select the **Use as a Gateway Log Source** parameter option for more log sources to be created from data that is collected by this configuration. Alternatively, if log sources are not automatically detected, you can manually create them by using Syslog for the **Protocol type** parameter option.

Procedure

1. Log in to QRadar.
2. On the **Admin** tab, click the QRadar Log Source Management app icon.
3. Click **New Log Source** > **Single Log Source**.
4. On the **Select a Log Source Type** page, select a custom log source type or an IBM log source type that supports the Google Cloud Pub/Sub protocol.
5. On the **Select a Protocol Type** page, from the **Select Protocol Type** list, select **Google Pub/Sub Protocol**.
6. On the **Configure the Log Source parameters** page, configure the log source parameters, and then click **Configure Protocol Parameters**. For more information about configuring Google Cloud Pub/Sub protocol parameters, see Adding a Google Cloud Pub/Sub log source in QRadar.

7. Test the connection to ensure that connectivity, authentication, and authorization are working. If available, view sample events from the subscription.
   a) Click **Test Protocol Parameters**, and then click **Start Test**.
   b) To fix any errors, click **Configure Protocol Parameters**, then test your protocol again.

   For more information about adding a log source in QRadar, see Adding a log source.

Google G Suite Activity Reports REST API protocol options

The Google G Suite Activity Reports REST API protocol is an active outbound protocol for IBM QRadarthat retrieves logs from Google G Suite.

Important: The Google G Suite Activity Reports REST API protocol is supported on QRadar 7.3.2 Fix Pack 6, build number 20191022133252 or later.

The following table describes the protocol-specific parameters for the Google G Suite Activity Reports REST API protocol:

Table 53. Google G Suite Activity Reports REST API protocol log source parameters

Parameter	Value
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Google G Suite log source, ensure that you give each one a unique name.
Delegated User Account Email	The Google user account that has report privileges.
Service Account Credentials	Authorizes access to Google's APIs for retrieving the events. The **Service Account Credentials** are contained in a JSON formatted file that you download when you create a new service account in the Google Cloud Platform.
Use Proxy	If QRadar accesses Google G Suite by using a proxy, enable this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	The time interval between log source queries to the Google G Suite Activity Reports API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 5 minutes.

Table 53. Google G Suite Activity Reports REST API protocol log source parameters (continued)	
Parameter	**Value**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.
Event Delay	The delay, in seconds, for collecting data. Google G Suite logs work on an eventual delivery system. To ensure that no data is missed, logs are collected on a delay. The default delay is 7200 seconds (2 hours), and can be set as low as 0 seconds.

Related concepts

“Google G Suite Activity Reports REST API protocol FAQ” on page 123

Got a question? Check these frequently asked questions and answers to help you understand the Google G Suite Activity Reports REST API protocol.

Related information

Adding a log source

Google G Suite Activity Reports REST API protocol FAQ

Got a question? Check these frequently asked questions and answers to help you understand the Google G Suite Activity Reports REST API protocol.

- “What is the event delay option used for?” on page 123
- “How does the event delay option work?” on page 124
- “What value do I use for the event delay option?” on page 124

What is the event delay option used for?

The event delay option is used to prevent events from being missed. Missed events, in this context, occur because they become available after the protocol updated its query range to a newer timeframe than the event’s arrival time. If an event occurred but wasn't posted to the Google G Suite Activity Reports REST API, then when the protocol queries for that event's creation time, the protocol doesn't get that event.

Example 1: The following example shows how an event can be lost.

The protocol queries the Google G Suite Activity Reports REST API at 2:00 PM to collect events between 1:00 PM – 1:59 PM. The Google G Suite Activity Reports REST API response returns the events that are available in the Google G Suite Activity Reports REST API between 1:00 PM - 1:59 PM. The protocol operates as if all of the events are collected. Then, it sends the next query to the Google G Suite Activity Reports REST API at 3:00 PM to get events that occurred between 2:00 PM – 2:59 PM. The problem with this scenario is that the Google G Suite Activity Reports REST API might not include all of the events that occurred between 1:00 PM – 1:59 PM. If an event occurred at 1:58 PM, that event might not be available in the Google G Suite Activity Reports REST API until 2:03 PM. However, the protocol already queried the 1:00 PM – 1:59 PM time range, and can't requery that range without getting duplicated events. This delay can take multiple hours.

Example 2: The following example shows **Example 1**, except in this scenario a 15-minute delay is added.

This example uses a 15-minute delay when the protocol makes query calls. When the protocol makes a query call to the Google G Suite Activity Reports REST API at 2:00 PM, it collects the events that occurred between 1:00 - 1:45 PM. The protocol operates as if all of the events are collected. Then, it sends the next query to the Google G Suite Activity Reports REST API at 3:00 PM and collects all events that occurred between 1:45 PM – 2:45 PM. Instead of missing the event, as in **Example 1**, it gets picked up in the next query call between 1:45 PM - 2:45 PM.

Example 3: The following example shows **Example 2**, except in this scenario the events are available a day later.

If the event occurred at 1:58 PM, but only became available to the Google G Suite Activity Reports REST API at 1:57 PM the next day, then the event delay from **Example 2** doesn't get that event. Instead, the event delay must be set to a higher value, in this case 24 hours.

How does the event delay option work?

Instead of querying from the **last received event time** to **current time**, the protocol queries from the **last received event time** to **current time** - <*event delay*>. The event delay is in seconds. For example, a delay of 15 minutes (900 seconds) means that it queries only up to 15 minutes ago. This query gives the Google G Suite Activity Reports REST API 15 minutes to make an event available before the event is lost. When the **current time** - <*event delay*> is less than the **last received event time**, the protocol doesn't query the Google G Suite Activity Reports REST API. Instead, it waits for the condition to pass before querying.

What value do I use for the event delay option?

The Google G Suite Activity Reports REST API can delay an event's availability. To prevent any events from being missed, you can set the **Event Delay** parameter option value to 168 hours (one week). However, the larger the event delay, the less real time the results are. For example, with a 24-hour event delay, you see events 24 hours after they occur instead of immediately. The value depends on how much risk you're willing to take and how important real-time data is. The default delay of 2 hours (7200 seconds) provides a value that is set in real time and also prevents most events from being missed. For more information about the delay, see Data retention and lag times (https://support.google.com/a/answer/7061566?hl=en).

HCL BigFix SOAP protocol configuration options (formerly known as IBM BigFix)

To receive Log Event Extended Format (LEEF) formatted events from HCL BigFix® appliances, configure a log source that uses the HCL BigFix SOAP protocol.

Important: HCL BigFix is formerly known as IBM BigFix.

This protocol requires HCL BigFix versions 8.2.x to 9.5.2, and the Web Reports application for HCL BigFix.

The HCL BigFix SOAP protocol is an outbound/active protocol that retrieves events in 30-second intervals over HTTP or HTTPS. As events are retrieved, the HCL BigFix DSM parses and categorizes the events.

The following table describes the protocol-specific parameters for the HCL BigFix SOAP protocol:

Table 54. IBM BigFix SOAP protocol parameters

Parameter	Description
Protocol Configuration	**HCL BigFix SOAP**
Log Source Identifier	Type the IP address or host name for your HCL BigFix appliance. The IP address or host name identifies your HCL BigFix as a unique event source in QRadar.

Table 54. IBM BigFix SOAP protocol parameters (continued)	
Parameter	**Description**
Use HTTPS	If a certificate is required to connect with HTTPS, copy the required certificates to the following directory: `/opt/qradar/conf/trusted_certificates`. Certificates that have following file extensions: `.crt`, `.cert`, or `.der` are supported. Copy the certificates to the trusted certificates directory before the log source is saved and deployed.
SOAP Port	By default, port 80 is the port number for communicating with HCL BigFix. Most configurations use port 443 for HTTPS communications.
Username	The username that you use to access BigFix.
Password	The password that you use to access BigFix.
Polling Interval (In Minutes)	The number of minutes between queries to the log files to check for new data. The default is 15 minutes. The minimum value for the polling interval is 1 minute, and the maximum value is 60 minutes.

HTTP Receiver protocol configuration options

To collect events from devices that forward HTTP or HTTPS requests, configure a log source to use the HTTP Receiver protocol.

The HTTP Receiver protocol is an inbound passive protocol. The HTTP Receiver acts as an HTTP server on the configured listening port and converts the request body of any received POST requests into events. It supports both HTTPS and HTTP requests.

Important: When you use the HTTP Receiver protocol, you must use a certificate that is issued by a certificate authority (CA). It can't be a self-signed certificate because it must be validated by a CA. For more information about setting up a CA certificate for HTTP Receiver, see “Setting up certificate-based authentication for HTTP Receiver” on page 130.

Important: If you are a QRadar on Cloud (QRoC) user, contact IBM support and open a support case to configure this certificate-based authentication if the target collector is the Console or Event Processor.

The following table describes the protocol-specific parameters for the HTTP Receiver protocol:

Table 55. HTTP Receiver protocol parameters	
Parameter	**Description**
Protocol Configuration	From the list, select **HTTP Receiver**.
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. Ensure that you give each log source a unique name.
Listen Port	The port that is used by IBM QRadar to accept incoming HTTP Receiver events. The default port is 12469. **Important:** Do not use port 514. Port 514 is used by the standard Syslog listener.

Table 55. HTTP Receiver protocol parameters (continued)	
Parameter	**Description**
Communication Type	The type of HTTP server that is created by the protocol. **HTTP** Creates an HTTP Server without encryption and verification **Important:** Not supported for QRadar on Cloud (QRoC). **HTTPs** Creates an HTTP Server with encryption and verification **HTTPs with Mutual TLS (mTLS)** Creates an HTTP Server that uses Mutual TLS Authentication (mTLS)
Server Certificate	Choose one of the following server certificate options. **PKCS12 Certificate Chain and Password** If you select this option, you must configure a path to the PKCS12 file and provide the password. If there is more than one entry in the PKCS12 file, you must provide an alias to specify which certificate entry to use. **Choose from QRadar Certificate Store** If you select this option, you must upload a certificate in the IBM QRadar Certificate Management app. In the app, set the certificate's **Purpose** as `Server` or `Server Client`, and its **Component** as `Log Source`. **Self-signed Generated Certificate (Deprecated)** If you select this option, then a self-signed generated certificate is used. If a certificate was not already generated, then one is generated to use. This certificate is self-signed and is the same as the TLS Syslog configurations that are using generated certificates on the same host.
Server Certificate Friendly Name	The friendly name of a certificate that is available in the QRadar Certificate Store, which is uploaded in the QRadar Certificate Management app. **Important:** The QRadar Certificate Management app is supported on QRadar 7.3.3 Fix Pack 6 or later.
PKCS12 Server Certificate Path	The absolute path to a PKCS12 file that contains a private key and certificate chain. If you select **PKCS12 Certificate Chain and Password** as the server certificate option, this parameter is displayed.
PKCS12 Password	The password for the PKCS12 file. If you select **PKCS12 Certificate Chain and Password** as the server certificate option, this parameter is displayed.

Table 55. HTTP Receiver protocol parameters (continued)	
Parameter	**Description**
PKCS12 Certificate Alias	The alias for the certificate entry in the PKCS12 file to use. If there is more than one entry in the PKCS12 file, then you must provide an alias to specify which certificate entry to use. When there is more than one certificate entry, leave this field blank to use the single certificate entry. If you select **PKCS12 Certificate Chain and Password** as the server certificate option, this parameter is displayed.
Use HTTP Authentication Token Header	This enables HTTP Header Authentication. When enabled, clients attempting to communicate with the HTTP Server must provide a valid access token via a Request Header.
Authentication Token Header Name	The HTTP Authentication Header is added to the HTTP request headers and contains information about the authentication header in use and the associated credentials. **Authentication Header**: This indicates the type of authentication in use. Common authentication headers include Basic, Digest, and Bearer.
Authentication Token Value	The Token Value included in the header depends on the authentication scheme under use. For example, in the case of Basic authentication, the Token Value consist of a username and password encoded in Base64 format.
Mutual TLS Authentication Truststore	If you select the **HTTPs with Mutual TLS (mTLS)** communication type, select one of these truststore types. **System Truststore** Initializes the server truststore by using the Operating System truststore on the target event collector. **Custom Truststore** Initializes the server truststore by using a user-provided Java keystore and password. **Client Certificate On Disk (Deprecated)** Ensures that the client certificate matches but does not validate the issuer. With this method, all clients must share one certificate.
Custom Truststore File Path	The absolute path to a custom truststore. You must copy the custom truststore to the QRadar Console or the Event Collector for the log source.
Custom Truststore Password	The password for the custom truststore.
Enable Issuer Verification	Verify that the client certificate was issued by a specific certificate or public key. A common use case is to verify that a specific intermediate CA was used to issue the client certificate.

Table 55. HTTP Receiver protocol parameters (continued)	
Parameter	**Description**
Issuer Certificate or Public Key	The root or intermediate issuer's certificate or public key in PEM format. Enter the certificate, including this text: `-----BEGIN CERTIFICATE-----` `-----END CERTIFICATE-----` Or enter the public key, including this text: `-----BEGIN PUBLIC KEY-----` `-----END PUBLIC KEY-----` If you enabled the **Enable Issuer Verification** parameter, this parameter is displayed.
Use CN Allowlist	Specify lists or patterns of common names that client certificates must match after trust is established. Enter plain text or a regular expression. Define multiple entries by entering each entry on a new line. The following list shows examples of the types of common name entries to use in your **CN Allowlist**. **Fixed name** `127.0.0.1` `1.1.1.1` **Wildcard name** `1.1.1.*` `.*` **Domain name** `www.host.*.com` `localhost` By default, this parameter is disabled.
Check Certificate Revocation	Checks certificate revocation status against the client certificate revocation list. To configure this option, you must have network connectivity to the URL that is specified by the client certificate's **CRL Distribution Points** field in the X509v3 extension, and the URL must support only certificate revocation list (CRL) format. OSCP is not supported.
Client Certificate Path (Deprecated)	Set the absolute path to the client certificate. You must copy the client certificate to the QRadar Console or the Event Collector for the log source. If you select **HTTPs with Mutual TLS (mTLS)** as the **Communication Type**, and you select **Client Certificate on Disk (Deprecated)** as the **Mutual TLS Authentication Truststore**, this parameter is displayed.

Table 55. HTTP Receiver protocol parameters (continued)

Parameter	Description
Message Pattern (Optional)	By default, the entire HTTP POST is processed as a single event. To divide the POST into multiple single-line events, provide a regular expression to denote the start of each event. If the pattern matches with the regular expression at least once in a line, then the line is treated as an event.
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. However, in rare circumstances the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing. When you enable the **Use As A Gateway Log Source** parameter, you can enable predictive parsing.
Log Source Identifier Pattern	When the **Use As A Gateway Log Source** option is selected, use this option to define a custom log source identifier for events that are processed. If the **Log Source Identifier Pattern** is not configured, QRadar receives events as unknown generic log sources. The **Log Source Identifier Pattern** field accepts key-value pairs, such as **key**=value, to define the custom Log Source Identifier for events that are being processed and for log sources to be automatically discovered, when applicable. **Key** is the Identifier Format String, which is the resulting source or origin value. Value is the associated regex pattern that is used to evaluate the current payload. The value (regex pattern) also supports capture groups, which can be used to further customize the key (Identifier Format String). Multiple key-value pairs can be defined by typing each pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found. When a match is found, a custom Log Source Identifier is displayed. The following examples show the multiple key-value pair functions: **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** `VPC-ACCEPT-OK`

Table 55. HTTP Receiver protocol parameters (continued)	
Parameter	**Description**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Enable Advanced Server Configuration Options	Enable this parameter to configure more server options. If you do not enable this parameter, the default values are used.
Max Payload Length (Byte)	The maximum payload size of a single event in bytes. The event is split when its payload size exceeds this value. The default value is 8192, and it must not be greater than 32767. When you enable the **Enable Advanced Server Configuration Options** parameter, this parameter is displayed.
TLS Protocols	The versions of TLS that can be accepted in this protocol. Send a request by using the same version that is selected for the server. **TLSv1.3** is supported from QRadar 7.5.0 UP5 onwards. **Important:** TLSv1.0 and TLSv1.1 are no longer supported as of QRadar 7.3.3 FP10, 7.4.3 FP3, and 7.5.0 CR. Future releases might not support TLSv1.0 and TLSv1.1.
Max POST method Request Length (MB)	The max size of a POST method request body in MB. If a POST request body size exceeds this value, an HTTP 413 status code is returned. The default value is 5, and it must not be greater than 10. When you enable the **Enable Advanced Server Configuration Options** parameter, this parameter is displayed.

Related information
Adding a log source
QRadar Certificate Management

Setting up certificate-based authentication for HTTP Receiver

When you use the HTTP Receiver protocol, you must use a certificate that is issued by a certificate authority (CA). It can't be a self-signed certificate because it must be validated by a CA.

About this task

Important: If you are a QRadar on Cloud (QRoC) user, contact IBM support and open a support case to configure this certificate-based authentication if the target collector is the Console or Event Processor.

Before you begin

Before you import a PKCS12 file to use with the HTTP Receiver, you need a PKCS12 file that includes the certificate private key, endpoint certificate, and any intermediate certificates that are needed. Root CAs can be included in the chain but are not mandatory.

If you have a private key and certificate instead of a PKCS12 certificate, you must complete the following steps to convert them to a PKCS12 certificate:

1. Locate the endpoint certificate private key, which is in PKCS1 encoding in PEM format. The file is called `certificate.key`. The private key must begin with `BEGIN RSA PRIVATE KEY` and end with `END RSA PRIVATE KEY`.

   Tip: If your key is in PEM format but begins with a `BEGIN PRIVATE KEY` header instead of `BEGIN RSA PRIVATE KEY`, then it is in PKCS8 encoding and must be converted to PKCS1 encoding before you continue.
2. Locate the certificate chain in PEM format, with each certificate appended in the following order in the `chain.crt` file. The endpoint certificate must be first, then followed by one or more intermediate certificates as needed.

   Important: If your certificate is issued directly by a Root CA, you must provide only the endpoint certificate.
3. Create the PKCS12 certificate with the `certificate.key` and `chain.crt` files by running the following command:

   ```
   openssl pkcs12 -export -out myserver.mycompany.net.p12 -inkey certificate.key -in chain.crt
   ```
4. Create an export password to protect the private key in the PKCS12 container. The password is used to import the certificate into the QRadar keystore.
5. Verify the details of the certificate by running the following command:

   ```
   keytool -list -v -keystore myserver.mycompany.net.p12 -storetype PKCS12
   ```

You can now import the PKCS12 certificate to use with HTTP Receiver.

IBM Cloud Object Storage protocol configuration options

The IBM Cloud Object Storage protocol for IBM QRadar is an outbound or active protocol that collects logs that are contained in objects from IBM Cloud Object Storage buckets.

Important: Before you configure the IBM Cloud Object Storage protocol, configure user access roles and service credentials to access the IBM Cloud Object Storage buckets.

You must have either the Reader, Writer, or Manager role to access the buckets. For more information about user access roles and permissions, see Bucket permissions (https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-iam-bucket-permissions).

You must create service credentials that include hash-based message authentication code (HMAC) credentials. For more information about service credentials, see Using HMAC credentials (https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-uhc-hmac-credentials-main).

Table 56. IBM Cloud Object Storage protocol common log source parameters

Parameter	Description
Protocol Configuration	IBM Cloud Object Storage
Log Source Identifier	Type a unique name for the log source. The log source identifier does not need to reference a specific server, and it can be the same value as the **Log Source Name**.
HMAC Access Key ID	The Access Key ID that was generated when you configured the service credentials.
HMAC Secret Access Key	The Secret Access Key that was generated when you configured the service credentials.
Endpoint	The public endpoint that is stated in the bucket configuration page.

Table 56. IBM Cloud Object Storage protocol common log source parameters (continued)	
Parameter	**Description**
Bucket Name	The name of the bucket that logs are stored in.
Prefix	The prefix filter value to limit collecting objects or file keys that begin with the prefix. To pull all files from the bucket, use a forward slash (/). **Important:** Changing the **Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. If the **Prefix** file path is used to specify folders, you must not begin the file path with a forward slash. For example, use `folder1/folder2` instead.
Event Format	The following event formats are supported: **LINEBYLINE** Raw log files that contain one record per line. You can use either `.gz`, `.gzip`, or `.zip` files for compression. **W3C** Files that contain generic W3C formatting data to output name-value-pair events (`.gz` files only).
Use As A Gateway Log Source	If you do not want to define a custom log source identifier for events, clear the checkbox. If you don't select **Use As A Gateway Log Source** and you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources.

Table 56. IBM Cloud Object Storage protocol common log source parameters (continued)

Parameter	Description
Log Source Identifier Pattern	If you select **Use As A Gateway Log Source**, you can define a custom log source identifier. Use this option for events that are being processed and for log sources that are automatically discovered. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom log source identifier. The key is the identifier format string, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom log source identifier is displayed. The following examples show multiple key-value pair functions: `Patterns` `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` `Events` `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` `Resulting custom log source identifier` `VPC-ACCEPT-OK`
Show Advanced Options	To configure the advanced options for event collection, set this option to **On**.
File Pattern	Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`. This option is available when you set **Show Advanced Options** to **On**.
Local Directory	The local directory on the Target Event Collector. The directory must exist before the protocol attempts to retrieve events. This option is available when you set **Show Advanced Options** to on.

Table 56. IBM Cloud Object Storage protocol common log source parameters (continued)	
Parameter	**Description**
Use Proxy	If QRadar accesses the IBM Cloud Object Storage by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** parameters. If the proxy does not require authentication, leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Type a time interval to determine how frequently the protocol polls for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds. The minimum value is 60 (seconds) or 1M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

IBM Fiberlink REST API protocol configuration options

To receive Log Event Extended Format (LEEF) formatted events from IBM MaaS360® appliances, configure a log source that uses the IBM Fiberlink® REST API protocol.

The IBM Fiberlink REST API protocol is an outbound (or active) protocol. As events are retrieved, the IBM MaaS360 DSM parses and categorizes events.

The following table describes the protocol-specific parameters for the IBM Fiberlink REST API protocol.

Table 57. IBM Fiberlink REST API protocol log source parameters	
Parameter	**Value**
Log Source Type	IBM Fiberlink MaaS360
Protocol Configuration	IBM Fiberlink REST API
Log Source Identifier	Type a unique identifier for the log source. The **Log Source Identifier** can be set to any valid value and does not need to reference a specific server. You can set the **Log Source Identifier** to the same value as the Log Source Name. If you have more than one IBM Fiberlink® MaaS360® log source that is configured, you might want to give them similar but unique names. For example, you can name the first log source `fiberlink1`, the second log source `fiberlink2`, and the third log source `fiberlink3`.

Table 57. IBM Fiberlink REST API protocol log source parameters (continued)	
Parameter	**Value**
Login URL	Copy the URL for the Fiberlink MaaS360 REST server.
Username	Type the username used to access the MaaS360 APIs. Users with the following administrator roles can access the APIs: • Service Administrator • Administrator • Administrator-Level 2
Password	Type the password used to access your MaaS360 APIs.
Secret Key	The secret key provided by Fiberlink Customer Service when you enable the REST API.
App ID	The app ID provided by Fiberlink Customer Service when you enable the REST API.
Billing ID	The billing ID for your Fiberlink MaaS360 account
Platform	The platform version of the Fiberlink MaaS360 console.
App Version	The app version of the application that corresponds to your REST API account.
Use Proxy	If IBM QRadar accesses the Fiberlink MaaS360 API by using a proxy, enable the **Use Proxy** option. If the proxy requires authentication, configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** and **Proxy Port** fields. This parameter is disabled by default.
Proxy IP or Hostname	The IP or hostname of the proxy server that you want to use. This parameter is available if the **Use Proxy** option is enabled.
Proxy Port	The port number used to communicate with the proxy. The default port number is 8080. This parameter is available if the **Use Proxy** option is enabled.
Proxy Username	The username that you use to access the proxy server. This parameter is available if the **Use Proxy** option is enabled.

Table 57. IBM Fiberlink REST API protocol log source parameters (continued)	
Parameter	**Value**
Proxy Password	The password that you use to access the proxy server. This parameter is available if the **Use Proxy** option is enabled.
Automatically Acquire Server Certificate(s)	If the **Yes** option is selected, the log source automatically downloads the server certificate and begins trusting the target server.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Recurrence	The time interval between log source queries to IBM Fiberlink MaaS360 for new events. The time interval can be in minutes (M), hours (H), or days (D). For example, 1 M, 3 H, 5 D. The default is 60 minutes (60 M).

IBM Security Randori REST API protocol configuration options

To receive events from IBM Security Randori, configure a log source to communicate with the IBM Security Randori REST API protocol.

The IBM Security Randori REST API protocol is an active outbound protocol that provides alerts about changes in an organizations attack surface. For example, new targets that are discovered.

Important: Before you can configure a log source for Randori, you must obtain your **API Key** from the Randori web portal.

For more information about obtaining this value, see How to Add an API token (https://www.ibm.com/docs/en/SSD5I5K/intapi_api_AddAPIToken.html).

The following table describes the protocol-specific parameters for the IBM Security Randori REST API protocol:

Table 58. IBM Security Randori REST API protocol parameters	
Parameter	**Description**
Protocol Configuration	**IBM Security Randori REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured IBM Security Randori log source, ensure that you give each one a unique name.

Table 58. IBM Security Randori REST API protocol parameters (continued)	
Parameter	**Description**
Instance	The **Instance** value is the URL that you use to access Randori, such as `app2.randori.io`. The structure for the **Instance** value is: `app[#].randori.io` where `[#]` is a number that might be required to access your Randori instance.
API Key	The API key that is used to access the IBM Security Randori REST API. For more information about obtaining this value, see How to Add an API token (https://www.ibm.com/docs/en/SSD5I5K/intapi_api_AddAPIToken.html).
Minimum Priority Score	Filters new targets by using the priority score that you select. • **Low** - All new targets • **Medium** - New targets with a priority greater than 20 • **High** - New targets with a priority of 30 or greater
Minimum Temptation	Filters existing targets that have a modified temptation value. This filter is based on the temptation value that you select. • **Low** - All targets with a modified temptation value • **Medium** - Targets with a temptation value greater than 14 • **High** - Targets with a temptation value greater than 29 • **Critical** - Targets with a temptation value greater than 39
Use Proxy	If the API is accessed by using a proxy, select this checkbox. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Specify how often the log collects data. The value can be in Minutes (M), Hours (H), or Days (D). The default is 1 minute.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Enable Advanced Options	Select this checkbox to enable the following configuration options: **Allow Untrusted** and **Override Workflow**. These parameters are only visible if you select this checkbox.
Initial Days of Historical Data	Enter the number of days before the current date to collect historical data. When you configure a new log source, IBM QRadar generates `New Target` events for existing targets that have a first-seen date within the number of days that you enter. This value is used only before the log source runs for the first time.

Table 58. IBM Security Randori REST API protocol parameters (continued)	
Parameter	**Description**
Allow Untrusted	If you enable this parameter, the protocol can accept self-signed and otherwise untrusted certificates that are located within the `/opt/qradar/conf/trusted_certificates/` directory. If you disable the parameter, the scanner trusts only certificates that are signed by a trusted signer. The certificates must be in PEM or RED-encoded binary format and saved as a `.crt` or `.cert` file. If you modify the workflow to include a hardcoded value for the **Allow Untrusted Certificates** parameter, the workflow overrides your selection in the UI. If you do not include this parameter in your workflow, then your selection in the UI is used.
Override Workflow	Enable this option to customize the workflow. When you enable this option, the **Workflow** and **Workflow Parameters** parameters appear.
Workflow	The XML document that defines how the protocol instance collects events from the target API. For more information about the default workflow, see "IBM Security Randori REST API protocol workflow" on page 138.
Workflow Parameters	The XML document that contains the parameter values used directly by the workflow. For more information about the default workflow parameters, see "IBM Security Randori REST API protocol workflow" on page 138.

IBM Security Randori REST API protocol workflow

You can customize your workflow and workflow parameters based on the default workflow.

A workflow is an XML document that describes the event retrieval process. The workflow defines one or more parameters, which can be explicitly assigned values in the workflow XML or can derive values from the workflow parameter values XML document. The workflow consists of multiple actions that run sequentially.

The default workflow and workflow parameter XML files are available on GitHub. For more information, see IBM Security Randori (https://github.com/IBM/IBM-QRadar-Universal-Cloud-REST-API/tree/master/IBM%20Verified/IBM%20Security%20Randori).

Randori default workflow

The following example shows the default Randori workflow:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Workflow name="IBMSecurityRandoriRestAPI" version="1.0" xmlns="http://qradar.ibm.com/
UniversalCloudRESTAPI/Workflow/V2">

    <Parameters>
        <Parameter name="instance"    label="Instance"    required="true" />
        <Parameter name="apiKey"    label="API Key"                    secret="true"
required="true" />
        <Parameter name="minimumPriority"    label="Minimum Priority" required="true"    />
        <Parameter name="minimumTemptation"    label="Minimum Temptation"    required="true" />
        <Parameter name="initialDaysOfHistoricalData" label="Initial Days of Historical Data"
required="true" default="1"/>
    </Parameters>
```

```
    <Actions>
        <Initialize path="/randoriDetections/detections/status_code" value="200"/> <!-- Sets
the initial status to 200. Once we get a value from the API, if the value is not 200 we will
sleep an additional 20 seconds. This prevents the protocol test event retriever from running
multiple times on failures. -->

        <If condition="${/randoriDetections/detections/status_code} != 200">
            <!-- ____________________________ Setting an internal sleep to slow down the protocol
test. Also applies in the main code, but only applies when the status code is in a bad
state._________________________ -->
            <Sleep duration="20000" />
        </If>

        <!-- ____________________________ Clears the status and sets the workflow to running
_____________________________ -->
        <ClearStatus />
        <SetStatus type="INFO" message="Workflow has started." />

        <!-- _____________________________Initialization Code_____________________________ -->
        <Initialize path="/randoriDetections/startTimeFirstSeenUnixTime" value="${time() -
(60000 * 60 * 24 * ${/initialDaysOfHistoricalData})}"/> <!-- days previous to initialize -->
        <Initialize path="/randoriDetections/startTimeTemptationLastModifiedUnixTime" value="$
{time() - (60000 * 60 * 24 * ${/initialDaysOfHistoricalData})}"/> <!-- days previous to
initialize -->

        <Initialize path="/randoriDetections/limit"     value="2000"/>          <!-- How many
we pullback at once, maximum of 2000 per request -->

        <!-- _____________________________Set the query bounds based off time values
_____________________________ -->
        <Set path="/randoriDetections/detectionOffset"     value="0"/>
        <Set path="/randoriDetections/startTimeFirstSeenUnixTime"    value="${/
randoriDetections/startTimeFirstSeenUnixTime}"/>
        <Set path="/randoriDetections/startTimeTemptationLastModifiedUnixTime"    value="${/
randoriDetections/startTimeTemptationLastModifiedUnixTime}"/>

                <!-- _____________________________Creates the formatted date for both temptation
and first seen in ISO-8601 format _____________________________ -->
        <FormatDate pattern="yyyy-MM-dd'T'HH:mm:ss.SSSSSSXXX" savePath="/randoriDetections/
startTimeFirstSeen" time="${/randoriDetections/startTimeFirstSeenUnixTime}"/>
        <FormatDate pattern="yyyy-MM-dd'T'HH:mm:ss.SSSSSSXXX" savePath="/randoriDetections/
startTimeTemptationLastModified" time="${/randoriDetections/
startTimeTemptationLastModifiedUnixTime}"/>

        <FormatDate pattern="yyyy-MM-dd'T'HH:mm:ss.SSSSSSXXX" savePath="/randoriDetections/
endtime" time="${/randoriDetections/endtimeMilli}"/>

        <!-- ____________________________ Sets the query that will be used for API Calls
_____________________________ -->
        <Set path="/randoriDetections/query" value='{"condition":"AND","rules":
[{"field":"table.authority","operator":"equal","value":"True"},
{"field":"table.affiliation_state","operator":"equal","value":"None"},{"condition":"OR","rules":
[{"condition":"AND","rules":
[{"ui_id":"target_first_seen","id":"table.target_first_seen","field":"table.target_first_seen","
type":"datetime","input":"text","randoriOnly":false,"label":"after","operator":"greater","value"
:"${/randoriDetections/startTimeFirstSeen}"},
{"ui_id":"target_first_seen","id":"table.target_first_seen","field":"table.target_first_seen","t
ype":"datetime","input":"text","randoriOnly":false,"label":"before","operator":"less_or_equal","
value":"${/randoriDetections/endtime}"},
{"field":"table.priority_score","operator":"greater_or_equal","value":${/minimumPriority}}]},
{"condition":"AND","rules":
[{"field":"table.temptation_last_modified","id":"table.temptation_last_modified","input":"text",
"type":"datetime","ui_id":"temptation_last_modified","randoriOnly":false,"label":"after","operat
or":"greater","value":"${/randoriDetections/startTimeTemptationLastModified}"},
{"field":"table.temptation_last_modified","id":"table.temptation_last_modified","input":"text","
type":"datetime","ui_id":"temptation_last_modified","randoriOnly":false,"label":"before","operat
or":"less_or_equal","value":"${/randoriDetections/endtime}"},
{"field":"table.target_temptation","operator":"greater_or_equal","value":${/
minimumTemptation}}]}]}]}'/>

        <!-- ____________________________ Stores the Tracked Newest Time in a separate variable.
This is updated and used only once the doWhile ends. _____________________________ -->
        <Set path="/randoriDetections/startTimeFirstSeenUnixTimeTemp" value="${/
randoriDetections/startTimeFirstSeenUnixTime}"/>
        <Set path="/randoriDetections/startTimeTemptationLastModifiedUnixTimeTemp" value="${/
randoriDetections/startTimeTemptationLastModifiedUnixTime}"/>

        <!--Note the following : We do not have a way to check this at the moment, but the data
can change between calls. Shouldn't happen, but if it does there should be minimal risk. -->
         <!-- ____________________________ Request events and loop if the event count = the offset
limit. _____________________________ -->
        <DoWhile condition="${/randoriDetections/detections/body/count} = ${/randoriDetections/
```

```
limit}">
            <CallEndpoint url="https://${/instance}/recon/api/v1/all-detections-for-target"
method="GET" savePath="/randoriDetections/detections">
                <BearerAuthentication token="${/apiKey}" />

                <QueryParameter name="limit"    value="${/randoriDetections/limit}" />
                <QueryParameter name="offset" value="${/randoriDetections/detectionOffset}"/>
                <QueryParameter name="sort"     value="id" />

                <!-- The query must be in base64 encoding. -->
                <QueryParameter name="q" value="${base64_encode(/randoriDetections/query)}" />

                <RequestHeader name="Accept" value="application/json" />
                <RequestHeader name="Content-Type" value="application/json" />
            </CallEndpoint>

            <!-- _____________________________ Catch any status code other than 200 (success). Note
502's for this protocol are throttle issues. _____________________________ -->
            <If condition="${/randoriDetections/detections/status_code} != 200">
                <If condition="${/randoriDetections/detections/status_code} = 502">
                    <Log type="ERROR" message="A 502 exception indicates the API throttle limit
was hit." />
                </If>
                <Log type="ERROR" message="${/randoriDetections/detections/status_code}: ${/
randoriDetections/detections/status_message}" />
                <Abort reason="${/randoriDetections/detections/status_code}: ${/
randoriDetections/detections/status_message}" />
            </If>
            <Else>
                <SetStatus type="INFO" message="Successfully Queried for events."/>
            </Else>

            <!-- _____________________________ Post Events _____________________________ -->
            <PostEvents path="/randoriDetections/detections/body/data" source="${/instance}" />
            <Log type="INFO" message="We received a total of ${count(/randoriDetections/
detections/body/data)} detections." />

            <!-- ____________________________ Update the last event time. Checks each event for
the time. ____________________________ -->
            <ForEach items="/randoriDetections/detections/body/data" item="/randoriDetections/
individualEventData">

                 <!-- _____________________________ Formats the events first seen and temptation
values into usuable unix timestamps _____________________________ -->
                <ParseDate pattern="yyyy-MM-dd'T'HH:mm:ss.SSSSSSXXX" date="${/randoriDetections/
individualEventData/target_first_seen}" savePath="/randoriDetections/tempfirstseen" />
                <ParseDate pattern="yyyy-MM-dd'T'HH:mm:ss.SSSSSSXXX" date="${/randoriDetections/
individualEventData/temptation_last_modified}" savePath="/randoriDetections/
temptemptationlastmodified" />

                <!-- _____________________________ Checks the doWhile loops tracked temp value
against each events time stamp to get the newest time value for temptation and first seen.
____________________________ -->
                <If condition="/randoriDetections/tempfirstseen > /randoriDetections/
startTimeFirstSeenUnixTimeTemp">
                    <Set path="/randoriDetections/startTimeFirstSeenUnixTimeTemp" value="${/
randoriDetections/tempfirstseen}"/>
                </If>

                <If condition="/randoriDetections/temptemptationlastmodified > /
randoriDetections/startTimeTemptationLastModifiedUnixTimeTemp">
                    <Set path="/randoriDetections/startTimeTemptationLastModifiedUnixTimeTemp"
value="${/randoriDetections/temptemptationlastmodified}"/>
                </If>
            </ForEach>

            <!-- _____________________________ Set new offset value for next query.
____________________________ -->
            <Set path="/randoriDetections/detectionOffset" value="${/randoriDetections/
detectionOffset + count(/randoriDetections/detections/body/data)}"/>
            <Log type="INFO" message="New offset to use: ${/randoriDetections/
detectionOffset}" />
        </DoWhile>

        <!-- ____________________________ Updates the tracked unix time with the value obtained
through the doWhile to only get new data from the next call._____________________________ -->
        <Set path="/randoriDetections/startTimeFirstSeenUnixTime" value="${/randoriDetections/
startTimeFirstSeenUnixTimeTemp}"/>
        <Set path="/randoriDetections/startTimeTemptationLastModifiedUnixTime" value="${/
randoriDetections/startTimeTemptationLastModifiedUnixTimeTemp}"/>

        <Log type="INFO" message="Completed receiving all of the detections for the current
```

```
time period." />

        <!-- No need to increment as the end time is excluded from the query-->
    </Actions>

    <Tests>
        <DNSResolutionTest              host="${/instance}"/>
        <TCPConnectionTest              host="${/instance}"/>
        <SSLHandshakeTest                 host="${/instance}"/>
        <HTTPConnectionThroughProxyTest url ="${/instance}"/>
    </Tests>
</Workflow>
```

Randori default workflow parameters

The following example shows the default Randori workflow parameters:

```
<?xml version="1.0" encoding="UTF-8" ?>
<WorkflowParameterValues xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
WorkflowParameterValues/V2">
    <Value name="instance"     value=""/>
    <Value name="apiKey"     value=""/>
    <Value name="minimumPriority" value=""/>
    <Value name="minimumTemptation" value=""/>
    <Value name="initialDaysOfHistoricalData" value=""/>
</WorkflowParameterValues>
```

IBM Security QRadar EDR REST API protocol configuration options

To receive events from IBM Security QRadar EDR, configure a log source to communicate with the IBM Security QRadar EDR REST API protocol.

The IBM Security QRadar EDR REST API protocol is an active outbound protocol that provides alerts about confirmed incidents of malware that are actively communicating or exfiltrating information.

Important: Before you can configure a log source for IBM Security QRadar EDR, you must obtain your **App ID** and **Secret Key** from the IBM Security QRadar EDR web portal.

1. Log in to your IBM Security QRadar EDR console.
2. On the **Administration** tab, select **API Applications**, and then click **Create Application**.
3. In the **Application Name** field, type a unique name for the application. Then, click **Create**.
4. Copy and save the **App ID** and **Secret Key** values. You must have these values to add a log source for IBM Security QRadar EDR.

The following table describes the protocol-specific parameters for the IBM Security QRadar EDR REST API protocol:

Table 59. IBM Security QRadar EDR REST API protocol parameters

Parameter	Description
Protocol Configuration	**IBM Security QRadar EDR REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured IBM Security QRadar EDR log source, ensure that you give each one a unique name.
Server Address	The IP address or hostname of the IBM Security QRadar EDR server.
App ID	The **App ID** value that you copied and saved from the IBM Security QRadar EDR application configuration.

Table 59. IBM Security QRadar EDR REST API protocol parameters (continued)	
Parameter	**Description**
Secret Key	The **Secret Key** value that you copied and saved from the IBM Security QRadar EDR application configuration.
Use Proxy	If the API is accessed by using a proxy, select this checkbox. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Specify how often the log collects data. The value can be in Minutes (M), Hours (H), or Days (D). The default is 1 minute.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Enable Advanced Options	Select this checkbox to enable the following configuration options: **Allow Untrusted**, **Override Workflow**, **Workflow**, and **Workflow Parameters**. These parameters are only visible if you select this checkbox.
Allow Untrusted	If you enable this parameter, the protocol can accept self-signed and otherwise untrusted certificates that are located within the `/opt/qradar/conf/trusted_certificates/` directory. If you disable the parameter, the scanner trusts only certificates that are signed by a trusted signer. The certificates must be in PEM or RED-encoded binary format and saved as a `.crt` or `.cert` file. If you modify the workflow to include a hardcoded value for the **Allow Untrusted Certificates** parameter, the workflow overrides your selection in the UI. If you do not include this parameter in your workflow, then your selection in the UI is used.
Override Workflow	Enable this option to customize the workflow. When you enable this option, the **Workflow** and **Workflow Parameters** parameters appear.
Workflow	The XML document that defines how the protocol instance collects events from the target API. For more information about the default workflow, see “IBM Security QRadar EDR REST API protocol workflow” on page 143.
Workflow Parameters	The XML document that contains the parameter values used directly by the workflow. For more information about the default workflow parameters, see “IBM Security QRadar EDR REST API protocol workflow” on page 143.

IBM Security QRadar EDR REST API protocol workflow

You can customize your workflow and workflow parameters based on the default workflow.

A workflow is an XML document that describes the event retrieval process. The workflow defines one or more parameters, which can be explicitly assigned values in the workflow XML or can derive values from the workflow parameter values XML document. The workflow consists of multiple actions that run sequentially.

The default workflow and workflow parameter XML files are available on GitHub. For more information, see IBM Security QRadar EDR (https://github.com/IBM/IBM-QRadar-Universal-Cloud-REST-API/tree/master/IBM%20Verified/ReaQta). *Update link?*

IBM Security QRadar EDR default workflow

The following example shows the default IBM Security QRadar EDR workflow:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Workflow name="ReaQta" version="1.0" xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
Workflow/V2">
  <Parameters>
    <Parameter name="app_id"            label="ReaQta Application ID"       required="true" />
    <Parameter name="secret_key"        label="ReaQta secret key"           required="true"
secret = "true"/>
    <Parameter name="reaqta_host"       label="ReaQta Host / IP Address"    required="true" />
  </Parameters>
  <Actions>
    <!-- Initialize receivedAfter timestamp -->
    <!-- 60 mins prior. Get updated at end of doWhile to current time to prepare for next run.
-->
    <Initialize path="/reaqtaData/receivedAfterMilli" value="${time()}" />
    <FormatDate pattern="yyyy-MM-dd'T'HH:mm:ss.SSS'Z'" timeZone="GMT" time="${/reaqtaData/
receivedAfterMilli}" savePath="/reaqtaData/receivedAfter_Formatted" />
    <!-- set the path to just be /alerts at first, but we will modify this as required in the
DoWhile loop -->
    <Set path="/reaqtaData/url" value="https://${/reaqta_host}/rqt-api/1/alerts"/>
    <!-- Get Auth Token -->
    <CallEndpoint url="https://${/reaqta_host}/rqt-api/1/authenticate" method="POST" savePath="/
reaqtaAuth/response">
      <RequestHeader name="Content-Type" value="application/json" />
      <RequestBody type="application/json" encoding="UTF-8">
        {
          "secret":"${/secret_key}",
          "id": "${/app_id}"
        }
      </RequestBody>
    </CallEndpoint>

    <If condition="/reaqtaAuth/response/status_code != 200">
      <Abort reason="${/reaqtaAuth/response/status_code}: ${/reaqtaAuth/response/
status_message}" />
    </If>
    <Set path="/reaqtaAuth/token" value="${/reaqtaAuth/response/body/token}"/>
    <Log type="DEBUG" message="We received an auth token: ${/reaqtaAuth/token}." />

    <!-- Get alerts -->

    <DoWhile condition="not empty(/reaqtaData/response/body/nextPage)"> <!-- There are still
alerts to post to QRadar -->
      <CallEndpoint url="${/reaqtaData/url}" method="GET" savePath="/reaqtaData/response">
        <QueryParameter name="receivedAfter" value="${/reaqtaData/receivedAfter_Formatted}"
omitIfEmpty="true" />
        <QueryParameter name="sortBy" value="receivedAt:asc" />
        <RequestHeader name="Content-Type" value="application/json" />
        <RequestHeader name="Authorization" value="Bearer ${/reaqtaAuth/token}" />
      </CallEndpoint>

      <Log type="DEBUG" message="We received a total of ${count(/reaqtaData/response/body/
result)} Offenses." />
      <Log type="DEBUG" message="Remaining alerts to retrieve: ${/reaqtaData/response/body/
remainingItems}" />

      <If condition="/reaqtaData/response/status_code != 200">
        <Abort reason="${/reaqtaData/response/status_code}: ${/reaqtaData/response/
status_message}" />
      </If>
```

```
      <Else>
        <ClearStatus />
      </Else>

      <If condition="${count(/reaqtaData/response/body/result)} > 0">
        <!-- Post the alerts -->
        <!-- Set host as the LSI -->
        <PostEvents path="/reaqtaData/response/body/result" source="${/reaqta_host}" />
        <ParseDate pattern="yyyy-MM-dd'T'HH:mm:ss.SSS'Z'" date="${max(/reaqtaData/response/body/
result/receivedAt)}" timeZone="UTC" savePath="/reaqtaData/receivedAfterMilli"/>
        <Set path="/reaqtaData/receivedAfterMilli" value="${/reaqtaData/receivedAfterMilli +
1}" />
        <!-- unset this for subsequent loops -->
        <Set path="/reaqtaData/receivedAfter_Formatted" value="" />
      </If>

      <!-- Set the next page if present -->
      <If condition="not empty(/reaqtaData/response/body/nextPage)">
        <Log type="DEBUG" message="Response contained a next page link." />
        <Set path="/reaqtaData/url" value="${/reaqtaData/response/body/nextPage}" />
      </If>
    </DoWhile>
  </Actions>
  <Tests>
    <DNSResolutionTest host="https://${/reaqta_host}"/>
    <TCPConnectionTest host="https://${/reaqta_host}"/>
    <HTTPConnectionThroughProxyTest url="https://${/reaqta_host}"/>
  </Tests>
</Workflow>
```

IBM Security QRadar EDR default workflow parameters

The following example shows the default IBM Security QRadar EDR workflow parameters:

```
<?xml version="1.0" encoding="UTF-8" ?>
<WorkflowParameterValues xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
WorkflowParameterValues/V2">
        <Value name="app_id"            value="App ID goes here"/>
        <Value name="secret_key"        value="Secret Key Goes here"/>
        <Value name="reaqta_host"       value="ReaQta Hostname or IP goes here"/>
</WorkflowParameterValues>
```

IBM Security Verify Event Service protocol configuration options

IBM Security Verify Event Service protocol is formerly known as IBM Cloud® Identity Event Service protocol.

To receive events from IBM Security Verify, configure a log source in IBM QRadar to use the IBM Security Verify Event Service protocol.

The IBM Security Verify protocol is an outbound/active protocol.

When you use the IBM Security Verify Event Service protocol, there are specific parameters that you must use.

Before you can add a log source in QRadar, you must configure IBM Security Verify server to send events to QRadar. For more information, see Configuring IBM Security Verify server to send events to QRadar.

The following table describes the protocol-specific parameters for the IBM Security Verify Event Service protocol:

Table 60. IBM Security Verify Event Service protocol log source parameters

Parameter	Value
Log Source Type	IBM Security Verify
Protocol Configuration	IBM Security Verify Event Service

Table 60. IBM Security Verify Event Service protocol log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured IBM Security Verify Event Service log source, ensure that you give each one a unique name.
Authorization End Point	https://*<your tenant>*.ice.ibmcloud.com
Client ID	The **Client ID** that you recorded when you completed the steps to generate credentials for use with the REST API in IBM Security Verify. For more information, see Configuring IBM Security Verify server to send events to QRadar.
Client Secret	The **Client Secret** that you recorded when you completed the steps to generate credentials for use with the REST API in IBM Security Verify. For more information, see Configuring IBM Security Verify server to send events to QRadar.
Management Events	To collect management events, enable this option. The default is enabled. If the **All Events** parameter is enabled, this option is hidden.
Authentication Events	To collect authentication events, enable this option. The default is enabled. If the **All Events** parameter is enabled, this option is hidden.
SSO Events	To collect Single Sign-On events, enable this option. The default is enabled. If the **All Events** parameter is enabled, this option is hidden.
Enable Advanced Options	If you want to configure advanced protocol parameters, enable this option. The default is disabled.
Advanced Event Types	If you want to collect more event types, enable this option. The default is disabled. If the **All Events** parameter is enabled, this option is hidden.

Table 60. IBM Security Verify Event Service protocol log source parameters (continued)	
Parameter	**Value**
Event Types	Enter the additional event types that you want to collect. Use a comma-separated list of custom event names. For example, `event_type1, event_type2, event_type3` If **Advanced Event Types** is disabled, this option is hidden.
All Events	To collect all event types that are stored on your tenant, enable this option. The default is disabled. If the **Enable Advanced Options** parameter is disabled, this option is hidden.
Use Proxy	Select **True** or **False**. The default is **False**.
Proxy IP or Hostname	The IP address or host name of the proxy server. If the **Use Proxy** parameter is **False**, this option is hidden.
Proxy Port	The port number that is used to communicate with the proxy. The default is 8080. If the **Use Proxy** parameter is **False**, this option is hidden.
Proxy Username	The username that is used to access the proxy. If **Use Proxy** is set to **False**, this option is hidden.
Proxy Password	The password that is used to access the proxy. If the **Use Proxy** parameter is set to **False**, this option is hidden.
Recurrence	The time interval between log source queries to IBM Security Verify for new events. The time interval can be in minutes (M), hours (H), or days (D). For example, 1M, 3H, 5D. The default is 1M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Related tasks

Adding a log source

JDBC protocol configuration options

QRadar uses the JDBC protocol to collect information from tables or views that contain event data from several database types.

The JDBC protocol is an outbound/active protocol. QRadar does not include a MySQL driver for JDBC. If you are using a DSM or protocol that requires a MySQL JDBC driver, you must download and install the *platform-independent* `MySQL Connector/J` from http://dev.mysql.com/downloads/connector/j/.

1. Copy the Java archive (JAR) file to `/opt/qradar/jars` and `/opt/ibm/si/services/ecs-ec-ingress/eventgnosis/lib/q1labs/`.
2. Restart Tomcat service by typing the following command:

```
systemctl restart tomcat
```

3. Restart event collection services by typing the following command:

```
systemctl restart ecs-ec-ingress
```

The following table describes the protocol-specific parameters for the JDBC protocol:

Table 61. JDBC protocol parameters

Parameter	Description
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source Type	Select your Device Support Module (DSM) that uses the JDBC protocol from the **Log Source Type** list.
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or hostname, use the IP address or hostname of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or hostname, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	Select the type of database that contains the events.
Database Name	The name of the database to which you want to connect.
Schema (Snowflake only)	This parameter specifies either the default schema to be used for the specified database post connection, or an empty string. The specified schema must be an existing schema for which the specified default role has privileges.
IP or Hostname	The IP address or hostname of the database server.
Warehouse (Snowflake only)	This parameter specifies the virtual warehouse to use post connection, or an empty string. The specified warehouse must be an existing warehouse for which the specified default role has privileges.

Table 61. JDBC protocol parameters (continued)	
Parameter	**Description**
Role (Snowflake only)	This parameter specifies the default access control role to be used in the Snowflake session initiated by the driver. The specified role must be an existing role that is already assigned to the specified user for the driver. If the specified role is not assigned to the user, then the role is not used during the session initiation by the driver.
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • DB2® - 50000 • Informix® - 9088 • MSDE - 1433 • MySQL - 3306 • Oracle - 1521 • Postgres - 5432 • Sybase - 5000 • Snowflake - 443 If you configure the **Database Instance** parameter and have an MSDE database type, leave the **Port** parameter blank.
Username	A user account for QRadar in the database.
Password	The password that is required to connect to the database.
Confirm Password	The password that is required to connect to the database.
Authentication Domain (MSDE only)	If you disable **Use Microsoft JDBC**, the **Authentication Domain** parameter is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance (MSDE or Informix only)	The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When you use a different port number from the default for SQL database resolution, leave this parameter blank.
Predefined Query (Optional)	Select a predefined database query for the log source. If a predefined query is not available for the log source type, you can select the **None** option. If the configuration guide for a specific integration states to use a predefined query, choose it from the list. Otherwise, select **None** and populate the remaining required values.
Table Name	The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).

Table 61. JDBC protocol parameters (continued)	
Parameter	**Description**
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If you defined a comma-separated list, the list must contain the field that is defined in the **Compare Field** parameter.
Compare Field	A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. When you set this parameter value, the protocol identifies events that were previously pulled by the protocol to ensure that duplicate events are not created.
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Start Date and Time (Optional)	Select or enter the start date and time for database polling. The format is yyyy-mm-dd HH:mm, where HH is specified by using a 24-hour clock. If this parameter is empty, polling begins immediately and repeats at the specified polling interval. This parameter is used to set the time and date at which the protocol connects to the target database to initialize event collection. It can be used along with the **Polling Interval** parameter to configure specific schedules for the database polls. For example, use these parameters to ensure that the poll happens at five minutes past the hour, every hour, or to ensure that the poll happens at exactly 1:00 AM each day. This parameter cannot be used to retrieve older table rows from the target database. For example, if you set the parameter to **Last Week**, the protocol does not retrieve all table rows from the previous week. The protocol retrieves rows that are newer than the maximum value of the **Compare Field** on initial connection.
Polling Interval	Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 20,000.

Table 61. JDBC protocol parameters (continued)	
Parameter	**Description**
Security Mechanism (Db2 only)	From the list, select the security mechanism that is supported by your Db2 server. If you don't want to select a security mechanism, select **None**. The default is **None**. For more information about security mechanisms that are supported by Db2 environments, see the IBM Support website (https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html)
Use Named Pipe Communication (MSDE only)	If you disable **Use Microsoft JDBC**, the **Use Named Pipe Communication** parameter is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.
Database Cluster Name	If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly. This parameter is required if you enable **Use Named Pipe Communication** and select the MSDE database type option.
Use NTLMv2 (MSDE only)	If you disable **Use Microsoft JDBC**, the **Use NTLMv2** parameter is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use Microsoft JDBC (MSDE only)	If you want to use the Microsoft JDBC driver, you must enable **Use Microsoft JDBC**. This parameter is enabled by default.
Use SSL (MSDE only)	Enable this option if your MSDE connection supports SSL.
SSL Certificate Hostname	This field is required when both **Use Microsoft JDBC** and **Use SSL** are enabled. This value must be the fully qualified domain name (FQDN) for the host. The IP address is not permitted. For more information about SSL certificates and JDBC, see the procedures at the following links: • QRadar: Configuring JDBC Over SSL with a Self-signed certificate (https://www.ibm.com/support/pages/node/246077) • Configuring JDBC Over SSL with an Externally-signed Certificate (https://www.ibm.com/support/pages/node/246079)

Table 61. JDBC protocol parameters (continued)	
Parameter	**Description**
Use Oracle Encryption(Oracle only)	*Oracle Encryption and Data Integrity settings* is also known as *Oracle Advanced Security*. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.
Database Locale (Informix only)	For multilingual installations, specify the language to use for the installation process (or software?). After you choose a language, you can then choose the character set that is used in the installation in the **Code-Set** parameter.
Code-Set (Informix only)	The **Code-Set** parameter displays after you choose a language for multilingual installations. Use this field to specify the character set to use.
Enabled	Select this checkbox to enable the log source. By default, the checkbox is selected.
Credibility	From the list, select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select the **Coalescing Events** checkbox to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select the **Store Event Payload** checkbox to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Enable Advanced Options	Select this checkbox to enable advanced options. When disabled, the default value is used.
Use With (No Lock) in SQL statements	Enable this option to append the tables in all SQL statements with "WITH (NOLOCK)".

JDBC - SiteProtector protocol configuration options

You can configure log sources to use the Java Database Connectivity (JDBC) - SiteProtector protocol to remotely poll IBM Proventia® Management SiteProtector® databases for events.

The JDBC - SiteProtector protocol is an outbound/active protocol that combines information from the SensorData1 and SensorDataAVP1 tables in the creation of the log source payload. The SensorData1 and SensorDataAVP1 tables are in the IBM Proventia® Management SiteProtector® database. The maximum number of rows that the JDBC - SiteProtector protocol can poll in a single query is 30,000 rows.

The following table describes the protocol-specific parameters for the JDBC - SiteProtector protocol:

Table 62. JDBC - SiteProtector protocol parameters

Parameter	Description
Protocol Configuration	**JDBC - SiteProtector**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured JDBC - SiteProtector log source, ensure that you give each one a unique name.
Database Type	From the list, select **MSDE** as the type of database to use for the event source.
Database Name	Type `RealSecureDB` as the name of the database to which the protocol can connect.
IP or Hostname	The IP address or host name of the database server.
Port	The port number that is used by the database server. The JDBC - SiteProtector configuration port must match the listener port of the database. The database must have incoming TCP connections enabled. If you define a **Database Instance** when with MSDE as the database type, you must leave the **Port** parameter blank in your log source configuration.
Username	If you want to track access to a database by the JDBC protocol, you can create a specific user for your QRadar system.
Authentication Domain	If you select MSDE and the database is configured for Windows, you must define a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance	If you select MSDE and you have multiple SQL server instances on one server, define the instance to which you want to connect. If you use a non-standard port in your database configuration, or access is blocked to port 1434 for SQL database resolution, you must leave the **Database Instance** parameter blank in your configuration.
Predefined Query	The predefined database query for your log source. Predefined database queries are only available for special log source connections.
Table Name	`SensorData1`
AVP View Name	`SensorDataAVP`
Response View Name	`SensorDataResponse`

Table 62. JDBC - SiteProtector protocol parameters (continued)	
Parameter	**Description**
Select List	Type * to include all fields from the table or view.
Compare Field	`SensorDataRowID`
Use Prepared Statements	Prepared statements allow the JDBC protocol source to set up the SQL statement, and then execute the SQL statement numerous times with different parameters. For security and performance reasons, use prepared statements. You can clear this check box to use an alternative method of querying that does not use pre-compiled statements.
Include Audit Events	Specifies to collect audit events from IBM Proventia Management SiteProtector®.
Start Date and Time	Optional. A start date and time for when the protocol can start to poll the database.
Polling Interval	The amount of time between queries to the event table. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. Numeric values without an H or M designator poll in seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Database Locale	For multilingual installations, use the **Database Locale** field to specify the language to use.
Database Codeset	For multilingual installations, use the **Codeset** field to specify the character set to use.
Use Named Pipe Communication	If you are using Windows authentication, enable this parameter to allow authentication to the AD server. If you are using SQL authentication, disable Named Pipe Communication.
Database Cluster Name	The cluster name to ensure that named pipe communications function properly.
Use NTLMv2	Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The **Use NTLMv2** check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use SSL	Enables SSL encryption for the JDBC protocol.
Log Source Language	Select the language of the events that are generated by the log source. The log source language helps the system parse events from external appliances or operating systems that can create events in multiple languages.

Juniper Networks NSM protocol configuration options

To receive Juniper Networks NSM and Juniper Networks Secure Service Gateway (SSG) logs events, configure a log source to use the Juniper Networks NSM protocol.

The Juniper Networks NSM protocol is an inbound/passive protocol.

The following table describes the protocol-specific parameters for the Juniper Networks Network and Security Manager protocol:

Table 63. Juniper Networks NSM protocol parameters

Parameter	Description
Log Source Type	**Juniper Networks Network and Security Manager**
Protocol Configuration	**Juniper NSM**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Juniper Networks NSM log source, ensure that you give each one a unique name.

Juniper Security Binary Log Collector protocol configuration options

You can configure a log source to use the Security Binary Log Collector protocol. With this protocol, Juniper appliances can send audit, system, firewall, and intrusion prevention system (IPS) events in binary format to QRadar.

The Security Binary Log Collector protocol in an inbound/passive protocol.

The binary log format from Juniper SRX or J Series appliances are streamed by using the UDP protocol. You must specify a unique port for streaming binary formatted events. The standard syslog port 514 cannot be used for binary formatted events. The default port that is assigned to receive streaming binary events from Juniper appliances is port 40798.

The following table describes the protocol-specific parameters for the Juniper Security Binary Log Collector protocol:

Table 64. Juniper Security Binary Log Collector protocol parameters

Parameter	Description
Protocol Configuration	**Security Binary Log Collector**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Juniper Security Binary Log Collector log source, ensure that you give each one a unique name.

Table 64. Juniper Security Binary Log Collector protocol parameters (continued)	
Parameter	**Description**
XML Template File Location	The path to the XML file used to decode the binary stream from your Juniper SRX or Juniper J Series appliance. By default, the device support module (DSM) includes an XML file for decoding the binary stream. The XML file is in the following directory: `/opt/qradar/conf/security_log.xml`.

Log File protocol configuration options

To receive events from remote hosts, configure a log source to use the Log File protocol.

The Log File protocol is an active outbound protocol that is intended for systems that write daily event logs. It is not appropriate to use the Log File protocol for devices that append information to their event files.

Log files are retrieved one at a time by using SFTP, FTP, SCP, or FTPS. The Log File protocol can manage plain text, compressed files, or file archives. Archives must contain plain-text files that can be processed one line at a time. When the Log File protocol downloads an event file, the information that is received in the file updates the **Log Activity** tab. If more information is written to the file after the download is complete, the appended information is not processed.

The following table describes the protocol-specific parameters for the Log File protocol:

Table 65. Log File protocol parameters	
Parameter	**Description**
Protocol Configuration	Log File
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Log File log source, make sure that you give each one a unique name.
Service Type	Select the protocol to use when retrieving log files from a remote server. • SFTP - Secure File Transfer protocol (default) • FTP - File transfer protocol • FTPS - File transfer protocol secure • SCP - Secure copy protocol The server that you specify in the **Remote IP or Hostname** field must enable the SFTP subsystem to retrieve log files with SCP or SFTP.
Remote IP or Hostname	Type the IP address or hostname of the device that contains the event log files.
Remote Port	If the remote host uses a nonstandard port number, you must adjust the port value to retrieve events.
Remote User	Type the username that you use to log in to the host that contains the event files.
Remote Password	Type the password that you use to log in to the host.

Table 65. Log File protocol parameters (continued)	
Parameter	**Description**
Enable Strict Host Key Checking	Enable this option to define a list of permitted public keys for the target host in the **Host Key List** parameter. **Note:** This option is only available when you select either SFTP (Secure File Transfer protocol) or SCP (Secure copy protocol) in the **Service Type** field.
Host Key List	Provide a list of Base64 encoded host keys to use when connecting to the target host. Separate multiple keys by using a newline and use blank lines for formatting. Supported host key types are: `ssh-dss`, `ssh-rsa`, `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, and `ecdsa-sha2-nistp521`. You can obtain these keys by running the OpenSSH command `ssh-keyscan` on Linux, or `ssh-keyscan.exe` on Windows, or getting the public key from the target system directly from a location similar to `/root/.ssh/id_rsa.pub`. Use the Base64 hash only and not the hostname or algorithm. **Note:** This option is only available when you select either SFTP (Secure File Transfer protocol) or SCP (Secure copy protocol) in the **Service Type** field.
SSH Key File	If the system is configured to use key authentication, type the SSH key. When an SSH key file is used, the **Remote Password** field is ignored. The SSH key must be located in the `/opt/qradar/conf/keys` directory. **Important:** The **SSH Key File** field no longer accepts a file path. It can't contain "/" or "~". Type the file name for the SSH key. The keys for existing configurations are copied to the `/opt/qradar/conf/keys` directory. To ensure uniqueness, the keys must have "_<*Timestamp*>" appended to the file name.
Remote Directory	For FTP, if the log files are in the remote user's home directory, you can leave the remote directory blank. A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted.
Recursive	Enable this checkbox to allow FTP or SFTP connections to recursively search subfolders of the remote directory for event data. Data that is collected from subfolders depends on matches to the regular expression in the FTP File Pattern. The **Recursive** option is not available for SCP connections.
FTP File Pattern	The regular expression (regex) that is needed to identify the files to download from the remote host.
FTP Transfer Mode	For ASCII transfers over FTP, you must select `NONE` in the **Processor** field and `LINEBYLINE` in the **Event Generator** field.

Table 65. Log File protocol parameters (continued)	
Parameter	**Description**
FTPS TLS Version	The TLS versions that are compatible with FTPS connections. Select **TLS 1.3** for the highest level of TLS security. When you select an option that supports multiple versions, the FTPS connection negotiates the latest version that is supported by both the client and the server. **TLS 1.3** is compatible with QRadar 7.5.0 Update Package 5 and later. **Important:** TLS 1.0 and TLS 1.1 are no longer supported by QRadar 7.4.3 Fix Pack 3 and 7.5.0 Candidate Release versions, and subsequent releases will cease supporting them. **Restriction:** QRadar supports Explicit FTPS only If the FTP server supports session reuse, ensure that you disable it in the FTP server configuration file. This configuration option is applicable when FTPS is selected in the **Service Type** parameter.
SCP Remote File	For SCP file transfers, type the name of the file on the remote host. You can choose only a single file. This parameter does not support adding multiple files, including methods like file globbing or regular expressions.
Start Time	Select the time of day for the log source to start the file import. This parameter works with the **Recurrence** parameter to establish when and how often the remote directory is scanned for files.
Recurrence	The time interval to determine how frequently the remote directory is scanned for new event log files. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.
Run On Save	Starts the log file import immediately after you save the log source configuration. When selected, this checkbox clears the list of previously downloaded and processed files. After the first file import, the Log File protocol follows the start time and recurrence schedule that the administrator defines.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.
Processor	If the files on the remote host are stored in an archive format, select the processor that is used to decompress the event log. If the files are not stored in an archive format, select **None**. The default value is **None**.
Ignore Previously Processed File(s)	Select this checkbox to track files that the log source processes. This option prevents duplicate events from files that are processed a second time. This checkbox applies to FTP and SFTP file transfers.
Change Local Directory	Changes the local directory on the **Target Event Collector** to store event logs before they are processed.
Local Directory	The local directory on the **Target Event Collector**. The directory must exist before the Log File protocol attempts to retrieve events.

Table 65. Log File protocol parameters (continued)

Parameter	Description
Event Generator	Choose one of the following file types to use as an event generator for the protocol. **LineByLine** Each line is processed as a single event. A 10 line file creates 10 separate events. **HPTandem** The file is processed as a HPTandem NonStop binary audit log. Each record in the log file (whether primary or secondary) is converted into text and processed as a single event. HPTandem audit logs use the following file name pattern: `[aA]\d{7}`. **WebSphere Application Server** Processes event logs for WebSphere Application Server. The remote directory must define the file path that is configured in the DSM. **W3C** Processes log files from sources that use the W3C format. The header of the log file identifies the order and data that is contained in each line of the file. **Fair Warning** Processes log files from Fair Warning devices that protect patient identity and medical information. The remote directory must define the file path to the event logs that the Fair Warning device generates. **DPI Subscriber Data** The file is processed as a DPI statistic log produced by a Juniper Networks MX router. The header of the file identifies the order and data that is contained in each line of the file. Each line in the file after the header is formatted to a tab-delimited `name=value` pair event. **SAP Audit Logs** Process files for SAP Audit Logs to keep a record of security-related events in SAP systems. **Oracle BEA WebLogic** Processes files for Oracle BEA WebLogic application log files. **Juniper SBR** Processes the event log files from Juniper Steel-belted RADIUS. **ID-Linked Multiline** Processes multiline event logs that contain a common value at the start of each line in a multiline event message. This option uses regular expressions to identify and reassemble the multiline event in to single event payload. **Line Matcher** Iterates through the lines until a line is found that matches the pattern, and discards any lines that do not match the pattern. **Oracle OS XML Audit** Processes the audit log produced by Oracle Database. **Oracle OS Multiline Audit** Processes multiline Oracle Audit logs that contains audit information like action, user, status, and so on. **RegEx Based Multiline** Iterates through the lines based on the start pattern, end pattern, and ignore pattern of the provided regular expressions, and discards any lines in the stream that do not match the patterns.

Table 65. Log File protocol parameters (continued)	
Parameter	**Description**
File Encoding	The character encoding that is used by the events in your log file.
Message ID Pattern	Type a regular expression (regex) that identifies a common value at the start of each line in a multiline event message.
Folder Separator	The character that is used to separate folders for your operating system. Most configurations can use the default value in the **Folder Separator** field. This field is intended for operating systems that use a different character to define separate folders. For example, periods that separate folders on mainframe systems.
Start Pattern RegEx	Type a regular expression (regex) that identifies the start pattern of each line.
End Pattern RegEx	Type a regular expression (regex) that identifies the end pattern of each line.
Ignore Pattern RegEx	Type a regular expressions (regex) to exclude a specific pattern in each line.
Date Time RegEx	Type a regular expression (regex) that identifies the date and time format of each line.
Date Time Format	Type a date and time format to identify the start of an event from each line.

Configure QRadar to use FTPS for the Log File protocol

To configure FTPS for the Log File protocol, you must place server SSL certificates on all QRadar Event Collectors that connect to your FTP server. If your SSL certificate is not RSA 2048, create a new SSL certificate.

The following command provides an example of creating a certificate on a LINUX system by using Open SSL:

```
openssl req -newkey rsa:2048 -nodes -keyout ftpserver.key -x509 -days 365 -out ftpserver.crt
```

Files on the FTP server that have a `.crt` file extension must be copied to the `/opt/qradar/conf/trusted_certificates` directory on each of your Event Collectors.

Microsoft Azure Event Hubs protocol configuration options

The Microsoft Azure Event Hubs protocol is an outbound and active protocol for IBM Security QRadar that collects events from Microsoft Azure Event Hubs.

Important: By default, each Event Collector can collect events from up to 1000 partitions before it runs out of file handles. If you want to collect from more partitions, you can contact IBM Support for advanced tuning information and assistance. For more information, see IBM Support.

The following parameters require specific values to collect events from Microsoft Azure Event Hubs appliances:

Table 66. Microsoft Azure Event Hubs log source parameters	
Parameter	**Value**
Use Event Hub Connection String	Authenticate with an Azure Event Hub by using a connection string. **Note:** The ability to toggle this switch to off is deprecated.
Event Hub Connection String	Authorization string that provides access to an Event Hub. For example, `Endpoint=sb://<Namespace Name>.servicebus.windows.net/;SharedAccess KeyNam Key Name>;SharedAccessKey=<SAS Key>; EntityPath=<Event Hub Name>`
Consumer Group	Specifies the view that is used during the connection. Each **Consumer Group** maintains its own session tracking. Any connection that shares consumer groups and connection information shares session tracking information.
Use Storage Account Connection String	Authenticates with an Azure Storage Account by using a connection string. **Note:** The ability to toggle this switch to off is deprecated.
Storage Account Connection String	Authorization string that provides access to a Storage Account. • Access Key example: `DefaultEndpointsProtocol=https;AccountName=<Storage Account Name>;AccountKey=<Storage Account Key>;EndpointSuffix=core.windows.net` • Shared Access Signature example: `BlobEndpoint=<Blob Endpoint>;QueueEndpoint=<Queue Endpoint>;FileEndpoint=<File Endpoint>;TableEndpoint=<Table Endpoint>;SharedAccessSignature=<Access Signature>`
Format Azure Linux Events To Syslog	Formats Azure Linux logs to a single-line syslog format that resembles standard syslog logging from Linux systems.
Convert VNet Flow Logs to IPFIX	Microsoft Azure VNet Flow Logs. Select this option to send flow logs to the **Network Activity** tab in QRadar.
Flow HostName	Enable **Convert VNet Flow Logs to IPFIX** to configure this parameter. The flow processor hostname where the Microsoft Azure VNet Flow Logs are sent.

Table 66. Microsoft Azure Event Hubs log source parameters (continued)

Parameter	Value
Flow Port	Enable **Convert VNet Flow Logs to IPFIX** to configure this parameter. The flow processor port where the Microsoft Azure VNet Flow Logs are sent.
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events that are being processed.
Log Source Identifier Pattern	When the **Use As A Gateway Log Source** option is selected, use this option to define a custom log source identifier for events that are processed. If the **Log Source Identifier Pattern** is not configured, QRadar receives events as unknown generic log sources. The **Log Source Identifier Pattern** field accepts key-value pairs, such as **key**=value, to define the custom Log Source Identifier for events that are being processed and for log sources to be automatically discovered when applicable. **Key** is the Identifier Format String, which is the resulting source or origin value. Value is the associated regex pattern that is used to evaluate the current payload. The value (regex pattern) also supports capture groups, which can be used to further customize the key (Identifier Format String). Multiple key-value pairs can be defined by typing each pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found. When a match is found, a custom Log Source Identifier is displayed. The following examples show the multiple key-value pair functionality: **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK

Table 66. Microsoft Azure Event Hubs log source parameters (continued)	
Parameter	**Value**
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Use Proxy	When you configure a proxy, all traffic for the log source travels through the proxy to access the Azure Event Hub. After you enable this parameter, configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not need authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank. **Note:** Digest Authentication for Proxy is not supported in the Java SDK for Azure Event Hubs. For more information, see Azure Event Hubs - Client SDKs (https://docs.microsoft.com/en-us/azure/event-hubs/sdks).
Proxy IP or Hostname	The IP address or hostname of the proxy server. This parameter appears when **Use Proxy** is enabled.
Proxy Port	The port number used to communicate with the proxy. The default value is 8080. This parameter appears when **Use Proxy** is enabled.
Proxy Username	The username for accessing the proxy server. This parameter appears when **Use Proxy** is enabled.
Proxy Password	The password for accessing the proxy server. This parameter appears when **Use Proxy** is enabled.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

The following table describes the Microsoft Azure Event Hubs log source parameters that are deprecated:

Table 67. Deprecated Microsoft Azure Event Hubs log source parameters	
Parameter	**Value**
Deprecated - Namespace Name	This option displays if **Use Event Hub Connection String** option is set to off. The name of the top-level directory that contains the Event Hub entities in the Microsoft Azure Event Hubs user interface.
Deprecated - Event Hub Name	This option displays if **Use Event Hub Connection String** option is set to off. The identifier for the Event Hub that you want to access. The **Event Hub Name** must match one of the Event Hub entities within the namespace.
Deprecated - SAS Key Name	This option displays if **Use Event Hub Connection String** option is set to off. The Shared Access Signature (SAS) name identifies the event publisher.
Deprecated - SAS Key	This option displays if **Use Event Hub Connection String** option is set to off. The Shared Access Signature (SAS) key authenticates the event publisher.
Deprecated - Storage Account Name	This option displays if **Use Storage Account Connection String** option is set to off. The name of the storage account that stores Event Hub data. The **Storage Account Name** is part of the authentication process that is required to access data in the Azure Storage Account.
Deprecated - Storage Account Key	This option displays if **Use Storage Account Connection String** option is set to off. An authorization key that is used for storage account authentication. The **Storage Account Key** is part of the authentication process that is required to access data in the Azure Storage Account.

Related concepts

"Gateway log source" on page 15

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

Related information

Adding a log source

Configuring Microsoft Azure Event Hubs to communicate with QRadar

The Microsoft Azure Event Hubs protocol collects events that are inside an Event Hub. This protocol collects events regardless of source provided they are inside the Event Hub. However, these events might not be parsable by an existing DSM.

Before you begin

To retrieve events in QRadar, you need to create a Microsoft Azure Storage Account and an Event Hub entity under the Azure Event Hub Namespace. For every Namespace, port 5671 must be open. For every Storage Account, port 443 must be open.

The Namespace hostname is usually `[Namespace Name].servicebus.windows.net` and the Storage Account hostname is usually `[Storage_Account_Name].blob.core.windows.net`. The Event Hub must have at least one Shared Access Signature that is created with Listen Policy and at least one Consumer Group.

Procedure

1. Obtain a Microsoft Azure storage account connection string by using one of the following methods.
   - If you want a log source that has full access to all permissions, obtain an access key. See step "2" on page 164.
   - If you want a log source with specific permissions for access, create a shared access signature (SAS). See step "3" on page 165.

   Important: To connect to a Microsoft Azure Event Hub, you must be able to create a block blob on the Azure Storage Account you select. Page and append blob types are not compatible with the Microsoft Azure Event Hubs Protocol.

   For more information, see Introduction to Azure Blob storage (https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction) and Understanding Block Blobs, Append Blobs, and Page Blobs (https://docs.microsoft.com/en-us/rest/api/storageservices/understanding-block-blobs--append-blobs--and-page-blobs). For further help, see Microsoft Support (https://azure.microsoft.com/en-us/support/options).
2. Obtain a Microsoft Azure Storage Account Connection String and access key.

   Use this method to obtain values that give the log source full access to the storage account.

   The **Storage Account Connection String** contains authentication for the **Storage Account Name** and the **Storage Account Key** that is used to access the data in the Azure Storage account.

   a) Log in to the Azure Portal. (https://portal.azure.com)

   b) From the dashboard, in the **All resources** section, select a **Storage account**.

   c) From the **All types** list, disable **Select All**. In the filter items search box, type `Storage Accounts`, and then select **Storage Accounts** from the list.

   d) From the **Storage account** menu, select **Access keys**.

   e) Record the value for the **Storage account name**. Use this value for the **`Storage Account Name`** parameter value when you configure a log source in IBM QRadar.

   f) From the **key 1** or **key 2** section, record the following values.
      - **Key** - Use this value for the **`Storage Account Key`** parameter value when you configure a log source in QRadar.
      - **Connection string** - Use this value for the **`Storage Account Connection String`** parameter value when you configure a log source in QRadar.

        Example:

        ```
        DefaultEndpointsProtocol=https;AccountName=[Storage Account Name]
        ;AccountKey=[Storage Account Key];EndpointSuffix=core.windows.net
        ```

Most storage accounts use `core.windows.net` for the end-point suffix, but this value can change depending on its location. For example, a government-related storage account might have a different endpoint suffix value. You can use the **Storage Account Name** and **Storage Account Key** values, or you can use the **Storage Account Connection String** value to connect to the Storage Account. You can use key1 or key2.

QRadar creates a container that is named `qradar` in the provided storage blob.

Tip: Through the Azure Event Hubs SDK, QRadar uses a container in the configured storage account blob to track event consumption from the Event Hub. A container that is named `qradar` is automatically created to store the tracking data, or you can manually create the container.

3. Generate a shared access signature (SAS).

   Use this method to obtain values to give the log source specific permissions for accessing the storage account.

   a) Log in to the Azure Portal. (https://portal.azure.com)

   b) From the dashboard, in the **All resources** section, select a **Storage account**.

   c) From the **All types** list, disable **Select All**. In the filter items search box, type `Storage Accounts`, and then select **Storage Accounts** from the list.

   d) From the **Storage account** menu, select **Shared access signature**.

   e) Configure a SAS with the following permissions:

   Important: These permissions are the minimum amount that you must give to your SAS, so QRadar can access Microsoft Azure. You can give the SAS more permissions.

Permission	Value
Allowed services	Blob
Allowed resource types	Container Object
Allowed permissions	Read Write Delete List

   f) Click **Generate SAS and connection string**.

   g) Record the following value:

   Shared access signature - Use this value for the **`Storage Account Connection String`** parameter value when you configure a log source in QRadar.

   Example:

```
BlobEndpoint=[BlobEndpoint];QueueEndpoint=[QueueEndpoint];FileEndpoint=[FileEndpoint];Tabl
eEndpoint=[TableEndpoint];SharedAccessSignature=[Access Signature]
```

4. Obtain a Microsoft Azure Event Hub Connection String.

   The Event Hub Connection String contains the **Namespace Name**, the path to the Event Hub within the namespace and the Shared Access Signature (SAS) authentication information.

   a) Log in to the Azure Portal (https://portal.azure.com).

   b) From the dashboard, in the **All resources** section, select an Event Hub. Record this value to use as the **`Namespace Name`** parameter value when you configure a log source in QRadar.

   c) In the **Entities** section, select **Event Hubs**. Record this value to use for the **`Event Hub Name`** parameter value when you configure a log source in QRadar.

d) From the **All types** list, disable **Select All**. In the **filter items** search box, type `event hub`, and then select **Event Hubs Namespace** from the list.

e) In the Event Hub section, select the event hub that you want to use from the list. Record this value to use for the Event Hub Name parameter value when you configure a log source in QRadar.

f) In the **Settings** section, select **Shared access policies**.

Important: In the Entities section, ensure that the Consumer Groups option is listed. If Event Hubs is listed, return to Step c.

i) Select a **POLICY** that contains a **Listen CLAIMS**. Record this value to use for the **SAS Key Name** parameter value when you configure a log source in QRadar.

ii) Record the values for the following parameters:

Primary key or Secondary key
Use the value for the **SAS Key** parameter value when you configure a log source in QRadar. The Primary key and Secondary key are functionally the same.

Connection string-primary key or Connection string-secondary key
Use this value for the **Event Hub Connection String** parameter value when you configure a log source in QRadar. The Connection string-primary key and Connection string-secondary key are functionally the same.

Example:

```
Endpoint=sb://[Namespace Name].servicebus.windows.net
/;SharedAccessKeyName=[SAS Key Name];SharedAccessKey=[SAS Key];
EntityPath=[Event Hub Name]
```

You can use the **Namespace Name**, **Event Hub Name**, **SAS Key Name** and **SAS Key** values, or you can use the **Event Hub Connection String** value to connect to the Event Hub.

5. In the **Entities** section, select **Consumer groups**. Record the value to use for the **Consumer Group** parameter value when you configure a log source in QRadar.

Important: Do not use the **$Default** consumer group that is automatically created. Use an existing consumer group that is not in use or create a new consumer group. Each consumer group must be used by only one device, such as QRadar.

Related reference
QRadar supported DSMs

Configuring VNet Flow Logs on the Microsoft Azure portal

The **Virtual Network (VNet) Flow Logs** event is a feature of Microsoft Azure Network Watcher. You can use the flow logs to log information about the IP traffic that is flowing through a virtual network.

Before you begin

To configure the **VNet flow logs** in the Microsoft Azure, complete the below prerequisites.

1. Configure **Event Hub**, **Consumer Group** and **Storage Account**.

Attention: If these tools are already created in your azure portal, you can skip the create process and gather the name of the tool.

2. Create a **Resource Group** for the same **Region** as that of the **VNet flow logs**. For more information, see Create resource groups.
3. Create a new **Event Hubs namespace** and enter the **Resource Group** and **Region**. For more information, see Create an Event Hubs namespace.

a. Create an **Event Hub** under the **Event Hub namespace**. For more information, see Create an event hub.

4. Create a shared access policy under the **Event Hub**. Assign **Send** and **Listen** access and configure the **Event Hub Connection String**.
5. Create a consumer group under the **Event Hub**.
6. From the Storage Account's Access Key, fetch the **Storage Account Connection String**.

Procedure

1. Create a **Virtual Network** with data traffic before you enable the **VNet flow logs**. For more information, see Create a virtual network and an Azure Bastion host.
2. Create a **Log Analytics Workspace** by entering the **Resource Group** and **Region**. For more information, see Create a Log Analytics workspace.
3. Enable **Network Watcher** and add the **Region** for which you are configuring the **VNet flow logs**. For more information, see Enable Network Watcher for your region.
4. Enable **VNet flow log**.
   a) Gather the **Region**, the **Virtual Network**, the **Storage Account**, and the **Log Analytics Workspace**.
   b) Enter the information in the below command. For more information, see Create, change, enable, disable, or delete VNet flow logs using the Azure CLI.

```
az network watcher flow-log create --location <region> --name <myVNetFlowLog> --resource-
group <myResourceGroup> --vnet <myVNet> --storage-account <myStorageAccount> --workspace
<myWorkspace> --interval 10 --traffic-analytics true
```

5. Create **Traffic Analytics**.
   a) Navigate to the **Log Analytics Workspace**.
   b) Select **Data Export** and click **Create Export Rule**.
   c) Enter the rule **Name** and select the table name **NTANetAnalytics**.
   d) Select **Event Hub** as the **Destination** name.
   e) Enter a **Subscription**.
   f) Enter the **Event Hub Workspace** name and **Event Hub** name.
   g) Click **Create**.
6. After completing the above steps, add the **Event Hub Connection String**, **Consumer Group** name and **Storage Account String** to the **Log Source**. The events are now recorded as per the configurations.

Related reference
QRadar supported DSMs

Troubleshooting Microsoft Azure Event Hubs protocol

To resolve issues with the Microsoft Azure Event Hubs protocol use the troubleshooting and support information. Find the errors by using the protocol testing tools in the QRadar Log Source Management app.

General troubleshooting

The following steps apply to all user input errors. The general troubleshooting procedure contains the first steps to follow any errors with the Microsoft Azure Event Hubs protocol.

1. If the **Use Event Hub Connection String** or **Use Storage Account Connection String** option is set to off, switch it to **On**. For more information about getting the connection strings, see Configuring Microsoft Azure Event Hubs to communicate with QRadar.

2. Confirm that the Microsoft Azure event hub connection string follows the format in the following example. Ensure that the **entityPath** parameter value is the name of your event hub.

```
Endpoint=sb://<Namespace
Name>.servicebus.windows.net/;SharedAccessKeyName=<SAS Key
Name>;SharedAccessKey=<SAS Key>;EntityPath=<Event Hub Name>
```

   After the log source is saved and closed, for security reasons, you can no longer see the entered values. If you don't see the values, enter them and then confirm their validity.

3. Confirm that the Microsoft Azure storage account connection string follows the format of the following example.

```
DefaultEndpointsProtocol=https;AccountName=<Storage Account
Name>;AccountKey=<Storage Account Key>;EndpointSuffix=core.windows.net
```

   After the log source is saved and closed, for security reasons, you can no longer see the entered values. If you don't see the values, reenter them and then confirm their validity.

4. Optional: For troubleshooting, set **Use As a Gateway Log Source** to **Off** and set **Format Azure Linux Events to Syslog** to **On**. This forces all events to go through the selected log source type. This can quickly determine whether minimum events are arriving and that there is no network or access issue.

   If you leave **Use As a Gateway Log Source** set to **On**, ensure that the events are not arriving in QRadar as **unknown**, **stored, or sim-generic**. If they are, it might explain why the protocol appears to be not working.

5. Ensure that the provided consumer group exists for the selected event hub. For more information, see Configuring Microsoft Azure Event Hubs to communicate with QRadar.
6. Enable the **Automatically Acquire Server Certificate** option or confirm that the certificate is manually added in QRadar.
7. Ensure that the QRadar system time is accurate; if the system time is not in real time, you might have network issues.
8. Ensure that the port 443 is open to the storage account host. The storage account host is usually *<Storage_Account_Name>.<something>*, where *<something>* usually refers to the endpoint suffix.
9. Ensure that port 5671 is open on the event hub host. The event hub host is usually the *<Endpoint>* from the event hub connection string.

For more information, see:

- “Illegal connection string format exception” on page 168
- “Storage exception” on page 169
- “Illegal Entity exception” on page 170
- “URI Syntax exception” on page 170
- “Invalid key exception” on page 171
- “Timeout exception” on page 171
- “Other exceptions” on page 172
- “Microsoft Azure Event Hubs protocol FAQ” on page 172

Illegal connection string format exception

Symptoms

Error: “Ensure that the Event Hub Connection String or Event Hub parameters are valid."

"This exception is thrown when the Event Hub Connection String or Event Hub information that is provided does not meet the requirements to be a valid connection string. An attempt will be made to query for content at the next retry interval."

Causes

The **Event Hub Connection String** doesn't match the specifications set by Microsoft. This error can also occur if unexpected characters, such as white space, are copied into the event hub connection string.

Resolving the problem

Follow these steps to resolve your illegal connection string error.

1. Ensure that the storage account connection string is valid and appears in a similar format to the following example:

   ```
   Endpoint=sb://<Namespace
   Name>.servicebus.windows.net/;SharedAccessKeyName=<SAS Key
   Name>;SharedAccessKey=<SAS Key>;EntityPath=<Event Hub Name>
   ```

2. When you move the event hub connection string from the Azure portal to IBM QRadar, ensure that no additional white space or invisible characters are added. Alternatively, before you copy the string, ensure that you don't copy any additional characters or white space.

Storage exception

Symptoms

Error: “Unable to connect to the Storage Account **[Storage Account Name]**. Ensure that the Storage Account Connection String is valid and that QRadar can connect to **[Storage Account Host Name]**."

"An error occurred that represents an exception for the Microsoft Azure Storage Service. An attempt will be made to query for content at the next retry interval."

Causes

Storage exception errors represent issues that occur when you authenticate with a storage account or when you communicate with a storage account. An attempt is made to query for content at the next retry interval. There are two common issues that might occur due to a storage exception.

1. The storage account connection string is invalid.
2. Network issues are preventing QRadar from communicating with the storage account.

Resolving the problem

Follow these steps to resolve your storage exception error.

1. Ensure that the storage account connection string is valid and displays in a similar format to the following example.

   ```
   DefaultEndpointsProtocol=https;AccountName=<Storage Account
   Name>;AccountKey=<Storage Account Key>;EndpointSuffix=core.windows.net
   ```

2. Ensure that QRadar can communicate with the storage account host on port 443.
3. Ensure that QRadar can communicate with the event hub on port 5671.
4. Verify that the system time in QRadar matches the current time. Security settings on the storage account prevent mismatched times between the server (storage account) and the client (QRadar).
5. Ensure that a certificate is downloaded manually or by using the **Automatically Acquire Server Certificate(s)** option. The certificates are downloaded from `<Storage Account Name>.blob.core.windows.net`.

Illegal Entity exception

Symptoms

Error: “An entity, such as the Event Hub, cannot be found. Verify that the Event Hub information provided is valid. This exception is thrown when the Event Hub Connection String or Event Hub information that is provided does not meet the requirements to be a valid connection string. An attempt will be made to query for content at the next retry interval.”

Error: "The messaging entity 'sb://qahub4.servicebus.windows.net/notreal' could not be found. To know more visit https://aka.ms/sbResourceMgrExceptions."

Error: "com.microsoft.azure.eventhubs.IllegalEntityException: The messaging entity 'sb://qahub4.servicebus.windows.net/notreal' could not be found. To know more visit https://aka.ms/sbResourceMgrExceptions."

Causes

The event hub (entity) doesn’t exist or the event hub connection string doesn’t contain a reference to an event hub (entity).

Resolving the problem

Follow these steps to resolve your illegal entity error.

1. Make sure that the event hub connection string contains the `entitypath` section and that it refers to the event hubs name. For example,

   ```
   Endpoint=sb://<Namespace
   Name>.servicebus.windows.net/;SharedAccessKeyName=<SAS Key
   Name>;SharedAccessKey=[SAS Key];EntityPath=<Event Hub Name>
   ```

2. Verify that the event hub exists on the Azure portal, and that the event hub path references the `entitypath` that you want to connect to.
3. Verify that the consumer group is created and entered correctly in the **Consumer Group** field.

URI Syntax exception

Symptoms

Error: “The Storage Account URI is malformed. Ensure that the Storage Account information is valid and properly formatted. Unable to connect to the host.”

Error: "Could not parse text as a URI reference. For more information see the “Raw Error Message". An attempt will be made to query for content at the next retry interval."

Causes

The URI that is formed from the storage account connection string is invalid. The URI is formed from the `DefaultEndpointsProtocol`, `AccountName`, and `EndpointSuffix` fields. If one of these fields is altered, this exception can occur.

Resolving the problem

Recopy the Storage Account Connection String from the Azure Portal. It displays similar to the following example:

```
DefaultEndpointsProtocol=https;AccountName=<Storage Accounts
Name>;AccountKey=<Storage Account Key>;EndpointSuffix=core.windows.net
```

Invalid key exception

Symptoms

Error: “The Storage Account Key was invalid. Unable to connect to the host.”

Error: “An invalid key was encountered. This error is commonly associated with passwords or authorization keys. For more information see the "Raw Error Message". An attempt will be made to query for content at the next retry interval”

Causes

The key that is formed from the storage account connection string is invalid. The storage account key is in the connection string. If the key is altered, it might become invalid.

Resolving the problem

From the Azure portal, recopy the storage account connection string. It displays similar to the following example:

```
DefaultEndpointsProtocol=https;AccountName=<Storage Account
Name>;AccountKey=<Storage Account Key>;EndpointSuffix=core.windows.net
```

Timeout exception

Symptoms

Error: “Ensure that there are no network related issues preventing the connection. Additionally ensure that the Event Hub and Storage Account Connection Strings are valid.”

Error: “The server did not respond to the requested operation within the specified time, which is controlled by OperationTimeout. The server might have completed the requested operation. This exception can be caused by network or other infrastructure delays. An attempt will be made to query for content at the next retry interval.”

Causes

The most common cause is that the connection string information is invalid. The network might be blocking communication, resulting in a timeout. While rare, it is possible that the default timeout period (60 seconds) is not long enough due to network congestion.

Resolving the problem

Follow these steps to resolve your timeout exception error.

1. When you copy the event hub connection string from the Azure portal to IBM QRadar, ensure that no additional white space or invisible characters are added. Alternatively, before you copy the string, ensure that you don't copy any additional characters or white space.
2. Verify that the storage account connection string is valid and appears in a similar format to the following example:

   ```
   DefaultEndpointsProtocol=https;AccountName=<Storage Account
   Name>;AccountKey=<Storage Account Key>;EndpointSuffix=core.windows.net
   ```
3. Ensure that QRadar can communicate with the storage account host on port 443, and with the event hub on ports 5671 and 5672.
4. Ensure that a certificate is downloaded manually or by using the **Automatically Acquire Server Certificate(s)** option. The certificates are downloaded from `<Storage Account Name>.blob.core.windows.net`.

5. Advanced- There is a hidden parameter that can increase the default timeout from 60 seconds. Contact support for assistance in getting the timeout increased.

Other exceptions

Symptoms

Error: “Ensure that there are no network related issues preventing the connection. Additionally ensure that the Event Hub and Storage Account Connection Strings are valid.”

Error: “An error occurred. For more information, see the \"Raw Error Message\". An attempt will be made to query for content at the next retry interval”

Causes

Exceptions in this category are unknown to the protocol and are unexpected. These exceptions can be difficult to troubleshoot and usually require research to resolve.

Resolving the problem

Follow these steps to resolve your error. They might resolve some of the more common issues.

1. Ensure that the event hub connection string uses the same or a similar format as displayed in the following example:

   ```
   Endpoint=sb://<Namespace
   Name>.servicebus.windows.net/;SharedAccessKeyName=<SAS Key
   Name>;SharedAccessKey=[SAS Key];EntityPath=<Event Hub Name>
   ```
2. When you move the event hub connection string from the Azure portal to IBM QRadar, ensure that no additional white space or invisible characters are added. Alternatively, before you copy the string, ensure that you don't copy any additional characters or white space.
3. Ensure that the storage account connection string is valid and displays in a similar format to the following example:

   ```
   DefaultEndpointsProtocol=https;AccountName=<Storage Account
   Name>;AccountKey=<Storage Account Key>;EndpointSuffix=core.windows.net
   ```
4. Ensure that QRadar can communicate with the storage account host on port 443, and with the event hub on port 5671 and 5672.
5. Verify that a certificate is downloaded manually or by using the **Automatically Acquire Server Certificate(s)** option. The certificates are downloaded from `<Storage Account Name>.blob.core.windows.net`.
6. Verify that the system time in QRadar matches the current time. Security settings on the storage account prevent mismatched times between the server (storage account) and the client (QRadar).

Microsoft Azure Event Hubs protocol FAQ

Use these frequently asked questions and answers to help you understand the Microsoft Azure Event Hubs protocol.

- “Why do I need a storage account to connect to an event hub?” on page 173
- “Why does the Microsoft Azure Event Hubs protocol use the storage account?” on page 173
- “How much data does the storage account need to store?” on page 173
- “Does my storage account need to contain events?” on page 173
- “What does a blob file that is created by the Microsoft Azure Event Hubs protocol look like?” on page 173
- “Can I use the same storage account with other event hubs?” on page 173

- “What do I do if the protocol isn't collecting events?” on page 173
- “Why do I need to open the ports for two different IPs that have different ports?” on page 174
- “Can I collect <Service/Product> events by using the Microsoft Event Hubs protocol?” on page 174
- “What does the Format Azure Linux Events To Syslog option do?” on page 174

Why do I need a storage account to connect to an event hub?

You must have a storage account for the Microsoft Azure Event Hubs protocol to manage the lease and partitions of an event hub. For more information, see the Event processor host documentation (https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-event-processor-host).

Why does the Microsoft Azure Event Hubs protocol use the storage account?

The Microsoft Azure Event Hubs protocol uses the storage account to track partition ownership. This protocol creates blob files in the Azure storage account in the `<Event Hub Name> → <Consumer group Name>` directory. Each blob file relates to a numbered partition that is managed by the event hub. For more information, see the Event processor host documentation (https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-event-processor-host).

How much data does the storage account need to store?

The amount of data that needs to be stored in a storage account is the number of partitions that are multiplied by ~150 bytes.

Does my storage account need to contain events?

No. Storing the logs in storage is an option that is provided by Microsoft. However, this option is not used by the protocol.

What does a blob file that is created by the Microsoft Azure Event Hubs protocol look like?

The following example shows what is stored in a blob file that is created by the protocol:

```
{"offset":"@latest","sequenceNumber":0,"partitionId":"3","epoch":8,"owner":"","token":""}”
```

Can I use the same storage account with other event hubs?

There are no restrictions on how many event hubs can store data in a storage account. You can use the same storage account for all log sources in the same QRadar environment. This creates a single location for all event hub partition management folders and files.

What do I do if the protocol isn't collecting events?

If the protocol appears to be working and the protocol testing tools pass all of the tests, and you don't see events, follow these steps to confirm whether events are posted.

1. Confirm that there are events for the event hub to collect. If the Azure side configuration is not correct, the event hub might not collect the events.
2. If the **Use as a Gateway Log Source** is enabled, do a payload search for events that the Event Hub log source collects. If you are not sure what the events should look like, then go to step 4.
3. If the **Use as a Gateway Log Source** option is enabled, and the protocol is not collecting events, test the same log source with the gateway disabled. By setting the **Use as a Gateway Log Source** to disabled, all collected events are forced to use the log source that is connected to the protocol. If events are arriving when the **Use as a Gateway Log Source** is disabled, but events are not arriving

when **Use as a Gateway Log Source** is enabled, there might be an issue with the log source identifier options or the Traffic Analysis can't automatically match the events to a DSM.

4. If you identified in Step 2 or Step 3 that the events are not coming in under the expected log source, there might be an issue with the event hub log sources *logsourceidentifierpattern*. For issues related to the event hub log source identifier pattern, you might need to contact Support.

Why do I need to open the ports for two different IPs that have different ports?

You need two different IPs to have different ports open because the Microsoft Azure Event Hub protocol communicates between the event hub host and the storage account host.

The event hub connection uses the Advanced Message Queuing Protocol (AMQP) with ports 5671 and 5672. The storage account uses HTTPS with ports 443. Because the storage account and the event hub have different IPs, you must open two different ports.

Can I collect <Service/Product> events by using the Microsoft Event Hubs protocol?

The Microsoft Event Hubs protocol collects all events that are sent to the event hub, but not all events are parsed by a supported DSM. For a list of supported DSMs, see QRadar supported DSMs.

What does the *Format Azure Linux Events To Syslog* option do?

This option takes the Azure Linux event, which is wrapped in a JSON format with metadata, and converts it to a standard syslog format. Unless there is a specific reason that the metadata on the payload is required, enable this option. When this option is disabled, the payloads do not parse with Linux DSMs.

(Back to top)

Microsoft Defender for Endpoint SIEM REST API protocol configuration options

Configure a Microsoft Defender® for Endpoint SIEM REST API protocol to receive events from supported Device Support Modules (DSMs).

The Microsoft Defender for Endpoint SIEM REST API protocol is an outbound/active protocol.

Important: Due to a change in the Microsoft Defender API suite as of 25 November 2021, Microsoft no longer allows the onboarding of new integrations with their SIEM API. For more information, see Deprecating the legacy SIEM API (https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/deprecating-the-legacy-siem-api/ba-p/3139643).

The Streaming API can be used with the Microsoft Azure Event Hubs protocol to provide event and alert forwarding to QRadar. For more information about the service and its configuration, see Configure Microsoft 365 Defender to stream Advanced Hunting events to your Azure Event Hub (https://docs.micosoft.com/en-us/microsoft-365/security/defender/streaming-api-event-hub?view=o365-worldwide)

The following table describes the protocol-specific parameters for the Microsoft Defender for Endpoint SIEM REST API protocol:

Table 68. Microsoft Defender for Endpoint SIEM REST API protocol

Parameter	Value
Log Source type	Microsoft 365 Defender
Protocol Configuration	Microsoft Defender for Endpoint SIEM REST API

Table 68. Microsoft Defender for Endpoint SIEM REST API protocol (continued)	
Parameter	**Value**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Microsoft Defender for Endpoint SIEM REST API log source, ensure that you give each one a unique name.
Authorization Server URL	The URL for the server that provides the authorization to obtain an access token. The access token is used as the authorization to collect events from Microsoft 365 Defender. The Authorization Server URL uses the following format: `"https://login.microsoftonline.com/<Tenant_ID>/oauth2/token"` where *<Tenant_ID>* is a UUID.
Resource	The resource that is used to access Microsoft 365 Defender SIEM API events.
Client ID	Ensures that the user is authorized to obtain an access token.
Client Secret	The **Client Secret** value is displayed only one time, and then is no longer visible. If you don't have access to the **Client Secret** value, contact your Microsoft Azure administrator to request a new client secret.
Region	Select the regions that are associated with Microsoft 365 Defender SIEM API that you want to collect logs from.
Other Region	Type the names of any additional regions that are associated with the Microsoft 365 Defender SIEM API that you want to collect logs from. Use a comma-separated list; for example, `region1,region2`.

Table 68. Microsoft Defender for Endpoint SIEM REST API protocol (continued)	
Parameter	**Value**
Use GCC Endpoints	Enable or disable the use of **GCC** and **GCC High & DOD** endpoints. **GCC** and **GCC High & DOD** endpoints are endpoints for US Government customers. **Tip:** When this parameter is enabled, you cannot configure the **Regions** parameter. For more information, see Microsoft Defender for Endpoint for US Government customers (https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/gov?view=o365-worldwide).
GCC Type	Select **GCC** or **GCC High & DOD**. • **GCC**: Microsoft's Government Community Cloud • **GCC High & DoD**: Compliant with the regulations from Department of Defense.
Use Proxy	If a proxy for QRadar is configured, all traffic for the log source travels through the proxy so that QRadar can access the Microsoft 365 Defender SIEM API. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	You can specify how often the log collects data. The format is M/H/D for Minutes/Hours/Days. The default is 5 M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

If you need to create virtual machines (VMs) and test the connection between Microsoft Defender for Endpoint and QRadar, see Microsoft Defender for Endpoint evaluation lab (https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/evaluation-lab?view=o365-worldwide).

Related tasks

Adding a log source

Related information

Microsoft Defender for Endpoint documentation

Microsoft DHCP protocol configuration options

To receive events from Microsoft DHCP servers, configure a log source to use the Microsoft DHCP protocol.

The Microsoft DHCP protocol is an active outbound protocol.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft DHCP protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/` directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

Restriction: The Microsoft authentication protocol NTLMv2 is not supported by the Microsoft DHCP protocol.

The following table describes the protocol-specific parameters for the Microsoft DHCP protocol:

Table 69. Microsoft DHCP protocol parameters

Parameter	Description
Protocol Configuration	**Microsoft DHCP**
Log Source Identifier	Type a unique hostname or other identifier unique to the log source.
Server Address	The IP address or host name of your Microsoft DHCP server.
Domain	Type the domain for your Microsoft DHCP server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access the DHCP server.
Password	Type the password that is required to access the DHCP server.
Confirm Password	Type the password that is required to access the server.
Folder Path	The directory path to the DHCP log files. The default is `/WINDOWS/system32/dhcp/`
File Pattern	The regular expression (regex) that identifies event logs. The log files must contain a three-character abbreviation for a day of the week. Use one of the following file patterns: English: • IPv4 file pattern: `DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`. • IPv6 file pattern: `DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`. • Mixed IPv4 and IPv6 file pattern: `Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)\.log`. Polish: • IPv4 file pattern: `DhcpSrvLog-(?:Pią|Pon|Sob|Wto|Śro|Czw|Nie)\.log` • IPv6 file pattern: `DhcpV6SrvLog-(?:Pt|Pon|So|Wt|Śr|Czw|Nie)\.log`

Table 69. Microsoft DHCP protocol parameters (continued)	
Parameter	**Description**
Recursive	Select this option if you want the file pattern to search the sub folders.
SMB Version	Select the version of SMB that you want to use. **AUTO** Auto-detects to the highest version that the client and server agree to use. **SMB1** Forces the use of SMB1. SMB1 uses the `jCIFS.jar` (Java ARchive) file. **Important:** SMB1 is no longer supported. All administrators must update existing configurations to use SMB2 or SMB3. **SMB2** Forces the use of SMB2. SMB2 uses the `jNQ.jar` file. **SMB3** Forces the use of SMB3. SMB3 uses the `jNQ.jar` file. **Note:** Before you create a log source with a specific SMB version (for example: SMBv1, SMBv2, and SMBv3), ensure that the specified SMB version is supported by the Windows OS that is running on your server. You also need to verify that SMB versions is enabled on the specified Windows Server. For more information about which Windows version supports which SMB versions, go to the Microsoft TechNet website (https://blogs.technet.microsoft.com/josebda/2012/06/06/windows-server-2012-which-version-of-the-smb-protocol-smb-1-0-smb-2-0-smb-2-1-or-smb-3-0-are-you-using-on-your-file-server/). For more information about how to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server, go to the Microsoft support website (https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server).
Polling Interval (in seconds)	The number of seconds between queries to the log files to check for new data. The minimum polling interval is 10 seconds. The maximum polling interval is 3,600 seconds.
Throttle events/sec	The maximum number of events the DHCP protocol can forward per second. The minimum value is 100 EPS. The maximum value is 20,000 EPS.
File Encoding	The character encoding that is used by the events in your log file.

Table 69. Microsoft DHCP protocol parameters (continued)	
Parameter	**Description**
File Exclusion List	A list of regular expressions that prevent certain file directories from opening. The list includes one regular expression per line. When a file or directory matches one of the regular expressions, that file or directory does not open. When a file is in use, other applications might not be able to use it. Use this parameter to prevent locking those files or to prevent the protocol from accessing specific files. The pattern does not apply to the full Folder Path. It applies only to the final directory that is listed in the path. The pattern applies against all files or directories that are found within the Folder Path's directory. The following list is the default value for this parameter: `/j50.*\.log` `dhcp\.mdb` `dhcp\.tmp` `j50\.chk`.
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Specifies the QRadar Event Collector that polls the remote log source. Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector.
Coalescing Events	Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the **Log Activity** tab. When this check box is clear, events are viewed individually and events are not bundled. New and automatically discovered log sources inherit the value of this check box from the **System Settings** configuration on the **Admin** tab. You can use this check box to override the default behavior of the system settings for an individual log source.

Microsoft Exchange protocol configuration options

To receive events from SMTP, OWA, and message tracking events from Microsoft Windows Exchange 2007, 2010, 2013 and 2017 servers, configure a log source to use the Microsoft Exchange protocol.

The Microsoft Exchange protocol is an outbound/active protocol.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft Exchange protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/`directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

Important: The Microsoft Exchange protocol does not support Microsoft Exchange 2003 or Microsoft authentication protocol NTLMv2 Session.

The following table describes the protocol-specific parameters for the Microsoft Exchange protocol:

Table 70. Microsoft Exchange protocol parameters

Parameter	Description
Protocol Configuration	**Microsoft Exchange**
Log Source Identifier	Type the IP address, host name, or name to identify your log source.
Server Address	The IP address or host name of your Microsoft Exchange server.
Domain	Type the domain for your Microsoft Exchange server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access your Microsoft Exchange server.
Password	Type the password that is required to access your Microsoft Exchange server.
Confirm Password	Type the password that is required to access your Microsoft Exchange server.
SMTP Log Folder Path	The directory path to access the SMTP log files. The default file path is `Program Files/Microsoft/Exchange Server/ TransportRoles/Logs/ProtocolLog` When the folder path is clear, SMTP event collection is disabled.
OWA Log Folder Path	The directory path to access OWA log files. The default file path is `Windows/system32/LogFiles/W3SVC1` When the folder path is clear, OWA event collection is disabled.
MSGTRK Log Folder Path	The directory path to access message tracking logs. The default file path is `Program Files/Microsoft/Exchange Server/ TransportRoles/Logs/MessageTracking` Message tracking is available on Microsoft Exchange 2017 or 2010 servers that are assigned the Hub Transport, Mailbox, or Edge Transport server role.
Use Custom File Patterns	Select this check box to configure custom file patterns. Leave the check box clear to use the default file patterns.

Table 70. Microsoft Exchange protocol parameters (continued)	
Parameter	**Description**
MSGTRK File Pattern	The regular expression (regex) that is used to identify and download the MSTRK logs. All files that match the file pattern are processed. The default file pattern is `MSGTRK\d+-\d+\.(?:log|LOG)$` All files that match the file pattern are processed.
MSGTRKMD File Pattern	The regular expression (regex) that is used to identify and download the MSGTRKMD logs. All files that match the file pattern are processed. The default file pattern is `MSGTRKMD\d+-\d+\.(?:log|LOG)$` All files that match the file pattern are processed.
MSGTRKMS File Pattern	The regular expression (regex) that is used to identify and download the MSGTRKMS logs. All files that match the file pattern are processed. The default file pattern is `MSGTRKMS\d+-\d+\.(?:log|LOG)$` All files that match the file pattern are processed.
MSGTRKMA File Pattern	The regular expression (regex) that is used to identify and download the MSGTRKMA logs. All files that match the file pattern are processed. The default file pattern is `MSGTRKMA\d+-\d+\.(?:log|`
SMTP File Pattern	The regular expression (regex) that is used to identify and download the SMTP logs. All files that match the file pattern are processed. The default file pattern is `*\.(?:log|LOG)$` All files that match the file pattern are processed.
OWA File Pattern	The regular expression (regex) that is used to identify and download the OWA logs. All files that match the file pattern are processed. The default file pattern is `*\.(?:log|LOG)$` All files that match the file pattern are processed.
Force File Read	If the check box is cleared, the log file is read only when QRadar detects a change in the modified time or file size.
Recursive	If you want the file pattern to search sub folders, use this option. By default, the check box is selected.

Table 70. Microsoft Exchange protocol parameters (continued)	
Parameter	**Description**
SMB Version	Select the version of SMB that you want to use. **AUTO** Auto-detects to the highest version that the client and server agree to use. **SMB1** Forces the use of SMB1. SMB1 uses the `jCIFS.jar` (Java ARchive) file. **Important:** SMB1 is no longer supported. All administrators must update existing configurations to use SMB2 or SMB3. **SMB2** Forces the use of SMB2. SMB2 uses the `jNQ.jar` file. **SMB3** Forces the use of SMB3. SMB3 uses the `jNQ.jar` file. **Note:** Before you create a log source with a specific SMB version (for example: SMBv1, SMBv2, and SMBv3), ensure that the specified SMB version is supported by the Windows OS that is running on your server. You also need to verify that SMB versions is enabled on the specified Windows Server. For more information about which Windows version supports which SMB versions, go to the Microsoft TechNet website (https://blogs.technet.microsoft.com/josebda/2012/06/06/windows-server-2012-which-version-of-the-smb-protocol-smb-1-0-smb-2-0-smb-2-1-or-smb-3-0-are-you-using-on-your-file-server/). For more information about how to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server, go to the Microsoft support website (https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server).
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.
Throttle Events/Sec	The maximum number of events the Microsoft Exchange protocol can forward per second.
File Encoding	The character encoding that is used by the events in your log file.

Microsoft Graph Security API protocol configuration options

To receive events from the Microsoft Graph Security API, configure a log source in IBM QRadar to use the Microsoft Graph Security API protocol.

The Microsoft Graph Security API protocol is an outbound/active protocol. Your DSM might also use this protocol. For a list of supported DSMs, see QRadar supported DSMs.

The following parameters require specific values to collect events from Microsoft Graph Security servers:

Table 71. Microsoft Graph Security log source parameters	
Parameter	**Value**
Log Source type	A custom log source type or a specific DSM that uses this protocol.
Protocol Configuration	Microsoft Graph Security API
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Microsoft Graph Security log source, ensure that you give each one a unique name.
Tenant ID	The **Tenant ID** value that is used for Microsoft Azure Active Directory authentication.
Client ID	The **Client ID** parameter value from your application configuration of Microsoft Azure Active Directory.
Client Secret	You receive the **Client Secret** password when you configure Microsoft Azure Event Directory. This password confirms that your user account is authorized to obtain an access token. You can obtain this value only when it is created, and it cannot be recovered later. If you lose your client secret password, you must create a new API key to continue to receive events from the Microsoft Graph Security API.
API	The API dictates the types and formats of events that the protocol can collect. Select an API that is compatible with the selected DSM. If you use the Microsoft Azure Security Center DSM, select **Alerts V1**. If you use the Microsoft 365 Defender DSM, select **Alerts V2**.
Service	Limits the events to a specific service or product. Select a product that is compatible with the selected DSM. You can use the **Other** option to remove the filter or to add more filter settings. If you use the Microsoft 365 Defender DSM, select **Microsoft Defender for Endpoint**.
Event Filter	Retrieve events by using the Microsoft Security Graph API query filter. For example, `severity eq 'high'`. Do not type "`filter=`" before the filter parameter. For more information about writing queries, see Curated Sample Queries (https://github.com/microsoftgraph/security-api-solutions/tree/master/Queries).

Table 71. Microsoft Graph Security log source parameters (continued)	
Parameter	**Value**
Use Proxy	If QRadar accesses the Microsoft Graph Security API by proxy, enable this checkbox. If the proxy requires authentication, configure the **Proxy Hostname or IP**, **Proxy Port**, **Proxy Username**, and **Proxy** fields. If the proxy does not require authentication, configure the **Proxy Hostname or IP** and **Proxy Port** fields.
Proxy IP or Hostname	The IP address or hostname of the proxy server. If the **Use Proxy** parameter is set to **False**, this option is hidden.
Proxy Port	The port number that is used to communicate with the proxy. The default is 8080. If the **Use Proxy** parameter is set to False, this option is hidden.
Proxy Username	The username that is used to communicate with the proxy. If **Use Proxy** is set to **False**, this option is hidden.
Proxy Password	The password that is used to access the proxy. If **Use Proxy** is set to **False**, this option is hidden.
Recurrence	Type a time interval beginning at the **Start Time** to determine how frequently the poll scans for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H - 2 hours, 15M - 15 minutes. The default is 1M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Show Advanced Options	To configure the advanced options for event collection, enable this option.
Login Endpoint	Specify the Azure AD Login Endpoint. The default value is `login.microsoftonline.com`. If you disable **Show Advanced Options**, this option is hidden.

Table 71. Microsoft Graph Security log source parameters (continued)	
Parameter	**Value**
Graph API Endpoint	Specify the Microsoft Graph Security API URL. The default value is `https://graph.microsoft.com`. If you disable **Show Advanced Options**, this option is hidden.

Configuring Microsoft Graph Security API to communicate with QRadar

Integrate the Microsoft Graph Security API with IBM QRadar before you use the protocol.

Before you begin

To integrate the Microsoft Graph Security API with QRadar, you need Microsoft Azure Active Directory.

Procedure

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console.
   - Protocol Common RPM
   - Microsoft Graph Security API Protocol RPM
2. Configure your Microsoft Graph Security API server to forward events to QRadar by following these instructions:
   a) Create an Azure AD application. For more information, see Use the portal to create an Azure AD application and service principal that can access resources (https://docs.microsoft.com/en-us/azure/active-directory/develop/how to-create-service-principal-portal).
   b) Set up an authorization in security API client applications. For more information, see Authorization and the Microsoft Graph Security API (https://docs.microsoft.com/en-us/graph/security-authorization).

      When you use the Alerts V1 API, you must include the following app roles in the Access Token:

      - `SecurityEvents.Read.All`
      - `User.Read.All`
      - `SecurityActions.Read.All`
      - `IdentityRiskyUser.Read.All`
      - `IdentityRiskEvent.Read.All`

      Important:

      When you use the Alerts V2 API, you must include the `SecurityEvents.Read.All` app role. Other types of events can require different roles.

      You must designate the app roles with **Application** permissions. If your environment does not accept **Application** permissions, you can use **Delegated** permissions.
3. Add a Microsoft Security Graph API protocol log source on the QRadar Console by using a custom log source type or a specific DSM that uses this protocol.

   For more information about supported DSMs, see QRadar supported DSMs. For more information about adding a log source in QRadar, see Adding a log source.

Migrating Microsoft Defender for Endpoint REST API log sources to Microsoft Graph Security API log sources

Microsoft deprecated the legacy SIEM API. To continue to receive data from Microsoft Defender for Endpoint in IBM QRadar, you must register a new application and create a Microsoft Graph Security API log source to collect the data.

For more information about the SIEM API deprecation, see Deprecating the legacy SIEM API (https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/deprecating-the-legacy-siem-api/ba-p/3139643).

Procedure

1. Register a new application.

   When you migrate to the Microsoft Graph Security API, the application permissions change; you must register a new application to ensure that the permissions are correct.

   a) Create an application that can be used to authenticate with the Microsoft Graph Security API.

      For more information, see Use the portal to create an Azure AD application and service principal that can access resources (https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal).

   b) Set the `SecurityAlert.Read.All` application permission.

   c) On the **Overview** page, you can find the **Client ID** and **Tenant ID**. Copy this information for when you create a log source.

   d) On the **Certificates and Secrets** page, click **New Secret** to create the client secret for the log source. Copy this information for when you create a log source.

2. Create a Microsoft 365 Defender log source that uses the Microsoft Graph Security API protocol.

   When you migrate to the Microsoft Graph Security API, you create a new log source to pull events from the new configuration. For more information, see Adding a log source.

   The following table describes the parameters that require specific values to collect Microsoft Graph Security API events from Microsoft 365 Defender.

Table 72. Microsoft Graph Security API log source parameters for the Microsoft 365 Defender DSM

Parameter	Value
Log Source type	Microsoft 365 Defender DSM
Protocol Configuration	Microsoft Graph Security API
Tenant ID	Enter the value that you obtained in step 3.
Client ID	Enter the value that you obtained in step 3.
Client Secret	Enter the value that you obtained in step 4.
API	**Alerts V2**
Service	**Microsoft Defender for Endpoint**
Show Advanced Options	Enable this parameter to configure the **Login Endpoint** and **Graph API Endpoint** parameters. **Important:** If your deployment is in a Government Community Cloud (GCC) environment, the **Login Endpoint** and **Graph API Endpoint** have specific values. For more information about these values, see National cloud deployments (https://docs.microsoft.com/en-us/graph/deployments).

Table 72. Microsoft Graph Security API log source parameters for the Microsoft 365 Defender DSM (continued)	
Parameter	**Value**
Login Endpoint	`login.microsoftonline.com`
Graph API Endpoint	`https://graph.microsoft.com`

For more information about the Microsoft Graph Security API protocol parameters, see "Microsoft Graph Security API protocol configuration options" on page 182.

Microsoft IIS protocol configuration options

You can configure a log source to use the Microsoft IIS protocol. This protocol supports a single point of collection for W3C format log files that are located on a Microsoft IIS web server.

The Microsoft IIS protocol is an outbound/active protocol.

To read the log files, folder paths that contain an administrative share (C$), require NetBIOS privileges on the administrative share (C$). Local or domain administrators have sufficient privileges to access log files on administrative shares.

Fields for the Microsoft IIS protocol that support file paths allow administrators to define a drive letter with the path information. For example, the field can contain the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/`directory for a public share folder path, but cannot contain the `c:/LogFiles` directory.

Restriction: The Microsoft authentication protocol NTLMv2 is not supported by the Microsoft IIS protocol.

The following table describes the protocol-specific parameters for the Microsoft IIS protocol:

Table 73. Microsoft IIS protocol parameters	
Parameter	**Description**
Protocol Configuration	**Microsoft IIS**
Log Source Identifier	Type the IP address, host name, or a unique name to identify your log source.
Server Address	The IP address or host name of your Microsoft IIS server.
Domain	Type the domain for your Microsoft IIS server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access your server.
Password	Type the password that is required to access your server.
Confirm Password	Type the password that is required to access the server.
Log Folder Path	The directory path to access the log files. For example, administrators can use the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/` directory for a public share folder path. However, the `c:/LogFiles` directory is not a supported log folder path. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the privileges that are required to read the log files. Local system or domain administrator privileges are also sufficient to access a log files that are on an administrative share.

Table 73. Microsoft IIS protocol parameters (continued)	
Parameter	**Description**
File Pattern	The regular expression (regex) that identifies the event logs.
Recursive	If you want the file pattern to search sub folders, use this option. By default, the check box is selected.
SMB Version	Select the version of SMB that you want to use. **AUTO** Auto-detects to the highest version that the client and server agree to use. **SMB1** Forces the use of SMB1. SMB1 uses the `jCIFS.jar` (Java ARchive) file. **Important:** SMB1 is no longer supported. All administrators must update existing configurations to use SMB2 or SMB3. **SMB2** Forces the use of SMB2. SMB2 uses the `jNQ.jar` file. **SMB3** Forces the use of SMB3. SMB3 uses the `jNQ.jar` file. **Note:** Before you create a log source with a specific SMB version (for example: SMBv1, SMBv2, and SMBv3), ensure that the specified SMB version is supported by the Windows OS that is running on your server. You also need to verify that SMB versions is enabled on the specified Windows Server. For more information about which Windows version supports which SMB versions, go to the Microsoft TechNet website (https://blogs.technet.microsoft.com/josebda/2012/06/06/windows-server-2012-which-version-of-the-smb-protocol-smb-1-0-smb-2-0-smb-2-1-or-smb-3-0-are-you-using-on-your-file-server/). For more information about how to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server, go to the Microsoft support website (https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server).
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.
Throttle Events/Sec	The maximum number of events the IIS protocol can forward per second.
File Encoding	The character encoding that is used by the events in your log file.

Note: If you use Advanced IIS Logging, you need to create a new log definition. In the **Log Definition** window, ensure that the following fields are selected in the **Selected Fields** section:

- Date-UTC
- Time-UTC
- URI-Stem
- URI-Querystring

- ContentPath
- Status
- Server Name
- Referer
- Win325Status
- Bytes Sent

Microsoft Security Event Log protocol configuration options

Support for the Windows Event Log protocols ended on 31 October 2022.

Important: Support for the Windows Event Log protocols ended on 31 October 2022. To continue collecting Windows Event Log events, you must select a new protocol type from the Microsoft Windows Security Event Log page. For more information, see QRadar: End of life announcement for WMI-based Microsoft Windows Security Event Log protocols (31 Oct 2022) (https://www.ibm.com/support/pages/node/6616223).

Microsoft Security Event Log over MSRPC Protocol

The Microsoft Security Event Log over MSRPC protocol (MSRPC) is an active outbound protocol that collects Windows events without an agent installed on the Windows host.

The MSRPC protocol uses the Microsoft Distributed Computing Environment/Remote Procedure Call (DCE/RPC) specification to provide agentless, encrypted event collection.

The following table lists the supported features of the MSRPC protocol.

Table 74. Supported features of the MSRPC protocol

Features	**Microsoft Security Event Log over MSRPC protocol**
Manufacturer	Microsoft
Connection test tool	The MSRPC test tool checks the connectivity between the QRadar appliance and a Windows host. The MSRPC test tool is part of the MSRPC protocol RPM and can be found in `/opt/qradar/jars` after you install the protocol. For more information, see MSRPC test tool (http://www.ibm.com/support/docview.wss?uid=swg21959348)

Table 74. Supported features of the MSRPC protocol (continued)

Features	**Microsoft Security Event Log over MSRPC protocol**
Protocol type	The remote procedure protocol type for collecting events. The protocol type depends on your operating system. Select one of the following options from the **Protocol Type** list: **MS-EVEN6** The default protocol type for new log sources. The protocol type that is used by QRadar to communicate with Windows Vista and Windows Server 2012 and later. **Important:** The **MS-EVEN (for Windows XP/2003)** option is no longer supported. However, it still appears in the **Protocol Type** list. **auto-detect (for legacy configurations)** Previous log source configurations for the Microsoft Windows Security Event Log DSM use the **auto-detect (for legacy configurations)** protocol type. Upgrade to the **MS_EVEN6** protocol type.
Maximum EPS rate	100 EPS / Windows host
Maximum overall EPS rate of MSRPC	8500 EPS / IBM QRadar 16xx or 18xx appliance
Maximum number of supported log sources	500 log sources / QRadar 16xx or 18xx appliance
Bulk log source support	Yes
Encryption	Yes
Supported event types	Application System Security DNS Server File Replication Directory Service logs
Supported Windows Operating Systems	Windows Server 2022 (including Core) WinCollect v10.1.2 and above Windows Server 2019 (including Core) Windows Server 2016 (including Core) Windows Server 2012 (including Core) Windows 10 Windows 11 WinCollect v10.1.2 and above

Table 74. Supported features of the MSRPC protocol (continued)	
Features	**Microsoft Security Event Log over MSRPC protocol**
Required permissions	The log source user must be a member of the Event Log Readers group. If this group is not configured, then domain admin privileges are usually required to poll a Windows event log across a domain. In some cases, the backup operators group can be used depending on how Microsoft Group Policy Objects are configured. • `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eventlog` • `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language` • `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft Windows\CurrentVersion`
Required RPM files	`PROTOCOL-WindowsEventRPC-`*`QRadar_release-Build_number`*`.noarch.rpm` `DSM-MicrosoftWindows-`*`QRadar_release-Build_number`*`.noarch.rpm` `DSM-DSMCommon-`*`QRadar_release-Build_number`*`.noarch.rpm`
Windows service requirements	• Remote Procedure Call (RPC) • RPC Endpoint Mapper
Windows port requirements	• TCP port 135 • TCP port 445 • TCP port that is dynamically allocated for RPC, from port 49152 up to 65535
Special features	Supports encrypted events by default.
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	A security content pack with Windows custom event properties is available on IBM Fix Central.
Intended application	Agentless event collection for Windows operating systems that can support 100 EPS per log source.
Tuning support	MSRPC is limited to 100 EPS / Windows host. For higher event rate systems, see the *IBM QRadar WinCollect User Guide*.
Event filtering support	MSRPC does not support event filtering. See the *IBM QRadar WinCollect User Guide* for this feature.
More information	Microsoft support (http://support.microsoft.com/)

MQ protocol configuration options

To receive messages from a message queue (MQ) service, configure a log source to use the MQ protocol. The protocol name displays in IBM QRadar as **MQ JMS**.

IBM MQ is supported.

The MQ protocol is an outbound/active protocol that can monitor multiple message queues, up to a maximum of 50 per log source.

The following table describes the protocol-specific parameters for the MQ protocol:

Table 75. MQ protocol parameters

Parameter	Description
Protocol Name	**MQ JMS**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured MQ log source, ensure that you give each one a unique name.
IP or Hostname	The IP address or host name of the primary queue manager.
Port	The default port that is used for communicating with the primary queue manager is 1414.
Standby IP or Hostname	The IP address or host name of the standby queue manager.
Standby Port	The port that is used to communicate with the standby queue manager.
Queue Manager	The name of the queue manager.
Channel	The channel through which the queue manager sends messages. The default channel is `SYSTEM.DEF.SVRCONN`.
Queue	The queue or list of queues to monitor. A list of queues is specified with a comma-separated list.
Username	The user name that is used for authenticating with the MQ service.
Password	Optional: The password that is used to authenticate with the MQ service.
Incoming Message Encoding	The character encoding that is used by incoming messages.
Process Computational Fields	Optional: Select this option only if the retrieved messages contain computational data that is defined in a COBOL copybook. The binary data in the messages is processed according to the field definition found in the specified copybook file.
CopyBook File Name	This parameter displays when **Process Computational Fields** is selected. The name of the copybook file to use for processing data. The CopyBook file must be placed in `/store/ec/mqjms/*`.
Event Formatter	Select the event formatting to be applied for any events that are generated from processing data containing computational fields. By default, **No Formatting** is used.

Table 75. MQ protocol parameters (continued)	
Parameter	**Description**
Include JMS Message Header	Select this option to include a header in each generated event containing JMS message fields such as the JMSMessageID and JMSTimestamp.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.

Related concepts

Creating a log source extensions document to get data into QRadar

Office 365 Message Trace REST API protocol configuration options

The Office 365 Message Trace REST API protocol for IBM Security QRadar collects message trace logs from the Message Trace REST API. This active outbound protocol is used to collect Office 365 email logs.

Important: As of 1 January 2023, Microsoft will no longer support basic authentication. To continue receiving Message Trace events, you must use modern authentication. Modern authentication uses OAuth 2.0 to authenticate and authorize access to the events. For more information about the deprecation of basic authentication, see Basic Authentication Deprecation in Exchange Online – September 2022 Update.

To use modern authentication, you must register a new application in the Microsoft Azure portal (https://portal.azure.com/). In the portal, you can obtain important values that you must use when you create a Microsoft Office 365 Message Trace log source.

1. Create an application that can be used to authenticate with the Office 365 Message Trace REST API. For more information, see Use the portal to create an Azure AD application and service principal that can access resources.
   a. Assign **Azure AD** roles to the application. For more information, see Assign Azure AD roles to the application.
   b. Set the **ReportingWebService.Read.All** application permission. For more information, see Specify the permissions your app requires to access the Reporting Web Service.
2. Obtain the **Client ID**, **Tenant ID**, and **Client Secret** values.
   a. On the **Overview** page of the application, locate and copy the **Client ID** and **Tenant ID** values. You use these values when you create a Microsoft Office 365 Message Trace log source. For more information, see Get tenant and app ID values for signing in.
   b. On the **Certificates and Secrets** page of the application, click **New Secret** to create the client secret, and then copy the client secret to a text editor. You use this value for the **Client Secret** parameter when you create a Microsoft Office 365 Message Trace log source. For more information, see Create a new application secret.

The following parameters require specific values to collect events from the Office 365 Message Trace REST API:

Important: If the **start date** and **end date** in an audit log run are overlapping, then there is duplication of events in the reports with different indexes. In such cases, you must manually handle the events in the reports.

Table 76. Office 365 Message Trace REST API protocol log source parameters	
Parameter	**Value**
Log Source Identifier	A unique name for the log source. The name can't include spaces and must be unique among all log sources of this type that are configured with the Office 365 Message Trace REST API protocol.
Authentication Method	Modern authentication uses OAuth 2.0 to authenticate and authorize access to the resource. Basic authentication uses the username and password. If you select the **Basic** authentication method, the **Office 365 User Account email** and **Office 365 User Account Password** parameters appear. Provide an Office 365 email account with proper permissions. **Important:** As of 1 January 2023, Microsoft will no longer support basic authentication. To continue receiving Message Trace events, you must use **Modern** authentication.
Client ID	The **Client ID** value from your application configuration of Microsoft Azure Active Directory. For more information, see Get tenant and app ID values for signing in.
Client Secret	The client secret that you created for your application on the Microsoft Azure portal. For more information, see Create a new application secret.
Tenant ID	The **Tenant ID** value that is used for Microsoft Azure Active Directory authentication. For more information, see Get tenant and app ID values for signing in.
Event Delay	The delay, in seconds, for collecting data. Office 365 Message Trace logs work on an eventual delivery system. To ensure that no data is missed, logs are collected on a delay. The default delay is 900 seconds (15 minutes), and can be set as low as 0 seconds.
Use Proxy	If the API is accessed by using a proxy, select this checkbox. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.

Table 76. Office 365 Message Trace REST API protocol log source parameters (continued)	
Parameter	**Value**
Enable Advanced Options	Select this option to modify the default values for the **Microsoft API Login Endpoint** and **Office 365 Message Trace API Management URL** parameters. If you do not enable this parameter, the default values are used.
Microsoft API Login Endpoint	Specify the Microsoft API login endpoint. The default value is `https://login.windows.net`. If you do not enable the **Enable Advanced Options** parameter, the default value is used.
Office 365 Message Trace API Management URL	The Office 365 Message Trace API management URL grants your token access to the specified resource. The default value is `https://outlook.office365.com`. If you do not enable the **Enable Advanced Options** parameter, the default value is used.
Recurrence	The time interval between log source queries to the Office 365 Message Trace REST API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 5 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Conditional access for reading reports

If you receive the error message "`Status Code: 401 | Status Reason: Unauthorized`," review the following Conditional Access policies documentation to confirm that the user account has access to the legacy application Office 365 Message Trace API:

- For more information about blocking and unblocking legacy content in Conditional Access policies, see Conditional Access: Block legacy authentication.
- For more information about creating Conditional Access policies for users and groups, see Conditional Access: Users and groups.
- For more information about creating Conditional Access policies for Cloud apps or actions, see Conditional Access: Cloud apps or actions.
- For more information about granting or blocking access to resources with a Conditional Access policy, see Conditional Access: Grant.

Related information

Adding a log source

“HTTP Status code 401” on page 196

Office 365 Management Activity API reference

Troubleshooting the Office 365 Message Trace REST API protocol

To resolve issues with the Office 365 Message Trace REST API protocol, use the troubleshooting and support information. Find the errors by using the protocol testing tools in the QRadar Log Source Management app.

General troubleshooting

The following steps apply to all user input errors. The general troubleshooting procedure contains the first steps to follow any errors with the Office 365 Message Trace REST API protocol.

1. If you use QRadar 7.3.2, software update 3 or later, run the testing tool before you enable the log source. If the testing tool doesn't pass all tests, the log source fails when enabled. If a test fails, an error message with more information displays.
2. Verify that the selected Event Collector can access the `reports.office365.com` host. This protocol connects by using HTTPS (port 443).
3. Verify that the Office 365 email account username and password are valid.
4. Ensure that the Office 365 email account has the correct permissions. For more information, see Office 365 Message Trace protocol FAQ.
5. Ensure that your access is not blocked to the Reporting Web Services legacy authentication protocol. For more information, see HTTP Status code 401.
6. Reenter all fields.
7. If available, rerun the testing tool.

For more information, see:

- HTTP Status code 401
- HTTP Status code 404
- Office 365 Message Trace protocol FAQ

HTTP Status code 401

Symptoms

Error: "Status Code: 401 | Status Reason: Unauthorized"

Error: "Invalid Office 365 User Account E-mail or Password"

Error: *<A response received from the Office 365 Message Trace REST API displays>*

Causes

QRadar connected to the Office 365 Message Trace protocol, but because of invalid user credentials, it could not authenticate.

Resolving the problem

To resolve your HTTP Status code 401 error, verify that the following conditions are met.

1. Verify that your Office 365 email account username and the account password are valid.
2. Check if your Microsoft security settings are blocking access to the Office 365 Message Trace REST API.

   To use the Office 365 Message Trace REST API, you need access to the Reporting Web Services legacy authentication protocol.

   For more information about blocking and unblocking legacy authentications, see How to: Block legacy authentication to Azure AD with Conditional Access (https://docs.microsoft.com/en-us/azure/active-

directory/conditional-access/block-legacy-authentication#indirectly-blocking-legacy-authentication). If you need assistance with configuring Azure AD with Conditional Access, contact Microsoft Support.

For more information about creating Conditional Access policies for users and groups, see Conditional Access: Users and groups (https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups).

For more information about creating Conditional Access policies for Cloud apps or actions, see Conditional Access: Cloud apps or actions (https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps).

For more information about granting or blocking access to resources with a Conditional Access policy, see Conditional Access: Grant (https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant).

HTTP Status code 404

Symptoms

Error: “Status Code : 404 | Status Reason: Not Found"

Error: "Occasionally 404 responses are related to the user account permissions not granting access to the Message Trace API”

Error: *<A response received from the Office 365 Message Trace REST API displays>*

Causes

404 responses are usually due to the server not being found. However, the Office 365 Message Trace REST API can return this response when the **User Account** that was provided does not have proper permissions. Most instances of this exception occur because the **User Account** does not have the necessary permissions.

Resolving the problem

To resolve your HTTP Status code 404 error, ensure that the user accounts have the necessary permissions. For more information, see Office 365 Message Trace REST API protocol FAQ.

Office 365 Message Trace REST API protocol FAQ

Got a question? Check these frequently asked questions and answers to help you understand the Office 365 Message Trace REST API protocol.

- “What permissions are required to collect logs from the Office 365 Message Trace REST API?” on page 197
- “What information is contained in the events that are collected by a Microsoft Office 365 Message Trace REST API protocol?” on page 198
- “What is the event delay option used for?” on page 198
- “How does the event delay option work?” on page 198
- “What value do I use for the event delay option?” on page 199

What permissions are required to collect logs from the Office 365 Message Trace REST API?

Use the same administrative permissions that you use to access the reports in the Office 365 organization. For more information, see Permissions. (https://docs.microsoft.com/en-us/previous-versions/office/developer/o365-enterprise-developers/jj984335(v=office.15)#permissions).

What information is contained in the events that are collected by a Microsoft Office 365 Message Trace REST API protocol?

This protocol returns the same information that is provided in the message trace in the Security and Compliance Center. For more information, see the Message trace in the Security & Compliance Center (https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/message-trace-scc?view=o365-worldwide).

Note: Extended and enhanced reports are not available when you use the Office 365 Message Trace REST API.

For a specific reference to the API that contains a list of MessageTrace report fields, see Fields (https://docs.microsoft.com/en-us/previous-versions/office/developer/o365-enterprise-developers/jj984335(v=office.15)#fields).

What is the event delay option used for?

The event delay option is used to prevent events from being missed. Missed events, in this context, occur because they become available after the protocol updated its query range to a newer time frame than the event's arrival time. If an event occurred but wasn't posted to the Office 365 Message Trace REST API, then when the protocol queries for that event's creation time, the protocol doesn't get that event.

Example 1: The following example shows how an event can be lost.

The protocol queries the Office 365 Message Trace API at 2:00 PM to collect events between 1:00 PM – 1:59 PM. The Office 365 Message Trace API response returns the events that are available in the Office 365 Message Trace API between 1:00 PM - 1:59 PM. The protocol operates as if all of the events are collected and then sends the next query to the Office 365 Message Trace API at 3:00 PM to get events that occurred between 1:45 PM – 2:59 PM. The problem with this scenario is that the Office 365 Message Trace API might not include all of the events that occurred between 1:00 PM – 1:59 PM. If an event occurred at 1:58 PM, that event might not be available in the Office 365 Message Trace API until 2:03 PM. However, the protocol has already queried the 1:00 PM – 1:59 PM time range, and can't re-query that range without getting duplicated events. This delay can vary between 1 minute to 24 hours.

Example 2: The following example shows **Example 1**, except in this scenario a 15-minute delay is added.

This example uses a 15-minute delay when the protocol makes query calls. When the protocol makes a query call to the Office 365 Message Trace API at 2:00 PM, it collects the events that occurred between 1:00 - 1:45 PM. The protocol operates as if all of the events are collected, sends the next query to the Office 365 Message Trace API at 3:00 PM and collects all events that occurred between 1:45 PM – 2:45 PM. Instead of the event being missed, as in **Example 1**, it gets picked up in the next query call between 1:45 PM - 2:45 PM.

Example 3: The following example shows **Example 2**, except in this scenario the events are available a day later.

If the event occurred at 1:58 PM, but only became available to the Office 365 Message Trace API at 1:57 PM the next day, then the event delay that is described in **Example 2** no longer gets that event. Instead, the event delay must be set to a higher value, in this case 24 hours.

How does the event delay option work?

Instead of querying from the **last received event time** to **current time**, the protocol queries from the **last received event time** to **current time** - <*event delay*>. The event delay is in seconds. For example, a delay of 15 minutes (900 seconds) means that it queries only up to 15 minutes ago. This query gives the Office 365 Message Trace API 15 minutes to make an event available before the event is lost. When the **current time** - <*event delay*> is less than the **last received event time**, the protocol doesn't query the Office 365 Message Trace API; it waits for the condition to pass before querying.

What value do I use for the event delay option?

The Office 365 Message Trace API can delay the event's availability for up to 24 hours. To prevent any events from being missed, the **Event Delay** parameter option value can be set to 24 hours. However, the larger the event delay, the less real time the results are. With a 24-hour event delay, you see events only 24 hours after they occur. The value depends on how much risk you're willing to take and how important real-time data is. This default delay of 15 minutes provides a value that is set in real time and also prevents most events from being missed. For more information about the delay, see Data granularity, persistence, and availability (https://docs.microsoft.com/en-us/previous-versions/office/developer/o365-enterprise-developers/jj984335(v=office.15)#data-granularity-persistence-and-availability).

(Back to top)

Office 365 REST API protocol configuration options

The Office 365 REST API protocol for IBM Security QRadar is an active outbound protocol.

The following table describes the protocol-specific parameters for the Office 365 REST API protocol:

Table 77. Office 365 REST API protocol log source parameters

Parameter	Value
Protocol Configuration	**Office 365 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Office 365 REST API log source, ensure that you give each one a unique name.
Client ID	In your application configuration of Azure Active Directory, this parameter is under **Client ID**.
Client Secret	In your application configuration of Azure Active Directory, this parameter is under **Value**.
Tenant ID	Used for Azure AD authentication.
Event Filter	The type of audit events to retrieve from Microsoft Office. • Azure Active Directory • Exchange • SharePoint • General • DLP
Use Proxy	For QRadar to access the Office 365 Management APIs, all traffic for the log source travels through configured proxies. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, keep the **Proxy Username** and **Proxy Password** fields empty.

Table 77. Office 365 REST API protocol log source parameters (continued)	
Parameter	**Value**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Show Advanced Options	Show optional advanced options for event collection. The **Advanced Options** values are in effect whether they are shown or not.
Management Activity API URL	Specify the Office 365 Management Activity API URL. Default is https://manage.office.com.
Azure AD Sign-in URL	Specify the Azure AD sign-in URL. Default is https://login.microsoftonline.com.

Okta REST API protocol configuration options

To receive events from Okta, configure a log source in IBM QRadar by using the Okta REST API protocol.

The Okta REST API protocol is an outbound/active protocol that queries Okta events and users API endpoints to retrieve information about actions that are completed by users in an organization.

The following table describes the protocol-specific parameters for the Okta REST API protocol:

Table 78. Okta REST API protocol parameters	
Parameter	**Description**
Log Source Identifier	A unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the log source **Name**. If you have more than one Okta log source that is configured, you might want to identify the first log source as `okta1`, the second log source as `okta2`, and the third log source as `okta3`.
`IP or Hostname`	oktaprise.okta.com
`Authentication Token`	A single authentication token that is generated by the Okta console and must be used for all API transactions.
`Use Proxy`	If QRadar accesses Okta by using a proxy, enable this option. When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access Okta. If the proxy requires authentication, configure the **Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Hostname	If you select **Use Proxy**, this parameter is displayed.

Table 78. Okta REST API protocol parameters (continued)	
Parameter	**Description**
Proxy Port	If you select **Use Proxy**, this parameter is displayed.
Proxy Username	If you select **Use Proxy**, this parameter is displayed.
Proxy Password	If you select **Use Proxy**, this parameter is displayed.
Recurrence	A time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds. The default is 1M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

OPSEC/LEA protocol configuration options

To receive events on port 18184, configure a log source to use the OPSEC/LEA protocol.

The OPSEC/LEA protocol is an outbound/active protocol.

The following table describes the protocol-specific parameters for the OPSEC/LEA protocol:

Table 79. OPSEC/LEA protocol parameters	
Parameter	**Description**
Protocol Configuration	**OPSEC/LEA**
Log Source Identifier	The IP address, host name, or any name to identify the device. Must be unique for the log source type.
Server IP	Type the IP address of the server.
Server Port	The port number that is used for OPSEC communication. The valid range is 0 - 65,536 and the default is 18184.
Use Server IP for Log Source	Select the **Use Server IP for Log Source** check box if you want to use the LEA server IP address instead of the managed device IP address for a log source. By default, the check box is selected.
Statistics Report Interval	The interval, in seconds, during which the number of syslog events are recorded in the `qradar.log` file. The valid range is 4 - 2,147,483,648 and the default interval is 600.
Authentication Type	From the list, select the **Authentication Type** that you want to use for this LEA configuration. The options are `sslca` (default), `sslca_clear`, or `clear`. This value must match the authentication method that is used by the server.
OPSEC Application Object SIC Attribute (SIC Name)	The Secure Internal Communications (SIC) name is the distinguished name (DN) of the application; for example: `CN=LEA, o=fwconsole..7psasx`.

Table 79. OPSEC/LEA protocol parameters (continued)	
Parameter	**Description**
Log Source SIC Attribute (Entity SIC Name)	The SIC name of the server, for example: `cn=cp_mgmt,o=fwconsole..7psasx`.
Specify Certificate	Select this check box if you want to define a certificate for this LEA configuration. QRadar attempts to retrieve the certificate by using these parameters when the certificate is needed.
Certificate Filename	This option appears only if **Specify Certificate** is selected. Type the file name of the certificate that you want to use for this configuration. The certificate file must be located in the `/opt/qradar/conf/trusted_certificates/lea` directory.
Certificate Authority IP	Type the Check Point Manager Server IP address.
Pull Certificate Password	Type the activation key password.
OPSEC Application	The name of the application that makes the certificate request.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select the **Coalescing Events** check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select the **Store Event Payload** check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Important: If you receive the error message **Unable to pull SSL certificate** after an upgrade, follow these steps:

1. Clear the **Specify Certificate** check box.
2. Reenter the password for **Pull Certificate Password**.

Oracle Database Listener protocol configuration options

To remotely collect log files that are generated from an Oracle database server, configure a log source to use the Oracle Database Listener protocol source.

The Oracle Database Listener protocol is an outbound/active protocol.

Before you configure the Oracle Database Listener protocol to monitor log files for processing, you must obtain the directory path to the Oracle database log files.

The following table describes the protocol-specific parameters for the Oracle Database Listener protocol:

Table 80. Oracle Database Listener protocol parameters

Parameter	Description
Protocol Configuration	**Oracle Database Listener**
Log Source Identifier	Type the IP address, host name, or a unique name to identify your log source.
Server Address	The IP address or host name of your Oracle Database Listener server.
Domain	Type the domain for your Oracle Database Learner server. This parameter is optional if your server is not in a domain.
Username	Type the user name that is required to access your server.
Password	Type the password that is required to access your server.
Confirm Password	Type the password that is required to access the server.
Log Folder Path	Type the directory path to access the Oracle Database Listener log files.
File Pattern	The regular expression (regex) that identifies the event logs.
Force File Read	Select this check box to force the protocol to read the log file when the timing of the polling interval specifies. When the check box is selected, the log file source is always examined when the polling interval specifies, regardless of the last modified time or file size attribute. When the check box is not selected, the log file source is examined at the polling interval if the last modified time or file size attributes changed.
Recursive	If you want the file pattern to search sub folders, use this option. By default, the check box is selected.

Table 80. Oracle Database Listener protocol parameters (continued)	
Parameter	**Description**
SMB Version	Select the version of SMB that you want to use. **AUTO** Auto-detects to the highest version that the client and server agree to use. **SMB1** Forces the use of SMB1. SMB1 uses the `jCIFS.jar` (Java ARchive) file. **Important:** SMB1 is no longer supported. All administrators must update existing configurations to use SMB2 or SMB3. **SMB2** Forces the use of SMB2. SMB2 uses the `jNQ.jar` file. **SMB3** Forces the use of SMB3. SMB3 uses the `jNQ.jar` file. **Note:** Before you create a log source with a specific SMB version (for example: SMBv1, SMBv2, and SMBv3), ensure that the specified SMB version is supported by the Windows OS that is running on your server. You also need to verify that SMB versions is enabled on the specified Windows Server. For more information about which Windows version supports which SMB versions, go to the Microsoft TechNet website (https://blogs.technet.microsoft.com/josebda/2012/06/06/windows-server-2012-which-version-of-the-smb-protocol-smb-1-0-smb-2-0-smb-2-1-or-smb-3-0-are-you-using-on-your-file-server/). For more information about how to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server, go to the Microsoft support website (https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server).
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.
Throttle events/sec	The maximum number of events the Oracle Database Listener protocol forwards per second.
File Encoding	The character encoding that is used by the events in your log file.

PCAP Syslog Combination protocol configuration options

To collect events from Juniper SRX Series Services Gateway or Juniper Junos OS Platform that forward packet capture (PCAP) data, configure a log source to use the PCAP Syslog Combination protocol.

The PCAP Syslog Combination protocol is an inbound/passive protocol.

Before you configure a log source that uses the PCAP Syslog Combination protocol, determine the outgoing PCAP port that is configured on the Juniper SRX Series Services Gateway or Juniper Junos OS Platform. PCAP data cannot be forwarded to port 514.

Note:

QRadar supports receiving PCAP data only from Juniper SRX Series Services Gateway or Juniper Junos OS Platform for each event collector.

The following table describes the protocol-specific parameters for the PCAP Syslog Combination protocol:

Table 81. PCAP Syslog Combination protocol parameters

Parameter	Description
Log Source Name	Type a unique name of the log source.
Log Source Description	Optional. Type a description for the log source.
Log Source Type	From the list, you can select either **Juniper SRX Series Services Gateway** or **Juniper Junos OS Platform**.
Protocol Configuration	From the list, select **PCAP Syslog Combination**.
Log Source Identifier	Type an IP address, host name, or name to identify the **Juniper SRX Series Services Gateway** or **Juniper Junos OS Platform** appliance. The log source identifier must be unique for the log source type.
Incoming PCAP Port	If the outgoing PCAP port is edited on the **Juniper SRX Series Services Gateway** or **Juniper Junos OS Platform** appliance, you must edit the log source to update the incoming PCAP Port. To edit the Incoming PCAP Port number, complete the following steps: 1. Type the new port number for receiving PCAP data 2. Click **Save**. The port update is complete and event collection starts on the new port number.
Enabled	Select this check box to enable the log source. When this check box is clear, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Select the credibility of the log source. The range is 0 (lowest) - 10 (highest). The default credibility is 5. Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events or adjusted as a response to user created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Select the target for the log source. When a log source actively collects events from a remote source, this field defines which appliance polls for the events. This option enables administrators to poll and process events on the target event collector, instead of the Console appliance. This can improve performance in distributed deployments.

Table 81. PCAP Syslog Combination protocol parameters (continued)	
Parameter	**Description**
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Coalescing events increase the event count when the same event occurs multiple times within a short time interval. Coalesced events provide administrators a way to view and determine the frequency with which a single event type occurs on the **Log Activity** tab. When this check box is clear, the events are displayed individually and the information is not bundled. New and automatically discovered log sources inherit the value of this check box from the **System Settings** configuration on the **Admin** tab. Administrators can use this check box to override the default behavior of the system settings for an individual log source.
Store Event Payload	Select this check box to enable the log source to store the payload information from an event. New and automatically discovered log sources inherit the value of this check box from the **System Settings** configuration on the **Admin** tab. Administrators can use this check box to override the default behavior of the system settings for an individual log source.
Log Source Extension	Optional. Select the name of the extension to apply to the log source. This parameter is available after a log source extension is uploaded. Log source extensions are XML files that contain regular expressions, which can override or repair the event parsing patterns that are defined by a device support module (DSM).
Extension Use Condition	From the list box, select the use condition for the log source extension. The options include: • **Parsing enhancement** - Select this option when most fields parse correctly for your log source. • **Parsing override** - Select this option when the log source is unable to correctly parse events.
Groups	Select one or more groups for the log source.

RabbitMQ protocol configuration options

To receive messages from a Cisco AMP DSM, configure a log source to use the RabbitMQ protocol.

The RabbitMQ protocol is an active outbound protocol.

Important: The Cisco AMP integration does not support private cloud if the Server Name Indication (SNI) is required. Contact Cisco for more details.

The following table describes the protocol-specific parameters for the RabbitMQ protocol:

Table 82. RabbitMQ protocol parameters	
Parameter	**Description**
Protocol Name	**RabbitMQ**

Table 82. RabbitMQ protocol parameters (continued)	
Parameter	**Description**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured RabbitMQ log source, ensure that you give each one a unique name.
Event Format	The Event Format tells the protocol what type of events to expect. Officially supported products have specific options available for them. For unsupported products, you can use **No Formatting** or **JSON**.
IP or Hostname	The IP address or hostname of the primary queue manager.
Port	The port that is provided by the AMQP service when a queue is created or viewed.
Queue	The queue or list of queues to monitor. A list of queues is specified with a comma-separated list.
Username	The username that is used for authenticating with the RabbitMQ service.
Password	The password that is used to authenticate with the RabbitMQ service.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Allow Untrusted Certificates	Enable this option when the endpoint is using a certificate that cannot be verified via the Certificate Chain. This would include a self-signed certificate, or one from a private CA that you do not want to import into your CA trust. This option should not be used for endpoints with a certificate issued by a Public CA (SaaS Products, Public Cloud Infrastructure, and so on.) The certificate must be downloaded in PEM or DER encoded binary format and then placed in the `/opt/qradar/conf/trusted_certificates/` directory with a `.cert` or `.crt` file extension.

Related concepts

"Copy the server certificate" on page 208
You need a server certificate to support HTTPS connections. QRadar supports certificates with the `.crt`, `.cert`, or `.der` file extensions.

Related information

Adding a log source

Copy the server certificate

You need a server certificate to support HTTPS connections. QRadar supports certificates with the `.crt`, `.cert`, or `.der` file extensions.

To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- Use SSH to log in to the QRadar Console or managed host and retrieve the certificate by typing the following command:

```
/opt/qradar/bin/getcert.sh <IP or Hostname for RabbitMQ> <Port for RabbitMQ>
```

A certificate is downloaded from the specified host name or IP address and placed into the `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

SDEE protocol configuration options

You can configure a log source to use the Security Device Event Exchange (SDEE) protocol. QRadar uses the protocol to collect events from appliances that use SDEE servers.

The SDEE protocol is an outbound/active protocol.

The following table describes the protocol-specific parameters for the SDEE protocol:

Table 83. SDEE protocol parameters

Parameter	Description
Protocol Configuration	**SDEE**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured SDEE log source, ensure that you give each one a unique name.
URL	The HTTP or HTTPS URL that is required to access the log source, for example, https://www.example.com/cgi-bin/sdee-server. For SDEE/CIDEE (Cisco IDS v5.x and later), the URL must end with `/cgi-bin/sdee-server`. Administrators with RDEP (Cisco IDS v4.x), the URL must end with `/cgi-bin/event-server`.
Force Subscription	When the check box is selected, the protocol forces the server to drop the least active connection and accept a new SDEE subscription connection for the log source.
Maximum Wait To Block For Events	When a collection request is made and no new events are available, the protocol enables an event block. The block prevents another event request from being made to a remote device that did not have any new events. This timeout is intended to conserve system resources.

Seculert Protection REST API protocol configuration options

To receive events from Seculert, configure a log source to use the Seculert Protection REST API protocol.

The Seculert Protection REST API protocol is an active outbound protocol that provides alerts about confirmed incidents of malware that are actively communicating or exfiltrating information.

Important: Before you can configure a log source for Seculert, you must use the following steps to obtain your API key from the Seculert web portal.

1. Log in to the Seculert web portal.
2. On the dashboard, click the **API** tab.
3. Copy the value for **Your API Key**.

The following table describes the protocol-specific parameters for the Seculert Protection REST API protocol:

Table 84. Seculert Protection REST API protocol parameters

Parameter	Description
Log Source Type	**Seculert**
Protocol Configuration	**Seculert Protection REST API**
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from Seculert. Each additional log source that you create when you have multiple installations ideally includes a unique identifier, such as an IP address or hostname.
API Key	The API key that is used for authenticating with the Seculert Protection REST API. The API key is obtained from the Seculert web portal.
Use Proxy	If the API is accessed by using a proxy, select this checkbox. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Specify how often the log collects data. The value can be in Minutes (M), Hours (H), or Days (D). The default is 10 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Enable Advanced Options	Select this checkbox to enable the following configuration options: **Server**, **API Version**, **Query Time Interval**, **Allow Untrusted Certificates**, **Override Workflow**, **Workflow**, and **Workflow Parameters**. These parameters are only visible if you select this checkbox.
Server	The server that is used for forming the API query. For example, `[Server]/1.1/incidents/records`. The default value is `https://api.seculert.com]../`.

Table 84. Seculert Protection REST API protocol parameters (continued)	
Parameter	**Description**
API Version	The API version that is used for forming the API query. For example, `https://api.seculert.com/[API Version]/incidents/records`. The default value is `1.1`.
Query Time Interval	The maximum time interval for each query to collect events. For example, if you set the interval as 15 minutes, the query collects events from the last query time to 15 minutes later. If the current time is less than 15 minutes since the last query, the query collects events from the last query time until the current time. The value must be in milliseconds (ms); 1000 ms is 1 second. The default value is 900000 ms (15 minutes).
Allow Untrusted	If you enable this parameter, the protocol can accept self-signed and otherwise untrusted certificates that are located within the `/opt/qradar/conf/trusted_certificates/` directory. If you disable the parameter, the scanner trusts only certificates that are signed by a trusted signer. The certificates must be in PEM or RED-encoded binary format and saved as a `.crt` or `.cert` file. If you modify the workflow to include a hardcoded value for the **Allow Untrusted Certificates** parameter, the workflow overrides your selection in the UI. If you do not include this parameter in your workflow, then your selection in the UI is used.
Override Work Flow	Enable this option to customize the workflow. When you enable this option, the **Workflow** and **Workflow Parameters** parameters appear.
Work Flow	The XML document that defines how the protocol instance collects events from the target API. For more information about the default workflow, see "Seculert Protection REST API protocol workflow" on page 211.
Workflow Parameters	The XML document that contains the parameter values used directly by the workflow. For more information about the default workflow parameters, see "Seculert Protection REST API protocol workflow" on page 211.
Enabled	By default, the checkbox is selected to enable the log source to communicate with QRadar.
Credibility	Select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.

Table 84. Seculert Protection REST API protocol parameters (continued)	
Parameter	**Description**
Coalescing Events	Select this checkbox to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this checkbox to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Seculert Protection REST API protocol workflow

You can customize your workflow and workflow parameters based on the default workflow.

A workflow is an XML document that describes the event retrieval process. The workflow defines one or more parameters, which can be explicitly assigned values in the workflow XML or can derive values from the workflow parameter values XML document. The workflow consists of multiple actions that run sequentially.

The default workflow and workflow parameter XML files are available on GitHub. For more information, see Seculert Protection (https://github.com/IBM/IBM-QRadar-Universal-Cloud-REST-API/tree/master/IBM%20Verified/Seculert%20Protection).

Seculert default workflow

The following example shows the default Seculert workflow:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Workflow name="Seculert" version="1.1" xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
Workflow/V2">
    <Parameters>
        <Parameter name="apiKey" label="API Key" required="true" />
        <Parameter name="queryTimeInterval" label="Query Time Interval" required="true"
default="900000" />
        <Parameter name="server" label="Server" required="true" default="https://
api.secert.com" />
        <Parameter name="apiVersion" label="API Version" required="true" default="1.1" />
    </Parameters>

    <Actions>
        <Log type="DEBUG" message="Initializing bookmark values" />
        <!-- Initialize the Bookmark -->
        <Initialize path="/bookmarkRecords" value="${time() - /queryTimeInterval}" />
        <Initialize path="/bookmarkAlerts" value="${time() - /queryTimeInterval}" />
        <Initialize path="/firstRun" value="1" />
        <Initialize path="/sevenDays" value="604800000" />

        <!-- Event retriever thread is a bit slow to kill error'd out provider threads, this
prevents duplicate errors. -->
        <If condition="/firstRun = 1" >
            <Sleep duration="2000" />
        </If>

        <Log type="DEBUG" message="Checking if the current bookmarks are older than 7 days." />
        <If condition="time() > /bookmarkRecords + /sevenDays" >
            <Set path="/bookmarkRecords" value="${time() - /sevenDays}" />
```

```
        </If>

        <If condition="time() > /bookmarkAlerts + /sevenDays" >
            <Set path="/bookmarkAlerts" value="${time() - /sevenDays}" />
        </If>
        <Set path="/doOnceMore" value="1" />

        <Log type="DEBUG" message="The current bookmark for bookmarkRecords is /
bookmarkRecords" />
        <Log type="DEBUG" message="The current bookmark for bookmarkAlerts is /
bookmarkAlerts" />
        <Log type="DEBUG" message="Iterating through events in till we are caught up." />
        <While condition="time() > /bookmarkRecords + /queryTimeInterval or /doOnceMore = 1">
            <!-- Get the start/end date. start_time=bookmark. End_time is the bookmark time + X
seconds (userconfigurable) -->
            <FormatDate pattern="MM/dd/yyyy HH:mm:ss" timeZone="UTC" time="${/bookmarkRecords}"
savePath="/start_time" />

            <If condition="time() > /bookmarkRecords + /queryTimeInterval" >
                <FormatDate pattern="MM/dd/yyyy HH:mm:ss" timeZone="UTC" time="${/
bookmarkRecords + /queryTimeInterval}" savePath="/end_time" />
            </If>
            <Else>
                <FormatDate pattern="MM/dd/yyyy HH:mm:ss" timeZone="UTC" time="${time()}"
savePath="/end_time" />
            </Else>

            <!-- Fetch Events -->
            <CallEndpoint url="${/server}/${/apiVersion}/incidents/records" method="GET"
savePath="/get_logs" >
                <QueryParameter name="format" value="leef" />
                <QueryParameter name="api_key" value="${/apiKey}" />
                <QueryParameter name="from_time" value="${/start_time}" />
                <QueryParameter name="to_time" value="${/end_time}" />
            </CallEndpoint>

            <Log type="DEBUG" message="Checking for errors." />
            <!-- Handle Errors -->
            <If condition="/get_logs/status_code != 200">
                <Abort reason="${/get_logs/status_code}: ${/get_logs/status_message}" />
             </If>

             <Log type="DEBUG" message="Splitting the event string by [\r\n] into an array
object" />
             <!-- Split the raw event list based of "\r\n-->
             <Split value="${/get_logs/body}" delimiter="\r\n" savePath="/values" />

            <!-- Post Events -->
            <If condition="count(/values) > 1" >
                <PostEvents path="/values" source="api.seculert.com" />
            </If>
            <Else>
                <If condition="not empty(/values[0])" >
                    <Set path="/successOrError" value="${substring(/values[0],2,7)}" />
                    <If condition="/successOrError = 'error'">
                        <Abort reason="${/values[0]}" />
                    </If>
                    <PostEvents path="/values" source="api.seculert.com" />
                </If>
            </Else>

             <Log type="DEBUG" message="Updating the bookmark value to the latest time." />
             <!-- Update Bookmark -->
             <If condition="time() > /bookmarkRecords + /queryTimeInterval" >
                 <Set path="/bookmarkRecords" value="${/bookmarkRecords + /
queryTimeInterval}" />
             </If>
             <Else>
                 <Set path="/bookmarkRecords" value="${time()}" />
                 <Set path="/doOnceMore" value="0" />
             </Else>
             <Sleep duration="5000" />
        </While>

        <Set path="/doOnceMore" value="1" />

        <While condition="time() > /bookmarkAlerts + /queryTimeInterval or /doOnceMore = 1">
            <!-- Get the start/end date. start_time=bookmark. End_time is the bookmark time + X
seconds (userconfigurable) -->
            <FormatDate pattern="MM/dd/yyyy HH:mm:ss" timeZone="UTC" time="${/bookmarkAlerts}"
savePath="/start_time" />
```

```
            <If condition="time() > /bookmarkRecords + /queryTimeInterval" >
                <FormatDate pattern="MM/dd/yyyy HH:mm:ss" timeZone="UTC" time="${/
bookmarkAlerts + /queryTimeInterval}" savePath="/end_time" />
            </If>
            <Else>
                <FormatDate pattern="MM/dd/yyyy HH:mm:ss" timeZone="UTC" time="${time()}"
savePath="/end_time" />
            </Else>

            <!-- Fetch Events -->
            <CallEndpoint url="${/server}/${/apiVersion}/incidents/alerts" method="GET"
savePath="/get_logs" >
                <QueryParameter name="format" value="leef" />
                <QueryParameter name="api_key" value="${/apiKey}" />
                <QueryParameter name="from_time" value="${/start_time}" />
                <QueryParameter name="to_time" value="${/end_time}" />
            </CallEndpoint>

            <Log type="DEBUG" message="Checking for errors." />
            <!-- Handle Errors -->
            <If condition="/get_logs/status_code != 200">
                <Abort reason="${/get_logs/status_code}: ${/get_logs/status_message}" />
            </If>

            <Log type="DEBUG" message="Splitting the event string by [\r\n] into an array
object" />
            <!-- Split the raw event list based of "\r\n-->
            <Split value="${/get_logs/body}" delimiter="\r\n" savePath="/values" />

            <!-- Post Events -->
            <If condition="count(/values) > 1" >
                <PostEvents path="/values" source="api.seculert.com" />
            </If>
            <Else>
                <If condition="not empty(/values[0])" >
                    <Set path="/successOrError" value="${substring(/values[0],2,7)}" />
                    <If condition="/successOrError = 'error'">
                        <Abort reason="${/values[0]}" />
                    </If>
                    <PostEvents path="/values" source="api.seculert.com" />
                </If>
            </Else>

            <Log type="DEBUG" message="Updating the bookmark value to the latest time." />
            <!-- Update Bookmark -->
            <If condition="time() > /bookmarkAlerts + /queryTimeInterval" >
                <Set path="/bookmarkAlerts" value="${/bookmarkAlerts + /queryTimeInterval}" />
            </If>
            <Else>
                <Set path="/bookmarkAlerts" value="${time()}" />
                <Set path="/doOnceMore" value="0" />
            </Else>
            <Sleep duration="5000" />
        </While>
    </Actions>
    <Tests>
        <DNSResolutionTest host="${/server}" />
        <TCPConnectionTest host="${/server}" />
        <HTTPConnectionThroughProxyTest url="${/server}" expectedResponseStatus="404" />
    </Tests>
</Workflow>
```

Seculert default workflow parameters

The following example shows the default workflow parameters for Seculert:

```
<?xml version="1.0" encoding="UTF-8" ?>
<WorkflowParameterValues xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
WorkflowParameterValues/V2">
  <Value name="apiKey"    value="" />
  <Value name="queryTimeInterval"    value="900000" />
  <Value name="server"    value="https://api.seculert.com" />
  <Value name="apiVersion"    value="1.1" />
</WorkflowParameterValues>
```

SMB Tail protocol configuration options

You can configure a log source to use the SMB Tail protocol. Use this protocol to watch events on a remote Samba share and receive events from the Samba share when new lines are added to the event log.

The SMB Tail protocol is an active outbound protocol.

The following table describes the protocol-specific parameters for the SMB Tail protocol:

Table 85. SMB Tail protocol parameters

Parameter	Description
Protocol Configuration	**SMB Tail**
Log Source Identifier	Type the IP address, hostname, or a unique name to identify your log source.
Server Address	The IP address or hostname of your SMB Tail server.
Domain	Type the domain for your SMB Tail server. This parameter is optional if your server is not in a domain.
Username	Type the username that is required to access your server.
Password	Type the password that is required to access your server.
Confirm Password	Confirm the password that is required to access the server.
Log Folder Path	The directory path to access the log files. For example, administrators can use the `c$/LogFiles/` directory for an administrative share, or the `LogFiles/` directory for a public share folder path. However, the `c:/LogFiles` directory is not a supported log folder path. If a log folder path contains an administrative share (C$), users with NetBIOS access on the administrative share (C$) have the privileges that are required to read the log files. Local system or domain administrator privileges are also sufficient to access all log files that are on an administrative share.
File Pattern	The regular expression (regex) that identifies the event logs.

Table 85. SMB Tail protocol parameters (continued)

Parameter	Description
SMB Version	Select the version of Server Message Block (SMB) that you want to use. **AUTO** Auto-detects to the highest version that the client and server agree to use. **SMB1** Forces the use of SMB1. SMB1 uses the `jCIFS.jar` (Java ARchive) file. **Important:** SMB1 is no longer supported. All administrators must update existing configurations to use SMB2 or SMB3. **SMB2** Forces the use of SMB2. SMB2 uses the `jNQ.jar` file. **SMB3** Forces the use of SMB3. SMB3 uses the `jNQ.jar` file. **Note:** Before you create a log source with a specific SMB version (for example: SMBv1, SMBv2, and SMBv3), ensure that the specified SMB version is supported by the Windows OS that is running on your server. You also need to verify that SMB versions are enabled on the specified Windows Server. For more information about which Windows version supports which SMB versions, go to the Microsoft TechNet website (https://blogs.technet.microsoft.com/josebda/2012/06/06/windows-server-2012-which-version-of-the-smb-protocol-smb-1-0-smb-2-0-smb-2-1-or-smb-3-0-are-you-using-on-your-file-server/). For more information about how to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server, go to the Microsoft support website (https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server).
Force File Read	If the checkbox is cleared, the log file is read only when QRadar detects a change in the modified time or file size.
Recursive	If you want the file pattern to search sub folders, use this option. By default, the checkbox is selected.
Polling Interval (in seconds)	Type the polling interval, which is the number of seconds between queries to the log files to check for new data. The default is 10 seconds.
Throttle Events/Sec	The maximum number of events the SMB Tail protocol forwards per second.
File Encoding	The character encoding that is used by the events in your log file.

Table 85. SMB Tail protocol parameters (continued)	
Parameter	**Description**
File Exclusion List	A list of regular expressions that prevent certain file directories from opening. The list includes one regular expression per line. When a file or directory matches one of the regular expressions, that file or directory does not open. When a file is in use, other applications might not be able to use it. Use this parameter to prevent locking those files or to prevent the protocol from accessing specific files. The pattern does not apply to the full Log Folder Path. It applies only to the final directory that is listed in the path. The pattern applies against all files or directories that are found within the Log Folder Path's directory. The following list is an example of what you can enter in this field. `/j50.*\.log` `dhcp\.mdb` `dhcp\.tmp`

SNMPv2 protocol configuration options

You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events.

The SNMPv2 protocol is an inbound/passive protocol.

The following table describes the protocol-specific parameters for the SNMPv2 protocol:

Table 86. SNMPv2 protocol parameters	
Parameter	**Description**
Protocol Configuration	**SNMPv2**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured SNMPv2 log source, ensure that you give each one a unique name.
Community	The SNMP community name that is required to access the system that contains SNMP events. For example, Public.
Include OIDs in Event Payload	Specifies that the SNMP event payload is constructed by using name-value pairs instead of the event payload format. When you select specific log sources from the **Log Source Types** list, OIDs in the event payload are required for processing SNMPv2 or SNMPv3 events.

Table 86. SNMPv2 protocol parameters (continued)	
Parameter	**Description**
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Coalescing events increase the event count when the same event occurs multiple times within a short time interval. Coalesced events provide administrators a way to view and determine the frequency with which a single event type occurs on the **Log Activity** tab. When this check box is clear, the events are displayed individually and the information is not bundled. New and automatically discovered log sources inherit the value of this check box from the **System Settings** configuration on the **Admin** tab. Administrators can use this check box to override the default behavior of the system settings for an individual log source.
Store Event Payload	Select this check box to enable the log source to store the payload information from an event. New and automatically discovered log sources inherit the value of this check box from the **System Settings** configuration on the **Admin** tab. Administrators can use this check box to override the default behavior of the system settings for an individual log source.

SNMPv3 protocol configuration options

You can configure a log source to use the SNMPv3 protocol to receive SNMPv3 events.

The SNMPv3 protocol is an inbound/passive protocol.

The following table describes the protocol-specific parameters for the SNMPv3 protocol:

Table 87. SNMPv3 protocol parameters	
Parameter	**Description**
Protocol Configuration	**SNMPv3**
Log Source Identifier	Type a unique name for the log source.
Authentication Protocol	The algorithm that you want to use to authenticate SNMPv3 traps: • **SHA** uses Secure Hash Algorithm (SHA) as your authentication protocol. • **MD5** uses Message Digest 5 (MD5) as your authentication protocol.
Authentication Password	The password to authenticate SNMPv3. Your authentication password must include a minimum of 8 characters.

Table 87. SNMPv3 protocol parameters (continued)	
Parameter	**Description**
Decryption Protocol	Select the algorithm that you want to use to decrypt the SNMPv3 traps. • DES • AES128 • AES192 • AES256 **Note:** If you select AES192 or AES256 as your decryption algorithm, you must install the Java Cryptography Extension. For more information about installing the Java Cryptography Extension on McAfee ePolicy Orchestrator, see Installing the Java Cryptography Extension.
Decryption Password	The password to decrypt SNMPv3 traps. Your decryption password must include a minimum of 8 characters.
User	The user name that was used to configure SNMPv3 on your appliance
Include OIDs in Event Payload	Specifies that the SNMP event payload is constructed by using name-value pairs instead of the standard event payload format. When you select specific log sources from the **Log Source Types** list, OIDs in the event payload are required for processing SNMPv2 or SNMPv3 events. **Important:** You must include OIDs in the event payload for processing SNMPv3 events for McAfee ePolicy Orchestrator.

Sophos Enterprise Console JDBC protocol configuration options

To receive events from Sophos Enterprise Consoles, configure a log source to use the Sophos Enterprise Console JDBC protocol.

The Sophos Enterprise Console JDBC protocol is an outbound/active protocol that combines payload information from application control logs, device control logs, data control logs, tamper protection logs, and firewall logs in the vEventsCommonData table. If the Sophos Enterprise Console does not have the Sophos Reporting Interface, you can use the standard JDBC protocol to collect antivirus events.

The following table describes the parameters for the Sophos Enterprise Console JDBC protocol:

Table 88. Sophos Enterprise Console JDBC protocol parameters	
Parameter	**Description**
Protocol Configuration	**Sophos Enterprise Console JDBC**

Table 88. Sophos Enterprise Console JDBC protocol parameters (continued)	
Parameter	**Description**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	**MSDE**
Database Name	The database name must match the database name that is specified in the **Log Source Identifier** field.
Port	The default port for MSDE in Sophos Enterprise Console is 1168. The JDBC configuration port must match the listener port of the Sophos database to communicate with QRadar. The Sophos database must have incoming TCP connections enabled. If a **Database Instance** is used with the MSDE database type, you must leave the **Port** parameter blank.
Authentication Domain	If your network does not use a domain, leave this field blank.
Database Instance	The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or administrators block access to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank.
Table Name	`vEventsCommonData`
Select List	`*`
Compare Field	`InsertedAt`
Use Prepared Statements	Prepared statements enable the protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most configurations can use prepared statements. Clear this check box to use an alternative method of querying that do not use pre-compiled statements.
Start Date and Time	Optional. A start date and time for when the protocol can start to poll the database. If a start time is not defined, the protocol attempts to poll for events after the log source configuration is saved and deployed.
Polling Interval	The polling interval, which is the amount of time between queries to the database. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.

Table 88. Sophos Enterprise Console JDBC protocol parameters (continued)	
Parameter	**Description**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.
Use Named Pipe Communication	If MSDE is configured as the database type, administrators can select this check box to use an alternative method to a TCP/IP port connection. Named pipe connections for MSDE databases require the user name and password field to use a Windows authentication username and password and not the database user name and password. The log source configuration must use the default named pipe on the MSDE database.
Database Cluster Name	If you use your SQL server in a cluster environment, define the cluster name to ensure that named pipe communications function properly.
Use NTLMv2	Forces MSDE connections to use the NTLMv2 protocol with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. The **Use NTLMv2** check box does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.

Sourcefire Defense Center eStreamer protocol options

Sourcefire Defense Center eStreamer protocol is now known as Cisco Firepower eStreamer protocol.

Syslog Redirect protocol overview

The Syslog Redirect protocol is a passive inbound protocol that is used as an alternative to the Syslog protocol. Use this protocol when you want QRadar to identify the specific device name that sent the events. QRadar can passively listen for Syslog events by using TCP or UDP on any unused port that you specify.

The following table describes the protocol-specific parameters for the Syslog Redirect protocol:

Table 89. Syslog Redirect protocol parameters	
Parameter	**Description**
Protocol Configuration	**Syslog Redirect**
Log Source Identifier	Enter a **Log Source Identifier** to use as a default. If the **Log Source Identifier Regex** cannot parse the **Log Source Identifier** from a particular payload by using the regex that is provided, the default is used.
Log Source Identifier Regex	Enter a regex to parse the **Log Source Identifier** from the payload.

Table 89. Syslog Redirect protocol parameters (continued)	
Parameter	**Description**
Log Source Identifier Regex Format String	Format string to combine capture groups from the Log Source Identifier Regex. For example: "$1" would use the first capture group. "$1$2" would concatenate capture groups 1 and 2. "$1 TEXT $2" would concatenate capture group 1, the literal "TEXT" and capture group 2. The resulting string is used as the new log source identifier.
Listen Port	Enter any unused port and set your log source to send events to QRadar on that port.
Protocol	From the list, select either **TCP** or **UDP**. The Syslog Redirect protocol supports any number of UDP syslog connections, but restricts TCP connections to 2500. If the syslog stream has more than 2500 log sources, you must enter a second log source and listen port number.
Perform DNS Lookup On Regex Match	Select the **Perform DNS Lookup On Regex Match** checkbox to enable DNS functionality, which is based on the **Log Source Identifier** parameter value. By default, the checkbox is not selected.
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Payload Size	The payload size is the length of data that is sent by the communicating endpoint. The default is 2048. The payload size must be an integer between 2048 and 32000.
Enabled	Select this checkbox to enable the log source. By default, the checkbox is selected.
Credibility	From the list, select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.

TCP Multiline Syslog protocol configuration options

The TCP Multiline Syslog protocol is a passive inbound protocol that uses regular expressions to identify the start and end pattern of multiline events.

The following example is a multiline event:

```
06/13/2012 08:15:15 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: <IP_address>
Source Port: 80
Destination Address: <IP_address>
Destination Port:444
```

The following table describes the protocol-specific parameters for the TCP Multiline Syslog protocol:

Table 90. TCP Multiline Syslog protocol parameters

Parameter	Description
Protocol Configuration	**TCP Multiline Syslog**
Log Source Identifier	Type an IP address or hostname to identify the log source. To use a source name instead of a log source identifier, select **Use Custom Source Name** and enter values for the **Source Name Regex** and **Source Name Formatting String** parameters. **Note:** These parameters are only available if **Show Advanced Options** is set to **Yes**.
Listen Port	The number of the port that accepts incoming TCP Multiline Syslog events. The default listen port is 12468. To edit the port number, complete the following steps: 1. Enter the new port number for the protocol. 2. Click **Save**. 3. On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**. **Attention:** When administrators click **Deploy Full Configuration**, the system restarts all services, which can create in a gap in data collection until the deployment completes.
Aggregation Method	The method that you use to aggregate your TCP Multiline Syslog data. You can choose one of the following methods: **ID-Linked Multiline** Processes multiline event logs that contain a common value at the start of each line. **Start/End Matching** Processes multiline events by specifying start and end patterns for the events.

Table 90. TCP Multiline Syslog protocol parameters (continued)

Parameter	Description
Event Start Pattern	This parameter is available when you set the **Aggregation Method** parameter to **Start/End Matching**. The regular expression (regex) that is required to identify the start of a TCP multiline event payload. Syslog headers typically begin with a date or timestamp. The protocol can create a single-line event that is based on solely on an event start pattern, such as a timestamp. When only a start pattern is available, the protocol captures all the information between each start value to create a valid event.
Event End Pattern	This parameter is available when you set the **Aggregation Method** parameter to **Start/End Matching**. This regular expression (regex) that is required to identify the end of a TCP multiline event payload. If the syslog event ends with the same value, use a regular expression to determine the end of an event. When only an **Event Start Pattern** is used and the sending device sends a few events (low EPS) in an interval, then the last sent event is not processed until the pipeline detects a new **Event Start Pattern**. For example, when a single "Test event" is sent, it might be invisible in the QRadar Log Activity without adding an **Event End Pattern**. To circumvent this scenario, send 2 to 3 test events at a time. Without an **Event End Pattern**, the last event is not captured until a new **Event Start Pattern** is detected.
Message ID Pattern	This parameter is available when you set the **Aggregation Method** parameter to **ID-Linked**. This regular expression (regex) is required to filter the event payload messages. The TCP multiline event messages must contain a common identifying value that repeats on each line of the event message.
Event Formatter	Use the **Windows Multiline** option for multiline events that are formatted specifically for Windows.
Show Advanced Options	The default is **No**. Select **Yes** if you want to customize the event data.
Use Custom Source Name	This parameter is available when you set **Show Advanced Options** to **Yes**. Select the checkbox if you want to customize the source name with regex.
Source Name Regex	This parameter is available when you check **Use Custom Source Name**. The regular expression (regex) that captures one or more values from event payloads that are handled by this protocol. These values are used with the **Source Name Formatting String** parameter to set a source or origin value for each event. This source value is used to route the event to a log source with a matching **Log Source Identifier** value.

Table 90. TCP Multiline Syslog protocol parameters (continued)	
Parameter	**Description**
Source Name Formatting String	This parameter is available when you enable **Use Custom Source Name**. You can use a combination of one or more of the following inputs to form a source value for event payloads that are processed by this protocol: • One or more capture groups from the **Source Name Regex**. To refer to a capture group, use *x* notation where *x* is the index of a capture group from the **Source Name Regex**. • The IP address where the event data originated from. To refer to the packet IP, use the token `$PIP$`. • Literal text characters. The entire **Source Name Formatting String** can be user-provided text. For example, if the **Source Name Regex** is `'hostname=(.*?)'` and you want to append `hostname.com` to the capture group 1 value, set the **Source Name Formatting String** to `\1.hostname.com`. If an event is processed that contains `hostname=ibm`, then the event payload's source value is set to `ibm.hostname.com`, and QRadar routes the event to a log source with that **Log Source Identifier**.
Use as a Gateway Log Source	This parameter is available when you set **Show Advanced Options** to **Yes**. When selected, events that flow through the log source are routed to other log sources, based on the source name tagged on the events. When this option is not selected and **Use Custom Source Name** is not enabled, incoming events are tagged with a source name that corresponds to the Log Source Identifier parameter.
Flatten Multiline Events into Single Line	This parameter is available when you set **Show Advanced Options** to **Yes**. Shows an event in one single line or multiple lines.
Retain Entire Lines during Event Aggregation	This parameter is available when you set **Show Advanced Options** to **Yes**. If you set the **ID-Linked Multiline** method for the **Aggregation Method** parameter, then this parameter can modify aggregated event data outputs. If you enable **Retain Entire Lines during Event Aggregation**, then all parts of events are kept when aggregating events with the same ID pattern. If you don't enable this parameter, the part of the events before the **Message ID Pattern** are discarded when the events are aggregated.
Time Limit	The number of seconds to wait for additional matching payloads before the event is pushed into the event pipeline. The default is 10 seconds.
Initial Number of Threads	The initial number of threads to use for formatting and posting events.

Table 90. TCP Multiline Syslog protocol parameters (continued)	
Parameter	**Description**
Maximum Number of Threads	The maximum number of threads to use for formatting and posting events. When the task queue is full, more threads are created up to the value set by the **Maximum Number of Threads** parameter.
Enabled	Select this checkbox to enable the log source.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector in your deployment to host the TCP Multiline Syslog listener.
Coalescing Events	Select this checkbox to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this checkbox to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

TCP Multiline Syslog protocol configuration use cases

To set the TCP Multiline Syslog listener log source to collect all events that are sent from the same system, follow these steps:

1. Leave **Use As A Gateway Log Source** and **Use Custom Source Name** cleared.
2. Enter the IP address of the system that is sending events in the **Log Source Identifier** parameter.

Figure 2. A QRadar log source collects events sent from a single system to a TCP Multiline Syslog Listener

If multiple systems are sending events to the TCP Multiline Syslog listener, or if one intermediary system is forwarding events from multiple systems and you want the events to be routed to separate log sources based on their syslog header or IP address, select the **Use As A Gateway Log Source** checkbox.

Note: QRadar checks each event for an RFC3164 or RFC5424-compliant syslog header, and if present, uses the IP or hostname from that header as the source value for the event. The event is routed to a log source with that same IP or hostname as its Log Source Identifier. If no such header is present, QRadar uses the source IP value from the network packet that the event arrived on as the source value for the event.

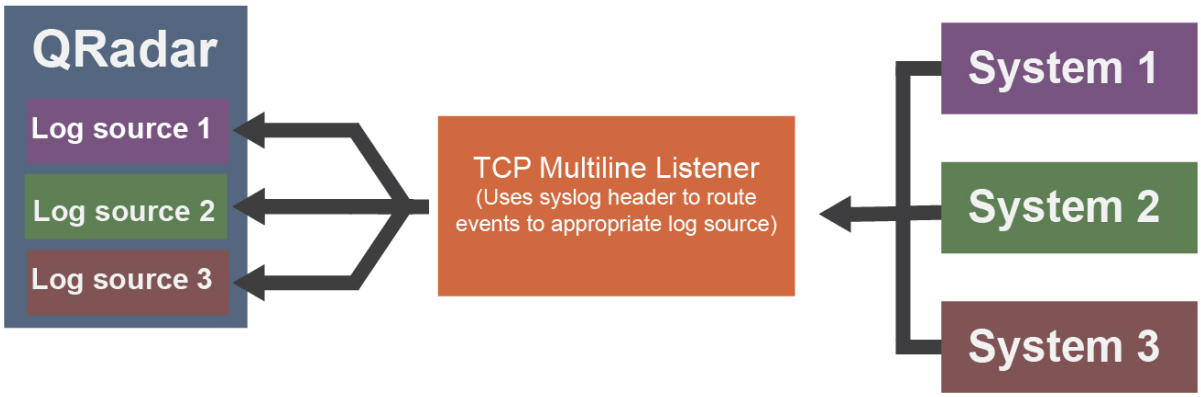


Figure 3. Separate QRadar log sources collect events sent from multiple systems to a TCP Multiline Listener, by using the syslog header.

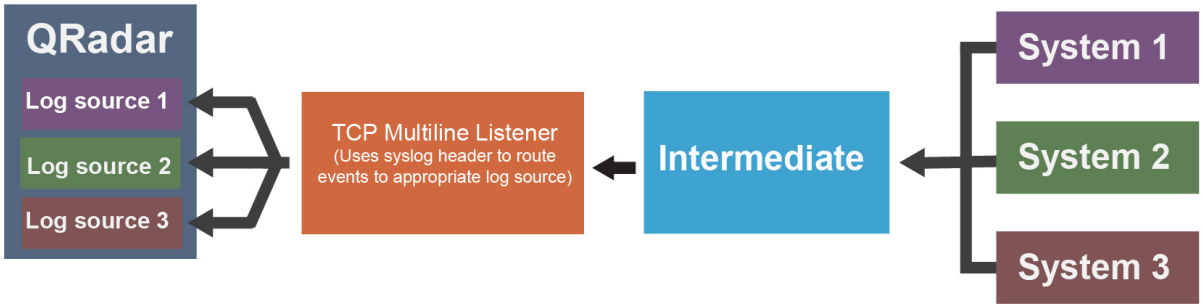


Figure 4. Separate QRadar log sources collect events sent from multiple systems and forwarded through an intermediate system to a TCP Multiline Listener, by using the syslog header.

To route events to separate log sources based on a value other than the IP or hostname in their syslog header, follow these steps:

1. Select the **Use Custom Source Name** checkbox.
2. Configure a **Source Name Regex** and **Source Name Formatting String** to customize how QRadar sets a source name value for routing the received events to log sources.

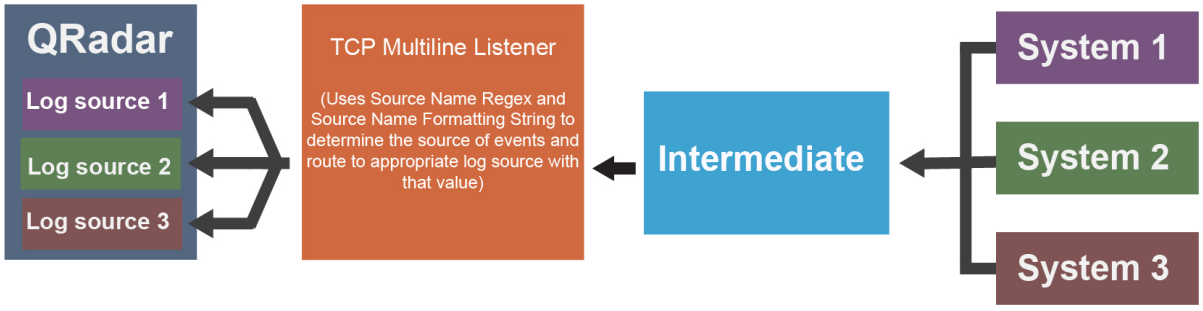


Figure 5. Separate QRadar log sources collect events sent from multiple systems and forwarded through an intermediate system to a TCP Multiline Listener, by using the Source Name Regex and Source Name Formatting String.

Related concepts

"Gateway log source" on page 15

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

TLS Syslog protocol configuration options

Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

The TLS Syslog protocol is a passive inbound protocol. The log source creates a listen port for incoming TLS Syslog events. By default, TLS Syslog log sources use the certificate and key that is generated by IBM QRadar. The TLS Log Source protocol supports the following functions.

- An **Event Collector** supports up to 1000 TLS connections.
- Each TLS Log Source (except **AutoDiscovered**) must use a unique port on that **Event Collector**.
- You can also create up to 1000 TLS Log Sources on an **Event Collector**.
- For **Pem** and **Key**, the **Key** must be in PKCS8/DER format.
- If you are using the **Cert Management** app, the **Key** must be in PKCS8 format.

The following table describes the protocol-specific parameters for the TLS Syslog protocol:

Table 91. TLS Syslog protocol parameters

Parameter	Description
Protocol Configuration	**TLS Syslog**
Log Source Identifier	An IP address or hostname to identify the log source.
TLS Listen Port	The default TLS listen port is 6514. **Important:** You can assign only one TLS Syslog log source to each TLS listen port.
Authentication Mode	The mode your TLS connection uses to authenticate. If you select the **TLS and Client Authentication** option, you must configure the certificate parameters.
Client Certificate Authentication	Select one of the following options from the list: • **CN Allowlist and Issuer Verification** • **Client Certificate on Disk**
Use CN Allowlist	Enable this parameter to use a CN allowlist.
CN Allowlist	The allowlist of trusted client certificate common names. You can enter plain text or a regular expression (regex). To define multiple entries, enter each one on a separate line.
Use Issuer Verification	Enable this parameter to use issuer verification.

Table 91. TLS Syslog protocol parameters (continued)	
Parameter	**Description**
Root/Intermediate Issuer's Certificate or Public key	Enter the Root/Intermediate issuer's certificate or public key in PEM format. • Enter the certificate, beginning with: `-----BEGIN CERTIFICATE-----` and ending with: `-----END CERTIFICATE-----` • Enter the public key beginning with: `-----BEGIN PUBLIC KEY-----` and ending with: `-----END PUBLIC KEY-----`
Check Certificate Revocation	Checks the certificate revocation status against the client certificate. This option requires network connectivity to the URL that is specified by the **CRL Distribution Points** field for the client certificate in the X509v3 extension.
Check Certificate Usage	Checks the contents of the certificate X509v3 extensions in the **Key Usage** and **Extended Key Usage** extension fields. For incoming client certificate, the allow values of X509v3 Key Usage are `digitalSignature` and `keyAgreement`. The allow value for X509v3 Extended Key Usage is `TLS Web Client Authentication`. This property is disabled by default.
Client Certificate Path	The absolute path to the client-certificate on disk. The certificate must be stored on the QRadar Console or Event Collector for this log source. **Important:** Ensure that the certificate file that you enter begins with: `-----BEGIN CERTIFICATE-----` and ends with: `-----END CERTIFICATE-----`
Server Certificate Type	The type of certificate to use for authentication for the server certificate and server key. Select one of the following options from the **Server Certificate Type** list: • **Generated Certificate** • **PEM Certificate and Private Key** • **PKCS12 Certificate Chain and Password** • **Choose from QRadar Certificate Store**

Table 91. TLS Syslog protocol parameters (continued)	
Parameter	**Description**
Generated Certificate	This option is available when you configure the **Certificate Type**. If you want to use the default certificate and key that is generated by QRadar for the server certificate and server key, select this option. The generated certificate is named `syslog-tls.cert` in the `/opt/qradar/conf/trusted_certificates/` directory on the target Event Collector that the log source is assigned to.
Single Certificate and Private Key	This option is available when you configure the **Certificate Type**. If you want to use a single PEM certificate for the server certificate, select this option and then configure the following parameters: • **Provided Server Certificate Path** - The absolute path to the server certificate. • **Provided Private Key Path** - The absolute path to the private key. **Important:** The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.
PKCS12 Certificate and Password	This option is available when you configure the **Certificate Type**. If you want to use a PKCS12 file that contains the server certificate and server key, select this option and then configure the following parameters: • **PKCS12 Certificate Path** - Type the file path for the PKCS12 file that contains the server certificate and server key. • **PKCS12 Password** - Type the password to access the PKCS12 file. • **Certificate Alias** - If there is more than one entry in the PKCS12 file, an alias must be provided to specify which entry to use. If only one alias is in the PKCS12 file, leave this field blank.
Choose from QRadar Certificate Store	This option is available when you configure the **Certificate Type**. You can use the Certificate Management app to upload a certificate from the QRadar Certificate Store.
Max Payload Length	The maximum payload length (characters) that is displayed for TLS Syslog message.
Maximum Connections	The **Maximum Connections** parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. For each Event Collector, there is a limit of 1000 connections, including enabled and disabled log sources, in the TLS Syslog log source configuration for each Event Collector. The default for each device connection is 50 but not the limit for each port. **Tip:** Automatically discovered log sources share a listener with another log source. For example, if you use the same port on the same event collector, it counts only one time toward the limit.

Table 91. TLS Syslog protocol parameters (continued)	
Parameter	**Description**
TLS Protocols	The TLS Protocol to be used by the log source. Select the "TLS 1.2 or later" option.
Use As A Gateway Log Source	Sends collected events through the QRadar Traffic Analysis Engine to automatically detect the appropriate log source. If you do not want to define a custom log source identifier for events, clear the checkbox. When this option is not selected and **Log Source Identifier Pattern** is not configured, QRadar receives events as unknown generic log sources.
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Log Source Identifier Pattern	Use the **Use As A Gateway Log Source** option to define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Enable Multiline	Aggregate multiple messages into single events based on a Start/End Matching or an ID-Linked regular expression.

Table 91. TLS Syslog protocol parameters (continued)	
Parameter	**Description**
Aggregation Method	This parameter is available when **Enable Multiline** is turned on. • **ID-Linked** - Processes event logs that contain a common value at the beginning of each line. • **Start/End Matching** - Aggregates events based on a start or end regular expression (regex).
Event Start Pattern	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **Start/End Matching**. The regular expression (regex) is required to identify the start of a TCP multiline event payload. Syslog headers typically begin with a date or timestamp. The protocol can create a single-line event that is based on solely on an event start pattern, such as a timestamp. When only a start pattern is available, the protocol captures all the information between each start value to create a valid event.
Event End Pattern	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **Start/End Matching**. This regular expression (regex) is required to identify the end of a TCP multiline event payload. If the syslog event ends with the same value, you can use a regular expression to determine the end of an event. The protocol can capture events that are based on solely on an event end pattern. When only an end pattern is available, the protocol captures all the information between each end value to create a valid event.
Message ID Pattern	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **ID-Linked**. This regular expression (regex) required to filter the event payload messages. The TCP multiline event messages must contain a common identifying value that repeats on each line of the event message.
Time Limit	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **ID-Linked**. The number of seconds to wait for more matching payloads before the event is pushed into the event pipeline. The default is 10 seconds.
Retain Entire Lines during Event Aggregation	This parameter is available when **Enable Multiline** is turned on and the **Aggregation Method** is set to **ID-Linked**. If you set the **Aggregation Method** parameter to **ID-Linked**, you can enable **Retain Entire Lines during Event Aggregation** to discard or keep the part of the events that precedes **Message ID Pattern**. You can enable this function only when concatenating events with the same ID pattern together.
Flatten Multiline Events Into Single Line	This parameter is available when **Enable Multiline** is turned on. Shows an event in one single line or multiple lines.

Table 91. TLS Syslog protocol parameters (continued)	
Parameter	**Description**
Event Formatter	This parameter is available when **Enable Multiline** is turned on. Use the **Windows Multiline** option for multiline events that are formatted specifically for Windows.

After the log source is saved, a syslog-tls certificate is created for the log source. The certificate must be copied to any device on your network that is configured to forward encrypted syslog. Other network devices that have a syslog-tls certificate file and the TLS listen port number can be automatically discovered as a TLS Syslog log source.

TLS Syslog use cases

The following use cases represent possible configurations that you can create:

Client Certificate on Disk
You can supply a client-certificate that enables the protocol to engage in client-authentication. If you select this option and provide the certificate, incoming connections are validated against the client-certificate.

CN Allowlist and Issuer Verification

If you selected this option, you must copy the issuer certificate (with the `.crt`, `.cert`, or `.der` file extensions) to the following directory:

`/opt/qradar/conf/trusted_certificates`

This directory is on the Target Event Collector that the log source is assigned to.

Any incoming client certificate is verified by the following methods to check whether the certificate was signed by the trusted issuer and other checks. You can choose one or both methods for client certificate authentication:

CN Allowlist

Provide an allowlist of trusted client certificate common names. You can enter plain text or a regular expression. Define multiple entries by entering each on a new line.

Issuer Verification

Provide a trusted client certificate's root or intermediate issuer certificate, or a public key in PEM format.

Check Certificate Revocation

Checks certificate revocation status against the client certificate. This option needs network connectivity to the URL that is specified by the **CRL Distribution Points** field in the client certificate for the X509v3 extension.

Check Certificate Usage

Checks the contents of the certificate X509v3 extensions in the **Key Usage** and **Extended Key Usage** extension fields. For incoming client certificate, the allow values of X509v3 Key Usage are `digitalSignature` and `keyAgreement`. The allow value for X509v3 Extended Key Usage is TLS `Web Client Authentication`.

User-provided Server Certificates
You can configure your own server certificate and corresponding private key. The configured TLS Syslog provider uses the certificate and key. Incoming connections are presented with the user-supplied certificate, rather than the automatically generated TLS Syslog certificate.

Default authentication

To use the default authentication method, use the default values for the **Authentication Mode** and **Certificate Type** parameters. After the log source is saved, a `syslog-tls` certificate is created for log source device. The certificate must be copied to any device on your network that forwards encrypted syslog data.

Related concepts

"Gateway log source" on page 15

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

Multiple log sources over TLS Syslog

You can configure multiple devices in your network to send encrypted Syslog events to a single TLS Syslog listen port. The TLS Syslog listener acts as a gateway, decrypts the event data, and feeds it within QRadar to extra log sources configured with the Syslog protocol.

When using the TLS Syslog protocol, there are specific parameters that you must use.

Multiple devices within your network that support TLS-encrypted Syslog can send encrypted events via a TCP connection to the TLS Syslog listen port. These encrypted events are decrypted by the TLS Syslog (gateway) and are injected into the event pipeline. The decrypted events get routed to the appropriate receiver log sources or to the traffic analysis engine for autodiscovery.

Events are routed within QRadar to log sources with a **`Log Source Identifier`** value that matches the source value of an event. For Syslog events with an RFC3164-, or RFC5425-, or RFC5424-compliant Syslog header, the source value is the IP address or the host name from the header. For events that do not have a compliant header, the source value is the IP address of the device that sent the Syslog event.

On QRadar, you can configure multiple log sources with the Syslog protocol to receive encrypted events that are sent to a single TLS Syslog listen port from multiple devices.

Note: Most TLS-enabled clients require the target server or listener's public certificate to authenticate the server's connection. By default, a TLS Syslog log source generates a certificate that is named **`syslog-tls.cert`** in `/opt/qradar/conf/trusted_certificates/` on the target Event Collector that the log source is assigned to. This certificate file must be copied to all clients that are making a TLS connection.

To add a log source over TLS Syslog, go to Adding a log source.

Note: You need to repeat the procedure for adding a log source for each device in your network. You can also add multiple receiver log sources in bulk from the **Log Sources** window. See Adding bulk log sources.

Related information

Adding a log source

UDP multiline syslog protocol configuration options

To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

The UDP multiline syslog protocol is an inbound/passive protocol. The original multiline event must contain a value that repeats on each line in order for a regular expression to capture that value and identify and reassemble the individual syslog messages that make up the multiline event. For example, this multiline event contains a repeated value, 2467222, in the conn field. This field value is captured so that all syslog messages that contain conn=2467222 are combined into a single event.

```
15:08:56 <IP_address> slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 <IP_address> slapd[517]: conn=2467222 op=2 SRCH base="dc=xxx"
15:08:56 <IP_address> slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 <IP_address> slapd[517]: conn=2467222 op=1 SRCH base="dc=xxx"
```

The following table describes the protocol-specific parameters for the UDP multiline syslog protocol:

Table 92. UDP multiline syslog protocol parameters	
Parameter	**Description**
Protocol Configuration	**UDP Multiline Syslog**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured UDP multiline syslog log source, ensure that you give each one a unique name.
Listen Port	The default port number that is used by QRadar to accept incoming UDP Multiline Syslog events is 517. You can use a different port in the range 1 - 65535. To edit a saved configuration to use a new port number, complete the following steps: 1. In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events. 2. Click **Save**. 3. Click **Deploy Changes** to make this change effective. The port update is complete and event collection starts on the new port number.
Message ID Pattern	The regular expression (regex) required to filter the event payload messages. The UDP multiline event messages must contain a common identifying value that repeats on each line of the event message.
Event Formatter	The event formatter that formats incoming payloads that are detected by the listener. Select **No Formatting** to leave the payload untouched. Select **Cisco ACS Multiline** to format the payload into a single-line event. In ACS syslog header, there are `total_seg` and `seg_num` fields. These two fields are used to rearrange ACS multiline events into a single-line event with correct order when you select the Cisco ACS Multiline option.
Show Advanced Options	The default is **No**. Select **Yes** if you want to configure advanced options.
Use Custom Source Name	Select the check box if you want to customize the source name with regex.

Table 92. UDP multiline syslog protocol parameters (continued)

Parameter	Description
Source Name Regex	Use the **Source Name Regex** and **Source Name Formatting String** parameters if you want to customize how QRadar determines the source of the events that are processed by this UDP Multiline Syslog configuration. For **Source Name Regex**, enter a regex to capture one or more identifying values from event payloads that are handled by this protocol. These values are used with the **Source Name Formatting String** to set a source or origin value for each event. This source value is used to route the event to a log source with a matching **Log Source Identifier** value when the **Use As A Gateway Log Source** option is enabled.
Source Name Formatting String	You can use a combination of one or more of the following inputs to form a source value for event payloads that are processed by this protocol: • One or more capture groups from the **Source Name Regex**. To refer to a capture group, use \x notation where x is the index of a capture group from the **Source Name Regex**. • The IP address from which the event data originated. To refer to the packet IP, use the token PIP. • Literal text characters. The entire **Source Name Formatting String** can be user-provided text. For example, `CiscoACS\1\2$PIP$`, where `\1\2` means first and second capture groups from the **Source Name Regex** value, and PIP is the packet IP.
Use As A Gateway Log Source	If this check box is clear, incoming events are sent to the log source with the **Log Source Identifier** matching the IP that they originated from. When checked, this log source serves as a single entry point or gateway for multiline events from many sources to enter QRadar and be processed in the same way, without the need to configure a UDP Multiline Syslog log source for each source. Events with an RFC3164- or RFC5424-compliant syslog header are identified as originating from the IP or host name in their header, unless the **Source Name Formatting String** parameter is in use, in which case that format string is evaluated for each event. Any such events are routed through QRadar based on this captured value. If one or more log sources exist with a corresponding **Log Source Identifier**, they are given the event based on configured Parsing Order. If they do not accept the event, or if no log sources exist with a matching **Log Source Identifier**, the events are analyzed for autodetection.
Flatten Multiline Events Into Single Line	Shows an event in one single line or multiple lines. If this check box is selected, all newline and carriage return characters are removed from the event.

Table 92. UDP multiline syslog protocol parameters (continued)	
Parameter	**Description**
Retain Entire Lines During Event Aggregation	Choose this option to either discard or keep the part of the events that comes before **Message ID Pattern** when the protocol concatenates events with same ID pattern together.
Time Limit	The number of seconds to wait for additional matching payloads before the event is pushed into the event pipeline. The default is 10 seconds.
Enabled	Select this check box to enable the log source.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the Event Collector in your deployment that should host the UDP Multiline Syslog listener.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the Coalescing Events list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related concepts

"Gateway log source" on page 15

Use a gateway log source to configure a protocol to use many Device Support Modules (DSMs) instead of relying on a single DSM type. With a gateway log source, event aggregator protocols can dynamically handle various event types.

VMware vCloud Director protocol configuration options

To collect events from VMware vCloud Director virtual environments, create a log source that uses the VMware vCloud Director protocol, which is an active outbound protocol.

The following table describes the protocol-specific parameters for the VMware vCloud Director protocol:

Table 93. VMware vCloud Director protocol parameters

Parameter	Description
Log Source Identifier	The log source name can't include spaces and must be unique among all log sources of this type that are configured with the VMware vCloud Director protocol.
Protocol Configuration	**VMware vCloud Director**
vCloud URL	The URL that is configured on your VMware vCloud appliance to access the REST API. The URL must match the address that is configured as the **VCD public REST API base URL** field on the vCloud server. For example, `https://<my.vcloud.server>/api`
User Name	The username that is required to remotely access the vCloud server. For example, `console/user@organization` If you want to configure a read-only account to use with IBM QRadar, create a vCloud user in your organization that has the **Console Access Only** permission.
Password	The password that is required to remotely access the vCloud Server.
Polling Interval (in seconds)	The amount of time between queries to the vCloud server for new events. The default polling interval is 10 seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Enable Advanced Options	Enable this option to configure more parameters.
API PageSize	The number of records to return per API call. The maximum is 128. If you select **Enable Advanced Options**, this parameter is displayed.
vCloud API Version	The vCloud version that is used in your API request. This version must match a version that is compatible with your vCloud installation. Use the following examples to help you determine which version is compatible with your vCloud installation: • vCloud API 33.0 (vCloud Director 10.0) • vCloud API 32.0 (vCloud Director 9.7) • vCloud API 31.0 (vCloud Director 9.5) • vCloud API 30.0 (vCloud Director 9.1) • vCloud API 29.0 (vCloud Director 9.0) If you select **Enable Advanced Options**, this parameter is displayed.

Table 93. VMware vCloud Director protocol parameters (continued)	
Parameter	**Description**
Allow Untrusted Certificates	When you connect to vCloud 5.1 or later, you must enable this option to allow self-signed, untrusted certificates. The certificate must be downloaded in PEM or DER encoded binary format and then placed in the `/opt/qradar/conf/trusted_certificates/` directory with a `.cert` or `.crt` file extension. If you select **Enable Advanced Options**, this parameter is displayed.
Use Proxy	If the server is accessed by using a proxy, select the **Use Proxy** checkbox. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field. If you select **Enable Advanced Options**, this parameter is displayed.
Proxy IP or Hostname	If you select **Use Proxy**, this parameter is displayed.
Proxy Port	If you select **Use Proxy**, this parameter is displayed. The port number that is used to communicate with the proxy. The default is 8080.
Proxy Username	If you select **Use Proxy**, this parameter is displayed.
Proxy Password	If you select **Use Proxy**, this parameter is displayed.

Chapter 10. Universal Cloud REST API protocol

The Universal Cloud REST API protocol is an outbound, active protocol for IBM QRadar. You can customize the Universal Cloud REST API protocol to collect events from various REST APIs, including data sources that do not have a specific DSM or protocol.

The Universal Cloud REST API protocol behavior is defined by a workflow XML document. You can create your own XML document, or you can get it from IBM Fix Central, or from third parties on GitHub.

Important: The Universal Cloud REST API protocol is supported on QRadar 7.3.2 or later, and the QRadar Log Source Management app must be installed. For more information about how to install the app, see Installing the QRadar Log Source Management app.

For Universal Cloud REST API protocol examples, see GitHub samples (https://github.com/ibm-security-intelligence/IBM-QRadar-Universal-Cloud-REST-API).

Tip: IBM supports only the workflows that are directly referenced in the *DSM Configuration Guide*. The workflows on GitHub can be used as educational resources but are not supported by IBM.

The following table describes the protocol-specific parameters for the Universal Cloud REST API protocol.

Table 94. Universal Cloud REST API protocol parameters

Parameter	Description
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the **Log Source Name**. If you have more than one configured Universal Cloud REST API log source, ensure that you give each one a unique name.
Workflow	The XML document that defines how the protocol instance collects events from the target API. For more information, see “Workflow” on page 241.
Workflow Parameter Values	The XML document that contains the parameter values used directly by the workflow. For more information, see “Workflow Parameter Values” on page 242.

Table 94. Universal Cloud REST API protocol parameters (continued)	
Parameter	**Description**
Allow Untrusted Certificates	If you enable this parameter, the protocol can accept self-signed and otherwise untrusted certificates that are located within the `/opt/qradar/conf/trusted_certificates/` directory. If you disable the parameter, the scanner trusts only certificates that are signed by a trusted signer. The certificates must be in PEM or RED-encoded binary format and saved as a `.crt` or `.cert` file. If you modify the workflow to include a hardcoded value for the **Allow Untrusted Certificates** parameter, the workflow overrides your selection in the UI. If you do not include this parameter in your workflow, then your selection in the UI is used.
Use Proxy	If the API is accessed by using a proxy, select this checkbox. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Recurrence	Specify how often the log collects data. The value can be in Minutes (M), Hours (H), or Days (D). The default is 10 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Related concepts

“Workflow” on page 241

The Workflow is an XML document that describes the event retrieval process. The Workflow defines one or more parameters, which can be explicitly assigned values in the Workflow XML or can derive values from the Workflow parameter values XML document. The Workflow consists of multiple actions that run sequentially. When you run the Workflow, the parameter values are added to the State, and the State can then be accessed and changed by actions as the Workflow runs.

“Workflow Parameter Values” on page 242

The Workflow Parameter Values is an XML document that contains the input parameters of a workflow instance. It is a set of name/value pairs where the name must match one of the parameters defined in the associated workflow. The following table shows the Workflow Parameter Values parameters.

“State” on page 242

The State is a JSON object that represents the data of a running Workflow. Because the State is not strictly defined, data is dynamically stored in the State.

Workflow

The Workflow is an XML document that describes the event retrieval process. The Workflow defines one or more parameters, which can be explicitly assigned values in the Workflow XML or can derive values from the Workflow parameter values XML document. The Workflow consists of multiple actions that run sequentially. When you run the Workflow, the parameter values are added to the State, and the State can then be accessed and changed by actions as the Workflow runs.

The following table shows the Workflow attributes.

Table 95. Workflow attributes

Name	Description	Required
name	The name of the Workflow.	Yes
description	The description of the Workflow.	No
version	The version of the Workflow.	Yes
minimumRecurrence	The minimum recurrence allowed for a Workflow in seconds. You can set this attribute for APIs that have a minimum amount of time between requests.	No

Parameters

Use the Workflow actions to access the parameter values. Parameters mostly consist of authentication credentials, but can be used for anything that you want the user to configure. The following table shows the Workflow parameters.

Table 96. Workflow parameters

Name	Data type	Description
name	String	The name of the parameter. The name must match the corresponding name value in the parameter values XML.
label	String	The display name of the parameter.
description	String	The description of the parameter.
required	Boolean	Indicates whether the parameter is required.
secret	Boolean	Indicates whether the parameter is confidential, for example, a password.
default	String	The default value of the parameter. If you don't enter a value for this parameter in the parameter values XML, the default value is used.

XML Example

This example shows a workflow example which requires a host with a username and password, where <x> is the version of the workflow schema that you are using.

```
<Workflow name="Test" version="1.0" xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/Workflow/
V<x>">
    <Parameters>
        <Parameter name="host" label="Host" required="true" />
        <Parameter name="username" label="Username" required="true" />
        <Parameter name="password" label="Password" required="true" />
    </Parameters>
```

```
    <Actions>
        ...
    </Actions>
</Workflow>
```

Workflow Parameter Values

The Workflow Parameter Values is an XML document that contains the input parameters of a workflow instance. It is a set of name/value pairs where the name must match one of the parameters defined in the associated workflow. The following table shows the Workflow Parameter Values parameters.

Table 97. Workflow Parameter Values parameters

Name	Data type	Description	Required
name	String	The name of the parameter, as defined in the workflow	Yes
value	String	The value of the parameter, as defined in the workflow	No

XML Example

In this example, the `host` parameter is given the value "mycloud.com". The `username` parameter is given the value "admin". And the `password` parameter is given the value "password123."

```
<?xml version="1.0" encoding="UTF-8" ?>
<WorkflowParameterValues xmlns="http://qradar.ibm.com/UniversalCloudRESTAPI/
WorkflowParameterValues/V1">
    <Value name="host"      value="" />
    <Value name="username"  value="" />
    <Value name="password"  value="" />
</WorkflowParameterValues>
```

State

The State is a JSON object that represents the data of a running Workflow. Because the State is not strictly defined, data is dynamically stored in the State.

JSON can store almost any kind of data and allows data to be classified in subobjects. API responses are stored in JSON format and events are assembled to be sent to the pipeline in JSON.

Persistence
The State is persisted and is not lost during upgrades, restarts, and deployments of IBM QRadar.

Encryption
The State supports encryption to prevent sensitive data from being displayed.

Querying
The State can be queried with JPath, which is a JSON query language that is similar to XPath for XML. For more information, see “JPath” on page 263.

Template Strings
A template string is a string that can contain JPath expressions. JPath expressions are referenced by using the `${...}` syntax. For more information, see “JPath” on page 263.

Example

You can use JPath expressions to determine a result from the following State.

```
{
    "some":
    {
        "value": 123
    }
}
```

The following table shows JPath expressions and their results.

Table 98. Template string examples

Description	Template string	Result
Simple value reference	"The value is ${/some/value}"	"The value is 123"
Arithmetic	"The value is ${/some/value * 2}"	"The value is 246"
Logical operations	"The expression is ${/some/value > 12}"	"The expression is true"
Built-in function	"The current time is ${time()}ms since epoch"	"The current time is 1586968388123ms since epoch"

Actions

Actions are the building blocks of the workflow. Each action has a specific purpose, such as calling HTTP endpoints, or posting events to the QRadar pipeline.

Abort

The Abort action aborts the workflow.

The workflow is aborted immediately, in error. If the terminate flag is false, the workflow resumes on the next recurrence, otherwise it stops until either the event collection service is restarted, or the log source is edited.

The following table shows the parameters for the Abort action.

Table 99. Abort action parameters

Name	Data type	Required	Notes
reason	String	Yes	The reason why the workflow was aborted. This string displays in the log source status as an error message.
terminate	Boolean	No	Indicates whether the event retrieval loop is terminated. The default is False. Use this parameter only in extreme situations. The parameter puts the log source in error and stops it completely. The log source restarts only when the event collection service is restarted, or if the log source is edited. You can use the terminate parameter to stop the workflow on authentication failure to prevent account lockouts.

XML Example:

This action stops the current execution of the workflow, but it runs again on the next recurrence. Until the log source status is cleared or updated, it includes the following error message:

```
The password for <user value> has expired.
```

```
<Abort reason="The password for '${/user}' has expired." />
```

Add

The Add action adds a value to an array in the State.

The following table shows the parameters for the Add action.

Table 100. Add action parameters

Name	Data type	Required	Notes
path	JPath	Yes	The location of the array. The path must reference an array value.
value	String/Number	Yes	

XML Example:

This action adds the string "V2hhdCBhIHdvbmRlcmZ1bCB3b3JsZC4uLg==" to the State at location `/tokens`.

```
<Add path="/tokens" value="V2hhdCBhIHdvbmRlcmZ1bCB3b3JsZC4uLg==" />
```

CallEndpoint

The CallEndpoint action calls an HTTP endpoint.

The following table shows the parameters for the CallEndpoint action.

Table 101. CallEndpoint action parameters

Name	Data type	Relationship	Required	Notes
method	Enumeration	Attribute	Yes	Possible values: • GET • POST • PUT • DELETE • PATCH
url	String	Attribute	Yes	The base URL of the endpoint (excluding the query parameters).

Table 101. CallEndpoint action parameters (continued)

Name	Data type	Relationship	Required	Notes
savePath	String	Attribute	No	The response is stored as a JSON object with the following format: **/response** { status_code: 200, status_message: "OK", headers: { "Date": "Tue, 16 Jun 2020 17:31:29 GMT", "Content-Type": "application/json", }, body: ... } If you do not provide a savePath value, the endpoint response is not saved in a default location. A savePath value must be provided if you want to store the response.
sslConfiguration	SSLConfiguration	Subelement	No	For more information, see SSLConfiguration.
authentication	Authentication	Subelement	No	An Authentication object must be one of the following types: • BasicAuthentication • BearerAuthentication • DigestAuthentication • New in V2 Akamai EdgeGrid Authentication • New in V2 Hawk Authentication
queryParameters	QueryParameter	Subelement	No	You can have more than one query parameter. For more information, see QueryParameter.
requestHeaders	RequestHeaders	Subelement	No	You can have more than one request header. For more information, see RequestHeader.

Table 101. CallEndpoint action parameters (continued)				
Name	**Data type**	**Relationship**	**Required**	**Notes**
body	RequestBody UrlEncodedFormRequestBody XmlRequestBody	Subelement	No	The body must be one of the following types: • RequestBody • UrlEncodedFormRequestBody • XmlRequestBody

The following table shows the parameters for SSLConfiguration.

Table 102. SSLConfiguration structure			
Name	**Data type**	**Required**	**Notes**
protocol	String	No	The SSL protocol to use. The default is TLSv1.2.
allowUntrustedServerCertificate	Boolean	No	Indicates whether untrusted server certificates are allowed. The default is False.

XML Example:

This example allows an untrusted server certificate.

```
<SSLConfiguration allowUntrustedServerCertificate="true" />
```

The following table shows the parameters for BasicAuthentication.

Table 103. BasicAuthentication structure		
Name	**Data type**	**Required**
username	String	Yes
password	String	No

XML Example:

This example sets an authentication username and password.

```
<BasicAuthentication username="${/username}" password="${/password}" />
```

The following table shows the parameters for BearerAuthentication.

Table 104. BearerAuthentication structure			
Name	**Data type**	**Required**	**Notes**
token	String	Yes	The access token.

XML Example:

This example sets an access token for authentication.

```
<BearerAuthentication token="${/access_token}" />
```

The following table shows the parameters for DigestAuthentication.

Table 105. DigestAuthentication structure		
Name	**Data type**	**Required**
username	String	Yes
password	String	Yes
realm	String	No
nonce	String	No
algorithm	String	No
qop	String	No
cnonce	String	No
nonceCount	String	No

XML Example:

This example sets a username and password for authentication.

```
<DigestAuthentication username="${/public_key}" password="${/private_key}" />
```

New in V2

The following table shows the parameters for Akamai EdgeGrid authentication.

Table 106. Akamai EdgeGrid authentication structure		
Name	**Data type**	**Required**
accessToken	String	Yes
clientToken	String	Yes
clientSecret	String	Yes

New in V2

The following table shows the parameters for Hawk authentication.

Table 107. Hawk authentication structure		
Name	**Data type**	**Required**
keyID	String	Yes
key	String	Yes
algorithm	String	Yes
hash	String	No
ext	String	No
app	String	No
dlg	String	No

The following table shows the parameters for QueryParameter.

Table 108. QueryParameter structure			
Name	**Data type**	**Required**	**Notes**
name	String	Yes	

Table 108. QueryParameter structure (continued)			
Name	**Data type**	**Required**	**Notes**
value	String	Yes	
omitIfEmpty	Boolean	No	Omits the parameter if the value is empty.

XML Example:

This example sets a name and value for a query, and omits the parameter if the value is empty.

```
<QueryParameter name="stream_position" value="${/bookmark}" omitIfEmpty="true" />
```

The following table shows the parameters for RequestHeader.

Table 109. RequestHeader structure			
Name	**Data type**	**Required**	**Notes**
name	String	Yes	
value	String	No	
omitIfEmpty	Boolean	No	Omits the header if the value is empty.

XML Example:

This example sets a name and value for a request header.

```
<RequestHeader name="authorization" value="client_id:${/client_id}, client_secret:${/
client_secret}" />
```

The following table shows the parameters for RequestBody.

Table 110. RequestBody structure			
Name	**Data type**	**Required**	**Notes**
type	String	Yes	Must be a valid HTTP request content-type. For example, application/json.
encoding	String	Yes	Must be a valid HTTP body encoding type. For example, UTF-8.
content	String	Yes	Include the body content between the opening and closing tags of the **<RequestBody>** element.

XML Example:

This example sets a content-type, body encoding, and content for a request body.

```
<RequestBody type="application/json" encoding="UTF-8">{ "grant_type": "client_credentials" }</
RequestBody>
```

The following table shows the parameters for UrlEncodedFormRequestBody.

Table 111. UrlEncodedFormRequestBody structure			
Name	**Data type**	**Required**	**Notes**
parameters	Map <String, String>	Yes	A collection of name/value pairs.

XML Example:

This example sets the name/value pairs for a URL encoded form request body.

```
<UrlEncodedFormRequestBody>
                <Parameter name="grant_type" value="urn:ietf:params:oauth:grant-type:jwt-
bearer" />
                <Parameter name="client_id" value="${/client_id}" />
                <Parameter name="client_secret" value="${/client_secret}" />
                <Parameter name="assertion" value="${/jwt_assertion}" />
            </UrlEncodedFormRequestBody>
```

The following table shows the parameters for XmlRequestBody.

Table 112. XmlRequestBody structure			
Name	**Data type**	**Required**	**Notes**
type	String	No	Must be a valid HTTP request content-type. For example, application/json.
encoding	String	No	Must be a valid HTTP body encoding type. For example, UTF-8.
content	XML	Yes	The actual XML content of the body must be nested within the **<XmlRequestBody>** element as subelements.

XML Example:

This example sets the content for an XML request body.

```
<XmlRequestBody>
                <authRequest>
                    <maaS360AdminAuth>
                        <billingID>${/billing_id}</billingID>
                        <platformID>${/platform_id}</platformID>
                        <appID>${/app_id}</appID>
                        <appVersion>${/app_version}</appVersion>
                        <appAccessKey>${/app_access_key}</appAccessKey>
                        <userName>${/username}</userName>
                        <password>${/password}</password>
                    </maaS360AdminAuth>
                </authRequest>
            </XmlRequestBody>
```

XML Example:

This action calls makes a POST request to https://${/host}/auth/oauth2/token with a request header and a request body, and saves the response in the State at `/get_access_token`.

```
<CallEndpoint url="https://${/host}/auth/oauth2/token" method="POST" savePath="/
get_access_token">
    <RequestHeader name="authorization" value="client_id:${/client_id}, client_secret:${/
client_secret}" />
    <RequestBody type="application/json" encoding="UTF-8">{ "grant_type":
"client_credentials" }</RequestBody>
</CallEndpoint>
```

ClearStatus

The ClearStatus action clears the runtime status of the protocol instance. This clears the status of the log source.

XML Example

This action clears any info, warning or error messages that are displayed for the log source.

```
<ClearStatus />
```

Copy

The Copy action copies one part of the State to another.

The following table shows the parameters for the Copy action.

Table 113. Copy action parameters

Name	Data type	Required	Notes
sourcePath	JPath	Yes	The path to copy. This path can be either a static path or a query.
targetPath	JPath	Yes	The location to which the path is copied. This path overwrites anything that is stored at this location.

XML Example

This action copies the objects from the array at `/events` with a **type_id** of 4 to an array at location `/interestingEvents`, and erasing anything that was stored there previously.

```
<Copy sourcePath="/events[@type_id = 4]" targetPath="/interestingEvents" />
```

Create JWTAccessToken

The JWTAccessToken action creates a JSON Web Token (JWT).

For more information, see JWT documentation.

The following table shows the parameters for the Create JWTAccessToken action.

Table 114. Create JWTAccessToken action parameters

Name	Data type	Relationship	Required	Notes®
Header	KeyValuePairs	Subelement	Yes	The set of name/value pairs that form the JWT header. For more information, see Table 115 on page 251
Payload	KeyValuePairs	Subelement	Yes	The set of name/value pairs that form the JWT payload. For more information, seeTable 116 on page 251

Table 114. Create JWTAccessToken action parameters (continued)				
Name	**Data type**	**Relationship**	**Required**	**Notes®**
Secret	String	Subelement	Yes	In V1, the Secret must be a Base64 PKCS8 PEM file. In V2 or later, it can be either a PVKS1 or PVKS8 PEM file, and can be entered as plain text or Base64 encoded. For more information, see Table 117 on page 251
savePath	JPath	Attribute	Yes	The location in the state to store this value.

Table 115. Header structure				
Name	**Data type**	**Description**	**Required**	**Notes**
name	String	The name of the header.	Yes	
value	String	The value of the header.	No	

Table 116. Payload structure				
Name	**Data type**	**Description**	**Required**	**Notes**
name	String	The name of the payload.	Yes	
value	String	The value of the payload.	No	

Table 117. Secret structure				
Name	**Data type**	**Description**	**Required**	**Notes**
value	String	The value of the secret.	No	

XML Example

This action creates a JWT with the provided header, payload and secret values, and saves it in the State at location `/access_token`.

```
<CreateJWTAccessToken savePath="/access_token">
    <Header>
        <Value name="alg" value="HS256" />
        <Value name="typ" value="JWT" />
    </Header>
    <Payload>
        <Value name="iss" value="${/api_key}" />
    </Payload>
    <Secret value="${/api_secret}" />
</CreateJWTAccessToken>
```

Delete

The Delete action deletes an element from the State.

The following table shows the parameters for the Delete action.

Table 118. Delete action parameters			
Name	**Data type**	**Required**	**Notes**
path	JPath	Yes	The location of the element to delete.

XML Example

This action deletes the value that exists in the State at location `/token`

```
<Delete path="/token" />
```

DoWhile

The DoWhile action loops a series of actions while a condition is true.

The condition is evaluated at the end of the loop. Even if the condition is never true, the contents are executed once. This action is different from the While action, where the condition is evaluated at the beginning of the loop.

The following table shows the parameters for the DoWhile action.

Table 119. DoWhile action parameters			
Name	**Data type**	**Required**	**Notes**
condition	JPath	Yes	The condition that determines whether to continue looping.
actions	JPath Condition	Yes	Must be a JPath expression that resolves to a value of `true` or `false`. References to the State should not be within the `${}` notation for JPath conditions. See "JPath" on page 263

XML Example

This action executes the nested CallEndpoint action and PostEvent action. If there is a value in the State at location `/next_page` the condition is true and the nested actions are executed, and the condition check is performed until the condition is false.

```
<DoWhile condition="/next_page != null">
    <CallEndpoint ... />
    <PostEvent path="/current/event" />
</DoWhile>
```

ForEach

The ForEach action executes a series of actions for each value in an array or object. In V1, the action works only for each value in an array.

The following table shows the parameters for the ForEach action.

Table 120. ForEach action parameters				
Name	**Data type**	**Description**	**Required**	**Notes**
item	JPath	The path to store the current item of the iteration.	Yes	The path to store the current item of the iteration.

Table 120. ForEach action parameters (continued)				
Name	**Data type**	**Description**	**Required**	**Notes**
items	JPath	The array in the State to iterate.	Yes	The array in the State to iterate.
actions	Actions[]	The sequence of actions to execute for each iteration.	Yes	The sequence of actions to execute for each iteration. Cannot be empty.

XML Example

An array of objects exists in the State at `/events`. This action iterates through the array and executes the nested PostEvent action for each object in the array.

```
<ForEach item="/current_event" items="/events">
  <PostEvent path="/current_event" source="${/host}" />
</ForEach>
```

FormatDate

The FormatDate action formats a UNIX timestamp to a date.

The following table shows the parameters for the FormatDate action.

Table 121. FormatDate action parameters			
Name	**Data type**	**Required**	**Notes**
pattern	String	Yes	See Java DateTimeFormatter for possible values.
timeZone	String	No	See Java DateTimeFormatter for possible values.
time	Number	No	The time to format, in milliseconds since epoch. The default is the current time.
savePath	JPath	Yes	The location to store the result.

XML Example

This action extracts the UNIX timestamp currently stored in the State at `/bookmark` and converts it to a meaningful timestamp in the following format in the UTC time zone.

```
yyyy-MM-dd'T'HH:mm:ss.SSS'Z'
```

```
<FormatDate pattern="yyyy-MM-dd'T'HH:mm:ss" timeZone="UTC" time="${/bookmark}"
savePath="/formatted_bookmark" />
```

The reformatted value is saved in the State at `/formatted_bookmark`.

GenerateHMAC

The GenerateHMAC action applies an HMAC hash to a given input.

The following table shows the parameters for the GenerateHMAC action.

Table 122. GenerateHMAC action parameters			
Name	**Data type**	**Required**	**Notes**
algorithm	Enumeration	Yes	Possible values: • MD5 • SHA1 • SHA256 • SHA512
secretKey	String	Yes	The secret to use.
message	String	Yes	The input message to process.
saveFormat	String	Yes	Possible values: • BASE64 • HEX
savePath	JPath	Yes	The location to store the result.

XML Example

This action generates an HMAC hash of the value stored in the State at `/value` . The hash is generated in hex format by using the SHA1 algorithm and the provided **secretKey**, and is saved in the State at location `/signature`.

```
<GenerateHMAC algorithm="SHA1" secretKey="${/secret_key}" message="${/value}" saveFormat="HEX"
savePath="/signature" />
```

If/ElseIf/Else

The If/ElseIf/Else actions execute actions if a condition is satisfied.

The If/ElseIf/Else actions execute nested actions based on one or more mutually-exclusive conditions:

- "If" conditions are always checked.
- "ElseIf" conditions are only checked if all preceding "If" and "ElseIf" conditions were not satisfied.
- "Else" actions have no condition; if none of the preceding "If" or "ElseIf" conditions were satisfied, the "Else" actions are automatically executed.

The following table shows the parameters for the If action.

Table 123. If action parameters			
Name	**Data type**	**Required**	**Notes**
condition	JPath	Yes	The condition to evaluate. Cannot be empty.
actions	Actions[]	Yes	The sequence of actions to execute if the condition is true. Cannot be empty.

The following table shows the parameters for the ElseIf action.

Table 124. ElseIf action parameters			
Name	**Data type**	**Required**	**Notes**
condition	JPath	Yes	The condition to evaluate. Cannot be empty.
actions	Actions[]	Yes	The sequence of actions to execute if the condition is true. Cannot be empty.

The following table shows the parameters for the Else action.

Table 125. Else action parameters			
Name	**Data type**	**Required**	**Notes**
actions	Actions[]	Yes	The sequence of actions to execute if none of the preceding "If" or "ElseIf" conditions are true. Cannot be empty.

XML Example

In this example, the following actions are taken:

- If the State value at location `/status` is 200, only the SetStatus action that sets the status to an INFO "Success" message is executed.
- If the `/status` value is 401, only the SetStatus action that sets the status to an ERROR "Authentication Failure" message is executed.
- If the `/status` value is 404, only the SetStatus action that sets the status to an ERROR "No Route Exists" message is executed.
- If the `/status` value is anything else, only the final SetStatus action is executed.

```
<If condition="/status = 200">
    <SetStatus type="INFO" message="Success." />
</If>
<ElseIf condition="/status = 401">
    <SetStatus type="ERROR" message="Authentication Failure." />
</ElseIf>
<ElseIf condition="/status = 404">
    <SetStatus type="ERROR" message="No Route Exists." />
</ElseIf>
<Else>
    <SetStatus type="ERROR" message="An unknown error (${/status}) has occurred." />
</Else>
```

Initialize

The Initialize action initializes a value in the State.

If a value exists in the location, the new value does not override the existing value.

Table 126. Initialize action parameters			
Name	**Data type**	**Required**	**Notes**
path	JPath	Yes	The location to initialize.
value	String/Number	Yes	The value to set.

XML Example

This action adds the value "1" to the State at location /bookmark, if no value exists at that location. If a value does exist at that location, the action does nothing.

```
<Initialize path="/bookmark" value="1" />
```

Log

The Log action logs troubleshooting messages.

Troubleshooting messages are typically stored in the QRadar log files at /var/log/qradar.error, var/log/qradar.log, and /var/log/qradar.java.debug

The following table shows the parameters for the Log action.

Table 127. Log action parameters

Name	Data type	Required	Notes
type	Enumeration	Yes	The log type. Possible values: • INFO • WARN • ERROR • DEBUG
message	String	Yes	The message to log.

XML Example

This action writes a DEBUG level log to the QRadar logs that contain the specified message.

```
<Log type="DEBUG" message="The value was ${/some_value}." />
```

Merge

The Merge action merges an array into an array, or an object into an object.

The following table shows the parameters for the Merge action.

Table 128. Merge action parameters

Name	Data type	Required	Notes
sourcePath	JPath	Yes	The object or array to copy from.
targetPath	JPath	Yes	The object or array to merge into.

XML Example:

This action copies all objects that have a type_id value of 4 in the array at location /events in the State to the array at /cumulativeEvents. Any objects already in /cumulativeEvents are preserved.

```
<Merge sourcePath="/events[@type_id = 4]" targetPath="/cummulativeEvents" />
```

ParseDate

The ParseDate action parses a date into a UNIX timestamp.

The ParseDate action is supported by the Java DateTimeFormatter. Some of the ParseDate action parameters are passed directly to Java.

The following table shows the parameters for the ParseDate action.

Table 129. ParseDate action parameters

Name	Data type	Required	Notes
pattern	String	Yes	The formatting pattern to use. See Java DateTimeFormatter for possible values.
timeZone	String	No	The time zone to use. See Java DateTimeFormatter for possible values.
date	String	Yes	The formatted date to parse.
savePath	JPath	Yes	The location to store the result.

XML Example:

This action converts the timestamp that is stored in the State at location `/formatted_time` to a UNIX timestamp and stores it in the State at location `/timestamp`. The current timestamp must be in the yyyy-MM-dd'T'HH:mm:ss'Z' format and represent a time in the Coordinated Universal Time (UTC) zone.

```
<ParseDate pattern="yyyy-MM-dd'T'HH:mm:ss" timeZone="UTC" time="${/formatted_time}"
savePath="/timestamp" />
```

PostEvent

The PostEvent action posts an event to the QRadar event pipeline, which allows the event to be parsed, correlated, and stored.

The following table shows the parameters for the PostEvent action.

Table 130. PostEvent action parameters

Name	Data type	Required	Notes
path	JPath	Yes	The path of the element to post.
encoding	String	No	The encoding of the event. Possible values: • UTF-8 • BASE64 • HEX The default is UTF-8.

Table 130. PostEvent action parameters (continued)			
Name	**Data type**	**Required**	**Notes**
source	String	Yes	The source (host) of the event. The source value is used to route the event within the event pipeline to the correct log source. The event is matched to the log source identifier of an existing log source. If no log source exists with a matching log source identifier, the event is stored without parsing and a copy of the event is sent to the log source autodetection engine. If a log source is autodetected from the event, it is created with its log source identifier set to the source value.

XML Example:

This action posts the string that is stored in the State at `/event` into the QRadar event pipeline as an event. If a log source has a log source identifier that matches the value that is stored in `/host`, the event is routed to that log source.

```
<PostEvent path="/event" source="${/host}" />
```

PostEvents

The PostEvents action posts an array of events to the QRadar event pipeline, which allows the events to be parsed, correlated, and stored.

The following table shows the parameters for the PostEvents action.

Table 131. PostEvents action parameters			
Name	**Data type**	**Required**	**Notes**
path	JPath	Yes	The path of the array element to post.
encoding	String	No	The encoding of the event. Possible values: • UTF-8 • BASE64 • HEX The default is UTF-8.

Table 131. PostEvents action parameters (continued)			
Name	**Data type**	**Required**	**Notes**
source	String	Yes	The source (host) of the event. The source value is used to route the event within the event pipeline to the correct log source. The event is matched to the log source identifier of an existing log source. If no log source exists with a matching log source identifier, the event is stored without parsing and a copy of the event is sent to the log source autodetection engine. If a log source is autodetected from the event, it is created with its log source identifier set to the source value.

XML Example:

This action posts the array of strings that are stored in the State at `/events` into the QRadar event pipeline as a series of events. If a log source has a log source identifier that matches the value that is stored in `/host`, the events are routed to that log source.

```
<PostEvents path="/events" host="${/host}" />
```

RegexCapture

The RegexCapture action captures part of a string with a regular expression (regex).

The following table shows the parameters for the RegexCapture action.

Table 132. RegexCapture action parameters			
Name	**Data type**	**Required**	**Notes**
pattern	RegEx	Yes	The regular expression pattern. The pattern must contain only one capture group. The regex pattern must be a Java-type regex. For more information, see Class Pattern (https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html).
value	String	Yes	The value to capture from.
savePath	JPath	Yes	The location to store the result.

XML Example:

This action runs the regex that is defined in the pattern to the string stored in the State as `/data`. The capture group value is stored in the State at location `/id`. The provided regex captures one or more digits that follow `"id="`.

```
<RegexCapture pattern="id=([0-9]+)" value="${/data}" savePath="/id" />
```

Set

The Set action sets a value in the State.

If a value exists at the location, the new value overrides the existing value.

The following table shows the parameters for the Set action.

Table 133. Set action parameters

Name	Data type	Required	Notes
path	JPath	Yes	The location to store the value.
value	String/Number	Yes	The value to set.

XML Example:

This action adds the value that is returned by the time() function to the State at location `/current_time`. If a value exists at that location, it is overwritten.

```
<Set path="/current_time" value="${time()}" />
```

SetStatus

The SetStatus action sets the runtime status of the protocol instance. This information appears in the status of the log source.

The following table shows the parameters for the SetStatus action.

Table 134. SetStatus action parameters

Name	Data type	Required	Notes
type	Enumeration	Yes	The status type. Possible values include: • INFO • WARN • ERROR
message	String	Yes	The status message.

XML Example:

This action sets the runtime status of the protocol instance to ERROR with a message that states:

`The password has expired`

This information is displayed as the log source status in the IBM QRadar Log Source Management app and API.

```
<SetStatus type="ERROR" message="The password has expired" />
```

Sleep

The Sleep action suspends the Workflow for a specified amount of time.

The following table shows the parameters for the Sleep action.

Table 135. Sleep action parameters			
Name	**Data type**	**Required**	**Notes**
duration	Number	Yes	The amount of time to wait, in milliseconds.

XML Example:

This action causes the Workflow to pause execution for 5 seconds.

```
<Sleep duration="5000" />
```

Split

The Split action splits a string.

For example, if an API returns a set of events as a long string, where each event is separated by a comma or other delimiter, you can split the string to use the PostEvent or PostEvents action.

The following table shows the parameters for the Split action.

Table 136. Split action parameters			
Name	**Data type**	**Required**	**Notes**
value	String	Yes	The value to split.
delimiter	String	No	The delimiter is a regex expression. Defaults to "newline". If a delimiter is supplied with regex elements, it must be a Java-type regex.
savePath	JPath	Yes	The location to store the result.

XML Example:

This action splits the string `"value 1,value 2,value 3"` into an array of three strings `"value1"`, `"value2"`, and `"value3"`. The strings are stored in the State at location `/values`.

```
<Split value="value 1,value 2,value 3" delimiter="," savePath="/values" />
```

While

The While action loops a series of nested actions while a condition is true.

The condition is evaluated at the beginning of the loop so if the condition is never true, it never executes its nested actions. This action is different from the DoWhile action, where the condition is evaluated at the end of the loop.

The following table shows the parameters for the While action.

Table 137. While action parameters			
Name	**Data type**	**Required**	**Notes**
condition	JPath	Yes	The condition that determines whether to continue looping. A loop is an execution of all nested actions.

Table 137. While action parameters (continued)			
Name	**Data type**	**Required**	**Notes**
actions	JPath Condition	Yes	The sequence of actions to execute. Must be a JPath expression that resolves to a value of `true` or `false`. References to the State should not be within the `${}` notation for JPath conditions. See "JPath" on page 263.

XML Example:

This action executes the nested CallEndpoint action if a value exists in the State at location `/next_page`. The While action executes the nested CallEndpoint action until the `/next_page` value is null. If `/next_page` is always null, the nested action is not executed.

```
<While condition="/next_page != null">
    <CallEndpoint ... />
</While>
```

Related concepts

"CallEndpoint" on page 244
The CallEndpoint action calls an HTTP endpoint.

"DoWhile" on page 252
The DoWhile action loops a series of actions while a condition is true.

XPathQuery

The XPathQuery action executes an XPath query on an XML document value.

If an API returns a response in XML format, you can extract a certain value or set of values from the response. You can use XPath to extract values.

The following table shows the parameters for the XPathQuery action.

Table 138. XPathQuery action parameters			
Name	**Data type**	**Required**	**Notes**
xmlPath	JPath	Yes	The location of the XML document in the State.
xPathQuery	XPath	Yes	
singleton	Boolean	No	Interprets the results as a single value instead of an array. The default is False.
savePath	JPath	Yes	The location to store the result.

XML Example:

This action executes the XPath query "`//event/id/text()`" against the XML document that is stored in the State at `/xml_events`, and stores it in the State at location `/event/id` as a single value.

```
<XPathQuery xmlPath="/xml_events" xPathQuery="//event/id/text()" singleton="true" savePath="/
event/id" />
```

JPath

JPath is a language for querying and manipulating JSON elements. You can use JPath to compute values, such as strings, numbers, and boolean values, from JSON elements.

Basic selection

Select elements by using a forward slash (/). Select array items by using square brackets ([ ]).

The following table shows examples of basic selection of JSON elements.

Table 139. Basic selection examples

Example	Description	State	Expression	Result
Primitive	Selects a JSON primitive.	`{ "object": { "attr1": "value1", "attr2": "value2" } }`	`/object/attr1`	`"value1"`
Object	Selects a JSON object.	`{ "object": { "attr1": "value1", "attr2": "value2" } }`	`/object`	`{ "attr1": "value1", "attr2": "value2" }`
Array	Selects a JSON array.	`{ "array": [ "value1", "value2" ] }`	`/array`	`[ "value1", "value2" ]`
Array Index	Selects an item of a JSON array by index. The index starts at 0.	`{ "array": [ 1.1, 2.2 ] }`	`/array[1]`	`2.2`
Nested	Selects an attribute of an object that is nested in an array.	`{ "array": [ { "id": 123 }, { "id": 456 } ] }`	`/array[1]/id`	`456`
Multiple Nested	Selects all attributes of an object that is nested in an array.	`{ "array": [ { "id": 123 }, { "id": 456 } ] }`	`/array/id`	`[ 123, 456 ]`
Single Quoted Keys	Selects key names by using single quotation marks.	`{ "name with spaces": { "some attribute": true, "another attribute": false } }`	`/'name with spaces'/'some attribute'`	`true`

Table 139. Basic selection examples (continued)				
Example	**Description**	**State**	**Expression**	**Result**
Double Quoted Keys	Selects key names by using double quotation marks.	`{ "name with spaces": { "some attribute": true, "another attribute": false } }`	`/"name with spaces"/"some attribute"`	`true`
Unicode Support	Selects by using Unicode keys and values.	`{ "a˙t˙t˙r˙": "v˙a˙l˙u˙e˙" }`	`/"a˙t˙t˙r˙"`	`"v˙a˙l˙u˙e˙"`

Query

Array elements can be queried by using square brackets ([ ]). The query is evaluated against all of the array elements. The query can select any fields of the element for comparison and reference anything in the JSON document.

The following table shows query operators. *a* and *b* can be either a constant or a JPath construct. Basic selection, query, arithmetic, and functions are JPath constructs.

Table 140. Query operators	
Operator	**Description**
a = *b*	Equal
a != *b*	Not equal
a > *b*	Greater than
a < *b*	Less than
a >= *b*	Greater than or equal
a <= *b*	Less than or equal
not *a*	Negates the result of *a*
exists *a*	Checks if *a* exists as an attribute

The following table shows examples of the query operators that you can apply to the array elements.

Table 141. Query examples				
Example	**Description**	**State**	**Expression**	**Result**
Equality (or Inequality)	Queries an array for objects with an attribute equal to a value.	`{ "array": [ { "id": 1, "name": "Object 1" }, { "id": 2, "name": "Object 2" }, { "id": 3, "name": "Object 3" } ] }`	`/array[@id = 2]`	`[ { "id": 2, "name": "Object 2" } ]`

Table 141. Query examples (continued)

Example	Description	State	Expression	Result
Greater than	Queries an array of objects with attributes greater than a value.	`{ "array": [ { "id": 1, "name": "Object 1" }, { "id": 2, "name": "Object 2" }, { "id": 3, "name": "Object 3" } ] }`	`/array[@id > 1]`	`[ { "id": 2, "name": "Object 2" }, { "id": 3, "name": "Object 3" } ]`
Primitives	Selects primitives from an array that passes a specific query.	`{ "array": [ "value 1", "value 2", "value 3" ] }`	`/array[@ != "value 2"]`	`[ "value 1", "value 3" ]`
And	Selects with the 'and' operator.	`{ "array": [ "value 1", "value 2", "value 3" ] }`	`/array[@ != "value 2" and @ != 'value 3']`	`[ "value 1" ]`
Or	Selects with the 'or' operator.	`{ "array": [ "value 1", "value 2", "value 3" ] }`	`/array[@ = "value 2" or @ = "value 3"]`	`[ "value 2", "value 3" ]`
Parentheses	Selects with parentheses.	`{ "array": [ "value 1", "value 2", "value 3" ] }`	`/array[not (@ = "value 2" or @ = "value 3")]`	`[ "value 1" ]`
Exists	Selects objects of an array that have a specific attribute.	`{ "array": [ { "id": 1, "name": "Object 1" }, { "id": 2, "name": "Object 2" }, { "id": 3, } ] }`	`/array[exists @name]`	`[ { "id": 1, "name": "Object 1" }, { "id": 2, "name": "Object 2" } ]`

Arithmetic operations in JSON elements

Some basic arithmetic operations can be applied to the JSON elements.

The following table shows arithmetic operators. *a* and *b* can be either a constant or a JPath construct. Basic selection, query, arithmetic, and functions are JPath constructs.

Table 142. Arithmetic operators

Operator	Description
a + *b*	Add
a - *b*	Subtract
a * *b*	Multiply
a / *b*	Divide

The following table shows examples of the arithmetic operations that you can apply to JSON elements.

Table 143. Arithmetic examples				
Example	**Description**	**State**	**Expression**	**Result**
Addition	Basic addition	`{ "attr1": 1, "attr2": 4 }`	`/attr1 + /attr2`	5
Subtraction	Basic subtraction	`{ "attr1": 1, "attr2": 4 }`	`/attr1 - /attr2`	-3
Multiplication	Basic multiplication	`{ "attr1": 2, "attr2": 4 }`	`/attr1 * /attr2`	8
Division	Basic division	`{ "attr1": 12, "attr2": 4 }`	`/attr1 / /attr2`	3
Parentheses	Arithmetic that uses parentheses.	`{ "attr1": 4, "attr2": 2 }`	`(/attr1 - /attr2) * (/attr1 + /attr2)`	12
Arithmetic as Array Index	Uses arithmetic to compute an array index.	`{ "attr1": 4, "attr2": 2, "array": [ "value 1", "value 2", "value 3", ] }`	`/array[/attr1 - /attr2]`	`"value 3"`
Arithmetic in Query	Uses arithmetic as part of a query.	`{ "attr1": 4, "attr2": 2, "array": [ { "id": 1, "name": "Object 1" }, { "id": 2, "name": "Object 2" }, { "id": 3, "name": "Object 3" } ] }`	`/array[@id != (/attr1 - /attr2)]`	`[ { "id": 1, "name": "Object 1" }, { "id": 3, "name": "Object 3" } ]`

Functions in JPath expressions

Some basic functions can be used in JPath expressions, such as using a function as part of a query.

The following table shows the basic functions that can be used in JPath expressions.

Table 144. Functions	
Function	**Description**
count(path)	Returns the number of items at a specific path expression. • For an object, returns the number of members. • For an array, returns the number of array elements. • For a string, returns the string length.
base64_encode(expr)	Returns the base64 encoded value of a specific expression.
base64_decode(expr)	Returns the base64 decoded value of a specific expression.
url_encode(expr)	Returns the url encoded value of a specific expression.

Table 144. Functions (continued)	
Function	**Description**
url_decode(expr)	Returns the url decoded value of a specific expression.
min(path)	Returns the minimum value from an array at a specific path expression.
max(path)	Returns the maximum value from an array at a specific path expression.
time()	Returns time in milliseconds since epoch.

The following table shows examples of basic functions that can be used in JPath expressions.

Table 145. Function examples				
Example	**Description**	**State**	**Expression**	**Result**
Function in query	Uses a function as part of a query.	`{ "array": [ { "id": 1, "timestamp": 1186978597 }, { "id": 2, "timestamp": 1286978597 }, { "id": 3, "timestamp": 17586978597 } ] }`	`/array[@timestamp > time()]`	`[ { "id": 3, "timestamp": 17586978597 } ]`
Find an event with the biggest timestamp	Uses the max() function in combination with a generated array of numbers.	`{ "array": [ { "id": 1, "timestamp": 1186978597 }, { "id": 2, "timestamp": 1286978597 }, { "id": 3, "timestamp": 17586978597 } ] }`	`max(/array/timestamp)`	`17586978597`

Command line testing tool

Use the command line tool to execute a workflow. The command line tool provides quick feedback while you develop or troubleshoot the contents of a workflow.

The command line tool does not interact with the live IBM QRadar event pipeline. Any events that are retrieved from the Universal Cloud REST API protocol are written to the QRadar Console.

New in V2

To run the tool in V2 or later, type the following command.

```
/opt/qradar/bin/test-workflow.sh
```

To run the tool in V1, add one or more commands to the end of the following command line to run the tool. If you don't specify any arguments, the entire usage is written.

```
java -cp "/opt/ibm/si/services/ecs-ec-ingress/
current/bin/*:/opt/ibm/si/services/ecs-ec-ingress/eventgnosis/lib/q1labs/*"
com.q1labs.semsources.sources.universalcloudrestapi.UniversalCloudRESTAPITest
```

The following table shows the commands for the command line testing tool.

Table 146. Command line testing tool usage	
Command	**Description**
`-?,--help`	Displays the usage and exits.
`-p <[user@]server:port>`	Specifies the proxy to use.
`-r <seconds>`	Specifies the poll frequency. In V2 or later, by default the tool runs only once. If you enter a frequency, the tool runs at that interval.
`-s <file>`	Specifies the file for state persistence.
`-v`	Displays more logging.
`-w <file>`	Specifies the workflow to load.
`-wp <file>`	Specifies the workflow parameter values to load. In V2 or later, this parameter is optional.

XML Example

In the following example, the command line is used to specify the workflow and workflow parameter values to load. The `-w` command is used to specify the `myworkflow.XML` workflow and the `-wp` command is used to specify the `myworkflow.parameter.values.xml` workflow parameter values.

```
/opt/qradar/bin/test-workflow.sh -w myworkflow.xml -wp myworkflow.parameter.values.xml
```

Chapter 11. Protocols that support Certificate Management

You can use Certificate Management to upload and manage certificates that can be used by log sources with supported protocols.

The following table lists the protocols that support Certificate Management.

Protocol	Fix Central link
TLS Syslog	Download TLS Syslog protocol
HTTP Receiver	Download HTTP Receiver protocol

Related information

QRadar Certificate Management

Part 3. DSMs

Chapter 12. 3Com Switch 8800

The IBM QRadar DSM for 3Com Switch 8800 receives events by using syslog.

The following table identifies the specifications for the 3Com Switch 8800 DSM:

Specification	Value
Manufacturer	3Com
DSM name	Switch 8800 Series
RPM file name	`DSM-3ComSwitch_QRadar-version_build-number.noarch.rpm`
Supported versions	3.01.30
Protocol	Syslog
QRadar recorded events	Status and network condition events
Automatically discovered?	Yes
Includes identity?	No
Includes custom event properties?	No
More information	For more information, see the 3Com link to public site website (https://www.3com.com)

To send 3COM Switch 8800 events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website (https://www.ibm.com/support/fixcentral) onto your QRadar Console:
   - Protocol Common RPM
   - DSM Common RPM
   - 3COM Switch 8800 DSM RPM
2. Configure each 3COM Switch 8800 instance to communicate with QRadar.
3. If QRadar does not automatically discover the DSM, create a log source on the QRadar Console for each 3COM Switch 8800 instance. Configure all the required parameters, and use the following table for specific values:

Parameter	Description
Log Source Type	3COM Switch 8800
Protocol Configuration	Syslog

Related tasks

Configuring your 3COM Switch 8800

Configure your 3COM Switch 8800 to forward syslog events to IBM QRadar.

Configuring your 3COM Switch 8800

Configure your 3COM Switch 8800 to forward syslog events to IBM QRadar.

Procedure

1. Log in to 3COM Switch 8800.
2. To enable the information center, type the following command:

   ```
   info-center enable
   ```
3. To configure the log host, type the following command:

   ```
   info-center loghost QRadar_ip_address facility informational language english
   ```
4. To configure the ARP and IP information modules, type the following commands.

   ```
   info-center source arp channel loghost log level informational
   info-center source ip channel loghost log level informational
   ```

Chapter 13. AhnLab Policy Center

The IBM QRadar DSM for AhnLab Policy Center retrieves events from the DB2 database that AhnLab Policy Center uses to store their log.

The following table identifies the specifications for the AhnLab Policy Center DSM:

Table 147. AhnLab Policy Center DSM specifications

Specification	Value
Manufacturer	AhnLab
DSM	AhnLab Policy Center
RPM file names	`DSM-AhnLabPolicyCenter-`*`QRadar-Release_Build-Number`*`.noarch.rpm`
Supported versions	4.0
Protocol	AhnLabPolicyCenterJdbc
QRadar recorded events	Spyware detection, Virus detection, Audit
Automatically discovered?	No
Includes identity	Yes
More information	Ahnlab website (https://global.ahnlab.com/)

To integrate AhnLab Policy Center DSM with QRadar, complete the following steps:

1. Download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - JDBC protocol RPM
   - AhnLabPolicyCenterJdbc protocol RPM
   - AhnLab Policy Center RPM

   Tip: For more information, see your DB2 documentation.
2. Ensure that your AhnLab Policy Center system meets the following criteria:
   - The DB2 Database allows connections from QRadar.
   - The port for AhnLabPolicyCenterJdbc Protocol matches the listener port of the DB2 Database.
   - Incoming TCP connections on the DB2 Database are enabled to communicate with QRadar.
3. For each AhnLab Policy Center server you want to integrate, create a log source on the QRadar Console. The following table identifies Ahnlab-specific protocol values:

Parameter	Value
Log Source Type	AhnLab Policy Center APC
Protocol Configuration	AhnLabPolicyCenterJdbc
Access credentials	Use the access credentials of the DB2 server.
Log Source Language	If you use QRadar v7.2 or later, you must select a log source language.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Chapter 14. Akamai Kona

The IBM QRadar DSM for Akamai Kona collects event logs from your Akamai Kona platforms.

The following table identifies the specifications for the Akamai KONA DSM:

Table 148. Akamai KONA DSM specifications

Specification	**Value**
Manufacturer	Akamai
Product	Kona
DSM RPM name	`DSM-AkamaiKona-`*`QRadar_Version-Build_Number`*`.noarch.rpm`
Protocol	HTTP Receiver, Akamai Kona REST API
Event Format	JSON
Recorded event types	All security events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Akamai Kona SIEM API Documentation

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configure an Akamai Kona log source by using the HTTP Receiver protocol

Collect events from Akamai Kona in QRadar by using the HTTP Receiver protocol.

Collect events by using the HTTP Receiver Protocol:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common RPM
   - DSMCommon RPM
   - HTTPReceiver Protocol RPM
   - Akamai KONA DSM RPM
2. Configure your Akamai KONA system to communicate with QRadar. For more information, contact Akamai.
3. If you plan to configure the log source to use the **HTTPs** and **Client Authentication** options, copy the Akamai KONA certificate to the target QRadar Event Collector.
4. For each Akamai KONA server that you want to integrate, create a log source on the QRadar Console. Configure all the required parameters. Use this table to configure Akamai Kona specific parameters:

Table 149. Akamai KONA log source parameters	
Parameter	**Description**
Log source type	Akamai KONA
Protocol Configuration	HTTP Receiver
Client Certificate Path	The absolute file path to the client certificate on the target QRadar Event Collector. Ensure that the Akamai KONA certificate is already copied to the Event Collector. If you select the **HTTPs** and **Client Authentication** option from the **Communication Type** list, the **`Client Certificate Path`** parameter is required.
Listen Port	The destination port that is configured on the Akamai KONA system. **Important:** Do not use port 514. Port 514 is used by the standard Syslog listener.
Message Pattern	The **`Message Pattern`** `'\{"type'` is for JSON format events.

For more information about this protocol, see "HTTP Receiver protocol configuration options" on page 125.

Restriction: This integration requires you to open a non-standard port in your firewall for incoming Akamai connections. Use an internal proxy to route the incoming Akamai connections. Do not point the Akamai data stream directly to the QRadar Console. For more information about opening a non-standard port in your firewall, consult your Network security professionals.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configure an Akamai Kona log source by using the Akamai Kona REST API protocol

Collect events from Akamai Kona in QRadar by using the Akamai Kona REST API protocol.

Collect events from Akamai Kona REST API:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common RPM
   - Akamai Kona REST API RPM
   - DSMCommon RPM
   - Akamai KONA DSM RPM
2. Configure Akamai Kona to send Security events to QRadar by using the Akamai Kona REST API protocol.
3. Configure Akamai Kona to communicate with QRadar.

   Note: The Akamai KONA DSM supports only JSON formatted events. Akamai's sample CEF and Syslog connector does not work with the Akamai KONA DSM.

4. Add a log source in QRadar.

   The following table describes the log source parameters that require specific values for Akamai KONA DSM event collection:

Table 150. Akamai KONA DSM log source parameters

Parameter	Value
Log Source Type	Akamai KONA
Protocol Configuration	Akamai Kona REST API
Host	Provided during the SIEM OPEN API provisioning in the Akamai Luna Control Center. The **Host** is a unique base URL that contains information about the appropriate rights to query the security events. This parameter is a password field because part of the value contains secret information.
Client Token	One of the two security parameters. This token is paired with **Client Secret** to make the client credentials. This token can be found after you provision the Akamai SIEM OPEN API.
Client Secret	One of the two security parameters. This secret is paired with **Client Token** to make the client credentials. This token can be found after you provision the Akamai SIEM OPEN API.
Access Token	Security parameter that is used with client credentials to authorize API client access for retrieving the security events. This token can be found after you provision the Akamai SIEM OPEN API.
Security Configuration ID	ID for each security configuration that you want to retrieve security events for. This ID can be found in the SIEM Integration section of your Akamai Luna portal. You can specify multiple configuration IDs in a comma-separated list. For example: `configID1,configID2`.
Use Proxy	If QRadar accesses Akamai Kona by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Automatically Acquire Server Certificate	Select Yes for QRadar to automatically download the server certificate and begin trusting the target server.

Table 150. Akamai KONA DSM log source parameters (continued)	
Parameter	**Value**
Recurrence	The time interval between log source queries to the Akamai SIEM API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 1 minute.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.

For more information about this protocol, see "Akamai Kona REST API protocol configuration options" on page 67.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Akamai Kona to communicate with QRadar

You must configure your Akamai Kona platform to make the security events available for IBM QRadar.

Procedure

1. Ensure that you have access to your Akamai Luna Control center (https://control.akamai.com) to configure and provision the SIEM integration.
2. Go to the Akamai online documentation (https://developer.akamai.com/tools/siem-integration/docs/siem.htm).
3. Follow steps 1 - 3 in the Akamai documentation to successfully provision the integration.
4. Record the values for the Host, Client Token, Client Secret, Access Token, and Security Configuration Key.

   You need these values when you configure a log source in QRadar.

Creating an event map for Akamai Kona events

Event mapping is required for a number of Akamai Kona events. Because of the customizable nature of policy rules, some events might not contain a predefined IBM QRadar Identifier (QID) map to categorize security events.

About this task

You can individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track recurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for Akamai Kona are categorized as unknown. Unknown events are easily identified as the **Event Name** column and **Low Level Category** columns display Unknown.

As your device forwards events to QRadar, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software. It is helpful

to know how to quickly search for unknown events. When you know how to search for unknown events, you might want to repeat this search until you are satisfied that most of your events are identified.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select the log source group or **Other**.

   Log sources that are not assigned to a group are categorized as Other.
6. From the **Log Source** list, select your Akamai Kona log source.
7. Click **Add Filter**.

   The **Log Activity** tab is displayed with a filter for your log source.
8. From the **View** list, select **Last Hour**.

   Any events that are generated by the Akamai Kona DSM in the last hour are displayed. Events that are displayed as unknown in the **Event Name** column or **Low Level Category** column require event mapping in QRadar.

   Tip: You can save your existing search filter by clicking **Save Criteria**.

What to do next

Modify the event map. For more information about modifying the event map for Akamai Kona, see "Modifying the event map for Akamai Kona" on page 281

Modifying the event map for Akamai Kona

You can manually map events to an external device in the IBM QRadar Identifier (QID) map tool. Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

About this task

Akamai Kona events that do not have a defined log source can't be mapped to a QRadar Identifier (QID) map by a mapped event. Events without a log source display as **SIM Generic Log** in the **Log Source** column.

Procedure

1. In the **Event Name** column, double-click an unknown event for Akamai Kona.

   The detailed event information is displayed.
2. Click **Map Event**.
3. From the **Browse for QID** pane, select any of the following search options to narrow the event categories for a QRadar Identifier (QID):

   - From the **High-Level Category** list, select a high-level event categorization.
   - For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *IBM QRadar Administration Guide*.
   - From the **Low-Level Category** list, select a low-level event categorization.
   - From the **Log Source Type** list, select a log source type.

   The **Log Source Type** list gives the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, Akamai Kona provides all events. You might select another product that likely captures similar events.

4. To search for a QID by name, type a name in the **QID/Name** field.

   The **QID/Name** field gives the option to filter the full list of QIDs for a specific word, for example, policy.
5. Click **Search**.

   A list of QIDs are displayed.
6. Select the QID that you want to associate to your unknown event.
7. Click **OK**.

   QRadar maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.

   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

Akamai Kona sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when you use the *Akamai Kona REST API* protocol for the *Akamai KONA* DSM:

Note: Each event might contain multiple Event IDs and Names.

Table 151. Akamai KONA sample message supported by Akamai Kona REST API.

Event name	Low-level category	Sample log message
The application is not available - Deny Rule	Warning	{"type":"akamai_siem","format":"json", "version":"1.0","attackData":{"configId":"<Config Id>" ,"policyId":"<Policy Id>","clientIP":"192.0.2.0", "rules":"970901","ruleVersions":"1","ruleMessages": "Application is not Available (HTTP 5XX)","ruleTags" :"AKAMAI/BOT/UNKNOWN_BOT","ruleData":"Vector Score : 4, DENY threshold: 2, Alert Rules: 3990001:970901 , Deny Rule: , Last Matched Message: Application is not Available (HTTP 5XX)","ruleSelectors":"", "ruleActions":"monitor"},"httpMessage":{"requestId" :"<Request Id>","start":"1517337032","protocol": "HTTP/1.1","method":"GET","host":"siem-sample.csi .edgesuite.net","port":"80","path":"path","request Headers":"User-Agent: curl/7.35.0Host: siem-sample. csi.edgesuite.netAccept: */*edge_maprule: ksd","status":"403","bytes":"298","responseHeaders": "Server: AkamaiGHostMime-Version: 1.0Content-Type: text/htmlContent-Length: 298Expires: Tue, 30 Jan 2018 18:30:32 GMTDate: Tue, 30 Jan 2018 18:30:32 GMTConnec tion: close"},"geo":{"continent":"<Continent>","count ry":"<Country>","city":"<City>","regionCode":"<Region Code>","asn":"<asn>"}} {"type":"akamai_siem","format":"json","version":"1.0","a ttackData":{"configId":"<Config Id>","policyId":"<Policy Id>","clientIP":"192.0.2.0","rules":"970901","ruleVersio ns":"1","ruleMessages":"Application is not Available (HTTP 5XX)","ruleTags":"AKAMAI/BOT/ UNKNOWN_BOT","ruleData":"Vector Score: 4, DENY threshold: 2, Alert Rules: 3990001:970901, Deny Rule: , Last Matched Message: Application is not Available (HTTP 5XX)","ruleSelectors":"","ruleActions":"monitor"},"httpM essage":{"requestId":"<Request Id>","start":"1517337032","protocol":"HTTP/ 1.1","method":"GET","host":"siem-sample.csi.edgesuite.net","port":"80","path":"path","req uestHeaders":"User-Agent: curl/7.35.0Host: siem-sample.csi.edgesuite.netAccept: */*edge_maprule: ksd","status":"403","bytes":"298","responseHeaders":"Ser ver: AkamaiGHostMime-Version: 1.0Content-Type: text/ htmlContent-Length: 298Expires: Tue, 30 Jan 2018 18:30:32 GMTDate: Tue, 30 Jan 2018 18:30:32 GMTConnection: close"},"geo": {"continent":"<Continent>","country":"<Country>","city": "<City>","regionCode":"<Region Code>","asn":"<asn>"}}

Table 151. Akamai KONA sample message supported by Akamai Kona REST API. (continued)

Event name	Low-level category	Sample log message
Anomaly Score Exceeded for Outbound	Suspicious Activity	{"type":"akamai_siem","format":"json", "version":"1.0","attackData":{"configId":"<Config Id> ","policyId":"<Policy Id>","clientIP":"192.0.2.0", "rules":"OUTBOUND-ANOMALY","ruleVersions":"4","rule Messages":"Anomaly Score Exceeded for Outbound", "ruleTags":"AKAMAI/POLICY/OUTBOUND_ANOMALY","rule Data":"curl_85D6E381D300243323148F63983BD735","rule Selectors":"","ruleActions":"alert"},"httpMessage": {"requestId":"<Request Id>","start":"1517337032", "protocol":"HTTP/1.1","method":"GET","host":"siem-sample.csi.edgesuite.net","port":"80","path":"path", "requestHeaders":"User-Agent: curl/7.35.0Host: siem-sample.csi.edgesuite.netAccept: */*edge_maprule: ksd" ,"status":"403","bytes":"298","responseHeaders": "Server: AkamaiGHostMime-Version: 1.0Content-Type: text/htmlContent-Length: 298Expires: Tue, 30 Jan 2018 18:30:32 GMTDate: Tue, 30 Jan 2018 18:30:32 GMTConnection: close"},"geo":{"continent":"<Continent> ","country":"<Country>","city":"<City>","regionCode": "<Region Code>","asn":"<asn>"}} {"type":"akamai_siem","format":"json","version":"1.0","attackData":{"configId":"<Config Id>","policyId":"<Policy Id>","clientIP":"192.0.2.0","rules":"OUTBOUND-ANOMALY","ruleVersions":"4","ruleMessages":"Anomaly Score Exceeded for Outbound","ruleTags":"AKAMAI/POLICY/OUTBOUND_ANOMALY","ruleData":"curl_85D6E381D300243323148F63983BD735","ruleSelectors":"","ruleActions":"alert"},"httpMessage":{"requestId":"<Request Id>","start":"1517337032","protocol":"HTTP/1.1","method":"GET","host":"siem-sample.csi.edgesuite.net","port":"80","path":"path","requestHeaders":"User-Agent: curl/7.35.0Host: siem-sample.csi.edgesuite.netAccept: */*edge_maprule: ksd","status":"403","bytes":"298","responseHeaders":"Server: AkamaiGHostMime-Version: 1.0Content-Type: text/htmlContent-Length: 298Expires: Tue, 30 Jan 2018 18:30:32 GMTDate: Tue, 30 Jan 2018 18:30:32 GMTConnection: close"},"geo":{"continent":"<Continent>","country":"<Country>","city":"<City>","regionCode":"<Region Code>","asn":"<asn>"}}

Chapter 15. Alibaba ActionTrail

The IBM QRadar DSM for Alibaba ActionTrail supports events that are collected from Alibaba Cloud Object Storage buckets with the help of Alibaba Cloud Object Storage protocol. It also supports Alibaba Cloud Simple Log Service Protocol.

The following table lists the specifications for the Alibaba ActionTrail DSM:

Table 152. Alibaba ActionTrail DSM specifications

Specification	**Value**
Manufacturer	Alibaba Cloud
DSM	Alibaba ActionTrail
RPM name	`DSM-AlibabaActionTrail-<QRadar_version-Build_number>.noarch.rpm`
Supported protocols	Alibaba Cloud Object Storage Alibaba Cloud Simple Log Service Syslog
Event format	JSON
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	ActionTrail

Related concepts

"Alibaba Cloud Object Storage protocol configuration options" on page 69
The Alibaba Cloud Object Storage protocol for IBM QRadar is an active outbound protocol that collects logs that are contained in objects from Alibaba Cloud Object Storage buckets.

"Alibaba Cloud Simple Log Service protocol configuration options" on page 71
The Alibaba Cloud Simple Log Service protocol for IBM QRadar is an outbound or active protocol that collects logs from a specific Log Store available in the Alibaba Cloud Log application.

Alibaba ActionTrail sample event message

Use this sample event message as a way of verifying a successful integration with IBM QRadar.

The following sample event message shows Logon to the Alibaba Cloud Management console.


```
{"eventId":"2542222-2222-2222-2222-500d4449 ****","eventVersion":1,"eventSource":"http://
account.test.com/test/login_aliyun.htm","sourceIpAddress":"10.0.0.1","userAgent":"Mozilla/5.0
(iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/
11111 Ariver/1.1.0 AliApp(AP/10.2.28.6000) AlipayClient/10.2.11.6000 Language/zh-Hans Region/
CN","eventType":"ConsoleSignin","userIdentity":
{"accountId":"11122223333***","principalId":"11122223333***","type":"root-
account","userName":"test"},"serviceName":"Customer","additionalEventData":
{"loginAccount":"user1","isMFAChecked":"false"},"extend":"2","requestId":"111111-6b56-2222-5555-
500d8d25***","eventTime":"2021-01-01T00:00:00Z","isGlobal":true,"acsRegion":"cn-
abcd","eventName":"ConsoleSignin"}
```

Table 153. Highlighted values in the Alibaba ActionTrail sample event	
QRadar field name	**Highlighted payload field name**
Event ID	**eventName**
Username	**userIdentity.userName**
Source IP	**sourceIpAddress**
Device Time	**eventTime**

The following sample event message is for Alibaba Cloud Simple Log Service Protocol.


```
{"owner_id":"1111111111111111","event":{"additionalEventData":
{"CallerBid":"11111"},"apiVersion":"2020-06-16","datasource":"pop-test-
east-1","eventSource":"alb.test-east-1.test.com","product":"Alb","requestParameters":
{"stsTokenPrincipalName":"test/example","AcsProduct":"Alb","X-Acs-Public-
Access":true,"MaxResults":50,"ClientPort":13230,"SignatureType":"","RegionId":"test-
east-1"},"sourceIpAddress":"audit.log.test.com","tlsDetails":
{"tlsVersion":"TLSv1.2","cipherSuite":"AAAAA-AAAAA-AAAAAA-AAA-
SHA384","clientProvidedHostHeader":"alb.test-
east-1.test.com"},"userAgent":"audit.log.test.com","userIdentity":
{"accessKeyId":"STS.N111111111111111111111","accountId":"1111111111111111","principalId":"11111
111111111111111:example","sessionContext":{"attributes":
{"mfaAuthenticated":"false"}},"type":"assumed-
role","userName":"test:example"},"eventId":"11151579-1111-1111-1111-
CCA7EC29C6C1","eventName":"ListLoadBalancers","eventType":"AliyunServiceEvent","acsRegion":"test
-east-1","serviceName":"ALB","eventTime":"2024-02-27T09:45:08Z"},"__topic__":"actiontrail_event"
,"__source__":"log_service","__time__":"1709027108"}
```


Table 154. Highlighted values in the Alibaba Cloud Simple Log Service Protocol sample event	
QRadar field name	**Highlighted payload field name**
Event ID	**event.eventName**
Username	**event.userIdentity.userName**
Source IP	**event.requestParameters.ClientPort**
Device Time	**event.eventTime**

Chapter 16. Amazon

IBM QRadar supports a range of Amazon products.

Amazon AWS Application Load Balancer Access Logs

The IBM QRadar DSM for Amazon Application Load Balancer Access Logs collects access logs from Amazon AWS Application Load Balancers. The logs are collected in an Amazon S3 bucket by a Simple Queue Service (SQS) queue.

To integrate Amazon Application Load Balancer Access Logs with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website.
   - Protocol Common RPM
   - Amazon AWS S3 REST API protocol RPM
   - DSM Common RPM
   - Amazon Application Load Balancer Access Logs DSM RPM
2. Configure your Amazon Application Load Balancer Access Logs application to communicate with QRadar. For more information, see Amazon AWS Enable access logging.
3. Publish flow logs to an SQS bucket. For more information, see Publishing flow logs to an S3 bucket.
4. Create the SQS queue that is used to receive ObjectCreated notifications, then configure S3 ObjectCreated notifications. For more information, see Create an SQS queue and configure S3 ObjectCreated notifications.
5. Configure the security credentials for your AWS user account. For more information, see Configuring security credentials for your AWS user account.
6. If QRadar does not automatically detect the log source, add an Amazon Application Load Balancer Access Logs log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Amazon AWS Application Load Balancer Access Logs DSM specifications

When you configure the Amazon AWS Application Load Balancer Access Logs, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported protocol is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Amazon AWS Application Load Balancer Access Logs DSM.

Table 155. Amazon AWS Application Load Balancer Access Logs DSM specifications

Specification	Value
Manufacturer	Amazon
DSM name	Amazon AWS Application Load Balancer Access Logs
RPM file name	DSM-*AmazonAWSALBAccessLogs-QRadar_version-build_number*.noarch.rpm
Protocol	Amazon AWS S3 REST API
Event format	Space delimited pre-defined fields

Table 155. Amazon AWS Application Load Balancer Access Logs DSM specifications (continued)	
Specification	**Value**
Recorded event types	Access logs
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Access logs for your Application Load Balancer

Publishing flow logs to an S3 bucket

Complete these steps to publish flow logs to an S3 bucket.

Procedure

1. Log in to your AWS Management console, and then from the **Services** menu, navigate to the **VPC Dashboard**.
2. Enable the check box for the VPC ID that you want to create flow logs for.
3. Click the **Flow Logs** tab.
4. Click **Create Flow Log**, and then configure the following parameters:

Table 156. Create Flow Log parameters	
Parameter	**Description**
Filter	Select **Accept, Reject, or All**.
Destination	Select **Send to an S3 Bucket**.
S3 Bucket ARN	Type the ARN for the S3 Bucket. Examples: • `arn:aws;s3:::myTestBucket` • `arn:aws:s3:::myTestBucket/testFlows`

5. Click **Create**.

   For more information about publishing flow logs to Amazon S3, see the Publishing Flow Logs to Amazon S3 documentation on the AWS website.

What to do next

Create the SQS queue that is used to receive ObjectCreated notifications.

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.

4. Creating ObjectCreated notifications.
5. Configuring security credentials for your AWS user account.
6. Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge.

Finding the S3 bucket that contains the data that you want to collect

You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **`Region Name`** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

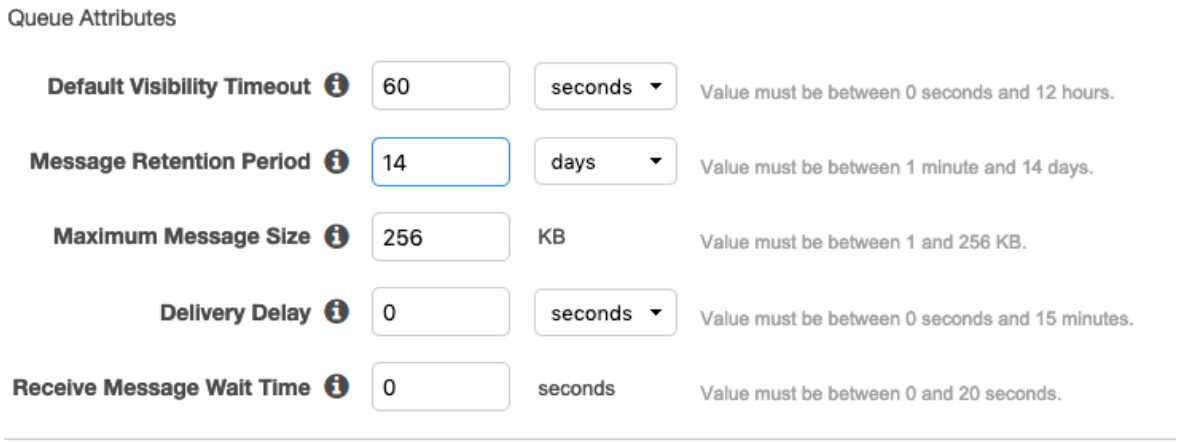
Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.
3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.

   - **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

   Use the default value for the remaining **Queue Attributes**.

   More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions

You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.
3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 157. Permission parameters	
Parameter	**Value**
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

   d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 158. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
      }
    }
  ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications

Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.
3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 159. Example: New ObjectCreated notification parameter configuration	
Parameter	**Value**
Name	Type a name of your choosing.
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

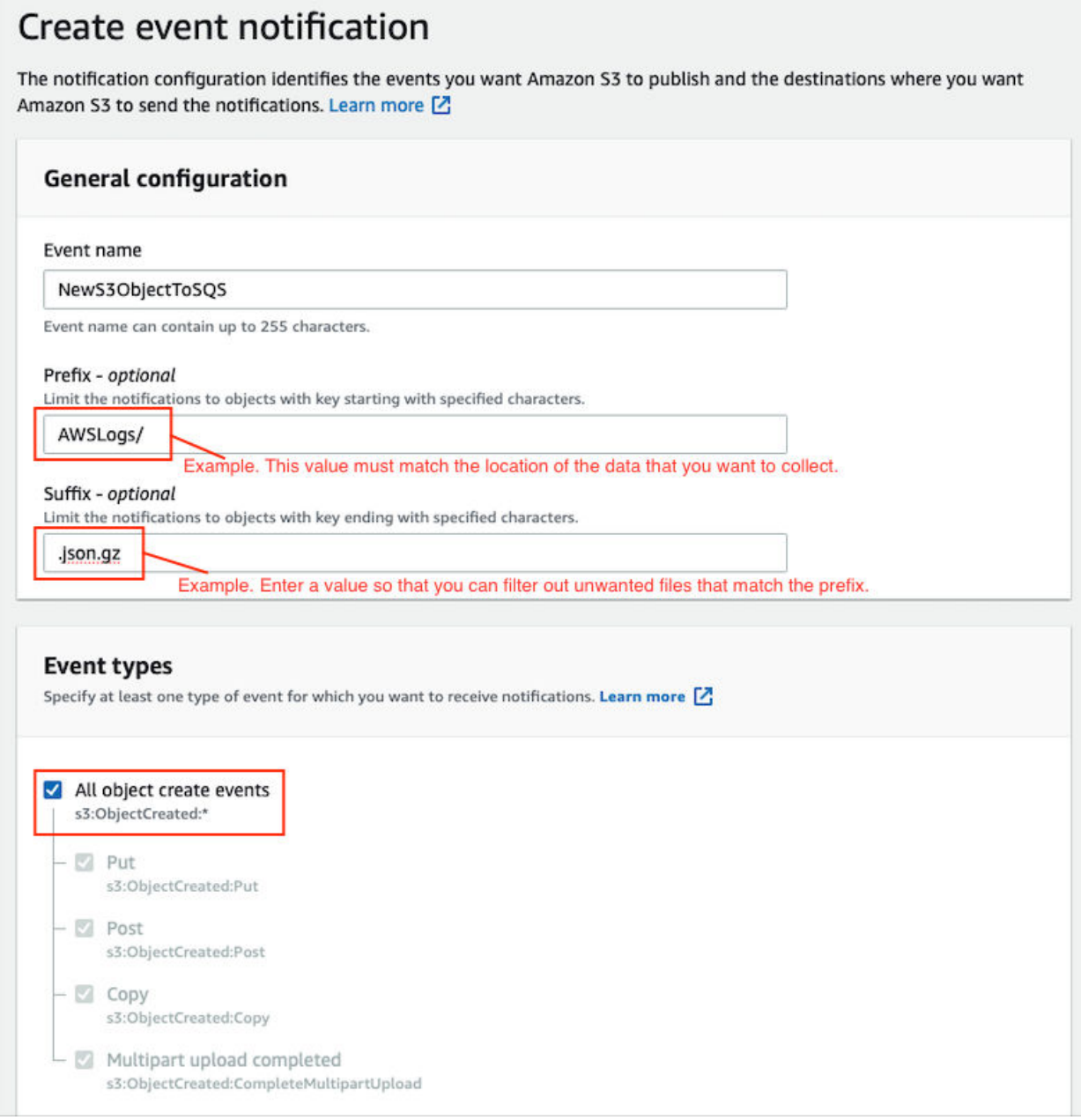


Figure 6. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

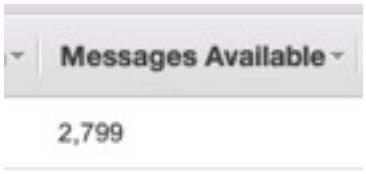


Figure 7. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

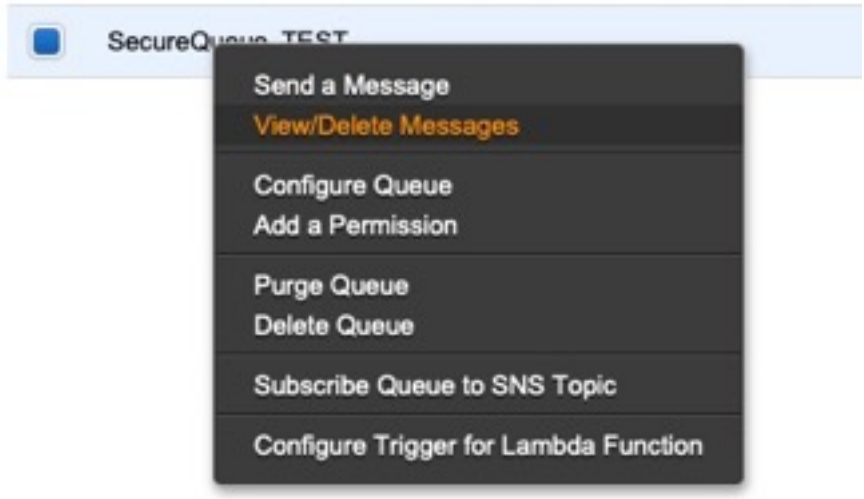


Figure 8. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

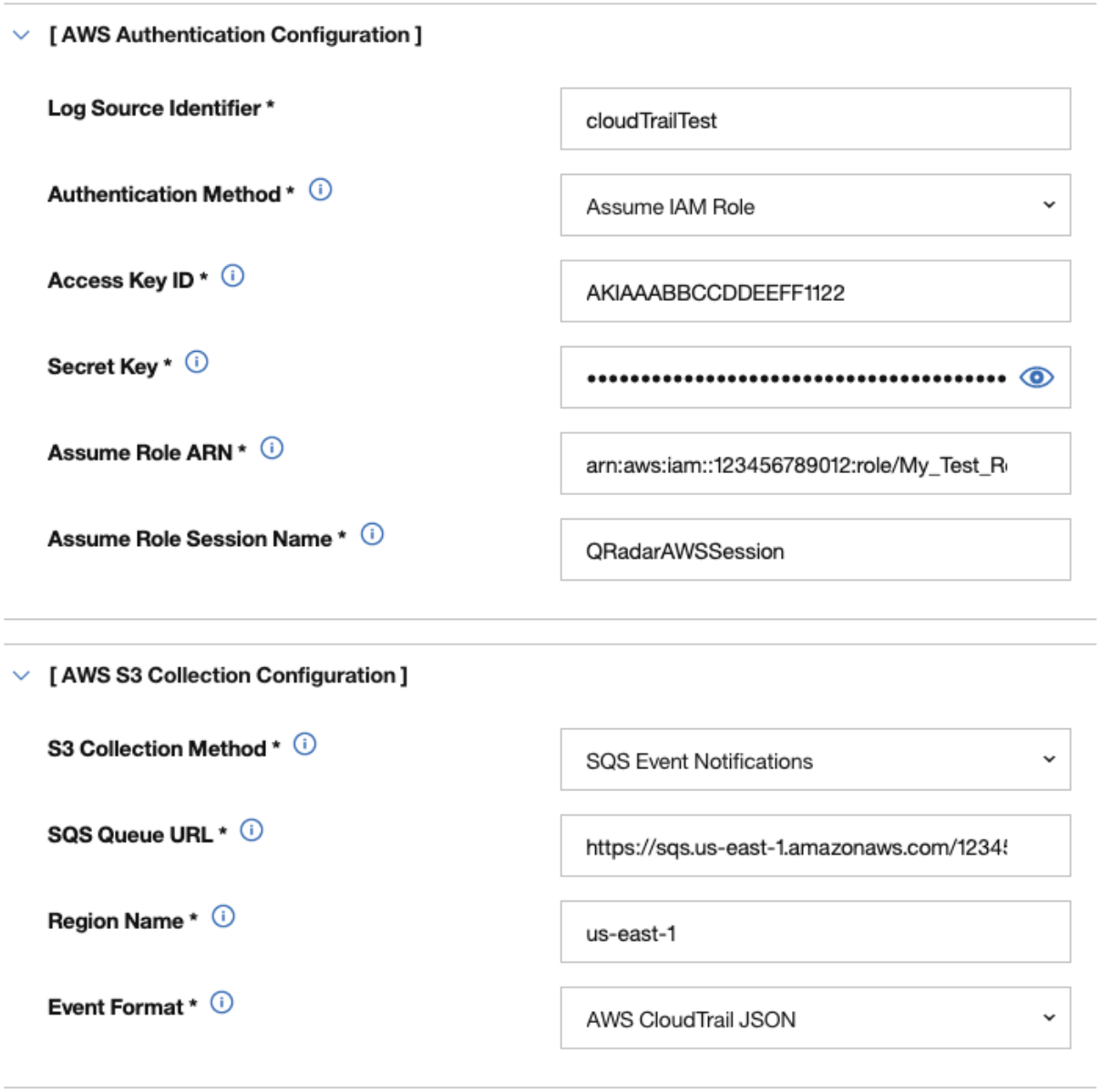


Figure 9. Example: Amazon AWS CloudTrail log source configuration in QRadar

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge

Create an Amazon EventBridge rule to forward ObjectCreated notifications to a target SQS queue.

Before you begin

Before you can create a rule in Amazon EventBridge, you must enable Amazon EventBridge on your AWS Management console. For more information, see Enabling Amazon EventBridge.

Procedure

1. Open the Amazon EventBridge console.
2. From the **Navigation** menu, click **Rules** > **Create rule**.
3. On the **Create rule** window, complete the following steps:
   a) Enter a name and description for the rule.

      Important: A rule can't have the same name as another rule that is both in the same region and on the same event bus.

   b) For **Event bus**, select the event bus that you want to associate with this rule. If you select **AWS default event bus**, the rule matches the events that come from your account.

   c) For **Rule type**, select **Rule with an event pattern**.
4. Click **Next**.
5. For **Event source**, select **AWS events or EventBridge partner events**.
6. For **Creation method**, select **Use pattern form**.
7. In the **Event pattern** window, configure the event pattern by completing the following steps:
   a) Select the values listed in the table for the following parameters:

Parameter	Value
Event source	**AWS services**
AWS service	**Simple Storage Service (S3)**
Event type	**Amazon S3 Event Notification**

   b) Click the **Specific event(s)** option and select **Object Created**.

c) Click **Specific bucket(s) by name** and enter the name of the specific bucket that you want to collect events from.

d) Optional: To enable notifications for a specific folder prefix or file extension, choose **Custom pattern (JSON editor)** instead of **Use pattern form** for the creation method, and create your custom event pattern.
For example, this event pattern filters for `Object Created` events in your bucket. In this example, `example/directory` is the directory prefix and `.png` is the suffix.

```
{
  "source": ["aws.s3"],
  "detail-type": ["Object Created"],
  "detail": {
    "bucket": {
      "name": ["<example-bucket>"]
    },
    "object": {
      "key": [{
        "prefix": "example/directory/"
      }],
      "key": [{
        "suffix": ".png"
      }]
    }
  }
}
```

e) Click **Add**, then click **Next**.

8. Choose the SQS queue that you want to use as the target. Enter the name of the queue, then click **Next**.
9. On the **Review and create** page, click **Create rule**.

Amazon AWS S3 REST API log source parameters for Amazon AWS Application Load Balancer Access Logs

If IBM QRadar does not automatically detect the log source, add an Amazon AWS Application Load Balancer Access Logs log source on the QRadar Console by using the Amazon AWS S3 REST API protocol.

When you use the Amazon AWS S3 REST API protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Amazon AWS S3 REST API events from Amazon AWS Application Load Balancer Access Logs:

Table 160. Amazon AWS S3 REST API protocol log source parameters for the Amazon AWS Application Load Balancer Access Logs DSM

Parameter	Value
Log Source type	Amazon AWS Application Load Balancer Access Logs
Protocol Configuration	Amazon AWS S3 REST API
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS Application Load Balancer Access Logs log source that is configured, you might want to identify the first log source as *awsalb1*, the second log source as *awsalb2*, and the third log source as *awsalb3*.
Event Format	LINEBYLINE

For a complete list of Amazon AWS S3 REST API protocol parameters and their values, see Amazon S3 REST API protocol configuration options.

Related tasks

Adding a log source

Amazon AWS Application Load Balancer Access Logs sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon AWS Application Load Balancer Access Logs sample message

The following sample event message uses the Amazon AWS REST API protocol and shows a log entry for an HTTPS listener setup on port 443 that forwards traffic to port 80, as specified in the rule configuration.

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com" "arn:aws:acm:us-
east-2:123456789012:certificate/12345678-1234-1234-1234-123456789012"
1 2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-" 10.0.0.1:80 200 "-" "-"
```

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188 192.168.131.39:2817
10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-
GCM-SHA256 TLSv1.2 arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com"
"arn:aws:acm:us-east-2:123456789012:certificate/12345678-1234-1234-1234-123456789012"1
2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-" 10.0.0.1:80 200 "-" "-"
```

Table 161. Highlighted values in the Amazon AWS Application Load Balancer Access Logs event payload

QRadar field name	Highlighted values in the event payload
Event ID	**https** + **authenticate,forward**
Source IP	**192.168.131.39**
Source Port	**2817**
Destination IP	**10.0.0.1**
Destination Port	**80**

Amazon AWS CloudTrail

The IBM QRadar DSM for Amazon AWS CloudTrail supports audit events that are collected from Amazon S3 buckets, and from a Log group in the AWS CloudWatch Logs.

The following table lists the specifications for the Amazon AWS CloudTrail DSM:

Table 162. Amazon AWS CloudTrail DSM specifications

Specification	Value
Manufacturer	Amazon
DSM	Amazon AWS CloudTrail
RPM name	DSM-AmazonAWSCloudTrail-*QRadar_version-Build_number*.noarch.rpm

Table 162. Amazon AWS CloudTrail DSM specifications (continued)	
Specification	**Value**
Supported protocols	• Amazon AWS S3 REST API • Amazon Web Services
Event format	Select **AWS CloudTrail JSON**. The log source retrieves JSON formatted events. **Important:** Only log files with the default CloudTrail log file name format can be collected. The filename format is *<AccountID>*_CloudTrail_*<RegionName>*_*<YYYYMMDDTHHmm>*Z_*UniqueString*.*<FileNameFormat>*. For example, `111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz`.
Recorded event types	Event versions 1.0, 1.02, 1.03, 1.04, 1.05, 1.06 and 1.08
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	For information about VPC Flow logs, see the Amazon website. For information about configuring QRadar V7.3.2 Fix Pack 1 in AWS Marketplace, see the 732 P1 Console available in AWS Marketplace video.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

“Configuring an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol” on page 301

If you want to collect AWS CloudTrail logs from Amazon S3 buckets, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

“Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol” on page 320

If you want to collect AWS CloudTrail logs from Amazon CloudWatch logs, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

“Configuring security credentials for your AWS user account” on page 310

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Configuring an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol

If you want to collect AWS CloudTrail logs from Amazon S3 buckets, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Amazon AWS S3 REST API Protocol RPM
   - DSMCommon RPM
   - Amazon Web Service RPM
   - Amazon AWS CloudTrail DSM RPM
2. Choose which method you will use to configure an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol.
   - "Configuring an Amazon AWS CloudTrail log source that uses an S3 bucket with an SQS queue" on page 301
   - "Configuring an Amazon AWS CloudTrail log source that uses an S3 bucket with a directory prefix" on page 314

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring an Amazon AWS CloudTrail log source that uses an S3 bucket with an SQS queue

If you want to collect AWS CloudTrail logs from multiple accounts or regions in an Amazon S3 bucket, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

About this task

Using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue instead of with a directory prefix has the following advantages:

- You can use one log source for an S3 bucket, rather than one log source for each region and account.
- There is a reduced chance of missing files because this method uses ObjectCreate notifications to determine when new files are ready.
- It's easy to balance the load across multiple Event Collectors because the SQS queue supports connections from multiple clients
- Unlike the directory prefix method, the SQS queue method does not require that the file names in the folders be in a string sorted in ascending order based on the full path. File names from custom applications don't always conform to this.
- You can monitor the SQS queue and set up alerts if it gets over a certain number of records. These alerts provide information about whether QRadar is either falling behind or not collecting events.
- You can use IAM Role authentication with SQS, which is Amazon's best practice for security.

- Certificate handling is improved with the SQS method and does not require the downloading of certificates to the Event Collector.

Procedure

1. Create the SQS queue that is used to receive ObjectCreated notifications.
2. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
3. Configure the security credentials for your AWS user account.
4. Add an Amazon AWS CloudTrail log source on the QRadar Console using an SQS queue

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.
5. Configuring security credentials for your AWS user account.
6. Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge.
7. Adding an Amazon AWS CloudTrail log source on the QRadar Console using an SQS queue.

Finding the S3 bucket that contains the data that you want to collect

You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **`Region Name`** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

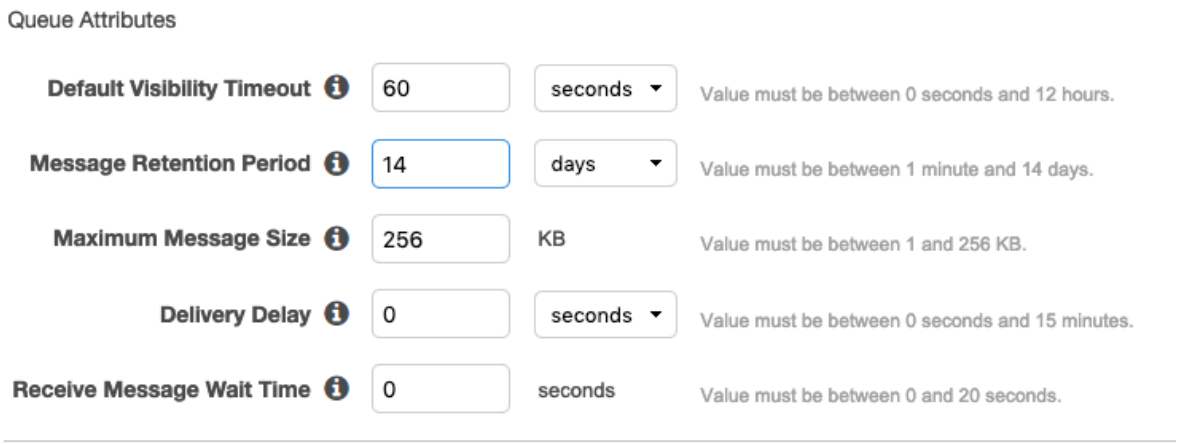
Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.

3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.
   - **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

   Use the default value for the remaining **Queue Attributes**.

   More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions
You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.
3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 163. Permission parameters	
Parameter	**Value**
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 164. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
      }
    }
  ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications
Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.
3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 165. Example: New ObjectCreated notification parameter configuration

Parameter	**Value**
Name	Type a name of your choosing.
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

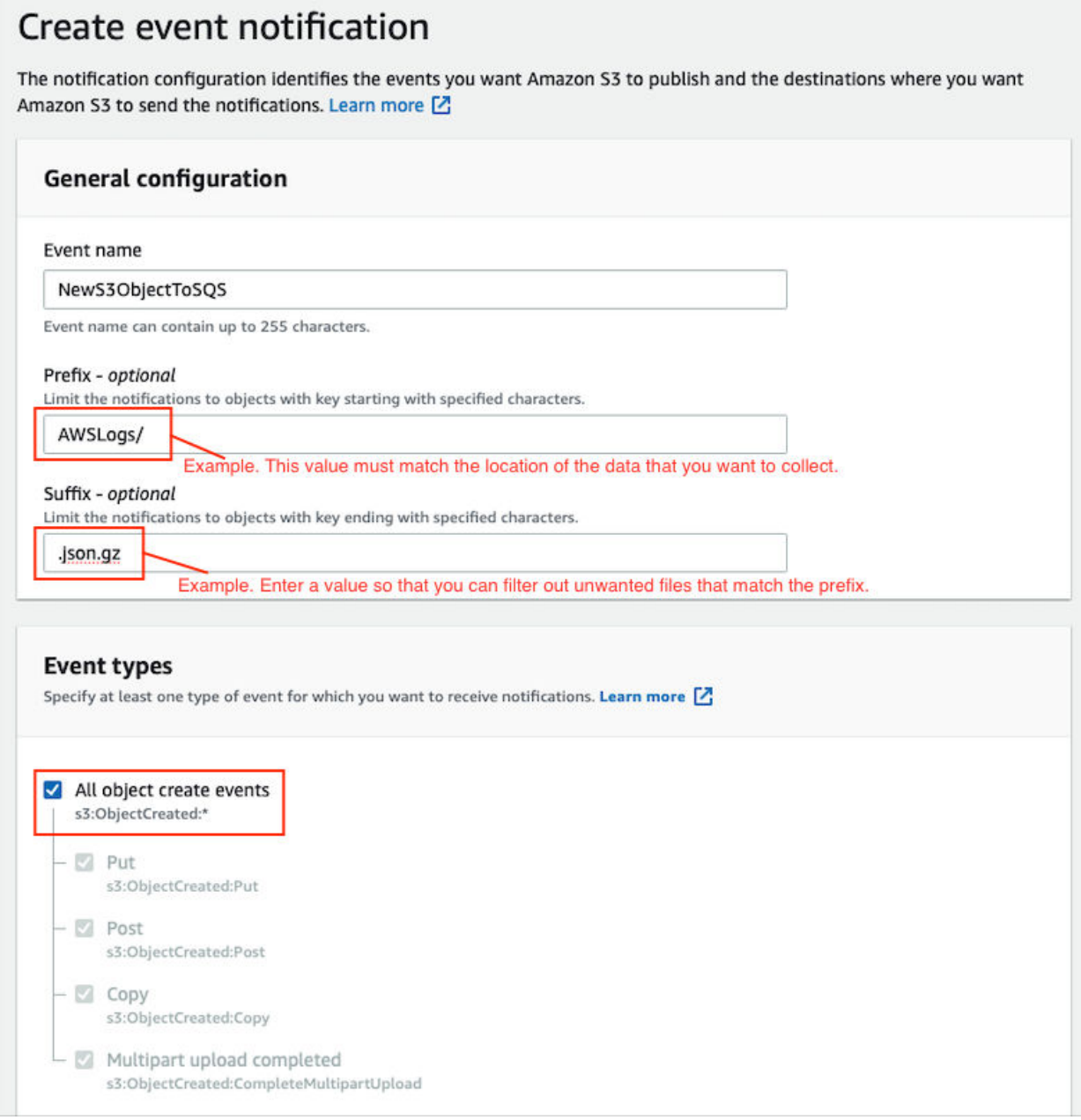


Figure 10. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

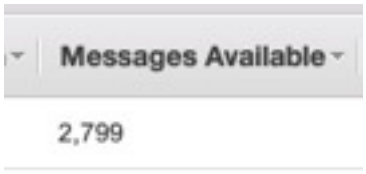


Figure 11. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

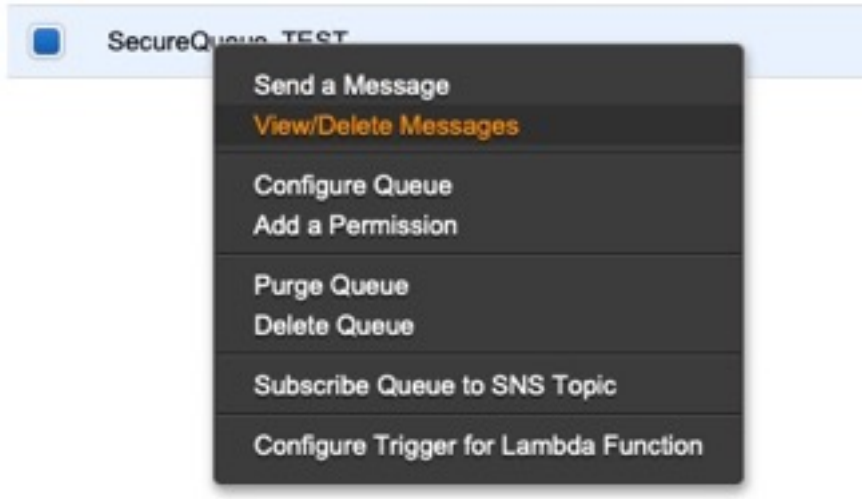


Figure 12. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

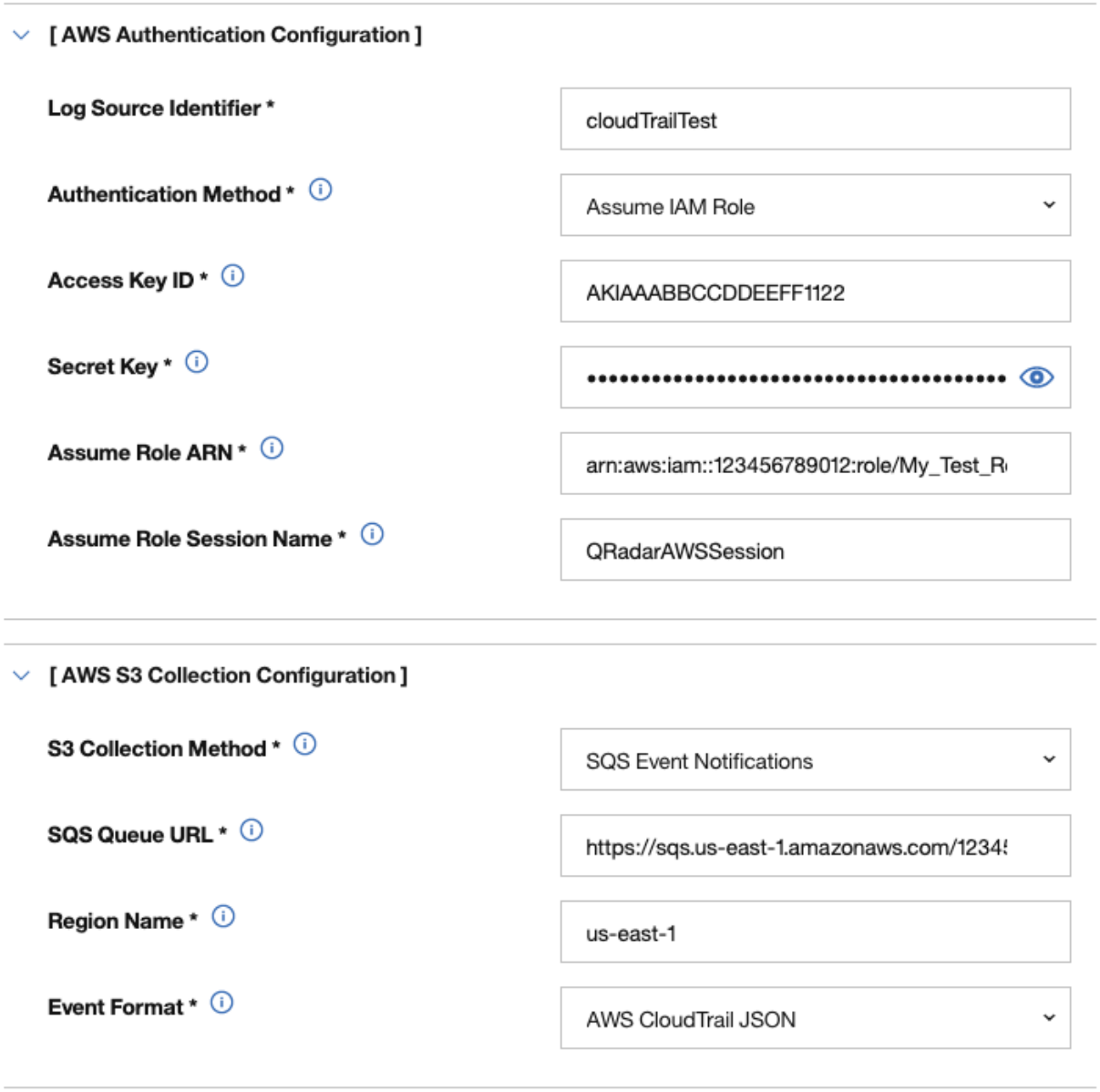


Figure 13. Example: Amazon AWS CloudTrail log source configuration in QRadar

Configuring security credentials for your AWS user account
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information
Adding a log source

Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge
Create an Amazon EventBridge rule to forward ObjectCreated notifications to a target SQS queue.

Before you begin

Before you can create a rule in Amazon EventBridge, you must enable Amazon EventBridge on your AWS Management console. For more information, see Enabling Amazon EventBridge.

Procedure

1. Open the Amazon EventBridge console.
2. From the **Navigation** menu, click **Rules** > **Create rule**.
3. On the **Create rule** window, complete the following steps:
   a) Enter a name and description for the rule.

      Important: A rule can't have the same name as another rule that is both in the same region and on the same event bus.

   b) For **Event bus**, select the event bus that you want to associate with this rule. If you select **AWS default event bus**, the rule matches the events that come from your account.

   c) For **Rule type**, select **Rule with an event pattern**.
4. Click **Next**.
5. For **Event source**, select **AWS events or EventBridge partner events**.
6. For **Creation method**, select **Use pattern form**.
7. In the **Event pattern** window, configure the event pattern by completing the following steps:
   a) Select the values listed in the table for the following parameters:

Parameter	Value
Event source	**AWS services**
AWS service	**Simple Storage Service (S3)**
Event type	**Amazon S3 Event Notification**

   b) Click the **Specific event(s)** option and select **Object Created**.

   c) Click **Specific bucket(s) by name** and enter the name of the specific bucket that you want to collect events from.

d) Optional: To enable notifications for a specific folder prefix or file extension, choose **Custom pattern (JSON editor)** instead of **Use pattern form** for the creation method, and create your custom event pattern.
For example, this event pattern filters for `Object Created` events in your bucket. In this example, `example/directory` is the directory prefix and `.png` is the suffix.

```
{
  "source": ["aws.s3"],
  "detail-type": ["Object Created"],
  "detail": {
    "bucket": {
      "name": ["<example-bucket>"]
    },
    "object": {
      "key": [{
        "prefix": "example/directory/"
      }],
      "key": [{
        "suffix": ".png"
      }]
    }
  }
}
```

e) Click **Add**, then click **Next**.

8. Choose the SQS queue that you want to use as the target. Enter the name of the queue, then click **Next**.
9. On the **Review and create** page, click **Create rule**.

Adding an Amazon AWS CloudTrail log source on the QRadar Console using an SQS queue
If you want to collect AWS CloudTrail logs from multiple accounts or regions in an Amazon S3 bucket, add a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

Procedure

1. Use the following table to set the parameters for an Amazon AWS CloudTrail log source that uses the Amazon AWS S3 REST API protocol and an SQS queue.

Table 166. Amazon AWS S3 REST API protocol log source parameters

Parameter	Description
Log Source Type	**Amazon AWS CloudTrail**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS CloudTrail log source that is configured, you might want to identify the first log source as *awscloudtrail1*, the second log source as *awscloudtrail2*, and the third log source as *awscloudtrail3*.

Table 166. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you select **SQS Event Notifications** for the **S3 Collection Method**. The supported **S3 Collection Method** is **Use a Specific Prefix**. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **AWS Cloud Trail JSON**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **SQS Event Notifications**.
SQS Queue URL	Enter the full URL, starting with `https://`, of the SQS queue that is set up to receive notifications for ObjectCreate events from S3.
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Log Source Identifier Pattern	This option is available when you set **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.

Table 166. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	How often a poll is made to scan for new data. If you are using the SQS event collection method, **SQS Event Notifications** can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, **Use a Specific Prefix** has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.

Table 166. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

Table 167. Amazon AWS CloudTrail sample message supported by Amazon AWS CloudTrail.		
Event name	**Low-level category**	**Sample log message**
Console Login	General Audit Event	{"eventVersion":"1.02", "userIdentity":{"type":"IAMUser", "principalId":"XXXXXXXXXXXXXXXXXXXXX", "arn":"arn:aws:iam::<Account_number>:user/ xx.xxccountId":"<Account_number>","userName": "<Username>"},"eventTime": "2016-05-04T14:10:58Z","eventSource": "f.amazonaws.com","eventName": "ConsoleLogin","awsRegion": "us-east-1","sourceIPAddress": "<Source_IP_address> Agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.1.1 Safari/537.36", "requestParameters":null, "responseElements": {"ConsoleLogin":"Success"}, "additionalEventData": {"LoginTo":"www.webpage.com", "MobileVersion":"No","MFAUsed":"No"}, "eventID":"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "eventType":"AwsConsoleSignIn", "recipientAccountId":"<Account_ID>"}

Configuring an Amazon AWS CloudTrail log source that uses an S3 bucket with a directory prefix

If you want to collect AWS CloudTrail logs from a single account and region in an Amazon S3 bucket, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol with a directory prefix.

About this task

If you have log sources in an S3 bucket from multiple regions or using multiple accounts, use the Amazon AWS S3 REST API protocol with an SQS queue instead of with a directory prefix.

Restriction: A log source using directory prefix can retrieve data from only one region and one account, so use a different log source for each region and account. Include the region folder name in the file path for the **`Directory Prefix`** value when you configure the log source.

Procedure

1. Finding an S3 bucket name and directory prefix.

2. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
3. Configure the security credentials for your AWS user account.
4. Add an Amazon AWS CloudTrail log source on the QRadar Console using a directory prefix.

Finding an S3 bucket name and directory prefix

An Amazon administrator must create a user and then apply the **AmazonS3ReadOnlyAccess** policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Note: Alternatively, you can assign more granular permissions to the bucket. The minimum required permissions are **s3:listBucket** and **s3:getObject**.

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Click **Services**.
2. From the list, select **Config**.
3. From the **Config** page, click the name of the Config.
4. Note the name of the S3 bucket that is displayed in the **S3 bucket** field.
5. Click the **Edit** icon.
6. Note the location path for the S3 bucket that is displayed underneath the **Log file prefix** field.

Creating an Identity and Access Management (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **s3:listBucket** and **s3:getObject** permissions to that user in the AWS Management Console. The QRadar user can then create a log source in QRadar.

About this task

The minimum required permissions are **s3:listBucket** and **s3:getObject**. You can assign other permissions to the user as needed.

Sample policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>",
                "arn:aws:s3:::<bucket_name>/AWSLogs/<AWS_account_number>/<DSM_name>/us-east-1/*"
            ]
        }
    ]
}
```

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**.

3. From the list, select **IAM**.
4. Click **Users** > **Add user**.
5. Create an Amazon AWS IAM user and then apply the **AmazonS3ReadOnlyAccess** policy.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Adding an Amazon AWS CloudTrail log source on the QRadar Console using a directory prefix

If you want to collect AWS CloudTrail logs from a single account and region in an Amazon S3 bucket, add a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol with a directory prefix.

Procedure

1. Use the following table to set the parameters for an Amazon AWS CloudTrail log source that uses the Amazon AWS S3 REST API protocol and a diretcory prefix.

Table 168. Amazon AWS S3 REST API protocol log source parameters

Parameter	Description
Log Source Type	**Amazon AWS CloudTrail**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS CloudTrail log source that is configured, you might want to identify the first log source as *awscloudtrail1*, the second log source as *awscloudtrail2*, and the third log source as *awscloudtrail3*.

Table 168. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see "Configuring security credentials for your AWS user account" on page 310. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you select **SQS Event Notifications** for the **S3 Collection Method**. The supported **S3 Collection Method** is **Use a Specific Prefix**. For more information about creating IAM users and assigning roles, see Creating an IAM user in the AWS Management Console. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **AWS Cloud Trail JSON**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **Use a Specific Prefix**.
Bucket Name	The name of the AWS S3 bucket where the log files are stored.

Table 168. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Directory Prefix	The root directory location on the AWS S3 bucket from where the CloudTrail logs are retrieved; for example, `AWSLogs/<AccountNumber>/CloudTrail/<RegionName>/` To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path. **Note:** • Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. • The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket. • If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use `folder1/folder2` instead).
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Log Source Identifier Pattern	This option is available when you set **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.

Table 168. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	How often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieves them. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 1 minute. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15 M = 15 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

Table 169. Amazon AWS CloudTrail sample message supported by Amazon AWS CloudTrail.

Event name	Low-level category	Sample log message
Console Login	General Audit Event	{"eventVersion":"1.02", "userIdentity":{"type":"IAMUser", "principalId":"XXXXXXXXXXXXXXXXXXXXX", "arn":"arn:aws:iam::<Account_number>:user/ xx.xxccountId":"<Account_number>","userName": "<Username>"},"eventTime": "2016-05-04T14:10:58Z","eventSource": "f.amazonaws.com","eventName": "ConsoleLogin","awsRegion": "us-east-1","sourceIPAddress": "<Source_IP_address> Agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.1.1 Safari/537.36", "requestParameters":null, "responseElements": {"ConsoleLogin":"Success"}, "additionalEventData": {"LoginTo":"www.webpage.com", "MobileVersion":"No","MFAUsed":"No"}, "eventID":"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "eventType":"AwsConsoleSignIn", "recipientAccountId":"<Account_ID>"}

Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol

If you want to collect AWS CloudTrail logs from Amazon CloudWatch logs, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common
   - Amazon AWS REST API Protocol RPM
   - Amazon Web Services Protocol RPM
   - DSMCommon RPM
   - Amazon AWS CloudTrail DSM RPM
2. Choose which method you will use to configure an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol.
   - “Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and Kinesis Data Streams” on page 321
   - “Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and CloudWatch Logs” on page 326

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5
“Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and CloudWatch Logs” on page 326

If you want to collect AWS CloudTrail logs from Amazon CloudWatch logs, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

"Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and Kinesis Data Streams" on page 321
If you want to collect AWS CloudTrail logs from Amazon Kinesis Data Streams, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and Kinesis Data Streams

If you want to collect AWS CloudTrail logs from Amazon Kinesis Data Streams, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. Follow the procedures in the AWS online documentation Sending Events to CloudWatch Logs (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/send-cloudtrail-events-to-cloudwatch-logs.html) to configure CloudTrail to deliver the logs in a log group of the AWS CloudWatch Logs.
2. Create CloudWatch Logs destinations and a CloudWatch Logs subscription filter.

   For more information about CloudWatch Logs Destinations and Subscriptions, see Cross-Account Log Data Sharing with Subscriptions.

   a) Create a CloudWatch Logs destination that points to a destination Kinesis Data Stream.

      Only one CloudWatch Logs destination is required per region and the destination Kinesis Data Stream can be in any region.

   b) Create a CloudWatch Logs subscription filter with a blank filter pattern to subscribe the destination to the CloudWatch Logs log group and match all events.

   The subscription filter is now associated with a Cloud Watch Logs log group that contains AWS CloudTrail logs, and delivers those logs to a Kineses Data Stream.
3. Add an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and Kinesis Data Streams.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Related information

Adding an Amazon CloudFront log source by using the Amazon Web Services protocol and Kinesis Data Streams

If you want to collect AWS CloudTrail logs from Amazon Kinesis Data Streams, add a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. Use the following table describes the parameters that require specific values to collect audit events from Amazon AWS CloudTrail by using the Amazon Web Services protocol:

Table 170. Amazon Web Services log source parameters for Amazon Kinesis Data Streams	
Parameter	**Description**
Protocol Configuration	Select **Amazon Web Services** from the Protocol Configuration list.
Authentication Method	**Access Key ID/Secret Key** Standard authentication that can be used from anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.
Assume an IAM Role	Enable this option to authenticate with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "`arn:`" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This parameter can contain only upper and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.
Assume Role External ID	**Assume Role External ID** is an optional identifier that is required to assume a role in a different account. If the account administrator, to which the role belongs, provides you with an external ID, then insert that value in the **Assume Role External ID** parameter. This value can either be a string, a passphrase, a GUID, or an account number. For more information, see AWS documentation Using an external ID for third-party access.
Regions	Toggle each region that is associated with the Amazon Web Service that you want to collect logs from.
AWS Service	From the **AWS Service** list, select **Kinesis Data Streams**.
Kinesis Data Stream	The Kinesis Data Stream from which to consume data.

Table 170. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Enable Kinesis Advanced Options	Enable the following optional advanced configuration values. Advanced option values are only used when this option is chosen; otherwise, the default values are used. **Initial Position in Stream** This option controls which data to pull on a newly configured log source. Select **Latest** to pull the latest data that is available. Select **Trim Horizon** to pull the oldest data that is available. **Kinesis Worker Thread Count** The number of worker threads to use for Kinesis Data Stream processing. Each worker thread can process approximately 10000 - 20000 events per second depending on record size and system load. If your log source is not able to process the new data in the stream, you can increase the number of threads here to a maximum of 16. The allowed range is 1 - 16. The default value is 2. **Checkpoint Interval** The interval (in seconds) at which to checkpoint data sequence numbers. Each record from a shard in a Kinesis Data Stream has a sequence number. Checkpointing your position allows this shard to resume processing at the same point if processing fails or a service restarts. A more frequent interval reduces data duplication but increases Amazon Dynamo DB usage. The allowed range is 1 - 3600 seconds. The default is 10 seconds. **Kinesis Application** Leave this option blank to have this log source consume data from all available shards in the Kinesis Data Stream. To have multiple log sources on multiple event processors scale log consumption without loss or duplication, use a common Kinesis Application across those log sources (Example: ProdKinesisConsumers). **Partition** Select this option to collect data from a specific partition in the Kinesis Data Stream by specifying a partition name.

Table 170. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Extract Original Event	Forwards only the original event that was added to the Kinesis Data Stream. Kinesis logs wrap the events that they receive with extra metadata. Select this option if you want only the original event that was sent to AWS without the additional stream metadata through Kinesis. The original event is the value for the message key that is extracted from the Kinesis log. The following Kinesis logs event example shows the original event that is extracted from the Kinesis log in highlighted text: `{"owner":"123456789012","subscriptionFilters":["allEvents"], "logEvents": [{"id":"35093963143971327215510178578576502306458824699048362100", "message":"{\"eventVersion\":\"1.05\",\"userIdentity\": {\"type\":\"AssumedRole\", \"principalId\":\"ARO1GH58EM3ESYDW3XHP6:test_session\",\"arn\":\"arn :aws:sts::123456789012:assumed-role\/CVDevABRoleToBeAssumed\/ test_visibility_session\", \"accountId\":\"123456789012\",\"accessKeyId\":\"ASIAXXXXXXXXXXXXXXX X\",\"sessionContext\":{\"sessionIssuer\": {\"type\":\"Role\",\"principalId\":\"AROAXXXXXXXXXXXXXXXX\", \"arn\":\"arn:aws:iam::123456789012:role\/ CVDevABRoleToBeAssumed\",\"accountId\":\"123456789012\", \"userName\":\"CVDevABRoleToBeAssumed\"},\"webIdFederationData\": {},\"attributes\":{\"mfaAuthenticated\":\"false\", \"creationDate\":\"2019-11-13T17:01:54Z\"}}},\"eventTime\":\"2019-11 -13T17:43:18Z\",\"eventSource\":\"cloudtrail.amazonaws.com\", \"eventName\":\"DescribeTrails\",\"awsRegion\":\"ap- northeast-1\",\"sourceIPAddress\":\"192.0.2.1\",\"requestParameters\ ":null,\"responseElements\":null, \"requestID\":\"41e62e80-b15d-4e3f-9b7e- b309084dc092\",\"eventID\":\"904b3fda-8e48-46c0-a923- f1bb2b7a2f2a\",\"readOnly\":true,\"eventType\":\"AwsApiCall\", \"recipientAccountId\":\"123456789012\"}","timestamp":1573667733143}],"messageType":"DATA_MESSAGE","logGroup":"CloudTrail\/ DefaultLogGroup","logStream":"123456789012_CloudTrail_us-east-2_2"}` {: .codeblock}
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events that are being processed.

Table 170. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   The actual CloudTrail logs are wrapped in a Kinesis Data Streams JSON payload:

Table 171. Kinesis Data Streams sample message supported by the Amazon AWS CloudTrail DSM

Event name	Low-level category	Sample log message
Describe Trails	Read Activity Attempted	{"owner":"123456789012","subscriptionFilters":["allEvents"], "logEvents": [{"id":"35101382794889527301913782399021634305485606205478862909", **"message":"{\"eventVersion\":\"1.05\",\"userIdentity\":{\"type\":\ "AssumedRole\",\"principalId\":\"AROA3GFMEP3ESYDW3XHP6: cloud_visibility_session\",\"arn\":\"arn:aws:sts::123456789012: assumed-role\/CVDevABRoleToBeAssumed\/cloud_visibility_session\", \"accountId\":\"123456789012\",\"accessKeyId\": \"ASIA3ABCDE3E6ZUV7IF5\",\"sessionContext\":{\"sessionIssuer\": {\"type\":\"Role\",\"principalId\":\"AROA3GABCD3ESYDW3XHP6\",\"arn\ ":\"arn:aws:iam::123456789012:role\/CVDevABRoleToBeAssumed\", \"accountId\":\"123456789012\"\"userName\":\ "CVDevABRoleToBeAssumed\"},\"webIdFederationData\":{},\ "attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\ "2019-11-17T13:34:07Z\"}}},\"eventTime\":\"2019-11-17T14:10:48Z\", \"eventSource\":\"cloudtrail.amazonaws.com\",\"eventName\":\ "DescribeTrails\",\"awsRegion\":\"ap-northeast-3\", \"sourceIPAddress\":\"192.0.2.1\",\"requestParameters\":null, \"responseElements\":null,\"requestID\":\ "31afb5b7-6857-467a-bce4-835ee7d02ad2\",\"eventID\": \"26caf544-010c-423a-88a1-ca71cbd243ca\",\"readOnly\" :true,\"eventType\":\"AwsApiCall\",\"recipientAccountId\":\ "123456789012\"}"**,"timestamp":1574000441797}],"messageType": "DATA_MESSAGE","logGroup":"CloudTrail\/DefaultLogGroup", "logStream":"123456789012_CloudTrail_us-east-2"}

Configuring an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and CloudWatch Logs

If you want to collect AWS CloudTrail logs from Amazon CloudWatch logs, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. “Creating an Identity and Access (IAM) user in the AWS Management Console” on page 326
2. “Creating a log group in Amazon CloudWatch Logs to retrieve logs in QRadar” on page 327
3. “Configure Amazon AWS CloudTrail to send log files to CloudWatch Logs” on page 327
4. “Configuring security credentials for your AWS user account” on page 327
5. “Adding an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and CloudWatch Logs” on page 327

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Creating an Identity and Access (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **CloudWatchLogsReadOnlyAccess** policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Create an Amazon AWS IAM user and then apply the **CloudWatchLogsReadOnlyAccess** policy.

What to do next

Amazon Web Services log source parameters for Amazon AWS Security Hub

Creating a log group in Amazon CloudWatch Logs to retrieve logs in QRadar

You must create a log group in Amazon CloudWatch Logs to make the log available for QRadar polling.

Procedure

1. Log in to your CloudWatch console (https://console.aws.amazon.com/cloudwatch).
2. Select **Logs** from left navigation pane.
3. Click **Actions** > **Create Log Group**.
4. Type the name of your log group. For example, `CloudTrailAuditLogs`.
5. Click **Create log group**.

   For more information about working with log groups and log streams, see https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working-with-log-groups-and-streams.html

Configure Amazon AWS CloudTrail to send log files to CloudWatch Logs

You must configure CloudTrail to deliver the logs in a log group of the AWS CloudWatch Logs.

Follow the procedures in the AWS online documentation Sending Events to CloudWatch Logs.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Adding an Amazon AWS CloudTrail log source by using the Amazon Web Services protocol and CloudWatch Logs

If you want to collect AWS CloudTrail logs from Amazon CloudWatch logs, add a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. Use the following table describes the parameters that require specific values to collect audit events from Amazon AWS CloudTrail by using the Amazon Web Services protocol:

Table 172. Amazon Web Services log source parameters for AWS CloudWatch Logs

Parameter	Description
Protocol Configuration	Select **Amazon Web Services** from the Protocol Configuration list.

Table 172. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)

Parameter	Description
Authentication Method	**Access Key ID/Secret Key** Standard authentication that can be used from anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.
Assume an IAM Role	Enable this option by authenticating with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "`arn:`" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This parameter can contain only upper and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.

Table 172. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)

Parameter	Description
Assume Role External ID	**Assume Role External ID** is an optional identifier that is required to assume a role in a different account. If the account administrator, to which the role belongs, provides you with an external ID, then insert that value in the **Assume Role External ID** parameter. This value can either be a string, a passphrase, a GUID, or an account number. For more information, see AWS documentation Using an external ID for third-party access.
Regions	Toggle each region that is associated with the Amazon Web Service that you want to collect logs from.
AWS Service	From the **AWS Service** list, select **CloudWatch Logs**.
Log Group	The name of the log group in Amazon CloudWatch where you want to collect logs from. **Tip:** A single log source collects CloudWatch Logs from one log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group.
Enable CloudWatch Advanced Options	Enable the following optional advanced configuration values. Advanced option values are only used when this option is chosen; otherwise, the default values are used. **Log Stream** The name of the log stream within a log group. If you want to collect logs from all log streams within a log group, leave this field blank. **Filter Pattern** Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specified are collected from CloudWatch Logs. If you type ACCEPT as the Filter Pattern value, only the events that contain the word ACCEPT are collected, as shown in the following example. `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Event Delay** Delay in seconds for collecting data. **Other Region(s)** Deprecated. Use **Regions** instead.

Table 172. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)

Parameter	Description
Extract Original Event	Forwards only the original event that was added to the CloudWatch Logs. CloudWatch logs wrap the events that they receive with extra metadata. Select this option if you want to collect only the original event that was sent to AWS without the additional stream metadata through CloudWatch Logs. The original event is the value for the message key that is extracted from the CloudWatch log. The following CloudWatch Logs event example shows the original event that is extracted from CloudWatch Logs in highlighted text: `{LogStreamName: 123456786_CloudTrail_us-east-2,` `Timestamp: 1505744407363, Message:` **`{"eventVersion":"1.05","userIdentity":`** **`{"type":`** **`"IAMUser","principalId":"AAAABBBCCCDDDBBBCCC",`** **`"arn":"arn:aws:iam::1234567890:user/<username>",`** **`"accountId":"1234567890","accessKeyId":`** **`"AAAABBBBCCCCDDDD","userName":"User-Name",`** **`"sessionContext":{"attributes":`** **`{"mfaAuthenticated":"false","creationDate":`** **`"2017-09-18T13:22:10Z"}},"invokedBy":`** **`"signin.amazonaws.com"},"eventTime":`** **`"2017-09-18T14:10:15Z","eventSource":`** **`"cloudtrail.amazonaws.com","eventName":`** **`"DescribeTrails","awsRegion":"us-east-1",`** **`"sourceIPAddress":"192.0.2.1","userAgent":`** **`"signin.amazonaws.com","requestParameters":`** **`{"includeShadowTrails":false,"trailNameList":`** **`[]},"responseElements":null,"requestID":`** **`"11b1a00-7a7a-11a1-1a11-44a4aaa1a","eventID":`** **`"a4914e00-1111-491d-bbbb-a0dd3845b302",`** **`"eventType":"AwsApiCall","recipientAccountId":`** **`"1234567890"}`**`,IngestionTime: 1505744407506,` `EventId:` `335792223611111122479126672222222513333}`
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events that are being processed.

Table 172. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)

Parameter	Description
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.

Table 172. Amazon Web Services log source parameters for AWS CloudWatch Logs (continued)	
Parameter	**Description**
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   The actual CloudTrail logs are wrapped in a CloudWatch logs JSON payload:

Table 173. Amazon CloudTrail Logs sample message supported by the Amazon AWS CloudTrail DSM		
Event name	**Low-level category**	**Sample log message**
Describe Trails	Read Activity Attempted	{LogStreamName: 1234567890_CloudTrail_us -east-2,Timestamp: 1505744407363,Message: **{"eventVersion":"1.05","userIdentity":{"type" :"IAMUser","principalId":"AIDAIEGANDWTHAAUMATYA", "arn":"arn:aws:iam::1234567890:user/QRadar-ITeam", "accountId":"1234567890","accessKeyId": "AAAABBBBCCCCDDDD","userName":"QRadar-ITeam", "sessionContext":{"attributes":{"mfaAuthenticated": "false","creationDate":"2017-09-18T13:22:10Z"}}, "invokedBy":"signin.amazonaws.com"},"eventTime": "2017-09-18T14:10:15Z","eventSource": "cloudtrail.amazonaws.com","eventName": "DescribeTrails","awsRegion":"us-east-1", "sourceIPAddress":"127.0.0.1","userAgent": "signin.amazonaws.com","requestParameters": {"includeShadowTrails":false,"trailNameList": []},"responseElements":null,"requestID": "17b7a04c-99cca-11a1-9d83-43d5bce2d2fc", "eventID":"a4444e00-55e5-4444-bbbb-a0dd3845b302", "eventType":"AwsApiCall","recipientAccountId": "1234567890"}**,IngestionTime: 1505744407506, EventId: 335792223627111111111111222222222222}

Configuring an Amazon AWS CloudTrail log source that uses Amazon Security Lake

You can collect AWS CloudTrail logs from multiple accounts or regions in an Amazon S3 bucket. IBM QRadar uses the Amazon AWS S3 REST API protocol to communicate with Amazon Security Lake, where QRadar obtains the CloudTrail logs.

Procedure

1. Configure Amazon Security Lake to log Open Cybersecurity Schema Framework (OCSF) data in Parquet format to an S3 bucket. For more information, see Collecting data from custom sources.

   Note: The supported OCSF version of the DSM is OCSF 1.0RC2. The version OCSF 1.1 is not currently supported.
2. Configure access to the OCSF data in Amazon Security Lake by using one of two methods.
   - To create a subscriber to provision the SQS queue and IAM role, see step 3.

     For more information about creating a subscriber, see Managing data access for Security Lake subscribers.
   - To manually configure the SQS queue and ObjectCreated notifications, see step 4.
3. Create a subscriber to provision the SQS queue and IAM role.
   a) When you create the subscription, take note of the following values: **SQS Queue URL**, **IAM Role ARN**, and **External ID**.
   b) If you plan to access this subscription from a different account than where Amazon Security Lake is set up, you must provide that account ID to configure the trust relationship properly.
4. Manually configure the SQS queue and ObjectCreated notifications.
   a) Configure an SQS queue to receive ObjectCreated notifications with either Amazon S3 Event Notifications or AWS EventBridge when new OCSF Parquet data is available in the Amazon Security Lake bucket in the folder you choose.
   b) Provision access keys with permission (either directly or with an **IAM Assume Role**) to access both the SQS queue and the bucket that contain the Amazon Security Lake data.

   For more information, see Create SQS and S3 object REST API.
5. Configure a log source in QRadar to collect and parse the data.

   Tip: When new OCSF parquet data is available, a message that contains the bucket name and object key of the file with the data to be processed is sent to the SQS queue. QRadar then downloads and processes this file.

What to do next

Add a CloudTrail log source in QRadar. For more information, see “Adding an Amazon AWS CloudTrail log source on the QRadar Console using an SQS queue” on page 311.

Related information

What Is Amazon EventBridge?

Amazon S3 Event Notifications

Amazon AWS CloudTrail sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon AWS CloudTrail sample message when you use the Amazon REST API protocol

The following sample event message shows the specified managed policy that is attached to a specified user.

```
{"eventVersion":"1.05","userIdentity":
{"type":"Root","principalId":"555555555555","arn":"arn:aws:iam::555555555555:root","accountId":"
555555555555","accessKeyId":"AAAAAA1AAAAA1A1AAA11","sessionContext":{"attributes":
{"mfaAuthenticated":"false","creationDate":"2019-06-11T16:43:07Z"}},"invokedBy":"signin.qradar.e
xample.test"},"eventTime":"2019-06-11T16:54:03Z","eventSource":"iam.qradar.example.test","eventN
ame":"AttachUserPolicy","awsRegion":"us-
east-1","sourceIPAddress":"172.16.89.242","userAgent":"signin.qradar.example.test","requestParam
eters":{"userName":"sampleuser","policyArn":"arn:aws:iam::aws:policy/
AmazonEC2ContainerRegistryFullAccess"},"responseElements":null,"requestID":"849df62f-8c69-11e9-
bb3c-
abc750f0b415","eventID":"bdcc7610-7f82-4cde-9f6e-1c3cb1927353","eventType":"AwsApiCall","recipie
ntAccountId":"555555555555"}
```

Amazon AWS CloudTrail sample message when you use the Amazon Web Services protocol

The following sample event message describes trails.

```
{LogStreamName: 111111111111_CloudTrail_us-east-2,Timestamp: 1505744407363,Message:
{"eventVersion":"1.05","userIdentity":
{"type":"IAMUser","principalId":"AAAAAAAAAAAAAAAAAAAAA","arn":"arn:aws:iam::111111111111:user/
Test-User","accountId":"111111111111","accessKeyId":"AAAAA1A1AA1AA1111AAA","userName":"Test-
User","sessionContext":{"attributes":
{"mfaAuthenticated":"false","creationDate":"2017-09-18T13:22:10Z"}},"invokedBy":"sub.domain.test
"},"eventTime":"2017-09-18T14:10:15Z","eventSource":"sub2.domain.test","eventName":"DescribeTrai
ls","awsRegion":"us-
east-1","sourceIPAddress":"192.168.10.187","userAgent":"sub.domain.test","requestParameters":
{"includeShadowTrails":false,"trailNameList":
[]},"responseElements":null,"requestID":"17b7a04c-9c7b-11e7-9d83-43d5bce2d2fc","eventID":"a4914e
00-65e5-491d-b1c6-
a0dd3845b302","eventType":"AwsApiCall","recipientAccountId":"111111111111"},IngestionTime:
1505744407506,EventId: 335792223627147609224791266721200538665139324678441533 44}
```

AWS Config

The IBM QRadar DSM for AWS Config supports events that are collected from Amazon S3 buckets, and from a Log group in the AWS Config Logs.

The following table lists the specifications for the AWS Config DSM:

Table 174. AWS Config DSM specifications

Specification	Value
Manufacturer	Amazon
DSM	AWSConfig
RPM name	DSM-AWSConfig-*QRadar_version-Build_number*.noarch.rpm
Supported protocols	• AmazonAWS S3 REST API • Syslog
Event format	JSON
Automatically discovered?	Yes
Includes identity?	No

Table 174. AWS Config DSM specifications (continued)	
Specification	**Value**
Includes custom properties?	Yes
More information	AWS Config

If you want to collect AWS Config logs from Amazon S3 buckets, configure a log source on the QRadar Console so that AWS Config can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar. For more information, see Configuring security credentials for your AWS user account.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

"Configuring an Amazon AWS Config log source by using the Amazon AWS S3 REST API protocol" on page 336

If you want to collect AWS Config logs from Amazon S3 buckets, configure a log source on the QRadar Console so that AWS Config can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

Enabling AWS Config logs

When you enable AWS Config logs, you must specify a destination for the log data.

About this task

Users must have the following permissions to enable AWS Config logs for delivery to Amazon S3.

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` on the Config instance
- `logs:CreateLogDelivery, logs:DeleteLogDelivery, logs:GetLogDelivery, logs:ListLogDeliveries`, and `logs:UpdateLogDelivery` on all resources
- `s3:GetBucketPolicy` and `s3:PutBucketPolicy` on the destination bucket

Procedure

1. Open the Amazon VPC console at Amazon VPC.
2. In the navigation pane, select **AWS Config**.
3. Select AWS Config.
4. On the **AWS Config logging configuration** tab, select `Modify AWS Config logging configuration`.
5. Enable **Deliver to Amazon S3**.
6. Enter the name, owner, and prefix of the destination bucket.
7. Click **Modify AWS Config logging configuration**.

Configuring an Amazon AWS Config log source by using the Amazon AWS S3 REST API protocol

If you want to collect AWS Config logs from Amazon S3 buckets, configure a log source on the QRadar Console so that AWS Config can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Amazon AWS S3 REST API Protocol RPM
   - DSM Common RPM
   - Amazon Web Service RPM
   - AWS Config DSM RPM
   - Select a method to configure an AWS Config log source by using the Amazon AWS S3 REST API protocol.
2. Select one of the following methods to configure an AWS Config log source by using the Amazon AWS S3 REST API protocol.
   - “Configuring an AWS Config log source that uses an S3 bucket with an SQS queue” on page 336.
   - “Configuring an AWS Config log source that uses an S3 bucket with a directory prefix” on page 348.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring an AWS Config log source that uses an S3 bucket with an SQS queue

If you want to collect AWS Config logs from multiple accounts or regions in an Amazon S3 bucket, configure a log source on the QRadar Console so that AWS Config can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

About this task

Using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue instead of with a directory prefix has the following advantages:

- You can use one log source for an S3 bucket, rather than one log source for each region and account.
- There is a reduced chance of missing files because this method uses ObjectCreated notifications to determine when new files are ready.
- It's easy to balance the load across multiple Event Collectors because the SQS queue supports connections from multiple clients.
- Unlike the directory prefix method, the SQS queue method does not require that the file names in the folders be in a string that is sorted in ascending order based on the full path. File names from custom applications don't always conform to this.
- You can monitor the SQS queue and set up alerts if it gets over a certain number of records. These alerts provide information about whether QRadar is either falling behind or not collecting events.
- You can use IAM Role authentication with SQS, which is Amazon's best practice for security.
- Certificate handling is improved with the SQS method and does not require the downloading of certificates to the Event Collector.

Procedure

1. Create the SQS queue that is used to receive ObjectCreated notifications.
2. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
3. Configure the security credentials for your AWS user account.
4. Add an AWS Config log source on the QRadar Console that uses an SQS queue.

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.
5. Configuring security credentials for your AWS user account.
6. Adding an AWS Config log source on the QRadar Console using an SQS queue.

Finding the S3 bucket that contains the data that you want to collect

You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **`Region Name`** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

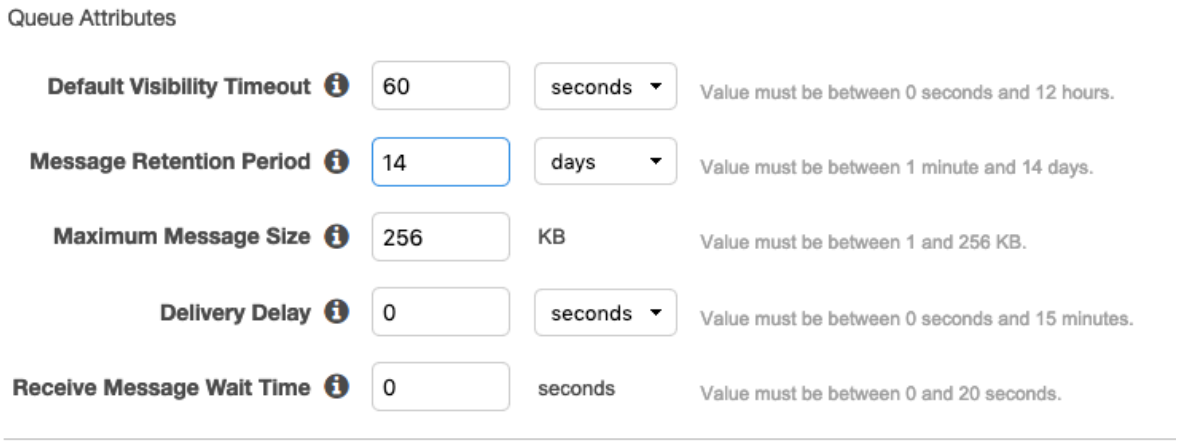
Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.
3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.

- **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
- **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

Use the default value for the remaining **Queue Attributes**.

More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions
You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.
3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 175. Permission parameters

Parameter	Value
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.

Table 175. Permission parameters (continued)	
Parameter	**Value**
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 176. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
      }
    }
  ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications
Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.

3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 177. Example: New ObjectCreated notification parameter configuration

Parameter	Value
Name	Type a name of your choosing.
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

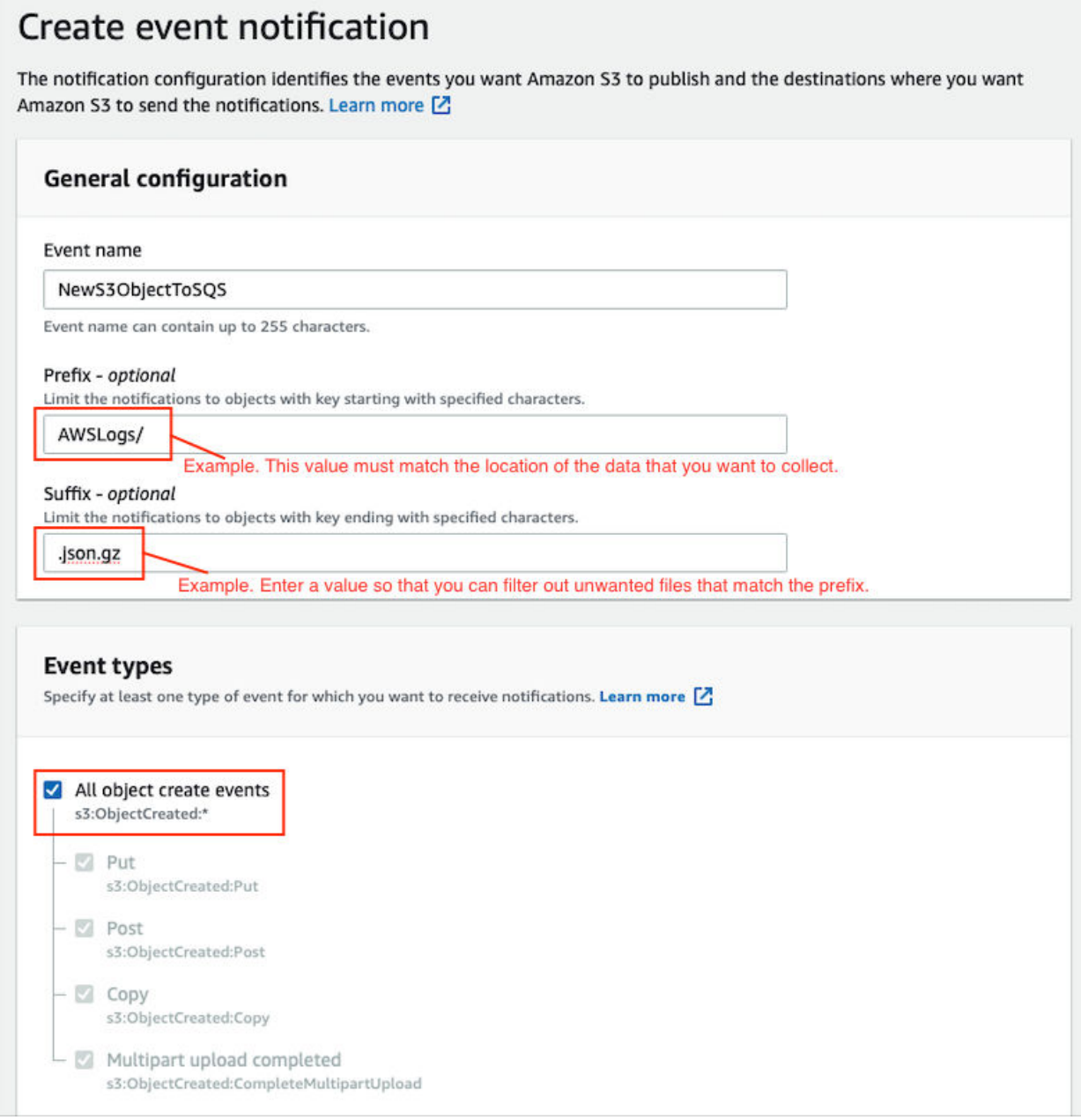


Figure 14. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

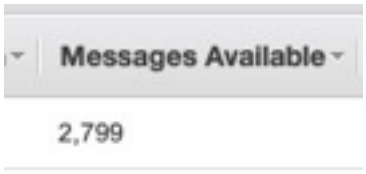


Figure 15. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

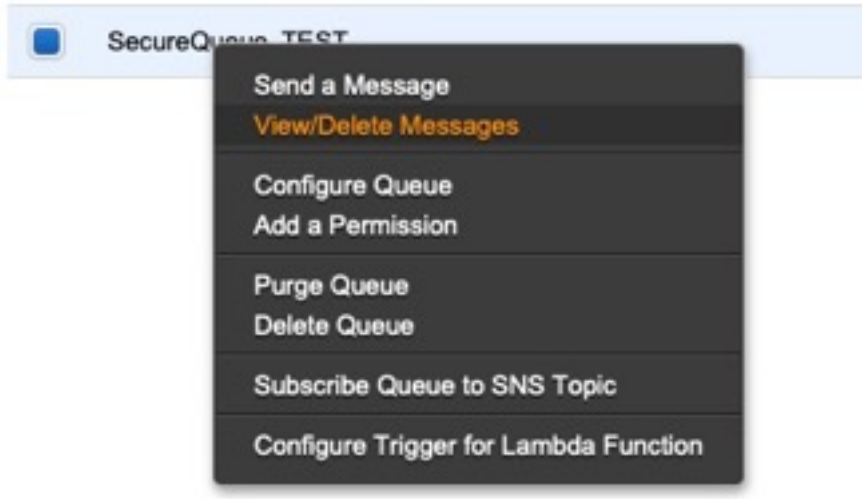


Figure 16. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

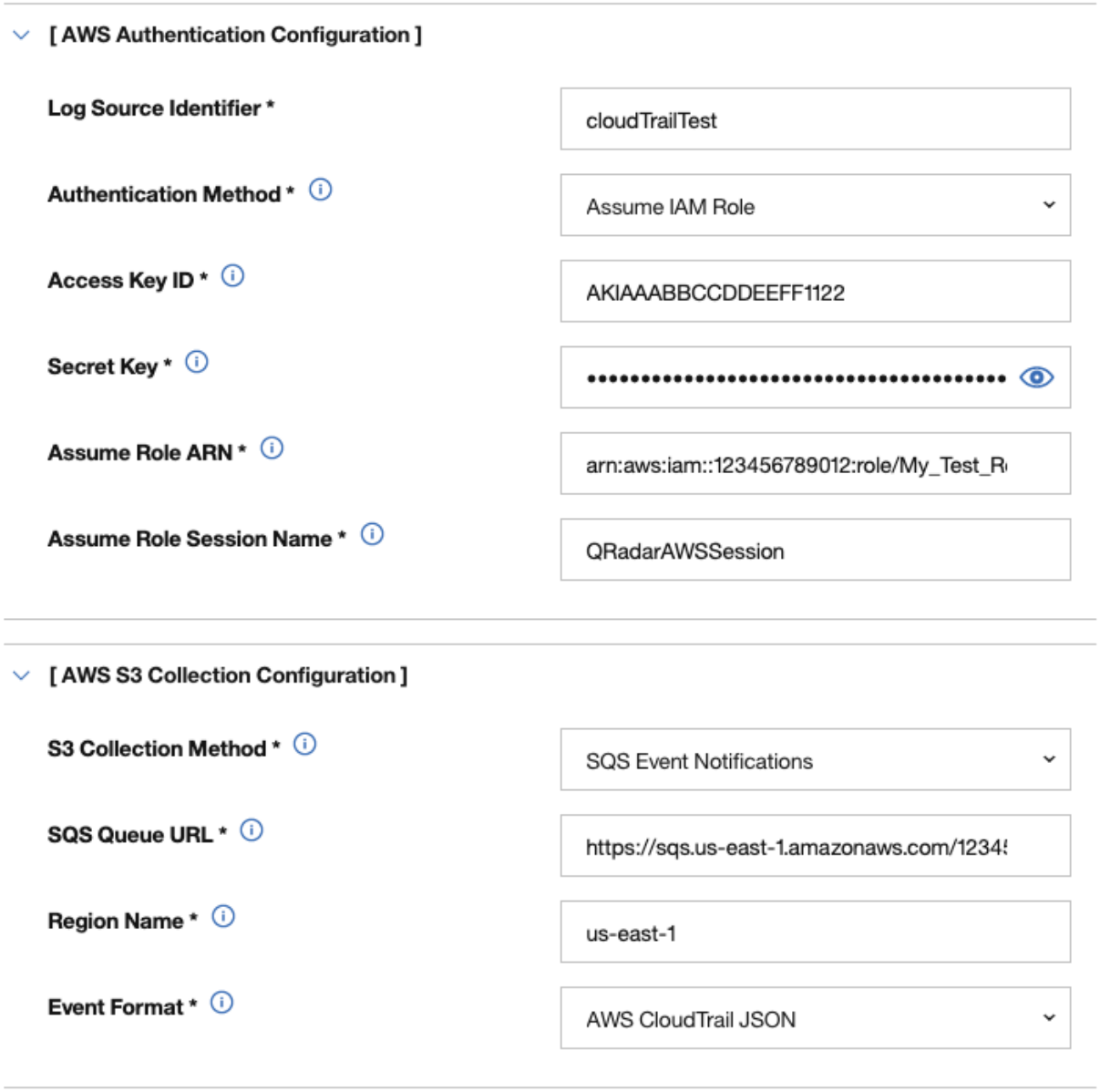


Figure 17. Example: Amazon AWS CloudTrail log source configuration in QRadar

Configuring security credentials for your AWS user account
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information
Adding a log source

Adding an AWS Config log source on the QRadar Console using an SQS queue
If you want to collect AWS Config logs from multiple accounts or regions in an Amazon S3 bucket, add a log source on the QRadar Console so that AWS Config can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

Procedure

1. Use the following table to set the parameters for an Amazon AWS Config log source that uses the Amazon AWS S3 REST API protocol and an SQS queue.

Table 178. Amazon AWS S3 REST API protocol log source parameters

Parameter	Description
Log Source Type	**AWS Config**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one AWS Config log source that is configured, you might want to identify the first log source as *awsconfig1*, the second log source as *awsconfig2*, and the third log source as *awsconfig3*.

Table 178. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you select **SQS Event Notifications** for the **S3 Collection Method**. The supported **S3 Collection Method** is **Use a Specific Prefix**. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **LINEBYLINE**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **SQS Event Notifications**.
SQS Queue URL	Enter the full URL, starting with `https://`, of the SQS queue that is set up to receive notifications for ObjectCreate events from S3.
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Log Source Identifier Pattern	This option is available when you set **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.

Table 178. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	How often a poll is made to scan for new data. If you are using the SQS event collection method, **SQS Event Notifications** can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, **Use a Specific Prefix** has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.

Table 178. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the AWS Config sample event messages.

Configuring an AWS Config log source that uses an S3 bucket with a directory prefix

If you want to collect AWS Config from a single account and region in an Amazon S3 bucket, configure a log source on the QRadar Console so AWS Config can communicate with QRadar by using the Amazon AWS S3 REST API protocol with a directory prefix.

About this task

If you have log sources in an S3 bucket from multiple regions or that use multiple accounts, use the Amazon AWS REST API protocol with an SQS queue instead of with a directory prefix.

Restriction: A log source that uses directory prefix can retrieve data from only one region and one account, so use a different log source for each region and account. Include the region folder name in the file path for the **`Directory Prefix`** value when you configure the log source.

Procedure

1. Find an S3 bucket name and directory prefix.
2. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
3. Configure the security credentials for your AWS user account.
4. Add an AWS Config log source on the QRadar Console using a directory prefix.

Finding an S3 bucket name and directory prefix

An Amazon administrator must create a user and then apply the **AmazonS3ReadOnlyAccess** policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Note: Alternatively, you can assign more granular permissions to the bucket. The minimum required permissions are **s3:listBucket** and **s3:getObject**.

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Click **Services**.
2. From the list, select **Config**.
3. From the **Config** page, click the name of the Config.
4. Note the name of the S3 bucket that is displayed in the **S3 bucket** field.
5. Click the **Edit** icon.
6. Note the location path for the S3 bucket that is displayed underneath the **Log file prefix** field.

Creating an Identity and Access Management (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **s3:listBucket** and **s3:getObject** permissions to that user in the AWS Management Console. The QRadar user can then create a log source in QRadar.

About this task

The minimum required permissions are **s3:listBucket** and **s3:getObject**. You can assign other permissions to the user as needed.

Sample policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>",
                "arn:aws:s3:::<bucket_name>/AWSLogs/<AWS_account_number>/<DSM_name>/us-east-1/*"
            ]
        }
    ]
}
```

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**.
3. From the list, select **IAM**.
4. Click **Users** > **Add user**.
5. Create an Amazon AWS IAM user and then apply the **AmazonS3ReadOnlyAccess** policy.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Adding an AWS Config log source on the QRadar Console using a directory prefix

If you want to collect AWS Config logs from a single account and region in an Amazon S3 bucket, add a log source on the QRadar Console so that Amazon AWS Config can communicate with QRadar by using the Amazon AWS S3 REST API protocol with a directory prefix.

Procedure

1. Use the following table to set the parameters for an Amazon AWS Config log source that uses the Amazon AWS S3 REST API protocol and a directory prefix.

Table 179. Amazon AWS S3 REST API protocol log source parameters

Parameter	Description
Log Source Type	**AWS Config**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one AWS Config log source that is configured, you might want to identify the first log source as *awsconfig1*, the second log source as *awsconfig2*, and the third log source as *awsconfig3*.
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see Configuring security credentials for your AWS user account. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you select **SQS Event Notifications** for the **S3 Collection Method**. The supported **S3 Collection Method** is **Use a Specific Prefix**. For more information about creating IAM users and assigning roles, see Creating an Identity and Access Management (IAM) user in the AWS Management Console. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.

Table 179. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **LINEBYLINE**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **Use a Specific Prefix**.
Bucket Name	The name of the AWS S3 bucket where the log files are stored.
Directory Prefix	The root directory location on the AWS S3 bucket from where the AWS Config logs are retrieved; for example, `AWSLogs/<AccountNumber>/Config/<RegionName>/` To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path. **Note:** • Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. • The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket. • If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use `folder1/folder2` instead).
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Log Source Identifier Pattern	This option is available when you set **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.
Show Advanced Options	Select this option if you want to customize the event data.

Table 179. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	How often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieves them. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 1 minute. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15 M = 15 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the “AWS Config sample event messages” on page 353.

AWS Config sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

AWS Config sample messages when you use the Amazon REST API protocol

Sample 1: The following sample event message shows that a resource is deleted.


```
"relatedEvents":[],"relationships":[],"supplementaryConfiguration":{},"tags":
{},"configurationItemVersion":"1.3","configurationItemCaptureTime":"2023-01-14T04:04:35.970Z","c
onfigurationStateId":123456789000,"awsAccountId":"987654321000","configurationItemStatus":"Resou
rceDeleted","resourceType":"AWS::SSM::AssociationCompliance","resourceId":"AWS::SSM::ManagedInst
anceInventory/i-0001bbbbbbbbbbbb","awsRegion":"us-
east-1","availabilityZone":"Regional","configurationStateMd5Hash":""}
```


Table 180. Highlighted values in the AWS Config sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**ResourceDeleted**
Event Category	**AWSConfig**
Timestamp	**2023-01-14T04:04:35.970Z**

Sample 2: The following sample event message shows the status of the configuration.


```
{"relatedEvents":[],"relationships":[],"configuration":
{"ReceiveMessageWaitTimeSeconds":"0","SqsManagedSseEnabled":"false","CreatedTimestamp":"15857620
81","DelaySeconds":"0","MessageRetentionPeriod":"345600","MaximumMessageSize":"262144","Visibili
tyTimeout":"30","LastModifiedTimestamp":"1585762081","QueueArn":"arn:aws:sqs:us-
east-1:987654321000:demo_queue"},"supplementaryConfiguration":{"Tags":{}},"tags":
{},"configurationItemVersion":"1.3","configurationItemCaptureTime":"2021-11-18T09:29:16.982Z","c
onfigurationStateId":123456789000,"awsAccountId":"987654321000","configurationItemStatus":"OK","
resourceType":"AWS::SQS::Queue","resourceId":"https://sqs.us-east-1.example.com/987654321000/
demo_queue","resourceName":"demo_queue","ARN":"arn:aws:sqs:us-
east-1:987654321000:demo_queue","awsRegion":"us-east-1","availabilityZone":"Not
Applicable","configurationStateMd5Hash":"","resourceCreationTime":"2020-04-01T17:28:01.000Z"}
```


Table 181. Highlighted values in the AWS Config sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**OK**
Event Category	**AWSConfig**
Timestamp	**2021-11-18T09:29:16**

Amazon AWS Elastic Kubernetes Service

The IBM QRadar DSM for Amazon AWS Elastic Kubernetes Service collects JSON formatted events from the log group of the Amazon CloudWatch logs service.

To integrate Amazon Elastic Kubernetes Service (Amazon EKS) with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (http://www.ibm.com/support).
   - Kubernetes Auditing DSM

- Amazon Web Services Protocol RPM
- DSM Common RPM
- Amazon AWS Kubernetes DSM RPM

2. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to send events to QRadar. For more information, see Configuring Amazon Elastic Kubernetes Service to communicate with QRadar
3. If QRadar does not automatically detect the log source, add an Amazon AWS Elastic Kubernetes Service log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Amazon AWS Elastic Kubernetes Service DSM specifications

When you configure Amazon AWS Elastic Kubernetes Service, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported version of Amazon AWS Elastic Kubernetes Service is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Amazon AWS Elastic Kubernetes Service DSM.

Table 182. Amazon AWS Elastic Kubernetes Service DSM specifications

Specification	**Value**
Manufacturer	Amazon
DSM name	Amazon AWS Elastic Kubernetes Service
RPM file name	DSM-*AmazonAWSKubernetes-QRadar_version-build_number*.noarch.rpm
Supported version	Kubernetes API 1.19
Protocol	Amazon Web Services
Event format	JSON
Recorded event types	Amazon AWS Kubernetes
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Amazon Elastic Kubernetes Service (Amazon EKS) documentation (https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html)

Configuring Amazon Elastic Kubernetes Service to communicate with QRadar

Before you can add a logsource in IBM QRadar, you must enable logging on your Amazon AWS console.

Before you begin

You must have a cluster that is created in the Amazon Container Services application. For more information about creating clusters, see your Amazon Elastic Kubernetes Service (Amazon EKS) documentation (https://docs.aws.amazon.com/eks/latest/userguide/create-cluster.html).

Procedure

1. Log in to your IAM console (https://console.aws.amazon.com/iam/).
2. Click **Services** > **Amazon Kubernetes Service** > **Clusters**.
3. From the **Clusters** list, select the cluster that you want to use, then click the **Configuration** tab.
4. Click the **Logging** tab and then enable the options that you want the logging service to monitor.
5. To create the log group, click **Manage logging**.
6. To view the log group, click **Services** > **CloudWatch** > **Log groups**. The log group displays in the **Log groups** list as `/aws/eks/<cluster name>/cluster`.
7. Click **Services** > **Amazon Kubernetes Service** > **Clusters**.
8. Click the **Details** tab, then record the **Cluster ARN** value. You need this value for the **Log Group** parameter value when you add a log source in QRadar.

What to do next

"Adding a log source" on page 5

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Amazon Web Services log source parameters for Amazon AWS Elastic Kubernetes Service

If IBM QRadar does not automatically detect the log source, add an Amazon AWS Elastic Kubernetes Service log source on the QRadar Console by using the Amazon Web Services protocol.

When you use the Amazon Web Service protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Amazon Web Services events from Amazon Elastic Kubernetes Service:

Table 183. Amazon Web Services log source parameters for the Amazon AWS Elastic Kubernetes Service DSM

Parameter	Value
Log Source type	Amazon AWS Elastic Kubernetes Service
Protocol Configuration	Amazon Web Services

Table 183. Amazon Web Services log source parameters for the Amazon AWS Elastic Kubernetes Service DSM (continued)

Parameter	Value
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from any location. **EC2 Instance IAM Role** If your QRadar managed host is running on an AWS EC2 instance, choose this option to use the **IAM Role** from the metadata that is assigned to the instance for authentication. No keys are required. **Tip:** This method works only for managed hosts that run within an AWS EC2 container.
Access Key ID	If you selected , **Access Key ID/ Secret Key** as the **Authentication Method**, configure this parameter. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. For more information about configuring the security credentials, see Configuring security credentials for your AWS user account.
Secret Access Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, configure this parameter. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. For more information about configuring the security credentials, see Configuring security credentials for your AWS user account.
Regions	Select the checkbox for each region that is associated with the Amazon Web Service that you want to collect logs from.
Other Regions	Enter the names of any additional regions that are associated with the Amazon Web Service that you want to collect logs from. To collect from multiple regions, use a comma-separated list, which is shown in the following example: `region1,region2`
AWS Service	The name of the Amazon Web Service. From the **AWS Service** list, select **CloudWatch Logs**.

Table 183. Amazon Web Services log source parameters for the Amazon AWS Elastic Kubernetes Service DSM (continued)

Parameter	Value
Log Group	The name of the log group in Amazon CloudWatch that you want to collect logs from. **Tip:** A single log source can collect CloudWatch logs from only one log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group.
Log Stream (Optional)	The name of the log stream within a log group that you want to collect logs from.
Filter Pattern (Optional)	Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specify are collected from CloudWatch Logs. If you enter **ACCEPT** as the Filter Pattern value, only events that contain the word **ACCEPT** are collected. The following example shows the effect of the **ACCEPT** value: `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}`
Extract Original Event	CloudWatch Logs wrap events that they receive with extra metadata. If you want only the original event that was added to the CloudWatch logs to be forwarded to QRadar, select this option. The original event is the value for the message key that is extracted from the CloudWatch Logs. The following CloudWatch logs event example shows the original event that is extracted from the CloudWatch log in bold text: `{LogStreamName: guardDutyLogStream,Timestamp: 1519849569827,Message:` **`{"version": "0", "id": "00-00", "detail-type": "GuardDuty Finding", "account": "1234567890", "region": "us-west-2", "resources": [], "detail": {"schemaVersion": "2.0", "accountId": "1234567890", "region": "us-west-2", "partition": "aws", "type": "Behavior:IAMUser/InstanceLaunchUnusual", "severity": 5.0, "createdAt": "2018-02-28T20:22:26.344Z", "updatedAt": "2018-02-28T20:22:26.344Z"}}`**`,IngestionTime: 1519849569862,EventId: 0000}`

Table 183. Amazon Web Services log source parameters for the Amazon AWS Elastic Kubernetes Service DSM (continued)

Parameter	Value
Use As A Gateway Log Source	When you select this option, the collected events flow through the QRadar Traffic Analysis engine and QRadar automatically detects one or more log sources. If the Amazon AWS S3 bucket is dedicated only to AWS Kubernetes events, do not select this checkbox. If the Amazon AWS S3 bucket contains data from multiple AWS sources, you must select this checkbox.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Automatically Acquire Server Certificates	If you select **Yes** from the list, QRadar downloads the certificate and begins trusting the target server. This function can be used to initialize a newly created log source and obtain certificates initially, or to replace expired certificates.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

For a complete list of Amazon Web Services protocol parameters and their values, see Amazon Web Services protocol configuration options.

Related tasks
Adding a log source

Amazon AWS Elastic Kubernetes Service sample event messages

Use these sample event messages to verify a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon AWS Elastic Kubernetes Service sample message when you use the Amazon Web Services protocol

Sample 1: The following sample event message shows that a watch role changed to an object of kind role.

{"kind":"Event","apiVersion":"audit.k8s.io/
v1","level":"Request","auditID":"8716c01c-7a52-4100-8e97-1b9640c72a2f","stage":"ResponseComplete",
"requestURI":"/apis/rbac.authorization.k8s.io/v1/roles?
allowWatchBookmarks=true&resourceVersion=1575982&timeout=6m33s&timeoutSeconds=393&watch=true","ver
b":"**watch**","user":{"username":"**system:kube-controller-manager**","groups":
["system:authenticated"]},"sourceIPs":["**10.0.46.47**"],"userAgent":"kube-controller-manager/v1.18.9
(linux/amd64) kubernetes/d1db3c4/shared-informers","objectRef":
{"resource":"**roles**","apiGroup":"rbac.authorization.k8s.io","apiVersion":"v1"},"responseStatus":
{"metadata":{},"status":"Success","message":"Connection closed
early","code":200},"requestReceivedTimestamp":"2021-03-29T19:15:03.945243Z","stageTimestamp":"**2021
-03-29T19:21:36.945705Z**","annotations":{"authorization.k8s.io/
decision":"allow","authorization.k8s.io/reason":"RBAC: allowed by ClusterRoleBinding
\"system:kube-controller-manager\" of ClusterRole \"system:kube-controller-manager\" to User
\"system:kube-controller-manager\""}}

{"kind":"Event","apiVersion":"audit.k8s.io/
v1","level":"Request","auditID":"8716c01c-7a52-4100-8e97-1b9640c72a2f","stage":"ResponseComplete
","requestURI":"/apis/rbac.authorization.k8s.io/v1/roles?
allowWatchBookmarks=true&resourceVersion=1575982&timeout=6m33s&timeoutSeconds=393&watch=true","v
erb":"**watch**","user":{"username":"**system:kube-controller-manager**","groups":
["system:authenticated"]},"sourceIPs":["**10.0.46.47**"],"userAgent":"kube-controller-manager/
v1.18.9 (linux/amd64) kubernetes/d1db3c4/shared-informers","objectRef":
{"resource":"**roles**","apiGroup":"rbac.authorization.k8s.io","apiVersion":"v1"},"responseStatus":
{"metadata":{},"status":"Success","message":"Connection closed
early","code":200},"requestReceivedTimestamp":"2021-03-29T19:15:03.945243Z","stageTimestamp":"**20
21-03-29T19:21:36.945705Z**","annotations":{"authorization.k8s.io/
decision":"allow","authorization.k8s.io/reason":"RBAC: allowed by ClusterRoleBinding
\"system:kube-controller-manager\" of ClusterRole \"system:kube-controller-manager\" to User
\"system:kube-controller-manager\""}}

Table 184. Highlighted values in the Amazon AWS Elastic Kubernetes Service event

QRadar field name	Highlighted values in the event payload
Event ID	**Watch**
Event Category	**roles**
Source IP	**10.0.46.47**
Username	**system:kube-controller-manager**
Device Time	**2021-03-29T19:21:36.945705Z**

Sample 2: The following sample event shows that the specified lease is replaced.

{LogStreamName: kube-apiserver-audit-e5c612db6e0f317f383ed50f22c28423,Timestamp:
1616696002054,Message: {"kind":"Event","apiVersion":"audit.k8s.io/
v1","level":"Metadata","auditID":"e4b88806-2ebf-45b7-8e92-998a33fb0689","stage":"ResponseComplete"
,"requestURI":"/apis/coordination.k8s.io/v1/namespaces/kube-system/leases/kube-controller-manager?
timeout=10s","verb":"**update**","user":{"username":"**system:kube-controller-manager**","groups":
["system:authenticated"]},"sourceIPs":["**10.0.184.90**"],"userAgent":"kube-controller-manager/
v1.18.9 (linux/amd64) kubernetes/d1db3c4/leader-election","objectRef":
{"resource":"**leases**","namespace":"kube-system","name":"kube-controller-
manager","uid":"a047cca1-2cda-4e10-9f5c-205de4effe90","apiGroup":"coordination.k8s.io","apiVersion
":"v1","resourceVersion":"36409"},"responseStatus":{"metadata":
{},"code":200},"requestReceivedTimestamp":"2021-03-25T18:13:21.066654Z","stageTimestamp":"**2021-03-
25T18:13:21.071075Z**","annotations":{"authorization.k8s.io/decision":"allow","authorization.k8s.io/
reason":"RBAC: allowed by ClusterRoleBinding \"system:kube-controller-manager\" of ClusterRole
\"system:kube-controller-manager\" to User \"system:kube-controller-manager\""}},IngestionTime:
1616696007143,EventId: 360535256052893949501645950667352553821914882891590533l2}

{LogStreamName: kube-apiserver-audit-e5c612db6e0f317f383ed50f22c28423,Timestamp:
1616696002054,Message: {"kind":"Event","apiVersion":"audit.k8s.io/
v1","level":"Metadata","auditID":"e4b88806-2ebf-45b7-8e92-998a33fb0689","stage":"ResponseComplet
e","requestURI":"/apis/coordination.k8s.io/v1/namespaces/kube-system/leases/kube-controller-
manager?timeout=10s","verb":"**update**","user":{"username":"**system:kube-controller-
manager**","groups":["system:authenticated"]},"sourceIPs":["**10.0.184.90**"],"userAgent":"kube-
controller-manager/v1.18.9 (linux/amd64) kubernetes/d1db3c4/leader-election","objectRef":
{"resource":"**leases**","namespace":"kube-system","name":"kube-controller-
manager","uid":"a047cca1-2cda-4e10-9f5c-205de4effe90","apiGroup":"coordination.k8s.io","apiVersi
on":"v1","resourceVersion":"36409"},"responseStatus":{"metadata":
{},"code":200},"requestReceivedTimestamp":"2021-03-25T18:13:21.066654Z","stageTimestamp":"**2021-0
3-25T18:13:21.071075Z**","annotations":{"authorization.k8s.io/
decision":"allow","authorization.k8s.io/reason":"RBAC: allowed by ClusterRoleBinding
\"system:kube-controller-manager\" of ClusterRole \"system:kube-controller-manager\" to User

\"system:kube-controller-manager\""}},IngestionTime: 1616696007143,EventId:
360535256052893949501645950667352553821914882891590533 12}

Table 185. Highlighted fields in the Amazon AWS Elastic Kubernetes Service event	
QRadar field name	**Highlighted values in the payload**
Event ID	**update**
Event Category	**leases**
Source IP	**10.0.184.90**
Username	**system:kube-controller-manager**
Device Time	**2021-03-25T18:13:21.071075Z**

Amazon AWS Network Firewall

The IBM QRadar DSM for Amazon AWS Network Firewall collects events from an Amazon AWS Network Firewall device by using the Amazon AWS REST API protocol.

Amazon AWS Network Firewall is a stateful network firewall that allows users to filter traffic at the perimeter of their Amazon Virtual Private Cloud (VPC) service.

To integrate Amazon AWS Network Firewall with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website. Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - AWS S3 REST API PROTOCOL RPM
   - Amazon AWS Network Firewall DSM RPM
2. Configure your Amazon AWS Network Firewall device to publish alert or flow logs to an S3 bucket. For more information, see your Amazon AWS documentation.
3. Create the SQS queue that is used to receive notifications ObjectCreated from the S3 bucket that you used is Step 2. For more information, see Create an SQS queue and configure S3 ObjectCreated notifications.
4. Configure security credentials for your AWS user account. For more information, see Configuring security credentials for your AWS user account.
5. Add an Amazon AWS Network Firewall log source on the QRadar Console by using the Amazon AWS REST API protocol. For more information, see Amazon AWS REST API log source parameters for Amazon AWS Network Firewall.

   Important: To receive flow logs in QRadar, a QRadar Flow Processor must be available and licensed. Unlike other log sources, AWS Network flow logs are not sent to the **Log Activity** tab. They are sent to the **Network Activity** tab.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Amazon AWS Network Firewall DSM specifications

When you configure the Amazon AWS Network Firewall DSM, understanding the specifications for the Amazon AWS Network Firewall DSM can help ensure a successful integration. For example, knowing what the supported version of Amazon AWS Network Firewall is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Amazon AWS Network Firewall DSM.

Table 186. Amazon AWS Network Firewall DSM specifications	
Specification	**Value**
Manufacturer	Amazon
DSM name	Amazon AWS Network Firewall
RPM file name	DSM-*AmazonAWSNetworkFirewall-QRadar_version-build_number*.noarch.rpm
Protocol	AWS S3 REST API
Automatically discovered?	No
Event format	JSON
Recorded event types	Firewall Alert logs, Firewall Flow logs
Includes identity?	No
Includes custom properties?	No

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.
5. Configuring security credentials for your AWS user account.

Finding the S3 bucket that contains the data that you want to collect

You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **Region Name** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

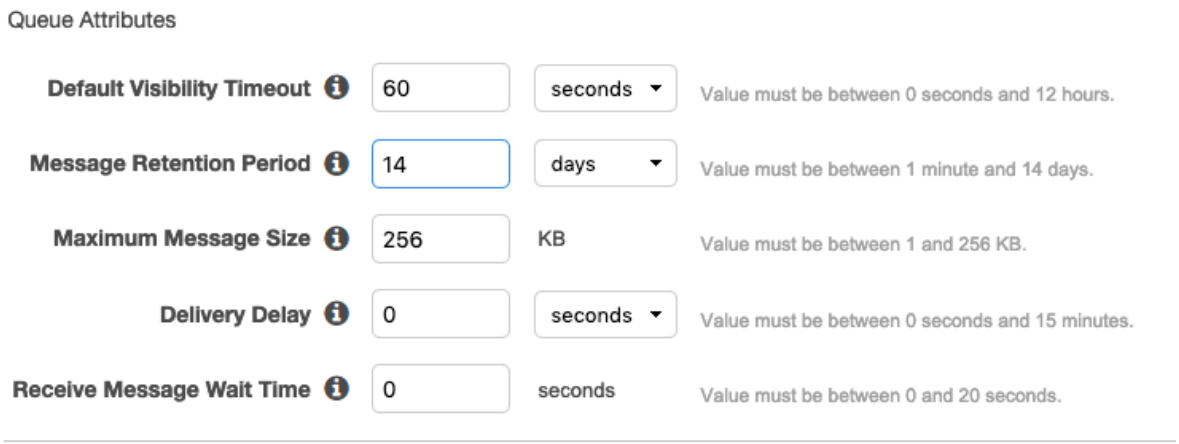
You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.
3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.
   - **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

   Use the default value for the remaining **Queue Attributes**.

   More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions

You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.

3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 187. Permission parameters	
Parameter	**Value**
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

   d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 188. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
```

```
        }
      }
    ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications

Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.
3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 189. Example: New ObjectCreated notification parameter configuration

Parameter	Value
Name	Type a name of your choosing.
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

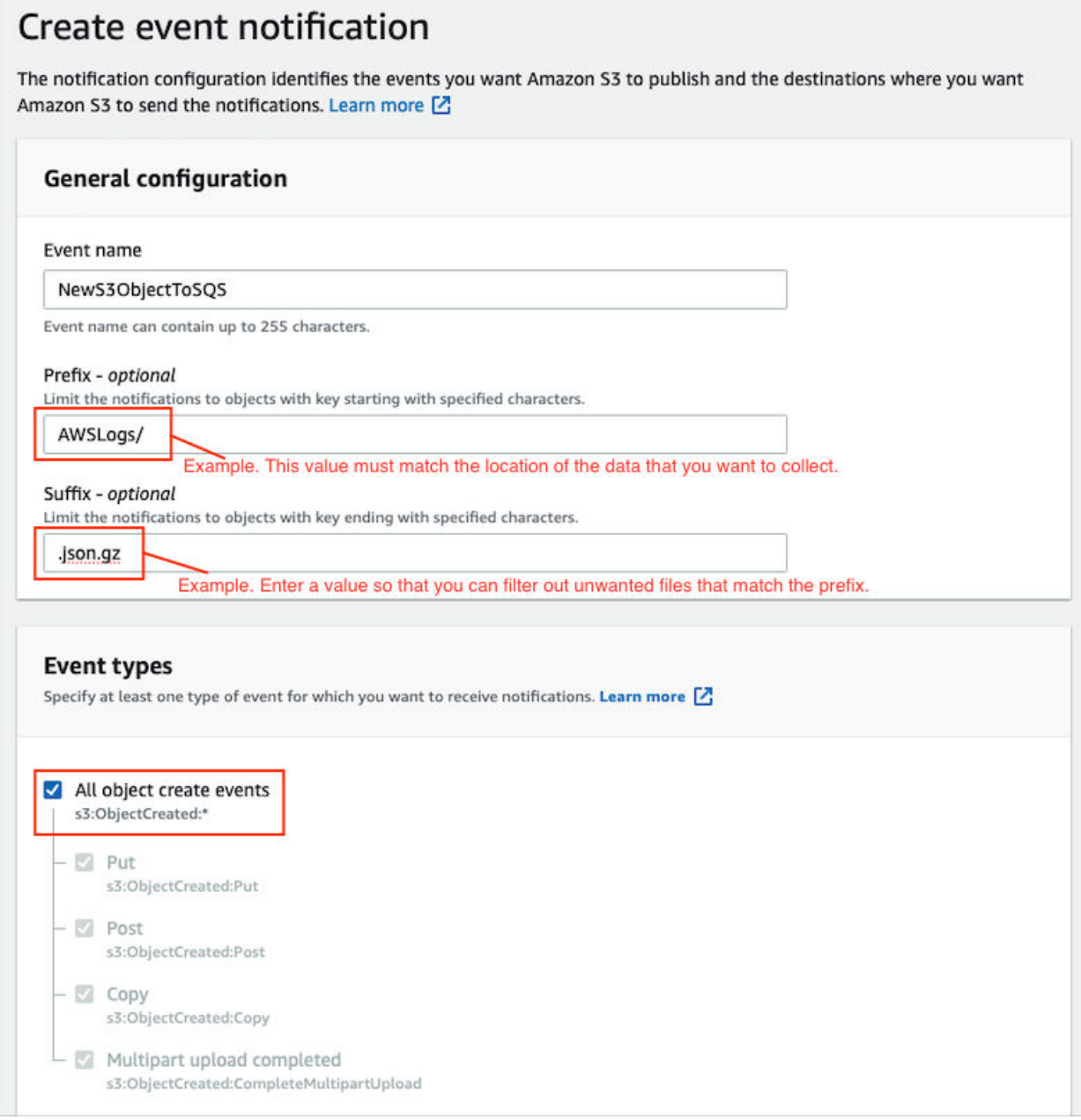


Figure 18. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

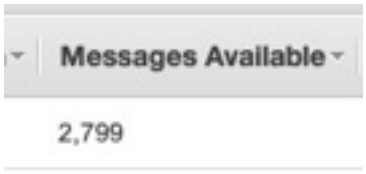


Figure 19. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

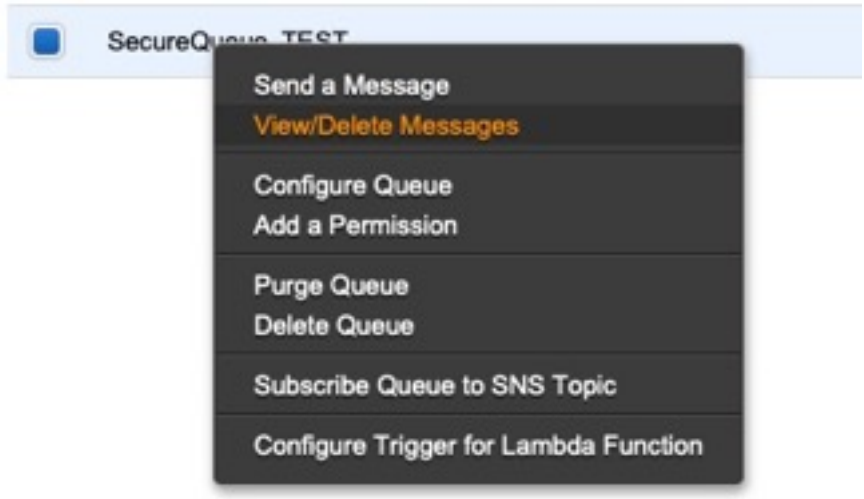


Figure 20. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

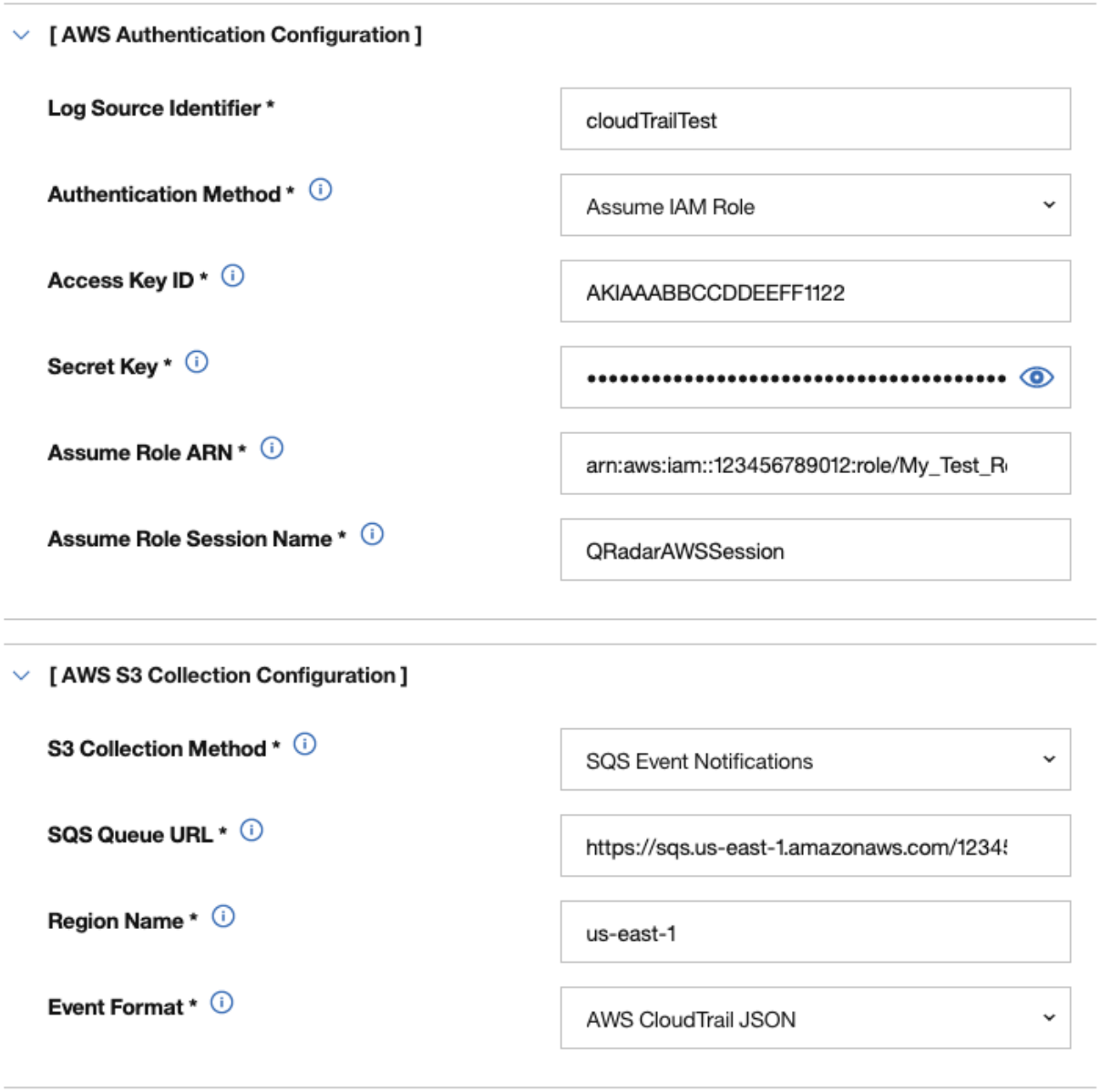


Figure 21. Example: Amazon AWS CloudTrail log source configuration in QRadar

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Amazon AWS S3 REST API log source parameters for Amazon AWS Network Firewall

If QRadar does not automatically detect the log source, add an Amazon AWS Network Firewall log source on the QRadar Console by using the Amazon AWS REST API protocol.

When using the Amazon AWS S3 REST API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Amazon AWS S3 REST API events from Amazon AWS Network Firewall:

Table 190. Amazon AWS S3 REST API log source parameters for the Amazon AWS Network Firewall DSM

Parameter	Value
Log Source type	Amazon AWS Network Firewall
Protocol Configuration	Amazon AWS S3 REST API
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS Network Firewall log source that is configured, you might want to identify the first log source as `awsnetworkfirewall1`, the second log source as `awsnetworkfirewall2`, and the third log source as `awsnetworkfirewall3`.
Event Format	If you have a QRadar Flow Processor available and licensed to receive flow logs, select **AWS Network Firewall**. If you do not have a QRadar Flow Processor available and licensed to receive flow logs, select **LINEBYLINE**.

For a complete list of Amazon AWS S3 REST API protocol parameters and their values, see Amazon AWS S3 REST API protocol configuration options.

Related tasks

Adding a log source

AWS Network Firewall sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon AWS Network Firewall sample messages when you use the Amazon AWS REST API protocol

Sample 1 - alert logs: The following sample event message shows that a connection is allowed by the firewall.

```
{"firewall_name":"firewall","availability_zone":"zone","event_timestamp":"1601074865","event":
{"timestamp":"2020-09-25T23:01:05.598481+0000","flow_id":1111111111111111,"event_type":"alert","
src_ip":"10.16.197.56","src_port":49157,"dest_ip":"10.16.197.55","dest_port":8883,"proto":"TCP",
"alert":
{"action":"allowed","signature_id":2,"rev":0,"signature":"","category":"","severity":3}}}
```

Table 191. Highlighted fields

QRadar field name	Highlighted payload field name
Logsource Time	**timestamp**
Event ID	**event_type** + **action**
Source IP	**src_ip**
Source Port	**src_port**
Destination IP	**dest_ip**
Destination Port	**dest_port**
Protocol	**proto**

Sample 2 - flow logs: The following sample event message shows netflow traffic.

```
{"firewall_name":"firewall","availability_zone":"us-
east-1b","event_timestamp":"1601587565","event":
{"timestamp":"2020-10-01T21:26:05.007515+0000","flow_id":1770453319291727,"event_type":"netflow"
,"src_ip":"45.129.33.153","src_port":47047,"dest_ip":"172.31.16.139","dest_port":16463,"proto":"
TCP","netflow":
{"pkts":1,"bytes":60,"start":"2020-10-01T21:25:04.070479+0000","end":"2020-10-01T21:25:04.070479
+0000","age":0,"min_ttl":241,"max_ttl":241},"tcp":{"tcp_flags":"02","syn":true}}}
```

Table 192. Highlighted fields

QRadar field name	Highlighted payload field name
Logsource Time	**timestamp**
Event ID	**event_type**
Source IP	**src_ip**
Source Port	**src_port**
Destination IP	**dest_ip**

Table 192. Highlighted fields (continued)	
QRadar field name	**Highlighted payload field name**
Destination Port	**dest_port**
Protocol	**proto**

Amazon AWS Route 53

The IBM QRadar DSM for Amazon AWS Route 53 collects events from an Amazon AWS Route 53 device by using the Amazon AWS S3 REST API and Amazon Web Services protocols.

To integrate Amazon AWS Route 53 with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - Protocol Common RPM
   - Amazon Web Services Protocol RPM (If you want to add a log source by using the Amazon Web Services protocol, download this RPM.)
   - Amazon AWS S3 REST API Protocol RPM (If you want to add a log source by using the Amazon AWS S3 REST API protocol, download this RPM.)
   - DSM Common RPM
   - Amazon AWS Route 53 DSM RPM
2. Optional: If you want QRadar to collect Amazon AWS Route 53 logs by using the Amazon Web Services protocol, see Configuring an Amazon AWS Route 53 log source by using the Amazon Web Services protocol.
3. Optional: If you want QRadar to collect Amazon AWS Route 53 logs by using the Amazon AWS S3 REST API protocol, select one of the following configuration methods. :

   Important: You can collect only AWS Resolver query logs when using these methods.

   - Configuring an Amazon AWS Route 53 log source that uses an S3 bucket with an SQS queue
   - Configuring an Amazon AWS Route 53 log source that uses an S3 bucket with a directory prefix

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Amazon AWS Route 53 DSM specifications

The IBM QRadar DSM for Amazon AWS Route 53 supports Public DNS log events that are collected from a log group in AWS CloudWatch Logs. Resolver query events that are collected from Amazon S3 buckets and from a log group in the AWS CloudWatch logs are also supported.

When you configure Amazon AWS Route 53, understanding the specifications for the Amazon AWS Route 53 DSM can help ensure a successful integration. For example, knowing what the supported protocols are before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Amazon AWS Route 53 DSM.

Table 193. Amazon AWS Route 53 DSM specifications	
Specification	**Value**
Manufacturer	Amazon
DSM name	Amazon AWS Route 53

Table 193. Amazon AWS Route 53 DSM specifications (continued)	
Specification	**Value**
RPM file name	DSM-*AmazonAWSRoute53-QRadar_version-build_number*.noarch.rpm
Protocol	• Amazon Web Services (Resolver and Public DNS query logs) • Amazon AWS S3 REST API (Resolver query logs only) • Syslog (The Syslog protocol uses common log source parameters)
Event format	• JSON (Resolver query logs) • Space delimited pre-defined fields (Public DNS query logs)
Recorded event types	Event versions 1.0
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	For more information about Public DNS query logs, see the Amazon website (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/query-logs.html) For more information about Resolver query logging, see the Amazon website (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-query-logs.html)

Configuring an Amazon AWS Route 53 log source by using the Amazon Web Services protocol and CloudWatch logs

To collect AWS Route 53 public DNS query logs or Resolver query logs, or both, from Amazon CloudWatch logs, add a log source on the QRadar Console by using the Amazon Web Services protocol.

Procedure

1. Create a log group in Amazon CloudWatch Logs to retrieve logs in QRadar.

   Important: For public DNS query logs, the log group must be in the US East (N.Virginia) region.
2. Configure AWS Route 53 to send logs to a log group in the AWS CloudWatch Logs.
   - For public DNS logs, configure public DNS query logging.
   - For Resolver query logs, configure Resolver query logging.
3. Create an Identity and Access (IAM) user in the AWS Management Console.
4. Configure security credentials for your AWS user account.
5. Amazon Web services log source parameters for Amazon AWS Route 53.

Configuring public DNS query logging

Before you can add a log source in IBM QRadar, you must configure logging for DNS queries.

Procedure

1. Log in to the AWS Management console to open the Route 53 console (https://console.aws.amazon.com/route53).
2. From the **Amazon Route 53** navigation pane, select **Hosted zones**.
3. Select the relevant hosted zone.
4. From the **Hosted zone details** section, click **Configure query logging**.
5. Select an existing log group or create a new log group.

   Important: The log group must be in the US East (N. Virginia) region.
6. If you see an alert about permissions, choose one of the following troubleshooting options:
   - If you have 10 resource policies, you reached the limit. Select one of your resource policies and click **Edit** to allow Route 53 to write logs to your log groups, then click **Save** and continue to step 7.
   - If this configuration is the first time that you have configured query logging, or if you have less than 10 resource policies, grant permission to Route 53 to write logs to your CloudWatch log groups by selecting **Grant permissions**, then continue to the next step.
7. To verify that the resource policy matches the CloudWatch Log log group and if Route 53 has permission to publish logs to CloudWatch, click **Permissions - optional**.
8. Click **Create**.

What to do next

Create an Identity and Access (IAM) user in the AWS Management Console

Configuring Resolver query logging

Before you can add a log source in IBM QRadar, you must configure Resolver query logging on the AWS Management console.

Procedure

1. Log in to your AWS Management console to open the Route 53 console.
2. From the **Route 53** navigation menu, select **Resolver** > **Query logging**.
3. From the region list, select the region where you want to create the query logging configuration.

   Tip: The region that you select must be the same region where you created the Amazon Virtual Private Clouds (VPCs) that you want to log queries for. If your VPCs are in multiple regions, create at least one query logging configuration for each region.
4. Click **Configure query logging**, then type a name for your query logging configuration. Your configuration name displays in the console in the list of query logging configurations.
5. In the **Query logs destination** section, select a destination where you want Resolver to publish query logs. QRadar supports CloudWatch Logs log group and S3 bucket as destinations for query logs.
   - If you are using the Amazon AWS S3 REST API, select **S3 bucket**.
   - If you are using the Amazon Web Services protocol, select **CloudWatch Logs log group**.
6. To log VPCs, in the **VPCs to log queries for** section, click **Add VPC**. DNS queries that originate in the VPCs that you select are logged. If you don't select any VPCs, no queries are logged by Resolver.
7. Click **Configure query logging**.

What to do next

Create an Identity and Access (IAM) user in the AWS Management Console

Creating an Identity and Access Management (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **s3:listBucket** and **s3:getObject** permissions to that user in the AWS Management Console. The QRadar user can then create a log source in QRadar.

About this task

The minimum required permissions are **s3:listBucket** and **s3:getObject**. You can assign other permissions to the user as needed.

Sample policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>",
                "arn:aws:s3:::<bucket_name>/AWSLogs/<AWS_account_number>/<DSM_name>/us-east-1/*"
            ]
        }
    ]
}
```

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**.
3. From the list, select **IAM**.
4. Click **Users** > **Add user**.
5. Create an Amazon AWS IAM user and then apply the **AmazonS3ReadOnlyAccess** policy.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Creating a log group in Amazon CloudWatch Logs to retrieve logs in QRadar

You must create a log group in Amazon CloudWatch Logs to make the log available for QRadar polling.

Procedure

1. Log in to your CloudWatch console (https://console.aws.amazon.com/cloudwatch).
2. Select **Logs** from left navigation pane.
3. Click **Actions** > **Create Log Group**.
4. Type the name of your log group. For example, `CloudTrailAuditLogs`.
5. Click **Create log group**.

   For more information about working with log groups and log streams, see https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Working-with-log-groups-and-streams.html

Amazon Web Services log source parameters for Amazon AWS Route 53

If you want to collect AWS Route 53 logs from Amazon CloudWatch logs, add a log source on the QRadar Console by using the Amazon Web Services protocol.

When you use the Amazon Web Services protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Amazon Web Services events from Amazon AWS Route 53:

Table 194. Amazon Web Services log source parameters for the Amazon AWS Route 53 DSM

Parameter	Value
Log Source type	**Amazon AWS Route 53**
Protocol Configuration	**Amazon Web Services**
Authentication Method	**Access Key ID/Secret Key** Standard authentication that can be used from anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.

Table 194. Amazon Web Services log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Assume an IAM Role	Enable this option by authenticating with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "arn:" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This parameter can contain only upper and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.
Regions	Toggle each region that is associated with the Amazon Web Service that you want to collect logs from.
AWS Service	From the **AWS Service** list, select **CloudWatch Logs**.
Log Group	The name of the log group in Amazon CloudWatch that you want to collect logs from. **Note:** A single log source collects CloudWatch Logs from one log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group.

Table 194. Amazon Web Services log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Enable CloudWatch Advanced Options	Enable the following optional advanced configuration values; otherwise the default values are used. **Log Stream** (Optional) The name of the log stream within a log group. If you want to collect logs from all log streams within a log group, leave this field blank. **Filter Pattern** (Optional) Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specified are collected from CloudWatch Logs. If you type ACCEPT as the Filter Pattern value, only the events that contain the word ACCEPT are collected, as shown in the following example. `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Event Delay** Delay in seconds for collecting data. **Other Region(s)** Deprecated. Use **Regions** instead.

Table 194. Amazon Web Services log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Extract Original Event	Forwards only the original event that was added to the CloudWatch Logs. CloudWatch logs wrap the events that they receive with extra metadata. Select this option if you want to collect only the original event that was sent to AWS without the additional stream metadata through CloudWatch Logs. The original event is the value for the message key that is extracted from the CloudWatch log. The following CloudWatch Logs event example shows the original event that is extracted from CloudWatch Logs in highlighted text: {LogStreamName: 123456786_CloudTrail_us-east-2,Timestamp: 1505744407363, Message: **{"eventVersion":"1.05","userIdentity": {"type":"IAMUser","principalId":"AAAABBBCCCDDDBBBCCC","arn":"arn:aws:iam::1234567890:user/<username>","accountId":"1234567890","accessKeyId":"AAAABBBBCCCCDDDD","userName":"User-Name","sessionContext":{"attributes": {"mfaAuthenticated":"false","creationDate":"2017-09-18T13:22:10Z"}},"invokedBy":"signin.amazonaws.com"},"eventTime":"2017-09-18T14:10:15Z","eventSource":"cloudtrail.amazonaws.com", "eventName":"DescribeTrails","awsRegion":"us-east-1","sourceIPAddress":"192.0.2.1","userAgent":"signin.amazonaws.com","requestParameters": {"includeShadowTrails":false,"trailNameList": []},"responseElements":null,"requestID":"11b1a00-7a7a-11a1-1a11-44a4aaa1a","eventID":"a4914e00-1111-491d-bbbb-a0dd3845b302","eventType":"AwsApiCall","recipientAccountId":"1234567890"}**,IngestionTime: 1505744407506,EventId: 335792223611111122479126672222222513333}
Use As A Gateway Log Source	If you do not want to define a custom log source identifier for events, clear the checkbox. If you don't select **Use As A Gateway Log Source** and you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources.

Table 194. Amazon Web Services log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier. This option can be defined for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.

Table 194. Amazon Web Services log source parameters for the Amazon AWS Route 53 DSM (continued)	
Parameter	**Value**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

For more information about the Amazon Web Services protocol, see Amazon Web Services protocol configuration options.

Related tasks
Adding a log source

Configuring an Amazon AWS Route 53 log source by using an S3 bucket with an SQS queue

You can collect AWS Route 53 Resolver query logs from multiple accounts or regions in an Amazon S3 bucket. Configure a log source on the QRadar Console so that Amazon AWS Route 53 can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

About this task

Using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue instead of with a directory prefix has the following advantages:

- You can use one log source for an S3 bucket, rather than one log source for each region and account.
- There is a reduced chance of missing files because this method uses ObjectCreate notifications to determine when new files are ready.
- It's easy to balance the load across multiple Event Collectors because the SQS queue supports connections from multiple clients.
- Unlike the directory prefix method, the SQS queue method does not require that the file names in the folders be in a string that is sorted in ascending order based on the full path. File names from custom applications don't always conform to this method.
- You can monitor the SQS queue and set up alerts if it gets over a certain number of records. These alerts provide information about whether QRadar is either falling behind or not collecting events.
- You can use IAM Role authentication with SQS, which is Amazon's best practice for security.
- Certificate handling is improved with the SQS method and does not require the downloading of certificates to the Event Collector.

Procedure

1. Configure Resolver query logging. In Step 5 of that procedure , select **S3 bucket** as the destination for query logs.
2. Create the SQS queue that is used to receive ObjectCreated notifications.
3. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
4. Configure the security credentials for your AWS user account.
5. Amazon AWS S3 REST API log source parameters for Amazon AWS Route 53 when using a SWS queue.

Configuring Resolver query logging

Before you can add a log source in IBM QRadar, you must configure Resolver query logging on the AWS Management console.

Procedure

1. Log in to your AWS Management console to open the Route 53 console.
2. From the **Route 53** navigation menu, select **Resolver** > **Query logging**.
3. From the region list, select the region where you want to create the query logging configuration.

   Tip: The region that you select must be the same region where you created the Amazon Virtual Private Clouds (VPCs) that you want to log queries for. If your VPCs are in multiple regions, create at least one query logging configuration for each region.
4. Click **Configure query logging**, then type a name for your query logging configuration. Your configuration name displays in the console in the list of query logging configurations.
5. In the **Query logs destination** section, select a destination where you want Resolver to publish query logs. QRadar supports CloudWatch Logs log group and S3 bucket as destinations for query logs.
   - If you are using the Amazon AWS S3 REST API, select **S3 bucket**.
   - If you are using the Amazon Web Services protocol, select **CloudWatch Logs log group**.
6. To log VPCs, in the **VPCs to log queries for** section, click **Add VPC**. DNS queries that originate in the VPCs that you select are logged. If you don't select any VPCs, no queries are logged by Resolver.
7. Click **Configure query logging**.

What to do next

Create an Identity and Access (IAM) user in the AWS Management Console

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.
5. Configuring security credentials for your AWS user account.

Finding the S3 bucket that contains the data that you want to collect

You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **`Region Name`** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

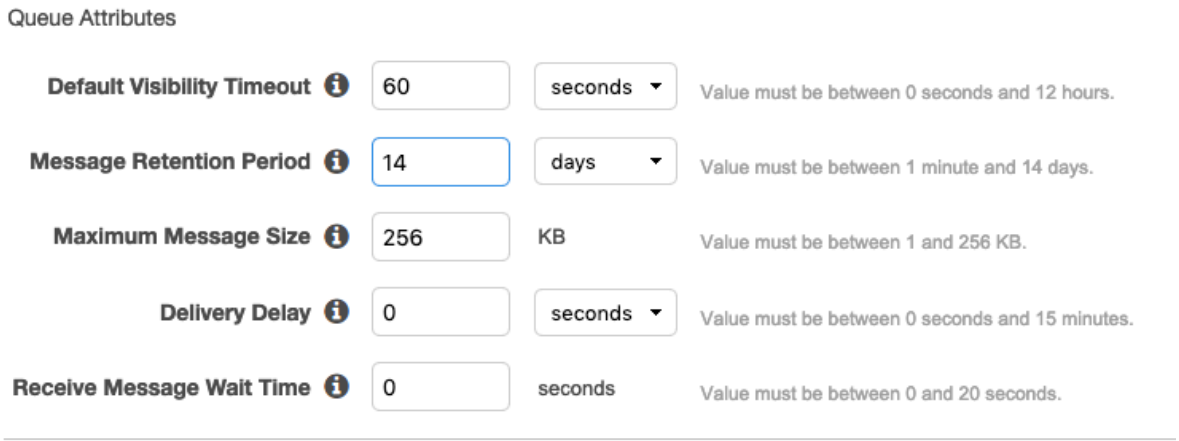
You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.
3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.
   - **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

   Use the default value for the remaining **Queue Attributes**.

   More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions

You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.
3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 195. Permission parameters	
Parameter	**Value**
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

   d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 196. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
```

```
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
      }
    }
  ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications

Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.
3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 197. Example: New ObjectCreated notification parameter configuration

Parameter	**Value**
Name	Type a name of your choosing.
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

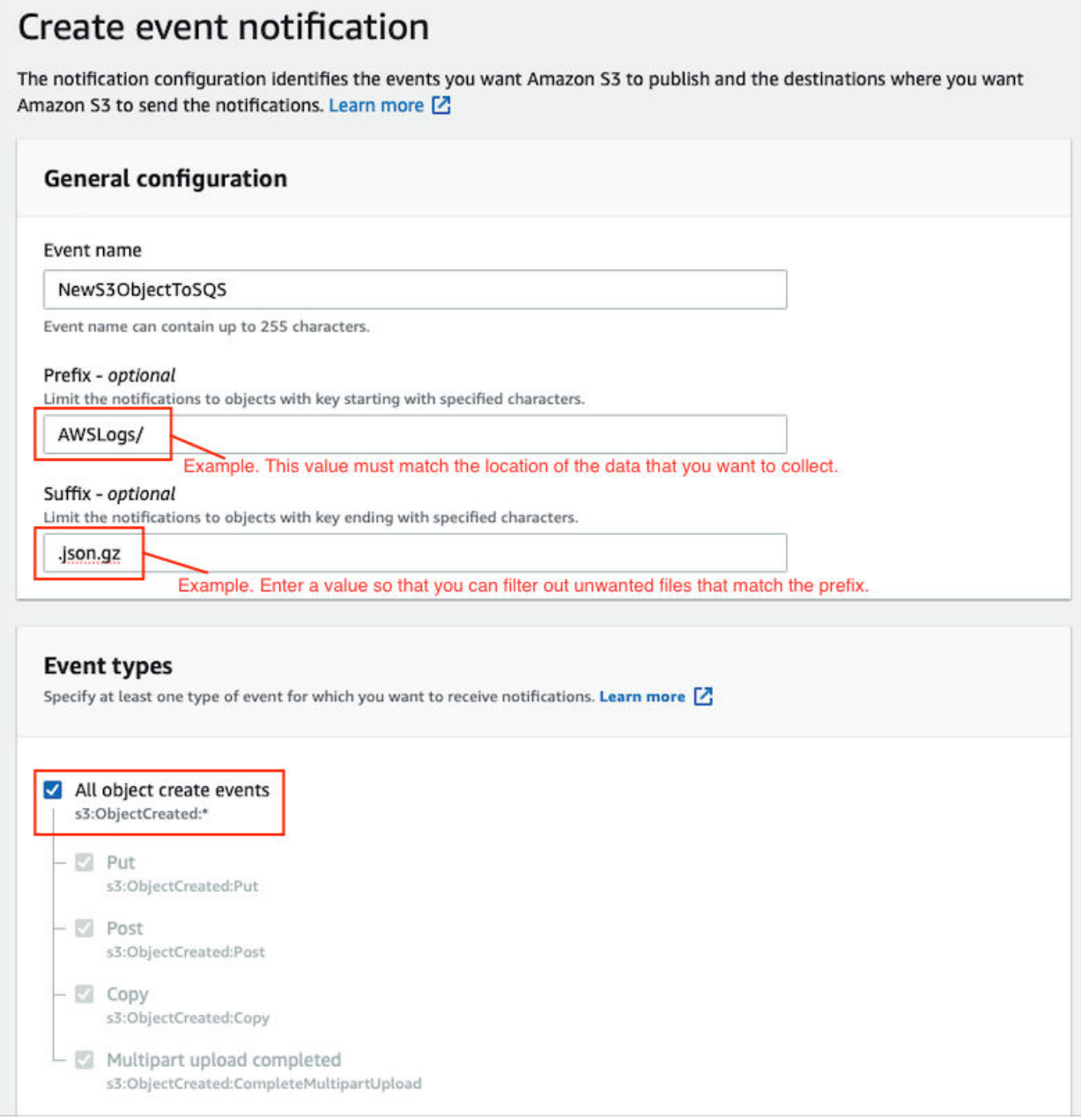


Figure 22. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

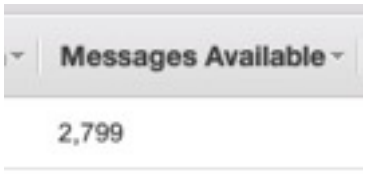


Figure 23. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

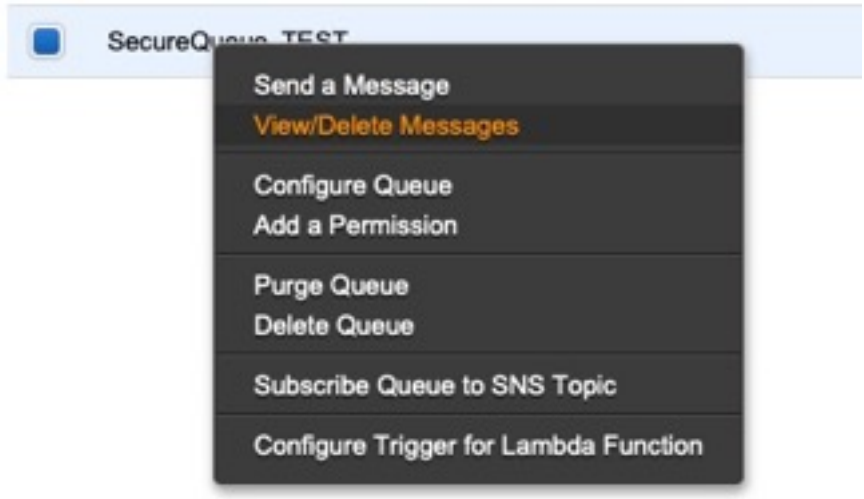


Figure 24. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

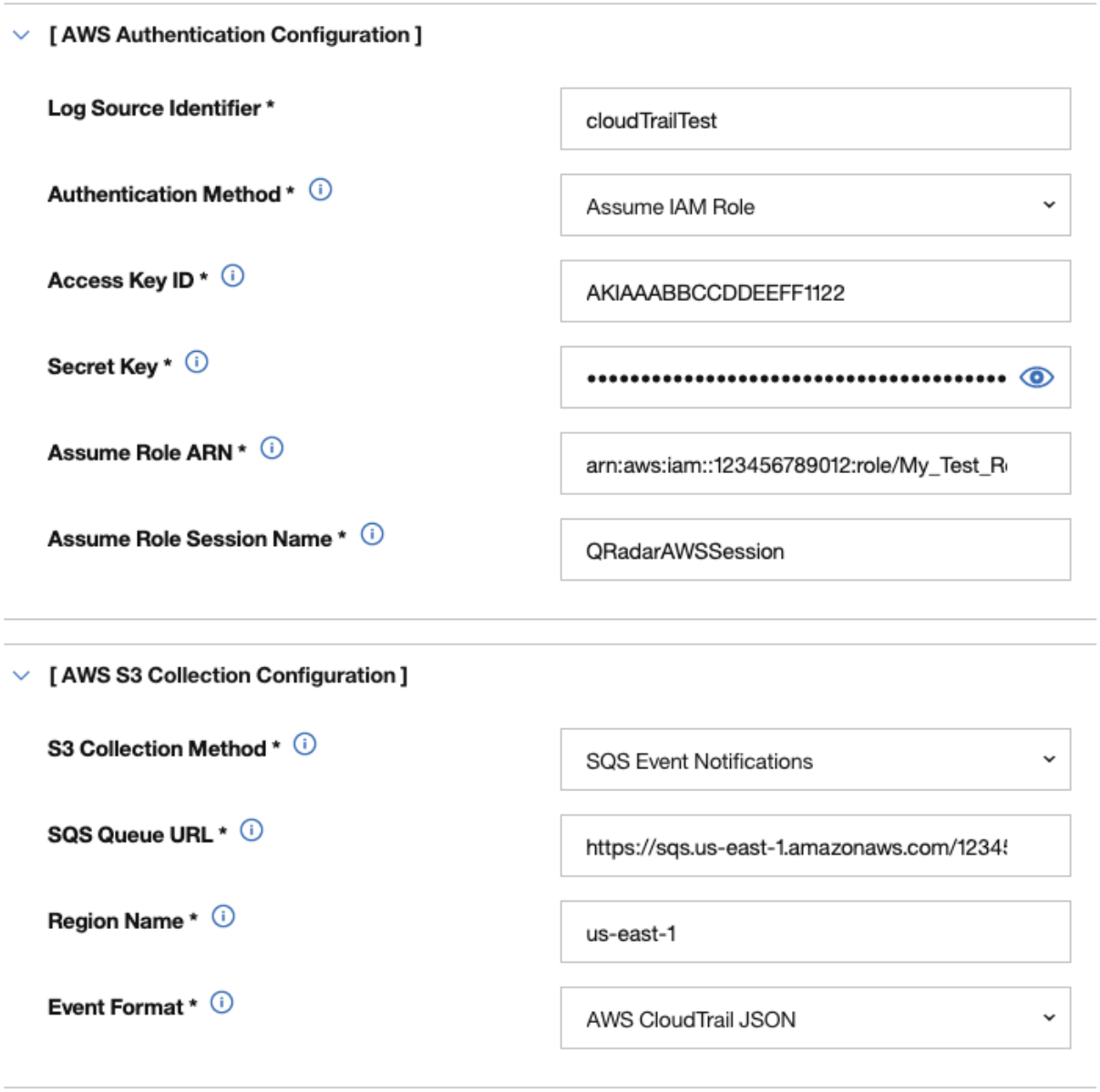


Figure 25. Example: Amazon AWS CloudTrail log source configuration in QRadar

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge

Create an Amazon EventBridge rule to forward ObjectCreated notifications to a target SQS queue.

Before you begin

Before you can create a rule in Amazon EventBridge, you must enable Amazon EventBridge on your AWS Management console. For more information, see Enabling Amazon EventBridge.

Procedure

1. Open the Amazon EventBridge console.
2. From the **Navigation** menu, click **Rules** > **Create rule**.
3. On the **Create rule** window, complete the following steps:
   a) Enter a name and description for the rule.

      Important: A rule can't have the same name as another rule that is both in the same region and on the same event bus.

   b) For **Event bus**, select the event bus that you want to associate with this rule. If you select **AWS default event bus**, the rule matches the events that come from your account.

   c) For **Rule type**, select **Rule with an event pattern**.
4. Click **Next**.
5. For **Event source**, select **AWS events or EventBridge partner events**.
6. For **Creation method**, select **Use pattern form**.
7. In the **Event pattern** window, configure the event pattern by completing the following steps:
   a) Select the values listed in the table for the following parameters:

Parameter	Value
Event source	**AWS services**
AWS service	**Simple Storage Service (S3)**
Event type	**Amazon S3 Event Notification**

   b) Click the **Specific event(s)** option and select **Object Created**.

c) Click **Specific bucket(s) by name** and enter the name of the specific bucket that you want to collect events from.

d) Optional: To enable notifications for a specific folder prefix or file extension, choose **Custom pattern (JSON editor)** instead of **Use pattern form** for the creation method, and create your custom event pattern.
For example, this event pattern filters for `Object Created` events in your bucket. In this example, `example/directory` is the directory prefix and `.png` is the suffix.

```
{
  "source": ["aws.s3"],
  "detail-type": ["Object Created"],
  "detail": {
    "bucket": {
      "name": ["<example-bucket>"]
    },
    "object": {
      "key": [{
        "prefix": "example/directory/"
      }],
      "key": [{
        "suffix": ".png"
      }]
    }
  }
}
```

e) Click **Add**, then click **Next**.

8. Choose the SQS queue that you want to use as the target. Enter the name of the queue, then click **Next**.
9. On the **Review and create** page, click **Create rule**.

Amazon AWS S3 REST API log source parameters for Amazon AWS Route 53 when using an SQS queue

If you want to collect AWS Route 53 Resolver query logs from multiple accounts or regions in an Amazon S3 bucket, add an Amazon AWS Route 53 log source on the QRadar Console by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

The following table describes the parameters for an Amazon AWS Route 53 log source that uses the Amazon AWS S3 REST API protocol:

Table 198. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM

Parameter	Value
Log Source type	Amazon AWS Route 53
Protocol Configuration	Amazon AWS S3 REST API
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS Route 53 log source that is configured, you might want to identify the first log source as *awsroute53-1*, the second log source as *awsroute53-2*, and the third log source as *awsroute53-3*.

Table 198. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see Configuring security credentials for your AWS user account. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you use the SQS Event Notifications collection method. For more information about creating IAM users and assigning roles, see Creating an Identity and Access Management (IAM) user in the AWS Management Console.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.
Secret Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Decret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **LINEBYLINE**. The log source collects JSON formatted events.
S3 Collection Method	Select **SQS Event Notifications**.
SQS Queue URL	Enter the full URL, starting with `https://`, of the SQS queue that is set up to receive notifications for ObjectCreate events from S3.
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar traffic analysis engine and for QRadar to automatically detect one or more log sources.

Table 198. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Log Source Identifier Pattern	This option is available when **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to **Yes**. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to **Yes**. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to **Yes**. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is `http://s3.amazonaws.com`
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key- name path-style` is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.

Table 198. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM (continued)	
Parameter	**Value**
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
Recurrence	How often a poll is made to scan for new data. When using the SQS event collection method, **SQS Event Notifications** can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

For more information about the Amazon AWS S3 REST API protocol, see Amazon AWS S3 REST API protocol configuration options.

Related tasks

Adding a log source

Configuring an Amazon AWS Route 53 log source by using an S3 bucket with a directory prefix

You can collect AWS Route 53 Resolver query logs from a single account and region in an Amazon S3 bucket. Add a log source on the QRadar Console so that Amazon AWS Route 53 can communicate with QRadar by using the Amazon AWS S3 REST API protocol with a directory prefix.

Before you begin

If you have log sources in an S3 bucket from multiple regions or you are using multiple accounts, use the Configuring an Amazon AWS Route 53 log source that uses an S3 bucket with an SQS queue procedure.

About this task

A log source that uses directory prefix can retrieve data from only one region and one account. Use a different log source for each region and account. Include the region folder name in the file path for the **Directory Prefix** parameter value when you configure the log source.

Procedure

1. Configure Resolver query logging. When you configure the **Query logs destination** parameter, select **S3 bucket** for the value.
2. Find an S3 bucket name and directory prefix for Amazon AWS Route 53.
3. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the AmazonS3ReadOnlyAccess policy.
4. Configure the security credentials for you AWS user account.
5. Amazon AWS S3 REST API log source parameters for Amazon AWS Route 53 when using a directory prefix.

Configuring Resolver query logging

Before you can add a log source in IBM QRadar, you must configure Resolver query logging on the AWS Management console.

Procedure

1. Log in to your AWS Management console to open the Route 53 console.
2. From the **Route 53** navigation menu, select **Resolver** > **Query logging**.
3. From the region list, select the region where you want to create the query logging configuration.

   Tip: The region that you select must be the same region where you created the Amazon Virtual Private Clouds (VPCs) that you want to log queries for. If your VPCs are in multiple regions, create at least one query logging configuration for each region.
4. Click **Configure query logging**, then type a name for your query logging configuration. Your configuration name displays in the console in the list of query logging configurations.
5. In the **Query logs destination** section, select a destination where you want Resolver to publish query logs. QRadar supports CloudWatch Logs log group and S3 bucket as destinations for query logs.
   - If you are using the Amazon AWS S3 REST API, select **S3 bucket**.
   - If you are using the Amazon Web Services protocol, select **CloudWatch Logs log group**.
6. To log VPCs, in the **VPCs to log queries for** section, click **Add VPC**. DNS queries that originate in the VPCs that you select are logged. If you don't select any VPCs, no queries are logged by Resolver.
7. Click **Configure query logging**.

What to do next

Create an Identity and Access (IAM) user in the AWS Management Console

Finding an S3 bucket name and directory prefix

An Amazon administrator must create a user and then apply the **AmazonS3ReadOnlyAccess** policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Note: Alternatively, you can assign more granular permissions to the bucket. The minimum required permissions are **s3:listBucket** and **s3:getObject**.

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Click **Services**.
2. From the list, select **Config**.
3. From the **Config** page, click the name of the Config.
4. Note the name of the S3 bucket that is displayed in the **S3 bucket** field.

5. Click the **Edit** icon.
6. Note the location path for the S3 bucket that is displayed underneath the **Log file prefix** field.

Creating an Identity and Access Management (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **s3:listBucket** and **s3:getObject** permissions to that user in the AWS Management Console. The QRadar user can then create a log source in QRadar.

About this task

The minimum required permissions are **s3:listBucket** and **s3:getObject**. You can assign other permissions to the user as needed.

Sample policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>",
                "arn:aws:s3:::<bucket_name>/AWSLogs/<AWS_account_number>/<DSM_name>/us-east-1/*"
            ]
        }
    ]
}
```

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**.
3. From the list, select **IAM**.
4. Click **Users** > **Add user**.
5. Create an Amazon AWS IAM user and then apply the **AmazonS3ReadOnlyAccess** policy.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Amazon AWS S3 REST API log source parameters for Amazon AWS Route 53 when using a directory prefix

If you want to collect AWS Route 53 Resolver query logs from a single account and region in an Amazon S3 bucket, add a log source on the IBM QRadar Console that uses the Amazon AWS S3 REST API protocol with a directory prefix.

When you use the Amazon AWS S3 REST API protocol with a directory prefix, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Amazon AWS S3 REST API events from Amazon AWS Route 53:

Table 199. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM

Parameter	Value
Log Source type	Amazon AWS Route 53
Protocol Configuration	Amazon AWS S3 REST API
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS Route 53 log source that is configured, you might want to identify the first log source as *awsroute53-1*, the second log source as *awsroute53-2*, and the third log source as *awsroute53-3*.
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see Configuring security credentials for your AWS user account. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you use the SQS Event Notifications collection method. For more information about creating IAM users and assigning roles, see Creating an Identity and Access Management (IAM) user in the AWS Management Console. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.

Table 199. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Decret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **AWS Cloud Trail JSON**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **Use a Specific Prefix**.
Bucket Name	The name of the AWS S3 bucket where the log files are stored.
Directory Prefix	The root directory location on the AWS S3 bucket from where the Resolver logs are retrieved; for example, `AWSLogs/<AccountNumber>/Resolver/<RegionName>/` To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path. **Note:** • Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. • The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket. • If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use `folder1/folder2` instead).
Region Name	The region that the SQS Queue or the AWS S3 bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3

Table 199. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM (continued)

Parameter	Value
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Log Source Identifier Pattern	This option is available when **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to **Yes**. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to **Yes**. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS S3 REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is `https://s3.amazonaws.com`.
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.

Table 199. Amazon AWS S3 REST API log source parameters for the Amazon AWS Route 53 DSM (continued)	
Parameter	**Value**
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
Recurrence	How often a poll is made to scan for new data. If you are using the SQS event collection method, **SQS Event Notifications** can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, **Use a Specific Prefix** has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

For more information about the Amazon AWS S3 REST API protocol, see Amazon AWS S3 REST API protocol configuration options.

Related tasks

Adding a log source

Configuring an Amazon Route 53 log source that uses Amazon Security Lake

You can collect Amazon Route 53 logs from multiple accounts or regions in an Amazon S3 bucket. IBM QRadar uses the Amazon AWS S3 REST API protocol to communicate with Amazon Security Lake, where QRadar obtains the Amazon Route 53 logs.

Procedure

1. Configure Amazon Security Lake to log Open Cybersecurity Schema Framework (OCSF) data in Parquet format to an S3 bucket. For more information, see Collecting data from custom sources.

Note: The supported OCSF version of the DSM is OCSF 1.0RC2. The version OCSF 1.1 is not currently supported.

2. Configure access to the OCSF data in Amazon Security Lake by using one of two methods.
   - To create a subscriber to provision the SQS queue and IAM role, see step 3.

     For more information about creating a subscriber, see Managing data access for Security Lake subscribers.
   - To manually configure the SQS queue and ObjectCreated notifications, see step 4.
3. Create a subscriber to provision the SQS queue and IAM role.
   a) When you create the subscription, take note of the following values: **SQS Queue URL**, **IAM Role ARN**, and **External ID**.
   b) If you plan to access this subscription from a different account than where Amazon Security Lake is set up, you must provide that account ID to configure the trust relationship properly.
4. Manually configure the SQS queue and ObjectCreated notifications.
   a) Configure an SQS queue to receive ObjectCreated notifications with either Amazon S3 Event Notifications or AWS EventBridge when new OCSF Parquet data is available in the Amazon Security Lake bucket in the folder you choose.
   b) Provision access keys with permission (either directly or with an **IAM Assume Role**) to access both the SQS queue and the bucket that contain the Amazon Security Lake data.

   For more information, see Create SQS and S3 object REST API.
5. Configure a log source in QRadar to collect and parse the data.

   Tip: When new OCSF parquet data is available, a message that contains the bucket name and object key of the file with the data to be processed is sent to the SQS queue. QRadar then downloads and processes this file.

What to do next

Add a Amazon Route 53 log source in QRadar. For more information, see “Configuring an Amazon AWS Route 53 log source by using an S3 bucket with an SQS queue” on page 380.

Related information

What Is Amazon EventBridge?

Amazon S3 Event Notifications

Amazon AWS Route 53 sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon AWS Route 53 sample message when you use the Amazon S3 REST API protocol

The following Amazon AWS Route 53 sample event message shows a response to a DNS query.


```
{"version":"1.100000","account_id":"769160150729","region":"us-east-1","vpc_id":"vpc-
d2153caa","query_timestamp":"2021-08-02T06:53:37Z","query_name":"logs.us-
east-1.example.com.","query_type":"A","query_class":"IN","rcode":"NOERROR","answers":
[{"Rdata":"10.46.155.107","Type":"A","Class":"IN"},
{"Rdata":"10.236.94.151","Type":"A","Class":"IN"},
{"Rdata":"10.236.94.222","Type":"A","Class":"IN"},
{"Rdata":"10.94.231.73","Type":"A","Class":"IN"},
{"Rdata":"10.236.94.196","Type":"A","Class":"IN"},
{"Rdata":"10.94.233.20","Type":"A","Class":"IN"},
{"Rdata":"10.236.94.154","Type":"A","Class":"IN"},
{"Rdata":"10.236.94.179","Type":"A","Class":"IN"}],"srcaddr":"172.31.82.134","srcport":"35535","
transport":"UDP","srcids":{"instance":"i-0b87871261ae87217"}}
```

Table 200. Highlighted fields in the Amazon AWS Route 53 event	
QRadar field name	**Highlighted payload field name**
Event ID	**query_type** + **rcode**
Category	The Category value is always **AWSRoute53** for Amazon AWS Route 53 logs.
Time	**query_timestamp**
Source IP	**srcaddr**
Source Port	**srcport**

Amazon AWS Route 53 sample message when you use the Amazon Web Services protocol

The following Amazon AWS Route 53 sample event message shows a response to a DNS query.

```
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP FRA6 2001:db8::1234
2001:db8:abcd::/48
```

Table 201. Highlighted fields in the Amazon AWS Route 53 sample event	
QRadar field name	**Highlighted payload field name**
Event ID	**ANY NOERROR**
Category	The Category value is always **AWSRoute53** for Amazon AWS Route 53 logs.
Time	**2017-12-13T08:16:03.983Z**
Source IP	**2001:db8::1234**

Amazon AWS Security Hub

The IBM QRadar DSM for Amazon AWS Security Hub collects events from the AWS CloudWatch log group of Amazon CloudWatch service.

To integrate Amazon AWS Security Hub with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - DSM Common RPM
   - Protocol Common RPM
   - Amazon Web Services Protocol RPM
   - Amazon AWS Security Hub DSM RPM
2. Create and configure an Amazon EventBridge rule to send events from AWS Security Hub to AWS CloudWatch log group. For more information, see Creating an EventBridge rule for sending events.
3. Create an Identity and Access (IAM) user in the Amazon AWS user interface when using the Amazon Web Services protocol. For more information, see Creating an Identity and Access (IAM) user in the AWS Management Console.
4. Add an Amazon AWS Security Hub log source on the QRadar Console. For more information, see Amazon Web Services log source parameters for Amazon AWS Security Hub.

Related concepts

"Amazon AWS Security Hub DSM specifications" on page 402

"Amazon Web Services log source parameters for Amazon AWS Security Hub" on page 403

“Amazon AWS Security Hub sample event message” on page 403
Use this sample event message to verify a successful integration with IBM QRadar.

Related tasks

“Adding a DSM” on page 4

“Creating an EventBridge rule for sending events” on page 402
You need to create and configure an Amazon EventBridge rule to send events from AWS Security Hub to AWS CloudWatch log group.

“Creating an Identity and Access (IAM) user in the AWS Management Console” on page 326

Amazon AWS Security Hub DSM specifications

The following table describes the specifications for the Amazon AWS Security Hub DSM.

Table 202. Amazon AWS Security Hub DSM specifications

Specification	**Value**
Manufacturer	Amazon
DSM name	AWS Security Hub
RPM file name	`DSM-AmazonAWSSecurityHub-`*`QRadar_version-build_number`*`.noarch.rpm`
Protocol	Amazon Web Services
Event format	JSON
Recorded event types	AWS Security Finding Format (ASFF)
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	AWS Security Hub documentation (https://docs.aws.amazon.com/securityhub/index.html)

Creating an EventBridge rule for sending events

You need to create and configure an Amazon EventBridge rule to send events from AWS Security Hub to AWS CloudWatch log group.

Procedure

1. Go to Amazon EventBridge (https://console.aws.amazon.com/events/home?region=us-east-1#/).
2. In the **Create a new rule** pane, click **Create rule**.
3. In the **Name and description** pane, type a name for your rule in the **Name** field and if you want, type a description for your rule in the **Description** field.
4. In the **Define pattern** pane, select **Event pattern**, and then select **Pre-defined pattern by service** to build an event pattern.
5. From the **Service provider** list, select **AWS**.
6. From the **Service name** list, select **SecurityHub**.
7. From the **Event type** list, select **All Events**.
8. In the **Select event bus** pane, select **AWS default event bus**.
9. In the **Select targets** pane, from the **Target** list, select **CloudWatch log group**.
10. In the **Log Group:** section, specify a new log group or select an existing log group from the list.

Important: You need the name of the log group when you configure a log source in QRadar.

11. Click **Create**.

What to do next

Creating an Identity and Access (IAM) user in the AWS Management Console

Creating an Identity and Access (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **CloudWatchLogsReadOnlyAccess** policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Create an Amazon AWS IAM user and then apply the **CloudWatchLogsReadOnlyAccess** policy.

What to do next

Amazon Web Services log source parameters for Amazon AWS Security Hub

Amazon Web Services log source parameters for Amazon AWS Security Hub

Add an Amazon AWS Security Hub log source on the QRadar Console to collect AWS CloudWatch logs by using the Amazon Web Services protocol.

When using the Amazon Web Services protocol to collect AWS CloudWatch logs, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect AWS CloudWatch logs with the Amazon Web Services protocol:

Table 203. Amazon Web Services log source parameters for the Amazon AWS Security Hub DSM

Parameter	Value
Log Source type	Amazon AWS Security Hub
Protocol Configuration	Amazon Web Services
Log Source Identifier	The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS Security Hub log source that is configured, you might want to identify the first log source as `awssecurityhub1`, the second log source as `awssecurityhub2`, and the third log source as `awssecurityhub3`.

For a complete list of Amazon Web Services protocol parameters and their values for collecting AWS CloudWatch logs, see Amazon Web Services protocol configuration options.

Related tasks

"Adding a log source" on page 5

Amazon AWS Security Hub sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon AWS Security Hub sample message when you use the Amazon Web Services protocol

```
{LogStreamName: SecurityHubLogStream,Timestamp:1568035216780,Message:
{"version":"0","id":"2b91a1e3-38d5-0160-7d19-8b21b5359b4c","detail-type":"Security Hub Findings
-
Imported","source":"aws.securityhub","account":"111111111111","time":"2019-09-09T13:20:16Z","reg
ion":"useast-1","resources":["..."],"detail":{"findings":
[{"SchemaVersion":"2018-10-08","Id":"...","ProductArn":"arn:aws:securityhub:useast-1::product/aw
s/guardduty","GeneratorId":"...","AwsAccountId":"111111111111","Types":["TTPs/
UnauthorizedAccess:IAMUser-
MaliciousIPCaller.Custom"],"FirstObservedAt":"2019-04-22T18:52:24.444Z","LastObservedAt":"...","
CreatedAt":"...","UpdatedAt":"...","Severity":{"Product":5,"Normalized":50},"Title":"API
GeneratedFindingAPIName was invoked from an IP address on a customthreat
list.","Description":"API was invoked from an IP address on the custom threat
list.","ProductFields":{},"Resources":
[{"Type":"AwsIamAccessKey","Id":"AWS::IAM::AccessKey:GeneratedFindingAccessKeyId","Partition":"a
ws","Region":"us-east-1","Details":{"AwsIamAccessKey":
{"UserName":"GeneratedFindingAWSService"}}}],"RecordState":"ACTIVE","WorkflowState":"NEW","appro
ximateArrivalTimestamp":1568035214.555}]}},IngestionTime: 1568035216790,EventId:
34968353831733509797102082883407915803695330140453142528}
```

Amazon AWS WAF

The IBM QRadar DSM for Amazon AWS WAF collects Amazon AWS REST API events from an Amazon AWS WAF service.

To integrate Amazon AWS WAF with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - Protocol Amazon Web Services RPM
   - Protocol Amazon AWS REST API RPM
   - Amazon AWS WAF DSM RPM
2. Configure your Amazon AWS WAF service to send events to QRadar. For more information about configuring Amazon AWS WAF, see Configuring Amazon AWS WAF to communicate with QRadar.
3. Add an Amazon AWS WAF log source on the QRadar Console. For more information about configuring the log source parameters, see Amazon AWS S3 REST API log source parameters for Amazon AWS AWF.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Amazon AWS WAF DSM specifications

When you configure the Amazon AWS WAF DSM, understanding the specifications for the Amazon AWS WAF DSM can help ensure a successful integration. For example, knowing what event types are supported by Amazon AWS WAF before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Amazon AWS WAF DSM.

Table 204. Amazon AWS WAF DSM specifications

Specification	Value
Manufacturer	Amazon AWS
DSM name	Amazon AWS WAF

Table 204. Amazon AWS WAF DSM specifications (continued)	
Specification	**Value**
RPM file name	DSM-*AmazonAWSWAF-QRadar_version-build_number*.noarch.rpm
Protocol	Amazon AWS S3 REST API
Event format	JSON
Recorded event types	Traffic allow, Traffic block
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	AWS WAF documentation (https://docs.aws.amazon.com/waf/latest/developerguide/waf-auth-and-access-control.html)

Configuring Amazon AWS WAF to communicate with QRadar

Before you can add a log source in IBM QRadar, you must configure Amazon AWS WAF to send logs to an Amazon Kinesis Data Firehouse Delivery Stream that uses an Amazon AWS S3 bucket.

Before you begin

You must have an Amazon Kinesis Data Firehose Delivery Stream configured. For more information, see the Amazon documentation about Creating an Amazon Kinesis Data Firehose Delivery Stream (https://docs.aws.amazon.com/firehose/latest/dev/basic-create.html).The delivery stream must be linked to the Amazon AWS S3 Bucket.

About this task

Logging must be enabled to forward events to QRadar. If you don't have logging enabled for Amazon AWS WAF, complete the following steps.

Procedure

1. Log in to your IAM console (https://console.aws.amazon.com/iam/).
2. Click **Services** > **WAF & Shield**.
3. From the **WAF & Shield** navigation menu, select **Web ACLs**.
4. Click the **Logging and metrics** tab.
5. To enable logging, click **Enable logging**.
6. From the region list, select your region.
7. From the **Web ACLs** list, select the Amazon Kinesis Data Firehose Delivery Stream that is linked to your Amazon AWS S3 bucket.
8. Click **Enable Logging**.

What to do next

Add a log source in QRadar.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Amazon AWS S3 REST API log source parameters for Amazon AWS WAF

If QRadar does not automatically detect the log source, add an Amazon AWS WAF log source on the QRadar Console by using the Amazon AWS S3 REST API protocol.

When you use the Amazon AWS S3 REST API protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Amazon AWS S3 REST API events from Amazon AWS WAF:

Table 205. Amazon AWS S3 REST API log source parameters for the Amazon AWS WAF DSM

Parameter	Value
Log Source type	**Amazon AWS WAF**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The Log Source Identifier can be the same value as the Log Source Name. If you have more than one Amazon AWS WAF log source that is configured, you might want to identify the first log source as `awswaf1`, the second log source as `awswaf2`, and the third log source as `awswaf3`.
Authentication Method	**Access Key ID / Secret Key**
Access Key	The Access key ID that you created when you configured your AWS security credentials. For more information, see Configuring security credentials for your AWS user account.
Secret Key	The Secret access key that you created when you configured your AWS security credentials. For more information, see Configuring security credentials for your AWS user account.

Table 205. Amazon AWS S3 REST API log source parameters for the Amazon AWS WAF DSM (continued)	
Parameter	**Value**
S3 Collection Method	**SQS Event Notifications**
SQS Queue URL	The full URL that begins with `https://`, for the SQS Queue that is set up to receive notifications for ObjectCreated events from S3.
Region Name	The region that is assigned to your Amazon AWS WAF. Example: us-east-2
Event Format	**LINEBYLINE**

For a complete list of Amazon AWS S3 REST API protocol parameters and their values, see Amazon AWS S3 REST API protocol configuration options.

Related tasks

Adding a log source

Amazon AWS WAF sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon AWS WAF sample messages when you use the Amazon AWS S3 REST API protocol

Sample 1: The following sample event message shows that Amazon AWS WAF allowed access the underlying resource.


```
{"timestamp":1613576332142,"formatVersion":1,"webaclId":"webaclId","terminatingRuleId":"First_Ru
le","terminatingRuleType":"REGULAR","action":"ALLOW","terminatingRuleMatchDetails":
[],"httpSourceName":"APIGW","httpSourceId":"11111111111111:1111111111:First_API_Gateway","ruleGr
oupList":[],"rateBasedRuleList":[],"nonTerminatingMatchingRules":
[],"requestHeadersInserted":null,"responseCodeSent":null,"httpRequest":
{"clientIp":"10.2.173.13","country":"country","headers":[{"name":"accept","value":"text/
html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9"},{"name":"accept-encoding","value":"gzip,
deflate, br"},{"name":"accept-language","value":"en-US,en;q=0.9"},{"name":"cache-
control","value":"max-age=0"},{"name":"Host","value":"1111111111.execute-
api.region.amazonaws.com"},{"name":"sec-fetch-dest","value":"document"},{"name":"sec-fetch-
mode","value":"navigate"},{"name":"sec-fetch-site","value":"none"},{"name":"sec-fetch-
user","value":"?1"},{"name":"upgrade-insecure-requests","value":"1"},{"name":"user-
agent","value":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/88.0.4324.150 Safari/537.36"},{"name":"X-Amzn-Trace-
Id","value":"Root=1-111111aaaaa1111111"},{"name":"X-Forwarded-For","value":"10.2.173.13"},
{"name":"X-Forwarded-Port","value":"443"},{"name":"X-Forwarded-Proto","value":"https"},
{"name":"Content-Length","value":"0"},{"name":"Connection","value":"Keep-Alive"}],"uri":"/
First_API_Gateway/pets","args":"","httpVersion":"HTTP/
1.1","httpMethod":"GET","requestId":"111111aaaa1aaa1"}}
```


Table 206. Highlighted fields in the Amazon AWS WAF sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**ALLOW**
Event Category	For this DSM, the value in QRadar is always **AmazonAWSWAF**.
Timestamp	**1613576332142**
Src IP	**10.2.173.13**

Sample 2: The following sample event message shows that Amazon AWS WAF blocked traffic to the underlying resource.


```
{"timestamp":16135764421213,"formatVersion":1,"webaclId":"webaclId","terminatingRuleId":"First_R
ule","terminatingRuleType":"REGULAR","action":"BLOCK","terminatingRuleMatchDetails":
[],"httpSourceName":"APIGW","httpSourceId":"11111111111111:1111111111:First_API_Gateway","ruleGr
oupList":[],"rateBasedRuleList":[],"nonTerminatingMatchingRules":
[],"requestHeadersInserted":null,"responseCodeSent":null,"httpRequest":
{"clientIp":"10.2.173.14","country":"country","headers":[{"name":"accept","value":"text/
html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9"},{"name":"accept-encoding","value":"gzip,
deflate, br"},{"name":"accept-language","value":"en-US,en;q=0.9"},{"name":"cache-
control","value":"max-age=0"},{"name":"Host","value":"1111111111.execute-
api.region.amazonaws.com"},{"name":"sec-fetch-dest","value":"document"},{"name":"sec-fetch-
mode","value":"navigate"},{"name":"sec-fetch-site","value":"none"},{"name":"sec-fetch-
user","value":"?1"},{"name":"upgrade-insecure-requests","value":"1"},{"name":"user-
agent","value":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/88.0.4324.150 Safari/537.36"},{"name":"X-Amzn-Trace-
Id","value":"Root=1-111111aaaaa1111111"},{"name":"X-Forwarded-For","value":"10.2.173.13"},
{"name":"X-Forwarded-Port","value":"443"},{"name":"X-Forwarded-Proto","value":"https"},
{"name":"Content-Length","value":"0"},{"name":"Connection","value":"Keep-Alive"}],"uri":"/
First_API_Gateway/pets","args":"","httpVersion":"HTTP/
1.1","httpMethod":"GET","requestId":"111111aaaa1aaa1"}}
```


Table 207. Highlighted values in the Amazon AWS WAF sample event

QRadar field name	Highlighted values in the event payload
Event ID	**BLOCK**
Event Category	For this DSM, the value in QRadar is always **AmazonAWSWAF**.
Timestamp	**16135764421213**
Src IP	**10.2.173.14**

Amazon CloudFront

The IBM QRadar DSM for Amazon CloudFront collects events from Amazon S3 Buckets and Amazon Kinesis Data Streams.

The following table lists the specifications for the Amazon CloudFront DSM:

Table 208. Amazon CloudFront DSM specifications

Specification	Value
Manufacturer	Amazon
DSM	Amazon CloudFront
RPM name	DSM-AmazonCloudFront-*QRadar_version-Build_number*.noarch.rpm
Supported protocols	Amazon Web Services
Event format	Tab Separated Value (TSV)
Recorded event types	RealTime Log - TSV
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Amazon CloudFront documentation (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/real-time-logs.html)

Related concepts

“Amazon CloudFront sample event message” on page 415
Use this sample event message to verify a successful integration with IBM QRadar.

Related tasks

“Adding a DSM” on page 4

“Configuring security credentials for your AWS user account” on page 310
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

“Configuring an Amazon CloudFront log source by using the Amazon Web Services protocol” on page 409
If you want to collect Amazon CloudFront logs from Amazon Kinesis Data Streams, configure a log source on the IBM QRadar Console so that Amazon CloudFront can communicate with QRadar by using the Amazon Web Services protocol.

Related information

Adding a log source

Configuring an Amazon CloudFront log source by using the Amazon Web Services protocol

If you want to collect Amazon CloudFront logs from Amazon Kinesis Data Streams, configure a log source on the IBM QRadar Console so that Amazon CloudFront can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common
   - Amazon Web Services Protocol RPM
   - DSMCommon RPM
   - Amazon CloudFront DSM RPM
2. Configure an Amazon CloudFront log source. For more information, see Configuring an Amazon log source by using the Amazon Web Services protocol and Kinesis Data Streams.

Related tasks

“Adding an Amazon CloudFront log source by using the Amazon Web Services protocol and Kinesis Data Streams” on page 410
If you want to collect Amazon CloudFront logs from Amazon Kinesis Data Streams, add a log source on the QRadar Console so that Amazon CloudFront can communicate with QRadar by using the Amazon Web Services protocol.

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring an Amazon CloudFront log source by using the Amazon Web Services protocol and Kinesis Data Streams

Before you can add a log source that uses the Amazon Web Services protocol in IBM QRadar, you must create a data stream and then create a real-time log configuration on the AWS Management Console.

Procedure

1. On the AWS Management console, create a data stream. For more information, see Creating a stream via the AWS Management Console.
2. On the AWS Management console, create real-time logs. For more information, see Real-time logs.

3. Create a real-time log configuration on the AWS Management Console.

   Important: Real-time log configuration requires all 40 fields to be configured. For more information, see Understanding real-time log configurations.

   The position/index number for the following fields must be as documented in the Amazon AWS Fields documentation:

   - `timestamp`
   - `c-ip`
   - `sc-status`
   - `x-edge`
   - `x-edge-result-type`
   - `c-port`
   - `x-edge-detailed-result-type`

   For example, the `c-ip` position, is in the 2 position and the `x-edge-detailed-result-type` is in the 33rd position.
4. Add an Amazon CloudFront log source in QRadar. Adding an Amazon CloudFront log source by using the Amazon Web Services protocol an Kinesis Data Streams.

Related tasks

"Adding an Amazon CloudFront log source by using the Amazon Web Services protocol and Kinesis Data Streams" on page 410
If you want to collect Amazon CloudFront logs from Amazon Kinesis Data Streams, add a log source on the QRadar Console so that Amazon CloudFront can communicate with QRadar by using the Amazon Web Services protocol.

"Adding a DSM" on page 4
"Adding a log source" on page 5

Adding an Amazon CloudFront log source by using the Amazon Web Services protocol and Kinesis Data Streams

If you want to collect Amazon CloudFront logs from Amazon Kinesis Data Streams, add a log source on the QRadar Console so that Amazon CloudFront can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. The following table describes the parameters that require specific values to collect audit events from Amazon CloudFront by using the Amazon Web Services protocol:

Table 209. Amazon Web Services log source parameters for Amazon Kinesis Data Streams

Parameter	Description
Protocol Configuration	Select **Amazon Web Services** from the Protocol Configuration list.
Authentication Method	**Access Key ID/Secret Key** Standard authentication that can be used from anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choosing this option uses the IAM role from the metadata that is assigned to the instance for authentication. No keys are required. This method works only for managed hosts that are running within an AWS EC2 container.

Table 209. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Access Key	The Access Key ID that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Access Key** parameter is displayed.
Secret Key	The Secret Key that was generated when you configured the security credentials for your AWS user account. If you selected **Access Key ID / Secret Key** or **Assume IAM Role**, the **Secret Key** parameter is displayed.
Assume an IAM Role	Enable this option to authenticate with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access.
Assume Role ARN	The full ARN of the role to assume. It must begin with "`arn:`" and can't contain any leading or trailing spaces, or spaces within the ARN. If you enabled **Assume an IAM Role**, the **Assume Role ARN** parameter is displayed.
Assume Role Session Name	The session name of the role to assume. The default is `QRadarAWSSession`. Leave as the default if you don't need to change it. This parameter can contain only upper and lowercase alphanumeric characters, underscores, or any of the following characters: `=,.@-` If you enabled **Assume an IAM Role**, the **Assume Role Session Name** parameter is displayed.
Assume Role External ID	**Assume Role External ID** is an optional identifier that is required to assume a role in a different account. If the account administrator, to which the role belongs, provides you with an external ID, then insert that value in the **Assume Role External ID** parameter. This value can either be a string, a passphrase, a GUID, or an account number. For more information, see AWS documentation Using an external ID for third-party access.
Regions	Toggle each region that is associated with the Amazon Web Service that you want to collect logs from.
AWS Service	From the **AWS Service** list, select **Kinesis Data Streams**.
Kinesis Data Stream	The Kinesis Data Stream from which to consume data.

Table 209. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Enable Kinesis Advanced Options	Enable the following optional advanced configuration values. Advanced option values are only used when this option is chosen; otherwise, the default values are used. **Initial Position in Stream** This option controls which data to pull on a newly configured log source. Select **Latest** to pull the latest data that is available. Select **Trim Horizon** to pull the oldest data that is available. **Kinesis Worker Thread Count** The number of worker threads to use for Kinesis Data Stream processing. Each worker thread can process approximately 10000 - 20000 events per second depending on record size and system load. If your log source is not able to process the new data in the stream, you can increase the number of threads here to a maximum of 16. The allowed range is 1 - 16. The default value is 2. **Checkpoint Interval** The interval (in seconds) at which to checkpoint data sequence numbers. Each record from a shard in a Kinesis Data Stream has a sequence number. Checkpointing your position allows this shard to resume processing at the same point if processing fails or a service restarts. A more frequent interval reduces data duplication but increases Amazon Dynamo DB usage. The allowed range is 1 - 3600 seconds. The default is 10 seconds. **Kinesis Application** Leave this option blank to have this log source consume data from all available shards in the Kinesis Data Stream. To have multiple log sources on multiple event processors scale log consumption without loss or duplication, use a common Kinesis Application across those log sources (Example: ProdKinesisConsumers). **Partition** Select this option to collect data from a specific partition in the Kinesis Data Stream by specifying a partition name.

Table 209. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)

Parameter	Description
Extract Original Event	Forwards only the original event that was added to the Kinesis Data Stream. Kinesis logs wrap the events that they receive with extra metadata. Select this option if you want only the original event that was sent to AWS without the additional stream metadata through Kinesis. The original event is the value for the message key that is extracted from the Kinesis log. The following Kinesis logs event example shows the original event that is extracted from the Kinesis log in highlighted text: `{"owner":"123456789012","subscriptionFilters":["allEvents"], "logEvents": [{"id":"35093963143971327215510178578576502306458824699048362100", "message":"{\"eventVersion\":\"1.05\",\"userIdentity\": {\"type\":\"AssumedRole\", \"principalId\":\"ARO1GH58EM3ESYDW3XHP6:test_session\",\"arn\":\"arn :aws:sts::123456789012:assumed-role\/CVDevABRoleToBeAssumed\/ test_visibility_session\", \"accountId\":\"123456789012\",\"accessKeyId\":\"ASIAXXXXXXXXXXXXXXX X\",\"sessionContext\":{\"sessionIssuer\": {\"type\":\"Role\",\"principalId\":\"AROAXXXXXXXXXXXXXXXX\", \"arn\":\"arn:aws:iam::123456789012:role\/ CVDevABRoleToBeAssumed\",\"accountId\":\"123456789012\", \"userName\":\"CVDevABRoleToBeAssumed\"},\"webIdFederationData\": {},\"attributes\":{\"mfaAuthenticated\":\"false\", \"creationDate\":\"2019-11-13T17:01:54Z\"}}},\"eventTime\":\"2019-11 -13T17:43:18Z\",\"eventSource\":\"cloudtrail.amazonaws.com\", \"eventName\":\"DescribeTrails\",\"awsRegion\":\"ap- northeast-1\",\"sourceIPAddress\":\"192.0.2.1\",\"requestParameters\ ":null,\"responseElements\":null, \"requestID\":\"41e62e80-b15d-4e3f-9b7e- b309084dc092\",\"eventID\":\"904b3fda-8e48-46c0-a923- f1bb2b7a2f2a\",\"readOnly\":true,\"eventType\":\"AwsApiCall\", \"recipientAccountId\":\"123456789012\"}","timestamp":1573667733143}],"messageType":"DATA_MESSAGE","logGroup":"CloudTrail\/ DefaultLogGroup","logStream":"123456789012_CloudTrail_us-east-2_2"}` (highlighted text: `{\"eventVersion\":\"1.05\",\"userIdentity\": {\"type\":\"AssumedRole\", \"principalId\":\"ARO1GH58EM3ESYDW3XHP6:test_session\",\"arn\":\"arn :aws:sts::123456789012:assumed-role\/CVDevABRoleToBeAssumed\/ test_visibility_session\", \"accountId\":\"123456789012\",\"accessKeyId\":\"ASIAXXXXXXXXXXXXXXX X\",\"sessionContext\":{\"sessionIssuer\": {\"type\":\"Role\",\"principalId\":\"AROAXXXXXXXXXXXXXXXX\", \"arn\":\"arn:aws:iam::123456789012:role\/ CVDevABRoleToBeAssumed\",\"accountId\":\"123456789012\", \"userName\":\"CVDevABRoleToBeAssumed\"},\"webIdFederationData\": {},\"attributes\":{\"mfaAuthenticated\":\"false\", \"creationDate\":\"2019-11-13T17:01:54Z\"}}},\"eventTime\":\"2019-11 -13T17:43:18Z\",\"eventSource\":\"cloudtrail.amazonaws.com\", \"eventName\":\"DescribeTrails\",\"awsRegion\":\"ap- northeast-1\",\"sourceIPAddress\":\"192.0.2.1\",\"requestParameters\ ":null,\"responseElements\":null, \"requestID\":\"41e62e80-b15d-4e3f-9b7e- b309084dc092\",\"eventID\":\"904b3fda-8e48-46c0-a923- f1bb2b7a2f2a\",\"readOnly\":true,\"eventType\":\"AwsApiCall\", \"recipientAccountId\":\"123456789012\"}`)
Use As A Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources. When you select this option, the **Log Source Identifier Pattern** can optionally be used to define a custom **Log Source Identifier** for events that are being processed.

Table 209. Amazon Web Services log source parameters for Amazon Kinesis Data Streams (continued)	
Parameter	**Description**
Log Source Identifier Pattern	If you selected **Use As A Gateway Log Source**, you can define a custom log source identifier for events that are being processed and for log sources to be automatically discovered when applicable. If you don't configure the **Log Source Identifier Pattern**, QRadar receives events as unknown generic log sources. Use key-value pairs to define the custom Log Source Identifier. The key is the Identifier Format String, which is the resulting source or origin value. The value is the associated regex pattern that is used to evaluate the current payload. This value also supports capture groups that can be used to further customize the key. Define multiple key-value pairs by typing each pattern on a new line. Multiple patterns are evaluated in the order that they are listed. When a match is found, a custom Log Source Identifier is displayed. The following examples show multiple key-value pair functions. **Patterns** `VPC=\sREJECT\sFAILURE` `$1=\s(REJECT)\sOK` `VPC-$1-$2=\s(ACCEPT)\s(OK)` **Events** `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}` **Resulting custom log source identifier** VPC-ACCEPT-OK
Use Predictive Parsing	If you enable this parameter, an algorithm extracts log source identifier patterns from events without running the regex for every event, which increases the parsing speed. **Tip:** In rare circumstances, the algorithm can make incorrect predictions. Enable predictive parsing only for log source types that you expect to receive high event rates and require faster parsing.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, select this option. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy IP or Hostname** field.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   The actual CloudFront logs are wrapped in a Kinesis Data Streams tab-separated value (TSV) payload:

Table 210. Kinesis Data Streams sample message supported by the Amazon CloudFront DSM		
Event name	**Low-level category**	**Sample log message**
hit_ok	Request Successful	1663583003.838 2001:DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF timeToFirstByte status scbytes GET https host /uri csbytes xEdgeLocation xedgeRequestId xHostHeader timeTaken csProtocolVersion cIpversion userAgent csReferer cs-cookie csUriQuery xEdgeResultResponseType xForwardedFor sslProtocol sslCipher xEdgeResultType fleEncryptedFields fleStatus scContentType scContentLen scRangeStart scRangeEnd 80 xEdgeDetailedResultType country csAcceptEncoding csAccept cacheBehaviour csHeader csHeaderName csHeaderCount

Amazon CloudFront sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon CloudFront sample message when you use the Amazon Web Services protocol

The following sample event message describes trails.

```
1663583003.838 2001:DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF timeToFirstByte status
scbytes GET https host /uri csbytes xEdgeLocation xedgeRequestId
xHostHeader timeTaken csProtocolVersion cIpversion userAgent csReferer cs-
cookie csUriQuery xEdgeResultResponseType xForwardedFor sslProtocol sslCipher
xEdgeResultType fleEncryptedFields fleStatus scContentType scContentLen
scRangeStart scRangeEnd 80 xEdgeDetailedResultType country csAcceptEncoding
csAccept cacheBehaviour csHeader csHeaderName csHeaderCount
```

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Amazon GuardDuty

The IBM QRadar DSM for Amazon GuardDuty collects Amazon GuardDuty events from the log group of the Amazon CloudWatch logs services.

The following table identifies the specifications for the Amazon GuardDuty DSM:

Table 211. Amazon GuardDuty DSM specifications

Specification	Value
Manufacturer	Amazon
DSM name	Amazon GuardDuty
RPM file name	`DSM-AmazonGuardDuty-QRadar_version-buildbuild_number.noarch.rpm`
Supported versions	GuardDuty Schema Version 2.0
Protocol	Amazon Web Services Amazon AWS REST API
Event format	JSON
Recorded event types	Amazon GuardDuty Findings
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	For more information, see the Amazon GuardDuty Documentation (https://aws.amazon.com/documentation/guardduty).

Configuring an Amazon GuardDuty log source by using the Amazon Web Services protocol

If you want to collect Amazon GuardDuty logs from the Amazon Cloud Watch group, configure a log source on the IBM QRadar Console so that Amazon Guard Duty can communicate with QRadar by using the Amazon Web Services protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website (https://www.ibm.com/support/fixcentral) onto your QRadar Console:
   - Protocol Common RPM
   - Amazon Web Services Protocol RPM
   - DSMCommon RPM
   - Amazon GuardDuty DSM RPM
2. Create and configure an Amazon EventBridge rule to send events from AWS Security Hub to AWS CloudWatch log group.
3. Create an Identity and Access (IAM) user in the Amazon AWS user interface when using the Amazon Web Services protocol.
4. Add a Log source for Amazon GuardDuty on the QRadar Console. The following table describes the Amazon Web Services protocol parameters that require specific values for Amazon GuardDuty Logs collection:

Table 212. Amazon GuardDuty Web Services protocol parameters	
Parameter	**Value**
Log source type	**Amazon GuardDuty**
Protocol configuration	**Amazon Web Services**
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used anywhere. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choose this option to use the **IAM Role** from the metadata assigned to the instance for authentication. No keys are required. **Note:** This method works only for managed hosts that run within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key**, the **Access Key ID** parameter displays. The **Access Key ID** was generated when you configured the security credentials for your AWS user account. For more information about configuring the security credentials, see Configuring security credentials for your AWS user account.
Secret Access Key	If you selected **Access Key ID / Secret Key**, the **Secret Access Key** parameter displays. The **Secret Key** was generated when you configured the security credentials for your AWS user account. For more information about configuring the security credentials, see Configuring security credentials for your AWS user account.
Regions	Select the check box for each region that is associated with the Amazon Web Service that you want to collect logs from.
Other Regions	Type the names of any additional regions that are associated with the Amazon Web Service that you want to collect logs from. To collect from multiple regions, use a comma-separated list, such as the following example: `region1,region2`
AWS Service	The name of the Amazon Web Service. From the **AWS Service** list, select **CloudWatch Logs**.

Table 212. Amazon GuardDuty Web Services protocol parameters (continued)

Parameter	Value
Log Group	The name of the log group in Amazon CloudWatch where you want to collect logs from. **Tip:** A single log source can collect CloudWatch logs from only one log group at a time. If you want to collect logs from multiple log groups, create a separate log source for each log group.
Log Stream (Optional)	The name of the log stream within a log group that you want to collect logs from.
Filter Pattern (Optional)	Type a pattern for filtering the collected events. This pattern is not a regex filter. Only the events that contain the exact value that you specify are collected from CloudWatch Logs. If you enter **ACCEPT** as the Filter Pattern value, only events that contain the word **ACCEPT** are collected. The following example shows the effect of the **ACCEPT** value: `{LogStreamName: LogStreamTest,Timestamp: 0,Message: ACCEPT OK,IngestionTime: 0,EventId: 0}`
Extract Original Event	CloudWatch Logs wrap events that it receives with extra metadata. If you want only the original event that was added to the CloudWatch logs to be forwarded to QRadar, select this option. The original event is the value for the message key that is extracted from the CloudWatch Logs. The following CloudWatch logs event example shows the original event that is extracted from the CloudWatch log in bold text: `{LogStreamName: guardDutyLogStream,Timestamp: 1519849569827,Message: {"version": "0", "id": "00-00", "detail-type": "GuardDuty Finding", "account": "1234567890", "region": "us-west-2", "resources": [], "detail": {"schemaVersion": "2.0", "accountId": "1234567890", "region": "us-west-2", "partition": "aws", "type": "Behavior:IAMUser/InstanceLaunchUnusual", "severity": 5.0, "createdAt": "2018-02-28T20:22:26.344Z", "updatedAt": "2018-02-28T20:22:26.344Z"}},IngestionTime: 1519849569862,EventId: 0000}`
Use As A Gateway Log Source	Do not select this check box.

Table 212. Amazon GuardDuty Web Services protocol parameters (continued)	
Parameter	**Value**
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Automatically Acquire Server Certificates	If you select **Yes** from the list, QRadar downloads the certificate and begins trusting the target server. This function can be used to initialize a newly created log source and obtain certificates initially, or to replace expired certificates.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Related tasks

"Creating an EventBridge rule for sending events" on page 419
You need to create and configure an Amazon EventBridge rule to send events from AWS Security Hub to AWS CloudWatch log group.

"Creating an Identity and Access (IAM) user in the AWS Management Console" on page 326
"Adding a DSM" on page 4
"Adding a log source" on page 5

Creating an EventBridge rule for sending events

You need to create and configure an Amazon EventBridge rule to send events from AWS Security Hub to AWS CloudWatch log group.

Procedure

1. Go to Amazon EventBridge.
2. In the **Create a new rule** pane, click **Create rule**.
3. In the **Name and description** pane, type a name for your rule in the **Name** field and if you want, type a description for your rule in the **Description** field.
4. In the **Define pattern** pane, select **Event pattern**, and then select **Pre-defined pattern by service** to build an event pattern.
5. From the **Service provider** list, select **AWS**.
6. From the **Service name** list, select **GuardDuty**.
7. From the **Event type** list, select **All Events**.
8. In the **Select event bus** pane, select **AWS default event bus**.
9. In the **Select targets** pane, from the **Target** list, select **CloudWatch log group**.

10. In the **Log Group:** section, specify a new log group or select an existing log group from the list.

    Important: You need the name of the log group when you configure a log source in QRadar.
11. Click **Create**.

What to do next

Creating an Identity and Access (IAM) user in the AWS Management Console

Creating an Identity and Access (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **CloudWatchLogsReadOnlyAccess** policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Create an Amazon AWS IAM user and then apply the **CloudWatchLogsReadOnlyAccess** policy.

What to do next

Amazon Web Services log source parameters for Amazon AWS Security Hub

Configuring an Amazon GuardDuty log source by using the Amazon AWS S3 REST API protocol

If you want to collect Amazon GuardDuty findings when you use an AWS S3 Bucket, add a log source in IBM QRadar by using the Amazon AWS S3 REST API protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common RPM
   - Amazon AWS REST API Protocol RPM
   - DSMCommon RPM
   - Amazon GuardDuty DSM RPM
2. Configure Amazon GuardDuty to forward events to an AWS S3 Bucket.
3. Use the following table to set the parameters for an Amazon AWS CloudTrail log source that uses the Amazon AWS S3 REST API protocol.

Table 213. Amazon AWS S3 REST API protocol log source parameters

Parameter	Description
Log Source Type	**Amazon GuardDuty**
Protocol Configuration	**Amazon AWS S3 REST API**

Table 213. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see Configuring security credentials for your AWS user account. **EC2 Instance IAM Role** If your QRadar managed host is running in an AWS EC2 instance, choose this option to use the **IAM Role** from the metadata that is assigned to the instance for authentication. No keys are required. **Important:** This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, configure this parameter. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. For more information about configuring the security credentials, see Configuring security credentials for your AWS user account.
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, configure this parameter. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket. For more information about configuring the security credentials. see Configuring security credentials for your AWS user account.
S3 Collection Method	Select one of the following collection methods. • **SQS Event Notifications** • **Use a Specific Prefix - Single Account/Region Only**
SQS Queue URL	If you selected **SQS Event Notifications** for the **S3 Collection Method**, configure this parameter. This field uses the full url of the SWS setup, beginning with https://, to receive notifications for ObjectCreate events from S3. For example, `https://sqs.us-east-2.amazonaws.com/1234567890123/CloudTrail_SQS_QRadar` For more information, see the *Configuring Amazon S3 event notifications* link to public site website (https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html) To ensure that all data is processed and messages are deleted from the queue after the files are successfully processed, this configuration must be the only consumer of this queue.

Table 213. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
Bucket Name	If you selected **Use a Specific Prefix - Single Account/Region Only** for the **S3 Collection Method**, configure this parameter. The name of the AWS S3 bucket where the log files are stored.
Directory Prefix	If you selected **Use a Specific Prefix - Single Account/Region Only** for the **S3 Collection Method**, configure this parameter. The root directory location on the AWS S3 bucket from where the CloudTrail logs are retrieved; for example, `AWSLogs/<AccountNumber>/CloudTrail/<RegionName>/` To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path. **Tip:** • Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. • The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket. • If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use `folder1/folder2` instead).
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Event Format	Select **LINEBYLINE**. The log files that are collected contain one record per line. Compression with `gzip` (`.gz` or `.gzip`) and `zip` (`.zip`) is supported.
Use as a Gateway Log Source	Do not enable this option.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Automatically Acquire Server Certificate	If you select Yes from the list, QRadar downloads the certificate and begins trusting the target server. This function can be used to initialize a newly created log source and obtain certificates initially, or to replace expired certificates.

Table 213. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Configuring an Amazon GuardDuty log source that uses Amazon Security Lake

You can collect Amazon GuardDuty logs from multiple accounts or regions in an Amazon S3 bucket. IBM QRadar uses the Amazon AWS S3 REST API protocol to communicate with Amazon Security Lake, where QRadar obtains the Amazon GuardDuty logs.

Procedure

1. Configure Amazon Security Lake to log Open Cybersecurity Schema Framework (OCSF) data in Parquet format to an S3 bucket. For more information, see Collecting data from custom sources.

   Note: The supported OCSF version of the DSM is OCSF 1.0RC2. The version OCSF 1.1 is not currently supported.
2. Configure access to the OCSF data in Amazon Security Lake by using one of two methods.
   - To create a subscriber to provision the SQS queue and IAM role, see step 3.

     For more information about creating a subscriber, see Managing data access for Security Lake subscribers.
   - To manually configure the SQS queue and ObjectCreated notifications, see step 4.
3. Create a subscriber to provision the SQS queue and IAM role.
   a) When you create the subscription, take note of the following values: **SQS Queue URL**, **IAM Role ARN**, and **External ID**.
   b) If you plan to access this subscription from a different account than where Amazon Security Lake is set up, you must provide that account ID to configure the trust relationship properly.

4. Manually configure the SQS queue and ObjectCreated notifications.
   a) Configure an SQS queue to receive ObjectCreated notifications with either Amazon S3 Event Notifications or AWS EventBridge when new OCSF Parquet data is available in the Amazon Security Lake bucket in the folder you choose.
   b) Provision access keys with permission (either directly or with an **IAM Assume Role**) to access both the SQS queue and the bucket that contain the Amazon Security Lake data.

   For more information, see "Create an SQS queue and configure S3 ObjectCreated notifications" on page 302.
5. Configure a log source in QRadar to collect and parse the data.

   Tip: When new OCSF parquet data is available, a message that contains the bucket name and object key of the file with the data to be processed is sent to the SQS queue. QRadar then downloads and processes this file.

What to do next

Add a CloudTrail log source in QRadar. For more information, see "Adding an Amazon GuardDuty log source on the QRadar Console using an SQS queue" on page 433.

Related information

What Is Amazon EventBridge?

Amazon S3 Event Notifications

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.

Finding the S3 bucket that contains the data that you want to collect

You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **`Region Name`** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

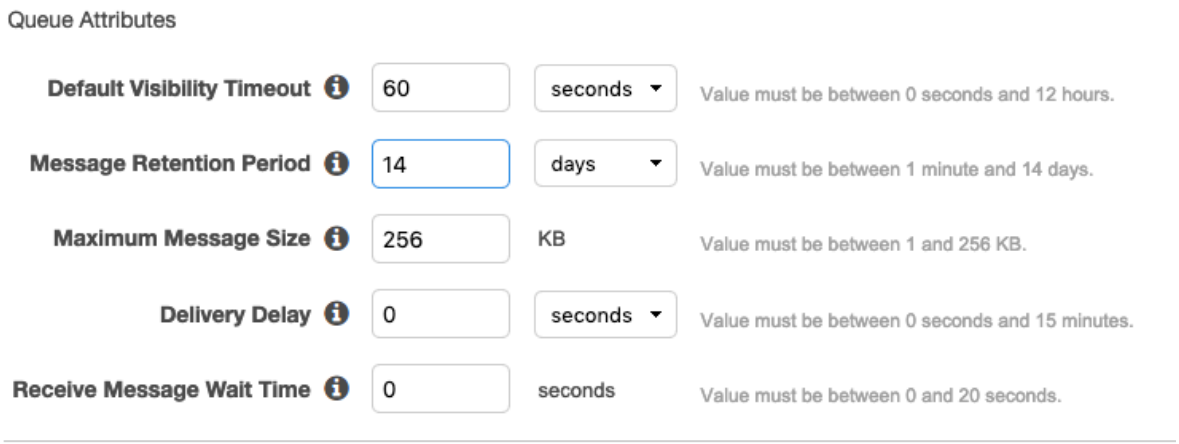
You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.
3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.
   - **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

   Use the default value for the remaining **Queue Attributes**.

   More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions

You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.

3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 214. Permission parameters	
Parameter	**Value**
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

   d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 215. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
```

```
        }
      }
    ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications

Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.
3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 216. Example: New ObjectCreated notification parameter configuration

Parameter	**Value**
Name	Type a name of your choosing.
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

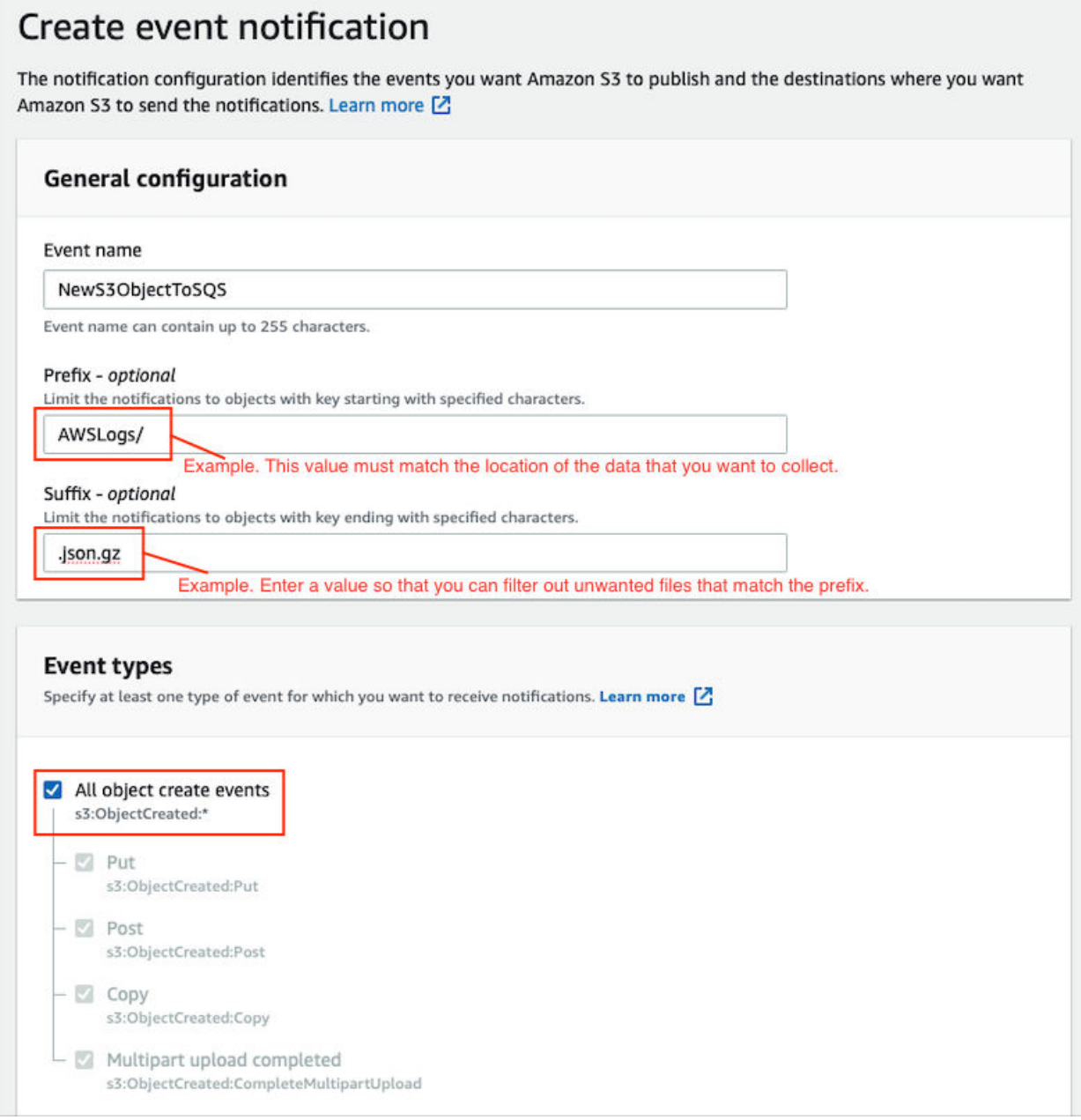


Figure 26. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

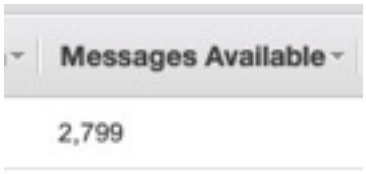


Figure 27. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

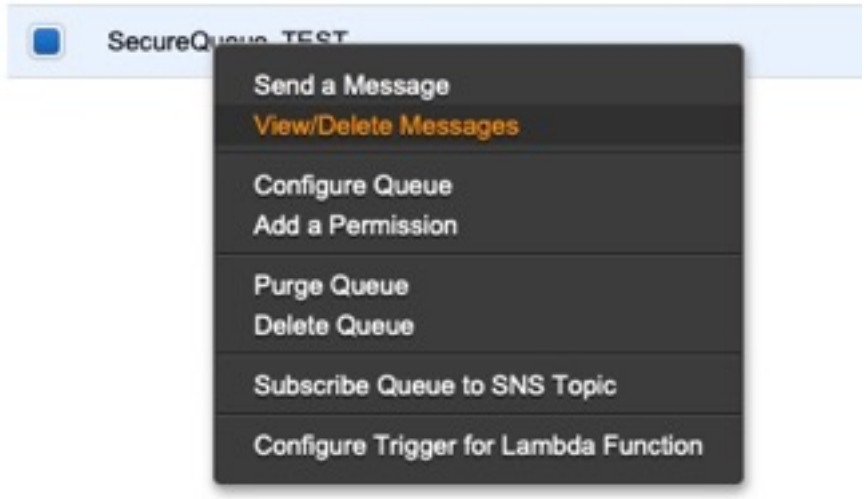


Figure 28. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

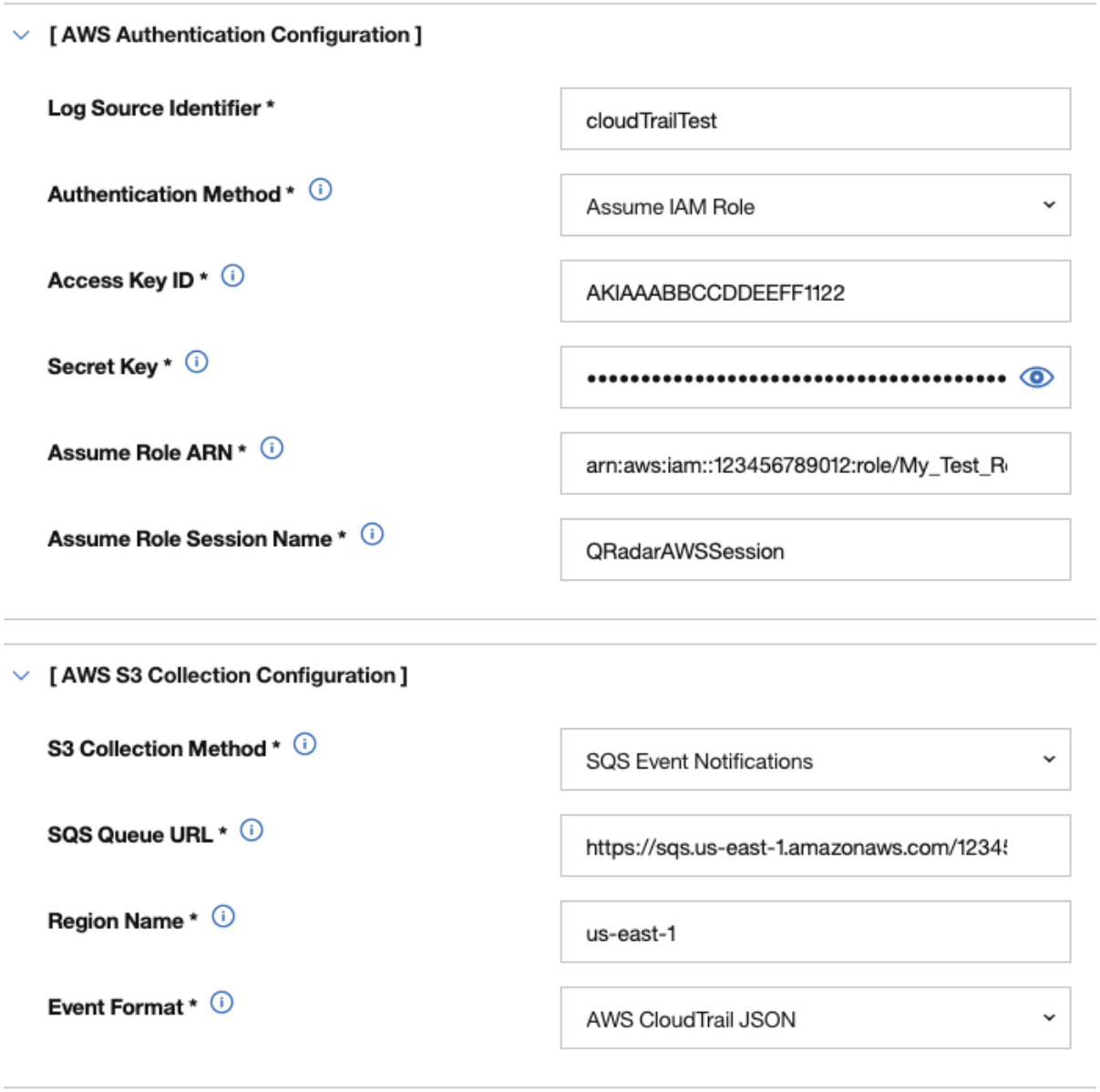


Figure 29. Example: Amazon AWS CloudTrail log source configuration in QRadar

Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge

Create an Amazon EventBridge rule to forward ObjectCreated notifications to a target SQS queue.

Before you begin

Before you can create a rule in Amazon EventBridge, you must enable Amazon EventBridge on your AWS Management console. For more information, see Enabling Amazon EventBridge.

Procedure

1. Open the Amazon EventBridge console.
2. From the **Navigation** menu, click **Rules** > **Create rule**.
3. On the **Create rule** window, complete the following steps:
   a) Enter a name and description for the rule.

      Important: A rule can't have the same name as another rule that is both in the same region and on the same event bus.

   b) For **Event bus**, select the event bus that you want to associate with this rule. If you select **AWS default event bus**, the rule matches the events that come from your account.

   c) For **Rule type**, select **Rule with an event pattern**.
4. Click **Next**.
5. For **Event source**, select **AWS events or EventBridge partner events**.
6. For **Creation method**, select **Use pattern form**.
7. In the **Event pattern** window, configure the event pattern by completing the following steps:
   a) Select the values listed in the table for the following parameters:

Parameter	Value
Event source	**AWS services**
AWS service	**Simple Storage Service (S3)**
Event type	**Amazon S3 Event Notification**

   b) Click the **Specific event(s)** option and select **Object Created**.

   c) Click **Specific bucket(s) by name** and enter the name of the specific bucket that you want to collect events from.

   d) Optional: To enable notifications for a specific folder prefix or file extension, choose **Custom pattern (JSON editor)** instead of **Use pattern form** for the creation method, and create your custom event pattern.
   For example, this event pattern filters for `Object Created` events in your bucket. In this example, `example/directory` is the directory prefix and `.png` is the suffix.

```
{
  "source": ["aws.s3"],
  "detail-type": ["Object Created"],
  "detail": {
    "bucket": {
      "name": ["<example-bucket>"]
    },
    "object": {
      "key": [{
        "prefix": "example/directory/"
      }],
      "key": [{
        "suffix": ".png"
      }]
    }
  }
}
```

e) Click **Add**, then click **Next**.

8. Choose the SQS queue that you want to use as the target. Enter the name of the queue, then click **Next**.
9. On the **Review and create** page, click **Create rule**.

Configuring Amazon GuardDuty to forward events to an AWS S3 Bucket

To collect events in QRadar, you must configure Amazon GuardDuty to forward events to an AWS S3 Bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. On the menu bar, type `GuardDuty` in the search field.
3. From the Navigation menu, select **Findings**.
4. From the **Frequency for updated findings** list, select **Update CWE and S3 every 15 minutes**.
5. In the S3 bucket section, click **Configure now**.
6. Click one of the following S3 bucket options:
   - **Existing bucket - In your account**
   - **Existing bucket - In another account**
   - **New bucket - Create a new bucket**
7. From the **Choose a bucket** list, select your S3 bucket.
8. Optional: Enter a path prefix in the **Log file prefix** field. A new folder is created in the bucket with the path prefix name that you specified. The path that follows the field is updated to reflect the path to exported findings in the bucket.
9. Select one of the following **KMS encryption** options:
   - Select **Choose key from your account**, and then from the **Key alias** list, select the key that you changed the policy for.
   - Select **Choose key from another account**, and then type the full ARN to the key that you changed the policy for.

   The key that you select must be in the same region as the S3 bucket. For more information about how to find the key ARN, go to *Finding the key ID and ARN* on the Amazon AWS website (https://docs.aws.amazon.com/kms/latest/developerguide/find-cmk-id-arn.html).

   For more information about key policies, go to *Using key policies in AWS KMS* on the Amazon AWS website (https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html).
10. Click **Save**.

    When you generate findings in GuardDuty, they are sent to your S3 Bucket.

Adding an Amazon GuardDuty log source on the QRadar Console using an SQS queue

If you want to collect Amazon GuardDuty logs from multiple accounts or regions in an Amazon S3 bucket, add a log source on the QRadar Console so that Amazon GuardDuty can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

Procedure

1. Use the following table to set the parameters for an Amazon GuardDuty log source that uses the Amazon AWS S3 REST API protocol and an SQS queue.

Table 217. Amazon AWS S3 REST API protocol log source parameters	
Parameter	**Description**
Log Source Type	**Amazon GuardDuty**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Amazon AWS CloudTrail log source that is configured, you might want to identify the first log source as *Guarddduty1*, the second log source as *guarddduty2*, and the third log source as *guarddduty3*.
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you select **SQS Event Notifications** for the **S3 Collection Method**. The supported **S3 Collection Method** is **Use a Specific Prefix**. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **AWS Cloud Trail JSON**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **SQS Event Notifications**.
SQS Queue URL	Enter the full URL, starting with `https://`, of the SQS queue that is set up to receive notifications for ObjectCreate events from S3.
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.

Table 217. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Log Source Identifier Pattern	This option is available when you set **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.

Table 217. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
Recurrence	How often a poll is made to scan for new data. If you are using the SQS event collection method, **SQS Event Notifications** can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, **Use a Specific Prefix** has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

Table 218. Amazon sample message supported by Amazon GuardDuty.		
Event name	**Low-level category**	**Sample log message**
Console Login	General Audit Event	{"eventVersion":"1.02", "userIdentity":{"type":"IAMUser", "principalId":"XXXXXXXXXXXXXXXXXXXX", "arn":"arn:aws:iam::<Account_number>:user/ xx.xxccountId":"<Account_number>","userName": "<Username>"},"eventTime": "2016-05-04T14:10:58Z","eventSource": "f.amazonaws.com","eventName": "ConsoleLogin","awsRegion": "us-east-1","sourceIPAddress": "<Source_IP_address> Agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.1.1 Safari/537.36", "requestParameters":null, "responseElements": {"ConsoleLogin":"Success"}, "additionalEventData": {"LoginTo":"www.webpage.com", "MobileVersion":"No","MFAUsed":"No"}, "eventID":"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx", "eventType":"AwsConsoleSignIn", "recipientAccountId":"<Account_ID>"}

Amazon GuardDuty sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Amazon GuardDuty sample message when you use the Amazon AWS S3 REST API protocol

Sample 1: The following sample event message shows that an IAM entity requested an API to disable S3 and block public access on a bucket.


```
{"schemaVersion":"2.0","accountId":"111111111111","region":"region","partition":"aws","id":"6ab9
71cccd774293fcb8a9eaff944711","arn":"arn:aws:guardduty:region:111111111111:detector/
42b0d9e4fcad1600d444fc52278999c2/finding/6ab971cccd774293fcb8a9eaff944711","type":"Policy:S3/
BucketBlockPublicAccessDisabled","resource":{"resourceType":"AccessKey","accessKeyDetails":
{"accessKeyId":"GeneratedFindingAccessKeyId","principalId":"GeneratedFindingPrincipalId","userTy
pe":"IAMUser","userName":"GeneratedFindingUserName"},"s3BucketDetails":
[{"arn":"arn:aws:s3:::bucketName","name":"bucketName","type":"Destination","createdAt":"15136126
92","owner":{"id":"CanonicalId of Owner"},"tags":
[{"key":"foo","value":"bar"}],"defaultServerSideEncryption":
{"encryptionType":"SSEAlgorithm","kmsMasterKeyArn":"arn:aws:kms:region:123456789012:key/key-
id"},"publicAccess":{"permissionConfiguration":{"bucketLevelPermissions":{"accessControlList":
{"allowsPublicReadAccess":false,"allowsPublicWriteAccess":false},"bucketPolicy":
{"allowsPublicReadAccess":false,"allowsPublicWriteAccess":false},"blockPublicAccess":
{"ignorePublicAcls":false,"restrictPublicBuckets":false,"blockPublicAcls":false,"blockPublicPoli
cy":false}},"accountLevelPermissions":{"blockPublicAccess":
{"ignorePublicAcls":false,"restrictPublicBuckets":false,"blockPublicAcls":false,"blockPublicPoli
cy":false}}},"effectivePermission":"NOT_PUBLIC"}}],"instanceDetails":
{"instanceId":"i-99999999","instanceType":"m3.xlarge","outpostArn":"arn:aws:outposts:region-
name:123456789000:outpost/
op-0fbc006e9abbc73c3","launchTime":"2016-08-02T02:05:06Z","platform":null,"productCodes":
[{"productCodeId":"GeneratedFindingProductCodeId","productCodeType":"GeneratedFindingProductCode
Type"}],"iamInstanceProfile":
{"arn":"GeneratedFindingInstanceProfileArn","id":"GeneratedFindingInstanceProfileId"},"networkIn
terfaces":[{"ipv6Addresses":
[],"networkInterfaceId":"test","privateDnsName":"GeneratedFindingPrivateDnsName","privateIpAddre
ss":"10.0.0.1","privateIpAddresses":
[{"privateDnsName":"GeneratedFindingPrivateName","privateIpAddress":"10.0.0.1"}],"subnetId":"Gen
eratedFindingSubnetId","vpcId":"GeneratedFindingVPCId","securityGroups":
[{"groupName":"GeneratedFindingSecurityGroupName","groupId":"GeneratedFindingSecurityId"}],"publ
icDnsName":"GeneratedFindingPublicDNSName","publicIp":"10.51.100.0"}],"tags":
[{"key":"GeneratedFindingInstaceTag1","value":"GeneratedFindingInstaceValue1"},
{"key":"GeneratedFindingInstaceTag2","value":"GeneratedFindingInstaceTagValue2"},
{"key":"GeneratedFindingInstaceTag3","value":"GeneratedFindingInstaceTagValue3"},
{"key":"GeneratedFindingInstaceTag4","value":"GeneratedFindingInstaceTagValue4"},
{"key":"GeneratedFindingInstaceTag5","value":"GeneratedFindingInstaceTagValue5"},
{"key":"GeneratedFindingInstaceTag6","value":"GeneratedFindingInstaceTagValue6"},
{"key":"GeneratedFindingInstaceTag7","value":"GeneratedFindingInstaceTagValue7"},
{"key":"GeneratedFindingInstaceTag8","value":"GeneratedFindingInstaceTagValue8"},
{"key":"GeneratedFindingInstaceTag9","value":"GeneratedFindingInstaceTagValue9"}],"instanceState
":"running","availabilityZone":"GeneratedFindingInstaceAvailabilityZone","imageId":"ami-99999999
","imageDescription":"GeneratedFindingInstaceImageDescription"}},"service":
{"serviceName":"guardduty","detectorId":"11a1a1a1aaaa1111a111aa11111111a1","action":
{"actionType":"AWS_API_CALL","awsApiCallAction":
{"api":"GeneratedFindingAPIName","serviceName":"GeneratedFindingAPIServiceName","callerType":"Re
mote IP","remoteIpDetails":{"ipAddressV4":"10.51.100.0","organization":
{"asn":"-1","asnOrg":"GeneratedFindingASNOrg","isp":"GeneratedFindingISP","org":"GeneratedFindin
gORG"},"country":{"countryName":"GeneratedFindingCountryName"},"city":
{"cityName":"GeneratedFindingCityName"},"geoLocation":
{"lat":44.972686,"lon":-65.860879}},"affectedResources":
{"AWS::S3::Bucket":"GeneratedFindingS3Bucket"}}},"resourceRole":"TARGET","additionalInfo":
{"unusual":{"hoursOfDay":[1513609200000],"userNames":
["GeneratedFindingUserName"]},"sample":true},"eventFirstSeen":"2020-06-23T23:53:14.222Z","eventL
astSeen":"2020-06-24T00:26:33.501Z","archived":false,"count":2},"severity":2,"createdAt":"2020-0
6-23T23:53:14.222Z","updatedAt":"2020-06-24T00:26:33.501Z","title":"Amazon S3 Block Public
Access was disabled for S3 bucket GeneratedFindingS3Bucket.","description":"Amazon S3 Block
Public Access was disabled for S3 bucket GeneratedFindingS3Bucket by GeneratedFindingUserName
calling GeneratedFindingAPIName. If this behavior is not expected, it may indicate a
configuration mistake or that your credentials are compromised."}
```

Table 219. QRadar field names and highlighted values in the Amazon GuardDuty sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Policy:S3/BucketBlockPublicAccessDisabled**
Source IP	**10.51.100.0**
Event Time	**2020-06-23T23:53:14.222Z**
Username	**GeneratedFindingUserName**

Sample 2: The following sample event message shows that the S3 server access logging is disabled for a bucket.


```
{"schemaVersion":"2.0","accountId":"111111111111","region":"region","partition":"aws","id":"90b9
71cccd774ee2570756fda343dd2a","arn":"arn:aws:guardduty:region:111111111111:detector/
42b0d9e4fcad1600d444fc52278999c2/finding/90b971cccd774ee2570756fda343dd2a","type":"Stealth:S3/
ServerAccessLoggingDisabled","resource":{"resourceType":"AccessKey","accessKeyDetails":
{"accessKeyId":"GeneratedFindingAccessKeyId","principalId":"GeneratedFindingPrincipalId","userTy
pe":"IAMUser","userName":"GeneratedFindingUserName"},"s3BucketDetails":
[{"arn":"arn:aws:s3:::bucketName","name":"bucketName","type":"Destination","createdAt":"15136126
92","owner":{"id":"CanonicalId of Owner"},"tags":
[{"key":"foo","value":"bar"}],"defaultServerSideEncryption":
{"encryptionType":"SSEAlgorithm","kmsMasterKeyArn":"arn:aws:kms:region:123456789012:key/key-
id"},"publicAccess":{"permissionConfiguration":{"bucketLevelPermissions":{"accessControlList":
{"allowsPublicReadAccess":false,"allowsPublicWriteAccess":false},"bucketPolicy":
{"allowsPublicReadAccess":false,"allowsPublicWriteAccess":false},"blockPublicAccess":
{"ignorePublicAcls":false,"restrictPublicBuckets":false,"blockPublicAcls":false,"blockPublicPoli
cy":false}},"accountLevelPermissions":{"blockPublicAccess":
{"ignorePublicAcls":false,"restrictPublicBuckets":false,"blockPublicAcls":false,"blockPublicPoli
cy":false}}},"effectivePermission":"NOT_PUBLIC"}}],"instanceDetails":
{"instanceId":"i-99999999","instanceType":"m3.xlarge","outpostArn":"arn:aws:outposts:region-
name:123456789000:outpost/
op-0fbc006e9abbc73c3","launchTime":"2016-08-02T02:05:06Z","platform":null,"productCodes":
[{"productCodeId":"GeneratedFindingProductCodeId","productCodeType":"GeneratedFindingProductCode
Type"}],"iamInstanceProfile":
{"arn":"GeneratedFindingInstanceProfileArn","id":"GeneratedFindingInstanceProfileId"},"networkIn
terfaces":[{"ipv6Addresses":
[],"networkInterfaceId":"test","privateDnsName":"GeneratedFindingPrivateDnsName","privateIpAddre
ss":"10.0.0.1","privateIpAddresses":
[{"privateDnsName":"GeneratedFindingPrivateName","privateIpAddress":"10.0.0.1"}],"subnetId":"Gen
eratedFindingSubnetId","vpcId":"GeneratedFindingVPCId","securityGroups":
[{"groupName":"GeneratedFindingSecurityGroupName","groupId":"GeneratedFindingSecurityId"}],"publ
icDnsName":"GeneratedFindingPublicDNSName","publicIp":"10.51.100.0"}],"tags":
[{"key":"GeneratedFindingInstaceTag1","value":"GeneratedFindingInstaceValue1"},
{"key":"GeneratedFindingInstaceTag2","value":"GeneratedFindingInstaceTagValue2"},
{"key":"GeneratedFindingInstaceTag3","value":"GeneratedFindingInstaceTagValue3"},
{"key":"GeneratedFindingInstaceTag4","value":"GeneratedFindingInstaceTagValue4"},
{"key":"GeneratedFindingInstaceTag5","value":"GeneratedFindingInstaceTagValue5"},
{"key":"GeneratedFindingInstaceTag6","value":"GeneratedFindingInstaceTagValue6"},
{"key":"GeneratedFindingInstaceTag7","value":"GeneratedFindingInstaceTagValue7"},
{"key":"GeneratedFindingInstaceTag8","value":"GeneratedFindingInstaceTagValue8"},
{"key":"GeneratedFindingInstaceTag9","value":"GeneratedFindingInstaceTagValue9"}],"instanceState
":"running","availabilityZone":"GeneratedFindingInstaceAvailabilityZone","imageId":"ami-99999999
","imageDescription":"GeneratedFindingInstaceImageDescription"}},"service":
{"serviceName":"guardduty","detectorId":"11a1a1a1aaaa1111a111aa11111111a1","action":
{"actionType":"AWS_API_CALL","awsApiCallAction":
{"api":"GeneratedFindingAPIName","serviceName":"GeneratedFindingAPIServiceName","callerType":"Re
mote IP","remoteIpDetails":{"ipAddressV4":"10.51.100.0","organization":
{"asn":"-1","asnOrg":"GeneratedFindingASNOrg","isp":"GeneratedFindingISP","org":"GeneratedFindin
gORG"},"country":{"countryName":"GeneratedFindingCountryName"},"city":
{"cityName":"GeneratedFindingCityName"},"geoLocation":
{"lat":44.972686,"lon":-65.860879}},"affectedResources":
{"AWS::S3::Bucket":"GeneratedFindingS3Bucket"}}},"resourceRole":"TARGET","additionalInfo":
{"unusual":{"hoursOfDay":[1513609200000],"userNames":
["GeneratedFindingUserName"]},"sample":true},"eventFirstSeen":"2020-06-23T23:53:14.222Z","eventL
astSeen":"2020-06-24T00:26:33.501Z","archived":false,"count":2},"severity":2,"createdAt":"2020-0
6-23T23:53:14.222Z","updatedAt":"2020-06-24T00:26:33.501Z","title":"Amazon S3 Server Access
Logging was disabled for S3 bucket GeneratedFindingS3Bucket.","description":"Amazon S3 Server
Access Logging was disabled for S3 bucket GeneratedFindingS3Bucket by GeneratedFindingUserName
calling PutBucketLogging. This can lead to lack of visibility into actions taken on the
affected S3 bucket and its objects if an event occurs."}
```

Table 220. QRadar field names and highlighted values in the Amazon GuardDuty sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Stealth:S3/ServerAccessLoggingDisabled**
Source IP	**10.51.100.0**
Event Time	**2020-06-23T23:53:14.222Z**
Username	**GeneratedFindingUserName**

Amazon VPC Flow Logs

The IBM QRadar integration for Amazon VPC (Virtual Private Cloud) Flow Logs collects VPC flow logs from an Amazon S3 bucket by using an SQS queue.

Important: This integration supports the default format for Amazon VPC Flow Logs and any custom formats that contain version 3, 4, or 5 fields. However, all version 2 fields must be included in your custom format. The default format includes the following fields.

```
${version} ${account-id} ${interface-id} ${srcaddr} ${dstadir} ${srcport} ${dstport} $
{protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}
```

For more information, see the Amazon VPC Flow Logs documentation.

To integrate Amazon VPC Flow Logs with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the following RPMs on your QRadar Console.
   - Protocol Common RPM
   - AWS S3 REST API PROTOCOL RPM

   Important: If you are installing the RPM to enable more AWS-related VPC flow fields in the QRadar Network Activity Flow Details window, then the following services must be restarted before they are visible. You don't need to restart the services for the protocol to function.

   Hostcontext
   To restart **host context**, see QRadar: Hostcontext service and the impact of a service restart (https://www.ibm.com/support/pages/qradar-hostcontext-service-and-impact-service-restart).

   Tomcat
   On the Console, click the **Admin** tab, and then click **Advanced** > **restart Web Server**.
2. Configure your Amazon VPC Flow Logs to publish the flow logs to an S3 bucket.
3. Create the SQS queue that is used to receive `ObjectCreated` notifications from the S3 bucket that you used in step 2.
4. Create security credentials for your AWS user account.
5. Add an Amazon VPC Flow Logs log source on the QRadar Console.

   Important: A Flow Processor must be available and have a FPM license to receive the flow logs. VPC Flow Log does not use an EPS license. Unlike other log sources, AWS VPC Flow Log events are not sent to the **Log Activity** tab. They are sent to the **Network Activity** tab.

   Important: When the VPC Flow Logs log source is configured by using Universal DSM, it does not generate any event. In this case, the **Last Event** time status remains blank.

   The following table describes the parameters that require specific values to collect events from Amazon VPC Flow Logs:

Table 221. Amazon VPC Flow Logs log source parameters	
Parameter	**Value**
Log Source type	A custom log source type.
Protocol Configuration	Amazon AWS S3 REST API
Target Event Collector	The Event Collector or Event Processor that receives and parses the events from this log source. **Tip:** This integration collects raw event logs of Amazon VPC Flow Logs from the target AWS S3 bucket. Then, it generates IPFIX flow records and forwards the records to the **VPC Flow Destination Hostname**. You can use a Flow Collector or a Flow Processor as the target event collector only when it is a combined Flow Collector and Flow Processor or an all-in-one console.
Log Source Identifier	Type a unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you configured more than one Amazon VPC flow Logs log source, you might want to name in an identifiable way. For example, you can identify the first log source as *vpcflowlogs1* and the second log source as *vpcflowlogs2*.
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see "Configuring security credentials for your AWS user account" on page 310. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication. No keys are needed. This method works only for managed hosts that are running within an AWS EC2 container.
Assume IAM Role	Enable this option by authenticating with an Access Key or EC2 instance IAM Role. Then, you can temporarily assume an IAM Role for access. This option is available only when you use the SQS Event Notifications collection method. For more information about creating IAM users and assigning roles, see Creating an Identity and Access Management (IAM) user in the AWS Management Console.
Event Format	AWS VPC Flow Logs
S3 Collection Method	SQS Event Notifications

Table 221. Amazon VPC Flow Logs log source parameters (continued)

Parameter	Value
VPC Flow Destination Hostname	The hostname or IP address of the Flow Processor where you want to send the VPC logs. **Tip:** For QRadar to accept IPFIX flow traffic, you must configure a NetFlow/IPFIX flow source that uses UDP. Most deployments can use a **default_Netflow** flow source and set the **VPC Flow Destination Hostname** to the hostname of that managed host. If the managed host that is configured with the NetFlow/IPFIX flow source is the same as the **Target Event Collector** that was chosen earlier in the configuration, you can set the **VPC Flow Destination Hostname** to *localhost*. For more information about creating flow sources, see the *IBM QRadar Administration Guide*.
VPC Flow Destination Port	The port for the Flow Processor where you want to send the VPC logs. **Important:** This port must be the same as the monitoring port that is specified in the NetFlow flow source. The port for the **default_Netflow** flow source is 2055.
SQS Queue URL	The full URL that begins with `https://`, for the SQS Queue that is set up to receive notifications for ObjectCreated events from S3.
Region Name	The region that is associated with the SQS queue and S3 bucket. Example: us-east-1, eu-west-1, ap-northeast-3
Show Advanced Options	The default is **No**. Select **Yes** if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is `http://s3.amazonaws.com`.

Table 221. Amazon VPC Flow Logs log source parameters (continued)	
Parameter	**Value**
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	How often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieves them. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 1 minute. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15 M = 15 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.

6. To send VPC flow logs to the IBM QRadar Cloud Visibility app for visualization, complete the following steps:
   a. On the Console, click the **Admin** tab, and then click **System Configuration** > **System Settings**.
   b. Click the **QFlow Settings** menu, and in the **IPFix additional field encoding** field, choose either the **TLV** or **TLV and Payload** format.
   c. Click **Save**.
   d. From the menu bar on the **Admin** tab, click **Deploy Full Configuration** and confirm your changes.

      Warning: When you deploy the full configuration, QRadar services are restarted. During this time, events and flows are not collected, and offenses are not generated.

   e. Refresh your browser.

For more information about configuring the Amazon AWS S3 REST API protocol, see Amazon AWS S3 REST API protocol configuration options.

Related concepts

"Create the SQS queue that is used to receive ObjectCreated notifications" on page 444
You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when using the Amazon AWS REST API protocol.

Related tasks

"Adding a DSM" on page 4
"Publishing flow logs to an S3 bucket" on page 288
Complete these steps to publish flow logs to an S3 bucket.

"Configuring security credentials for your AWS user account" on page 310

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Related information

Adding a log source

Amazon VPC Flow Logs specifications

The following table describes the specifications for collecting Amazon VPC Flow Logs.

Table 222. Amazon VPC Flow Logs specifications

Specification	Value
Manufacturer	Amazon
DSM name	A custom log source type
RPM file name	AWS S3 REST API PROTOCOL
Supported versions	Flow logs v5
Protocol	AWS S3 REST API PROTOCOL
Event format	IPFIX by using QRadar Flow Sources
Recorded event types	Network Flows
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Amazon's VPC Flow Logs documentation (https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html)

Publishing flow logs to an S3 bucket

Complete these steps to publish flow logs to an S3 bucket.

Procedure

1. Log in to your AWS Management console, and then from the **Services** menu, navigate to the **VPC Dashboard**.
2. Enable the check box for the VPC ID that you want to create flow logs for.
3. Click the **Flow Logs** tab.
4. Click **Create Flow Log**, and then configure the following parameters:

Table 223. Create Flow Log parameters

Parameter	Description
Filter	Select **Accept, Reject, or All**.
Destination	Select **Send to an S3 Bucket**.
S3 Bucket ARN	Type the ARN for the S3 Bucket. Examples: • `arn:aws;s3:::myTestBucket` • `arn:aws:s3:::myTestBucket/testFlows`

5. Click **Create**.

   For more information about publishing flow logs to Amazon S3, see the Publishing Flow Logs to Amazon S3 documentation on the AWS website.

What to do next

Create the SQS queue that is used to receive ObjectCreated notifications.

Create the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when using the Amazon AWS REST API protocol.

To create the SQS queue and configure S3 ObjectCreated notifications, see the AWS S3 REST API documentation about "Creating ObjectCreated notifications" on page 305.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

AWS Verified Access

The IBM QRadar DSM for AWS Verified Access supports events that are collected from Amazon S3 buckets, and from a Log group in the AWS Verified Access Logs.

Before you can integrate AWS Verified Access Logs with QRadar, you need to enable Verfied Access logs on the Amazon VPC console. To enable Verified Access logs, you must have permissions for delivery to Amazon S3.

For more information about permissions for delivery to Amazon S3 and enabling AWS Verified Access logs, go to the Enable Access Logs documentation on the Amazon website (https://docs.aws.amazon.com/verified-access/latest/ug/access-logs-enable.html).

Tip: When you enable Verified Access Logs, select the option to enable delivery to Amazon S3.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

"Configuring an AWS Verified Access log source by using the Amazon AWS S3 REST API protocol" on page 445

If you want to collect AWS Verified Access logs from Amazon S3 buckets, configure a log source on the QRadar Console so that AWS Verified Access can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

AWS Verified Access DSM specifications

When you configure the AWS Verified Access DSM, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported protocols are before you begin can help reduce frustration during the configuration process.

The following table lists the specifications for the AWS Verified Access DSM:

Table 224. AWS Verified Access DSM specifications

Specification	**Value**
Manufacturer	Amazon
DSM	AWS Verified Access
RPM name	`DSM-AWSVerifiedAccess-`*`QRadar_version-Build_number`*`.noarch.rpm`
Supported protocols	• Amazon AWS S3 REST API • Syslog
Event format	JSON
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	Yes
More information	For more information about AWS Verified Access logs, go to the AWS website.

Configuring an AWS Verified Access log source by using the Amazon AWS S3 REST API protocol

If you want to collect AWS Verified Access logs from Amazon S3 buckets, configure a log source on the QRadar Console so that AWS Verified Access can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Amazon AWS S3 REST API Protocol RPM
   - DSMCommon RPM
   - Amazon Web Service RPM
   - AWS Verified Access DSM RPM
2. Choose which method that you want to use to configure an AWS Verified Access log source by using the Amazon AWS S3 REST API protocol.
   - "Configuring an AWS Verified Access log source that uses an S3 bucket with an SQS queue" on page 446

- "Configuring an AWS Verified Access log source that uses an S3 bucket with a directory prefix" on page 458

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring an AWS Verified Access log source that uses an S3 bucket with an SQS queue

If you want to collect AWS Verified Access logs from multiple accounts or regions in an Amazon S3 bucket, configure a log source on the QRadar Console so that AWS Verified Access can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

About this task

Using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue instead of with a directory prefix has the following advantages:

- You can use one log source for an S3 bucket, rather than one log source for each region and account.
- There is a reduced chance of missing files because this method uses ObjectCreated notifications to determine when new files are ready.
- It's easy to balance the load across multiple Event Collectors because the SQS queue supports connections from multiple clients
- Unlike the directory prefix method, the SQS queue method does not require that the file names in the folders be in a string that is sorted in ascending order based on the full path. File names from custom applications don't always conform to this.
- You can monitor the SQS queue and set up alerts if it gets over a certain number of records. These alerts provide information about whether QRadar is either falling behind or not collecting events.
- You can use IAM Role authentication with SQS, which is Amazon's best practice for security.
- Certificate handling is improved with the SQS method and does not require the downloading of certificates to the Event Collector.

Procedure

1. Create the SQS queue that is used to receive ObjectCreated notifications.
2. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
3. Configure the security credentials for your AWS user account.
4. Add an AWS Verified Access log source on the QRadar Console that uses an SQS queue.

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.
2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.

Related tasks

"Adding a log source" on page 5

Finding the S3 bucket that contains the data that you want to collect
You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **`Region Name`** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications
You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

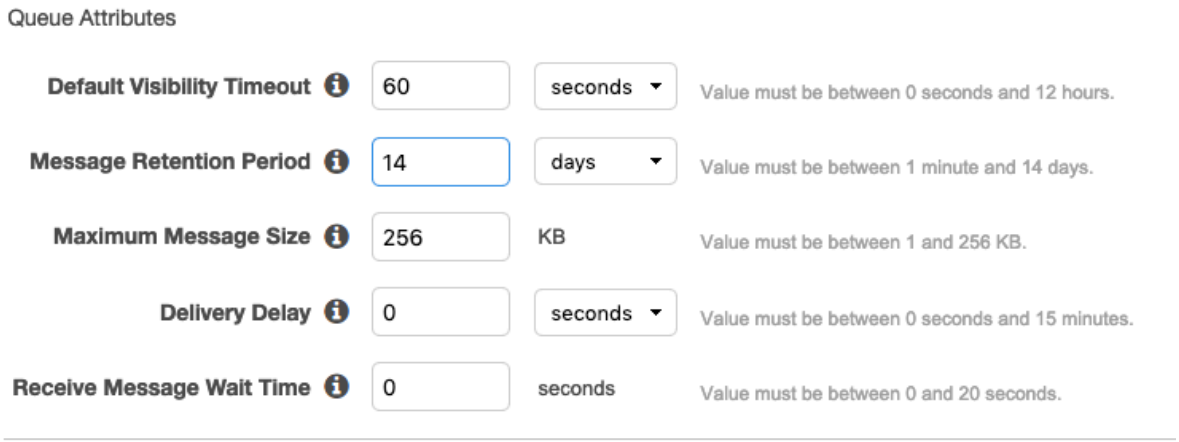
Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.
3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.

   - **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

   Use the default value for the remaining **Queue Attributes**.

   More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions
You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.
3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 225. Permission parameters	
Parameter	**Value**
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

   d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 226. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
      }
    }
  ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications
Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.
3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 227. Example: New ObjectCreated notification parameter configuration	
Parameter	**Value**
Name	Type a name of your choosing.

Table 227. Example: New ObjectCreated notification parameter configuration (continued)

Parameter	Value
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

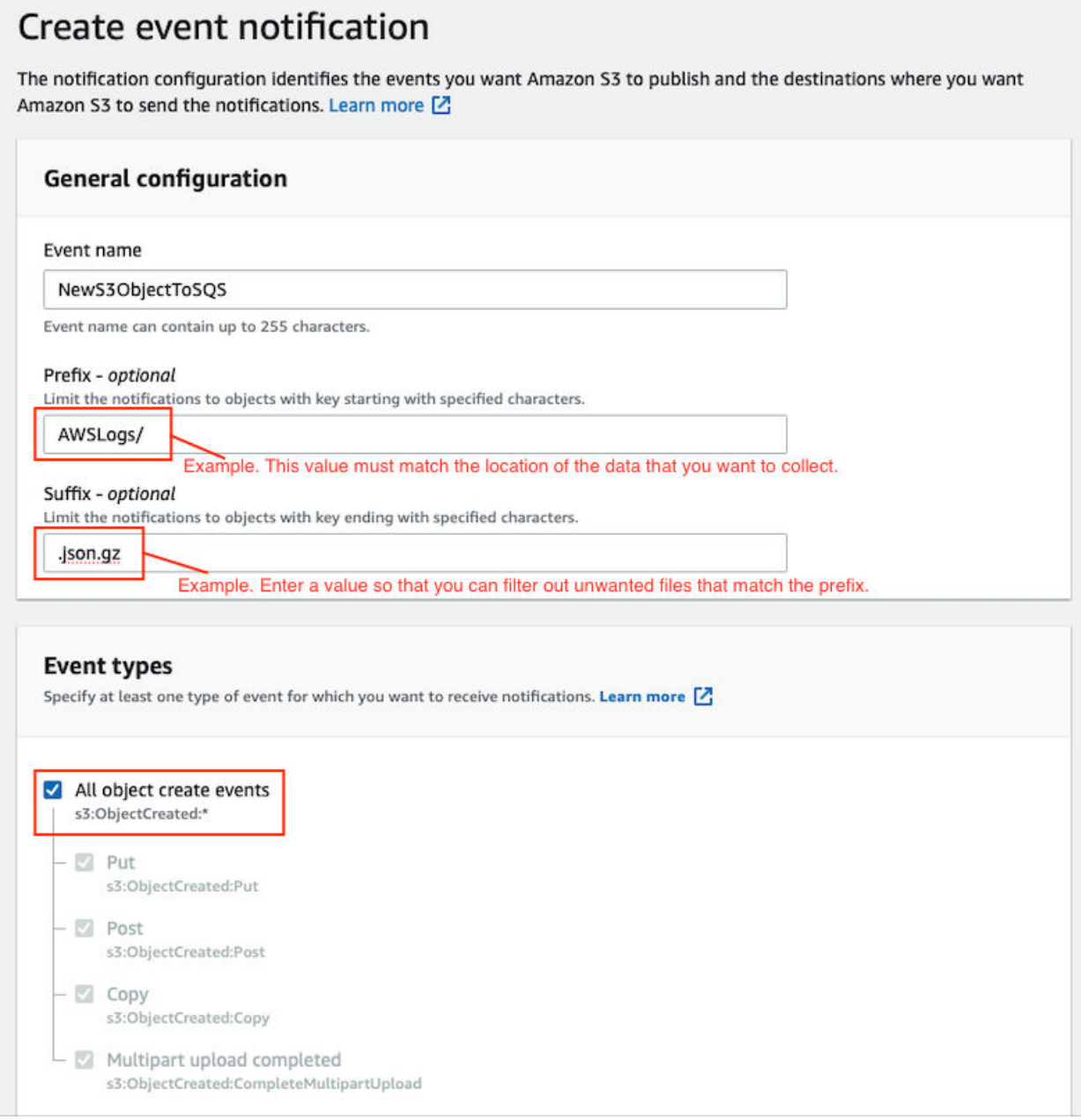


Figure 30. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

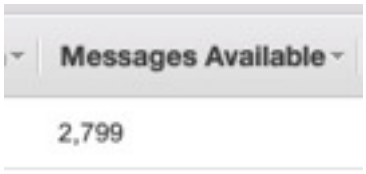


Figure 31. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

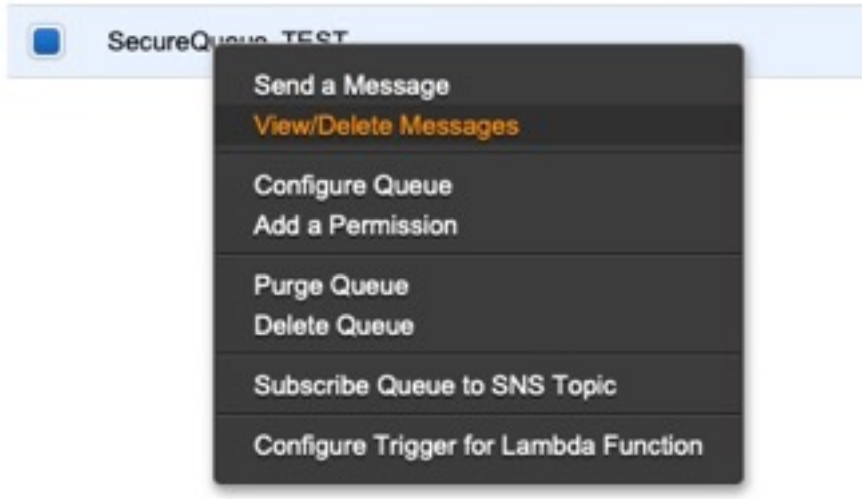


Figure 32. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

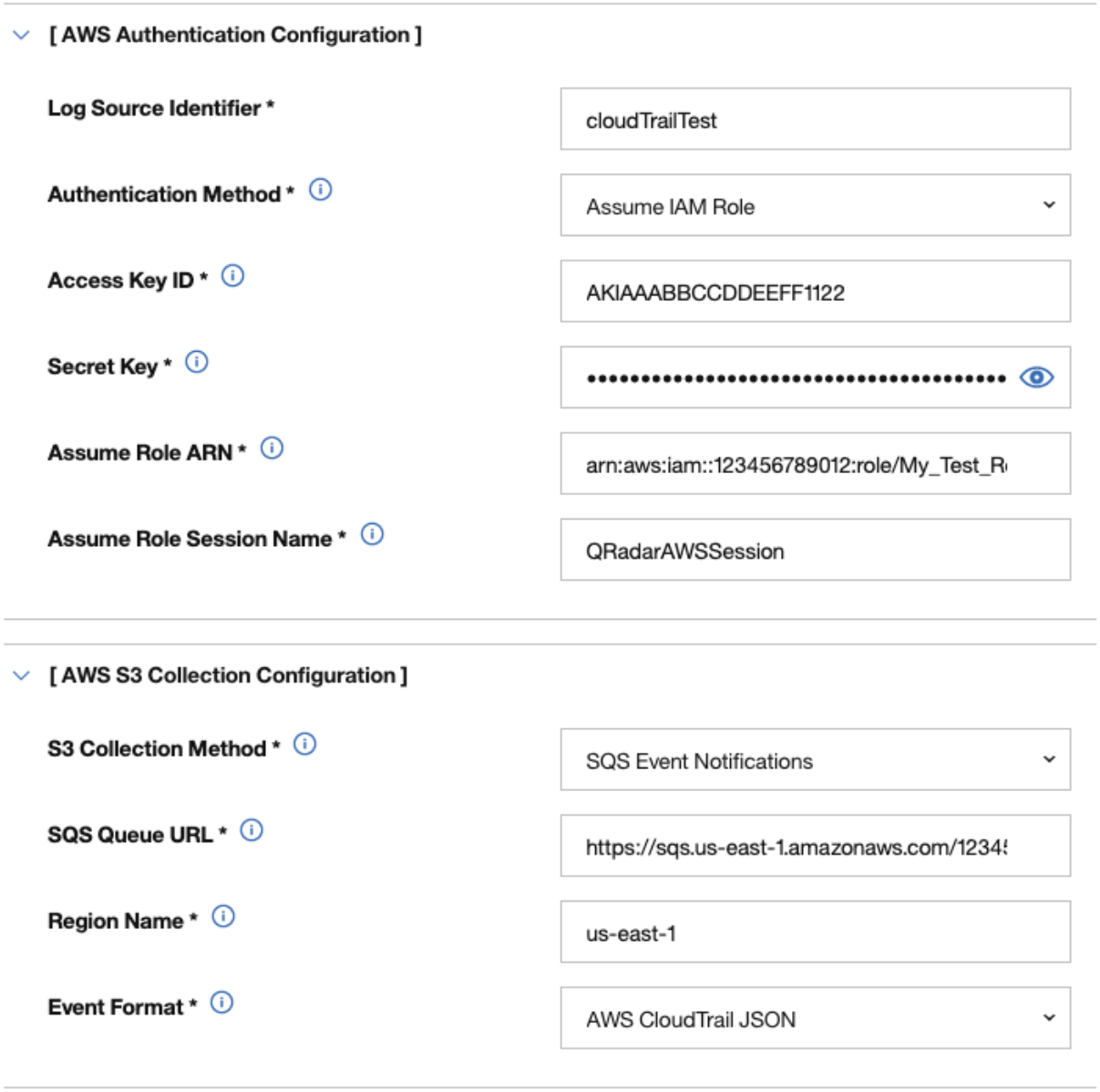


Figure 33. Example: Amazon AWS CloudTrail log source configuration in QRadar

Configuring security credentials for your AWS user account
You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information
Adding a log source

Adding an AWS Verified Access log source on the QRadar Console using an SQS queue
If you want to collect AWS Verified Access logs from multiple accounts or regions in an Amazon S3 bucket, add a log source on the QRadar Console so that AWS Verified Access can communicate with QRadar by using the Amazon AWS S3 REST API protocol and a Simple Queue Service (SQS) queue.

Procedure

1. Use the following table to set the parameters for an Amazon AWS Verified Access log source that uses the Amazon AWS S3 REST API protocol and an SQS queue.

Table 228. Amazon AWS S3 REST API protocol log source parameters

Parameter	Description
Log Source Type	**AWS Verified Access**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one AWS Verified Access log source that is configured, you might want to identify the first log source as *awsverifiedaccess1*, the second log source as *awsverifiedaccess2*, and the third log source as *awsverifiedaccess3*.

Table 228. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you select **SQS Event Notifications** for the **S3 Collection Method**. The supported **S3 Collection Method** is **Use a Specific Prefix**. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata that is assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **LINEBYLINE**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **SQS Event Notifications**.
SQS Queue URL	Enter the full URL, starting with `https://`, of the SQS queue that is set up to receive notifications for ObjectCreate events from S3.
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Log Source Identifier Pattern	This option is available when you set **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.

Table 228. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Show Advanced Options	Select this option if you want to customize the event data.
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	How often a poll is made to scan for new data. If you are using the SQS event collection method, **SQS Event Notifications** can have a minimum value of 10 (seconds). Because SQS Queue polling can occur more often, a lower value can be used. If you are using the Directory Prefix event collection method, **Use a Specific Prefix** has a minimum value of 60 (seconds) or 1M. Because every listBucket request to an AWS S3 bucket incurs a cost to the account that owns the bucket, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the poll is made for new data. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15M = 15 minutes, 30 = seconds.

Table 228. Amazon AWS S3 REST API protocol log source parameters (continued)	
Parameter	**Description**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the AWS Config sample event messages.

Configuring an AWS Verified Access log source that uses an S3 bucket with a directory prefix

If you want to collect AWS Verified Access from a single account and region in an Amazon S3 bucket, configure a log source on the QRadar Console so AWS Verified Access can communicate with QRadar by using the Amazon AWS S3 REST API protocol with a directory prefix.

About this task

If you have log sources in an S3 bucket from multiple regions or that use multiple accounts, use the Amazon AWS REST API protocol with an SQS queue instead of with a directory prefix.

Restriction: A log source that uses directory prefix can retrieve data from only one region and one account, so use a different log source for each region and account. Include the region folder name in the file path for the **`Directory Prefix`** value when you configure the log source.

Procedure

1. Finding an S3 bucket name and directory prefix.
2. Create an Amazon AWS Identity and Access Management (IAM) user and then apply the **AmazonS3ReadOnlyAccess** policy.
3. Configure the security credentials for your AWS user account.
4. Add an AWS Verified Access log source on the QRadar Console using a directory prefix.

Finding an S3 bucket name and directory prefix

An Amazon administrator must create a user and then apply the **AmazonS3ReadOnlyAccess** policy in the AWS Management Console. The QRadar user can then create a log source in QRadar.

Note: Alternatively, you can assign more granular permissions to the bucket. The minimum required permissions are **s3:listBucket** and **s3:getObject**.

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Click **Services**.
2. From the list, select **Config**.
3. From the **Config** page, click the name of the Config.
4. Note the name of the S3 bucket that is displayed in the **S3 bucket** field.
5. Click the **Edit** icon.
6. Note the location path for the S3 bucket that is displayed underneath the **Log file prefix** field.

Creating an Identity and Access Management (IAM) user in the AWS Management Console

An Amazon administrator must create a user and then apply the **s3:listBucket** and **s3:getObject** permissions to that user in the AWS Management Console. The QRadar user can then create a log source in QRadar.

About this task

The minimum required permissions are **s3:listBucket** and **s3:getObject**. You can assign other permissions to the user as needed.

Sample policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>",
                "arn:aws:s3:::<bucket_name>/AWSLogs/<AWS_account_number>/<DSM_name>/us-east-1/*"
            ]
        }
    ]
}
```

For more information about permissions that are related to bucket operations, go to the AWS documentation website.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**.
3. From the list, select **IAM**.
4. Click **Users** > **Add user**.
5. Create an Amazon AWS IAM user and then apply the **AmazonS3ReadOnlyAccess** policy.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

Adding an AWS Verified Access log source on the QRadar Console using a directory prefix

If you want to collect AWS Verified Access logs from a single account and region in an Amazon S3 bucket, add a log source on the QRadar Console so that Amazon AWS Verified Access can communicate with QRadar by using the Amazon AWS S3 REST API protocol with a directory prefix.

Procedure

1. Use the following table to set the parameters for an Amazon AWS Verified Access log source that uses the Amazon AWS S3 REST API protocol and a directory prefix.

Table 229. Amazon AWS S3 REST API protocol log source parameters

Parameter	Description
Log Source Type	**AWS Verified Access**
Protocol Configuration	**Amazon AWS S3 REST API**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one AWS Verified Access log source that is configured, you might want to identify the first log source as *awsverifiedaccess1*, the second log source as *awsverifiedaccess2*, and the third log source as *awsverifiedaccess3*.
Authentication Method	**Access Key ID / Secret Key** Standard authentication that can be used from anywhere. For more information about configuring security credentials, see "Configuring security credentials for your AWS user account" on page 310. **Assume IAM Role** Authenticate with keys and then temporarily assume a role for access. This option is available only when you select **SQS Event Notifications** for the **S3 Collection Method**. The supported **S3 Collection Method** is **Use a Specific Prefix**. For more information about creating IAM users and assigning roles, see Creating an IAM user in the AWS Management Console. **EC2 Instance IAM Role** If your managed host is running on an AWS EC2 instance, choosing this option uses the IAM Role from the instance metadata assigned to the instance for authentication; no keys are required. This method works only for managed hosts that are running within an AWS EC2 container.
Access Key ID	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Access Key ID** parameter is displayed. The **Access Key ID** that was generated when you configured the security credentials for your AWS user account. This value is also the **Access Key ID** that is used to access the AWS S3 bucket.

Table 229. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
Secret Key	If you selected **Access Key ID / Secret Key** for the **Authentication Method**, the **Secret Key ID** parameter is displayed. The **Secret Key** that was generated when you configured the security credentials for your AWS user account. This value is also the **Secret Key ID** that is used to access the AWS S3 bucket.
Event Format	Select **LINEBYLINE**. The log source retrieves JSON formatted events.
S3 Collection Method	Select **Use a Specific Prefix**.
Bucket Name	The name of the AWS S3 bucket where the log files are stored.
Directory Prefix	The root directory location on the AWS S3 bucket from where the AWS Verified Access logs are retrieved; for example, `AWSLogs/<AccountNumber>/VerifiedAccess/<RegionName>/` To pull files from the root directory of a bucket, you must use a forward slash (/) in the **Directory Prefix** file path. **Note:** • Changing the **Directory Prefix** value clears the persisted file marker. All files that match the new prefix are downloaded in the next pull. • The **Directory Prefix** file path cannot begin with a forward slash (/) unless only the forward slash is used to collect data from the root of the bucket. • If the **Directory Prefix** file path is used to specify folders, you must not begin the file path with a forward slash (for example, use `folder1/folder2` instead).
Region Name	The region that the SQS Queue or the S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.
Log Source Identifier Pattern	This option is available when you set **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.
Show Advanced Options	Select this option if you want to customize the event data.

Table 229. Amazon AWS S3 REST API protocol log source parameters (continued)

Parameter	Description
File Pattern	This option is available when you set **Show Advanced Options** to Yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.json\.gz`
Local Directory	This option is available when you set **Show Advanced Options** to Yes. The local directory on the Target Event Collector. The directory must exist before the AWS S3 REST API PROTOCOL attempts to retrieve events.
S3 Endpoint URL	This option is available when you set **Show Advanced Options** to Yes. The endpoint URL that is used to query the AWS REST API. If your endpoint URL is different from the default, type your endpoint URL. The default is http://s3.amazonaws.com
Use S3 Path-Style Access	Forces S3 requests to use path-style access. This method is deprecated by AWS. However, it might be required when you use other S3 compatible APIs. For example, the `https://s3.region.amazonaws.com/bucket-name/key-name` path-style is automatically used when a bucket name contains a period (.). Therefore, this option is not required, but can be used.
Use Proxy	If QRadar accesses the Amazon Web Service by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
Recurrence	How often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieves them. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost. Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 1 minute. The time interval can include values in hours (H), minutes (M), or days (D). For example, 2H = 2 hours, 15 M = 15 minutes.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

2. To verify that QRadar is configured correctly, review the AWS Verified Access sample event messages.

AWS Verified Access sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

AWS Verified Access sample messages when you use the Amazon REST API protocol

Sample 1: The following sample event message shows that access to an application is granted.


```
2023-02-16T20: 43: 03.713Z{"activity":"Access
Granted","activity_id":"1","category_name":"Application
Activity","category_uid":"8","class_name":"Access Logs","class_uid":"208001","device":
{"ip":"10.0.0.1","os":{"name":"Windows
11","type":"Windows","type_id":100},"type":"Unknown","type_id":0,"uid":"99c111111111740d3a2222222f4ba65a","hw_info":
{"serial_number":"ec211111b-2222-3333-438b-52fd84444f05"}},"duration":"0.185","end_time":"1676046036224","time":"1676046036224","http_request":{"http_method":"GET","url":
{"hostname":"test.exmple.com","path":"/","port":443,"scheme":"h2","text":"https://
test.example.com:443/"},"user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36","version":"HTTP/
2.0"},"http_response":{"code":200},"identity":{"authorizations":[{"decision":"Allow","policy":
{"name":"inline"}},{"decision":"Allow","policy":{"name":"inline"}}],"idp":
{"name":"idc","uid":"vatp-03870111111e9779af"},"user":
{"email_addr":"test@example.com","name":"testuser","uid":"281111e0-2222-33333-a99e-
e59444037876"}},"message":"","metadata":
{"uid":"Root=1-6311111d4-57b0b8e7722222226c26acae","logged_time":1676046491347,"version":"","product":{"name":"Verified
Access","version":"0.1","vendor_name":"AWS"}},"ref_time":"2023-02-10T16:20:36.224567Z","proxy":
{"ip":"10.0.0.2","port":443,"svc_name":"Verified
Access","uid":"vai-01a31111151959c75"},"severity":"Informational","severity_id":"1","src_endpoint":
{"ip":"10.0.0.1","port":49339},"start_time":"1676046036039","status_code":"100","status_details":"Access
Granted","status_id":"1","status":"Success","type_uid":"20800101","type_name":"AccessLogs:
Access Granted","unmapped":null}
```


Table 230. Highlighted values in the AWS Verified Access sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Access Granted**
Event Category	In QRadar, the value is **AWSVerifiedAccess**
Timestamp	**1676046036224**
Src IP	**10.0.0.1**
Src Port	**49339**
Username	**testuser**

Sample 2: The following sample event message shows that access to an application is denied.


```
2023-02-16T20: 43: 03.713Z{"activity":"Access
Denied","activity_id":"2","category_name":"Application
Activity","category_uid":"8","class_name":"Access
Logs","class_uid":"208001","device":null,"duration":"0.001","end_time":"1676241408699","time":"1676241408699","http_request":{"http_method":"GET","url":
{"hostname":"test.example.com","path":"/","port":443,"scheme":"https","text":"https://
test.example.com:443/"},"user_agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36","version":"HTTP/
1.1"},"http_response":{"code":400},"identity":null,"message":"","metadata":
{"uid":"Root=1-11111111-7b1b7c702222236d4d63390b","logged_time":1676241792675,"version":"","product":{"name":"Verified
Access","version":"0.1","vendor_name":"AWS"}},"ref_time":"2023-02-12T22:36:48.699777Z","proxy":
{"ip":"10.0.0.2","port":443,"svc_name":"Verified
```

```
Access","uid":"vai-01a32222251959c75"},"severity":"Informational","severity_id":"1","src_endpoin
t":
{"ip":"10.0.0.1","port":53511},"start_time":"1676241408698","status_code":"200","status_details"
:"Authentication
Denied","status_id":"2","status":"Failure","type_uid":"20800102","type_name":"AccessLogs:
Access Denied","unmapped":null}
```


Table 231. Highlighted values in the AWS Verified Access sample event

QRadar field name	Highlighted values in the event payload
Event ID	**Authentication Denied**
Event Category	In QRadar, the value is **AWSVerifiedAccess**
Timestamp	**1676241408699**
Src Port	**53511**

Chapter 17. Ambiron TrustWave ipAngel

The IBM QRadar DSM for Ambiron TrustWave ipAngel receives Snort-based events from the ipAngel console.

The following table identifies the specifications for the Ambiron TrustWave ipAngel DSM:

Table 232. Ambiron TrustWave ipAngel DSM specifications

Specification	**Value**
Manufacturer	Ambiron
DSM name	Ambiron TrustWave ipAngel
RPM file name	`DSM-AmbironTrustwaveIpAngel-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V4.0
Protocol	Syslog
Recorded event types	Snort-based events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Ambiron website (http://www.apache.org)

To send Ambiron TrustWave ipAngel events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Ambiron TrustWave ipAngel DSM RPM from the IBM Support Website onto your QRadar Console.
2. Configure your Ambiron TrustWave ipAngel device to forward your cache and access logs to QRadar. For information on forwarding device logs to QRadar, see your vendor documentation.
3. Add an Ambiron TrustWave ipAngel log source on the QRadar Console. The following table describes the parameters that require specific values that are required for Ambiron TrustWave ipAngel event collection:

Table 233. Ambiron TrustWave ipAngel log source parameters

Parameter	**Value**
Log Source type	Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)
Protocol Configuration	Syslog

Chapter 18. APC UPS

The IBM QRadar DSM for APC UPS accepts syslog events from the APC Smart-Uninterruptible Power Supply (UPS) family of products.

Restriction: Events from RC-Series Smart-UPS are not supported.

The following table identifies the specifications for the APC UPS DSM:

Table 234. APC UPS DSM specifications

Specification	**Value**
Manufacturer	APC
DSM name	APC UPS
RPM file name	DSM-APCUPS-*Qradar_version-build_number*.noarch.rpm
Protocol	Syslog
Recorded event types	UPS events Battery events Bypass events Communication events Input power events Low battery condition events SmartBoost events SmartTrim events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	APC website (http://www.apc.com)

To send APC UPS events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the APC UPS DSM RPM from the IBM Support Website onto your QRadar Console.
2. Create an APC UPS log source on the QRadar Console and use the following table to configure the specific values that are required to collect APC UPS events:

   Table 235. APC UPS log source parameters

Parameter	**Value**
Log Source type	APC UPS
Protocol Configuration	Syslog

3. Configure your APC UPS device to forward syslog events to QRadar.

Related tasks

Adding a DSM

Adding a log source

Configuring your APC UPS to forward syslog events
To collect events from your APC UPS, you must configure the device to forward syslog events to IBM QRadar.

Configuring your APC UPS to forward syslog events

To collect events from your APC UPS, you must configure the device to forward syslog events to IBM QRadar.

Procedure

1. Log in to the APC Smart-UPS web interface.
2. In the navigation menu, click **Network > Syslog**.
3. From the **Syslog** list, select **Enable**.
4. From the **Facility** list, select a facility level for your syslog messages.
5. In the **Syslog Server** field, type the IP address of your QRadar Console or Event Collector.
6. From the **Severity** list, select **Informational**.
7. Click **Apply**.

APC UPS sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

APC UPS sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that a site wiring fault exists.

```
<10>Jan 10 15:25:44 apc.ups.test UPS: A site wiring fault exists. 0x0235
```


```
<10>Jan 10 15:25:44 apc.ups.test UPS: A site wiring fault exists. 0x0235
```


Table 236. Highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	A site wiring fault exists

Sample 2: The following sample event message shows that the local network management interface to UPS communication is restored.

```
<14>Jan 11 12:45:12 apc.ups.test UPS: Restored the local network management interface-to-UPS communication. 0x0101
```


```
<14>Jan 11 12:45:12 apc.ups.test UPS: Restored the local network management interface-to-UPS communication. 0x0101
```


Table 237. Highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	Restored the local network management interface-to-UPS communication

Chapter 19. Apache HTTP Server

The IBM QRadar DSM for Apache HTTP Server accepts Apache events by using syslog or syslog-ng.

QRadar records all relevant HTTP status events. The following procedure applies to Apache DSMs operating on UNIX/Linux operating systems only.

Do not run both syslog and syslog-ng at the same time.

Select one of the following configuration methods:

- "Configuring Apache HTTP Server with syslog" on page 469
- "Configuring Apache HTTP Server with syslog-ng" on page 470

Configuring Apache HTTP Server with syslog

You can configure your Apache HTTP Server to forward events with the syslog protocol.

About this task

The following procedure applies to Apache DSMs operating on most UNIX or Linux operating systems. Check your vendor's documentation for more information about configuring the server.

Procedure

1. Log in to the server that hosts Apache, as the root user.
2. Edit the Apache configuration file `httpd.conf`.
3. Add the following information in the Apache configuration file to specify the custom log format:

   ```
   LogFormat "%h %A %l %u %t \"%r\" %>s %p %b" <log format name>
   ```

   Where <*log format name*> is a variable name you provide to define the log format.
4. Add the following information in the Apache configuration file to specify a custom path for the syslog events:

   ```
   CustomLog "|/usr/bin/logger -t httpd -p <facility>.<priority>" <log format name>
   ```

   Where:

   - <*facility*> is a syslog facility, for example, local0.
   - <*priority*> is a syslog priority, for example, info or notice.
   - <*log format name*> is a variable name that you provide to define the custom log format. The log format name must match the log format name that is defined in Step 3.

   For example,

   ```
   CustomLog "|/usr/bin/logger -t httpd -p local1.info" MyApacheLogs
   ```
5. Type the following command to disable *hostname* lookup:

   ```
   HostnameLookups off
   ```
6. Save the Apache configuration file.
7. Edit the syslog configuration file.

   ```
   /etc/syslog.conf
   ```
8. Add the following information to your syslog configuration file:

   ```
   <facility>.<priority> <TAB><TAB>@<host>
   ```

   Where:

- <*facility*> is the syslog facility, for example, local0. This value must match the value that you typed in Step 4.
- <*priority*> is the syslog priority, for example, info or notice. This value must match the value that you typed in Step 4.
- <TAB> indicates you must press the **Tab** key.
- <*host*> is the IP address of the QRadar Console or Event Collector.

9. Save the syslog configuration file.
10. Type the following command to restart the syslog service:

    ```
    /etc/init.d/syslog restart
    ```

11. Restart Apache to complete the syslog configuration.

    The configuration is complete. The log source is added to QRadar as syslog events from Apache HTTP Servers are automatically discovered. Events that are forwarded to QRadar by Apache HTTP Servers are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Apache HTTP Server

If QRadar does not automatically detect the log source, add an Apache HTTP Server log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Apache HTTP Server:

Table 238. Syslog log source parameters for the Apache HTTP Server DSM

Parameter	Value
Log Source name	Type the name of your log source.
Log Source description	Type a description for your log source.
Log Source type	**Apache HTTP Server**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Apache installations.

Related tasks

"Adding a log source" on page 5

Configuring Apache HTTP Server with syslog-ng

You can configure your Apache HTTP Server to forward events with the syslog-ng protocol.

Procedure

1. Log in to the server that hosts Apache, as the root user.
2. Edit the Apache configuration file.

   ```
   /etc/httpd/conf/httpd.conf
   ```

3. Add the following information to the Apache configuration file to specify the **LogLevel**:

   ```
   LogLevel info
   ```

   The **LogLevel** might already be configured to the info level; it depends on your Apache installation.
4. Add the following to the Apache configuration file to specify the custom log format:

```
LogFormat "%h %A %l %u %t \"%r\" %>s %p %b" <log format name>
```

Where <*log format name*> is a variable name you provide to define the custom log format.

5. Add the following information to the Apache configuration file to specify a custom path for the syslog events:

```
CustomLog "|/usr/bin/logger -t 'httpd' -u /var/log/httpd/apache_log.socket"
<log format name>
```

The log format name must match the log format name that is defined in Step 4.

6. Save the Apache configuration file.
7. Edit the syslog-ng configuration file.

```
/etc/syslog-ng/syslog-ng.conf
```

8. Add the following information to specify the destination in the syslog-ng configuration file:

```
source s_apache {
              unix-stream("/var/log/httpd/apache_log.socket"
              max-connections(512)
              keep-alive(yes));
};
destination auth_destination { <udp|tcp> ("<IP address>" port(514)); };
log{
    source(s_apache);
    destination(auth_destination);
};
```

Where:

<*IP address*> is the IP address of the QRadar Console or Event Collector.

<*udp|tcp*> is the protocol that you select to forward the syslog event.

9. Save the syslog-ng configuration file.
10. Type the following command to restart syslog-ng:

```
service syslog-ng restart
```

11. You can now configure the log source in QRadar.

The configuration is complete. The log source is added to QRadar as syslog events from Apache HTTP Servers are automatically discovered. Events that are forwarded to QRadar by Apache HTTP Servers are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Apache HTTP Server

If QRadar does not automatically detect the log source, add an Apache HTTP Server log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Apache HTTP Server:

Table 239. Syslog log source parameters for the Apache HTTP Server DSM

Parameter	Value
Log Source name	Type the name of your log source.
Log Source description	Type a description for your log source.
Log Source type	**Apache HTTP Server**
Protocol Configuration	**Syslog**

Table 239. Syslog log source parameters for the Apache HTTP Server DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Apache installations.

Related tasks

"Adding a log source" on page 5

Apache HTTP Server sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Apache HTTP Server sample messages when you use the Syslog protocol

Sample 1: The following sample event is generated when a user is authenticated.

```
<86>Jun 28 06:00:19 apache.httpserver.test sshd[11148]: pam_vas: Authentication <succeeded>
for <Active Directory> user: <svc_unix> account: <DOMAINNAME\svc_unix_secscan> service: <sshd>
reason: <>
```


```
<86>Jun 28 06:00:19 apache.httpserver.test sshd[11148]: pam_vas: Authentication <succeeded>
for <Active Directory> user: <svc_unix> account: <DOMAINNAME\svc_unix_secscan> service: <sshd>
reason: <>
```


Table 240. Highlighted values in the Apache HTTP Server event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Authentication user** (extracted from the event content)
Event Category	**sshd**
Username	**svc_unix**

Sample 2: The following sample event message shows that an HTTP 403 system status occurred.

```
Oct 21 10:05:35 apache.httpserver.test httpd: 10.100.100.101 172.16.210.237 - - [26/Jan/
2006:12:24:54 +0000] "HEAD / HTTP/1.0" 403 123 "-" "-"
```


```
Oct 21 10:05:35 apache.httpserver.test httpd: 10.100.100.101 172.16.210.237 - - [26/Jan/
2006:12:24:54 +0000] "HEAD / HTTP/1.0" 403 123 "-" "-"
```


Table 241. Highlighted values in the Apache HTTP Server event	
QRadar field name	**Highlighted values in Apache event**
Event ID	**403**
Event Category	apache (extracted from the event content)
Source IP	**10.100.100.101**
Destination IP	**172.16.210.237**

Chapter 20. Apple Mac OS X

The IBM QRadar DSM for Apple Mac OS X accepts events by using syslog.

QRadar records all relevant firewall, web server access, web server error, privilege escalation, and informational events.

To integrate Apple Mac OS X events with QRadar, you must manually create a log source to receive syslog events.

To complete this integration, you must configure a log source, then configure your Apple Mac OS X to forward syslog events. Syslog events that are forwarded from Apple Mac OS X devices are not automatically discovered. Syslog events from Apple Mac OS X can be forwarded to QRadar on TCP port 514 or UDP port 514.

Apple Mac OS X DSM specifications

Understanding the specifications for the Apple Mac OS X DSM helps to ensure a successful integration. For example, knowing what the supported version of Apple Mac OS X is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Apple Mac OS X DSM.

Table 242. Apple Mac OS X DSM specifications

Specification	**Value**
Manufacturer	Apple
DSM name	Apple Mac OS X
RPM file name	DSM-*AppleOSX-QRadar_version-build_number*.noarch.rpm
Supported version	10.12
Protocol	Syslog
Recorded event types	Firewall, web server access, web server error, privilege, and informational events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No

Syslog log source parameters for Apple Mac OS X

If QRadar does not automatically detect the log source, add an Apple Mac OS X log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Apple Mac OS X:

Table 243. Syslog log source parameters for the Apple Mac OS X DSM

Parameter	**Value**
Log Source name	A name of your log source.

Table 243. Syslog log source parameters for the Apple Mac OS X DSM (continued)	
Parameter	**Value**
Log Source description	A description for your log source.
Log Source type	**Mac OS X**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Apple Mac OS X device.

Related tasks

"Adding a log source" on page 5

Configuring syslog on your Apple Mac OS X

Configure syslog on systems that run Apple Mac OS X operating systems by using a log stream script to send the MAC system logs to QRadar.

Procedure

1. To implement the 7.3-QRADAR-QRSCRIPT-logStream-1.0 fix, download the following files from IBM Fix Central. (https://www-945.ibm.com/support/fixcentral/swg/downloadFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=Linux&function=fixId&fixids=7.3-QRADAR-QRSCRIPT-logStream-1.0&includeRequisites=1&includeSupersedes=0&downloadMethod=http)
   - logStream.pl.tar.gz (2.88 KB)
   - 7.3-QRADAR-QRSCRIPT-logStream.sha256 (41 bytes)
2. From the terminal, go to the folder that you chose to contain the `logStream.pl` file that you extracted.
3. To make the `logStream.pl` file an executable file, type the following command:

   ```
   chmod +x logStream.pl
   ```

4. Create an executable shell script with an `.sh` extension with the following naming convention:

   <FILE_NAME>`.sh`
5. Add the following command to the file that you created:

   ```
   #!/bin/sh /Users/<PathToPerlScript>/logStream.pl -<Parameters1> <Value1> -<Parameters2>
   <Value2>
   ```

   The path is an absolute path that usually starts from `/Users/...`.

   You can use the following parameters for `logStream.pl`:

Table 244. `logStream.pl` parameters	
Parameter	**Description**
-H	The **-H** parameter defines the host name or IP to send the logs to.
-p	The **-p** parameter defines the port on the remote host, where a syslog receiver is listening. If this parameter is not specified, by default the `logStream.pl` script uses the TCP port 514 for sending events to QRadar.

Table 244. `logStream.pl` parameters (continued)	
Parameter	**Description**
-0	The **-0** parameter overrides the automatic host name from the OS's `/bin/hostname` command.
-s	The syslog header format default is 5424 (RFC5424 time stamp), but 3339 can be specified instead to output the time stamp in RFC3339 format.
-u	The **-u** parameter forces logStream to send events by using UDP.
-v	The **-v** parameter displays the version information for the logStream.
-x	The **-x** parameter is an exclusion filter in grep extended Regex format. For example: `parentalcontrolsd|com.apple.Webkit.WebContent`

Example:

```
#!/bin/sh /Users/……/logStream.pl -H 172.16.70.135
```

6. Save your changes.
7. From the terminal, go to the folder that contains the shell file that you created.
8. To make the perl file an executable file, type the following command:

```
chmod +x <FILE_NAME>.sh
```

9. In the terminal, create a file with a `.plist` file extension as in the following example:

   <fileName>`.plist`.
10. Add the following XML command to the file:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
   <dict>
      <key>Label</key>
      <string>com.logSource.app</string>
      <key>Program</key>
      <string>/Users/…[Path_to_Shell_Script_Created_In_Step2]/[FILE_NAME].sh</string>
      <key>RunAtLoad</key>
      <true />
   </dict>
</plist>
```

The XML command holds data in key-value pair. The following table provides the key-value pairs:

Table 245. Key-value pairs	
Key	**Value**
Label	`com.logSource.app`
Program	`/Users/…[`*`Path_To_Shell_Script_Created_In Step2`*`]…/`*`[FILE_NAME]`*`.sh`
RunAtLoad	True

Note:

The value of the **Label** key must be unique for each `.plist` file. For example, if you use the **Label** value `com.logSource.app` for one `.plist` file, you can't use the same value for another `.plist` file.

The Program key holds the path of the shell script that you want to run. The path is an absolute path that usually starts from `/Users/...`.

The **RunAtLoad** key shows events when you want to run your shell program automatically.

11. Save your changes.
12. To make the `.plist` file an executable file, type the following command:

```
chmod +x <FILE_NAME>.plist
```

13. Copy the file to `/Library/LaunchDaemons/` by using the following command:

```
sudo cp <Path_To_Your_plist_file> /Library/LaunchDaemons/
```

14. Restart your Mac system.
15. Log in to QRadar, and then from the **Log Activity** tab, verify that events are arriving from the Apple Mac system. If events are arriving as Sim Generic, you must manually configure a log source for the Apple Mac system.

Example: Consider the following event:

```
<13>1 2020-06-25T16:06:55.198987-0300 AAAA-MacBook-Pro.local trustd[130]:
[com.apple.securityd.policy] cert[2]: AnchorTrusted =(leaf)[force]> 0
```

The log source parameter values for that event are:

Table 246. Log source parameters

Parameter	Value
Log Source Type	Apple Mac OS X
Protocol Configuration	Syslog
Log Source Identifier	*AAAA-MacBook-Pro*.local

Apple Mac OS X sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Apple Mac OS X sample message when you use the Syslog protocol

The following sample event message shows an invalid user.

May 1 10:33:35 apple.macosx.test sshd[8565]: **Invalid user testUser** from **192.168.0.1**

```
May  1 10:33:35 apple.macosx.test sshd[8565]: Invalid user testUser from 192.168.0.1
```

Table 247. Highlighted values in the Apple Mac OS X sample event

QRadar field name	Highlighted payload field name
Event ID	**Invalid user** is extracted from the event.
Username	**testUser** is extracted from the event.
Source IP	**192.168.0.1** is extracted from the event.
Device Time	**May 1 10:33:35** is extracted from the event header.

Chapter 21. Application Security DbProtect

The IBM QRadar DSM for Application Security DbProtect collects event from DbProtect devices that are installed with the Log Event Extended Format (LEEF) Service.

The following table identifies the specifications for the Application Security DbProtect DSM:

Table 248. Application Security DbProtect DSM specifications

Specification	**Value**
Manufacturer	Application Security, Inc
DSM name	DbProtect
RPM file name	`DSM-AppSecDbProtect-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	v6.2 v6.3 v6.3sp1 v6.3.1 v6.4
Protocol	LEEF
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Application Security website (http://www.appsecinc.com/)

To send Application Security DbProtect events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Application Security DbProtect DSM RPM from the IBM Support Website onto your QRadar Console.
2. Configure your Application Security DbProtect device to communicate with QRadar. Complete the following steps:
   a. Install the DbProtect LEEF Relay Module.
   b. Configure the DbProtect LEEF Relay
   c. Configure DbProtect alerts.
3. If QRadar does not automatically detect the log source, add an Application Security DbProtect log source on the QRadar Console. Configure all required parameters, and use the following table for DbProtect-specific values:

Table 249. Application Security DbProtect log source parameters

Parameter	**Value**
Log Source type	Application Security DbProtect
Protocol Configuration	Syslog

Installing the DbProtect LEEF Relay Module

To enable DbProtect to communicate with IBM QRadar, install the DbProtect LEEF Relay module on the same server as the DbProtect console.

Before you begin

Before you install the DbProtect LEEF Relay module on a Windows 2003 host, you must install Windows Imaging Components. The `wic_x86.exe` file contains the Windows Imaging Components and is on the Windows Server Installation CD. For more information, see your Windows 2003 Operating System documentation.

About this task

The LEEF Relay module for DbProtect translates the default events messages to Log Event Extended Format (LEEF) messages for QRadar. Before you can receive events in QRadar, you must install and configure the LEEF Service for your DbProtect device to forward syslog events. The DbProtect LEEF Relay requires that you install the .NET 4.0 Framework, which is bundled with the LEEF Relay installation.

Procedure

1. Download the DbProtect LEEF Relay module for DbProtect from the Application Security, Inc. customer portal (http://www.appsecinc.com).
2. Save the setup file to the same host as your DbProtect console.
3. Click **Accept** to agree with the Microsoft .NET Framework 4 End-User License Agreement.
4. In the **DbProtect LEEF Relay module installation Wizard**, click **Next**.
5. To select the default installation path, click **Next**.

   If you change the default installation directory, make note of the file location.
6. On the **Confirm Installation** window, click **Next**.
7. Click **Close**.

What to do next

"Configuring the DbProtect LEEF Relay" on page 478

Configuring the DbProtect LEEF Relay

After you install the DbProtect LEEF Relay module, configure the service to forward events to IBM QRadar.

Before you begin

Stop the DbProtect LEEF Relay service before you edit any configuration values.

Procedure

1. Log in to the DbProtect LEEF Relay server.
2. Access the `C:\Program Files (x86)\AppSecInc\AppSecLEEFConverter` directory.
3. Edit the `AppSecLEEFConverter.exe.config` file. Configure the following values:

Parameter	Description
SyslogListenerPort	The port number that the DbProtect LEEF Relay uses to listen for syslog messages from the DbProtect console.
SyslogDestinationHost	The IP address of your QRadar Console or Event Collector.
SyslogDestinationPort	514

Parameter	Description
LogFileName	A file name for the DbProtect LEEF Relay to write debug and log messages. The LocalSystem user account that runs the DbProtect LEEF Relay service must have write privileges to the file path that you specify.

4. Save the configuration changes to the file.
5. On the desktop of the DbProtect console, select **Start** > **Run**.
6. Type the following command:

   ```
   services.msc
   ```

7. Click **OK**.
8. In the details pane of the **Services** window, verify the **DbProtect LEEF Relay** is started and set to **automatic startup**.
9. To change a service property, right-click the service name, and then click **Properties**.
10. Using the **Startup type** list, select **Automatic**.
11. If the **DbProtect LEEF Relay** is not started, click **Start**.

What to do next

"Configuring DbProtect alerts" on page 479

Configuring DbProtect alerts

Configure sensors on your DbProtect console to generate alerts.

Procedure

1. Log in to the DbProtect console.
2. Click the **Activity Monitoring** tab.
3. Click the **Sensors** tab.
4. Select a sensor and click **Reconfigure**.
5. Select a database instance and click **Reconfigure**.
6. Click **Next** until the **Sensor Manager Policy** window is displayed.
7. Select the **Syslog** check box and click **Next**.
8. In the **Send Alerts to the following Syslog console** field, type the IP address of your DbProtect console.
9. In the **Port** field, type the port number that you configured in the **SyslogListenerPort** field of the DbProtect LEEF Relay.

   Tip: By default, 514 is the default Syslog listen port for the DbProtect LEEF Relay.
10. Click **Add**.
11. Click **Next** until you reach the **Deploy to Sensor** window.
12. Click **Deploy to Sensor**.

Chapter 22. Arbor Networks

Several Arbor Networks devices can be integrated with IBM QRadar.

This section provides information on the following DSMs:

- "Arbor Networks Peakflow SP" on page 481
- "Arbor Networks Pravail" on page 484

Arbor Networks Peakflow SP

IBM QRadar can collect and categorize syslog and TLS syslog events from Arbor Networks Peakflow SP appliances that are in your network.

Arbor Networks Peakflow SP appliances store the syslog events locally.

To collect local syslog events, you must configure your Peakflow SP appliance to forward the syslog events to a remote host. QRadar automatically discovers and creates log sources for syslog events that are forwarded from Arbor Networks Peakflow SP appliances. QRadar supports syslog events that are forwarded from Peakflow V5.8 to V8.1.2.

To configure Arbor Networks Peakflow SP, complete the following steps:

1. On your Peakflow SP appliance, create a notification group for QRadar.
2. On your Peakflow SP appliance, configure the global notification settings.
3. On your Peakflow SP appliance, configure your alert notification rules.
4. If automatic updates are not enabled for QRadar, RPMs are available for download from the IBM support website. Download and install the most recent version of the following RPMs on your QRadar Console.
   - DSMCommon RPM
   - Arbor Networks Peakflow SP DSM RPM
5. Configure your Arbor Networks Peakflow SP appliance to send syslog or TLS syslog events to QRadar.
6. If QRadar does not automatically detect the log source, add an Arbor Networks Peakflow SP log source on the QRadar Console. The following tables describe the parameters that require specific values to collect events from Arbor Networks Peakflow SP:

Table 250. Arbor Networks Peakflow SP log source parameters

Parameter	Value
Log Source type	Arbor Networks Peakflow SP
Protocol Configuration	Select **Syslog** or **TLS Syslog**
Log Source Identifier	Type a unique name for the log source.

Related concepts

"TLS Syslog protocol configuration options" on page 227
Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Supported event types for Arbor Networks Peakflow SP

The Arbor Networks Peakflow DSM for IBM QRadar collects events from several categories.

Each event category contains low-level events that describe the action that is taken within the event category. For example, authentication events can have low-level categories of `login successful` or `login failure`.

The following list defines the event categories that are collected by QRadar from Peakflow SP appliances:

- Denial of Service (DoS) events
- Authentication events
- Exploit events
- Suspicious activity events
- System events

Configuring a remote syslog in Arbor Networks Peakflow SP

To collect events, you must configure a new notification group or edit existing groups to add IBM QRadar as a remote syslog destination.

Procedure

1. Log in to your Peakflow SP configuration interface as an administrator.
2. In the navigation menu, select **Administration** > **Notification** > **Groups**.
3. Click **Add Notification Group**.
4. In the **Destinations** field, type the IP address of your QRadar system.
5. In the **Port** field, type 514 as the port for your syslog destination.
6. From the **Facility** list, select a syslog facility.
7. From the **Severity** list, select **info**.

   The informational severity collects all event messages at the informational event level and higher severity.
8. Click **Save**.
9. Click **Configuration Commit**.

Configuring global notifications settings for alerts in Arbor Networks Peakflow SP

Global notifications in Arbor Networks Peakflow SP provide system notifications that are not associated with rules.

About this task

This procedure defines how to add IBM QRadar as the default notification group and enable system notifications.

Procedure

1. Log in to the configuration interface for your Arbor Networks Peakflow SP appliance as an administrator.
2. In the navigation menu, select **Administration** > **Notification** > **Global Settings** .
3. In the **Default Notification Group** field, select the notification group that you created for QRadar syslog events.
4. Click **Save**.

5. Click **Configuration Commit** to apply the configuration changes.
6. Log in to the Arbor Networks Peakflow SP command-line interface as an administrator.
7. Type the following command to list the current alert configuration:

   ```
   services sp alerts system_errors show
   ```
8. Optional: Type the following command to list the fields names that can be configured:

   ```
   services sp alerts system_errors ?
   ```
9. Type the following command to enable a notification for a system alert:

   `services sp alerts system_errors` <*name*> `notifications enable`

   Where <*name*> is the field name of the notification.
10. Type the following command to commit the configuration changes:

    ```
    config write
    ```

Configuring alert notification rules in Arbor Networks Peakflow SP

To generate events, you must edit or add rules to use the notification group that IBM QRadar uses as a remote syslog destination.

Procedure

1. Log in to your Arbor Networks Peakflow SP configuration interface as an administrator.
2. In the navigation menu, select **Administration** > **Notification** > **Rules**.
3. Select one of the following options:
   - Click a current rule to edit the rule.
   - Click **Add Rule** to create a new notification rule.
4. Configure the following values:

Table 251. Arbor Networks Peakflow SP notification rule parameters

Parameter	Description
Name	Type the IP address or host name as an identifier for events from your Peakflow SP installation. The log source identifier must be a unique value.
Resource	Type a CIDR address or select a managed object from the list of Peakflow resources.
Importance	Select the **Importance** of the rule.
Notification Group	Select the **Notification Group** that you assigned to forward syslog events to QRadar.

5. Repeat these steps to configure any other rules that you want to create.
6. Click **Save**.
7. Click **Configuration Commit** to apply the configuration changes.

   QRadar automatically discovers and creates a log source for Arbor Networks Peakflow SP appliances. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.

Syslog log source parameters for Arbor Networks Peakflow SP

If QRadar does not automatically detect the log source, add an Arbor Networks Peakflow SP log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Arbor Networks Peakflow SP:

Table 252. Syslog log source parameters for the Arbor Networks Peakflow SP DSM

Parameter	Value
Log Source name	The name of your log source.
Log Source description	Type a description for your log source.
Log Source type	**Arbor Networks Peakflow**
Protocol Configuration	**Syslog**
Log Source Identifier	The IP address or host name is used as an identifier for events from your Peakflow SP installation. The log source identifier must be a unique value.
Credibility	The credibility of the log source. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event.
Target Event Collector	The event collector to use as the target for the log source.
Coalescing Events	Enables the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	The incoming payload encoder for parsing and storing the logs.
Store Event Payload	Enables the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related tasks

"Adding a log source" on page 5

Arbor Networks Pravail

The IBM QRadar DSM for Arbor Networks Pravail receives event logs from your Arbor Networks Pravail servers.

The following table identifies the specifications for the Arbor Networks Pravail DSM:

Table 253. Arbor Networks Pravail DSM specifications	
Specification	**Value**
Manufacturer	Arbor Networks
DSM	Arbor Networks Pravail
RPM file name	`DSM-ArborNetworksPravail-`*`build_number`*`.noarch.rpm`
Protocol	Syslog
Recorded events	All relevant events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Arbor Networks website (www.arbornetworks.com)

To send Arbor Networks Pravail events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Arbor Networks Pravail RPM from the IBM Support Website onto your QRadar Console:
2. Configure each Arbor Networks Pravail system to send events to QRadar.
3. If QRadar does not automatically discover the Arbor Pravail system, create a log source on the QRadar Console. Configure the required parameters, and use the following table for the Arbor Pravail specific parameters:

Table 254. Arbor Pravail parameters	
Parameter	**Value**
Log Source Type	Arbor Networks Pravail
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring your Arbor Networks Pravail system to send events to IBM QRadar

To collect all audit logs and system events from Arbor Networks Pravail, you must add a destination that specifies QRadar as the syslog server.

Adding a log source

Configuring your Arbor Networks Pravail system to send events to IBM QRadar

To collect all audit logs and system events from Arbor Networks Pravail, you must add a destination that specifies QRadar as the syslog server.

Procedure

1. Log in to your Arbor Networks Pravail server.
2. Click **Settings & Reports**.
3. Click **Administration** > **Notifications**.
4. On the **Configure Notifications** page, click **Add Destinations.**
5. Select **Syslog**.
6. Configure the following parameters:

Table 255. Syslog parameters	
Parameter	**Description**
Host	The IP address of the QRadar Console
Port	514
Severity	Info
Alert Types	The alert types that you want to send to the QRadar Console

7. Click **Save**.

Arbor Networks Pravail sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Arbor Networks Pravail sample message when you use the Syslog protocol

The following sample event message shows that a malformed SIP traffic is blocked.

<25>**May 15 17:17:31** arbornetworks.pravail.test arbor-networks-aps: **Blocked Host**: Blocked host **192.168.124.175** at 05:16 by **Block Malformed SIP Traffic** using UDP/**5060** (SIP) destination **192.168.161.35** source port **5060**,URL: https://arbornetworks.pravail.test/summary/

<25>**May 15 17:17:31** arbornetworks.pravail.test arbor-networks-aps: **Blocked Host**: Blocked host **192.168.124.175** at 05:16 by **Block Malformed SIP Traffic** using UDP/**5060** (SIP) destination **192.168.161.35** source port **5060**,URL: https://arbornetworks.pravail.test/summary/

Table 256. Highlighted values in the Arbor Pravail sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Block Malformed SIP Traffic**
Event Category	**Blocked Host**
Source IP	**192.168.124.175**
Source Port	**5060**
Destination IP	**192.168.161.35**
Destination Port	**5060**
Device Time	**May 15 17:17:31**

Chapter 23. Arpeggio SIFT-IT

The IBM QRadar DSM for SIFT-IT accepts syslog events from Arpeggio SIFT-IT running on IBM i that are formatted as Log Event Extended Format (LEEF).

QRadar supports events from Arpeggio SIFT-IT 3.1 and later installed on IBM i version 5 revision 3 (V5R3) and later.

Arpeggio SIFT-IT supports syslog events from the journal QAUDJRN in LEEF format.

Example:

```
Jan 29 01:33:34 <Server> LEEF:1.0|Arpeggio|SIFT-IT|3.1|PW_U|sev=3
usrName=<Username> src=<Source_IP_address> srcPort=543 jJobNam=QBASE
jJobUsr=<Username> jJobNum=1664 jrmtIP=<SourceIP_address> jrmtPort=543
jSeqNo=4755 jPgm=QWTMCMNL jPgmLib=QSYS jMsgId=PWU0000 jType=U jUser=ROOT
jDev=QPADEV000F jMsgTxt=Invalid user id <Username>. Device <Device_ID>.
```

Events that SIFT-IT sends to QRadar are determined with a configuration rule set file. SIFT-IT includes a default configuration rule set file that you can edit to meet your security or auditing requirements. For more information about configuring rule set files, see your *SIFT-IT User Guide*.

Configuring a SIFT-IT agent

Arpeggio SIFT-IT can forward syslog events in LEEF format with SIFT-IT agents.

About this task

A SIFT-IT agent configuration defines the location of your IBM QRadar installation, the protocol and formatting of the event message, and the configuration rule set.

Procedure

1. Log in to your IBM i.
2. Type the following command and press Enter to add SIFT-IT to your library list:

   `ADDLIBLE SIFTITLIB0`
3. Type the following command and press Enter to access the SIFT-IT main menu:

   `GO SIFTIT`
4. From the main menu, select **1. Work with SIFT-IT Agent Definitions**.
5. Type 1 to add an agent definition for QRadar and press Enter.
6. In the **SIFT-IT Agent Name** field, type a name.

   For example, QRadar.
7. In the **Description** field, type a description for the agent.

   For example, `Arpeggio agent for` QRadar.
8. In the **Server host name or IP address** field, type the location of your QRadar Console or Event Collector.
9. In the **Connection type** field, type either *TCP, *UDP, or *SECURE.

   The *SECURE option requires the TLS protocol.
10. In the **Remote port number** field, type 514.

    By default, QRadar supports both TCP and UDP syslog messages on port 514.
11. In the **Message format options** field, type *QRadar.
12. Optional: Configure any additional parameters for attributes that are not QRadar specific.

The additional operational parameters are described in the *SIFT-IT User Guide*.

13. Press F3 to exit to the **Work with SIFT-IT Agents Description** menu.
14. Type 9 and press Enter to load a configuration rule set for QRadar.
15. In the **Configuration file** field, type the path to your QRadar configuration rule set file.

    Example:

    `/sifitit/Qradarconfig.txt`
16. Press F3 to exit to the **Work with SIFT-IT Agents Description** menu.
17. Type 11 to start the QRadar agent.

What to do next

Syslog events that are forwarded by Arpeggio SIFT-IT in LEEF format are automatically discovered by QRadar. In most cases, the log source is automatically created in QRadar after a few events are detected. If the event rate is low, you might be required to manually create a log source for Arpeggio SIFT-IT in QRadar.

Until the log source is automatically discovered and identified, the event type displays as Unknown on the **Log Activity** tab of QRadar.

Related concepts

"TLS Syslog protocol configuration options" on page 227

Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

Syslog log source parameters for Arpeggio SIFT-IT

If QRadar does not automatically detect the log source, add a Arpeggio SIFT-IT log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Arpeggio SIFT-IT:

Table 257. Syslog log source parameters for the Arpeggio SIFT-IT DSM

Parameter	Value
Log Source name	Type the name of your log source.
Log Source description	Type a description for your log source.
Log Source type	**Arpeggio SIFT-IT**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Arpeggio SIFT-IT installation.

Related tasks

"Adding a log source" on page 5

Additional information

After you create your IBM QRadar agent definition, you can use your Arpeggio SIFT-IT software and QRadar integration to customize your security and auditing requirements.

You can customize the following security and auditing requirements:

- Create custom configurations in Arpeggio SIFT-IT with granular filtering on event attributes.

For example, filtering on job name, user, file or object name, system objects, or ports. All events that are forwarded from SIFT-IT and the contents of the event payload in QRadar are easily searched.

- Configure rules in QRadar to generate alerts or offenses for your security team to identify potential security threats, data loss, or breaches in real time.
- Configuring processes in Arpeggio SIFT-IT to trigger real-time remediation of issues on your IBM i.
- Creating offenses for your security team from Arpeggio SIFT-IT events in QRadar with the **Offenses** tab or configuring email job logs in SIFT-IT for your IBM i administrators.
- Creating multiple configuration rule sets for multiple agents that run simultaneously to handle specific security or audit events.

For example, you can configure one QRadar agent with a specific rule set for forwarding all IBM i events, then develop multiple configuration rule sets for specific compliance purposes. You can easily manage configuration rule sets for compliance regulations, such as FISMA, PCI. HIPPA, SOX, or ISO 27001. All of the events that are forwarded by SIFT-IT QRadar agents are contained in a single log source and categorized to be easily searched.

Chapter 24. Array Networks SSL VPN

The IBM QRadar DSM for Array Networks SSL VPN collects events from an ArrayVPN appliance by using syslog.

QRadar records all relevant SSL VPN events that are forwarded by using syslog on TCP port 514 or UDP port 514.

Syslog log source parameters for Array Networks SSL VPN

If QRadar does not automatically detect the log source, add a Array Networks SSL VPN log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Array Networks SSL VPN:

Table 258. Syslog log source parameters for the Array Networks SSL VPN DSM

Parameter	Value
Log Source Name	Type the name of your log source.
Log Source Description	Type a description for your log source.
Log Source type	**Array Networks SSL VPN Access Gateways**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source.

Related tasks

"Adding a log source" on page 5

Chapter 25. Aruba Networks

Several Aruba devices can be integrated with IBM QRadar.

Aruba ClearPass Policy Manager

The IBM QRadar DSM for Aruba ClearPass Policy Manager can collect event logs from your Aruba ClearPass Policy Manager servers.

The following table identifies the specifications for the Aruba ClearPass Policy Manager DSM:

Table 259. Aruba ClearPass Policy Manager DSM specifications

Specification	**Value**
Manufacturer	Aruba Networks
DSM name	ClearPass
RPM file name	`DSM-ArubaClearPass-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	6.5.0.71095 to 6.11.1
Event format	LEEF
Recorded event types	Session Audit System Insight
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Aruba Networks website

To integrate Aruba ClearPass Policy Manager with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Aruba ClearPass DSM RPM
   - DSMCommon RPM
2. Configure your Aruba ClearPass Policy Manager device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an Aruba ClearPass log source on the QRadar Console. The following table describes the parameters that require specific values for Aruba ClearPass Policy Manager event collection:

Table 260. Aruba ClearPass Policy Manager log source parameters

Parameter	**Value**
Log Source type	Aruba ClearPass Policy Manager
Protocol Configuration	Syslog

Related tasks

"Adding a log source" on page 5

Configuring Aruba ClearPass Policy Manager to communicate with QRadar

To collect syslog events from Aruba ClearPass Policy Manager, you must add an external syslog server for the IBM QRadar host, then create one or more syslog filters for your syslog server.

About this task

For Session and Insight® events, full event parsing works only for the default fields that are provided by Aruba ClearPass Policy Manager. Session and Insight events that are created by a user, and have different combinations of fields, might appear as **Unknown Session Log**, or **Unknown Insight Log**.

The following table shows the field categories and their default fields that you can use:

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager

Export template	Predefined field groups	Default-selected columns
Insight Logs	Radius Authentications	Auth.Username Auth.Host-MAC-Address Auth.Protocol Auth.NAS-IP-Address CppmNode.CPPM-Node Auth.Login-Status Auth.Service Auth.Source Auth.Roles Auth.Enforcement-Profiles
Insight Logs	Radius Failed Authentications	Auth.Username Auth.Host-MAC-Address Auth.NAS-IP-Address CppmNode.CPPM-Node Auth.Service CppmErrorCode.Error-Code-Details CppmAlert.Alerts

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Insight Logs	RADIUS Accounting	Radius.Username Radius.Calling-Station-Id Radius.Framed-IP-Address Radius.NAS-IP-Address Radius.Start-Time Radius.End-Time Radius.Duration Radius.Input-bytes Radius.Output-bytes
Insight Logs	tacacs Authentication	tacacs.Username tacacs.Remote-Address tacacs.Request-Type tacacs.NAS-IP-Address tacacs.Service tacacs.Auth-Source tacacs.Roles tacacs.Enforcement-Profiles tacacs.Privilege-Level
Insight Logs	tacacs Failed Authentication	tacacs.Username tacacs.Remote-Address tacacs.Request-Type tacacs.NAS-IP-Address tacacs.Service CppmErrorCode.Error-Code-Details CppmAlert.Alerts

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Insight Logs	WEBAUTH	Auth.Username Auth.Host-MAC-Address Auth.Host-IP-Address Auth.Protocol Auth.System-Posture-Token CppmNode.CPPM-Node Auth.Login-Status Auth.Service Auth.Source Auth.Roles Auth.Enforcement-Profiles
Insight Logs	WEBAUTH Failed Authentications	Auth.Username Auth.Host-MAC-Address Auth.Host-IP-Address Auth.Protocol Auth.System-Posture-Token CppmNode.CPPM-Node Auth.Login-Status Auth.Service CppmErrorCode.Error-Code-Details CppmAlert.Alerts
Insight Logs	Application Authentication	Auth.Username Auth.Host-IP-Address Auth.Protocol CppmNode.CPPM-Node Auth.Login-Status Auth.Service Auth.Source Auth.Roles Auth.Enforcement-Profiles

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Insight Logs	Failed Application Authentication	Auth.Username Auth.Host-IP-Address Auth.Protocol CppmNode.CPPM-Node Auth.Login-Status Auth.Service CppmErrorCode.Error-Code-Details CppmAlert.Alerts
Insight Logs	Endpoints	Endpoint.MAC-Address Endpoint.MAC-Vendor Endpoint.IP-Address Endpoint.Username Endpoint.Device-Category Endpoint.Device-Family Endpoint.Device-Name Endpoint.Conflict Endpoint.Status Endpoint.Added-At Endpoint.Updated-At
Insight Logs	Clearpass Guest	Guest.Username Guest.MAC-Address Guest.Visitor-Name Guest.Visitor-Company Guest.Role-Name Guest.Enabled Guest.Created-At Guest.Starts-At Guest.Expires-At

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Insight Logs	Onboard Enrollment	OnboardEnrollment.Username OnboardEnrollment.Device-Name OnboardEnrollment.MAC-Address OnboardEnrollment.Device-Product OnboardEnrollment.Device-Version OnboardEnrollment.Added-At OnboardEnrollment.Updated-At
Insight Logs	Onboard Certificate	OnboardCert.Username OnboardCert.Mac-Address OnboardCert.Subject OnboardCert.Issuer OnboardCert.Valid-From OnboardCert.Valid-To OnboardCert.Revoked-At
Insight Logs	Onboard OCSP	OnboardOCSP.Remote-Address OnboardOCSP.Response-Status-Name OnboardOCSP.Timestamp
Insight Logs	Clearpass System Events	CppmNode.CPPM-Node CppmSystemEvent.Source CppmSystemEvent.Level CppmSystemEvent.Category CppmSystemEvent.Action CppmSystemEvent.Timestamp
Insight Logs	Clearpass Configuration Audit	CppmConfigAudit.Name CppmConfigAudit.Action CppmConfigAudit.Category CppmConfigAudit.Updated-By CppmConfigAudit.Updated-At

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Insight Logs	Posture Summary	Endpoint.MAC-Address Endpoint.IP-Address Endpoint.Hostname Endpoint.Usermame Endpoint.System-Agent-Type Endpoint.System-Agent-Version Endpoint.System-Client-OS Endpoint.System-Posture-Token Endpoint.Posture-Healthy Endpoint.Posture-Unhealthy
Insight Logs	Posture Firewall Summary	Endpoint.MAC-Address Endpoint.IP-Address Endpoint.Hostname Endpoint.Usermame Endpoint.System-Agent-Type Endpoint.System-Agent-Version Endpoint.System-Client-OS Endpoint.System-Posture-Token Endpoint.Firewall-APT Endpoint.Firewall-Input Endpoint.Firewall-Output
Insight Logs	Posture Antivirus Summary	Endpoint.MAC-Address Endpoint.IP-Address Endpoint.Hostname Endpoint.Usermame Endpoint.System-Agent-Type Endpoint.System-Agent-Version Endpoint.System-Client-OS Endpoint.System-Posture-Token Endpoint.Antivirus-APT Endpoint.Antivirus-Input Endpoint. Antivirus-Output

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Insight Logs	Posture Antispyware Summary	Endpoint.MAC-Address Endpoint.IP-Address Endpoint.Hostname Endpoint.Usermame Endpoint.System-Agent-Type Endpoint.System-Agent-Version Endpoint.System-Client-OS Endpoint.System-Posture-Token Endpoint.Antispyware-APT Endpoint.Antispyware-Input Endpoint.Antispyware-Output
Insight Logs	Posture DiskEncryption Summary	Endpoint.MAC-Address Endpoint.IP-Address Endpoint.Hostname Endpoint.Usermame Endpoint.System-Agent-Type Endpoint.System-Agent-Version Endpoint.System-Client-OS Endpoint.System-Posture-Token Endpoint.DiskEncryption-APT Endpoint.DiskEncryption-Input Endpoint.DiskEncryption-Output
Insight Logs	Posture Windows Hotfixes Summary	Endpoint.MAC-Address Endpoint.IP-Address Endpoint.Hostname Endpoint.Usermame Endpoint.System-Agent-Type Endpoint.System-Agent-Version Endpoint.System-Client-OS Endpoint.System-Posture-Token Endpoint.HotFixes-APT Endpoint.HotFixes-Input Endpoint.HotFixes-Output

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Session Logs	Logged in Users	Common.Username Common.Service Common.Roles Common.Host-MAC-Address RADIUS.Acct-Framed-IP-Address Common.NAS-IP-Address Common.Request-Timestamp
Session Logs	Failed Authentications	Common.Username Common.Service Common.Roles RADIUS.Auth-Source RADIUS.Auth-Method Common.System-Posture-Token Common.Enforcement-Profiles Common.Host-MAC-Address Common.NAS-IP-Address Common.Error-Code Common.Alerts Common.Request-Timestamp
Session Logs	RADIUS Accounting	RADIUS.Acct-Username RADIUS.Acct-NAS-IP-Address RADIUS.Acct-NAS-Port RADIUS.Acct-NAS-Port-Type RADIUS.Acct-Calling-Station-Id RADIUS.Acct-Framed-IP-Address RADIUS.Acct-Session-Id RADIUS.Acct-Session-Time RADIUS.Acct-Output-Pkts RADIUS.Acct-Input-Pkts RADIUS.Acct-Output-Octets RADIUS.Acct-Input.Octets RADIUS.Acct-Service-Name RADIUS.Acct-Timestamp

Table 261. Default categories and fields for Session and Insight events provided by Aruba ClearPass Policy Manager (continued)

Export template	Predefined field groups	Default-selected columns
Session Logs	tacacs+ Administration	Common.Username Common.Service tacacs.Remote-Address tacacs.Privilege.Level Common.Request-Timestamp
Session Logs	tacacs+ Accounting	Common.Username Common.Service tacacs.Remote-Address tacacs.Acct-Flags tacacs.Privilege.Level Common.Request-Timestamp
Session Logs	Web Authentication	Common.Username Common.Host-MAC-Address WEBAUTH.Host-IP-Address Common.Roles Common.System-Posture-Token Common.Enforcement-Profiles Common.Request-Timestamp
Session Logs	Guest Access	Common.Username RADIUS.Auth-Method Common.Host-MAC-Address Common.Roles Common.System-Posture-Token Common.Enforcement-Profiles Common.Request-Timestamp
Session Logs	Network Access	Common.Username Common.Service Common.Roles Common.NAS-IP-Address Common.Request-Timestamp

Procedure

1. Log in to your Aruba ClearPass Policy Manager server.
2. Start the Administration Console.

3. Click **External Servers** > **Syslog Targets**.
4. Click **Add**, and then configure the details for the QRadar host.
5. On the Administration Console, click **External Servers** > **Syslog Export Filters**
6. Click **Add**.
7. Select **LEEF** for the **Export Event Format Type**, and then select the **Syslog Server** that you added.
8. Click **Save**.

TCP Multiline Syslog log source parameters for Aruba ClearPass Policy Manager

The Aruba ClearPass Policy Manager DSM for IBM QRadar accepts Syslog events with log sources that are configured with the TCP Multiline Syslog protocol when the events are fragmented.

If QRadar does not automatically detect a log source, add the Aruba ClearPass Policy Manager log source on the QRadar Console by using the TCP Multiline Syslog protocol.

The following table describes the parameters that require specific values to collect TCP Multiline Syslog events from Aruba ClearPass Policy Manager:

Table 262. TCP Multiline Syslog log source parameters for the Aruba ClearPass Policy Manager DSM

Parameter	Value
Log Source type	Aruba ClearPass Policy Manager
Protocol Configuration	TCP Multiline Syslog
Log Source Identifier	Type the IP address or host name to identify the log source. To use a source name instead of a log source identifier, select **Use Custom Source Name** and enter the values for **Source Name Regex** and **Source Name Formatting String**. **Important:** These parameters are available only if **Show Advanced Options** is set to **Yes**. The log source identifier must be a unique value.
Listen Port	The port number that accepts incoming TCP Multiline Syslog events. The default **Listen Port** is **12468**. To edit the port number, complete the following steps: 1. Enter the new port number for the protocol. 2. Click **Save**. 3. Under the **Admin** tab, click **Advanced** > **Deploy Full Configuration**. **Important:** When the admin clicks **Deploy Full Configuration**, the system restarts all services, which can create in a gap in the data collection until the deployment is completed.
Aggregation Method	ID-Linked

Table 262. TCP Multiline Syslog log source parameters for the Aruba ClearPass Policy Manager DSM (continued)

Parameter	Value
Message ID Pattern	This parameter is available when you set **Aggregation Method** to **ID-Linked**. This regular expression (regex) is used to filter the event payload messages. The TCP multiline event messages must contain a common identifying value that repeats on each line of the event message. **Important:** In the case of message ID, enter this pattern: `messageId=(\d+)\d\d`
Event Formatter	No formatting
Show Advanced Options	Yes
Use Custom Source Name	Off
Use as a Gateway Log Source	Off, unless you have multiple Aruba devices sending to the same port.
Flatten Multiline Events Into Single Line	On
Retain Entire Lines During Event Aggregation	Off
Time Limit	3

The following is a sample event message for Aruba ClearPass Policy Manager for TCP Multiline Syslog protocol:

```
<135>Jul 21 14:15:58 10.0.0.0 LEEF:1.0|Aruba Networks|ClearPass|6.10.2.182283|13002|
messageId=5496525-2-0    Common.Username=Test    Common.Service=WIRELESS_MAC-AUTH-SERVICE
Common.Roles=IOT-DEVICE, [User Authenticated]     RADIUS.Auth-Source=Local:localhost
RADIUS.Auth-Method=MAC-AUTH    Common.System-Posture-Token=UNKNOWN
Common.Enforcement-Profiles=WIRELESS_BAS-ROLE, RETURN-DEVICE-NAME    Common.Host-MAC-
Address=test
Common.NAS-IP-Address=10.0.0.1    Common.Error-Code=0
Common.Alerts=Policy server: Failed to construct filter=SELECT\n
CASE WHEN expire_time is null or expire_time > now() THEN 'false'\n
ELSE 'true'\n      END AS is_expired,\n
CASE WHEN enabled = true THEN 'true' ELSE 'false' END as is_enabled\nFROM
tips_guest_users\nWHERE
((guest_type = 'USER') AND (user_id = '%{Endpoint:Username}') AND (app_name != 'Onboard')).
\nFailed to get value for attributes=[AccountEnabled, AccountExpired]
Common.Request-Timestamp=2023-07-21 14:15:45-04    src=10.0.0.1
<135>Jul 21 14:15:58 10.0.0.0 LEEF:1.0|Aruba Networks|ClearPass|6.10.2.182283|13002|
messageId=5496525-2-1
devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z    cat=Session Logs
```

For a complete list of TCP Multiline Syslog protocol parameters and their values, see “TCP Multiline Syslog protocol configuration options” on page 222.

Related tasks

“Adding a log source” on page 5

Aruba ClearPass Policy Manager sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Aruba ClearPass Policy Manager sample message when you use the syslog protocol

The following sample event message shows that a user with the username "user2" from IP address 10.1.1.5 is logged in to IP address 10.1.1.4 by using TACACS authentication.

```
<143>Sep 05 2018 09:10:03.062 CDT aruba.clearpass.test LEEF:1.0|Aruba
Networks|ClearPass|6.6.10.106403|3006|messageId=00000001-1-0    Tacacs.Username=user2
Tacacs.Remote-Address=10.1.1.3    Tacacs.Request-Type=TACACS_AUTHORIZATION    Tacacs.NAS-IP-
Address=10.1.1.4    Tacacs.Service=Tacacs Service Name    Tacacs.Auth-Source=Tacacs Auth Source
Name    Tacacs.Roles= [User Authenticated]|Role Name    Tacacs.Enforcement-Profiles=Enforcement
Profile Name    Tacacs.Privilege-Level=1    src=10.1.1.5    devTimeFormat=MMM dd yyyy
HH:mm:ss.SSS z    cat=Insight Logs
```

Table 263. Highlighted fields

QRadar field name	Highlighted payload field name
Username	**Tacacs.Username**
Destination IP Address	**Tacacs.NAS-IP-Address**
Source IP Address	**src**

Aruba Introspect

The IBM QRadar DSM for Aruba Introspect collects events from an Aruba Introspect device.

The following table describes the specifications for the Aruba Introspect DSM:

Table 264. Aruba Introspect DSM specifications

Specification	Value
Manufacturer	Aruba
DSM name	Aruba Introspect
RPM file name	DSM-ArubaIntrospect-*QRadar_version-build_number*.noarch.rpm
Supported versions	1.6
Protocol	Syslog
Event format	Name-value pair (NVP)
Recorded event types	Security System Internal Activity Exfiltration Infection Command & Control
Automatically discovered?	Yes
Includes identity?	No

Table 264. Aruba Introspect DSM specifications (continued)	
Specification	**Value**
Includes custom properties?	No
More information	Aruba website (https://www.arubanetworks.com)

To integrate Aruba Introspect with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (http://www.ibm.com/support).
   - DSMCommon RPM
   - ArubaIntrospect DSM RPM
2. Configure your Aruba Introspect device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an Aruba Introspect log source on the QRadar Console. The following table describes the parameters that require specific values for Aruba Introspect event collection:

Table 265. Aruba Introspect log source parameters	
Parameter	**Value**
Log Source type	Aruba Introspect
Protocol Configuration	Syslog
Log Source Identifier	A unique identifier for the log source.

4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   The following table shows a sample event message for Aruba Introspect

Table 266. Aruba Introspect sample event message

Event name	Low level category	Sample log message
Cloud Exfiltration	Suspicious Activity	May 6 20:04:38 <Server> May 7 03:04:38 lab-an-node msg_type=alert detection_time= "2016-05-06 20:04:23 -07:00" alert_name="Large DropBox Upload" alert_type="Cloud Exfiltration" alert_category= "Network Access" alert_severity=60 alert_confidence=20 attack_stage =Exfiltration user_name=<Username> src_host_name=example.com src_ip=<Source_IP_address> dest_ip=Destination_IP_address1>, <Destination_IP_address2>,... description="User <Username> on host example.com uploaded 324.678654 MB to Dropbox on May 05, 2016; compared with users in the whole Enterprise who uploaded an average of 22.851 KB during the same day" alert_id=xxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxx_xxxxxxxx xxxxxxxx_Large_DropBox_Upload May 6 20:04:38 <Server>May 7 03:04:38 lab-an-node msg_type=alert detection_time="2016-05-06 20:04:23 -07:00" alert_name="Large DropBox Upload" alert_type="Cloud Exfiltration" alert_category="Network Access" alert_severity=60 alert_confidence=20 attack_stage=Exfiltration user_name=<Username> src_host_name=example.com src_ip=<Source_IP_address> dest_ip=Destination_IP_address1>,<Dest ination_IP_address2>,... description="User <Username> on host example.com uploaded 324.678654 MB to Dropbox on May 05, 2016; compared with users in the whole Enterprise who uploaded an average of 22.851 KB during the same day" alert_id=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxx_xxxxxxxxxxxxxxx_Large _DropBox_Upload

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring Aruba Introspect to communicate with QRadar

Before IBM QRadar can collect events from Aruba Introspect, you must configure Aruba Introspect to send events to QRadar.

Procedure

1. Log in to the Aruba Introspect Analyzer.
2. Configure forwarding.
   a) Click **System Configuration** > **Syslog Destinations**.
   b) Configure the following forwarding parameters:

Table 267. Aruba Introspect Analyzer forwarding parameters	
Parameter	**Value**
Syslog Destination	IP or host name of the QRadar Event Collector.
Protocol	TCP or UDP
Port	514

3. Configure notification.
   a) Click **System Configuration** > **Security Alerts / Emails** > **Add New**.
   b) Configure the following notification parameters:

Table 268. Aruba Introspect Analyzer notification parameters	
Parameter	**Value**
Enable Alert Syslog Forwarding	Enable the **Enable Alert Syslog Forwarding** check box.
Sending Notification	As Alerts are produced. You can customize this setting to send in batches instead of a live stream.
TimeZone	Your local time zone.

Note: Leave **Query**, **Severity**, and **Confidence** values as default to send all Alerts. These values can be customized to filter out and send only a subset of Alerts to QRadar.

What to do next

To help you troubleshoot, you can look at the forwarding logs in the `/var/log/notifier.log` file.

When a new notification is created, as described in Step 3, alerts for the last week that match the **Query**, **Severity**, and **Confidence** fields are sent.

Aruba Mobility Controllers

The Aruba Mobility Controllers DSM for IBM QRadar accepts events by using syslog.

QRadar records all relevant events that are forwarded by using syslog on TCP port 514 or UDP port 514.

Configuring your Aruba Mobility Controller

You can configure the Aruba Wireless Networks (Mobility Controller) device to forward syslog events to IBM QRadar.

Procedure

1. Log in to Aruba Mobility Controller.
2. From the top menu, select **Configuration**.
3. From the **Switch** menu, select **Management**.
4. Click the **Logging** tab.
5. From the **Logging Servers** menu, select **Add**.
6. Type the IP address of the QRadar server that you want to collect logs.
7. Click **Add**.
8. Optional: Change the logging level for a module:
   a) Select the check box next to the name of the logging module.

b) Choose the logging level that you want to change from the list that is displayed at the bottom of the window.

9. Click **Done**.
10. Click **Apply**.

Syslog log source parameters for Aruba Mobility Controllers

If QRadar does not automatically detect the log source, add a Aruba Mobility Controllers log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Aruba Mobility Controllers:

Table 269. Syslog log source parameters for the Aruba Mobility Controllers DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for your log source.
Log Source type	**Aruba Mobility Controller**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source.

Related tasks

"Adding a log source" on page 5

Aruba Mobility Controllers sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Aruba Mobility Controllers sample message when you use the Syslog protocol

The following sample event shows a user authentication has succeeded.

```
<141>Mar 20 10:48:41 2014 aruba.mobility.test authmgr[3469]: <522008> <NOTI> <Test-1
192.168.94.12>  User Authentication Successful: username=user1 MAC=00:00:5E:00:53:01
IP=10.124.163.132 role=role1 VLAN=123 AP=Test-A/Test-B SSID=testID1 AAA profile=testID1_AAA auth
method=802.1x auth server=test_server
```


```
<141>Mar 20 10:48:41 2014 aruba.mobility.test authmgr[3469]: <522008> <NOTI> <Test-1
192.168.94.12>  User Authentication Successful: username=user1 MAC=00:00:5E:00:53:01
IP=10.124.163.132 role=role1 VLAN=123 AP=Test-A/Test-B SSID=testID1 AAA profile=testID1_AAA
auth method=802.1x auth server=test_server
```


Table 270. Highlighted values in the Aruba Mobility Controllers sample event

QRadar field name	Highlighted values in the event payload
EventID	**authmgr_noti_user_auth** extracted from the **Event ID** field in QRadar
Username	**User1**
Source IP	**10.124.163.132**
Source MAC	**00:00:5E:00:53:01**

Table 270. Highlighted values in the Aruba Mobility Controllers sample event (continued)	
QRadar field name	**Highlighted values in the event payload**
Device Time	**Mar 20, 2014, 10:48:41 AM**

Chapter 26. Avaya VPN Gateway

The IBM QRadar DSM for Avaya VPN Gateway can collect event logs from your Avaya VPN Gateway servers.

The following table identifies the specifications for the Avaya VPN Gateway DSM.

Table 271. Avaya VPN Gateway DSM specifications

Specification	Value
Manufacturer	Avaya Inc.
DSM	Avaya VPN Gateway
RPM file name	`DSM-AvayaVPNGateway-7.1-799033.noarch.rpm` `DSM-AvayaVPNGateway-7.2-799036.noarch.rpm`
Supported versions	9.0.7.2
Protocol	syslog
QRadar recorded events	OS, System Control Process, Traffic Processing, Startup, Configuration Reload, AAA Subsystem, IPsec Subsystem
Automatically discovered	Yes
Includes identity	Yes
More information	http://www.avaya.com

Avaya VPN Gateway DSM integration process

You can integrate Avaya VPN Gateway DSM with IBM QRadar.

About this task

To integrate Avaya VPN Gateway DSM with QRadar, use the following procedure:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Syslog protocol RPM
   - DSMCommon RPM
   - Avaya VPN Gateway RPM
2. For each instance of Avaya VPN Gateway, configure your Avaya VPN Gateway system to enable communication with QRadar.
3. If QRadar automatically discovers the log source, for each Avaya VPN Gateway server you want to integrate, create a log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring your Avaya VPN Gateway system for communication with IBM QRadar

To collect all audit logs and system events from Avaya VPN Gateway, you must specify QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your Avaya VPN Gateway command-line interface (CLI).
2. Type the following command:

   ```
   /cfg/sys/syslog/add
   ```
3. At the prompt, type the IP address of your QRadar system.
4. To apply the configuration, type the following command:

   ```
   apply
   ```
5. To verify that the IP address of your QRadar system is listed, type the following command:

   ```
   /cfg/sys/syslog/list
   ```

Syslog log source parameters for Avaya VPN Gateway

If QRadar does not automatically detect the log source, add a Avaya VPN Gateway log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Avaya VPN Gateway:

Table 272. Syslog log source parameters for the Avaya VPN Gateway DSM

Parameter	Value
Log Source type	**Avaya VPN Gateway**
Protocol Configuration	**Syslog**

Related tasks

"Adding a log source" on page 5

Avaya VPN Gateway sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Avaya VPN Gateway sample message when you use the Syslog protocol

Sample 1: The following sample event shows that the remote user has logged out from the VPN.

```
<134>Dec  9 19:38:32 avaya.vpngateway.test SSL: Informational SSL VPN Logout Vpn="1"
SrcIp="192.168.0.1" User="testuser" Reason="logout"
```


```
<134>Dec  9 19:38:32 avaya.vpngateway.test SSL: Informational SSL VPN Logout Vpn="1"
SrcIp="192.168.0.1" User="testuser" Reason="logout"
```

Table 273. Highlighted values in the Avaya VPN Gateway event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**VPN Logout**
Username	**testuser**
Source IP	**192.168.0.1**
Device Time	**Dec 9, 2020, 7:38:32 PM**

Sample 2: The following sample event shows that the log in to the VPN succeeded.

```
<134>Dec  9 19:36:15 avaya.vpngateway.test SSL: Informational SSL VPN LoginSucceeded Vpn="1"
SrcIp="10.147.0.26" Method="ipsec" User="testUser" Groups="testGroup " TunIP="10.147.0.26"
```

```
<134>Dec  9 19:36:15 avaya.vpngateway.test SSL: Informational SSL VPN LoginSucceeded Vpn="1"
SrcIp="192.168.0.1" Method="ipsec" User="testUser" Groups="testGroup " TunIP="10.147.0.26"
```

Table 274. Highlighted values in the Avaya VPN Gateway sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**VPN LoginSucceeded TunIP**
Username	**testUser**
Source IP	**192.168.0.1**
Destination IP	**10.147.0.26**
Identity Group Name	**testGroup**
Device Time	**Dec 9, 2020, 7:36:15 PM**

Chapter 27. BalaBit IT Security

The BalaBit Syslog-ng Agent application can collect and forward syslog events for the Microsoft Security Event Log DSM and the Microsoft ISA DSM in IBM QRadar.

BalaBit IT Security for Microsoft Windows Events

The Microsoft Windows Security Event Log DSM in IBM QRadar can accept Log Event Extended Format (LEEF) events from BalaBit's Syslog-ng Agent.

The BalaBit Syslog-ng Agent forwards the following Windows events to QRadar by using syslog:

- Windows security
- Application
- System
- DNS
- DHCP
- Custom container event logs

Before you can receive events from BalaBit IT Security Syslog-ng Agents, you must install and configure the agent to forward events.

Before you begin

Review the following configuration steps before you configure the BalaBit Syslog-ng Agent:

1. Install the BalaBit Syslog-ng Agent on your Windows host. For more information, see your BalaBit Syslog-ng Agent documentation.
2. Configure Syslog-ng Agent Events.
3. Configure QRadar as a destination for the Syslog-ng Agent.
4. Restart the Syslog-ng Agent service.
5. Optional. Configure the log source in QRadar.

Configuring the Syslog-ng Agent event source

Before you can forward events to IBM QRadar, you must specify what Windows-based events the Syslog-ng Agent collects.

Procedure

1. From the **Start** menu, select **All Programs** > **syslog-ng Agent for Windows** > **Configure syslog-ng Agent for Windows**.

   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and select **Eventlog Sources**.
3. Double-click **Event Containers**.

   The **Event Containers Properties** window is displayed.
4. From the **Event Containers** pane, select the **Enable** radio button.
5. Select a check box for each event type you want to collect:
   - **Application** - Select this check box if you want the device to monitor the Windows application event log.
   - **Security** - Select this check box if you want the device to monitor the Windows security event log.

- **System** - Select this check box if you want the device to monitor the Windows system event log.

Note: BalaBit's Syslog-ng Agent supports other event types, such as DNS or DHCP events by using custom containers. For more information, see your *BalaBit Syslog-ng Agent documentation*.

6. Click **Apply**, and then click **OK**.

   The event configuration for your BalaBit Syslog-ng Agent is complete. You are now ready to configure QRadar as a destination for Syslog-ng Agent events.

Configuring a syslog destination

The Syslog-ng Agent enables you to configure multiple destinations for your Windows based events.

About this task

To configure IBM QRadar as a destination, you must specify the IP address for QRadar, and then configure a message template for the LEEF format.

Procedure

1. From the **Start** menu, select **All Programs** > **Syslog-ng Agent for Windows** > **Configure syslog-ng Agent for Windows**.

   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and click **Destinations**.
3. Double-click **Add new server**.

   The **Server Property** window is displayed.
4. Click the **Server** tab, and then click **Set Primary Server**.
5. Configure the following parameters:
   - **Server Name** - Type the IP address of your QRadar Console or Event Collector.
   - **Server Port** - Type 514 as the TCP port number for events to be forwarded to QRadar.
6. Click the **Messages** tab.
7. From the **Protocol** list, select **Legacy BSD Syslog Protocol**.
8. In the **Template** field, define a custom template message for the protocol by typing:

   ```
   <${PRI}>${BSDDATE} ${HOST} LEEF:${MSG}
   ```

   The information that is typed in this field is space delimited.
9. In the **Event Message Format** pane, in the **Message Template** field, type or copy and paste the following text to define the format for the LEEF events:

   Note: It is suggested that you do not change the text.

   ```
   1.0|Microsoft|Windows|2k8r2|${EVENT_ID}|devTime=${R_YEAR}-${R_MONTH}-$
   {R_DAY}T${R_HOUR}:${R_MIN}:${R_SEC}GMT${TZOFFSET} devTimeFormat=yyyy-MM-
   dd'T'HH:mm:ssz cat=${EVENT_TYPE} sev=${EVENT_LEVEL} resource=${HOST}
   usrName=${EVENT_USERNAME} application=${EVENT_SOURCE} message=${EVENT_MSG}
   ```

   Note: The LEEF format uses tab as a delimiter to separate event attributes from each other. However, the delimiter does not start until after the last pipe character for `{Event_ID}`. The following fields must include a tab before the event name: *devTime*, *devTimeFormat*, *cat*, *sev*, *resource*, *usrName*, *application*, and *message*.

   You might need to use a text editor to copy and paste the LEEF message format into the **Message Template** field.
10. Click **OK**.

    The destination configuration is complete. You are now ready to restart the Syslog-ng Agent service.

Restarting the Syslog-ng Agent service

Before the Syslog-ng Agent can forward LEEF formatted events, you must restart the Syslog-ng Agent service on the Windows host.

Procedure

1. From the **Start** menu, select **Run**.

   The **Run** window is displayed.
2. Type the following text:

   ```
   services.msc
   ```
3. Click **OK**.

   The **Services** window is displayed.
4. In the **Name** column, right-click on **Syslog-ng Agent for Windows**, and select **Restart**.

   After the Syslog-ng Agent for Windows service restarts, the configuration is complete. Syslog events from the BalaBit Syslog-ng Agent are automatically discovered by IBM QRadar. The Windows events that are automatically discovered are displayed as Microsoft Windows Security Event Logs on the **Log Activity** tab.

Syslog log source parameters for BalaBit IT Security for Microsoft Windows Events

If QRadar does not automatically detect the log source, add a BalaBit IT Security for Microsoft Windows Events log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from BalaBit Syslog-ng Agent:

Table 275. Syslog log source parameters for the BalaBit IT Security for Microsoft Windows Events DSM

Parameter	Value
Log Source Name	Type a name for your BalaBit Syslog-ng Agent log source.
Log Source Description	Type a description for the log source.
Log Source type	Microsoft Windows **Security Event Log**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from the BalaBit Syslog-ng Agent.

Related tasks

"Adding a log source" on page 5

BalaBit IT Security for Microsoft ISA or TMG Events

You can integrate the BalaBit Syslog-ng Agent application to forward syslog events to IBM QRadar.

The BalaBit Syslog-ng Agent reads Microsoft ISA or Microsoft TMG event logs, and forwards syslog events by using the Log Event Extended Format (LEEF).

The events that are forwarded by BalaBit IT Security are parsed and categorized by the Microsoft Internet and Acceleration (ISA) DSM for QRadar. The DSM accepts both Microsoft ISA and Microsoft Threat Management Gateway (TMG) events.

Before you begin

Before you can receive events from BalaBit IT Security Syslog-ng Agents you must install and configure the agent to forward events.

Note: This integration uses BalaBit's Syslog-ng Agent for Windows and BalaBit's Syslog-ng PE to parse and forward events to QRadar for the DSM to interpret.

Review the following configuration steps before you attempt to configure the BalaBit Syslog-ng Agent:

To configure the BalaBit Syslog-ng Agent, you must take the following steps:

1. Install the BalaBit Syslog-ng Agent on your Windows host. For more information, see your *BalaBit Syslog-ng Agent vendor documentation*.
2. Configure the BalaBit Syslog-ng Agent.
3. Install a BalaBit Syslog-ng PE for Linux or Unix in relay mode to parse and forward events to QRadar. For more information, see your *BalaBit Syslog-ng PE vendor documentation*.
4. Configure syslog for BalaBit Syslog-ng PE.
5. Optional. Configure the log source in QRadar.

Configure the BalaBit Syslog-ng Agent

Before you can forward events to IBM QRadar, you must specify the file source for Microsoft ISA or Microsoft TMG events in the Syslog-ng Agent collects.

If your Microsoft ISA or Microsoft TMG appliance is generating event files for the Web Proxy Server and the Firewall Service, both files can be added.

Configuring the BalaBit Syslog-ng Agent file source

Use the BalaBit Syslog-ng Agent file source to define the base log directory and files that are to be monitored by the Syslog-ng Agent.

Procedure

1. From the **Start** menu, select **All Programs** > **syslog-ng Agent for Windows** > **Configure syslog-ng Agent for Windows**.

   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and select **File Sources**.
3. Select the **Enable** radio button.
4. Click **Add** to add your Microsoft ISA and TMG event files.
5. From the **Base Directory** field, click **Browse** and select the folder for your Microsoft ISA or Microsoft TMG log files.
6. From the **File Name Filter** field, click **Browse** and select a log file that contains your Microsoft ISA or Microsoft TMG events.

   Note: The **File Name Filter** field supports the wild card (*) and question mark (?) characters, which help you to find log files that are replaced, when they reach a specific file size or date.
7. In the **Application Name** field, type a name to identify the application.
8. From the **Log Facility** list, select **Use Global Settings**.
9. Click **OK**.

   To add additional file sources, repeat steps 4 to 9.

10. Click **Apply**, and then click **OK**.

    The event configuration is complete. You are now ready to configure a syslog destinations and formatting for your Microsoft TMG and ISA events.

    Web Proxy Service events and Firewall Service events are stored in individual files by Microsoft ISA and TMG.

Configuring a BalaBit Syslog-ng Agent syslog destination

The event logs captured by Microsoft ISA or TMG cannot be parsed by the BalaBit Syslog-ng Agent for Windows, so you must forward your logs to a BalaBit Syslog-ng Premium Edition (PE) for Linux or UNIX.

About this task

To forward your TMG and ISA event logs, you must specify the IP address for your PE relay and configure a message template for the LEEF format. The BalaBit Syslog-ng PE acts as an intermediate syslog server to parse the events and to forward the information to IBM QRadar.

Procedure

1. From the **Start** menu, select **All Programs** > **syslog-ng Agent for Windows** > **Configure syslog-ng Agent for Windows**.

   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and click **Destinations**.
3. Double-click **Add new Server**.
4. On the **Server** tab, click **Set Primary Server.**
5. Configure the following parameters:
   - For the **Server Name** type the IP address of your BalaBit Syslog-ng PE relay.
   - For the **Server Port** type 514 as the TCP port number for events that are forwarded to your BalaBit Syslog-ng PE relay.
6. Click the **Messages** tab.
7. From the **Protocol** list, select **Legacy BSD Syslog Protocol**.
8. From the **File Message Format** pane, in the **Message Template** field, type the following code:

   ```
   ${FILE_MESSAGE}${TZOFFSET}
   ```
9. Click **Apply**, and then click **OK**.

   The destination configuration is complete. You are now ready to filter comment lines from the event log.

Filtering the log file for comment lines

The event log file for Microsoft ISA or Microsoft TMG might contain comment markers. Comments must be filtered from the event message.

Procedure

1. From the **Start** menu, select **All Programs** > **Syslog-ng Agent for Windows** > **Configure syslog-ng Agent for Windows**.

   The **Syslog-ng Agent** window is displayed.
2. Expand the **Syslog-ng Agent Settings** pane, and select **Destinations**.
3. Right-click on your IBM QRadar **Syslog destination** and select **Event Filters** > **Properties**.

   The **Global event filters Properties** window is displayed.
4. Configure the following values:

- From the **Global file filters** pane, select **Enable**.
- From the **Filter Type** pane, select **Black List Filtering**.

5. Click **OK**.
6. From the **Filter List** menu, double-click **Message Contents**.

   The **Message Contents Properties** window is displayed.
7. From the **Message Contents** pane, select **Enable**.
8. In the **Regular Expression** field, type the following regular expression:

   ^#
9. Click **Add**.
10. Click **Apply**, and then click **OK**.

    The event messages with comments are no longer forwarded.

    Note: You might need to restart Syslog-ng Agent for Windows service to begin syslog forwarding. For more information, see your *BalaBit Syslog-ng Agent documentation*.

Configuring a BalaBit Syslog-ng PE Relay

The BalaBit Syslog-ng Agent for Windows sends Microsoft TMG and ISA event logs to a Balabit Syslog-ng PE installation, which is configured in relay mode.

About this task

The relay mode installation is responsible for receiving the event log from the BalaBit Syslog-ng Agent for Windows, parsing the event logs in to the LEEF format, then forwarding the events to IBM QRadar by using syslog.

To configure your BalaBit Syslog-ng PE Relay, you must:

1. Install BalaBit Syslog-ng PE for Linux or Unix in relay mode. For more information, see your BalaBit Syslog-ne PE vendor documentation.
2. Configure syslog on your Syslog-ng PE relay.

The BalaBit Syslog-ng PE formats the TMG and ISA events in the LEEF format based on the configuration of your `syslog.conf` file. The `syslog.conf` file is responsible for parsing the event logs and forwarding the events to QRadar.

Procedure

1. Using SSH, log in to your BalaBit Syslog-ng PE relay command-line interface (CLI).
2. Edit the following file:

   `/etc/syslog-ng/etc/syslog.conf`
3. From the destinations section, add an IP address and port number for each relay destination.

   For example,

   ```
   ###### # destinations destination d_messages { file("/var/log/
   messages"); }; destination d_remote_tmgfw { tcp("QRadar_IP"
   port(QRadar_PORT) log_disk_fifo_size(10000000) template(t_tmgfw)); };
   destination d_remote_tmgweb { tcp("QRadar_IP" port(QRadar_PORT)
   log_disk_fifo_size(10000000) template(t_tmgweb)); };
   ```

   Where:

   QRadar_IP is the IP address of your QRadar Console or Event Collector.

   QRadar_Port is the port number that is required for QRadar to receive syslog events. By default, QRadar receives syslog events on port 514.

4. Save the syslog configuration changes.
5. Restart Syslog-ng PE to force the configuration file to be read.

   The BalaBit Syslog-ng PE configuration is complete. Syslog events that are forwarded from the BalaBit Syslog-ng relay are automatically discovered by QRadar as Microsoft Windows Security Event Logs on the Log Activity tab. For more information, see the *IBM QRadar Users Guide*.

   Note: When you are using multiple syslog destinations, messages are considered to be delivered when they successfully arrive at the primary syslog destination.

Syslog log source parameters for BalaBit IT Security for Microsoft ISA or TMG Events

If QRadar does not automatically detect the log source, add a BalaBit IT Security for Microsoft ISA or TMG Events log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from BalaBit IT Security for Microsoft ISA or TMG Events:

Table 276. Syslog log source parameters for the BalaBit IT Security for Microsoft ISA or TMG Events DSM

Parameter	Value
Log Source Name	Type a name for the log source.
Log Source Description	Type a description for the log source.
Log Source type	Microsoft **ISA**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for Microsoft ISA or Microsoft Threat Management Gateway events from the BalaBit Syslog-ng Agent.

Related tasks

“Adding a log source” on page 5

Chapter 28. Barracuda

IBM QRadar supports a range of Barracuda devices.

Barracuda Spam & Virus Firewall

You can integrate Barracuda Spam & Virus Firewall with IBM QRadar.

The Barracuda Spam & Virus Firewall DSM for QRadar accepts both mail syslog events and web syslog events from Barracuda Spam & Virus Firewall appliances.

Mail syslog events contain the event and action that is taken when the firewall processes email. Web syslog events record information on user activity, and configuration changes that occur on your Barracuda Spam & Virus Firewall appliance.

Before you begin

Syslog messages are sent to QRadar from Barracuda Spam & Virus Firewall by using UDP port 514. You must verify that any firewalls between QRadar and your Barracuda Spam & Virus Firewall appliance allow UDP traffic on port 514.

Configuring syslog event forwarding

You can configure syslog forwarding for Barracuda Spam & Virus Firewall.

Procedure

1. Log in to the Barracuda Spam & Virus Firewall web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Advanced Networking**.
4. In the **Mail Syslog** field, type the IP address of your QRadar Console or Event Collector.
5. Click **Add**.
6. In the **Web Interface Syslog** field, type the IP address of your QRadar Console or Event Collector.
7. Click **Add**.

Syslog log source parameters for Barracuda Spam Firewall

If QRadar does not automatically detect the log source, add a Barracuda Spam & Virus Firewall log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Barracuda Spam & Virus Firewall:

Table 277. Syslog log source parameters for the Barracuda Spam & Virus Firewall DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source type	**Barracuda Spam & Virus Firewall**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source.

Related tasks

"Adding a log source" on page 5

Barracuda Spam and Virus Firewall sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Barracuda Spam & Virus Firewall sample message when you use the syslog protocol

Sample 1: This sample event shows that a message is blocked because the user doesn't exist.

```
Apr 11 11:24:37 2012 barracuda.firewall.test inbound/pass1[25713]: user[192.168.0.1]
1334157877-03f828647122cb90001-hUkLV9 1334157877 1334157877 RECV admin1@qradar.example.com
x7ZYJv5uCwenuD/3xNuYx0cYIAkqevlHLIZSj4XeuVOySIBOB8EwFiQ9lpD3MAgI 2 8 No such user (x7ZYJv5uCwenuD/
3xNuYx0cYIAkqevlHLIZSj4XeuVOySIBOB8EwFiQ9lpD3MAgI)
```


```
Apr 11 11:24:37 2012 barracuda.firewall.test inbound/pass1[25713]: user[192.168.0.1]
1334157877-03f828647122cb90001-hUkLV9 1334157877 1334157877 RECV admin1@qradar.example.com
x7ZYJv5uCwenuD/3xNuYx0cYIAkqevlHLIZSj4XeuVOySIBOB8EwFiQ9lpD3MAgI 2 8 No such user
(x7ZYJv5uCwenuD/3xNuYx0cYIAkqevlHLIZSj4XeuVOySIBOB8EwFiQ9lpD3MAgI)
```


Table 278. Highlighted values in the Barracuda Spam & Virus Firewall event

QRadar field name	Highlighted values in the event payload
Event ID	**Blocked Message** is extracted from the **Event ID** field in QRadar
Event Category	**No such user**
Source IP	**192.168.0.1**
Username	**x7ZYJv5uCwenuD/3xNuYx0cYIAkqevlHLIZSj4XeuVOySIBOB8EwFiQ9lpD3MAgI**
Device time	**Apr 11 11:24:37 2012**

Sample 2: This sample event shows that a message is blocked because of political intentions.

```
<23>scan[9097]: user[192.168.0.1] 1366829265-05f5cb11fe1b9a50001-wlKzrS 1366829265
1366829266 SCAN ENC admin2@qradar.example.com qIWHXoYEpfP+Ut0/6KYPSBB/+f368IWMkt7vCt/
wP0iySIBOB8EwFiQ9lpD3MAgI - 2 70 example.org SZ:3117 Subj: Random Email Subject Line
```


```
<23>scan[9097]: user[192.168.0.1] 1366829265-05f5cb11fe1b9a50001-wlKzrS 1366829265
1366829266 SCAN ENC admin2@qradar.example.com qIWHXoYEpfP+Ut0/6KYPSBB/+f368IWMkt7vCt/
wP0iySIBOB8EwFiQ9lpD3MAgI - 2 70 example.org SZ:3117 Subj: Random Email Subject Line
```


Table 279. Highlighted values in the Barracuda Spam & Virus Firewall sample event

QRadar field name	Highlighted values in the event payload
Event ID	**Blocked Message** is extracted from the **Event ID** field in QRadar
Event Category	**Intent - political** is extracted from the **Event Category** field in QRadar
Source IP	**192.168.0.1**
Username	**qIWHXoYEpfP+Ut0/6KYPSBB/+f368IWMkt7vCt/ wP0iySIBOB8EwFiQ9lpD3MAgI**

Barracuda Web Application Firewall

The IBM QRadar DSM for Barracuda Web Application Firewall collects syslog LEEF and custom events from Barracuda Web Application Firewall devices.

The following table identifies the specifications for the Barracuda Web Application Firewall DSM:

Table 280. Barracuda Web Application Firewall DSM specifications

Specification	Value
Manufacturer	Barracuda
DSM name	Web Application Firewall
RPM file name	DSM-BarracudaWebApplicationFirewall-*QRadar_version-build_number*.noarch.rpm
Supported versions	V7.0.x and later
Protocol type	Syslog
QRadar recorded event types	System Web Access Audit
Automatically discovered?	If LEEF-formatted payloads, the log source is automatically discovered. If custom-formatted payloads, the log source is not automatically discovered.
Included identity?	Yes
More information	Barracuda Networks website (https://www.barracuda.com)

To collect syslog events from Barracuda Web Application Firewall, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Barracuda Web Application Firewall DSM RPM
   - DSMCommon RPM
2. Configure your Barracuda Web Application Firewall device to send syslog events to QRadar.
3. Add a Barracuda Web Application Firewall log source on the QRadar Console. The following table describes the parameters that require specific values that are required for Barracuda Web Application Firewall event collection:

Table 281. Barracuda Web Application Firewall log source parameters

Parameter	Value
Log Source type	Barracuda Web Application Firewall
Protocol Configuration	Syslog

Configuring Barracuda Web Application Firewall to send syslog events to QRadar

Configure your Barracuda Web Application Firewall appliance to send syslog events to IBM QRadar.

Before you begin

Verify that firewalls between the Barracuda appliance and QRadar allow UDP traffic on port 514.

Procedure

1. Log in to the Barracuda Web Application Firewall web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Export Logs**.
4. Click **Add Syslog Server**.
5. Configure the parameters:

Option	Description
Name	The name of the QRadar Console or Event Collector
Syslog Server	The IP address of your QRadar Console or Event Collector.
Port	The port that is associated with the IP address of your QRadar Console or Event Collector. If syslog messages are sent by UDP, use the default port, 514.
Connection Type	The connection type that transmits the logs from the Barracuda Web Application Firewall to the QRadar Console or Event Collector. UDP is the default protocol for syslog communication.
Validate Server Certificate	**No**

6. In the **Log Formats** pane, select a format from the list box for each log type.
   - If you are using newer versions of Barracuda Web Application Firewall, select **LEEF 1.0 (QRadar)**.
   - If you are using older versions of Barracuda Web Application Firewall, select **Custom Format**.
7. Click **Save Changes**.

Configuring Barracuda Web Application Firewall to send syslog events to QRadar for devices that do not support LEEF

If your device does not support LEEF, you can configure syslog forwarding for Barracuda Web Application Firewall.

Procedure

1. Log in to the Barracuda Web Application Firewall web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Export logs**.
4. Click **Syslog Settings**.
5. Configure a syslog facility value for the following options:

Option	Description
Web Firewall Logs Facility	Select a syslog facility between **Local0** and **Local7**.

Option	Description
Access Logs Facility	Select a syslog facility between **Local0** and **Local7**.
Audit Logs Facility	Select a syslog facility between **Local0** and **Local7**.
System Logs Facility	Select a syslog facility between **Local0** and **Local7**.

Setting a syslog unique facility for each log type allows the Barracuda Web Application Firewall to divide the logs in to different files.

6. Click **Save Changes**.
7. In the **Name** field, type the name of the syslog server.
8. In the **Syslog** field, type the IP address of your QRadar Console or Event Collector.
9. From the **Log Time Stamp** option, select **Yes**.
10. From the **Log Unit Name** option, select **Yes**.
11. Click **Add**.
12. From the **Web Firewall Logs Format** list box, select **Custom Format**.
13. In the **Web Firewall Logs Format** field, type the following custom event format:
    `t=%t|ad=%ad|ci=%ci|cp=%cp|au=%au`
14. From the **Access Logs Format** list box, select **Custom Format**.
15. In the **Access Logs Format** field, type the following custom event format:
    `t=%t|p=%p|s=%s|id=%id|ai=%ai|ap=%ap|ci=%ci|cp=%cp|si=%si|sp=%sp|cu=%cu`
16. From the **Audit Logs Format** list box, select **Custom Format**.
17. In the **Audit Logs Format** field, type the following custom event format:
    `t=%t|trt=%trt|an=%an|li=%li|lp=%lp`
18. Click **Save Changes**.
19. From the navigation menu, select **Basic** > **Administration**
20. From the System/Reload/Shutdown pane, click **Restart**.

Results

The syslog configuration is complete after your Barracuda Web Application Firewall restarts. Events that are forwarded to QRadar by Barracuda Web Application Firewall are displayed on the **Log Activity** tab.

Barracuda Web Filter

You can integrate Barracuda Web Filter appliance events with IBM QRadar.

The Barracuda Web Filter DSM for IBM QRadar accepts web traffic and web interface events in syslog format that are forwarded by Barracuda Web Filter appliances.

Web traffic events contain the events, and any actions that are taken when the appliance processes web traffic. Web interface events contain user login activity and configuration changes to the Web Filter appliance.

Before you begin

Syslog messages are forward to QRadar by using UDP port 514. You must verify that any firewalls between QRadar and your Barracuda Web Filter appliance allow UDP traffic on port 514.

Configuring syslog event forwarding

Configure syslog forwarding for Barracuda Web Filter.

Procedure

1. Log in to the Barracuda Web Filter web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Syslog**.
4. From the **Web Traffic Syslog** field, type the IP address of your QRadar Console or Event Collector.
5. Click **Add**.
6. From the **Web Interface Syslog** field, type the IP address of your QRadar Console or Event Collector.
7. Click **Add**.

   The syslog configuration is complete.

Syslog log source parameters for Barracuda Web Filter

If QRadar does not automatically detect the log source, add a Barracuda Web Filter log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Barracuda Web Filter:

Table 282. Syslog log source parameters for the Barracuda Web Filter DSM

Parameter	Value
Log Source Name	The name of your log source.
Log Source Description	Type a description for your log source.
Log Source type	**Barracuda Web Filter**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Barracuda Web Filter appliance.

Related tasks

“Adding a log source” on page 5

Barracuda Web Filter sample event message

Use this sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Barracuda Web Filter sample message when you use the Syslog protocol

The following sample event message shows a failed login.

```
<142> web: [10.22.111.109] FAILED_LOGIN (leec)
```

Table 283. Highlighted fields in the Barracuda Web Filter event	
QRadar field name	**Highlighted payload field name**
Event ID	**FAILED_LOGIN**
SRC IP	**10.22.111.109**
Username	**leec**

Chapter 29. BeyondTrust PowerBroker

The IBM QRadar DSM for BeyondTrust PowerBroker logs all events to a multi-line format in a single event log that is viewed by using Beyond Trust's *pblog* utility.

You must be on a Linux, Unix or AIX® operating system to integrate BeyondTrust PowerBroker with QRadar.

To integrate BeyondTrust PowerBroker with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the BeyondTrust PowerBroker DSM RPM on your QRadar Console.
2. Configure BeyondTrust PowerBroker to communicate with QRadar. See Configuring BeyondTrust PowerBroker to communicate with QRadar.

For more information about TLS syslog log source parameters, see TLS syslog protocol configuration options.

Related concepts

"TLS Syslog protocol configuration options" on page 227
Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

"BeyondTrust PowerBroker DSM specifications" on page 534
The following table describes the specifications for the BeyondTrust PowerBroker DSM.

"BeyondTrust PowerBroker sample event message" on page 534
Use this sample event messages as a way of verifying a successful integration with QRadar.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5
"Configuring BeyondTrust PowerBroker to communicate with QRadar" on page 532

Syslog log source parameters for BeyondTrust PowerBroker

If QRadar does not automatically detect the log source, add a BeyondTrust PowerBroker log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from BeyondTrust PowerBroker:

Table 284. Syslog log source parameters for the BeyondTrust PowerBroker DSM

Parameter	Value
Log Source type	**BeyondTrust PowerBroker**
Protocol Configuration	**Syslog**
Log Source Identifier	Type a unique IP address or host name.

Table 284. Syslog log source parameters for the BeyondTrust PowerBroker DSM (continued)	
Parameter	**Value**
Store Event Payload	Select this check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** list in the **System Settings** window, which is accessible on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source.

Related tasks

"Adding a log source" on page 5

TLS Syslog log source parameters for BeyondTrust PowerBroker

If QRadar does not automatically detect the log source, add a BeyondTrust PowerBroker log source on the QRadar Console by using the TLS Syslog protocol.

When using the TLS Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect TLS Syslog events from BeyondTrust PowerBroker:

Table 285. TLS Syslog log source parameters for the BeyondTrust PowerBroker DSM	
Parameter	**Value**
Log Source type	**BeyondTrust PowerBroker**
Protocol Configuration	**TLS Syslog**
Log Source Identifier	Type a unique IP address or host name.

Related tasks

"Adding a log source" on page 5

Configuring BeyondTrust PowerBroker to communicate with QRadar

If you use a Linux, Unix or AIX operating system, complete the following procedure.

BeyondTrust *pblogs* must be reformatted by using a script and then forwarded to IBM QRadar. You need to download and configure a script for your BeyondTrust PowerBroker appliance before you can forward events to QRadar.

Procedure

1. Download the following file from the IBM support website (http://www.ibm.com/support):

   `pbforwarder.pl.gz`
2. Copy the file to the device that hosts BeyondTrust PowerBroker.

   Note: Perl 5.8 must be installed on the device that hosts BeyondTrust PowerBroker.
3. Type the following command to extract the file:

```
gzip -d pbforwarder.pl.gz
```

4. Type the following command to set the script file permissions:

```
chmod +x pbforwarder.pl
```

5. Use SSH to log in to the device that hosts BeyondTrust PowerBroker.

   The credentials that are used need to have read, write, and execute permissions for the log file.

6. Type the appropriate command parameters:

Table 286. Command parameters

Parameters	Description
-h	The **-h** parameter defines the syslog host that receives the events from BeyondTrust PowerBroker. This is the IP address of your QRadar Console or QRadar Event Collector.
-t	The **-t** parameter defines that the command-line is used to tail the log file and monitor for new output from the listener. For PowerBroker, this command must be specified as `"pblog -l -t"`.
-p	The **-p** parameter defines the TCP port to be used when forwarding events. If nothing is specified, the default is port 514.
-H	The **-H** parameter defines the host name or IP address for the syslog header of all sent events. This should be the IP address of the BeyondTrust PowerBroker.
-r	The **-r** parameter defines the directory name where you want to create the process ID (`.pid`) file. The default is `/var/run`. This parameter is ignored if **-D** is specified.
-l	The **-l** parameter defines the directory name where you want to create the lock file. The default is `/var/lock`. This parameter is ignored if **-D** is specified.
-D	The **-D** parameter defines that the script runs in the foreground. The default setting is to run as a daemon and log all internal messages to the local syslog server.
-f	The **-f** parameter defines the syslog facility and optionally, the severity for messages that are sent to the Event Collector. If no value is specified, `user.info` is used.
-a	The **-a** parameter enables an AIX compatible *ps* method. This command is only needed when you run BeyondTrust PowerBroker on AIX systems.
-d	The **-d** parameter enables debug logging.
-v	The **-v** parameter displays the script version information.

7. Type the following command to start the `pbforwarder.pl` script. Use the following example as a guide.

```
pbforwarder.pl -h <IP address> -t "pblog -l -t"
```

Where <*IP address*> is the IP address of your QRadar or Event Collector.

8. Optional: If you want to stop the script from forwarding events to QRadar, type the following command to stop the `pbforwarder.pl` script:

```
kill -QUIT `cat /var/run/pbforwarder.pl.pid`
```

9. Optional: If the script loses connection or stops working, type the following command to reconnect the `pbforwarder.pl` script:

```
kill -HUP `cat /var/run/pbforwarder.pl.pid`
```

QRadar automatically detects and creates a log source from the syslog events that are forwarded from a BeyondTrust PowerBroker.

BeyondTrust PowerBroker DSM specifications

The following table describes the specifications for the BeyondTrust PowerBroker DSM.

Table 287. BeyondTrust PowerBroker DSM specifications

Specification	**Value**
Manufacturer	BeyondTrust
DSM name	BeyondTrust PowerBroker
RPM file name	`DSM-BeyondTrustPowerBroker-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	4.0
Protocol	Syslog, TLS syslog
Event format	System, Application
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	BeyondTrust web page (https://www.beyondtrust.com/products/powerbroker/)

BeyondTrust PowerBroker sample event message

Use this sample event messages as a way of verifying a successful integration with QRadar.

The following table provides a sample event message for the BeyondTrust PowerBroker DSM:

Table 288. BeyondTrust PowerBroker sample syslog message

Event name	Low level category	Sample log message
Finish pbrun terminated	Information	<14>Feb 15 13:23:09 qradar4292 pbforwarder.pl: DEVICETYPE = PowerBroker EVENTID = PB EVENTCAT = unknown DDATE = USER = SRC = DST = EVENT_HEADER = ac15208e4eaddff b1BB002 Finish pbrun terminated: signal 1 (Hangup) unknown signal code event = "Finish" exitdate = "2011/10/30" exitstatus = "pbrun terminated: signal 1 (Hangup) unknown signal code" exittime = "21:01:49" i18n_exitdate = "10/30/11 " i18n_exittime = "21:01:49" logpid = 22085786 uniqueid = "ac15208e4eaddffb1BB002" <14>Feb 15 13:23:09 qradar4292 pbforwarder.pl: DEVICETYPE = PowerBroker EVENTID = PB EVENTCAT = unknown DDATE = USER = SRC = DST = EVENT_HEADER = ac15208e4eaddffb1BB002 Finish pbrun terminated: signal 1 (Hangup) unknown signal code event = "Finish" exitdate = "2011/10/30" exitstatus = "pbrun terminated: signal 1 (Hangup) unknown signal code" exittime = "21:01:49" i18n_exitdate = "10/30/11" i18n_exittime = "21:01:49" logpid = 22085786 uniqueid = "ac15208e4eaddffb1BB002"

Chapter 30. BlueCat Networks Adonis

The BlueCat Networks Adonis DSM for IBM QRadar accepts events that are forwarded in Log Event Extended Format (LEEF) by using syslog from BlueCat Adonis appliances that are managed with BlueCat Proteus.

QRadar supports BlueCat Networks Adonis appliances by using version 6.7.1-P2 and later.

You might be required to include a patch on your BlueCat Networks Adonis to integrate DNS and DHCP events with QRadar. For more information, see *KB-4670* and your *BlueCat Networks documentation*.

Supported event types

IBM QRadar is capable of collecting all relevant events related to DNS and DHCP queries.

This includes the following events:

- DNS IPv4 and IPv6 query events
- DNS name server query events
- DNS mail exchange query events
- DNS text record query events
- DNS record update events
- DHCP discover events
- DHCP request events
- DHCP release events

Event type format

The LEEF format consists of a pipe (|) delimited syslog header and a space delimited event payload.

For example:

```
Aug 10 14:55:30 <Server> LEEF:1.0|BCN|Adonis|6.7.1|DNS_Query|cat=A_record
src=<Source_IP_address> url=test.example.com
```

If the syslog events forwarded from your BlueCat Adonis appliances are not formatted similarly to the sample above, you must examine your device configuration. Properly formatted LEEF event messages are automatically discovered by the BlueCat Networks Adonis DSM and added as a log source to IBM QRadar.

Before you begin

BlueCat Adonis must be configured to generate events in Log Event Extended Format (LEEF) and to redirect the event output to QRadar using syslog.

BlueCat Networks provides a script on their appliances to assist you with configuring syslog. To complete the syslog redirection, you must have administrative or root access to the command line interface of the BlueCat Adonis or your BlueCat Proteus appliance. If the syslog configuration script is not present on your appliance, contact your BlueCat Networks representative.

Configuring BlueCat Adonis

You can configure your BlueCat Adonis appliance to forward DNS and DHCP events to IBM QRadar SIEM.

Procedure

1. Using SSH, log in to your BlueCat Adonis appliance.

2. On the command-line interface type the following command to start the syslog configuration script:

   `/usr/local/bluecat/QRadar/setup-QRadar.sh`
3. Type the IP address of your QRadar Console or Event Collector.
4. Type `yes` or `no` to confirm the IP address.

   The configuration is complete when a success message is displayed.

   The log source is added to QRadar as BlueCat Networks Adonis syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab. If the events are not automatically discovered, you can manually configure a log source.

Syslog log source parameters for BlueCat Networks Adonis

If QRadar does not automatically detect the log source, add a Blue Cat Networks Adonis log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Blue Cat Networks Adonis:

Table 289. Syslog log source parameters for the Blue Cat Networks Adonis DSM

Parameter	Value
Log Source name	The name of your log source.
Log Source description	Type a description for your log source.
Log Source type	**BlueCat Networks Adonis**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your BlueCat Networks Adonis appliance.

Related tasks

"Adding a log source" on page 5

Chapter 31. Blue Coat

IBM QRadar supports a range of Blue Coat products.

Blue Coat SG

The IBM QRadar DSM for Blue Coat SG collects events from Blue Coat SG appliances.

The following table lists the specifications for the Blue Coat SG DSM:

Table 290. Blue Coat SG DSM specifications

Specification	**Value**
Manufacturer	Blue Coat
DSM name	Blue Coat SG Appliance
RPM file name	`DSM-BlueCoatProxySG-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	SG v4.x and later
Protocol	Syslog Log File Protocol
Recorded event types	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	Yes
More information	Blue Coat website (http://www.bluecoat.com)

To send events from Blue Coat SG to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Blue Coat SG DSM RPM from the IBM Support Website (https://www.ibm.com/support/fixcentral) onto your QRadar Console.
2. Configure your Blue Coat SG device to communicate with QRadar. Complete the following steps:
   a. Create a custom event format.
   b. Create a log facility.
   c. Enable access logging.
   d. Configure Blue Coat SG for either Log File protocol or syslog uploads.

The instructions provided describe how to configure Blue Coat SG by using a custom name-value pair format. However, QRadar supports the following formats:

- Custom Format
- SQUID
- NCSA
- main
- IM
- Streaming
- smartreporter

- bcreportermain_v1
- bcreporterssl_v1
- p2p
- SSL
- bcreportercifs_v1
- CIFS
- MAPI

These standard formats can change between Blue Coat SG versions, which might keep them from being parsed correctly. When you configure Blue Coat SG by using a custom name-value pair format, parsing is more reliable.

Related concepts

Creating extra custom format key-value pairs

Log File log source parameters for Blue Coat SG

Related tasks

Creating a log facility

To use the custom log format that you created for IBM QRadar, you must associate the custom log format to a facility.

Enabling access logging

You must enable access logging on your Blue Coat SG device.

Configuring Blue Coat SG for syslog

To allow syslog event collection, you must configure your Blue Coat SG appliance to forward syslog events to IBM QRadar.

Creating a custom event format for Blue Coat SG

To collect events from Blue Coat SG, create a custom event format.

Procedure

1. Log in to the **Blue Coat Management Console**.
2. Select **Configuration > Access Logging > Formats**.
3. Select **New**.
4. Type a format name for the custom format.
5. Select **Custom format string**.
6. Type the following custom format:

Attention: The line breaks in these examples will cause this configuration to fail. Copy the code blocks into a text editor, remove the line breaks, and paste as a single line in the **Custom Format** column.

```
Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-address)
|dstport=$(cs-uri-port)|username=$(cs-username)|devicetime=$(gmttime)|s-action=$(s-action)|
sc-status=$(sc-status)|cs-method=$(cs-method)|time-taken=$(time-taken)|sc-bytes=$(sc-bytes)|
cs-bytes=$(cs-bytes)|cs-uri-scheme=$(cs-uri-scheme)|cs-host=$(cs-host)|cs-uri-path=$(cs-
uri-path)|cs-uri-query=$(cs-uri-query)|cs-uri-extension=$(cs-uri-extension)|cs-auth-group=$
(cs-auth-group)|rs(Content-Type)=$(rs(Content-Type))|cs(User-Agent)=$(cs(User-Agent))|
cs(Referer)=$(cs(Referer))|sc-filter-result=$(sc-filter-result)|filter-category=$(sc-filter-
category)|cs-uri=$(cs-uri)
```

7. Select **Log Last Header** from the list.
8. Click **OK**.
9. Click **Apply**.

Note: The custom format for QRadar supports more key-value pairs by using the Blue Coat ELFF format. For more information, see “Creating extra custom format key-value pairs” on page 546.

What to do next

Create a log facility on your Blue Coat device.

Related tasks

Creating a log facility

To use the custom log format that you created for IBM QRadar, you must associate the custom log format to a facility.

Creating a log facility

To use the custom log format that you created for IBM QRadar, you must associate the custom log format to a facility.

Procedure

1. Select **Configuration > Access Logging > Logs**.
2. Click **New**.
3. Configure the following parameters:

Parameter	Description
Log Name	A name for the log facility.
Log Format	The custom format you that created.
Description	A description for the log facility.

4. Click **OK**.
5. Click **Apply**.

Related tasks

Enabling access logging

You must enable access logging on your Blue Coat SG device.

Enabling access logging

You must enable access logging on your Blue Coat SG device.

Procedure

1. Select **Configuration > Access Logging > General**.
2. Select the **Enable Access Logging** check box.
3. Optional: If you use Blue Coat SGOS 6.2.11.2 Proxy Edition, complete the following steps:
   a) Select **Config > Policy > Visual Policy Manager**.
   b) In the **Policy** section, add **Web Access Layer for Logging**.
   c) Select **Action > Edit** and enable logging to the log facility.
4. Click **Apply**.

Related concepts

Creating extra custom format key-value pairs

Configuring Blue Coat SG for FTP uploads

To collect Blue Coat SG events using FTP, configure the Blue Coat SC to upload events to a FTP server using the Blue Coat upload client.

Procedure

1. Select **Configuration** > **Access Logging** > **Logs** > **Upload Client**.

2. From the **Log** list, select the log that contains your custom format.
3. From the **Client type** list, select **FTP Client**.
4. Select the **text file** option.
5. Click **Settings**.
6. From the **Settings For** list, select **Primary FTP Server**.
7. Configure the following values:

Parameter	Description
Host	The IP address of the FTP server that you want to forward the Blue Coat events.
Port	The FTP port number.
Path	The directory path for the log files.
Username	The user name to access the FTP server.

8. Click **OK**.
9. Select the **Upload Schedule** tab.
10. From the **Upload the access log** option, select **Periodically**.
11. Configure the **Wait time between connect attempts** option.
12. Select to upload the log file to the FTP daily or on an interval.
13. Click **Apply**.

Syslog log source parameters for Blue Coat SG

If QRadar does not automatically detect the log source, add a Blue Coat SG log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Blue Coat SG:

Table 291. Syslog log source parameters for the Blue Coat SG DSM

Parameter	Value
Log Source name	Type a name of your log source.
Log Source description	Type a description for your log source.
Log Source type	**Blue Coat SG Appliance**
Protocol Configuration	**Syslog**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow QRadar to identify a log file to a unique event source.

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related tasks

"Adding a log source" on page 5

Log File log source parameters for Blue Coat SG

If QRadar does not automatically detect the log source, add a Blue Coat SG log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from Blue Coat SG:

Table 292. Log File log source parameters for the Blue Coat SG DSM

Parameter	Value
Log Source name	Type a name of your log source.
Log Source description	Type a description for your log source.
Log Source type	**Blue Coat SG Appliance**
Protocol Configuration	**Log File**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are recommended as they allow QRadar to identify a log file to a unique event source.
Service Type	From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535. The options include: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.
Remote User	Type the user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select **SCP** or **SFTP** as the Service Type, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.

Table 292. Log File log source parameters for the Blue Coat SG DSM (continued)	
Parameter	**Value**
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. For FTP only. If your log files are in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The Recursive option is ignored if you configure SCP as the Service Type.
FTP File Pattern	If you select **SFTP** or **FTP** as the Service Type, this option gives you the option to configure the regular expression (regex) required to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing. The FTP file pattern that you specify must match the name you assigned to your event files. For example, to collect files that end with `.log`, type the following: `.*\.log` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: https://docs.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option appears only if you select **FTP** as the Service Type. The **FTP Transfer Mode** parameter gives you the option to define the file transfer mode when you retrieve log files over FTP. From the list, select the transfer mode that you want to apply to this log source: You must select **NONE** for the Processor parameter and **LINEBYLINE** the Event Generator parameter when you use ASCII as the FTP Transfer Mode.
SCP Remote File	If you select **SCP** as the Service Type you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type `00:00` to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24 hour clock, in the following format: HH:MM.

Table 292. Log File log source parameters for the Blue Coat SG DSM (continued)	
Parameter	**Value**
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the **Run On Save** completes, the log file protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	If the files located on the remote host are stored in a zip, gzip, tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that have already been processed by the log file protocol. QRadar examines the log files in the remote directory to determine if a file has been previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that have not been previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define a local directory on your QRadar system for storing downloaded files during processing. We recommend that you leave this check box clear. When this check box is selected, the Local Directory field is displayed, which allows you to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select LineByLine. The Event Generator applies additional processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related concepts

Blue Coat SG

The IBM QRadar DSM for Blue Coat SG collects events from Blue Coat SG appliances.

Related tasks

"Adding a log source" on page 5

Configuring Blue Coat SG for syslog

To allow syslog event collection, you must configure your Blue Coat SG appliance to forward syslog events to IBM QRadar.

Before you begin

Note: When you send syslog events to multiple syslog destinations, a disruption in availability in one syslog destination might interrupt the stream of events to other syslog destinations from your Blue Coat SG appliance.

Procedure

1. Select **Configuration** > **Access Logging** > **Logs** > **Upload Client**.
2. From the **Log** list, select the log that contains your custom format.
3. From the **Client type** list, select **Custom Client**.
4. Click **Settings**.
5. From the **Settings For** list, select **Primary Custom Server**.
6. In the **Host** field, type the IP address for your QRadar system.
7. In the **Port** field, type 514.
8. Click **OK**.
9. Select the **Upload Schedule** tab.
10. From the **Upload the access log** list, select **Continuously**.
11. Click **Apply**.

Creating extra custom format key-value pairs

Use the Extended Log File Format (ELFF) custom format to forward specific Blue Coat data or events to IBM QRadar.

The custom format is a series of pipe-delimited fields that start with the `Bluecoat|` field and contains the `$(Blue Coat ELFF)` parameter.

For example:

```
Bluecoat|src=$(c-ip)|srcport=$(c-port)|dst=$(cs-uri-address)|dstport=$(cs-uri-port)|username=$(cs-username)|devicetime=$(gmttime)|s-action=$(s-action)|sc-status=$(sc-status)|cs-method=$(cs-method)
```

Table 293. Custom Format examples

Blue Coat ELFF Parameter	QRadar Custom Format Example
sc-bytes	$(sc-bytes)
rs(Content-type)	$(rs(Content-Type))

For more information about available Blue Coat ELFF parameters, see your Blue Coat appliance documentation.

Blue Coat SG sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Blue Coat SG sample message when you use the Syslog protocol

The following sample event message shows that access was denied by a filter.

```
2016-11-07 13:13:54 44 172.28.51.1 407 TCP_DENIED 2251 492 GET http clients5.example.com
80 /complete/search ?hl=de-DE&q=t&client=ie8&inputencoding=UTF-8&outputencoding=UTF-8 - - - - -
"Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko" DENIED "Search Engines/Portals" -
192.168.165.34
```

```
2016-11-07 13:13:54 44 172.28.51.1 407 TCP_DENIED 2251 492 GET http clients5.example.com 80
/complete/search ?hl=de-DE&q=t&client=ie8&inputencoding=UTF-8&outputencoding=UTF-8 - - - - -
"Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko" DENIED "Search Engines/Portals"
- 192.168.165.34
```

Table 294. Highlighted values in the Blue Coat SG event

QRadar field name	Highlighted values in the event payload
Event ID	**TCP_DENIED**
Event Category	For this DSM, the value in QRadar is always **WebProxy**
Source IP	**172.28.51.1**
Destination IP	**192.168.165.34**
Destination port	**80**

Blue Coat Web Security Service

The IBM QRadar DSM for Blue Coat Web Security Service collects events from the Blue Coat Web Security Service.

The following table describes the specifications for the Blue Coat Web Security Service DSM:

Table 295. Blue Coat Web Security Service DSM specifications

Specification	Value
Manufacturer	Blue Coat
DSM name	Blue Coat Web Security Service
RPM file name	DSM-BlueCoatWebSecurityService-*Qradar_version-build_number*.noarch.rpm
Event format	Blue Coat ELFF
Recorded event types	Access
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Blue Coat website (https://www.bluecoat.com)

To integrate Blue Coat Web Security Service with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common RPM
   - Blue Coat Web Security Service REST API Protocol RPM
   - Blue Coat Web Security Service DSM RPM
2. Configure Blue Coat Web Security Service to allow QRadar access to the Sync API.
3. Add a Blue Coat Web Security Service log source on the QRadar Console. The following table describes the parameters that require specific values for Blue Coat Web Security Service event collection:

Table 296. Blue Coat Web Security Service log source parameters

Parameter	Value
Protocol Configuration	The protocol that is used to receive events from the Blue Coat Web Security Service. You can specify the following protocol configuration options: Blue Coat Web Security Service REST API (recommended) Forwarded
API Username	The API user name that is used for authenticating with the Blue Coat Web Security Service. The API user name is configured through the Blue Coat Threat Pulse Portal.
Password	The password that is used for authenticating with the Blue Coat Web Security Service.
Confirm Password	The password that is used for authenticating with the Blue Coat Web Security Service.
Use Proxy	When you configure a proxy, all traffic for the log source travels through the proxy for QRadar to access the Blue Coat Web Security Service. Configure the **Proxy IP or Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Automatically Acquire Server Certificate(s)	Select **Yes** for QRadar to automatically download the server certificate and begin trusting the target server.
Recurrence	You can specify the frequency of data collection. The format is M/H/D for Minutes/Hours/Days. The default is 5 M.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.

Related tasks

"Adding a log source" on page 5
"Adding a DSM" on page 4

Configuring Blue Coat Web Security Service to communicate with QRadar

To collect events from Blue Coat Web Security Service, you must create an API key for IBM QRadar. If an API key exists, Blue Coat Web Security Service is already configured.

Procedure

1. Log in to the Blue Coat Threat Pulse portal.
2. Switch to **Service** mode.
3. Click **Account Maintenance** > **MDM, API Keys**.
4. Click **Add API key**, type a user name and password for the API key, and then click **Add**.

   You need the user name and password when you configure the log source for the API.

Blue Coat Web Security Service sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Blue Coat Web Security Service sample message when you use the Blue Coat Web Security REST API protocol

Important: Due to formatting, paste the message format into a text editor and then remove any carriage return or line feed characters.

```
source-log-file=cloud_26754_20190506090002.log.gz x-bluecoat-request-tenant-id=
26754    date=2019-05-06    time=09:03:
46    x-bluecoat-appliance-name="AA11-aaa1_test"    time-taken=13
    c-ip=10.10.10.11    cs-userdn=OS\
estUser    cs-auth-groups=-    x-exception-id=-    sc-filter-result=OBSERVED
cs-categories="Technology/Internet;Web Ads/Analytics"    cs(Referer)=-    sc-status=
200    s-action=TCP_NC_MISS    cs-method=GET    rs(Content-
Type)=application/json    cs-uri-scheme=https    cs-host=domain.test
cs-uri-port=443    cs-uri-path=/settings/v2.0/analog/ASAP_VES
cs-uri-query=?os=windows&osver=10.0.17134.1.amd64fre.rs4_release.180410-1804&deviceid=%1111
111111-9C67-47FB-AE69-111111111111%7D    cs-uri-extension=-    cs(User-Agent)="OneSet
tingsQuery"    s-ip=192.168.15.66    sc-bytes=835    cs-bytes=255    x-data-leak
-detected=-    x-virus-id=-    x-bluecoat-location-id=0    x-bluecoat-location-name
="client"    x-bluecoat-access-type=client_connector    x-bluecoat-application-name="
-"    x-bluecoat-application-operation="-"    r-ip=10.10.10.
12    r-supplier-country="Ireland"    x-rs-certificate-validate-status=CERT_VALID
x-rs-certificate-observed-errors=none    x-cs-ocsp-error=-    x-rs-ocsp-error=-
x-rs-connection-negotiated-ssl-version=TLSv1.2    x-rs-connection-negotiated-cipher=ECDHE
-RSA-AES128-GCM-SHA256    x-rs-connection-negotiated-cipher-size=128    x-rs-certifica
te-hostname=domain.test    x-rs-certificate-hostname-categories="Technology/Internet;Web
Ads/Analytics"    x-cs-connection-negotiated-ssl-version=TLSv1.2    x-cs-connection-ne
gotiated-cipher=ECDHE-RSA-AES256-GCM-SHA384    x-cs-connection-negotiated-cipher-size=
256    x-cs-certificate-subject=-    cs-icap-status=ICAP_NOT_SCANNED    cs-icap-e
rror-details=-    rs-icap-status=ICAP_NOT_SCANNED    rs-icap-error-details=-
s-supplier-ip=10.10.10.12    s-supplier-country=-    s-supplier-failures=-
x-cs-client-ip-country="Test Country"    cs-threat-risk=-    x-rs-certificate-hostnam
e-threat-risk=unlicensed    x-client-agent-type=unified-agent    x-client-os=architec
ture=x86_64%20name=Windows%2010%20Enterprise%20version=10.0.17134    x-client-agent-sw=4
.10.3.225009    x-client-device-id=11111111-fcd7-4e60-b92b-111111111111    x-client-d
evice-name=TestName01    x-client-device-type=-    x-client-security-posture-details
=-    x-client-security-posture-risk-score=-    x-bluecoat-reference-id=-    x-sc
-connection-issuer-keyring=SSL_Intercept_1    x-sc-connection-issuer-keyring-alias=
-    x-cloud-rs=-    x-bluecoat-placeholder=-    cs(X-Requested-With)=-    x-b
luecoat-transaction-uuid=fdc8d949880e442a-000000000bda1726-000000005ccff872
```

Table 297. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**s-action** If the **s-action** field doesn't contain a valid value, the **cs-method** field is used.
Source IP	**c-ip**
Destination IP	**r-ip**
Destination Port	**cs-uri-port**
Device Time	**date** + **time**
Username	**cs-userdn**

Chapter 32. Box

The IBM QRadar DSM for Box collects enterprise events from a Box enterprise account.

The following table describes the specifications for the Box DSM:

Table 298. Box DSM specifications

Specification	**Value**
Manufacturer	Box
DSM name	Box
RPM file name	DSM-BoxBox-*QRadar_version-build_number*.noarch.rpm
Supported versions	N/A
Protocol	Box REST API
Event format	JSON
Recorded event types	Administrator and enterprise events Box Shield Alerts
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	For more information, see the Box link to the public site website (https://www.box.com/home).

To integrate Box with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website (https://www.ibm.com/support/fixcentral) onto your QRadar Console:
   - Protocol Common RPM
   - Box REST API Protocol RPM
   - Box DSM RPM
2. Configure your Box Enterprise account for API access. For more information, see your Box documentation (https://docs.box.com/docs/configuring-box-platform).
3. The following table describes the parameters that require specific values for Box event collection:

Table 299. Box log source parameters

Parameter	**Value**
Log Source type	Box
Protocol Configuration	Box REST API
Client ID	Generated in the **OAuth2 parameters** pane of the Box administrator configuration.
Client Secret	Generated in the **OAuth2 parameters** pane of the Box administrator configuration.

Table 299. Box log source parameters (continued)	
Parameter	**Value**
Key ID	Generated in the **Public Key Management** pane after you submit the public key.
Enterprise ID	Used for access token request.
Private Key File Name	The private key file name in the `/opt/qradar/conf/trusted_certificates/box/` directory in QRadar.
Use Proxy	If QRadar accesses the Box API by using a proxy, select the **Use Proxy** checkbox. If the proxy requires authentication, configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, configure the **Proxy Server** and **Proxy Port** fields.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Recurrence	The time interval between log source queries to the Box API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 10 minutes.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Box to communicate with QRadar

To retrieve administrator logs from your Box enterprise account, configure Box and your IBM QRadar Console. You must have a Box developer account.

Before you begin

Generate a private and public RSAkey pair for the JSON Web Token (JWT) assertion.

Tip: If you are a QRadar on Cloud user and the Target Collector is either Console or Events Processor, you must open a case and upload the Private Key (in DER format). DevOps then adds that Private Key to `/opt/qradar/conf/trusted_certificates/box`.

1. Log in to the Console or Linux server that has an `openssl` command.
   - For a private key, type the following command:

     ```
     openssl genrsa -out box_private_key.pem 2048
     ```

   - For a public key, type the following command:

```
openssl rsa -pubout -in box_private_key.pem -out box_public_key.pem
```

2. Save a copy of the public key. You paste the contents of the public key into the **Add Public Key** text box when you configure Box for API access.
3. Convert the private key to DER by typing the following command on one line:

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in box_private_key.pem -out
box_private_key.der -nocrypt
```

4. Store the private key on your managed host in QRadar.
   a. Create a directory called "box" in the `/opt/qradar/conf/trusted_certificates/` directory in QRadar.
   b. Copy the private key `.DER` file to the `/opt/qradar/conf/trusted_certificates/box` directory that you created. Do not store the private key in any other location.
   c. Configure the log source by using only the file name of the private key file in the `/opt/qradar/conf/trusted_certificates/box` directory. Ensure that you type the file name correctly in the **Private Key File Name** field when you configure the log source.
5. Copy the private key to the `/opt/qradar/conf/trusted_certificates/box` directory.

   Tip: If you configure the log source before you store the private key, an error message is displayed.

Procedure

1. Create and configure an application for your QRadar appliance.
   a) Log in to the Box **Developers** portal (http://developers.box.com/). You now have access to the Admin and Box Consoles.
   b) Click **Create New App** > **Custom App**.
   c) In the **Custom App** window, select **Server Authentication (with JWT)**.
   d) In the **App Name** field, type a name for the app, and then click **Create App**.
   e) On the **Configuration** tab, from the **OAuth2 Credentials** row, record the **Client ID** and the **Client Secret**. You need the **Client ID** and the **Client Secret** when you add a log source in QRadar.
   f) In the **App Access Level** row, select **App + Enterprise Access**.
   g) In the **Application Scopes** row, configure the following parameters.

Table 300. Application Scopes parameters

Parameter	Value
Content Actions	Ensure that the **Read all files and folders stored in Box** and **Write all files and folders stored in Box** checkboxes are selected.
Administrative Actions	Ensure that the **Manage enterprise properties** checkbox is selected. Ensure that the **Manage users**, **Manage groups**, and **Manage retention policies** checkboxes are cleared.
Developer Actions	Ensure that all the checkboxes are cleared.

   h) In the **Add and Manage Public Keys** row, click **Add a Public Key**.
   i) Open the public key file that you copied from QRadar. In the **Add a new Public Key** window, paste the contents of the public key file in the **Public Key** field.
   j) Click **Verify and Save**, and then record the **Key ID**. You need the **Key ID** when you add the log source in QRadar.

k) To ensure that the properties are stored on the server, click **Save Changes**.

A `Successfully updated the app.` message is displayed.

2. To submit the app, on the **Authorization** tab, click **Review and Submit**.
3. In the **Review App Authorization Submission** window, click **Submit**.
4. Locate your Box Enterprise ID.
   a) Log in to the Admin Console, and then click **Account & Billing** > **Enterprise ID**.
   b) Click the **Account Info** tab and record your Box **`Enterprise ID`**.
5. Authorize your application.
   a) Log in to the Box Console.
   b) From the navigation menu, click **Apps**.
   c) On the **Custom Apps Manager** tab, find your app and click **More** (**...**).
   d) In the **Authorize App** window, verify that the **`Application Access`** level is **All Users** and that the API key is the **Client ID** that you recorded, and then click **Authorize**.

   If your app is configured correctly, the **`Authorization Status`** displays as **Authorized** and the **`Enablement Status`** displays as **Enabled**.

For more information about configuring Box, see Applications (https://developer.box.com/guides/applications/).

What to do next

Verify that QRadar is configured to receive events from your Box DSM. If QRadar is configured correctly, no error messages appear in the **Edit a log source** window.

Box sample event messages

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Box sample messages when you use the Box REST protocol

Sample 1: The following sample event message shows that the user *User Name*, from IP address *10.0.0.1*, added an application key to Box.

```
{"source":
{"type":"application","name":"QRadarBox","api_key":"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"},"created_
by":{"type":"user","id":"262196057","name":"User
Name","login":"user.name@domain.test"},"created_at":"2016-02-10T07:49:07-08:00","event_id":"4037
02014","event_type":"APPLICATION_PUBLIC_KEY_ADDED","ip_address":"10.0.0.1","type":"event","sessi
on_id":null,"additional_details":null}
```

Table 301. Highlighted fields

QRadar field name	Highlighted payload field name
Username	**`name`**
Device Time	**`created_at`**
Event ID	**`event_type`**
Source IP Address	**`ip_address`**

Sample 2: The following sample event message shows that a `Suspicious Location` alert was generated based on `Download` activity by the user *Some name*.

```
{"source":null,"created_by":{"type":"user","id":"2","name":"Unknown
User","login":""},"action_by":null,"created_at":"2019-12-20T11:38:56-08:00","event_id":"97f1b31f
```

```
-f143-4777-81f8-1b557b39ca33","event_type":"SHIELD_ALERT","ip_address":"10.1.2.3","type":"event"
,"session_id":null,"additional_details":{"shield_alert":{"rule_category":"Suspicious
Locations","rule_id":"123","rule_name":"Suspicious Location","risk_score":60,"alert_summary":
{"alert_activities":
[{"occurred_at":"2019-12-20T11:37:05-08:00","event_type":"Download","item_name":"xyz.txt","item_
type":"file","item_id":"127","item_path":"ABC/DEF","ip_info":
{"ip":"10.2.3.4","latitude":"44.9727","longitude":"-65.8609","registrant":"Registrant Company
Name","country_code":"CA","city_name":"Saint John","region_name":"New
Brunswick"},"service_name":"Box Excel Online
Previewer"}]},"alert_id":2398,"priority":"medium","user":{"id":2320,"name":"Some
name","email":"some@domain.test"},"link":"https://app.box.com/master/shield/alerts/
123412341234","created_at":"2019-12-20T11:37:15-08:00"}}}
```


Table 302. Highlighted fields

QRadar field name	Highlighted payload field name
Device Time	**created_at**
Source IP Address	**ip_address**
Event ID	**rule_category** When the **event_type** value is **SHIELD_ALERT**, a Box Shield alert is indicated and the **rule_category** field is used for the **Event ID**.
Severity	**risk_score** The **risk_score** field severity value range is 1 - 100. In QRadar, the severity value range is 1 - 10. QRadar divides the **risk_score** field severity value by 10, and then rounds it to the nearest integer.
Username	**name**

Chapter 33. Bridgewater

The Bridgewater Systems DSM for IBM QRadar accepts events by using syslog.

QRadar records all relevant events that are forwarded from Bridgewater AAA Service Controller devices by using syslog.

Configuring Syslog for your Bridgewater Systems Device

You must configure your Bridgewater Systems appliance to send syslog events to IBM QRadar.

Procedure

1. Log in to your Bridgewater Systems device command-line interface (CLI).
2. To log operational messages to the RADIUS and Diameter servers, open the following file:

   `/etc/syslog.conf`
3. To log all operational messages, uncomment the following line:

   `local1.info /WideSpan/logs/oplog`
4. To log error messages only, change the `local1.info /WideSpan/logs/oplog` line to the following line:

   `local1.err /WideSpan/logs/oplog`

   Note: RADIUS and Diameter system messages are stored in the `/var/adm/messages` file.
5. Add the following line:

   `local1.*@`<*IP address*>

   Where <*IP address*> is the IP address your QRadar Console.
6. The RADIUS and Diameter server system messages are stored in the `/var/adm/messages` file. Add the following line for the system messages:

   <*facility*>`*@`<*IP address*>

   Where:

   <*facility*> is the facility that is used for logging to the `/var/adm/messages` file.

   <*IP address*> is the IP address of your QRadar Console.
7. **Save** and exit the file.
8. Send a hang-up signal to the syslog daemon to make sure that all changes are enforced:

   ```
   kill -HUP `cat /var/run/syslog.pid`
   ```

   The configuration is complete. The log source is added to QRadar as Bridgewater Systems appliance events are automatically discovered. Events that are forwarded to QRadar by your Bridgewater Systems appliance are displayed on the **Log Activity** tab.

Syslog log source parameters for Bridgewater Systems

If QRadar does not automatically detect the log source, add a Bridgewater Systems log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Bridgewater:

Table 303. Syslog log source parameters for the Bridgewater Systems DSM	
Parameter	**Value**
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	**Bridgewater Systems AAA Service Controller**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Bridgewater Systems appliance.

Related tasks

“Adding a log source” on page 5

Chapter 34. Broadcom

Broadcom is formerly known as CA Technologies. The name remains as CA Technologies in QRadar

IBM QRadar supports a number of Broadcom DSMs.

Broadcom CA ACF2

Broadcom CA ACF2 is formerly known as CA Technologies ACF2. The name remains CA ACF2 in QRadar.

The Broadcom CA Access Control Facility (ACF2) DSM collects events from a Broadcom CA ACF2 image on an IBM z/OS mainframe by using IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect CA ACF2 events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html) .
2. Configure your IBM z/OS image to write events in LEEF format. For more information, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).
3. Create a log source in QRadar for CA ACF2.
4. If you want to create a custom event property for CA ACF2 in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS® image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.

- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zSecureV240sc275638?OpenDocument).

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS®
- IBM RACF®
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

Table 304. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Log File log source parameter

If QRadar does not automatically detect the log source, add a IBM z/OS, IBM CICS, IBM RACF, IBM DB2, Broadcom CA Top Secret, or Broadcom CA ACF2 log source on the QRadar Console by using the Log File Protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, or CA ACF2:

Table 305. Log File log source parameters

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	Select your DSM name.
Protocol Configuration	**Log File**

Table 305. Log File log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.
Service Type	From the **Service Type** list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535. The options include ports: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.

Table 305. Log File log source parameters (continued)

Parameter	Value
Remote User	Type the user name or user ID necessary to log in to the system that contains your event files. • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length. • If your log files are on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <*product_name*>.<*timestamp*>.gz The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with z0S and end with .gz, type the following code: z0S.*\.gz Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions (https://docs.oracle.com/javase/tutorial/essential/regex/).

Table 305. Log File log source parameters (continued)	
Parameter	**Value**
FTP Transfer Mode	This option displays only if you select **FTP** as the **Service Type**. From the list, select **Binary**. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as `zip`, `gzip`, `tar`, or `tar+gzip` archive files.
SCP Remote File	If you select **SCP** as the **Service Type** you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type `00:00` to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	If you want the Log File protocol to run immediately after you click **Save**, select this check box. After the **Run On Save** completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.

Table 305. Log File log source parameters (continued)	
Parameter	**Value**
Processor	From the list, select **gzip**. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is previously processed by the Log File protocol. If a previously processed file is detected, the Log File protocol does not download the file for processing. All files that are not previously processed are downloaded. This option applies only to FTP and SFTP service types.
Change Local Directory?	Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the **Local Directory** field is displayed, which gives you the option to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select **LineByLine**. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

"Adding a log source" on page 5

Integrate Broadcom CA ACF2 with IBM QRadar by using audit scripts

The Broadcom CA Access Control Facility (ACF2) DSM collects events and audit transactions on the IBM mainframe with the Log File protocol.

`QexACF2.load.trs` is a TERSED file that contains a PDS loadlib with the QEXACF2 program. A TERSED file is similar to a zip file and requires you to use the TRSMAIN program to decompress the contents. The TRSMAIN program is available from IBM Support (www.ibm.com/support).

To upload a TRS file from a workstation, you must preallocate a file with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL= 1024, BLKSIZE=6144. The file transfer type must be BINARY APPEND. If the transfer type is TEXT or TEXT APPEND, then the file cannot decompress properly.

After you upload the file to the mainframe into the allocated dataset, the TERSED file can be UNPACKED with the TRSMAIN utility by using the sample JCL also included in the tar package. A return code of 0008 from the TRSMAIN utility indicates that the dataset is not recognized as a valid TERSED file. This code

(0008) error might be the result of the file not being uploaded to the mainframe with the correct DCB attributes, or because the transfer was not performed with the BINARY APPEND transfer mechanism.

After you have successfully UNPACKED the loadlib file, you can run the QEXACF2 program with the sample JCL file. The sample JCL file is contained in the tar collection. To run the QEXACF2 program, you must modify the JCL to your local naming conventions and JOB card requirements. You might also need to use the STEPLIB DD if the program is not placed in a LINKLISTED library.

To integrate CA ACF2 events into IBM QRadar:

1. The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.
2. The CA ACF2 data is extracted from the live repository with the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.
3. The `QexACF2.load.trs` program pulls data from the SMF formatted file. The `QexACF2.load.trs` program pulls only the relevant events and fields for QRadar and writes that information in a compressed format for compatibility. The information is saved in a location accessible by QRadar.
4. QRadar uses the Log File protocol source to retrieve the output file information on a scheduled basis. QRadar then imports and processes this file.

Configuring Broadcom CA ACF2 that uses audit scripts to integrate with IBM QRadar

IBM QRadar uses scripts to audit events from Broadcom CA ACF2 installations, which are collected by using the log file protocol.

Procedure

1. From the IBM support website (http://www.ibm.com/support), download the following compressed file:

   `qexacf2_bundled.tar.gz`
2. On a Linux operating system, extract the file:

   `tar -zxvf qexacf2_bundled.tar.gz`

   The following files are contained in the archive:

   - `QexACF2.JCL.txt` - Job Control Language file
   - `QexACF2.load.trs` - Compressed program library (requires IBM TRSMAIN)
   - `trsmain sample JCL.txt` - Job Control Language for TRSMAIN to decompress the `.trs` file
3. Load the files onto the IBM mainframe by using the following methods:

   Upload the sample `QexACF2_trsmain_JCL.txt` and `QexACF2.JCL.txt` files by using the TEXT protocol.
4. Upload the `QexACF2.load.trs` file by using a BINARY mode transfer and append to a preallocated data set. The `QexACF2.load.trs` file is a tersed file that contains the executable file (the mainframe program `QexACF2`). When you upload the `.trs` file from a workstation, preallocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

   Note: `QexACF2` is a small C mainframe program that reads the output of the TSSUTIL (EARLOUT data) line by line. `QexACF2` adds a header to each record that contains event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for QRadar and the blank suppression reduces network traffic to QRadar. This program does not consume CPU or I/O disk resources.
5. Customize the `trsmain sample_JCL.txt` file according to your installation-specific parameters.

Example: Jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

The `trsmain sample_JCL.txt` file uses the IBM utility TRSMAIN to extract the program that is stored in the `QexACF2.load.trs` file.

An example of the `QexACF2_trsmain_JCL.txt` file includes the following information:

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14
//D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXACF2.LOAD.TRS
// UNIT=SYSDA,
// SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE DD DISP=SHR,DSN=<yourhlq>.QEXACF2.LOAD.TRS
//OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD,
// SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
//
```

The `.trs` input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the QexACF2 program as a member.

6. You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in LINKLST. The program does not require authorization.
7. After you upload, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct data set name of the library that will contain the program.
8. The `QexACF2_jcl.txt` file is a text file that contains a sample JCL. You must configure the job card to meet your configuration.

   The `QexACF2_jcl.txt` sample file includes:

```
//QEXACF2 JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXACF2 JCL VERSION 1.0 OCTOBER, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
```

```
//QEXACF2 JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXACF2 JCL VERSION 1.0 OCTOBER, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
//*************************************************************
//SET1 SET SMFIN='MVS1.SMF.RECORDS(0)',
// QEXOUT='Q1JACK.QEXACF2.OUTPUT',
// SMFOUT='Q1JACK.ACF2.DATA'
//*************************************************************
//* Delete old datasets *
//*************************************************************
//DEL EXEC PGM=IEFBR14
//DD1 DD DISP=(MOD,DELETE),DSN=&SMFOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//DD2 DD DISP=(MOD,DELETE),DSN=&QEXOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset *
//*************************************************************
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&QEXOUT,
// SPACE=(CYL,(100,100)),
```

```
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute ACFRPTPP (Report Preprocessor GRO) to extract ACF2*
//* SMF records *
//*************************************************************
//PRESCAN EXEC PGM=ACFRPTPP
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//RECMAN1 DD DISP=SHR,DSN=&SMFIN
//SMFFLT DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
// DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
// UNIT=SYSALLDA
//*************************************************************
//* execute QEXACF2 *
//*************************************************************
//EXTRACT EXEC PGM=QEXACF2,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
```

```
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CFG DD DUMMY
//ACFIN DD DISP=SHR,DSN=&SMFOUT
//ACFOUT DD DISP=SHR,DSN=&QEXOUT
//*************************************************************
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//*
```

9. After the output file is created, schedule a job to a transfer the output file to an interim FTP server. The output file is forwarded to an interim FTP server.

   You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

   Example:

   ```
   //FTP EXEC PGM=FTP,REGION=3800K
   //INPUT DD *
   <IPADDR>
   <USER>
   <PASSWORD>
   PUT '<ACFOUT' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
   QUIT
   //OUTPUT DD SYSOUT=*
   //SYSPRINT DD SYSOUT=*
   ```

   Where:

   <*IPADDR*> is the IP address or host name of the interim FTP server to receive the output file.

   <*USER*> is the user name that is needed to access the interim FTP server.

   <*PASSWORD*> is the password that is needed to access the interim FTP server.

   <*THEIPOFTHEMAINFRAMEDEVICE*> is the destination of the mainframe or interim FTP server that receives the output.

   Example:

   ```
   PUT 'xxxxxx.xxxxxxx.OUTPUT.C320' /<IP_address>/ACF2/QEXACF2.OUTPUT.C320
   ```

   <QEXOUTDSN> is the name of the output file that is saved to the interim FTP server.

   You are now ready to configure the Log File protocol.
10. Schedule QRadar to retrieve the output file from CA ACF2.

If the zOS platform is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is needed and QRadar can pull the output file directly from the mainframe. The following text must be commented out using `//*` or deleted from the `QexACF2_jcl.txt file`:

```
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<ACFOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<ACFOUT>
QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

What to do next

You are now ready to configure the log source in QRadar.

Broadcom CA Top Secret

Broadcom CA Top Secret is formerly known as CA Technologies Top Secret. The name remains CA Top Secret in QRadar.

The Broadcom CA Top Secret DSM collects events from a Broadcom CA Top Secret image on an IBM z/OS mainframe by using IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect CA Top Secret events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements.
   For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html) .
2. Configure your IBM z/OS image to write events in LEEF format. For more information, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).
3. Create a log source in QRadar for CA Top Secret.
4. If you want to create a custom event property for CA Top Secret in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the

INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)

- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zSecureV240sc275638?OpenDocument).

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Log File log source parameter

If QRadar does not automatically detect the log source, add a IBM z/OS, IBM CICS, IBM RACF, IBM DB2, Broadcom CA Top Secret, or Broadcom CA ACF2 log source on the QRadar Console by using the Log File Protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, or CA ACF2:

Table 306. Log File log source parameters

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	Select your DSM name.
Protocol Configuration	**Log File**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.

Table 306. Log File log source parameters (continued)	
Parameter	**Value**
Service Type	From the **Service Type** list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535. The options include ports: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.
Remote User	Type the user name or user ID necessary to log in to the system that contains your event files. • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length. • If your log files are on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.

Table 306. Log File log source parameters (continued)	
Parameter	**Value**
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <*product_name*>.<*timestamp*>.gz The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with z0S and end with .gz, type the following code: z0S.*\.gz Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions (https://docs.oracle.com/javase/tutorial/essential/regex/).
FTP Transfer Mode	This option displays only if you select **FTP** as the **Service Type**. From the list, select **Binary**. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select **SCP** as the **Service Type** you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.

Table 306. Log File log source parameters (continued)

Parameter	Value
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	If you want the Log File protocol to run immediately after you click **Save**, select this check box. After the **Run On Save** completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is previously processed by the Log File protocol. If a previously processed file is detected, the Log File protocol does not download the file for processing. All files that are not previously processed are downloaded. This option applies only to FTP and SFTP service types.

Table 306. Log File log source parameters (continued)	
Parameter	**Value**
Change Local Directory?	Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the **Local Directory** field is displayed, which gives you the option to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select **LineByLine**. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

"Adding a log source" on page 5

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

Table 307. Log source parameters	
Parameter	**Value**
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Integrate Broadcom CA Top Secret with IBM QRadar by using audit scripts

The Broadcom CA Top Secret DSM collects events and audit transactions on the IBM mainframe with the Log File protocol.

IBM QRadar records all relevant and available information from the event.

To integrate CA Top Secret events into QRadar:

1. The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.
2. At midnight, the CA Top Secret data is extracted from the live repository by using the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.
3. The `qextopsloadlib` program pulls data from the SMF formatted file. The `qextopsloadlib` program only pulls the relevant events and fields for QRadar and writes that information in a condensed format for compatibility. The information is saved in a location accessible by QRadar.
4. QRadar uses the Log File protocol source to retrieve the output file information on a scheduled basis. QRadar then imports and processes this file.

Configuring Broadcom CA Top Secret that uses audit scripts to integrate with IBM QRadar

The Broadcom CA Top Secret DSM collects events and audit transactions on the IBM mainframe by using the Log File protocol.

Procedure

1. From the IBM support website (http://www.ibm.com/support), download the following compressed file:

   `qextops_bundled.tar.gz`
2. On a Linux operating system, extract the file:

   `tar -zxvf qextops_bundled.tar.gz`

   The following files are contained in the archive:

   - `qextops_jcl.txt`
   - `qextopsloadlib.trs`
   - `qextops_trsmain_JCL.txt`
3. Load the files onto the IBM mainframe by using any terminal emulator file transfer method.

   Upload the sample `qextops_trsmain_JCL.txt` and `qextops_jcl.txt` files by using the TEXT protocol.
4. Upload the `qextopsloadlib.trs` file by using a BINARY mode transfer. The `qextopsloadlib.trs` file is a tersed file that contains the executable (the mainframe program qextops). When you upload the `.trs` file from a workstation, preallocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

   Note: `Qextops` is a small C mainframe program that reads the output of the TSSUTIL (EARLOUT data) line by line. `Qextops` adds a header to each record that contains event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for QRadar and the blank suppression reduces network traffic to QRadar. This program does not consume CPU or I/O disk resources.
5. Customize the `qextops_trsmain_JCL.txt` file according to your installation-specific requirements.

   The `qextops_trsmain_JCL.txt` file uses the IBM utility TRSMAIN to extract the program that is stored in the `qextopsloadlib.trs` file.

   An example of the `qextops_trsmain_JCL.txt` file includes:

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14
```

```
//D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXTOPS.TRS
// UNIT=SYSDA,
// SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE DD DISP=SHR,DSN=<yourhlq>.QEXTOPS.TRS
//OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD,
// SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA
//
```

You must update the file with your installation specific information for parameters, such as, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

The `.trs` input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the `qextops` program as a member.

6. You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in the LINKLST. The program does not require authorization.
7. Following the upload, copy the program to an existing link listed library or add a STEPLIB DD statement with the correct data set name of the library that contains the program.
8. The `qextops_jcl.txt` file is a text file that contains a sample JCL. You must configure the job card to meet your configuration.

   The `qextops_jcl.txt` sample file includes:

```
//QEXTOPS JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M
//*
//*QEXTOPS JCL version 1.0 September, 2010
//*
//*************************************************************
//* Change below dataset names to sites specific datasets names*
//*************************************************************
//SET1 SET TSSOUT='Q1JACK.EARLOUT.ALL',
// EARLOUT='Q1JACK.QEXTOPS.PROGRAM.OUTPUT'
//*************************************************************
//* Delete old datasets *
//*************************************************************//
```

```
DEL EXEC PGM=IEFBR14
//DD1 DD DISP=(MOD,DELETE),DSN=&TSSOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//DD2 DD DISP=(MOD,DELETE),DSN=&EARLOUT,
// UNIT=SYSDA,
// SPACE=(CYL,(10,10)),
// DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset *
//*************************************************************
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&EARLOUT,
// SPACE=(CYL,(100,100)),
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute Top Secret TSSUTIL utility to extract smf records*
//*************************************************************
//REPORT EXEC PGM=TSSUTIL
//SMFIN DD DISP=SHR,DSN=&SMFIN1
//SMFIN1 DD DISP=SHR,DSN=&SMFIN2
//UTILOUT DD DSN=&UTILOUT,
// DISP=(,CATLG),UNIT=SYSDA,SPACE=(CYL,(50,10),RLSE),
// DCB=(RECFM=FB,LRECL=133,BLKSIZE=0)
//EARLOUT DD DSN=&TSSOUT,
// DISP=(NEW,CATLG),UNIT=SYSDA,
// SPACE=(CYL,(200,100),RLSE),
// DCB=(RECFM=VB,LRECL=456,BLKSIZE=27816)
//UTILIN DD *
NOLEGEND
REPORT EVENT(ALL) END
/*
```

```
//*************************************************************
//EXTRACT EXEC PGM=QEXTOPS,DYNAMNBR=10,
// TIME=1440
//STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//CFG DD DUMMY
//EARLIN DD DISP=SHR,DSN=&TSSOUT
//EARLOUT DD DISP=SHR,DSN=&EARLOUT
//*************************************************************
//FTP EXEC PGM=FTP,REGION=3800K
//INPUT DD *
<IPADDR>
<USER>
<PASSWORD>
PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<QUIT
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

9. After the output file is created, schedule a job to a transfer the output file to an interim FTP server. The output file is forwarded to an interim FTP server.

   You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

   Example:

   ```
   //FTP EXEC PGM=FTP,REGION=3800K
   //INPUT DD *
   <IPADDR>
   <USER>
   <PASSWORD>
   PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
   QUIT
   //OUTPUT DD SYSOUT=*
   //SYSPRINT DD SYSOUT=*
   ```

   Where:

   <*IPADDR*> is the IP address or host name of the interim FTP server to receive the output file.

   <*USER*> is the user name that is needed to access the interim FTP server.

   <*PASSWORD*> is the password that is needed to access the interim FTP server.

   <*THEIPOFTHEMAINFRAMEDEVICE*> is the destination of the mainframe or interim FTP server that receives the output.

   Example:

   ```
   PUT 'xxxxxx.xxxxxxx.OUTPUT.C320' /<IP_address>/CA/QEXTOPS.OUTPUT.C320
   ```

   <QEXOUTDSN> is the name of the output file that is saved to the interim FTP server.

   You are now ready to configure the Log File protocol.

10. Schedule QRadar to collect the output file from CA Top Secret.

    If the zOS platform is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is needed and QRadar can pull the output file directly from the mainframe. The following text must be commented out using `//*` or deleted from the `qextops_jcl.txt file`:

    ```
    //FTP EXEC PGM=FTP,REGION=3800K
    //INPUT DD *
    <IPADDR>
    <USER>
    <PASSWORD>
    PUT '<EARLOUT>' EARL_<THEIPOFTHEMAINFRAMEDEVICE>/<EARLOUT>
    QUIT
    //OUTPUT DD SYSOUT=*
    //SYSPRINT DD SYSOUT=*
    ```

What to do next

You are now ready to configure the log source in QRadar.

Broadcom Symantec SiteMinder

Broadcom Symantec SiteMinder is formerly known as CA SiteMinder. The name remains as CA SiteMinder in QRadar

The IBM QRadar Symantec SiteMinder DSM collects syslog-ng events from Symantec SiteMinder appliances.

The Symantec SiteMinder DSM collects access and authorization events that are logged in the `smaccess.log` file, then forwards the events to IBM QRadar by using syslog-ng.

To integrate Symantec SiteMinder with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the CA SiteMinder DSM RPM from the IBM support website (https://www.ibm.com/support).
2. Configure your Symantec SiteMinder appliance to send events to QRadar. For more information, see Configuring syslog-ng for Symantec SiteMinder.
3. Add a Symantec SiteMinder log source on the QRadar Console.

Broadcom Symantec SiteMinder DSM specifications

When you configure the Broadcom Symantec SiteMinder DSM, understanding the specifications for the Broadcom Symantec SiteMinder DSM can help ensure a successful integration. For example, knowing what the supported version of Broadcom Symantec SiteMinder is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Symantec SiteMinder DSM.

Table 308. Symantec SiteMinder DSM specifications

Specification	**Value**
Manufacturer	Broadcom
DSM name	CA SiteMinder
RPM file name	`DSM-`*`CASiteMinder-QRadar_version-build_number`*`.noarch.rpm`
Supported version	SiteMinder 12.8
Protocol	Syslog, Log File
Event format	Syslog
Recorded event types	All events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Symantec SiteMinder documentation (https://www.broadcom.com/products/cyber-security/identity/siteminder)

Syslog log source parameters for Broadcom Symantec SiteMinder

If QRadar does not automatically detect the log source, add a Broadcom Symantec SiteMinder log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Symantec SiteMinder:

Table 309. Syslog log source parameters for the Symantec SiteMinder DSM

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	**CA SiteMinder**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for your Symantec SiteMinder appliance.
Enabled	Select this check box to enable the log source. By default, this check box is selected.
Credibility	From the list, type the credibility value of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source device. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value that is configured in the **Coalescing Events** list in the **System Settings** window, which is accessible on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source that you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar *Administration Guide.*

Table 309. Syslog log source parameters for the Symantec SiteMinder DSM (continued)	
Parameter	**Value**
Store Event Payload	Select this check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** list in the **System Settings** window, which is accessible on the **Admin** tab. When you create a new log source or update the configuration for an automatically discovered log source that you can override the default value by configuring this check box for each log source. For more information, see the IBM QRadar *Administration Guide.*

Related tasks

"Adding a log source" on page 5

Configuring syslog-ng for Broadcom Symantec SiteMinder

You must configure your Broadcom Symantec SiteMinder appliance to forward syslog-ng events to your QRadar Console or Event Collector.

About this task

IBM QRadar can collect syslog-ng events from TCP or UDP syslog sources on port 514.

To configure syslog-ng for Symantec SiteMinder:

Procedure

1. Using SSH, log in to your Symantec SiteMinder appliance as a root user.
2. Edit the syslog-ng configuration file.

   `/etc/syslog-ng.conf`
3. Add the following information to specify the access log as the event file for syslog-ng:

```
source s_siteminder_access { file("/opt/apps/siteminder/sm66/siteminder/log/
smaccess.log"); };
```

4. Add the following information to specify the destination and message template:

```
destination d_remote_q1_siteminder {udp("<QRadar IP>" port(514) template ("$PROGRAM
$MSG\n"));};
```

   Where <*QRadar IP*> is the IP address of the QRadar Console or Event Collector.
5. Add the following log entry information:

```
log {source(s_siteminder_access);destination(d_remote_q1_siteminder);};
```

6. Save the `syslog-ng.conf` file.
7. Type the following command to restart syslog-ng:

   `service syslog-ng restart`

   After the syslog-ng service restarts, the Symantec SiteMinder configuration is complete. Events that are forwarded to QRadar by Symantec SiteMinder are displayed on the **Log Activity** tab.

Broadcom Symantec SiteMinder sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Symantec SiteMinder sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that authorization is accepted.

```
<173>Mar 11 15:53:54 ca.siteminder.test ca-siteminder [Auth][AuthAccept][][ca.siteminder.test]
[11/Mar/2021:15:53:45 -0500][31l-apache-aaaaa111-agent][A1aAaAAAAAaAa11aaaaAaaA1AAA=]
[CN=Test Useruser,OU=Standard,OU=Domain Users,DC=ad,DC=example,DC=com]
[01-00001a11-0111-1a1a-1111-11a111a10000][root-realm][01-000011aa-1111-111a-aaa1-111111a1a1aa]
[10.236.235.223][/aaaa/aaaAaaaAaaaaaAaaaaaaaaaa.jsp][GET][Production AD][plswa245:636
plswa246:636,plswa247:636 plswa245:636,prewa223:636 prewa224:636,prewa225:636
prewa223:636,prewa226:636 prewa227:636,plswa248:636 plswa248:636,plswa246:636
plswa247:636,prewa224:636 prewa225:636,prewa227:636 prewa226:636,plswa245:636
plswa246:636,plswa246:636 plswa247:636,plswa247:636 plswa245:636,prewa223:636
prewa224:636,prewa224:636 prewa225:636,prewa225:636 prewa223:636,prewa226:636
prewa227:636,prewa227:636 prewa226:636,plswa248:636 plswa248:636,plswa245:636
plswa246:636,prewa223:636 prewa224:636,prewa224:636 prewa225:636,prewa225:636
prewa223:636,prewa226:636 prewa227:636,prewa227:636 prewa226:636,plswa248:636 plswa248:636]
[LDAP:][idletime=3600;maxtime=7200;authlevel=5;][][http://aaaaa111.aaa.example.com-11][][][][][]
```

Table 310. Highlighted fields in the Symantec SiteMinder event

QRadar field name	Highlighted values in the event payload
Event ID	**AuthAccept**
Source IP	**10.236.235.223**
Username	**Test Useruser**
Log Source Time	**11/Mar/2021:15:53:45 -0500** (extracted from **date** and **time** fields)
Identity IP	**10.236.235.223**
Identity Username	**Test Useruser**

Sample 2: The following sample event message shows an authorization logout.

```
AuthLogout osand001 [24/May/2012:14:14:50 -0500] "10.6.172.171
uid=Testuser01TesTU@example.com,ou=people,ou=AAAA A AA-AAAAA LTD.,ou=dcp,dc=aaaaaa,dc=com"
"aaaa01aaa01-aaaa1  " [] [41]  [] []
```

Table 311. Highlighted fields in the Symantec SiteMinder event

QRadar field name	Highlighted values in the event payload
Event ID	**AuthLogout**
Source IP	**10.6.172.171**
Username	**Testuser01TesTU@example.com**
Log Source Time	**24/May/2012:14:14:50 -0500** (extracted from **date** and **time** fields)

Chapter 35. Brocade Fabric OS

IBM QRadar can collect and categorize syslog system and audit events from Brocade switches and appliances that use Fabric OS V7.x.

To collect syslog events, you must configure your switch to forward syslog events. Each switch or appliance must be configured to forward events.

Events that you forward from Brocade switches are automatically discovered. A log source is configured for each switch or appliance that forwards events to QRadar.

Configuring syslog for Brocade Fabric OS appliances

To collect events, you must configure syslog on your Brocade appliance to forward events to IBM QRadar.

Procedure

1. Log in to your appliance as an admin user.
2. To configure an address to forward syslog events, type the following command:

   `syslogdipadd <IP address>`

   Where *<IP address>* is the IP address of the QRadar Console, Event Processor, Event Collector, or all-in-one system.
3. To verify the address, type the following command:

   `syslogdipshow`

Results

As the Brocade switch generates events the switch forwards events to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded by the Brocade appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console and that the **Log Activity** tab displays events from the Brocade appliance.

Brocade Fabric OS sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Brocade Fabric OS sample message when you use the Syslog protocol

The following sample event shows that a simple network management protocol (SNMP) login occurred. An IP address is displayed when the login occurs over a remote connection.

```
<190>Nov  3 15:08:04 brocade.fabricos.test raslogd: AUDIT, 2020/11/03-15:08:04
(CET), [SNMP-3020], INFO, SECURITY, NONE/admin/NONE/None/CLI, aa_111/aaaaa_11/AAA 128,
7.4.2e, , , , , , , Event: Login, Info: SNMP login attempt via  IP: 10.236.171.12, Time: Tue Nov
3 15:08:01 2020
```


```
<190>Nov  3 15:08:04 brocade.fabricos.test raslogd: AUDIT, 2020/11/03-15:08:04
(CET), [SNMP-3020], INFO, SECURITY, NONE/admin/NONE/None/CLI, aa_111/aaaaa_11/AAA 128,
7.4.2e, , , , , , , Event: Login, Info: SNMP login attempt via  IP: 10.236.171.12, Time: Tue
Nov  3 15:08:01 2020
```

Table 312. Highlighted values in the Brocade Fabric OS event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**SNMP-3020**
Source IP	**10.236.171.12**

Chapter 36. Carbon Black

Several Carbon Black DSMs can be integrated with IBM QRadar

Carbon Black

The IBM QRadar DSM for Carbon Black collects endpoint protection events from a Carbon Black server.

The following table describes the specifications for the Carbon Black DSM:

Table 313. Carbon Black DSM specifications

Specification	Value
Manufacturer	Carbon Black
DSM name	Carbon Black
RPM file name	`DSM-CarbonBlackCarbonBlack-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	5.1 and later
Protocol	Syslog
Recorded event types	Watchlist hits
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Carbon Black website (https://www.carbonblack.com/products/cb-response/)

To integrate Carbon Black with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Carbon Black DSM RPM
   - DSMCommon RPM
2. Configure your Carbon Black device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Carbon Black log source on the QRadar Console. The following table describes the parameters that require specific values for Carbon Black event collection:

   Table 314. Carbon Black log source parameters

Parameter	Value
Log Source type	Carbon Black
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Carbon Black to communicate with QRadar

To collect events from Carbon Black, you must install and configure cb-event-forwarder to send Carbon Black events to IBM QRadar.

Before you begin

Install the Carbon Black Enterprise RPM and ensure that it is running. You can install the cb-event-forwarder on any 64-bit Linux computer that is running CentOS 6.x. It can be installed on the same computer as the Carbon Black server, or on another computer. If you are forwarding many events, for example, all file modifications, registry modifications, or both, to QRadar, install `cb-event-forwarder` on a separate server. If you are not forwarding many events to QRadar, you can install the cb-event-forwarder on the Carbon Black server.

If you are installing the cb-event-forwarder on a computer other than the Carbon Black server, you must configure the Carbon Black server:

1. Ensure that TCP port 5004 is open through the iptables firewall on the Carbon Black server. The event-forwarder connects to TCP port 5004 on the Carbon Black server to connect to the Cb message bus.
2. Get the RabbitMQ user name and password from the `/etc/cb/cb.conf` file on the Carbon Black server. Search for the RabbitMQUser and RabbitMQPassword variables and note their values.

About this task

You can find the following instructions, source code, and quick start guide on the GitHub website (https://github.com/carbonblack/cb-event-forwarder/).

Procedure

1. If it is not already installed, install the CbOpenSource repository:

   ```
   cd /etc/yum.repos.dcurl -O https://opensource.carbonblack.com/release/x86_64/
   CbOpenSource.repo
   ```

2. Install the RPM for cb-event-forwarder:

   ```
   yum install cb-event-forwarder
   ```

3. Modify the `/etc/cb/integrations/event-forwarder/cb-event-forwarder.conf` file to include `udpout=<`*`QRadar_IP_address`*`>:514`, and then specify LEEF as the output format: `output_format=leef`.
4. If you are installing on a computer other than the Carbon Black server, copy the RabbitMQ user name and password into the *rabbit_mq_username* and *rabbit_mq_password* variables in the `/etc/cb/integrations/event-forwarder/cb-event-forwarder.conf` file. In the *cb_server_hostname* variable, enter the host name or IP address of the Carbon Black server.
5. Ensure that the configuration is valid by running the cb-event-forwarder in check mode:

   `/usr/share/cb/integrations/event-forwarder/cb-event-forwarder -check`.

   If valid, the message `Initialized output` displays. If there are errors, the errors are printed to your screen.
6. Choose the type of event that you want to capture.

   By default, Carbon Black publishes the all feed and watchlist events over the bus. If you want to capture raw sensor events or all binaryinfo notifications, you must enable those features in the `/etc/cb/cb.conf` file.

   - To capture raw sensor events, edit the `DatastoreBroadcastEventTypes` option in the `/etc/cb/cb.conf` file to enable broadcast of the raw sensor events that you want to export.

- To capture binary observed events, edit the `EnableSolrBinaryInfoNotifications` option in the `/etc/cb/cb.conf` file and set it to `True`.

7. If any variables were changed in `/etc/cb/cb.conf`, restart the Carbon Black server: "service cb-enterprise restart".
8. Start the cb-event-forwarder service by using the initctl command: `initctl start cb-event-forwarder`.

   Note: You can stop the cb-event-forwarder service by using the initctl command: `initctl stop cb-event-forwarder`.

Carbon Black sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Carbon Black sample message when you use the Syslog protocol

Sample 1: The following sample event message shows a watchlist query that is matching a process.

```
LEEF:1.0|CB|CB|5.1|alert.watchlist.hit.query.process|alert_severity=50.625
alert_type=watchlist.hit.query.process    alliance_score_srstrust=-100    cb_server=None
childproc_count=1    comms_ip=192.168.230.5    computer_name=W7-LOW
created_time=2015-10-29T04:33:06.713157Z    crossproc_count=0    feed_id=-1
feed_name=My Watchlists    feed_rating=3.0    filemod_count=0
group=Default Group    hostname=W7-LOW    interface_ip=192.168.230.5
ioc_attr={"highlights": ["PREPREPREacrord32.exePOSTPOSTPOST"]}    ioc_confidence=0.5
ioc_type=query    md5=AD7B9C14083B52BC532FBA5948342B98    modload_count=14
netconn_count=0    os_type=windows    process_guid=00000016-0000-0804-01d1-17153be2e8cd
process_name=cmd.exe    process_path=c:\windows\system32\cmd.exe    regmod_count=0
report_score=75    segment_id=1    sensor_criticality=3.0    sensor_id=22
status=Unresolved    timestamp=1446093201.95    type=alert.watchlist.hit.query.process
unique_id=3ee47556-3e8e-4232-b975-30ba7fbf0037    username=BIT9SEAD\user10
watchlist_id=11    watchlist_name=Unusual Parents
```

Table 315. Highlighted values in the Carbon Black sample event

QRadar field name	Highlighted field names or values in the event payload
Event ID	**alert.watchlist.hit.query.process**
Event Category	For this DSM, the value in QRadar is always **CarbonBlack**
Source IP	**interface_ip**
Username	**username**
Device time	**created_time**

Carbon Black Bit9 Parity

To collect events, you must configure your Carbon Black Bit9 Parity device to forward syslog events in Log Event Extended Format (LEEF).

Procedure

1. Log in to the Carbon Black Bit9 Parity console with Administrator or PowerUser privileges.
2. From the navigation menu on the left side of the console, select **Administration** > **System Configuration**.

   The **System Configuration** window is displayed.
3. Click **Server Status**.

   The **Server Status** window is displayed.

4. Click **Edit**.
5. In the **Syslog address** field, type the IP address of your QRadar Console or Event Collector.
6. From the **Syslog format** list, select **LEEF (Q1Labs)**.
7. Select the **Syslog enabled** check box.
8. Click **Update**.

   The configuration is complete. The log source is added to IBM QRadar as Carbon Black Bit9 Parity events are automatically discovered. Events that are forwarded to QRadar by Carbon Black Bit9 Parity are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Carbon Black Bit9 Parity

If QRadar does not automatically detect the log source, add a Carbon Black Bit9 Parity log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Carbon Black Bit9 Parity:

Table 316. Syslog log source parameters for the Carbon Black Bit9 Parity DSM

Parameter	Value
Log Source type	Carbon Black Bit9 Parity
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name for the Carbon Black Bit9 Parity device.

Related tasks

"Adding a log source" on page 5

Bit9 Security Platform

Use the IBM QRadar SIEM DSM for Carbon Black Bit9 Security Platform to collect events from Carbon Black Bit9 Parity devices.

The following table identifies the specifications for the Bit9 Security Platform DSM:

Table 317. DSM specifications for Bit9 Security Platform

Specification	Value
Manufacturer	Carbon Black
DSM name	Bit9 Security Platform
RPM file name	`DSM-Bit9Parity-build_number.noarch.rpm`
Supported versions	V6.0.2 and up
Event format	Syslog
Supported event types	All events
Automatically discovered?	Yes
Included identity?	Yes
More information	Bit9 website (http://www.bit9.com)

To integrate Bit9 Security Platform with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the Bit9 Security Platform DSM RPM.
2. Configure your Bit9 Security Platform device to enable communication with QRadar. You must create a syslog destination and forwarding policy on the Bit9 Security Platform device.
3. If QRadar does not automatically detect Bit9 Security Platform as a log source, create a Bit9 Security Platform log source on the QRadar Console. Use the following Bit9 Security Platform values to configure the log source parameters:

Parameter	Value
Log Source Identifier	The IP address or host name of the Bit9 Security Platform device
Log Source Type	Bit9 Security Platform
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Carbon Black Bit9 Security Platform to communicate with QRadar

Configure your Carbon Black Bit9 Security Platform device to forward events to IBM QRadar in LEEF format.

Procedure

1. Log in to the Carbon Black Bit9 Security Platform console with Administrator or PowerUser privileges.
2. From the navigation menu, select **Administration** > **System Configuration**.
3. Click **Server Status** and click **Edit**.
4. In the **Syslog address** field, type the IP address of your QRadar Console or Event Collector.
5. From the **Syslog format** list, select **LEEF (Q1Labs)**.
6. Select the **Syslog enabled** check box and click **Update**.

Chapter 37. Centrify Infrastructure Services

The IBM QRadar DSM for Centrify Infrastructure Services collects events from Centrify Infrastructure Services standard logs.

The following table describes the specifications for the Centrify Infrastructure Services DSM:

Table 318. Centrify Infrastructure Services DSM specifications

Specification	**Value**
Manufacturer	Centrify
DSM name	Centrify Infrastructure Services
RPM file name	`DSM-CentrifyInfrastructureServices-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	Centrify Infrastructure Services 2017
Protocol	Syslog, TLS Syslog and WinCollect
Event format	name-value pair (NVP)
Recorded event types	Audit Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Centrify website (https://www.centrify.com/support/documentation/server-suite/)

To integrate Centrify Infrastructure Services with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of Centrify Infrastructure Services DSM RPM on your QRadar Console.

   Note: If you use the WinCollect protocol configuration option, install the latest WinCollect agent bundle (`.sfs` file) on your QRadar Console.

2. To send syslog or Windows events to QRadar, configure your UNIX, Linux, or Windows device where the Centrify Infrastructure Services standard logs are available.

3. If QRadar does not automatically detect the log source, add a Centrify Infrastructure Services log source on the QRadar Console.

   The following table describes the parameters that require specific values to collect events from Centrify Infrastructure Services:

   Table 319. Centrify Infrastructure Services log source parameters

Parameter	**Value**
Log Source type	Centrify Infrastructure Services
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the UNIX, Linux, or Windows device that sends Centrify Infrastructure Services events to QRadar.

4. Optional: To add a Centrify Infrastructure Services log source to receive Syslog events from network devices that support TLS Syslog event forwarding, configure the log source on the QRadar Console to use the TLS Syslog protocol.

Table 320. Centrify Infrastructure Services TLS Syslog log source parameters	
Parameter	**Value**
Log Source type	Centrify Infrastructure Services
Protocol Configuration	TLS Syslog
Log Source Identifier	Type a unique identifier for the log source.
TLS Protocols	Select the version of TLS that is installed on the client.

Note: To receive encrypted Syslog events from up to 50 network devices that support TLS Syslog event forwarding, configure a log source to use the TLS Syslog protocol.

Related concepts

"TLS Syslog protocol configuration options" on page 227
Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring WinCollect agent to collect event logs from Centrify Infrastructure Services

You can forward Windows events to IBM QRadar by using WinCollect.

To forward Windows events by using WinCollect, install WinCollect agent on a Windows host. Download the WinCollect agent setup file from the IBM Support website (https://www.ibm.com/support). Add a Centrify Infrastructure Services log source and assign it to the WinCollect agent.

The following table describes the values that are required for the WinCollect log source parameters.

Table 321. WinCollect log source parameters	
Parameter	**Value**
Log Source type	Centrify Infrastructure Services
Protocol Configuration	WinCollect
Log Source Identifier	The IP address or host name of the Windows machine from which you want to collect Windows events. The log source identifier must be unique for the log source type.
Local System	Select the **Local System** check box to disable the remote collection of events for the log source. The log source uses local system credentials to collect and forward logs to QRadar. You need to configure the **Domain**, **Username**, and **Password** parameters if remote collection is required.

Table 321. WinCollect log source parameters (continued)	
Parameter	**Value**
Event Rate Tuning Profile	For the default polling interval of 3000 ms, the approximate Events per second (EPS) rates attainable are as follows: • Default (Endpoint): 33-50 EPS • Typical Server: 166-250 EPS • High Event Rate Server: 416-625 EPS For a polling interval of 1000 ms, the approximate EPS rates are as follows: • Default (Endpoint): 100-150 EPS • Typical Server: 500-750 EPS • High Event Rate Server: 1250-1875 EPS For more information about tuning WinCollect, go to the IBM Support website (http://www.ibm.com/support/docview.wss?uid=swg21672193).
Polling Interval (ms)	The interval, in milliseconds, between times when WinCollect polls for new events.
Application or Service Log Type	Select **None** for the **Application or Service Log Type**.
Standard Log Types	Do not enable the check box for any of the log types. Select **No Filtering** as the log filter type for the following log types: **Security**, **System**, **Application**, **DNS Server**, **File Replication Service**, and **Directory Service**.
Event Types	You must select at least one event type.

Table 321. WinCollect log source parameters (continued)	
Parameter	**Value**
XPath Query	To forward only Centrify Audit events, you must specify the XPath filter. The query is in XML format and can be created by using Custom View Properties of Microsoft Event Viewer. For more information about creating an XPath query, go to the Creating a custom view documentation on the IBM Support website (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.wincollect.doc/t_ug_wincollect_creating_customview.html). **Important:** When you create the custom view, ensure that the **By Source** option is selected. From the **Event sources** list, select the application name of the Centrify Audit Events. Example XPath query: `<QueryList>` `<Query Id="0" Path="Application">` `<SelectPath="Application">*[System` `[Provider[@Name='Centrify AuditTrail` `V2']]]</Select>` `</Query>` `</QueryList>`
Enable Active Directory Lookups	Do not select the check box.
WinCollect**Agent**	Select your WinCollect agent from the list.
Target Internal Destination	Use any managed host with an event processor component as an internal destination.

For more information about WinCollect log source parameters, go to the Common WinCollect log source parameters documentation on the IBM Support website (https://www.ibm.com/support/knowledgecenter/en/SS42VS_SHR/com.ibm.wincollect.doc/r_ug_wincollect_comon_parameters.html).

Configuring Centrify Infrastructure Services on a UNIX or Linux device to communicate with QRadar

You can configure your UNIX or Linux device to send audit events to IBM QRadar. The audit events are available locally in the syslog event logs where the Centrify Infrastructure Services is installed and configured.

Procedure

1. Log in to your Centrify Infrastructure Services device.
2. Ensure that syslog or rsyslog is installed:
   - To verify that syslog is installed, type `service syslog status`.
   - To verify that rsyslog is installed, type `service rsyslog status`.
3. If syslog or rsyslog is not installed, install them by using your preferred method based on your UNIX or Linux device. For example, you can type the following command to install rsyslog on a Linux device:

   ```
   yum install rsyslog
   ```

4. To forward events to your QRadar Event Collector, open the `rsyslog.conf` file or the `syslog.conf` file that is located in `/etc/` directory, and then add the following line:

   `:msg, contains, "AUDIT_TRAIL" @@<QRadar Event Collector IP>:514`

   Example: `:msg, contains, "AUDIT_TRAIL" @@127.0.0.1:514`
5. Restart the syslog or rsyslog service:

   - If you are using syslog, type `service syslog restart`.
   - If you are using rsyslog, type `service rsyslog restart`.

   Note: The Centrify Linux agent might forward some Linux system messages with the Audit Trail logs. If no specific category is found, the Linux OS log source type in QRadar discovers the Linux messages and normalizes them as stored.

Centrify Infrastructure Services sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table shows sample event messages from Centrify Infrastructure Services:

Table 322. Centrify Infrastructure Services sample message

Event name	Low-level category	Sample log message
Remote login success	Remote Access Login Succeeded	<13>May 09 20:58:48 127.1.1.1 AgentDevice=WindowsLog AgentLogFile=Application Plugin Version=7.2.6.39 Source=Centrify AuditTrail V2 Computer=Centrify WindowsAgent.Centrify.lab OriginatingComputer=127.1.1.1 User=user Domain =CENTRIFY EventID=1234 EventID Code=1234 EventType=4 Event Category=4 RecordNumber=1565 TimeGenerated=1494374321 TimeWritten=1494374321 Level=Informational Keywords= ClassicTask=None Opcode=Info Message=Product: Centrify Suite Category: Direct Authorize - Windows Event name: Remote login success Message: User successfully logged on remotely using role 'Windows Login/CentrifyTest'. May 09 16:58:41 centrifywindowsagent. centrify.lab dzagent[2008]: INFO AUDIT_TRAIL|Centrify Suite |DirectAuthorize - Windows| 1.0|3|Remote login success|5 |user=username userSid=domain \username sessionId=6 centrify EventID=6003 DAInst=N/A DASess ID=N/A role=Windows Login/ CentrifyTest desktopguid=7678b3 5e-00d0-4ddf-88f5-6626b8b1ec4b <13>May 09 20:58:48 127.1.1.1 AgentDevice=WindowsLog AgentLogFile=Application PluginVersion=7.2.6.39 Source=Centrify AuditTrail V2 Computer=CentrifyWindowsAgent.Centrify.l ab OriginatingComputer=127.1.1.1 User=user Domain=CENTRIFY EventID=1234 EventIDCode=1234 EventType=4 EventCategory=4 RecordNumber=1565 TimeGenerated=1494374321 TimeWritten=1494374321 Level=Informational Keywords=ClassicTask=None Opcode=Info Message=Product: Centrify Suite Category: DirectAuthorize - Windows Event name: Remote login success Message: User successfully logged on remotely using role 'Windows Login/ CentrifyTest'. May 09 16:58:41 centrifywindowsagent.centrify.lab dzagent[2008]: INFO AUDIT_TRAIL| Centrify Suite|DirectAuthorize - Windows|1.0|3|Remote login success|5| user=username userSid=domain\username sessionId=6 centrifyEventID=6003 DAInst=N/A DASessID=N/A role=Windows Login/CentrifyTest desktopguid=7678b35e-00d0-4ddf-88f5-6626 b8b1ec4b

Table 322. Centrify Infrastructure Services sample message (continued)

Event name	Low-level category	Sample log message
The user logged in to the system successfully	User Login Success	<38>May 4 23:45:19 hostname adclient[1472]: INFO AUDIT _TRAIL|Centrify Suite|Centrify Commands|1.0|200|The user login to the system successfully|5|user =user pid=1234 utc=1493952319951 centrifyEventID=18200 DASessID= c6b7551c-31ea-8743-b870- cdef47393d07 DAInst=Default Installation status=SUCCESS service =sshd tty=/dev/pts/2 <38>May 4 23:45:19 hostname adclient[1472]: INFO AUDIT_TRAIL| Centrify Suite|Centrify Commands|1.0| 200|The user login to the system successfully|5|user=user pid=1234 utc=1493952319951 centrifyEventID=18200 DASessID=c6b7551c-31ea-8743-b870- cdef47393d07 DAInst=DefaultInstallation status=SUCCESS service=sshd tty=/dev/pts/2

Chapter 38. Check Point

Several Check Point products can be integrated with IBM QRadar.

The following products are supported:

- Firewall
- SmartDefense
- IPS
- Anti Malware
- Anti-Bot
- Antivirus
- Mobile Access
- DDoS Protector
- Security Gateway/Management
- Threat Emulation
- URL Filtering
- DLP
- Application Control
- Identity Logging
- VPN
- Endpoint Security
- VPN-1 and FireWall-1

Depending on your Operating System, the procedures for the Check Point device might vary. The documented procedures are based on the Check Point SecurePlatform Operating system.

Integrate Check Point by using syslog

This section describes how to ensure that the IBM QRadar Check Point DSMs accept Check Point events by using syslog.

To configure Check Point to forward syslog events to IBM QRadar complete the following steps:

Important: If Check Point SmartCenter is installed on Microsoft Windows, you must integrate Check Point with QRadar by using OPSEC.

1. Type the following command to access the Check Point console as an expert user:

   ```
   expert
   ```

   A password prompt appears.
2. Type your expert console password. Press the Enter key.
3. Open the following file:

   ```
   /etc/rc.d/rc3.d/S99local
   ```
4. Add the following lines:

   ```
   $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority> /dev/null
   2>&1 &
   ```

   Where:

   - <*facility*> is a syslog facility, for example, local3.

- <*priority*> is a syslog priority, for example, info.

For example:

```
$FWDIR/bin/fw log -ftn | /usr/bin/logger -p local3.info > /dev/null 2>&1 &
```

5. Save and close the file.
6. Open the `syslog.conf` file.
7. Add the following line:

   <*facility*>.<*priority*> <TAB><TAB>@<*host*>

   Where:

   - <*facility*> is the syslog facility, for example, local3. This value must match the value that you typed in Step 4.
   - <*priority*> is the syslog priority, for example, info or notice. This value must match the value that you typed in Step 4.

   <TAB> indicates you must press the Tab key.

   <*host*> indicates the QRadar Console or managed host.
8. Save and close the file.
9. Enter the following command to restart syslog:
   - In Linux: `service syslog restart`
   - In Solaris: `/etc/init.d/syslog start`
10. Enter the following command:

    ```
    nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority>
    > /dev/null 2>&1 &
    ```

    Where:

    - <*facility*> is a Syslog facility, for example, local3. This value must match the value that you typed in Step 4.
    - <*priority*> is a Syslog priority, for example, info. This value must match the value that you typed in Step 4.

The configuration is complete. The log source is added to QRadar as Check Point syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Syslog log source parameters for Check Point

If QRadar does not automatically detect the log source, add a Check Point log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Check Point:

Table 323. Syslog log source parameters for the Check Point DSM

Parameter	Value
Log Source type	**Check Point**
Protocol Configuration	**Syslog**

Table 323. Syslog log source parameters for the Check Point DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Check Point devices.

Related tasks
Adding a log source

Syslog sample event messages for Check Point

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Check Point sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that a trusted connection is identified and marked as an elephant flow.

```
<13>Sep 30 07:13:59 checkpoint.checkpoint.test 30Sep2020 07:13:59
10.1.253.3 product: VPN-1 &FireWall-1; src: 10.3.5.15; s_port: 61172;
dst: 10.254.4.3; service: 53; proto: udp; rule:; policy_id_tag:
product=VPN-1 & FireWall-1[db_tag={666B9F89-D1F9-7848-B5FB- BF8D97B768F8};mgmt=fw-
mgmt;date=1601441138;policy_name=CBS_policy_Simplified_PlusDeskt];dst_machine_name: ***
Confidential ***;dst_user_name: *** Confidential ***;fw_message: Connection is
marked as trusted elephant flow. Use fastaccel tool to edit configuration
if needed.;has_accounting: 0;i/f_dir: inbound;is_first_for_luuid: 131072;logId:
-1;log_sequence_num: 11;log_type: log;log_version: 5;origin_sic_name: CN=x01_fw1,O=fw-
mgmt.cu.com.pl.8pjujj;snid: 0;src_machine_name: *** Confidential ***;src_user_name: ***
Confidential ***;user: *** Confidential ***;
```

Table 324. Highlighted values in the Check Point sample event	
QRadar field name	**Highlighted values in the event payload**
Username	***** Confidential *****
Source IP	**10.3.5.15**
Source port	**61172**
Destination IP	**10.254.4.3**
Destination port	**53**
Device time	**Sep 30 07:13:59**

Sample 2: The following sample event message shows that a user login is successful.

```
LEEF:2.0|Check Point|Linux OS|1.0|Log In|cat=Linux OS devTime=1539878943
usrName=cpaction=Log In ifdir=inbound loguid={0x5bc8b020,0x3,0x6a9610ac,0xee29cd8}
origin=172.16.150.106 sequencenum=4 version=5    application=su default_device_message=<86>su:
pam_unix(su:session):session opened for user cp_postgres by (uid\\=0)
facility=security/authorization messages login_status=succeeded product_category=OS
syslog_severity=Informational
```

Table 325. Highlighted values in the Check Point sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Log In succeeded**

Table 325. Highlighted values in the Check Point sample event (continued)	
QRadar field name	**Highlighted values in the event payload**
Event category	**Linux OS**
Username	**cp**
Source IP	**172.16.150.106**
Device time	**Oct 18 13:09:03 ADT**
Identity IP	**172.16.150.106**
Identity username	**cp**

Integrate Check Point by using OPSEC

This section describes how to ensure that IBM QRadar accepts Check Point events using Open Platform for Security (OPSEC/LEA).

To integrate Check Point OPSEC/LEA with QRadar, you must create two Secure Internal Communication (SIC) files and enter the information in to QRadar as a Check Point log source.

Check Point configuration overview

To integrate Check Point with QRadar, you must complete the following procedures in sequence:

1. Add QRadar as a host for Check Point.
2. Add an OPSEC application to Check Point.
3. Locate the Log Source Secure Internal Communications DN.
4. In QRadar, configure the OPSEC LEA protocol.
5. Verify the OPSEC/LEA communications configuration.

Adding a Check Point Host

You can add IBM QRadar as a host in Check Point SmartCenter:

Procedure

1. Log in to the Check Point SmartCenter user interface.
2. Select **Objects** > **New Host**.
3. Enter the information for your Check Point host:
   - **Object Name** - Specify a name for the host. For example, QRadar.
   - **IP address** - The IP address of QRadar
4. Click **OK**.

What to do next

Creating an OPSEC Application Object

Creating an OPSEC Application Object

After you add IBM QRadar as a host in Check Point SmartCenter, you can create the OPSEC Application Object.

Procedure

1. Open the Check Point SmartConsole user interface.

2. Select **Objects** > **More Object Types** > **Server** > **OPSEC Application** > **New Application**.
3. Configure your OPSEC Application:
   a) Configure the following **OPSEC Application Properties** parameters.

Table 326. OPSEC Application Properties	
Parameter	**Value**
Name	Specify a name for the OPSEC application. For example, QRadar-OPSEC
Host	QRadar
Client Entities	LEA

   b) Click **Communication**.
   c) In the **One-time password** field, type the password that you want to use.
   d) In the **Confirm one-time password** field, type the password that you used for **One-time password**.
   e) Click **Initialize**.
   f) Click **Close**.
4. Select **Menu** > **Install Policy**
5. Click **Publish & Install**.
6. Click **Install**.
7. Select **Menu** > **Install Database**.
8. Click **Install**.

   Note: The SIC value is required for the OPSEC Application Object SIC attribute parameter when you configure the Check Point log source in QRadar. The value can be found by viewing the OPSEC Application Object after it is created.

   The OPSEC Application Object resembles the following example:

```
CN=QRadar=OPSEC,0=cpmodule..tdfaaz
```

Results

If you have issues after you install the database policy, contact your system administrator to restart Check Point services on the central SmartCenter server that hosts the policy files. After services restart, the updated policies are pushed to all Check Point appliances.

Locating the log source SIC

After you create the OPSEC Application Object, you can locate the Log Source SIC from the Check Point SmartConsole.

Procedure

1. Select **Objects** > **Object Explorer**.
2. In the Categories tree, select **Gateways and Servers** under **Networks Objects**.
3. Select your Check Point Log Host object.
4. Copy the Secure Internal Communication (SIC).

   Important: Depending on your Check Point version, the **Communication** button displays the SIC attribute. You can locate the SIC attribute from the Check Point Management Server command-line interface. You must use the **`cpca_client lscert`** command from the command-line interface of the Management Server to display all certificates.

Important: The Log Source SIC Attribute resembles the following example: `cn=cp_mgmt,o=cpmodule...tdfaaz`. For more information, see your *Check Point Command Line Interface Guide*.

You must now install the Security Policy from the Check Point SmartConsole user interface.

What to do next

You are now ready to configure the OPSEC LEA protocol. For more information, see OPSEC/LEA log source parameters for Check Point.

OPSEC/LEA log source parameters for Check Point

If QRadar does not automatically detect the log source, add a Check Point log source on the QRadar Console by using the OPSEC/LEA protocol.

When using the OPSEC/LEA protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect OPSEC/LEA events from Check Point:

Table 327. OPSEC/LEA log source parameters for the Check Point DSM

Parameter	Value
Log Source type	**Check Point**
Protocol Configuration	**OPSEC/LEA**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Check Point devices.

For a complete list of OPSEC/LEA protocol parameters and their values, see "OPSEC/LEA protocol configuration options" on page 201.

Related tasks

Adding a log source

Edit your OPSEC communications configuration

This section describes how to modify your Check Point configuration to allow OPSEC communications on non-standard ports.

It also explains how to configure communications in a clear text, unauthenticated stream, and verify the configuration in IBM QRadar.

Change your Check Point Custom Log Manager (CLM) IP address

If your Check Point configuration includes a Check Point Custom Log Manager (CLM), you might eventually need to change the IP address for the CLM, which impacts any of the automatically discovered Check Point log sources from that CLM in QRadar. When you manually add the log source for the CLM by using the OPSEC/LEA protocol, all Check Point firewalls that forward logs to the CLM are automatically discovered by QRadar. These automatically discovered log sources cannot be edited. If the CLM IP address changes, you must edit the original Check Point CLM log source that contains the OPSEC/LEA protocol configuration and update the server IP address and log source identifier.

After you update the log source for the new Check Point CLM IP address, then any new events reported from the automatically discovered Check Point log sources are updated.

Important: Do not delete and re-create your Check Point CLM or automatically discovered log sources in QRadar. Deleting a log source does not delete event data, but can make finding previously recorded events more difficult.

Changing the default port for OPSEC LEA communication

Change the default port (18184) on which OPSEC LEA communicates.

Procedure

1. At the command-line prompt of your Check Point SmartCenter Server, type the following command to stop the firewall services:

   ```
   cpstop
   ```

2. Depending on your Check Point SmartCenter Server operating system, open the following file:

   - Linux - `$FWDIR\conf\fwopsec.conf`
   - Windows - `%FWDIR%\conf\fwopsec.conf`

   The default contents of this file are as follows:

   ```
   # The VPN-1 default settings are:
   # # sam_server auth_port 0 # sam_server port 18183
   # # lea_server auth_port 18184 # lea_server port 0
   # # ela_server auth_port 18187 # ela_server port 0
   # # cpmi_server auth_port 18190
   # # uaa_server auth_port 19191 # uaa_server port 0 #
   ```

3. Change the default **lea_server auth_port** from 18184 to another port number.
4. Remove the hash (*#*) mark from that line.

   Example:

   ```
   lea_server auth_port 18888 # lea_server port 0
   ```

5. Save and close the file.
6. Type the following command to start the firewall services:

   ```
   cpstart
   ```

Configuring OPSEC LEA for unencrypted communications

You can configure the OPSEC LEA protocol for unencrypted communications:

Procedure

1. At the command-line prompt of your Check Point SmartCenter Server, stop the firewall services by typing the following command:

   ```
   cpstop
   ```

2. Depending on your Check Point SmartCenter Server operating system, open the following file:

   - Linux - `$FWDIR\conf\fwopsec.conf`
   - Windows - `%FWDIR%\conf\fwopsec.conf`

3. Change the default **lea_server auth_port** from 18184 to `0`.
4. Change the **default lea_server port** from 0 to 18184.
5. Remove the hash (*#*) marks from both lines.

   Example:

   ```
   lea_server auth_port 0 lea_server port 18184
   ```

6. Save and close the file.
7. Type the following command to start the firewall services:

   ```
   cpstart
   ```

Integrating Check Point by using TLS Syslog

Before you can add a log source in IBM QRadar, you need to generate certificates on the QRadar Console and then copy the certificates on your Check Point device.

Procedure

1. Using SSH, log in to your QRadar Console.
2. Generate the root CA key by typing the following command:

```
openssl genrsa -out RootCA.key 2048
```

3. Generate the root CA pem by typing the following command:

```
openssl req -x509 -new -nodes -key RootCA.key -days 2048 -out RootCA.pem
```

Important: When prompted to provide Distinguished Name (DN) information about the certificate, you might want to use `CheckpointRootCA` as the **Common Name** value. The **Common Name** value can't be the same **Common Name** value that you use for any other certificates. All other fields are optional and can be left blank. However, if you purchase an SSL certificate from a certificate authority, you might need to configure more fields, such as **Organization** to accurately reflect your organization's information.

4. To generate the client key, type the following command:

```
openssl genrsa -out log_exporter.key 2048
```

Important: Do not share the client key with anyone.

5. To generate the client certificate sign request, type the following command:

```
openssl req -new -key log_exporter.key -out log_exporter.csr
```

Important: When prompted to provide Distinguished Name (DN) information about the certificate, you might want to use the Check Point IP address as the **Common Name** value. The **Common Name** value can't be the same **Common Name** value that you use for any other certificates. All other fields are optional and can be left blank. When you type a value for the **A challenge password** field, do not use special characters for the password. If you purchase an SSL certificate from a certificate authority, you might need to configure more fields, such as **Organization** to accurately reflect your organization's information.

6. To sign the certificate by using the CA files, type the following command:

```
openssl x509 -req -in log_exporter.csr -CA RootCA.pem -CAkey RootCA.key -CAcreateserial
-out log_exporter.crt -days 2048 -sha256
```

7. To convert the certificate to p12 format, type the following command:

```
openssl pkcs12 -inkey log_exporter.key -in log_exporter.crt -export -out log_exporter.p12
```

Important: When you type a value for the **Export password field**, do not use special characters for the password.

8. Generate the server key by typing the following command:

```
openssl genrsa -out syslogServer.key 2048
```

Important: Do not share the server key with anyone.

9. Generate the server certificate sign request by typing the following command:

```
openssl req -new -key syslogServer.key -out syslogServer.csr
```

Important: When prompted to provide Distinguished Name (DN) information about the certificate, you might want to use the QRadar IP address as the **Common Name** value. The **Common Name**

value can't be the same **Common Name** value that you use for any other certificates. All other fields are optional and can be left blank. When you type a value for the **A challenge password** field, do not use special characters for the password. If you purchase an SSL certificate from a certificate authority, you might need to configure more fields, such as **Organization** to accurately reflect your organization's information.

10. To sign the certificate by using the CA files, type the following command:

```
openssl x509 -req -in syslogServer.csr -CA RootCA.pem -CAkey RootCA.key -CAcreateserial
-out syslogServer.crt -days 2048 -sha256
```

11. To convert the server certificate and key to a p12 file, type the following command:

```
openssl pkcs12 -inkey syslogServer.key -in syslogServer.crt -export -out syslogServer.p12
```

Important: When you type a value for the **Enter Export Password** field, do not use special characters for the password.

12. Using SSH, log in to your Check Point device.
13. To access expert mode, type the following command:

```
Expert
```

14. Create a `certs` directory inside your `deployment` directory:

`mkdir -p $EXPORTERDIR/targets/`*`<deployment_name>`*`/certs`

Where *<deployment_name>* is the hostname of your QRadar Console.

15. Copy the `RootCA.pem` and `log_exporter.p12` that you created in Steps 3 and 7 to the directory that you created on your Check Point device in Step 13 by typing the following command:

```
scp root@qradar_ip:RootCA.pem log_exporter.p12 $EXPORTERDIR/targets/<deployment_name>/certs/
```

16. Type the following commands:

```
chmod +r RootCA.pem
```

```
chmod +r log_exporter.p12
```

```
cp_log_export add name <deployment_name>  target-server <QRadar_host_IP> protocol
tcp target-port <port_from_log_source_config> format leef encrypted true ca-cert
$EXPORTERDIR/targets/<deployment_name>/certs/RootCA.pem client-cert $EXPORTERDIR/targets/
<deployment_name>/certs/log_exporter.p12 client-secret <password_for_p12>
```

For more information about TLS configuration, see your Check Point documentation (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#TLS Configuration).

What to do next

Add a log source in QRadar by using the TLS Syslog protocol. For more information, see TLS Syslog log source parameters for Check Point and Adding a log source.

TLS syslog log source parameters for Check Point

If QRadar does not automatically detect the log source, add a Check Point log source on the QRadar Console by using the TLS syslog protocol.

When using the TLS Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect TLS Syslog events from Check Point:

Table 328. TLS Syslog log source parameters for the Check Point DSM	
Parameter	**Value**
Log Source type	**Check Point**
Protocol Configuration	**TLS Syslog**
Log Source Identifier	Type the IP address of your Check Point server as an identifier for events from your Check Point devices.
TLS Listen Port	6514
Authentication Mode	**TLS and Client Authentication**
Client Certificate Path	<*full_path_to_file*>/log_exporter.crt
Certificate Type	**PKCS12 Certificate Chain and Password**
PKCS12 Certificate Path	<full_path_to_the_file>/ syslogServer.p12
PKCS12 Password	The password for the PKCS12 Certificate.
Certificate Alias	This field must be empty.
Max Payload Length	4096
Maximum Connections	50

For a complete list of TLS Syslog protocol parameters and their values, see TLS syslog protocol configuration options.

Related tasks

Adding a log source

Syslog Redirect log source parameters for Check Point

If QRadar does not automatically detect the log source, add a Check Point log source on the QRadar Console by using the Syslog Redirect protocol.

When using the Syslog Redirect protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog Redirect events from Check Point:

Table 329. Syslog Redirect log source parameters for the Check Point DSM	
Parameter	**Value**
Log Source type	**Check Point**
Protocol Configuration	**Syslog Redirect**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Check Point devices.

For a complete list of Syslog Redirect protocol parameters and their values, see Syslog Redirect protocol overview.

Related tasks

Adding a log source

Configuring Check Point to forward LEEF events to QRadar

To forward LEEF events to IBM QRadar, use the Check Point Log Exporter and configure a new target for the logs.

Before you begin

Log Exporter can be installed on several versions of Check Point. Before you send events in LEEF format to QRadar, ensure that you have the correct version of Check Point and Log Exporter installed in your environment.

The following table describes where LEEF events are supported.

Table 330. Check Point versions that support LEEF

Check Point version	Comments
R81.10	Log Exporter is included in this version.
R80.20	Log Exporter is included in this version.
R80.10	Install Log Exporter and then install the hotfix after.
R77.30	Install Log Exporter and then install the hotfix after.

Check Point R80.20

If you want to preserve the Log Exporter configuration before you upgrade to Check Point R80.20, follow the backup and restore Log Exporter instructions on the Check Point website. (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk127653).

Check Point R80.10

Ensure that Check Point version R80.10 is installed on the following servers:

- R80.10 Multi-Domain Log Server
- Security Management Server
- Log Server
- SmartEvent Server

You can install Log Exporter on version R80.10 Jumbo Hotfix Take 56 or later. The hotfix must be installed after Jumbo is installed. If you want to upgrade Jumbo, uninstall the hotfix, upgrade Jumbo, and then reinstall the hotfix. For more information, see the installation topic on the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Installation).

Check Point R77.30

Ensure that Check Point version R77.30 is installed on the following servers:

- Multi-Domain server
- Multi-Domain Log Server
- Log Server
- SmartEvent Server

You can install Log Exporter on version R77.30 Jumbo Hotfix Take 292 or later. The hotfix must be installed after Jumbo is installed. If you want to upgrade Jumbo, uninstall the hotfix, upgrade Jumbo, and then reinstall the hotfix. For more information, see the installation topic on the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Installation).

Procedure

1. To access the expert mode on the Check Point Log Exporter console by using the command-line interface, type `expert`, then press Return.
2. Type your expert password, then press Return.
3. Type the following command:

```
cp_log_export add name <name> [domain-server <domain-server> target-server <target-server
IP address> target-port <target-port>protocol <(udp|tcp)> format <(syslog)|(cef)|(leef)>
[optional arguments]
```

Tip: If your server is not part of a domain, do not include the **`domain-server`** field in the setup command.

A new target directory and default files are created in the `$EXPORTERDIR/targets/<deployment_name>` directory.

The following table shows sample parameters and their values.

Table 331. Sample target configuration

Parameter	Value
`Name`	*<service_name>*
`Enabled`	True
`Target-server`	*<QRadar_IP_address>*
`Target-port`	514
`Protocol`	TCP
`Format`	LEEF
`Read-mode`	Semi-unified The default value for the Read-mode parameter is `Semi-unified` to ensure that complete data is collected.

For more information about other commands, go to the Check Point website (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323#Deployment Script Additional Commands).

4. To change a configuration, type `cp_log_export set`.
5. To verify a configuration in an existing deployment, type `cp_log_export show`.
6. To start Log Exporter automatically, type the following command: `cp_log_export restart`.

   By default, Log Exporter doesn't start automatically.

Results

If QRadar isn't receiving events from Check Point, try these troubleshooting tips:

- Check the `$EXPORTERDIR/targets/<deployment_name>/conf/LeefFieldsMapping.xml` file for attributes-mapping issues.
- Check the `$EXPORTERDIR/targets/<deployment_name>/conf/LeefFormatDefinition.xml` file for LEEF header-mapping issues.
- Check the file paths. File paths might change with Check Point updates. If a configuration file can't be found, contact your Check Point administrator.

For more troubleshooting information, see the Troubleshooting Check Point Syslog LEEF Events from the Log Exporter (cp_log_export) Utility technote (https://www.ibm.com/support/docview.wss?uid=ibm10876650).

Configuring QRadar to receive LEEF events from Check Point

By default, Check Point LEEF events are mapped to the legacy OPSEC LEA event-mapping schema. If you want to change the way that IBM QRadar maps events, you can use the DSM Editor to disable legacy event mapping.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click **DSM Editor**.
3. From the **Select Log Source Type** window, select **Check Point** from the list, and click **Select**.
4. On the **Configuration** tab, set **Display DSM Parameters Configuration** to **on**.
5. From the **Event Collector** list, select the event collector for the log source.
6. Set **Disable legacy event mapping** to **on**.
7. Set **Enable SmartDefense Signature Event IDs** to **on**.

   The value in the **signature** field is used as the event ID for SmartDefense. By default, events for Check Point SmartDefense use the value in the **attack** field for parsing.
8. Click **Save** and close out the DSM Editor.

Integration of Check Point Firewall events from external syslog forwarders

Check Point Firewall events can be forwarded from external sources, such as Splunk Forwarders, or other third-party syslog forwarders that send events to IBM QRadar.

When Check Point Firewall events are provided from external sources in syslog format, the events identify with the IP address in the syslog header. This identification causes events to identify incorrectly when they are processed with the standard syslog protocol. The syslog redirect protocol provides administrators a method to substitute an IP address from the event payload into the syslog header to correctly identify the event source.

To substitute an IP address, administrators must identify a common field from their Check Point Firewall event payload that contains the proper IP address. For example, events from Splunk Forwarders use `orig=` in the event payload to identify the original IP address for the Check Point firewall. The protocol substitutes in the proper IP address to ensure that the device is properly identified in the log source. As Check Point Firewall events are forwarded, QRadar automatically discovers and create new log sources for each unique IP address.

Substitutions are that are performed with regular expressions and can support either TCP or UDP syslog events. The protocol automatically configures iptables for the initial log source and port configuration. If an administrator decides to change the port assignment a Deploy Full Configuration is required to update the iptables configuration and use the new port assignment.

Check Point Multi-Domain Management (Provider-1)

You can configure IBM QRadar to integrate with a Check Point Multi-Domain Management (Provider-1) device.

All events from Check Point Multi-Domain Management (Provider-1) are parsed by using the Check Point DSM. You can integrate Check Point Multi-Domain Management (Provider-1) using one of the following methods:

- “Integrating syslog for Check Point Multi-Domain Management (Provider-1)” on page 610

- "Configuring OPSEC for Check Point Multi-Domain Management (Provider-1) " on page 611

Note: Depending on your Operating System, the procedures for using the Check Point Multi-Domain Management (Provider-1) device can vary. The following procedures are based on the Check Point SecurePlatform operating system.

Integrating syslog for Check Point Multi-Domain Management (Provider-1)

This method ensures that the Check Point Multi-Domain Management (Provider-1) DSM for IBM QRadar accepts Check Point Multi-Domain Management (Provider-1) events by using syslog.

About this task

QRadar records all relevant Check Point Multi-Domain Management (Provider-1) events.

Configure syslog on your Check Point Multi-Domain Management (Provider-1) device:

Procedure

1. Type the following command to access the console as an expert user:

   ```
   expert
   ```

   A password prompt is displayed.
2. Type your expert console password. Press the Enter key.
3. Type the following command:

   ```
   csh
   ```
4. Select the wanted customer logs:

   ```
   mdsenv <customer name>
   ```
5. Input the following command:

   ```
   # nohup $FWDIR/bin/fw log -ftn | /usr/bin/logger -p <facility>.<priority>
   2>&1 &
   ```

   Where:

   - <*facility*> is a syslog facility, for example, local3.
   - <*priority*> is a syslog priority, for example, info.

   You are now ready to configure the log source in QRadar.

   The configuration is complete. The log source is added to QRadar as the Check Point Multi-Domain Management Provider-1 syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.

Syslog log source parameters for Check Point Multi-Domain Management (Provider-1)

If QRadar does not automatically detect the log source, add a Check Point Multi-Domain Management (Provider-1) log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Check Point Multi-Domain Management (Provider-1):

Table 332. Syslog log source parameters for the Check Point Multi-Domain Management (Provider-1) DSM

Parameter	Value
Log Source type	**Check Point**

Table 332. Syslog log source parameters for the Check Point Multi-Domain Management (Provider-1) DSM (continued)	
Parameter	**Value**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for your Check Point Multi-Domain Management (Provider-1) appliance.

Related tasks

"Adding a log source" on page 5

Configuring OPSEC for Check Point Multi-Domain Management (Provider-1)

This method ensures that the IBM QRadar Check Point FireWall-1 DSM accepts Check Point Multi-Domain Management (Provider-1) events by using OPSEC.

About this task

In the Check Point Multi-Domain Management (Provider-1) Management Domain GUI (MDG), create a host object that represents the QRadar. The *leapipe* is the connection between the Check Point Multi-Domain Management (Provider-1) and QRadar.

To reconfigure the Check Point Multi-Domain Management (Provider-1) SmartCenter (MDG):

Procedure

1. To create a host object, open the Check Point SmartDashboard user interface and select **Manage** > **Network Objects** > **New** > **Node** > **Host**.
2. Type the Name, IP address, and write comments if needed.
3. Click **OK**.
4. Select **Close**.
5. To create the OPSEC connection, select **Manage** > **Servers and OPSEC Applications** > **New** > **OPSEC Application Properties**.
6. Type a Name, and write comments if needed.

   The Name that you enter must be different than the name used in Step 2.
7. From the **Host** drop-down menu, select the QRadar **host object** that you created.
8. From **Application Properties**, select **User Defined** as the Vendor type.
9. From **Client Entries**, select **LEA**.
10. To configure the Secure Internal Communication (SIC) certificate, click **Communication** and enter an activation key.
11. Select **OK** and then **Close**.
12. To install the Policy on your firewall, select **Policy** > **Install** > **OK**.

OPSEC/LEA log source parameters for Check Point Multi-Domain Management (Provider-1)

If QRadar does not automatically detect the log source, add a Check Point Multi-Domain Management (Provider-1) log source on the QRadar Console by using the OPSEC/LEA protocol.

When using the OPSEC/LEA protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect OPSEC/LEA events from Check Point Multi-Domain Management (Provider-1):

Table 333. OPSEC/LEA log source parameters for the Check Point Multi-Domain Management (Provider-1) DSM	
Parameter	**Value**
Log Source type	**Check Point**
Protocol Configuration	**OPSEC/LEA**
Log Source Identifier	Type the IP address for the log source. This value must match the value that you typed in the **Server IP** parameter.

For a complete list of OPSEC/LEA protocol parameters and their values, see "OPSEC/LEA protocol configuration options" on page 201.

Related tasks

"Adding a log source" on page 5

Check Point Multi-Domain Management (Provider-1) sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Check Point Multi-Domain Management (Provider-1) sample messages when you use the LEEF protocol

Sample 1: The following sample event message shows an informational event that was generated by the clock daemon.

```
LEEF:2.0|Check Point|Syslog|1.0|Check Point Log|cat=Syslog    devTime=1537528801
ifdir=inbound    loguid={0x0,0x0,0x0,0x0}    origin=172.16.150.106    sequencenum=1
version=5    default_device_message=<78>crond[30156]: (root) CMD (/usr/lib/sa/sa1 1 1)
facility=clock daemon    syslog_severity=Informational
```

Sample 2: The following sample event message shows an application control event that contains specific details about the application; such as the category, name, description, ID, and properties of the application. This sample also contains rules that determine who can access the application and the matched category that is matched by the rule base.

```
LEEF:2.0|Check Point|Application Control|1.0|Allow|cat=Application Control
devTime=1393855342    srcPort=35275    sev=8    ifdir=outbound    ifname=eth1-05
loguid={0x54f411c8,0x9,0xbd0317ac,0x187a}    origin=10.1.76.67    version=1
app_category=Network Protocols    app_desc=Telnet is a network protocol used on the Internet
or local area networks to provide a bidirectional interactive text-oriented communications
facility using a virtual terminal connection. User data is interspersed in-band with
Telnet control information in an 8-bit byte oriented data connection over the Transmission
Control Protocol (TCP). Supported from: R75.    app_id=60095597    app_properties=Allows
remote connect, High Risk, Network Protocols    app_rule_id={C54A11A6-BDE9-11DF-9B35-
C21D241F6A6A}    app_rule_name=Any Allow Log    app_sig_id=60095597:1    appi_name=Telnet
Protocol    dst=10.9.240.147    matched_category=Network Protocols    origin_sic_name=CN\
\=ny1,O\\=ny..8ye75g    product=Application Control    proto=6    proxy_src_ip=10.0.36.27
service=50008    src=10.0.36.27
```

Chapter 39. Cilasoft QJRN/400

IBM QRadar collects detailed audit events from Cilasoft QJRN/400® software for IBM i.

To collect events, administrators can configure Cilasoft QJRN/400 to forward events with syslog, or optionally configure the integrated file system (IFS) to write events to a file. Syslog provides real-time events to QRadar and provides automatic log source discovery for administrators, which is the easiest configuration method for event collection. The IFS option provides an optional configuration to write events to a log file, which can be read remotely by using the log file protocol. QRadar supports syslog events from Cilasoft QJRN/400 V5.14.K and later.

To configure Cilasoft QJRN/400, complete the following tasks:

1. On your Cilasoft QJRN/400 installation, configure the Cilasoft Security Suite to forward syslog events to QRadar or write events to a file.
2. For syslog configurations, administrators can verify that the events forwarded by Cilasoft QJRN/400 are automatically discovered on the Log Activity tab.

Cilasoft QJRN/400 configurations that use IFS to write event files to disk are considered an alternative configuration for administrators that cannot use syslog. IFS configurations require the administrator to locate the IFS file and configure the host system to allow FTP, SFTP, or SCP communications. A log source can then be configured to use the log file protocol with the location of the event log file.

Configuring Cilasoft QJRN/400

To collect events, you must configure queries on your Cilasoft QJRN/400 to forward syslog events to IBM QRadar.

Procedure

1. To start the Cilasoft Security Suite, type the following command:

   `IJRN/QJRN`

   The account that is used to make configuration changes must have ADM privileges or USR privileges with access to specific queries through an **`Extended Access`** parameter.
2. To configure the output type, select one of the following options:

   To edit several selected queries, type 2EV to access the Execution Environment and change the **Output Type** field and type SEM.
3. To edit large numbers of queries, type the command CHGQJQRYA and change the **Output Type** field and type SEM.
4. On the Additional Parameters screen, configure the following parameters:

Table 334. Cilasoft QJRN/400 output parameters

Parameter	Description
Format	Type *LEEF to configure the syslog output to write events in Log Event Extended Format (LEEF). LEEF is a special event format that is designed to for IBM QRadar.

Table 334. Cilasoft QJRN/400 output parameters (continued)	
Parameter	**Description**
Output	To configure an output type, use one of the following parameters to select an output type: *SYSLOG - Type this parameter to forward events with the syslog protocol. This option provides real-time events. *IFS - Type this parameter to write events to a file with the integrated file system. This option requires the administrator to configure a log source with the log file protocol. This option writes events to a file, which can be read in only 15-minute intervals.
IP Address	Enter the IP address of your IBM QRadar system. If an IP address for IBM QRadar is defined as a special value in the WRKQJVAL command, you can type *CFG. Events can be forwarded to either the QRadar Console, an Event Collector, an Event Processor, or your IBM QRadar all-in-one appliance.
Port	Type 514 or *CFG as the port for syslog events. By default, *CFG automatically selects port 514.
Tag	This field is not used by IBM QRadar.
Facility	This field is not used by IBM QRadar.
Severity	Select a value for the event severity. For more information about severity that is assigned to *QRY destinations, look up the command **WRKQJFVAL** in your *Cilasoft documentation*.

For more information on Cilasoft configuration parameters, see the *Cilasoft QJRN/400 User's Guide*.

Syslog events that are forwarded to IBM QRadar are viewable on the **Log Activity** tab.

Syslog log source parameters for Cilasoft QJRN/400

If QRadar does not automatically detect the log source, add a Cilasoft QJRN/400 log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cilasoft QJRN/400:

Table 335. Syslog log source parameters for the Cilasoft QJRN/400 DSM	
Parameter	**Value**
Log Source type	Cilasoft QJRN/400

Table 335. Syslog log source parameters for the Cilasoft QJRN/400 DSM (continued)	
Parameter	**Value**
Protocol Configuration	Syslog If Cilasoft QJRN/400 is configured to write events to the integrated file system with the *IFS option, the administrator must select **Log File**, and then configure the log file protocol.
Log Source Identifier	Type the IP address of your Cilasoft QJRN/400 installation.
Enabled	Select the **Enabled** check box to enable the log source. By default, the check box is selected.
Credibility	Select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in IBM QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the **Incoming Event Payload** encoder for parsing and storing the logs.
Store Event Payload	Select the **Store Event Payload** check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in IBM QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related tasks

“Adding a log source” on page 5

Chapter 40. Cisco

Several Cisco DSMs can be integrated with IBM QRadar.

Cisco ACE Firewall

The IBM QRadar DSM for Cisco ACE Firewall collects syslog events from a Cisco ACE Firewall device.

QRadar accepts events that are forwarded from Cisco ACE Firewall by using the Syslog protocol. QRadar records all relevant events. Before you configure QRadar to integrate with an ACE firewall, you must configure your Cisco ACE Firewall to forward all device logs to QRadar.

Configuring Cisco ACE Firewall

Before you can collect Cisco ACE Firewall logs in IBM QRadar, you must forward Cisco ACE device logs to QRadar.

Procedure

1. Log in to your Cisco ACE device.
2. From the **Shell Interface**, select **Main Menu** > **Advanced Options** > **Syslog Configuration**.
3. The **Syslog Configuration** menu varies depending on whether there are any syslog destination hosts configured yet. If no syslog destinations are configured, create one by selecting the **Add First Server** option. Click **OK**.
4. Type the host name or IP address of the destination host and port in the **First Syslog Server** field. Click **OK**.

   The system restarts with new settings. When finished, the Syslog server window displays the host that is configured.
5. Click **OK**.

   The **Syslog Configuration** menu is displayed. Notice that options for editing the server configuration, removing the server, or adding a second server are now available.
6. If you want to add another server, click **Add Second Server**.

   At any time, click the **View Syslog options** to view existing server configurations.
7. To return to the **Advanced** menu, click **Return**.

   The configuration is complete. The log source is added to QRadar as Cisco ACE Firewall events are automatically discovered. Events that are forwarded to QRadar by Cisco ACE Firewall appliances are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco ACE Firewall

If QRadar does not automatically detect the log source, add a Cisco ACE Firewall log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco ACE Firewall:

Table 336. Syslog log source parameters for the Cisco ACE Firewall DSM

Parameter	Value
Log Source type	Cisco ACE Firewall
Protocol Configuration	Syslog

Table 336. Syslog log source parameters for the Cisco ACE Firewall DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco ACE Firewall.

Related tasks

"Adding a log source" on page 5

Cisco ACS

The Cisco ACS DSM for IBM QRadar accepts syslog ACS events by using syslog and UDP multiline.

QRadar records all relevant and available information from the event. You can integrate Cisco ACS with QRadar by using one of the following methods:

- Configure your Cisco ACS device to directly send syslog to QRadar for Cisco ACS v5.x. See "Configuring Syslog for Cisco ACS v5.x" on page 618.
- Configure your Cisco ACS device to directly send syslog to QRadar for Cisco ACS v4.x. See "Configuring Syslog for Cisco ACS v4.x" on page 620.
- Configure your Cisco ACS device to directly send UDP multiline syslog to QRadar. See "UDP Multiline Syslog log source parameters for Cisco ACS" on page 621

Configuring Syslog for Cisco ACS v5.x

The configuration of syslog forwarding from a Cisco ACS appliance with software version 5.x involves several steps.

About this task

You must complete the following tasks:

Procedure

1. Create a Remote Log Target
2. Configure global logging categories
3. Configure a log source

Creating a Remote Log Target

Creating a remote log target for your Cisco ACS appliance.

Log in to your Cisco ACS appliance.

On the navigation menu, click **System Administration** > **Configuration** > **Log Configuration** > **Remote Log Targets**.

The **Remote Log Targets** page is displayed.

Click **Create**.

Configure the following parameters:

Table 337. Remote target parameters	
Parameter	**Description**
Name	Type a name for the remote syslog target.
Description	Type a description for the remote syslog target.
Type	Select **Syslog**.
IP address	Type the IP address of QRadar or your Event Collector.

Click **Submit**.

You are now ready to configure global policies for event logging on your Cisco ACS appliance.

Configuring global logging categories

To configure Cisco ACS to forward log failed attempts to IBM QRadar:

Procedure

1. On the navigation menu, click **System Administration** > **Configuration** > **Log Configuration** > **Global**.

   The **Logging Categories** window is displayed.
2. Select the **Failed Attempts** logging category and click **Edit**.
3. Click **Remote Syslog Target**.
4. From the **Available targets** window, use the arrow key to move the syslog target for QRadar to the **Selected targets** window.
5. Click **Submit**.

   You are now ready to configure the log source in QRadar.

Syslog log source parameters for Cisco ACS v5.x

If QRadar does not automatically detect the log source, add a Cisco ACS v5.x log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco ACS v5.x:

Table 338. Syslog log source parameters for the Cisco ACS DSM	
Parameter	**Value**
`Log Source type`	Cisco ACS
`Protocol Configuration`	Syslog
`Log Source Identifier`	Type the IP address or hostname for the log source. The identifier helps you determine which events came from your Cisco ACS appliance.

Related tasks

"Adding a log source" on page 5

Configuring Syslog for Cisco ACS v4.x

The configuration of syslog forwarding from a Cisco ACS appliance with software version 4.x involves a few steps.

About this task

Complete the following steps:

Procedure

1. Configure syslog forwarding
2. Configure a log source

Configuring syslog forwarding for Cisco ACS v4.x

Configuration of an ACS device to forward syslog events to IBM QRadar.

About this task

Take the following steps to configure the ACS device to forward syslog events to QRadar

Procedure

1. Log in to your Cisco ACS device.
2. On the navigation menu, click **System Configuration**.

   The **System Configuration** page opens.
3. Click **Logging**.

   The logging configuration is displayed.
4. In the Syslog column for **Failed Attempts**, click **Configure**.

   The **Enable Logging** window is displayed.
5. Select the **Log to Syslog Failed Attempts report** check box.
6. Add the following Logged Attributes:
   - **Message-Type**
   - **User-Name**
   - **Nas-IP-Address**
   - **Authen-Failure-Code**
   - **Caller-ID**
   - **NAS-Port**
   - **Author-Data**
   - **Group-Name**
   - **Filter Information**
   - **Logged Remotely**
7. Configure the following syslog parameters:

Table 339. Syslog parameters

Parameter	Description
IP	Type the IP address of QRadar.
Port	Type the syslog port number of IBM QRadar. The default is port 514.

Table 339. Syslog parameters (continued)	
Parameter	**Description**
Max message length (Bytes) - Type	Type 1024 as the maximum syslog message length.

Note: Cisco ACS provides syslog report information for a maximum of two syslog servers.

8. Click **Submit**.

   You are now ready to configure the log source in QRadar.

Syslog log source parameters for Cisco ACS v4.x

If QRadar does not automatically detect the log source, add a Cisco ACS v4.x log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco ACS v4.x:

Table 340. Syslog log source parameters for the Cisco ACS DSM	
Parameter	**Value**
Log Source type	Cisco ACS
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or hostname for the log source. The identifier helps you determine which events came from your Cisco ACS appliance.

Related tasks

"Adding a log source" on page 5

UDP Multiline Syslog log source parameters for Cisco ACS

The Cisco ACS DSM for IBM QRadar accepts syslog events from Cisco ACS appliances with log sources that are configured to use the UDP Multiline Syslog protocol.

If QRadar does not automatically detect the log source, add a Cisco ACS log source on the QRadar Console by using the UDP Multiline Syslog protocol.

The following table describes the parameters that require specific values to collect UDP Multiline Syslog events from Cisco ACS:

Table 341. UDP Multiline Syslog log source parameters for the Cisco ACS DSM	
Parameter	**Value**
Log Source type	Cisco ACS
Protocol Configuration	UDP Multiline Syslog

Table 341. UDP Multiline Syslog log source parameters for the Cisco ACS DSM (continued)	
Parameter	**Value**
Log Source Identifier	The Packet IP address of the source data. If you select **Show Advanced options** and you select the **Use As A Gateway Log Source** option, the **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Cisco ACS log source that is configured, you might want to identify the first log source as *ciscoacs1*, the second log source as *ciscoacs2*, and the third log source as *ciscoacs3*. For for more information about using a gateway, see "UDP multiline syslog protocol configuration options" on page 233.
Listen Port	The default port number that is used by QRadar to accept incoming UDP Multiline Syslog events is 517. You can use a different port. The valid port range is 1 - 65535.
Message ID Pattern	\s(\d{10})\s
Event Formatter	Select **Cisco ACS Multiline** from the list.

For a complete list of UDP Multiline Syslog protocol parameters and their values, see "UDP multiline syslog protocol configuration options" on page 233.

Related tasks

"Adding a log source" on page 5

Cisco ACS sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco ACS sample message when you use the Syslog protocol

The following sample event is a passed authentication event.

```
<181>Jul 22 06:43:25 cisco.acs.test CSCOacs_Passed_Authentications 0082331393 3
0 2017-07-22 06:43:25.226 +00:00 1076613766 5203 NOTICE Device-Administration:
Session Authorization succeeded, ACSVersion=acs-192.168.0.1-B.462.x86_64, ConfigVersionId=149,
Device IP Address=10.129.16.29, DestinationIPAddress=10.20.64.165, DestinationPort=49,
UserName=qradar_user1 Protocol=Tacacs, RequestLatency=6, Type=Authorization, Privilege-
Level=0, Authen-Type=PAP, Service=PPP, User=qradar_user1 Port=ssh, Authen-Method=TacacsPlus,
Service-Argument=ppp, Protocol-Argument=ip, AcsSessionID=qradar/266281348/80642976,
AuthenticationIdentityStore=AD1, AuthenticationMethod=Lookup, SelectedAccessService=Default
Device Admin, SelectedShellProfile=F5-RW, IdentityGroup=IdentityGroup:All Groups:Network Admin,
Step=13005 , Step=15008 , Step=15004 , Step=15012 , Step=15041 , Step=15006 , Step=15013 ,
Step=24432 , Step=24325 , Step=24313 , Step=24319 , Step=24367 , Step=24367 , Step=24323 ,
Step=24326 , Step=24327 , Step=24351 , Step=24420 ,
```

```
<181>Jul 22 06:43:25 cisco.acs.test CSCOacs_Passed_Authentications 0082331393 3 0
2017-07-22 06:43:25.226 +00:00 1076613766 5203 NOTICE Device-Administration: Session
Authorization succeeded, ACSVersion=acs-192.168.0.1-B.462.x86_64, ConfigVersionId=149,
```

```
Device IP Address=10.129.16.29, DestinationIPAddress=10.20.64.165, DestinationPort=49,
UserName=qradar_user1 Protocol=Tacacs, RequestLatency=6, Type=Authorization, Privilege-
Level=0, Authen-Type=PAP, Service=PPP, User=qradar_user1 Port=ssh, Authen-Method=TacacsPlus,
Service-Argument=ppp, Protocol-Argument=ip, AcsSessionID=qradar/266281348/80642976,
AuthenticationIdentityStore=AD1, AuthenticationMethod=Lookup, SelectedAccessService=Default
Device Admin, SelectedShellProfile=F5-RW, IdentityGroup=IdentityGroup:All Groups:Network Admin,
Step=13005 , Step=15008 , Step=15004 , Step=15012 , Step=15041 , Step=15006 , Step=15013 ,
Step=24432 , Step=24325 , Step=24313 , Step=24319 , Step=24367 , Step=24367 , Step=24323 ,
Step=24326 , Step=24327 , Step=24351 , Step=24420 ,
```

Table 342. Highlighted values in the Cisco ACS event

QRadar field name	Highlighted values in the event payload
Event ID	**Passed_Authentications**
Source IP	**10.129.16.29**
Destination IP	**10.20.64.165**
Destination Port	**49**
Username	**qradar_user1**

Configuring Cisco Aironet to forward events

The IBM QRadar DSM for Cisco Aironet accepts Cisco EMBLEM Format events by using Syslog.

Procedure

1. Establish a connection to the Cisco Aironet device by using one of the following methods:
   - Telnet to the wireless access point
   - Access the console
2. Type the following command to access privileged EXEC mode:

   `enable`
3. Type the following command to access global configuration mode:

   `config terminal`
4. Type the following command to enable message logging:

   `logging on`
5. Configure the syslog facility. The default is local7.

   `logging` <*facility*>

   where <*facility*> is, for example, local7.
6. Type the following command to log messages to your QRadar:

   `logging` <*IP address*>

   where <*IP address*> is the IP address of your QRadar.
7. Enable **`timestamp`** on log messages:

   `service timestamp log datatime`
8. Return to privileged EXEC mode:

   `end`
9. View your entries:

   `show running-config`
10. Save your entries in the configuration file:

    `copy running-config startup-config`

The configuration is complete. The log source is added to QRadar as Cisco Aironet events are automatically discovered. Events that are forwarded to QRadar by Cisco Aironet appliances are displayed on the **Log Activity** tab of QRadar.

Results

The log source is added to QRadar as Cisco Aironet events are automatically discovered. Events that are forwarded to QRadar by Cisco Aironet appliances are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco Aironet

If QRadar does not automatically detect the log source, add a Cisco Aironet log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco Aironet:

Table 343. Syslog log source parameters for the Cisco Aironet DSM

Parameter	Value
Log Source type	Cisco Aironet
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco Aironet appliance.

Related tasks

"Adding a log source" on page 5

Cisco ASA

You can integrate a Cisco Adaptive Security Appliance (ASA) with IBM QRadar.

A Cisco ASA DSM accepts events through syslog or NetFlow by using NetFlow Security Event Logging (NSEL). QRadar records all relevant events. Before you configure QRadar, you must configure your Cisco ASA device to forward syslog or NetFlow NSEL events.

Choose one of the following options:

- Forward events to QRadar by using syslog. See "Integrate Cisco ASA Using Syslog" on page 624
- Forward events to QRadar by using NetFlow (NSEL). See "Integrate Cisco ASA for NetFlow by using NSEL" on page 626

Integrate Cisco ASA Using Syslog

Integrating Cisco ASA by using syslog involves the configuration of a log source, and syslog forwarding.

Use the following information to help you integrate Cisco ASA by using the syslog protocol:

- "Configuring syslog forwarding" on page 625
- "Syslog log source parameters for Cisco ASA" on page 625

Configuring syslog forwarding

To configure Cisco ASA to forward syslog events, some manual configuration is required.

Procedure

1. Log in to the Cisco ASA device.
2. Type the following command to access privileged EXEC mode:

   ```
   enable
   ```
3. Type the following command to access global configuration mode:

   ```
   conf t
   ```
4. Enable logging:

   ```
   logging enable
   ```
5. Configure the logging details:

   ```
   logging console warning
   ```

   ```
   logging trap warning
   ```

   ```
   logging asdm warning
   ```

   Note: The Cisco ASA device can also be configured with `logging trap informational` to send additional events. However, this may increase the event rate (Events Per Second) of your device.
6. Type the following command to configure logging to IBM QRadar:

   `logging host` <*interface*> <*IP address*>

   Where:

   - <*interface*> is the name of the Cisco Adaptive Security Appliance interface.
   - <*IP address*> is the IP address of QRadar.

   Note: Using the command **`show interfaces`** displays all available interfaces for your Cisco device.
7. Disable the output object name option:

   ```
   no names
   ```

   Disable the output object name option to ensure that the logs use IP addresses and not the object names.
8. Exit the configuration:

   ```
   exit
   ```
9. Save the changes:

   ```
   write mem
   ```

Results

The configuration is complete. The log source is added to QRadar as Cisco ASA syslog events are automatically discovered. Events that are forwarded to QRadar by Cisco ASA are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco ASA

If QRadar does not automatically detect the log source, add a Cisco ASA log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco ASA:

Table 344. Syslog log source parameters for the Cisco ASA DSM	
Parameter	**Value**
Log Source type	Cisco Adaptive Security Appliance (ASA)
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco ASA appliance.

Related tasks

"Adding a log source" on page 5

Integrate Cisco ASA for NetFlow by using NSEL

Integrating Cisco ASA for Netflow by using NSEL involves two steps.

Use the following information to help you integrate Cisco ASA for Netflow by using the NSEL protocol:

- "Configuring NetFlow Using NSEL" on page 626
- "Cisco NSEL log source parameters for Cisco ASA" on page 627

Configuring NetFlow Using NSEL

You can configure Cisco ASA to forward NetFlow events by using NSEL.

Procedure

1. Log in to the Cisco ASA device command-line interface (CLI).
2. Type the following command to access privileged EXEC mode:

   ```
   enable
   ```
3. Type the following command to access global configuration mode:

   ```
   conf t
   ```
4. Disable the output object name option:

   ```
   no names
   ```
5. Type the following command to enable NetFlow export:

   `flow-export destination` <*interface-name*> <*ipv4-address or hostname*> <*udp-port*>

   Where:

   - <*interface-name*> is the name of the Cisco Adaptive Security Appliance interface for the NetFlow collector.
   - <*ipv4-address or hostname*> is the IP address or host name of the Cisco ASA device with the NetFlow collector application.
   - <*udp-port*> is the UDP port number to which NetFlow packets are sent.

   Note: IBM QRadar typically uses port 2055 for NetFlow event data on QRadar QFlow Collectors. You must configure a different UDP port on your Cisco Adaptive Security Appliance for NetFlow by using NSEL.
6. Type the following command to configure the NSEL class-map:

   ```
   class-map flow_export_class
   ```
7. Choose one of the following traffic options:

To configure a NetFlow access list to match specific traffic, type the command:

```
match access-list flow_export_acl
```

8. To configure NetFlow to match any traffic, type the command:

   ```
   match any
   ```

   Note: The Access Control List (ACL) must exist on the Cisco ASA device before you define the traffic match option in "Configuring NetFlow Using NSEL" on page 626.
9. Type the following command to configure the NSEL policy-map:

   ```
   policy-map flow_export_policy
   ```
10. Type the following command to define a class for the flow-export action:

    ```
    class flow_export_class
    ```
11. Type the following command to configure the flow-export action:

    `flow-export event-type all destination` <*IP address*>

    Where <*IP address*> is the IP address of QRadar.

    Note: If you are using a Cisco ASA version before v8.3 you can skip"Configuring NetFlow Using NSEL" on page 626 as the device defaults to the flow-export destination. For more information, see your *Cisco ASA documentation*.
12. Type the following command to add the service policy globally:

    ```
    service-policy flow_export_policy global
    ```
13. Exit the configuration:

    ```
    exit
    ```
14. Save the changes:

    ```
    write mem
    ```

    You must verify that your collector applications use the **Event Time** field to correlate events.

Cisco NSEL log source parameters for Cisco ASA

If QRadar does not automatically detect the log source, add a Cisco ASA log source on the QRadar Console by using the Cisco NSEL protocol.

Note: Your system must be running the current version of the NSEL protocol to integrate with a Cisco ASA device that uses NetFlow and NSEL. The NSEL protocol is available on IBM Support, http://www.ibm.com/support, or through auto updates in QRadar.

The following table describes the parameters that require specific values to collect Cisco NSEL events from Cisco ASA:

Table 345. Cisco NSEL log source parameters for the Cisco ASA DSM

Parameter	Value
Log Source type	Cisco Adaptive Security Appliance (ASA)
Protocol Configuration	Cisco NSEL
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco ASA appliance.

Table 345. Cisco NSEL log source parameters for the Cisco ASA DSM (continued)	
Parameter	**Value**
Collector Port	Type the UDP port number that is used by Cisco ASA to forward NSEL events. The valid range of the **Collector Port** parameter is 1-65535. QRadar typically uses port 2055 for NetFlow event data on the QRadar QFlow Collector. You must define a different UDP port on your Cisco Adaptive Security Appliance for NetFlow that uses NSEL.

For a complete list of Cisco NSEL protocol parameters and their values, see "Cisco NSEL protocol configuration options" on page 116.

Related tasks

"Adding a log source" on page 5

Removing leading domain names from usernames when Cisco ASA events are processed

If you want to change the way that IBM QRadar processes Cisco Adaptive Security Appliance (ASA) events, use the DSM Editor to remove leading domain names from usernames.

By default, Cisco ASA events include leading domain names in usernames.

Procedure

1. On the **Admin** tab, in the **Data Sources** section, click **DSM Editor**.
2. From the **Select Log Source Type** window, select **Cisco Adaptive Security Appliance (ASA)** from the list, and then click **Select**.
3. Click the **Configuration** tab, and then set **Display DSM Parameters Configuration** to **on**.
4. From the **Event Collector** list, select the event collector for the log source.
5. Set **Remove leading domain name from username** to **on**.
6. Click **Save** and then close the DSM Editor.

Collecting IP addresses for Cisco ASA Teardown TCP connection events

If you want IBM QRadar to collect IP addresses for Teardown TCP collection events from Cisco Adaptive Security Appliance (ASA), use the DSM Editor.

Procedure

1. On the **Admin** tab, in the **Data Sources** section, click **DSM Editor**.
2. From the **Select Log Source Type** window, select **Cisco Adaptive Security Appliance (ASA)** from the list, and then click **Select**.
3. Click the **Configuration** tab, and then set **Display DSM Parameters Configuration** to **on**.
4. Set **Teardown IP Connection** to **on**.
5. Click **Save** and then close the DSM Editor.

Cisco ASA sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco ASA sample message when you use the Syslog protocol

The following sample event message shows that the Internet Key Exchange (IKE) protocol obtained an address for the client private IP address from DHCP, or from the address pool. The sample event message also shows that the IP address is assigned to the client.

```
Aug 11 08:10:34 cisco.asa.test %ASA-6-713228: Group = groupx, Username = userx, IP = 192.0.2.10,
Assigned private IP address 192.0.2.11 to remote user
```


```
Aug 11 08:10:34 cisco.asa.test %ASA-6-713228: Group = groupx, Username = userx, IP =
192.0.2.10, Assigned private IP address 192.0.2.11 to remote user
```


Table 346. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**713228**
Source IP	**192.0.2.10**
Username	**userx**
Post NAT Source IP	**192.0.2.11**
Identity IP	**192.0.2.11**
Identity Group Name	**groupx**
Identity Username	**userx**
Device Time	**Aug 11 08:10:34**

Cisco AMP

The IBM QRadar DSM for Cisco Advanced Malware Protection (Cisco AMP) collects event logs from your Cisco AMP for Endpoints platform. The DSM for Cisco AMP uses the RabbitMQ protocol.

Important: The Cisco AMP integration does not support private cloud if the Server Name Indication (SNI) is required. Contact Cisco for more details.

To integrate Cisco AMP with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the following RPMs on your QRadar Console.

   Important: You need QRadar V7.2.8 Patch 9 (V7.2.8.20170726184122) or later to install the RabbitMQ Protocol RPM.

   - Protocol Common RPM
   - DSMCommon RPM
   - RabbitMQ Protocol RPM
   - Cisco AMP DSM RPM
2. Create a Cisco AMP Client ID and API key. Alternatively, you can request access to an already created event stream from your administrator. For more information about creating these values, go to the Creating a Cisco AMP Client ID and API key procedure.
3. Create a Cisco AMP event stream. For more information about creating the event stream, go to the “Creating a Cisco AMP event stream” on page 631 procedure.
4. Add a Cisco AMP log source on the QRadar Console for a user to manage the Cisco AMP event stream.

Related concepts

“Cisco AMP event stream configuration” on page 633

Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

Related tasks

"Adding a DSM" on page 4

Cisco AMP DSM specifications

The following table describes the specifications for the Cisco AMP DSM.

Table 347. Cisco AMP DSM specifications

Specification	Value
Manufacturer	Cisco
DSM	Cisco AMP
RPM name	`DSM-CiscoAMP-`*`QRadar_version-Build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	RabbitMQ
Event format	Cisco AMP
Recorded event types	All security events For a detailed list of supported events, go to the Cisco AMP for Endpoints API documentation. (https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fevent_types&api_host=api.amp.cisco.com&api_resource=Event+Type&api_version=v1) **Note:** Network traffic is supported only for Data Flow Control (DCF) events.
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Cisco website (https://api-docs.amp.cisco.com/)

Creating a Cisco AMP Client ID and API key for event queues

A Cisco AMP administrator must create a Client ID and an API key in the Cisco AMP for Endpoints portal. These keys are used to manage queues.

Before you begin

If you do not have administrator privileges, request the Client ID and API key values from your administrator. If you want QRadar to automatically manage the event stream, you need these values when you configure a log source in QRadar.

Procedure

1. Log in to the Cisco AMP for Endpoints portal as an administrator.
2. Click **Accounts** > **API Credentials**.
3. In the **API Credentials** pane, click **New API Credential**.

4. In the **Application name** field, type a name, and then select **Read & Write**.

   You must have read & write access to manage event streams on your Cisco AMP for Endpoints platform.
5. Click **Create**.
6. From the **API Key Details** section, copy the values for the **3rd Party API Client ID** and the **API Key**. You need these values to manage queues.

What to do next

Create a Cisco AMP event stream.

Related concepts

"Cisco AMP event stream configuration" on page 633

Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

Related tasks

"Creating a Cisco AMP event stream" on page 631

The Cisco AMP for Endpoints API returns the Advanced Message Queuing Protocol (AMQP) credentials in several Cisco AMP for Endpoints API query responses.

"Adding a log source" on page 5

Creating a Cisco AMP event stream

The Cisco AMP for Endpoints API returns the Advanced Message Queuing Protocol (AMQP) credentials in several Cisco AMP for Endpoints API query responses.

Procedure

1. Download the curl command line tool from the curl download website (https://curl.haxx.se/download.html).

   You can run the curl command on your Cisco server or QRadar Console.
2. To create a Cisco AMP event stream, type one of the following command examples. You need the parameter values when you configure a log source in IBM QRadar.

   This command can run on any device. It does not need to run on the Event Collector.

   Important: Due to formatting issues, paste the queries into a text editor and then remove any carriage return or line feed characters.

   Example 1: Default API call to get all Event IDs and all Group GUIDs in a single event stream.

```
curl -X POST -H 'accept: application/json' \-H 'content-type: application/json' \-H 'accept:
application/json' \-H 'accept-encoding: identity' --compressed \-H 'Accept-Encoding: gzip,
deflate' \-d '{"name":"<STREAMNAME>"}' \-u <CLIENTID:APIKEY> \'https://api.amp.cisco.com/v1/
event_streams'
```

   Example 2: API call with multiple defined Event IDs and Group GUIDs.

```
curl -X POST -H 'accept: application/json' \-H 'content-type: application/json'
\-H 'accept: application/json' \-H 'accept-encoding: identity' --compressed \-
H 'Accept-Encoding: gzip, deflate' \-d '{"name":"<STREAMNAME>", \"event_type":
[1090519105, 1090519102,553648199,1090519112], \"group_guid":["0a00a0aa-0000-000a-
a000-0a0aa0a0aaa0","aa00a0aa-0000-000a-a000-0a0aa0a0aaa0"]}' \-u <CLIENTID:APIKEY> \'https://
api.amp.cisco.com/v1/event_streams'
```

   Example 3: API call with a single defined Event ID and Group GUID.

```
curl -X POST -H 'accept: application/json' \-H 'content-type: application/json' \-
H 'accept: application/json' \-H 'accept-encoding: identity' --compressed \-H 'Accept-
Encoding: gzip, deflate' \-d '{"name":"<STREAMNAME>", \"event_type": [1090519112],
\"group_guid":["aa00a0aa-0000-000a-a000-0a0aa0a0aaa0"]}' \-u <CLIENTID:APIKEY> \'https://
api.amp.cisco.com/v1/event_streams'
```

When you input the query, the following values must be configured:

- <*STREAMNAME*> is a name of your choosing for the event stream.
- <*group_guid*> is the group GUID that you want to use to link to the <*0a00a0aa-0000-000a-a000-0a0aa0a0aaa0*> event stream. You can consult your Cisco AMP API to find a group GUID value, or you can leave this value blank.
- <*CLIENTID:APIKEY*> is the **Client ID** and the **API key** that you created.

If you are in the Asia Pacific Japan and China (APJC) region, change `'https://api.amp.cisco.com/v1/event_streams'` to `'https://api.apjc.amp.cisco.com/v1/event_streams'`.

If you are in the European region, change `'https://api.amp.cisco.com/v1/event_streams'` to `'https://api.eu.amp.cisco.com/v1/event_streams'`.

Sample Query Response:


```
{
   "version":"v1.2.0",
   "metadata":{
      "links":{
         "self":"https://api.amp.cisco.com/v1/event_streams"
      }
   },
   "data":{
      "id":2216,
      "name":"STREAMNAME",
      "group_guids":[
         "0a00a8aa-0000-000a-a000-0a0aa0a0aaa0"
      ],
      "event_types":[
         553648130,
         554696714
      ],
      "amqp_credentials":{
         "user_name":"1116-aa00a0000000000000a0",
         "queue_name":"event_stream_1116",
         "password":"0a0aa00a0a0aa000000a0000aa0000aa0a00000a",
         "host":"export-streaming.amp.cisco.com",
         "port":"443",
         "proto":"https"
      }
   }
}
```


Each log source can accept a single stream regardless of the number of event types or `group_guids` requested in the stream. If the Cisco AMP API accepts the request and returns the stream connection information, you can connect to that information.

For more information, see Cisco documentation (https://api-docs.amp.cisco.com/api_actions/details?api_action=POST+%2Fv1%2Fevent_streams&api_host=api.amp.cisco.com&api_resource=EventStream&api_version=v1).

What to do next

Configure a log source in QRadar for a user to manage the Cisco AMP event stream.

Related concepts

"Cisco AMP event stream configuration" on page 633

Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

Related tasks

"Adding a log source" on page 5

Cisco AMP event stream configuration

Configure a log source in QRadar to manage a specific event stream that you want QRadar to collect events from.

To connect to a specific Cisco AMP event stream, you also need to have access to the Advanced Message Queuing Protocol (AMQP) credentials that are provided by the Cisco AMP for Endpoints API.

The Cisco AMP for Endpoints API is used to manage event streams. For more information about supported queries to manage the Cisco AMP for Enpoint API, see Cisco AMP for Endpoints API.

Important: If an issue occurs while you use the Cisco AMP for Endpoints API, contact your Cisco administrator for assistance. For Cisco contact information, see Cisco Support.

The following table describes the parameters that require specific values to collect events from the Cisco AMP for Endpoints API by using the RabbitMQ protocol:

Table 348. RabbitMQ protocol log source parameters

Parameter	Description
Log Source Type	**Cisco AMP**
Protocol Configuration	**RabbitMQ**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If more than one Cisco AMP log source is configured, you might identify the first log source as *CiscoAMP1*, the second log source as *CiscoAMP2*, and so on.
Event Format	You must select **Cisco AMP**.
IP or Hostname	The IP address or host name that is used for the Cisco AMP for Endpoints API event stream. You can find the IP or host name in the **AMQP credentials** field. For more information about AMQP credentials, see Creating a Cisco AMP event stream.
Port	The port that is used for the Cisco AMP for Endpoints API event stream. You can find the port number in the **AMQP credentials** field. For more information about AMQP credentials, see Creating a Cisco AMP event stream.
Queue	The queue name that is used for the Cisco AMP for Endpoints API event stream. You can find the queue name value in the **AMQP credentials** field. For more information about the AMQP credentials, see “Creating a Cisco AMP event stream” on page 631.
Username	The user name that is used for the Cisco AMP for Endpoints API event stream. You can find the user name value in the **AMQP credentials** field. For more information about AMQP credentials, see “Creating a Cisco AMP event stream” on page 631.

Table 348. RabbitMQ protocol log source parameters (continued)	
Parameter	**Description**
Password	The password that is used for the Cisco AMP for Endpoints API event stream. You can find the password value in the **AMQP credentials** field. For more information about AMQP credentials, see “Creating a Cisco AMP event stream” on page 631 .
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Allow Untrusted Certificates	Enable this option when the endpoint is using a certificate that cannot be verified via the Certificate Chain. This would include a self-signed certificate, or one from a private CA that you do not want to import into your CA trust. This option should not be used for endpoints with a certificate issued by a Public CA (SaaS Products, Public Cloud Infrastructure, and so on.) The certificate must be downloaded in PEM or DER encoded binary format and then placed in the `/opt/qradar/conf/trusted_certificates/` directory with a `.cert` or `.crt` file extension.

Related concepts

“Copy the server certificate” on page 208
You need a server certificate to support HTTPS connections. QRadar supports certificates with the `.crt`, `.cert`, or `.der` file extensions.

Related tasks

“Adding a log source” on page 5

Copy the server certificate

You need a server certificate to support HTTPS connections. QRadar supports certificates with the `.crt`, `.cert`, or `.der` file extensions.

To copy a certificate to the `/opt/qradar/conf/trusted_certificates` directory, choose one of the following options:

- Manually copy the certificate to the `/opt/qradar/conf/trusted_certificates` directory by using SCP or SFTP.
- Use SSH to log in to the QRadar Console or managed host and retrieve the certificate by typing the following command:

```
/opt/qradar/bin/getcert.sh <IP or Hostname for RabbitMQ> <Port for RabbitMQ>
```

A certificate is downloaded from the specified host name or IP address and placed into the `/opt/qradar/conf/trusted_certificates` directory in the appropriate format.

Cisco AMP sample event message

Use this sample event to verifying a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Cisco AMP sample message when you use the RabbitMQ protocol

The following sample event message shows that a DFC threat is detected.


```
{"id":6629038896162275332,"timestamp":1543443393,"timestamp_nanoseconds":258000000,"date":"2018-
11-28T22:16:33+00:00","event_type":"DFC Threat
Detected","event_type_id":1090519084,"detection_id":"6629038896162275330","connector_guid":"conn
ector_guid","group_guids":["group_guids"],"severity":"High","computer":
{"connector_guid":"connector_guid","hostname":"example.com","external_ip":"172.16.0.0","user":"r
oot","active":true,"network_addresses":[{"ip":"172.16.0.0","mac":"00-00-5E-00-53-00"}],"links":
{"computer":"computer","trajectory":"trajectory","group":"group"}},"network_info":{"remote_ip":
"172.16.0.1","remote_port": 443,"local_ip": "10.51.100.0","local_port": 55807,"nfm":
{"direction":"Outgoing connection from","protocol":"UDP"},"parent":
{"process_id":2608,"disposition":"Clean","file_name":"chrome.exe","identity": {"sha256":
"sha256","sha1": "sha1","md5": "md5"}}}}
```


Table 349. Highlighted values in the Cisco AMP sample event message

QRadar field name	Highlighted payload field name
Event ID	event_type_id
Category	CiscoAMP
Source IP	local_ip
Source Port	local_port
Network Addresses	remote_ip
Destination Port	remote_port
Log Source TIME	timestamp

Cisco CallManager

The Cisco CallManager DSM for IBM QRadar collects application events that are forwarded from Cisco CallManager devices that are using Syslog.

Before events can be received in QRadar, you must configure your Cisco Call Manager device to forward events. After you forward Syslog events from Cisco CallManager, QRadar automatically detects and adds Cisco CallManager as a log source.

Configuring syslog forwarding

Before events can be received in QRadar, you must configure your Cisco CallManager device to forward events.

Procedure

1. Log in to your Cisco CallManager.
2. Select **System Enterprise** > **Parameters**.

   The **Enterprise Parameters Configuration** is displayed.
3. In the **Remote Syslog Server Name** field, type the IP address of the QRadar Console.
4. From the **Syslog Severity For Remote Syslog messages** list, select **Informational**.

   This option configures the severity level of the messages that are collected.

5. Click **Save**.
6. Click **Apply Config**.

What to do next

You are now ready to configure a syslog log source for Cisco CallManager.

Syslog log source parameters for Cisco CallManager

If QRadar does not automatically detect the log source, add a Cisco CallManager log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco CallManager:

Table 350. Syslog log source parameters for the Cisco CallManager DSM

Parameter	Value
Log Source type	Cisco CallManager
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco CallManager device.

Related tasks

"Adding a log source" on page 5

Cisco CallManager sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco CallManager sample message when you use the syslog protocol

The following sample event message shows that a user is successfully added to a group.

```
<179>10499: : : 7454: cisco.callmanager.test Aug 21 2020
17:02:45 UTC :   %UC_CALLMANAGER-3-DeviceUnregistered: %[DeviceName=DEVICENAME]
[IPAddress=172.23.136.216][Protocol=SIP][DeviceType=550][Description=Description][Reason=13]
[IPAddrAttributes=0][UNKNOWN_PARAMNAME:LastSignalReceived=SIPStationDPrimaryLineTimeout]
[AppID=Cisco CallManager][ClusterID=Cluster-ID][NodeID=NODEID]: Device unregistered
```


```
<179>10499: : : 7454: cisco.callmanager.test Aug 21 2020
17:02:45 UTC :   %UC_CALLMANAGER-3-DeviceUnregistered: %[DeviceName=DEVICENAME]
[IPAddress=172.23.136.216][Protocol=SIP][DeviceType=550][Description=Description][Reason=13]
[IPAddrAttributes=0][UNKNOWN_PARAMNAME:LastSignalReceived=SIPStationDPrimaryLineTimeout]
[AppID=Cisco CallManager][ClusterID=Cluster-ID][NodeID=NODEID]: Device unregistered
```


Table 351. Highlighted fields

QRadar field name	Highlighted payload field name
Log Source Time	**Aug 21 2020 17:02:45 UTC**
Event ID	**%UC_CALLMANAGER-3-DeviceUnregistered**
IP address	**IPAddress**

Table 351. Highlighted fields (continued)	
QRadar field name	**Highlighted payload field name**
Event Category	**AppID**
Event Name	**Device unregistered**

Cisco CatOS for Catalyst Switches

The IBM QRadar DSM for Cisco Catalyst Switches running Cisco CatOS accepts events by using syslog.

QRadar records all relevant device events. Before you configure a Cisco CatOS device in QRadar, you must configure your device to forward syslog events.

Configuring syslog forwarding for Cisco CatOS devices

Before you configure a Cisco CatOS device in IBM QRadar, you must configure your device to forward syslog events.

Procedure

1. Log in to your Cisco CatOS user interface.
2. Type the following command to access privileged EXEC mode:

   `enable`
3. Configure the system to **`timestamp`** messages:

   `set logging timestamp enable`
4. Type the following command with the IP address of IBM QRadar:

   `set logging server` <*IP address*>
5. Limit messages that are logged by selecting a severity level:

   `set logging server severity` <*server severity level*>
6. Configure the facility level to be used in the message. The default is local7.

   `set logging server facility` <*server facility parameter*>
7. Enable the switch to send syslog messages to the QRadar.

   `set logging server enable`

What to do next

You are now ready to configure the log source in QRadar.

Syslog log source parameters for Cisco CatOS for Catalyst Switches

If QRadar does not automatically detect the log source, add a Cisco CatOS for Catalyst Switches log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco CatOS for Catalyst Switches:

Table 352. Syslog log source parameters for the Cisco CatOS for Catalyst Switches DSM	
Parameter	**Value**
`Log Source type`	Cisco CatOS for Catalyst Switches
`Protocol Configuration`	Syslog

Table 352. Syslog log source parameters for the Cisco CatOS for Catalyst Switches DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco CatOS for Catalyst Switch device.

Related tasks

"Adding a log source" on page 5

Cisco CatOS for Catalyst Switches sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco CatOS for Catalyst Switches sample message when you use the Syslog protocol

Sample 1: The following sample event shows that a user logged in successfully.

```
<165>7622: Mar 12 09:19:27.675 PHT: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: user1]
[Source: 172.20.40.35] [localport: 22] at 09:19:27 PHT Mon Mar 12 2018
```


```
<165>7622: Mar 12 09:19:27.675 PHT: %SEC_LOGIN-SW1-5-LOGIN_SUCCESS: Login Success [user: user1]
[Source: 172.20.40.35] [localport: 22] at 09:19:27 PHT Mon Mar 12 2018
```


Table 353. Highlighted values in the Cisco CatOS for Catalyst Switches event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**LOGIN_SUCCESS**
Username	**user1**
Source IP	**172.20.40.35**

Sample 2: The following sample event shows that a user logged out successfully.

```
<166>7627: Mar 12 09:25:07.481 PHT: %SYS-SW1-6-LOGOUT: User qradar has exited tty session
3(172.20.40.35)
```


```
<166>7627: Mar 12 09:25:07.481 PHT: %SYS-SW1-6-LOGOUT: User qradar has exited tty session
3(172.20.40.35)
```


Table 354. Highlighted values in the Cisco CatOS for Catalyst Switches sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**LOGOUT**
Username	**qradar**
Source IP	**172.20.40.35**

Cisco Cloud Web Security

The IBM QRadar DSM for Cisco Cloud Web Security (CWS) collects web usage logs from a Cisco Cloud Web Security (CWS) storage by using an Amazon S3 - compatible API.

The following table describes the specifications for the Cisco Cloud Web Security DSM:

Table 355. Cisco Cloud Web Security DSM specifications

Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco Cloud Web Security
RPM file name	`DSM-CiscoCloudWebSecurity-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Amazon AWS S3 REST API
Event format	W3C
Recorded event types	All web usage logs
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Cisco CWS product information (https://www.cisco.com/go/cws)

To integrate Cisco Cloud Web Security with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website, in the order that they are listed, on your QRadar Console:
   - Protocol Common RPM
   - Amazon AWS REST API Protocol RPM
   - DSMCommon RPM
   - Cisco Cloud Web Security DSM RPM
2. Enable Log Extraction in your Cisco ScanCenter (administration portal).
3. Add a Cisco Cloud Web Security log source on the QRadar Console. The following table describes the parameters that require specific values for Cisco Cloud Web Security event collection:

Table 356. Cisco Cloud Web Security log source parameters

Parameter	**Value**
Log Source type	Cisco Cloud Web Security
Protocol Configuration	Amazon AWS S3 REST API
Log Source Identifier	The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you configured more than one Cisco CWS log source, you might want to identify the first log source as ciscocws1, the second log source as ciscocws2, and the third log source as ciscocws13.

Table 356. Cisco Cloud Web Security log source parameters (continued)	
Parameter	**Value**
Signature Version	Select **Signature Version 2**. If your Cisco CWS API is using **Signature Version 4**, contact your system administrator.
Region Name (Signature V4 only)	The region that is associated with the Amazon S3 bucket.
Service Name (Signature V4 only)	Type `s3`. The name of the Amazon Web Service.
Bucket Name	The name of the Cisco CWS bucket where the log files are stored.
Endpoint URL	`https://vault.scansafe.com/`
Public Key	The access key to enable log extraction from the Cisco CWS bucket.
Access Key	The secret key to enable log extraction from the Cisco CWS bucket.
Directory Prefix	The location of the root directory on the Cisco CWS storage bucket from where the Cisco CWS logs are retrieved. For example, the root directory location might be `cws-logs/`.
File Pattern	`.*?\.txt\.gz`
Event Format	**W3C**. The log source retrieves W3C text formatted events.
Use Proxy	When a proxy is configured, all traffic for the log source travels through the proxy so that QRadar can access the Amazon AWS S3 buckets. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, leave the **Proxy Username** and **Proxy Password** fields blank.
Automatically Acquire Server Certificate(s)	If you select **Yes**, QRadar downloads the certificate and begins trusting the target server.
Recurrence	Specifies how often the Amazon AWS S3 REST API Protocol connects to the Cisco CWS API to check for new files, and retrieves them if they exist. The format is M/H/D for Minutes/Hours/Days. The default is 5 M. Every access to an AWS S3 bucket incurs a monetary cost to the account that owns the bucket. Therefore, a smaller recurrence value increases the cost.

The following table shows a sample event message from Cisco Cloud Web Security:

Table 357. Cisco Cloud Web Security sample message

Event name	Low level category	Sample log message
c:comp - block	Access Denied	2016-08-22 18:22:34 GMT <IP_address1> <IP_address1> GET http www.example.com 80 / Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0 - 0 0 0 <IP_address2> c:comp Block all block category Computers and Internet <IP_address1> 0 Unknown 2016-08-22 18:22:34 GMT <IP_address1> <IP_address1> GET http www.example.com 80 / Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0 - 0 0 0 <IP_address2> c:comp Block all block category Computers and Internet <IP_address1> 0 Unknown

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Cloud Web Security to communicate with QRadar

To send events from Cloud Web Security to IBM QRadar, you must enable log extraction in Cisco CWS ScanCenter.

Before you begin

The log extraction service must be enabled and provisioned for your company. You must have super user administrator privileges to access the **Log Extraction** page.

Procedure

1. Log in to your Cisco ScanCenter account.
2. Click the **Admin** tab to view the administration menus.
3. From the **Your Account** menu, click **Log Extraction**.
4. In the **Actions** column in the **Credentials** area, click **Issue Key**.
5. In the **Warning** dialog box, click **Issue & Download**.

   A key pair is issued and the `keypair.csv` file is downloaded.

   The **Access Key** and **Last issued** column values are updated. The secret key does not display in the user interface (UI).
6. Open the `keypair.csv` file and make a copy of the **accessKey** and **secretKey**.

   The `keypair.csv` file contains a 20 character string access key and a 40 character string secret key. The key pair values that you copied are used when you configure the log source in QRadar.
7. From the **Connection Details** pane, copy and record the values in the **Endpoint** and **Bucket** columns.

   The connection details values that you copied are used when you configure the log source in QRadar.

What to do next

Configure the log source in QRadar.

For more information about Cisco CWS log extraction, see the *Cisco ScanCenter Administrator Guide, Release 5.2* on the Cisco website (https://search.cisco.com/search?query=cisco%20scancenter%20administrator%20guide&locale=enUS&tab=Cisco).

Related tasks

"Adding a log source" on page 5

Cisco CSA

You can integrate a Cisco Security Agent (CSA) server with IBM QRadar.

The Cisco CSA DSM accepts all events by using the syslog, SNMPv1 and SNMPv2 protocols. QRadar records all configured Cisco CSA alerts.

Configuring Cisco CSA to send events to IBM QRadar

Configuration of your Cisco CSA server to forward events.

About this task

Take the following steps to configure your Cisco CSA server to forward events:

Procedure

1. Open the **Cisco CSA** user interface.
2. Select **Events** > **Alerts**.
3. Click **New**.

   The **Configuration View** window is displayed.
4. Type in values for the following parameters:
   - **Name** - Type a name that you want to assign to your configuration.
   - **Description** - Type a description for the configuration. This step is not a requirement.
5. From the **Send Alerts**, select the event set from the list to generate alerts.
6. Select the **SNMP** check box.
7. Type a Community name.

   The Community name that is entered in the CSA user interface must match the Community name that is configured on IBM QRadar. This option is only available for the SNMPv2 protocol.
8. For the **Manager IP address** parameter, type the IP address of QRadar.
9. Click **Save**.

   You are now ready to configure the log source in QRadar.

Syslog log source parameters for Cisco CSA

If QRadar does not automatically detect the log source, add a Cisco CSA log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco CSA devices:

Table 358. Syslog log source parameters for the Cisco CSA DSM	
Parameter	**Value**
Log Source type	Cisco CSA
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco CSA device.

Related tasks

"Adding a log source" on page 5

SNMPv1 log source parameters for Cisco CSA

If QRadar does not automatically detect the log source, add a Cisco CSA log source on the QRadar Console by using the SNMPv1 protocol.

When using the SNMPv1 protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMPv1 events from Cisco CSA devices:

Table 359. SNMPv1 log source parameters for the Cisco CSA DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source type	Cisco CSA
Protocol Configuration	SNMPv1
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco CSA device.
Community	Type the SNMP community name required to access the system containing SNMP events. The default is Public.
Include OIDs in Event Payload	Clear the Include OIDs in Event Payload checkbox, if selected. This options allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.

Related tasks

"Adding a log source" on page 5

SNMPv2 log source parameters for Cisco CSA

If QRadar does not automatically detect the log source, add a Cisco CSA log source on the QRadar Console by using the SNMPv2 protocol.

When using the SNMPv2 protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMPv2 events from Cisco CSA devices:

Table 360. SNMPv2 log source parameters for the Cisco CSA DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source type	Cisco CSA
Protocol Configuration	SNMPv2
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco CSA device.
Community	Type the SNMP community name required to access the system containing SNMP events. The default is Public.
Include OIDs in Event Payload	Clear the Include OIDs in Event Payload checkbox, if selected. This options allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.

For more information about the SNMPv2 protocol, see SNMPv2 protocol configuration options.

Related tasks

"Adding a log source" on page 5

Cisco Duo

The IBM QRadarDSM for Cisco Duo collects Cisco Duo logs by using the Cisco Duo protocol.

To integrate Cisco Duo with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - Universal Cloud REST API protocol
   - Cisco Duo protocol RPM
   - Cisco Duo DSM RPM
2. Configure Cisco Duo to communicate with QRadar by configuring the Admin API on your Cisco Duo dashboard. For more information, see Configuring Cisco Duo to communicate with QRadar.
3. Add a Cisco Duo log source on the QRadar Console by using the Cisco Duo protocol. For more information, see Cisco Duo protocol log source parameters for Cisco Duo.

Related tasks

"Adding a DSM" on page 4

“Adding a log source” on page 5

Cisco Duo DSM specifications

When you configure the Cisco Duo DSM, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported version of Cisco Duo is before you begin can help reduce frustration during the configuration process.

The QRadar DSM for Cisco Duo collects authentication events from the Cisco Duo Admin API.

The following table describes the specifications for the Cisco Duo DSM.

Table 361. Cisco Duo DSM specifications

Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco Duo
RPM file name	DSM-*CiscoDuoSecurity-QRadar_version-build_number*.noarch.rpm
Supported version	Admin API v2
Protocol	Cisco Duo
Event format	JSON
Recorded event types	Authentication logs
Automatically discovered?	yes
Includes identity?	yes
Includes custom properties?	no
More information	Cisco Duo documentation about the Admin API (https://duo.com/docs/adminapi#about-the-admin-api)

Configuring Cisco Duo to communicate with QRadar

Before you can add a log source in IBM QRadar, you need to configure the Admin API from your Cisco Dashboard.

Procedure

1. Log in to the Duo Admin Panel as an administrator.
2. Go to **Applications**, then click **Protect an Application**.
3. Find **Admin API** in the list, then click **Protect**.
4. From the permissions menu, select **Grant read log** permission.

   This permission is required for the Cisco Duo protocol to read authentication logs from the Admin API.
5. Record the values for the **Integration Key**, **Secret Key**, and **API hostname**. You need these values when you configure the Cisco Duo log source in QRadar.
6. Click **Save changes**.

   Important: Because Cisco Duo has rate limits on API calls, you can create only one log source for each customer account.

Related tasks

“Adding a log source” on page 5

Cisco Duo protocol log source parameters for Cisco Duo

If QRadar does not automatically detect the log source, add a Cisco Duo log source on the QRadar Console by using the Cisco Duo protocol.

When you use the Cisco Duo protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect authentication events from the Cisco Duo Admin API:

Table 362. Cisco Duo log source parameters for the Cisco Duo DSM

Parameter	Value
Log Source type	Cisco Duo
Protocol Configuration	Cisco Duo
Log Source Identifier	Type a unique name for the log source as an identifier for events from Cisco Duo. The value of the **Log Source Identifier** parameter must match the **Host** parameter when you are using the Cisco Duo default workflow. If the Cisco Duo default workflow is modified, then the **Log Source Identifier** must match the **Source** value - `source="${/host}"` that is used under the `PostEvents` section. For more information, see Cisco Duo protocol workflow.

For a complete list of Cisco Duo protocol parameters and their values, see Cisco Duo protocol configuration options.

Related tasks

Adding a log source

Cisco Duo sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco Duo sample message when you use the Cisco Duo protocol

Sample 1: The following sample event message shows that a customer successfully enrolled with Cisco Duo.

```
{"access_device":
{"browser":"Firefox","browser_version":"84.0","epkey":null,"flash_version":"uninstalled","hostna
me":null,"ip":"10.120.139.72","is_encryption_enabled":"unknown","is_firewall_enabled":"unknown",
"is_password_set":"unknown","java_version":"uninstalled","location":
{"city":"city","country":"country","state":"state"},"os":"Mac OS
X","os_version":"11.0","security_agents":"unknown"},"alias":"unknown","application":
{"key":"1111111111AAAAAAAAAA","name":"1Password"},"auth_device":{"ip":null,"location":
{"city":null,"country":null,"state":null},"name":"514-894-3479"},"email":null,"event_type":"enro
llment","factor":"sms_passcode","isotimestamp":"2021-10-04T19:40:32.385977+00:00","ood_software"
:null,"reason":null,"result":"success","timestamp":1633376432,"trusted_endpoint_status":"unknown
","txid":"1a32fe06-cc6c-4a34-9f08-43e23fb1f4b3","user":{"groups":
[],"key":"1111111111AAAAAAAABB","name":"test.user@example.com"}}
```

Table 363. Highlighted fields in the Cisco Duo event

QRadar field name	Highlighted payload field name
Event ID	**event_type**

Table 363. Highlighted fields in the Cisco Duo event (continued)	
QRadar field name	**Highlighted payload field name**
Source IP	**ip**
Username	**name**

Sample 2: The following sample event message shows that an end user approved an authentication request.


```
{"access_device":
{"browser":null,"browser_version":null,"epkey":null,"flash_version":null,"hostname":null,"ip":"1
0.10.10.10","is_encryption_enabled":"unknown","is_firewall_enabled":"unknown","is_password_set":
"unknown","java_version":null,"location":
{"city":null,"country":null,"state":null},"os":null,"os_version":null,"security_agents":"unknown
"},"alias":"testuser","application":{"key":"1111111111AAAAAAAAAA","name":"macOS"},"auth_device":
{"ip":"142.120.139.72","location":
{"city":"Ottawa","country":"Canada","state":"Ontario"},"name":"514-894-3479"},"email":"test.user
@example.com","event_type":"authentication","factor":"duo_push","isotimestamp":"2021-10-06T14:22
:47.921053+00:00","ood_software":null,"reason":"user_approved","result":"success","timestamp":16
33530167,"trusted_endpoint_status":"unknown","txid":"73eb9ca7-45d1-4f97-
af0b-7c15700f6f2f","user":{"groups":[],"key":"1111111111AAAAAAAABB","name":"testuser"}}
```


Table 364. Highlighted fields in the Cisco Duo sample event	
QRadar field name	**Highlighted payload field name**
Event ID	**reason**
Source IP	**ip**
Username	**name**
Identity IP	**ip**
Identity Username	**name**

Cisco Firepower Management Center

The IBM QRadar DSM for Cisco Firepower Management Center collects Cisco Firepower Management Center events by using the eStreamer API service.

Cisco Firepower Management Center is formerly known as Cisco FireSIGHT Management Center.

QRadar supports Cisco Firepower Management Center V 5.2 to V 7.1.

Configuration overview

To integrate QRadar with Cisco Firepower Management Center, you must create certificates in the Firepower Management Center interface, and then add the certificates to the QRadar appliances that receive eStreamer event data.

If your deployment includes multiple Cisco Firepower Management Center appliances, you must copy the certificate for each appliance that sends eStreamer events to any temporary location on the QRadar Event Collector. The certificate allows the Cisco Firepower Management Center appliance and the QRadar Console or QRadar Event Collectors to communicate by using the eStreamer API to collect events.

To integrate QRadar with Cisco Firepower Management Center, complete the following steps:

1. Create the eStreamer certificate on your Firepower Management Center appliance. For more information about creating eStreamer certificates, see “Creating Cisco Firepower Management Center 5.x, 6.x, and 7.x certificates” on page 650.
2. Import a Cisco Firepower Management Center certificate in QRadar. For more information about importing a certificate, see “Importing a Cisco Firepower Management Center certificate in QRadar” on page 651.

3. Add a Cisco Firepower Management Center log source on the QRadar Console. For more information about Cisco Firepower Management Center log source parameters, see "Cisco Firepower Management Center log source parameters" on page 652.

Supported event types

QRadar supports the following event types from Cisco Firepower Management Center:

- Discovery Events
- Correlation and White List Events
- Impact Flag Alerts
- User Activity
- Malware Events
- File Events
- Connection Events
- Intrusion Events
- Intrusion Event Packet Data
- Intrusion Event Extra Data

Intrusion events that are categorized by the Cisco Firepower Management Center DSM in QRadar use the same QRadar Identifiers (QIDs) as the Snort DSM to ensure that all intrusion events are categorized properly.

Intrusion events in the 1,000,000 - 2,000,000 range are user-defined rules in Cisco Firepower Management Center. User-defined rules that generate events are added as an **Unknown** event in QRadar, and include additional information that describes the event type. For example, a user-defined event can identify as **Unknown:Buffer Overflow** for Cisco Firepower Management Center.

The following table provides sample event messages for the Cisco Firepower Management Center DSM:

Table 365. Cisco Firepower Management Center sample messages supported by the Cisco Firepower Management Center device.

Event name	Low level category	Sample log message
User Login Change Event	Computer Account Changed	DeviceType=Estreamer DeviceAddress =<IP_address> CurrentTime=150774 0597988 netmapId=0 recordTyp e=USER_LOGIN_CHANGE_EVENT record Length=142 timestamp=01 May 201 5 12:13:50 detectionEngineRef= 0 ipAddress=<IP_address> MACAddres s=<MAC_address> hasIPv6=tru e eventSecond=1430491035 eve ntMicroSecond=0 eventType=USER_ LOGIN_INFORMATION fileNumber=00 000000 filePosition=00000000 ipV6Address=<IPv6_address> userLoginInformation.timestamp= 1430491035 userLoginInformati on.ipv4Address=<IP_address> userLog inInformation.userName=username userLoginInformation.userRef=0 userLoginInformation.protocol Ref=710 userLoginInformation.ema il= userLoginInformation.ipv6Ad dress=<IP_address> userLoginIn formation.loginType=0 userLogi nInformation.reportedBy=IPAddress"

Table 365. Cisco Firepower Management Center sample messages supported by the Cisco Firepower Management Center device. (continued)

Event name	Low level category	Sample log message
User Removed Change Event	User Account Removed	DeviceType=Estreamer DeviceAddress =<IP_address> CurrentTime=15077 43344985 netmapId=0 recordTyp e=USER_REMOVED_CHANGE_EVENT reco rdLength=191 timestamp=21 Sep 201 7 14:53:14 detectionEngineRef= 0 ipAddress=<IP_address> MACAddress =<MAC_address> hasIPv6=tru e eventSecond=1506016392 event MicroSecond=450775 eventType=DELE TE_USER_IDENTITY fileNumber=0000 0000 filePosition=00000000 ip V6Address=<IPv6_address> userIn formation.id=1 userInformatio n.userName=username userInformat ion.protocol=710 userInformation .firstName=firstname userInformation .lastName=lastname userInformation .email=EmailAddress userInformation.department=R esearch userInformation.phone =000-000-0000
INTRUSION EVENT EXTRA DATA RECORD	Information	DeviceType=Estreamer DeviceAddress =<IP_address> CurrentTime=150774 0690263 netmapId=0 recordType= INTRUSION_EVENT_EXTRA_DATA_RECORD r ecordLength=49 timestamp=01 May 20 15 15:32:53 eventExtraData.eventId= 393275 eventExtraData.eventSecond= 1430505172 eventExtraData.managed Device.managedDeviceId=6 eventExtr aData.managedDevice.name=manageddevic e.<Server>.example.com eventExtraData .extraDataType.eventExtraDataType.ty pe=10 eventExtraData.extraDataTyp e.eventExtraDataType.name=HTTP Hostn ame eventExtraData.extraDataType .eventExtraDataType.encoding=String eventExtraData.extraData= www.example.com
RUA User record	Information	DeviceType=Estreamer DeviceAddress =<IP_address> CurrentTime=15077 40603372 netmapId=0 recordTyp e=RUA_USER_RECORD recordLength= 21 timestamp=11 Oct 2017 13:50: 02 userRef=2883 protocolRef= 710 userName=UserName

Related tasks

“Adding a DSM” on page 4

Related information

Cisco: Firepower Management Center DSM and changes to auto discovered syslog events

Creating Cisco Firepower Management Center 5.x, 6.x, and 7.x certificates

IBM QRadar requires a certificate for every Cisco Firepower Management Center appliance in your deployment. Certificates are generated in pkcs12 format and must be converted to a keystore and a truststore file, which are usable by QRadar appliances.

Procedure

1. Log in to your Cisco Firepower Management Center interface.
   - If you are using version 5.x, select **System** > **Local** > **Registration**.
   - If you are using version 6.x, select **System** > **Integration**.
   - If you are using version 7.x, click the **System** gear icon, then select **Integration**.
2. Click the **eStreamer** tab.
3. Select the types of events that you want Cisco Firepower Management Center to send to QRadar, and then click **Save**.

   The following image lists the types of events that Cisco Firepower Management Center sends to QRadar.

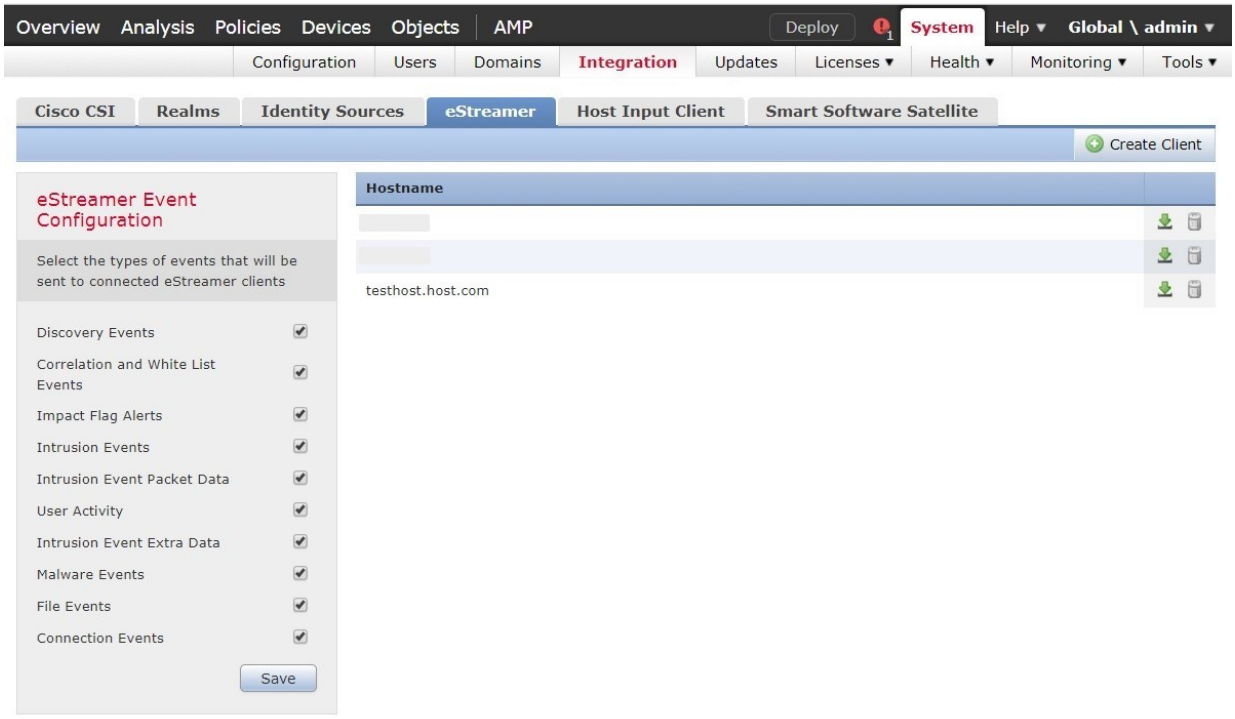


Figure 34. Cisco Firepower Management Center eStreamer Event Configuration

4. Click **Create Client** in the upper right side of the window.
5. In the **Hostname** field, type the IP address or host name, depending on which of the following conditions applies to your environments.
   - If you use a QRadar Console or you use a QRadar All-in-One appliance to collect eStreamer events, type the IP address or host name of your QRadar Console.
   - If you use a QRadar Event Collector to collect eStreamer events, type the IP address or host name for the Event Collector.
   - If you use QRadar High Availability (HA), type the virtual IP address.
6. In the **Password** field, type a password for your certificate. If you choose to provide a password, the password is required to import the certificate.
7. Click **Save**.

The new client is added to the eStreamer Client list and the host can communicate with the eStreamer API on port 8302.

8. Click **Download Certificate** for your host to save the pkcs12 certificate to a file location.
9. Click **OK** to download the file.

What to do next

You are now ready to import your Cisco Firepower Management Center certificate to your QRadar appliance.

Related tasks

"Importing a Cisco Firepower Management Center certificate in QRadar" on page 651

The `estreamer-cert-import.pl` script for QRadar converts your pkcs12 certificate file to a keystore and truststore file and copies the certificates to your QRadar appliance. Repeat this procedure for each Firepower Management Center pkcs12 certificate that you need to import to your QRadar Console or Event Collector.

Importing a Cisco Firepower Management Center certificate in QRadar

The `estreamer-cert-import.pl` script for QRadar converts your pkcs12 certificate file to a keystore and truststore file and copies the certificates to your QRadar appliance. Repeat this procedure for each Firepower Management Center pkcs12 certificate that you need to import to your QRadar Console or Event Collector.

Before you begin

You must have `root` or `su - root` privileges to run the `estreamer-cert-import.pl` import script.

About this task

The `estreamer-cert-import.pl` import script is stored on your QRadar Event Collector when you install the Cisco Firepower eStreamer protocol.

The script converts and imports only 1 pkcs12 file at a time. You are required to import a certificate only for the QRadar appliance that receives the Firepower Management Center events. For example, after the Firepower Management Center event is categorized and normalized by an Event Collector in a QRadar deployment, it is forwarded to the QRadar Console. In this scenario, you would import a certificate to the Event Collector.

When you import a new certificate, existing Firepower Management Center certificates on the QRadar appliance are renamed to `estreamer.keystore.old` and `estreamer.truststore.old`.

Procedure

1. Log in as the root user by using SSH on the QRadar appliance that will receive the events.
2. Copy the downloaded certificate from your Firepower Management Center appliance to a temporary directory on the QRadar Event Collector.
3. Type the following command to import your pkcs12 file.

```
/opt/qradar/bin/estreamer-cert-import.pl -f <pkcs12_absolute_filepath> options
```

The **`-f`** parameter is required. All other parameters that are described in the following table are optional.

Table 366. Import script command parameters

Parameter	Description
`-f`	Identifies the file name of the pkcs12 files to import.

Table 366. Import script command parameters (continued)	
Parameter	**Description**
-o	Overrides the default eStreamer name for the keystore and truststore files. Use the **-o** parameter when you integrate multiple Firepower Management Center devices. For example, `/opt/qradar/bin/estreamer-cert-import.pl -f <file name> -o <IP_address>` The import script creates the following files: • `/opt/qradar/conf/<IP_address>.keystore` • `/opt/qradar/conf/<IP_address>.truststore`
-d	Enables verbose mode for the import script. Verbose mode is intended to display error messages for troubleshooting purposes when pkcs12 files fail to import properly.
-p	Specifies a password if a password was provided when you generated the pkcs12 file.
-v	Displays the version information for the import script.
-h	Displays a help message about using the import script.

Results

The import script displays the location where the import files were copied.

Example:

```
[root@VM199-22 ~]# /opt/qradar/bin/estreamer-cert-import.pl -f yourCertificate.pkcs12 -o 61estreamer
Successfully generated truststore file [/opt/qradar/conf/61estreamer.truststore].
Successfully generated keystore file [/opt/qradar/conf/61estreamer.keystore].
```

Figure 35. Sample import script output

Cisco Firepower Management Center log source parameters

When you add a Cisco Firepower Management Center log source on the QRadar Console by using the Cisco Firepower eStreamer protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Cisco Firepower Management Center events from the eStreamer API service.

Table 367. Cisco Firepower eStreamer protocol log source parameters for the Cisco Firepower Management Center DSM	
Parameter	**Value**
Log Source type	Cisco Firepower Management Center
Protocol Configuration	Cisco Firepower eStreamer

For a complete list of Cisco Firepower eStreamer protocol parameters and their values, see Cisco Firepower eStreamer protocol configuration options.

Related tasks

"Adding a log source" on page 5

Cisco Firepower Threat Defense

The IBM QRadar DSM for Cisco Firepower Threat Defense (FTD) collects syslog events from a Cisco Firepower Threat Defense appliance. The syslog events that are collected by the Cisco Firepower Threat Defense DSM were previously collected by the Cisco Firepower Management Center DSM.

QRadar collects the following event types from Cisco Firepower Threat Defense appliances:

- Device health and network-related logs from FTD devices
- Connection, security intelligence, and intrusion logs from FTD devices
- Logs for file and malware events.

For more information about syslog message types for Cisco Firepower Threat Defense, see Firepower Syslog Message Types on the Cisco website. (https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/analyze_events_using_external_tools.html#id_85461)

To integrate Cisco Firepower Threat Defense with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Cisco Firepower Threat Defense DSM RPM
   - Cisco Firewall Devices DSM RPM
2. Configure your Cisco Firepower Threat Defense device to send events to QRadar. For more information, see Configuring Cisco Firepower Threat Defense to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a Cisco Firepower Threat Defense log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Cisco Firepower Threat Defense DSM specifications

When you configure the Cisco Firepower Threat Defense, understanding the specifications for the Cisco Firepower Threat Detection DSM can help ensure a successful integration. For example, knowing what the supported version of Cisco Firepower Threat Defense is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Cisco Firepower Threat Defense DSM.

Table 368. Cisco Firepower Threat Defense DSM specifications

Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco Firepower Threat Defense
RPM file name	`DSM-CiscoFirepowerThreatDefense-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported version	6.3
Protocol	Syslog

Table 368. Cisco Firepower Threat Defense DSM specifications (continued)	
Specification	**Value**
Event format	Syslog Comma-separated values (CSV) Name-value pair (NVP)
Recorded event types	Intrusion Connection
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Firepower Management Center Configuration Guide, Version 6.6 (https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/analyze_events_using_external_tools.html)

Configuring Cisco Firepower Threat Defense to communicate with QRadar

To send intrusion or connection events to QRadar by using the syslog protocol, you need to enable external logging and configure basic settings on your Cisco Firepower appliance.

Procedure

1. Log in to your Cisco Firewall appliance.
2. Enable external logging. For more information, see FTD Platform Settings That Apply to Security Event Syslog Messages (https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/platform_settings_for_firepower_threat_defense.html#id_84926).
3. Enable Logging Destinations. For more information, see FTD Platform Settings That Apply to Security Event Syslog Messages (https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/platform_settings_for_firepower_threat_defense.html#id_84926).
4. Deploy changes. For more information, see Deploy Configuration Changes (https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/policy_management.html#task_75E181687ECF4EFC8EB6AF4509C20C0B).

What to do next

If QRadar does not automatically detect the log source, add a log source in QRadar. For more information, see Adding a log source.

Configuring QRadar to use previous connection event processing for Cisco Firepower Threat Defense

If you want to change the way that IBM QRadar parses connection events an enable earlier behavior without adding action results, use the DSM Editor to enable previous connection event processing.

By default, Cisco Firepower Threat Defense connection events are extended with firewall action results **ALLOW** or **BLOCK**.

Procedure

1. On the **Admin** tab, in the **Data Sources** section, click **DSM Editor**.
2. From the **Select Log Source Type** window, select **Cisco Firepower Threat Defense** from the list, and then click **Select**.
3. Click the **Configuration** tab, and then set **Display DSM Parameters Configuration** to on.
4. Set **Use Previous Connection Event Processing** to on.
5. Click **Save**.

Cisco Firepower Threat Defense sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Cisco Firepower Threat Defense sample message when you use the Syslog protocol

The following sample shows an intrusion event that has a Generator ID (GID) and Snort IDs (SID).

```
Aug 14 08:59:30 192.168.0.7 SFIMS : %FTD-5-430001: Protocol: tcp, SrcIP: 10.1.1.57, DstIP:
10.5.12.209, SrcPort: 2049, DstPort: 746, Priority: 1, GID: 1, SID: 648, Revision: 18,
Message: \"INDICATOR-SHELLCODE x86 NOOP\", Classification: Executable Code was Detected, User:
No Authentication Required, ACPolicy: test, NAPPolicy: Balanced Security and Connectivity,
InlineResult: Blocked
```

Table 369. Highlighted values in the Cisco Firepower Threat Defense sample event message

QRadar field name	Highlighted payload values
Event ID	As an intrusion event, a concatenation of the **GID** and **SID** is used.
Category	As an intrusion event, the category is set to Snort.
Device Time	If not provided in the DSM, **Aug 14 08:59:30** is taken from the syslog header.
Source IP	**SrcIP**
Destination IP	**DstIP**
Source Port	**SrcPort**
Destination Port	**DstPort**
Protocol	**Protocol**
Severity	**5** The value in this field is converted and mapped to an appropriate QRadar severity value.

Cisco FWSM

You can integrate Cisco Firewall Service Module (FWSM) with IBM QRadar.

The Cisco FWSM DSM for QRadar accepts FWSM events by using syslog. QRadar records all relevant Cisco FWSM events.

Configuring Cisco FWSM to forward syslog events

To integrate Cisco FWSM with IBM QRadar, you must configure your Cisco FWSM appliances to forward syslog events to QRadar.

Procedure

1. Use a console connection, telnet, or SSH, to log in to the Cisco FWSM.
2. Enable logging:

   `logging on`
3. Change the logging level:

   `logging trap` <*level*>

   Where <*level*> is set from levels 1-7. By default, the logging trap level is set to 3 (error).
4. Designate QRadar as a host to receive the messages:

   `logging host` [*interface*] *ip_address [tcp[/port] | udp[/port]] [format emblem]*

   For example:

   `logging host dmz1 192.0.2.1`

   Where 192.0.2.1 is the IP address of your QRadar system.

   You are now ready to configure the log source in QRadar.

Syslog log source parameters for Cisco FWSM

If QRadar does not automatically detect the log source, add a Cisco FWSM log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco FWSM :

Table 370. Syslog log source parameters for the Cisco FWSM DSM

Parameter	Value
Log Source type	Cisco Firewall Services Module (FWSM)
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco FWSM device.

Related tasks

"Adding a log source" on page 5

Cisco Identity Services Engine

The IBM QRadar DSM for Cisco Identity Services Engine (ISE) collects device events from Cisco ISE appliances by using the UDP multiline syslog protocol.

The following table describes the specifications for the Cisco Identity Services Engine DSM:

Table 371. Cisco Identity Services Engine DSM specifications	
Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco Identity Services Engine
RPM file name	`DSM-CiscoISE-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	1.1 to 2.2
Protocol	UDP Multiline Syslog
Event format	Syslog
Recorded event types	Device events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Cisco website (https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html)

To integrate Cisco ISE with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs on your QRadar Console. RPMs are available for download from the IBM support website (http://www.ibm.com/support):
   - DSMCommon RPM
   - Cisco Identity Services Engine DSM RPM
2. Configure your Cisco ISE appliance to send UDP multiline syslog events to QRadar.
3. Add a Cisco Identity Services Engine log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from Cisco ISE:

Table 372. Cisco Identity Services Engine log source parameters	
Parameter	**Value**
Log Source type	Cisco Identity Service Engine
Protocol Configuration	UDP Multiline Syslog
Log Source Identifier	The IP address or host name of the Cisco Identity Service Engine device that sends UDP Multiline Syslog events to QRadar.

Table 372. Cisco Identity Services Engine log source parameters (continued)	
Parameter	**Value**
Listen Port	Type 517 as the port number used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65535. **Note:** UDP Multiline Syslog events can be assigned to any port that is not in use, except for port 514. The default port that is assigned to the UDP Multiline protocol is UDP port 517. For a list of ports that are used by QRadar, see *Common ports and servers used by QRadar* in the *IBM QRadar Administration Guide* or in the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_ports_and_servers.html). To edit a saved configuration to use a new port number, complete the following steps: a. In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events. b. Click **Save**. The port update is complete and event collection starts on the new port number.
Message ID Pattern	Type the following regular expression (regex) to filter the event payload messages: `CISE_\S+ (\d{10})`

For a complete list of UDP multiline syslog protocol parameters and their values, see UDP multiline syslog protocol configuration options.

4. Configure a remote logging target on your Cisco ISE appliance.
5. Configure the event logging categories on your Cisco ISE appliance.

Related concepts

"UDP multiline syslog protocol configuration options" on page 233
To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5
"Configuring a remote logging target in Cisco ISE" on page 659
To forward syslog events to IBM QRadar, you must configure your Cisco ISE appliance with a remote logging target.

"Configuring logging categories in Cisco ISE" on page 659

The Cisco Identity Services Engine DSM for IBM QRadar collects syslog events from multiple event logging categories. To define which events are forwarded to QRadar, you must configure each event logging category on your Cisco ISE appliance.

Configuring a remote logging target in Cisco ISE

To forward syslog events to IBM QRadar, you must configure your Cisco ISE appliance with a remote logging target.

Procedure

1. Log in to your Cisco ISE Administration Interface.
2. From the navigation menu, select **Administration** > **System** > **Logging** > **Remote Logging Targets**.
3. Click **Add**, and then configure the following parameters:

Option	Description
Name	Type a unique name for the remote target system.
Description	You can uniquely identify the target system for users.
IP Address	Type the IP address of the QRadar Console or Event Collector.
Port	Type 517 or use the port value that you specified in your Cisco ISE log source for QRadar
Facility Code	From the **Facility Code** list, select the syslog facility to use for logging events.
Maximum Length	Type 1024 as the maximum packet length allowed for the UDP syslog message.

4. Click **Submit**.

What to do next

Configure the logging categories that are forwarded by Cisco ISE to QRadar.

Configuring logging categories in Cisco ISE

The Cisco Identity Services Engine DSM for IBM QRadar collects syslog events from multiple event logging categories. To define which events are forwarded to QRadar, you must configure each event logging category on your Cisco ISE appliance.

Procedure

1. Log in to your Cisco ISE Administration Interface.
2. From the navigation menu, select **Administration** > **System** > **Logging** > **Logging Categories**.

   The following list shows the supported event logging categories for the IBM QRadar DSM for Cisco Identity Services Engine:

   - AAA audit
   - Failed attempts
   - Passed authentication
   - AAA diagnostics
   - Administrator authentication and authorization
   - Authentication flow diagnostics
   - Identity store diagnostics
   - Policy diagnostics
   - Radius diagnostics

- Guest
- Accounting
- Radius accounting
- Administrative and operational audit
- Posture and client provisioning audit
- Posture and client provisioning diagnostics
- Profiler
- System diagnostics
- Distributed management
- Internal operations diagnostics
- System statistics

3. Select an event logging category, and then click **Edit**.
4. From the **Log Severity** list, select a severity for the logging category.
5. In the **Target** field, add your remote logging target for QRadar to the **Select** box.
6. Click **Save**.
7. Repeat this process for each logging category that you want to forward to QRadar.

   Events that are forwarded by Cisco ISE are displayed on the **Log Activity** tab in QRadar.

Cisco Identity Services Engine sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Cisco Identity Services Engine sample message when you use the UDP multiline syslog protocol

The following sample event shows that the endpoint failed authentication several times for the same scenario and was rejected.

```
<181>Aug  9 07:36:33 cisco.ise.test CISE_Failed_Attempts 0038700411 4 0 2018-08-09 07:36:3
3.085 +00:00 0762919669 5449 NOTICE RADIUS: Endpoint failed authentication of the same scenario
severa
l times and was rejected, ConfigVersionId=582, Device IP Address=172.23.104.125, Device
Port=43017, De
stinationIPAddress=172.23.100.5, DestinationPort=1812, RadiusPacketType=AccessRequest,
UserName=qradar
, Protocol=Radius, NetworkDeviceName=TE-ST-TES-TTE-ST1, User-Name=12a3412341b2 NAS-IP-
Address=172.23.1
04.125, NAS-Port=8, Service-Type=Framed, Framed-MTU=1300,
State=37CPMSessionID=7d6817ac01e6f8114dee6b5
b\;42SessionID=cisco.ise.test/319421106/32782955\;, Called-Station-ID=00-00-5E-00-53-83:LOFIMO,
Callin
g-Station-ID=00-00-5E-00-53-A2, NAS-Identifier=TE-ST-TES-TTE-ST1 Acct-Session-Id=5b6bee4d/
00:00:5E:00:
53:64/33045704, NAS-Port-Type=Wireless - IEEE 802.11, Tunnel-Type=(tag=0) VLAN, Tunnel-Medium-
Type=(ta
g=0) 802, Tunnel-Private-Group-ID=(tag=0) 40, Chargeable-User-Identity=\}, Location-
Capable=00:00:00:01,
```

```
<181>Aug  9 07:36:33 cisco.ise.test CISE_Failed_Attempts 0038700411 4 0
2018-08-09 07:36:33.085 +00:00 0762919669 5449 NOTICE RADIUS: Endpoint
failed authentication of the same scenario several times and was
rejected, ConfigVersionId=582, Device IP Address=172.23.104.125, Device Port=43017,
DestinationIPAddress=172.23.100.5, DestinationPort=1812, RadiusPacketType=AccessRequest,
UserName=qradar, Protocol=Radius, NetworkDeviceName=TE-ST-TES-TTE-ST1, User-Name=12a3412341b2
NAS-IP-Address=172.23.104.125, NAS-Port=8, Service-Type=Framed, Framed-MTU=1300,
State=37CPMSessionID=7d6817ac01e6f8114dee6bb\;42SessionID=cisco.ise.test/319421106/32782955\;,
Called-Station-ID=00-00-5E-00-53-83:LOFIMO, Calling-Station-ID=00-00-5E-00-53-A2, NAS-
Identifier=TE-ST-TES-TTE-ST1 Acct-Session-Id=5b6bee4d/00:00:5E:00:53:64/33045704, NAS-Port-
```

```
Type=Wireless - IEEE 802.11, Tunnel-Type=(tag=0) VLAN, Tunnel-Medium-Type=(tag=0) 802, Tunnel-
Private-Group-ID=(tag=0) 40, Chargeable-User-Identity=\}, Location-Capable=00:00:00:01,
```

Cisco IDS/IPS

You can integrate a Cisco IDS/IPS security device with IBM QRadar.

The Cisco IDS/IPS DSM for IBM QRadar collects Cisco IDS/IPS for events by using the Security Device Event Exchange (SDEE) protocol.

The SDEE specification defines the message format and the protocol that is used to communicate the events that are generated by your Cisco IDS/IPS security device. QRadar supports SDEE connections by polling directly to the IDS/IPS device and not the management software, which controls the device.

Note: You must have security access or web authentication on the device before you connect to QRadar.

After you configure your Cisco IDS/IPS device, you must configure the SDEE protocol in QRadar. When you configure the SDEE protocol, you must define the URL that is used to access the device. An example of a URL that defines the device is `https//www.example.com/cgi-bin/sdee-server`.

You must use `http` or `https` in the URL, which is specific to your Cisco IDS version.

- When you use RDEP (for Cisco IDS 4.0), ensure that the URL has `/cgi-bin/event-server` at the end of the URL. An example URL is `https://www.example.com/cgi-bin/event-server`.
- When you use SDEE/CIDEE (for Cisco IDS 5.x and later), ensure that the URL has `/cgi-bin/sdee-server` at the end of the URL. An example URL is `https://www.example/cgi-bin/sdee-server`.

SDEE log source parameters for Cisco IDS/IPS

If QRadar does not automatically detect the log source, add a Cisco Intrusion Prevention System (IPS) log source on the QRadar Console by using the Security Device Event Exchange (SDEE) protocol.

The following table describes the parameters that require specific values to collect SDEE events from Cisco IDS/IPS devices:

Table 373. SDEE log source parameters for the Cisco IDS/IPS DSM

Parameter	Value
Log Source type	Cisco Intrusion Prevention System (IPS)
Protocol Configuration	SDEE
Log Source Identifier	Type an IP address, host name, or name to identify the SDEE event source. The identifier helps you determine which events came from your Cisco IDS/IPS device.
URL	Type the URL address to access the log source. You must use an `http` or `https` in the URL. Here are some examples: • If you are using SDEE/CIDEE (for Cisco IDS v5.x and later), check that `/cgi-bin/sdee-server` is at the end of the URL. For example, `https://www.example.com/cgi-bin/sdee-server`. • If you are using RDEP (for Cisco IDS v4.0), check that `/cgi-bin/event-server` is at the end of the URL. For example, `https://www.example.com/cgi-bin/event-server`.

Table 373. SDEE log source parameters for the Cisco IDS/IPS DSM (continued)	
Parameter	**Value**
Username	Type the user name. This user name must match the SDEE URL user name that is used to access the SDEE URL. The user name can be up to 255 characters in length.
Password	Type the user password. This password must match the SDEE URL password that is used to access the SDEE URL. The password can be up to 255 characters in length.
Events / Query	Type the maximum number of events to retrieve per query. The valid range is 0 - 501 and the default is 100.
Force Subscription	Select this check box if you want to force a new SDEE subscription. The check box forces the server to drop the least active connection and accept a new SDEE subscription connection for this log source. By default, the check box is selected. Clearing the check box continues with any existing SDEE subscription.
Severity Filter Low	Select this check box if you want to configure the severity level as low. Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.
Severity Filter Medium	Select this check box if you want to configure the severity level as medium. Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.
Severity Filter High	Select this check box if you want to configure the severity level as high. Log sources that support SDEE return only the events that match this severity level. By default, the check box is selected.

For a complete list of SDEE protocol parameters and their values, see "SDEE protocol configuration options" on page 208.

Related tasks

"Adding a log source" on page 5

Cisco IOS

The IBM QRadar DSM for Cisco IOS accepts Cisco IOS events by using syslog. QRadar records all relevant events.

The following Cisco switches and routers are automatically discovered as Cisco IOS series devices, and their events are parsed by the DSM for Cisco IOS:

- Cisco 12000 Series Routers
- Cisco 6500 Series Switches
- Cisco 7600 Series Routers
- Cisco Carrier Routing System
- Cisco Integrated Services Router.

Make sure that all access control lists (ACLs) are set to LOG.

Configuring Cisco IOS to forward events

You can configure a Cisco IOS-based device to forward events.

About this task

Take the following steps to configure your Cisco device:

Procedure

1. Log in to your Cisco IOS Server, switch, or router.
2. Type the following command to log in to the router in privileged-exec:

   `enable`
3. Type the following command to switch to configuration mode:

   `conf t`
4. Type the following commands:

   `logging` <*IP address*>

   `logging source-interface` <*interface*>

   Where:

   - <*IP address*> is the IP address of the IBM QRadar host and the SIM components.
   - <*interface*> is the name of the interface, for example, dmz, lan, ethernet0, or ethernet1.
5. Type the following to configure the priority level:

   `logging trap` *warning*

   `logging console` *warning*

   Where *warning* is the priority setting for the logs.
6. Configure the syslog facility:

   `logging facility` *syslog*
7. Save and exit the file.
8. Copy the `running-config` to `startup-config` by typing the following command:

   `copy running-config startup-config`

   You are now ready to configure the log source in QRadar.

   The configuration is complete. The log source is added to QRadar as Cisco IOS events are automatically discovered. Events that are forwarded to QRadar by Cisco IOS-based devices are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco IOS

If QRadar does not automatically detect the log source, add a Cisco IOS log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from a Cisco IOS device:

Table 374. Syslog log source parameters for the Cisco IOS DSM

Parameter	Value
Log Source type	Select one of the following devices: • Cisco IOS • Cisco 12000 Series Routers • Cisco 6500 Series Switches • Cisco 7600 Series Routers • Cisco Carrier Routing System • Cisco Integrated Services Router
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco IOS device.

Related tasks

"Adding a log source" on page 5

Cisco IOS sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco IOS sample message when you use the Syslog protocol

Sample 1: This sample event shows that a TCP session is dropped.

```
<190>2116989: cisco.ios.test: Aug  1 13:42:04.497: %IOSXE-6-PLATFORM:  SIP1: cpp_cp: QFP:0.0
Thread:001 TS:00006808302886264846 %FW-6-DROP_PKT: Dropping tcp pkt from Vlan100 10.1.2.230:12321
=> 172.16.3.20:42150(target:class)-(ESP-DMVPN:class-default) due to Policy drop:classify result
with ip ident 1203 tcp flag 0x2, seq 1227798955, ack 0
```

```
<190>2116989: cisco.ios.test: Aug  1 13:42:04.497: %IOSXE-6-PLATFORM:  SIP1: cpp_cp:
QFP:0.0 Thread:001 TS:00006808302886264846 %FW-6-DROP_PKT: Dropping tcp pkt from Vlan100
10.1.2.230:12321 => 172.16.3.20:42150(target:class)-(ESP-DMVPN:class-default) due to Policy
drop:classify result with ip ident 1203 tcp flag 0x2, seq 1227798955, ack 0
```

Table 375. Highlighted values in the Cisco IOS event

QRadar field name	Highlighted values in the event payload
Event ID	**%FW-6-DROP_PKT**
Event Category	**IOS**
Source IP	**10.1.2.230**

Table 375. Highlighted values in the Cisco IOS event (continued)	
QRadar field name	**Highlighted values in the event payload**
Source Port	**12321**
Destination IP	**172.16.3.20**
Destination Port	**42150**
Protocol	**6**

Sample 2: This sample event shows the opening of an inspection session. The message is issued at the start of each inspected session and it records the source and destination addresses, and ports.

```
<190>1321321: cisco.ios.test: Jul 12 15:42:06.035: %IOSXE-6-PLATFORM:  SIP1: cpp_cp:
QFP:0.0 Thread:001 TS:00005087480388332015 %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(DMVPN-
ESP:CLS_ESP-Out):Start tcp session: initiator (192.168.150.120:49290) -- responder
(10.40.0.27:20000) from Tunnel1
```


```
<190>1321321: cisco.ios.test: Jul 12 15:42:06.035: %IOSXE-6-PLATFORM:  SIP1: cpp_cp:
QFP:0.0 Thread:001 TS:00005087480388332015 %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-(DMVPN-
ESP:CLS_ESP-Out):Start tcp session: initiator (192.168.150.120:49290) -- responder
(10.40.0.27:20000) from Tunnel1
```


Table 376. Highlighted values in the Cisco IOS sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**SESS_AUDIT_TRAIL_START**
Event Category	**IOS**
Source IP	**192.168.150.120:49290**
Source Port	**49290**
Destination IP	**10.40.0.27**
Destination Port	**20000**
Protocol	**6**

Cisco IronPort

IBM QRadar DSM for Cisco IronPort retrieves logs from the following Cisco products: Cisco IronPort, Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA). The Cisco IronPort DSM retrieves web content filtering events (W3C format), Text Mail Logs, and System Logs.

To integrate Cisco IronPort with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website (https://www.ibm.com/support/fixcentral/) onto your QRadar Console:
   - Log File Protocol RPM
   - Cisco IronPort DSM RPM
2. Configure Cisco IronPort to communicate with QRadar.
3. Optional: Add a Cisco IronPort log source by using the Log File protocol.
4. Optional: Add a Cisco IronPort log source by using the Syslog protocol.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Cisco IronPort DSM specifications

The following table describes the specifications for the Cisco IronPort DSM.

Table 377. Cisco IronPort DSM specifications

Specification	Value
Manufacturer	Cisco
DSM name	Cisco IronPort
RPM file name	`DSM-CiscoIronPort-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	• Cisco IronPort: V5.5, V6.5, V7.1, V7.5 • Cisco ESA: V10.0 • Cisco WSA: V10.0
Protocol	Syslog: Cisco IronPort, Cisco WSA Log File Protocol: Cisco IronPort, Cisco ESA
Event format	W3C
Recorded event types	Text Mail Logs, System Logs, Web Content, Filtering Events **Important:** Critical, Warning and Information logs are supported.
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Cisco Email Security Appliance (http://www.cisco.com/c/en/us/products/security/email-security/index.html) Cisco Web Security Appliance (http://www.cisco.com/c/en/us/products/security/web-security-appliance/index.html)

Configuring Cisco IronPort appliances to communicate with QRadar

Complete the configuration on Cisco IronPort appliances so that they can send events to QRadar.

Procedure

1. To configure your Cisco IronPort Appliance to push Web Content Filter events, you must configure a log subscription for the Web Content Filter that uses the W3C format. For more information, see your Cisco IronPort documentation.
2. To configure your Cisco Email Security Appliance (ESA) to push message data, anti-virus events, you must configure a log subscription. For more information, see the Cisco ESA documentation: Configuring Log Subscriptions (https://www.cisco.com/c/dam/en/us/td/docs/security/esa/esa10-0/ESA_10-0_User_Guide.pdf).
3. To configure your Cisco Web Security Appliance (WSA) to push Web Proxy filtering and traffic monitoring activity events, you must configure a log subscription. For more information, see the Cisco WSA documentation: Adding and Editing Log Subscriptions (https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/wsa_10-0/WSA_10-1-0_UserGuide.pdf).

Note: When you add a log subscription on your Cisco Web Security Appliance (WSA), the **Log Style** parameter value must be **Squid**.

Configuring a Cisco IronPort and Cisco ESA log source by using the log file protocol

You can configure a log source on the QRadar Console so that Cisco IronPort and Cisco Email Security Appliance (ESA) can communicate with QRadar by using the log file protocol.

Procedure

Configure a Cisco IronPort log source on the QRadar Console by using the log file protocol. The following tables describe the Log File log source parameters that require specific values for retrieving logs from Cisco IronPort and Cisco ESA.

Table 378. Cisco IronPort log source parameters for Log File

Parameter	Value
Log Source type	Cisco IronPort
Protocol Configuration	Log File Protocol
Log Source Identifier	The **Log Source Identifier** can be any valid value, including the same value as the **Log Source Name** parameter, and doesn't need to reference a specific server.
Service Type	From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP** or **Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that contains the event log files.
Remote Port	Type the port that is used to communicate with the remote host. The valid range is 1 - 65535. The options include: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.
Remote User	Type the user name necessary to log in to the host that contains the event files.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.

Table 378. Cisco IronPort log source parameters for Log File (continued)	
Parameter	**Value**
SSH Key File	If the system is configured to use key authentication, type the path to the SSH key. When an SSH key file is used, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved. The directory path is relative to the user account that is used to log in. **Note:** For FTP only. If the log files are in the remote user's home directory, you can leave the remote directory blank. A blank remote directory field supports systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box to enable the file pattern to search sub folders. By default, the check box is clear. This option is ignored for SCP file transfers.
FTP File Pattern	Must use a regular expression that matches the log files that are generated. The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that end with .log, type the following command: `.*\.log`. For more information, see the Oracle Java documentation (http://docs.oracle.com/javase/tutorial/essential/regex/).
Start Time	Type the time of day for the log source to start the file import. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files.
Recurrence	Type a time interval to determine how frequently the remote directory is scanned for new event log files. The minimum value is 15 minutes. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.

Table 378. Cisco IronPort log source parameters for Log File (continued)	
Parameter	**Value**
Run On Save	Select this check box to start the log file import immediately after the administrator saves the log source. After the first file import, the log file protocol follows the start time and recurrence schedule that is defined by the administrator. When selected, this check box clears the list of previously downloaded and processed files.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	From the list, select **gzip**.
Ignore Previously Processed File(s)	Select this check box to track files that were processed by the log file protocol. QRadar examines the log files in the remote directory to determine if a file was previously processed by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that weren't previously processed are downloaded. This option only applies to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on the QRadar Console for storing downloaded files during processing. Administrators can leave this check box clear for more configurations. When this check box is selected, the **Local Directory** field is displayed so that you can configure the local directory to use for storing files.
Event Generator	W3C. The Event Generator uses W3C to process the web content filter log files.
File Encoding	From the list box, select the character encoding that is used by the events in your log file.

Table 378. Cisco IronPort log source parameters for Log File (continued)	
Parameter	**Value**
Folder Separator	Type the character that is used to separate folders for your operating system. The default value is /. Most configurations can use the default value in **Folder Separator** field. This field is intended for operating systems that use a different character to define separate folders. For example, periods that separate folders on mainframe systems.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring a Cisco IronPort and Cisco WSA log source by using the Syslog protocol

You can configure a log source on the QRadar Console so that the Cisco IronPort Appliance and Cisco Web Security Appliance (WSA) can communicate with QRadar by using the Syslog protocol.

Procedure

Configure a Cisco IronPort log source on the QRadar Console by using Syslog. The following tables describe the Syslog log source parameters that require specific values for retrieving logs from Cisco IronPort and Cisco WSA.

Table 379. Cisco IronPort log source parameters for Syslog	
Parameter	**Value**
Log Source type	Cisco IronPort
Protocol Configuration	Syslog
Log Source Identifier	The IPv4 address or host name that identifies the log source. If your network contains multiple devices that are attached to a single management console, specify the IP address of the individual device that created the event. A unique identifier, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Cisco IronPort sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco IronPort sample message when you use the Syslog protocol

The following sample event message shows that authentication is failed with Cisco IronPort for an IP.

```
<38>Oct 27 10:45:17 cisco.ironport.test proxylogs: Info: PROX_AUTH : 36407 : [22607] Basic
Authentication failed for IP: (172.16.0.1)
```

Table 380. Highlighted fields in the Cisco IronPort event

QRadar field name	Highlighted payload field name
Event ID	Login Failed (The value in QRadar is always Login Failed for a payload that contains **`Basic Authentication failed for IP`**).
Event Category	The value in QRadar is **IronPort**.
Source IP	**`172.16.0.1`**
Log Source Time	**`Oct 27 10:45:17`**

Cisco Meraki

The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

To integrate Cisco Meraki with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the Cisco Meraki DSM RPM on your QRadar Console.
2. Configure your Cisco Meraki device to send Syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Cisco Meraki log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from Cisco Meraki:

Table 381. Cisco Meraki Syslog log source parameters

Parameter	Value
Log Source type	Cisco Meraki
Protocol Configuration	Syslog
Log Source Identifier	The IPv4 address or host name that identifies the log source. If your network contains multiple devices that are attached to a single management console, specify the IP address of the individual device that created the event. A unique identifier, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.

Tip: Cisco Meraki does not send events with RFC3164 or RFC5424 headers. As a result, log sources are auto discovered with the log source identifier of the packet IP of the event instead of the hostname or IP address that is in the header. Use the Syslog redirect protocol to use the value in the header instead of the value in the packet IP. For more information, see the QRadar: Syslog Redirect Protocol FAQ documentation on the support website (https://www.ibm.com/support/pages/qradar-syslog-redirect-protocol-faq).

Related concepts

Configure Cisco Meraki to communicate with IBM QRadar

To collect Cisco Meraki events, configure your Cisco Meraki device to send Syslog events to QRadar.

Cisco Meraki sample event messages
Use these sample event messages as a way of verifying a successful integration with QRadar.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Related reference

Cisco Meraki DSM specifications
When you configure the Cisco Meraki DSM, understanding the specifications for the Cisco Meraki DSM can help ensure a successful integration. For example, knowing what protocol to use before you begin can help reduce frustration during the configuration process.

Cisco Meraki DSM specifications

When you configure the Cisco Meraki DSM, understanding the specifications for the Cisco Meraki DSM can help ensure a successful integration. For example, knowing what protocol to use before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Cisco Meraki DSM.

Table 382. Cisco Meraki DSM specifications

Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco Meraki
RPM file name	DSM-*CiscoMeraki-QRadar_version-build_number*.noarch.rpm
Supported versions	N/A
Protocol	Syslog
Event format	Syslog
Recorded event types	Events Flows security_event ids_alerted
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Cisco Meraki product information (https://Meraki.cisco.com)

Related concepts

Cisco Meraki
The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

Configure Cisco Meraki to communicate with IBM QRadar

To collect Cisco Meraki events, configure your Cisco Meraki device to send Syslog events to QRadar.

Configure Cisco Meraki to communicate with QRadar by following the *Syslog Server Overview and Configuration* steps on the Cisco Meraki website (https://documentation.meraki.com/zGeneral_Administration/Monitoring_and_Reporting/Syslog_Server_Overview_and_Configuration).

Related concepts

Cisco Meraki

The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

Cisco Meraki sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco Meraki sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows an outbound flow event that is used to initiate an IP session. It also shows the source, destination, and port number values along with the firewall rule that they matched.

```
<134>1 1515988859.626061236 appliance flows src=172.21.84.107 dst=10.52.193.137
mac=5C:E0:C5:22:85:E4 protocol=tcp
sport=50395 dport=443 pattern: allow all
```

```
<134>1 1515988859.626061236 appliance flows src=172.21.84.107 dst=10.52.193.137
mac=5C:E0:C5:22:85:E4 protocol=tcp sport=50395 dport=443 pattern: allow all
```

Table 383. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	In QRadar, the value is always *Outbound Flow Allow* for these types of events.
Source IP	**src**
Destination IP	**dst**
Destination MAC	**mac**
Protocol	**protocol**
Source Port	**sport**
Destination Port	**dport**

Sample 2: The following sample event message shows a security event that is generated when an array out of bounds write attempt is made. It also shows the source, destination, port numbers, destination MAC, and protocol values.

```
<134>1 1516050030.553653046 cisco.meraki.test security_event ids_alerted signature=1:45148:1
priority=1 timestamp=1516050030.236281 dhost=00:00:5E:00:53:BC direction=ingress
protocol=tcp/ip src=10.79.70.235:80
dst=172.21.47.130:61019 message: BROWSER-IE Microsoft Internet Explorer
Array out of bounds write attempt
```

```
<134>1 1516050030.553653046 cisco.meraki.test security_event ids_alerted
signature=1:45148:1priority=1 timestamp=1516050030.236281 dhost=00:00:5E:00:53:BC
direction=ingress protocol=tcp/ip src=10.79.70.235:80 dst=172.21.47.130:61019 message: BROWSER-
IE Microsoft Internet Explorer Array out of bounds write attempt
```

Table 384. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**signature**
Source IP	**src**

Table 384. Highlighted fields (continued)	
QRadar field name	**Highlighted payload field name**
Source Port	The value that is used for the **Source Port** displays after the colon in the **src** value. For example, **80**.
Destination IP	**dst**
Destination Port	The value that is used for the **Destination Port** displays after the colon in the **dst** value. For example, **61019**.
Destination MAC	**dhost**
Protocol	**protocol**

Related concepts

Cisco Meraki

The IBM QRadar DSM for Cisco Meraki collects Syslog events from a Cisco Meraki device.

Related information

QRadar: Syslog Redirect Protocol FAQ

Cisco NAC

The Cisco NAC DSM for IBM QRadar accepts events by using syslog.

QRadar records all relevant audit, error, failure events, quarantine, and infected system events. Before you configure a Cisco NAC device in QRadar, you must configure your device to forward syslog events.

Configuring Cisco NAC to forward events

You can configure Cisco NAC to forward syslog events:

Procedure

1. Log in to the Cisco NAC user interface.
2. In the Monitoring section, select **Event Logs**.
3. Click the **Syslog Settings** tab.
4. In the **Syslog Server Address** field, type the IP address of your IBM QRadar.
5. In the **Syslog Server Port** field, type the syslog port number. The default is 514.
6. In the **System Health Log Interval** field, type the frequency, in minutes, for system statistic log events.
7. Click **Update**.

   You are now ready to configure the log source in QRadar.

Syslog log source parameters for Cisco NAC

If QRadar does not automatically detect the log source, add a Cisco NAC log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco NAC devices :

Table 385. Syslog log source parameters for the Cisco NAC DSM	
Parameter	**Value**
Log Source type	Cisco NAC appliance
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco NAC device.

Related tasks

"Adding a log source" on page 5

Cisco Nexus

The Cisco Nexus DSM for IBM QRadar supports alerts from Cisco NX-OS devices.

Syslog is used to forward events from Cisco Nexus to QRadar. Before you can integrate events with QRadar, you must configure your Cisco Nexus device to forward syslog events.

Configuring Cisco Nexus to forward events

You can configure syslog on your Cisco Nexus server to forward events:

Procedure

1. Type the following command to switch to configuration mode:

   `config t`
2. Type the following commands:

   `logging server` <*IP address*> <*severity*>

   Where:

   - <*IP address*> is the IP address of your QRadar Console.
   - <*severity*> is the severity level of the event messages, that range 0 - 7 in value.

   For example, `logging server 192.0.2.1 6` forwards information level (6) syslog messages to 192.0.2.1.
3. Type the following command to configure the interface for sending syslog events:

   `logging source-interface loopback`
4. Type the following command to save your current configuration as the startup configuration:

   `copy running-config startup-config`

   The configuration is complete. The log source is added to IBM QRadar as Cisco Nexus events are automatically discovered. Events that are forwarded to QRadar by Cisco Nexus are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco Nexus

If QRadar does not automatically detect the log source, add a Cisco Nexus log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco Nexus devices :

Table 386. Syslog log source parameters for the Cisco Nexus DSM	
Parameter	**Value**
Log Source type	Cisco Nexus
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco Nexus device.

For information about configuring a Virtual Device Context (VDC) on your Cisco Nexus device, see your vendor documentation.

Related tasks

"Adding a log source" on page 5

Cisco Nexus sample event message

Use these sample event messages to verify a successful integration with IBM QRadar.

Cisco Nexus sample message when you use the Syslog protocol

The following sample event message shows a pluggable authentication module (PAM) authentication failed event.

```
<187>Jul  1 15:21:27 <domain> : 2014 Jul  1 15:21:27.206 CEST: %AUTHPRIV-3-SYSTEM_MSG:
pam_aaa:Authentication failed for user <user> from <IP> - sshd[XXXX]
```

The following sample shows a Radius error message.

```
<187>XXXX: 2016 Jun 30 22:05:09 GMTuno: %RADIUS-3-RADIUS_ERROR_MESSAGE: RADIUS server <IP> failed
to respond
```

Cisco Pix

You can integrate Cisco Pix security appliances with IBM QRadar.

The Cisco Pix DSM for QRadar accepts Cisco Pix events by using syslog. QRadar records all relevant Cisco Pix events.

Configuring Cisco Pix to forward events

You can configure Cisco Pix to forward events.

Procedure

1. Log in to your Cisco PIX appliance by using a console connection, telnet, or SSH.
2. Type the following command to access Privileged mode:

   ```
   enable
   ```
3. Type the following command to access Configuration mode:

   ```
   conf t
   ```
4. Enable logging and time stamp the logs:

   ```
   logging on
   ```

   ```
   logging timestamp
   ```
5. Set the log level:

```
logging trap warning
```

6. Configure logging to IBM QRadar:

   `logging host` <*interface*> <*IP address*>

   Where:

   - <*interface*> is the name of the interface, for example, DMZ, LAN, ethernet0, or ethernet1.
   - <*IP address*> is the IP address of the QRadar host.

   The configuration is complete. The log source is added to QRadar as Cisco Pix Firewall events are automatically discovered. Events that are forwarded to QRadar by Cisco Pix Firewalls are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco Pix

If QRadar does not automatically detect the log source, add a Cisco Pix Firewall log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco Pix Firewall devices :

Table 387. Syslog log source parameters for the Cisco Pix DSM

Parameter	Value
Log Source type	Cisco Pix Firewall
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco Pix Firewall.

Related tasks

"Adding a log source" on page 5

Cisco Secure Workload

The IBM QRadarDSM for Cisco Secure Workload collects events from a Cisco Secure Workload platform.

To integrate Cisco Secure Workload with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (https://www.ibm.com/support). Download and install the Cisco Secure Workload DSM RPM on your QRadar Console.
2. Configure your Cisco Secure Workload platform to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a Cisco Secure Workload log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from the Cisco Secure Workload platform:

Table 388. Cisco Secure Workload Syslog log source parameters

Parameter	Value
Log Source type	Cisco Secure Workload
Protocol Configuration	Syslog

Table 388. Cisco Secure Workload Syslog log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	The IP address or hostname that identifies the log source. The identifier helps you determine which events came from your Cisco Secure Workload platform.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Cisco Secure Workload DSM specifications

The Cisco Secure Workload DSM supports events that are collected from the Cisco Secure Workload platform with the help of Syslog protocol.

The following table describes the specifications for Cisco Secure Workload DSM.

Table 389. Cisco Secure Workload DSM specifications	
Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco Secure Workload
RPM file name	DSM-*CiscoSecureWorkload-QRadar_version-build_number*.noarch.rpm
Protocol	Syslog
Event format	JSON
Recorded event types	Forensics Enforcement Sensor Compliance
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Product Information: Cisco Secure Workload product information User Guide: Cisco Secure Workload Overview

Configure Cisco Secure Workload to communicate with IBM QRadar

To collect Cisco Secure Workload events, configure your Cisco Secure Workload platform to send events to QRadar.

Configure Cisco Secure Workload to communicate with QRadar by following the configuration steps on the Cisco Secure Workload website (https://www.cisco.com/c/en/us/td/docs/security/workload_security/secure_workload/user-guide/3_7/cisco-secure-workload-user-guide/alerts.html).

Cisco Secure Workload sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco Secure Workload sample message when you use the Syslog protocol

The following sample event message shows an alert that detects that the agent is not reachable. This alert triggers when the agent has not communicated with the Secure Workload cluster.

```
<4>2023-08-23T05:42:59Z cisco.secureworkload.test Tetration Alert[20]: [WARNING]
{"keyId":"ENF::1111111aaaaaaa-
agent_not_reachable","eventTime":"1692769304000","alertTime":"1692769380596","alertText":"Agent
Not Reachable: test-nodepool1-1234-
vmss000002","severity":"MEDIUM","tenantId":"123456","type":"ENFORCEMENT","alertDetails":"{\"detail
s\":{\"AgentType\":\"ENFORCER\",\"Bios\":\"11111111-0582-4D63-
B138-111111111\",\"CurrentVersion\":\"3.7.1.40-enforcer\",\"DesiredVersion\":\"3.8.1.1-
enforcer\",\"HostName\":\"example-nodepool1-1234-vmss000002\",\"IP\":\"10.0.0.1 (Gateway IP)
\",\"Platform\":\"Ubuntu-18.04\"},\"agent_uuid\":\"1111111aaaaaaa\",\"scope_name\":\"CSW-
TME\",\"scope_id\":\"111111111\",\"vrf_id\":123456}","rootScopeId":"111111111"}
```


```
<4>2023-08-23T05:42:59Z cisco.secureworkload.test Tetration Alert[20]: [WARNING]
{"keyId":"ENF::1111111aaaaaaa-
agent_not_reachable","eventTime":"1692769304000","alertTime":"1692769380596","alertText":"Agent
Not Reachable: test-nodepool1-1234-
vmss000002","severity":"MEDIUM","tenantId":"123456","type":"ENFORCEMENT","alertDetails":"{\"deta
ils\":{\"AgentType\":\"ENFORCER\",\"Bios\":\"11111111-0582-4D63-
B138-111111111\",\"CurrentVersion\":\"3.7.1.40-enforcer\",\"DesiredVersion\":\"3.8.1.1-
enforcer\",\"HostName\":\"example-nodepool1-1234-vmss000002\",\"IP\":\"10.0.0.1 (Gateway IP)
\",\"Platform\":\"Ubuntu-18.04\"},\"agent_uuid\":\"1111111aaaaaaa\",\"scope_name\":\"CSW-
TME\",\"scope_id\":\"111111111\",\"vrf_id\":123456}","rootScopeId":"111111111"}
```


Table 390. Highlighted fields

QRadar field name	Highlighted payload field value
Event ID	Agent Not Reachable
Severity	Medium
Source IP	10.0.0.1
Device Time	Wednesday August 23, 2023 05:42:59 (am) in time zone UTC (UTC)

Related information

QRadar: Syslog Redirect Protocol FAQ

Cisco Stealthwatch

The IBM QRadar DSM for Cisco Stealthwatch receives events from a Cisco Stealthwatch device.

The following table identifies the specifications for the Cisco Stealthwatch DSM:

Table 391. Cisco Stealthwatch DSM specifications

Specification	Value
Manufacturer	Cisco
DSM name	Cisco Stealthwatch
RPM file name	DSM-CiscoStealthwatch-*QRadar_version-build_number*.noarch.rpm
Supported versions	6.8
Protocol	Syslog

Table 391. Cisco Stealthwatch DSM specifications (continued)	
Specification	**Value**
Event format	LEEF
Recorded event types	Anomaly, Data Hoarding, Exploitation, High Concern Index, High DDoS Source Index, High Target Index, Policy Violation, Recon, High DDoS Target Index, Data Exfiltration, C&C
Automatically discovered?	Yes
Includes identity?	No
Includes Custom properties?	No
More information	Cisco Stealthwatch website (http://www.cisco.com)

To integrate Cisco Stealthwatch with QRadar, complete the following steps:

1. If automatic updates are not configured, download the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Cisco Stealthwatch DSM RPM
2. Configure your Cisco Stealthwatch device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Cisco Stealthwatch log source on the QRadar Console. The following table describes the parameters that require specific values for Cisco Stealthwatch event collection:

Table 392. Cisco Stealthwatch Syslog log source parameters	
Parameter	**Value**
Log Source type	Cisco Stealthwatch
Protocol Configuration	Syslog
Log Source	A unique identifier for the log source.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Cisco Stealthwatch to communicate with QRadar

Cisco Stealthwatch can forward events of different message types, including customized syslog messages, to third parties.

Procedure

1. Log in to the Stealthwatch Management Console (SMC) as an administrator.
2. In the menu bar, click **Configuration** > **Response Management**.
3. From the **Actions** section in the **Response Management** menu, click **Add** > **Syslog Message**.
4. In the Add Syslog Message Action window, configure the following parameters:

Parameter	**Value**
Name	The name for the syslog message action.
Enabled	This check box is enabled by default.

Parameter	Value
IP Address	The IP address of the QRadar Event Collector.
Port	The default port is port 514.
Format	Select **Syslog Formats**.

5. Enter the following custom format:

```
LEEF:2.0|Lancope|Stealthwatch|6.8|{alarm_type_id}|0x7C|src={source_ip}|
dst={target_ip}|dstPort={port}|proto={protocol}|msg={alarm_type_description}|
fullmessage={details}|start={start_active_time}|end={end_active_time}|
cat={alarm_category_name}|alarmID={alarm_id}|sourceHG={source_host_group_names}|
targetHG={target_host_group_names}|sourceHostSnapshot={source_url}|
targetHostSnapshot={target_url}|flowCollectorName={device_name}|flowCollectorIP={device_ip}|
domain={domain_name}|exporterName={exporter_hostname}|exporterIPAddress ={exporter_ip}|
exporterInfo={exporter_label}|targetUser={target_username}|targetHostname={target_hostname}|
sourceUser={source_username}|alarmStatus={alarm_status}|alarmSev={alarm_severity_name}
```

6. Select the custom format from the list and click **OK**.

   Note: Use the **Test** button to send test message to QRadar

7. Click **Response Management** > **Rules**.
8. Click **Add** and select **Host Alarm**.
9. Provide a rule name in the **Name** field.
10. Create rules by selecting values from the **Type** and **Options** menus. To add more rules, click the ellipsis icon. For a Host Alarm, combine as many possible types in a statement as possible.
11. In the **Action** dialog, select **IBM QRadar syslog action** for both **Active** and **Inactive** conditions. The event is forwarded to QRadar when any predefined condition is satisfied.

Cisco Stealthwatch sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cisco Stealthwatch sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that watched port is active.

```
<134>Sep 12 14:03:02 cisco.stealthwatch.test StealthWatch[4969]: LEEF:2.0|
Lancope|Stealthwatch|6.8|13|0x7C|src=10.243.54.38|dst=10.100.11.12|dstPort=784|proto=6|msg=A
watched port number has become active.|fullmessage=IANA-
Unassigned (784/tcp) from 10.100.11.12|start=2019-09-12T14:02:30Z|
end=|cat=Watch Port Active|alarmID=3X-1F6B-86U2-YUUR-7|sourceHG=Country|
targetHG=Catch All|sourceHostSnapshot=https://10.36.52.20/test-page/test.html#/host/
10.243.54.38|targetHostSnapshot=https://10.36.52.20/landing-page/abc.html#/host/10.100.11.12|
flowCollectorName=flow|flowCollectorIP=10.20.25.23|domain=abcd.ab.example.test|exporterName=|
exporterIPAddress =|exporterInfo=|targetUser=|targetHostname=|sourceUser=|alarmStatus=ACTIVE|
alarmSev=Major
```

Table 393. Highlighted values in the Cisco Stealthwatch sample event message

QRadar field name	Highlighted fields and values in the event payload
Event ID	**13**
Event Category	**Watch Port Active**
Source IP	**src**
Destination IP	**dst**
Destination Port	**dstPort**

Table 393. Highlighted values in the Cisco Stealthwatch sample event message (continued)	
QRadar field name	**Highlighted fields and values in the event payload**
Protocol	**proto**

Sample 2: The following sample event message shows that there is suspicious activity.

```
<134>Sep 12 13:19:27 cisco.stealthwatch.test StealthWatch[4969]: LEEF:2.0|Lancope|Stealthwatch|
6.8|99|0x7C|src=10.10.10.10|dst=10.237.198.232|dstPort=80|proto=6|msg=The host has been
observed doing something bad to another host.|fullmessage=Source Host is http (80/tcp)
client to target.host.name (10.237.198.232)|start=2019-09-05T08:48:34Z|end=2019-09-05T08:48:34Z|
cat=Anomaly|alarmID=3Y-13Y1-QJJ2-YYA9-U|sourceHG=Department, Inside|targetHG=target,
Outside|sourceHostSnapshot=https://10.10.10.20/some/path|targetHostSnapshot=https://10.10.10.20/
some/path|flowCollectorName=Collector|flowCollectorIP=10.10.10.20|domain=Corporate
Domain|exporterName=exporter.host.name|exporterIPAddress =10.20.30.40|
exporterInfo=exporter.host.name (10.20.30.40)|targetUser=admin|targetHostname=www.host.test|
sourceUser=admin|alarmStatus=ACTIVE|alarmSev=Critical
```

Table 394. Highlighted values in the Cisco Stealthwatch sample event message	
QRadar field name	**Highlighted fields and values in the event payload**
Event ID	**99**
Event Category	**Anomaly**
Source IP	**src**
Destination IP	**dst**
Destination Port	**dstPort**
Protocol	**proto**

Cisco Umbrella

The IBM QRadar DSM for Cisco Umbrella collects DNS logs from Cisco Umbrella storage by using an Amazon S3 compatible API.

To integrate Cisco Umbrella with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console in the order that they are listed.
   - Protocol Common RPM
   - Amazon AWS REST API Protocol RPM
   - Cisco Cloud Web Security DSM RPM
   - Cisco Umbrella DSM RPM
2. Configure your Cisco Umbrella to communicate with QRadar.
3. Add a Cisco Umbrella log source on the QRadar Console. The following table describes the parameters that require specific values for Cisco Umbrella event collection.

Table 395. Amazon AWS S3 REST API log source parameters	
Parameter	**Value**
Log Source type	Cisco Umbrella
Protocol Configuration	Amazon AWS S3 REST API

Table 395. Amazon AWS S3 REST API log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you configured more than one Cisco Umbrella log source, you might want to identify the first log source as `ciscoumbrella1`, the second log source as `ciscoumbrella2`, and the third log source as `ciscoumbrella3`.
Region Name (Signature V4 only)	The region that is associated with the Amazon S3 bucket.
Bucket Name	The name of the AWS S3 bucket where the log files are stored. For example, the bucket name might be `cisco-managed-us-west-1`.
S3 Endpoint URL	`https://s3.amazonaws.com/<bucketname>` The endpoint URL that is used to query the AWS S3 REST API. The endpoint URL can be different depending on the device configurations. **Important:** You must have an Endpoint URL to configure a Cisco managed AWS S3 bucket and a customer-managed AWS S3 bucket.
Directory Prefix	*<path>*/ The location of the root directory on the Cisco Umbrella storage bucket from where the Cisco Umbrella logs are retrieved. For example, the root directory location might be `dnslogs/`.
File Pattern	`.*?\.csv\.gz`
Event Format	Select **Cisco Umbrella CSV** from the list. The log source retrieves CSV formatted events.

For a complete list of Amazon AWS S3 REST API protocol parameters and their values, see Amazon AWS S3 REST API protocol configuration options.

Related concepts

"Configure Cisco Umbrella to communicate with QRadar" on page 684
IBM QRadar collects Cisco Umbrella events from an Amazon S3 bucket. You must configure your Cisco Umbrella to forward events to QRadar.

"Cisco Umbrella DSM specifications" on page 684
The following table describes the specifications for the Cisco Umbrella DSM.

"Cisco Umbrella sample event messages" on page 684
Use these sample event messages as a way of verifying a successful integration with QRadar.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configure Cisco Umbrella to communicate with QRadar

IBM QRadar collects Cisco Umbrella events from an Amazon S3 bucket. You must configure your Cisco Umbrella to forward events to QRadar.

To configure Cisco Umbrella, see Cisco documentation (https://support.umbrella.com/hc/en-us/articles/231248488-Configuring-QRadar-for-use-with-Cisco-Umbrella-Log-Management-in-AWS-S3).

Important: You must have an Endpoint URL to configure a Cisco managed AWS S3 bucket and a customer managed AWS S3 bucket.

Cisco Umbrella DSM specifications

The following table describes the specifications for the Cisco Umbrella DSM.

Table 396. Cisco Umbrella DSM specifications

Specification	**Value**
Manufacturer	Cisco
DSM name	Cisco Umbrella
RPM file name	`DSM-CiscoUmbrella-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Amazon AWS S3 REST API
Event format	Cisco Umbrella CSV
Recorded event types	DNS Proxy IP
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Cisco Umbrella product information page (https://umbrella.cisco.com)

Cisco Umbrella sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following tables provide sample event messages for the Cisco Umbrella DSM:

Table 397. Cisco Umbrella sample syslog message

Event name	Low level category	Sample log message
NOERROR	18081 (DNS In Progress)	{"sourceFile":"test_2017-11-17-15-30-dcd8.csv.gz","EventType":"DNSLog","Timestamp":"2017-11-17 15:30:27","MostGranularIdentity":"Test","Identities":"Test","InternalIp":"<IP_address>","ExternalIp":"<External_IP_address>","Action":"Allowed","QueryType":"28 (AAAA)","ResponseCode":"NOERROR","Domain":"abc.aws.amazon.com.","Categories":"Ecommerce/Shopping"} {"sourceFile":"test_2017-11-17-15-30-dcd8.csv.gz","EventType":"DNSLog","Timestamp":"2017-11-17 15:30:27","MostGranularIdentity":"Test","Identities":"Test","InternalIp":"<IP_address>","ExternalIp":"<External_IP_address>","Action":"Allowed","QueryType":"28 (AAAA)","ResponseCode":"NOERROR","Domain":"abc.aws.amazon.com.","Categories":"Ecommerce/Shopping"}

Table 398. Cisco Umbrella sample event message

Event name	Low level category	Sample log message
NOERROR	18081 (DNS In Progress)	"2015-01-16 17:48:41","Active DirectoryUserName","ActiveDirectoryUserName,ADSite,Network","<IP_address1>","<IP_address2>","Allowed","1 (A)","NOERROR","domain-visited.com.","Chat,Photo Sharing,Social Networking,Allow List" "2015-01-16 17:48:41","ActiveDirectoryUserName","ActiveDirectoryUserName,ADSite,Network","<IP_address1>","<IP_address2>","Allowed","1 (A)","NOERROR","domain-visited.com.","Chat,Photo Sharing,Social Networking,Allow List"

Cisco VPN 3000 Concentrator

The IBM QRadar DSM for Cisco VPN 3000 Concentrator accepts Cisco VPN Concentrator events by using syslog.

About this task

QRadar records all relevant events. Before you can integrate with a Cisco VPN concentrator, you must configure your device to forward syslog events to QRadar.

Procedure

1. Log in to the Cisco VPN 3000 Concentrator command-line interface (CLI).
2. Type the following command to add a syslog server to your configuration:

   `set logging server` <*IP address*>

   Where <*IP address*> is the IP address of QRadar or your Event Collector.
3. Type the following command to enable system messages to be logged to the configured syslog servers:

   `set logging server enable`

4. Set the facility and severity level for syslog server messages:
   - `set logging server facility` <*server_facility_parameter*>
   - `set logging server severity` <*server_severity_level*>

Results

The log source is added to QRadar as Cisco VPN Concentrator events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco VPN 3000 Concentrator

If QRadar does not automatically detect the log source, add a Cisco VPN 3000 Series Concentrator log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco VPN 3000 Series Concentrator devices:

Table 399. Syslog log source parameters for the Cisco VPN 3000 Concentrator DSM

Parameter	Value
Log Source type	Cisco VPN 3000 Series Concentrator
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco VPN 3000 Series Concentrator devices.

Related tasks

"Adding a log source" on page 5

Cisco Wireless LAN Controllers

The IBM QRadar DSM for Cisco Wireless LAN Controllers collects events that are forwarded from Cisco Wireless LAN Controller devices by using Syslog or SNMPv2.

If you collect events from Cisco Wireless LAN Controllers, select the best collection method for your configuration. The Cisco Wireless LAN Controller DSM for QRadar supports both syslog and SNMPv2 events. However, syslog provides all available Cisco Wireless LAN Controller events, whereas SNMPv2 sends only a limited set of security events to QRadar.

Configuring syslog for Cisco Wireless LAN Controller

You can configure the Cisco Wireless LAN Controller to forward syslog events to IBM QRadar.

Procedure

1. Log in to your Cisco Wireless LAN Controller interface.
2. Click the **Management** tab.
3. From the menu, select **Logs** > **Config**.
4. In the **Syslog Server IP Address** field, type the IP address of your QRadar Console.
5. Click **Add**.
6. From the **Syslog Level** list, select a logging level.

The **Information** logging level allows the collection of all Cisco Wireless LAN Controller events above the **Debug** logging level.

7. From the **Syslog Facility** list, select a facility level.
8. Click **Apply**.
9. Click **Save Configuration**.

What to do next

You are now ready to configure a syslog log source for Cisco Wireless LAN Controller.

Syslog log source parameters for Cisco Wireless LAN Controllers

If QRadar does not automatically detect the log source, add a Cisco Wireless LAN Controller log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco Wireless LAN Controllers:

Table 400. Syslog log source parameters for the Cisco Wireless LAN Controller DSM

Parameter	Value
Log Source type	Cisco Wireless LAN Controllers
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco Wireless LAN Controller.
Enabled	Select the **Enabled** check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value that is configured in the **Coalescing Events** drop-down list in the QRadar **Settings** window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically-discovered log source, you can override the default value by configuring this check box for each log source. For more information on settings, see the *IBM QRadar Administration Guide*.

Table 400. Syslog log source parameters for the Cisco Wireless LAN Controller DSM (continued)	
Parameter	**Value**
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** drop-down list in the QRadar **Settings** window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source that you can override the default value by configuring this check box for each log source.

Related tasks

"Adding a log source" on page 5

Configuring SNMPv2 for Cisco Wireless LAN Controller

SNMP event collection for Cisco Wireless LAN Controllers allows the capture of events for IBM QRadar

About this task

The following events are collected:

- SNMP Config Event
- bsn Authentication Errors
- LWAPP Key Decryption Errors

Procedure

1. Log in to your Cisco Wireless LAN Controller interface.
2. Click the **Management** tab.
3. From the menu, select **SNMP** > **Communities**.

   You can use the one of the default communities that are created or create a new community.
4. Click **New**.
5. In the **Community Name** field, type the name of the community for your device.
6. In the **IP Address** field, type the IP address of QRadar.

   The IP address and IP mask that you specify is the address from which your Cisco Wireless LAN Controller accepts SNMP requests. You can treat these values as an access list for SNMP requests.
7. In the **IP Mask** field, type a subnet mask.
8. From the **Access Mode** list, select **Read Only** or **Read/Write**.
9. From the **Status** list, select **Enable**.
10. Click **Save Configuration** to save your changes.

What to do next

You are now ready to create a SNMPv2 trap receiver.

Configuring a trap receiver for Cisco Wireless LAN Controller

Trap receivers that are configured on Cisco Wireless LAN Controllers define where the device can send SNMP trap messages.

About this task

To configure a trap receiver on your Cisco Wireless LAN Controller, take the following steps:

Procedure

1. Click the **Management** tab.
2. From the menu, select **SNMP** > **Trap Receivers**.
3. In the **Trap Receiver Name** field, type a name for your trap receiver.
4. In the **IP Address** field, type the IP address of IBM QRadar.

   The IP address you specify is the address to which your Cisco Wireless LAN Controller sends SNMP messages. If you plan to configure this log source on an Event Collector, you want to specify the Event Collector appliance IP address.
5. From the **Status** list, select **Enable**.
6. Click **Apply** to commit your changes.
7. Click **Save Configuration** to save your settings.

What to do next

You are now ready to create a SNMPv2 log source in QRadar.

SNMPv2 log source parameters for Cisco Wireless LAN Controllers

If QRadar does not automatically detect the log source, add a Cisco Wireless LAN Controller log source on the QRadar Console by using the SNMPv2 protocol.

The following table describes the parameters that require specific values to collect SNMPv2 events from Cisco Wireless LAN Controllers:

Table 401. SNMPv2 log source parameters for the Cisco Wireless LAN Controller DSM

Parameter	Value
Log Source type	Cisco Wireless LAN Controllers
Protocol Configuration	SNMPv2
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco Wireless LAN Controller.
Community	Type the SNMP community name that is needed to access the system that contains the SNMP events. The default is Public.
Include OIDs in Event Payload	Select the **Include OIDs in Event Payload** check box. This option allows the SNMP event payload to be constructed by using name-value pairs instead of the standard event payload format. OIDs in the event payload are needed to process SNMPv2 or SNMPv3 events from certain DSMs.

Table 401. SNMPv2 log source parameters for the Cisco Wireless LAN Controller DSM (continued)	
Parameter	**Value**
Enabled	Select the **Enabled** check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. Automatically discovered log sources use the default value that is configured in the **Coalescing Events** drop-down in the QRadar **Settings** window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source.
Store Event Payload	Select this check box to enable or disable QRadar from storing the event payload. Automatically discovered log sources use the default value from the **Store Event Payload** drop-down in the QRadar **Settings** window on the **Admin** tab. However, when you create a new log source or update the configuration for an automatically discovered log source, you can override the default value by configuring this check box for each log source.

For a complete list of SNMPv2 protocol parameters and their values, see "SNMPv2 protocol configuration options" on page 216.

Related tasks

"Adding a log source" on page 5

Cisco Wireless Services Module

You can integrate a Cisco Wireless Services Module (WiSM) device with IBM QRadar.

A Cisco WiSM DSM for QRadar accepts events by using syslog. Before you can integrate QRadar with a Cisco WiSM device, you must configure Cisco WiSM to forward syslog events.

Configuring Cisco WiSM to forward events

You can configure Cisco WiSM to forward syslog events to IBM QRadar.

Procedure

1. Log in to the Cisco Wireless LAN Controller user interface.
2. Click **Management** > **Logs** > **Config**.

   The **Syslog Configuration** window is displayed.
3. In the **Syslog Server IP Address** field, type the IP address of the QRadar host that receives the syslog messages.
4. Click **Add**.
5. Using the **Syslog Level** list, set the severity level for filtering syslog messages to the syslog servers by using one of the following severity levels:

   - **Emergencies** - Severity level 0
   - **Alerts** - Severity level 1 (Default)
   - **Critical** - Severity level 2
   - **Errors** - Severity level 3
   - **Warnings** - Severity level 4
   - **Notifications** - Severity level 5
   - **Informational** - Severity level 6
   - **Debugging** - Severity level 7

   If you set a syslog level, only those messages whose severity level is equal to or less than the selected syslog level are sent to the syslog server. For example, if you set the syslog level to **Warnings** (severity level 4), only those messages whose severity is 0 - 4 are sent to the syslog servers.
6. From the **Syslog Facility** list, set the facility for outgoing syslog messages to the syslog server by using one of the following facility levels:

   - **Kernel** - Facility level 0
   - **User Process** - Facility level 1
   - **Mail** - Facility level 2
   - **System Daemons** - Facility level 3
   - **Authorization** - Facility level 4
   - **Syslog** - Facility level 5 (default value)
   - **Line Printer** - Facility level 6
   - **USENET** - Facility level 7
   - **Unix-to-Unix Copy** - Facility level 8
   - **Cron** - Facility level 9
   - **FTP Daemon** - Facility level 11
   - **System Use 1** - Facility level 12
   - **System Use 2** - Facility level 13
   - **System Use 3** - Facility level 14
   - **System Use 4** - Facility level 15
   - **Local Use 0** - Facility level 16
   - **Local Use 1** - Facility level 17
   - **Local Use 2** - Facility level 18

- **Local Use 3** - Facility level 19
- **Local Use 4** - Facility level 20
- **Local Use 5** - Facility level 21
- **Local Use 6** - Facility level 22
- **Local Use 7** - Facility level 23

7. Click **Apply**.
8. From the **Buffered Log Level** and the **Console Log Level** lists, select the severity level for log messages sent to the controller buffer and console by using one of the following severity levels:
   - **Emergencies** - Severity level 0
   - **Alerts** - Severity level 1
   - **Critical** - Severity level 2
   - **Errors** - Severity level 3 (default value)
   - **Warnings** - Severity level 4
   - **Notifications** - Severity level 5
   - **Informational** - Severity level 6
   - **Debugging** - Severity level 7

   If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to **Warnings** (severity level 4), only those messages whose severity is 0 - 4 are logged.
9. Select the **File Info** check box if you want the message logs to include information about the source file. The default value is enabled.
10. Select the **Proc Info** check box if you want the message logs to include process information. The default value is disabled.
11. Select the **Trace Info** check box if you want the message logs to include trace back information. The default value is disabled.
12. Click **Apply** to commit your changes.
13. Click **Save Configuration** to save your changes.

    The configuration is complete. The log source is added to QRadar as Cisco WiSM events are automatically discovered. Events that are forwarded by Cisco WiSM are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Cisco WiSM

If QRadar does not automatically detect the log source, add a Cisco Wireless Services Module (WiSM) log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Cisco WiSM devices:

Table 402. Syslog log source parameters for the Cisco Wireless Services Module DSM

Parameter	Value
Log Source type	Cisco Wireless Services Module (WiSM)
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The identifier helps you determine which events came from your Cisco WiSM device.

Related tasks

“Adding a log source” on page 5

Chapter 41. Citrix

The Citrix NetScaler DSM for IBM QRadar accepts all relevant audit log events by using syslog.

The Citrix Access Gateway DSM accepts access, audit, and diagnostic events that are forwarded from your Citrix Access Gateway appliance by using syslog.

Citrix Access Gateway

Configure Syslog on your Citrix Access Gateway to forward events to the QRadar Console or Event Collector.

Procedure

1. Log in to your Citrix Access Gateway web interface.
2. Click the **Access Gateway Cluster** tab.
3. Select **Logging/Settings**.
4. In the **Server** field, type the IP address of your QRadar Console or Event Collector.
5. From the **Facility** list, select a syslog facility level.
6. In the **Broadcast interval (mins)**, type `0` to continuously forward syslog events to QRadar.
7. Click **Submit** to save your changes.

Results

The configuration is complete. The log source is added to QRadar as Citrix Access Gateway events are automatically discovered. Events that are forwarded to QRadar by Citrix Access Gateway are displayed on the **Log Activity** tab in QRadar.

Syslog log source parameters for Citrix Access Gateway

If QRadar does not automatically detect the log source, add a Citrix Access Gateway log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Citrix Access Gateway:

Table 403. Syslog log source parameters for the Citrix Access Gateway DSM

Parameter	Value
Log Source type	**Citrix Access Gateway**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Citrix Access Gateway appliance.

Related tasks

"Adding a log source" on page 5

Citrix NetScaler

To integrate Citrix NetScaler events with IBM QRadar, you must configure Citrix NetScaler to forward syslog events.

Procedure

1. Using SSH, log in to your Citrix NetScaler device as a root user.
2. Type the following command to add a remote syslog server:

   `add audit syslogAction <ActionName> <IP Address> -serverPort 514 -logLevel Info -dateFormat DDMMYYYY`

   Where:

   <*ActionName*> is a descriptive name for the syslog server action.

   <*IP Address*> is the IP address or host name of your QRadar Console.

   Example:

   ```
   add audit syslogAction action-QRadar 192.0.2.1 -serverPort 514 -logLevel Info -dateFormat DDMMYYYY
   ```

3. Type the following command to add an audit policy:

   `add audit syslogPolicy` <*PolicyName*> <*Rule*> <*ActionName*>

   Where:

   <*PolicyName*> is a descriptive name for the syslog policy.

   <*Rule*> is the rule or expression the policy uses. The only supported value is `ns_true`.

   <*ActionName*> is a descriptive name for the syslog server action.

   Example:

   ```
   add audit syslogPolicy policy-QRadar ns_true action-QRadar
   ```

4. Type the following command to bind the policy globally:

   `bind system global` <*PolicyName*> `-priority` <*Integer*>

   Where:

   <*PolicyName*> is a descriptive name for the syslog policy.

   <*Integer*> is a number value that is used to rank message priority for multiple policies that are communicating by using syslog.

   Example:

   ```
   bind system global policy-QRadar -priority 30
   ```

   When multiple policies have priority (represented by a number value that is assigned to them) the lower number value is evaluated before the higher number value.
5. Type the following command to save the Citrix NetScaler configuration.

   `save config`
6. Type the following command to verify that the policy is saved in your configuration:

   `sh system global`

   Note: For information on configuring syslog by using the Citrix NetScaler user interface, see http://support.citrix.com/article/CTX121728 or your vendor documentation.

The configuration is complete. The log source is added to QRadar as Citrix NetScaler events are automatically discovered. Events that are forwarded by Citrix NetScaler are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Citrix NetScaler

If QRadar does not automatically detect the log source, add a Citrix NetScaler log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Citrix NetScaler:

Table 404. Syslog log source parameters for the Citrix NetScaler DSM

Parameter	Value
Log Source type	**Citrix NetScaler**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Citrix NetScaler devices.

Related tasks

"Adding a log source" on page 5

Citrix NetScaler sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Citrix NetScaler sample message when you use the Syslog protocol

The following sample event message shows a successful SSL handshake.

Tip: Citrix NetScaler does not send events with RFC3164 or RFC5424 headers, so the log source is not discovered by using a hostname or IP address in the header. Instead, log sources are automatically discovered by using the log source identifier of the event's packet IP. Use the Syslog Redirect protocol to use the value in the header instead of the value in the packet IP. For more information, see QRadar: Syslog Redirect Protocol FAQ (https://www.ibm.com/support/pages/qradar-syslog-redirect-protocol-faq).

```
<135> 12/04/2017:17:21:00 GMT citrix.netscaler.test 0-PPE-1 : SSLLOG SSL_HANDSHAKE_SUCCESS
5743593 0 :  SPCBId 87630 - ClientIP 172.25.184.157 - ClientPort 19849 - VserverServiceIP
10.254.14.94 - VserverServicePort 443 - ClientVersion TLSv1.2 - CipherSuite "RC4-MD5 TLSv1.2
Non-Export 128-bit" - Session Reuse
```

Table 405. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**SSL_HANDSHAKE_SUCCESS**
Source IP	**172.25.184.157**
Source Port	**19849**
Destination IP	**10.254.14.94**
Destination Port	**443**

Table 405. QRadar field names and highlighted values in the event payload (continued)	
QRadar field name	**Highlighted values in the event payload**
Device Time	**12/04/2017:17:21:00 GMT**

Chapter 42. Cloudera Navigator

The IBM QRadar DSM for Cloudera Navigator collects events from Cloudera Navigator.

The following table identifies the specifications for the Cloudera Navigator DSM:

Table 406. Cloudera Navigator DSM specifications

Specification	**Value**
Manufacturer	Cloudera
DSM name	Cloudera Navigator
RPM file name	`DSM-ClouderaNavigator-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	v2.0
Protocol	Syslog
Recorded event types	Audit events for HDFS, HBase, Hive, Hue, Cloudera Impala, Sentry
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Cloudera Navigator website (www.cloudera.com)

To integrate Cloudera Navigator with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Cloudera Navigator DSM RPM
2. Configure your Cloudera Navigator device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Cloudera Navigator log source on the QRadar Console. The following table describes the parameters that require specific values for Cloudera Navigator event collection:

   Table 407. Cloudera Navigator log source parameters

Parameter	**Value**
Log Source type	Cloudera Navigator
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name in the Syslog header. Use the packet IP address, if the Syslog header does not contain an IP address or host name.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Cloudera Navigator to communicate with QRadar

You can configure Cloudera Navigator device to send JSON format syslog events to IBM QRadar.

Before you begin

Ensure that Cloudera Navigator can access port 514 on the QRadar system.

About this task

When you install Cloudera Navigator, all audit logs are collected automatically. However, you must configure Cloudera Navigator to send audits logs to QRadar by using syslog.

Procedure

1. Do one of the following tasks:
   - Click **Clusters** > **Cloudera Management Service** > **Cloudera Management Service**.
   - On the **Status** tab of the **Home** page, click the **Cloudera Management Service** link in **Cloudera Management Service** table.
2. Click the **Configuration** tab.
3. Search for **`Navigator Audit Server Logging Advanced Configuration Snippet`**.
4. Depending on the format type, enter one of the following values in the **Value** field:
   - `log4j.logger.auditStream = TRACE,SYSLOG`
   - `log4j.appender.SYSLOG = org.apache.log4j.net.SyslogAppender`
   - `log4j.appender.SYSLOG.SyslogHost = <QRadar Hostname>`
   - `log4j.appender.SYSLOG.Facility = Local2`
   - `log4j.appender.SYSLOG.FacilityPrinting = true`
   - `log4j.additivity.auditStream = false`
5. Click **Save Changes**.

Chapter 43. Cloudflare Logs

The IBM QRadar DSM for Cloudflare Logs collects Cloudflare instance events by using the HTTP Receiver protocol or the Amazon AWS S3 REST API protocol.

Integrate Cloudflare Logs with QRadar by using the HTTP Receiver protocol

To integrate Cloudflare Logs with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - HTTP Receiver Protocol RPM
   - DSM Common RPM
   - Cloudflare Logs DSM RPM
2. Configure your Cloudflare instance to send events to QRadar. For more information, see Configure Cloudflare to send events to QRadar when you use the HTTP Receiver protocol.
3. If QRadar does not automatically detect the log source, add a Cloudflare Logs log source on the QRadar Console. For more information, see HTTP Receiver log source parameters for Cloudflare Logs.

Integrate Cloudflare Logs with QRadar by using the Amazon AWS S3 REST API protocol

To integrate Cloudflare Logs with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - Amazon AWS S3 REST API Protocol RPM
   - DSM Common RPM
   - Cloudflare Logs DSM RPM
2. Configure your Cloudflare instance to send events to QRadar. For more information, see Configuring Cloudflare Logs to forward logs to send events to QRadar when you use the Amazon S3 REST API protocol .
3. If QRadar does not automatically detect the log source, add a Cloudflare Logs log source on the QRadar Console. For more information, see Amazon REST S3 REST API log source parameters for Cloudflare Logs.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Cloudflare Logs DSM specifications

When you configure Cloudflare Logs, understanding the specifications for the Cloudflare Logs DSM can help ensure a successful integration. For example, knowing what protocols are supported for Cloudflare Logs before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Cloudflare Logs DSM.

Table 408. Cloudflare Logs DSM specifications	
Specification	**Value**
Manufacturer	Cloudflare
DSM name	Cloudflare Logs
RPM file name	DSM-*CloudflareLogs-QRadar_version-build_number*.noarch.rpm
Protocols	HTTP Receiver Amazon AWS S3 REST API
Event format	JSON
Recorded event types	HTTP events, Firewall events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Cloudflare website (https://www.cloudflare.com)

Configure Cloudflare to send events to IBM QRadar when you use the HTTP Receiver protocol

To send Cloudflare Firewall or Cloudflare HTTP events to QRadar when you use the HTTP Receiver protocol, you need to start the Logpush job that you created.

1. To send Cloudflare Firewall events to QRadar, start the Logpush job that you created by typing the following command:

```
curl -s https://api.cloudflare.com/client/v4/zones/<zone_id>/logpush/jobs -X POST -d
'{ "name": "<name>", "logpull_options":
"fields=Action,ClientIP,ClientASN,ClientASNDescription,ClientCountry,ClientIPClass,ClientRefe
rerHost,ClientRefererPath,ClientRefererQuery,ClientRefererScheme,ClientRequestHost,ClientRequ
estMethod,ClientRequestPath,ClientRequestProtocol,ClientRequestQuery,ClientRequestScheme,Clie
ntRequestUserAgent,EdgeColoCode,EdgeResponseStatus,Kind,MatchIndex,Metadata,OriginResponseSta
tus,OriginatorRayID,RayID,RuleID,Source,Datetime&timestamps=rfc3339", "destination_conf":
"<QRadar_URL:LogSource_Port>", "max_upload_bytes": 5000000, "max_upload_records": 1000,
"dataset": "firewall_events", "enabled": true}' -H "X-Auth-Email: <X-Auth-Email>" -H "X-Auth-
Key: <X-Auth-Key>"
```

2. To send Cloudflare HTTP events to QRadar, start the Logpush job that you created by typing the following command:

```
curl -s https://api.cloudflare.com/client/v4/zones/<zone_id>/logpush/jobs -X POST -d
'{ "name": "<name>", "logpull_options":
"fields=ClientRequestMethod,EdgeResponseStatus,ClientIP,ClientSrcPort,CacheCacheStatus,Client
Country,ClientDeviceType,ClientIPClass,ClientMTLSAuthCertFingerprint,ClientMTLSAuthStatus,Cli
entRegionCode,ClientRequestBytes,ClientRequestHost,ClientRequestPath,ClientRequestProtocol,Cl
ientRequestReferer,ClientRequestScheme,ClientRequestSource,ClientRequestURI,ClientRequestUser
Agent,ClientSSLCipher,ClientSSLProtocol,ClientXRequestedWith,EdgeEndTimestamp,EdgeRequestHost
,EdgeResponseBodyBytes,EdgeResponseBytes,EdgeServerIP,EdgeStartTimestamp,SecurityActions,Secu
rityRuleIDs,SecuritySources,OriginIP,OriginResponseStatus,OriginSSLProtocol,ParentRayID,RayID
,SecurityAction,WAFAttackScore,SecurityRuleID,SecurityRuleDescription,WAFSQLiAttackScore,WAFX
SSAttackScore,EdgeStartTimestamp&timestamps=rfc3339", "destination_conf":
"<QRadar_URL:LogSource_Port>", "max_upload_bytes": 5000000, "max_upload_records": 1000,
"dataset": "http_requests", "enabled": true}' -H "X-Auth-Email: <X-Auth-Email>" -H "X-Auth-
Key: <X-Auth-Key>"
```

Important:

- For the LogSource Port, you must choose one of the following open ports from Cloudflare:
  - 443 Do not use on QRadar console

- 8088 QRadar on Cloud or On-premises
- 2433 QRadar on On-premises only

When the command is executed, the events are forwarded to QRadar.

Related concepts

"HTTP Receiver log source parameters for Cloudflare Logs" on page 713

Related tasks

"Adding a log source" on page 5

Configuring Cloudflare Logs to send events to IBM QRadar when you use the Amazon S3 REST API protocol

When you use the Amazon S3 REST API protocol, IBM QRadar collects Cloudflare Log events from an Amazon S3 bucket.

Before you begin

Complete the following steps:

1. Configure your Cloudflare instance to push events by creating a Logpush job. For more information, see Manage via the Cloudflare UI (https://developers.cloudflare.com/logs/logpush/logpush-dashboard).
2. To create a Logpush job to send Firewall events, you need to configure and manage jobs by using the Logpush API. For more information, see Manage via the Logpush API (https://developers.cloudflare.com/logs/logpush/logpush-configuration-api).

About this task

If the Logpush job is created in the Cloudflare UI or by using the Logpush REST API, you must complete the following procedure.

Procedure

1. Log in to the Cloudflare UI (https://dash.cloudflare.com/login).
2. Select the site where you are configuring logs.
3. Click **Analysis** > **Logs**.
4. If the **Pushing** switch is in the off position, toggle the switch to **On**.
5. Click **Edit** and then ensure that the appropriate fields are selected, based on which data set is selected.
   - HTTP requests - **ClientRequestMethod**, **Client IP**, **ClientSrcPort**, **EdgeResponseStatus**, **EdgeStartTimestamp**
   - Firewall events - **Action**, **Datetime**, **ClientIP**

What to do next

Create an SQS Queue and configure S3 ObjectCreated Notifications.

Create an SQS queue and configure S3 ObjectCreated notifications

Before you can add a log source in IBM QRadar, you must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Complete the following procedures:

1. Finding the S3 Bucket that contains the data that you want to collect.

2. Creating the SQS queue that is used to receive the ObjectCreated notifications from the S3 Bucket that you used in Step 1.
3. Setting up SQS queue permissions.
4. Creating ObjectCreated notifications.
5. Configuring security credentials for your AWS user account.
6. Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge.
7. Adding an Amazon AWS CloudTrail log source on the QRadar Console using an SQS queue.

Finding the S3 bucket that contains the data that you want to collect

You must find and note the region for S3 bucket that contains the data that you want to collect.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to **S3**.
3. From the **AWS Region** column in the **Buckets** list, note the region where the bucket that you want to collect data from is located. You need the region for the **`Region Name`** parameter value when you add a log source in IBM QRadar.
4. Enable the checkbox beside the bucket name, and then from the panel that opens to the right, click **Copy Bucket ARN** to copy the value to the clipboard. Save this value or leave it on the clipboard. You need this value when you set up **SQS queue permissions**.

Creating the SQS queue that is used to receive ObjectCreated notifications

You must create an SQS queue and configure S3 ObjectCreated notifications in the AWS Management Console when you use the Amazon AWS S3 REST API protocol.

Before you begin

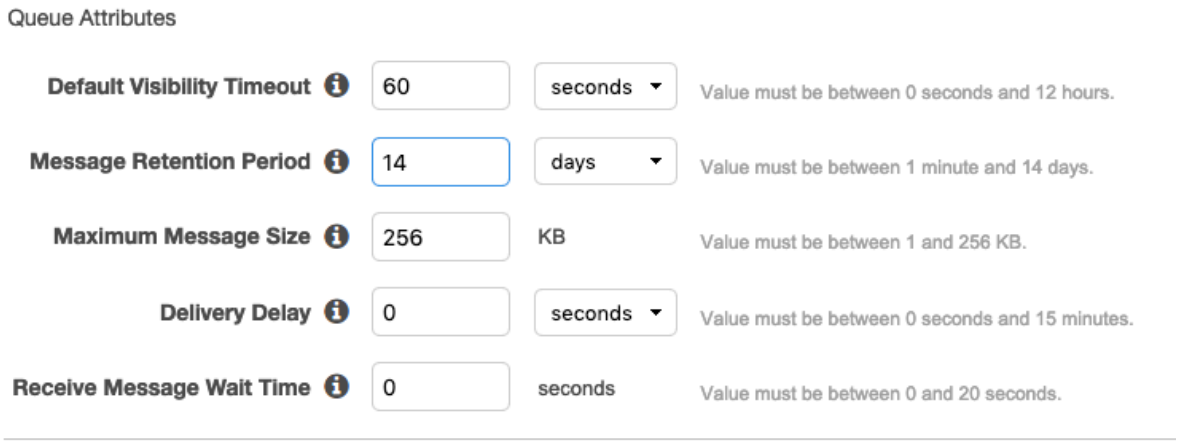
You must complete **Finding the S3 Bucket that contains the data that you want to collect**. The SQS Queue must be in the same region as the AWS S3 bucket that the queue is collecting from.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, and then go to the Simple Queue Service Management Console.
3. In the upper right of the window, change the region to where the bucket is located. You noted this value when you completed the **Finding the S3 Bucket that contains the data that you want to collect** procedure.
4. Select **Create New Queue**, and then type a value for the **Queue Name**.
5. Click **Standard Queue**, select **Configure Queue**, and then change the default values for the following **Queue Attributes**.
   - **Default Visibility Timeout** - 60 seconds (You can use a lower value. In the case of load balanced collection, duplicate events might occur with values of less than 30 seconds. This value can't be 0.)
   - **Message Retention Period** - 14 days (You can use a lower value. In the event of an extended collection, data might be lost.)

   Use the default value for the remaining **Queue Attributes**.

   More options such as **Redrive Policy** or **SSE** can be used depending on the requirements for your AWS environment. These values should not affect the data collection.



6. Select **Create Queue**.

Setting up SQS queue permissions

You must set up SQS queue permissions for users to access the queue.

Before you begin

You must complete **Creating the SQS queue that is used to receive ObjectCreated notifications**.

You can set the SQS queue permissions by using either the Permissions Editor or a JSON policy document.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Go to the SQS Management Console, and then select the queue that you created from the list.
3. From the **Details** panel, record the **ARN** field value.

   For example: **arn:aws:sqs:us-east-1:123456789012:MySQSQueueName**
4. To set the SQS queue **Access policy (Permissions)** by using the **AWS Policy generator**, complete the following steps:
   a) Select **Policy Type** > **SQS Queue Policy**.
   b) Add an Access Policy statement.
   c) From the **Access policy** tab, click **Policy generator**, and then configure the following parameters:

Table 409. Permission parameters	
Parameter	**Value**
Effect	Click **Allow**.
Principal	Type `*(Everybody)`.
Actions	From the list, select **SendMessage**
Amazon Resource Name (ARN)	Type your queue ARN: *arn:aws:sqs:us-east-1:123456789012:MySQSQueueName*

   d) Click **Add Conditionals (Optional)**, and then configure the following parameters:

Table 410. Add Conditionals (Optional) parameters	
Parameter	**Value**
Qualifier	None
Condition	**ARNLike**
Key	Type `aws:SourceArn`.
Value	The ARN of the S3 bucket from when you completed the "Finding the S3 bucket that contains the data that you want to collect" on page 302 procedure. For example: `aws:s3:::my-example-s3bucket`

5. To set the SQS queue permissions by using a JSON policy document, complete the following steps:
   a) Click **Add Condition** > **Add Statement.** > **Generate Policy**.
   b) Copy and paste the following JSON policy into the **Access policy** window:

      Copy and paste might not preserve the white space in the JSON policy. The white space is required. If the white space is not preserved when you paste the JSON policy, paste it into a text editor and restore the white space. Then, copy and paste the JSON policy from your text editor into the **Edit Policy Document** window.

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-1:123456789012:MySQSQueueName",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::my-example-s3bucket"
        }
      }
    }
  ]
}
```

6. Click **Review Policy**. Ensure that the data is correct, and then click **Save Changes**.

Creating ObjectCreated notifications

Configure ObjectCreated notifications for the folders that you want to monitor in the bucket.

Procedure

1. Log in to the AWS Management Console as an administrator.
2. Click **Services**, go to **S3**, and then select a bucket.
3. Click the **Properties** tab, and in the **Events** pane, click **Add notification**. Configure the parameters for the new event.

   The following table shows an example of an ObjectCreated notification parameter configuration:

Table 411. Example: New ObjectCreated notification parameter configuration	
Parameter	**Value**
Name	Type a name of your choosing.
Events	Select **All object create events**.
Prefix	AWSLogs/ **Tip:** You can choose a prefix that contains the data that you want to find, depending on where the data is located and what data that you want to go to the queue. For example, AWSLogs/, CustomPrefix/AWSLogs/, AWSLogs/123456789012/.
Suffix	json.gz
Send to	SQS queue **Tip:** You can send the data from different folders to the same or different queues to suit your collection or QRadar tenant needs. Choose one or more of the following methods: • Different folders that go to different queues • Different folders from different buckets that go to the same queue • Everything from a single bucket that goes to a single queue • Everything from multiple buckets that go to a single queue
SQS	The **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**.

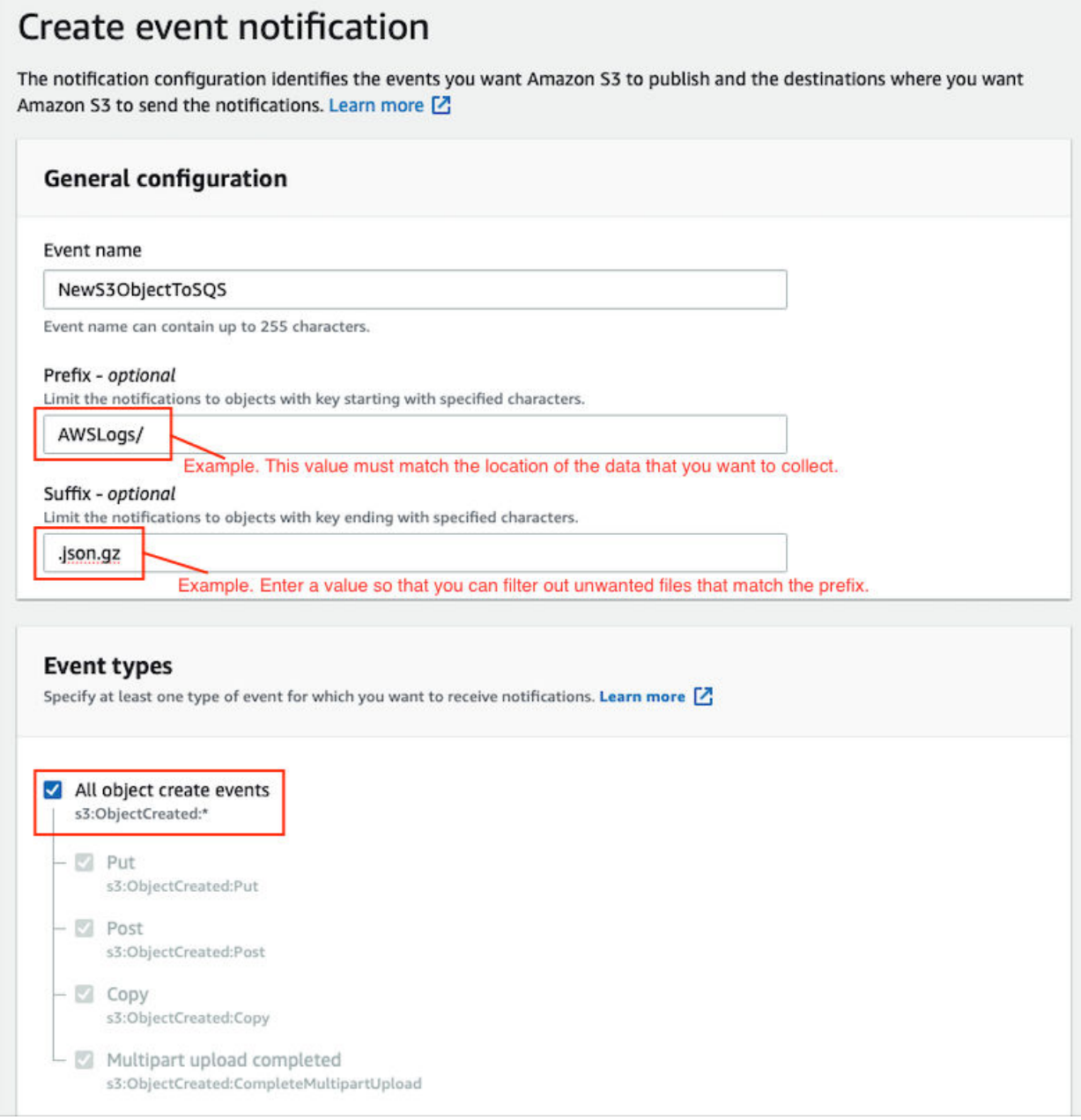


Figure 36. Example: Events

In the example in figure 1 of a parameter configuration, notifications are created for `AWSLogs/` from the root of the bucket. When you use this configuration, All ObjectCreated events trigger a notification. If there are multiple accounts and regions in the bucket, everything gets processed. In this example, `json.gz` is used. This file type can change depending on the data that you are collecting. Depending on the content in your bucket, you can omit the extension or choose an extension that matches the data you are looking for in the folders where you have events set up.

After approximately 5 minutes, the queue that contains data displays. In the **Messages Available** column, you can view the number of messages.

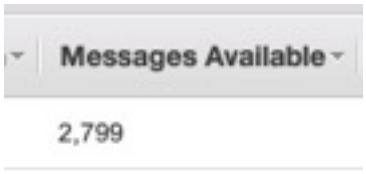


Figure 37. Number of available messages

4. Click **Services**, then go to **Simple Queue Services**.
5. Right-click the **Queue Name** from step 4 of **Creating the SQS queue that is used to receive the ObjectCreated notifications**, then select **View/Delete Messages** to view the messages.

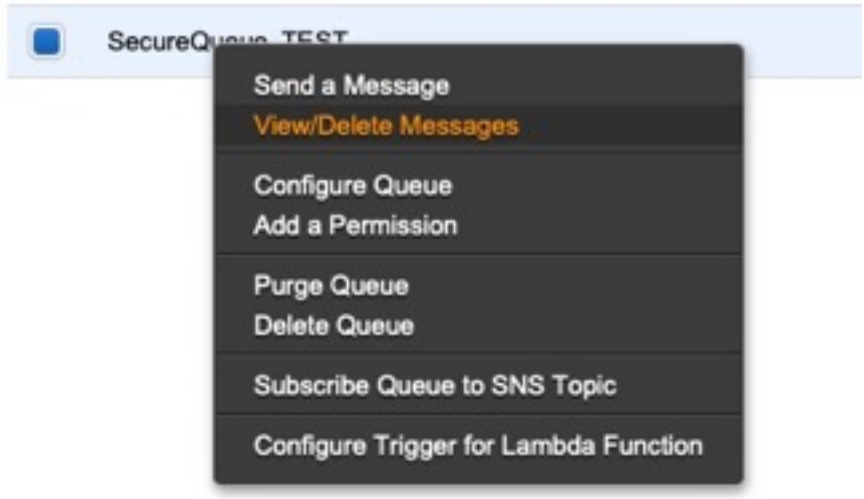


Figure 38. SecureQueue TEST list

Example: Sample message

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-east-2",
         "eventTime":"2018-12-19T01:51:03.251Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AWS:AIDAIZLCFC5TZD36YHNZY"
         },
         "requestParameters":{
            "sourceIPAddress":"52.46.82.38"
         },
         "responseElements":{
            "x-amz-request-id":"6C05F1340AA50D21",
            "x-amz-id-2":"9e8KovdAUJwmYu1qnEv+urrO8T0vQ+UOpkPnFYLE6agmJSn745
/T3/tVs0Low/vXonTdATvW23M="
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"test_SQS_Notification_1",
            "bucket":{
               "name":"myBucketName",
               "ownerIdentity":{
                  "principalId":"A2SGQBYRFBZET"
               },
               "arn":"arn:aws:s3:::myBucketName"
            },
            "object":{
               "key":"AWSLogs/123456789012/CloudTTrail/eu-west-
```

```
3/2018/12/19/123456789012_CloudTrail_eu-west-3_TestAccountTrail
_us-east-2_20181219T014838Z.json.gz",
                "size":713,
                "eTag":"1ff1209e4140b4ff7a9d2b922f57f486",
                "sequencer":"005C19A40717D99642"
            }
        }
    }
  ]
}
```

Tip: In the **key** value, your DSM name displays.

6. Click **Services**, then navigate to **IAM**.
7. Set a **User** or **Role** permission to access the SQS queue and for permission to download from the target bucket. The user or user role must have permission to read and delete from the SQS queue. For information about adding, managing and changing permissions for IAM users, see the IAM Users documentation. After QRadar reads the notification, and then downloads and processes the target file, the message must be deleted from the queue.

   Sample Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "sqs:DeleteMessage",
                "sqs:ReceiveMessage",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket_name>/AWSLogs/*",
                "arn:aws:sqs:us-east-2:<AWS_account_number>:<queue_name>"
            ]
        }
    ]
}
```

   You can add multiple buckets to the S3 queue. To ensure that all objects are accessed, you must have a trailing /* at the end of the folder path that you added.

   You can add this policy directly to a user, a user role, or you can create a minimal access user with **sts:AssumeRole** permissions only. When you configure a log source in QRadar, configure the **assume Role ARN** parameter for QRadar to assume the role. To ensure that all files waiting to be processed in a single run (emptying the queue) can finish without retries, use the default value of 1 hour for the **API Session Duration** parameter.

   When you use assumed roles, ensure that the ARN of the user that is assuming the role is in the **Trusted Entities** for that role. You can view the trusted entities that can assume the rule from the **Trust Relationship** tab in **IAM Role**. In addition, the user must have permission to assume roles in that (or any) account. The following examples show a sample trust policy:

   Allow all IAM users within a specific AWS account to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:root"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
    ]
}
```

Allow a specific user to assume a role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::YOUR_ACCOUNT_ID:user/USERNAME"
            },
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::YOUR_ACCOUNT_ID:role/ROLE_NAME"
        }
```

The following image example shows a sample Amazon AWS CloudTrail log source configuration in QRadar.

Tip: Use the Amazon AWS S3 REST API log source parameter values for your DSM when you configure your log source.

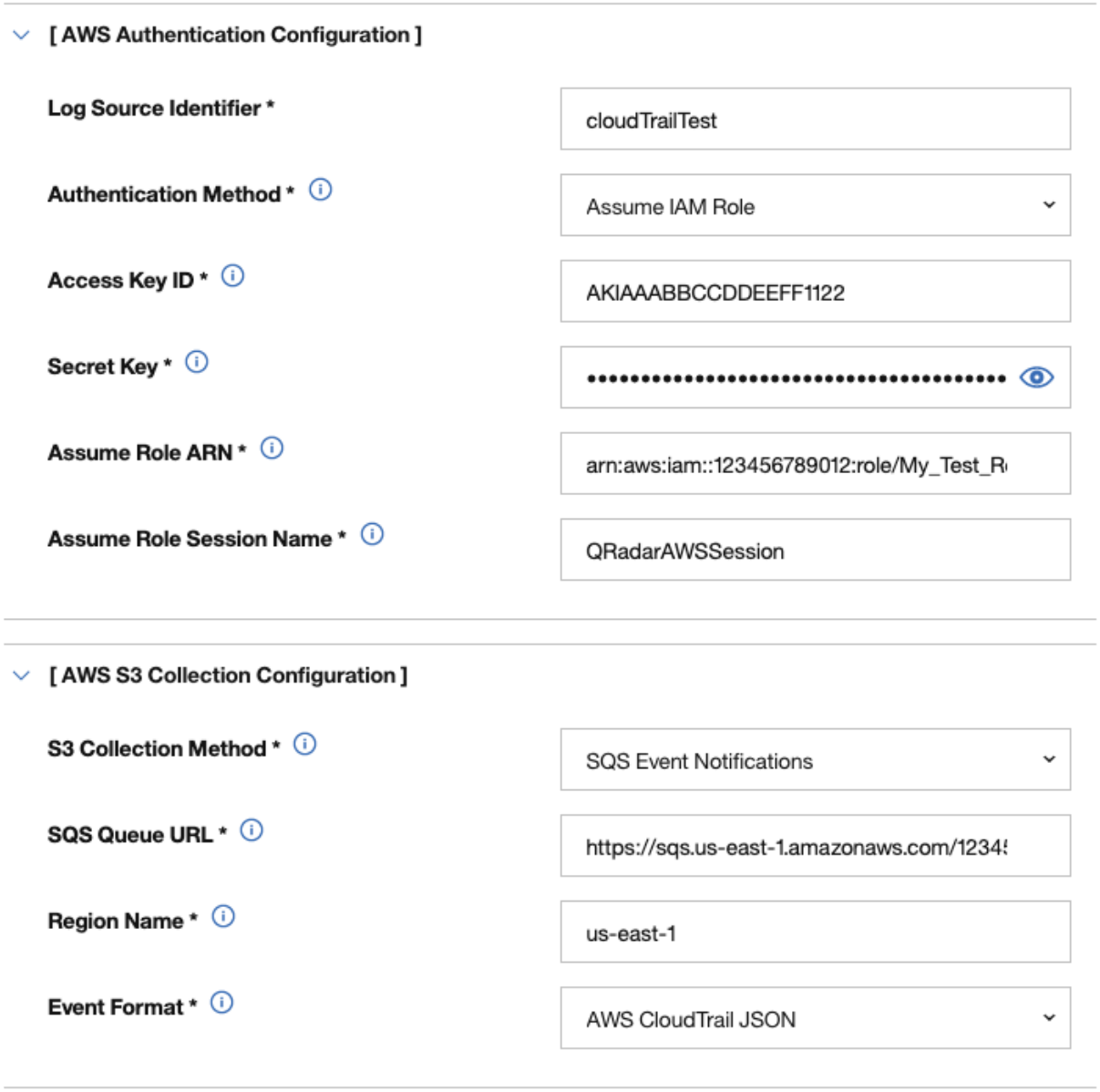


Figure 39. Example: Amazon AWS CloudTrail log source configuration in QRadar

Forwarding ObjectCreated notifications to the SQS queue by using Amazon EventBridge

Create an Amazon EventBridge rule to forward ObjectCreated notifications to a target SQS queue.

Before you begin

Before you can create a rule in Amazon EventBridge, you must enable Amazon EventBridge on your AWS Management console. For more information, see Enabling Amazon EventBridge.

Procedure

1. Open the Amazon EventBridge console.
2. From the **Navigation** menu, click **Rules** > **Create rule**.
3. On the **Create rule** window, complete the following steps:
   a) Enter a name and description for the rule.

      Important: A rule can't have the same name as another rule that is both in the same region and on the same event bus.

   b) For **Event bus**, select the event bus that you want to associate with this rule. If you select **AWS default event bus**, the rule matches the events that come from your account.
   c) For **Rule type**, select **Rule with an event pattern**.
4. Click **Next**.
5. For **Event source**, select **AWS events or EventBridge partner events**.
6. For **Creation method**, select **Use pattern form**.
7. In the **Event pattern** window, configure the event pattern by completing the following steps:
   a) Select the values listed in the table for the following parameters:

Parameter	Value
Event source	**AWS services**
AWS service	**Simple Storage Service (S3)**
Event type	**Amazon S3 Event Notification**

   b) Click the **Specific event(s)** option and select **Object Created**.
   c) Click **Specific bucket(s) by name** and enter the name of the specific bucket that you want to collect events from.
   d) Optional: To enable notifications for a specific folder prefix or file extension, choose **Custom pattern (JSON editor)** instead of **Use pattern form** for the creation method, and create your custom event pattern.
   For example, this event pattern filters for `Object Created` events in your bucket. In this example, `example/directory` is the directory prefix and `.png` is the suffix.

```
{
  "source": ["aws.s3"],
  "detail-type": ["Object Created"],
  "detail": {
    "bucket": {
      "name": ["<example-bucket>"]
    },
    "object": {
      "key": [{
        "prefix": "example/directory/"
      }],
      "key": [{
        "suffix": ".png"
      }]
    }
  }
}
```

e) Click **Add**, then click **Next**.

8. Choose the SQS queue that you want to use as the target. Enter the name of the queue, then click **Next**.
9. On the **Review and create** page, click **Create rule**.

Configuring security credentials for your AWS user account

You must have your AWS user account access key and the secret access key values before you can configure a log source in QRadar.

Procedure

1. Log in to your IAM console.
2. Select **Users** from left navigation pane and then select your user name from the list.
3. To create the access keys, click the **Security Credentials** tab, and in the **Access Keys** section, click **Create access key**.
4. Download the CSV file that contains the keys or copy and save the keys.

   Tip: Save the Access key ID and Secret access key. You need them when you configure a log source in QRadar.

   You can view the Secret access key only when it is created.

Related information

Adding a log source

HTTP Receiver log source parameters for Cloudflare Logs

If IBM QRadar does not automatically detect the log source, add a Cloudflare Logs log source on the QRadar Console by using the HTTP Receiver protocol.

When you use the HTTP Receiver protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect HTTP Receive events from Cloudflare Logs:

Table 412. HTTP Receiver log source parameters for the Cloudflare Logs DSM

Parameter	Value
Log Source type	Cloudflare Logs
Protocol Configuration	HTTP Receiver
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Cloudflare Logs log source that is configured, you might want to identify the first log source as `Cloudflare1`, the second log source as `Cloudflare2`, and the third log source as `Cloudflare3`.
Communication Type	HTTP or HTTPS, depending on the QRadar url that is used to integrate with QRadar.
TLS version	TLSv1.2

Table 412. HTTP Receiver log source parameters for the Cloudflare Logs DSM (continued)	
Parameter	**Value**
Listen Port	The QRadar port that is used to integrate with Cloudflare and is used in the command to start the Logpush job.
Message Pattern	.*

For a complete list of HTTP Receiver protocol parameters and their values, see HTTP Receiver protocol configuration options.

Related tasks

Adding a log source

Amazon AWS S3 REST API log source parameters for Cloudflare Logs

If IBM QRadar does not automatically detect the log source, add a Cloudflare Logs log source on the QRadar Console by using the Amazon AWS S3 REST API protocol.

When you use the Amazon AWS S3 REST API protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Amazon AWS S3 REST API events from Cloudflare Logs:

Table 413. Amazon AWS S3 REST API log source parameters for the Cloudflare Logs DSM	
Parameter	**Value**
Log Source type	Cloudflare Logs
Protocol Configuration	Amazon AWS S3 REST API
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you have more than one Cloudflare Logs log source that is configured, you might want to identify the first log source as `Cloudflare1`, the second log source as `Cloudflare2`, and the third log source as `Cloudflare3`.
Event Format	Select **LINEBYLINE** from the list.
Use as a Gateway Log Source	Select this option for the collected events to flow through the QRadar Traffic Analysis engine and for QRadar to automatically detect one or more log sources.

Table 413. Amazon AWS S3 REST API log source parameters for the Cloudflare Logs DSM (continued)	
Parameter	**Value**
Log Source Identifier Pattern	This option is available when **Use as a Gateway Log Source** is set to yes. Use this option if you want to define a custom Log Source Identifier for events being processed. This field accepts key value pairs to define the custom Log Source Identifier, where the key is the Identifier Format String, and the value is the associated regex pattern. You can define multiple key value pairs by entering a pattern on a new line. When multiple patterns are used, they are evaluated in order until a match is found and a custom Log Source Identifier can be returned.
Show Advanced Options	Select this option.
File Pattern	This option is available when Show Advanced Options is set to yes. Type a regex for the file pattern that matches the files that you want to pull; for example, `.*?\.log\.gz`

For a complete list of Amazon AWS S3 REST API protocol parameters and their values, see Amazon AWS S3 REST API protocol configuration options.

Related tasks

Adding a log source

Cloudflare Logs sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Cloudflare Logs sample messages

Sample 1: The following sample event message shows that an HTTP GET request is sent to the hostname `host.domain.test`, and the server response is status code 200.


```
{"ClientIP":"10.0.0.1","ClientRequestHost":"host.domain.test","ClientRequestMethod":"GET","Clien
tRequestURI":"/cdn-cgi/images/cf-icon-
cloud.png","EdgeEndTimestamp":"2020-10-13T19:49:36Z","EdgeResponseBytes":1895,"EdgeResponseStatu
s":200,"EdgeStartTimestamp":"2020-10-13T19:49:36Z","RayID":"5e1b95b9ea390cc5","SecurityAction":"
unknown","WAFFlags":"0","WAFMatchedVar":"","SecurityRuleID":"","SecurityRuleDescription":"","Cac
heCacheStatus":"unknown","CacheResponseBytes":0,"CacheResponseStatus":0,"CacheTieredFill":false,
"ClientASN":855,"ClientCountry":"xx","ClientDeviceType":"desktop","ClientIPClass":"noRecord","Cl
ientRequestBytes":1049,"ClientRequestPath":"/cdn-cgi/images/cf-icon-
cloud.png","ClientRequestProtocol":"HTTP/1.1","ClientRequestReferer":"http://host.domain.test/
cdn-cgi/styles/main.css","ClientRequestUserAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/
537.36","ClientSSLCipher":"NONE","ClientSSLProtocol":"none","ClientSrcPort":53851,"ClientXReques
tedWith":"","EdgeColoCode":"EWR","EdgeColoID":11,"EdgePathingOp":"unknown","EdgePathingSrc":"und
ef","EdgePathingStatus":"cloudflareInternalEndpoint","EdgeRequestHost":"","EdgeResponseCompressi
onRatio":1,"EdgeResponseContentType":"image/png","EdgeServerIP":"","SecurityActions":
[],"SecurityRuleIDs":[],"SecuritySources":
[],"OriginIP":"","OriginResponseBytes":0,"OriginResponseHTTPExpires":"","OriginResponseHTTPLastM
odified":"","OriginResponseStatus":0,"OriginResponseTime":0,"OriginSSLProtocol":"unknown","Paren
tRayID":"00","WorkerCPUTime":0,"WorkerStatus":"unknown","WorkerSubrequest":false,"WorkerSubreque
stCount":0,"ZoneID":304427638}
```

Table 414. QRadar field names and highlighted values in the event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	**ClientRequestMethod** + **EdgeResponseStatus** For HTTP Request events as shown in the sample, the Event ID is constructed by using the **ClientRequestMethod** field and the **EdgeResponseStatus** field. They are concatenated together with an underscore between the fields.
Source IP	**ClientIP**
Source Port	**ClientSrcPort**
Device Time	**EdgeStartTimestamp**

Sample 2: The following sample event message shows that an HTTP POST request is sent to the hostname `host.domain.test`, and the server response is status code 200.

{"**ClientRequestMethod**":"POST","**ClientIP**":"10.0.0.1","**ClientSrcPort**":53851,"CacheCacheStatus":"dynamic","ClientCountry":"xx","ClientDeviceType":"desktop","ClientIPClass":"noRecord","ClientMTLSAuthCertFingerprint":"","ClientMTLSAuthStatus":"unknown","ClientRegionCode":"xx","ClientRequestBytes":2935,"ClientRequestHost":"host.domain.test","ClientRequestPath":"/console/test/QRadar.getAlertMessages","ClientRequestProtocol":"HTTP/2","ClientRequestReferer":"https://host.domain.test/console/qradar/jsp/test.jsp","ClientRequestScheme":"https","ClientRequestSource":"eyeball","ClientRequestURI":"/console/test/QRadar.getAlertMessages","ClientRequestUserAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15) Firefox/108.0","ClientSSLCipher":"None","ClientSSLProtocol":"TLSv1.3","ClientXRequestedWith":"","EdgeRequestHost":"host.domain.test","EdgeResponseBodyBytes":50,"EdgeResponseBytes":805,"EdgeServerIP":"10.0.0.1","SecurityActions":["allow"],"SecurityRuleIDs":["66668d0ae9c2222222222a600d17448"],"SecuritySources":["firewallRules"],"OriginIP":"10.0.0.1","OriginResponseStatus":200,"OriginSSLProtocol":"TLSv1.2","ParentRayID":"00","RayID":"78b4476e33333af2","SecurityAction":"unknown","WAFAttackScore":0,"SecurityRuleID":"","SecurityRuleDescription":"","WAFSQLiAttackScore":0,"WAFXSSAttackScore":0,"**EdgeEndTimestamp**":"2023-01-19T11:37:33Z","EdgeStartTimestamp":"2023-01-19T11:37:33Z","**EdgeResponseStatus**":200}

Table 415. QRadar field names and highlighted values in the event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	**ClientRequestMethod** + **EdgeResponseStatus** For HTTP Request events as shown in the sample, the Event ID is constructed by using the **ClientRequestMethod** field and the **EdgeResponseStatus** field. They are concatenated together with an underscore between the fields.
Source IP	**ClientIP**
Source Port	**ClientSrcPort**
Device Time	**EdgeStartTimestamp**

Sample 3: The following sample event message shows that an HTTP GET Forbidden request is sent to the hostname `host.domain.test`, and the server response is status code 403.

{"**ClientRequestMethod**":"GET","**ClientIP**":"10.0.0.1","**ClientSrcPort**":53851,"CacheCacheStatus":"unknown","ClientCountry":"xx","ClientDeviceType":"desktop","ClientIPClass":"noRecord","ClientMTLSAuthCertFingerprint":"","ClientMTLSAuthStatus":"unknown","ClientRegionCode":"xx","ClientRequestBytes":2927,"ClientRequestHost":"host.domain.test","ClientRequestPath":"/api/gui_app_framework/test","ClientRequestUserAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15) Firefox/108.0","ClientSSLCipher":"None","ClientSSLProtocol":"TLSv1.3","ClientXRequestedWith":"","EdgeRequestHost":"","EdgeResponseBodyBytes":1751,"EdgeResponseBytes":2166,"EdgeServerIP":"","SecurityActions":["allow","block"],"SecurityRuleIDs":["66668d0ae9c2222222222a600d17448","111106BNULL"],"SecuritySources":["firewallRules","waf"],"OriginIP":"","OriginResponseStatus":0,"OriginSSLProtocol":"unknown","ParentRayID":"00","RayID":"78b4476e33333af2","SecurityAction":"drop","WAFAttackScore":0,"SecurityRuleID":"111106BNULL","SecurityRuleDescription":"SQLi - IS

NULL","WAFSQLiAttackScore":0,"WAFXSSAttackScore":0,"EdgeEndTimestamp":"2023-01-19T13:06:18Z","**EdgeStartTimestamp**":"2023-01-19T13:06:18Z","**EdgeResponseStatus**":403}

Table 416. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**ClientRequestMethod** + **EdgeResponseStatus** For HTTP Request events as shown in the sample, the Event ID is constructed by using the **ClientRequestMethod** field and the **EdgeResponseStatus** field. They are concatenated together with an underscore between the fields.
Source IP	**ClientIP**
Source Port	**ClientSrcPort**
Device Time	**EdgeStartTimestamp**

Sample 4: The following sample event message shows that an HTTP GET Not Modified request is sent to the hostname `host.domain.test`, and the server response is status code 304.

{"**ClientRequestMethod**":"GET","**ClientIP**":"10.0.0.1","**ClientSrcPort**":53851,"CacheCacheStatus":"miss","ClientCountry":"xx","ClientDeviceType":"desktop","ClientIPClass":"noRecord","ClientMTLSAuthCertFingerprint":"","ClientMTLSAuthStatus":"unknown","ClientRegionCode":"xx","ClientRequestBytes":2682,"ClientRequestHost":"host.domain.test","ClientRequestPath":"/console/test/1057/static/js/test.js","ClientRequestProtocol":"HTTP/2","ClientRequestReferer":"https://host.domain.test/console/plugins/1057/","ClientRequestScheme":"https","ClientRequestSource":"eyeball","ClientRequestURI":"/console/test/1057/static/js/test.js","ClientRequestUserAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15) Firefox/108.0","ClientSSLCipher":"None","ClientSSLProtocol":"TLSv1.3","ClientXRequestedWith":"","EdgeRequestHost":"host.domain.test","EdgeResponseBodyBytes":0,"EdgeResponseBytes":366,"EdgeServerIP":"10.0.0.1","SecurityActions":["allow"],"SecurityRuleIDs":["6666d0ae9c2222222222a600d17448"],"SecuritySources":["firewallRules"],"OriginIP":"10.0.0.1","OriginResponseStatus":304,"OriginSSLProtocol":"TLSv1.2","ParentRayID":"00","RayID":"78b4476e33333af2","SecurityAction":"unknown","WAFAttackScore":0,"SecurityRuleID":"","SecurityRuleDescription":"","WAFSQLiAttackScore":0,"WAFXSSAttackScore":0,"EdgeEndTimestamp":"2023-01-19T13:06:15Z","**EdgeStartTimestamp**":"2023-01-19T13:06:14Z","**EdgeResponseStatus**":304}

Table 417. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**ClientRequestMethod** + **EdgeResponseStatus** For HTTP Request events as shown in the sample, the Event ID is constructed by using the **ClientRequestMethod** field and the **EdgeResponseStatus** field. They are concatenated together with an underscore between the fields.
Source IP	**ClientIP**
Source Port	**ClientSrcPort**
Device Time	**EdgeStartTimestamp**

Sample 5: The following sample event message shows that an HTTP POST firewall request is sent to the hostname `host.domain.test`, and the server response is status code 200.

{"Action":"allow","**ClientIP**":"10.0.0.1","ClientASN":45116,"ClientASNDescription":"GTPL-AS-AP Gujarat Telelink Pvt Ltd","ClientCountry":"xx","ClientIPClass":"noRecord","ClientRefererHost":"host.domain.test","ClientRefererPath":"/console/test/jsp/test.jsp","ClientRefererQuery":"","ClientRefererScheme":"https","ClientRequestHost":"host.domain.test","**ClientRequestMethod**":"POST","ClientRequestPath":"/console/test/QRadar.getIngressNewVersion","ClientRequestProtocol":"HTTP/2","ClientRequestQuery":"","ClientRequestScheme":"https","ClientRequestUserAgent":"Mozilla/5.0

```
(Macintosh; Intel Mac OS X 10.15) Firefox/
108.0","EdgeColoCode":"BOM","EdgeResponseStatus":200,"Kind":"firewall","MatchIndex":0,"Metadata"
:
{"filter":"007b761e8a762222222f4528222ebe67","type":"customer"},"OriginResponseStatus":200,"Orig
inatorRayID":"00","RayID":"78b4476e33333af2","RuleID":"6538d0a111114f6aad22222600d17448","Source
":"firewallrules","Datetime":"2023-01-19T11:58:00Z"}
```


Table 418. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**ClientRequestMethod** + **EdgeResponseStatus** For Firewall Request events as shown in the sample, the Event ID is constructed by using the **ClientRequestMethod** field and the **EdgeResponseStatus** field. They are concatenated together with an underscore between the fields.
Source IP	**ClientIP**
Device Time	**Datetime**

Sample 6: The following sample event message shows that an HTTP request matches a firewall rule and the connection request is dropped by the firewall.


```
{"Datetime":"2020-11-12T02:52:18Z","RayName":"5f0cf4c5fc8ce76c","Source":"firewallrules","RuleId
":"6e40b9ea4da54b22a112626996d3111f","Action":"drop","EdgeColoName":"EWR","ClientIP":"10.0.0.1",
"ClientCountryName":"xx","ClientASNDescription":"ASN-DESCRIPTION","UserAgent":"curl/
7.29.0","ClientRequestHTTPMethodName":"GET","ClientRequestHTTPHost":"host.domain.test"}
```


Table 419. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**Action**
Source IP	**ClientIP**
Device Time	**Datetime**

Chapter 44. CloudPassage Halo

The CloudPassage Halo DSM for IBM QRadar can collect event logs from the CloudPassage Halo account.

The following table identifies the specifications for the CloudPassage Halo DSM:

Table 420. CloudPassage Halo DSM Specifications	
Specification	**Value**
Manufacturer	CloudPassage
DSM name	CloudPassage Halo
RPM file name	DSM-CloudPassageHalo-*build_number*.noarch.rpm
Supported versions	All
Event format	Syslog, Log file
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	No
More information	CloudPassage website (www.cloudpassage.com)

To integrate CloudPassage Halo with QRadar, use the following steps:

1. If automatic updates are not enabled, download the latest versions of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - CloudPassage Halo RPM
2. Configure your CloudPassage Halo to enable communication with QRadar.
3. If QRadar does not automatically detect CloudPassage Halo as a log source, create a CloudPassage Halo log source on the QRadar Console.

Configuring CloudPassage Halo for communication with QRadar

To collect CloudPassage Halo events, download and configure the CloudPassage Halo Event Connector script to send syslog events to QRadar.

Before you begin

Before you can configure the Event Connector, you must create a read-only CloudPassage API key. To create a read-only key, log in to your CloudPassage Portal and click **Add New Key** on the **Site Administration** window.

About this task

The Event Connector script requires Python 2.6 or later to be installed on the host on which the Event Connector script runs. The Event Connector makes calls to the CloudPassage Events API, which is available to all Halo subscribers.

Note: You can configure the CloudPassage Halo Event Collect to write the events to file for QRadar to retrieve by using the Log File Protocol, however, this method is not recommended.

Procedure

1. Log in to the CloudPassage Portal.

2. Go to **Settings > Site Administration**.
3. Click the **API Keys** tab.
4. Click **Show** for the key you want to use.
5. Copy the key ID and secret key into a text file.

   Ensure that the file contains only one line, with the key ID and the secret key separated by a vertical bar/pipe (|), for example, `your_key_id|your_secret_key`. If you want to retrieve events from multiple Halo accounts, add an extra line for each account.
6. Save the file as `haloEvents.auth`.
7. Download the Event Connector script and associated files from https://github.com/cloudpassage/halo-event-connector-python.
8. Copy the following files to a Linux or Windows system that has Python 2.6 (or later) installed:
   - haloEvents.py
   - cpapi.py
   - cputils.py
   - remote_syslog.py (use this script only if you deploy the Event Connector on Windows and you want to send events through syslog)
   - haloEvents.auth
9. Set the environment variables on the Linux or Windows system:
   - On Linux, include the full path to the Python interpreter in the PATH environment variable.
   - On Windows, set the following variables:
     - Set the PATH variable to include the location of `haloEvents.py` and the Python interpreter.
     - Set the PYTHONPATH variable to include the location of the Python libraries and the Python interpreter.
10. To send events through syslog with the Event Connector is deployed on a Windows system, run the haloEvents.py script with the **`--leefsyslog=<QRadar IP>`** switch:

    ```
    haloEvents.py --leefsyslog=192.0.2.1
    ```

    By default, the Event Connector retrieves existing events on initial connection and then retrieves onlynew events thereafter. To start event retrieval from a specific date, rather than retrieving all historical events on startup, use the **`--starting=<date>`** switch, where date is in the YYYY-MM-DD format:

    ```
    haloEvents.py --leefsyslog=192.0.2.1 --starting=2014-04-02
    ```
11. To send events through syslog and deploy the Event Connector on a Linux system, configure the local logger daemon.
    a) To check which logger the system uses, type the following command:

       ```
       ls -d /etc/*syslog*
       ```

       Depending on what Linus distribution you have, the following files might be listed:

       - `rsyslog.conf`
       - `syslog-ng.conf`
       - `syslog.conf`

    b) Edit the appropriate `.conf` file with relevant information for your environment.

       Example configuration for syslog-ng:

       ```
       source s_src {
             file("/var/log/leefEvents.txt");
       };
       destination d_qradar {
            udp("qradar_hostname" port(514));
       };
       log {
       ```

```
    source(s_src); destination(d_qradar);
};
```

c) To run the `haloEvents.py` script with the **leeffile=<filepath>** switch, type the following command:

`haloEvents.py --leeffile=/var/log/leefEvents.txt`

You can include **--starting=YYYY-MM-DD** switch to specify the date from which you want events to be collected for on initial startup.

Notice: As an alternative to using syslog, you can write events to a file for QRadar to retrieve by using the Log File protocol. For Windows or Linux to write the events to a file instead, use the **--leeffile=<filename>** switch to specify the file to write to.

Syslog log source parameters for CloudPassage Halo

If QRadar does not automatically detect the log source, add a CloudPassage Halo log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from CloudPassage Halo:

Table 421. Syslog log source parameters for the CloudPassage Halo DSM

Parameter	Value
Log Source type	**CloudPassage Halo**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your CloudPassage Halo devices.

Related tasks

Adding a log source

Log File log source parameters for CloudPassage Halo

If QRadar does not automatically detect the log source, add a CloudPassage Halo log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from CloudPassage Halo:

Table 422. Log File log source parameters for the CloudPassage Halo DSM

Parameter	Value
Log Source type	**CloudPassage Halo**
Protocol Configuration	**Log File**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your CloudPassage Halo devices.

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related tasks
Adding a log source

Chapter 45. CloudLock Cloud Security Fabric

The IBM QRadar DSM for CloudLock Cloud Security Fabric collects events from the CloudLock Cloud Security Fabric service.

The following table describes the specifications for the CloudLock Cloud Security Fabric DSM:

Table 423. CloudLock Cloud Security Fabric DSM specifications

Specification	**Value**
Manufacturer	CloudLock
DSM name	CloudLock Cloud Security Fabric
RPM file name	`DSM-CloudLockCloudSecurityFabric-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	NA
Protocol	Syslog
Event format	Log Event Extended Format (LEEF)
Recorded event types	Incidents
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Cloud Cybersecurity (https://www.cloudlock.com/products/)

To integrate CloudLock Cloud Security Fabric with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console in the order that they are listed:
   - DSMCommon RPM
   - CloudLock Cloud Security Fabric DSM RPM
2. Configure your CloudLock Cloud Security Fabric service to send Syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a CloudLock Cloud Security Fabric log source on the QRadar Console. The following table describes the parameters that require specific values for CloudLock Cloud Security Fabric event collection:

   Table 424. CloudLock Cloud Security Fabric log source parameters

Parameter	**Value**
Log Source type	CloudLock Cloud Security Fabric
Protocol Configuration	Syslog

The following table provides a sample event message for the CloudLock Cloud Security Fabric DSM:

Table 425. CloudLock Cloud Security Fabric sample message supported by the CloudLock Cloud Security Fabric service

Event name	Low level category	Sample log message
New Incident	Suspicious Activity	LEEF: 1.0|Cloudlock|API|v2|Incidents| match_count=2 sev=1 entity_id=ebR4q6DxvA entity_origin _type=document group=None url=https://example.com/ a/path/file/d/<File_path_ID/ view?usp=drivesdk CloudLockID=xxxxxxxxxx updated_at= 2016¬01-20T15:42:15.128356+0000 entity_owner_email= user@example.com cat=NEW entity_origin_id= <File_path_ID> entity_mime_type=text/ plain devTime=2016¬01-20T15:42:14.913178+0000 policy=Custom Regex resource=confidential.txt usrName= Admin Admin realm=domain policy_id=xxxxxxxxxx devTimeFormat=yyyy¬MM-dd'T'HH:mm:ss.SSSSSSZ LEEF: 1.0|Cloudlock|API|v2|Incidents|match_count=2 sev=1 entity_id=ebR4q6DxvA entity_origin_type=document group=None url=https://example.com/a/path/file/d/ <File_path_ID/view?usp=drivesdk CloudLockID=xxxxxxxxxx updated_at=2016¬01-20T15:42:15.128356+0000 entity_owner_email=user@example.com cat=NEW entity_origin_id=<File_path_ID> entity_mime_type=text/ plain devTime=2016¬01-20T15:42:14.913178+0000 policy=Custom Regex resource=confidential.txt usrName=Admin Admin realm=domain policy_id=xxxxxxxxxx devTimeFormat=yyyy¬MM-dd'T'HH:mm:ss.SSSSSSZ

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring CloudLock Cloud Security Fabric to communicate with QRadar

You can configure CloudLock Cloud Security Fabric to communicate with QRadar by using a Python script.

Before you begin

- To collect incidents from CloudLock, a script that makes CloudLock API calls is required. This script collects incidents and coverts them to Log Event Extended Format (LEEF).
- Python is required.

Procedure

1. Generate a CloudLock API token. To generate an API token in CloudLock, open the Settings. Go to the **Integrations** panel. Copy the Access token that appears on the page.
2. Go to the CloudLock Support website (https://www.cloudlock.com/support/). Open a support case to obtain the `cl_sample_incidents.py` file and then schedule the script for event collection.

Chapter 46. Correlog Agent for IBM z/OS

The CorreLog Agent for IBM z/OS DSM for IBM QRadar can collect event logs from your IBM z/OS servers.

The following table identifies the specifications for the CorreLog Agent for IBM z/OS DSM:

Specification	Value
Manufacturer	CorreLog
DSM name	CorreLog Agent for IBM z/OS
RPM file name	`DSM-CorreLogzOSAgent_qradar-version_build-number.noarch.rpm`
Supported versions	7.1 7.2
Protocol	Syslog LEEF
QRadar recorded events	All events
Automatically discovered	Yes
Includes identity	No
Includes custom event properties	No
More information	Correlog website (https://correlog.com/solutions-and-services/sas-correlog-mainframe.html)

To integrate CorreLog Agent for IBM z/OS DSM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent CorreLog Agent for IBM z/OS RPM from the IBM Support Website onto your QRadar Console.
2. For each CorreLog Agent instance, configure your CorreLog Agent system to enable communication with QRadar.
3. If QRadar does not automatically discover the DSM, create a log source on the QRadar Console for each CorreLog Agent system you want to integrate. Configure all the required parameters, but use the following table for specific Correlog values:

Parameter	Description
Log Source Type	CorreLog Agent for IBM zOS
Protocol Configuration	Syslog

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring your CorreLog Agent system for communication with QRadar

For the procedure to configure your Correlog Agent system for communication with QRadar, see the CZA - CorreLog Agent for z/OS manual that you received from CorreLog with your Agent for z/OS software distribution.

About this task

Use the following sections of the CZA - CorreLog Agent for z/OS manual:

- General considerations in **Section 1: Introduction**.
- Procedure in **Section 2: Installation**.
- Procedure in the **Section 3: Configuration**.

  Ensure that you complete the **Tailoring the Installation for a Proprietary Syslog Extension/IBM QRadar instructions**.

  When you start the CorreLog agent, if QRadar does not collect z/OS events, see the **Troubleshooting topic in Section 3**.
- If you want to customize the optional CorreLog Agent parameter file, review QRadar normalized event attributes in **Appendix G: Fields**.

Chapter 47. CrowdStrike Falcon

The IBM QRadar DSM for CrowdStrike Falcon collects Syslog events that are forwarded by a Falcon SIEM Connector.

To integrate CrowdStrike Falcon with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - CrowdStrike Falcon Host DSM RPM
2. Configure your Falcon SIEM connector to send events to QRadar. For more information, see Configuring CrowdStrike Falcon to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a CrowdStrike Falcon log source on the QRadar Console. For more information, see Syslog log source parameters for CrowdStrike Falcon.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

CrowdStrike Falcon DSM specifications

When you configure CrowdStrike Falcon understanding the specifications for the CrowdStrike Falcon DSM can help ensure a successful integration. For example, knowing what the supported version of CrowdStrike Falcon is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the CrowdStrike Falcon DSM.

Table 426. CrowdStrike Falcon DSM specifications

Specification	Value
Manufacturer	CrowdStrike
DSM name	CrowdStrike Falcon
RPM file name	DSM-*CrowdStrikeFalconHost-QRadar_version-build_number*.noarch.rpm
Protocol	Syslog
Event format	LEEF, JSON

Table 426. CrowdStrike Falcon DSM specifications (continued)	
Specification	**Value**
Recorded event types	Incident Incident summary Detection summary Authentication Detection status update Uploaded IoCs Network containment IP whitelisting Policy management CrowdStrike store Falcon firewall management Real time response Event streams
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	CrowdStrike Falcon Platform website (https://www.crowdstrike.com/endpoint-security-products/falcon-platform/)

Configuring CrowdStrike Falcon to communicate with QRadar

To send LEEF events from CrowdStrike Falcon to IBM QRadar, you must install and configure Falcon SIEM connector.

Tip: To obtain CrowdStrike event data, you can also use the CrowdStrike app extension from the IBM Security App Exchange. For more information, see How to Use CrowdStrike with IBM's QRadar (https://www.crowdstrike.com/blog/tech-center/crowdstrike-qradar/).

Before you begin

You must have Falcon Administrator privileges to generate API credentials.

Procedure

1. Obtain a Client ID, Client Secret key and Base URL to configure Falcon SIEM Connector.
   a) Log in to your CrowdStrike Falcon.
   b) From the Falcon menu, in the **Support** pane, click **API Clients and KeysSelect**.
   c) Click **Add new API client**.
   d) In the **API SCOPES** pane, select **Event streams** and then enable the **Read** option.
   e) To save your changes, click **Add**.
   f) Record the **Client ID**, **Client Secret** and **Base URL** values.
2. Install the Falcon SIEM Connector. You must have **Admin (root)** privileges.

Note: The SIEM Connector must be deployed on premise, on a system that has one the following operating systems:

- CentOS/RHEL 6.x - 7.x (64 bit)
- Ubuntu 14.x (64 bit)
- Ubuntu 16.04 (64-bit)
- Ubuntu 18.04 (64-bit)

a) Download the RPM installer package for your operating system to your Linux server.

b) To install the package, type one of the following commands:

- If you have a CentOS operating system, type the `sudo rpm -Uvh <installer package>` command.
- If you have a Ubuntu operating system, type the `sudo dpkg -i <installer package>` command.

The Falcon SIEM Connector installs in the `/opt/crowdstrike/` directory by default.

A service is created in the `/etc/init.d/cs.falconhoseclientd/` directory.

3. Configure the SIEM Connector to forward LEEF events to QRadar.

The configuration files are located in the `/opt/crowdstrike/etc/` directory.

- Rename `cs.falconhoseclient.leef.cfg` to `cs.falconhoseclient.cfg` for LEEF configuration settings. The SIEM Connector uses `cs.falconhoseclient.cfg` configuration by default.

The following table describes some of the key parameter values for forwarding LEEF events to QRadar.

Table 427. Key parameter values

Key	Description	Value
version	The version of authentication to be used. In this case, it is the API Key Authentication version.	2
api_url	The SIEM connector connects to this endpoint URL.	Specify one of the following values based on your Cloud. • `https://api.crowdstrike.com/sensors/entities/datafeed/v2(US-1)` • `https://api.us-2.crowdstrike.com/sensors/entities/datafeed/v2 (US-2)` • `https://api.eu-1.crowdstrike.com/sensors/entities/datafeed/v2 (EU-1)` • `https://api.laggar.gcw.crowdstrike.com/sensors/entities/datafeed/v2 (US-GOV-1)`
app_id	An arbitrary string identifier for connecting to Falcon Streaming API.	Any string. For example, `FHAPI-LEEF`
client_id	The client_id value is used as the credential for client verification.	Obtained at Step 1

Table 427. Key parameter values (continued)		
Key	**Description**	**Value**
client_secret	The client_secret value is used as the credential for client verification.	Obtained at Step 1
send_to_syslog_ server	To enable or disable Syslog push to Syslog server, set the flag to true or false.	True
host	The IP or host name of the SIEM.	The QRadar SIEM IP or host name where the Connector is forwarding the LEEF events.
header_delim	Header prefix and fields are delimited by this value.	The value must be a pipe (|).
field_delim	The delimiter value that is used to separate key-value pairs.	The value must be a tab (\t).
time_fields	This datetime field value is converted to a specified time format.	The default field is devTime (device time). If a custom LEEF key is used for setting the device time, use a different field name .

4. To start the SIEM Connector service, type one of the following one of the following commands:
   - If you have a CentOS operating system, type the `sudo service cs.falconhoseclientd start` command.
   - If you have a Ubunto 14.x operating system, type the `sudo start cs.falconhoseclientd` command.
   - If you have a Ubuntu 16.04 or later operating system, type the `sudo systemctl start cs.falconhoseclientd.service` command.
5. Optional: If you want to stop the SIEM Connector service, type one of the following commands:
   - If you have a CentOS operating system, type the `sudo service cs.falconhoseclientd stop` command.
   - If you have a Ubunto 14.x operating system, type the `sudo stop cs.falconhoseclientd` command.
   - If you have a Ubuntu 16.04 or later operating system, type the `sudo systemctl stop cs.falconhoseclientd.service` command.
6. Optional: If you want to restart the SIEM Connector service, type one of the following commands:
   - If you have a CentOS operating system, type the `sudo service cs.falconhoseclientd restart` command.
   - If you have a Ubunto 14.x operating system, type the `sudo restart cs.falconhoseclientd` command.
   - If you have an Ubuntu 16.04 or later operating system, type the `sudo systemctl restart cs.falconhoseclientd.service` command.

What to do next

Add a Syslog log source in QRadar. For more information, see Syslog log source parameters for CrowdStrike Falcon.

Syslog log source parameters for CrowdStrike Falcon

If QRadar does not automatically detect the log source, add a CrowdStrike Falcon log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Syslog events from CrowdStrike Falcon Connector:

Table 428. Syslog log source parameters for the CrowdStrike Falcon DSM

Parameter	Value
Log Source type	CrowdStrike Falcon
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name where the Falcon SIEM Connector is installed.

For more information about the protocol parameters and their values, see Adding a log source.

CrowdStrike Falcon Host sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

CrowdStrike Falcon Host sample message when you use the Syslog protocol

The following sample shows a detection summary event that was generated when a known malware accessed a document on the host. This event contains the details of the document and the time that the document was accessed.

```
LEEF:1.0|CrowdStrike|FalconHost|1.0|Suspicious Activity| devTime=2016-06-09 02:57:28
src=10.1.1.1 srcPort=49220 dst=10.1.1.2 domain=I cat=NetworkAccesses usrName=test
devTimeFormat=yyyy-MM-dd HH:mm:ss connDir=0 dstPort=443 resource=<Resource> proto=TCP
url=https://example.com/url
```

Table 429. QRadar field names and highlighted values in the event payloads

QRadar field name	Highlighted values in the event payload
Event ID	**Suspicious Activity**
Category	**CrowdStrike** + **FalconHost**
Source IP	**10.1.1.1**
Source Port	**49220**
Destination IP	**10.1.1.2**
Destination Port	**443**
Event Time	**2016-06-09 02:57:28**
Username	**test**

Chapter 48. CrowdStrike Falcon Data Replicator

The IBM QRadar DSM for CrowdStrike Falcon Data Replicator collects JSON events from a CrowdStrike Falcon Data Replicator.

To integrate the CrowdStrike Falcon Data Replicator with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console.
   - Protocol Common RPM
   - Amazon AWS S3 REST API Protocol RPM
   - DSM Common RPM
   - CrowdStrike Falcon Host DSM RPM
2. Configure your CrowdStrike Falcon Data Replicator device to send events to QRadar. For more information, see "Configuring CrowdStrike Falcon Data Replicator to communicate with IBM QRadar" on page 734.
3. If QRadar does not automatically detect the log source, add a CrowdStrike Falcon Data Replicator log source on the QRadar Console. For more information, see "Amazon AWS S3 REST API parameters for CrowdStrike Falcon Data Replicator log source" on page 734.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

CrowdStrike Falcon Data Replicator DSM specifications

The IBM QRadar DSM for CrowdStrike Falcon Data Replicator supports events that are collected from CrowdStrike FDR by using the Amazon AWS S3 REST API protocol.

The following table lists the specifications for the CrowdStrike Falcon Data Replicator DSM.

Table 430. CrowdStrike Falcon Data Replicator DSM specifications

Specification	**Value**
Manufacturer	CrowdStrike
DSM name	Falcon Data Replicator
RPM file name	DSM-*CrowdStrikeFalconDataReplicator-QRadar_version-Build_number*.noarch.rpm
Supported protocols	Amazon AWS S3 REST API
Event format	JSON
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Falcon Data Replicator(https://falcon.us-2.crowdstrike.com/documentation/page/fa572b1c/falcon-data-replicator)

Configuring CrowdStrike Falcon Data Replicator to communicate with IBM QRadar

To collect CrowdStrike Falcon Data Replicator events, configure your Falcon Data Replicator to send JSON events to QRadar.

The IBM QRadar DSM for CrowdStrike Falcon Data Replicator supports events that are collected from the Falcon Data Replicator, with the help of Amazon AWS S3 REST API protocol.

Procedure

Configure CrowdStrike Falcon Data Replicator to communicate with QRadar by following the *Configuration* steps under **Falcon Data Replicator setup** at Crowdstrike FDR(https://falcon.us-2.crowdstrike.com/documentation/page/fa572b1c/falcon-data-replicator).

What to do next

Add a CrowdStrike Falcon Data Replicator - Amazon AWS S3 REST log source in QRadar. For more information, see "Amazon AWS S3 REST API parameters for CrowdStrike Falcon Data Replicator log source" on page 734.

Amazon AWS S3 REST API parameters for CrowdStrike Falcon Data Replicator log source

The IBM QRadar DSM for CrowdStrike Falcon Data Replicator collects JSON events from a CrowdStrike Falcon Data Replicator.

If QRadar does not automatically detect the log source, add a CrowdStrike Falcon Data Replicator log source on the QRadar Console by using the Amazon AWS REST API protocol.

Configure specific parameters when you are using the Amazon AWS REST API protocol.

The following table describes the parameters that require specific values to collect the Amazon AWS REST API events from CrowdStrike Falcon Data Replicator:

Table 431. CrowdStrike Falcon Data Replicator log source parameters

Parameter	Value
Log Source type	CrowdStrike Falcon Data Replicator
Protocol Configuration	Amazon AWS REST API
Log Source Identifier	Type a unique name for the log source.
Event Format	Select **LINEBYLINE**

For a complete list of Amazon AWS S3 REST API protocol parameters and their values, see Amazon AWS S3 REST API protocol configuration options.

For more information about the protocol parameters and their values, see Adding a log source.

CrowdStrike Falcon Data Replicator sample event message

The Falcon Data Replicator feed consists of regular transfers of data (data memory dumps) rather than ongoing streams of data.

The following sample event message shows primary and secondary events that are collected from falcon data replicator.

Primary Events


```
{"event_simpleName":"SensorHeartbeat","ConfigStateHash":"401382615","NetworkContainmentState":"0
","aip":"10.0.0.0","ConfigIDBase":"65994763","SensorStateBitMap":"0","ConfigBuild":"1007.3.00177
06.11","event_platform":"Win","ConfigurationVersion":"10","Entitlements":"15","name":"SensorHear
tbeatV4","ConfigIDPlatform":"3","id":"*****-****-490e-*****-
****8","ConfigIDBuild":"17706","EffectiveTransmissionClass":"0","aid":"****11****","ProvisionSta
te":"1","timestamp":"1705904285259","cid":"56177c****11****0a0d64485abf698b5018d95f6c"}
```


Table 432. Highlighted values in the CrowdStrike Falcon Data Replicator sample primary event

QRadar field name	Highlighted payload field name
Event ID	**event_simpleName**
Source IP	**aip**
Device Time	**timestamp**


```
{"eid":118,"UserIp":"10.0.0.3","CustomerIdString":"56177c****11****0a0d64485abf698b5018d95f6c","
EventType":"Event_ExternalApiEvent","OperationName":"logged","UTCTimestamp":1705980053283,"Audit
KeyValues":[{"ValueString":"123******","Key":"APIClientID"},
{"ValueString":"56177c****11****0a0d64485abf698b5018d95f6c","Key":"cid"}],"Success":true,"Extern
alApiType":"Event_AuthActivityAuditEvent","Nonce":1,"ServiceName":"api_request","UserId":"","Age
ntIdString":"","cid":"56177c****11****0a0d64485abf698b5018d95f6c","timestamp":"2024-01-23T03:20:
53Z"}
```


Table 433. Highlighted values in the CrowdStrike Falcon Data Replicator sample primary event

QRadar field name	Highlighted payload field name
Event ID	**EventType**
Source IP	**UserIp**
Device Time	**timestamp**

Secondary Events


```
{"GatewayIP":"172.31.80.1","GatewayMAC":"00-00-5E-00-53-00","InterfaceAlias":"Ethernet
2","InterfaceDescription":"AWS PV Network Device
#0","LocalAddressIP4":"10.0.0.12","MAC":"00-00-5E-00-53-01","MACPrefix":"00-00-5E","_time":"1704
503615.475","aid":"123******","cid":"123******"}
```


Table 434. Highlighted values in the CrowdStrike Falcon Data Replicator sample secondary event

QRadar field name	Highlighted payload field name
Event ID	**falcondatareplicator_secondary_event(Fixed for secondary events)**
Source IP	**aip**
Source Mac	**MAC**
Device Time	**time**

Note: Secondary events are considered as metadata for primary events. If the feed is configured for secondary events, then the Event ID is parsed as described in table 3.

Types of Secondary Events

The different types of Secondary Events that are supported by IBM QRadar for CrowdStrike Falcon Data Replicator are given in the table.

Table 435. Types of secondary events in CrowdStrike Falcon Data Replicator	
Event name	**Description**
aid_master	Contains information for each host, such as hostname, domain, country, and sensor version. **Note:** This event is updated approx. every 5 minutes.
managedassets	Contains a list of assets that are running the Falcon sensor.
notmanaged	Contains a list of assets that are discovered by Falcon, which do not have the sensor installed.
appinfo	Contains information for every visible application in the environment such as company, file name, and version.
userinfo	Contains user information such as username, login time, and also when the password was last set.

Chapter 49. CRYPTOCard CRYPTO-Shield

The IBM QRadar DSM for CRYPTOCard CRYPTO-Shield for QRadar accepts events by using syslog.

To integrate CRYPTOCard CRYPTO-Shield events with QRadar, you must manually create a log source to receive syslog events.

Before you can receive events in QRadar, you must configure a log source, then configure your CRYPTOCard CRYPTO-Shield to forward syslog events. Syslog events that are forwarded from CRYPTOCard CRYPTO-Shield devices are not automatically discovered. QRadar can receive syslog events on port 514 for both TCP and UDP.

Configuring syslog for CRYPTOCard CRYPTO-Shield

To configure your CRYPTOCard CRYPTO-Shield device to forward syslog events:

Procedure

1. Log in to your CRYPTOCard CRYPTO-Shield device.
2. Configure the following System Configuration parameters:

   Important: You must have CRYPTOCard Operator access with the assigned default Super-Operator system role to access the System Configuration parameters.

   - `log4j.appender.<protocol>` - Directs the logs to a syslog host where:
     - <*protocol*> is the type of log appender, that determines where you want to send logs for storage. The options are as follows: ACC, DBG, or LOG. For this parameter, type the following entry: `org.apache.log4j.net.SyslogAppender`
   - `log4j.appender.<protocol>.SyslogHost <IP address>` - Type the IP address or host name of the syslog server where:
     - <*Protocol*> is the type of log appender, that determines where you want to send logs for storage. The options are as follows: ACC, DBG, or LOG.
     - <*IP address*> is the IP address of the IBM QRadar host to which you want to send logs.

   Specify the *IP address* parameter after the `log4j.apender.<protocol>` parameter is configured.

   The configuration is complete. Events that are forwarded to QRadar by CRYPTOCard CRYPTO-Shield are displayed on the **Log Activity** tab.

Syslog log source parameters for CRYPTOCard CRYPTO-Shield

If QRadar does not automatically detect the log source, add a CRYPTOCard CRYPTO-Shield log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from CRYPTOCard CRYPTO-Shield:

Table 436. Syslog log source parameters for the CRYPTOCard CRYPTO-Shield DSM

Parameter	Value
Log Source type	**CRYPTOCard CRYPTOShield**
Protocol Configuration	**Syslog**

Table 436. Syslog log source parameters for the CRYPTOCard CRYPTO-Shield DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your CRYPTOCard CRYPTO-Shield devices.

Related tasks

Adding a log source

Chapter 50. CyberArk

IBM QRadar provides DSMs to support several different CyberArk devices.

CyberArk Identity

The IBM QRadar DSM for CyberArk Identity collects logs from a CyberArk Identity log source.

Important: The Centrify Identity Platform DSM name is now the CyberArk Identity DSM. The DSM RPM name remains as Centrify Identity Platform in QRadar.

To integrate CyberArk Identity with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol Common RPM
   - Centrify Redrock REST API Protocol RPM
   - DSMCommon RPM
   - Centrify Identity Platform DSM RPM
2. Configure your CyberArk Identity DSM to communicate with QRadar.
3. Add a CyberArk Identity log source on the QRadar Console. The following table describes the Centrify Redrock REST API protocol parameters that require specific values to collect events from CyberArk Identity:

Table 437. Centrify Redrock REST API protocol log source parameters	
Parameter	**Value**
Log Source type	CyberArk Identity
Protocol Configuration	Centrify Redrock REST API

   For a complete list of Centrify Redrock REST API protocol parameters and their values, see Centrify Redrock REST API protocol configuration options.

Related concepts

"CyberArk Identity DSM specifications" on page 739
The following table describes the specifications for the CyberArk Identity DSM.

"CyberArk Identity sample event message" on page 741
Use this sample event message as a way of verifying a successful integration with QRadar.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5
"Configuring CyberArk Identity to communicate with QRadar" on page 740

CyberArk Identity DSM specifications

The following table describes the specifications for the CyberArk Identity DSM.

Note: The CyberArk Identity DSM was formerly called Centrify Identity Platform.

Table 438. CyberArk Identity DSM specifications	
Specification	**Value**
Manufacturer	Centrify

Table 438. CyberArk Identity DSM specifications (continued)	
Specification	**Value**
DSM name	CyberArk Identity
RPM file name	`DSM-CentrifyIdentityPlatform-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Centrify Redrock REST API
Event format	JSON
Recorded event types	SaaS Core Internal Mobile
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	CyberArk website (https://www.cyberark.com)

Configuring CyberArk Identity to communicate with QRadar

To send events to QRadar from CyberArk Identity, create a user role and configure a user policy on CyberArk Identity. The QRadar user can then create a log source in QRadar.

Important: Centrify Identity Platform is now CyberArk Identity. The DSM RPM name remains as Centrify Identity Platform in QRadar.

Before you begin

Ensure that you have the Tenant ID and admin login details that are supplied by CyberArk. Ensure that you have the correct user permissions for the CyberArk admin portal to complete the following steps:

Procedure

1. Log in to your CyberArk Identity admin portal.
2. Create a CyberArk Identity user role:
   a) From the navigation pane, click **Roles** > **Add Role**.
   b) In the **Name** field, type the name for the role.
   c) Select **Members**, and then click **Add**.
   d) In the **Add Members** window, search for the user name to assign to the role, and then select the member.
   e) Click **Add**.
   f) Select **Administrative Rights**, and then click **Add**.
   g) From the **Description** list, select **Read Only System Administrator**.
   h) Click **Save**.
3. Create an authentication profile:
   a) From the navigation pane, click **Settings** > **Authentication**.
   b) From the **Platform** menu, click **Authentication Profiles**.

c) Click **Add Profile**, and then type a name for the profile in the **Profile Name** field.

d) From the **Challenge 1** pane in the **Authentication Mechanisms** window, select **Password**.

e) From the **Challenge Pass-Through Duration** list, select **30 minutes**, and then click **OK**. The default is 30 minutes.

Important: Do not select any options from the **Challenge 2** pane in the **Authentication Mechanisms** window. Select options only from the **Challenge 1** pane.

4. Configure a user policy:

a) From the navigation pane, click **Policies** > **Add Policy Set**.

b) From the **Policy Setting** pane, type a name for the policy in the **Name** field.

c) From the **Policy Assignment** pane, click **Specified Roles**.

d) Click **Add**.

e) From the **Select Role** window, select the role that you created in Step 2 from the **Role** list, and then click **Add**.

f) From the **Policy Settings** menu, select **Login Policies** > **Centrify Portal**.

g) From the **Enable authentication policy controls** window, select **Yes**.

h) From the **Default Profile** pane, select the authentication profile that you created in Step 3 from the **Default Profile** list.

i) Click **Save**.

Note: If you have difficulty when configuring CyberArk Identity to communicate with QRadar, contact your CyberArk administrator or your CyberArk contact.

CyberArk Identity sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following sample event message shows a user login attempt when you use the Centrify Redrock REST API protocol for the CyberArk Identity DSM:


```
{"RequestIsMobileDevice": false,"AuthMethod": "MultiAuth","Level":
"Error","UserGuid": "c2c7bcc6-9560-44e0-8dff-5be221cd37ee","Mechanism":
"EMail","Tenant": "AAM0428","FromIPAddress": "<IP_address>","ID":
"772c2e1908a4f11b.W03.c5ab.a936852233b2232d","RequestDeviceOS": "Windows","EventType":
"Cloud.Core.Login.MultiFactorChallenge","RequestHostName": "192.0.2.1","ThreadType":
"RestCall","UserName": "username@example.com","NormalizedUser":
"username@example.com","WhenLogged": "/Date(1472679431199)/","WhenOccurred": "/
Date(1472679431199)/","Target": "username@example.com"}
```


CyberArk Privileged Threat Analytics

The IBM QRadar DSM for CyberArk Privileged Threat Analytics collects events from a CyberArk Privileged Threat Analytics device.

The following table describes the specifications for the CyberArk Privileged Threat Analytics DSM:

Table 439. CyberArk Privileged Threat Analytics DSM specifications

Specification	Value
Manufacturer	CyberArk
DSM name	CyberArk Privileged Threat Analytics
RPM file name	DSM-CyberArkPrivilegedThreatAnalytics-*Qradar_version-build_number*.noarch.rpm
Supported versions	V3.1
Protocol	Syslog

Table 439. CyberArk Privileged Threat Analytics DSM specifications (continued)	
Specification	**Value**
Recorded event types	Detected security events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	CyberArk website (http://www.cyberark.com)

To integrate CyberArk Privileged Threat Analytics with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - CyberArk Privileged Threat Analytics DSM RPM
   - DSMCommon RPM
2. Configure your CyberArk Privileged Threat Analytics device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a CyberArk Privileged Threat Analytics log source on the QRadar Console. The following table describes the parameters that require specific values for CyberArk Privileged Threat Analytics event collection:

Table 440. CyberArk Privileged Threat Analytics log source parameters	
Parameter	**Value**
Log Source type	CyberArk Privileged Threat Analytics
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring CyberArk Privileged Threat Analytics to communicate with QRadar

To collect all events from CyberArk Privileged Threat Analytics, you must specify IBM QRadar as the syslog server and configure the syslog format. The CyberArk Privileged Threat Analytics device sends syslog events that are formatted as Log Event Extended Format (LEEF).

Procedure

1. On the CyberArk Privileged Threat Analytics machine, go to the `/opt/tomcat/diamond-resources/local/` directory, and open the `systemparm.properties` file in a text editor such as vi.
2. Uncomment the `syslog_outbound` property and then edit the following parameters:

Parameter	**Value**
Host	The host name or IP address of the QRadar system.
Port	514
Protocol	UDP
Format	LEEF

The following is an example of the syslog_outbound property:

```
syslog_outbound=[{"host": "SIEM_MACHINE_ADDRESS", "port": "514", "format":
"LEEF", "protocol": "UDP"}]
```

The following is an example of the syslog_outbound property specifying multiple syslog recipients, separated by commas:

```
syslog_outbound=[{"host": "SIEM_MACHINE_ADDRESS", "port": "514", "format":
"LEEF", "protocol": "UDP"} , {"host": "SIEM_MACHINE_ADDRESS1", "port":
"514", "format": "LEEF", "protocol": "UDP"} , …]
```

3. Save the `systemparm.properties` configuration file, and then close it.
4. Restart CyberArk Privileged Threat Analytics.

CyberArk Vault

The CyberArk Vault DSM for IBM QRadar accepts events by using syslog that is formatted for Log Event Extended Format (LEEF).

QRadar records both user activities and safe activities from the CyberArk Vault in the audit event logs. CyberArk Vault integrates with QRadar to forward audit logs by using syslog to create a detailed log of privileged account activities.

Event type format

CyberArk Vault must be configured to generate events in Log Event Extended Format (LEEF) and to forward these events by using syslog. The LEEF format consists of a pipe (|) delimited syslog header, and tab separated fields in the log payload section.

If the syslog events from CyberArk Vault are not formatted properly, examine your device configuration or software version to ensure that your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to QRadar.

Configuring syslog for CyberArk Vault

To configure CyberArk Vault to forward syslog events to IBM QRadar, you must edit a file to specify parameters.

Procedure

1. Log in to your CyberArk device.
2. Edit the `DBParm.ini` file.
3. Configure the following parameters:

Table 441. Syslog parameters

Parameter	Description
SyslogServerIP	Type the IP address of QRadar.
SyslogServerPort	Type the UDP port that is used to connect to QRadar. The default value is 514.

Table 441. Syslog parameters (continued)	
Parameter	**Description**
SyslogMessageCodeFilter	Configure which message codes are sent from the CyberArk Vault to QRadar. You can define specific message numbers or a range of numbers. By default, all message codes are sent for user activities and safe activities. **Example:** To define a message code of 1,2,3,30 and 5-10, you must type: `1,2,3,5-10,30`.
SyslogTranslatorFile	Type the file path to the LEEF `.xsl` translator file. The translator file is used to parse CyberArk audit records data in the syslog protocol.

4. Copy LEEF `.xsl` to the location specified by the **`SyslogTranslatorFile`** parameter in the `DBParm.ini` file.

Results

The configuration is complete. The log source is added to QRadar as CyberArk Vault events are automatically discovered. Events that are forwarded by CyberArk Vault are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for CyberArk Vault

If QRadar does not automatically detect the log source, add a CyberArk Vault log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from CyberArk Vault:

Table 442. Syslog log source parameters for the CyberArk Vault DSM	
Parameter	**Value**
`Log Source type`	**CyberArk Vault**
`Protocol Configuration`	**Syslog**
`Log Source Identifier`	Type the IP address or host name for the log source as an identifier for events from your CyberArk Vault devices.

Related tasks

Adding a log source

Chapter 51. CyberGuard Firewall/VPN Appliance

The CyberGuard Firewall VPN Appliance DSM for IBM QRadar accepts CyberGuard events by using syslog.

QRadar records all relevant CyberGuard events for CyberGuard KS series appliances that are forwarded by using syslog.

Configuring syslog events

To configure a CyberGuard device to forward syslog events:

Procedure

1. Log in to the CyberGuard user interface.
2. Select the **Advanced** page.
3. Under **System Log**, select **Enable Remote Logging**.
4. Type the IP address of IBM QRadar.
5. Click **Apply**.

   The configuration is complete. The log source is added to QRadar as CyberGuard events are automatically discovered. Events that are forwarded by CyberGuard appliances are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for CyberGuard

If QRadar does not automatically detect the log source, add a CyberGuard log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from CyberGuard:

Table 443. Syslog log source parameters for the CyberGuard DSM

Parameter	Value
Log Source type	**CyberGuard TSP Firewall/VPN**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your CyberGuard devices.

Related tasks

Adding a log source

Chapter 52. Damballa Failsafe

The Failsafe DSM for IBM QRadar accepts syslog events by using the Log Event Extended Format (LEEF), enabling QRadar to record all relevant Damballa Failsafe events.

Damballa Failsafe must be configured to generate events in Log Event Extended Format(LEEF) and forward these events by using syslog. The LEEF format consists of a pipe (|) delimited syslog header, and tab separated fields in the log event payload.

If the syslog events that are forwarded from your Damballa Failsafe are not correctly formatted in LEEF format, you must check your device configuration or software version to ensure that your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to QRadar.

Configuring syslog for Damballa Failsafe

To collect events, you must configure your Damballa Failsafe device to forward syslog events to IBM QRadar.

Procedure

1. Log in to your Damballa Failsafe Management Console.
2. From the navigation menu, select **Setup** > **Integration Settings**.
3. Click the QRadar tab.
4. Select **Enable Publishing to** IBM QRadar.
5. Configure the following options:
   - **Hostname** - Type the IP address or Fully Qualified Name (FQN) of your QRadar Console.
   - **Destination Port** - Type 514. By default, QRadar uses port 514 as the port for receiving syslog events.
   - **Source Port** - This input is not a requirement. Type the Source Port your Damballa Failsafe device uses for sending syslog events.
6. Click **Save**.

   The configuration is complete. The log source is added to QRadar as Damballa Failsafe events are automatically discovered. Events that are forwarded by Damballa Failsafe are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Damballa Failsafe

If QRadar does not automatically detect the log source, add a Damballa Failsafe log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Damballa Failsafe:

Table 444. Syslog log source parameters for the Damballa Failsafe DSM

Parameter	Value
Log Source type	**Damballa Failsafe**
Protocol Configuration	**Syslog**

Table 444. Syslog log source parameters for the Damballa Failsafe DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Damballa Failsafe devices.

Related tasks
Adding a log source

Chapter 53. DG Technology MEAS

The IBM QRadar DSM for DG Technology MEAS can collect event logs from your DG Technology MEAS servers.

The following table identifies the specifications for the DG Technology MEAS DSM:

Table 445. DSM Specifications for DG Technology MEAS	
Specification	**Value**
Manufacturer	DG Technology
Log source type	DG Technology MEAS
RPM file name	`DSM-DGTechnologyMEAS-`*`build_number`*`.noarch.rpm`
Supported versions	8.x
Protocol configuration	LEEF Syslog
Supported event types	Mainframe events
Automatically discovered?	Yes
Includes identity?	No
Includes custom event properties	No
More information	DG Technology website (http://www.dgtechllc.com)

To integrate DG Technology MEAS DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent DG Technology MEAS RPM from the IBM Support Website onto your QRadar Console.
2. For each instance of DG Technology MEAS, configure your DG Technology MEAS system to enable communication with QRadar.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring your DG Technology MEAS system for communication with QRadar

To collect all audit logs and system events from DG Technology MEAS, you must specify QRadar as the syslog server.

Procedure

1. Log in to your DG Technology MEAS server.
2. Type the following command:

```
java meas/MeasServer 41000 m=qwl lo=IP_address_of_QRadar_host
```

Results

When QRadar receives events from your DG Technology MEAS, a log source is automatically created and listed on the **Log Sources** window.

Chapter 54. Digital China Networks (DCN)

The Digital China Networks (DCN) DCS/DCRS Series DSM for IBM QRadar can accept events from Digital China Networks (DCN) switches by using syslog.

IBM QRadar records all relevant IPv4 events that are forwarded from DCN switches. To integrate your device with QRadar, you must configure a log source, then configure your DCS or DCRS switch to forward syslog events.

Supported Appliances

The DSM supports the following DCN DCS/DCRS Series switches:

- DCS - 3650
- DCS - 3950
- DCS - 4500
- DCRS - 5750
- DCRS - 5960
- DCRS - 5980
- DCRS - 7500
- DCRS - 9800

Configuring a DCN DCS/DCRS Series Switch

To collect events, you must configure your DCN DCS/DCRS Series switch in IBM QRadar.

Procedure

1. Log in to your DCN DCS/DCRS Series Switch command-line interface (CLI).
2. Type the following command to access the administrative mode:

   ```
   enable
   ```
3. Type the following command to access the global configuration mode:

   ```
   config
   ```

   The command-line interface displays the configuration mode prompt:

   ```
   Switch(Config)#
   ```
4. Type the following command to configure a log host for your switch:

   ```
   logging <IP address> facility <local> severity <level>
   ```

   Where:

   - <*IP address*> is the IP address of the QRadar Console.
   - <*local*> is the syslog facility, for example, local0.
   - <*level*> is the severity of the syslog events, for example, informational. If you specify a value of informational, you forward all information level events and later (more severe), such as, notifications, warnings, errors, critical, alerts, and emergencies.

   For example,

   ```
   logging <IP_address> facility local0 severity informational
   ```
5. Type the following command to save your configuration changes:

   ```
   write
   ```

The configuration is complete. You can verify the events that are forwarded to QRadar by viewing events in the **Log Activity** tab.

Syslog log source parameters for DCN DCS/DCRS Series switches

If QRadar does not automatically detect the log source, add a DCN DCS/DCRS Series switches log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from DCN DCS/DCRS Series switches:

Table 446. Syslog log source parameters for the DCN DCS/DCRS Series switches DSM

Parameter	Value
Log Source type	**DCN DCS/DCRS Series**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your DCN DCS/DCRS Series switches devices.

Related tasks

Adding a log source

Chapter 55. Enterprise-IT-Security.com SF-Sherlock

The IBM QRadar DSM for Enterprise-IT-Security.com SF-Sherlock collects logs from your Enterprise-IT-Security.com SF-Sherlock servers.

The following table describes the specifications for the Enterprise-IT-Security.com SF-Sherlock DSM:

Table 447. Enterprise-IT-Security.com SF-Sherlock DSM specifications

Specification	**Value**
Manufacturer	Enterprise-IT-Security.com
DSM name	Enterprise-IT-Security.com SF-Sherlock
RPM file name	`DSM-EnterpriseITSecuritySFSherlock-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	v8.1 and later
Event format	Log Event Extended Format (LEEF)
Recorded event types	All_Checks, DB2_Security_Configuration, JES_Configuration, Job_Entry_System_Attack, Network_Parameter, Network_Security, No_Policy, Resource_Access_Viol, Resource_Allocation, Resource_Protection, Running_System_Change, Running_System_Security, Running_System_Status, Security_Dbase_Scan, Security_Dbase_Specialty, Security_Dbase_Status, Security_Parm_Change, Security_System_Attack, Security_System_Software, Security_System_Status, SF-Sherlock, Sherlock_Diverse, Sherlock_Diverse, Sherlock_Information, Sherlock_Specialties, Storage_Management, Subsystem_Scan, Sysplex_Security, Sysplex_Status, System_Catalog, System_File_Change, System_File_Security, System_File_Specialty, System_Log_Monitoring, System_Module_Security, System_Process_Security, System_Residence, System_Tampering, System_Volumes, TSO_Status, UNIX_OMVS_Security, UNIX_OMVS_System, User_Defined_Monitoring, xx_Resource_Prot_Templ
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Enterprise-IT-Security website (http:/www.enterprise-it-security.com)

To integrate Enterprise-IT-Security.com SF-Sherlock with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Enterprise-IT-Security.com SF-Sherlock DSM RPM
   - DSM Common RPM
2. Configure your Enterprise-IT-Security.com SF-Sherlock device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a Enterprise-IT-Security.com SF-Sherlock log source on the QRadar Console. The following table describes the parameters that require specific values for Enterprise-IT-Security.com SF-Sherlock event collection:

Table 448. Enterprise-IT-Security.com SF-Sherlock log source parameters

Parameter	Value
Log Source type	Enterprise-IT-Security.com SF-Sherlock
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Enterprise-IT-Security.com SF-Sherlock to communicate with QRadar

Before you can send SF-Sherlock events and assessment details to QRadar, implement the SF-Sherlock 2 QRadar connection kit.

About this task

The information that is sent to QRadar can be defined and selected in detail. Regardless of the selected transfer method, all information reaches QRadar as LEEF-formatted records.

Procedure

1. Install the UMODQR01 and UMODQR02 SF-Sherlock SMP/E user modifications by using the corresponding SHERLOCK.SSHKSAMP data set members.
2. If you send SF-Sherlock's LEEF records to a QRadar syslog daemon, which is generally the preferred transfer method, you must install the SF-Sherlock universal syslog message router in the USS environment of z/OS. You will find all installation details within the UNIXCMDL member of the SHERLOCK.SSHKSAMP data set.
3. Optional: If you transfer the logs by FTP or another technique, you must adapt the UMODQR01 user modification.
4. Enter the IP address for the QRadar LEEF syslog server, transfer method (UDP or TCP), and port number (514) in the QRADARSE member of SF-Sherlock's `init-deck` parameter configuration file.
5. Allocate the QRadar related log data set by using the ALLOCQRG job of the SHERLOCK.SSHKSAMP data set. It is used by the SHERLOCK started procedure (STC) to keep all QRadar LEEF records transferring to QRadar.
6. The QRDARTST member of the SHERLOCK.SSHKSAMP data set can be used to test the SF-Sherlock 2 QRadar message routing connection. If QRadar receives the test events, the implementation was successful.
7. Enable the SF-Sherlock 2 QRadar connection in your SF-Sherlock installation by activating QRADAR00 (event monitoring) and optionally, the QRADAR01 (assessment details) `init-deck` members, through the already prepared `ADD QRADARxx` statements within the $BUILD00 master control member.
8. Refresh or recycle the SHERLOCK started procedure to activate the new master control member that enables the connection of SF-Sherlock to QRadar.

Chapter 56. Epic SIEM

The IBM QRadar DSM for Epic SIEM can collect event logs from your Epic SIEM.

The following table identifies the specifications for the Epic SIEM DSM:

Table 449. Epic SIEM DSM specifications

Specification	**Value**
Manufacturer	Epic
DSM name	Epic SIEM
RPM file name	`DSM-EpicSIEM-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	Epic 2014, Epic 2015, Epic 2017, Epic 2022
Event format	LEEF
Recorded event types	Audit Authentication
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Epic website

To integrate Epic SIEM DSM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Epic SIEM DSM RPM
   - DSMCommon RPM
2. Configure your Epic SIEM device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an Epic SIEM log source on the QRadar Console. The following table describes the parameters that require specific values for Epic SIEM event collection:

   Table 450. Epic SIEM log source parameters

Parameter	**Value**
Log Source type	Epic SIEM
Protocol Configuration	Syslog

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring Epic SIEM 2014 to communicate with QRadar

To collect syslog events from Epic SIEM 2014, you must add an external syslog server for the IBM QRadar host.

Procedure

1. If all web services are not enabled for your instance of Interconnect, complete the following steps to run the required **SendSIEMSyslogAudit** service:
   a) To access the **Interconnect Configuration Editor**, click **Start** > **Epic 2014** > **Interconnect** > ***your_instance*** > **Configuration Editor**.
   b) In the **Configuration Editor**, select the **Business Services** form.
   c) On the **Service Category** tab, click **SendSIEMSyslogAudit**.
   d) Click **Save**
2. Log in to your Epic server.
3. Click **Epic System Definitions (%ZeUSTBL)** > **Security** > **Auditing Options** > **SIEM Syslog Settings** > **SIEM Syslog Configuration**.
4. Use the following table to configure the parameters:

Parameter	Description
SIEM Host	The host name or IP address of the QRadar appliance.
SIEM Port	514
SIEM Format	LEEF (Log Event Extended Format).

5. From the **SIEM Syslog Settings** menu, click **SIEM Syslog** and set it to `enabled`.

   The SIEM Syslog Sending daemon is automatically started when the environment is set to **runlevel Up** or when you enable **SIEM Syslog**.
6. If you want to stop the daemon, from the **SIEM Syslog Settings** menu, click **SIEM Syslog** and set it to disabled.

   Important: If you stop the daemon when the syslog setting is enabled, the system continues to log data without purging. If you want to stop the daemon when the syslog setting is enabled, contact your Epic representative or your system administrator.

Configuring Epic SIEM 2015 to communicate with QRadar

To collect events in IBM QRadar, you must configure the messaging queue values on your Epic SIEM 2015 system.

Procedure

1. From the command line, select **Interconnect Administrator's Menu** > **Messaging Queues Setup**.
2. Type an asterisk (*) to create the EMPSYNC queue.
3. Enter the queue values identified in the following table for each of the prompts.

Table 451. Queue values for EMPSYNC prompts

Prompt	Value
Queue ID	Type an ID for the queue.
Queue Name	EMPSYNC
Descriptor	EMPSYNC

Table 451. Queue values for EMPSYNC prompts (continued)	
Prompt	**Value**
Run on Node	Press the **Enter** key. The value is automatically populated.
IC Servers	Press the **Enter** key, without typing a value.
Edit advanced settings for this queue?	**Yes**
Does this queue handle synchronous outgoing messages?	**Yes**
Associate this descriptor with a queue type for outgoing communication?	**Yes**
Queue Type	**EMP**

4. Type an asterisk (*) to create the EMPASYNC queue.
5. Enter the queue values identified in the following table for each of the prompts.

Table 452. Queue values for EMPASYNC prompts	
Prompt	**Value**
Queue ID	Type an ID for the queue.
Queue Name	EMPASYNC
Descriptor	EMPASYNC
Run on Node	Press the **Enter** key. The value is automatically populated.
IC Servers	Press the **Enter** key, without typing a value.
Edit advanced settings for this queue?	**Yes**
Does this queue handle synchronous outgoing messages?	**No**
Associate this descriptor with a queue type for outgoing communication?	**Yes**
Queue Type	**EMP**

6. Deploy a new interconnect instance by using Kuiper.
7. Access the **Interconnect Configuration Editor** in Windows, by clicking **Start** > **Epic 2015** > **Interconnect** > ***your_instance*** > **Configuration Editor**.
8. Select the **General Web Service Host** role.
9. In **Cache Connections**, manually add the queue by the queue type, **EMP**.
10. Set the number of threads to **2**.

    For more information about thread count recommendations, refer to your Epic documentation.

    Important: Do not enable any services on the **Business Services** tab.
11. Log in to your Epic server.
12. Click **Epic System Definitions (%ZeUSTBL)** > **Security** > **Auditing Options** > **SIEM Syslog Settings**.
13. Select **SIEM Syslog Configuration**, and then configure the following parameters:

Parameter	**Value**
SIEM Host	Your QRadar Event Collector host name or IP address.

Parameter	Value
SIEM Port	514
SIEM Format	LEEF (Log Event Extended Format)
Check Application Layer Response	Disable

14. Return to the **SIEM Syslog Settings Menu**.
15. Select **SIEM Syslog** and set it to **Enabled**.

    Note: The SIEM Syslog Sending daemon is automatically started when the environment is set to **runlevel Up** or when you enable **SIEM Syslog**. If you want to stop the daemon, from the **SIEM Syslog Settings** menu, click **SIEM Syslog** and set it to **Disabled**.

Configuring Epic SIEM 2017 to communicate with QRadar

To collect events in IBM QRadar, you must configure the messaging queue values on your Epic SIEM 2017 system.

Procedure

1. From the command line, select **Interconnect Administrator's Menu** > **Messaging Queues Setup**.
2. Type an asterisk (*) to create the EMPSYNC queue.
3. Enter the queue values identified in the following table for each of the prompts.

Table 453. Queue values for EMPSYNC prompts

Prompt	Value
Queue ID	Type an ID for the queue.
Queue Name	EMPSYNC
Descriptor	EMPSYNC
Run on Node	Press the **Enter** key. The value is automatically populated.
IC Servers	Press the **Enter** key, without typing a value.
Edit advanced settings for this queue?	**Yes**
Does this queue handle synchronous outgoing messages?	**Yes**
Associate this descriptor with a queue type for outgoing communication?	**Yes**
Queue Type	**EMP**

4. Type an asterisk (*) to create the EMPASYNC queue.
5. Enter the queue values identified in the following table for each of the prompts.

Table 454. Queue values for EMPASYNC prompts

Prompt	Value
Queue ID	Type an ID for the queue.
Queue Name	EMPASYNC
Descriptor	EMPASYNC

Table 454. Queue values for EMPASYNC prompts (continued)	
Prompt	**Value**
Run on Node	Press the **Enter** key. The value is automatically populated.
IC Servers	Press the **Enter** key, without typing a value.
Edit advanced settings for this queue?	**Yes**
Does this queue handle synchronous outgoing messages?	**No**
Associate this descriptor with a queue type for outgoing communication?	**Yes**
Queue Type	**EMP**

6. Deploy a new interconnect instance by using Kuiper.
7. Access the **Interconnect Configuration Editor** in Windows, by clicking **Start** > **Epic 2017** > **Interconnect** > ***your_instance*** > **Configuration Editor**.
8. Select the **General Web Service Host** role.
9. In **Cache Connections**, manually add the queue by the queue type, **EMP**.
10. Set the number of threads to **2**.

    For more information about thread count recommendations, see your Epic documentation.

    Important: Do not enable any services on the **Business Services** tab.
11. Log in to your Epic server.
12. Click **Epic System Definitions (%ZeUSTBL)** > **Security** > **Auditing Options** > **SIEM Syslog Settings**.
13. Select **SIEM Syslog Configuration**, and then configure the following parameters:

Parameter	**Value**
SIEM Host	Your QRadar Event Collector host name or IP address.
SIEM Port	514
SIEM Format	LEEF (Log Event Extended Format)
Check Application Layer Response	Disable

14. Return to the **SIEM Syslog Settings Menu**.
15. If you want to reduce traffic that comes in to your SIEM system, disable the auditing events that your system does not require:
    a) Click **SIEM Syslog Configuration Options** > **Edit Events List**.
    b) From the **Edit Events List**, select **T** for each event that you want to disable.
    c) Click **Q** to quit.
16. Select **SIEM Syslog** and set it to **Enabled**.

    Note: The SIEM Syslog Sending daemon is automatically started when the environment is set to **runlevel Up** or when you enable **SIEM Syslog**. If you want to stop the daemon, from the **SIEM Syslog Settings** menu, click **SIEM Syslog** and set it to **Disabled**.

Configuring Epic SIEM 2022 to communicate with QRadar

To collect events in IBM QRadar, you must configure the messaging queue values on your Epic SIEM 2022 system.

Procedure

1. Create two custom queues by following the steps in the Create an Interconnect Queue.

   Important: Verify that the **EMPSYNC** queue is synchronous and the **EMPASYNC** queue is asynchronous.

   Enter **EMP** as the **Queue Type** for both queues.
2. Configure a new interconnect instance based on the SIEM use case.
3. Configure the **Syslog** protocol.
4. Click **Epic System Definitions (%ZeUSTBL or Epic Application Access)** > **Client Systems** > **Epic System Definitions**.

   Important: Epic System Definitions are accessible only to system administrators.
5. Click **Security** > **Auditing Options** > **SIEM Syslog Settings**.
6. Select **SIEM Syslog Configuration**, and configure the following parameters:

Parameter	Value
SIEM Host	Your QRadar Event Collector host name or IP address.
SIEM Port	514
SIEM Format	LEEF (Log Event Extended Format)
TCP Response	No
End Chars	ENDTAGNULL. The tag <SyslogEnd> is sent and then 10.
Starting in August 2023:	Use TLS

7. Return to the **SIEM Syslog Settings Menu**.
8. If you want to reduce traffic that comes in to your SIEM system, disable the auditing events that your system does not require:
   a) Click **SIEM Syslog Configuration Options** > **Edit Events List**.
   b) From the **Edit Events List**, select **T** for each event that you want to disable.
   c) Click **Q** to quit.
9. Select **SIEM Syslog** and set it to **Enabled**.

   Important: The SIEM Syslog Sending daemon is automatically started when the environment is set to **runlevel Up** or when you enable **SIEM Syslog**. If you want to stop the daemon, from the **SIEM Syslog Settings** menu, click **SIEM Syslog** and set it to **Disabled**.

Chapter 57. ESET Remote Administrator

The IBM QRadar DSM for ESET Remote Administrator collects logs from ESET Remote Administrator.

The following table describes the specifications for the ESET Remote Administrator DSM:

Table 455. ESET Remote Administrator DSM specifications

Specification	**Value**
Manufacturer	ESET
DSM name	ESET Remote Administrator
RPM file name	`DSM-ESETRemoteAdministrator-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	6.4.270
Protocol	Syslog
Event format	Log Event Extended Format (LEEF)
Recorded event types	Threat Firewall aggregated Host Intrusion Protection System (HIPS) aggregated Audit
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	ESET website (https://www.eset.com/us/support/download/business/remote-administrator-6)

To integrate ESET Remote Administrator with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - ESET Remote Administrator DSM RPM
2. Configure your ESET Remote Administrator server to send LEEF formatted syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an ESET Remote Administrator log source on the QRadar Console. The following table describes the parameters that require specific values for ESET Remote Administrator event collection:

Table 456. ESET Remote Administrator log source parameters

Parameter	**Value**
Log Source type	ESET Remote Administrator
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the ESET Remote Administration server.

4. To check that QRadar parses the events correctly, review the following sample event message.

   The following table shows a sample event message from ESET Remote Administrator:

Table 457. ESET Remote Administrator sample message

Event name	Low level category	Sample log message
Native user login	User Login Success	<14>1 2016-08-15T14:52:31.888Z hostname ERAServer 28021 - - LEEF:1.0|ESET|RemoteAdministrator|<Version>|Native user login|cat=ESET RA Audit Event sev=2 devTime=Aug 15 2016 14:52:31 devTime Format=MMM dd yyyy HH:mm:ss src=<Source_IP_address> domain=Native user action=Login attempt target=username detail=Native user 'username' attempted to authenticate. result=Success <14>1 2016-08-15T14:52:31.888Z hostname ERAServer 28021 - - LEEF:1.0|ESET|RemoteAdministrator|<Version>|Native user login|cat=ESET RA Audit Event sev=2 devTime=Aug 15 2016 14:52:31 devTimeFormat=MMM dd yyyy HH:mm:ss src=<Source_IP_address> domain=Native user action=Login attempt target=username detail=Native user 'username' attempted to authenticate. result=Success

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring ESET Remote Administrator to communicate with QRadar

Configure your ESET Remote Administrator (ERA) server to send LEEF formatted syslog events to IBM QRadar.

About this task

To complete the configuration, you must enable the Syslog server, and then configure the logging settings.

Note:

The required parameters listed in the following steps are configured in the **Server Settings** pane. To see a graphic, go to the ESET website. (http://help.eset.com/era_admin/64/en-US/index.html?admin_server_settings_export_to_syslog.htm)

Procedure

1. Log in to your ERA web console.
2. In the **Admin** navigation pane, click **Server Settings**.
3. In the **SYSLOG SERVER** area, select the **Use Syslog server** check box.
4. In the **Host** field, type the host name for your QRadar Event Collector.
5. In the **Port** field, type 514.
6. In the **LOGGING** area, select the **Export logs to Syslog** check box.
7. From the **Exported logs format** list, select **LEEF**.
8. Click **Save**.

Chapter 58. Exabeam

The IBM QRadar DSM for Exabeam collects events from an Exabeam device.

The following table describes the specifications for the Exabeam DSM:

Table 458. Exabeam DSM specifications

Specification	Value
Manufacturer	Exabeam
DSM name	Exabeam
RPM file name	`DSM-ExabeamExabeam-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	1.7 and v2.0
Recorded event types	Critical Anomalous
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Exabeam website (http://www.exabeam.com)

To integrate Exabeam with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Exabeam DSM RPM from the IBM Support Website onto your QRadar Console:
2. Configure your Exabeam device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an Exabeam log source on the QRadar Console. The following table describes the parameters that require specific values for Exabeam event collection:

Table 459. Exabeam log source parameters

Parameter	Value
Log Source type	Exabeam
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Exabeam to communicate with QRadar

To collect syslog events from Exabeam, you must add a destination that specifies QRadar as the syslog server.

Procedure

1. Log in to your Exabeam user interface (https://<*Exabeam_IP*>:8484).
2. Select `https://`<*Exabeam_IP*>`:8484` and type `#setup` at the end of the url address.

https://<*Exabeam_IP*>:8484/#setup

3. In the **Navigation** pane, click **Incident Notification**.
4. Select **Send via Syslog** and configure the following syslog parameters.

Parameter	Description
IP Address or Hostname	The IP address of the QRadar Event Collector .
Protocol	TCP
Port	514
Syslog Severity Level	Emergency

Exabeam sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Exabeam sample message when you use the Syslog protocol

The following sample event message shows a critical Exabeam event. A high risk user session is detected.

```
<85>Apr 06 22:03:02 exabeam.exabeam.test Exabeam: timestamp="2015-04-21T15:55:21.503+08:00"
id="testUser-20140402150331" url="http://localhost:8484/#sessions/userx-20140402150331"
score="105" start_time="2014-04-02T15:03:31+0800" end_time="1970-01-01T08:00:00+0800"
status="open" user="userx" src_host="test-host01-userx" src_ip="192.0.150.7" accounts="testUser"
labels="" assets="test-host01-userx" zones="test.zone.test" top_reasons="First logon to
workstation for user,First logon to network zone,Abnormal logon to network zone for group"
reasons_count="10" events_count="1" alerts_count="0"
```

Table 460. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**105** is critical and is extracted from the **score** value.
Source IP	**192.0.150.7**
Username	**userx**
Device Time	**2015-04-21T15:55:21.503+08:00**

Chapter 59. Extreme

IBM QRadar accepts events from a range of Extreme DSMs.

Extreme 800-Series Switch

The Extreme 800-Series Switch DSM for IBM QRadar accepts events by using syslog.

QRadar records all relevant audit, authentication, system, and switch events. Before you configure your Extreme 800-Series Switch in QRadar, you must configure your switch to forward syslog events.

Configuring your Extreme 800-Series Switch

Configuring the Extreme 800-Series Switch to forward syslog events.

About this task

To manually configure the Extreme 800-Series Switch:

Procedure

1. Log in to your Extreme 800-Series Switch command-line interface.

   You must be a system administrator or operator-level user to complete these configuration steps.
2. Type the following command to enable syslog:

   ```
   enable syslog
   ```
3. Type the following command to create a syslog address for forwarding events to QRadar:

   ```
   create syslog host 1 <IP address> severity informational facility local7
   udp_port 514 state enable
   ```

   Where: *<IP address>* is the IP address of your QRadar Console or Event Collector.
4. Type the following command to forward syslog events by using an IP interface address:

   ```
   create syslog source_ipif <name> <IP address>
   ```

   Where:

   - *<name>* is the name of your IP interface.
   - *<IP address>* is the IP address of your QRadar Console or Event Collector.

   The configuration is complete. The log source is added to QRadar as Extreme 800-Series Switch events are automatically discovered. Events that are forwarded to QRadar by Extreme 800-Series Switches are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Extreme 800-Series Switches

If QRadar does not automatically detect the log source, add a Extreme 800-Series Switches log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Extreme 800-Series Switches:

Table 461. Syslog log source parameters for the Extreme 800-Series Switches DSM

Parameter	Value
Log Source type	**Extreme 800-Series Switch**

Table 461. Syslog log source parameters for the Extreme 800-Series Switches DSM (continued)	
Parameter	**Value**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme 800-Series Switches devices.

Related tasks
Adding a log source

Extreme Dragon

The Extreme Dragon DSM for IBM QRadar accepts Extreme events by using syslog to record all relevant Extreme Dragon events.

About this task

To configure your QRadar Extreme Dragon DSM, use the following procedure:

Procedure

1. Create an Alarm Tool policy by using a Syslog notification rule. See “Creating a Policy for Syslog ” on page 766.
2. Configure the log source within QRadar. See “Syslog log source parameters for Extreme Dragon” on page 768.
3. Configure Dragon Enterprise Management Server (EMS) to forward syslog messages. See “Configure the EMS to forward syslog messages” on page 768.

Creating a Policy for Syslog

This procedure describes how to configure an Alarm Tool policy by using a syslog notification rule in the Log Event Extended Format (LEEF) message format.

About this task

LEEF is the preferred message format for sending notifications to Dragon Network Defense when the notification rate is high or when IPv6 addresses are displayed. If you do not want to use syslog notifications in LEEF format, refer to your *Extreme Dragon documentation* for more information.

To configure Extreme Dragon with an Alarm Tool policy by using a syslog notification rule, complete the following steps:

Procedure

1. Log in to the Extreme Dragon EMS.
2. Click the **Alarm Tool** icon.
3. Configure the Alarm Tool Policy:

   In the **Alarm Tool Policy View** > **Custom Policies** menu tree, right-click and select **Add Alarm Tool Policy**.
4. In the **Add Alarm Tool Policy** field, type a policy name.

   For example:

   QRadar

5. Click **OK**.
6. In the menu tree, select **QRadar**.
7. To configure the event group:

   Click the **Events Group** tab.
8. Click **New**.

   The **Event Group Editor** is displayed.
9. Select the event group or individual events to monitor.
10. Click **Add**.

    A prompt is displayed.
11. Click **Yes**.
12. In the right column of the **Event Group Editor**, type `Dragon-Events`.
13. Click **OK**.
14. Configure the Syslog notification rule:

    Click the **Notification Rules** tab.
15. Click **New**.
16. In the name field, type QRadar`-RuleSys`.
17. Click **OK**.
18. In the **Notification Rules** pane, select the newly created QRadar**-RuleSys** item.
19. Click the **Syslog** tab.
20. Click **New**.

    The **Syslog Editor** is displayed.
21. Update the following values:
    - **Facility** - Using the **Facility** list, select a facility.
    - **Level** - Using the **Level** list, select **notice**.
    - **Message** - Using the **Type** list, select **LEEF**.

    ```
    LEEF:Version=1.0|Vendor|Product|ProductVersion|eventID|devTime|
    ```

    ```
    proto|src|sensor|dst|srcPort|dstPort|direction|eventData|
    ```

    The LEEF message format delineates between fields by using a pipe delimiter between each keyword.
22. Click **OK**.
23. Verify that the notification events are logged as separate events:

    Click the **Global Options** tab.
24. Click the **Main** tab.
25. Make sure that **Concatenate Events** is not selected.
26. Configure the alarm information:

    Click the **Alarms** tab.
27. Click **New**.
28. Type values for the parameters:
    - **Name** - Type QRadar**-Alarm**.
    - **Type** - Select **Real Time**.
    - **Event Group** - Select **Dragon-Events**.
    - **Notification Rule** - Select the QRadar**-RuleSys** check box.
29. Click **OK**.

30. Click **Commit**.
31. Navigate to the **Enterprise View**.
32. Right-click on the **Alarm Tool** and select **Associate Alarm Tool Policy**.
33. Select the newly created QRadar **policy**. Click **OK**.
34. In the **Enterprise** menu, right-click the policy and select **Deploy**.

    You are now ready to configure a syslog log source in QRadar.

Syslog log source parameters for Extreme Dragon

If QRadar does not automatically detect the log source, add a Extreme Dragon log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Extreme Dragon:

Table 462. Syslog log source parameters for the Extreme Dragon DSM

Parameter	Value
Log Source type	**Extreme Dragon Network IPS**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme Dragon devices.

Related tasks

Adding a log source

Configure the EMS to forward syslog messages

Starting with Dragon Enterprise Management Server (EMS) v7.4.0 appliances, you must use syslog-ng for forwarding events to a Security and Information Manager such as IBM QRadar.

Syslogd has been replaced by syslog-ng in Dragon EMS v7.4.0 and later.

To configure EMS to forward syslog messages, you must choose one of the following:

- If you are using syslog-ng and Extreme Dragon EMS v7.4.0 and later, see "Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later" on page 768.
- If you are using syslogd and Extreme Dragon EMS v7.4.0 and below, see "Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier" on page 769.

Configuring syslog-ng Using Extreme Dragon EMS V7.4.0 and later

This section describes the steps to configure syslog-ng in non-encrypted mode and syslogd to forward syslog messages to IBM QRadar.

About this task

If you are using encrypted syslog-ng, refer to your *Extreme documentation*.

Do not run both syslog-ng and syslogd at the same time.

To configure syslog-ng in non-encrypted mode:

Procedure

1. On your EMS system, open the following file:

   `/opt/syslog-ng/etc/syslog-ng.conf`
2. Configure a **Facility** filter for the Syslog notification rule.

   For example, if you selected **facility** local1:

   ```
   filter filt_facility_local1 {facility(local1); };
   ```
3. Configure a **Level** filter for the Syslog notification rule.

   For example, if you selected **level** notice:

   ```
   filter filt_level_notice {level(notice); };
   ```
4. Configure a destination statement for the QRadar.

   For example, if the IP address of the QRadar is 192.0.2.1 and you want to use syslog port of 514, type:

   ```
   destination siem { tcp("192.0.2.1" port(514)); };
   ```
5. Add a log statement for the notification rule:

   ```
   log { source(s_local); filter (filt_facility_local1); filter
   (filt_level_notice); destination(siem); };
   ```
6. Save the file and restart syslog-ng.

   ```
   cd /etc/rc.d ./rc.syslog-ng stop ./rc.syslog-ng start
   ```
7. The Extreme Dragon EMS configuration is complete.

Configuring syslogd Using Extreme Dragon EMS V7.4.0 and earlier

If your Dragon Enterprise Management Server (EMS) is using a version earlier than V7.4.0 on the appliance, you must use syslogd for forwarding events to a Security and Information Manager such as IBM QRadar.

Procedure

1. On the Dragon EMS system, open the following file:

   `/etc/syslog.conf`
2. Add a line to forward the **facility** and **level** you configured in the syslog notification rule to QRadar.

   For example, to define the **facility** local1 and **level** notice:

   `local1.notice @<IP address>`

   Where:

   <*IP address*> is the IP address of the QRadar system.
3. Save the file and restart syslogd.

   ```
   cd /etc/rc.d ./rc.syslog stop ./rc.syslog start
   ```

   The Extreme Dragon EMS configuration is complete.

Extreme HiGuard Wireless IPS

The Extreme HiGuard Wireless IPS DSM for IBM QRadar records all relevant events by using syslog

Before you configure the Extreme HiGuard Wireless IPS device in QRadar, you must configure your device to forward syslog events.

Configuring Enterasys HiGuard

To configure the device to forward syslog events:

Procedure

1. Log in to the HiGuard Wireless IPS user interface.
2. In the left navigation pane, click **Syslog**, which allows the management server to send events to designated syslog receivers.

   The **Syslog Configuration** pane is displayed.
3. In the **System Integration Status** section, **enable** syslog integration.

   Enabling syslog integration allows the management server to send messages to the configured syslog servers. By default, the management server enables syslog.

   The **Current Status** field displays the status of the syslog server. The choices are: **Running** or **Stopped**. An error status is displayed if one of the following occurs:

   - One of the configured and enabled syslog servers includes a host name that cannot be resolved.
   - The management server is stopped.
   - An internal error occurred. If this error occurs, contact Enterasys Technical Support.
4. From **Manage Syslog Servers**, click **Add**.

   The **Syslog Configuration** window is displayed.
5. Type values for the following parameters:

   - **Syslog Server (IP Address/Hostname)** - Type the IP address or host name of the syslog server where events are sent.

   Note: Configured syslog servers use the DNS names and DNS suffixes configured in the **Server initialization and Setup Wizard** on the HWMH Config Shell.

   - **Port Number** - Type the port number of the syslog server to which HWMH sends events. The default is 514.
   - **Message Format** - Select **Plain Text** as the format for sending events.
   - **Enabled?** - Select **Enabled?** if you want events to be sent to this syslog server.
6. Save your configuration.

   The configuration is complete. The log source is added to IBM QRadar as HiGuard events are automatically discovered. Events that are forwarded to QRadar by Enterasys HiGuard are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Extreme HiGuard

If QRadar does not automatically detect the log source, add a Extreme HiGuard log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Extreme HiGuard:

Table 463. Syslog log source parameters for the Extreme HiGuard DSM

Parameter	Value
Log Source type	**Extreme HiGuard**
Protocol Configuration	**Syslog**

Table 463. Syslog log source parameters for the Extreme HiGuard DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme HiGuard devices.

Related tasks
Adding a log source

Extreme HiPath Wireless Controller

The Extreme HiPath Wireless Controller DSM for IBM QRadar records all relevant events by using syslog.

QRadar supports the following Extreme HiPath Wireless Controller events:

- Wireless access point events
- Application log events
- Service log events
- Audit log events

Configuring your HiPath Wireless Controller

To integrate your Extreme HiPath Wireless Controller events with IBM QRadar, you must configure your device to forward syslog events.

About this task

To forward syslog events to QRadar:

Procedure

1. Log in to the HiPath Wireless Assistant.
2. Click **Wireless Controller Configuration**.

   The **HiPath Wireless Controller Configuration** window is displayed.
3. From the menu, click **System Maintenance**.
4. From the **Syslog section**, select the **Syslog Server IP** check box and type the IP address of the device that receives the syslog messages.
5. Using the **Wireless Controller Log Level** list, select **Information**.
6. Using the **Wireless AP Log Level** list, select **Major**.
7. Using the **Application Logs** list, select **local.0**.
8. Using the **Service Logs** list, select **local.3**.
9. Using the **Audit Logs** list, select **local.6**.
10. Click **Apply**.

    You are now ready to configure the log source in QRadar.

Syslog log source parameters for Extreme HiPath

If QRadar does not automatically detect the log source, add a Extreme HiPath log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Extreme HiPath:

Table 464. Syslog log source parameters for the Extreme HiPath DSM	
Parameter	**Value**
Log Source type	**Extreme HiPath**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme HiPath devices.

Related tasks

Adding a log source

Extreme Matrix Router

The Extreme Matrix Router DSM for IBM QRadar accepts Extreme Matrix events by using SNMPv1, SNMPv2, SNMPv3, and syslog.

About this task

You can integrate Extreme Matrix Router version 3.5 with QRadar. QRadar records all SNMP events, syslog login, logout, and login failed events. Before you configure QRadar to integrate with Extreme Matrix, you must take the following steps:

Procedure

1. Log in to the switch/router as a privileged user.
2. Type the following command:

   ```
   set logging server <server number> description <description> facility
   <facility> ip_addr <IP address> port <port> severity <severity>
   ```

   Where:

   - <*server number*> is the server number with values 1 - 8.
   - <*description*> is a description of the server.
   - <*facility*> is a syslog facility, for example, local0.
   - <*IP address*> is the IP address of the server that receives the syslog messages.
   - <*port*> is the default UDP port that the client uses to send messages to the server. Use port 514 unless otherwise stated.
   - <*severity*> is the server severity level with values 1 - 9, where 1 indicates an emergency, and 8 is debug level.

   For example:

   ```
   set logging server 5 description ourlogserver facility local0 ip_addr
   192.0.2.1 port 514 severity 8
   ```
3. You are now ready to configure the log source in QRadar.

   Select **Extreme Matrix E1 Switch** from the **Log Source Type** list.

Related tasks

“Adding a log source” on page 5

Extreme Matrix K/N/S Series Switch

The Extreme Matrix Series DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant Matrix K-Series, N-Series, or S-Series standalone device events.

About this task

Before you configure QRadar to integrate with a Matrix K-Series, N-Series, or S-Series, take the following steps:

Procedure

1. Log in to your Extreme Matrix device command-line interface (CLI).
2. Type the following commands:
   a. `set logging server 1 ip-addr <IP Address of Event Processor> state enable`
   b. `set logging application RtrAcl level 8`
   c. `set logging application CLI level 8`
   d. `set logging application SNMP level 8`
   e. `set logging application Webview level 8`
   f. `set logging application System level 8`
   g. `set logging application RtrFe level 8`
   h. `set logging application Trace level 8`
   i. `set logging application RtrLSNat level 8`
   j. `set logging application FlowLimt level 8`
   k. `set logging application UPN level 8`
   l. `set logging application AAA level 8`
   m. `set logging application Router level 8`
   n. `set logging application AddrNtfy level 8`
   o. `set logging application OSPF level 8`
   p. `set logging application VRRP level 8`
   q. `set logging application RtrArpProc level 8`
   r. `set logging application LACP level 8`
   s. `set logging application RtrNat level 8`
   t. `set logging application RtrTwcb level 8`
   u. `set logging application HostDoS level 8`
   v. `set policy syslog extended-format enable`

   For more information on configuring the Matrix Series routers or switches, consult your vendor documentation.
3. You are now ready to configure the log sources in QRadar.

   To configure QRadar to receive events from an Extreme Matrix Series device, select **Extreme Matrix K/N/S Series Switch** from the **Log Source Type** list.

Related tasks

"Adding a log source" on page 5

Extreme NetSight Automatic Security Manager

The Extreme NetSight Automatic Security Manager DSM for IBM QRadar accepts events by using syslog.

About this task

QRadar records all relevant events. Before you configure an Extreme NetSight Automatic Security Manager device in QRadar, you must configure your device to forward syslog events.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Automatic Security Manager user interface.
2. Click the **Automated Security Manager** icon to access the **Automated Security Manager Configuration** window.

   Note: You can also access the **Automated Security Manager Configuration** window from the **Tool** menu.
3. From the left navigation menu, select **Rule Definitions**.
4. Choose one of the following options:

   If a rule is configured, highlight the rule. Click **Edit**.
5. To create a new rule, click **Create**.
6. Select the **Notifications** check box.
7. Click **Edit**.

   The **Edit Notifications** window is displayed.
8. Click **Create**.

   The **Create Notification** window is displayed.
9. Using the **Type** list, select **Syslog**.
10. In the **Syslog Server IP/Name** field, type the IP address of the device that receives syslog traffic.
11. Click **Apply**.
12. Click **Close**.
13. In the **Notification** list, select the notification that is configured.
14. Click **OK**.
15. You are now ready to configure the log source in QRadar.

    To configure QRadar to receive events from an Extreme NetSight Automatic Security Manager device, select **Extreme NetsightASM** from the **Log Source Type** list.

    For more information about your Extreme NetSight Automatic Security Manager device, see your vendor documentation.

Related tasks

"Adding a log source" on page 5

Extreme NAC

The Extreme NAC DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant events.

For details on configuring your Extreme NAC appliances for syslog, consult your vendor documentation. After the Extreme NAC appliance is forwarding syslog events to QRadar, the configuration is complete. The log source is added to QRadar as Extreme NAC events are automatically discovered. Events that are forwarded by Extreme NAC appliances are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Extreme NAC

If QRadar does not automatically detect the log source, add a Extreme NAC log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Extreme NAC:

Table 465. Syslog log source parameters for the Extreme NAC DSM

Parameter	Value
Log Source type	**Extreme NAC**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme NAC devices.

Related tasks

Adding a log source

Configuring Extreme stackable and stand-alone switches

The Extreme stackable and stand-alone switches DSM for IBM QRadar accepts events by using syslog.

About this task

QRadar records all relevant events. Before you configure an Extreme stackable and stand-alone switches device in QRadar, you must configure your device to forward syslog events.

To configure the device to forward syslog events to QRadar:

Procedure

1. Log in to the Extreme stackable and stand-alone switch device.
2. Type the following command:

   ```
   set logging server <index> [ip-addr <IP address>] [facility <facility>]
   [severity <severity>] [descr <description>] [port <port] [state <enable |
   disable>]
   ```

   Where:

   - <*index*> is the server table index number (1 - 8) for this server.
   - <*IP address*> is the IP address of the server you want to send syslog messages. You do not have to enter an IP address. If you do not define an IP address, an entry in the Syslog server table is created with the specified index number, and a message is displayed indicating that there is no assigned IP address.
   - <*facility*> is a syslog facility. Valid values are local0 to local7. You do not have to enter a facility value. If the value is not specified, the default value that is configured with the **`set logging`** default command is applied.
   - <*description*> is a description of the facility/server. You do not have to enter a description.
   - <*port*> is the default UDP port that the client uses to send messages to the server. If not specified, the default value that is configured with the **`set logging`** default command is applied. You do not have to enter a port value.

- <enable | disable> enables or disables this facility/server configuration. You do not have to choose an option. If the state is not specified, it does not default to either `enable` or `disable`.
- <*severity*> is the server severity level that the server will log messages. The valid range is 1 - 8. If not specified, the default value that is configured with the **`set logging`** default command is applied. You do not have to input a severity value. The following are valid values:
- 1: Emergencies (system is unusable)
- 2: Alerts (immediate action needed)
- 3: Critical conditions
- 4: Error conditions
- 5: Warning conditions
- 6: Notifications (significant conditions)
- 7: Informational messages
- 8: Debugging message

3. You can now ready to configure the log source in QRadar.

   To configure QRadar to receive events from an Extreme stackable and stand-alone switch device:

   From the **Log Source Type** list, select one of the following options:

   - **Extreme stackable and stand-alone switches**
   - **Extreme A-Series**
   - **Extreme B2-Series**
   - **Extreme B3-Series**
   - **Extreme C2-Series**
   - **Extreme C3-Series**
   - **Extreme D-Series**
   - **Extreme G-Series**
   - **Extreme I-Series**

   For more information about your Extreme stackable and stand-alone switches, see your vendor documentation.

Related tasks

“Adding a log source” on page 5

Extreme Networks ExtremeWare

The Extreme Networks ExtremeWare DSM for IBM QRadar records all relevant Extreme Networks ExtremeWare and Extremeware XOS device events by using syslog.

To integrate QRadar with an ExtremeWare device, you must configure a log source in QRadar, then configure your Extreme Networks ExtremeWare and Extremeware XOS devices to forward syslog events. For more information, see How to configure a syslog server (https://gtacknowledge.extremenetworks.com/articles/How_To/How-to-configure-a-syslog-server). QRadar does not automatically discover or add log sources for syslog events from ExtremeWare appliances.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Syslog log source parameters for Extreme Networks ExtremeWare

If QRadar does not automatically detect the log source, add a Extreme Networks ExtremeWare log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Extreme Networks ExtremeWare:

Table 466. Syslog log source parameters for the Extreme Networks ExtremeWare DSM

Parameter	Value
Log Source type	**Extreme Networks ExtremeWare Operating System (OS)**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme Networks ExtremeWare devices.

Related tasks

Adding a log source

Extreme XSR Security Router

The Extreme XSR Security Router DSM for IBM QRadar accepts events by using syslog.

About this task

QRadar records all relevant events. Before you configure an Extreme XSR Security Router in QRadar, you must configure your device to forward syslog events.

For more information about your Extreme XSR Security Router, see your vendor documentation.

To configure the device to send syslog events to QRadar:

Procedure

1. Using Telnet or SSH, log in to the XSR Security Router command-line interface.
2. Type the following commands to access config mode:
   a. `enable`
   b. `config`
3. Type the following command:

   `logging <IP address> low`

   Where: <*IP address*> is the IP address of your QRadar.
4. Exit from config mode.

   `exit`
5. Save the configuration:

   `copy running-config startup-config`

   You are now ready to configure the log sources in QRadar.

Related concepts

"Syslog log source parameters for Extreme XSR Security Router" on page 778

Syslog log source parameters for Extreme XSR Security Router

If QRadar does not automatically detect the log source, add a Extreme XSR Security Router log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Extreme XSR Security Router:

Table 467. Syslog log source parameters for the Extreme XSR Security Router DSM

Parameter	Value
Log Source type	**Extreme XSR Security Routers**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Extreme XSR Security Router devices.

Related tasks

Adding a log source

Chapter 60. F5 Networks

IBM QRadar accepts events from a range of F5 Networks DSMs.

F5 Networks BIG-IP AFM

The F5 Networks BIG-IP Advanced Firewall Manager (AFM) DSM for IBM QRadar accepts syslog events that are forwarded from F5 Networks BIG-IP AFM systems in name-value pair format.

About this task

QRadar can collect the following events from F5 BIG-IP appliances with Advanced Firewall Managers:

- Network events
- Network Denial of Service (DoS) events
- Protocol security events
- DNS events
- DNS Denial of Service (DoS) events

Before you can configure the Advanced Firewall Manager, you must verify that your BIG-IP appliance is licensed and provisioned to include Advanced Firewall Manager.

Procedure

1. Log in to your BIG-IP appliance Management Interface.
2. From the navigation menu, select **System** > **License**.
3. In the **License Status** column, verify that the Advanced Firewall Manager is licensed and enabled.
4. To enable the Advanced Firewall Manager, select **System** > **Resource** > **Provisioning**.
5. From the **Provisioning** column, select the check box and select **Nominal** from the list.
6. Click **Submit** to save your changes.

Configuring a logging pool

A logging pool is used to define a pool of servers that receive syslog events. The pool contains the IP address, port, and a node name that you provide.

Procedure

1. From the navigation menu, select **Local Traffic** > **Pools**.
2. Click **Create**.
3. In the **Name** field, type a name for the logging pool.

   For example, Logging_Pool.
4. From the **Health Monitor** field, in the **Available** list, select **TCP** and click **<<**.

   This clicking action moves the TCP option from the Available list to the Selected list.
5. In the **Resource** pane, from the **Node Name** list, select **Logging_Node** or the name you defined in “Configuring a logging pool” on page 779.
6. In the **Address** field, type the IP address for the QRadar Console or Event Collector.
7. In the **Service Port** field, type 514.
8. Click **Add**.
9. Click **Finish**.

Creating a high-speed log destination

The process to configure logging for BIG-IP AFM requires that you create a high-speed logging destination.

Procedure

1. From the navigation menu, select **System** > **Logs** > **Configuration** > **Log Destinations**.
2. Click **Create**.
3. In the **Name** field, type a name for the destination.

   For example, Logging_HSL_dest.
4. In the **Description** field, type a description.
5. From the **Type** list, select **Remote High-Speed Log**.
6. From the **Pool Name** list, select a logging pool from the list of remote log servers.

   For example, Logging_Pool.
7. From the **Protocol** list, select **TCP**.
8. Click **Finish**.

Creating a formatted log destination

The formatted log destination is used to specify any special formatting that is required on the events that are forwarded to the high-speed logging destination.

Procedure

1. From the navigation menu, select **System** > **Logs** > **Configuration** > **Log Destinations**.
2. Click **Create**.
3. In the **Name** field, type a name for the logging format destination.

   For example, Logging_Format_dest.
4. In the **Description** field, type a description.
5. From the **Type** list, select **Remote Syslog**.
6. From the **Syslog Format** list, select **Syslog**.
7. From the **High-Speed Log Destination** list, select your high-speed logging destination.

   For example, Logging_HSL_dest.
8. Click **Finished**.

Creating a log publisher

Creating a publisher allows the BIG-IP appliance to publish the formatted log message to the local syslog database.

Procedure

1. From the navigation menu, select **System** > **Logs** > **Configuration** > **Log Publishers**.
2. Click **Create**.
3. In the **Name** field, type a name for the publisher.

   For example, Logging_Pub.
4. In the **Description** field, type a description.
5. From the **Destinations** field, in the Available list, select the log destination name that you created in “Configuring a logging pool” on page 779 and click **<<** to add items to the Selected list.

This clicking action moves your logging format destination from the Available list to the Selected list. To include local logging in your publisher configuration, you can add **local-db** and **local-syslog** to the Selected list.

Creating a logging profile

Use the Logging profile to configure the types of events that your Advanced Firewall Manager is producing and to associate these events with the logging destination.

Procedure

1. From the navigation menu, select **Security** > **Event Logs** > **Logging Profile**.
2. Click **Create**.
3. In the **Name** field, type a name for the log profile.

   For example, Logging_Profile.
4. In the **Network Firewall** field, select the **Enabled** check box.
5. From the **Publisher** list, select the log publisher that you configured.

   For example, Logging_Pub.
6. In the **Log Rule Matches** field, select the **Accept**, **Drop**, and **Reject** check boxes.
7. In the **Log IP Errors** field, select the **Enabled** check box.
8. In the **Log TCP Errors** field, select the **Enabled** check box.
9. In the **Log TCP Events** field, select the **Enabled** check box.
10. In the **Storage Format** field, from the list, select **Field-List**.
11. In the **Delimiter** field, type , (comma) as the delimiter for events.
12. In the **Storage Format** field, select all of the options in the **Available Items** list and click **<<**.

    This clicking action moves all of the Field-List options from the **Available** list to the **Selected** list.
13. In the **IP Intelligence** pane, from the **Publisher** list, select the log publisher that you configured.

    For example, Logging_Pub.
14. Click **Finished**.

Associating the profile to a virtual server

The log profile you created must be associated with a virtual server in the **Security Policy** tab. This association allows the virtual server to process your network firewall events, along with local traffic.

About this task

Take the following steps to associate the profile to a virtual server.

Procedure

1. From the navigation menu, select **Local Traffic** > **Virtual Servers**.
2. Click the name of a virtual server to modify.
3. From the **Security** tab, select **Policies**.
4. From the **Log Profile** list, select **Enabled**.
5. From the **Profile** field, in the **Available** list, select **Logging_Profile** or the name you specified in “Creating a logging profile” on page 781 and click **<<**.

   This clicking action moves the Logging_Profile option from the **Available** list to the **Selected** list.
6. Click **Update** to save your changes.

The configuration is complete. The log source is added to IBM QRadar as F5 Networks BIG-IP AFM syslog events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP AFM are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for F5 Networks BIG-IP AFM

If QRadar does not automatically detect the log source, add a F5 Networks BIG-IP AFM log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from F5 Networks BIG-IP AFM:

Table 468. Syslog log source parameters for the F5 Networks BIG-IP AFM DSM

Parameter	Value
Log Source type	**F5 Networks BIG-IP AFM**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP AFM devices.

Related tasks

Adding a log source

F5 Networks BIG-IP AFM sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

F5 Networks BIG-IP AFM sample message when you use the syslog protocol

The following sample event message shows that a connection was dropped by the firewall.

```
<134>Apr 30 19:22:53 f5networks.bigipafm.test 1 2019-04-30T19:22:53.800131+02:00 testCompa
ny tmm 13301 23003142 [F5@12276 date_time="Apr 30 2019 19:22:52" bigip_mgmt_ip="10.13.101.251"
hostnam
e="testCompany" context_type="Virtual Server" context_name="/Common/V1_VmUAG_8443"
ip_intelligence_po
licy_name="/Common/V1_VmUAG.app/V1_VmUAG_ip_intelligence" source_ip="192.168.0.1"
dest_ip="172.16.0.1"
source_port="8080" dest_port="8443" vlan="/Common/Vlan290" ip_protocol="TCP" route_domain="1"
ip_in
telligence_threat_name="windows_exploits,spam_sources" action="Drop"
attack_type="custom_category" tr
anslated_source_ip="" translated_dest_ip="" translated_source_port="" translated_dest_port=""
transla
ted_vlan="" translated_ip_protocol="" translated_route_domain="" sa_translation_type=""
sa_translatio
n_pool="" flow_id="0000000000000000"] "Apr 30 2019
19:22:52","10.13.101.251","testCompany","","","","
Virtual Server","/Common/V1_VmUAG_8443","/Common/V1_VmUAG.app/
V1_VmUAG_ip_intelligence","192.168.0.1",
"172.16.0.1","8080","8443","/Common/
Vlan290","TCP","1","windows_exploits,spam_sources","Drop","custom
_category","","","","","","","","","","0000000000000000"
```

```
<134>Apr 30 19:22:53 f5networks.bigipafm.test 1 2019-04-30T19:22:53.800131+02:00 testCompany
tmm 13301 23003142 [F5@12276 date_time="Apr 30 2019 19:22:52" bigip_mgmt_ip="10.13.101.251"
hostname="testCompany" context_type="Virtual Server" context_name="/Common/V1_VmUAG_8443"
ip_intelligence_policy_name="/Common/V1_VmUAG.app/V1_VmUAG_ip_intelligence"
source_ip="192.168.0.1" dest_ip="172.16.0.1" source_port="8080" dest_port="8443" vlan="/Common/
Vlan290" ip_protocol="TCP" route_domain="1"
ip_intelligence_threat_name="windows_exploits,spam_sources" action="Drop"
```

```
attack_type="custom_category" translated_source_ip="" translated_dest_ip=""
translated_source_port="" translated_dest_port="" translated_vlan="" translated_ip_protocol=""
translated_route_domain="" sa_translation_type="" sa_translation_pool=""
flow_id="0000000000000000"] "Apr 30 2019
19:22:52","10.13.101.251","testCompany","","","","Virtual Server","/Common/V1_VmUAG_8443","/
Common/V1_VmUAG.app/V1_VmUAG_ip_intelligence","192.168.0.1","172.16.0.1","8080","8443","/Common/
Vlan290","TCP","1","windows_exploits,spam_sources","Drop","custom_category","","","","","","","
","","","0000000000000000"
```

F5 Networks BIG-IP APM

The F5 Networks BIG-IP Access Policy Manager (APM) DSM for IBM QRadar collects access and authentication security events from a BIG-IP APM device by using syslog.

To configure your BIG-IP LTM device to forward syslog events to a remote syslog source, choose your BIG-IP APM software version:

- “Configuring Remote Syslog for F5 BIG-IP APM V11.x to V14.x ” on page 783
- “Configuring a Remote Syslog for F5 BIG-IP APM 10.x ” on page 783

Configuring Remote Syslog for F5 BIG-IP APM V11.x to V14.x

You can configure syslog for F5 BIG-IP APM V11.x to V14.x.

About this task

To configure a remote syslog for F5 BIG-IP APM V11.x to V14.x take the following steps:

Procedure

1. Log in to the command-line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:

   `tmsh syslog remote server {<Name> {host <IP address>}}`

   Where:

   - *<Name>* is the name of the F5 BIG-IP APM syslog source.
   - *<IP address>* is the IP address of the QRadar Console.

   For example,

   `bigpipe syslog remote server {BIGIP_APM {host 192.0.2.1}}`
3. Type the following to save the configuration changes:

   `tmsh save sys config partitions all`

   The configuration is complete. The log source is added to QRadar as F5 Networks BIG-IP APM events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP APM are displayed on the **Log Activity** tab in QRadar.

Configuring a Remote Syslog for F5 BIG-IP APM 10.x

You can configure syslog for F5 BIG-IP APM 10.x

About this task

To configure a remote syslog for F5 BIG-IP APM 10.x take the following steps:

Procedure

1. Log in to the command-line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:

```
bigpipe syslog remote server {<Name> {host <IP address>}}
```

Where:

- <*Name*> is the name of the F5 BIG-IP APM syslog source.
- <*IP address*> is the IP address of QRadar Console.

For example,

```
bigpipe syslog remote server {BIGIP_APM {host 192.0.2.1}}
```

3. Type the following to save the configuration changes:

```
bigpipe save
```

The configuration is complete. The log source is added to IBM QRadar as F5 Networks BIG-IP APM events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP APM are displayed on the **Log Activity** tab.

Syslog log source parameters for F5 Networks BIG-IP APM

If QRadar does not automatically detect the log source, add a F5 Networks BIG-IP APM log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from F5 Networks BIG-IP APM:

Table 469. Syslog log source parameters for the F5 Networks BIG-IP APM DSM

Parameter	Value
Log Source type	**F5 Networks BIG-IP APM**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP APM devices.

Related tasks

Adding a log source

F5 Networks BIG-IP APM sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

F5 Networks BIG-IP APM sample message when you use the syslog protocol

The following sample event message shows that an ACL is matched. It also shows that the TCP traffic from 192.168.194.160:54636 to 172.16.0.12:4446 is allowed.

```
<173>Oct 25 11:52:34 f5networks.bigipapm.test notice tmm[20338]: 01580002:5: /path/to_file
_123:Common:b77e0b8e: allow ACL: /path/to_other_file_123:2 packet: tcp 192.168.194.160:54636 ->
172.16.0.12:4446
```

```
<173>Oct 25 11:52:34 f5networks.bigipapm.test notice tmm[20338]: 01580002:5: /
path/to_file_123:Common:b77e0b8e: allow ACL: /path/to_other_file_123:2 packet: tcp
192.168.194.160:54636 -> 172.16.0.12:4446
```

Note: For more information about F5 APM DSM, see the "Log message format" section in the *Reviewing BIG-IP log files* article. https://my.f5.com/manage/s/article/K16197

F5 Networks BIG-IP ASM

The IBM QRadar F5 Networks BIG-IP Application Security Manager (ASM) DSM collects web application security events from BIG-IP ASM appliances by using syslog.

About this task

To forward syslog events from an F5 Networks BIG-IP ASM appliance to QRadar, you must configure a logging profile.

A logging profile can be used to configure remote storage for syslog events, which can be forwarded directly to QRadar.

Procedure

1. Log in to the F5 Networks BIG-IP ASM appliance user interface.
2. In the **navigation** pane, select **Application Security** > **Options**.
3. Click **Logging Profiles**.
4. Click **Create**.
5. From the **Configuration** list, select **Advanced**.
6. Type a descriptive name for the **Profile Name** property.
7. Optional: Type a **Profile Description**.

   If you do not want data logged both locally and remotely, clear the **Local Storage** check box.
8. Select the **Remote Storage** check box.
9. From the **Type** list, select 1 of the following options:
   a) In BIG-IP ASM V12.1.2 or earlier, select **Reporting Server**.
   b) In BIG-IP ASM V13.0.0 or later, select **key-value pairs**.
   c) Or, select **Common Event Format**. Log messages are in Common Event Format (CEF).
10. From the **Protocol** list, select **TCP**.
11. In the **IP Address** field, type the IP address of the QRadar Console and in the **Port** field, type a port value of 514.
12. Select the **Guarantee Logging** check box.

    Note: Enabling the **Guarantee Logging** option ensures the system log requests continue for the web application when the logging utility is competing for system resources. Enabling the **Guarantee Logging** option can slow access to the associated web application.
13. Select the **Report Detected Anomalies** check box to allow the system to log details.
14. Click **Create**.

    The display refreshes with the new logging profile. The log source is added to QRadar as F5 Networks BIG-IP ASM events are automatically discovered. Events that are forwarded by F5 Networks BIG-IP ASM are displayed on the Log Activity tab of QRadar.

Syslog log source parameters for F5 Networks BIG-IP ASM

If QRadar does not automatically detect the log source, add a F5 Networks BIG-IP ASM log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from F5 Networks BIG-IP ASM:

Table 470. Syslog log source parameters for the F5 Networks BIG-IP ASM DSM	
Parameter	**Value**
Log Source type	**F5 Networks BIG-IP ASM**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP ASM devices.

Related tasks

Adding a log source

F5 Networks BIG-IP ASM sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

F5 Networks BIG-IP ASM sample messages when you use the syslog protocol

Sample 1: The following sample event message shows a distributed attack event.

```
<134>Jul 25 11:47:52 f5networks.asm.test
ASM:software_version="14.1.0",current_mitigation="alarm",unit_hostname="f5networks.asm.test",man
agement_ip_address="10.192.138.11",management_ip_address_2="",operation_mode="Transparent",date_
time="2019-07-25 11:41:38",policy_apply_date="2019-07-23 15:24:21",policy_name="/Common/
extranet_sonstige",vs_name="/Common/extranet-
t.qradar.example.test_443",anomaly_attack_type="Distributed Attack",uri="/
qradar.example.test",attack_status="ongoing",detection_mode="Number of Failed Logins
Increased",severity="Emergency",mitigated_entity_name="username",mitigated_entity_value="exnyjtg
k",mitigated_ipaddr_geo="N/
A",attack_id="2508639270",mitigated_entity_failed_logins="0",mitigated_entity_failed_logins_thre
shold="3",mitigated_entity_total_mitigations="0",mitigated_entity_passed_challenges="0",mitigate
d_entity_passed_captchas="0",mitigated_entity_rejected_logins="0",leaked_username_login_attempts
="0",leaked_username_failed_logins="0",leaked_username_time_of_last_login_attempt="2497667872",n
ormal_failed_logins="78",detected_failed_logins="70",failed_logins_threshold="100",normal_login_
attempts="91",detected_login_attempts="78",login_attempts_matching_leaked_credentials="0",total_
mitigated_login_attempts="60",total_client_side_integrity_challenges="0",total_captcha_challenge
s="0",total_blocking_page_challenges="0",total_passed_client_side_integrity_challenges="0",total
_passed_captcha_challenges="0",total_drops="0",total_successful_mitigations="0",protocol="HTTPS"
,login_attempts_matching_leaked_credentials_threshold="100",login_stress="73"
```

Sample 2: The following sample event shows multiple violations. The event contains the following violations:

1. Illegal URL length
2. Illegal request length
3. Illegal query string length
4. Illegal meta character in parameter value
5. Illegal file type
6. Illegal URL
7. Attack signature detected

When the sample event is parsed in QRadar, a separate event is created for each of the seven violations.

```
"Aug 18 11:16:29 f5networks.asm.test.com
ASM:unit_hostname=\"3600.lab.asm.f5net.com\",management_ip_address=\"172.30.0.20\",web_applicati
on_name=\"web_app\",policy_name=\"web_app_default\",policy_apply_date=\"2009-18-08
11:14:38\",violations=\"Illegal URL length,Illegal request length,Illegal query string
length,Illegal meta character in parameter value,Illegal file type,Illegal URL,Attack signature
detected\",support_id=\"5268275531735896872\",request_status=\"blocked\",response_code=\"0\",ip_
```

```
client=\"192.168.74.169\",method=\"GET\",protocol=\"HTTP\",uri=\"/phpauction/
search.php\",request=\"GET /phpauction/search.php?=&q=%3Cscript%3E%3C%2Fscript%3E&=Go%21 HTTP/
1.1\r\nHost: 172.30.0.30\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2 (.NET CLR 3.5.30729)\r\nAccept: text/html,application/
xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-us,en;q=0.5\r\nAccept-
Encoding: gzip,deflate\r\nAccept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\nKeep-Alive:
300\r\nConnection: keep-alive\r\nReferer: http://172.30.0.30/phpauction/search.php?
=&q=&=Go%21\r\nCookie:
TS2ea638=06f729a2c8f7d2c81fb76cdb434e073c543a36821980e75c4a8aef2b7b46979e7d2f9f63;
PHPAUCTION_SESSION=6r1f07tgsrlhum7q9n0mg0t8km7a93vi;
TS2ea638_75=a7f08552d2fc6e940f63c857254937f4:opos:Z9Zh11Py:1733471822;
TS2ea638_77=true_f4ec77a26f91b0a0;
TS8e2e48_75=46010be86e9787e6dd19db8aefea16eb:pprp:2N2l5F4r:1055951111;
TS8e2e48=9eb461f32f3a45e199c2929420da867ba2a59adceb6547144a8aefee;
TS8e2e48_77=true_47bd19fe37fe9407\r\n\r\n\",query_string=\"=&q=%3Cscript%3E%3C%2Fscript%3E&=Go%2
1\",x_forwarded_for_header_value=\"\",sig_ids=\"200000098,200000092\",sig_names=\"XSS script
tag (Parameter),XSS script tag end (Parameter)\",date_time=\"2009-18-08
11:16:28\",severity=\"Critical\",attack_type=\"Buffer Overflow,Information Leakage,Cross Site
Scripting (XSS),Forceful Browsing\",geo_location=\"N/
A\",src_port=\"4715\",dest_port=\"80\",dest_ip=\"172.30.0.30\"
```

F5 Networks BIG-IP ASM sample messages with CEF events when you use the syslog protocol

Sample 1: The following sample event shows an automated client access *wget* event.

```
<131>Sep 19 13:53:34 f5networks.bigipasm.test ASM:CEF:0|F5|ASM|11.3.0|200021069|Automated
client access \"wget\"|5|dvchost=f5networks.bigipasm.test dvc=192.168.73.34 cs1=topaz4-web4
cs1Label=policy_name cs2=/Common/topaz4-web4 cs2Label=http_class_name deviceCustomDate1=Sep
19 2012 13:49:25 deviceCustomDate1Label=policy_apply_date externalId=18205860747014045723
act=blocked cn1=0 cn1Label=src=10.4.1.101 spt=52975 dst=10.4.1.200 dpt=80
requestMethod=GET app=HTTP cs5=N/A cs5Label=x_forwarded_for_header_value rt=Sep 19
2012 13:53:33 deviceExternalId=0 cs4=Non-browser Client cs4Label=attack_type cs6=N/A
cs6Label=geo_location c6a1= c6a1Label=device_address c6a2= c6a2Label=source_address
c6a3= c6a3Label=destination_address c6a4=N/A c6a4Label=ip_address_intelligence msg=N/A
suid=86c4f8bf7349cac9 suser=N/A request=/ cs3Label=full_request cs3=GET / HTTP/1.0\r\nUser-
Agent: Wget/1.12 (linux-gnu)\r\nAccept: /\r\nHost: 10.4.1.200\r\nConnection: Keep-Alive\r\n\r\n
```

Table 471. Highlighted fields in the F5 Networks BIG-IP ASM event

QRadar field name	Highlighted payload field name
Event ID	The value in QRadar is **200021069**
Source IP	**src**
Source Port	**spt**
Destination IP	**dst**
Destination Port	**dpt**

Sample 2: The following sample event shows an HTTP protocol compliance failed event.

```
<131>May  6 01:28:20 f5networks.bigipasm.test ASM:CEF:0|F5|ASM|11.6.1|Host header
contains IP address|HTTP protocol compliance failed|5|dvchost=f5networks.bigipasm.test
dvc=10.11.229.202 cs1=/Common/asmpolicy_application1 cs1Label=policy_name cs2=/Common/
asmpolicy_application1 cs2Label=http_class_name deviceCustomDate1=May 06 2015 01:24:07
deviceCustomDate1Label=policy_apply_date externalId=9397100255637405701 act=blocked cn1=0
cn1Label=response_code src=10.101.90.17 spt=49160 dst=10.101.90.14 dpt=80 requestMethod=GET
app=HTTP cs5=N/A cs5Label=x_forwarded_for_header_value rt=May 06 2015 01:28:19
deviceExternalId=0 cs4=N/A cs4Label=attack_type cs6=N/A cs6Label=geo_location c6a1=
c6a1Label=device_address c6a2= c6a2Label=source_address c6a3= c6a3Label=destination_address
c6a4=N/A c6a4Label=ip_address_intelligence msg=N/A suid=cf868410a228bb45 suser=N/A request=/
cs3Label=full_request cs3=GET / HTTP/1.1\r\nAccept: application/x-ms-application, image/jpeg,
application/xaml+xml, imag
```

Table 472. Highlighted fields in the F5 Networks BIG-IP ASM event

QRadar field name	Highlighted payload field name
Event ID	The value in QRadar is **HTTP protocol compliance failed**

Table 472. Highlighted fields in the F5 Networks BIG-IP ASM event (continued)	
QRadar field name	**Highlighted payload field name**
Source IP	**src**
Source Port	**spt**
Destination IP	**dst**
Destination Port	**dpt**

F5 Networks BIG-IP ASM sample messages with JSON events when you use the syslog protocol

The following sample event shows BOT Defense Violation event.


```
{"@timestamp":"2023-09-22T14:12:53.488921Z","_visitor_id":"xxxx","action":"allow","app":"test","
app_type":"test-io-demo","as_number":"1234","as_org":"test b.v.","asn":"test b.v.
(1234)","authority":"demo.test.net","bot_defense":{"automation_type":"Token
Missing","insight":"MALICIOUS","recommendation":"Action_alert","status_code":"0"},"browser_type"
:"Opera","city":"city","cluster_name":"test-io","country":"NL","dcid":"xxxx-
yyyy","device_type":"Other","domain":"demo.test.net","dst":"","dst_instance":"","dst_ip":"10.3.0
.1","dst_port":"0","dst_site":"","hostname":"master-8","http_version":"HTTP/
1.1","is_new_dcid":false,"kubernetes":{"container_name":"test","host":"master","labels":
{"app":"test"},"namespace_name":"test-system","pod_id":"e358ed2d-xxxx-yyyy-
zzzz-2c5610ab14fd","pod_name":"test"},"latitude":"0.0000","longitude":"0.0000","messageid":"149c
116e-xxxx-yyyy-zzzz-0242ac120002","method":"GET","namespace":"demo-
shop","network":"10.3.0.2","original_headers":["host","method","scheme","user-
agent","cookie","x-forwarded-for","x-forwarded-proto","x-envoy-external-address","x-request-
id","test-request-id"],"path":"/","region":"NL-NH","req_headers":"{\"Cookie\":\"shop_session-
id=dcc83f26-xxxx-yyyy-zzzz-7486e1810932; xx=xx-yy; aa=xxxx; bb=xxxx; cc=xxxx|1|0|
xxxx\",\"Host\":\"demo.test.net\",\"Method\":\"GET\",\"Scheme\":\"https\",\"User-
Agent\":\"Mozilla/5.0 (Windows NT 10.0; xx) test/xx.36 (KHTML, like test) Chrome/10.3.0.4
Safari/123.36 OPR/10.3.0.5\",\"X-Envoy-External-Address\":\"10.3.0.6\",\"X-F5-Request-
Id\":\"73a366d8-xxxx-yyyy-zzzz-77b3289c73f2\",\"X-Forwarded-For\":\"10.3.0.8\",\"X-Forwarded-
Proto\":\"https\",\"X-Request-Id\":\"73a366d8-xxxx-yyyy-
zzzz-77b3289c73f2\"}","req_headers_size":903,"req_id":"73a366d8-xxxx-yyyy-
zzzz-77b3289c73f2","req_params":"","req_path":"/","req_size":"903","rsp_code":"0","rsp_code_clas
s":"UNKNOWN","rsp_size":"11406","sec_event_name":"BOT Defense
Violation","sec_event_type":"bot_defense_sec_event","severity":"info","site":"ams9-
ams","sni":"demo.test.net","source":"f5xc","src":"N:public","src_instance":"NL","src_ip":"10.3.0
.9","src_port":"44366","src_site":"a-ams","stream":"svcfw","tag":"test","tenant":"f5-
test","time":"2023-09-22T14:12:53.488Z","tls_fingerprint":"aa","user":"Cookie-shop_session-id-
dcc83f26-xxxx-yyyy-zzzz-7486e1810932","user_agent":"Mozilla/5.0 (Windows NT 10.0; WOW64) test/
537.36 (KHTML, like test) Chrome/90.0.4430.212 Safari/123.36 OPR/10.3.0.11","vh_name":"ves-io-
test","vhost_id":"78c99480-xxxx-yyyy-zzzz-f4e8efe7eea6","x_forwarded_for":"10.3.0.12"}
```


Table 473. Highlighted fields in the F5 Networks BIG-IP ASM event	
QRadar field name	**Highlighted payload field name**
Event ID	The value in QRadar is **BOT Defense Violation**
Source IP	**src_ip**
Source Port	**src_port**
Destination IP	**dst_ip**
Destination Port	**dst_port**

F5 Networks BIG-IP LTM

The F5 Networks BIG-IP Local Traffic Manager (LTM) DSM for IBM QRadar collects networks security events from a BIG-IP device by using syslog.

Before events can be received in QRadar, you must configure a log source for QRadar, and then configure your BIG-IP LTM device to forward syslog events. Create the log source before events are forwarded

as QRadar does not automatically discover or create log sources for syslog events from F5 BIG-IP LTM appliances.

F5 Networks BIG-IP LTM DSM specifications

When you configure F5 Networks BIG-IP LTM, understanding the specifications for the F5 Networks BIG-IP LTM DSM can help ensure a successful integration. For example, knowing what the supported version of F5 Networks BIG-IP LTM is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the F5 Networks BIG-IP LTM DSM.

Table 474. F5 Networks BIG-IP LTM DSM specifications

Specification	Value
Manufacturer	F5 Networks
DSM name	F5 Networks BIG-IP LTM
RPM file name	DSM-*F5NetworksBigIP-QRadar_version-build_number*.noarch.rpm
Supported version	9.4.2 to 14.x
Protocol	Syslog
Event format	Syslog, CSV
Recorded event types	All events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	F5 Networks product resources (https://www.f5.com/services/resources

Syslog log source parameters for F5 Networks BIG-IP LTM

Add a F5 Networks BIG-IP LTM log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from F5 Networks BIG-IP LTM:

Table 475. Syslog log source parameters for the F5 Networks BIG-IP LTM DSM

Parameter	Value
Log Source type	**F5 Networks BIG-IP LTM**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks BIG-IP LTM devices.

Related tasks

Adding a log source

Configuring syslog forwarding in BIG-IP LTM

You can configure your BIG-IP LTM device to forward syslog events.

You can configure syslog for the following BIG-IP LTM software version:

- “Configuring Remote Syslog for F5 BIG-IP LTM V11.x to V14.x ” on page 790
- “Configuring Remote Syslog for F5 BIG-IP LTM V10.x ” on page 790
- “Configuring Remote Syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8” on page 791

Configuring Remote Syslog for F5 BIG-IP LTM V11.x to V14.x

You can configure syslog for F5 BIG-IP LTM 11.x to V14.x.

About this task

To configure syslog for F5 BIG-IP LTM V11.x to V14.x take the following steps:

Procedure

1. Log in to the command-line of your F5 BIG-IP device.
2. To log in to the Traffic Management Shell (tmsh), type the following command:

   ```
   tmsh
   ```
3. To add a syslog server, type the following command:

   ```
   modify /sys syslog remote-servers add {<Name> {host <IP address> remote-port
   514}}
   ```

   Where:

   - *<Name>* is a name that you assign to identify the syslog server on your BIG-IP LTM appliance.
   - *<IP address>* is the IP address of IBM QRadar.

   For example,

   ```
   modify /sys syslog remote-servers add {BIGIPsyslog {host 192.0.2.1 remote-
   port 514}}
   ```
4. Save the configuration changes:

   ```
   save /sys config
   ```

   Events that are forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the **Log Activity** tab in QRadar.

Configuring Remote Syslog for F5 BIG-IP LTM V10.x

You can configure syslog for F5 BIG-IP LTM V10.x.

About this task

To configure syslog for F5 BIG-IP LTM V10.x take the following steps:

Procedure

1. Log in to the command line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:

   ```
   bigpipe syslog remote server {<Name> {host <IP_address>}}
   ```

   Where:

   - *<Name>* is the name of the F5 BIG-IP LTM syslog source.

- <*IP_address*> is the IP address of IBM QRadar.

  For example:

  ```
  bigpipe syslog remote server {BIGIPsyslog {host 192.0.2.1}}
  ```

3. Save the configuration changes:

   ```
   bigpipe save
   ```

   Note: F5 Networks modified the syslog output format in BIG-IP V10.x to include the use of `local/` before the host name in the syslog header. The syslog header format that contains `local/` is not supported in QRadar, but a workaround is available to correct the syslog header. For more information, see http://www.ibm.com/support.

   Events that are forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the **Log Activity** tab in QRadar.

Configuring Remote Syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8

You can configure syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8.

About this task

To configure syslog for F5 BIG-IP LTM V9.4.2 to V9.4.8 take the following steps:

Procedure

1. Log in to the command-line of your F5 BIG-IP device.
2. Type the following command to add a single remote syslog server:

   ```
   bigpipe syslog remote server <IP address>
   ```

   Where: <*IP address*> is the IP address of IBM QRadar.

   For example:

   ```
   bigpipe syslog remote server 192.0.2.1
   ```

3. Type the following to save the configuration changes:

   ```
   bigpipe save
   ```

   The configuration is complete. Events that are forwarded from your F5 Networks BIG-IP LTM appliance are displayed on the **Log Activity** tab in QRadar.

F5 Networks BIG-IP LTM sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

F5 Networks BIG-IP LTM sample event messages when you use the Syslog protocol

Sample 1: The following sample event message shows a Pool member's monitor status.

```
<133>Nov  5 14:01:50 f5networks.bigip.test notice mcpd[5281]: 01070638:5: Pool member
2001:20:5004:1606::89:8790 monitor status down.
```


```
<133>Nov  5 14:01:50 f5networks.bigip.test notice mcpd[5281]: 01070638:5: Pool member
2001:20:5004:1606::89:8790 monitor status down.
```


Table 476. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**01070638** is extracted from the event.

Table 476. Highlighted fields (continued)	
QRadar field name	**Highlighted payload field name**
Destination IP v6	**2001:20:5004:1606::89** is extracted from the event.
Destination Port	**8790** is extracted from the event.
Device Time	**Nov 5 14:01:50** is extracted from the event.

Sample 2: The following sample event message shows that IP-INTELLIGENCE accepted a packet.

```
<134>Apr 23 08:16:55 f5networks.bigip.test info
tmm[1286]: 23003142 "","10.240.252.242","hostname.test","","","","Virtual
Server","/Common/TEST-TESTA.AA.local_HTTPS_VIP","/Common/IP-Intelligence-
ALL","192.168.146.233","10.243.32.100","47707","443","/Common/
VLAN-332","TCP","0","scanners,windows_exploits,spam_sources","Accept","custom_category",
"","","","","","","","","","0000000000000000"
```

```
<134>Apr 23 08:16:55 f5networks.bigip.test info tmm[1286]: 23003142
"","10.240.252.242","hostname.test","","","","Virtual Server","/Common/TEST-
TESTA.AA.local_HTTPS_VIP","/Common/IP-Intelligence-
ALL","192.168.146.233","10.243.32.100","47707","443","/Common/
VLAN-332","TCP","0","scanners,windows_exploits,spam_sources","Accept","custom_category","","",""
,"","","","","","","0000000000000000"
```

Table 477. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**Accept** is extracted from the event.
Source IP	**192.168.146.233** is extracted from the event.
Source Port	**47707** is extracted from the event.
Destination IP	**10.243.32.100** is extracted from the event.
Destination Port	**443** is extracted from the event.
Protocol	**TCP** is extracted from the event.
Device Time	**Apr 23 08:16:55** is extracted from the event.

F5 Networks FirePass

The F5 Networks FirePass DSM for IBM QRadar collects system events from an F5 FirePass SSL VPN device using syslog.

By default, remote logging is disabled and must be enabled in the F5 Networks FirePass device. Before receiving events in QRadar, you must configure your F5 Networks FirePass device to forward system events to QRadar as a remote syslog server.

Configuring syslog forwarding for F5 FirePass

To forward syslog events from an F5 Networks BIG-IP FirePass SSL VPN appliance to IBM QRadar, you must enable and configure a remote log server.

About this task

The remote log server can forward events directly to your QRadar Console or any Event Collector in your deployment.

Procedure

1. Log in to the F5 Networks FirePass Admin Console.

2. On the navigation pane, select **Device Management** > **Maintenance** > **Logs**.
3. From the **System Logs** menu, select the **Enable Remote Log Server** check box.
4. From the **System Logs** menu, clear the **Enable Extended System Logs** check box.
5. In the **Remote host** parameter, type the IP address or host name of your QRadar.
6. From the **Log Level** list, select **Information**.

   The **Log Level** parameter monitors application level system messages.
7. From the **Kernel Log Level** list, select **Information**.

   The **Kernel Log Level** parameter monitors Linux kernel system messages.
8. Click **Apply System Log Changes**.

   The changes are applied and the configuration is complete. The log source is added to QRadar as F5 Networks FirePass events are automatically discovered. Events that are forwarded to QRadar by F5 Networks BIG-IP ASM are displayed on the **Log Activity** tab in QRadar.

Syslog log source parameters for F5 Networks FirePass

If QRadar does not automatically detect the log source, add a F5 Networks FirePass log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from F5 Networks FirePass:

Table 478. Syslog log source parameters for the F5 Networks FirePass DSM

Parameter	Value
Log Source type	**F5 Networks FirePass**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your F5 Networks FirePass devices.

Related tasks

Adding a log source

Chapter 61. Fair Warning

The Fair Warning DSM for IBM QRadar retrieves event files from a remote source by using the log file protocol.

QRadar records event categories from the Fair Warning log files about user activity that is related to patient privacy and security threats to medical records. Before you can retrieve log files from Fair Warning, you must verify that your device is configured to generate an event log. Instructions for generating the event log can be found in your *Fair Warning documentation*.

When you configure the log file protocol, make sure that the host name or IP address that is configured in the Fair Warning system is the same as configured in the **Remote Host** parameter in the log file protocol configuration.

Log File log source parameters for Fair Warning

If QRadar does not automatically detect the log source, add a Fair Warning log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from Fair Warning:

Table 479. Log File log source parameters for the Fair Warning DSM

Parameter	Value
Log Source type	**Fair Warning**
Protocol Configuration	**Log File**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Fair Warning devices.
FTP File Pattern	Type a regular expression that matches the log files that are generated by the Fair Warning system.
Remote Directory	Type the path to the directory that contains logs from your Fair Warning device.
Event Generator	**Fair Warning**

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related tasks

Adding a log source

Fair Warning sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Fair Warning sample message when you use the Log File protocol

Sample 1: The following sample event message shows that an employee is snooping in the Fair Warning DSM.

```
FairWarning::Alert Time Stamp=2010-08-06 19:25:29.0     Alert ID=71     Alert Name=Epic:
Employee Snooping      Event Source=Epic HS    Category=HIPAA Best Practice    Severity=high
Timestamp=2010-08-05 00:00:01.0 Event ID=1155646552611  User ID=111     User Name=Test User
User First Name=Test    User Last Name=User     Patient ID=1111 Patient Name=Admin root Patient
First Name=Admin        Patient Last Name=root  Event Type=PATIENT CLINICAL INFO        Event
Description=MR_REPORTS    Workstation ID=11111.11 Workstation IP=10.16.22.21     FileName=/path/
test.txt
```

```
FairWarning::Alert Time Stamp=2010-08-06 19:25:29.0     Alert ID=71     Alert Name=Epic:
Employee Snooping      Event Source=Epic HS    Category=HIPAA Best Practice    Severity=high
Timestamp=2010-08-05 00:00:01.0 Event ID=1155646552611  User ID=111     User Name=Test User
User First Name=Test    User Last Name=User     Patient ID=1111 Patient Name=Admin root Patient
First Name=Admin        Patient Last Name=root  Event Type=PATIENT CLINICAL INFO        Event
Description=MR_REPORTS    Workstation ID=11111.11 Workstation IP=10.16.22.21      FileName=/
path/test.txt
```

Table 480. Highlighted values in the Fair Warning event

QRadar field name	Highlighted values in the event payload
Event ID	**Epic: Employee Snooping**
Source IP	**10.16.22.21**
Username	**Test User**
Device Time	**Aug 6, 2010, 7:25:29 PM** (extracted from date and time fields)

Sample 2: The following sample event message shows excess failed logins.

```
FairWarning::Alert Time Stamp=2010-08-08 19:35:45.0     Alert ID=86     Alert Name=Epic Failed
Logins- Exceeding Thresholds     Event Source=Epic Failed Logins Category=Medical Identity
Theft Severity=high   Timestamp=2010-08-07 08:26:00.0 Event ID=1155644965984  User ID=2222
User Name=TestTest UserUser     User First Name=TestTest        User Last Name=UserUser
Department=AA   Application=111111-2222222.2    Event Description=A setup or operations error
occured. Please consult a system administrator    Details:   Epic LDAP User (extended) login
failed  49-ELDAP_FAIL_SBIND:failed to sbind (bind+search) using given credentials  49:Invalid
credentials    Workstation IP=10.251.243.41    FileName=/path/test.txt
```

```
FairWarning::Alert Time Stamp=2010-08-08 19:35:45.0     Alert ID=86     Alert Name=Epic Failed
Logins- Exceeding Thresholds     Event Source=Epic Failed Logins Category=Medical Identity
Theft Severity=high   Timestamp=2010-08-07 08:26:00.0 Event ID=1155644965984  User ID=2222
User Name=TestTest UserUser     User First Name=TestTest        User Last Name=UserUser
Department=AA   Application=111111-2222222.2    Event Description=A setup or operations error
occured. Please consult a system administrator    Details:   Epic LDAP User (extended) login
failed  49-ELDAP_FAIL_SBIND:failed to sbind (bind+search) using given credentials  49:Invalid
credentials    Workstation IP=10.251.243.41    FileName=/path/test.txt
```

Table 481. Highlighted values in the Fair Warning sample event

QRadar field name	Highlighted values in the event payload
Event ID	**Epic Failed Logins- Exceeding Thresholds**
Source IP	**10.251.243.41**
Username	**TestTest UserUser**
Device Time	**Aug 8, 2010, 7:35:45 PM** (extracted from date and time fields)

Chapter 62. Fasoo Enterprise DRM

The IBM QRadar DSM for Fasoo Enterprise DRM (Digital Rights Management) collects logs from a Fasoo Enterprise DRM device.

The following table describes the specifications for the Fasoo Enterprise DRM DSM:

Table 482. Fasoo Enterprise DRM DSM specifications

Specification	**Value**
Manufacturer	Fasoo
DSM name	Fasoo Enterprise DRM
RPM file name	DSM-FasooFED-*QRadar_version-build_number*.noarch.rpm
Supported versions	5.0
Protocol	JDBC
Event format	name-value pair (NVP)
Recorded event types	Usage events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Fasoo website (http://en.fasoo.com/Fasoo-Enterprise-DRM)

To integrate Fasoo Enterprise DRM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - JDBC Protocol RPM
   - DSMCommon RPM
   - FasooFED DSM RPM
2. Configure a log source to connect to the Fasoo Enterprise DRM database and retrieve event.
3. Add a Fasoo Enterprise DRM log source on the QRadar Console. The following table describes the parameters that require specific values to collect event from Fasoo Enterprise DRM:

Table 483. Fasoo Enterprise DRM JDBC log source parameters

Parameter	**Value**
Log Source type	Fasoo Enterprise DRM
Protocol Configuration	JDBC

Table 483. Fasoo Enterprise DRM JDBC log source parameters (continued)

Parameter	Value
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	From the list, select the type of the Fasoo Enterprise DRM database.
Database Name	The name of the Fasoo Enterprise DRM database.
IP or Hostname	The IP address or host name of the Fasoo Enterprise DRM database server.
Port	The port number that is used by the database server.
Username	The user name that is required to connect to the database.
Password	The password that is required to connect to the database. The password can be up to 255 characters in length.
Confirm Password	The confirmation password must be identical to the password that you typed for the **Password** parameter.
Authentication Domain	If you did not select **Use Microsoft JDBC**, **Authentication Domain** is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance	The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank in the log source configuration.
Predefined Query (Optional)	Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the **none** option.
Table Name	view_fut_log The name of the view that includes the event records.

Table 483. Fasoo Enterprise DRM JDBC log source parameters (continued)	
Parameter	**Value**
Select List	Type an asterisk (*) to select all fields from the table or view. The list of fields to include when the table is polled for events.
Compare Field	log_date The **Compare Field** is used to identify new events that are added between queries to the table.
Start Date and Time (Optional)	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm, with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Use Prepared Statements	Select the check box if you want to use prepared statements. Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Polling Interval	The amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values that are entered without an H or M poll in seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 20,000 EPS.
Use Named Pipe Communication	If you did not select **Use Microsoft JDBC**, **Use Named Pipe Communication** is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.
Database Cluster Name	If you selected **Use Named Pipe Communication**, the **Database** parameter displays. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.

Table 483. Fasoo Enterprise DRM JDBC log source parameters (continued)	
Parameter	**Value**
Use NTLMv2	If you did not select **Use Microsoft JDBC**, **Use NTLMv2** is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use Microsoft JDBC	If you want to use the Microsoft JDBC driver, you must enable **Use Microsoft JDBC**.
Use SSL	Select this option if your connection supports SSL.
Microsoft SQL Server Hostname	If you selected **Use Microsoft JDBC** and **Use SSL**, the **Microsoft SQL Server Hostname** parameter is displayed. You must type the host name for the Microsoft SQL server.

For more information about configuring JDBC parameters, see c_logsource_JDBCprotocol.dita

4. Verify that QRadar is configured correctly.

   The following table shows a sample normalized event message from Fasoo Enterprise DRM:

Table 484. Fasoo Enterprise DRM sample message

Event name	Low level category	Sample log message
Edit - successful	Update Activity Succeeded	log_id: "xxxxxxxxxxxxxxxxxxxxx" log_date: "2016-03-21 14:17:36.000" log_type: "1" product: "1" purpose: "16" usage_result: "1" license_status: "0" ip: "<Numeric>" user_code: "usercode" user_name: "username" user_dept_code: "xxxxxxxxxxxxxxxxxxx" user_dept_name: "userdeptname" position_code: "P001" position_name: "Employee" content_code: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" current_content_name: "New Microsoft PowerPoint Presentation.pptx" content_name: "New Microsoft PowerPoint Presentation.pptx" sec_level_code: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" sec_level_name: "Basic" system_code: "NULL" system_name: "NULL" owner_code: "ownercode" owner_name: "ownername" owner_dept_code: "xxxxxxxxxxxxxxxxxxx" owner_dept_name: "ownerdeptname" content_create-date: "2016-03-21 03:41:28.000" entry_date: "2016-03-21 13:18:26.670" log_id: "xxxxxxxxxxxxxxxxxxxxx" log_date: "2016-03-21 14:17:36.000" log_type: "1" product: "1" purpose: "16" usage_result: "1" license_status: "0" ip: "<Numeric>" user_code: "usercode" user_name: "username" user_dept_code: "xxxxxxxxxxxxxxxxxxx" user_dept_name: "userdeptname" position_code: "P001" position_name: "Employee" content_code: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" current_content_name: "New Microsoft PowerPoint Presentation.pptx" content_name: "New Microsoft PowerPoint Presentation.pptx" sec_level_code: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" sec_level_name: "Basic" system_code: "NULL" system_name: "NULL" owner_code: "ownercode" owner_name: "ownername" owner_dept_code: "xxxxxxxxxxxxxxxxxxx" owner_dept_name: "ownerdeptname" content_create-date: "2016-03-21 03:41:28.000" entry_date: "2016-03-21 13:18:26.670"

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Fasoo Enterprise DRM to communicate with QRadar

For IBM QRadar to collect log event data, you must create a database view.

Before you begin

The script in this procedure is only intended for MS SQL Servers. For other database types, modifications to the script will be required for the target database type.

Procedure

1. Log in to SQL Server Management Studio.
2. Create a custom view in your Fasoo database.

```
USE fed5;
GO
CREATE VIEW view_fut_log
AS
SELECT
dbo.fut_log.log_id,
dbo.fut_log.log_date,
dbo.fut_log.log_type,
dbo.fut_log.product,
dbo.fut_log.purpose,
dbo.fut_log.usage_result,
dbo.fut_log.license_status,
dbo.fut_log.ip,
dbo.fut_user.user_code,
dbo.fut_user.user_name,
dbo.fut_user.user_dept_code,
dbo.fut_user.user_dept_name,
dbo.fut_log.position_code,
dbo.fut_log.position_name,
dbo.fut_content.content_code,
dbo.fut_content.current_content_name,
dbo.fut_content.content_name,
dbo.fut_content.sec_level_code,
dbo.fut_content.sec_level_name,
dbo.fut_content.system_code,
dbo.fut_content.system_name,
dbo.fut_log.owner_code,
dbo.fut_log.owner_name,
dbo.fut_log.owner_dept_code,
dbo.fut_log.owner_dept_name,
dbo.fut_content.content_create_date,
dbo.fut_log.entry_date
FROM dbo.fut_log
INNER JOIN dbo.fut_user
ON dbo.fut_log.user_id =
dbo.fut_user.user_id
INNER JOIN dbo.fut_content
ON dbo.fut_log.content_id =
dbo.fut_content.content_id
GO
```

Chapter 63. Fidelis XPS

The Fidelis XPS DSM for IBM QRadar accepts events that are forwarded in Log Event Extended Format (LEEF) from Fidelis XPS appliances by using syslog.

QRadar can collect all relevant alerts that are triggered by policy and rule violations that are configured on your Fidelis XPS appliance.

Event type format

Fidelis XPS must be configured to generate events in Log Event Extended Format (LEEF) and forward these events by using syslog. The LEEF format consists of a pipe (|) delimited syslog header, and tab separated fields that are positioned in the event payload.

If the syslog events forwarded from your Fidelis XPS are not formatted in LEEF format, you must examine your device configuration or software version to ensure that your appliance supports LEEF. Properly formatted LEEF event messages are automatically discovered and added as a log source to QRadar.

Configuring Fidelis XPS

You can configure syslog forwarding of alerts from your Fidelis XPS appliance.

Procedure

1. Log in to CommandPost to manage your Fidelis XPS appliance.
2. From the navigation menu, select **System** > **Export**.

   A list of available exports is displayed. The list is empty the first time you use the export function.
3. Select one of the following options:
   - Click **New** to create a new export for your Fidelis XPS appliance.
   - Click **Edit** next to an export name to edit an existing export on your Fidelis XPS appliance.

   The **Export Editor** is displayed.
4. From the **Export Method** list, select **Syslog LEEF**.
5. In the **Destination** field, type the IP address or host name for IBM QRadar.

   For example, `192.0.2.1:::514`

   The **Destination** field does not support non-ASCII characters.
6. From **Export Alerts**, select one of the following options:
   - **All alerts** - Select this option to export all alerts to QRadar. This option is resource-intensive and it can take time to export all alerts.
   - **Alerts by Criteria** - Select this option to export specific alerts to QRadar. This option displays a new field where you can define your alert criteria.
7. From **Export Malware Events**, select **None**.
8. From **Export Frequency**, select **Every Alert / Malware**.
9. In the **Save As** field**,** type a name for your export.
10. Click **Save**.
11. Optional: To verify that events are forwarded to QRadar, you can click **Run Now**.

    Run Now is intended as a test tool to verify that alerts selected by criteria are exported from your Fidelis appliance. This option is not available if you selected to export all events in “Configuring Fidelis XPS” on page 803.

The configuration is complete. The log source is added to QRadar as Fidelis XPS syslog events are automatically discovered. Events that are forwarded to QRadar by Fidelis XPS are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Fidelis XPS

If QRadar does not automatically detect the log source, add a Fidelis XPS log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Fidelis XPS:

Table 485. Syslog log source parameters for the Fidelis XPS DSM

Parameter	Value
Log Source type	**Fidelis XPS**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Fidelis XPS devices.

Related tasks

Adding a log source

Fidelis XPS sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Fidelis XPS sample message when you use the Syslog protocol

The following sample event message is generated when a packet contains excess data.

```
<13>Dec 23 11:52:05 fidelis.xps.test LEEF:1.0|Fidelis Cybersecurity|direct2500|8.1.3|Packet has
excess data| act=alert cs2=https://brtdc-dlpcp1/j/alert.html?7eaa5696-a995-11e5-b197-6cae8b611c2a
cs2Label=linkback cs5=0 cs5Label=compression dst=10.89.233.135 dstPort=60228 fname=<n/a>
cs4=<n/a> cs4Label=from cs6=default cs6Label=group cs1=DNS Analyzer Policy cs1Label=policy
proto=DNS dvc=10.89.213.11 dvchost=brtdc-dlps1.phillips66.net sev=4 src=10.64.55.4 srcPort=53
msg=Packet has excess data devTime=1450889524000 duser=<n/a> usrName=<n/a> target=<n/a>
```

```
<13>Dec 23 11:52:05 fidelis.xps.test LEEF:1.0|Fidelis Cybersecurity|direct2500|8.1.3|
Packet has excess data| act=alert cs2=https://brtdc-dlpcp1/j/alert.html?7eaa5696-a995-11e5-
b197-6cae8b611c2a cs2Label=linkback cs5=0 cs5Label=compression dst=10.89.233.135 dstPort=60228
fname=<n/a> cs4=<n/a> cs4Label=from cs6=default cs6Label=group cs1=DNS Analyzer
Policy cs1Label=policy proto=DNS dvc=10.89.213.11 dvchost=brtdc-dlps1.phillips66.net sev=4
src=10.64.55.4 srcPort=53 msg=Packet has excess data devTime=1450889524000 duser=<n/a>
usrName=<n/a> target=<n/a>
```

Table 486. Highlighted values in the Fidelis XPS sample event message

QRadar field name	Highlighted values in the event payload
Event ID	**Packet has excess data**
Source IP	**10.64.55.4**
Source Port	**53**
Destination IP	**10.89.233.135**

Table 486. Highlighted values in the Fidelis XPS sample event message (continued)	
QRadar field name	**Highlighted values in the event payload**
Destination Port	**60228**
Username	**<n/a>**

Chapter 64. FireEye

The IBM QRadar DSM for FireEye accepts syslog events in Log Event Extended Format (LEEF) and Common Event Format (CEF).

This DSM applies to FireEye CMS, MPS, EX, AX, NX, FX, and HX appliances. QRadar records all relevant notification alerts that are sent by FireEye appliances.

The following table identifies the specifications for the FireEye DSM.

Table 487. FireEye DSM specifications

Specification	**Value**
Manufacturer	FireEye
DSM name	FireEye MPS
Supported versions	CMS, MPS, EX, AX, NX, FX, and HX
RPM file name	DSM-FireEyeMPS-*QRadar_version-Build_number*.noarch.rpm
Protocol	**Syslog** and **TLS Syslog**
Event Format	Common Event Format (CEF). CEF:0 is supported.
QRadar recorded event types	All relevant events
Auto discovered?	Yes
Includes identity?	No
More information	FireEye website (www.fireeye.com)

To integrate FireEye with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the DSM Common and FireEye MPS RPM from the IBM Support Website onto your QRadar Console.
2. Download and install the latest TLS Syslog Protocol RPM on QRadar.
3. For each instance of FireEye in your deployment, configure the FireEye system to forward events to QRadar.
4. For each instance of FireEye, create an FireEye log source on the QRadar Console. The following tables explain how to configure a log source in Syslog and TLS Syslog for FireEye.

Table 488. Configuring the Syslog log source protocols for FireEye

Parameter	**Description**
Log Source Type	**FireEye**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your device.

Table 489. Configuring the TLS Syslog log source protocols for FireEye

Parameter	**Description**
Log Source Type	**FireEye**

Table 489. Configuring the TLS Syslog log source protocols for FireEye (continued)	
Parameter	**Description**
Protocol Configuration	**TLS Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your device.
TLS Listen Port	The default TLS listen port is 6514.
Authentication Mode	The mode by which your TLS connection is authenticated. If you select the TLS and Client Authentication option, you must configure the certificate parameters.
Certificate Type	The type of certificate to use for authentication. If you select the **Provide Certificate** option, you must configure the file paths for the server certificate and the private key.
Provided Server Certificate Path	The absolute path to the server certificate.
Provided Private Key Path	The absolute path to the private key. **Note:** The corresponding private key must be a DER-encoded PKCS8 key. The configuration fails with any other key format.
Maximum Connections	The Maximum Connections parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. The connection limit across all TLS syslog log source configurations is 1000 connections for each Event Collector. The default for each device connection is 50. **Note:** Automatically discovered log sources that share a listener with another log source, such as if you use the same port on the same event collector, count only one time towards the limit.

Look at "Adding a log source" on page 5 for more common parameters that occur in Syslog and "TLS Syslog protocol configuration options" on page 227 for more TLS Syslog protocol-specific parameters and their configurations.

Related tasks

"Configuring your FireEye HX system for communication with QRadar" on page 809
To enable FireEye HX to communicate with IBM QRadar, configure your FireEye HX appliance to forward syslog events.

"Configuring your FireEye system for communication with QRadar" on page 809
To enable FireEye to communicate with IBM QRadar, configure your FireEye appliance to forward syslog events.

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring your FireEye system for communication with QRadar

To enable FireEye to communicate with IBM QRadar, configure your FireEye appliance to forward syslog events.

Procedure

1. Log in to the FireEye appliance by using the CLI.
2. To activate configuration mode, type the following commands:

   ```
   enable
   configure terminal
   ```
3. To enable rsyslog notifications, type the following command:

   ```
   fenotify rsyslog enable
   ```
4. To add QRadar as an rsyslog notification consumer, type the following command:

   ```
   fenotify rsyslog trap-sink QRadar
   ```
5. To specify the IP address for the QRadar system that you want to receive rsyslog trap-sink notifications, type the following command:

   ```
   fenotify rsyslog trap-sink QRadar address <QRadar_IP_address>
   ```
6. To define the rsyslog event format, type the following command:

   ```
   fenotify rsyslog trap-sink QRadar prefer message format leef
   ```
7. To save the configuration changes to the FireEye appliance, type the following command:

   ```
   write memory
   ```

Related tasks

“Configuring your FireEye HX system for communication with QRadar” on page 809
To enable FireEye HX to communicate with IBM QRadar, configure your FireEye HX appliance to forward syslog events.

Configuring your FireEye HX system for communication with QRadar

To enable FireEye HX to communicate with IBM QRadar, configure your FireEye HX appliance to forward syslog events.

Procedure

1. Log in to the FireEye HX appliance by using the CLI.
2. To activate configuration mode, type the following commands:

   ```
   enable
   configure terminal
   ```
3. To add a remote syslog server destination, type the following commands:

   ```
   logging <remote_IP_address> trap none
   logging <remote_IP_address> trap override class cef priority info
   ```
4. To save the configuration changes to the FireEye HX appliance, type the following command:

   ```
   write mem
   ```

Configuring a FireEye log source in QRadar

IBM QRadar automatically creates a log source after your QRadar Console receives FireEye events. If QRadar does not automatically discover FireEye events, you can manually add a log source for each instance from which you want to collect event logs.

About this task

If you are using QRadar 7.3.1 and later, you can add a log source by using the QRadar Log Source Management app.

In QRadar 7.5.0 Update Package 4 and later, when you click the **Log Sources** icon, the QRadar Log Source Management app opens.

Procedure

1. Log in to QRadar
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **FireEye**.
7. Using the **Protocol Configuration** list, select **Syslog**.
8. In the **Log Source Identifier** field, type the IP address or host name of the FireEye appliance.
9. Configure the remaining parameters.
10. Click **Save**.
11. On the **Admin** tab, click **Deploy Changes**.

FireEye sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

FireEye sample message when you use the Syslog or TLS syslog protocol

The following sample event message shows that an Indicator of Compromise (IOC) was detected.

```
<149>Jul 23 18:54:24 fireeye.mps.test cef[5159]: CEF:0|fireeye|HX|4.8.0|IOC Hit Found|IOC
Hit Found|10|rt=Jul 23 2019 16:54:24 UTC dvchost=fireeye.mps.test categoryDeviceGroup=/IDS
categoryDeviceType=Forensic Investigation categoryObject=/Host cs1Label=Host Agent Cert Hash
cs1=fwvqcmXUHVcbm4AFK01cim dst=192.168.1.172 dmac=00-00-5e-00-53-00 dhost=test-host1 dntdom=test
deviceCustomDate1Label=Agent Last Audit deviceCustomDate1=Jul 23 2019 16:54:22 UTC
cs2Label=FireEye Agent Version cs2=29.7.0 cs5Label=Target GMT Offset cs5=+PT2H cs6Label=Target
OS cs6=Windows 10 Pro 17134 externalId=17688554 start=Jul 23 2019 16:53:18 UTC categoryOutcome=/
Success categorySignificance=/Compromise categoryBehavior=/Found cs7Label=Resolution cs7=ALERT
cs8Label=Alert Types cs8=exc act=Detection IOC Hit msg=Host test-host1 IOC compromise alert
categoryTupleDescription=A Detection IOC found a compromise indication. cs4Label=IOC Name
cs4=SVCHOST SUSPICIOUS PARENT PROCESS
```


```
<149>Jul 23 18:54:24 fireeye.mps.test cef[5159]: CEF:0|fireeye|HX|4.8.0|IOC Hit Found|IOC
Hit Found|10|rt=Jul 23 2019 16:54:24 UTC dvchost=fireeye.mps.test categoryDeviceGroup=/IDS
categoryDeviceType=Forensic Investigation categoryObject=/Host cs1Label=Host Agent Cert
Hash cs1=fwvqcmXUHVcbm4AFK01cim dst=192.168.1.172 dmac=00-00-5e-00-53-00 dhost=test-host1
dntdom=test deviceCustomDate1Label=Agent Last Audit deviceCustomDate1=Jul 23 2019 16:54:22 UTC
cs2Label=FireEye Agent Version cs2=29.7.0 cs5Label=Target GMT Offset cs5=+PT2H cs6Label=Target
OS cs6=Windows 10 Pro 17134 externalId=17688554 start=Jul 23 2019 16:53:18 UTC categoryOutcome=/
Success categorySignificance=/Compromise categoryBehavior=/Found cs7Label=Resolution cs7=ALERT
cs8Label=Alert Types cs8=exc act=Detection IOC Hit msg=Host test-host1 IOC compromise alert
categoryTupleDescription=A Detection IOC found a compromise indication. cs4Label=IOC Name
cs4=SVCHOST SUSPICIOUS PARENT PROCESS
```

Table 490. Highlighted values in the FireEye event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	**IOC Hit Found**
Event Category	FireEyeMPS (extracted from the event content)
Destination IP	**192.168.1.172**
Destination MAC	**00-00-5e-00-53-00**
Log Source Time	**Jul 23 2019 16:54:24 UTC**

Chapter 65. Forcepoint

IBM QRadar supports a range of Forcepoint DSMs.

FORCEPOINT is formerly known as Websense.

Related concepts

WebsenseQRadar supports a range of Websense DSMs.

Forcepoint Stonesoft Management Center

The IBM QRadar DSM for Forcepoint Stonesoft Management Center collects events from a StoneGate device by using syslog.

The following table describes the specifications for the Stonesoft Management Center DSM:

Table 491. Stonesoft Management Center DSM specifications

Specification	Value
Manufacturer	FORCEPOINT
DSM name	Stonesoft Management Center
RPM file name	`DSM-StonesoftManagementCenter-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	5.4 to 6.1
Protocol	Syslog
Event format	LEEF
Recorded event types	Management Center, IPS, Firewall, and VPN events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	FORCEPOINT website (https://www.forcepoint.com)

To integrate FORCEPOINT Stonesoft Management Center with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Stonesoft Management Center DSM RPM
2. Configure your StoneGate device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Stonesoft Management Center log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from Stonesoft Management Center:

Table 492. Stonesoft Management Center log source parameters

Parameter	Value
Log Source type	Stonesoft Management Center
Protocol Configuration	Syslog

Table 492. Stonesoft Management Center log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	Type a unique name for the log source.

4. Verify that QRadar is configured correctly.

   The following table shows a sample normalized event message from Stonesoft Management Center:

Table 493. Stonesoft Management Center sample message		
Event name	**Low level category**	**Sample log message**
Generic_UDP-Rugged-Director-Denial-Of-Service	Misc DoS	`LEEF:1.0|FORCEPOINT|IPS|5.8.5| Generic_UDP-Rugged-Director-Denial-Of-Service|devTimeFormat=MMM dd yyyy HH:mm:ss srcMAC=00:00:00:00:00:00 sev=2 dstMAC=00:00:00:00:00:00 devTime=Feb 23 201710:13:58 proto=17 dstPort=00000 srcPort=00000 dst=127.0.0.1 src=127.0.0.1action=Permit logicalInterface=NY2-1302-DMZ_IPS_ASA_Primary sender="username" Sensor`

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring FORCEPOINT Stonesoft Management Center to communicate with QRadar

Configure Stonesoft Management Center to communicate with QRadar by editing the `LogServerConfiguration.txt` file. Configuring the text file allows Stonesoft Management Center to forward events in LEEF format by using syslog to QRadar.

Procedure

1. Log in to the appliance that hosts your Stonesoft Management Center.
2. Stop the Stonesoft Management Center Log Server.
3. In Windows, select one of the following methods to stop the Log Server.
   - Stop the Log Server in the Windows **Services** list.
   - Run the batch file `<installation path>/bin/sgStopLogSrv.bat`.

   In Linux - To stop the Log Server in Linux, run the script `<installation path>/bin/sgStopLogSrv.sh`
4. Edit the `LogServerConfiguration.txt` file. The configuration file is located in the following directory:

   `<installation path>/data/LogServerConfiguration.txt`
5. Configure the following parameters in the `LogServerConfiguration.txt` file:

Table 494. Log server configuration options		
Parameter	**Value**	**Description**
SYSLOG_EXPORT_FORMAT	LEEF	Type LEEF as the export format to use for syslog.

Table 494. Log server configuration options (continued)		
Parameter	**Value**	**Description**
SYSLOG_EXPORT_ALERT	YES | NO	Type one of the following values: • Yes - Exports alert entries to QRadar by using the syslog protocol. • No - Alert entries are not exported.
SYSLOG_EXPORT_FW	YES | NO	Type one of the following values: • Yes - Exports firewall and VPN entries to QRadar by using the syslog protocol. • No - Firewall and VPN entries are not exported.
SYSLOG_EXPORT_IPS	YES | NO	Type one of the following values: • Yes - Exports IPS logs to QRadar by using the syslog protocol. • No - IPS logs are not exported.
SYSLOG_PORT	514	Type 514 as the UDP port for forwarding syslog events to QRadar.
SYSLOG_SERVER_ADDRESS	QRadar IPv4 Address	Type the IPv4 address of your QRadar Console or Event Collector.

6. Save the `LogServerConfiguration.txt` file.
7. Start the Log Server.
   - Windows - Type `<installation path>/bin/sgStartLogSrv.bat`.
   - Linux - Type `<installation path>/bin/sgStartLogSrv.sh`.

   For detailed configuration instructions, see the StoneGate Management Center Administrator's Guide.

What to do next

You are now ready to configure a traffic rule for syslog.

Note: A firewall rule is only required if your QRadar Console or Event Collector is separated by a firewall from the Stonesoft Management Server. If no firewall exists between the Stonesoft Management Server and QRadar, you need to configure the log source in QRadar.

Configuring a syslog traffic rule for FORCEPOINT Stonesoft Management Center

If your Stonesoft Management Center and QRadar are separated by a firewall in your network, you must modify your firewall or IPS policy to allow traffic between the Stonesoft Management Center and QRadar.

Procedure

1. From the Stonesoft Management Center, select one of the following methods for modifying a traffic rule.
   - **Firewall policies** - Select **Configuration** > **Configuration** > **Firewall**.
   - **IPS policies** - Select **Configuration** > **Configuration** > **IPS**.

2. Select the type of policy to modify.
   - **Firewall** - Select **Firewall Policies** > **Edit Firewall Policy**.
   - **IPS** - Select **IPS Policies** > **Edit Firewall Policy**.
3. Add an IPv4 Access rule by configuring the following parameters for the firewall policy:

Parameter	Value
Source	Type the IPv4 address of your Stonesoft Management Center Log server.
Destination	Type the IPv4 address of your QRadar Console or Event Collector.
Service	Select **Syslog (UDP)**.
Action	Select **Allow**.
Logging	Select **None**.

   Note: In most cases, you might want to set the logging value to **None**. Logging syslog connections without configuring a syslog filter can create a loop. For more information, see the *StoneGate Management Center Administrator's Guide*.
4. Save your changes and then refresh the policy on the firewall or IPS.

What to do next

You are now ready to configure the log source in QRadar.

Forcepoint Sidewinder

Forcepoint Sidewinder is formerly known as McAfee Firewall Enterprise. The IBM QRadar DSM for Forcepoint Sidewinder collects logs from a Forcepoint Sidewinder Firewall Enterprise device by using the Syslog protocol.

To integrate Forcepoint Sidewinder with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the Forcepoint Sidewinder DSM RPM on your QRadar Console.
2. Configure Forcepoint Sidewinder to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a Forcepoint Sidewinder log source on the QRadar Console. The following table describes the parameters that require specific values for Forcepoint Sidewinder event collection:

Table 495. Forcepoint Sidewinder log source parameters

Parameter	Value
Log Source type	Forcepoint Sidewinder
Protocol Configuration	Syslog

Related concepts

“Configure Forcepoint Sidewinder to communicate with QRadar” on page 817
Before you can configure QRadar to integrate with Forcepoint Sidewinder, you must configure syslog on your Forcepoint Sidewinder Firewall Enterprise device.

Related tasks

“Adding a log source” on page 5
“Adding a DSM” on page 4

Forcepoint Sidewinder DSM specifications

The following table describes the specifications for the Forcepoint Sidewinder DSM.

Table 496. Forcepoint Sidewinder DSM specifications

Specification	Value
Manufacturer	Forcepoint
DSM name	Forcepoint Sidewinder
RPM file name	`DSM-ForcepointSidewinder-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V6.1
Event format	Syslog
Recorded event types	Forcepoint Sidewinder audit events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Forcepoint website (https://www.forcepoint.com)

Configure Forcepoint Sidewinder to communicate with QRadar

Before you can configure QRadar to integrate with Forcepoint Sidewinder, you must configure syslog on your Forcepoint Sidewinder Firewall Enterprise device.

When you configure your Forcepoint Sidewinder device to forward syslog events to QRadar, export the logs in Sidewinder Export Format (SEF).

For more information about configuring your Forcepoint Sidewinder device, see the *Forcepoint Sidewinder Administration Guide* (https://www.websense.com/content/support/library/si/v70/mgmt/si_70103_ag_a_en-us.pdf).

Related tasks

“Adding a log source” on page 5

Forcepoint Sidewinder sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when you use the Syslog protocol for the Forcepoint Sidewinder DSM:

Table 497. Forcepoint Sidewinder sample message supported by Forcepoint Sidewinder.		
Event name	**Low-level category**	**Sample log message**
nettraffic@status_conn_close	Firewall Session Closed	<131>May 16 11:41:11 auditd: date="May 16 15:41:11 2006 GMT",fac=f_ftpproxy,area=a_server,type=t_nettraffic,pri=p_major,pid=2718,ruid=0,euid=0,pgid=2718,logid=0,cmd=pftp,domain=PFTx,edomain=PFTx,srcip=192.168.0.1,srcport=4597,srcburb=internal,dstip=192.168.0.2,dstport=21,dstburb=external,protocol=6,bytes_written_to_client=0,bytes_written_to_server=0,service_name=pftp,reason="closing connection",status=conn_close,acl_id=default-outgoingrule,cache_hit=0,remote_logname=anonymous,request_command=QUIT,request_status=1,start_time="Tue May 16 11:41:06 2006",netsessid=4469f2920002870e

Forcepoint TRITON

The Forcepoint V-Series Content Gateway DSM for IBM QRadar supports events for web content from several Forcepoint TRITON solutions, including Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series appliances.

About this task

Forcepoint TRITON collects and streams event information to QRadar by using the Forcepoint Multiplexer component. Before you configure QRadar, you must configure the Forcepoint TRITON solution to provide LEEF formatted syslog events.

Before you can configure Forcepoint TRITON Web Security solutions to forward events to QRadar, you must ensure that your deployment contains a Forcepoint Multiplexer.

The Forcepoint Multiplexer is supported on Windows, Linux, and on Forcepoint V-Series appliances.

To configure a Forcepoint Multiplexer on a Forcepoint Triton or V-Series appliance:

Procedure

1. Install an instance of Forcepoint Multiplexer for each Forcepoint Policy Server component in your network.
   - For Microsoft Windows - To install the Forcepoint Multiplexer on Windows, use the TRITON Unified Installer. The Triton Unified Installer is available for download at http://www.myforcepoint.com.
   - For Linux - To install the Forcepoint Multiplexer on Linux, use the Web Security Linux Installer. The Web Security Linux Installer is available for download at http://www.myforcepoint.com.

   For information on adding a Forcepoint Multiplexer to software installations, see your *Forcepoint Security Information Event Management (SIEM) Solutions* documentation.
2. Enable the Forcepoint Multiplexer on a V-Series appliance that is configured as a full policy source or user directory and filtering appliance:
   a) Log in to your Forcepoint TRITON Web Security Console or V-Series appliance.
3. From the Appliance Manager, select **Administration** > **Toolbox** > **Command Line Utility**.
4. Click the **Forcepoint Web Security** tab.
5. From the **Command** list, select **multiplexer**, then use the **enable** command.
6. Repeat “Forcepoint TRITON” on page 818 and “Forcepoint TRITON” on page 818 to enable one Multiplexer instance for each Policy Server instance in your network.

If more than one Multiplexer is installed for a Policy Server, only the last installed instance of the Forcepoint Multiplexer is used. The configuration for each Forcepoint Multiplexer instance is stored by its Policy Server.

What to do next

You can now configure your Forcepoint TRITON appliance to forward syslog events in LEEF format to QRadar.

Configuring syslog for Forcepoint TRITON

To collect events, you must configure syslog forwarding for Forcepoint TRITON.

Procedure

1. Log in to your Forcepoint TRITON Web Security Console.
2. On the **Settings** tab, select **General** > **SIEM Integration**.
3. Select the **Enable SIEM integration for this Policy Server** check box.
4. In the **IP address or hostname** field, type the IP address of your QRadar.
5. In the **Port** field, type 514.
6. From the **Transport protocol** list, select either the **TCP** or **UDP** protocol option.

   QRadar supports syslog events for TCP and UDP protocols on port 514.
7. From the **SIEM format** list, select **syslog/LEEF (QRadar)**
8. Click **OK** to cache any changes.
9. Click **Deploy** to update your Forcepoint TRITON security components or V-Series appliances.

   The Forcepoint Multiplexer connects to Forcepoint Filtering Service and ensures that event log information is provided to QRadar.

Syslog log source parameters for Forcepoint TRITON

When you add a Forcepoint TRITON log source on the QRadar Console by using the syslog protocol, there are specific parameters you must use.

The following table describes the parameters that require specific values to collect syslog events from Forcepoint TRITON:

Table 498. Syslog log source parameters for the Forcepoint TRITON DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for your log source.
Log Source Type	Forcepoint V Series
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier or events from Forcepoint TRITON or V-series appliance.

Related tasks

“Adding a log source” on page 5
“Adding a DSM” on page 4

Forcepoint V-Series Data Security Suite

The Forcepoint V-Series Data Security Suite DSM for IBM QRadar supports Forcepoint V-Series appliances and the Data Security Suite (DSS) software.

Configuring syslog for Forcepoint V-Series Data Security Suite

The Forcepoint V-Series Data Security Suite DSM accepts events using syslog. Before you can integrate IBM QRadar you, must enable the Forcepoint V-Series appliance to forward syslog events in the Data Security Suite (DSS) Management Console.

Procedure

1. Select **Policies** > **Policy Components** > **Notification Templates**.
2. Select an existing Notification Template or create a new template.
3. Click the **General** tab.
4. Click **Send Syslog Message**.
5. Select **Options** > **Settings** > **Syslog** to access the Syslog window.

   The syslog window enables administrators to define the IP address/host name and port number of the syslog in their organization. The defined syslog receives incident messages from the Forcepoint Data Security Suite DSS Manager.
6. The syslog is composed of the following fields:

   ```
   DSS Incident|ID={value}|action={display value - max}|urgency= {coded}|policy
   categories={values,,,}|source={value-display name}|destinations={values...}|channel={display
   name}|matches= {value}|detaills={value}
   ```

   - Max length for policy categories is 200 characters.
   - Max length for destinations is 200 characters.
   - Details and source are reduced to 30 characters.
7. Click **Test Connection** to verify that your syslog is accessible.

What to do next

You can now configure the log source in QRadar. The configuration is complete. The log source is added to QRadar as OSSEC events are automatically discovered. Events that are forwarded to QRadar by OSSEC are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Forcepoint V-Series Data Security Suite

If QRadar does not automatically detect the log source, add a Forcepoint V-Series Data Security Suite log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Forcepoint V-Series Data Security Suite:

Table 499. Syslog log source parameters for the Forcepoint V-Series Data Security Suite DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Forcepoint V Series
Protocol Configuration	Syslog

Table 499. Syslog log source parameters for the Forcepoint V-Series Data Security Suite DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Forcepoint V-Series Data Security Suite DSM.

Related tasks

"Adding a log source" on page 5

Forcepoint V-Series Data Security Suite sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Forcepoint V-Series Data Security Suite sample message when you use the Syslog protocol

The following sample event message shows that a protected cloud app request was forwarded.

```
<159>Jul 21 14:38:55 forcepoint.vseries.test LEEF:1.0|Forcepoint|Security|8.5.0|
transaction:permitted|sev=1    cat=147    usrName=-    loginID=-    src=10.104.165.142
srcPort=54983    srcBytes=1773    dstBytes=1819    dst=172.16.9.3    dstPort=443    proxyStatus-
code=200    serverStatus-code=200    duration=152    method=POST    disposition=1069
contentType=text/xml; charset\=UTF-8    reason=-    policy=-    role=8    userAgent=Google
Update/1.3.35.452;winhttp;cup-ecdsa    url=https://update.domain.test/service/update2?
cup2key\=10:1538947168&cup2hreq\=c1111111ce111111111111e1a111c1111d1ca111f11a1cf1efbb11b1111111a
1 logRecordSource=OnPrem
```

Table 500. QRadar field names and highlighted values in the event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	The **Event ID** is mapped from the **disposition** value of **1069** .
Event Category	The **Event Category** is mapped from the **cat** value of **147** .
Source IP	**10.104.165.142**
Source Port	**54983**
Destination IP	**172.16.9.3**
Destination Port	**443**
Severity	**1**
Device Time	**Jul 21 14:38:55**

Forcepoint V-Series Content Gateway

The Forcepoint V-Series Content Gateway DSM for IBM QRadar supports events for web content on Forcepoint V-Series appliances with the Content Gateway software.

The Forcepoint V-Series Content Gateway DSM accepts events using syslog to stream events or by using the log file protocol to provide events to QRadar. Before you can integrate your appliance with QRadar, you must select one of the following configuration methods:

- To configure syslog for your Forcepoint V-Series, see Configure Syslog for Forcepoint V-Series Data Security Suite.

- To configure the log file protocol for your Forcepoint V-Series, see Log file protocol for Forcepoint V-Series Content Gateway.

Configure syslog for Forcepoint V-Series Content Gateway

The Forcepoint V-Series DSM supports Forcepoint V-Series appliances that run the Forcepoint Content Gateway on Linux software installations.

Before you configure IBM QRadar, you must configure the Forcepoint Content Gateway to provide LEEF formatted syslog events.

Configuring the Management Console for Forcepoint V-Series Content Gateway

You can configure event logging in the Content Gateway Manager.

Procedure

1. Log into your Forcepoint Content Gateway Manager.
2. Click the **Configure** tab.
3. Select **Subsystems** > **Logging**.

   The **General Logging Configuration** window is displayed.
4. Select **Log Transactions and Errors**.
5. Select **Log Directory** to specify the directory path of the stored event log files.

   The directory that you define must exist and the Forcepoint user must have read and write permissions for the specified directory.

   The default directory is `/opt/WGC/logs`.
6. Click **Apply**.
7. Click the **Custom** tab.
8. In the **Custom Log File Definitions** window, type the following text for the LEEF format.

```
<LogFormat>               <Name = "leef"/>               <Format = "LEEF:1.0|Forcepoint|WCG|
7.6|              %<wsds>|cat=%<wc>               src=%<chi> devTime=%<cqtn>
devTimeFormat=dd/MMM/yyyy:HH:mm:ss Z               http-username=%<caun> url=%<cquc>
              method=%<cqhm> httpversion=%<cqhv>
cachecode=%<crc>dstBytes=%<sscl> dst=%<pqsi>               srcBytes=%<pscl> proxy-status-
code=%<pssc>               server-status-code=%<sssc> usrName=%<wui>
duration=%<ttms>"/>          </LogFormat>
```

```
<LogObject>               <Format = "leef"/>               <Filename = "leef"/>
</LogObject>
```

   Note: The fields in the LEEF format string are *tab separated*. You might be required to type the LEEF format in a text editor and then cut and paste it into your web browser to retain the tab separations. The definitions file ignores extra white space, blank lines, and all comments.
9. Select **Enabled** to enable the *custom logging* definition.
10. Click **Apply**.

What to do next

You can now enable event logging for your Forcepoint Content Gateway.

Enabling Event Logging for Forcepoint V-Series Content Gateway

If you are using a Forcepoint V-Series appliance, contact Forcepoint Technical Support to enable this feature.

Procedure

1. Log in to the command-line Interface (CLI) of the server running Forcepoint Content Gateway.
2. Add the following lines to the end of the `/etc/rc.local` file:

```
( while [ 1 ] ; do tail -n1000 -F /opt/WCG/logs/leef.log | nc <IP Address> 514 sleep 1
done ) &
```

   Where <*IP Address*> is the IP address for IBM QRadar.
3. To start logging immediately, type the following command:

```
nohup /bin/bash -c "while [ 1 ] ; do tail -F /opt/WCG/logs/leef.log | nc <IP Address> 514;
sleep 1; done" &
```

   Note: You might need to type the logging command in "Enabling Event Logging for Forcepoint V-Series Content Gateway" on page 823 or copy the command to a text editor to interpret the quotation marks.

   The configuration is complete. The log source is added to QRadar as syslog events from Forcepoint V-Series Content Gateway are automatically discovered. Events forwarded by Forcepoint V-Series Content Gateway are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Forcepoint V-Series Content Gateway

If QRadar does not automatically detect the log source, add a Forcepoint V-Series Content Gateway log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Forcepoint V-Series Content Gateway:

Table 501. Syslog log source parameters for the Forcepoint V-Series Content Gateway DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Forcepoint V Series
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Forcepoint V-Series Content Gateway appliance.

Related tasks

"Adding a log source" on page 5

Log file protocol for Forcepoint V-Series Content Gateway

The log file protocol allows IBM QRadar to retrieve archived log files from a remote host.

The Forcepoint V-Series DSM supports the bulk loading of log files from your Forcepoint V-Series Content Gateway using the log file protocol to provide events on a scheduled interval. The log files contain transaction and error events for your Forcepoint V-Series Content Gateway:

Configuring the Content Management Console for Forcepoint V-Series Content Gateway

Configure event logging in the Content Management Console.

Procedure

1. Log into your Forcepoint Content Gateway interface.
2. Click the **Configure** tab.
3. Select **Subsystems** > **Logging**.
4. Select **Log Transactions and Errors**.
5. Select **Log Directory** to specify the directory path of the stored event log files.

   The directory you define must already exist and the Forcepoint user must have read and write permissions for the specified directory.

   The default directory is `/opt/WGC/logs.`
6. Click **Apply**.
7. Click the **Formats** tab.
8. Select **Netscape Extended Format** as your format type.
9. Click **Apply**.

What to do next

You can now enable event logging for your Forcepoint V-Series Content Gateway.

Log File log source parameters for Forcepoint V-Series Content Gateway

If QRadar does not automatically detect the log source, add a Forcepoint V-Series Content Gateway log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from Forcepoint V-Series Content Gateway:

Table 502. Log File log source parameters for the Forcepoint V-Series Content Gateway DSM

Parameter	Value
Log Source type	**Forcepoint V Series**
Protocol Configuration	**Log File**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Forcepoint V-Series Content Gateway devices.
Service Type	**Secure File Transfer Protocol (SFTP)**
FTP File Pattern	`extended.log_.*.old`
Remote Directory	`/opt/WCG/logs`
Event Generator	**LINEBYLINE**

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related tasks

Adding a log source

Forcepoint V-Series Content Gateway sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Forcepoint V-Series Content Gateway sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that access is blocked by websense.

```
<159>Jul 16 16:37:26 forcepoint.vseries.test LEEF:1.0|Forcepoint|Security|8.5.3|
transaction:blocked|sev=7    cat=1504    usrName=qradar1    loginID=qradar1    src=10.223.7.33
srcPort=34311    srcBytes=0    dstBytes=0    dst=10.10.10.10    dstPort=443    proxyStatus-
code=403    serverStatus-code=0    duration=66    method=POST    disposition=1064
contentType=-    reason=0-17336-Generic.Content.Web.RTSS    policy=Super Administrator**IM
Chat and Conferencing Policy    role=8    userAgent=Mozilla/5.0 (Windows NT
6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169
Safari/537.36    url=https://www.qradar.example.test/psettings/jobs/profile-shared-with-recruiter
logRecordSource=%<logRecordSource>
```

```
<159>Jul 16 16:37:26 forcepoint.vseries.test LEEF:1.0|Forcepoint|Security|8.5.3|
transaction:blocked|sev=7    cat=1504    usrName=qradar1    loginID=qradar1
src=10.223.7.33    srcPort=34311    srcBytes=0    dstBytes=0    dst=10.10.10.10
dstPort=443    proxyStatus-code=403    serverStatus-code=0    duration=66    method=POST
disposition=1064    contentType=-    reason=0-17336-Generic.Content.Web.RTSS    policy=Super
Administrator**IM Chat and Conferencing Policy    role=8    userAgent=Mozilla/5.0 (Windows
NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/
537.36    url=https://www.qradar.example.test/psettings/jobs/profile-shared-with-recruiter
logRecordSource=%<logRecordSource>
```

Table 503. Highlighted values in the Forcepoint V-Series Content Gateway event payload

QRadar field name	Highlighted values in the event payload
Event ID	**disposition**
Category	**cat**
Source IP	**src**
Source Port	**srcPort**
Destination IP	**dst**
Destination Port	**dstPort**
Username	**usrName**

Sample 2: The following sample event message shows that access is permitted by websense.

```
<159>Jun 25 10:45:18 forcepoint.vseries.test LEEF:1.0|Forcepoint|Security|8.5.3|
transaction:permitted|sev=1    cat=209    usrName=testUser    loginID=testID
src=10.252.88.231    srcPort=7434    srcBytes=636    dstBytes=63385    dst=10.10.10.10
dstPort=443    proxyStatus-code=200    serverStatus-code=200    duration=32
method=GET    disposition=1065    contentType=text/html; charset\=utf-8    reason=0-14057-
Generic.Content.Web.RTSS    policy=testPolicy Videos from testCompany    role=8
userAgent=Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/72.0.3626.121 Safari/537.36    url=https://www.qradar.example.test/watch?v\=VsxpUZaggcw
logRecordSource=%<logRecordSource>
```

```
<159>Jun 25 10:45:18 forcepoint.vseries.test LEEF:1.0|Forcepoint|Security|8.5.3|
transaction:permitted|sev=1    cat=209    usrName=testUser    loginID=testID
src=10.252.88.231    srcPort=7434    srcBytes=636    dstBytes=63385    dst=10.10.10.10
dstPort=443    proxyStatus-code=200    serverStatus-code=200    duration=32
method=GET    disposition=1065    contentType=text/html; charset\=utf-8    reason=0-14057-
Generic.Content.Web.RTSS    policy=testPolicy Videos from testCompany    role=8
userAgent=Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/72.0.3626.121 Safari/537.36    url=https://www.qradar.example.test/watch?v\=VsxpUZaggcw
logRecordSource=%<logRecordSource>
```

Table 504. Highlighted values in the Forcepoint V-Series Content Gateway event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	**disposition**
Category	**cat**
Source IP	**src**
Source Port	**srcPort**
Destination IP	**dst**
Destination Port	**dstPort**
Username	**usrName**

Chapter 66. ForeScout CounterACT

The ForeScout CounterACT DSM for IBM QRadar accepts Log Event Extended Format (LEEF) events from CounterACT using syslog.

QRadar records the following ForeScout CounterACT events:

- Denial of Service (DoS)
- Authentication
- Exploit
- Suspicious
- System

Syslog log source parameters for ForeScout CounterACT

If QRadar does not automatically detect the log source, add a ForeScout CounterACT log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from ForeScout CounterACT:

Table 505. Syslog log source parameters for the ForeScout CounterACT DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	ForeScout CounterACT
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ForeScout CounterACT appliance.

Related tasks

"Adding a log source" on page 5

Configuring the ForeScout CounterACT Plug-in

Before you configure IBM QRadar, you must install a plug-in for your ForeScout CounterACT appliance and configure ForeScout CounterACT to forward syslog events to QRadar.

About this task

To integrate QRadar with ForeScout CounterACT, you must download, install, and configure a plug-in for CounterACT. The plug-in extends ForeScout CounterACT and provides the framework for forwarding LEEF events to QRadar.

Procedure

1. From the ForeScout website (https://www.forescout.com), download the plug-in for ForeScout CounterACT.
2. Log in to your ForeScout CounterACT appliance.

3. From the CounterACT Console toolbar, select **Options** > **Plugins** > **Install**. Select the location of the plug-in file.

   The plug-in is installed and displayed in the **Plug-ins** pane.
4. From the **Plug-ins** pane, select the QRadar plug-in and click **Configure**.

   The **Add** QRadar wizard is displayed.
5. In the **Server Address** field, type the IP address of QRadar.
6. From the **Port** list, select **514**.
7. Click **Next**.
8. From the **Assigned CounterACT devices** pane, choose one of the following options:
   - **Default Server** - Select this option to make all devices on this ForeScout CounterACT, forward events to QRadar.
   - **Assign CounterACT devices** - Select this option to assign which individual devices that are running on ForeScout CounterACT forward events to QRadar. The Assign CounterACT devices option is only available if you have one or more ForeScout CounterACT servers.
9. Click **Finish**.

   The plug-in configuration is complete. You are now ready to define the events that are forwarded to QRadar by ForeScout CounterACT policies.

Configuring ForeScout CounterACT Policies

ForeScout CounterACT policies test conditions to trigger management and remediation actions on the appliance.

About this task

The plug-in provides an extra action for policies to forward the event to the IBM QRadar by using syslog. To forward events to QRadar, you must define a CounterACT policy that includes the QRadar update action.

The policy condition must be met at least one time to initiate an event send to QRadar. You must configure each policy to send updates to QRadar for events you want to record.

Procedure

1. Select a policy for ForeScout CounterACT.
2. From the **Actions tree**, select **Audit** > **Send Updates** to QRadar Server.
3. From the **Contents** tab, configure the following value:

   Select the **Send host property results** check box.
4. Choose one of the type of events to forward for the policy:
   - **Send All** - Select this option to include all properties that are discovered for the policy to QRadar.
   - **Send Specific** - Select this option to select and send only specific properties for the policy to QRadar.
5. Select the **Send policy status** check box.
6. From the **Trigger** tab, select the interval ForeScout CounterACT uses for forwarding the event to QRadar:
   - **Send when the action starts** - Select this check box to send a single event to QRadar when the conditions of your policy are met.
   - **Send when information is updated** - Select this check box to send a report when there is a change in the host properties that are specified in the **Contents** tab.

- **Send periodically every** - Select this check box to send a reoccurring event to QRadar on an interval if the policy conditions are met.

7. Click **OK** to save the policy changes.
8. Repeat this process to configure any additional policies with an action to send updates to QRadar.

   The configuration is complete. Events that are forwarded by ForeScout CounterACT are displayed on the **Log Activity** tab of QRadar.

ForeScout CounterACT sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

ForeScout CounterACT sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that an authentication certificate issuer is detected.

```
LEEF:1.0|ForeScout|CounterACT|8.0.1-99|agent_auth_issuer|cat=Property    sev=1
src=10.84.144.14    usrName=testUser    srcMAC=00:00:5E:00:53:00    domain=testDomain
identHostName=testHostName    Folder_Name=Authentication    Property_Name=Authentication
Certificate Issuer    devTime=Mar  7 2019 07:50:32.000 EST    devTimeFormat=MMM dd yyyy
HH:mm:ss.SSS z    Property_Value=\DC=BLAH\DC=testDomain\CN=testDomain2-CA
```


```
LEEF:1.0|ForeScout|CounterACT|8.0.1-99|agent_auth_issuer|cat=Property    sev=1
src=10.84.144.14    usrName=testUser    srcMAC=00:00:5E:00:53:00    domain=testDomain
identHostName=testHostName    Folder_Name=Authentication    Property_Name=Authentication
Certificate Issuer    devTime=Mar  7 2019 07:50:32.000 EST    devTimeFormat=MMM dd yyyy
HH:mm:ss.SSS z    Property_Value=\DC=BLAH\DC=testDomain\CN=testDomain2-CA
```


Table 506. Highlighted values in the Forescout CounterACT sample event

QRadar field name	Highlighted values in the event payload
Event ID	**agent_auth_issuer**
Category	**Property**
Source IP	**10.84.144.14**
Username	**testUser**
Device Time	**Mar 7 2019 07:50:32.000 EST**

Sample 2: The following sample event message shows when the last credentials succeeded on this host.

```
LEEF:1.0|ForeScout|CounterACT|8.0.1-99|cached_credentials|cat=Property    sev=1
src=192.168.74.25    usrName=qradar1    srcMAC=00:00:5E:00:53:C8    domain=testDomain
identHostName=D-q1labs1    Folder_Name=    Property_Name=Last credentials to succeed on this
host    devTime=Mar 26 2019 15:56:14.000 PDT    devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z
Property_Value=admin1@example.test2001:db8:4D1C:A2FA:3EC9:C66D:8522:B7A4
```


```
LEEF:1.0|ForeScout|CounterACT|8.0.1-99|cached_credentials|cat=Property    sev=1
src=192.168.74.25    usrName=qradar1    srcMAC=00:00:5E:00:53:C8    domain=testDomain
identHostName=D-q1labs1    Folder_Name=    Property_Name=Last credentials to succeed on this
host    devTime=Mar 26 2019 15:56:14.000 PDT    devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z
Property_Value=admin1@example.test2001:db8:4D1C:A2FA:3EC9:C66D:8522:B7A4
```


Table 507. Highlighted values in the Forescout CounterACT sample event

QRadar field name	Highlighted values in the event payload
Event ID	**cached_credentials**
Category	**Property**
Source IP	**192.168.74.25**

Table 507. Highlighted values in the Forescout CounterACT sample event (continued)	
QRadar field name	**Highlighted values in the event payload**
Username	**qradar1**
Device Time	**Mar 26 2019 15:56:14.000 PDT**

Chapter 67. Fortinet FortiGate Security Gateway

The IBM QRadar SIEM DSM for Fortinet FortiGate Security Gateway collects events from Fortinet FortiGate Security Gateway and Fortinet FortiAnalyzer products.

The following table identifies the specifications for the Fortinet FortiGate Security Gateway DSM:

Table 508. Fortinet FortiGate Security Gateway DSM specifications

Specification	**Value**
Manufacturer	Fortinet
DSM name	Fortinet FortiGate Security Gateway
RPM file name	`DSM-FortinetFortiGate-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	FortiOS 6.4 and earlier
Protocol	Syslog Syslog Redirect
Recorded event types	All events
Auto discovered?	Yes
Includes identity?	Yes
Includes custom properties?	Yes
More information	Fortinet website (http://www.fortinet.com)

To integrate Fortinet FortiGate Security Gateway DSM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the Fortinet FortiGate Security Gateway RPM from the IBM Support Website onto your QRadar Console:
2. Download and install the Syslog Redirect protocol RPM to collect events through Fortinet FortiAnalyzer. When you use the Syslog Redirect protocol, QRadar can identify the specific Fortinet FortiGate Security Gateway firewall that sent the event.
3. For each instance of Fortinet FortiGate Security Gateway, configure your Fortinet FortiGate Security Gateway system to send syslog events to QRadar.
4. If QRadar does not automatically detect the log source for Fortinet FortiGate Security Gateway, you can manually add the log source. For the protocol configuration type, select **Syslog**, and then configure the parameters.
5. If you want QRadar to receive events from Fortinet FortiAnalyzer, manually add the log source. For the protocol configuration type, select **Syslog Redirect**, and then configure the parameters.

   The following table lists the specific parameter values that are required for Fortinet FortiAnalyzer event collection:

Parameter	Value
Log Source Identifier Regex	**devname="?([\w-]+)**
Listen Port	**517**
Protocol	**UDP**

For more information about configuring Syslog Redirect protocol parameters, see Syslog Redirect protocol overview.

Related concepts

Fortinet FortiGate Security Gateway sample event messages
Use these sample event messages to verify a successful integration with IBM QRadar.

Related tasks

Configuring a syslog destination on your Fortinet FortiGate Security Gateway device
To forward Fortinet FortiGate Security Gateway events to IBM QRadar, you must configure a syslog destination.

Configuring a syslog destination on your Fortinet FortiAnalyzer device
To forward Fortinet FortiAnalyzer events to IBM QRadar, you must configure a syslog destination.

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring a syslog destination on your Fortinet FortiGate Security Gateway device

To forward Fortinet FortiGate Security Gateway events to IBM QRadar, you must configure a syslog destination.

Procedure

1. Log in to the command line on your Fortinet FortiGate Security Gateway appliance.
2. Type the following commands, in order, replacing the variables with values that suit your environment.

```
config log syslogd setting
set status enable
set facility <facility_name>
set csv {disable | enable}
set port <port_integer>
set reliable enable
set server <IP_address>
end
example: set facility syslog
```

Note: If you set the value of `reliable` as `enable`, it sends as TCP; if you set the value of `reliable` as `disable`, it sends as UDP.

What to do next

Your deployment might have multiple Fortinet FortiGate Security Gateway instances that are configured to send event logs to FortiAnalyzer. If you want to send FortiAnalyzer events to QRadar, see Configuring a syslog destination on your Fortinet FortiAnalyzer device.

Configuring a syslog destination on your Fortinet FortiAnalyzer device

To forward Fortinet FortiAnalyzer events to IBM QRadar, you must configure a syslog destination.

Procedure

1. Log in to your FortiAnalyzer device.
2. On the **Advanced** tree menu, select **Syslog Forwarder**.
3. On the toolbar, click **Create New**.
4. Configure the **Syslog Server** parameters:

Parameter	Description
Port	The default port is 514.

5. Click **OK**.

Fortinet FortiGate Security Gateway sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Fortinet FortiGate Security Gateway sample messages when you use the Syslog or the Syslog Redirect protocol

Important: Due to formatting, paste the message format into a text editor and then remove any carriage return or line feed characters.

Sample 1: The following sample shows an attempt to use a remote-access vulnerability that affects Microsoft Exchange Server. A remote attacker uses the vulnerability by sending an email with a meeting request that contains specially crafted vCal and iCal calendar data. As a result, the attacker might be able to take control of a vulnerable system.

```
<185>date=2011-05-09 time=14:31:07 devname=exampleDeviceName device_id=EXAMPLEDEVID2
log_id=0987654321 type=ips subtype=signature pri=alert severity=high carrier_ep="N/A"
profilegroup="N/A" profiletype="N/A" profile="Example_Profile" src=10.10.10.10 dst=10.20.20.20
src_int=exampleVlan2 dst_int=exampleVlan1 policyid=4 identidx=0 serial=123456 status=detected
proto=6 service=smtp vd="exampleDomain" count=1 src_port=50000 dst_port=8080
attack_id=11897 sensor=exampleSensor ref=url.example.test user="N/A" group=Example_Group
incident_serialno=1234567890 msg="email: MS.Exchange.Mail.Calender.Buffer.Overflow"
```

Table 509. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**attack_id**
Source IP	**src**
Source Port	**src_port**
Destination IP	**dst**
Destination Port	**dst_port**
Protocol	**proto**
Policy	**policyid**
Device Time	**date** + **time**

Sample 2: The following sample shows that routing information has changed.

```
date=2020-09-17 time=01:36:20 logid="0100022921" type="event"subtype="system" level="critical"
vd="root" eventtime=1600331781108372788 tz="-0700" logdesc="Routing information changed"
name="Google_Ping" interface="TEST-INF1" status="down" msg="Static route on interface TEST-INF1
may be removed by health-check Google_Ping. Route:  (10.10.10.27->10.10.8.8 ping-down)"
```

Table 510. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**logdesc** + **level**
Device Time	**date** + **time**

Sample 3: The following sample shows that a firewall is allowed.

```
date=2020-09-10 time=05:01:35 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="root" eventtime=1599739296076496743 tz="-0700" srcip=192.168.14.111
srcport=54923 srcintf="internal" srcintfrole="lan" dstip=192.168.14.112 dstport=80
dstintf="wan1" dstintfrole="wan" srccountry="Reserved" dstcountry="Test Country"
sessionid=53159 proto=6 action="close" policyid=1 policytype="policy" poluuid="a9b81e06-
c6a0-51e8-e434-a05c75d5ad74" policyname="Internet_Access" service="HTTP" trandisp="snat"
transip=172.16.72.26 transport=54923 appid=17735 app="Facebook_Apps" appcat="Social.Media"
apprisk="medium" applist="default" duration=187 sentbyte=2333 rcvdbyte=2585 sentpkt=42
rcvdpkt=42 vwlid=6 vwlservice="Facebook-Instagram" vwlquality="Seq_num(1 wan1), alive,
sla(0x1), cfg_order(0), cost(10), selected" utmaction="allow" countapp=1 sentdelta=1092
rcvddelta=780 utmref=65515-3302
```

Table 511. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**utmaction**
Source IP	**srcip**
Source Port	**srcport**
Destination IP	**dstip**
Destination Port	**dstport**
Pre NAT Source IP	**srcip**
Pre NAT Source Port	**srcport**
Post NAT Source IP	**transip**
Post NAT Source Port	**transport**
Protocol	**proto**
Policy	**policyid**
Duration Seconds	**duration**
Device Time	**date** + **time**

Related concepts

Fortinet FortiGate Security Gateway

The IBM QRadar SIEM DSM for Fortinet FortiGate Security Gateway collects events from Fortinet FortiGate Security Gateway and Fortinet FortiAnalyzer products.

Configuring QRadar to categorize App Ctrl events for Fortinet Fortigate Security Gateway

If you want to categorize App Ctrl events based on the **Action** field in IBM QRadar, use the DSM Editor to enable the **App Ctrl** events.

By default, Fortinet Fortigate Security Gateway **App Ctrl** events are categorized as **notice/informational**.

Procedure

1. On the **Admin** tab, in the **Data Sources** section, click **DSM Editor**.
2. From the **Select Log Source Type** window, select **Fortinet FortiGate Security Gateway** from the list, and click **Select**.
3. On the **Configuration** tab, set **Display DSM Parameters Configuration** to **On**.
4. From the **Event Collector** list, select the event collector for the log source, and click **Select**.
5. Set **Categorize App Ctrl Logs Based on Action Field** to **On**.
6. Click **Save** and close the DSM Editor.

Chapter 68. Foundry FastIron

You can integrate a Foundry FastIron device with IBM QRadar to collect all relevant events using syslog.

To do this you must configure syslog and your log source.

Configuring syslog for Foundry FastIron

To integrate IBM QRadar with a Foundry FastIron RX device, you must configure the appliance to forward syslog events.

Procedure

1. Log in to the Foundry FastIron device command-line interface (CLI).
2. Type the following command to enable logging:

   `logging on`

   Local syslog is now enabled with the following defaults:

   - Messages of all syslog levels (Emergencies - Debugging) are logged.
   - Up to 50 messages are retained in the local syslog buffer.
   - No syslog server is specified.
3. Type the following command to define an IP address for the syslog server:

   `logging host <IP Address>`

   Where <*IP Address*> is the IP address of your QRadar.

   You are now ready to configure the log source in QRadar.

Syslog log source parameters for Foundry FastIron

If QRadar does not automatically detect the log source, add a Foundry FastIron log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Foundry FastIron:

Table 512. Syslog log source parameters for the Foundry FastIron DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Foundry FastIron
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Foundry FastIron appliance.

Related tasks

"Adding a log source" on page 5

Chapter 69. FreeRADIUS

The IBM QRadar DSM for FreeRADIUS collects events from your FreeRADIUS device.

The following table lists the specifications for the FreeRADIUS DSM:

Table 513. FreeRADIUS DSM specifications

Specification	**Value**
Manufacturer	FreeRADIUS
DSM name	FreeRADIUS
RPM file name	DSM-FreeRADIUS-*Qradar_version-build_number*.noarch.rpm
Supported versions	V2.x
Event format	Syslog
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	FreeRADIUS website (http://freeradius.org)

To send logs from FreeRADIUS to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the FreeRADIUS DSM RPM from the IBM Support Website onto your QRadar Console.
2. Configure your FreeRADIUS device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a FreeRADIUS log source on the QRadar Console. The following table describes the parameters that require specific values for FreeRADIUS event collection:

Table 514. FreeRADIUS log source parameters

Parameter	**Value**
Log Source type	FreeRADIUS
Protocol Configuration	Syslog

Configuring your FreeRADIUS device to communicate with QRadar

Configure FreeRADIUS to send logs to the syslog daemon of the host and configure the daemon to send events to QRadar.

Before you begin

You must have a working knowledge of syslog configuration and the Linux distribution.

About this task

FreeRADIUS has multiple distributions. Some files might not be in the same locations that are described in this procedure. For example, the location of the FreeRADIUS startup script is based on distribution. Conceptually, the configuration steps are the same for all distributions.

Procedure

1. Log in to the system that hosts FreeRADIUS.
2. Edit the `/etc/freeradius/radius.conf` file.
3. Change the text in the file to match the following lines:

```
logdir = syslog
Log_destination = syslog
log{
    destination = syslog
    syslog_facility = daemon
    stripped_names = no
    auth = yes
    auth_badpass = no
    auth_goodpass = no
}
```

4. Edit the `/etc/syslog.conf` file.
5. To configure log options, add the following text.

   # .=notice logs authentication messages (L_AUTH).
   # <facility_name>.=notice
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>

   # .=err logs module errors for FreeRADIUS.
   #<facility_name>.=err
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>

   # .* logs messages to the same target.
   # <facility_name>.*
   @<IP_address_of_QRadar_Event_Collector_or_QRadar_Console>

   An example syslog facility name is *local1*. You can rename it.

   To configure a log option, remove the comment tag (*#*) from one of the active lines that contains an `@` symbol.
6. If the configuration change does not load automatically, restart the syslog daemon. The method to restart the syslog daemon depends on the distribution that is used. The following table lists possible methods.

Operating system distribution	Command to restart daemon
Red Hat Enterprise Linux	service syslog restart
Debian Linux or Ubuntu Linux	`/etc/init.d/syslog` restart
FreeBSD operating system	`/etc/rc.d/syslog`d restart

7. Add the following options to the FreeRADIUS startup script:
   - `-l syslog`
   - `-g` *<facility_name>*

   The `-g` value must match the facility name in Step 5.
8. Restart FreeRADIUS.

Chapter 70. Generic

The generic DSMs for IBM QRadar record all relevant authorization and firewall events by using Syslog. Generic refers to a non-vendor specific group of supported application types.

You must configure QRadar to interpret the incoming generic events, and manually create a log source.

QRadar supports the following generic DSMs:

- Generic authorization server
- Generic firewall

Generic authorization Server

The generic authorization server DSM for IBM QRadar records all relevant generic authorization events by using Syslog. Generic refers to a non-vendor specific group of supported application types.

You must configure QRadar to interpret the incoming generic authorization events, and manually create a log source.

Configuring event properties for authorization events

You must manually configure IBM QRadar to interpret the incoming generic authorization events:

Procedure

1. Forward all authentication server logs to your QRadar system.

   For information about forwarding authentication server logs to QRadar, see the vendor documentation for your authorized server.
2. Open the following file:

   `/opt/QRadar/conf/genericAuthServer.conf`

   Make sure you copy this file to systems that host the Event Collector and the QRadar Console.
3. Restart the Tomcat server:

   ```
   service tomcat restart
   ```

   A message is displayed indicating that the Tomcat server is restarted.
4. Enable or disable regular expressions in your patterns by setting the **`regex_enabled`** property. By default, regular expressions are disabled.
   For example:

   `regex_enabled=false`

   When you set the **`regex_enabled`** property to `false`, the system generates regular expressions (regex) based on the tags you entered when you try to retrieve the corresponding data values from the logs.

   When you set the **`regex_enabled`** property to `true`, you can define custom regex to control patterns. These regex configurations are applied directly to the logs and the first captured group is returned. When you define custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see http://download.oracle.com/javase/tutorial/essential/regex/.

   To integrate the generic authorization server with QRadar, make sure that you specify the classes directly instead of using the predefined classes. For example, the digit class `(/\d/)` becomes `/[0-9]/`. Rewrite the expression to use the primitive qualifiers `(/?/,/*/ and /+/)` rather than using numeric qualifiers.

5. Add the following lines to the genericAuthServer.conf file:

```
login_success_pattern=<login success pattern>
login_failed_pattern=<login failure pattern>
logout_pattern=<logout pattern>
source_ip_pattern=<source IP pattern>
source_port_pattern=<source port pattern>
user_name_pattern=<for pattern>
```

The following table provides examples of values that you can use for each pattern.

Pattern	Value	Example
login_success=<*login success pattern*>	Accepted password	The following log message shows login_success_pattern=Accepted password: Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from <IP_address> port 1727 ssh2
login_failed_pattern=<*login failure pattern*>	Failed password	The following log message shows login_failed_pattern=Failed password: Jun 27 12:58:33 expo sshd[20627]: Failed password for root from <IP_address> port 1849 ssh2
logout_pattern=<*logout pattern*>	session closed	The following log message shows logout_pattern=session closed: Jun 27 13:00:01 expo su(<Username>)[22723]: session closed for user genuser
source_ip_pattern=<*source IP pattern*>	from	The following log message shows source_ip_pattern=from: Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from <IP_address> port 1727 ssh2

Pattern	Value	Example
source_port_pattern=<*source port pattern*>	port	The following log message shows source_port_pattern=port: Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from <IP_address> port 1727 ssh2
user_name_pattern=<*for pattern*>	for	The following log message shows user_name_pattern=for: Jun 27 12:11:21 expo sshd[19926]: Accepted password for root from <IP_address> port 1727 ssh2

Tip: All entries are case-insensitive.

What to do next

You are now ready to configure the log source in QRadar.

Syslog log source parameters for generic authorization server

If QRadar does not automatically detect the log source, add a non-vendor specific generic authorization server log source on the QRadar Console by using the Syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from generic authorization server:

Table 515. Syslog log source parameters for the generic authorization server DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Configurable Authentication
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your generic authorization appliance.

Related tasks

“Adding a log source” on page 5

Generic firewall

The generic firewall DSM for IBM QRadar records all relevant events by using Syslog.

You must configure QRadar to interpret the incoming generic firewall events, and manually create a log source.

Configuring event properties for generic firewall events

You must manually configure IBM QRadar to interpret the incoming generic firewall events.

Procedure

1. Forward all firewall logs to QRadar.

   For information about forwarding firewall logs from your generic firewall to QRadar, see the vendor documentation for your firewall events.
2. Open the following file:

   `/opt/QRadar/conf/genericFirewall.conf`

   Make sure you copy this file to systems that host the Event Collector and the QRadar Console.
3. Restart the Tomcat server:

   `service tomcat restart`

   A message is displayed indicating that the Tomcat server is restarted.
4. Enable or disable regular expressions in your patterns by setting the **`regex_enabled`** property. By default, regular expressions are disabled.

   For example:

   `regex_enabled=false`

   When you set the **`regex_enabled`** property to `false`, the system generates regular expressions based on the tags you entered while you try to retrieve the corresponding data values from the logs.

   When you set the **`regex_enabled`** property to `true`, you can define custom regex to control patterns. These regex configurations are directly applied to the logs and the first captured group is returned. When you define custom regex patterns, you must adhere to regex rules, as defined by the Java programming language. For more information, see http://download.oracle.com/javase/tutorial/essential/regex/.

   To integrate a generic firewall with QRadar, make sure that you specify the classes directly instead of using the predefined classes. For example, the digit class `(/\d/)` becomes `/[0-9]/`. Rewrite the expression to use the primitive qualifiers `(/?/,/*/ and /+/)` rather than using numeric qualifiers.
5. Add the following lines to the `genericFirewall.conf` file:

   ```
   accept_pattern=<accept pattern>
   deny_pattern=<deny pattern>
   source_ip_pattern=<source ip pattern>
   source_port_pattern=<source port pattern>
   destination_ip_pattern=<destination ip pattern>
   ```

   The following table provides examples of values that you can use for each pattern.

Pattern	Value	Example
accept pattern=<*accept pattern*>	Packet accepted	The following log message shows accept pattern=Packet accepted: Aug. 5, 2005 08:30:00 Packet accepted. Source IP: <Source_IP_address> Source Port: 80 Destination IP: <Destination_IP_address> Destination Port: 80 Protocol: tcp
deny_pattern=<*deny pattern*>	Packet denied	The following log message shows deny_pattern=Packet denied: Aug. 5, 2005 08:30:00 Packet denied. Source IP: <Source_IP_address> Source Port: 21 Destination IP: <Destination_IP_address> Destination Port: 21 Protocol: tcp
source_ip_pattern=<*source IP pattern*>	from	The following log message shows source_ip_pattern=Source IP: Aug. 5, 2005 08:30:00 Packet accepted. Source IP: <Source_IP_address> Source Port: 80 Destination IP: <Destination_IP_address> Destination Port: 80 Protocol: tcp
source_port_pattern=<*source port pattern*>	port	The following log message shows source_port_pattern=Source Port: Aug. 5, 2005 08:30:00 Packet accepted. Source IP: <Source_IP_address> Source Port: 80 Destination IP: <Destination_IP_address> Destination Port: 80 Protocol: tcp

Pattern	Value	Example
destination_ip_pattern=<*destination IP pattern*>	from	The following log message shows destination_ip_pattern=Destination IP. Aug. 5, 2005 08:30:00 Packet accepted. Source IP: <Source_IP_address> Source Port: 80 Destination IP: <Destination_IP_address> Destination Port: 80 Protocol: tcp
destination_port_pattern=<*destination port pattern*>	port	The following log message shows destination_port_pattern=Destination Port: Aug. 5, 2005 08:30:00 Packet accepted. Source IP: <Source_IP_address> Source Port: 80 Destination IP: <Destination_IP_address> Destination Port: 80 Protocol: tcp
protocol_pattern=<*protocol pattern*>	protocol	The following log message shows protocol_pattern=Protocol: Aug. 5, 2005 08:30:00 Packet accepted. Source IP: <Source_IP_address> Source Port: 80 Destination IP: <Destination_IP_address> Destination Port: 80 Protocol: tcp

Tip: Patterns are case-insensitive and you can add multiple patterns. For multiple patterns, separate by using a # symbol.

6. Save and exit the file.

What to do next

You are now ready to configure the log source in QRadar.

Syslog log source parameters for generic firewall

If QRadar does not automatically detect the log source, add a generic firewall log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from generic firewall:

Table 516. Syslog log source parameters for the generic firewall DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Configurable Firewall Filter
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your generic firewall appliance.

Related tasks

"Adding a log source" on page 5

Chapter 71. genua genugate

The IBM QRadar DSM for genua genugate collects events from a genua genugate device.

genua genugate produces logs from third-party software such as openBSD and sendMail. The genua genugate DSM provides basic parsing for the logs from these third-party devices. To achieve more specify parsing for these logs, install the specific DSM for that device.

The following table lists the specifications for the genua genugate DSM:

Table 517. genua genugate DSM specifications

Specification	**Value**
Manufacturer	genua
DSM name	genua genugate
RPM file name	`DSM-GenuaGenugate-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	8.2 and later
Protocol	Syslog
Recorded event types	General error messages High availability General relay messages Relay-specific messages genua programs/daemons EPSI Accounting Daemon - gg/src/acctd Configfw FWConfig ROFWConfig User-Interface Webserver
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	genua website (https://www.genua.de/en/solutions/high-resistance-firewall-genugate.html)

To send genua genugate events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - genua genugate DSM RPM
2. Configure your genua genugate device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a genua genugate log source on the QRadar Console. Configure all required parameters and use the following table to identify specific values for genua genugate:

Table 518. genua genugate log source parameters	
Parameter	**Value**
Log Source type	genua genugate
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring genua genugate to send events to QRadar
Configure genua genugate to send events to IBM QRadar.

Adding a log source

Configuring genua genugate to send events to QRadar

Configure genua genugate to send events to IBM QRadar.

Procedure

1. Log in to genua genugate.
2. Click **System** > **Sysadmin** > **Logging page**.
3. In the IBM QRadar **IP Address** field, type the IP address of your QRadar Console or Event Collector.
4. Select the **Accounting to External** check box.
5. Click **OK**.

genua genugate sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

genua genugate sample message when you use the Syslog protocol

The following sample message event shows a ssh-relay event and associated information.

```
Oct 12 04:28:18 genua.genugate.test sshrelay[1077]: LEEF:1.0|genua|
genugate|8.2|E4067|devTime=2014-10-12T04:28:18+0200    devTimeFormat=yyyy-MM-dd'T'HH:mm:ssZ
laddr=127.128.0.242    lport=1    msg=Error for \"CONNECT\": Code=1 Msg=connect failed: Operation
timed out. No response from server. (192.168.130.14:22)    relay_name=ssh    rnum=247    sev=6
srcPreNAT=192.168.132.12    srcPreNATPort=38070
```

```
Oct 12 04:28:18 genua.genugate.test sshrelay[1077]: LEEF:1.0|genua|genugate|
8.2|E4067|devTime=2014-10-12T04:28:18+0200    devTimeFormat=yyyy-MM-dd'T'HH:mm:ssZ
laddr=127.128.0.242    lport=1    msg=Error for \"CONNECT\": Code=1 Msg=connect failed:
Operation timed out. No response from server. (192.168.130.14:22)    relay_name=ssh
rnum=247    sev=6    srcPreNAT=192.168.132.12    srcPreNATPort=38070
```

Table 519. Highlighted values in the genua genugate sample event message	
QRadar field name	**Highlighted values in the event payload**
Event ID	**E4067**
Source IP	For this DSM, the value in QRadar is always **127.0.0.1** when the payload does not contain a Source IP.

Table 519. Highlighted values in the genua genugate sample event message (continued)	
QRadar field name	**Highlighted values in the event payload**
Destination IP	**192.168.130.14**
Destination Port	**22**
Pre NAT Source IP	**192.168.132.12**
Pre NAT Source Port	**38070**

Chapter 72. Google

IBM QRadar supports a range of Google products.

Google Cloud Audit Logs

The IBM QRadar DSM for Google Cloud Audit Logs collects JSON events from a Google Cloud service.

To integrate Google Cloud Audit Logs with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - GoogleCloudAudit DSM RPM
   - DSM Common RPM
   - GoogleCloudPubSub protocol RPM
   - GoogleCommon protocol RPM
   - Protocol Common RPM
2. Configure your Google Cloud Audit Logs service to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a log source for Google Cloud Audit Logs on the QRadar Console.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Google Cloud Audit Logs DSM specifications

When you configure the Google Cloud Audit Logs, understanding the specifications for the Google Cloud Audit Logs DSM can help ensure a successful integration. For example, knowing what the supported services of Google Cloud Audit Logs is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Google Cloud Audit Logs DSM.

Table 520. Google Cloud Audit Logs DSM specifications

Specification	**Value**
Manufacturer	Google
DSM name	Google Cloud Audit Logs
RPM file name	DSM-*GoogleCloudAudit-7.4-QRadar_version-build_number*.noarch.rpm
Supported services	Google Compute Engine Identity Access Management Identity Platform Cloud Storage
Protocol	Google Cloud Pub/Sub
Event format	JSON

Table 520. Google Cloud Audit Logs DSM specifications (continued)	
Specification	**Value**
Recorded event types	Storage, list, update
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Google Cloud Audit Logs documentation (https://cloud.google.com/logging/docs/audit)

Configuring Google Cloud Audit Logs to communicate with QRadar

Before you can add a log source in IBM QRadar, you must set up a functioning Pub/Sub system on your Google Cloud console.

Procedure

1. Create a Google account. For more information, see Create a Google Account (https://support.google.com/accounts/answer/27441?hl=en).
2. Set up a Pub/Sub system on your Google Cloud console. For more information, see Quickstart: building a functioning Pub/Sub system (https://cloud.google.com/pubsub/docs/quickstart-py-mac).

   Important: When you create service account credentials on the Google Cloud platform, use the following service account credentials:

```
{
  "type": "service_account",
  "project_id": "<project_id>",
  "private_key_id": "<private_key_id>",
  "private_key": “<private_key>",
  "client_email": "<client_email>",
  "client_id": "111111111111111111",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "< client_x509_cert_url >"
}
```

What to do next

Add a log source in QRadar. For more information, see Google Cloud Pub/Sub protocol log source parameters for Google Cloud Audit Logs.

Google Cloud Pub/Sub protocol log source parameters for Google Cloud Audit Logs

If QRadar does not automatically detect the log source, add a Google Cloud Audit Logs log source on the QRadar Console by using the Google Cloud Pub/Sub protocol.

When using the Google Cloud Pub/Sub protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Google Cloud Pub/Sub events from Google Cloud Audit Log Service:

Table 521. Google Cloud Pub/Sub protocol log source parameters for the Google Cloud Audit Log DSM	
Parameter	**Value**
Log Source type	Google Cloud Audit Logs

Table 521. Google Cloud Pub/Sub protocol log source parameters for the Google Cloud Audit Log DSM (continued)	
Parameter	**Value**
Protocol Configuration	Google Pub/Sub Protocol
Log Source Identifier	Use the IP address as a identifier for events from your Google Cloud Audit Log Service. The log source identifier must be a unique value.

For a complete list of Google Cloud Pub/Sub protocol parameters and their values, see Google Cloud Pub/Sub protocol configuration options..

Related tasks

Adding a log source

Google Cloud Audit Logs sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Google Cloud Audit Logs sample message when you use the Google Cloud Pub/Sub protocol: list of objects retrieved

The following sample event message shows the retrieval of a list of objects that match the criteria that are provided. This retrieval is the result of an action that was taken by Google Cloud Storage.


```
{"insertId":"a1aaaaa11aaa","logName":"projects/clover-pciprod/logs/cloudaudit.googleapis.
com%2Fdata_access","protoPayload":{"@type":"type.googleapis.com/google.cloud.audit.AuditLog",
"authenticationInfo":{"principalEmail":"user@test"},
"authorizationInfo":[{"granted":true,"permission":"storage.objects.list","resource":"projects
/_/buckets/rivus-file-cache-clover-pciprod","resourceAttributes":{}}],
"methodName":"storage.objects.list","requestMetadata":
{"callerIp":"10.135.0.42","callerNetwork":"//compute.googleapis.com/projec
ts/clover-vpc-pci/global/networks/__unknown__","callerSuppliedUserAgent":"Clover Google-API-Jav
a-Client Google-HTTP-Java-Client/1.28.0 (gzip),gzip(gfe)","destinationAttributes":{},"requestAt
tributes":{"auth":{},"time":"2020-04-08T23:35:14.487672816Z"}},"resourceLocation":{"currentLoca
tions":["location"]},"resourceName":"projects/_/buckets/rivus-file-cache-clover-pciprod",
"serviceName":"storage.googleapis.com","status":{}},
"receiveTimestamp":"2020-04-08T23:35:15.981168264Z","resource":{"labels":
{"bucket_name":"rivus-file-cache-clover-pciprod","location":"location","project_id":"clover-pc
iprod"},"type":"gcs_bucket"},"severity":"INFO","timestamp":"2020-04-08T23:35:14.483227095Z"}
```



```
{"insertId":"a1aaaaa11aaa","logName":"projects/clover-pciprod/logs/cloudaudit.googleapis.
com%2Fdata_access","protoPayload":{"@type":"type.googleapis.com/google.cloud.audit.AuditLog",
"authenticationInfo":{"principalEmail":"user@test"},
"authorizationInfo":[{"granted":true,"permission":"storage.objects.list","resource":"projects
/_/buckets/rivus-file-cache-clover-pciprod","resourceAttributes":{}}],
"methodName":"storage.objects.list","requestMetadata":
{"callerIp":"10.135.0.42","callerNetwork":"//compute.googleapis.com/projec
ts/clover-vpc-pci/global/networks/__unknown__","callerSuppliedUserAgent":"Clover Google-API-Jav
a-Client Google-HTTP-Java-Client/1.28.0 (gzip),gzip(gfe)","destinationAttributes":{},"requestAt
tributes":{"auth":{},"time":"2020-04-08T23:35:14.487672816Z"}},"resourceLocation":{"currentLoca
tions":["location"]},"resourceName":"projects/_/buckets/rivus-file-cache-clover-pciprod",
"serviceName":"storage.googleapis.com","status":{}},
"receiveTimestamp":"2020-04-08T23:35:15.981168264Z","resource":{"labels":
{"bucket_name":"rivus-file-cache-clover-pciprod","location":"location","project_id":"clover-pc
iprod"},"type":"gcs_bucket"},"severity":"INFO","timestamp":"2020-04-08T23:35:14.483227095Z"}
```


Table 522. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**MethodName**

Table 522. Highlighted fields (continued)	
QRadar field name	**Highlighted payload field name**
Event Category	**serviceName**
Logsource Time	**receivedTimestamp**
Username	**authenticationInfo** + **principalEmail**
Source IP	**requestMetadata** + **callerIp**

Google Cloud Audit Logs sample message when you use the Google Cloud Pub/Sub protocol: object information modified

The following sample event message shows the modification of an object's information and is the result of an action that was taken by Google Cloud Storage.


```
{"insertId":"a1aaaaa11aaa","logName":"projects/clover-pciprod/logs/cloudaudit.googleapis.
com%2Fdata_access","protoPayload":{"@type":"type.googleapis.com/google.cloud.audit.AuditLog",
"authenticationInfo":{"principalEmail":"user@test"},"authorizationInfo":
[{"granted":true,"permission":"storage.objects.update","resource":"projects/_/buckets/rivus-
file-cache-clover-pciprod/objects/NORTH_ADJUSTMENT/2020/04/08/USER#A11AAA.11111111.111111.te
st.example","resourceAttributes":{}}],"methodName":"storage.objects.update"
,"requestMetadata":{"callerIp":"10.135.0.42","callerNetwork":"//compute.
googleapis.com/projects/clover-vpc-pci/global/networks/__unknown__","callerSuppliedUserAgent":
"Clover Google-API-Java-Client Google-HTTP-Java-Client/1.28.0 (gzip),gzip(gfe)","destinationAt
tributes":{},"requestAttributes":{"auth":{},"time":"2020-04-08T23:35:26.176068572Z"}},"resourc
eLocation":{"currentLocations":["location"]},"resourceName":"projects/_/buckets/rivus-file-cac
he-clover-pciprod/objects/NORTH_ADJUSTMENT/2020/04/08/USER#A11AAA.11111111.111111.test.example
","serviceName":"storage.googleapis.com","status":{}},"receiveTimestamp":
"2020-04-08T23:35:27.212247517Z","resource":{"labels":{"bucket_name":"rivus-file-cache-clover-
pciprod","location":"location","project_id":"clover-pciprod"},"type":"gcs_bucket"},"severity":
"INFO","timestamp":"2020-04-08T23:35:26.171189525Z"}
```



```
{"insertId":"a1aaaaa11aaa","logName":"projects/clover-pciprod/logs/cloudaudit.googleapis.
com%2Fdata_access","protoPayload":{"@type":"type.googleapis.com/google.cloud.audit.AuditLog",
"authenticationInfo":{"principalEmail":"user@test"},"authorizationInfo":
[{"granted":true,"permission":"storage.objects.update","resource":"projects/_/buckets/rivus-
file-cache-clover-pciprod/objects/NORTH_ADJUSTMENT/2020/04/08/USER#A11AAA.11111111.111111.te
st.example","resourceAttributes":{}}],"methodName":"storage.objects.update"
,"requestMetadata":{"callerIp":"10.135.0.42","callerNetwork":"//compute.
googleapis.com/projects/clover-vpc-pci/global/networks/__unknown__","callerSuppliedUserAgent":
"Clover Google-API-Java-Client Google-HTTP-Java-Client/1.28.0 (gzip),gzip(gfe)","destinationAt
tributes":{},"requestAttributes":{"auth":{},"time":"2020-04-08T23:35:26.176068572Z"}},"resourc
eLocation":{"currentLocations":["location"]},"resourceName":"projects/_/buckets/rivus-file-cac
he-clover-pciprod/objects/NORTH_ADJUSTMENT/2020/04/08/USER#A11AAA.11111111.111111.test.example
","serviceName":"storage.googleapis.com","status":{}},"receiveTimestamp":
"2020-04-08T23:35:27.212247517Z","resource":{"labels":{"bucket_name":"rivus-file-cache-clover-
pciprod","location":"location","project_id":"clover-pciprod"},"type":"gcs_bucket"},"severity":
"INFO","timestamp":"2020-04-08T23:35:26.171189525Z"}
```


Table 523. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**principalEmail**
Event Category	**methodName**
Logsource Time	**callerIp**
Username	**serviceName**
Source IP	**timestamp**

Google Cloud Platform - Cloud DNS

The IBM QRadar DSM for Google Cloud Platform - Cloud DNS collects JSON events from a Google Cloud DNS service.

To integrate Google Cloud Platform - Cloud DNS with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - GoogleCloudDNS DSM RPM
   - DSM Common RPM
   - GoogleCloudPubSub protocol RPM
   - GoogleCommon protocol RPM
   - Protocol Common RPM
2. Configure your Google Cloud Platform - Cloud DNS service to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a log source for Google Cloud Platform - Cloud DNS on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Google Cloud Platform - Cloud DNS DSM specifications

When you configure Google Cloud Platform - Cloud DNS, understanding the specifications for the Google Cloud Platform - Cloud DNS DSM can help ensure a successful integration. For example, knowing what the supported services of Google Cloud Platform - Cloud DNS are before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Google Cloud Platform - Cloud DNS DSM.

Table 524. Google Cloud Platform - Cloud DNS DSM specifications

Specification	**Value**
Manufacturer	Google
DSM name	Google Cloud Platform - Cloud DNS
RPM file name	DSM-*GoogleCloudDNS*-7.4-*QRadar_version-build_number*.noarch.rpm
Supported services	Google Cloud DNS
Protocol	Google Cloud Pub/Sub Syslog
Event format	JSON
Recorded event types	Cloud DNS
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Google Cloud Platform - Cloud DNS documentation (https://cloud.google.com/dns/docs/overview)

Configuring Google Cloud Platform - Cloud DNS to communicate with QRadar

Before you can add a log source in IBM QRadar, you must set up a functioning Pub/Sub system on your Google Cloud console.

Procedure

1. Create a Google account. For more information, see Create a Google Account (https://support.google.com/accounts/answer/27441?hl=en).
2. Set up a Pub/Sub system on your Google Cloud console. For more information, see Quickstart: building a functioning Pub/Sub system (https://cloud.google.com/pubsub/docs/quickstart-py-mac).

   Important: When you create service account credentials on the Google Cloud platform, use the following service account credentials:

```
{
  "type": "service_account",
  "project_id": "<project_id>",
  "private_key_id": "<private_key_id>",
  "private_key": “<private_key>",
  "client_email": "<client_email>",
  "client_id": "111111111111111111",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "< client_x509_cert_url >"
}
```

What to do next

Add a log source in QRadar. For more information, see Google Cloud Pub/Sub protocol log source parameters for Google Cloud Platform - Cloud DNS.

Google Cloud Pub/Sub protocol log source parameters for Google Cloud Platform - Cloud DNS

If QRadar does not automatically detect the log source, add a Google Cloud Platform - Cloud DNS log source on the QRadar Console by using the Google Cloud Pub/Sub protocol.

When you use the Google Cloud Pub/Sub protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Google Cloud Pub/Sub events from Google Cloud DNS Service:

Table 525. Google Cloud Pub/Sub protocol log source parameters for the Google Cloud Platform - Cloud DNS DSM

Parameter	Value
Log Source type	Google Cloud Platform - Cloud DNS
Protocol Configuration	Google Pub/Sub Protocol
Log Source Identifier	Use the IP address as a identifier for events from your Google Cloud DNS Service. The log source identifier must be a unique value.

For a complete list of Google Cloud Pub/Sub protocol parameters and their values, see Google Cloud Pub/Sub protocol configuration options.

Related tasks

Adding a log source

Google Cloud Platform - Cloud DNS sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Google Cloud Audit Logs sample message when you use the Google Cloud Pub/Sub protocol: list of objects retrieved

The following sample event message shows the retrieval of a list of objects that match the criteria that are provided. This retrieval is the result of an action that was taken by Google Cloud Storage.


```
{"insertId":"1es1wwue2wo69","jsonPayload":
{"authAnswer":true,"destinationIP":"10.239.32.109","protocol":"UDP","queryName":"qradar74.google
cloud.integrationtesting.net.","queryType":"AAAA","responseCode":"NOERROR","serverLatency":0,"so
urceIP":"10.194.97.4","structuredRdata":[]},"logName":"projects/qradar-iteam-262212/logs/
dns.googleapis.com%2Fdns_queries","receiveTimestamp":"2022-06-09T20:03:20.12015449Z","resource":
{"labels":{"location":"global","project_id":"qradar-
iteam-262212","source_type":"internet","target_name":"googlecloud-integrationtesting-
net","target_type":"public-
zone"},"type":"dns_query"},"severity":"INFO","timestamp":"2022-06-09T20:03:19.792706324Z"}
```


Table 526. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**queryType** + **responseCode**
Event Category	The value in QRadar is **GoogleCloudDNS**, which is the name of the service.
Logsource Time	**timestamp**
Destination IP	**destinationIP**
Source IP	**sourceIP**

Google Cloud Platform Firewall

The IBM QRadar DSM for Google Cloud Platform Firewall collects Google Cloud Pub/Sub events from a Google Cloud Platform Firewall service.

To integrate Google Cloud Platform Firewall with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Google Cloud Firewall Platform DSM RPM
   - Protocol GoogleCloudPubSub RPM
   - Protocol GoogleCommon RPM
2. Configure your Google Cloud Platform Firewall service to send events to QRadar. For more information, see Configuring Google Cloud Platform Firewall to communicate with QRadar.
3. Add a Google Cloud Platform Firewall log source on the QRadar Console. For more information, see Google Cloud Pub/Sub log source parameters for Google Cloud Platform Firewall.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Google Cloud Platform Firewall DSM specifications

When you configure the Google Cloud Platform Firewall DSM, understanding the specifications for the Google Cloud Platform Firewall DSM can help ensure a successful integration. For example, knowing what protocol to use for Google Cloud Platform Firewall before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Google Cloud Platform Firewall DSM.

Table 527. Google Cloud Platform Firewall DSM specifications

Specification	**Value**
Manufacturer	Google
DSM name	Google Cloud Platform Firewall
RPM file name	DSM-*GoogleCloudPlatformFirewall-QRadar_ version-build_number*.noarch.rpm
Protocol	Google Cloud Pub Sub
Event format	JSON
Recorded event types	Firewall Allow, Firewall Deny
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Google Cloud Firewall Rules Logging overview documentation (https://cloud.google.com/vpc/docs/firewall-rules-logging

Configuring Google Cloud Platform Firewall to communicate with QRadar

Before you can add a log source in IBM QRadar, you must set up a functioning Pub/Sub system on your Google Cloud console.

Procedure

1. Create a Google account. For more information, see Create a Google Account (https://support.google.com/accounts/answer/27441?hl=en).
2. Set up a Pub/Sub system on your Google Cloud console. For more information, see Quickstart: building a functioning Pub/Sub system (https://cloud.google.com/pubsub/docs/quickstart-py-mac).

   Important: When you create service account credentials on the Google Cloud platform, use the following service account credentials:

```
{
  "type": "service_account",
  "project_id": "<project_id>",
  "private_key_id": "<private_key_id>",
  "private_key": “<private_key>",
  "client_email": "<client_email>",
  "client_id": "111111111111111111",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "< client_x509_cert_url >"
}
```

What to do next

Add a log source in QRadar. For more information, see Google Cloud Pub/Sub log source parameters for Google Cloud Platform Firewall.

Google Cloud Pub/Sub log source parameters for Google Cloud Platform Firewall

If QRadar does not automatically detect the log source, add a Google Cloud Platform Firewall log source on the QRadar Console by using the Google Cloud Pub/Sub protocol.

When using the Google Cloud Pub/Sub protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Google Cloud Pub/Sub events from Google Cloud Platform Firewall:

Table 528. Google Cloud Pub/Sub log source parameters for the Google Cloud Platform Firewall DSM

Parameter	Value
Log Source type	Google Cloud Platform Firewall
Protocol Configuration	Google Cloud Pub/Sub
Log Source Identifier	Use the IP address as an identifier for events from your Google Cloud Platform Firewall service. The log source identifier must be a unique value.

For a complete list of Google Cloud Pub/Sub protocol parameters and their values, see Google Cloud Pub/Sub protocol configuration options.

Related tasks

Adding a log source

Sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Google Cloud Platform Firewall sample message when you use the Google Cloud Pub/Sub protocol

The following sample event message shows that traffic is allowed by Google Cloud Platform Firewall.


```
{"insertId":"a11aaaa1aa1aa1","jsonPayload":{"remote_location":{"country":"country","continent":
"continent"},"instance":{"project_id":"qradar-gcp-blog-demo","region":"country","zone":"country-
c","vm_name":
"instance-1"},"disposition":"ALLOWED","vpc":{"subnetwork_name":"qradar-a11aaaa1aa1aa1-1",
"project_id":"qradar-gcp-blog-demo","vpc_name":"qradar-a11aaaa1aa1aa1-1"},"rule_details":
{"reference":
"network:qradar-a11aaaa1aa1aa1-1/firewall:allow-
ssh","priority":65534,"direction":"INGRESS","ip_port_info":
[{"port_range":["22"],"ip_protocol":"TCP"}],"source_range":["0.0.0.0/0"],"action":"ALLOW"},
"connection":{"protocol":6,"dest_port":22,
"dest_ip":"10.128.0.2","src_port":61572,
"src_ip":"10.52.43.69"}},"resource":{"type":"gce_subnetwork","labels":{"project_id":
"qradar-gcp-blog-demo","subnetwork_id":"8495198078164383457","subnetwork_name":"qradar-
a11aaaa1aa1aa1-1",
"location":"country-c"}},"timestamp":"2020-08-19T22:01:42.473623155Z","logName":
"projects/qradar-gcp-blog-demo/logs/
compute.googleapis.com%2Ffirewall","receiveTimestamp":"2020-08-19T22:
01:50.856989345Z"}
```



```
{"insertId":"a11aaaa1aa1aa1","jsonPayload":{"remote_location":
{"country":"country","continent":"continent"},"instance":{"project_id":"qradar-gcp-blog-
```

```
demo","region":"country","zone":"country-
c","vm_name":"instance-1"},"disposition":"ALLOWED","vpc":{"subnetwork_name":"qradar-
a11aaaa1aa1aa1-1","project_id":"qradar-gcp-blog-demo","vpc_name":"qradar-
a11aaaa1aa1aa1-1"},"rule_details":{"reference""network:qradar-a11aaaa1aa1aa1-1/firewall:allow-
ssh","priority":65534,"direction":"INGRESS","ip_port_info":[{"port_range":
["22"],"ip_protocol":"TCP"}],"source_range":["0.0.0.0/0"],"action":"ALLOW"},"connection":
{"protocol":6,"dest_port":22,"dest_ip":"10.128.0.2","src_port":61572,"src_ip":"10.52.43.69"}},"r
esource":{"type":"gce_subnetwork","labels":{"project_id""qradar-gcp-blog-
demo","subnetwork_id":"8495198078164383457","subnetwork_name":"qradar-
a11aaaa1aa1aa1-1","location":"country-
c"}},"timestamp":"2020-08-19T22:01:42.473623155Z","logName":"projects/qradar-gcp-blog-demo/logs/
compute.googleapis.com%2Ffirewall","receiveTimestamp":"2020-08-19T22:01:50.856989345Z"}
```


Table 529. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**disposition**
Logsource Time	**timestamp**
Source IP	**connection** + **src_ip**
Source Port	**connection** + **src_port**
Destination IP	**connection** + **dest_ip**
Destination Port	**connection** + **dest_port**

Google G Suite Activity Reports

The IBM QRadar DSM for Google G Suite Activity Reports receives JSON events from the Google G Suite Activity Reports API.

Important: Google G Suite Activity Reports is supported in QRadar 7.3.2.6, build number 20191022133252 or later.

To integrate Google G Suite Activity Reports with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - Google Common RPM
   - Google G Suite Activity Reports REST API protocol RPM
   - Google G Suite Activity Reports DSM RPM
2. Configure your Google G Suite Activity Reports device to send events to QRadar. For more information, see “Configuring Google G Suite Activity Reports to communicate with QRadar” on page 863.
3. Add a Google G Suites Activity Reports log source on the QRadar Console. For more information about configuring the log source, see “Google G Suite Activity Reports log source parameters” on page 866.

Related tasks

“Adding a DSM” on page 4

Related information

t_logsource_add.dita#AddingALogSource

Google G Suite Activity Reports DSM specifications

When you configure Google G Suite Activity Reports, understanding the specifications for the Google G Suite Activity Reports DSM can help ensure a successful integration. For example, knowing what protocol to use before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Google G Suite Activity Reports DSM.

Table 530. Google G Suite Activity Reports DSM specifications	
Specification	**Value**
Manufacturer	Google
DSM name	Google G Suite Activity Reports
RPM file name	DSM-*GoogleGSuiteActivityReports-QRadar_version-build_number*.noarch.rpm
Protocol	Google G Suite Activity Reports REST API
Event format	JSON
Recorded event types	Admin, drive, login, user accounts
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Google G Suite Admin SDK Reports API (https://developers.google.com/admin-sdk/reports/v1/get-start/getting-started)

Related concepts

"Google G Suite Activity Reports" on page 862

The IBM QRadar DSM for Google G Suite Activity Reports receives JSON events from the Google G Suite Activity Reports API.

Configuring Google G Suite Activity Reports to communicate with QRadar

Before you can add a log source in QRadar, you must assign a role to a user, create a custom role with reports access, create a service account and grant API access to a service account in Google G Suite.

You must be a Google administrator with the ability to manage users. If you do not have access, contact your Google administrator.

Assigning a role to a user

Procedure

1. Log in to the Google Admin console (https://admin.google.com), and then click `Users` to access the **Users** page.

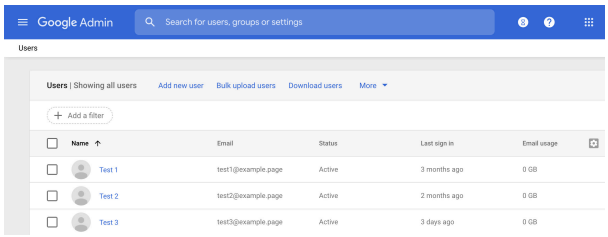


Figure 40. Google Admin users

Picture: ©2018 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

2. Click the name of the user that you want to grant access to.
3. Click in the **Admin roles and privileges** section to open the **Admin roles and privileges** page, and then click **Edit** to assign a role that includes reports access for the selected user.

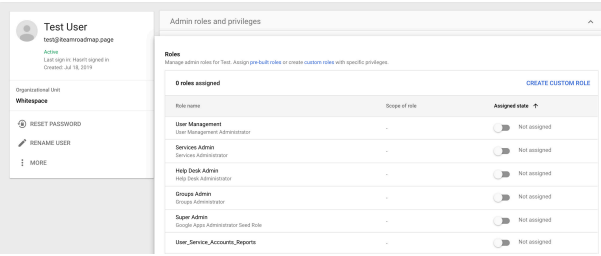


Figure 41. Admin roles and privileges

Picture: ©2018 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

4. Optional: If the **Super Admin** role was not used in Step 3, create a new role that has reports access. By default, the **Super Admin** role has this privilege.
   a) Click **CREATE CUSTOM ROLE**.
   b) On the **Admin roles** page, click **CREATE A NEW ROLE**.

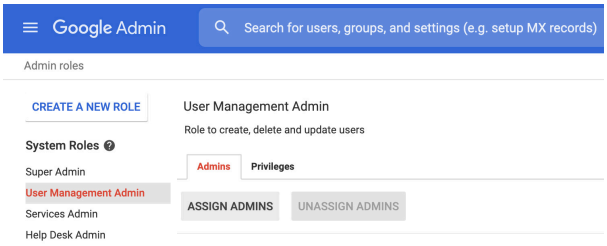


Figure 42. Create a new role

Picture: ©2018 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

   c) On the **Privileges** tab, select the **Reports** check box, and then click **Save**.

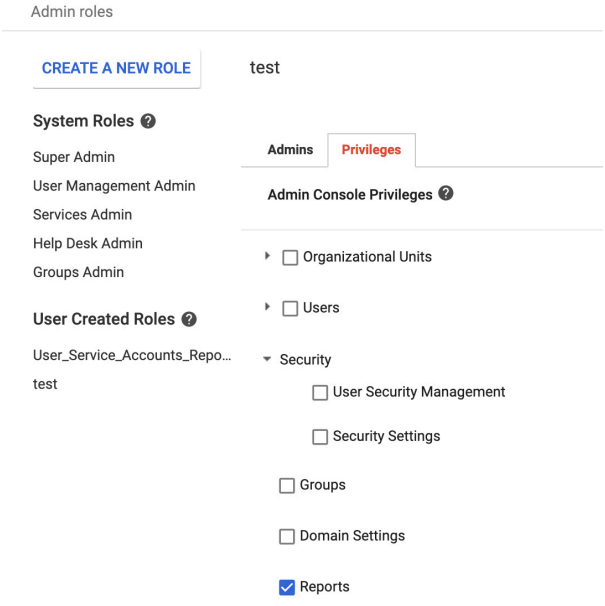


Figure 43. New role privileges

Picture: ©2018 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

This role appears in the roles section as an option when you assign a role to a user.

Creating a service account with viewer access

Procedure

1. On the Google Cloud Platform (GCP) APIs & Services page (https://console.cloud.google.com/apis/dashboard), click **Credentials**.
2. From the navigation menu, select **Credentials**.
3. Click **+CREATE CREDENTIALS** > **Service account**.
4. In the **Service account name** field, type a name for the service account, then click **CREATE AND CONTINUE**.
5. From the **Select a role** list, select **Actions Viewer**, then click **CONTINUE**.
6. In the **Service account user role** field, type the name for your user.
7. In the **Service account admins role** field, type the name for your user.
8. Click **DONE**.
9. In the **Service Accounts** section, select the service account that you created.
10. In the **API Keys** section, click **Add Key**.

    You need the contents of the key for the **Service Account Credentials** parameter value when you add a log source in QRadar.

Granting API client access to a service account

Procedure

1. On the Google Admin page (https://admin.google.com/ac/home?hl=en), from the navigation menu, select **Security** > **API Controls**.
2. In the Domain wide delegation section, click **MANAGE DOMAIN WIDE DELEGATION**

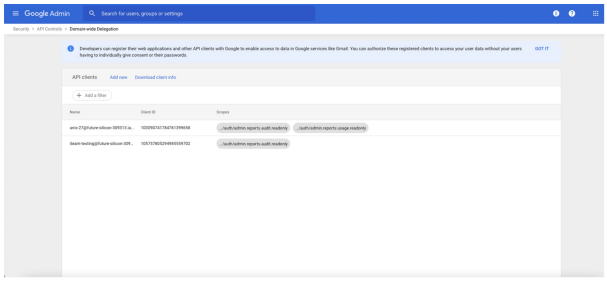


Figure 44. Manage Domain-wide Deleglion

Picture: ©2021 Google LLC, used with permission. Google and the Google logo are registered trademarks of Google LLC.

3. To add a new client ID, click **Add new**.
4. In the **Client ID** field, enter the value for the API key that you added when you created a service account.
5. In the **OAuth Scopes (comma-delimited)** field, type `https://www.googleapis.com/auth/admin.reports.audit.readonly`.
6. Click **AUTHORIZE**.

What to do next

Add a Google G Suite Activity Reports log source on the QRadar Console by using the Google G Suite Activity Reports REST API. For more information, see “Google G Suite Activity Reports log source parameters” on page 866.

Google G Suite Activity Reports log source parameters

When you add a Google G Suite Activity Reports log source on the QRadar Console by using the Google G Suite Activity Reports REST API, you must use specific parameters.

The following table describes the parameters that require specific values to collect Google G Suite Activity Reports events from Google G Suite.

Table 531. Google G Suite Activity Reports REST API protocol log source parameters for the Google G Suite Activity Reports DSM

Parameter	Value
Log Source type	Google G Suite Activity Reports
Protocol Type	Google G Suite Activity Reports REST API
Service Account Credentials	Authorizes access to Google's APIs for retrieving the events. Copy and paste the contents of the JSON formatted file that you downloaded when you completed "Configuring Google G Suite Activity Reports to communicate with QRadar" on page 863.
Delegated User Account Email	The Google user account that has report privileges.

For a complete list of Google G Suite Activity Reports REST API protocol parameters and their values, see Google G Suite Activity Reports REST API protocol options.

Related concepts

"Google G Suite Activity Reports" on page 862
The IBM QRadar DSM for Google G Suite Activity Reports receives JSON events from the Google G Suite Activity Reports API.

Related tasks

"Adding a DSM" on page 4

Google G Suite Activity Reports sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides sample event messages when you use the Google G Suite Activity Reports REST API protocol for the Google G Suite Activity Reports DSM.

Table 532. Google G Suite Activity Reports sample message supported by Google G Suite Activity Reports.

Event name	Low-level category	Sample log message
Login_success	User login success	{"actor"{"email":"xxx@xxxxxx.xxx","profileId": "xxxxxxxxxxxxxxxx"},"etag":"\"3InmzELrmhMYx7Wvxlz3Nl lOopE/m2bw4uWdXlHjVQ4P1Az5ED46P4w\"","events":[{"name ":"login_success","parameters":[{"name":"login_type", "value":"google_password"},{"multiValue":["password"] ,"name":"login_challenge_method"},{"boolValue":false, "name":"is_suspicious"}],"type":"login"}],"id":{"appl icationName":"login","customerId":"xxxxxxx","time":"2 019-05-22T20:03:42.047Z","uniqueQualifier":"239837479 183"},"ipAddress":"<IP_address>","kind":"admin#report s#activity"} {"actor"{"email":"xxx@xxxxxx.xxx","profileId":"xxxxxx xxxxxxxxxxx"},"etag":"\"3InmzELrmhMYx7Wvxlz3NllOopE/ m2bw4uWdXlHjVQ4P1Az5ED46P4w\"","events": [{"name":"login_success","parameters": [{"name":"login_type","value":"google_password"}, {"multiValue": ["password"],"name":"login_challenge_method"}, {"boolValue":false,"name":"is_suspicious"}],"type":"l ogin"}],"id": {"applicationName":"login","customerId":"xxxxxxx","ti me":"2019-05-22T20:03:42.047Z","uniqueQualifier":"239 837479183"},"ipAddress":"<IP_address>","kind":"admin# reports#activity"}
edit	Update Activity Succeeded	{"actor"{"email":"xxx@xxxxxx.xxx","profileId" :"xxxxxxxxxxxxxxxxx"},"etag":"\"3InmzELrmhMYx7Wvxlz3N l lOopE/9tDfe88oL_ydXHALurRrMoRrLH4\"","events": [{"name" :"edit","parameters": [{"boolValue":true,"name":"primar y_event"},{"boolValue":true,"name":"billable"}, {"name" :"doc_id","value":"1rLEPjwJTitDL08LKhU0QlGxWE7yzNWRiC V rRQ0KfN9Y"},{"name":"doc_type","value":"document"},{" name":"doc_title","value":"Untitleddocument"},{"name" :"visibility","value":"private"},{"name":"owner","va lue":"xxx@xxxxxx.xxx"},{"boolValue":false,"name":"ow ner_is_team_drive"}],"type":"access"}],"id":{"applic ationName":"drive","customerId":"xxxxxxx","time":"20 19-0603T16:38:11.461Z","uniqueQualifier":"6949699212 699371308"},"ipAddress":"<IP_address>","kind":"admi n#reports#activity"

Troubleshooting Google G Suite Activity Reports

To resolve issues with the Google G Suite Activity Reports DSM, use the troubleshooting and support information. Errors can be found by using the protocol testing tools in the QRadar Log Source Management app.

General troubleshooting

The following steps apply to all user input. The general troubleshooting procedure contains the first steps to follow for any errors with the Google G Suite Activity Reports REST API protocol. Many of the errors related to the Google G Suite Activity Reports REST API protocol can be solved with these basic steps.

1. Check for any spelling mistakes or unnecessary characters in the **User Account** field.
2. Reenter all fields.

3. Create a service account credential file and enter it into the **Service Account Credentials** field.

For more information, see:

- "Invalid private keys" on page 868
- "Authorization errors" on page 868
- "Invalid email or username errors" on page 869
- "Invalid JSON formatting" on page 869
- "Network errors" on page 869
- "Google G Suite Activity Reports FAQ" on page 870

Invalid private keys

Symptoms

Error: "An I/O operation failed or was interrupted. For further details, see the "Raw Error Message" and the additional messages"

Error: "List of potentially invalid parameters: Service Account Credentials"

Error: "Unexpected exception reading PKCS data"

Causes

These errors indicate that the Service Account Credentials contain an invalid private key value. This error is commonly caused by issues with the value that is entered into the **Service Account** field.

Resolving the problem

Follow these steps to resolve your invalid private key error.

1. Check for any spelling mistakes or unnecessary characters in the **User Account** field.
2. Reenter all fields.
3. Create a service account credential file and enter it into the **Service Account Credentials** field.

Authorization errors

Symptoms

Error: "An I/O operation failed or was interrupted. For further details see the "Raw Error Message" and the additional messages"

Error: "List of potentially invalid parameters : Service Account Credentials"

Error: "Client is unauthorized to retrieve access tokens using this method, or client not authorized for any of the scopes requested."

Causes

These errors relate to service account authorization. Authorization issues commonly occur when required permissions are not provided to the service account or user account. The service account needs domain-wide read access. The user account requires reports access.

Resolving the problem

Follow these steps to resolve your authorization error.

1. Verify that the service account is correctly configured with domain-wide services.
2. Ensure that the user account has a role with reports access.

Invalid email or username errors

Symptoms

Error: “An I/O operation failed or was interrupted.”

Error: "error_description" : "Not a valid email or user ID."

Error: “List of potentially invalid parameters : User Account and Service Account Credentials”

Causes

These errors usually occur if the provided user account doesn’t exist, or the **client_email** field within the service account credentials is invalid. A common reason for this error is typographical errors in the user account field.

Resolving the problem

Ensure that the user account exists.

Ensure that the **Delegated User Account Email** account is the Google user account that has reports privileges and not the **client_email property** value in the `Service Account Credentials` JSON file.

Invalid JSON formatting

Symptoms

Error: “Service Account Credentials don't appear to be in a valid json format.”

Error: “An error occurred indicating a json parsing problem. Usually used when non-well-formed content (content that does not conform to JSON syntax as per specification) is encountered. For further details see the "Raw Error Message" and the additional messages”

Error: “Invalid UTF-8 start byte”

Error: “An error occurred indicating a json parsing problem. Usually used when non-well-formed content (content that does not conform to JSON syntax as per specification) is encountered. For further details see the "Raw Error Message" and the additional messages”

Causes

These errors occur when the service account credentials are not in a valid JSON format.

Resolving the problem

Follow these steps to resolve your invalid JSON formatting error.

1. Verify that the service account credentials are in a valid JSON format.

   Tip: An online JSON formatter can identify problems with the JSON format.
2. If the error persists, generate a new service account credentials key.

Network errors

Symptoms

Error: “Error obtaining sample events :: Network is unreachable (connect failed”

Causes

IBM QRadar cannot connect to Google servers to receive Google G Suite Activity Reports events. This error can be related to many network issues, including proxy issues.

Resolving the problem

Follow these steps to resolve your network error.

1. Ensure that the target event collector has access to the internet.
2. Ensure that there are no network configurations that are blocking access to Google Admin. Contact your network administrator if you are unable to connect to Google Admin.
3. Check that the network can access the following hosts:
   - googleapis.com:443
   - oauth2.googleapis.com:443

Google G Suite Activity Reports FAQ

Use these frequently asked questions and answers to help you understand Google G Suite Activity Reports.

- "Why does the service account need domain-wide read access?" on page 870
- "Why does the user account need reports access?" on page 870
- "Why does Google G Suite Activity Reports use service accounts to authorize access instead of other authentication methods?" on page 870
- "What types of events are collected by the Google G Suite Activity Reports API?" on page 870
- "Why do you need a user account if you have service account credentials?" on page 871
- "What does a standard Service Account Credentials file look like?" on page 871
- "What host and ports are used by this protocol?" on page 871
- "Are there any alternatives to the officially documented authorization method?" on page 871

Why does the service account need domain-wide read access?

The domain-wide read access allows the service account to impersonate a user. Without domain-wide read access, the service account is unable to obtain reports access.

Why does the user account need reports access?

The events that the Google Activity Reports protocol retrieves all come from the reports function of Google Admin. This access is required to retrieve any events from the Google Activity Reports API.

Why does Google G Suite Activity Reports use service accounts to authorize access instead of other authentication methods?

The following document contains a section that is named "Service accounts," which explains in detail the difference between service accounts and other methods of authorization. Service accounts are different from other methods of authorization because they can act without requiring user consent. Service accounts are intended for server to server communications. For more information, see Using OAuth 2.0 to Access Google APIs (https://developers.google.com/identity/protocols/OAuth2).

What types of events are collected by the Google G Suite Activity Reports API?

This protocol collects only admin, user accounts, login, and drive events. These events are detailed in the reports section of the G Suite Admin SDK Activities list (https://developers.google.com/admin-sdk/reports/v1/reference/activities/list).

Why do you need a user account if you have service account credentials?

For a service account to have access to the reports API it needs to impersonate an existing user. For more information, see domain-wide delegation (https://developers.google.com/admin-sdk/directory/v1/guides/delegation).

What does a standard Service Account Credentials file look like?

In a real Service Account Credentials file, the empty fields are populated with values that are related to the service account.

```
{
"type": "service_account",
"project_id": “”,
"private_key_id": "",
"private_key": "-----BEGIN PRIVATE KEY-----\n=\n-----END PRIVATE KEY-----\n",
"client_email": "",
"client_id": "",
"auth_uri": "https://accounts.google.com/o/oauth2/auth",
"token_uri": "https://oauth2.googleapis.com/token",
"auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
"client_x509_cert_url": ""
}
```

What host and ports are used by this protocol?

The following hosts and ports are used by this protocol:

Host	Description
oauth2.googleapis.com:443	Authentication server used by Google to authenticate API access.
googleapis.com:443	Googles API server. Used to access the Google G Suite Activity Reports API.

Are there any alternatives to the officially documented authorization method?

The Google G Suite Activity Reports API requires both a user account and a service account. Due to these restrictions, it is not possible to delegate the required permissions to just the service account or just the user account. If the offered authorization method is not satisfactory, contact IBM Support.

(Back to top)

Chapter 73. Great Bay Beacon

The Great Bay Beacon DSM for IBM QRadar supports syslog alerts from the Great Bay Beacon Endpoint Profiler.

QRadar records all relevant Endpoint security events. Before you can integrate Great Bay Beacon with QRadar, you must configure your Great Bay Beacon Endpoint Profiler to forward syslog event messages to QRadar.

Configuring syslog for Great Bay Beacon

You can configure your Great Bay Beacon Endpoint Profiler to forward syslog events.

Procedure

1. Log in to your Great Bay Beacon Endpoint Profiler.
2. To create an event, select **Configuration** > **Events** > **Create Events**.

   A list of currently configured events is displayed.
3. From the **Event Delivery Method** pane, select the **Syslog** check box.
4. To apply your changes, select **Configuration Apply Changes** > **Update Modules**.
5. Repeat "Configuring syslog for Great Bay Beacon" on page 873 to configure all of the events that you want to monitor in IBM QRadar.
6. Configure QRadar as an external log source for your Great Bay Beacon Endpoint Profiler.

   For information on configuring QRadar as an external log source, see the *Great Bay Beacon Endpoint Profiler Configuration Guide*.

   You are now ready to configure the log source in QRadar.

Syslog log source parameters for Great Bay Beacon

If QRadar does not automatically detect the log source, add a Great Bay Beacon log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Great Bay Beacon:

Table 533. Syslog log source parameters for the Great Bay Beacon DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Great Bay Beacon
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Great Bay Beacon appliance.

Related tasks

"Adding a log source" on page 5

Chapter 74. H3C Technologies

IBM QRadar accepts events from a range of H3C Technologies DSMs.

H3C Comware Platform

The IBM QRadar DSM for the H3C Comware Platform collects events from a number of network devices from H3C Technologies. QRadar supports H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices.

The following table describes the specifications for the H3C Comware Platform DSM:

Table 534. H3C Comware Platform DSM specifications

Specification	**Value**
Manufacturer	H3C Technologies Co., Limited
DSM name	H3C Comware Platform, H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices.
RPM file name	`DSM-H3CComware-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V7
Protocol	Syslog
Event format	NVP
Recorded event types	System
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	H3C Technologies (http://www.h3c.com)

To integrate H3C Comware Platform, H3C Switches, H3C Routers, H3C Wireless LAN Devices, or H3C IP Security Devices with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the H3C Comware Platform DSM RPM from the IBM Support Website onto your QRadar Console.
2. Configure your H3C Comware Platform router or device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a H3C Comware Platform log source on the QRadar Console. The following table describes the parameters that require specific values for H3C Comware Platform event collection:

   Table 535. H3C Comware Platform log source parameters

Parameter	**Value**
Log Source type	H3C Comware Platform
Protocol Configuration	Syslog

The following table provides a sample syslog event message for the H3C Comware Platform DSM:

Table 536. H3C Comware Platform sample syslog message		
Event name	**Low level category**	**Sample log message**
A user's AAA request is rejected	AAA Session Denied	<188>Jun 14 17:11:11 2013 HP %%10AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain =domain1-Service=login- UserName=cwf@system; AAA is failed. <188>Jun 14 17:11:11 2013 HP %%10AAA/5/AAA_FAILURE: -AAAType=AUTHOR- AAADomain=domain1- Service=login- UserName=cwf@system; AAA is failed.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring H3C Comware Platform to communicate with QRadar

To collect H3C Comware Platform events, enable syslog settings and configure a log host. H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices are supported by QRadar.

Procedure

1. Log in to the **command line** interface by using the console port, or by using Telnet or SSH.

   For more information about login methods, see the *Logging into the CLI* section in the configuration guide for your H3C devices.
2. To access the system view, type the `<system_name> system-view` command.
3. To enable the syslog settings, type the following commands in the order that they are listed.
   a. `info-center source default loghost deny`
   b. `info-center source AAA loghost level informational`
   c. `info-center source ACL loghost level informational`
   d. `info-center source FIPS loghost level informational`
   e. `info-center source HTTPD loghost level informational`
   f. `info-center source IKE loghost level informational`
   g. `info-center source IPSEC loghost level informational`
   h. `info-center source LOGIN loghost level informational`
   i. `info-center source LS loghost level informational`
   j. `info-center source PKI loghost level informational`
   k. `info-center source PORTSEC loghost level informational`
   l. `info-center source PWDCTL loghost level informational`
   m. `info-center source RADIUS loghost level informational`
   n. `info-center source SHELL loghost level informational`
   o. `info-center source SNMP loghost level informational`
   p. `info-center source SSHS loghost level informational`
   q. `info-center source TACACS loghost level informational`
   r. `info-center loghost <QRadar Event Collector IP> 514`
4. To exit the system view, type the `quit <system_name>` command.

Chapter 75. HBGary Active Defense

The HBGary Active Defense DSM for IBM QRadar accepts several event types that are forwarded from HBGary Active Defense devices, such as access, system, system configuration, and policy events.

Events from Active Defense are forwarded in the Log Event Extended Format (LEEF) to QRadar using syslog. Before you can configure QRadar, you must configure a route for your HBGary Active Defense device to forward events to a syslog destination.

Configuring HBGary Active Defense

You can configure a route for syslog events in Active Defense for QRadar.

Procedure

1. Log in to the Active Defense Management Console.
2. From the navigation menu, select **Settings** > **Alerts**.
3. Click **Add Route**.
4. In the **Route Name** field, type a name for the syslog route you are adding to Active Defense.
5. From the **Route Type** list, select **LEEF (Q1 Labs)**.
6. In the **Settings** pane, configure the following values:
   - **Host** - Type the IP address or hostname for your QRadar Console or Event Collector.
   - **Port** - Type 514 as the port number.
7. In the **Events** pane, select any events that you want to forward to QRadar.
8. Click **OK** to save your configuration changes.

   The Active Defense device configuration is complete. You are now ready to configure a log source in QRadar. For more information on configuring a route in Active Defense, see your *HBGary Active Defense User Guide*.

Syslog log source parameters for HBGary Active Defense

If QRadar does not automatically detect the log source, add a HBGary Active Defense log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from HBGary Active Defense:

Table 537. Syslog log source parameters for the HBGary Active Defense DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	HBGary Active Defense
Protocol Configuration	Syslog

Table 537. Syslog log source parameters for the HBGary Active Defense DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for your HBGary Active Defense device. The IP address or host name identifies your HBGary Active Defense device as a unique event source in QRadar.

Related tasks

“Adding a log source” on page 5

Chapter 76. HCL BigFix (formerly known as IBM BigFix)

If IBM QRadar does not automatically detect the log source, add an HCL BigFix log source on the QRadar Console by using the IBM BigFix SOAP protocol.

Important: HCL BigFix is formerly known as IBM BigFix. The name remains as IBM BigFix in QRadar.

When you use the IBM BigFix SOAP protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect IBM BigFix SOAP events from HCL BigFix:

Table 538. IBM BigFix SOAP log source parameters for the HCL BigFix DSM

Parameter	Value
Log Source type	IBM BigFix
Protocol Configuration	HCL BigFix SOAP
Log Source Identifier	Type the IP address or host name for your HCL BigFix appliance. The IP address or host name identifies your HCL BigFix as a unique event source in QRadar.
Port	Type the port number that is used to connect to HCL BigFix by using the SOAP API. By default, port 80 is the port number for communicating with HCL BigFix. If you are use HTTPS, you must update this field to the HTTPS port number for your network. Most configurations use port 443 for HTTPS communications.
Use HTTPS	Enable this option to connect by using HTTPS. If you enable this option, the host name or IP address you specify uses HTTPS to connect to your HCL BigFix. If a certificate is required to connect by using HTTPS, you must copy any certificates that are required by the QRadar Console or managed host to the following directory: `/opt/qradar/conf/trusted_certificates` QRadar support certificates with the following file extensions: `.crt`, `cert`, or `.der`. Copy any required certificates to the trusted certificates directory before you save and deploy your changes.
Username	Type the username that you use to access your HCL BigFix.
Password	Type the password that you use to access your HCL BigFix.
Confirm Password	Confirm the password that is required to access your HCL BigFix.

For a complete list of IBM BigFix SOAP protocol parameters and their values, see IBM BigFix SOAP protocol configuration options.

For more information about configuring QRadar to import HCL BigFix vulnerabilities assessment information, see the *IBM QRadar Vulnerability Assessment Configuration Guide*.

Related tasks

“Adding a log source” on page 5

Chapter 77. Honeycomb Lexicon File Integrity Monitor (FIM)

You can use the Honeycomb Lexicon File Integrity Monitor (FIM) DSM with IBM QRadar to collect detailed file integrity events from your network.

QRadar supports syslog events that are forwarded from Lexicon File Integrity Monitor installations that use Lexicon mesh v3.1 and later. The syslog events that are forwarded by Lexicon FIM are formatted as Log Event Extended Format (LEEF) events by the Lexicon mesh service.

To integrate Lexicon FIM events with QRadar, you must complete the following tasks:

1. On your Honeycomb installation, configure the Lexicon mesh service to generate syslog events in LEEF.
2. On your Honeycomb installation, configure any Lexicon FIM policies for your Honeycomb data collectors to forward FIM events to your QRadar Console or Event Collector.
3. On your QRadar Console, verify that a Lexicon FIM log source is created and that events are displayed on the **Log Activity** tab.
4. Optional. Ensure that no firewall rules block communication between your Honeycomb data collectors and the QRadar Console or Event Collector that is responsible for receiving events.

Supported Honeycomb FIM event types logged by QRadar

The Honeycomb FIM DSM for IBM QRadar can collect events from several event categories.

Each event category contains low-level events that describe the action that is taken within the event category. For example, file rename events might have a low-level category of either file rename successful or file rename failed.

The following list defines the event categories that are collected by QRadar for Honeycomb file integrity events:

- Baseline events
- Open file events
- Create file events
- Rename file events
- Modify file events
- Delete file events
- Move file events
- File attribute change events
- File ownership change events

QRadar can also collect Windows and other log files that are forwarded from Honeycomb Lexicon. However, any event that is not a file integrity event might require special processing by a custom log source type or a log source extension in QRadar.

Configuring the Lexicon mesh service

To collect events in a format that is compatible with IBM QRadar, you must configure your Lexicon mesh service to generate syslog events in LEEF.

Procedure

1. Log in to the Honeycomb LexCollect system that is configured as the dbContact system in your network deployment.

2. Locate the Honeycomb installation directory for the `installImage` directory.

   For example, `c:\Program Files\Honeycomb\installImage\data`.
3. Open the `mesh.properties` file.

   If your deployment does not contain Honeycomb LexCollect, you can edit `mesh.properties` manually.

   For example, `c:\Program Files\mesh`
4. To export syslog events in LEEF, edit the **formatter** field.

   For example, `formatter=leef`.
5. Save your changes.

   The mesh service is configured to output LEEF events. For information about the Lexicon mesh service, see your *Honeycomb documentation*.

Syslog log source parameters for Honeycomb Lexicon File Integrity Monitor

If QRadar does not automatically detect the log source, add a Honeycomb Lexicon File Integrity Monitor log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Honeycomb Lexicon File Integrity Monitor:

Table 539. Syslog log source parameters for the Honeycomb Lexicon File Integrity Monitor DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Honeycomb Lexicon File Integrity Monitor
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Honeycomb Lexicon FIM installation. The **Log Source Identifier** must be unique value.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.

Table 539. Syslog log source parameters for the Honeycomb Lexicon File Integrity Monitor DSM (continued)	
Parameter	**Value**
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related tasks

"Adding a log source" on page 5

Chapter 78. Hewlett Packard Enterprise

IBM QRadar can be integrated with several Hewlett Packard Enterprise (HPE) DSMs.

HPE Network Automation

The IBM QRadar DSM for HPE Network Automation collects events from HPE Network Automation software.

The following table describes the specifications for the HPE Network Automation DSM:

Table 540. HPE Network Automation DSM specifications

Specification	**Value**
Manufacturer	Hewlett Packard Enterprise
DSM name	HP Network Automation
RPM file name	`DSM-HPNetworkAutomation-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V10.11
Protocol	Syslog
Event format	LEEF
Recorded event types	All operational and configuration network events.
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Hewlett Packard Enterprise Network Automation (https://www.hpe.com/us/en/solutions/telecom-network-automation.html)

To integrate HPE Network Automation software with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the following RPMs from the IBM Support Website (https://www.ibm.com/support).
   - DSMCommon DSM RPM
   - HP Network Automation DSM RPM
2. Configure your HPE Network Automation software to send LEEF events to QRadar.
3. If QRadar does not automatically detect the log source, add an HPE Network Automation log source on the QRadar Console. The following table describes the parameters that require specific values for HPE Network Automation event collection:

Table 541. HPE Network Automation log source parameters

Parameter	**Value**
Log Source type	HP Network Automation
Protocol Configuration	Syslog

Table 541. HPE Network Automation log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	The IP address or host name of the device from where QRadar collects HP Network Automation events.

The following table shows a sample LEEF message from the HPE Network Automation DSM:

Table 542. HPE Network Automation sample message supported by the HPE Network Automation software		
Event name	**Low level category**	**Sample log message**
Device Snapshot	Information	LEEF:1.0|HP|Network Automation|v10|Device Snapshot| devTime=Wed Jul 06 08:26:45 UTC 2016 devTimeFormat=EEE MMM dd HH:mm:ss Z yyyy src=<Source_IP_address> eventId=11111111 usrName=UserName eventText=Snapshot of configuration taken LEEF:1.0|HP|Network Automation|v10| Device Snapshot|devTime=Wed Jul 06 08:26:45 UTC 2016 devTimeFormat=EEE MMM dd HH:mm:ss Z yyyy src=<Source_IP_address> eventId=11111111 usrName=UserName eventText=Snapshot of configuration taken

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring HPE Network Automation Software to communicate with QRadar

Configure HPE Network Automation Software to send LEEF events to IBM QRadar.

Before you begin

You must have administrator access to the HPE Network Automation Software user interface.

Procedure

1. Log in to the HPE Network Automation Software user interface.
2. In the **Admin** menu, select **Event Notification & Response Rules**.
3. Click **New Event Notification & Respone Rule**.
4. Configure the parameters for HPE Network Automation.

   The following table describes the parameter values to send LEEF events to QRadar:

Parameter	**Value**
Add Email and Event Rule named	You can use any string. For example, `QRadar_logs`.
To take this action	Select **Send Syslog Message** from the list.

Parameter	Value
When the following events occur	a. Select all of the events. b. Enable the **of any importance** button. c. To take action for For Policy No-Compliance events, enable the **for all policies** button.
Rule Status	Enable the **Active** button.
Syslog Hostname	QRadar host name or IP address.
Syslog Port	514
Syslog Message	`LEEF:1.0|HP|Network Automation|v10|$EventType$|devTime=$EventDate$ devTimeFormat=EEE MMM dd HH:mm:ss Z yyyy src=$IPAddress$ eventId=$EventID$ usrName=$EventUserName$ eventText=$EventText$` **Tip:** All event attributes are tab delimited. For example, devTime, devTimeFormat, and more. Copy the **Syslog Message** value into a text editor, and then verify that the attributes are tab delimited and remove any new line characters. The version number v10 in the LEEF header can be replaced with the exact version of your HPE Network Automation software. If you change any other components of the format string, events might not normalize or unknown events might occur.

5. Click **Save**.

HPE ProCurve

You can integrate an HPE ProCurve device with IBM QRadar to record all relevant HPE Procurve events using syslog.

About this task

Take the following steps to configure your HPE ProCurve device to forward syslog events to QRadar.

Procedure

1. Log into the HPE ProCurve device.
2. Type the following command to make global configuration level changes.

   `config`

   If successful, the CLI will change to the following prompt:

   `ProCurve(config)#`
3. Type the following command:

   `logging <syslog-ip-addr>`

   Where: <*syslog-ip-addr*> is the IP address of QRadar.
4. To exit config mode, press CTRL+Z.
5. Type the following command: `write mem` to save the current configuration to the startup configuration for your HPE ProCurve device.

   You are now ready to configure the log source in QRadar.

What to do next

Adding a log source

Syslog log source parameters for HPE ProCurve

If QRadar does not automatically detect the log source, add an HPE ProCurve log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from HPE ProCurve:

Table 543. Syslog log source parameters for the HPE ProCurve DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	HP ProCurve
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for your HPE ProCurve appliance.

Related tasks

"Adding a log source" on page 5

HPE Tandem

You can integrate an HPE Tandem device with IBM QRadar. An HPE Tandem device accepts SafeGuard Audit file events by using a log file protocol source.

About this task

A log file protocol source allows QRadar to retrieve archived log files from a remote host. The HPE Tandem DSM supports the bulk loading of log files by using the log file protocol source.

When you configure your HPE Tandem device to use the log file protocol, ensure that the hostname or IP address that is configured in the HPE Tandem device and in the Remote Host parameter are the same.

The SafeGuard Audit file names use the following format:

Annnnnnn

The single alphabet character A is followed by a seven-digit decimal integer nnnnnnn, which increments by 1 each time a name is generated in the same audit pool.

You are now ready to configure the log source and protocol in QRadar.

Procedure

1. From the **Log Source Type** list, select **HP Tandem**.
2. To configure the log file protocol, from the **Protocol Configuration** list, select **Log File**.
3. From the **Event Generator** list, select **HPTANDEM**

   Note: Your system must be running the current version of the log file protocol to integrate with an HPE Tandem device:

   For more information about HPE Tandem, see your vendor documentation.

For more information about configuring the Log File protocol in QRadar, see Log File protocol configuration options.

HPE Tandem sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

HPE Tandem sample message when you use the Syslog protocol

The following sample event message shows that permission to attempt the requested operation is denied.

```
HPTandemHostname=172.16.90.30    auditFileName=/store/tmp/AAAAAAAA.log
recordType=ZSFG_VAL_AUD_REC_PRIMARY    recordLength=436
auditNumber.auditNumber=BBBBBBBBBBBBBBBBBBB    timeReported=18 Sep 2012
22:32:28    timeReceived=18 Sep 2012 22:32:28
veracity=ZSFG_VAL_VER_TR    groupCount=0    operation=ZSFG_VAL_OPER_UPDATE
outcome=ZSFG_VAL_OUTCOME_DENIED    masterAuditNumber.auditNumber=BBBBBBBBBBBBBBBBBBB
subject.subjectType=151    subject.subjectUserNumber.userNumberGroup=255
subject.subjectUserNumber.userNumberMember=1    subject.subjectUsername=USERNAME
subject.creatorUserNumber.userNumberGroup=255    subject.creatorUserNumber.userNumberMember=1
subject.subjectCreatorName=SUPER.SUPERUSER    subject.subjectSystemNumber=1
subject.subjectSystemName=\TEST    subject.subjectAuthLocNumber=1
subject.subjectAuthLocName=\TEST    subject.subjectProcessName=\TEST.4,578
subject.subjectSsid.ssidOwner=    subject.subjectSsid.ssidNumber=8224
subject.subjectSsid.ssidVersion=8224    subject.subjectTerminalName=\TEST.$CCCCCC#DDDDDDD
auditCreator.subjectType=151    auditCreator.subjectUserNumber.userNumberGroup=255
auditCreator.subjectUserNumber.userNumberMember=255
auditCreator.subjectUsername=SUPER.SUPER    auditCreator.creatorUserNumber.userNumberGroup=255
auditCreator.creatorUserNumber.userNumberMember=255
auditCreator.subjectCreatorName=SUPER.SUPER    auditCreator.subjectSystemNumber=1
auditCreator.subjectSystemName=\TEST    auditCreator.subjectAuthLocNumber=1
auditCreator.subjectAuthLocName=\TEST    auditCreator.subjectProcessName=\TEST.$EEEE
,4,309    auditCreator.subjectSsid.ssidOwner=FFFFFF
auditCreator.subjectSsid.ssidNumber=94    auditCreator.subjectSsid.ssidVersion=18182
auditCreator.subjectTerminalName=$ZHOME    objectType.objectType=200
objectType.ownerIsRemote=701    objectType.ownerUserNumber.userNumberGroup=111
objectType.ownerUserNumber.userNumberMember=1    objectType.ownerUserName=GGG.HHHHHHH
objectType.objectName.type=200    objectType.objectName.objectName=$DATA.FTP.GETAPF3
```


```
HPTandemHostname=172.16.90.30    auditFileName=/store/tmp/AAAAAAAA.log
recordType=ZSFG_VAL_AUD_REC_PRIMARY    recordLength=436
auditNumber.auditNumber=BBBBBBBBBBBBBBBBBBB    timeReported=18 Sep 2012
22:32:28    timeReceived=18 Sep 2012 22:32:28
veracity=ZSFG_VAL_VER_TR    groupCount=0    operation=ZSFG_VAL_OPER_UPDATE
outcome=ZSFG_VAL_OUTCOME_DENIED    masterAuditNumber.auditNumber=BBBBBBBBBBBBBBBBBBB
subject.subjectType=151    subject.subjectUserNumber.userNumberGroup=255
subject.subjectUserNumber.userNumberMember=1    subject.subjectUsername=USERNAME
subject.creatorUserNumber.userNumberGroup=255
subject.creatorUserNumber.userNumberMember=1    subject.subjectCreatorName=SUPER.SUPERUSER
subject.subjectSystemNumber=1    subject.subjectSystemName=\TEST
subject.subjectAuthLocNumber=1    subject.subjectAuthLocName=\TEST
subject.subjectProcessName=\TEST.4,578    subject.subjectSsid.ssidOwner=
subject.subjectSsid.ssidNumber=8224    subject.subjectSsid.ssidVersion=8224
subject.subjectTerminalName=\TEST.$CCCCCC#DDDDDDD    auditCreator.subjectType=151
auditCreator.subjectUserNumber.userNumberGroup=255
auditCreator.subjectUserNumber.userNumberMember=255
auditCreator.subjectUsername=SUPER.SUPER
auditCreator.creatorUserNumber.userNumberGroup=255
auditCreator.creatorUserNumber.userNumberMember=255
auditCreator.subjectCreatorName=SUPER.SUPER    auditCreator.subjectSystemNumber=1
auditCreator.subjectSystemName=\TEST    auditCreator.subjectAuthLocNumber=1
auditCreator.subjectAuthLocName=\TEST    auditCreator.subjectProcessName=\TEST.$EEEE
,4,309    auditCreator.subjectSsid.ssidOwner=FFFFFF
auditCreator.subjectSsid.ssidNumber=94    auditCreator.subjectSsid.ssidVersion=18182
auditCreator.subjectTerminalName=$ZHOME    objectType.objectType=200
objectType.ownerIsRemote=701    objectType.ownerUserNumber.userNumberGroup=111
objectType.ownerUserNumber.userNumberMember=1    objectType.ownerUserName=GGG.HHHHHHH
objectType.objectName.type=200    objectType.objectName.objectName=$DATA.FTP.GETAPF3
```

Table 544. Highlighted values in the HPE Tandem sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**ZSFG_VAL_OPER_UPDATE**
Event Category	**ZSFG_VAL_OUTCOME_DENIED**
Username	**USERNAME**
Log Source Time	**18 Sep 2012 22:32:28**

Hewlett Packard Enterprise UniX (HPE-UX)

To forward events from Hewlett Packard Enterprise UniX (HPE-UX) to IBM QRadar, configure your HPE-UX device to send syslog events to QRadar.

About this task

You can configure syslog on your HPE-UX device to forward events to QRadar.

Procedure

1. Log in to the HPE-UX device command-line interface.
2. Open the following file:

   `/etc/syslog.conf`
3. Add the following line:

   <*facility*>.<*level*><*destination*>

   Where:

   - <*facility*> is `auth`.
   - <*level*> is `info`.
   - <*destination*> is the IP address of the QRadar Console.
4. Save and exit the file.
5. Type the following command to ensure that `syslogd` enforces the changes to the `syslog.conf` file.

   ```
   kill -HUP `cat /var/run/syslog.pid`
   ```

   Tip: Back quotation marks are used in the command-line.

What to do next

Add a log source in QRadar.

Related concepts

“Syslog log source parameters for Hewlett Packard Enterprise UniX (HPE-UX)” on page 890

Syslog log source parameters for Hewlett Packard Enterprise UniX (HPE-UX)

If QRadar does not automatically detect the log source, add a Hewlett Packard Enterprise UniX log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Hewlett Packard Enterprise UniX :

Table 545. Syslog log source parameters for the Hewlett Packard Enterprise UniX DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Hewlett Packard UniX
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for your Hewlett Packard Enterprise UniX device.

Related tasks

“Adding a log source” on page 5

Chapter 79. Huawei

IBM QRadar can integrate with several Huawei DSMs.

Huawei AR Series Router

The Huawei AR Series Router DSM for IBM QRadar can accept events from Huawei AR Series Routers by using syslog.

QRadar records all relevant IPv4 events that are forwarded from Huawei AR Series Router. To integrate your device with QRadar, you must create a log source, then configure your AR Series Router to forward syslog events.

Supported routers

The DSM supports events from the following Huawei AR Series Routers:

- AR150
- AR200
- AR1200
- AR2200
- AR3200

Syslog log source parameters for Huawei AR Series Router

If QRadar does not automatically detect the log source, add a Huawei AR Series Router log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Huawei AR Series Router:

Table 546. Syslog log source parameters for the Huawei AR Series Router DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Huawei AR Series Router
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address, host name, or name for the log source as an identifier for your Huawei AR Series Router. Each log source that you create for your Huawei AR Series Router must include a unique identifier, such as an IP address or host name.

Related tasks

"Adding a log source" on page 5

Configuring Your Huawei AR Series Router

To forward syslog events to IBM QRadar, you must configure your Huawei AR Series Router as an information center, then configure a log host.

About this task

The log host that you create for your Huawei AR Series Router can forward events to your QRadar Console or an Event Collector.

Procedure

1. Log in to your Huawei AR Series Router command line Interface (CLI).
2. Type the following command to access the system view:

   ```
   system-view
   ```
3. Type the following command to enable the information center:

   ```
   info-center enable
   ```
4. Type the following command to send informational level log messages to the default channel:

   ```
   info-center source default channel loghost log level informational debug
   state off trap state off
   ```
5. Optional: To verify your Huawei AR Series Router source configuration, type the command:

   ```
   display channel loghost
   ```
6. Type the following command to configure the IP address for QRadar as the log host for your switch:

   ```
   info-center loghost <IP address> facility <local>
   ```

   Where:

   - <*IP address*> is the IP address of the QRadar Console or Event Collector.
   - <*local*> is the syslog facility, for example, local0.

   For example,

   ```
   info-center loghost <IP_address> facility local0
   ```
7. Type the following command to exit the configuration:

   ```
   quit
   ```

   The configuration is complete. You can verify events that are forwarded to QRadar by viewing events on the **Log Activity** tab.

Huawei S Series Switch

The Huawei S Series Switch DSM for IBM QRadar can accept events from Huawei S Series Switch appliances by using syslog.

QRadar records all relevant IPv4 events that are forwarded from Huawei S Series Switches. To integrate your device with QRadar, you must configure a log source, then configure your S Series Switch to forward syslog events.

Supported switches

The DSM supports events from the following Huawei S Series Switches:

- S5700
- S7700
- S9700

Syslog log source parameters for Huawei S Series Switch

If QRadar does not automatically detect the log source, add a Huawei S Series Switch log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Huawei S Series Switch:

Table 547. Syslog log source parameters for the Huawei S Series Switch DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Huawei S Series Switch
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address, host name, or name for the log source as an identifier for your Huawei S Series Switch. Each log source that you create for your Huawei S Series Switch must include a unique identifier, such as an IP address or host name.

Related tasks

"Adding a log source" on page 5

Configuring Your Huawei S Series Switch

To forward syslog events to IBM QRadar, you must configure your Huawei S Series Switch as an information center, then configure a log host.

About this task

The log host that you create for your Huawei S Series Switch can forward events to your QRadar Console or an Event Collector.

Procedure

1. Log in to your Huawei S Series Switch command line Interface (CLI).
2. Type the following command to access the system view:

   ```
   system-view
   ```
3. Type the following command to enable the information center:

   ```
   info-center enable
   ```
4. Type the following command to send informational level log messages to the default channel:

   ```
   info-center source default channel loghost log level informational debug
   state off trap state off
   ```
5. Optional: To verify your Huawei S Series Switch source configuration, type the command:

   ```
   display channel loghost
   ```
6. Type the following command to configure the IP address for QRadar as the log host for your switch:

   ```
   info-center loghost <IP address> facility <local>
   ```

Where:

- <*IP address*> is the IP address of the QRadar Console or Event Collector.
- <*local*> is the syslog facility, for example, local0.

For example,

```
info-center loghost <IP_address> facility local0
```

7. Type the following command to exit the configuration:

   ```
   quit
   ```

   The configuration is complete. You can verify events that are forwarded to QRadar by viewing events on the **Log Activity** tab.

Huawei S Series Switch sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Huawei S Series Switch sample message when you use the Syslog protocol

Important: Due to formatting, paste the message format into a text editor and then remove any carriage return or line feed characters.

The following event shows that the source MAC address in the ARP packet is invalid.

```
May 22 2012 09:43:39huawei.sseriesswitch.test%%01SECE/3/ARPS_DROP_PACKET_SRC_MAC(l):
Invalidsourcemacaddress.(SourceMAC=0000-0000-0000,SourceIP=10.10.10.11,SourceInterface=
XGigabitEthernet5/0/0,DropTime=2012/05/22 09:43:39)
```

Table 548. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**SECE/3/ARPS_DROP_PACKET_SRC_MAC** The Event ID is extracted from the payload header.
Source IP	**SourceIP** The Source IP can be the **SourceAddress**, **SourceIP**, or **Source** fields, which are available in the payload.
Source MAC	**SourceMAC**
Device Time	**May 22 2012 09:43:39** The device time is extracted from the payload header.

Chapter 80. HyTrust CloudControl

The IBM QRadar DSM for HyTrust CloudControl collects events from HyTrust CloudControl devices.

The following table lists the specifications for the HyTrust CloudControl DSM:

Table 549. HyTrust CloudControl DSM specifications

Specification	**Value**
Manufacturer	Hytrust
DSM name	HyTrust CloudControl
RPM file name	`DSM-HyTrustCloudControl-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V3.0.2 through V3.6.0
Protocol	Syslog
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Hytrust web site (http://www.hytrust.com)

To collect HyTrust CloudControl events, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - HyTrust CloudControl DSM RPM
2. Configure your HyTrust CloudControl device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a HyTrust CloudControl log source on the QRadar Console. The following table describes the parameters that require specific values that are required for HyTrust CloudControl event collection:

   Table 550. HyTrust CloudControl log source parameters

Parameter	**Value**
Log Source type	HyTrust CloudControl
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring HyTrust CloudControl to communicate with QRadar

To collect HyTrust CloudControl events, you must configure your third-party device to send events to IBM QRadar

Adding a log source

Configuring HyTrust CloudControl to communicate with QRadar

To collect HyTrust CloudControl events, you must configure your third-party device to send events to IBM QRadar

Procedure

1. Log in to HyTrust CloudControl.
2. From the HTA Management Console, select **Configuration** > **Logging**.
3. From the **HTA Logging Aggregation options**, select **External**.
4. From the **Logging Aggregation Template Type** options, select either **Proprietary** or **CEF**.
5. In the **HTA Syslog Servers** field, type the IP address for QRadar.

Chapter 81. IBM

IBM QRadar supports a number of IBM DSMs.

IBM AIX

IBM QRadar provides the IBM AIX Audit and IBM AIX Server DSMs to collect and parse audit or operating system events from IBM AIX devices.

IBM AIX Server DSM overview

The IBM AIX Server DSM collects operating system and authentication events using syslog for users that interact or log in to your IBM AIX appliance.

The following table identifies the specifications for both IBM AIX DSM Server:

Table 551. IBM AIX Server DSM specifications

Specification	Value
Manufacturer	IBM
DSM names	IBM AIX Server
RPM file names	`DSM-IBMAIXServer-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V5.X, V6.X, and V7.X
Protocol type	Syslog
QRadar recorded event types	Login or logoff events Session opened or session closed events Accepted password and failed password events Operating system events
Automatically discovered?	Yes
Includes identity?	Yes
More information	IBM website (http://www.ibm.com/)

To integrate IBM AIX Server events with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - IBM AIX Server DSM RPM
2. Configure your IBM AIX Server device to send syslog events to QRadar.
3. Configure a syslog-based log source for your IBM AIX Server device. Use the following protocol-specific parameters:

Parameter	Description
Log Source Type	IBM AIX Server
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring your IBM AIX Server device to send syslog events to QRadar

To collect syslog audit events from your IBM AIX Server device, redirect your audit log output from your IBM AIX device to the IBM QRadar Console or Event Collector.

Adding a log source

"Adding a DSM" on page 4

"Adding a log source" on page 5

"Configuring your IBM AIX Server device to send syslog events to QRadar" on page 900

To collect syslog audit events from your IBM AIX Server device, redirect your audit log output from your IBM AIX device to the IBM QRadar Console or Event Collector.

Configuring your IBM AIX Server device to send syslog events to QRadar

To collect syslog audit events from your IBM AIX Server device, redirect your audit log output from your IBM AIX device to the IBM QRadar Console or Event Collector.

Procedure

1. Log in to your IBM AIX appliance as a root user.
2. Open the `/etc/syslog.conf` file.
3. To forward the system authentication logs to QRadar, add the following line to the file:

   `auth.info @QRadar_IP_address`

   A tab must separate auth.info and the IP address of QRadar.

   For example:

   ```
   ##### begin /etc/syslog.conf mail.debug /var/adm/maillogmail.none /var/adm/
   maillogauth.notice /var/adm/authloglpr.debug /var/adm/lpd-errskern.debug /var/adm/
   messages*.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info /var/adm/
   messagesauth.info            @<IP_address>##### end /etc/syslog.conf
   ```

4. Save and exit the file.
5. Restart the syslog service:

   `refresh -s syslogd`

IBM AIX Server sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM AIX Server sample message when you use the Syslog protocol

The following sample event message shows that the sshd connection is closed.

<38>**Nov 21 16:19:05** ibm.aix.test **sshd**[7471482]: **Connection closed** by **10.5.88.146** [preauth]

```
<38>Nov 21 16:19:05 ibm.aix.test sshd[7471482]: Connection closed by 10.5.88.146 [preauth]
```

Table 552. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**sshd** + **Connection closed** (extracted from the payload)
Device Time	**Nov 21 16:19:05**

Table 552. Highlighted fields (continued)	
QRadar field name	**Highlighted payload field name**
Source IP	**10.5.88.146**

IBM AIX Audit DSM overview

The IBM AIX Audit DSM collects detailed audit information for events that occur on your IBM AIX appliance.

The following table identifies the specifications for the IBM AIX Audit DSM:

Table 553. IBM AIX Audit DSM specifications	
Specification	**Value**
Manufacturer	IBM
DSM names	IBM AIX Audit
RPM file names	DSM-IBMAIXAudit-*QRadar_version-build_number*.noarch.rpm
Supported versions	V6.1 and V7.1
Protocol type	Syslog Log File Protocol
QRadar recorded event types	Audit events
Automatically discovered?	Yes
Includes identity?	No
More information	IBM website (http://www.ibm.com/)

To integrate IBM AIX Audit events with QRadar, complete the following steps:

1. Download the latest version of the IBM AIX Audit DSM from the IBM Support Website.
2. For syslog events, complete the following steps:
   a. Configure your IBM AIX Audit device to send syslog events to QRadar. See “Configuring IBM AIX Audit DSM to send syslog events to QRadar ” on page 903.
   b. If QRadar does not automatically discover the log source, add an IBM AIX Audit log source. Use the following IBM AIX Audit-specific values in the log source configuration:

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Syslog

3. For log file protocol events, complete the following steps:
   a. Configure your IBM AIX Audit device to convert audit logs to the log file protocol format.
   b. Configure a log file protocol-based log source for your IBM AIX Audit device. Use the following protocol-specific values in the log source configuration:

Parameter	Value
Log Source Type	IBM AIX Audit
Protocol Configuration	Log File

Parameter	Value
Service Type	The protocol to retrieve log files from a remote server. **Important:** If you select the SCP and SFTP service type, ensure that the server that is specified in the **Remote IP or Hostname** parameter has the SFTP subsystem enabled.
Remote Port	If the host for your event files uses a non-standard port number for FTP, SFTP, or SCP, adjust the port value.
SSH Key File	If you select SCP or SFTP as the Service Type, use this parameter to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** parameter is ignored.
Remote Directory	The directory location on the remote host where the files are retrieved. Specify the location relative to the user account you are using to log in. **Restriction:** For FTP only. If your log files are in a remote user home directory, leave the remote directory blank to support operating systems where a change in the working directory (CWD) command is restricted.
FTP File Pattern	The FTP file pattern must match the name that you assigned to your AIX audit files with the **-n** parameter in the audit script. For example, to collect files that start with AIX_AUDIT and end with your time stamp value, type `AIX_Audit_*`.
FTP Transfer Mode	ASCII is required for text event logs that are retrieved by the log file protocol by using FTP.
Processor	NONE
Change Local Directory?	Leave this check box clear.
Event Generator	LineByLine The Event Generator applies more processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

Adding a DSM

Configuring IBM AIX Audit DSM to send syslog events to QRadar

To collect syslog audit events from your IBM AIX Audit device, redirect your audit log output from your IBM AIX device to the IBM QRadar Console or Event Collector.

Configuring IBM AIX Audit DSM to send log file protocol events to QRadar

Configure the audit.pl script to run each time that you want to convert your IBM AIX audit logs to a readable event log format for QRadar.

Adding a log source

Configuring IBM AIX Audit DSM to send syslog events to QRadar

To collect syslog audit events from your IBM AIX Audit device, redirect your audit log output from your IBM AIX device to the IBM QRadar Console or Event Collector.

About this task

On an IBM AIX appliance, you can enable or disable classes in the audit configuration. The IBM AIX default classes capture a large volume of audit events. To prevent performance issues, you can tune your IBM AIX appliance to reduce the number of classes that are collected. For more information about audit classes, see your IBM AIX appliance documentation.

Procedure

1. Log in to your IBM AIX appliance.
2. Open the audit configuration file:

   `/etc/security/audit/config`
3. Edit the Start section to disable the **binmode** element and enable the **streammode** element:

   ```
   binmode = off
   ```

   ```
   streammode = on
   ```
4. Edit the Classes section to specify which classes to audit.
5. Save the configuration changes.
6. Open the `streamcmds` file:

   `/etc/security/audit/streamcmds`
7. Add the following line to the file:

   ```
   /usr/sbin/auditstream | /usr/sbin/auditselect -m -e "command != logger && command !=
   auditstream && command != auditpr && command != auditselect"|auditpr -t0 -h eclrRdi -v |awk
   -u 'NR%2{printf "%s ",$0;next}{print;}' | /usr/bin/logger -p local0.debug -r &
   ```
8. Save the configuration changes.
9. Edit the syslog configuration file to specify a debug entry and the IP address of the QRadar Console or Event Collector:

   `*.debug @`*`ip_address`*

   Tip: A tab must separate *.debug from the IP address.
10. Save the configuration changes.
11. Reload your syslog configuration:

    `refresh -s syslogd`
12. Start the audit script on your IBM AIX appliance:

    `audit start`

What to do next

The IBM AIX Audit DSM automatically discovers syslog audit events that are forwarded from IBM AIX to QRadar and creates a log source. If the events are not automatically discovered, you can manually configure a log source.

Configuring IBM AIX Audit DSM to send log file protocol events to QRadar

Configure the audit.pl script to run each time that you want to convert your IBM AIX audit logs to a readable event log format for QRadar.

Before you begin

Ensure that Perl 5.8 or later is installed on your IBM AIX computer.

About this task

To send log file protocol events from IBM AIX to QRadar, you must edit these files:

Audit configuration file

The audit configuration file identifies the event classes that are audited and the location of the event log file on your IBM AIX appliance. The IBM AIX default classes capture many audit events. To prevent performance issues, you can configure the classes in the audit configuration file. For more information about configuring audit classes, see your IBM AIX documentation.

Audit script

The audit script uses the audit configuration file to identify which audit logs to read and converts the binary logs to single-line events that QRadar can read. The log file protocol can then retrieve the event log from your IBM AIX appliance and import the events to QRadar. The audit script uses the audit.pr file to convert the binary audit records to event log files QRadar can read.

Run the audit script each time that you want to convert your audit records to readable events. You can use a cron job to automate this process. for example, you can add `0 * * * * /audit.pl` to allow the audit script to run hourly. For more information, see your system documentation.

Procedure

1. Log in to your IBM AIX appliance.
2. Configure the audit configuration file:
   a) Open the audit configuration file:

      `etc/security/audit/config`

   b) Edit the Start section to enable the **binmode** element.

      ```
      binmode = on
      ```

   c) In the Start section, edit the configuration to determine which directories contain the binary audit logs.
      The default configuration for IBM AIX auditing writes binary logs to the following directories:

      ```
      trail = /audit/trail
      bin1 = /audit/bin1
      bin2 = /audit/bin2
      binsize = 10240
      cmds = /etc/security/audit/bincmds
      ```

      In most cases, you do not have to edit the binary file in the bin1 and bin2 directories.

   d) In the Classes section, edit the configuration to determine which classes are audited. For information on configuring classes, see your IBM AIX documentation.

   e) Save the configuration changes.
3. Audit on your IBM AIX system:

   `audit start`
4. Install the audit script:
   a) From IBM Fix Central (https://www.ibm.com/support/fixcentral/), search for the `audit.pl.gz` and select the download that corresponds to your version of QRadar.

b) Download the `audit.pl.gz` file.

c) Copy the audit script to a folder on your IBM AIX appliance.

d) Extract the file:

```
tar -zxvf audit.pl.gz
```

e) Start the audit script:

```
./audit.pl
```

You can add the following parameters to modify the command:

Parameter	Description
-r	Defines the results directory where the audit script writes event log files for QRadar. If you do not specify a results directory, the script writes the events to the following `/audit/results/` directory. The results directory is used in the **Remote Directory** parameter in the log source configuration uses this value. To prevent errors, verify that the results directory exists on your IBM AIX system.
-n	Defines a unique name for the event log file that is generated by audit script. The **FTP File Pattern** parameter in the log source configuration uses this name to identify the event logs that the log source must retrieve in QRadar
-l	Defines the name of the last record file.
-m	Defines the maximum number of audit files to retain on your IBM AIX system. By default, the script retains 30 audit files. When the number of audit files exceeds the value of the **-m** parameter, the script deletes the audit file with the oldest time stamp.
-t	Defines the directory that contains the audit trail file. The default directory is `/audit/trail`.

What to do next

The IBM AIX Audit DSM automatically discovers log file protocol audit events that are forwarded from IBM AIX to QRadar and creates a log source. If the events are not automatically discovered, you can manually configure a log source.

IBM BigFix Detect

The IBM BigFix Detect DSM for QRadar is deprecated.

IBM CICS

The IBM CICS DSM collects events from IBM Custom Information Control System (CICS®) on an IBM z/OS® mainframe that uses IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect IBM CICS events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html) .
2. Configure your IBM z/OS image to write events in LEEF format. For more information, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).
3. Create a log source in QRadar for IBM CICS.
4. If you want to create a custom event property for IBM CICS in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (https://www.ibm.com/docs/en/SS2RWS_2.4.0/com.ibm.zsecure.doc_2.4.0/zsec_install.pdf).

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

Table 554. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Log File log source parameter

If QRadar does not automatically detect the log source, add a IBM z/OS, IBM CICS, IBM RACF, IBM DB2, Broadcom CA Top Secret, or Broadcom CA ACF2 log source on the QRadar Console by using the Log File Protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, or CA ACF2:

Table 555. Log File log source parameters

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	Select your DSM name.
Protocol Configuration	**Log File**

Table 555. Log File log source parameters (continued)

Parameter	Value
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.
Service Type	From the **Service Type** list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535. The options include ports: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.

Table 555. Log File log source parameters (continued)

Parameter	Value
Remote User	Type the user name or user ID necessary to log in to the system that contains your event files. • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length. • If your log files are on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: `<product_name>.<timestamp>.gz` The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with z0S and end with `.gz`, type the following code: `z0S.*\.gz` Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions (https://docs.oracle.com/javase/tutorial/essential/regex/).

Table 555. Log File log source parameters (continued)	
Parameter	**Value**
FTP Transfer Mode	This option displays only if you select **FTP** as the **Service Type**. From the list, select **Binary**. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as `zip`, `gzip`, `tar`, or `tar+gzip` archive files.
SCP Remote File	If you select **SCP** as the **Service Type** you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type `00:00` to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	If you want the Log File protocol to run immediately after you click **Save**, select this check box. After the **Run On Save** completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.

Table 555. Log File log source parameters (continued)	
Parameter	**Value**
Processor	From the list, select **gzip**. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is previously processed by the Log File protocol. If a previously processed file is detected, the Log File protocol does not download the file for processing. All files that are not previously processed are downloaded. This option applies only to FTP and SFTP service types.
Change Local Directory?	Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the **Local Directory** field is displayed, which gives you the option to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select **LineByLine**. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

"Adding a log source" on page 5

IBM Cloud Activity Tracker

The IBM QRadar DSM for IBM Cloud Activity Tracker collects Apache Kafka events from an IBM Cloud Activity Tracker application.

To integrate IBM Cloud Activity Tracker with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - Kafka Protocol RPM
   - DSM Common RPM
   - IBM Cloud Activity Tracker DSM RPM
2. Configure your IBM Cloud Activity Tracker system to send events to QRadar. For more information, see Configuring IBM Cloud Activity Tracker to communicate with QRadar.

3. If QRadar does not automatically detect the log source, add an IBM Cloud Activity Tracker log source on the QRadar Console. For more information, see Apache Kafka log source parameters for IBM Cloud Activity Tracker.

Related concepts

"Apache Kafka log source parameters for IBM Cloud Activity Tracker" on page 913

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

IBM Cloud Activity Tracker DSM specifications

When you configure the IBM Cloud Activity Tracker DSM, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported event format for IBM Cloud Activity Tracker is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the IBM Cloud Activity Tracker DSM.

Table 556. IBM Cloud Activity Tracker DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBM Cloud Activity Tracker
RPM file name	DSM-*IBMCloudActivityTracker-QRadar_version-build_number*.noarch.rpm
Protocol	Apache Kafka
Event format	JSON
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	IBM Cloud Activity Tracker documentation (https://cloud.ibm.com/apidocs/activity-tracker)

Configuring IBM Cloud Activity Tracker to communicate with QRadar

Before you can add a log source in IBM QRadar, you must note the values in the event stream topic and service credentials of IBM Cloud Activity Tracker. You need these values when you configure the log source.

Before you begin

IBM Cloud Activity Tracker must be configured with an event stream service instance that has at least one topic and two service credentials. For more information, see the IBM Cloud documentation topics about *Creating an Event Streams service instance*, *Create a topic*, and *Create credentials*.

Procedure

1. Log in to IBM Cloud (https://cloud.ibm.com).
2. From the navigation menu, select **Resource List**.
3. Expand **Services and Software**, then select your event stream instance.
4. From the Event Streams menu, select **Topics**. Note the topic name that you want to link to QRadar. You need the topic name when you configure the **Topic List** parameter in QRadar.

5. From the menu, select **Service credentials**.
6. From the **Service credentials** list, expand the read service credential. Note the JSON object text. You need the values from the JSON object text when you configure the **Bootstrap Server List**, **SASL Username**, and **SASL Password** parameters in QRadar.

   Tip: For more information about configuring IBM Cloud Activity Tracker to communicate with QRadar, see the Configuring an Event Streams target documentation (https://cloud.ibm.com/docs/atracker?topic=atracker-getting-started-target-event-streams).

Related concepts

Apache Kafka log source parameters for IBM Cloud Activity Tracker

Related tasks

Adding a log source

Apache Kafka log source parameters for IBM Cloud Activity Tracker

If IBM QRadar does not automatically detect the log source, add an IBM Cloud Activity Tracker log source on the QRadar Console by using the Apache Kafka protocol.

When you use the Apache Kafka protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Apache Kafka events from IBM Cloud Activity Tracker:

Table 557. Apache Kafka log source parameters for the IBM Cloud Activity Tracker DSM

Parameter	Value
Log Source type	IBM Cloud Activity Tracker
Protocol Configuration	Apache Kafka
Log Source Identifier	Type a unique name for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If more than one IBM Cloud Activity Tracker log source is configured, you might want to identify the first log source as ibmactivitytracker1 and the second log source as ibmactivitytracker2.
Bootstrap Server List	The **kafka_brokers_sasl** field value from the JSON object text that you noted when you completed the Configuring IBM Cloud Activity Tracker to communicate with QRadar procedure.
Use SASL Authentication	Enabled
SASL Username	The **user** field value from the JSON object text that you noted when you completed the Configuring IBM Cloud Activity Tracker to communicate with QRadar procedure.
SASL Password	The **password** field value from the JSON object text that you noted when you completed the Configuring IBM Cloud Activity Tracker to communicate with QRadar procedure.

For a complete list of Apache Kafka protocol parameters and their values, see Apache Kafka protocol configuration options.

Important: The IBM Cloud Event Streams certificate must be renewed on a 90-day expiry cycle. For this reason, the certificate must be updated in the QRadar truststore for communication to continue. Choose one the following options:

- If you are a QRadar on-premises user, to add the certificate to the `/opt/qradar/conf/trusted_certificates/` directory, you need to run the **`getcert.sh`** command in the `/opt/qradar/getcert.sh` directory. Run the following commands:

  ```
  cd /opt/qradar/conf/trusted_certificates/
  ```

  ```
  /opt/qradar/bin/getcert.sh <Kafka URL>
  ```

  The *<Kafka URL>* is similar to `m4ydv39cxnxjm4pq.svc02.us-east.eventstreams.cloud.ibm.com`.
- If you are a QRadar on Cloud user, contact IBM support and open a support case to get the renewed certificate placed in the truststore.

For more information about IBM Event Streams certificates, see the IBM Event Streams documentation (https://ibm.github.io/event-streams/getting-started/connecting/).

Related tasks

Adding a log source

IBM Cloud Activity Tracker sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Cloud Activity Tracker sample messages when you use the Apache Kafka protocol

Sample 1: The following sample event message shows that the occurrence is viewed successfully.


```
{"_source":{"_host":"security-
advisor","_logtype":"json","_file":"file_name","_line":"{\"outcome\":\"success\",\"typeURI\":\"u
rl\",\"eventType\":\"activity\",\"eventTime\":\"2021-07-01T00:36:53.62+0000\",\"action\":\"secur
ity-
advisor.findings.read\",\"id\":\"1111111a-1a11-1111-111a-11111111a1aa\",\"correlationId\":\"1111
111a-1a11-1111-111a-11111111a1aa\",\"initiator\":
{\"id\":\"1111111a-1a11-1111-111a-11111111a1aa\",\"name\":\"username\",\"authnId\":\"1111111a-1a
11-1111-111a-11111111a1aa\",\"authnName\":\"Author\",\"typeURI\":\"service/security/account/
user\",\"host\":{\"agent\":\"Apache-HttpClient/4.5.9 (Java/
1.8.0_281)\",\"address\":\"10.41.87.6,10.74.72.121\",\"addressType\":\"IPv4\"},\"credential\":
{\"type\":\"user\"}},\"target\":{\"id\":\"id\",\"name\":\"findingsapi\",\"typeURI\":\"security-
advisor/occurrence\"},\"observer\":{\"name\":\"ActivityTracker\"},\"reason\":
{\"reasonCode\":200,\"reasonType\":\"OK\"},\"requestData\":{\"providerId\":\"security-
advisor\",\"occurrenceId\":\"1111111a-1a11-1111-111a-11111111a1aa\"},\"responseData\":
{\"Context account id\":\"1111111a-1a11-1111-111a-11111111a1aa\",\"email\":
{},\"occurrenceId\":\"xforce\",\"Occurrence kind\":\"FINDING\",\"Context region\":\"us-
south\",\"Occurrence creation time\":\"2021-07-01T00:34:46.952210Z\",\"data_transferred\":
{},\"network\":{\"client\":{},\"server\":{}},\"Occurrence
name\":\"1111111a-1a11-1111-111a-11111111a1aa/providers/security-advisor/occurrences/
xforce-111111111111-111\",\"Note name\":\"1111111a-1a11-1111-111a-11111111a1aa/providers/
security-advisor/notes/xforce-client_response\",\"Occurrence update
time\":\"2021-07-01T00:34:46.952003Z\"},\"severity\":\"normal\",\"message\":\"Security Advisor:
read findingsapi\",\"dataEvent\":true,\"logSourceCRN\":\"crn:v1:bluemix:public:security-
advisor:us-south:a/
aa111111aaa111aaa1a111a111111111:::\",\"saveServiceCopy\":true}","_rawline":null,"_ts":aa111111a
aa111aaa1a111a111111111,"_platform":"security-advisor","_app":"crn:v1:bluemix:public:security-
advisor:us-south:a/
aa111111aaa111aaa1a111a111111111:::","_ip":"10.9.14.3","_id":"11111111111111111","outcome":"suc
cess","typeURI":"typeURI","eventType":"activity","eventTime":"2021-07-01T00:36:53.62+0000","acti
on":"security-
advisor.findings.read","id":"1111111a-1a11-1111-111a-11111111a1aa","correlationId":"1111111a-1a1
1-1111-111a-11111111a1aa","severity":"normal","message":"Security Advisor: read
findingsapi","dataEvent":true,"logSourceCRN":"crn:v1:bluemix:public:security-advisor:us-south:a/
aa111111aaa111aaa1a111a111111111:::","saveServiceCopy":true,"o_initiator":
{"id":"authnId","name":"name","authnId":"iam-
```

```
identifier","authnName":"testuser","typeURI":"service/security/account/user","o_host":
{"agent":"Apache-HttpClient/4.5.9 (Java/
1.8.0_281)","address":"10.41.87.6,10.74.72.121","addressType":"IPv4"},"o_credential":
{"type":"user"}},"o_target":{"id":"crn:v1:bluemix:public:security-advisor:us-south:a/
aa111111aaa111aaa1a111a111111111::111111111111-111","name":"findingsapi","typeURI":"security-
advisor/occurrence"},"o_observer":{"name":"ActivityTracker"},"o_reason":
{"reasonCode":200,"reasonType":"OK"},"o_requestData":{"providerId":"security-
advisor","occurrenceId":"xforce-111111111111-111"},"o_responseData":{"Context account
id":"aa111111aaa111aaa1a111a111111111","occurrenceId":"xforce","Occurrence
kind":"FINDING","Context region":"us-south","Occurrence creation
time":"2021-07-01T00:34:46.952210Z","Occurrence name":"aa111111aaa111aaa1a111a111111111/
providers/security-advisor/occurrences/xforce-1625099685333-735","Note
name":"aa111111aaa111aaa1a111a111111111/providers/security-advisor/notes/xforce-
client_response","Occurrence update time":"2021-07-01T00:34:46.952003Z","o_email":
{},"o_data_transferred":{},"o_network":{"client":"{}","server":"{}"}}}}
```


Table 558. Highlighted fields in the IBM Cloud Activity Tracker event	
QRadar field name	**Highlighted payload field name**
Event Time	eventTime
Event ID	outcome + action
Event Category	In QRadar, the value is **IBMActivityTrackerSecurityAdvisorService**.
Source IP	address
Username	name

Sample 2: The following sample event message shows that an occurrence is created successfully.


```
{"_source":{"_host":"security-
advisor","_logtype":"json","_file":"crn:v1:bluemix:public:security-advisor:us-south:a/
aa111111aaa111aaa1a111a111111111:::","_line":"{\"outcome\":\"success\",\"typeURI\":\"http://
schemas.dmtf.org/cloud/audit/1.0/
event\",\"eventType\":\"activity\",\"eventTime\":\"2021-07-01T00:29:37.07+0000\",\"action\":\"se
curity-
advisor.findings.write\",\"id\":\"1111111a-1a11-1111-111a-11111111a1aa\",\"correlationId\":\"111
1111a-1a11-1111-111a-11111111a1aa\",\"initiator\":
{\"id\":\"1111111a-1a11-1111-111a-11111111a1aa\",\"name\":\"IBM (security-advisor)
\",\"authnId\":\"1111111a-1a11-1111-111a-11111111a1aa\",\"authnName\":\"SA internal
Service\",\"typeURI\":\"service/security/account/serviceid\",\"host\":
{\"address\":\"10.126.255.165,10.187.197.4\",\"addressType\":\"IPv4\"},\"credential\":
{\"type\":\"apikey\"}},\"target\":{\"id\":\"crn:v1:bluemix:public:security-advisor:us-south:a/
aa111111aaa111aaa1a111a111111111::occurrence:xforce-111111111111-111\",\"name\":\"findingsapi\",
\"typeURI\":\"security-advisor/occurrence\"},\"observer\":
{\"name\":\"ActivityTracker\"},\"reason\":
{\"reasonCode\":200,\"reasonType\":\"OK\"},\"requestData\":{\"Replace existing
occurrence\":true,\"providerId\":\"security-advisor\",\"context\":{\"Context region\":\"us-
south\"},\"finding\":{\"network\":{\"client\":{},\"server\":{}},\"data_transferred\":
{}},\"Occurrence kind\":\"FINDING\",\"occurrenceId\":\"xforce-111111111111-111\",\"Note
name\":\"aa111111aaa111aaa1a111a111111111/providers/security-advisor/notes/xforce-
client_response\"},\"responseData\":{\"email\":{},\"data_transferred\":{},\"network\":
{\"client\":{},\"server\":{}},\"Occurrence name\":\"aa111111aaa111aaa1a111a111111111/providers/
security-advisor/occurrences/
xforce-111111111111-111\"},\"severity\":\"normal\",\"message\":\"Security Advisor: write
findingsapi\",\"dataEvent\":true,\"logSourceCRN\":\"crn:v1:bluemix:public:security-advisor:us-
south:a/
aa111111aaa111aaa1a111a111111111:::\",\"saveServiceCopy\":true}","_rawline":null,"_ts":aa111111a
aa111aaa1a111a111111111,"_platform":"security-advisor","_app":"crn:v1:bluemix:public:security-
advisor:us-south:a/
aa111111aaa111aaa1a111a111111111:::","_ip":"10.9.14.3","_id":"aa111111aaa111aaa1a111a111111111",
"outcome":"success","typeURI":"http://schemas.dmtf.org/cloud/audit/1.0/
event","eventType":"activity","eventTime":"2021-07-01T00:29:37.07+0000","action":"security-
advisor.findings.write","id":"1111111a-1a11-1111-111a-11111111a1aa","correlationId":"d600ce3f-3c
d8-4a34-867a-fd8f3630b39c","severity":"normal","message":"Security Advisor: write
findingsapi","dataEvent":true,"logSourceCRN":"crn:v1:bluemix:public:security-advisor:us-south:a/
aa111111aaa111aaa1a111a111111111:::","saveServiceCopy":true,"o_initiator":
{"id":"1111111a-1a11-1111-111a-11111111a1aa","name":"IBM (security-
advisor)","authnId":"iam-1111111a-1a11-1111-111a-11111111a1aa","authnName":"SA internal
Service","typeURI":"service/security/account/serviceid","o_host":
{"address":"10.126.255.165,10.187.197.4","addressType":"IPv4"},"o_credential":
{"type":"apikey"}},"o_target":{"id":"crn:v1:bluemix:public:security-advisor:us-south:a/
aa111111aaa111aaa1a111a111111111::occurrence:xforce-111111111111-111","name":"findingsapi","type
URI":"security-advisor/occurrence"},"o_observer":{"name":"ActivityTracker"},"o_reason":
{"reasonCode":200,"reasonType":"OK"},"o_requestData":{"Replace existing
```

```
occurrence":true,"providerId":"security-advisor","Occurrence
kind":"FINDING","occurrenceId":"xforce-111111111111-111","Note
name":"aa111111aaa111aaa1a111a111111111/providers/security-advisor/notes/xforce-
client_response","o_context":{"Context region":"us-south"},"o_finding":{"network":"{\n
\"client\": {},\n  \"server\": {}\n}","data_transferred":"{}"}},"o_responseData":{"Occurrence
name":"aa111111aaa111aaa1a111a111111111/providers/security-advisor/occurrences/
xforce-111111111111-111","o_email":{},"o_data_transferred":{},"o_network":
{"client":"{}","server":"{}"}}}}
```


Table 559. Highlighted fields in the IBM Cloud Activity Tracker event	
QRadar field name	**Highlighted payload field name**
Event Time	eventTime
Event ID	outcome + action
Event Category	In QRadar, the value is **IBMActivityTrackerSecurityAdvisorService**.
Source IP	address
Username	name

Sample 3: The following sample event message shows that an occurrence is viewed successfully.


```
{"timestamp":1680032637,"line":"{\"eventTime\":\"2023-03-28T19:43:57.01+0000\",\"correlationId\"
:\"11111111-1111-1111-1111-111111111111\",\"action\":\"atracker.route.read\",\"severity\":\"norm
al\",\"initiator\":
{\"id\":\"testid-000000AAA0\",\"name\":\"user1@example.com\",\"authnId\":\"testid-000000AAA0\",\
"authnName\":\"user1\",\"typeURI\":\"service/security/account/user\",\"credential\":
{\"type\":\"user\"},\"host\":
{\"address\":\"10.0.0.1\",\"addressType\":\"CSE\",\"agent\":\"platform-services-go-sdk/0.31.2
(lang=go; arch=arm64; os=darwin; go.version=go1.19.5)\"}},\"target\":{\"name\":\"qradar-es-
route\",\"id\":\"crn:v1:bluemix:public:atracker:global:a/
11aa1111a111111a1111a1a11111a1111a111aaa::route:a111aaa1-aa1a-1111-
aa1a-1a111a11aa11\",\"typeURI\":\"atracker/route\"},\"outcome\":\"success\",\"reason\":
{\"reasonCode\":200,\"reasonType\":\"OK\"},\"observer\":
{\"name\":\"ActivityTracker\"},\"requestData\":{\"requestURI\":\"https://us-
south.atracker.cloud.ibm.com/api/v2/routes/a111aaa1-aa1a-1111-
aa1a-1a111a11aa11\"},\"responseData\":{\"response\":\"success\",\"route\":{\"id\":\"a111aaa1-
aa1a-1111-aa1a-1a111a11aa11\",\"name\":\"qradar-es-
route\",\"crn\":\"crn:v1:bluemix:public:atracker:global:a/
11aa1111a111111a1111a1a11111a1111a111aaa::route:a111aaa1-aa1a-1111-
aa1a-1a111a11aa11\",\"version\":0,\"rules\":[{\"locations\":[\"us-south\",\"us-
east\",\"global\"],\"target_ids\":[\"a111aaa1-aa1a-1111-
aa1a-1a111a11aa11\"]}],\"api_version\":2,\"created_at\":\"2023-03-28T18:56:14.269Z\",\"updated_a
t\":\"2023-03-28T18:56:14.269Z\"}},\"logSourceCRN\":\"crn:v1:bluemix:public:atracker:us-south:a/
11aa1111a111111a1111a1a11111a1111a111aaa:::\",\"saveServiceCopy\":true,\"dataEvent\":false,\"mes
sage\":\"Activity Tracker Event Routing: read route\"}","file":"/var/log/at/atracker/api/
api-111a11a1a1-1aaaa.log"}
```


Table 560. Highlighted fields in the IBM Cloud Activity Tracker event	
QRadar field name	**Highlighted payload field name**
Event Time	eventTime
Event ID	outcome + action
Event Category	In QRadar, the value is **IBMActivityTracker**.
Source IP	address
Username	name

Sample 4: The following sample event message of an AT event is generated when the API server creates a certificate for a given gateway.

```
<sample event 1 in event.txt file>
```

Table 561. Highlighted fields in the IBM Cloud Activity Tracker event	
QRadar field name	**Highlighted payload field name**
Event Time	eventTime
Event ID	action + outcome
Event Category	In QRadar, the value is **IBMActivityTracker**.
Source IP	address
Username	name

IBM Cloud Platform (formerly known as IBM Bluemix Platform)

IBM Cloud Platform is formerly known as IBM Bluemix® Platform. The name remains the same in IBM QRadar.

The IBM QRadar DSM for the IBM Cloud Platform collects events from your IBM Cloud Platform.

The following table identifies the specifications for the IBM Cloud Platform DSM:

Table 562. IBM Bluemix Platform DSM specifications	
Specification	**Value**
Manufacturer	IBM
DSM name	IBM Bluemix Platform
RPM file name	DSM-IBMBluemixPlatform-*QRadar_version-build_number*.noarch.rpm
Supported versions	N/A
Protocol	Syslog, TLS Syslog
Recorded event types	All System (Cloud Foundry) events, some application events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	IBM Cloud website (https://www.ibm.com/cloud)

To integrate IBM Cloud Platform with QRadar, complete the following steps:

You must complete the installation, third-party configuration, and QRadar configuration procedures in the order listed. Installation must always be first, but you can invert the order of the other two procedures, In some cases, no action is required for the third-party configuration and you can omit the procedure.

1. If automatic updates are not enabled, download and install the most recent version of the IBM Bluemix Platform DSM RPM from the IBM Support Website (https://www.ibm.com/support) onto your QRadar Console:
2. Configure your IBM Cloud Platform device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an IBM Cloud Platform log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring IBM Cloud Platform to communicate with QRadar

To collect IBM Cloud Platform events, you must configure your third-party instance to send events to QRadar.

Before you begin

You must have an app running in IBM Cloud so that you can create log drains.

Procedure

1. From the Cloud Foundry command-line interface, type the following command to create a drain:

   ```
   cf cups drain_name -l syslog://QRadar_IP_Address:514
   ```

   Alternatively, use the following command:

   ```
   cf cups drain_name -l syslog-tls://QRadar_IP_Address:1513
   ```

   1513 is the port that is used to communicate with QRadar.
2. Bind the service instance with the following command:

   ```
   cf bind-service BusinessApp_name drain_name
   ```

Integrating IBM Cloud Platform with QRadar

In most installations, there is only the RPM. For installations where there are multiple RPMs required, (for example a PROTOCOL RPM and a DSMCommon RPM), ensure that the installation sequence reflects RPM dependency.

Procedure

1. If required, download and install the latest TLS Syslog RPM from the IBM Support Website (https://www.ibm.com/support) onto your QRadar Console. You can install a protocol by using the procedure to manually install a DSM. If automatic updates are configured to install protocol updates, this procedure is not necessary.
2. Download and install the latest DSMCommon RPM from the IBM Support Website (https://www.ibm.com/support) onto your QRadar Console. If automatic updates are configured to install DSM updates, this procedure is not necessary.
3. Download and install the latest IBM Bluemix Platform RPM from the IBM Support Website (https://www.ibm.com/support) onto your QRadar Console. If automatic updates are configured to install DSM updates, this procedure is not necessary.

What to do next

Configure a log source in QRadar by using Syslog or TLS syslog.

Syslog log source parameters for IBM Cloud Platform

If QRadar does not automatically detect the log source, add an IBM Cloud Platform log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from IBM Cloud Platform:

Table 563. Syslog log source parameters for the IBM Cloud Platform DSM	
Parameter	**Value**
Log Source type	IBM Bluemix Platform
Protocol Configuration	Syslog
Log Source Identifier	The IP address of the Cloud Loggregator. **Important:** It might be necessary to include the IP address and the port, as the Log Source Identifier. For example, `192.0.2.1:1513`.

Related tasks

"Adding a log source" on page 5

TLS Syslog log source parameters IBM Cloud Platform

If IBM QRadar does not automatically detect the log source, add an IBM Cloud Platform log source on the QRadar Console by using the TLS Syslog protocol.

When using the TLS Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect TLS Syslog events from IBM Cloud Platform:

Table 564. TLS Syslog log source parameters for the IBM Cloud Platform DSM	
Parameter	**Value**
Log Source type	IBM Bluemix Platform
Protocol Configuration	TLS Syslog
Log Source Identifier	Type the IP address of the IBM Cloud Loggregator. **Important:** It might be necessary to include the IP address and the port, as the Log Source Identifier. For example, `192.0.2.1:1513`.

For more information about TLS syslog log source parameters, see TLS syslog protocol configuration options.

Related tasks

"Adding a log source" on page 5

IBM Cloud Platform sample event messages

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Cloud sample message when you use the Syslog protocol

The following sample event message shows that a route is unregistered.

```
Feb 22 20:00:39 ibm.bluemixplatform.test 10.59.107.50 [job=router index=1]
{"log_level":1,"timestamp":1519329639.0902693,"message":"unregister-
route","source":"vcap.gorouter.subscriber","data":{"message":"{\"uris\":[\"p-mysql.sys-
pcf05.cf.example.com\"],\"host\":\"10.68.232.5\",\"port\":8081,\"tags\":null,\"private_instance_
id\":\"aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee\"}"}}
```

Table 565. QRadar field names for the IBM Cloud Platform sample event	
QRadar field name	**Highlighted values in the payload**
Event ID	**unregister-route**
Category	This DSM doesn't have a category field to key from for the device in the payloads. QRadar provides the value **Cloud Foundry** as a static category.
Log Source Time	**1519329639.0902693**
Source IP	**10.68.232.5**
Source Port	**8081**

IBM DataPower

The IBM QRadar DSM collects event logs from your IBM DataPower® system.

IBM DataPower is formerly known as IBM WebSphere® DataPower.

The following table identifies the specifications for the IBM DataPower DSM.

Table 566. IBM DataPower DSM specifications	
Specification	**Value**
Manufacturer	IBM
DSM Name	DataPower
RPM file name	DSM-IBMDataPower-*QRadar_version-build_number*.noarch.rpm
Supported versions	FirmwareV6 and V7
Protocol	Syslog
QRadar recorded event types	All Events
Log source type in QRadar UI	IBM DataPower
Auto discovered?	Yes
Includes identity?	No
Includes custom properties?	No
For more information	IBM web page (http://www.ibm.com/)

To send events from IBM DataPower to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM DataPower DSM from the IBM Support Website onto your QRadar Console.
2. For each instance of IBM DataPower, configure the IBM DataPower system to communicate with QRadar.
3. If QRadar does not automatically discover IBM DataPower, create a log source for each instance of IBM DataPower on the QRadar Console. Use the following IBM DataPower specific values:

Parameter	Value
Log Source Type	IBM DataPower
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring IBM DataPower to communicate with QRadar

To collect IBM DataPower events, configure your third-party system to send events to IBM QRadar.

Related information

Adding a log source

Configuring IBM DataPower to communicate with QRadar

To collect IBM DataPower events, configure your third-party system to send events to IBM QRadar.

Before you begin

Review the DataPower logging documents to determine which logging configuration changes are appropriate for your deployment. See IBM Knowledge Center (https://www.ibm.com/docs/en/SS9H2Y_10cd/com.ibm.dp.doc/logtarget_logs.html).

Procedure

1. Log in to your IBM DataPower system.
2. In the search box on the left navigation menu, type `Log Target`.
3. Select the matching result.
4. Click **Add**.
5. In the **Main** tab, type a name for the log target.
6. From the **Target Type** list, select **syslog**.
7. In the **Local Identifier** field, type an identifier to be displayed in the **Syslog event payloads** parameter on the QRadar user interface.
8. In the **Remote Host** field, type the IP address or host name of your QRadar Console or Event Collector.
9. In the **Remote Port** field, type 514.
10. Under **Event Subscriptions**, add a base logging configuration with the following parameters:

Parameter	Value
Event Category	`all`
Minimum Event Priority	`warning` **Important:** To prevent a decrease in system performance, do not use more than one word for the **Minimum Event Priority** parameter.

11. Apply the changes to the log target.
12. Review and save the configuration changes.

IBM DB2

The IBM DB2 DSM collects events from an IBM DB2 mainframe that uses IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect IBM DB2 events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html) .
2. Configure your IBM DB2 image to write events in LEEF format. For more information, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).
3. Create a log source in QRadar for IBM DB2.
4. If you want to create a custom event property for IBM DB2 in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (https://www.ibm.com/docs/en/SS2RWS_2.4.0/com.ibm.zsecure.doc_2.4.0/zsec_install.pdf).

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret

- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

Table 567. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Log File log source parameter

If QRadar does not automatically detect the log source, add a IBM z/OS, IBM CICS, IBM RACF, IBM DB2, Broadcom CA Top Secret, or Broadcom CA ACF2 log source on the QRadar Console by using the Log File Protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, or CA ACF2:

Table 568. Log File log source parameters

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	Select your DSM name.
Protocol Configuration	**Log File**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.

Table 568. Log File log source parameters (continued)	
Parameter	**Value**
Service Type	From the **Service Type** list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535. The options include ports: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.
Remote User	Type the user name or user ID necessary to log in to the system that contains your event files. • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length. • If your log files are on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.

Table 568. Log File log source parameters (continued)	
Parameter	**Value**
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <*product_name*>.<*timestamp*>.gz The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with z0S and end with .gz, type the following code: z0S.*\.gz Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions (https://docs.oracle.com/javase/tutorial/essential/regex/).
FTP Transfer Mode	This option displays only if you select **FTP** as the **Service Type**. From the list, select **Binary**. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select **SCP** as the **Service Type** you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.

Table 568. Log File log source parameters (continued)	
Parameter	**Value**
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	If you want the Log File protocol to run immediately after you click **Save**, select this check box. After the **Run On Save** completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is previously processed by the Log File protocol. If a previously processed file is detected, the Log File protocol does not download the file for processing. All files that are not previously processed are downloaded. This option applies only to FTP and SFTP service types.

Table 568. Log File log source parameters (continued)	
Parameter	**Value**
Change Local Directory?	Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the **Local Directory** field is displayed, which gives you the option to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select **LineByLine**. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

"Adding a log source" on page 5

Integrating IBM DB2 Audit Events

The IBM DB2 DSM allows you to integrate your DB2 audit logs into IBM QRadar for analysis.

The db2audit command creates a set of comma-delimited text files with a .del extension that defines the scope of audit data for QRadar when auditing is configured and enabled. Comma-delimited files created by the db2audit command include:

- audit.del
- checking.del
- context.del
- execute.del
- objmaint.del
- secmaint.del
- sysadmin.del
- validate.del

To integrate the IBM DB2 DSM with QRadar, you must:

1. Use the db2audit command to ensure the IBM DB2 records security events. See your *IBM DB2 vendor documentation* for more information.
2. Extract the DB2 audit data of events contained in the instance to a log file, depending on your version of IBM DB2.
3. Use the Log File protocol source to pull the output instance log file and send that information back to QRadar on a scheduled basis. QRadar then imports and processes this file.

Related tasks

"Extracting audit data for DB2 v8.x to v9.4" on page 928
You can extract audit data when you are using IBM DB2 v8.x to v9.4.

"Extracting audit data for DB2 v9.5" on page 928

You can extract audit data when you are using IBM DB2 v9.5.

Extracting audit data for DB2 v8.x to v9.4

You can extract audit data when you are using IBM DB2 v8.x to v9.4.

Procedure

1. Log into a DB2 account with SYSADMIN privilege.
2. Type the following start command to audit a database instance:

   ```
   db2audit start
   ```

   For example, the start command response might resemble the following output:

   ```
   AUD00001 Operation succeeded.
   ```
3. Move the audit records from the instance to the audit log:

   ```
   db2audit flush
   ```

   For example, the flush command response might resemble the following output:

   ```
   AUD00001 Operation succeeded.
   ```
4. Extract the data from the archived audit log and write the data to `.del` files:

   ```
   db2audit extract delasc
   ```

   For example, an archive command response might resemble the following output:

   ```
   AUD00001 Operation succeeded.
   ```

   Note: Double-quotation marks (") are used as the default text delimiter in the ASCII files, do not change the delimiter.
5. Remove non-active records:

   ```
   db2audit prune all
   ```
6. Move the `.del` files to a storage location where IBM QRadar can pull the file. The movement of the comma-delimited (`.del`) files should be synchronized with the file pull interval in QRadar.

   You are now ready to create a log source in QRadar to collect DB2 log files.

Extracting audit data for DB2 v9.5

You can extract audit data when you are using IBM DB2 v9.5.

Procedure

1. Log in to a DB2 account with SYSADMIN privilege.
2. Move the audit records from the database instance to the audit log:

   ```
   db2audit flush
   ```

   For example, the flush command response might resemble the following output:

   ```
   AUD00001 Operation succeeded.
   ```
3. Archive and move the active instance to a new location for future extraction:

   ```
   db2audit archive
   ```

   For example, an archive command response might resemble the following output:

   ```
   Node AUD Archived or Interim Log File Message
   ---- --- ---------------------------
   - 0 AUD00001 dbsaudit.instance.log.0.20091217125028 AUD00001 Operation succeeded.
   ```

   Note: In DB2 v9.5 and later, the archive command replaces the prune command.

The archive command moves the active audit log to a new location, effectively pruning all non-active records from the log. An archive command must be complete before an extract can be executed.

4. Extract the data from the archived audit log and write the data to `.del` files:

   ```
   db2audit extract delasc from files db2audit.instance.log.0.200912171528
   ```

   For example, an archive command response might resemble the following output:

   ```
   AUD00001 Operation succeeded.
   ```

   Note: Double-quotation marks (") are used as the default text delimiter in the ASCII files, do not change the delimiter.

5. Move the `.del` files to a storage location where IBM QRadar can pull the file. The movement of the comma-delimited (`.del`) files should be synchronized with the file pull interval in QRadar.

   You are now ready to create a log source in QRadar to collect DB2 log files.

IBM DB2 sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM DB2 sample message when you use the Syslog protocol or the Log File protocol

The following sample event message shows that there was a successful termination of a database connection.

```
"2019-06-20-05.57.54.575413","EXECUTE","CONNECT
RESET",9,0,"TESTDB","testaa","TESTAA",,0,0,"10.223.104.6.54936.190620002754","db2jcc_application",
,"TEST123",,,,,,,,,,,,,,,"OTHER",,,,,,,,,,,
```

```
 "2019-06-20-05.57.54.575413","EXECUTE","CONNECT
 RESET",9,0,"TESTDB","testaa","TESTAA",,0,0,"10.223.104.6.54936.190620002754","db2jcc_application
 ",,"TEST123",,,,,,,,,,,,,,,"OTHER",,,,,,,,,,,
```

Table 569. Highlighted values in the IBM DB2 sample event message

QRadar field name	Highlighted values in the event payload
Username	**testaa**
Log Source Time	**2019-06-20-05.57.54.575413**

IBM DLC Metrics

The IBM QRadar DSM for IBM Disconnected Log Collector Metrics collects Syslog metric events from an IBM Disconnected Log Collector Metrics device.

To integrate IBM Disconnected Log Collector Metrics with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - IBM DLC Metrics DSM RPM
2. Configure your IBM Disconnected Log Collector Metrics device to send events to QRadar. For more information, see the IBM Disconnected Log Collector documentation (https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.dlc.doc/c_dlc_overview.html).
3. If QRadar does not automatically detect the log source, add an IBM Disconnected Log Collector Metrics log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

IBM DLC Metrics DSM specifications

When you configure IBM Disconnected Log Collector, understanding the specifications for the IBM DLC Metrics DSM can help ensure a successful integration. For example, knowing what the supported version of IBM Disconnected Log Collector is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the IBM DLC Metrics DSM.

Table 570. IBM DLC Metrics DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBM DLC Metrics
RPM file name	DSM-*IBMDLCMetrics-QRadar_version-build_number*.noarch.rpm
Supported version	1.5
Protocol	Syslog, Forwarded
Event format	LEEF
Recorded event types	All DLC Metrics event types
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	IBM Disconnected Log Collector documentation (https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.dlc.doc/c_dlc_overview.html)

Configuring IBM Disconnected Log Collector to communicate with QRadar

To forward events to IBM QRadar, you must edit the configuration file on your Disconnected Log Collector (DLC) console.

Before you begin

IBM Disconnected Log Collector must be configured to collect events and forward them to QRadar. For more information, see the IBM Disconnected Log Collector documentation (https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.dlc.doc/c_dlc_overview.html).

About this task

IBM Disconnected Log Collector 1.5 sends some metric events to QRadar to monitor some key statistics from your Disconnected Log Collector. Disconnected Log Collector sends 3 different metric events once every minute.

The following table describes the 3 metric event types that are sent to QRadar.

Table 571. Metric event types that are sent to QRadar		
Component name	**Metric ID**	**Description**
EventProcessingFilterQueue	SpillFilesCount	If the incoming event rate exceeds the capacity to process the events, the count increases.
ecs-dlc_dlc_TCP_TO_QRADAR	SpillFilesCount	If DLC is disconnected, or the incoming event rate exceeds outgoing EPS setting in DLC, the count increases.
Source Monitor	EventRate	The current eps rate that is collected by DLC.

Procedure

1. Log in to your Disconnected Log console. You must have permission to edit files and restart services.
2. Go to the `/opt/ibm/si/services/dlc/conf/config.json` file.
3. Change the line `"DLCMetricsEventsEnabled":false"` to `"DLCMetricsEventsEnabled":true"`, and then save your changes.
4. To restart the Disconnected Log Collector service, type the following command:

   ```
   systemctl restart dlc
   ```

What to do next

If QRadar does not automatically detect the log source, add a Forwarded log source on the QRadar Console.

Forwarded Log source parameters for IBM DLC Metrics

If QRadar does not automatically detect the log source, add an IBM Disconnected Log Collector Metrics log source on the QRadar Console by using the Forwarded protocol.

When you use the Forwarded protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Forwarded events from IBM Disconnected Log Collector Metrics:

Table 572. Forwarded log source parameters for the IBM DLC Metrics DSM	
Parameter	**Value**
Log Source type	IBM DLC Metrics
Protocol Configuration	Forwarded
Log Source Identifier	The hostname of your IBM Disconnected Log Collector device. If Disconnected Log Collector is configured for TLS, add the UUID of the device. For example, `qavm88-145.q1labs.lab277f291f-dca9-4c59-978a-9d6deb0223b0`.

Related tasks

Adding a log source

IBM DLC Metrics sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

IBM Disconnected Log Collector sample message when you use the Syslog protocol

The following sample event message is a standard IBM DLC Metrics message that contains data for one of the Disconnected Log Collector device metrics in the payload.

```
<134>1 2020-07-30T15:01:00.759-04:00 ibm.dlcmetrics.test DLC 6074 - - [NOT:0000006000][10.0.2.3/-
-] [-/- -]LEEF:1.0|IBM|DLC|1.6.0.dev.0|DLCMetrics|
src=10.0.2.3    InstanceID=c9fb78ae-41f5-4f8d-8d61-43a87b7e3bc0    ComponentType=sources
ComponentName=Source Monitor    MetricID=EventRate Value=96.6
```

```
<134>1 2020-07-30T15:01:00.759-04:00 ibm.dlcmetrics.test DLC 6074 - - [NOT:0000006000]
[10.0.2.3/- -] [-/- -]LEEF:1.0|IBM|DLC|1.6.0.dev.0|DLCMetrics|
src=10.0.2.3    InstanceID=c9fb78ae-41f5-4f8d-8d61-43a87b7e3bc0    ComponentType=sources
ComponentName=Source Monitor    MetricID=EventRate Value=96.6
```

Table 573. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**DLCMetrics**
Source IP	**10.0.2.3** is extracted from the **src** parameter.
Device time	**2020-07-30T15:01:00.759-04:00**
Log Source Identifier	**ibm.dlcmetrics.test**

Tip: The **Event Category** value in QRadar is always **IBMDLCMetrics**.

IBM Federated Directory Server

The IBM QRadar DSM collects events from IBM Federated Directory Server systems.

The following table identifies the specifications for the IBM Federated Directory Server DSM:

Table 574. IBM Federated Directory Server DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM Federated Directory Server
RPM file name	DSM-IBMFederated DirectoryServer-*Qradar_version-build_number*.noarch.rpm
Supported versions	V7.2.0.2 and later
Event format	LEEF
Recorded event types	FDS Audit
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Security Directory Server information in the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSVJJU/welcome.html)

To send events from IBM Federated Directory Server to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - IBM Federated Directory Server DSM RPM
2. Configure QRadar monitoring on your IBM Federated Directory Server device.
3. If QRadar does not automatically detect the log source, add an IBM Federated Directory Server log source on the QRadar Console. The following table describes the parameters that require specific values for IBM Federated Directory Server event collection:

Table 575. IBM Federated Directory Serve log source parameters

Parameter	Value
Log Source type	IBM Federated Directory Server
Protocol Configuration	Syslog
Log Source Identifier	The source IP or host name of the IBM Federated Directory Server.

Related tasks

Adding a DSM

Configuring IBM Federated Directory Server to monitor security events

Configure IBM Federated Directory Server to monitor security events, which are generated when an entry is added, modified, or deleted in the target

Related information

Adding a log source

Configuring IBM Federated Directory Server to monitor security events

Configure IBM Federated Directory Server to monitor security events, which are generated when an entry is added, modified, or deleted in the target

Procedure

1. Log in to your IBM Federated Directory Server.
2. In the navigation pane, under **Common Settings**, click **Monitoring**.
3. On the **Monitoring** page, click the QRadar tab.
4. To indicate that you want to monitor security events, on the QRadar page, select **Enabled** .
5. Configure the parameters
6. In the **Map file** field, specify the path and file name of the map file that configures the various QRadar LEEF attributes for the event.
7. Click **Select** to browse for the map file. The default value points to the `LDAPSync/QRadar.map` file.
8. In the **Date format mask** field, specify a standard Java `SimpleDateFormat` mask to use for date values that are written in mapped LEEF attributes.

   This value controls both the value of the **devTimeFormat** attribute and the formatting of date values in the event. The default value is the ISO 8601 standard mask, `MMM dd yy HH:mm:ss`, which creates a string, `Oct 16 12 15:15:57`.

IBM Guardium

IBM Guardium®® is a database activity and audit tracking tool for system administrators to retrieve detailed auditing events across database platforms.

These instructions require that you install the 8.2p45 fix for InfoSphere® Guardium. For more information about this fix, see the Fix Central website at http://www.ibm.com/support/fixcentral/.

IBM QRadar collects informational, error, alert, and warnings from IBM Guardium by using syslog. IBM QRadar receives IBM Guardium Policy Builder events in the Log Event Extended Format (LEEF).

QRadar can only automatically discover and map events of the default policies that ship with IBM Guardium. Any user configured events that are required are displayed as unknowns in QRadar and you must manually map the unknown events.

Configuration overview

The following list outlines the process that is required to integrate IBM Guardium with QRadar.

1. Create a syslog destination for policy violation events. For more information, see "Creating a syslog destination for events" on page 934.
2. Configure your existing policies to generate syslog events. For more information, see "Configuring policies to generate syslog events" on page 935.
3. Install the policy on IBM Guardium. For more information, see "Installing an IBM Guardium Policy " on page 936.
4. Configure the log source in QRadar. For more information, see "Syslog log source parameters for IBM Guardium" on page 936.
5. Identify and map unknown policy events in QRadar. For more information, see "Creating an event map for IBM Guardium events" on page 936.

Creating a syslog destination for events

To create a syslog destination for these events on IBM Guardium, you must log in to the command line interface (CLI) and define the IP address for IBM QRadar.

Procedure

1. Using SSH, log in to IBM Guardium as the default user.

   Username: <*username*>

   Password: <*password*>
2. Type the following command to configure the syslog destination for informational events:

   `store remote add daemon.info <IP address>:<port> <tcp|udp>`

   For example,

   `store remote add daemon.info <IP_address> tcp`

   Where:

   - <*IP address*> is the IP address of your QRadar Console or Event Collector.
   - <*port*> is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
   - <tcp|udp> is the protocol that is used to communicate to the QRadar Console or Event Collector.
3. Type the following command to configure the syslog destination for warning events:

   `store remote add daemon.warning <IP address>:<port> <tcp|udp>`

   Where:

- <*IP address*> is the IP address of your QRadar Console or Event Collector.
- <*port*> is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
- <tcp|udp> is the protocol that is used to communicate to the QRadar Console or Event Collector.

4. Type the following command to configure the syslog destination for error events:

   `store remote add daemon.err <IP address>:<port> <tcp|udp>`

   Where:

   - <*IP address*> is the IP address of your QRadar Console or Event Collector.
   - <*port*> is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
   - <tcp|udp> is the protocol that is used to communicate to the QRadar Console or Event Collector.

5. Type the following command to configure the syslog destination for alert events:

   `store remote add daemon.alert <IP address>:<port> <tcp|udp>`

   Where:

   - <*IP address*> is the IP address of your QRadar Console or Event Collector.
   - <*port*> is the syslog port number that is used to communicate to the QRadar Console or Event Collector.
   - <tcp|udp> is the protocol that is used to communicate to the QRadar Console or Event Collector.

   You are now ready to configure a policy for IBM InfoSphere Guardium.

Configuring policies to generate syslog events

Policies in IBM Guardium are responsible for reacting to events and forwarding the event information to IBM QRadar.

Procedure

1. Click the **Tools** tab.
2. From the left navigation, select **Policy Builder**.
3. From the **Policy Finder** pane, select an existing policy and click **Edit Rules**.
4. Click **Edit this Rule individually**.

   The **Access Rule Definition** is displayed.
5. Click **Add Action**.
6. From the **Action** list, select one of the following alert types:

   - **Alert Per Match** - A notification is provided for every policy violation.
   - **Alert Daily** - A notification is provided the first time a policy violation occurs that day.
   - **Alert Once Per Session** - A notification is provided per policy violation for unique session.
   - **Alert Per Time Granularity** - A notification is provided per your selected time frame.
7. From the **Message Template** list, select QRadar.
8. From **Notification Type**, select **SYSLOG**.
9. Click **Add**, then click **Apply**.
10. Click **Save**.
11. Repeat "Configuring policies to generate syslog events" on page 935 for all rules within the policy that you want to forward to QRadar.

    For more information on configuring a policy, see your *IBM InfoSphere Guardium* vendor documentation. After you have configured all of your policies, you are now ready to install the policy on your IBM Guardium system.

Note: Due to the configurable policies, QRadar can only automatically discover the default policy events. If you have customized policies that forward events to QRadar, you must manually create a log source to capture those events.

Installing an IBM Guardium Policy

Any new or edited policy in IBM Guardium must be installed before the updated alert actions or rule changes can occur.

Procedure

1. Click the **Administration Console** tab.
2. From the left navigation, select **Configuration** > **Policy Installation**.
3. From the **Policy Installer** pane, select a policy that you modified in "Configuring policies to generate syslog events" on page 935.
4. From the **drop-down** list, select **Install and Override**.

   A confirmation is displayed to install the policy to all Inspection Engines.
5. Click **OK**.

   For more information on installing a policy, see your *IBM InfoSphere Guardium* vendor documentation. After you install all of your policies, you are ready to configure the log source in IBM QRadar.

Syslog log source parameters for IBM Guardium

If QRadar does not automatically detect the log source, add an IBM Guardium log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from IBM Guardium:

Table 576. Syslog log source parameters for the IBM Guardium DSM

Parameter	Value
Log Source type	IBM Guardium
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the IBM InfoSphere Guardium appliance.

Related tasks

"Adding a log source" on page 5

Creating an event map for IBM Guardium events

Event mapping is needed for some IBM Guardium events. Due to the customizable nature of policy rules, most events, except the default policy events do not contain a predefined IBM QRadar Identifier (QID) map to categorize security events.

About this task

You can individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track recurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for IBM Guardium are categorized as unknown. Unknown events are easily identified as the **Event Name** column and **Low Level Category** columns display Unknown.

As your device forwards events to QRadar, it can take time to categorize all events for a device. Some events might not be generated immediately by the event source appliance or software. It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, we suggest that you repeat this search until you are satisfied that most of your events are identified.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select the log source group or **Other**.

   Log sources that are not assigned to a group are categorized as Other.
6. From the **Log Source** list, select your IBM Guardium log source.
7. Click **Add Filter**.

   The **Log Activity** tab is displayed with a filter for your log source.
8. From the **View** list, select **Last Hour**.

   Any events that are generated by the IBM Guardium DSM in the last hour are displayed. Events that are displayed as unknown in the **Event Name** column or **Low Level Category** column require event mapping in QRadar.

   Note: You can save your existing search filter by clicking **Save Criteria**.

   You are now ready to modify the event map.

Modifying the event map

Modifying an event map allows for the manual categorization of events to a IBM QRadar Identifier (QID) map. Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

About this task

IBM Guardium event map events that don't have a defined log source are not mapped to an event. Events without a log source display **SIM Generic Log** in the **Log Source** column.

Procedure

1. On the **Event Name column**, double-click an unknown event for IBM Guardium.

   The detailed event information is displayed.
2. Click **Map Event**.
3. From the **Browse for QID** pane, select any of the following search options to narrow the event categories for a QRadar Identifier (QID):
   - From the **High-Level Category** list, select a high-level event categorization.
   - For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *IBM QRadar Administration Guide*.
   - From the **Low-Level Category** list, select a low-level event categorization.
   - From the **Log Source Type** list, select a log source type.

   The **Log Source Type** list gives the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, IBM Guardium provides policy events, you might select another product that likely captures similar events.
4. To search for a QID by name, type a name in the **QID/Name** field.

The **QID/Name** field gives the option to filter the full list of QIDs for a specific word, for example, policy.

5. Click **Search**.

   A list of QIDs are displayed.

6. Select the QID you want to associate to your unknown event.
7. Click **OK**.

   QRadar maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.

   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

IBM Guardium sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Guardium sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that an attempted login to the database is not successful.

```
<30>Aug 19 12:33:31 ibm.guardium.test guard_sender[4486]:
LEEF:1.0|IBM|Guardium|8.0|Login failures|ruleID=20026|ruleDesc=Login failures|severity=INFO|
devTime=2013-8-19 6:34:41|serverType=DB2|classification=|category=|dbProtocolVersion=3.0|usrName=|
sourceProgram=DB2JCC_APPLICATION|start=1376908481000|dbUser=user|dst=10.30.2.124|dstPort=50000|
src=10.30.5.152|srcPort=38754|protocol=TCP|type=LOGIN_FAILED|violationID=15|sql=|error=08001-
XXXX:30082-01
```

```
<30>Aug 19 12:33:31 ibm.guardium.test guard_sender[4486]:
LEEF:1.0|IBM|Guardium|8.0|Login failures|ruleID=20026|ruleDesc=Login
failures|severity=INFO|devTime=2013-8-19 6:34:41|serverType=DB2|classification=|category=|
dbProtocolVersion=3.0|usrName=|sourceProgram=DB2JCC_APPLICATION|start=1376908481000|dbUser=user|
dst=10.30.2.124|dstPort=50000|src=10.30.5.152|srcPort=38754|protocol=TCP|type=LOGIN_FAILED|
violationID=15|sql=|error=08001-XXXX:30082-01
```

Table 577. Highlighted values in the IBM Guardium sample event

QRadar field name	Highlighted values in the event payload
Event ID	**Login failures**
Username	**user**
Source IP	**10.30.5.152**
Source port	**38754**
Destination IP	**10.30.2.124**
Destination port	**50000**
Device time	**Aug 19 12:33:31**

Sample 2: The following sample event message shows that unauthorized users on cardholder objects are detected.

```
<25>Jun 11 13:47:19 ibm.guardium.test guard_sender[3432]: LEEF:1.0|IBM|Guardium|8.0|Unauthorized
Users on Cardholder Objects - Alert|ruleID=159|ruleDesc=Unauthorized  Users on
Cardholder Objects - Alert|severity=MED|devTime=2013-6-11 12:46:21|serverType=MS SQL SERVER|
classification=Violation|category=PCI|dbProtocolVersion=8.0|usrName=|sourceProgram=ABCDEF.EXE|
start=1370965581000|dbUser=SYSTEM|dst=172.16.107.92|dstPort=1433|src=172.16.107.92|srcPort=60621|
protocol=TCP|type=SQL_LANG|violationID=0|sql=SELECT * FROM EPOAgentHandlerAssignment
```

```
INNER JOIN EPOAgentHandlerAssignmentPriority ON (EPOAgentHandlerAssignment.AutoID
= EPOAgentHandlerAssignmentPriority.AssignmentID) ORDER BY
EPOAgentHandlerAssignmentPriority.Priority ASC|error=TDS_MS-
```

```
<25>Jun 11 13:47:19 ibm.guardium.test guard_sender[3432]: LEEF:1.0|IBM|Guardium|8.0|
Unauthorized  Users on Cardholder Objects - Alert|ruleID=159|ruleDesc=Unauthorized
Users on Cardholder Objects - Alert|severity=MED|devTime=2013-6-11 12:46:21|
serverType=MS SQL SERVER|classification=Violation|category=PCI|dbProtocolVersion=8.0|usrName=|
sourceProgram=ABCDEF.EXE|start=1370965581000|dbUser=SYSTEM|dst=172.16.107.92|dstPort=1433|
src=172.16.107.92|srcPort=60621|protocol=TCP|type=SQL_LANG|violationID=0|sql=SELECT * FROM
EPOAgentHandlerAssignment INNER JOIN EPOAgentHandlerAssignmentPriority ON
(EPOAgentHandlerAssignment.AutoID = EPOAgentHandlerAssignmentPriority.AssignmentID) ORDER
BY EPOAgentHandlerAssignmentPriority.Priority ASC|error=TDS_MS-
```

Table 578. Highlighted values in the IBM Guardium sample event

QRadar field name	Highlighted values in the event payload
Event ID	**Unauthorized Users on Cardholder Objects - Alert**
Username	**SYSTEM**
Source IP	**172.16.107.92**
Source port	**60621**
Destination IP	**172.16.107.92**
Destination port	**1433**
Device time	**Jun 11 13:47:19**

IBM i

The IBM QRadar DSM for IBM i, formerly known as AS/400 iSeries, collects audit records and event information from IBM i systems.

The following table identifies the specifications for the IBM i DSM:

Table 579. IBM i DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM i
Supported versions	5R4
RPM file name	DSM-IBMi-*QRadar_version-build_number*.noarch.rpm
Protocol	Log File Protocol Syslog
Event Format	• Common Event Format (CEF) - CEF:0 is supported. • Log Event Extended Format (LEEF) - LEEF:1.0 is supported.
Recorded event types	Audit records and events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No

Table 579. IBM i DSM specifications (continued)	
Specification	**Value**
More information	IBM website (http://www.ibm.com/)

To collect events from IBM i systems, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM i DSM RPM from the IBM Support Website onto your QRadar Console.
2. Configure your IBM i system to communicate with QRadar.
3. Add an IBM i log source on the QRadar Console by using the following table to configure the parameters that are required to collect IBM i events:

Table 580. IBM i log source parameters	
Parameter	**Value**
Log Source Type	IBM i
Protocol Configuration	Log File If you are using the PowerTech Interact or LogAgent for System i® software to collect CEF formatted syslog messages, you must select the **Syslog** option
Service Type	Secure File Transfer Protocol (SFTP)

For more information about configuring parameters for the Log File protocol, see Log File protocol configuration options.

Related tasks

Configuring IBM i to integrate with IBM QRadar
You can integrate IBM i with IBM QRadar.

Adding a DSM

Configuring Townsend Security Alliance LogAgent to integrate with QRadar
You can collect all audit logs and system events from Townsend Security Alliance LogAgent. You must configure Alliance LogAgent for the IBM QRadar LEEF and configure a destination that specifies QRadar as the syslog server.

Related information

Adding a log source

Configuring IBM i to integrate with IBM QRadar

You can integrate IBM i with IBM QRadar.

Procedure

1. From IBM Fix Central (http://www.ibm.com/support/fixcentral), download the following file:

   `AJLIB.SAVF`
2. Copy the `AJLIB.SAVF` file to a computer or terminal that has FTP access to IBM i.
3. Create a generic online SAVF file on the IBM i by typing the following command:

   ```
   CRTSAVF  QGPL/SAVF
   ```
4. Use FTP on the computer or terminal to replace the IBM i generic SAVF file with the `AJLIB.SAVF` file that you downloaded.

   Type the following commands:

```
bin
cd qgpl
lcd c:\
put ajlib.savf AJLIB
quit
```

If you are transferring your SAVF file from another IBM i system, send the file by placing the FTP sub-command mode BINARY before the GET or PUT statement.

5. Restore the AJLIB file on IBM i by typing the following command:

   ```
   RSTLIB SAVLIB(AJLIB) DEV(*SAVF) SAVF(QGPL/AJLIB)
   ```

   AJLIB provides the mapping and data transfer support that is needed to send IBM i audit journal entries to QRadar.

6. Run **AJLIB/SETUP**

   The setup screen is used to configure AJLIB for FTP, SFTP, or a local path to receive the processed entries.

   The server user ID is required for FTP or SFTP, and a password is required for FTP. While FTP handles line delimiter conversions, you set the line feed to the expected value for the type of system that receives the SFTP transfers.

7. If you want to use SFTP, run **AJLIB/GENKEY**.

   This command generates the SSH key pair that is required for SFTP authentication. If the key pair exists, it is not replaced. If you want to generate a new key pair, before you run this command, remove the existing key files from the `/ajlib/.ssh` directory.

   For more information about SSH key pair configuration on the IBM i , see http://www-01.ibm.com/support/docview.wss?uid=nas8N1012710

8. After you generate a key pair, use the following steps to enable the use of the key pair on the server:

   a) Copy the `id_rsa.pub` file from the `/ajlib` directory to the SSH server, and then install it in the appropriate folder.

   b) Ensure that the SSH server is added to the `known_hosts` file of the user profile that runs the **AJLIB/AUDITJRN** command.

9. Use the appropriate user profile to do the following steps:

   a) Start a PASE (Portable Application Solutions Environment) shell by typing the following command:

      ```
      call qp2term
      ```

   b) Start a session with the SSH server by typing the following command:

      ```
      ssh -T <user>@<serveraddress>
      ```

   c) If prompted, accept the system key, and enter a password.

   d) Type `exit`, to close the SSH session.

   If you want to run these steps under a different IBM i profile than the one that runs the **AJLIB/AUDITRN** command, copy the `.ssh` directory and `known_hosts` file to the home directory of the profile that is used to run this command.

10. To configure the filtering of specific entry types, use the **AJLIB/SETENTTYP** command.

11. Set up the data collection start date and time for the audit journal library (AJLIB) by typing the following command:

    ```
    AJLIB/DATETIME
    ```

    If you start the audit journal collector, a failure message is sent to QSYSOPR.

    The setup function sets a default start date and time for data collection from the audit journal to 08:00:00 of the current day.

To preserve your previous start date and time information from a previous installation, you must run **AJLIB/DATETIME**. Record the previous start date and time and type those values when you run **AJLIB/SETUP**. The start date and time must contain a valid date and time in the six character system date and system time format. The end date and time must be a valid date and time or left blank.

12. Run **AJLIB/AUDITJRN**.

    The audit journal collection program starts and sends the records to your remote FTP server: If the transfer to the FTP server fails, a message is sent to QSYS0PR. The process for starting **AJLIB/AUDITJRN** is typically automated by an IBM i job Scheduler, which collects records periodically.

    If the FTP transfer is successful, the current date and time information is written into the start time for **AJLIB/DATETIME** to update the gather time, and the end time is set to blank. If the FTP transfer fails, the export file is erased and no updates are made to the gather date or time.

What to do next

For more information about AJLIB field definitions, see Commonly asked IBM i (AS/400 iSeries) DSM Integration Questions for QRadar (https://www.ibm.com/support/pages/node/246075).

Manually extracting journal entries for IBM i

You can run the DSPJRN command to extract journal entries for IBM i when an audit journal receiver chain is broken.

About this task

Run the ALJIB/DATETIME command to set the Start Date to *OUTF. This command forces the processing program to use the pre-built QTEMP/AUDITJRN outfile for parsing, instead of using the date time to extract journal entries. After you run the parsing program command AJLIB/AUDITJRN, the DATETIME is set to the new processing date.

Procedure

1. Log in to your IBM i system command-line interface (CLI).
2. Run **DSPJRN**.

   The only changeable parameters in the following example are **RCVRNG** and **ENTTYP**. Do not change any other command parameters. Ensure that **ENTTP** matches the **AJLIB/SETENTTYP** command settings.

   ```
   DSPJRN JRN(QSYS/QAUDJRN) RCVRNG(AUDRCV0001 AUDRCV0003)
   JRNCDE((T)) ENTTYP(*ALL)
   OUTPUT(*OUTFILE) OUTFILFMT(*TYPE5) OUTFILE(QTEMP/AUDITJRN)
   ENTDTALEN(*VARLEN 16000 100)
   ```

3. To set the **Date Time** to use outfile ***OUTF** support, run the **AJLIB/DATETIME** command.

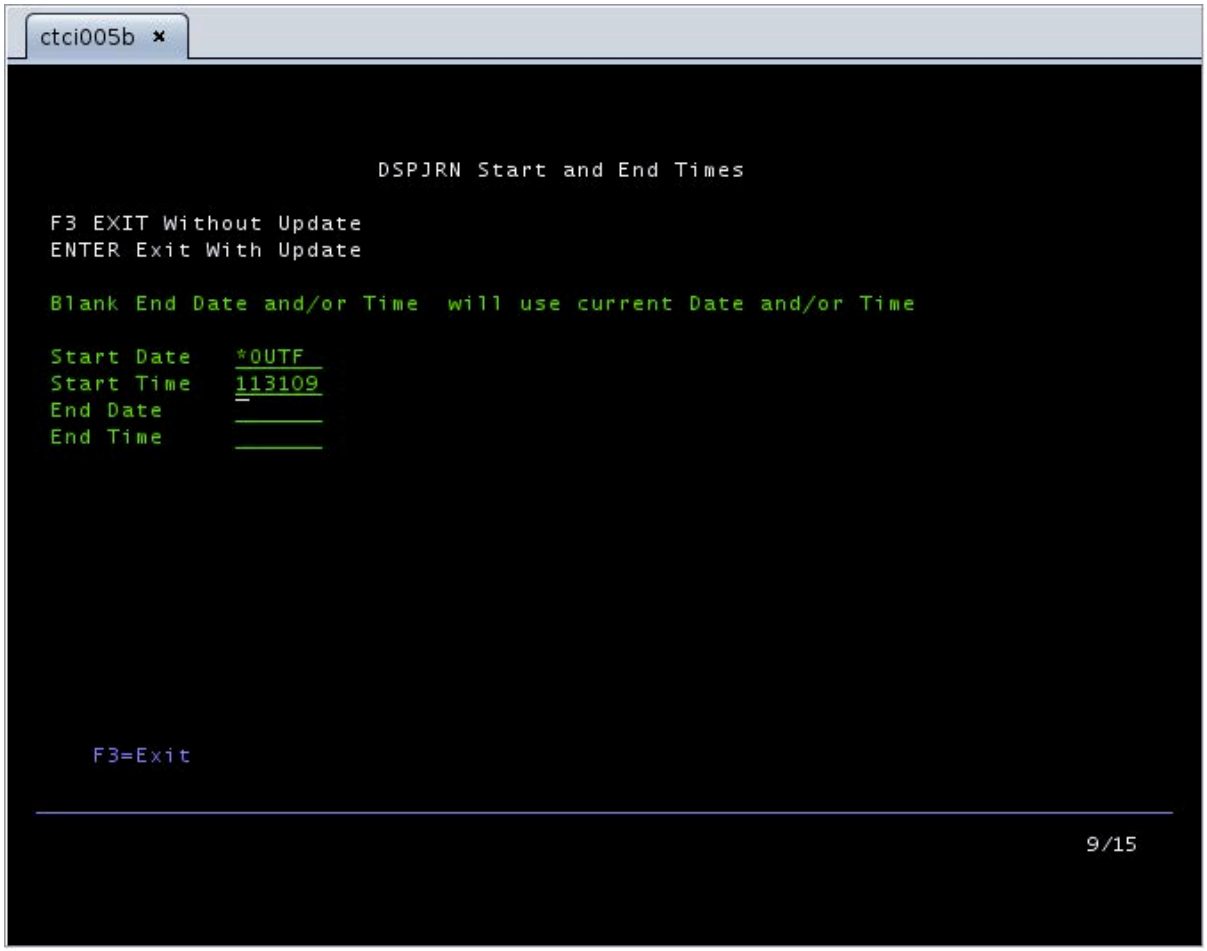


Figure 45. DSPJRN Start and End Times

4. Run **AJLIB/AUDITJRN**.

Results

The **DATETIME** is set to the next start date.

Pulling Data when you use the Log File Protocol

You can configure IBM i as the log source, and to use the log file protocol in IBM QRadar:

Procedure

1. To configure QRadar to receive events from an IBM i system, you must select the IBM i option from the **Log Source Type** list when you add a log source in QRadar.
2. To configure the log file protocol for the IBM i DSM, you must select the **Log File** option from the **Protocol Configuration** list and define the location of your FTP server connection settings.

   Note: If you are using the PowerTech Interact or LogAgent for System i software to collect CEF formatted syslog messages, you must select the **Syslog** option from the **Protocol Configuration** list.
3. Use the log file protocol option that you select a secure protocol for transferring files, such as Secure File Transfer Protocol (SFTP).

What to do next

For a complete list of Log File protocol parameter options, see Log File protocol configuration options.

Related tasks

"Adding a log source" on page 5

Configuring Townsend Security Alliance LogAgent to integrate with QRadar

You can collect all audit logs and system events from Townsend Security Alliance LogAgent. You must configure Alliance LogAgent for the IBM QRadar LEEF and configure a destination that specifies QRadar as the syslog server.

Procedure

1. Log in to your Townsend Security Alliance LogAgent appliance.
2. Add the **ALLSYL100** to your library list by typing the following command: **`addlible allsy1100`**.
3. To display the main menu select **go symain**.
4. Select the option for Configuration
5. Select **Configure Alliance LogAgent** and configure the following parameters.

Parameter	Description
Interface version	4=IBM QRadar LEEF
Transmit	1=Yes
Data queue control	1=Yes
Format	4=IBM QRadar LEEF

6. From the configuration menu, select **Work With TCP Clients**.
7. Select option 2 to change the **SYSLOGD** client and configure the following parameters.

Parameter	Description
Status	1=Active
Autostart client	1=Yes
Remote IP address	IP address of QRadar
Remote port number	514

8. From the **Configuration** menu, select **Start LogAgent Subsystem**. Events flow to QRadar.

What to do next

After TCP services start, consider automatically starting the Alliance LogAgent subsystem by modifying your `IPL  QSTRUP` program to include the following statements:

```
/* START ALLIANCE LOGAGENT */
QSYS/STRSBS ALLSYL100/ALLSYL100
MONMSG MSGID(CPF0000)
```

For more information about installing and configuring for **Independent Auxiliary Storage Pool** operation, and more filter options for events, see your vendor documentation.

IBM i sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

IBM i sample message when you use the Syslog protocol

The following sample event message shows that DRDA Distributed Relational DB access is allowed.

Important: The logs that you send to QRadar must be tab-delimited. If you cut and paste the code from this sample, make sure that you press the tab key where indicated by the *<tab>* variables, then remove the variables.

```
<176>Apr 24 15:31:58 ibm.i.test LEEF:1.0|Raz-Lee iSecurity|Firewall|1.0|GRE7860|
usrName=USERNAME<tab>devTime=2019-04-24-15.31.58.000<tab>devTimeFormat=yyyy-MM-dd-
HH.mm.ss.SSS<tab>source=172.16.1.1<tab>sev=10<tab>jobName=948290/QUSER/
QRWTSRVR<tab>pgmName=*NONE<tab>pgmLib=*NONE<tab>entryType=36/A<tab>entryDesc=DRDA Distributed
Relational DB access<tab>Action_allowed=1<tab>Src_user_before_Pre-
chk=USERNAME<tab>Source_system=SYSTEM1<tab>Decision_level=USSRV<tab>Authority_set_to_user=USERNA
ME<tab>Server_Id=36
```

Table 581. Highlighted values in the IBM i event payload

QRadar field name	Highlighted values in the event payload
Event ID	**GRE7860**
Username	**USERNAME**
Severity	**10**

IBM IMS

The IBM Information Management System (IMS) DSM for IBM QRadar allows you to use an IBM mainframe to collect events and audit IMS database transactions.

To integrate IBM IMS events with QRadar, you must download scripts that allow IBM IMS events to be written to a log file.

Overview of the event collection process:

1. The IBM mainframe records all security events as Service Management Framework (SMF) records in a live repository.
2. The IBM IMS data is extracted from the live repository using the SMF dump utility. The SMF file contains all of the events and fields from the previous day in raw SMF format.
3. The `qeximsloadlib.trs` program pulls data from the SMF formatted file. The `qeximsloadlib.trs` program only pulls the relevant events and fields for QRadar and writes that information in a condensed format for compatibility. The information is saved in a location accessible by QRadar.
4. QRadar uses the log file protocol source to retrieve the output file information for QRadar on a scheduled basis. QRadar then imports and processes this file.

Configuring IBM IMS

You can integrate IBM IMS with QRadar:

Procedure

1. From the IBM support website (http://www.ibm.com/support), download the following compressed file:

   `QexIMS_bundled.tar.gz`
2. On a Linux-based operating system, extract the file:

   `tar -zxvf qexims_bundled.tar.gz`

   The following files are contained in the archive:

   - `qexims_jcl.txt` - Job Control Language file
   - `qeximsloadlib.trs` - Compressed program library (requires IBM TRSMAIN)
   - `qexims_trsmain_JCL.txt` - Job Control Language for TRSMAIN to decompress the `.trs` file

3. Load the files onto the IBM mainframe by using the following methods:

   Upload the sample `qexims_trsmain_JCL.txt` and `qexims_jcl.txt` files by using the TEXT protocol.
4. Upload the `qeximsloadlib.trs` file by using BINARY mode transfer and append to a pre-allocated data set. The `qeximsloadlib.trs` file is a tersed file that contains the executable (the mainframe program QexIMS). When you upload the `.trs` file from a workstation, pre-allocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL= 1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

   Note: QexIMS is a small C mainframe program that reads the output of the IMS log file (EARLOUT data) line by line. QexIMS adds a header to each record that contains event information, for example, record descriptor, the date, and time. The program places each field into the output record, suppresses trailing blank characters, and delimits each field with the pipe character. This output file is formatted for QRadar and the blank suppression reduces network traffic to QRadar. This program does not need much CPU or I/O disk resources.
5. Customize the `qexims_trsmain_JCL.txt` file according to your installation-specific information for parameters.

   For example, jobcard, data set naming conventions, output destinations, retention periods, and space requirements.

   The `qexims_trsmain_JCL.txt` file uses the IBM utility TRSMAIN to extract the program that is stored in the `qeximsloadlib.trs` file.

   An example of the `qexims_trsmain_JCL.txt` file includes:

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V
//DEL EXEC PGM=IEFBR14 //D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXIMS.TRS
// UNIT=SYSDA, // SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE DD DISP=SHR,DSN=<yourhlq>.QEXIMS.TRS
//OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD, // SPACE=(CYL,(1,1,5),RLSE),UNIT=SYSDA
//
```

   The `.trs` input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the qexims program as a member.
6. You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in LINKLST. The program does not require authorization.
7. The `qexims_jcl.txt` file is a text file that contains a sample JCL. You must configure the job card to meet your configuration.

   The `qexims_jcl.txt` sample file includes:

```
//QEXIMS JOB (T,JXPO,JKSD0093),DEV,NOTIFY=Q1JACK,
// MSGCLASS=P,
// REGION=0M //* //*QEXIMS JCL VERSION 1.0 FEBRUARY 2011
//*
//*************************************************************
//* Change dataset names to site specific dataset names *
```

```
//*************************************************************
//SET1 SET IMSOUT='Q1JACK.QEXIMS.OUTPUT',
// IMSIN='Q1JACK.QEXIMS.INPUT.DATA'
//*************************************************************
//* Delete old datasets *
//*************************************************************
//DEL EXEC PGM=IEFBR14 //DD1 DD DISP=(MOD,DELETE),DSN=&IMSOUT,
// UNIT=SYSDA, // SPACE=(CYL,(10,10)), // DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset
//*************************************************************
//ALLOC EXEC PGM=IEFBR14 //DD1 DD DISP=(NEW,CATLG),DSN=&IMSOUT,
// SPACE=(CYL,(21,2)),
```

```
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//EXTRACT EXEC PGM=QEXIMS,DYNAMNBR=10,
// TIME=1440 //STEPLIB DD DISP=SHR,DSN=Q1JACK.C.LOAD
//SYSTSIN DD DUMMY
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=* //IMSIN DD DISP=SHR,DSN=&IMSIN
//IMSOUT DD DISP=SHR,DSN=&IMSOUT
//*FTP EXEC PGM=FTP,REGION=3800K //*INPUT DD *
//*<target server>
//*<USER>
//*<PASSWORD>
//*ASCII //*PUT '<IMSOUT>' /TARGET DIRECTORY>/<IMSOUT>
//*QUIT
//*OUTPUT DD SYSOUT=* //*SYSPRINT DD SYSOUT=*
//*
```

8. After the output file is created, you must make one of the following choices:
   - Schedule a job to transfer the output file to an interim FTP server.
   - Each time the job completes, the output file is forwarded to an interim FTP server. You must configure the following parameters in the sample JCL to successfully forward the output to an interim FTP server:

   For example:

   ```
   //*FTP EXEC PGM=FTP,REGION=3800K
   //*INPUT DD *
   //*<target server>
   //*<USER>
   //*<PASSWORD> //*ASCII //*PUT '<IMSOUT>'
   /TARGET DIRECTORY>/<IMSOUT>
   //*QUIT //*OUTPUT DD SYSOUT=*
   //*SYSPRINT DD SYSOUT=*
   ```

   Where:

   - <*target server*> is the IP address or host name of the interim FTP server to receive the output file.
   - <*USER*> is the user name required to access the interim FTP server.
   - <*PASSWORD*> is the password required to access the interim FTP server.
   - <*IMSOUT*> is the name of the output file saved to the interim FTP server.

   For example:

   ```
   PUT 'Q1JACK.QEXIMS.OUTPUT.C320' /192.0.2.1/IMS/QEXIMS.OUTPUT.C320
   ```

   Note: You must remove commented lines that begin with //* for the script to properly forward the output file to the interim FTP server.

   You are now ready to configure the log file protocol.
9. Schedule QRadar to retrieve the output file from IBM IMS.

   If the mainframe is configured to serve files through FTP, SFTP, or allow SCP, then no interim FTP server is required and QRadar can pull the output file directly from the mainframe. The following text must be commented out using //* or deleted from the `qexims_jcl.txt` file:

   ```
   //*FTP EXEC PGM=FTP,REGION=3800K //*INPUT DD *
   //*<target server>
   //*<USER> //*<PASSWORD> //*ASCII
   //*PUT '<IMSOUT>'
   /<TARGET DIRECTORY>/<IMSOUT>
   //*QUIT //*OUTPUT DD SYSOUT=*
   //*SYSPRINT DD SYSOUT=*
   ```

   You are now ready to configure the log file protocol.

Log File log source parameters for IBM IMS

If QRadar does not automatically detect the log source, add an IBM IMS log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM IMS:

Table 582. Log File log source parameters for the IBM IMS DSM

Parameter	Value
Log Source type	IBM IMS
Protocol Configuration	Log File
Log Source Identifier	Type the IP address or host name for the log source. The log source identifier must be unique for the log source type.

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related tasks

"Adding a log source" on page 5

IBM Informix Audit

The IBM Informix® Audit DSM allows IBM QRadar to integrate IBM Informix audit logs into QRadar for analysis.

QRadar retrieves the IBM Informix archived audit log files from a remote host using the log file protocol configuration. QRadar records all configured IBM Informix Audit events.

When configuring your IBM Informix to use the log file protocol, make sure the host name or IP address configured in the IBM Informix is the same as configured in the **Remote Host** parameter in the log file protocol configuration.

You are now ready to configure the log source and protocol in QRadar:

- To configure QRadar to receive events from an IBM Informix device, you must select the IBM Informix Audit option from the **Log Source Type** list.
- To configure the log file protocol, you must select the **Log File** option from the **Protocol Configuration** list.

Use a secure protocol for transferring files, such as Secure File Transfer Protocol (SFTP).

Related concepts

"Log File protocol configuration options" on page 155
To receive events from remote hosts, configure a log source to use the Log File protocol.

Related tasks

"Adding a log source" on page 5

IBM Lotus Domino

You can integrate an IBM Lotus® Domino® device with IBM QRadar. An IBM Lotus Domino device accepts events by using SNMP.

Setting Up SNMP Services

Set up SNMP services on the IBM Lotus Domino server to accept events.

Procedure

1. Install the Lotus Domino SNMP Agent as a service. From the command prompt, go to the Lotus\Domino directory and type the following command:

   ```
   lnsnmp -SC
   ```
2. Confirm that the Microsoft SNMP service is installed.
3. Start the SNMP and LNSNMP services. From a command prompt, type the following commands:
   - `net start snmp`
   - `net start lnsnmp`
4. Select **Start** > **Program** > **Administrative Tools** > **Services** to open the **Services MMC**
5. Double-click on the **SNMP** service and select the **Traps** tab.
6. In the **Community name** field, type `public` and click **add to list**.
7. In the **Traps destinations** section, select **Add** and type the IP address of your IBM QRadar. Click **Add**.
8. Click **OK**.
9. Confirm that both SNMP agents are set to **Automatic** so they run when the server boots.

Setting up SNMP in AIX

TCP/IP and SNMP must be properly installed and configured on the server before you set up SNMP in AIX.

Before you begin

You must log in as a root user.

Procedure

1. Stop the LNSNMP service with the following command:

   ```
   lnsnmp.sh stop
   ```
2. Stop the SNMP subsystem with the following command:

   ```
   stopsrc -s snmpd
   ```
3. Configure SNMP to accept LNSNMP as an SMUX peer. Add the following line to `/etc/snmpd.peers`

   ```
   "Lotus Notes Agent" 1.3.6.1.4.1.334.72 "NotesPasswd"
   ```
4. Configure SNMP to accept an SMUX association from LNSNMP. Add the following line to `/etc/snmpd.conf` or `/etc/snmpdv3.conf`

   ```
   smux 1.3.6.1.4.1.334.72 NotesPasswd
   ```
5. Start the SNMP subsystem with the following command:

   ```
   startsrc -s snmpd
   ```
6. Start the LNSNMP service with the following command:

   ```
   lnsnmp.sh start
   ```
7. Create a link to the LNSNMP script

   ```
   ln -f -s /opt/ibm/lotus/notes/latest/ibmpow/lnsnmp.sh /etc/lnsnmp.rc
   ```

8. Configure LNSNMP service to start during the system restart. Add the following line to the end of `/etc/rc.tcpip`

   ```
   /etc/lnsnmp.rc start
   ```

Starting the Domino Server Add-in Tasks

After you configure the SNMP services, you must start the Domino server add-in tasks for each Domino partition.

Procedure

1. Log in to the Domino Server console.
2. To support SNMP traps for Domino events, type the following command to start the Event Interceptor add-in task:

   ```
   load intrcpt
   ```
3. To support Domino statistic threshold traps, type the following command to start the Statistic Collector add-in task:

   ```
   load collect
   ```
4. Arrange for the add-in tasks to be restarted automatically the next time that Domino is restarted. Add **`intrcpt`** and **`collect`** to the *ServerTasks* variable in Domino's `NOTES.INI file`.

Configuring SNMP Services

You can configure SNMP services:

About this task

Configurations might vary depending on your environment. See your vendor documentation for more information.

Procedure

1. Open the Domino Administrator utility and authenticate with administrative credentials.
2. Click the **Files** tab, and the **Monitoring Configuration** (`events4.nsf`) document.
3. Expand the **DDM Configuration** Tree and select **DDM Probes By Type**.
4. Select **Enable Probes**, and then select **Enable All Probes In View**.

   Note: You might receive a warning when you complete this action. This warning is a normal outcome, as some of the probes require more configuration.
5. Select **DDM Filter**.

   You can either create a new DDM Filter or edit the existing DDM Default Filter.
6. Apply the DDM Filter to enhanced and simple events. Choose to log all event types.
7. Depending on the environment, you can choose to apply the filter to all servers in a domain or only to specific servers.
8. Click **Save**. Close when finished.
9. Expand the **Event Handlers** tree and select **Event Handlers By Server**.
10. Select **New Event Handler**.
11. Configure the following parameters:

    - **Basic - Servers to monitor**: Choose to monitor either all servers in the domain or only specific servers.
    - **Basic - Notification trigger**: Any event that matches the criteria.
    - **Event - Criteria to match**: Events can be any type.

- **Event - Criteria to match**: Events must be one of these priorities (Check all the boxes).
- **Event - Criteria to match**: Events can have any message.
- **Action - Notification method**: SNMP Trap.
- **Action - Enablement**: Enable this notification.

12. Click **Save**. Close when finished.

    You are now ready to configure the log source in IBM QRadar.

SNMPv2 log source parameters for IBM Lotus Domino

If QRadar does not automatically detect the log source, add an IBM Lotus Domino log source on the QRadar Console by using the SNMPv2 protocol.

When using the SNMPv2 protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMPv2 events from IBM Lotus Domino:

Table 583. SNMPv2 log source parameters for the IBM Lotus Domino DSM

Parameter	Value
Log Source type	IBM Lotus Domino
Protocol Configuration	SNMPv2
Log Source Identifier	Type an IP address, host name, or name to identify the SNMPv2 event source. IP addresses or host names are recommended as they allow QRadar to identify a log file to a unique event source.

For a complete list of SNMPv2 protocol parameters and their values, see "SNMPv2 protocol configuration options" on page 216.

Related tasks

"Adding a log source" on page 5

IBM Lotus Domino sample event messages

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Lotus Domino sample message when you use the SNMPv2 protocol

The following sample event message shows the successful authentication for SMTP server.

```
CN=w2k864d/O=q1labs 6 5 1248804028 SMTP Server: Authentication succeeded for user testuser;
connecting host example.com 17863
```

Table 584. Highlighted fields in the IBM Lotus Domino event

QRadar field name	Highlighted payload field name
Event ID	The event ID in QRadar is **smtp_auth_succeeded**.
Username	**testuser**
Device Time	The device time in QRadar is **Tuesday July 28, 2009 15:00:28 (pm)**.

IBM MaaS360 Security

The IBM MaaS360 Security DSM for IBM QRadar collects event logs from the MaaS360 Security console.

The following table identifies the specifications for the IBM MaaS360 Security DSM:

Table 585. IBM MaaS360 Security DSM Specification	
Specification	**Value**
Manufacturer	IBM
DSM name	IBM MaaS360 Security
RPM file name	DSM-IBMFiberlinkMaaS360
Supported versions	N/A
Event format	LEEF, JSON
QRadar recorded event types	Compliance rule events Device enrollment events Action history events
Automatically discovered?	No
Included identity?	Yes
Includes custom properties?	No
More information	MaaS360 Security website (http://www.maas360.com/)

To integrate IBM MaaS360 Security with QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - DSMCommon RPM
   - IBM Fiberlink REST API Protocol RPM
   - IBM MaaS360 Security RPM
2. Configure your MaaS360 Security instance to enable communication with QRadar.
3. Add an IBM MaaS360 Security log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

IBM Fiberlink REST API log source parameters for IBM MaaS360 Security

If QRadar does not automatically detect the log source, add a IBM MaaS360 Security log source on the QRadar Console by using the IBM Fiberlink REST API protocol.

When using the IBM Fiberlink REST API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect IBM Fiberlink REST API events from IBM MaaS360 Security:

Table 586. IBM Fiberlink REST API log source parameters for the IBM MaaS360 Security DSM	
Parameter	**Value**
`Log Source type`	IBM MaaS360 Security

Table 586. IBM Fiberlink REST API log source parameters for the IBM MaaS360 Security DSM (continued)	
Parameter	**Value**
Protocol Configuration	IBM Fiberlink REST API
Log Source Identifier	Type a unique identifier for the log source. The **Log Source Identifier** can be set to any valid value and does not need to reference a specific server. You can set the **Log Source Identifier** to the same value as the Log Source Name. If you have more than one IBM MaaS360 Security log source that is configured, you might want to identify the first log source as *MaaS3601*, the second log source as *MaaS3602*, and the third log source as *MaaS3603*.

For a complete list of IBM Fiberlink REST API protocol parameters and their values, see IBM Fiberlink REST API protocol configuration options.

Related concepts

IBM MaaS360 Security sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Related tasks

"Adding a log source" on page 5

IBM MaaS360 Security sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM MaaS360 Security sample message when you use the IBM Fiberlink REST API protocol

The following sample event message shows that a Change Policy is executed for OS versions in IBM MaaS360 Security.

```
LEEF:1.0|IBM|Fiberlink MaaS360|1.0|OS Versions|cat=Change Policy - Executed     usrName=test 1
devTime=2014-05-08T07:29:26Z    devTimeFormat=yyyy-MM-dd&aaaa;T&aaaa;HH:mm:ss&aaaa;Z&aaaa;
ruleset=1040 psr kr rule        platformName=aAA        deviceName=Aaaaaa&aaaa;s iAaa
aaaaa     rule=OS Versions        action=Change Policy    actionStatus=Executed
maas360DeviceID=AaaaA1AAAAAAAA1
```


```
LEEF:1.0|IBM|Fiberlink MaaS360|1.0|OS Versions|cat=Change Policy - Executed     usrName=test 1
devTime=2014-05-08T07:29:26Z    devTimeFormat=yyyy-MM-dd&aaaa;T&aaaa;HH:mm:ss&aaaa;Z&aaaa;
ruleset=1040 psr kr rule        platformName=aAA        deviceName=Aaaaaa&aaaa;s iAaa
aaaaa     rule=OS Versions        action=Change Policy    actionStatus=Executed
maas360DeviceID=AaaaA1AAAAAAAA1
```


Table 587. Highlighted values in the IBM MaaS360 Security event	
QRadar field name	**Highlighted values in the payload**
Event ID	**OS Versions**
Event Category	**Change Policy - Executed**
Username	**test 1**

Related concepts

IBM Fiberlink REST API log source parameters for IBM MaaS360 Security

IBM Manage Virtual Server

The IBM QRadar DSM for IBM Manage Virtual Server collects events that are generated by the QRadar IBM Manage Virtual Server process.

To integrate IBM Manage Virtual Server with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website. Download and install the most recent version of the **IBMManageVirtualServer DSM** RPM on your QRadar Console.
2. If QRadar does not automatically detect the log source, add an IBM Manage Virtual Server log source on the QRadar Console. For more information, see "Syslog log source parameters for IBM Manage Virtual Server" on page 954.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

IBM Manage Virtual Server DSM specifications

The IBM QRadar DSM for IBM Manage Virtual Server supports events that are generated by the IBM Manage Virtual Server process with the help of Syslog protocol.

The following table lists the specifications for the IBM Manage Virtual Server DSM.

Table 588. IBM Manage Virtual Server DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBMManageVirtualServer
RPM file name	DSM-*IBMManageVirtualServer-QRadar_version-Build_number*.noarch.rpm
Supported protocols	Syslog
Event format	Log Event Extended Format (LEEF)
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No

Syslog log source parameters for IBM Manage Virtual Server

If QRadar does not automatically detect the log source, add an IBM Manage Virtual Server log source on the QRadar Console by using the Syslog protocol.

The following table describes the parameters that require specific values to collect Syslog events from the IBM Manage Virtual Server:

Table 589. IBM Manage Virtual Server log source parameters

Parameter	**Value**
Log Source Name	Type a name for the log source.
Log Source Description	Type a description for the log source.

Table 589. IBM Manage Virtual Server log source parameters (continued)	
Parameter	**Value**
Log Source Type	MVSCount
Protocol Configuration	Syslog
Log Source Identifier	ibm.managevirtualserver

Related tasks

"Adding a log source" on page 5

IBM Manage Virtual Server sample event message

Use the following sample event messages to verify a successful integration with IBM QRadar.

Sample event message 1

In the following sample event message, the event indicates the IBM Manage Virtual Server with source IP.

```
May 2 03:15:26 ibm.managevirtualserver LEEF:2.0|IBMQRadarMvs|IBM Manage Virtual Server|1.0|
Asset|src=10.0.0.1  devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX
devTime=2024-05-02T03:15:26.250-03  cat=MVS Asset Creation
```

Table 590. Highlighted values in the IBM Manage Virtual Server: sample event message 1	
QRadar field name	**Highlighted payload field name**
Event ID	**Asset**
Source IP	**src**
Device Time	**devTime**

Sample event message 2

In the following sample event message, the event indicates the IBM Manage Virtual Server with source IP and Source MAC.

```
May 2 03:15:26 ibm.managevirtualserver LEEF:2.0|IBMQRadarMvs|IBM Manage Virtual Server|1.0|
Asset|src=10.0.0.1  srcMAC=macadr    devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX
devTime=2024-05-02T03:15:26.299-03  cat=MVS Asset Creation
```

Table 591. Highlighted values in the IBM Manage Virtual Server: sample event message 2	
QRadar field name	**Highlighted payload field name**
Event ID	**Asset**
Source IP	**src**
Device Time	**devTime**
Source MAC	**srcMac**

Sample event message 3

In the following sample event message, the event indicates the IBM Manage Virtual Server with source IP, Source MAC, and User name.

```
May 2 03:15:26 ibm.managevirtualserver LEEF:2.0|IBMQRadarMvs|
IBM Manage Virtual Server|1.0|Asset|src=10.0.0.1 usrName=admin2  srcMAC= macadr
```

```
devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX    devTime=2024-05-02T03:15:26.300-03  cat=MVS Asset
Creation
```

Table 592. Highlighted values in the IBM Manage Virtual Server: sample event message 3	
QRadar field name	**Highlighted payload field name**
Event ID	**Asset**
Source IP	**src**
Device Time	**devTime**
Source MAC	**srcMac**
User Name	**usrName**

Sample event message 4

In the following sample event message, the event indicates the IBM Manage Virtual Server with source IP, Source MAC, Host name and User name.

```
May 2 03:15:26 ibm.managevirtualserver LEEF:2.0|IBMQRadarMvs|
IBM Manage Virtual Server|1.0|Asset|src=10.0.0.1    usrName=admin3  hostName=hoastname3 srcMAC=
macadr
devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX    devTime=2024-05-02T03:15:26.301-03  cat=MVS Asset
Creation
```

Table 593. Highlighted values in the IBM Manage Virtual Server: sample event message 4	
QRadar field name	**Highlighted payload field name**
Event ID	**Asset**
Source IP	**src**
Device Time	**devTime**
Source MAC	**srcMac**
User Name	**usrName**
Host Name	**hostName**

IBM Privileged Session Recorder

The IBM QRadar DSM for IBM Privileged Session Recorder can collect event logs from your IBM Privileged Session Recorder device.

The following table lists the specifications for the IBM Privileged Session Recorder DSM.

Table 594. IBM Privileged Session Recorder specifications	
Specification	**Value**
Manufacturer	IBM
DSM name	Privileged Session Recorder
RPM filename	DSM-IBMPrivilegedSessionRecorder
Protocol	JDBC
QRadar recorded event types	Command Execution Audit Events
Automatically discovered?	No
Includes identity?	No

Table 594. IBM Privileged Session Recorder specifications (continued)	
Specification	**Value**
More information	IBM website (http://www.ibm.com/)

To collect IBM Privileged Session Recorder events, use the following procedures:

1. If automatic updates are not enabled, download and install the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol-JDBC RPM
   - IBM Privileged Session Recorder DSM RPM
2. On the IBM Security Privileged Identity Manager dashboard, obtain the database information for the Privileged Session Recorder data store and configure your IBM Privileged Session Recorder DB2 database to allow incoming TCP connections.
3. For each instance of IBM Privileged Session Recorder, create an IBM Privileged Session Recorder log source on the QRadar Console. Use the following table to define the Imperva SecureSphere parameters:

Table 595. IBM Privileged Session Recorder log source parameters	
Parameter	**Description**
Log Source Type	IBM Privileged Session Recorder
Protocol Configuration	JDBC
Log Source Identifier	*DATABASE@HOSTNAME*
Database Type	DB2
Database Name	The Session Recorder data store name that you configured on the IBM Privileged Identity Manager dashboard.
IP or Hostname	The Session Recorder database server address.
Port	The port that is specified on IBM Privileged Identity Manager dashboard.
Username	The DB2 database user name
Password	The DB2 database password
Predefined Query	IBM Privileged Session Recorder
Use Prepared Statements	This option must be selected.
Start Date and Time	The initial date and time for the JDBC retrieval.

Related tasks

Adding a DSM

Configuring IBM Privileged Session Recorder to communicate with QRadar

Configuring IBM Privileged Session Recorder to communicate with QRadar

Before you can configure a log source in IBM Privileged Session Recorder for IBM QRadar, obtain the database information for the Privileged Session Recorder data store. You must also configure your IBM Privileged Session Recorder DB2 database to allow incoming TCP connections from QRadar.

IBM Privileged Session Recorder is a component of IBM Security Privileged Identity Manager.

Procedure

1. Log in to the IBM Security Privileged Identity Manager web user interface.
2. Select the **Configure Privileged Identity Manager** tab.
3. Select **Database Server Configuration** in the **Manage External Entities** section.
4. In the table, double-click the **Session Recording data store** row in the **Database Server Configuration** column.
5. 5. Record the following parameters to use when you configure a log source in QRadar:

IBM Privileged Session Recorder Field	QRadar Log Source Field
Hostname	IP or Hostname
Port	Port
Database name	Database Name
Database administrator ID	Username

JDBC log source parameters for IBM Privileged Session Recorder

If QRadar does not automatically detect the log source, add an IBM Privileged Session Recorder log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from IBM Privileged Session Recorder:

Table 596. JDBC log source parameters for the IBM Privileged Session Recorder DSM

Parameter	Value
Log Source type	IBM Privileged Session Recorder
Protocol Configuration	JDBC

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

"Adding a log source" on page 5

IBM Proventia

IBM QRadar supports IBM Proventia Management SiteProtector and IBM ISS Proventia DSMs.

IBM Proventia Management SiteProtector

The IBM Proventia® Management SiteProtector DSM for IBM QRadar accepts SiteProtector events by polling the SiteProtector database.

The DSM allows QRadar to record Intrusion Prevention System (IPS) events and audit events directly from the IBM SiteProtector database.

Note: The IBM Proventia Management SiteProtector DSM requires the latest JDBC Protocol to collect audit events.

The IBM Proventia Management SiteProtector DSM for IBM QRadar can accept detailed SiteProtector events by reading information from the primary SensorData1 table. The SensorData1 table is generated with information from several other tables in the IBM SiteProtector database. SensorData1 remains the primary table for collecting events.

IDP events include information from SensorData1, along with information from the following tables:

- SensorDataAVP1
- SensorDataReponse1

Audit events include information from the following tables:

- AuditInfo
- AuditTrail

Audit events are not collected by default and make a separate query to the AuditInfo and AuditTrail tables when you select the **Include Audit Events** check box. For more information about your SiteProtector database tables, see your vendor documentation.

Before you configure QRadar to integrate with SiteProtector, we suggest that you create a database user account and password in SiteProtector for QRadar.

Your QRadar user must have read permissions for the SensorData1 table, which stores SiteProtector events. The JDBC - SiteProtector protocol allows QRadar to log in and poll for events from the database. Creating a QRadar account is not required, but it is recommended for tracking and securing your event data.

Note: Ensure that no firewall rules are blocking the communication between the SiteProtector console and QRadar.

JDBC log source parameters for IBM Proventia Management SiteProtector

If QRadar does not automatically detect the log source, add an IBM Proventia Management SiteProtector log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from IBM Proventia Management SiteProtector:

Table 597. JDBC log source parameters for the IBM Proventia Management SiteProtector DSM

Parameter	Value
Log Source type	IBM Proventia Management SiteProtector
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.

For a complete list of JDBC protocol parameters and their values, see JDBC protocol configuration options.

Related tasks

"Adding a log source" on page 5

IBM ISS Proventia

The IBM Integrated Systems Solutions®® (ISS) Proventia DSM for IBM QRadar records all relevant IBM Proventia® events by using SNMP.

Procedure

1. In the **Proventia Manager** user interface navigation pane, expand the **System node**.
2. Select **System**.
3. Select **Services**.

   The **Service Configuration** page is displayed.
4. Click the **SNMP** tab.
5. Select **SNMP Traps Enabled**.
6. In the **Trap Receiver** field, type the IP address of your QRadar you want to monitor incoming SNMP traps.
7. In the **Trap Community** field, type the appropriate community name.
8. From the **Trap Version** list, select the trap version.
9. Click **Save Changes**.

   You are now ready to configure QRadar to receive SNMP traps.
10. To configure QRadar to receive events from an ISS Proventia device. From the **Log Source Type** list, select IBM **Proventia Network Intrusion Prevention System (IPS)**.

    For more information about your ISS Proventia device, see your vendor documentation.

Related concepts

"SNMPv2 protocol configuration options" on page 216
You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events.

"SNMPv3 protocol configuration options" on page 217
You can configure a log source to use the SNMPv3 protocol to receive SNMPv3 events.

IBM QRadar Packet Capture

The IBM QRadar DSM for IBM QRadar Packet Capture collects events from an IBM Security Packet Capture device.

The following table describes the specifications for the IBM QRadar Packet Capture DSM:

Table 598. IBM QRadar Packet Capture DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBM QRadar Packet Capture
RPM file name	`DSM-IBMQRadarPacketCapture-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	IBM QRadar Packet Capture V7.2.3 to V7.2.7 IBM QRadar Network Packet Capture V7.3.0
Protocol	Syslog
Event format	LEEF
Recorded event types	All events
Automatically discovered?	Yes

Table 598. IBM QRadar Packet Capture DSM specifications (continued)	
Specification	**Value**
Includes identity?	No
Includes custom properties?	No
More information	IBM Docs (https://www.ibm.com/support/knowledgecenter/SS42VS_latest/com.ibm.qradar.doc/c_pcap_introduction.html)

To integrate IBM QRadar Packet Capture with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - IBM QRadar Packet Capture DSM RPM
2. Configure your IBM QRadar Packet Capture device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an IBM QRadar Packet Capture log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from IBM QRadar Packet Capture:

Table 599. IBM QRadar Packet Capture log source parameters	
Parameter	**Value**
Log Source type	IBM QRadar Packet Capture
Protocol Configuration	Syslog

4. To verify that QRadar is configured correctly, review the following tables to see examples of parsed event messages.

   Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

   The following table shows a sample event message from IBM QRadar Packet Capture:

Table 600. IBM QRadar Packet Capture sample message		
Event name	**Low level category**	**Sample log message**
User Added	User Account Added	May 10 00:01:04 <Server> LEEF: 2.0|IBM|QRadar Packet Capture|7.2.7.255-1G |UserAdded|cat=Admin msg=User <Username> has been added May 10 00:01:04 <Server>LEEF: 2.0|IBM|QRadar PacketCapture| 7.2.7.255-1G|UserAdded|cat=Admin msg=User<Username> has been added

   The following table shows a sample event message from IBM QRadar Network Packet Capture:

Table 601. IBM QRadar Network Packet Capture sample message

Event name	Low level category	Sample log message
Packet Capture Statistics	Information	<14>Mar 1 20:39:41 <Server> LEEF: 2.0|IBM|Packet Capture|7.3.0|1|^| captured_packets=8844869^captured _packets_udp=4077106^captured_ bytes_udp=379169082^total_packets =9090561^captured_bytes=27938019 18^captured_bytes_tcp=2379568101 ^compression_ratio=27.4^captured _packets_tcp=4356387^oldest_packet =2017-03-01T20:39:41.915555490Z^ total_bytes=2853950159 <14>Mar 1 20:39:41 <Server> LEEF:2.0| IBM|Packet Capture|7.3.0|1|^| captured_packets=8844869^captured_pack ets_udp=4077106^captured_bytes_udp=379 169082^total_packets=9090561^captured_ bytes=2793801918^captured_bytes_tcp=23 79568101^compression_ratio=27.4^captur ed_packets_tcp=4356387^oldest_packet=2 017-03-01T20:39:41.915555490Z^total_by tes=2853950159

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring IBM QRadar Packet Capture to communicate with QRadar

To collect IBM QRadar Packet Capture events, you must configure event forwarding to a remote syslog server.

Procedure

1. Using SSH, log in to your IBM QRadar Packet Capture device as the root user.
2. Choose one of the following options to enable syslog.
   a) `Option 1:` Open the `/etc/rsyslog.conf` file in a text editor such as vi:

   ```
   vi /etc/rsyslog.conf
   ```

   Then add the following line at the end of the file:

   ```
   *.* @@<QRadar Event collector IP>:514
   ```

   b) `Option 2:` Create the `<filename>.conf` file in the `/etc/rsyslog.d/` directory, and then add the following line to the file that you created:

   ```
   *.* @@<QRadar Event collector IP>:514
   ```

3. Restart the Syslog service by typing the following command:

   ```
   service rsyslog restart
   ```

   The message logs are sent to the QRadar Event Collector and local copies are saved.

   Note: QRadar parses only LEEF events for IBM QRadar Packet Capture. On the **Log Activity** tab in QRadar, the **Event Name** displays as **IBM QRadar Packet Capture Message** and the **Low Level Category** displays as **Stored** for all other events.

What to do next

To verify that LEEF events are being logged on your IBM QRadar Packet Capture device, inspect `/var/log/messages`.

```
tail /var/log/messages
```

Configuring IBM QRadar Network Packet Capture to communicate with QRadar

To collect IBM QRadar Network Packet Capture events, you must configure a remote Syslog server for your IBM QRadar Network Packet Capture appliance.

Procedure

1. Log in to your IBM QRadar Network Packet Capture appliance as administrator.
2. Click **Admin**.
3. In the **REMOTE SYSLOG SETUP** pane, enable **system logging**.
4. Enable the **UPD** or **TCP** protocol, depending on your transfer settings.
5. In the **Remote Syslog Server Port** field, type the port number that you want to use to send remote syslog events. The default port number for remote syslog is 514.
6. In the **Remote Syslog Server** field, type the IP address for your QRadar Event Collector to which you want to send events.
7. Click **Apply**.

   Note: QRadar parses only LEEF events for IBM QRadar Network Packet Capture. On the **Log Activity** tab in QRadar, the **Event Name** displays as **IBM QRadar Packet Capture Message** and the **Low Level Category** displays as **Stored** for all other events.

IBM QRadar Network Security XGS

The IBM QRadar Network Security XGS DSM accepts events by using the Log Event Extended Format (LEEF), which enables IBM QRadar to record all relevant events.

The following table identifies the specifications for the IBM QRadar Network Security XGS DSM:

Table 602. IBM QRadar Network Security XGS specifications

Specification	Value
Manufacturer	IBM
DSM	QRadar Network Security XGS
RPM file name	DSM-IBMQRadarNetworkSecurityXGS-QRadar_version-build_number.noarch,rpm
Supported versions	v5.0 with fixpack 7 to v5.4
Protocol	Syslog
Event format	LEEF
QRadar recorded events	All relevant system, access, and security events
Automatically discovered	Yes
Includes identity	No

Table 602. IBM QRadar Network Security XGS specifications (continued)	
Specification	**Value**
More information	IBM QRadar Network Security (XGS) Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSHLHV_5.4.0/com.ibm.alps.doc/alps_collateral/alps_dochome_stg.htm)

Before you configure a Network Security XGS appliance in QRadar, you must configure remote syslog alerts for your IBM QRadar Network Security XGS rules or policies to forward events to QRadar.

Configuring IBM QRadar Network Security XGS Alerts

All event types are sent to IBM QRadar by using a remote syslog alert object that is LEEF enabled.

About this task

Remote syslog alert objects can be created, edited, and deleted from each context in which an event is generated. Log in to the IBM QRadar Network Security XGS local management interface as admin to configure a remote syslog alert object, and go to one of the following menus:

- **Manage** > **System Settings** > **System Alerts** (System events)
- **Secure** > **Network Access Policy** (Access events)
- **Secure** > **IPS Event Filter Policy** (Security events)
- **Secure** > **Intrusion Prevention Policy** (Security events)
- **Secure** > **Network Access Policy** > **Inspection** > **Intrusion Prevention Policy**

In the **IPS Objects**, the **Network Objects** pane, or the **System Alerts** page, complete the following steps.

Procedure

1. Click **New** > **Alert** > **Remote Syslog**.
2. Select an existing remote syslog alert object, and then click **Edit**.
3. Configure the following options:

Table 603. Syslog configuration parameters	
Option	**Description**
Name	Type a name for the syslog alert configuration.
Remote Syslog Collector	Type the IP address of your QRadar Console or Event Collector.
Remote Syslog Collector Port	Type 514 for the **Remote Syslog Collector Port**.
Remote LEEF Enabled	Select this check box to enable LEEF formatted events. This is a required field. If you do not see this option, verify that you have software version 5.0 with fixpack 7 to v5.4 installed on your IBM QRadar Security Network appliance.
Comment	Typing a comment for the syslog configuration is optional.

4. Click **Save Configuration**.

   The alert is added to the **Available Objects** list.

5. To update your IBM QRadar Network Security XGS appliance, click **Deploy**.
6. Add the LEEF alert object for QRadar to the following locations:
   - One or more rules in a policy
   - **Added Objects** pane on the **System Alerts** page
7. Click **Deploy**

   For more information about the Network Security XGS device, click **Help** in the QRadar Network Security XGS local management interface browser client window or access the online *IBM QRadar Network Security XGS documentation*.

Syslog log source parameters for IBM QRadar Network Security XGS

If QRadar does not automatically detect the log source, add a IBM QRadar Network Security XGS log source on the QRadar Console by using the Syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from IBM QRadar Network Security XGS:

Table 604. Syslog log source parameters for the IBM QRadar Network Security XGS DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Type	IBM QRadar **Network Security XGS**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM QRadar Network Security XGS.

Related tasks

"Adding a log source" on page 5

IBM RACF

The IBM RACF DSM collects events from an IBM z/OS mainframe by using IBM Security zSecure.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can retrieve the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to retrieve events on a polling interval, which enables QRadar to retrieve the events on the schedule that you define.

To collect IBM RACF events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements.
   For more information about prerequisite requirements, see the IBM Security zSecure Suite 2.2.1 Prerequisites (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/prereqs_qradar.html) .
2. Configure your IBM z/OS image to write events in LEEF format. For more information, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/setup_data_prep_qradar.html).
3. Create a log source in QRadar for IBM RACF.

4. If you want to create a custom event property for IBM RACF in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note (http://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/TechNotes/IBM_zOS_CustomEventProperties.pdf).

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the IBM Security zSecure Suite 2.2.1: Procedure for near real-time (http://www.ibm.com/support/knowledgecenter/en/SS2RWS_2.2.1/com.ibm.zsecure.doc_2.2.0/installation/smf_proc_real_time_qradar.html)
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

For instructions on installing and configuring zSecure, see the IBM Security zSecure Suite: CARLa-Driven Components Installation and Deployment Guide (https://www.ibm.com/docs/en/SS2RWS_2.4.0/com.ibm.zsecure.doc_2.4.0/zsec_install.pdf).

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Log File log source parameter

If QRadar does not automatically detect the log source, add a IBM z/OS, IBM CICS, IBM RACF, IBM DB2, Broadcom CA Top Secret, or Broadcom CA ACF2 log source on the QRadar Console by using the Log File Protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, or CA ACF2:

Table 605. Log File log source parameters

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	Select your DSM name.
Protocol Configuration	**Log File**

Table 605. Log File log source parameters (continued)

Parameter	Value
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.
Service Type	From the **Service Type** list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535. The options include ports: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.

Table 605. Log File log source parameters (continued)	
Parameter	**Value**
Remote User	Type the user name or user ID necessary to log in to the system that contains your event files. • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length. • If your log files are on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <*product_name*>.<*timestamp*>.gz The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with z0S and end with .gz, type the following code: z0S.*\.gz Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions (https://docs.oracle.com/javase/tutorial/essential/regex/).

Table 605. Log File log source parameters (continued)	
Parameter	**Value**
FTP Transfer Mode	This option displays only if you select **FTP** as the **Service Type**. From the list, select **Binary**. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as `zip`, `gzip`, `tar`, or `tar+gzip` archive files.
SCP Remote File	If you select **SCP** as the **Service Type** you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type `00:00` to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.
Run On Save	If you want the Log File protocol to run immediately after you click **Save**, select this check box. After the **Run On Save** completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.

Table 605. Log File log source parameters (continued)	
Parameter	**Value**
Processor	From the list, select **gzip**. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is previously processed by the Log File protocol. If a previously processed file is detected, the Log File protocol does not download the file for processing. All files that are not previously processed are downloaded. This option applies only to FTP and SFTP service types.
Change Local Directory?	Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the **Local Directory** field is displayed, which gives you the option to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select **LineByLine**. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

"Adding a log source" on page 5

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

Table 606. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Integrate IBM RACF with IBM QRadar by using audit scripts

The IBM RACF DSM collects events and audit transactions on the IBM mainframe with the Log File protocol.

QRadar records all relevant and available information from the event.

Note: zSecure integration is the only integration that provides custom events to the log source. Custom events can be displayed even when you collect events by using the Native QEXRACF integration.

Use the following procedure to integrate the IBM RACF events into QRadar:

1. The IBM mainframe system records all security events as Service Management Framework (SMF) records in a live repository.
2. At midnight, the IBM RACF data is extracted from the live repository by using the SMF dump utility. The RACFICE utility IRRADU00 (an IBM utility) creates a log file that contains all of the events and fields from the previous day in an SMF record format.
3. The QEXRACF program pulls data from the SMF formatted file. The program pulls only the relevant events and fields for QRadar and writes that information in a condensed format for compatibility. The information is also saved in a location accessible by QRadar.
4. QRadar uses the Log File protocol source to pull the QEXRACF output file and retrieves the information on a scheduled basis. QRadar then imports and process this file.

Configuring IBM RACF that uses audit scripts to integrate with IBM QRadar

IBM QRadar uses scripts to audit events from IBM RACF installations, which are collected by using the Log File protocol.

Procedure

1. Download the `qexracf_bundled.tar.gz` from the IBM support website.
2. On a Linux-based operating system, use the following command to extract the file:

   ```
   tar -zxvf qexracf_bundled.tar.gz
   ```

   The following files are contained in the archive:

   - `qexracf_jcl.txt`
   - `qexracfloadlib.trs`
   - `qexracf_trsmain_JCL.txt`
3. Load the files onto the IBM mainframe by using any terminal emulator file transfer method.

   Upload the `qexracf_trsmain_JCL.txt` and `qexracf_jcl.txt` files by using the TEXT protocol.

Upload the QexRACF `loadlib.trs` file by using binary mode and append to a preallocated data set. The QexRACF `loadlib.trs` file is a tersed file that contains the executable (the mainframe program QEXRACF).

When you upload the `.trs` file from a workstation, preallocate a file on the mainframe with the following DCB attributes: DSORG=PS, RECFM=FB, LRECL=1024, BLKSIZE=6144. The file transfer type must be binary mode and not text.

4. Customize the `qexracf_trsmain_JCL.txt` file according to your installation-specific requirements.

   The `qexracf_trsmain_JCL.txt` file uses the IBM utility Trsmain to decompress the program that is stored in the QexRACF `loadlib.trs` file.

   The following is an example of the `qexracf_trsmain_JCL.txt` file includes the following code:

```
//TRSMAIN JOB (yourvalidjobcard),Q1labs,
// MSGCLASS=V //DEL EXEC PGM=IEFBR14
//D1 DD DISP=(MOD,DELETE),DSN=<yourhlq>.QEXRACF.TRS // UNIT=SYSDA,
// SPACE=(CYL,(10,10))
//TRSMAIN EXEC PGM=TRSMAIN,PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE DD DISP=SHR,DSN=<yourhlq>.QEXRACF.TRS
//OUTFILE DD DISP=(NEW,CATLG,DELETE),
// DSN=<yourhlq>.LOAD,
// SPACE=(CYL,(10,10,5),RLSE),UNIT=SYSDA //
```

   You must update the file with your installation specific information for parameters, such as, jobcard, data set naming conventions, output destinations, retention periods, and space needs.

   The `.trs` input file is an IBM TERSE formatted library and is extracted by running the JCL, which calls the TRSMAIN. This tersed file, when extracted, creates a PDS linklib with the QEXRACF program as a member.

5. You can STEPLIB to this library or choose to move the program to one of the LINKLIBs that are in the LINKLST. The program does not require authorization.
6. When the upload is complete, copy the program to an existing link listed library or add a STEPLIB DD statement that has the correct dataset name of the library that will contain the program.
7. The `qexracf_jcl.txt` file is a text file that contains a sample JCL deck to provide you with the necessary JCL to run the IBM IRRADU00 utility. This allows QRadar to obtain the necessary IBM RACF events. Configure the job card to meet your local standards.

   An example of the `qexracf_jcl.txt` file has the following code.

```
//QEXRACF JOB (<your valid jobcard>),Q1LABS,
// MSGCLASS=P, // REGION=0M //*
//*QEXRACF JCL version 1.0 April 2009 //*
//*************************************************************
//* Change below dataset names to sites specific datasets names *
//*************************************************************
//SET1 SET SMFOUT='<your hlq>.CUSTNAME.IRRADU00.OUTPUT',
// SMFIN='<your SMF dump ouput dataset>',
// QRACFOUT='<your hlq>.QEXRACF.OUTPUT'
//*************************************************************
//* Delete old datasets *
//*************************************************************
//DEL EXEC PGM=IEFBR14 //DD2 DD DISP=(MOD,DELETE),DSN=&QRACFOUT,
// UNIT=SYSDA, // SPACE=(TRK,(1,1)), // DCB=(RECFM=FB,LRECL=80)
//*************************************************************
//* Allocate new dataset *
```

```
//*************************************************************
//ALLOC EXEC PGM=IEFBR14
//DD1 DD DISP=(NEW,CATLG),DSN=&QRACFOUT,
// SPACE=(CYL,(1,10)),UNIT=SYSDA,
// DCB=(RECFM=VB,LRECL=1028,BLKSIZE=6144)
//*************************************************************
//* Execute IBM IRRADU00 utility to extract RACF smf records *
//*************************************************************
//IRRADU00 EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//ADUPRINT DD SYSOUT=*
//OUTDD DD DSN=&SMFOUT,SPACE=(CYL,(100,100)),DISP=(,CATLG),
```

```
// DCB=(RECFM=FB,LRECL=8192,BLKSIZE=40960),
// UNIT=SYSALLDA
//SMFDATA DD DISP=SHR,DSN=&SMFIN
//SMFOUT DD DUMMY
//SYSIN DD *INDD(SMFDATA,OPTIONS(DUMP))
OUTDD(SMFOUT,TYPE(30:83)) ABEND(NORETRY)
USER2(IRRADU00) USER3(IRRADU86) /*
//EXTRACT EXEC PGM=QEXRACF,DYNAMNBR=10,
// TIME=1440
//*STEPLIB DD DISP=SHR,DSN=
<the loadlib containing the QEXRACF program if not in LINKLST>
//SYSTSIN DD DUMMY //SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//RACIN DD DISP=SHR,DSN=&SMFOUT
//RACOUT DD DISP=SHR,DSN=&QRACFOUT //
//*************************************************************
//* FTP Output file from C program (Qexracf) to an FTP server *
//* QRadar will go to that FTP Server to get file *
//* Note you need to replace <user>, <password>,<serveripaddr>*
//* <THEIPOFTHEMAINFRAMEDEVICE> and <QEXRACFOUTDSN> *
//*************************************************************
//*FTP EXEC PGM=FTP,REGION=3800K //*INPUT DD *
//*<FTPSERVERIPADDR>
//*<USER>
//*<PASSWORD>
//*ASCII //*PUT '<QEXRACFOUTDSN>'
/<THEIPOFTHEMAINFRAMEDEVICE>/<QEXRACFOUTDSN>
//*QUIT //*OUTPUT DD SYSOUT=*
//*SYSPRINT DD SYSOUT=* //* //*
```

8. After the output file is created, you must send this file to an FTP server.
   This action ensures that every time you run the utility, the output file is sent to a specific FTP server for processing at the end of the script. If the z/OS platform is configured to serve files through FTP or SFTP, or allow SCP, then no interim server is needed and QRadar can pull those files directly from the mainframe. If an interim FTP server is needed, QRadar requires a unique IP address for each IBM RACF log source or they are joined as one system.

IBM Red Hat OpenShift

The IBM QRadar DSM for Red Hat® OpenShift® collects auditing and infrastructure events from a Red Hat OpenShift cluster.

To integrate Red Hat OpenShift with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - DSM Common RPM
   - Kubernetes Auditing DSM RPM
   - IBM Red Hat OpenShift DSM RPM
2. Configure Red Hat OpenShift to forward events to QRadar. See “Configuring Red Hat OpenShift to communicate with QRadar” on page 974.
3. If QRadar does not automatically detect the log source, add a log source on the QRadar Console. See “IBM Red Hat OpenShift Syslog log source parameters” on page 974.

   For more information about adding a log source, see Adding a log source.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

IBM Red Hat OpenShift DSM specifications

When you configure Red Hat OpenShift, understanding the specifications for the IBM Red Hat OpenShift DSM can help ensure a successful integration. For example, knowing what the supported version of Red Hat OpenShift is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the IBM Red Hat OpenShift DSM.

Table 607. IBM Red Hat OpenShift DSM specifications

Specification	**Value**
Manufacturer	Red Hat
DSM name	IBM Red Hat OpenShift
RPM file name	DSM-*IBMRedHatOpenShift-QRadar_version-build_number*.noarch.rpm
Supported version	Red Hat OpenShift 5.2.4
Protocol	Syslog
Event format	JSON
Recorded event types	Audit and Infrastructure
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	Yes
More information	Understanding the logging subsystem for Red Hat OpenShift (https://docs.openshift.com/container-platform/4.10/logging/cluster-logging.html)

Configuring Red Hat OpenShift to communicate with QRadar

To send events from Red Hat OpenShift to QRadar, you must specify QRadar as the syslog server.

Procedure

1. A Red Hat OpenShift cluster must be running on your system. For more information about creating a logging instance cluster, see the Red Hat OpenShift documentation about Understanding the logging subsystem for Red Hat OpenShift (https://docs.openshift.com/container-platform/4.10/logging/cluster-logging.html).
2. To forward logs to QRadar, see the Red Hat OpenShift documentation about Forwarding logs to external third-party logging systems (https://docs.openshift.com/container-platform/4.10/logging/cluster-logging-external.html).

What to do next

"IBM Red Hat OpenShift Syslog log source parameters" on page 974

Related tasks

"Adding a log source" on page 5

IBM Red Hat OpenShift Syslog log source parameters

Add an IBM Red Hat OpenShift log source that uses the Syslog protocol in IBM QRadar.

When you use the Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Syslog events from Red Hat OpenShift:

Table 608. Syslog protocol parameters for the IBM Red Hat OpenShift DSM	
Parameter	**Value**
Log source type	IBM Red Hat OpenShift
Protocol Configuration	Syslog
Log source identifier	The IP address or hostname of the Red Hat OpenShift server.

Related tasks

"Adding a log source" on page 5

IBM Red Hat OpenShift sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Red Hat OpenShift sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that audit type events are received from the cluster.

```
<15>1 2023-02-06T09:52:42.243795+00:00 ibm.redhatopenshift.test myapp myproc mymsg -
{"kind":"Event","apiVersion":"audit.k8s.io/
v1","level":"Metadata","auditID":"45459782-7777-4444-9e49-
ccdc07a66cbd","stage":"ResponseComplete","requestURI":"/api/v1/namespaces/ kube-node-
lease","verb":"get","user":{"username":"testuser","uid":"420c62cd2  IBM Red Hat OpenShift DRAFT -
NOT FOR PUBLICATION bbbb-4444-92f0-f52bfd543e98","groups":["system:masters"]},"sourceIPs":
["::1"],"userAgent":"kube-apiserver/v1.23.5+8471591 (linux/amd64) kubernetes/3c28e7a","objectRef":
{"resource":"namespaces","namespace":"kube-nodelease","name":"kube-node-
lease","apiVersion":"v1"},"responseStatus":{"metadata":
{},"code":200},"requestReceivedTimestamp":"2023-02-06T07:00:02.814290Z","stageTimestamp":"2023-02-
06T07:00:02.{"authorization.k8s.io/decision":"allow","authorization.k8s.io/
reason":""},"@timestamp":"2023-02-06T07:00:02.814290Z","k8s_audit_level":"Metadata","message":null
,"hostname":{"collector":{"ipaddr4":"10.22.40.128","inputname":"fluent-
pluginsystemd","name":"fluentd","received_at":"2023-02-06T07:00:02.838164+00:00","version":"1.14.6
 1.6.0"}},"openshift":{"labels":
{"syslog":"qradartcp"}},"viaq_msg_id":"YYYYYY111111aaaaaa","log_type":"audit"}
```

Table 609. Highlighted fields in the IBM Red Hat OpenShift event	
QRadar field name	**Highlighted payload field name**
Event ID	**get**
Event Category	**namespaces**
Source IP	**SourceIPs**
Username	**username**
Device Time	**stageTimestamp**

Sample 2: The following sample event message shows that infrastructure event types are received from the cluster.

```
<15>1 2023-02-15T17:07:09.514393+00:00 ibm.redhatopenshift.test myapp myproc mymsg -
{"_SOURCE_MONOTONIC_TIMESTAMP":"2311043623145","systemd":{"t":
{"BOOT_ID":"444444aaaaaa","MACHINE_ID":"333333aaaaaa","TRANSPORT":"kernel"},"u":
{"SYSLOG_FACILITY":"0","SYSLOG_IDENTIFIER":"kernel"}},"level":"info","message":"device
veth5db1717a entered promiscuous mode","hostname":"test.host.com","pipeline_metadata":
{"collector":{"ipaddr4":"10.22.44.158","inputname":"fluent-
pluginsystemd","name":"fluentd","received_at":"2023-02-15T15:36:25.306285+00:00","version":"1.14.6
 1.6.0"}},"openshift":{"labels":
```

{"syslog":"qradartcp"}},"**@timestamp**":"2023-02-15T15:36:25.212659+00:00","viaq_msg_id":"YYYYYY11111
1aaaaaa","log_type":"infrastructure"}

Table 610. Highlighted fields in the IBM Red Hat OpenShift event	
QRadar field name	**Highlighted payload field name**
Event ID	**`infrastructure`** + **`info`**
Event Category	The **Event Category** value is always **IBMRedHatOpenShift** in QRadar.
Source IP	**`ipaddr4`**
Device Time	**`@timestamp`**

IBM SAN Volume Controller

The IBM QRadar DSM for IBM SAN Volume Controller collects events from IBM SAN Volume Controller.

Important: This DSM supports only the Cloud Auditing Data Federation (CADF) event format that includes monitoring and protection related to cloud account's create, update, removal and cloud backup activity events from IBM SAN Volume Controller.

The following table describes the specifications for the IBM SAN Volume Controller DSM:

Table 611. IBM SAN Volume Controller DSM specifications	
Specification	**Value**
Manufacturer	IBM
DSM name	IBM SAN Volume Controller
RPM file name	`DSM-IBMSANVolumeController-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Syslog
Event format	CADF
Recorded event types	activity, control, and monitor audit events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	IBM SAN Volume Controller website (http://www-03.ibm.com/systems/storage/software/virtualization/svc/)

To integrate IBM SAN Volume Controller with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website, in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - IBM SAN Volume Controller DSM RPM
2. Configure your IBM SAN Volume Controller server to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an IBM SAN Volume Controller log source on the QRadar Console. The following table describes the parameters that require specific values for IBM SAN Volume Controller event collection:

Table 612. IBM SAN Volume Controller log source parameters	
Parameter	**Value**
Log Source type	IBM SAN Volume Controller
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the IBM SAN Volume Controller server.

4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

   The following table shows a sample event message for IBM SAN Volume Controller:

Table 613. IBM SAN Volume Controller sample message		
Event name	**Low level category**	**Sample log message**
Backup Successful	Backup Activity Succeeded	`Oct 12 20:02:33 Cluster_<IP_address> IBM2145: {"typeURI": "http://example.com/cloud/audit/1.0/event","eventTime": "2016-10-12T20:02:30.000000+0000","target": {"typeURI": "service/storage/object","id": "0","name": "username"},"observer": {"typeURI": "service/network/cluster/logger","id": "10032004394","name": "username"},"tags": ["Backup"],"eventType": "activity","measurements": [{"metric": {"metricId": "www.example.com/svc/Cloud/Backup_Time/0000000000/000/0","name": "Time of backup being copied or restored","unit": "YYMMDDHHMMSS"},"result": "2016/10/12/20/02/30"},{"metric": {"metricId": "www.example.com/svc/Cloud/Backup_Generation_Number/0000000000/000/0","name": "Volume backup generation number","unit": "Natural Number"},"result": "1"}],"initiator": {"typeURI": "service/network/node","host": {"address": "<IP_address>"},"attachments": [{"content":"60050764008010E5000000000000000","typeURI": "text/plain","name": "volume_uuid"}],"name": "username","id": "1"},"reason": {"reasonCode": "200","reasonType": "http://www.example.com/assignments/http-status-codes/http-status-codes.xml"},"action": "backup","outcome": "success","id": "xxxxxxxxxxx-xxxxxxxxxx-xxx"}`

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring IBM SAN Volume Controller to communicate with QRadar

To collect events from IBM SAN Volume Controller, you must configure IBM SAN Volume Controller (SVC) cluster to send events to QRadar from a syslog server.

Procedure

1. Use SSH to log in to the SVC cluster command-line interface (CLI).
2. Type the following command to configure a remote syslog server to send CADF events to QRadar:

   ```
   svctask mksyslogserver -ip <QRadar_Event_Collector_IP_Address> error
   <on_or_off> -warning <on_or_off> -info <on_or_off> -cadf on
   ```

   The following example shows a command that is used to configure a remote syslog server to send CADF events:

   ```
   svctask mksyslogserver -ip 192.0.2.1 -error on -warning on -info on -cadf on
   ```

   Note: The error and warning flags are CADF event types that SVC sends to syslog servers.

IBM Security Access Manager for Enterprise Single Sign-On

You can use the IBM® Security Access Manager for Enterprise Single Sign-On DSM for IBM QRadar to receive events that are forwarded by using syslog.

QRadar can collect events from IBM Security Access Manager for Enterprise Single Sign-On version 8.1 or 8.2.

Events that are forwarded by the IBM Security Access Manager for Enterprise Single Sign-On include audit, system, and authentication events.

Events are read from the following database tables and forwarded by using syslog:

- IMSLOGUserService
- IMSLOGUserAdminActivity
- IMSLOGUserActivity

All events that are forwarded to QRadar from IBM Security Access Manager for Enterprise Single Sign-On use ### as a syslog field-separator. IBM Security Access Manager for Enterprise Single Sign-On forwards events to QRadar by using UDP on port 514.

Before you begin

To configure syslog forwarding for events, you must be an administrator or your user account must include credentials to access the IMS Configuration Utility.

Any firewalls that are configured between your IBM Security Access Manager for Enterprise Single Sign-On and QRadar are ideally configured to allow UDP communication on port 514. This configuration requires you to restart your IBM Security Access Manager for Enterprise Single Sign-On appliance.

Configuring a log server type

IBM Security Access Manager for Enterprise Single Sign-On appliance requires you to configure a log server type to forward syslog formatted events:

Procedure

1. Log in to the IMS Configuration Utility for IBM Security Access Manager for Enterprise Single Sign-On.

   For example, https://localhost:9043/webconf
2. From the navigation menu, select **Advanced Settings** > IMS **Server** > **Logging** > **Log Server Information**.
3. From the **Log server types** list, select **syslog**.
4. Click **Add**.
5. Click **Update** to save the configuration.

Configuring syslog forwarding

To forward events to QRadar, you must configure a syslog destination on your IBM Security Access Manager for Enterprise Single Sign-On appliance.

Procedure

1. Log in to the IMS Configuration Utility for IBM Security Access Manager for Enterprise Single Sign-On. For example, `https://localhost:9043/webconf`.
2. From the navigation menu, select **Advanced Settings** > **IMS Server** > **Logging** > **Syslog**.
3. Configure the following syslog parameter options:

Table 614. Syslog parameters

Field	Description
Enable syslog	From the **Available Tables** list, you must select the following tables, and click **Add**. • **logUserService** • **logUserActivity** • **logUserAdminActivity**
Syslog server port	Type 514 as the port number used for forwarding events to QRadar.
Syslog server hostname	Type the IP address or host name of your QRadar Console or Event Collector.
Syslog logging facility	Type an integer value to specify the facility of the events that are forwarded to QRadar. The default value is 20.
Syslog field-separator	Type *###* as the characters used to separate name-value pair entries in the syslog payload.

4. Click **Update** to save the configuration.
5. Restart your IBM Security Access Manager for Enterprise Single Sign-On appliance.

Results

The log source is added to QRadar as IBM Security Access Manager for Enterprise Single Sign-On syslog events are automatically discovered. Events that are forwarded to QRadar are displayed on the **Log Activity** tab.

Syslog log source parameters for IBM Security Access Manager for Enterprise Single Sign-On

If QRadar does not automatically detect the log source, add an IBM Security Access Manager for Enterprise Single Sign-On log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from IBM Security Access Manager for Enterprise Single Sign-On:

Table 615. Syslog log source parameters for the IBM Security Access Manager for Enterprise Single Sign-On DSM	
Parameter	**Value**
Log Source type	IBM Security Access Manager for Enterprise Single Sign-On
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM Security Access Manager for Enterprise Single Sign-On appliance.

Related tasks

"Adding a log source" on page 5

IBM Security Access Manager for Mobile

The IBM QRadar DSM for IBM Security Access Manager for Mobile collects logs from an IBM Security Access Manager for Mobile device, and an IBM Identity as a Service (IDaaS) device.

The following table identifies the specifications for the IBM Security Access Manager for Mobile DSM:

Table 616. IBM Security Access Manager for Mobile DSM specifications	
Specification	**Value**
Manufacturer	IBM
DSM name	IBM Security Access Manager for Mobile
RPM file name	DSM-IBMSecurityAccessManagerForMobile-7.x-*Qradar_version*-*Buildbuild_number*.noarch.rpm
Supported versions	IBM Security Access Manager for Mobile v8.0.0 IBM IDaaS v2.0
Event Format	Common Base Event Format Log Event Extended Format (LEEF)

Table 616. IBM Security Access Manager for Mobile DSM specifications (continued)	
Specification	**Value**
Recorded event types	IBM_SECURITY_AUTHN IBM_SECURITY_TRUST IBM_SECURITY_RUNTIME IBM_SECURITY_CBA_AUDIT_MGMT IBM_SECURITY_CBA_AUDIT_RTE IBM_SECURITY_RTSS_AUDIT_AUTHZ IBM_SECURITY_SIGNING CloudOE Operations Usage IDaas Appliance Audit IDaaS Platform Audit
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	www.ibm.com/software (http://www-03.ibm.com/software/products/en/access-mgr-mobile).

To integrate IBM Security Access Manager for Mobile with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:

   TLS Syslog Protocol RPM

   IBM Security Access Manager for Mobile DSM RPM
2. Configure your IBM Security Access Manager for Mobile device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an IBM Security Access Manager for Mobile log source on the QRadar console. The following table describes the parameters that require specific values for IBM Security Access Manager for Mobile and IBM Identity as a Service event collection:

Table 617. IBM Security Access Manager for Mobile log source parameters	
Parameter	**Value**
Log Source type	IBM Security Access Manager for Mobile or IBM Identity as a Service
Protocol Configuration	TLS Syslog
Log Source Identifier	The IP address or host name in the Syslog header. Use the packet IP address, if the Syslog header does not contain an IP address or host name.
TLS Listen Port	Type the port number to accept incoming TLS Syslog Event.

4. Saving the log source creates a listen port for incoming TLS Syslog events and generates a certificate for the network devices. The certificate must be copied to any device on your network that can forward encrypted syslog. Additional network devices with a syslog-tls certificate file and the TLS listen port number can be automatically discovered as a TLS syslog log source in QRadar.

Configuring IBM Security Access Manager for Mobile to communicate with QRadar

Configure IBM Security Access Manager for Mobile to send audit logs to IBM QRadar through TLS syslog.

Before you begin

Ensure that IBM Security Access Manager for Mobile has access to QRadar for TLS syslog communication.

Procedure

1. Select **Monitor Analysis and Diagnosis** > **Logs** > **Audit Configuration**.
2. Click the **Syslog** tab and enter the information in the following table.

Field	Value
Enable audit log	Click **Enable audit log**.
Enable verbose audit events	Click **Enable verbose audit events**. Audit events that are not verbose do not contain the JSON payload, which contains details of user activity.
Location of syslog server	Select **On a remote server**
Host	The QRadar server host name or IP.
Port	The port number that you want to use for QRadar to accept incoming TLS syslog events.
Protocol	Select **TLS**
Certificate database (truststore)	The truststore that validates the syslog server certificate.
Enable client certificate authentication	Click **Enable client certificate authentication**. The client can do client certificate authentication during the SSL handshake upon server request.
Certificate database (keystore)	The keystore for client certificate authentication.
Certificate label	The personal certificate for client certificate authentication
Enable disk failover	Clear **Enable disk failover**.

3. Click **Save**.
4. Click **Click here to review the changes or apply them to the system** to review pending changes.
5. Click **Deploy Changes**.

   The runtime server restarts automatically if any of the new changes require a restart.

Configuring IBM IDaaS Platform to communicate with QRadar

You can enable IBM IDaaS Platform audit events to be generated in LEEF format on your IBM IDaaS console.

Before you begin

Ensure that IBM IDaaS Platform is installed and configured on your WAS console.

Procedure

1. Access the IDaas Platform configuration file on your WAS console. *<WAS_home>*/profiles/*<profile_name>*/config/idaas/platform.cofig.properties
2. If the platform.config.properties file does not contain a set of audit properties, configure the following options:

Property	Description
audit.enabled=true	Audit property is enabled.
audit.syslog.message.format=leef **audit.syslog.server=<IP_address>**	Valid type is LEEF.
audit.syslog.transport=TRANSPORT_UDP **audit.syslog.server.port=514**	Transport values are TRANSPORT_UDP and TRANSPORT_TLS.

3. Restart the IBM IDaaS Platform application on your WAS console.

Configuring an IBM IDaaS console to communicate with QRadar

You can enable audit events to be generated in LEEF Syslog format on your IBM IDaaS console.

Before you begin

Ensure that your IBM IDaaS console is installed and configured.

Procedure

1. Select **Secure Access Control** > **Advanced Configuration**.
2. Type idaas.audit.event in the **Filter** text box. The default format is Syslog.
3. Click **Edit**.
4. Select **LEEFSyslog**
5. Click **Save**.
6. Click **Deploy Changes**.

IBM Security Verify Directory

The IBM QRadar DSM for IBM Security Verify Directory collects event logs from your IBM Security Verify Directory.

To integrate IBM Security Verify Directory with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - IBM Security Verify Directory DSM RPM

2. Configure each IBM Security Verify Directory system in your network to enable communication with QRadar.
3. If QRadar does not automatically detect the log source, add a log source on the QRadar Console.

Related tasks

"Adding a log source" on page 5

IBM Security Verify Directory DSM specifications

When you configure the IBM Security Verify Directory DSM, understanding the specifications for the IBM Security Verify Directory DSM can help ensure a successful integration. For example, knowing what protocol to use before you begin can help reduce frustration during the configuration process.

The following table identifies the specifications for the IBM Security Verify Directory DSM:

Table 618. IBM Security Verify Directory DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM	IBM Security Verify Directory (formerly known as IBM Security Directory Server)
RPM file name	DSM-IBMSecurityDirectoryServer-*build_number*.noarch.rpm
Supported version	6.3.1 or later
Protocol	Syslog (LEEF)
QRadar recorded events	All relevant events
Automatically discovered	Yes
Includes identity	Yes
For more information	IBM website

Configuring IBM Security Verify Directory to communicate with QRadar

IBM QRadar can collect LEEF formatted audit events from your IBM Security Verify Directory.

About this task

To configure IBM Security Verify Directory to send logs to IBM QRadar, you must use the IBM Security Verify Directory command line to add an auxiliary object class and then set values for the QRadar log management attributes.

Procedure

1. Create a file (file_name) on the IBM Security Verify Directory or IBM Security Director Server with the following content:

```
dn: cn=Audit, cn=Log Management, cn=Configuration
changetype: modify
add: objectclass
objectclass: ibm-slapdQRadarConfig
```

2. To add the auxiliary object class `ibm-slapdQRadarConfig` for QRadar configuration attributes to `cn=Audit,cn=Log Management,cn=Configuration`, run the following command:

```
# idsldapmodify -h host_name -p portnumber -D cn=RDN_value -w password -f file_name
```

3. Create a new file (new_file) with the following content:

```
dn: cn= specific_log_name, cn=Log Management, cn=configuration
changetype: modify
add:ibm-slapdLogEventQRadarEnabled
ibm-slapdLogEventQRadarEnabled: true
-
add:ibm-slapdLogEventQRadarHostName
ibm-slapdLogEventQRadarHostName: host_name_of_qradar_instance
-
add: ibm-slapdLogEventQRadarPort
ibm-slapdLogEventQRadarPort: port_of_qradar_instance
-
add: ibm-slapdLogEventQRadarMapFilesLocation
ibm-slapdLogEventQRadarMapFilesLocation: directory_location_of_qradar_mapfiles
```

4. Replace the following values in the new_file content:
   a) Replace `host_name_of_qradar_instance` with the destination QRadar Event Collector hostname or IP address.
   b) Replace `port_of_qradar_instance` with 514.
   c) If IBM Security Directory Server or IBM Security Verify Directory is installed, replace `directory_location_of_qradar_mapfiles` with `/opt/ibm/ldap/<INSTALLED_VERSION>/idstools/idslogmgmt/`.
   d) If V6.3.1 is installed, replace `directory_location_of_qradar_mapfiles` with `/opt/ibm/ldap/V6.3.1/idstools/idslogmgmt/`.
   e) If V6.4 is installed, replace `directory_location_of_qradar_mapfiles` with `/opt/ibm/ldap/V6.4/idstools/idslogmgmt/`.

   For example:

```
dn: cn= specific_log_name, cn=Log Management, cn=configuration
changetype: modify
add:ibm-slapdLogEventQRadarEnabled
ibm-slapdLogEventQRadarEnabled: true
-
add:ibm-slapdLogEventQRadarHostName
ibm-slapdLogEventQRadarHostName: qradar-collector.example.com
-
add: ibm-slapdLogEventQRadarPort
ibm-slapdLogEventQRadarPort: 514
-
add: ibm-slapdLogEventQRadarMapFilesLocation
ibm-slapdLogEventQRadarMapFilesLocation: /opt/ibm/ldap/V6.3.1/idstools/idslogmgmt/
```

5. To set the attribute values for QRadar integration, run the following command:

```
# idsldapmodify -h host_name -p portnumber -D cn=RDN_value -w password -f new_file
```

6. To start an instance, run the following command:

```
# ibmslapd -I <instance_name> -n
```

7. Optional: To start log management locally, run the following command:

```
# idslogmgmt -I <instance_name>
```

   To start, get status, and stop log management remotely, run the following commands:

```
# ibmdirctl -D <adminDN> -w <password> -h <host_name> -p <administration server port
number> startlogmgmt# ibmdirctl -D <adminDN> -w <password> -h <host_name> -p <administration
server port number> statuslogmgmt# ibmdirctl -D <adminDN> -w <password> -h <host_name> -p
<administration server port number> stoplogmgmt
```

Syslog log source parameters for IBM Security Verify Directory

If QRadar does not automatically detect the log source, add an IBM Security Verify Directory log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from IBM Security Verify Directory:

Table 619. Syslog log source parameters for the IBM Security Verify Directory DSM

Parameter	Value
Log Source type	IBM Security Verify Directory
Protocol Configuration	Syslog

Related tasks

"Adding a log source" on page 5

IBM Security Guardium Insights

IBM Security Guardium Insights is a modern data security solution. It is built to adapt to changing environments, connect to critical IT and security tools, streamline compliance and audit processes, and intelligently respond to data threats.

The IBM Security Guardium Insights DSM collects rules alerts that are forwarded from IBM Security Guardium Insights.

IBM QRadar collects informational, error, alert, and warnings from IBM Guardium by using syslog. QRadar receives IBM Guardium Policy Builder events in the Log Event Extended Format (LEEF).

QRadar can only automatically discover and map events of the default rules that are included with IBM Security Guardium Insights. Any user-configured events that are needed are displayed as unknowns in QRadar and you must manually map the unknown events.

To integrate IBM Security Guardium Insights with QRadar, complete the following steps:

1. In IBM Security Guardium Insights, configure a syslog alert Integration that Includes the QRadar LEEF header in templates. For more information, see Configuring syslog alerts (https://www.ibm.com/docs/en/guardium-insights/3.2.x?topic=integrations-configuring-syslog-alerts).
2. Create a policy rule action in IBM Security Guardium Insights that uses the syslog alert integration. For more information, see Creating a custom policy (https://www.ibm.com/docs/en/guardium-insights/3.2.x?topic=policies-creating-custom-policy).
3. Configure an IBM Security Guardium Insights log source in QRadar. For more information, see Syslog log source parameters for IBM Security Guardium Insights.
4. Identify and map unknown events for IBM Security Guardium Insights in QRadar . For more information, see Creating an event map for IBM Guardium events.
5. You can use sample event messages to verify a successful integration with QRadar. For more information, see IBM Security Guardium Insights sample event messages.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Related reference

"IBM Security Guardium Insights DSM specifications" on page 987

When you configure IBM Security Guardium Insights, understanding the specifications for the IBM Security Guardium Insights DSM can help ensure a successful integration. For example, knowing what

the supported protocol for IBM Security Guardium Insights is before you begin can help reduce frustration during the configuration process.

IBM Security Guardium Insights DSM specifications

When you configure IBM Security Guardium Insights, understanding the specifications for the IBM Security Guardium Insights DSM can help ensure a successful integration. For example, knowing what the supported protocol for IBM Security Guardium Insights is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the IBM Security Guardium Insights DSM.

Table 620. IBM Security Guardium Insights data source type specifications

Specification	**Value**
Manufacturer	IBM Security
DSM name	IBM Security Guardium Insights
RPM name	`DSM-IBMSecurityGuardiumInsights-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported protocol	Syslog
Event format	LEEF
Recorded event types	Out of Box Policy Violation Rules
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	• To install IBM Security Guardium Insights on premises, go to Setting up IBM Security Guardium Insights (https://www.ibm.com/docs/en/guardium-insights/3.2.x?topic=installing). • For on premises IBM Security Guardium Insights configuration instructions, go to Configuring syslog alerts (https://www.ibm.com/docs/en/guardium-insights/3.2.x?topic=integrations-configuring-syslog-alerts). • To use IBM Security Guardium Insights Saas, go to Getting started (https://www.ibm.com/docs/en/guardium-insights/saas?topic=getting-started). • For Saas based IBM Security Guardium Insights configuration instructions, go to Configuring syslog alerts (https://www.ibm.com/docs/en/guardium-insights/saas?topic=integrations-configuring-syslog-alerts)

Syslog log source parameters for IBM Security Guardium Insights

If QRadar does not automatically detect the log source, add an IBM Guardium log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from IBM Guardium:

Table 621. Syslog log source parameters for the IBM Guardium DSM	
Parameter	**Value**
Log Source type	IBM Security Guardium Insights
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or hostname for the IBM InfoSphere Guardium appliance.

Related tasks

"Adding a log source" on page 5

Creating an event map for IBM Guardium events

Event mapping is needed for some IBM Guardium events. Due to the customizable nature of policy rules, most events, except the default policy events do not contain a predefined IBM QRadar Identifier (QID) map to categorize security events.

About this task

You can individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track recurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for IBM Guardium are categorized as unknown. Unknown events are easily identified as the **Event Name** column and **Low Level Category** columns display Unknown.

As your device forwards events to QRadar, it can take time to categorize all events for a device. Some events might not be generated immediately by the event source appliance or software. It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, we suggest that you repeat this search until you are satisfied that most of your events are identified.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select the log source group or **Other**.

   Log sources that are not assigned to a group are categorized as Other.
6. From the **Log Source** list, select your IBM Guardium log source.
7. Click **Add Filter**.

   The **Log Activity** tab is displayed with a filter for your log source.
8. From the **View** list, select **Last Hour**.

   Any events that are generated by the IBM Guardium DSM in the last hour are displayed. Events that are displayed as unknown in the **Event Name** column or **Low Level Category** column require event mapping in QRadar.

   Note: You can save your existing search filter by clicking **Save Criteria**.

   You are now ready to modify the event map.

Modifying the event map

Modifying an event map allows for the manual categorization of events to a IBM QRadar Identifier (QID) map. Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

About this task

IBM Guardium event map events that don't have a defined log source are not mapped to an event. Events without a log source display **SIM Generic Log** in the **Log Source** column.

Procedure

1. On the **Event Name column**, double-click an unknown event for IBM Guardium.

   The detailed event information is displayed.
2. Click **Map Event**.
3. From the **Browse for QID** pane, select any of the following search options to narrow the event categories for a QRadar Identifier (QID):
   - From the **High-Level Category** list, select a high-level event categorization.
   - For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *IBM QRadar Administration Guide*.
   - From the **Low-Level Category** list, select a low-level event categorization.
   - From the **Log Source Type** list, select a log source type.

   The **Log Source Type** list gives the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, IBM Guardium provides policy events, you might select another product that likely captures similar events.
4. To search for a QID by name, type a name in the **QID/Name** field.

   The **QID/Name** field gives the option to filter the full list of QIDs for a specific word, for example, policy.
5. Click **Search**.

   A list of QIDs are displayed.
6. Select the QID you want to associate to your unknown event.
7. Click **OK**.

   QRadar maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.

   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

IBM Security Guardium Insights sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Security Guardium Insights sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that an attempted login to the database is not successful.

```
<6>2023-05-28T03:55:22Z ibm.guardiuminsight.test qradar[14]: LEEF:1.0|IBM|Guardium|3.0|
6472d05f7125753b04c11c8d|xa6|5 failed logins within 1 minute for any user
```

```
on any database|x7c|eventTime=2023-01-07T00:00:00Z|serverType=POSTGRESQL|client=10.0.0.248|
clientName=|server=10.0.0.72|serverName=|clientPort=2878|serverPort=432|serviceName=TIDNCSAE7M|
databaseName=POSTGRES|netProtocol=TCP|dbProtocol=AURORA POSTGRESQL|
dbProtocol Version=12.12.2|dbUser=user2|userName=|sourceProgram=|authCode=0|
requestType=LOGIN_FAILED|lastError=28P01|sql=|sqlStatus=EXCEPTION
```

Table 622. Highlighted values in the IBM Security Guardium Insights sample event

QRadar field name	Highlighted values in the event payload
Event ID	**Login_failed**
Username	**user2**
Source IP	**10.0.0.248**
Source port	**2878**
Destination IP	**10.0.0.72**
Destination port	**432**
Device time	**2023-05-28T03:55:22Z**

Sample 2: The following sample event message shows the event ID that is generated based on an out of the box rule violation description.

```
<6>2023-05-24T06:15:26Z ibm.guardiuminsight.test qradar[14]: LEEF:1.0|IBM|Guardium|3.0|
646daaf39ed5984ef46404a7|xa6|sql err|x7c|eventTime=2023-01-01T00:00:00Z|serverType=POSTGRESQL|
client=10.0.0.5|clientName=|server=10.0.0.6|serverName=34682495|clientPort=6785|serverPort=200|
serviceName=3468249|databaseName=3468|netProtocol=TCP|dbProtocol=UC: POSTGRESQL|
dbProtocol Version=|dbUser=user1|userName=user11|sourceProgram=|authCode=0|requestType=UNKNOWN|
lastError=syntax error at or near . at character 22|sql=NA|sqlStatus=EXCEPTION
```

Table 623. Highlighted values in the IBM Security Guardium Insights sample event

QRadar field name	Highlighted values in the event payload
Event ID	**sql err**
Username	**user11**
Source IP	**10.0.0.5**
Source port	**6785**
Destination IP	**10.0.0.6**
Destination port	**200**
Protocol	**6**
Device time	**2023-01-01T00:00:00Z**

IBM Security Identity Governance

The IBM QRadar DSM for IBM Security Identity Governance collects audit events from IBM Security Governance servers.

The following table identifies the specifications for the IBM Security Identity Governance DSM:

Table 624. IBM Security Identity Governance (ISIG) DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM Security Identity Governance

Table 624. IBM Security Identity Governance (ISIG) DSM specifications (continued)	
Specification	**Value**
RPM file name	`DSM-IBMSecurityIdentityGovernance-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	IBM Security Identity Governance V5.1.1
Protocol	JDBC
Event format	NVP
Recorded event types	Audit
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	IBM website (https://www.ibm.com)

To integrate IBM Security Identity Governance with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console. If multiple DSM RPMs are required, the integration sequence must reflect the DSM RPM dependency.
   - IBM Security Identity Governance (ISIG) DSM RPM
   - JDBC Protocol RPM
2. Configure a JDBC log source to poll for events from your IBM Security Identity Governance database.
3. Ensure that no firewall rules block communication between QRadar and the database that is associated with IBM Security Identity Governance.
4. If QRadar does not automatically detect the log source, add an IBM Security Identity Governance log source on the QRadar Console. The following table describes the parameters that require specific values for IBM Security Identity Governance event collection:

Table 625. IBM Security Identity Governance DSM log source parameters	
Parameter	**Value**
Log Source Name	Type a unique name for the log source.
Log Source Description	Type a description for the log source.
Log Source Type	IBM Security Identity Governance
Protocol Configuration	JDBC

Table 625. IBM Security Identity Governance DSM log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	Select **Oracle** or **DB2** for the database that you want to use as the event source.
Database Name	The name of the database to which you want to connect.
IP or Hostname	The IP address or host name of the IBM Security Governance database server.
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix - 9088 • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the **Port** field blank.
Username	A user account for QRadar in the database.
Password	The password that is required to connect to the database.
Predefined Query	Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the **none** option.
Table Name	AUDIT_LOG

Table 625. IBM Security Identity Governance DSM log source parameters (continued)	
Parameter	**Value**
Select List	*
Compare Field	ID
Use Prepared Statements	Enable the check box.
Start Date and Time	The initial date and time for database polling.
Polling Interval	The amount of time, in seconds, between queries to the database table. The default polling interval is 10 seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 20,000 EPS.
Security Mechanism	From the list, select the security mechanism that is supported by your DB2 server. If you don't want to select a security mechanism, select **None**. The default is **None**. For more information about security mechanisms that are supported by DB2 environments, see the IBM Support website (https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html)
Use Oracle Encryption	*Oracle Encryption and Data Integrity settings* is also known as *Oracle Advanced Security*. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.

For more information about configuring JDBC parameters, see c_logsource_JDBCprotocol.dita

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

JDBC log source parameters for IBM Security Identity Governance

If QRadar does not automatically detect the log source, add a IBM Security Identity Governance log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from IBM Security Identity Governance:

Table 626. JDBC log source parameters for the IBM Security Identity Governance DSM	
Parameter	**Value**
Log Source type	IBM Security Identity Governance
Protocol Configuration	JDBC
Table Name	AUDIT_LOG
Compare Field	ID

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

"Adding a log source" on page 5

IBM Security Identity Manager

The IBM QRadar DSM for IBM Security Identity Manager accepts audit, recertification, and system events from IBM Security Identity Manager appliances.

To integrate IBM Security Identity Manager with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the DSM Common RPM on your QRadar Console.
2. Configure your IBM Security Identity Manager to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a IBM Security Identity Manager log source on the QRadar Console.

To collect events with QRadar, you must have the IBM Security Identity Manager JDBC protocol that is installed, which allows QRadar to poll for event information in the ITIMDB database. IBM Security Identity Manager events are generated from the audit table along with several other tables from the database.

Before you configure QRadar to integrate with IBM Security Identity Manager, create a database user account and password in IBM Security Identity Manager for QRadar. Your QRadar user needs read permission for the ITIMDB database, which stores IBM Security Identity Manager events.

The IBM Security Identity Manager protocol allows QRadar to log in and poll for events from the database. Creating a QRadar account is not required, but it is suggested for tracking and securing your event data.

Note: Ensure that no firewall rules are blocking the communication between your IBM Security Identity Manager appliance and QRadar.

Related concepts

"IBM Security Identity Manager JDBC log source parameters for IBM Security Identity Manager" on page 994

IBM Security Identity Manager JDBC log source parameters for IBM Security Identity Manager

If QRadar does not automatically detect the log source, add an IBM Security Identity Manager log source on the QRadar Console by using the IBM Security Identity Manager JDBC protocol.

When using the IBM Security Identity Manager JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from IBM Security Identity Manager:

Table 627. IBM Security Identity Manager JDBC log source parameters for the IBM Security Identity Manager DSM

Parameter	Value
Log Source type	IBM Security Identity Manager
Protocol Configuration	IBM Security Identity Manager JDBC
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM Security Identity Manager devices.
Database Type	From the **Database Type** list, select a database to use for the event source. The options include the following databases: • DB2 - Select this option if DB2 is the database type on your IBM Security Identity Manager appliance. DB2 is the default database type. • **MSDE** - Select this option if MSDE is the database type on your IBM Security Identity Manager appliance. • **Oracle** - Select this option if Oracle is the database type on your IBM Security Identity Manager appliance.
Database Name	The name of the database to which you want to connect.
IP or Hostname	Type the IP address or host name of the IBM Security Identity Manager appliance.
Port	Type the port number that is used by the database server. The default that is displayed depends on the selected **Database Type**. The valid range is 0 - 65536. The default for DB2 is port 50000. The JDBC configuration port must match the listener port of the database. The database must have incoming TCP connections that are enabled to communicate with QRadar. The default port number for all options include: • DB2 - 50000 • MSDE - 1433 • Oracle - 1521 If you define a database Instance when you use MSDE as the database type, you must leave the **Port** parameter blank in your configuration.
Username	Type the database user name. The user name can be up to 255 alphanumeric characters in length. The user name can also include underscores (_).

Table 627. IBM Security Identity Manager JDBC log source parameters for the IBM Security Identity Manager DSM (continued)

Parameter	Value
Password	Type the database password. The password can be up to 255 characters in length.
Schema Name	Type `ISIMUSER` in the **Schema Name** field.
Table Name	Type `AUDIT_EVENT` as the name of the table or view that includes the event records. If you change the value of this field from the default, events cannot be properly collected by the IBM Security Identity Manager JDBC protocol. The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Select List	Type * to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if needed for your configuration. The list must contain the field that is defined in the **Compare Field** parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type `TIMESTAMP` to identify new events added between queries to the table by their time stamp. The compare field can be up to 255 alphanumeric characters in length. The list can include the special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Start Date and Time (Optional)	Configure the start date and time for database polling. The **Start Date and Time** parameter must be formatted as yyyy-MM-dd HH: mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.

Table 627. IBM Security Identity Manager JDBC log source parameters for the IBM Security Identity Manager DSM (continued)

Parameter	Value
Polling Interval	Type the polling interval in seconds, which is the amount of time between queries to the database table. The default polling interval is 30 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Authentication Domain	If you select **MSDE** as the **Database Type**, the **Authentication Domain** field is displayed. If your network is configured to validate users with domain credentials, you must define a Windows Authentication Domain. Otherwise, leave this field blank. The authentication domain must contain alphanumeric characters. The domain can include the following special characters: underscore (_), en dash (-), and period(.).
Database Instance	If you select **MSDE** as the **Database Type**, the **Database Instance** field is displayed. Type the instance to which you want to connect, if you have multiple SQL server instances on one server. If you use a non-standard port in your database configuration, or access to port 1434 for SQL database resolution is blocked, you must leave the **Database Instance** parameter blank in your configuration.

Table 627. IBM Security Identity Manager JDBC log source parameters for the IBM Security Identity Manager DSM (continued)	
Parameter	**Value**
Use Named Pipe Communication	If you select **MSDE** as the **Database Type**, the **Use Named Pipe Communication** check box is displayed. By default, this check box is clear. Select this check box to use an alternative method to a TCP/IP port connection. When you use Named Pipe connection, the user name and password must be the appropriate Windows authentication user name and password and not the database user name and password. Also, you must use the default Named Pipe.
Use NTLMv2	If you select **MSDE** as the **Database Type**, the **Use NTLMv2** check box is displayed. Select the **Use NTLMv2** check box to force MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
Database Cluster Name	If you select the **Use Named Pipe Communication** check box, the **Database Cluster Name** parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.

Related tasks

"Adding a log source" on page 5

IBM Security Network IPS (GX)

The IBM Security Network IPS (GX) DSM for IBM Security QRadar collects LEEF-based events from IBM Security Network IPS appliances by using the syslog protocol.

The following table identifies the specifications for the IBM Security Network IPS (GX) DSM:

Parameter	Value
Manufacturer	IBM
DSM	Security Network IPS (GX)
RPM file name	DSM-IBMSecurityNetworkIPS-*QRadar_version-Build_number*.noarch.rpm
Supported versions	v4.6 and later (UDP) v4.6.2 and later (TCP)
Protocol	syslog (LEEF)

Parameter	Value
QRadar recorded events	Security alerts (including IPS and SNORT) Health alerts System alerts IPS events (Including security, connection, user defined, and OpenSignature policy events)
Automatically discovered?	Yes
Includes identity?	No

To integrate the IBM Security Network IPS (GX) appliance with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM Security Network IPS (GX) RPMs from the IBM Support Website onto your QRadar Console.
2. For each instance of IBM Security Network IPS (GX), configure your IBM Security Network IPS (GX) appliance to enable communication with QRadar.
3. If QRadar does not automatically discover the log source, create a log source for each instance of IBM Security Network IPS (GX) on your network.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring your IBM Security Network IPS (GX) appliance for communication with QRadar

To collect events with QRadar, you must configure your IBM Security Network IPS (GX) appliance to enable syslog forwarding of LEEF events.

Before you begin

Ensure that no firewall rules block the communication between your IBM Security Network IPS (GX) appliance and QRadar.

Procedure

1. Log in to your IPS Local Management Interface.
2. From the navigation menu, select **Manage System Settings** > **Appliance** > **LEEF Log Forwarding**.
3. Select the **Enable Local Log** check box.
4. In the **Maximum File Size** field, configure the maximum file size for your LEEF log file.
5. From the Remote Syslog Servers pane, select the **Enable** check box.
6. In the **Syslog Server IP/Host** field, type the IP address of your QRadar Console or Event Collector.
7. In the **TCP Port** field, type 514 as the port for forwarding LEEF log events.

   Note: If you use v4.6.1 or earlier, use the **UDP Port** field.
8. From the event type list, enable any event types that are forwarded to QRadar.
9. If you use a TCP port, configure the **`crm.leef.fullavp`** tuning parameter:
   a) From the navigation menu, select **Manage System Settings** > **Appliance** > **Tuning Parameters**.
   b) Click **Add Tuning Parameters**.
   c) In the **Name** field, type `crm.leef.fullavp`.
   d) In the **Value** field, type `true`.
   e) Click **OK**.

Syslog log source parameters for IBM Security Network IPS (GX)

If QRadar does not automatically detect the log source, add an IBM Security Network IPS (GX) log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from IBM Security Network IPS (GX):

Table 628. Syslog log source parameters for the IBM Security Network IPS (GX) DSM

Parameter	Value
Log Source type	IBM Security Network IPS (GX)
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name for the log source as an identifier for events from your IBM Security Network IPS (GX) appliance.

Related tasks

"Adding a log source" on page 5

IBM Security Privileged Identity Manager

The IBM QRadar DSM for IBM Security Privileged Identity Manager collects events by using the JDBC protocol.

The following table identifies the specifications for the IBM Security Privileged Identity Manager DSM:

Table 629. IBM Security Privileged Identity Manager DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM Security Privileged Identity Manager
RPM file name	DSM-IBMSecurityPrivilegedIdentityManager-*QRadar_version-build_number*.noarch.rpm
Supported versions	V1.0.0 to V2.1.1
Protocol	JDBC
Recorded event types	Audit Authentication System
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	IBM Security Privileged Identity Manager website (https://www.ibm.com/support/knowledgecenter/en/SSRQBP/welcome.html)

To collect events from IBM Security Privileged Identity Manager, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto yourQRadar Console:
   - JDBC Protocol Rational® Portfolio Manager
   - IBM Security Privileged Identity Manager DSM RPM
2. Configure IBM Security Privileged Identity Manager to communicate with QRadar.
3. Add an IBM Security Privileged Identity Manager log source on the QRadar Console. The following table describes the parameters that require specific values for event collection:

Table 630. IBM Security Privileged Identity Manager JDBC log source parameters

Parameter	Value
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	IBM Security Privileged Identity Manager
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	MSDE
Database Name	The database name must match the database name that is specified in the **Log Source Identifier** field.
IP or Hostname	Must match the value in the **Hostname** field in IBM Security Privileged Identity Manager.
Port	Must match the value in the **Port** field in IBM Security Privileged Identity Manager.
Username	Must match the value in the **Database administrator ID** field in IBM Security Privileged Identity Manager.
Password	The password that is used to connect to the database.
Authentication Domain	If you did not select **Use Microsoft JDBC**, **Authentication Domain** is displayed. The domain for MSDE databases that are a Windows domain. If your network does not use a domain, leave this field blank.

Table 630. IBM Security Privileged Identity Manager JDBC log source parameters (continued)	
Parameter	**Value**
Database Instance	The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank in the log source configuration.
Predefined Query	Select **None**.
Table Name	<*DB2ADMIN*>.V_PIM_AUDIT_EVENT Replace *DB2ADMIN* with the actual database schema name as identified in the **Database Administrator ID** parameter in IBM Security Privileged Identity Manager.
Select List	Type an asterisk (*) to select all fields from the table or view.
Compare Field	Identifies new events that are added to the table between queries. Type TIMESTAMP.
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and run the SQL statement numerous times with different parameters. Select this check box.
Start Date and Time (Optional)	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	The amount of time between queries to the event table. Use the default **Polling Interval** value of **10**.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 20,000.
Use Named Pipe Communication	If you did not select **Use Microsoft JDBC**, **Use Named Pipe Communication** is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.

Table 630. IBM Security Privileged Identity Manager JDBC log source parameters (continued)	
Parameter	**Value**
Database Cluster Name	If you selected **Use Named Pipe Communication**, the **Database** parameter displays. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.
Use NTLMv2	If you did not select **Use Microsoft JDBC**, **Use NTLMv2** is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use SSL	Select this option if your connection supports SSL.
Microsoft SQL Server Hostname	If you selected **Use Microsoft JDBC** and **Use SSL**, the **Microsoft SQL Server Hostname** parameter is displayed. You must type the host name for the Microsoft SQL server.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring IBM Security Privileged Identity Manager to communicate with QRadar

To communicate with IBM QRadar, the IBM Security Privileged Identity Manager DB2 database must have incoming TCP connections enabled.

Procedure

1. Log in to IBM Security Privileged Identity Manager.
2. Click the **Configure Privileged Identity Manager** tab.
3. In the **Manage External Entities** pane, select **Database Server Configuration**.
4. Double-click the **Identity data store** row in the **Database Server Configuration** column.
5. Record the values for the following parameters. You need these values when you configure a log source in QRadar.
   - Host name
   - Port
   - Database name
   - Database Administrator ID

6. **Important:** If you are using ISPIM 2.0.2 FP 6 and later, do not complete this step.

   Create a view in IBM Security Privileged Identity Manager DB2 database in the same schema as identified in the **Database Administrator ID** parameter, by running the following SQL statement:

```
CREATE view V_PIM_AUDIT_EVENT ASSELECT ae.ID, ae.itim_event_category as event_category,
ae.ENTITY_NAME, service.NAME service_name, ae.ENTITY_DN, ae.ENTITY_TYPE, ae.ACTION,
ae.INITIATOR_NAME, ae.INITIATOR_DN, ae.CONTAINER_NAME, ae.CONTAINER_DN, ae.RESULT_SUMMARY,
ae.TIMESTAMP, lease.POOL_NAME, lease.LEASE_DN, lease.LEASE_EXPIRATION_TIME,
lease.JUSTIFICATION,ae.COMMENTS, ae.TIMESTAMP2, ae.WORKFLOW_PROCESS_IFROM AUDIT_EVENT aeLEFT
OUTER JOIN AUDIT_MGMT_LEASE lease ON (ae.id = lease.event_id)LEFT OUTER JOIN
SA_EVALUATION_CREDENTIAL cred ON (LOWER(ae.entity_dn) = LOWER(cred.DN))LEFT OUTER JOIN
V_SA_EVALUATION_SERVICE service ON (LOWER(cred.service_dn) = LOWER(service.dn));
```

IBM Security Privileged Identity Manager sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when you use the JDBC protocol for the IBM Security Privileged Identity Manager DSM:

Table 631. IBM Security Privileged Identity Manager sample message supported by the IBM Security Privileged Identity DSM.

Event name	Low-level category	Sample log message
CredentialLease Management GetPassword SUCCESS	Information	ID: "4988747757478318080" EVENT_CATEGORY: "CredentialLeaseManagement" ENTITY_NAME: "suser1" RESOURCE_NAME: "PIM 202 Data Tier" ENTITY_DN: "erglobalid=8684147307608490000,ou=credentials,ou=credCatalog,erglobalid=0000000000000000000,ou=ibm,dc=com" ENTITY_TYPE: "Credential" ACTION: "GetPassword" INITIATOR_NAME: "user" INITIATOR_DN: "eruid=user,ou=systemUser,ou=itim,ou=ibm,dc=com" CONTAINER_NAME: "USWest" CONTAINER_DN: "erglobalid=3874502227230100000,ou=orgChart,erglobalid=0000000000000000000,ou=ibm,dc=com" RESULT_SUMMARY: "SUCCESS" TIMESTAMP: "2018-10-05 17:17:05:320 GMT" POOL_NAME: "" LEASE_DN: "" LEASE_EXPIRATION_TIME: "" JUSTIFICATION: "" COMMENTS: "null" TIMESTAMP2: "null" IDP_NAME: "" SESSION_ID: "" TARGET: "" CLIENT_IP: "" RECORDING_ID: "" CRED_TYPE: "PASSWORD"

IBM Security QRadar EDR

Enrich SIEM logs with high-fidelity endpoint alerts by using the IBM Security QRadar EDR DSM.

IBM Security QRadar EDR is formerly known as IBM Security ReaQta. The DSM RPM name remains as IBM Security ReaQta.

Integrating IBM Security QRadar EDR with QRadar SIEM

Tip: You can integrate IBM Security QRadar EDR with QRadar SIEM with no impact to your EPS count. Contact your IBM sales representative or IBM Business Partner for details.

To integrate QRadar EDR with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - PROTOCOL IBMSecurityReaQtaRESTAPI RPM
   - DSM - IBMSecurityReaQta DSM RPM

2. Configure your QRadar EDR platform to send alerts to QRadar. See Configuring IBM Security QRadar EDR to communicate with QRadar.
3. Add a QRadar EDR log source that uses the IBM Security QRadar EDR protocol on the QRadar Console. See "IBM Security QRadar EDR REST API data source parameters for QRadar EDR" on page 1006.

   For more information about adding a log source, see Adding a log source.
4. Configure QRadar to collect only the first username from the QRadar EDR alert for the username parameter value. See Configuring QRadar to collect only the first username from the alert.

Adding your additional EPS

When you have entitlements to both IBM QRadar and IBM Security QRadar EDR, you are entitled to an extra 100 EPS to use in QRadar. To add this additional EPS in QRadar, follow these steps:

1. Contact your local sales representative and provide them with your sales order numbers to obtain the license key.
2. Upload the license key in QRadar.
3. Allocate the license key to a host.
4. Deploy the changes.

Related concepts

"IBM Security QRadar EDR REST API data source parameters for QRadar EDR" on page 1006
Add an IBM Security QRadar EDR log source that uses the IBM Security QRadar EDR REST API protocol in IBM QRadar.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

"Configuring QRadar EDR to communicate with QRadar" on page 1006
To send events from IBM Security QRadar EDR to IBM QRadar, you need an API ID and a Secret Key.

"Configuring QRadar to collect only the first username from the alert " on page 1007

Related reference

"QRadar EDR DSM specifications" on page 1005
When you configure IBM Security QRadar EDR, understanding the specifications for the QRadar EDR DSM can help ensure a successful integration. For example, knowing what the supported version of QRadar EDR is before you begin can help reduce frustration during the configuration process.

QRadar EDR DSM specifications

When you configure IBM Security QRadar EDR, understanding the specifications for the QRadar EDR DSM can help ensure a successful integration. For example, knowing what the supported version of QRadar EDR is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the QRadar EDR DSM.

Table 632. QRadar EDR DSM specifications

Specification	**Value**
Manufacturer	IBM Security
DSM name	IBM Security QRadar EDR
RPM file name	DSM-*IBMSecurityReaQta-QRadar_version-build_number*.noarch.rpm
Supported version	3.9.0
Protocol	IBM Security QRadar EDR REST API

Table 632. QRadar EDR DSM specifications (continued)	
Specification	**Value**
Event format	JSON
Recorded event types	Alerts
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	Yes
More information	IBM Security QRadar EDR as a Service documentation

Configuring QRadar EDR to communicate with QRadar

To send events from IBM Security QRadar EDR to IBM QRadar, you need an API ID and a Secret Key.

Procedure

1. Log in to your QRadar EDR console.
2. Go to **Administration** > **API Applications**.
3. Click **Create Application**.
4. In the **Application Name** field, type a name for the application, then click **Create**.
5. Copy and save the **App ID** and the **Secret Key** values. You need these values when you add a log source in QRadar.

What to do next

Adding a log source that uses the IBM Security QRadar EDR REST API protocol

Related tasks

"Adding a log source" on page 5

IBM Security QRadar EDR REST API data source parameters for QRadar EDR

Add an IBM Security QRadar EDR log source that uses the IBM Security QRadar EDR REST API protocol in IBM QRadar.

When you use the IBM Security QRadar EDR REST API protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collectIBM Security QRadar EDR REST API events from QRadar EDR.

Table 633. IBM Security QRadar EDR REST API protocol parameters for the IBM Security QRadar EDR DSM	
Parameter	**Value**
`Log source type`	IBM Security QRadar EDR
`Protocol Configuration`	IBM Security QRadar EDR REST API
`Log source identifier`	The **Log source identifier** must match the server address or the server name of the QRadar EDR hive.
`Server Address`	The IP or hostname of the QRadar EDR server.

Table 633. IBM Security QRadar EDR REST API protocol parameters for the IBM Security QRadar EDR DSM (continued)	
Parameter	**Value**
App ID	The **App ID** value that you saved when you completed the "Configuring QRadar EDR to communicate with QRadar" on page 1006.
Secret Key	The **Secret Key** value that you saved when you completed the "Configuring QRadar EDR to communicate with QRadar" on page 1006.

Full a complete list of IBM Security QRadar EDR REST API protocol parameters and their values, see IBM Security QRadar EDR REST API protocol.

Related tasks

"Adding a log source" on page 5

"Configuring QRadar EDR to communicate with QRadar" on page 1006

To send events from IBM Security QRadar EDR to IBM QRadar, you need an API ID and a Secret Key.

Configuring QRadar to collect only the first username from the alert

If you want to change the way that IBM QRadar processes IBM Security QRadar EDR events, use the DSM Editor to collect only the first username from the alert.

By default, the QRadar EDR DSM collects all usernames from the alert, combines them into a comma-separated list and places them in the **username** field.

Procedure

1. On the **Admin** tab, in the **Data Sources** section, click **DSM Editor**.
2. From the **Select Log Source Type** window, select **IBM Security QRadar EDR** from the list, and click **Select**.
3. On the **Configuration** tab, set **Display DSM Parameters Configuration** to **on**.
4. From the **Event Collector** list, select the event collector for the log source.
5. Set **Get First Username** to **on**.
6. Click **Save** and close the DSM Editor.

QRadar EDR sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Security QRadar EDR sample message when you use the IBM Security QRadar EDR REST API protocol

The following sample event message shows the alert that was generated when a customer successfully enrolled with QRadar EDR.


```
{"id":"885873017052213250","localId":"885872997599021058","endpointId":"885857527403642880","tri
ggerCondition":6,"endpoint":
{"id":"885857527403642880","machineId":"eba24ff6f42f32e7b693b2aad82476c3612d934b08d0999ff0520a91
d2871a45","osType":1,"cpuVendor":1,"arch":2,"cpuDescr":"Intel(R) Xeon(R) CPU           X5650  @
2.67GHz","kernel":"10.0","os":"Windows 10
Pro","name":"\","state":1,"registrationTime":"2022-07-14T13:21:32.973Z","agentVersion":"3.6.1","
componentsVersions":[{"name":"keeper","version":"3.6.0","build":"19.1627291555548.commit"},
{"name":"probos","version":"3.5.0","build":"3.5.0"},
```

```
{"name":"rqtsentry","version":"3.6.1","build":"119.1632119719010.commit"},
{"name":"rqtnetsentry","version":"3.6.0","build":"44.1627295520120.commit"},
{"name":"installer","version":"3.6.1","build":""}],"isVirtualMachine":false,"isDomainController"
:false,"isServer":false,"sessionStart":"2022-07-14T13:21:36.953Z","sessionEnd":"2022-07-14T21:45
:57.434Z","lastSeenAt":"2022-07-14T21:40:57.434Z","disconnectionReason":0,"localAddr":"10.0.0.11
9","hvStatus":0,"macs":["00:00:5e:00:53:ff"],"isolated":false,"connected":true,"tags":
[],"groups":[{"id":"847194699834851335","name":"Digital Sales","description":"Digital Sales
Group"}],"avInstalled":false},"triggerEvents":
[{"id":"885873015911350273","category":"policies","localId":"885872997569660929","endpointId":"8
85857527403642880","receivedAt":"2022-07-14T14:23:05.718Z","happenedAt":"2022-07-14T14:23:01.345
Z","relevance":88,"severity":"medium","trigger":true,"manuallyAdded":false,"process":
{"id":"885857527403642880:7664:1657808581301","parentId":"885857527403642880:3172:1657804956599"
,"endpointId":"885857527403642880","program":{"path":"c:\\users\\admin\\appdata\\roaming\
\bittorrent\
\bittorrent.exe","filename":"bittorrent.exe","md5":"3a72aae846afdd8c7f070f390a2151b0","sha1":"da
db6c535731cf4445ee8ce2c216585ccc80760b","sha256":"63a52c497a4a0f8c62d7686486fd3be8c3297024e336c0
953ab2dcad9dceed3c","certInfo":{"signer":"BitTorrent Inc","issuer":"Symantec Class 3 SHA256
Code Signing
CA","trusted":true,"expired":false},"size":2106408,"arch":"x32","fsName":"bittorrent.exe"},"user
":"DESKTOP-EXAMPLE123\
\Admin","pid":7664,"startTime":"2022-07-14T14:23:01.301Z","ppid":3172,"pstartTime":"2022-07-14T1
3:22:36.599Z","userSID":"S-1-5-21-979315260-1110968185-3366233752-1001","privilegeLevel":"MEDIUM
","noGui":false,"logonId":"0x41483"},"eventType":28,"data":{"matched":
[{"policyId":"851883733567930372","versionId":"851883733567934469","policyTitle":"Hive-Cloud
policy on:
63a52c497a4a0f8c62d7686486fd3be8c3297024e336c0953ab2dcad9dceed3c","policyDescription":"Automatic
 policy","scope":"global","groups":[],"matcher":
{"id":"851883733567938566","hash":"63a52c497a4a0f8c62d7686486fd3be8c3297024e336c0953ab2dcad9dcee
d3c","alg":1,"type":2}}],"_t":"r"}}],"totalEventCount":34857,"byTypeEventCount":
[{"type":37,"count":8297},{"type":12,"count":6663},{"type":5,"count":5267},
{"type":65,"count":4395},{"type":8,"count":3420},{"type":21,"count":3257},
{"type":38,"count":1765},{"type":7,"count":966},{"type":6,"count":744},{"type":57,"count":35},
{"type":10,"count":20},{"type":2,"count":12},{"type":3,"count":5},{"type":11,"count":3},
{"type":13,"count":3},{"type":9,"count":2},{"type":14,"count":1},{"type":28,"count":1},
{"type":30,"count":1}],"impact":88,"severity":"medium","closed":true,"closedAt":"2022-07-14T14:2
4:50.582Z","activityState":"archived","terminationReason":0,"receivedAt":"2022-07-14T14:23:05.99
0Z","happenedAt":"2022-07-14T14:23:01.352Z","tags":[],"endpointState":
{"osType":1,"cpuVendor":1,"arch":2,"cpuDescr":"Intel(R) Xeon(R) CPU           X5650  @
2.67GHz","kernel":"10.0","os":"Windows 10 Pro","hvStatus":0,"name":"DESKTOP-
EXAMPLE123","isolated":false,"localAddr":"10.0.0.119","macs":
["00:00:5e:00:53:ff"],"componentsVersions":
[{"name":"keeper","version":"3.6.0","build":"19.1627291555548.commit"},
{"name":"probos","version":"3.5.0","build":"3.5.0"},
{"name":"rqtsentry","version":"3.6.1","build":"119.1632119719010.commit"},
{"name":"rqtnetsentry","version":"3.6.0","build":"44.1627295520120.commit"},
{"name":"installer","version":"3.6.1","build":""}],"endpointVersion":"3.6.1","tags":[],"groups":
[{"id":"847194699834851335","name":"Digital Sales","description":"Digital Sales
Group"}]},"alertStatus":"malicious"}
```


Table 634. Highlighted fields in the QRadar EDR event

QRadar field name	Highlighted payload field name
Event ID	**6**
Source IP	**10.0.0.119**
Username	**DESKTOP-EXAMPLE123\\Admin**
Source Mac	**00:00:5e:00:53:ff**

IBM Security Randori Recon

The IBM QRadar DSM for IBM Security Randori Recon collects alerts from Randori Recon.

To integrate Randori Recon with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - PROTOCOL IBMSecurityRandoriRESTAPI RPM
   - DSM IBMSecurityRandoriRESTAPI DSM RPM

2. Add a Randori Recon log source that uses the IBM Security Randori REST API protocol on the QRadar Console. See "IBM Security Randori REST API protocol log source parameters for IBM Security Randori Recon" on page 1009.

   Tip: Before you can configure a log source for Randori Recon in QRadar, you must obtain an API Key from the Randori web portal. You need to have a Randori account to access the portal. For more information about obtaining this value, see How to Add an API token (https://www.ibm.com/docs/en/SSD5I5K/intapi_api_AddAPIToken.html).

   For more information about adding a log source in QRadar, see Adding a log source.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

IBM Security Randori Recon DSM specifications

When you configure the IBM Security Randori Recon DSM, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported protocols for Randori Recon are before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the IBM Security Randori Recon DSM.

Table 635. IBM Security Randori Recon DSM specifications

Specification	Value
Manufacturer	IBM Security
DSM name	IBM Security Randori Recon
RPM file name	DSM-*IBMSecurityRandoriRecon-QRadar_version-build_number*.noarch.rpm
Protocol	IBM Security Randori REST API
Event format	JSON
Recorded event types	Detections
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No

IBM Security Randori REST API protocol log source parameters for IBM Security Randori Recon

Add an IBM Security Randori Recon log source that uses the IBM Security Randori REST API protocol.

When you use the IBM Security Randori REST API protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect IBM Security Randori REST API events from Randori Recon:

Table 636. IBM Security Randori REST API source parameters for the IBM Security Randori Recon DSM

Parameter	Value
Log Source type	IBM Security Randori Recon
Protocol Configuration	IBM Security Randori REST API

Table 636. IBM Security Randori REST API source parameters for the IBM Security Randori Recon DSM (continued)	
Parameter	**Value**
Log Source Identifier	The **Log Source identifier** can be any valid value and does not need to reference a specific server. It can also be the same value as the Log Source Name. If you have more than one configured IBM Security Randori REST API data source, ensure that you give each one a unique name.
API Key	The **API key** that is used to access the IBM Security Randori REST API. You must have Randori access to obtain the API key value. For more information about obtaining this value, see How to Add an API token (https://www.ibm.com/docs/en/SSD5I5K/intapi_api_AddAPIToken.html).

For a complete list of IBM Security Randori REST API protocol parameters and their values, see IBM Security Randori REST API protocol configuration options.

Related tasks

Adding a log source

IBM Security Randori Recon sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Security Randori Recon sample message when you use the IBM Security Randori REST API protocol

The following sample event message shows the alert that was generated when a customer successfully enrolled with Randori Recon.


```
{"affiliation_state":"None","applicability":4,"attack_note":"","authority":false,"authority_dist
ance":2,"authority_override":false,"authorization_state":"None","banners_uuid":"0e26bfc","cert_u
uid":null,"characteristics_count":0,"confidence":60,"cpe":
{"cpe_version":null,"edition":null,"language":null,"other":null,"part":null,"product":null,"str"
:"","sw_edition":null,"target_hw":null,"target_sw":null,"update":null,"vendor":null,"version":nu
ll},"criticality":2,"deleted":false,"description":"connection.","detection_criteria":{"ip":
{"address":"10.0.0.1","version":4},"tcp":
{"port":23}},"detection_relevance":1020,"enumerability":1,"exploitability":0,"first_seen":"2022-
07-07T01:03:59.245455+00:00","headers_uuid":null,"hostname":null,"hostname_id":null,"id":"fde879
07","impact_score":"None","ip":"10.0.0.1","ip_id":"fa7e4","ip_str":"10.0.0.1","last_seen":"2022-
08-14T03:39:44.607092+00:00","lens_id":"08638","lens_view":"public","name":"Telnet","org_id":"e0
8411e","path":null,"perspective":"0000-0000-0000000000000","perspective_name":"PUBLIC","poc_email
":null,"poc_id":null,"port":23,"post_exploit":3,"priority_impact_factor":0.0,"priority_score":20
0.1,"priority_status_factor":0.0,"priority_tags_factor":0.0,"private_weakness":0,"protocol":"tcp
","public_weakness":0,"randori_notes":"","reference":"","research":2,"screenshot_uuid":"48f8832c
","service_id":"0e19f","status":"None","tags":{"Amazon":
{"content":"Amazon","display":true,"entity_id":"4bf907","org_id":"923af11e","time_added":"2022-0
7-08T15:00:34.855899+00:00"}},"target_confidence":60,"target_first_seen":"2022-07-07T01:21:23.27
7675+00:00","target_id":"4b907","target_last_seen":"2022-08-14T03:50:44.731212+00:00","target_nu
m_detections":1,"target_temptation":10,"tech_category":null,"temptation_last_modified":"2022-07-
07T01:03:59.245455+00:00","thumbnail_uuid":"45d86","vendor":"Generic","version":""}
```

Table 637. Highlighted fields in the Randori Recon event	
QRadar field name	**Highlighted payload field name**
Event ID	Randori Target - Low Priority
Source IP	ip
Port	port

IBM Security Trusteer

The IBM QRadar DSM for IBM Security Trusteer® collects HTTP Receiver events from an IBM Security Trusteer device.

To integrate IBM Security Trusteer with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - IBM Security Trusteer DSM RPM
   - HTTP Receiver Protocol RPM
2. Contact your IBM Security Trusteer deployment manager to configure IBM Security Trusteer to forward events to QRadar.
3. If QRadar does not automatically detect the log source, add an IBM Security Trusteer log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

IBM Security Trusteer DSM specifications

When you configure the IBM Security Trusteer DSM, understanding the specifications for the IBM Security Trusteer DSM can help ensure a successful integration. For example, knowing what the supported version of IBM Security Trusteer is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the IBM Security Trusteer DSM.

Table 638. IBM Security Trusteer DSM specifications	
Specification	**Value**
Manufacturer	IBM
DSM name	IBM Security Trusteer
RPM file name	`DSM-IBMSecurityTrusteer-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported version	N/A
Protocol	HTTP Receiver
Event format	JSON
Recorded event types	Trusteer alerts
Automatically discovered?	Yes
Includes identity?	No

Table 638. IBM Security Trusteer DSM specifications (continued)	
Specification	**Value**
Includes custom properties?	No
More information	IBM Trusteer Pinpoint Verify (https://www.ibm.com/products/trusteer-pinpoint-verify)

HTTP Receiver log source parameters for IBM Security Trusteer

If QRadar does not automatically detect the log source, add a IBM Security Trusteer log source on the QRadar Console by using the HTTP Receiver protocol.

When using the HTTP Receiver protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect HTTP Receiver events from IBM Security Trusteer:

Table 639. HTTP Receiver log source parameters for the IBM Security Trusteer DSM	
Parameter	**Value**
Log Source type	IBM Security Trusteer
Protocol Configuration	HTTP Receiver
Log Source Identifier	The IP address, hostname, or any name to identify the device. The name must be unique for the log source type.
Listen Port	The port that is used by QRadar to accept incoming HTTP Receiver events. The port must match the port that is configured on your IBM Security Trusteer device. The default port is 12469. **Important:** Do not use port 514. Port 514 is used by the standard Syslog listener.

For a complete list of HTTP Receiver protocol parameters and their values, see HTTP Receiver protocol configuration options.

Related tasks

Adding a log source

IBM Security Trusteer sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

IBM Security Trusteer sample messages when you use the HTTP Receiver protocol

Sample 1:

The following sample event message shows that the same device made multiple suspicious access attempts. It also shows that the event was generated from the user IP address 10.10.0.2.

```
{"feed_name":"account_takeover","version":"9","datetime":"2020-06-10
07:32:29","event_id":"e783d0dc7ae","last_user_ip":"10.0.0.2","last_user_ipv6":null,"app_name":"t
rusteerqa_business","detected_at":"http://
host.domain2.test","activity":"policy58","translated_recommendation":null,"recommendation_reason
_text":"Suspicious multiple accesses pattern from the same
```

```
device","recommendation_reason_id":58,"risk_score":950,"resolution_id":"qnuwkfqcdajojinseudfxbhf
tlimptpu","policy_manager_recommendation":null,"policy_manager_reason":null,"policy_manager_reas
on_id":null,"policy_manager_risk_score":null,"persistent_device_id":"N/
A","new_device_indication_zero_one":0,"country":null,"region":null,"city":null,"isp":null,"organ
ization":null,"useragent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) HeadlessChrome/72.0.3626.121 Safari/
537.36","referrer":"","x_forwarded_for":"10.0.0.2","screen_resolution":null,"screen_dpi":24,"scr
een_touch":0,"client_time_zone":0,"rapport_machine_id":"","client_language":"en-
US","platform":"Linux x86_64","cpu":"Linux x86_64","os":"Linux","accept_encoding":"gzip,
deflate","mimes":0,"navigator_props":4231119849,"browser_version":"72.0.3626","client_charset":"
UTF-8","browser":"Chrome","accept_charset":"","accept_language":"","network_data":"10.0.0.2","pl
ugins":0,"malware_logical_name":"","infection_severity":"high","malware_signature":null,"formatt
ed_is_targeted":"Maybe","encrypted_user_id":"","encryption_key_id":"trusteerqa.1.20110112-102448
","app_id":"multi_login_tma","customer_session_id":"2s3as2jek91t98mb3mggkrt881","persistent_user
_id":"aaaabbbbcccc0006"}
```

```
{"feed_name":"account_takeover","version":"9","datetime":"2020-06-10
 07:32:29","event_id":"e783d0dc7ae","last_user_ip":"10.0.0.2","last_user_ipv6":null,"app_name"
:"trusteerqa_business","detected_at":"http://
host.domain2.test","activity":"policy58","translated_recommendation"
:null,"recommendation_reason_text":"Suspicious multiple accesses pattern from the same device"
,"recommendation_reason_id":58,"risk_score":950,"resolution_id":"qnuwkfqcdajojinseudfxbhftlimp
tpu","policy_manager_recommendation":null,"policy_manager_reason":null,"policy_manager_reason_id"
:null,"policy_mana
ger_risk_score":null,"persistent_device_id":"N/
A","new_device_indication_zero_one":0,"country":null,"region":null,
"city":null,"isp":null,"organization":null,"useragent":"Mozilla/5.0 (X11;
Linux x86_64) AppleWebKit/537.36 (KHTML
, like Gecko) HeadlessChrome/
72.0.3626.121 Safari/537.36","referrer":"","x_forwarded_for":"10.0.0.2","screen_reso
lution":null,"screen_dpi":24,"screen_touch":0,"client_time_zone":0,"rapport_machine_id":"",
"client_language":"en-
US","platform":"Linux x86_64","cpu":"Linux x86_64","os":"Linux","accept_encoding":"gzip,
deflate","mimes":0,"navi
gator_props":4231119849,"browser_version":"72.0.3626","client_charset":"UTF-8","browser":"Chrome"
,"accept_charset
":"","accept_language":"","network_data":"10.0.0.2","plugins":0,"malware_logical_name":"",
"infection_severity":"high","malware_signature":null,"formatted_is_targeted":"Maybe","encr
ypted_user_id":"","encryption_key_id":"trusteerqa.1.20110112-102448","app_id":"multi_login_tma",
"customer_session_id":"2s3as2jek91t98mb3mggkrt881","persistent_user_id":"aaaabbbbcccc0006"}
```


Table 640. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**recommendation_reason_id**
Event Name	**recommendation_reason_text**
Source IP	**last_user_ip**
Device Time	**datetime**

Sample 2 (with IPv6):

The following sample event message shows that unusual activity from a suspicious device that uses the Tor browser was detected. It also shows that the event was generated from the user IP address 10.10.0.2.


```
{"feed_name":"account_takeover","version":"9","datetime":"2018-08-07
12:11:31","event_id":"ecdc7245542","last_user_ip":null,"last_user_ipv6":"2001:DB8:AAAA:BBBB:CCCC
:DDDD:EEEE:FFFF","app_name":"tma2","detected_at":"https://
host.domain.test","activity":"login","translated_recommendation":"Alert","recommendation_reason_
text":"Unusual activity from a suspicious device using the Tor
browser","recommendation_reason_id":71,"risk_score":114,"resolution_id":"zguiblxuursugnjtulwawxh
cmwixsfbs","policy_manager_recommendation":null,"policy_manager_reason":null,"policy_manager_rea
son_id":null,"policy_manager_risk_score":null,"persistent_device_id":"N/
A","new_device_indication_zero_one":0,"country":"US","region":"99","city":null,"isp":"This is
some ISP text","organization":"Test Organization","useragent":"Mozilla/5.0 (Windows NT 6.1;
Trident/7.0; rv:11.0) like Gecko","referrer":"/test/test/
TAF","x_forwarded_for":"10.10.0.2","screen_resolution":null,"screen_dpi":8,"screen_touch":5,"cli
ent_time_zone":0,"rapport_machine_id":"-","client_language":"tr-TR","platform":"Linux
x86_64","cpu":"Linux x86_64","os":"Windows 7","accept_encoding":"gzip, deflate,
br","mimes":0,"navigator_props":4168486725,"browser_version":"11.0","client_charset":"UTF-8","br
owser":"IE","accept_charset":"","accept_language":"tr-TR,tr;q=0.8,en-
US;q=0.5,en;q=0.3","network_data":"10.10.0.2","plugins":3,"malware_logical_name":"","infection_s
everity":"high","malware_signature":null,"formatted_is_targeted":"Maybe","encrypted_user_id":"14
```

D007Bc5cABF5dB23a24CB6CEF7a903f677a43Fbf27EaC34d0bE3242477337f8CF38A65c357b34480AFaBaaC8aBc60d6F
8c3B05fdcbB1eDBaaF5fCd5eb8b704Eeac1F05a0a9067cEb9bc0AedA7aa9aF0016D1cA6C2AD3cEF6D22fb6B9E976ffbC
cD60652Ca4Fc2EA0A8559AD4bc0c4FfE7c3537Bc3fdacaC9a322c4fC96d5cb05320E7FBAeac5E2a89aD5DAbcBF4575e2
05bc5a0DF35e06c2026C3df1D8728bAf1aD3120DC0","encryption_key_id":"","app_id":"tma2","customer_ses
sion_id":"ADf9FbFe9C01FDc5251FdFeEDCe16Cfa","persistent_user_id":"aaaabbbbcccc0002"}

{"feed_name":"account_takeover","version":"9","**datetime**":"2018-08-07 12:11:31","event_id"
:"ecdc7245542","**last_user_ip**":null,"**last_user_ipv6**":"2001:DB8:AAAA:BBBB:CCCC:DDDD:EEEE:FFFF",
"app_name":"tma2","detected_at":"https://
host.domain.test","activity":"login","translated_recommendation":"Alert",
"**recommendation_reason_text**":"Unusual activity from a suspicious device using the Tor browser",
"**recommendation_reason_id**":71,"risk_score":114,"resolution_id":"zguiblxuursugnjtulwawxhcmwixsfbs",
"policy_manager_recommendation":null,"policy_manager_reason":null,
"policy_manager_reason_id":null,"policy_manager_risk
_score":null,"persistent_device_id":"N/
A","new_device_indication_zero_one":0,"country":"US","region":"99","city":null,
"isp":"This is some ISP
text","organization":"Test Organization","useragent":"Mozilla/5.0 (Windows NT 6.1; Trident/7.0
; rv:11.0) like Gecko","referrer":"/
test/test/TAF","x_forwarded_for":"10.10.0.2","screen_resolution":null,"screen_dpi"
:8,"screen_touch":5,"client_time_zone":0,"rapport_machine_id":"-","client_language":"tr-
TR","platform":"Linux x86_64"
,"cpu":"Linux x86_64","os":"Windows 7","accept_encoding":"gzip, deflate, br","mimes":0,
"navigator_props":4168486725,"browser_version":"11.0","client_charset":"UTF-8","browser":
"IE","accept_charset":"","accept_language"
:"tr-TR,tr;q=0.8,en-
US;q=0.5,en;q=0.3","network_data":"10.10.0.2","plugins":3,"malware_logical_name":"","infection
_severity":"high"
,"malware_signature":null,"formatted_is_targeted":"Maybe","encrypted_user_id":"14D007Bc5cABF5d
B23a24CB6CEF7a903f677a43Fbf27EaC34d0b
E3242477337f8CF38A65c357b34480AFaBaaC8aBc60d6F8c3B05fdcbB1eDBaaF5fCd5eb8b704Eeac1F05a0a9067cEb
9bc0AedA7aa9aF0016D1cA6C2AD3cEF6D22fb
6B9E976ffbCcD60652Ca4Fc2EA0A8559AD4bc0c4FfE7c3537Bc3fdacaC9a322c4fC96d5cb05320E7FBAeac5E2a89aD
5DAbcBF4575e205bc5a0DF35e06c2026C3df1
D8728bAf1aD3120DC0","encryption_key_id":"","app_id":"tma2","customer_session_id":"ADf9FbFe9C0
1FDc5251FdFeEDCe16Cfa","persistent_use
r_id":"aaaabbbbcccc0002"}

Table 641. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**recommendation_reason_id**
Event Name	**recommendation_reason_text**
Source IP	**last_user_ip**
Device Time	**datetime**

IBM Security Trusteer Apex Advanced Malware Protection

The IBM Security Trusteer Apex™ Advanced Malware Protection DSM collects and forwards event data from a Trusteer Apex Advanced Malware Protection system to IBM QRadar.

QRadar collects the following items from the Trusteer Apex Advanced Malware Protection system:

- Syslog events
- Log files (from an intermediary server that hosts flat feed files from the system.)
- Syslog events through SSL/TLS authentication

The following table lists the specifications for the IBM Security Trusteer Apex Advanced Malware Protection DSM:

Table 642. IBM Security Trusteer Apex Advanced Malware Protection DSM specifications

Specification	Value
Manufacturer	IBM
DSM name	IBM Security Trusteer Apex Advanced Malware Protection

Table 642. IBM Security Trusteer Apex Advanced Malware Protection DSM specifications (continued)	
Specification	**Value**
RPM file name	`DSM-TrusteerApex-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	Syslog/LEEF event collection: Apex Local Manager 2.0.45 LEEF: `ver_1303.1` Flat File Feed: v1, v3, and v4
Protocol	Syslog Log File TLS Syslog
Recorded event types	Malware Detection Exploit Detection Data Exfiltration Detection Lockdown for Java Event File Inspection Event Apex Stopped Event Apex Uninstalled Event Policy Changed Event ASLR Violation Event ASLR Enforcement Event Password Protection Event
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	IBM Security Trusteer Apex Advanced Malware Protection website (http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware)

To configure IBM Security Trusteer Apex Advanced Malware Protection event collection, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Log File Protocol RPM
   - TLS Syslog Protocol RPM
   - IBM Security Trusteer Apex Advanced Malware Protection DSM RPM
2. Choose one of the following options:
   - To send syslog events to QRadar, see "Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar" on page 1018.

- To send syslog events by using TLS Syslog Protocol to QRadar, see "Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar" on page 1019
- To collect log files from IBM Security Trusteer Apex Advanced Malware Protection through an intermediary server, see "Configuring a Flat File Feed service" on page 1021.

3. If QRadar doesn't automatically discover the log source, add an IBM Security Trusteer Apex Advanced Malware Protection log source on the QRadar Console.

   The following table describes the parameters that require specific values for IBM Security Trusteer Apex Advanced Malware Protection syslog event collection:

Table 643. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Syslog protocol

Parameter	Value
Log Source type	IBM Security Trusteer Apex Advanced Malware Protection
Protocol Configuration	**Syslog**
Log Source Identifier	The IP address or host name from the syslog header. If the syslog header does not contain an IP address or a host name, use the packet IP address.

The following table describes the parameters that require specific values for IBM Security Trusteer Apex Advanced Malware Protection TLS Syslog event collection:

Table 644. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for TLS Syslog protocol

Parameter	Value
Log Source Type	IBM Security Trusteer Apex Advanced Malware Protection
Protocol Configuration	**TLS Syslog**
Log Source Identifier	The IP address or host name from the syslog header. If the syslog header doesn't contain an IP address or a host name, use the packet IP address.
TLS Listen Port	The default port is 6514.
Authentication Mode	TLS
Certificate Type	Select the **Provide Certificate** option from the list.
Maximum Connections	The Maximum Connections parameter controls how many simultaneous connections the TLS Syslog protocol can accept for each Event Collector. For each Event Collector, there is a limit of 1000 connections across all TLS syslog log source configurations. The default for each device connection is 50. **Note:** Automatically discovered log sources that share a listener with another log source count only one time towards the limit. For example, the same port on the same event collector.

Table 644. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for TLS Syslog protocol (continued)	
Parameter	**Value**
TLS Protocols	Select the version of TLS installed on the client from the drop down list.
Provided Server Certificate Path	Absolute path of server certificate. For example, `/opt/qradar/conf/trusted_certificates/apex-alm-tls.cert`
Provided Private Key Path	Absolute path of PKCS#8 private key. For example, `/etc/pki/tls/private/apex-alm-tls.pk8`

Important: When you use the TLS syslog, and you want to use an FQDN to access the system, you must generate your own certificate for the listener, and then specify it in the TLS syslog configuration.

The following table describes the parameters that require specific values for IBM Security Trusteer Apex Advanced Malware Protection log file collection:

Table 645. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol	
Parameter	**Value**
Log Source Type	IBM Security Trusteer Apex Advanced Malware Protection
Protocol Configuration	**Log File**
Log Source Identifier	The IP address or host name of the server that hosts the Flat File Feed.
Service Type	**SFTP**
Remote IP or Hostname	The IP address or host name of the server that hosts the Flat File Feed.
Remote Port	22
Remote User	The user name that you created for QRadar on the server that hosts the Flat File Feed.
SSH Key File	If you use a password, leave this field blank.
Remote Directory	The log file directory where the Flat File Feed is stored.
Recursive	To avoid pulling the same file repeatedly to QRadar, do not select this option.
FTP File Pattern	`"trusteer_feeds_.*?_[0-9]{8}_[0-9]*?\.csv"`
Start Time	The time that you want your log file protocol to start collecting log files.
Recurrence	The polling interval for log file retrieval.
Run On Save	Must be enabled.
Processor	**None**

Table 645. IBM Security Trusteer Apex Advanced Malware Protection log source parameters for Log File Protocol (continued)	
Parameter	**Value**
Ignore Previously Processed Files	Must be enabled.
Event Generator	**LINEBYLINE**
File Encoding	**UTF-8**

Related concepts

Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar

You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events through secure socket layer (SSL) or transport layer security (TLS) to IBM QRadar.

Related tasks

Adding a DSM

Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar

You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to IBM QRadar.

Configuring a Flat File Feed service

Adding a log source

Configuring IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to QRadar

You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events to IBM QRadar.

Before you begin

Install an Apex Local Manager on your Trusteer Management Application™ (TMA).

For more information about configuring your IBM Security Trusteer Apex Advanced Malware Protection to communicate with QRadar, see:

- *IBM Security Trusteer Apex Advanced Malware Protection Local Manager - Hybrid Solution Reference Guide*
- *IBM Security Trusteer Apex Advanced Malware Protection Feeds Reference Guide*

Note: SSL/TLS authentication is not supported.

Procedure

1. Log in to Trusteer Management Application (TMA).
2. Select **Apex Local Manager & SIEM Settings**.
3. Optional: If the Apex Local Manager wizard doesn't automatically display, click **Add**.
4. Type the name of the Apex Local Manager.
5. Select the **Enable** check box and click **Next**.
6. Type the server settings for QRadar and click **Next**.
7. Optional: If you use a separate syslog server for the Apex Local Manager system events, type the settings.
8. Click **Finish**.

Configuring IBM Security Trusteer Apex Advanced Malware Protection to send TLS Syslog events to QRadar

You can configure IBM Security Trusteer Apex Advanced Malware Protection to send syslog events through secure socket layer (SSL) or transport layer security (TLS) to IBM QRadar.

Complete the following steps to establish a secure channel for transmitting logs between Apex Trusteer and QRadar:

1. Create TLS/SSL Server Certificates and private key.
2. Create Client Authentication certificates in a PKCS#12 container for Apex Local Manager.
3. Configure the QRadar log source for IBM Security Trusteer Apex Advanced Malware Protection.
4. Configure the Apex Local Manager(ALM).

Creating a TLS/SSL server certificate and private key

To establish a communication between QRadar and Apex Local Manager (ALM) by using TLS encryption, you must create a self-signed certificate with public and private key pairs.

Procedure

1. Log in to QRadar as a root user by using SSH.
2. Create a self-signed certificate. For example:

```
openssl req -new -x509 -newkey rsa:2048 -days 3650 -sha512 -nodes -x509 -subj "/C=US/
ST=<State>/L=<City>/O=IBM/OU=IBM Security/CN=qradar FQDN or ip address" -keyout apex-alm-
tls.key -out apex-alm-tls.cert
```

3. Convert the private key to the required DER encode PKCS#8 format:

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in apex-alm-tls.key -out apex-alm-tls.pk8
-nocrypt
```

Note:

- Use a unique filename if a certificate needs to be changed or updated.
- Put the certificate file in `/opt/qradar/conf/trusted_certificates`.
- Do not place the PKCS#8 formatted key file in `/opt/qradar/conf/trusted_certificates`.

Warning: Make sure that you complete this step so that the connection works between ALM and QRadar.

Creating Client Authentication certificates and keys for Apex Local Manager

Configuring an ALM for TLS Syslog authentication requires a PKCS#12 file that contains the certificate and private key.

Procedure

1. Create a self-signed certificate and private key. For example,

```
openssl req -new -x509 -newkey rsa:2048 -days 3650 -sha512 -nodes -x509 -subj "/C=US/
ST=<State>/L=<City>/O=IBM/OU=IBM Security/CN=ALM FQDN or IP Address" -keyout alm-client-
syslog-tls.key -out  alm-client-syslog-tls.cert
```

2. Create the PKCS#12 container:

```
openssl pkcs12 -export -inkey alm-client-syslog-tls.key -in alm-client-syslog-tls.cert -out
alm-client-syslog-tls.p12 -name "alm-client-syslog-tls"
```

Attention: Make note of the password that you entered. The password is required when you configure the Apex Local Manager.

Configuring the Apex Local Manager

Configure the Apex Local Manager through a customer-assigned Apex Trusteer Management Application (TMA) original server.

Procedure

1. Log in to the Apex TMA.
2. From the left navigation menu, click the **Administration** accordion to expand the options available.
3. Click the **Apex Local Manager & SIEM Settings**.
4. Click **Add** and complete the following steps:
   a) Select the option to enable this Apex Local Manager.
   b) Enter a unique name.
5. Click **Next**.
6. From the **SIEM/Syslog Server Settings** page, provide a value for the following parameters:

Table 646. Apex Local Manager SIEM/Syslog server setting parameters

Parameter	Description
Type	IBM Security Q-Radar SIEM (LEEF)
Hostname	*<fqdn of the Qradar appliance>*
Port	Default is 6514.
Protocol	**TCP with SSL/TLS**
PKCS#12 Upload File	Upload the local PKCS#12 file
Encryption Password	The password that was entered during the creation of the client authentication certificates for Apex Local Manager.
CA Certificate Upload File	Upload local certifcate file. For example, `apex-alm-tls.cert`

7. Click **Next**.
8. From the **System Events Setting** page, provide a value for the following parameters:

Table 647. System events setting parameters

Parameter	Description
Hostname	*<QRadar FQDN or IP Address>*
Port	Default is 6514
Protocol	**Syslog with SSL/TLS**
PKCS#12 Upload File	Upload the local PKCS#12 file. For example, `alm-client-syslog.tls.p12`
Encryption Password	The password that was entered during the creation of the client authentication certificates for Apex Local Manager.
CA Certificate Upload File	Upload local certifcate file. For example, `apex-alm-tls.cert`

9. Click **Finish** to save the configuration.
10. Select the new entry.
11. Copy the **Provisioning key.**

What to do next

See "“Configuring the ALM instance” on page 1021"

Configuring the ALM instance

Configure the ALM instance by using the provisioning key copied from the Apex Local Manager.

Procedure

1. Log in to the Apex Local Manager at:

   ```
   https://ipaddress:8443
   ```

2. From the **General Settings** page, paste the provisioning key into the field and click the **Synchronize Settings**.

   Note: A message will be displayed that states that the settings synchronized successfully.
3. Click the **Test Connection** to send test event to QRadar and validate the connection.

Configuring a Flat File Feed service

For IBM QRadar to retrieve log files from IBM Security Trusteer Apex Advanced Malware Protection, you must set up a flat file feed service on an intermediary SFTP-enabled server. The service enables the intermediary server to host the flat files that it receives from IBM Security Trusteer Apex Advanced Malware Protection and allows for connections from external devices so that QRadar can retrieve the log files.

To configure IBM Security Trusteer Apex Advanced Malware Protection to send flat file feed to the intermediary server, contact IBM Trusteer support.

About this task

Flat file feed use a CSV format. Each feed item is written to the file on a separate line, which contains several comma-separated fields. Each field contains data that describes the feed item. The first field in each feed line contains the feed type.

Procedure

1. Enable an SFTP-enabled server and ensure that external devices can reach it.
2. Log in to the SFTP-enabled server.
3. Create a user account on the server for IBM Security Trusteer Apex Advanced Malware Protection.
4. Create a user account for QRadar.
5. Optional: Enable SSH key-based authentication.

What to do next

After you set up the intermediary server, record the following details:

- Target SFTP server name and IP addresses
- SFTP server port (standard port is 22)
- The file path for the target directory
- SFTP user name if SSH authentication is not configured

- Upload frequency (from 1 minute to 24 hours)
- SSH public key in RSA format

IBM Trusteer support uses the intermediary server details when they configure IBM Security Trusteer Apex Advanced Malware Protection to send flat file feed.

IBM Security Trusteer Apex Local Event Aggregator

IBM QRadar can collect and categorize malware, exploit, and data exfiltration detection events from Trusteer Apex Local Event Aggregator.

To collect syslog events, you must configure your Trusteer Apex Local Event Aggregator to forward syslog events to QRadar. Administrators can use the Apex L.E.A. management console interface to configure a syslog target for events. QRadar automatically discovers and creates log sources for syslog events that are forwarded from Trusteer Apex Local Event Aggregator appliances. QRadar supports syslog events from Trusteer Apex Local Event Aggregator V1304.x and later.

To integrate events with QRadar, administrators can complete the following tasks:

1. On your Trusteer Apex Local Event Aggregator appliance, configure syslog server.
2. On your QRadar system, verify that the forwarded events are automatically discovered.

Configuring syslog for Trusteer Apex Local Event Aggregator

To collect events, you must configure a syslog server on your Trusteer Apex Local Event Aggregator to forward syslog events.

Procedure

1. Log in to the Trusteer Apex L.E.A. management console.
2. From the navigation menu, select **Configuration**.
3. To export the current Trusteer Apex Local Event Aggregator configuration, click **Export** and save the file.
4. Open the configuration file with a text editor.
5. From the `syslog.event_targets` section, add the following information:

   ```
   {
   host": "<QRadar IP address>", "port": "514", "proto": "tcp"
   }
   ```
6. Save the configuration file.
7. From the navigation menu, select **Configuration**.
8. Click **Choose file** and select the new configuration file that contains the event target IP address.
9. Click **Import**.

   As syslog events are generated by the Trusteer Apex Local Event Aggregator, they are forwarded to the target specified in the configuration file. The log source is automatically discovered after enough events are forwarded to QRadar. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created. The **Log Activity** tab displays events from Trusteer Apex Local Event Aggregator.

IBM Security Verify (formerly known as IBM Cloud Identity)

IBM Security Verify is formerly known as IBM Cloud Identity. The DSM RPM name remains as IBM Cloud Identity.

The IBM QRadar DSM for IBM Security Verify collects JSON events from an IBM Security Verify service.

To integrate IBM Security Verify with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common RPM
   - IBM Security Verify Event Service protocol RPM
   - IBM Cloud Identity DSM RPM
2. Configure your IBM Security Verify server to send events to QRadar. For more information, see "Configuring QRadar to pull events from IBM Security Verify" on page 1024.
3. Add an IBM Security Verify log source on the QRadar Console. For more information about IBM Security Verify log source parameters, see "IBM Security Verify Event Service log source parameters for IBM Security Verify" on page 1025.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

IBM Security Verify DSM Specifications

When you configure IBM Security Verify, understanding the specifications for the IBM Security Verify DSM can help ensure a successful integration. For example, knowing what the supported version of IBM Security Verify is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the IBM Security Verify DSM.

Table 648. IBM Security Verify DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBM Security Verify
RPM file name	DSM-*IBMCloudIdentity-QRadar_version-build_number*.noarch.rpm
Supported version	1.0
Protocol	IBM Security Verify Event Service
Event format	JSON

Table 648. IBM Security Verify DSM specifications (continued)	
Specification	**Value**
Recorded event types	• Account sync • Adaptive risk • Authentication • Certification campaign • Drop off • Fulfillment • Management • MFA authentication • Privacy consent • Register • Risk • SSO • SLO • Threat • Token
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	IBM Security Verify documentation

Configuring QRadar to pull events from IBM Security Verify

To send JSON events to QRadar by using the REST API, you must create an API Client for the QRadar system that connects to the IBM Security Verify service.

Procedure

1. Ensure that you can access your IBM Security Verify tenant's administrative portal.
2. Complete the steps to generate credentials for use with the REST API in IBM Security Verify. For more information about the Getting Credentials procedure, see Getting Started (https://www.ibm.com/blogs/security-identity-access/getting-started-with-ibm-cloud-identity-rest-apis/).

   Important: Record the **Client ID** and **Client Secret** values from the Getting Credentials procedure in Step 2. You need these values when you add a log source in QRadar.
3. Ensure that the API Client you use for the IBM Security Verify Event Service protocol has **Read reports** or **Manage reports** access permission.

What to do next

"Adding a log source" on page 5

IBM Security Verify Event Service log source parameters for IBM Security Verify

If IBM QRadar does not automatically detect the log source, add an IBM Security Verify log source on the QRadar Console by using the IBM Security Verify Event Service protocol.

When using the IBM Security Verify Event Service protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect IBM Security Verify Event Service events from IBM Security Verify:

Table 649. IBM Security Event Service log source parameters for the IBM Security Verify DSM

Parameter	Value
Log Source type	IBM Security Verify
Protocol Configuration	IBM Security Verify Event Service
Log Source Identifier	https://<*your tenant*>.ice.ibmcloud.com/v1.0/applications

For a complete list of IBM Security Verify Event Service protocol parameters and their values, see IBM Security Verify Event Service protocol configuration options.

Related tasks

Adding a log source

IBM Security Verify sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Security Verify sample messages when you use the IBM Security Verify Event Service protocol

The following table describes the sample event messages for the IBM Security Verify Event Service protocol.

Table 650. Sample event messages for the IBM Security Verify DSM Event Service protocol

Event name	Low-level category	Sample log message
Created IP Client Success	**Create activity succeeded**	{ "geoip": { "continent_name": "North America", "as_org": "AMAZON-02", "city_name": "Saint John", "country_iso_code": "CAN", "ip": "10.11.111.111", "country_name": "Canada", "region_name": "New Brunswick", "location": { "lon": "-65.860879", "lat": "44.972686" }, "asn": 11111 }, "data": { "result": "success", "api_grant_type": "authorization_code", "clientid": "aaaa1111-5cc7-45d9-b8ad- bbbb2222", "performedby": "123400SAAA", "performedby_type": "user", "resource": "api_client", "origin": "10.0.4.1", "performedby_username": "username@ca.example.com", "action": "created", "devicetype": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:121.0) Gecko/20100101 Firefox/121.0", "performedby_realm": "www.example.com", "target": "Sample app" }, "year": 2024, "event_type": "management", "month": 1, "indexed_at": 1705605751362, "tenantid": "88465b1f- e4c2-4e7e- b03e-421c03301806", "tenantname": "username.verify.example.com ", "correlationid": "CORR_ID- AK22a0103e-9ef9-4273-8947- aab0a5d85271", "servicename": "apisecurity", "id": "ssss3333-aa44- ff44-83e3-aaaaaa222222", "time": 1705605751055, "day": 18 }

Table 650. Sample event messages for the IBM Security Verify DSM Event Service protocol (continued)

Event name	Low-level category	Sample log message
SSO Login Success	**User login success**	{ "geoip": { "continent_name": "North America", "as_org": "AMAZON-02", "city_name": "Saint John", "country_iso_code": "Canada", "country_iso_code": "CAN", "ip": "10.11.111.111", "country_name": "Canada", "region_name": "New Brunswick", "location": { "lon": "-65.860879", "lat": "44.972686" }, "asn": 11111 }, "data": { "result": "success", "subtype": "saml", "providerid": "example.com", "origin": "2001:db8:ffff:ffff:ffff:fff f:ffff:ffff", "realm": "cloudIdentityRealm", "samlassertion": "1111111111111111", "applicationid": "2222222222222222222", "userid": "333B3B33BB", "applicationtype": "Box", "devicetype": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0", "username": "username", "applicationname": "SMGAdaptiveAccessBox" }, "year": 2023, "event_type": "sso", "month": 7, "indexed_at": 1689692204024, "tenantid": "3cc33c3-3c33-3c33- c3c3-33c33ccc3c3", "tenantname": "name.ite1.idng.example.com" , "correlationid": "CORR_ID- DD44d44d44-444d-44d4- d444-444dd4444fd4", "servicename": "saml_runtime", "id": "5e55e5e5- e555-555-555-5e55e5e5e55e", "time": 1689692192869, "day": 18 }

Table 650. Sample event messages for the IBM Security Verify DSM Event Service protocol (continued)

Event name	Low-level category	Sample log message
MFA Login Success	**User login success**	{ "geoip": { "continent_name": "North America", "as_org": "AMAZON-02", "city_name": "Saint John", "country_iso_code": "Canada", "country_iso_code": "CAN", "ip": "10.11.111.111", "country_name": "Canada", "region_name": "New Brunswick", "location": { "lon": "-65.860879", "lat": "44.972686" }, "asn": 11111 }, "data": { "result": "success", "mfamethod": "Voice OTP", "subtype": "mfa", "subject": "503R3T76MX", "origin": "2001:DB8:FFFF:FFFF:FFFF:FFF F:FFFF:FFFF", "realm": "cloudIdentityRealm", "sourcetype": "clouddirectory", "mfadevice": "22222222222", "devicetype": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0", "username": "bbbbbbb", "target": "https:// tenantname.ite1.idng.example .com/saml/sps/auth? stateid=a1a1a1a1-a1a1-a1a1- a1a1-a1a1a1a1a1" }, "year": 2023, "event_type": "authentication", "month": 7, "indexed_at": 1689692204022, "tenantid": "3ccc333c3-3c33-3c33- c3c3-333c33ccc3c3", "tenantname": "tenantname.ite1.idng.exampl e.com", "correlationid": "CORR_ID- DD4d24ddd44-ddd4-4444-444- d444ddd4dd4", "servicename": "authsvc", "id": "e5555555-555e-55ee-5555-5ee 5e5e555e5", "time": 1689692191331, "day": 18 }

IBM Sense

The IBM QRadar DSM for IBM Sense collects notable events from a local or external system that generates Sense events.

The following table describes the specifications for the IBM Sense DSM:

Table 651. IBM Sense DSM specifications

Specification	**Value**
Manufacturer	IBM
DSM name	IBM Sense
RPM file name	DSM-IBMSense-*Qradar_version-build_number*.noarch.rpm
Supported versions	1
Protocol	Syslog
Event format	LEEF
Recorded event types	User Behavior User Geography User Time User Access User Privilege User Risk Sense Offense Resource Risk
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	IBM website (http://www.ibm.com)

To integrate IBM Sense with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - IBM Sense DSM RPM
   - DSMCommon RPM

The following table shows a sample event message for IBM Sense:

Table 652. IBM Sense sample message.		
Event name	**Low level category**	**Sample log message**
Behavior Change	User Behavior	`LEEF:2.0|IBM|Sense|1.0|Behavior Change|cat=User Behavior description= score= scoreType= confidence= primaryEntity= primaryEntityType= additionalEntity= additionalEntityType= beginningTimestamp= endTimestamp= sensorDomain= referenceId1= referenceId2= referenceId3= referenceId4= referenceURL= originalSenseEventName=`

Related tasks

"Adding a DSM" on page 4

Configuring IBM Sense to communicate with QRadar

The User Behavior Analytics (UBA) app uses the IBM Sense DSM to add user risk scores and offenses into QRadar. When the app is installed, an IBM Sense log source is automatically created and configured by the app. No user input or configuration is required.

IBM SmartCloud Orchestrator

The IBM QRadar DSM for IBM SmartCloud® Orchestrator collects audit logs from the SmartCloud Orchestrator system.

The following table identifies specifications for the IBM SmartCloud Orchestrator DSM.

Table 653. IBM SmartCloud Orchestrator specifications	
Specification	**Value**
Manufacturer	IBM
DSM name	SmartCloud Orchestrator
RPM file name	`DSM-IBMSmartCloudOrchestrator-`*`Qradar_version_build number`*`.noarch.rpm`
Supported versions	V2.3 FP1 and later
Protocol type	IBM SmartCloud Orchestrator REST API
QRadar recorded event types	Audit Records
Log source type in the QRadar UI	IBM SmartCloud Orchestrator
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties	No
More information	http://ibm.com

To integrate IBM SmartCloud Orchestrator with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMS from the IBM Support Website onto your QRadar Console:
   - IBM SmartCloud Orchestrator RPM
   - IBM SmartCloud Orchestrator RESTAPI protocol RPM
2. Create an IBM SmartCloud Orchestrator log source on the QRadar Console. Use the following values for the SmartCloud-specific parameters:

Parameter	Description
Log Source Type	IBM SmartCloud Orchestrator.
Protocol Configuration	IBM SmartCloud Orchestrator REST API
IP or Hostname	The IP address or server name of the SmartCloud Orchestrator.

No action is required on the IBM SmartCloud Orchestrator system. After you create the log source, QRadar starts collecting logs from IBM SmartCloud Orchestrator.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Installing IBM SmartCloud Orchestrator

Integrate SmartCloud Orchestrator with IBM QRadar

Procedure

1. Download and install the latest DSMCommon RPM from the IBM Support Website onto your QRadar Console. If automatic updates are configured to install DSM updates, this step is not necessary.
2. Download and install the latest IBM SmartCloud Orchestrator RESTAPI Protocol RPM from the IBM Support Website onto to your QRadar Console.
3. Download and install the latest IBM SmartCloud Orchestrator RPM from the IBM Support Website onto your QRadar Console. If automatic updates are configured to install DSM updates, this step is not necessary.

IBM SmartCloud Orchestrator log source parameters

If QRadar does not automatically detect the log source, add a IBM SmartCloud Orchestrator log source on the QRadar Console by using the IBM SmartCloud Orchestrator REST API protocol.

When using the IBM SmartCloud Orchestrator REST API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect IBM SmartCloud Orchestrator events:

Table 654. IBM SmartCloud Orchestrator log source parameters

Parameter	Value
Log Source type	**IBM SmartCloud Orchestrator**
Protocol Configuration	IBM SmartCloud **Orchestrator REST API**
IP or Hostname	The IP address or server name of the SmartCloud Orchestrator.
Username	The user name of the SmartCloud Orchestrator console user.

Table 654. IBM SmartCloud Orchestrator log source parameters (continued)	
Parameter	**Value**
Password	The password of the SmartCloud Orchestrator console user.
Confirm Password	This option confirms that the password was entered correctly.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 5000.
Recurrence	How often this log source attempts to obtain data. Can be in Minutes, Hours, Days (default 5 minutes).

Related tasks

"Adding a log source" on page 5

IBM Tivoli Access Manager for e-business

The IBM Tivoli® Access Manager for e-business DSM for IBM QRadar accepts access, audit, and HTTP events forwarded from IBM Tivoli Access Manager.

QRadar collects audit, access, and HTTP events from IBM Tivoli Access Manager for e-business by using syslog. Before you can configure QRadar, you must configure Tivoli Access Manager for e-business to forward events to a syslog destination.

Tivoli Access Manager for e-business supports WebSEAL, a server that applies fine-grained security policy to the Tivoli Access Manager protected Web object space. For more information about WebSEAL, see IBM Tivoli Access Manager WebSEAL overview (http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1359-00/en_US/HTML/am51_webseal_guide10.htm#j1031993).

Configuring Tivoli Access Manager for e-business

You can configure syslog on your Tivoli Access Manager for e-business to forward events.

Procedure

1. Log in to Tivoli Access Manager's IBM Security Web Gateway.
2. From the navigation menu, select **Secure Reverse Proxy Settings** > **Manage** > **Reverse Proxy**.

   The **Reverse Proxy** pane is displayed.
3. From the **Instance column**, select an instance.
4. Click the **Manage** list and select **Configuration** > **Advanced**.

   The text of the WebSEAL configuration file is displayed.
5. Locate the Authorization API Logging configuration.

   The remote syslog configuration begins with `logcfg`.

   For example, to send authorization events to a remote syslog server:

   `# logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name>`
6. Copy the remote syslog configuration (`logcfg`) to a new line without the comment (`#`) marker.

7. Edit the remote syslog configuration.

   For example,

   ```
   logcfg = audit.azn:rsyslog server=<IP address>,port=514,log_id=<log name>
   logcfg = audit.authn:rsyslog server=<IP address>,port=514,log_id=<log name>
   logcfg = http:rsyslog server=<IP address>,port=514,log_id=<log name>
   ```

   Where:

   - <*IP address*> is the IP address of your QRadar Console or Event Collector.
   - <*Log name*> is the name assigned to the log that is forwarded to QRadar. For example, `log_id=WebSEAL-log`.

8. Customize the `request.log` file.

   For example,

   ```
   request-log-format = isam-http-request-log|client-ip=%a|server-
   ip=%A|client-logname=%l|remote-user=%u|time=%t|port=%p|protocol=%H|request-
   method=%m|response-status=%s|url=%U|bytes=%b|remote-host=%h|request=%r
   ```

9. Click **Submit**.

   The **Deploy** button is displayed in the navigation menu.

10. From the navigation menu, click **Deploy**.
11. Click **Deploy**.

    You must restart the reverse proxy instance to continue.

12. From the **Instance** column, select your instance configuration.
13. Click the **Manage** list and select **Control** > **Restart**.

    A status message is displayed after the restart completes. For more information on configuring a syslog destination, see your *IBM Tivoli Access Manager for e-business* vendor documentation. You are now ready to configure a log source in QRadar.

Syslog log source parameters for IBM Tivoli Access Manager for e-business

If QRadar does not automatically detect the log source, add an IBM Tivoli Access Manager for e-business log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from IBM Tivoli Access Manager for e-business:

Table 655. Syslog log source parameters for the IBM Tivoli Access Manager for e-business DSM

Parameter	Value
Log Source name	Type a name of your log source.
Log Source description	Type a description for your log source.
Log Source type	IBM Tivoli **Access Manager for e-business**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for your IBM Tivoli Access Manager for e-business appliance. The IP address or host name identifies your IBM Tivoli Access Manager for e-business as a unique event source in QRadar.

Related tasks

"Adding a log source" on page 5

IBM Tivoli Access Manager for e-business sample event message

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM Tivoli Access Manager for e-business sample message when you use the Syslog protocol

The following sample event message shows that an HTTP GET request received a response with a status code of 200, indicating a successful request.

```
<134>Aug 22 08:48:41 ibm.tivoliaccessmanager.test isam-http-request-log|client-
ip=172.16.3.226|server-ip=172.16.3.235|clientlogname=-|remote-user=unauthenticated|time=22/Aug/
2018:08:48:27 -0300|port=443|request-method=GET|response-status=200|
url=/QRadar/images/botones/ibm.png|bytes=6631|remote-host=172.16.3.226|Session-Index=acc3ef2e-
a5ff-11e8-ad5b-0050568a5f8e|X-Forwarded-For=192.168.0.1|Host-Header=ibm.tivoli.test|Junction=/
qradar|Transaction-Identifier=474|
```

Table 656. Highlighted fields in the IBM Tivoli Access Manager for e-business event

QRadar field name	Highlighted field name
Source IP	**`X-Forwarded-For`** **Important:** If this field is not present, the **`client-ip`** field is used instead.
Destination IP	**`server-ip`**

IBM Tivoli Endpoint Manager

IBM Tivoli® Endpoint Manager is now known as IBM BigFix.

Related concepts

"HCL BigFix (formerly known as IBM BigFix)" on page 879

IBM WebSphere Application Server

The IBM WebSphere® Application Server DSM for IBM QRadar accepts events using the log file protocol source.

QRadar records all relevant application and security events from the WebSphere Application Server log files.

Configuring IBM WebSphere

You can configure IBM WebSphere Application Server events for IBM QRadar.

Procedure

1. Using a web browser, log in to the IBM WebSphere administrative console.
2. Click **Environment** > **WebSphere Variables**.
3. Define Cell as the Scope level for the variable.
4. Click **New**.
5. Configure the following values:

- **Name** - Type a name for the cell variable.
- **Description** - Type a description for the variable (optional).
- **Value** - Type a directory path for the log files.

  For example:

  ```
  {QRADAR_LOG_ROOT} = /opt/IBM/WebSphere/AppServer/profiles/Custom01/logs/
  QRadar
  ```

  You must create the target directory that is specified in “Configuring IBM WebSphere ” on page 1034 before proceeding.

6. Click **OK**.
7. Click **Save**.
8. You must restart the WebSphere Application Server to save the configuration changes.

   Note: If the variable you created affects a cell, you must restart all WebSphere Application Servers in the cell before you continue.

What to do next

You are now ready to customize the logging option for the IBM WebSphere Application Server DSM.

Customizing the Logging Option

You must customize the logging option for each application server WebSphere uses and change the settings for the JVM Logs (Java Virtual Machine logs).

Procedure

1. **Select Servers** > **Application Servers**.
2. Select your WebSphere Application Server to load the server properties.
3. Select **Logging and Tracing** > **JVM Logs**.
4. Configure a name for the JVM log files.

   For example:

   `System.Out` log file name:

   `${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemOut.log`

   `System.Err` log file name:

   `${QRADAR_LOG_ROOT}/${WAS_SERVER_NAME}-SystemErr.log`
5. Select a time of day to save the log files to the target directory.
6. Click **OK**.
7. You must restart the WebSphere Application Server to save the configuration changes.

   Note: If the JVM Logs changes affect the cell, you must restart all of the WebSphere Application Servers in the cell before you continue.

   You are now ready to import the file into IBM QRadar using the log file protocol.

Log File log source parameters for IBM WebSphere

If QRadar does not automatically detect the log source, add a IBM WebSphere log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM WebSphere:

Table 657. Log File log source parameters for the IBM WebSphere DSM	
Parameter	**Value**
Log Source name	Type a name of your log source.
Log Source description	Type a description for your log source.
Log Source type	IBM WebSphere **Application Server**
Protocol Configuration	**Log File**
Log Source Identifier	Type an IP address, host name, or name to identify your IBM WebSphere Application Server as an event source in QRadar. IP addresses or host names are recommended as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple IBM WebSphere Application Serves that provides logs to a file repository, specify the IP address or host name of the device that created the event log. This allows events to be identified at the device level in your network, instead of identifying the file repository.
Service Type	From the list, select the protocol that you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of your IBM WebSphere Application Server storing your event log files.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535. The options include FTP ports: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.
Remote User	Type the user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.

Table 657. Log File log source parameters for the IBM WebSphere DSM (continued)	
Parameter	**Value**
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, this parameter allows for the definition of an SSH private key file. The **Remote Password** field is ignored when you provide an SSH Key File.
Remote Directory	Type the directory location on the remote host to the cell and file path you specified in “Configuring IBM WebSphere ” on page 1034. This is the directory that you created containing your IBM WebSphere Application Server event files. For FTP only. If your log files are located in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders. By default, the check box is clear. The **Recursive** option is ignored if you configure **SCP** as the **Service Type**.
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, this option allows for the configuration of the regular expression (regex) to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. The FTP file pattern that you specify must match the name that you assigned to your JVM logs in “Customizing the Logging Option” on page 1035. For example, to collect system logs, type the following code: `System.*\.log` Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option appears only if you select **FTP** as the **Service Type**. The **FTP Transfer Mode** parameter allows for the definition of the file transfer mode when log files are retrieved over FTP. From the list, select the transfer mode that you want to apply to this log source: • **Binary** - Select **Binary** for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. • **ASCII** - Select **ASCII** for log sources that require an ASCII FTP file transfer. You must select **None** for the Processor parameter and **LINEBYLINE** the **Event Generator** parameter when you use ASCII as the **FTP Transfer Mode**.
SCP Remote File	If you select **SCP** as the **Service Type** you must type the file name of the remote file.

Table 657. Log File log source parameters for the IBM WebSphere DSM (continued)	
Parameter	**Value**
Start Time	Type the time of day you want the processing to begin. This parameter functions with the **Recurrence** value to establish when and how often the **Remote Directory** is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the directory to be scanned every 2 hours. The default is 1H. When you schedule a log file protocol, select a recurrence time for the log file protocol shorter than the scheduled write interval of the WebSphere Application Server log files. This ensures that WebSphere events are collected by the log file protocol before the new log file overwrites the old event log.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting Run On Save clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	If the files on the remote host are stored in a `zip`, `gzip`, `tar`, or `tar+gzip` archive format, select the processor that allows the archives to be expanded and the contents to be processed.
Ignore Previously Processed File(s)	Select this check box to track files that are processed. Files that are previously processed are not processed a second time. This check box applies only to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on your QRadar that you want to use for storing downloaded files during processing. We recommend that you leave the check box clear. When the check box is selected, the **Local Directory** field is displayed, which gives the option of configuring the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select WebSphere **Application Server**. The Event Generator applies more processing, which is specific to retrieved event files for IBM WebSphere Application Server events.

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related tasks

"Adding a log source" on page 5

IBM WebSphere sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM WebSphere sample message when you use the Syslog protocol

The following sample event message shows a failed login.

```
WebSphere::EVENT_TIME=8/1/12 12:01:59:603 EDT   EVENT_ID=null  EVENT_TYPE=W   RAW_EVENT=[8/1/12
12:01:59:603 EDT] 00000032 LogonAction   W org.apache.commons.logging.impl.Jdk14Logger warn Bad
username/password from someone claiming to be 'hayfordk' from address 10.0.8.108
```

Table 658. QRadar field names and highlighted values in the IBM WebSphere event payload

QRadar field name	Highlighted values in the event payload
Event ID	The value in QRadar is Login Fail
Event Category	**W**
SRC IP	**10.0.8.108**
Event Time	**8/1/12 12:01:59:603 EDT**

IBM WebSphere DataPower

IBM WebSphere DataPower is now known as IBM Datapower.

Related concepts

IBM DataPower

IBM z/OS

The IBM z/OS DSM collects events from an IBM z/OS® mainframe that uses IBM Security zSecure or IBM Z Security and Compliance Center.

When you use a zSecure process, events from the System Management Facilities (SMF) can be transformed into Log Event Extended Format (LEEF) events. These events can be sent near real-time by using UNIX Syslog protocol or IBM QRadar can collect the LEEF event log files by using the Log File protocol and then process the events. When you use the Log File protocol, you can schedule QRadar to collect events on a polling interval, which enables QRadar to collect the events on the schedule that you define.

To collect IBM z/OS events, complete the following steps:

1. Verify that your installation meets any prerequisite installation requirements. For more information about the requirements, see zSecure CARLa-Driven Components Installation and Deployment Guide: Prerequisites or IBM Z Security and Compliance Center: System requirements.
2. Configure your IBM z/OS image to write events in LEEF format. For more information, see the zSecure CARLa-Driven Components Installation and Deployment Guide: Data preparation for SIEM.
3. Create a log source in QRadar for IBM z/OS.
4. If you want to create a custom event property for IBM z/OS in QRadar, for more information, see the IBM Security Custom Event Properties for IBM z/OS technical note.

Before you begin

Before you can configure the data collection process, you must complete the basic zSecure installation process and complete the post-installation activities to create and modify the configuration.

The following prerequisites are required:

- You must ensure parmlib member IFAPRDxx is enabled for IBM Security zSecure Audit on your z/OS image.
- The SCKRLOAD library must be APF-authorized.
- If you are using the direct SMF INMEM real-time interface, you must have the necessary software installed (APAR OA49263) and set up the SMFPRMxx member to include the INMEM keyword and parameters. If you decide to use the CDP interface, you must also have CDP installed and running. For more information, see the zSecure CARLa-Driven Components Installation and Deployment Guide: Procedure for near real-time.
- You must configure a process to periodically refresh your CKFREEZE and UNLOAD data sets.
- If you are using the Log File protocol method, you must configure a SFTP, FTP, or SCP server on your z/OS image for QRadar to download your LEEF event files.
- If you are using the Log File protocol method, you must allow SFTP, FTP, or SCP traffic on firewalls that are located between QRadar and your z/OS image.

For instructions on installing and configuring zSecure, see the IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide.

For instructions about installing and configuring IBM Z Security and Compliance Center, see the Z Security and Compliance Center Guide.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Create a log source for near real-time event feed

The Syslog protocol enables IBM QRadar to receive System Management Facilities (SMF) events in near real-time from a remote host.

The following DSMs are supported:

- IBM z/OS
- IBM CICS
- IBM RACF
- IBM DB2
- CA Top Secret
- CA ACF2

If QRadar does not automatically detect the log source, add a log source for your DSM on the QRadar console.

The following table describes the parameters that require specific values for event collection for your DSM:

Table 659. Log source parameters

Parameter	Value
Log Source type	Select your DSM name from the list.
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Log File log source parameter

If QRadar does not automatically detect the log source, add a IBM z/OS, IBM CICS, IBM RACF, IBM DB2, Broadcom CA Top Secret, or Broadcom CA ACF2 log source on the QRadar Console by using the Log File Protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from IBM z/OS, IBM CICS, IBM RACF, IBM DB2, CA Top Secret, or CA ACF2:

Table 660. Log File log source parameters

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	Select your DSM name.
Protocol Configuration	**Log File**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are suggested as they allow QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as multiple z/OS images or a file repository that contains all of your event logs, you must specify a name, IP address, or host name for the image or location that uniquely identifies events for the DSM log source. This specification enables events to be identified at the image or location level in your network that your users can identify.
Service Type	From the **Service Type** list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. • SFTP - SSH File Transfer Protocol • FTP - File Transfer Protocol • SCP - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service type requires that the server that is specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the device that stores your event log files.

Table 660. Log File log source parameters (continued)	
Parameter	**Value**
Remote Port	Type the TCP port on the remote host that is running the selected **Service Type**. The valid range is 1 - 65535. The options include ports: • FTP - TCP Port 21 • SFTP - TCP Port 22 • SCP - TCP Port 22 If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.
Remote User	Type the user name or user ID necessary to log in to the system that contains your event files. • If your log files are on your IBM z/OS image, type the user ID necessary to log in to your IBM z/OS. The user ID can be up to 8 characters in length. • If your log files are on a file repository, type the user name necessary to log in to the file repository. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to the host.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, this parameter gives you the option to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in.
Recursive	If you want the file pattern to search sub folders in the remote directory, select this check box. By default, the check box is clear. If you configure SCP as the Service Type, the Recursive option is ignored.

Table 660. Log File log source parameters (continued)	
Parameter	**Value**
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, you can configure the regular expression (regex) needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. The IBM z/OS mainframe that uses IBM Security zSecure Audit writes event files by using the pattern: <*product_name*>.<*timestamp*>.gz The FTP file pattern that you specify must match the name that you assigned to your event files. For example, to collect files that start with z0S and end with .gz, type the following code: z0S.*\.gz Use of this parameter requires knowledge of regular expressions (regex). For more information about regex, see Lesson: Regular Expressions (https://docs.oracle.com/javase/tutorial/essential/regex/).
FTP Transfer Mode	This option displays only if you select **FTP** as the **Service Type**. From the list, select **Binary**. The binary transfer mode is needed for event files that are stored in a binary or compressed format, such as zip, gzip, tar, or tar+gzip archive files.
SCP Remote File	If you select **SCP** as the **Service Type** you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. For example, type 00:00 to schedule the Log File protocol to collect event files at midnight. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the remote directory to be scanned every 2 hours from the start time. The default is 1H.

Table 660. Log File log source parameters (continued)	
Parameter	**Value**
Run On Save	If you want the Log File protocol to run immediately after you click **Save**, select this check box. After the **Run On Save** completes, the Log File protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	From the list, select **gzip**. Processors enable event file archives to be expanded and contents are processed for events. Files are processed after they are downloaded to QRadar. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed by the Log File protocol. QRadar examines the log files in the remote directory to determine whether a file is previously processed by the Log File protocol. If a previously processed file is detected, the Log File protocol does not download the file for processing. All files that are not previously processed are downloaded. This option applies only to FTP and SFTP service types.
Change Local Directory?	Select this check box to define a local directory on your QRadar for storing downloaded files during processing. It is suggested that you leave this check box clear. When this check box is selected, the **Local Directory** field is displayed, which gives you the option to configure the local directory to use for storing files.

Table 660. Log File log source parameters (continued)	
Parameter	**Value**
Event Generator	From the **Event Generator** list, select **LineByLine**. The Event Generator applies more processing to the retrieved event files. Each line is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

"Adding a log source" on page 5

IBM zOS sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

IBM zOS sample message when you use the Syslog protocol

The following sample event message shows event summary information.

```
LEEF:1.0|IBM|z/OS|2.4|119-12|devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
devTime=2020-05-17T8:31:30.100+0200     usrName=User01  name=SYSTEM     jobname=User01
src=172.16.0.1  srcPort=1000    dst=172.16.0.2  dstPort=3000    srcBytes=0      dstBytes=0
srcPackets=0    dstPackets=0    FIPSlvl=Off     FIPS140=No      IPproto=TCP
jobid=JOB01023  sysname=SYSTEM  sysplex=PLEX1   stack=TCPIP     tlsalg=AES      tlschn=CBC
tlskeylen=128   tlsCCertSig=RSA-SHA1    tlsKexAlg=DHE-RSA       tlsMsgAuth=HMAC-SHA1
tlsNegCipher=00AB       tlsProtVer=TLSv1.1      tlsSCertSig=RSA-SHA1    connsBeg=1
connsEnd=3      partialBeg=1    partialEnd=2    shortBeg=2      shortEnd=1      activeBeg=1
activeEnd=1     saConnId=000004Q2       dn=TLS_server_subject:'CN=COM1,OU=ORG1,O=IBM,C=US'
TLS_server_issuer:'CN=COM2,OU=ORG1,O=IBM,C=US' TLS_client_subject:'CN=COM1,OU=ORG1,O=IBM,C=US'
TLS_client_issuer:'CN=COM2,OU=ORG1,O=IBM,C=US'        action=INIT     sum=Connection initiation
TLSv1.1 AES-CBC-128 server RSA-1024 client RSA-1024 local port 3000 CN=COM1,OU=ORG1,O=IBM,C=US
```

Table 661. QRadar field names and highlighted values in the IBM zOS event payload	
QRadar field name	**Highlighted values in the event payload**
Event Category	**z/OS**
Event ID	**119-12**
Event Summary (custom)	**Connection initiation TLSv1.1 AES-CBC-128 server RSA-1024 client RSA-1024 local port 3000 CN=COM1,OU=ORG1,O=IBM,C=US**
Source IP	**172.16.0.1**
Source Port	**1000**
Destination IP	**172.16.0.2**
Destination Port	**3000**
Username	**User01**

IBM zSecure Alert

The IBM QRadar DSM for IBM zSecure Alert collects Syslog events from a IBM zSecure Alert.

To integrate IBM zSecure Alert with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website. Download and install the most recent version of the DSM Common RPM on your QRadar Console:
2. Configure your IBM zSecure Alert to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a IBM zSecure Alert log source on the QRadar Console.

The alert configuration on your IBM zSecure Alert appliance determines which alert conditions you want to monitor and forward to QRadar. To collect events in QRadar, you must configure your IBM zSecure Alert appliance to forward events in a UNIX syslog event format by using the QRadar IP address as the destination. For information on configuring UNIX syslog alerts and destinations, see the IBM Security zSecure Alert User Reference Manual.

Related concepts

"Syslog log source parameters for IBM zSecure Alert" on page 1046

Syslog log source parameters for IBM zSecure Alert

If QRadar does not automatically detect the log source, add an IBM zSecure Alert log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from IBM zSecure Alert:

Table 662. Syslog log source parameters for the IBM zSecure Alert DSM

Parameter	Value
Log Source type	IBM zSecure Alert
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM zSecure Alert.

Related tasks

"Adding a log source" on page 5

Chapter 82. ISC BIND

The IBM QRadar DSM for Internet System Consortium (ISC) BIND collects Syslog events from your ISC BIND device.

Complete the following steps to configure ISC BIND to communicate with QRadar.

About this task

You can configure syslog on your ISC BIND device to forward events to QRadar.

Procedure

1. Log in to your ISC BIND device.
2. Open the following file to add a logging clause:

```
named.conf
logging {
channel <channel_name> {
syslog <syslog_facility>;
severity <critical | error | warning | notice | info | debug [level ] |
dynamic >;
print-category yes;
print-severity yes;
print-time yes;
};
category queries {
<channel_name>;
};
category notify {
<channel_name>;
};
category network {
<channel_name>;
};
category client {
<channel_name>;
};
};
For Example:
logging {
channel QRadar {
syslog local3;
```

```
severity info;
};
category queries {
QRadar;
};
category notify {
QRadar;
};
category network {
QRadar;
};
category client {
QRadar;
};
};
```

3. Save and exit the file.
4. Edit the syslog configuration to log to your QRadar using the facility you selected in Chapter 82, "ISC BIND," on page 1047:

   `<syslog_facility>.* @<IP_address>`

   Where *<IP Address>* is the IP address of your QRadar.

   For example:

   `local3.* @<IP_address>`

   Note: QRadar only parses logs with a severity level of info or higher.
5. Restart the following services.

```
service syslog restart
service named restart
```

What to do next

Add a log source in QRadar.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

ISC BIND DSM specifications

When you configure ISC BIND, understanding the specifications for the ISC BIND DSM can help ensure a successful integration. For example, knowing what the supported version of ISC BIND is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the ISC BIND DSM.

Table 663. ISC BIND DSM specifications

Specification	Value
Manufacturer	Internet Systems Consortium (ISC)

Table 663. ISC BIND DSM specifications (continued)	
Specification	**Value**
DSM name	ISC BIND
RPM file name	DSM-*IscBind-QRadar_version-build_number*.noarch.rpm
Supported versions	9.9, 9.11, 9.12
Protocol	Syslog
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	ISC BIND (https://www.isc.org/bind/)

Syslog log source parameters for ISC BIND

If QRadar does not automatically detect the log source, add an ISC BIND log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from ISC Bind:

Table 664. Syslog log source parameters for the ISC Bind DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	ISC Bind
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ISC Bind appliance.

Related tasks

"Adding a log source" on page 5

ISC BIND sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

ISC BIND sample message when you use the Syslog protocol

The following sample event message shows an address query.

```
<158>Sep 28 14:19:30 isc.bind.test named2[1885]: client @0a0a00000a0a00 203.0.113.2#35705 (abc-exam.d.example.com): query: test.example.com IN A +E(0)DC (192.168.10.70)
```

```
<158>Sep 28 14:19:30 isc.bind.test named2[1885]: client @0a0a00000a0a00 203.0.113.2#35705 (abc-
exam.d.example.com): query: test.example.com IN A +E(0)DC (192.168.10.70)
```

Table 665. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**IN A**
Source IP	**203.0.113.2**
Destination IP	**192.168.10.70**
Source Port	**35705**
Device Time	**Sep 28 14:19:30** (extracted from date and time fields)

Chapter 83. Illumio Adaptive Security Platform

The IBM QRadar DSM for Illumio Adaptive Security Platform collects events from the Illumio Policy Compute Engine (PCE).

The following table describes the specifications for the Illumio Adaptive Security Platform DSM:

Table 666. Illumio Adaptive Security Platform DSM specifications

Specification	**Value**
Manufacturer	Illumio
DSM name	Illumio Adaptive Security Platform
RPM file name	`DSM-IllumioAdaptiveSecurityPlatform-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Syslog
Event format	Log Event Extended Format (LEEF)
Recorded event types	Audit Traffic
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Illumio website (https://www.illumio.com)

To integrate Illumio Adaptive Security Platform with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto, in the order that they are listed, on your QRadar Console:
   - DSMCommon RPM
   - Illumio Adaptive Security Platform DSM RPM
2. Configure your Illumio PCE to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an Illumio Adaptive Security Platform log source on the QRadar Console. The following table describes the parameters that require specific values for Illumio Adaptive Security Platform event collection:

   Table 667. Illumio Adaptive Security Platform log source parameters

Parameter	**Value**
Log Source type	Illumio Adaptive Security Platform
Protocol Configuration	Syslog
Log Source Identifier	A unique identifier for the log source.

4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

The following table shows a sample event message from Illumio Adaptive Security Platform:

Table 668. Illumio Adaptive Security Platform sample message

Event name	Low level category	Sample log message
flow_allowed	Firewall Permit	<14>1 2016-08-08T22:18:24.000+00:00 hostname1 illumio_pce/collector 5458 - - sec=694704.253 sev=INFO pid=5458 tid=14554040 rid=0 LEEF:2.0|Illumio|PCE|16.6.0|flow_allowed|cat=flow_summary devTime=2016-08-08T15:20:55-07:00 devTimeFormat=yyyy-MM-dd'T'HH:mm:ssX proto=udp sev=1 src=<Source_IP_address> dst=<Destination_IP_address> dstPort=14000 srcBytes=0 dstBytes=15936 count=1 dir=I hostname=hostname2 intervalSec=3180 state=T workloadUUID=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx <14>1 2016-08-08T22:18:24.000+00:00 hostname1 illumio_pce/collector 5458 - - sec=694704.253 sev=INFO pid=5458 tid=14554040 rid=0 LEEF:2.0|Illumio|PCE|16.6.0|flow_allowed|cat=flow_summary devTime=2016-08-08T15:20:55-07:00 devTimeFormat=yyyy-MM-dd'T'HH:mm:ssX proto=udp sev=1 src=<Source_IP_address> dst=<Destination_IP_address> dstPort=14000 srcBytes=0 dstBytes=15936 count=1 dir=I hostname=hostname2 intervalSec=3180 state=T workloadUUID=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Illumio Adaptive Security Platform to communicate with QRadar

To forward events to IBM QRadar, you must configure Exporting Events to Syslog and Syslog Forwarding for your Illumio PCE.

Related tasks

"Configuring Exporting Events to Syslog for Illumio PCE" on page 1053

All audit and traffic summaries are sent to syslog in JSON format by default. The default configuration must be updated so that the events are exported in LEEF format.

"Configuring Syslog Forwarding for Illumio PCE" on page 1053

Because the PCE software exports logs to a local syslog, you must configure either rsyslog or syslog-ng service on each node in your PCE cluster to forward these logs to QRadar.

Configuring Exporting Events to Syslog for Illumio PCE

All audit and traffic summaries are sent to syslog in JSON format by default. The default configuration must be updated so that the events are exported in LEEF format.

Procedure

1. Stop the PCE software so that changes to the PCE `runtime_env.yml` file can be made.
2. Enable LEEF formatting by configuring the PCE `runtime_env.yml` parameter **`syslog_event_export_format`**.

   ```
   syslog_event_export_format:leef
   ```

3. Export traffic summaries to Syslog by configuring the PCE `runtime_env.yml` parameter **`export_flow_summaries_to_syslog`**:

   ```
   export_flow_summaries_to_syslog:
        accepted
        potentially_blocked
        blocked
   ```

   Tip: By default, the PCE exports all audit events to Syslog. Therefore, no configuration is required to enable exporting audit events.

   The **`export_flow_summaries_to_syslog`** parameter should be considered experimental and the mechanism for configuring this feature might change in a future release.

   Note: The **`export_flow_summaries_to_syslog`** parameter should be considered experimental and the mechanism for configuring this feature might change in a future release.
4. Type the **`./illumio-pce-env check`** command to validate the syntax of the configuration file.
5. Start the PCE software.

What to do next

Configure Syslog Forwarding

Configuring Syslog Forwarding for Illumio PCE

Because the PCE software exports logs to a local syslog, you must configure either rsyslog or syslog-ng service on each node in your PCE cluster to forward these logs to QRadar.

Procedure

1. If you want to configure rsyslog, complete the following steps.
   a) Edit the `/etc/rsyslog.conf` file by adding the following entries or uncomment if they are already present. Replace <*QRadar Event Collector IP*> with the IP address of the QRadar event collector:

   ```
   ### LEEF (flow data, audit events) ###
   if $syslogseverity <= 6 \
    and $syslogtag startswith 'illumio_pce/collector[' \
    and $msg contains 'LEEF:' \
    and $msg contains '|Illumio|PCE|' \
    and $msg contains 'cat=flow_summary' \
   then @@<QRadar Event Collector IP>:514

   if $syslogseverity <= 6 \
    and $syslogtag startswith 'illumio_pce/' \
    and $msg contains 'LEEF:' \
    and $msg contains '|Illumio|PCE|' \
   ```

```
 and $msg contains 'audit_events' \
then @@<QRadar Event Collector IP>:514
```

b) Restart the rsyslog service.

```
service rsyslog restart
```

2. If you want to configure syslog-ng, complete the following steps.

a) Edit the `/etc/syslog-ng/syslog-ng.conf` file by adding the following entries or uncomment if they are already present. Replace <*QRadar Event Collector IP*> with the IP address of the QRadar event collector:

```
#destination d_net { tcp("<QRadar Event
 Collector IP>" port(514) flush_lines(1)); };
#log { source(s_src); filter(flow_events);
 destination(d_net); };#log { source(s_src);
 filter(audit_events); destination(d_net); };

### LEEF (flow data, audit events) ###
filter flow_events {
 level(info..emerg)
 and program("^illumio_pce/collector$")
 and message('LEEF:[^\|]+\|Illumio\|PCE\|')
 and message('cat=flow_summary');
};

filter audit_events {
 level(info..emerg)
 and program("^illumio_pce/")
 and message('LEEF:[^\|]+\|Illumio\|PCE\|')
 and message('cat=[^ #]*audit_events');
};
```

b) Restart the syslog-ng service.

```
service syslog-ng restart
```

Chapter 84. Imperva Incapsula

The IBM QRadar DSM for Imperva Incapsula collects logs from an Imperva Incapsula service.

The following table describes the specifications for the Imperva Incapsula DSM:

Table 669. Imperva Incapsula DSM specifications

Specification	**Value**
Manufacturer	Imperva
DSM name	Imperva Incapsula
RPM file name	`DSM-ImpervaIncapsula-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Syslog
Event format	LEEF
Recorded event types	Access events and Security alerts
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Imperva Incapsula website (https://www.incapsula.com/)

To integrate Imperva Incapsula with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Imperva Incapsula DSM RPM
2. Configure the Log download utility to collect logs and then forward the logs to QRadar.
3. If QRadar does not automatically detect the log source, add an Imperva Incapsula log source on the QRadar Console. The following table describes the parameters that require specific values to collect event from Imperva Incapsula:

   Table 670. Imperva Incapsula log source parameters

Parameter	**Value**
Log Source type	Imperva Incapsula
Protocol Configuration	Syslog

4. Verify that QRadar is configured correctly.

   Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

   The following table shows a sample normalized event message from Imperva Incapsula:

Table 671. Imperva Incapsula sample message

Event name	Low level category	Sample log message
REQ_PASSED	Information	LEEF:1.0| Incapsula| SIEMintegration| 1.0|Normal| fileId=fid sourceServiceName =ssname siteid=siteid suid=suid requestClientAppl ication=reqcliapp cs2=true cs2Label=Javascri pt Support cs3=true cs3Label=CO Support src=<Source_IP_address> cs1=NA cs1Label=Cap Support cs5Label=clappsig dproc=Browser cs6=Internet Explorer cs6Label=clapp calCountryOrRegio n=[XX] cs7=xx.xx cs7Label=latitude cs8=xx.xx cs8Label=longitude Customer=customer start=start requestMethod=GET cn1=200 proto=HTTP cat=REQ_PASSED LEEF:1.0|Incapsula|SIEMintegration| 1.0|Normal| fileId=fidsourceServiceName=ssnamesite id=siteidsuid=suidrequestClientApplica tion=reqcliappcs2=truecs2Label=Javascr ipt Supportcs3=truecs3Label=COSupportsrc=< Source_IP_address>cs1=NAcs1Label=CapSu pportcs5Label=clappsigdproc=Browsercs6 =InternetExplorercs6Label=clappcalCoun tryOrRegion=[XX]cs7=xx.xxcs7Label=lati tudecs8=xx.xxcs8Label=longitudeCustome r=customerstart=startrequestMethod=GET cn1=200proto=HTTPcat=REQ_PASSED

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Imperva Incapsula to communicate with QRadar

To collect events from Imperva Incapsula, a Python script is required.

The script, configuration files, and instructions, can be obtained from the GitHub website (https://github.com/imperva/incapsula/logs-downloader).

Procedure

1. Install the script dependencies by using a package manager such as apt-get or pip. The script dependencies must be installed on an intermediary server that is not QRadar. The following dependencies might require additional modules, depending on your operating system:
   - M2Crypto
   - loggerglue
   - crypto.cipher
2. To collect log events, run the script.
   a) Create a new local directory or use the default directory to store the script configuration file. The `Settings.Config` file is stored in this local directory. The default directory is `/etc/incapsula/logs/config`. To get the `Settings.Config` file, go to the GitHub website (https://github.com/imperva/incapsula-logs-downloader).
   b) Configure the parameter values for the `Settings.Config` configuration file.

Table 672. Parameter values for the `Settings.Config` configuration file

Parameter	Value
APIID	Your API ID.
APIKEY	Your API key.
SAVE_LOCALLY	A Yes or No value that instructs Incapsula whether to maintain the log files after they are processed. When set to No, the files are deleted. The default is YES.
PROCESS_DIR	The directory where Incapsula automatically saves the logs after extracting them. The default is `/tmp/processed/`
BASEURL	The URL of your logs repository in the Incapsula cloud. This URL is displayed in the **Incapsula Administration Console Settings** window as the **Log Server URL** field.
USEPROXY	Specify YES to use a proxy to download the files. The default is NO.
PROXYSERVER	If you choose to use a proxy server, when you type the proxy URL, use the <*https://1.1.1.1:8080*> format.
SYSLOG_ENABLE	Type YES. A Yes or No value that instructs Incapsula about whether to send the files by using syslog. The default is YES.
SYSLOG_ADDRESS	The IP address for QRadar
SYSLOG_PORT	514

Table 672. Parameter values for the `Settings.Config` configuration file (continued)	
Parameter	**Value**
USE_CUSTOM_CA_FILE	In case the service's certificate is not in the bundle, the default is NO.
CUSTOM_CA_FILE	The file path for the custom certificate file.

3. Run the following command to start the LogsDownloader script and retrieve logs:

```
python LogsDownloader.py -c <path_to_config_folder> -l <path_to_system_logs_folder> -v
<system_logs_level>
```

The -c, -l, and -v parameters are optional. If the parameter values are not specified, the following table describes the default values that are used:

Table 673. LogsDownloader.py parameter values	
Parameter	**Value**
<*path_to_config_folder*>	The default is `/etc/incapsula/logs/config`
<*path_to_system_logs_folder*>	The <*path_to_system_logs_folder*> is the folder where the LogsDownloader.py script output log file is stored. This parameter does not refer to your Incapsula logs. The default is `/var/log/incapsula/logsDownloader/`
<*system_logs_level*>	The logging level for the script output log. Supported values are info, debug, and error. The default value is **info**.

Note:

- If the **SAVE_LOCALLY** parameter is set to YES, the downloaded log files can be found in the PROCESS_DIR directory.
- After the files are downloaded, the script saves the name of the last file it collects as `LastKnownDownloadedFileId.txt` in the <*path_to_config_folder*> directory. If you want to collect all of the historical logs, you must delete this file.
- For more information about setting up an intermediary server, see Imperva Incapsula's Web Protection - Log Integration (https://docs.imperva.com/bundle/cloud-application-security/page/settings/log-integration.htm).

Chapter 85. Imperva SecureSphere

The IBM QRadar DSM for Imperva SecureSphere collects all relevant syslog events from your Imperva SecureSphere devices.

The following table lists the specifications for the Imperva SecureSphere DSM:

Table 674. Imperva SecureSphere DSM

Specification	Value
Manufacturer	Imperva
DSM name	SecureSphere
RPM file name	`DSM-ImpervaSecuresphere-`*`QRadar-version-Build_number`*`.noarch.rpm`
Supported versions	v6.2 and v7.x to v13 Release Enterprise Edition (Syslog) v9.5 to v13 (LEEF)
Event format	syslog LEEF
QRadar recorded event types	Firewall policy events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Imperva website (http://www.imperva.com)

To send events from Imperva SecureSphere devices to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Imperva SecureSphere DSM RPM from the IBM Support Website onto your QRadar Console.
2. For each instance of Imperva SecureSphere, configure the Imperva SecureSphere appliance to communicate with QRadar. On your Imperva SecureSphere appliance, complete the following steps
   a. Configure an alert action.
   b. Configure a system event action.
3. If QRadar does not automatically discover the Imperva SecureSphere log source, create a log source for each instance of Imperva SecureSphere on your network. Use the following table to define the Imperva SecureSphere-specific parameters:

   Table 675. Imperva SecureSphere log source parameters

Parameter	Description
Log Source Type	Imperva SecureSphere
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring an alert action for Imperva SecureSphere

Configure your Imperva SecureSphere appliance to forward syslog events for firewall policy alerts to QRadar.

Configuring a system event action for Imperva SecureSphere
Configure your Imperva SecureSphere appliance to forward syslog system policy events to QRadar.

Adding a log source
“Configuring an alert action for Imperva SecureSphere ” on page 1060
Configure your Imperva SecureSphere appliance to forward syslog events for firewall policy alerts to QRadar.

“Configuring a system event action for Imperva SecureSphere” on page 1061
Configure your Imperva SecureSphere appliance to forward syslog system policy events to QRadar.

“Configuring Imperva SecureSphere V11.0 to V13 to send database audit records to QRadar” on page 1063
To send database audit records from Imperva SecureSphere V11.0 to V13 IBM QRadar, create a custom action set, add an action interface, and then configure an audit policy.

Configuring an alert action for Imperva SecureSphere

Configure your Imperva SecureSphere appliance to forward syslog events for firewall policy alerts to QRadar.

About this task

Use the following list to define a message string in the **Message** field for each event type you want to forward:

Tip: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters. Paste as a single line in the **Custom Format** column.

Database alerts (V9.5 and V10 to V13)

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|${Alert.alertType} $
{Alert.immediateAction}|Alert ID=${Alert.dn}|devTimeFormat=[see note]|
devTime=${Alert.createTime}|Alert type=${Alert.alertType}|src=${Alert.sourceIp}|
usrName=${Event.struct.user.user}|Application name=${Alert.applicationName}|dst=$
{Event.destInfo.serverIp}|Alert Description=${Alert.description}|Severity=${Alert.severity}|
Immediate Action=${Alert.immediateAction}|SecureSphere Version=${SecureSphereVersion}
```

File server alerts (V9.5 and V10 to V13)

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|${Alert.alertType} $
{Alert.immediateAction}|Alert ID={Alert.dn}|devTimeFormat=[see note]|devTime=$
{Alert.createTime}|Alert type=${Alert.alertType}|src=${Alert.sourceIp} |
usrName=${Event.struct.user.username}|Domain=${Event.struct.user.domain}|Application
name=${Alert.applicationName}|dst=${Event.destInfo.serverIp}|Alert Description=$
{Alert.description}|Severity=${Alert.severity} |Immediate Action=${Alert.immediateAction} |
SecureSphere Version=${SecureSphereVersion}
```

Web application firewall alerts (V9.5 and V10 to V13)

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|${Alert.alertType}
${Alert.immediateAction}|Alert ID=${Alert.dn}|
devTimeFormat=[see note]|devTime=${Alert.createTime}|
Alert type=${Alert.alertType}|src=${Alert.sourceIp}|srcPort=$!{Event.sourceInfo.sourcePort}|
usrName=${Alert.username}|Application name=${Alert.applicationName}|dst=$
{Event.destInfo.serverIp}|dstPort=$!{Event.destInfo.serverPort}|Service name=$
{Alert.serviceName}|Event Description=${Alert.description}|Severity=${Alert.severity}|
Simulation Mode=${Alert.simulationMode}|Immediate Action=${Alert.immediateAction}
```

All alerts (V6.2 and V7 to V13 Release Enterprise Edition)

```
DeviceType=ImpervaSecuresphere Alert|an=$!
{Alert.alertMetadata.alertName}|at=SecuresphereAlert|sp=$!{Event.sourceInfo.sourcePort}|s=$!
{Event.sourceInfo.sourceIp}|d=$!{Event.destInfo.serverIp}|dp=$!{Event.destInfo.serverPort}|
u=$!{Alert.username}|g=$!{Alert.serverGroupName}|ad=$!{Alert.description}
```

Tip: The **devTimeFormat** parameter does not include a value because you can configure the time format on the SecureSphere appliance. Review the time format of your SecureSphere appliance and specify the appropriate time format.

Procedure

1. Log in to SecureSphere by using administrative privileges.
2. Click the **Policies** tab.
3. Click the **Action Sets** tab.
4. Generate events for each alert that the SecureSphere device generates:
   a) Click **New** to create a new action set for an alert.
   b) Move the action to the **Selected Actions** list.
   c) Expand the **System Log** action group.
   d) In the **Action Name** field, type a name for your alert action.
   e) From the **Apply to event type** list, select **Any event type**.
   f) In the **Syslog host** field, type the IP address of the QRadar appliance to which you want to send events.
   g) In the **Syslog log level** list, select **INFO**.
   h) In the **Message** field, define a message string for your event type.
   i) In the **Facility** field, type `syslog`.
   j) Select the **Run on Every Event** check box.
   k) Click **Save**.
5. To trigger syslog events, associate each of your firewall policies to an alert action:
   a) From the navigation menu, click **Policies > Security > Firewall Policy**.
   b) Select the policy that you want to use for the alert action.
   c) Click the **Policy** tab.
   d) From the **Followed Action** list, select your new action and configure the parameters.

      Tip: Configure established connections as either blocked, inbound, or outbound. Always allow applicable service ports.
   e) Ensure that your policy is configured as enabled and is applied to the appropriate server groups.
   f) Click **Save**.

Configuring a system event action for Imperva SecureSphere

Configure your Imperva SecureSphere appliance to forward syslog system policy events to QRadar.

About this task

Use the following list to define a message string in the **Message** field for each event type you want to forward:

Tip: Line breaks in code examples can cause configurations to fail. For each alert, copy the code blocks into a text editor, remove any line breaks, and paste as a single line in the **Custom Format** column.

System events (V9.5 and V10 to V13)

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|${Event.eventType}|Event
ID=${Event.dn}|devTimeFormat=[see note]|devTime=${Event.createTime}|
Event Type=${Event.eventType}|Message=${Event.message}|Severity=$
{Event.severity.displayName}|usrName=${Event.username}|SecureSphere Version=$
{SecureSphereVersion}
```

Database audit records (V9.5 and V10 to V13)

```
LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}|${Event.struct.eventType}|Server
Group=${Event.serverGroup}|Service Name=${Event.serviceName}|Application
Name=${Event.applicationName}|Source Type=${Event.sourceInfo.eventSourceType}|
User Type=${Event.struct.user.userType}|usrName=${Event.struct.user.user}|
User Group=${Event.struct.userGroup}|Authenticated=${Event.struct.user.authenticated}|
App User=${Event.struct.applicationUser}|src=${Event.sourceInfo.sourceIp}|Application=$
{Event.struct.application.application}|OS User=${Event.struct.osUser.osUser}|
Host=${Event.struct.host.host}|Service Type=${Event.struct.serviceType}|dst=$
{Event.destInfo.serverIp}|Event Type=${Event.struct.eventType}|Operation=$
{Event.struct.operations.name}|Operation type=${Event.struct.operations.operationType}|
Object name=${Event.struct.operations.objects.name}|Object
type=${Event.struct.operations.objectType}|Subject=${Event.struct.operations.subjects.name}|
Database=${Event.struct.databases.databaseName}|Schema=${Event.struct.databases.schemaName}|
Table Group=$
{Event.struct.tableGroups.displayName}|Sensitive=${Event.struct.tableGroups.sensitive}|
Privileged=${Event.struct.operations.privileged}|Stored Proc=$
{Event.struct.operations.storedProcedure}|Completed Successfully=$
{Event.struct.complete.completeSuccessful}|Parsed Query=${Event.struct.query.parsedQuery}|
Bind Vaiables=${Event.struct.rawData.bindVariables}|Error=$
{Event.struct.complete.errorValue}|Response Size=${Event.struct.complete.responseSize}|
Response Time=${Event.struct.complete.responseTime}|Affected Rows=$
{Event.struct.query.affectedRows}| devTimeFormat=[see note]|devTime=${Event.createTime}
```

All events (V6.2 and V7.x to V13 Release Enterprise Edition)

```
DeviceType=ImpervaSecuresphere Event|et=$!{Event.eventType}|
dc=Securesphere System Event|sp=$!{Event.sourceInfo.sourcePort}|s=$!
{Event.sourceInfo.sourceIp}|d=$!{Event.destInfo.serverIp}|dp=$!{Event.destInfo.serverPort}|
u=$!{Event.username}|t=$!{Event.createTime}|sev=$!{Event.severity}|m=$!{Event.message}
```

Note: The **devTimeFormat** parameter does not include a value because you can configure the time format on the SecureSphere appliance. Review the time format of your SecureSphere appliance and specify the appropriate time format.

Procedure

1. Log in to SecureSphere by using administrative privileges.
2. Click the **Policies** tab.
3. Click the **Action Sets** tab.
4. Generate events for each alert that the SecureSphere device generates:
   a) Click **New** to create a new action set for an alert.
   b) Type a name for the new action set.
   c) Move the action to the **Selected Actions** list.
   d) Expand the **System Log** action group.
   e) In the **Action Name** field, type a name for your alert action.
   f) From the **Apply to event type** list, select **Any event type**.
   g) In the **Syslog host** field, type the IP address of the QRadar appliance to which you want to send events.
   h) In the **Syslog log level** list, select **INFO**.
   i) In the **Message** field, define a message string for your event type.
   j) In the **Facility** field, type `syslog`.
   k) Select the **Run on Every Event** check box.
   l) Click **Save**.
5. To trigger syslog events, associate each of your system event policies to an alert action:
   a) From the navigation menu, click **Policies** > **System Events**.
   b) Select or create the system event policy that you want to use for the alert action.
   c) Click the **Followed Action** tab.

d) From the **Followed Action** list, select your new action and configure the parameters.

Tip: Configure established connections as either blocked, inbound, or outbound. Always allow applicable service ports.

e) Click **Save**.

Configuring Imperva SecureSphere V11.0 to V13 to send database audit records to QRadar

To send database audit records from Imperva SecureSphere V11.0 to V13 IBM QRadar, create a custom action set, add an action interface, and then configure an audit policy.

Procedure

1. Create a custom action set:
   a) Log in to your Imperva SecureSphere system.
   b) In the **Main** workspace, select **Policies** > **Action Sets**.
   c) In the **Action Sets** pane, click the green plus sign icon.
   d) In the **Action Set** text box, type a name for the action set. For example, `QRadar SIEM`.
   e) From the **Apply to event type** list, select **Audit**.
   f) Click **Create**.
2. Add the action interface that you want to be part of the action set to the **Selected Actions** pane:
   a) Click the green up arrow icon, and then select **Gateway System Log** > **log audit event to System Log (Gateway System Log)**.
   b) Configure the following action interface parameters:

Parameter	Value
Name	Type the name that you created for the action set. For example, `QRadar SIEM`.
Protocol	Select **UDP**.
Host	Type the IP address or the host name of the QRadar appliance for which you want to send events.
Port	514
Syslog Log Level	Info
Facility	syslog

Parameter	Value
Message	**Tip:** The line breaks in the code example might cause this configuration to fail. For each alert, copy the code block below into a text editor, remove the line breaks, and paste as a single line in the **Message** field. `LEEF:1.0|Imperva|SecureSphere|${SecureSphereVersion}\|${Alert.alertType} ${Alert.immediateAction}\|Alert ID=${Alert.dn}|devTimeFormat=yyyy-MM-dd HH:mm:ss.S|devTime=${Alert.createTime}\|Alert type=${Alert.alertType}|src=${Alert.sourceIp}\|usrName=${Event.struct.user.user}|Application name=${Alert.applicationName}\|dst=${Event.destInfo.serverIp}|Alert Description=${Alert.description}\|Severity=${Alert.severity}|Immediate Action=${Alert.immediateAction}\|SecureSphere Version=${SecureSphereVersion}`

a) Select the **Run on Every Event** check box.

3. Configure an audit policy for the events that you want to send to QRadar:
   a) In the Main workspace, click **Policies** > **Audit**.
   b) Click **Create DB Service**.
   c) Type a name for the policy.
   d) Select **Use Existing**, and then select a policy from the list.
   e) Click the **Match Criteria** tab, and then enter the criteria for the policy.
   f) Click the **Apply To** tab, and then select the server group.
   g) Click the **External Logger** tab.
   h) From the **Syslog** list, select the **QRadar SIEM** that you configured.
   i) Optional: If you select a pre-defined policy from the **Syslog** list, configure the **Apply to** and **External Logger** fields.
   j) Click **Save**.

What to do next

You must define an audit policy or configure a pre-defined policy for each type of audit event that you want to send to QRadar.

Chapter 86. Infoblox NIOS

The IBM QRadar DSM for Infoblox NIOS collects Syslog events from an Infoblox NIOS device.

To integrate Infoblox NIOS with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Infoblox DSM RPM
2. Configure your Infoblox device to send syslog events to QRadar. For more information about sending syslog events from Infoblox, see your Infoblox NIOS documentation (https://docs.infoblox.com/display/ILP/NIOS).
3. Add an Infoblox log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from Infoblox NIOS:

Table 676. Infoblox NIOS Syslog log source parameters

Parameter	Value
Log Source Name	Type a unique name for the log source.
Log Source Type (Optional)	Type a description for the log source.
Log Source type	Infoblox NIOS
Protocol Configuration	Syslog

Related tasks

"Adding a log source" on page 5

Infoblox NIOS DSM specifications

The following table describes the specifications for the Infoblox NIOS DSM.

Table 677. Infoblox NIOS DSM specifications

Specification	Value
Manufacturer	Infoblox
DSM name	Infoblox NIOS
RPM file name	DSM-*Infoblox NIOS-QRadar_version-build_number*.noarch.rpm
Supported versions	6.x to 8.x
Protocol	Syslog
Event format	Syslog
Recorded event types	• ISC Bind events • Linux DHCP events • Linux Server events • Apache events
Automatically discovered?	No

Table 677. Infoblox NIOS DSM specifications (continued)	
Specification	**Value**
Includes identity?	Yes
Includes custom properties?	No
More information	For information about configuring your Infoblox NIOS device to send Syslog events to QRadar, see your Infoblox NIOS documentation (https://docs.infoblox.com/display/ILP/NIOS).

Infoblox NIOS sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Infoblox NIOS sample message when you use the Syslog protocol

The following sample event message shows the response message that is received when querying on a record.

```
<30>May  3 16:30:50 infoblox.nios.test named[2259]: 03-May-2018 16:30:50.385 client
192.168.163.1#44783: view 3: UDP: query: www.example.com IN A response: NOERROR -A
www.example.com.
300 IN CNAME www.example.com.;
```

```
<30>May  3 16:30:50 infoblox.nios.test named[2259]: 03-May-2018 16:30:50.385 client
192.168.163.1#44783: view 3: UDP: query: www.example.com IN A response: NOERROR -A
www.example.com. 300 IN CNAME www.example.com.;
```

Chapter 87. iT-CUBE agileSI

The iT-CUBE agileSI DSM for IBM QRadarcan accept security-based and audit SAP events from agileSI installations that are integrated with your SAP system.

QRadar uses the event data that is defined as security risks in your SAP environment to generate offenses and correlate event data for your security team. SAP security events are written in Log Event Extended Format (LEEF) to a log file produced by agileSI. QRadar retrieves the new events by using the SMB Tail protocol. To retrieve events from agileSI, you must create a log source by using the SMB Tail protocol and provide QRadar credentials to log in and poll the LEEF formatted agileSI event file. QRadar is updated with new events each time the SMB Tail protocol polls the event file for new SAP events.

Configuring agileSI to forward events

To configure agileSI, you must create a logical file name for your events and configure the connector settings with the path to your agileSI event log.

About this task

The location of the LEEF formatted event file must be in a location viewable by Samba and accessible with the credentials you configure for the log source in IBM QRadar.

Procedure

1. In agileSI core system installation, define a logical file name for the output file that contains your SAP security events.

   SAP provides a concept that gives you the option to use platform-independent logical file names in your application programs. Create a logical file name and path by using transaction "FILE" (Logical File Path Definition) according to your organization's requirements.
2. Log in to agileSI.

   For example, `http://<sap-system-url:port>/sap/bc/webdynpro/itcube/ ccf?sap-client=<client>&sap-language=EN`

   Where:

   - <*sap-system-url*> is the IP address and port number of your SAP system, such as <IP_address>:50041.
   - <*client*> is the agent in your agileSI deployment.
3. From the menu, click **Display/Change** to enable change mode for agileSI.
4. From the toolbar, select **Tools** > **Core Consumer Connector Settings**.

   The Core Consumer Connector Settings are displayed.
5. Configure the following values:

   From the **Consumer Connector** list, select **Q1 Labs**.
6. Select the **Active** check box.
7. From the **Connector Type** list, select **File**.
8. From the **Logical File Name** field, type the path to your logical file name you configured in “Configuring agileSI to forward events ” on page 1067.

   For example, `/ITCUBE/LOG_FILES`.

   The file that is created for the agileSI events is labeled `LEEFYYYYDDMM.TXT` where `YYYYDDMM` is the year, day, and month. The event file for the current day is appended with new events every time the extractor runs. *iT-CUBE* agileSI creates a new LEEF file for SAP events daily.

9. Click **Save**.

   The configuration for your connector is saved. Before you can complete the agileSI configuration, you must deploy the changes for agileSI by using extractors.
10. From the toolbar, select **Tools** > **Extractor Management**.

    The Extractor Management settings are displayed.
11. Click **Deploy all**.

    The configuration for agileSI events is complete. You are now ready to configure a log source in QRadar.

SMB Tail log source parameters for iT-CUBE agileSI

If QRadar does not automatically detect the log source, add an iT-CUBE agileSI log source on the QRadar Console by using the SMB Tail protocol.

When using the SMB Tail protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SMB Tail events from iT-CUBE agileSI:

Table 678. SMB Tail log source parameters for the iT-CUBE agileSI DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	iT-CUBE agileSI
Protocol Configuration	SMB Tail
Log Source Identifier	Type the IP address, host name, or name for the log source as an identifier for your *iT-CUBE* agileSI events.

For a complete list of SMB Tail protocol parameters and their values, see c_logsource_SMBtailprotocol.dita.

Related tasks

"Adding a log source" on page 5

Chapter 88. Itron Smart Meter

The Itron Smart Meter DSM for IBM QRadar collects events from an Itron Openway Smart Meter by using syslog.

The Itron Openway Smart Meter sends syslog events to QRadar by using Port 514. For details of configuring your meter for syslog, see your *Itron Openway Smart Meter* documentation.

Syslog log source parameters for Itron Smart Meter

If QRadar does not automatically detect the log source, add an Itron Smart Meter log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Itron Smart Meter:

Table 679. Syslog log source parameters for the Itron Smart Meter DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Itron Smart Meter
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Itron Openway Smart Meter installation.

Related tasks

"Adding a log source" on page 5

Chapter 89. Juniper Networks

IBM QRadar supports a range of Juniper Networks DSMs.

Juniper Networks AVT

The Juniper Networks Application Volume Tracking (AVT) DSM for IBM QRadar accepts events by using Java Database Connectivity (JDBC) protocol.

About this task

QRadar records all relevant events. To integrate with Juniper Networks NSM AVT data, you must create a view in the database on the Juniper Networks NSM server. You must also configure the Postgres database configuration on the Juniper Networks NSM server to allow connections to the database since, by default, only local connections are allowed.

Note: This procedure is provided as a guideline. For specific instructions, see your vendor documentation.

Procedure

1. Log in to your Juniper Networks AVT device command-line interface (CLI).
2. Open the following file:

   `/var/netscreen/DevSvr/pgsql/data/pg_hba.conf file`
3. Add the following line to the end of the file:

   `host all all <IP address>/32 trust`

   Where: <*IP address*> is the IP address of your QRadar Console or Event Collector that you want to connect to the database.
4. Reload the Postgres service:

   ```
   su - nsm -c "pg_ctl reload -D /var/netscreen/DevSvr/pgsql/data"
   ```
5. As the Juniper Networks NSM user, create the view by using the following input:

   ```
   create view strm_avt_view as SELECT a.name, a.category, v.srcip,v.dstip,v.dstport, v."last",
   u.name as userinfo, v.id, v.device, v.vlan,v.sessionid, v.bytecnt,v.pktcnt, v."first" FROM
   avt_part v JOIN app a ON v.app =a.id JOIN userinfo u ON v.userinfo = u.id;
   ```

   The view is created.

   You are now ready to configure the log source in QRadar.

JDBC log source parameters for Juniper Networks AVT

If QRadar does not automatically detect the log source, add a Juniper Networks AVT log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Juniper Networks AVT:

Table 680. JDBC log source parameters for the Juniper Networks AVT DSM

Parameter	Value
Log Source Type	Juniper Networks AVT
Protocol Configuration	JDBC

Table 680. JDBC log source parameters for the Juniper Networks AVT DSM (continued)	
Parameter	**Value**
Database Type	**Postgres**
Database Name	`profilerDb`
IP or Hostname	The IP address or host name of the SQL server that hosts the Juniper Networks AVT database.
Username	Type the user name the log source can use to access the Juniper Networks AVT database.
Password	Type the password the log source can use to access the Juniper Networks AVT database. The password can be up to 255 characters in length.
Predefined Query	From the list, select **Juniper Networks AVT**.
Use Prepared Statements	The **Use Prepared Statements** check box must be clear. The Juniper Networks AVT DSM does not support prepared statements.
Polling Interval	Type the polling interval, which is the amount of time between queries to the view you created. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values that are entered without an H or M poll in seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 20,000 EPS.

Note: Selecting a parameter value greater than 5 for the **Credibility** parameter weights your Juniper Networks AVT log source with a higher importance that is compared to other log sources in QRadar.

For a complete list of JDBC parameters and their values, see c_logsource_JDBCprotocol.dita.

Related tasks

"Adding a log source" on page 5

Juniper Networks DDoS Secure

Juniper Networks DDoS Secure is now known as NCC Group DDoS Secure.

Related concepts

"NCC Group DDoS Secure" on page 1233

The IBM QRadar DSM for NCC Group DDoS Secure collects events from NCC Group DDoS Secure devices.

Juniper Networks DX Application Acceleration Platform

The Juniper DX Application Acceleration Platform DSM for IBM QRadar uses syslog to receive events. QRadar records all relevant status and network condition events. Before you configure QRadar, you must configure your Juniper device to forward syslog events.

The Juniper Networks DX Platform product is end of life (EOL), and is no longer supported by Juniper.

Procedure

1. Log in to the Juniper DX user interface.
2. Browse to the wanted cluster configuration (Services - Cluster Name), Logging section.
3. Select the **Enable Logging** check box.
4. Select your log format.

   QRadar supports Juniper DX logs by using the common and perf2 formats only.
5. Select the log delimiter format.

   QRadar supports comma delimited logs only.
6. In the **Log Host** section, type the IP address of your QRadar system.
7. In the **Log Port** section, type the UDP port on which you want to export logs.
8. You are now ready to configure the log source in QRadar.

Configuring IBM QRadar to receive events from a Juniper DX Application Acceleration Platform

About this task

You can configure QRadar to receive events from a Juniper DX Application Acceleration Platform.

Procedure

From the **Log Source Type** list, select the **Juniper DX Application Acceleration Platform** option.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Juniper Networks EX Series Ethernet Switch

The Juniper EX Series Ethernet Switch DSM for IBM QRadar accepts events by using syslog.

About this task

The Juniper EX Series Ethernet Switch DSM supports Juniper EX Series Ethernet Switches running Junos OS. Before you can integrate QRadar with a Juniper EX Series Ethernet Switch, you must configure your Juniper EX Series Switch to forward syslog events.

Procedure

1. Log in to the Juniper EX Series Ethernet Switch command line interface (CLI).
2. Type the following command:

   ```
   configure
   ```

3. Type the following command:

   `set system syslog host <IP address> <option> <level>`

   Where:

   - <*IP address*> is the IP address of your QRadar.
   - <*level*> is info, error, warning, or any.
   - <*option*> is one of the following options from Table 681 on page 1074.

Table 681. Juniper Networks EX Series switch options

Option	Description
any	All facilities
authorization	Authorization system
change-log	Configuration change log
conflict-log	Configuration conflict log
daemon	Various system processes
dfc	Dynamic flow capture
explicit-priority	Include priority and facility in messages
external	Local external applications
facility-override	Alternative facility for logging to remote host
firewall	Firewall filtering system
ftp	FTP process
interactive-commands	Commands run by the UI
kernel	Kernel
log-prefix	Prefix for all logging to this host
match	Regular expression for lines to be logged
pfe	Packet Forwarding Engine
user	User processes

   For example:

   `set system syslog host <IP_address> firewall info`

   This command example configures the Juniper EX Series Ethernet Switch to send info messages from firewall filter systems to your QRadar.

4. Repeat steps 1-3 to configure any additional syslog destinations and options. Each additional option must be identified by using a separate syslog destination configuration.
5. You are now ready to configure the Juniper EX Series Ethernet Switch in QRadar.

Configuring IBM QRadar to receive events from a Juniper EX Series Ethernet Switch

You can configure QRadar to receive events from a Juniper EX Series Ethernet Switch:

Procedure

From the **Log Source Type** list, select **Juniper EX-Series Ethernet Switch** option.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Juniper Networks IDP

The Juniper IDP DSM for IBM QRadar accepts events using syslog. QRadar records all relevant Juniper IDP events.

About this task

You can configure a sensor on your Juniper IDP to send logs to a syslog server:

Procedure

1. Log in to the Juniper NSM user interface.
2. In NSM, double-click the **Sensor in Device Manager**.
3. Select **Global Settings**.
4. Select **Enable Syslog**.
5. Type the Syslog Server IP address to forward events to QRadar.
6. Click **OK**.
7. Use **Update Device** to load the new settings onto the IDP Sensor.

   The format of the syslog message that is sent by the IDP Sensor is as follows:

```
<day id>, <record id>, <timeReceived>, <timeGenerated>, <domain>, <domainVersion>,
<deviceName>, <deviceIpAddress>, <category>, <subcategory>,<src zone>, <src intface>, <src
addr>, <src port>, <nat src addr>, <nat src port>, <dstzone>, <dst intface>, <dst addr>,
<dst port>, <nat dst addr>, <nat dst port>,<protocol>, <rule domain>, <rule domainVersion>,
<policyname>, <rulebase>, <rulenumber>, <action>, <severity>, <is alert>, <elapsed>, <bytes
in>, <bytes out>, <bytestotal>, <packet in>, <packet out>, <packet total>, <repeatCount>,
<hasPacketData>, <varData Enum>, <misc-str>, <user str>, <application str>, <uri str>
```

   See the following syslog example:

```
[syslog@juniper.net dayId="20061012" recordId="0" timeRecv="2006/10/12 21:52:21"
timeGen="2006/10/12 21:52:21" domain="" devDomVer2="0" device_ip="<IP_address>"
cat="Predefined" attack="TROJAN:SUBSEVEN:SCAN" srcZn="NULL" srcIntf="NULL"
srcAddr="<Source_IP_address>" srcPort="63396" natSrcAddr="NULL" natSrcPort="0" dstZn="NULL"
dstIntf="NULL" dstAddr="<Destination_IP_address>" dstPort="27374" natDstAddr="NULL"
natDstPort="0" protocol="TCP" ruleDomain="" ruleVer="5" policy="Policy2" rulebase="IDS"
ruleNo="4" action="NONE" severity="LOW" alert="no" elaspedTime="0" inbytes="0" outbytes="0"
totBytes="0" inPak="0" outPak="0" totPak="0" repCount="0" packetData="no" varEnum="31"
misc="<017>'interface=eth2" user="NULL" app="NULL" uri="NULL"]
```

Configure a log source

Juniper NSM is a central management server for Juniper IDP. You can configure IBM QRadar to collect and represent the Juniper IDP alerts as coming from a central NSM, or QRadar can collect syslog from the individual Juniper IDP device.

To configure QRadar to receive events from Juniper Networks Secure Access device:

From the **Log Source Type** list, select **Juniper Networks Intrusion Detection and Prevention (IDP)**.

. For more information about Juniper IDP, see your *Network and Security Manager* documentation.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Juniper Networks Infranet Controller

The Juniper Networks Infranet Controller DSM for IBM QRadar is now known as Pulse Secure Infranet Controller.

Related concepts

"Pulse Secure Infranet Controller" on page 1379
The Pulse Secure Infranet Controller DSM for IBM QRadar accepts DHCP events by using syslog. QRadar records all relevant events from a Pulse Secure Infranet Controller.

Juniper Networks Firewall and VPN

The Juniper Networks Firewall and VPN DSM for IBM QRadar accepts Juniper Firewall and VPN events by using UDP syslog.

About this task

QRadar records all relevant firewall and VPN events.

Note: TCP syslog is not supported. You must use UDP syslog.

You can configure your Juniper Networks Firewall and VPN device to export events to QRadar.

Procedure

1. Log in to your **Juniper Networks Firewall and VPN** user interface.
2. Select **Configuration** > **Report Settings** > **Syslog**.
3. Select the **Enable Syslog Messages** check box.
4. Type the IP address of your QRadar Console or Event Collector.
5. Click **Apply**.

   You are now ready to configure the log source in QRadar.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring IBM QRadar to receive events

About this task

You can configure QRadar to receive events from a Juniper Networks Firewall and VPN device.

Procedure

From the **Log Source Type** list, select **Juniper Networks Firewall and VPN** option.

For more information about your Juniper Networks Firewall and VPN device, see your Juniper documentation.

Juniper Networks Firewall sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Juniper Networks Firewall and VPN sample message when you use the syslog protocol

The following sample event message shows that a user is successfully added to a group.

```
<164>TSSP-IM-VFW-008: NetScreen device_id=TSSP-IM-VFW-008  [Root]system-warning-00515: Admin user
expect has logged on via Telnet from 10.12.2.5:37314 (2012-07-25 11:50:21)
```

```
<164>TSSP-IM-VFW-008: NetScreen device_id=TSSP-IM-VFW-008  [Root]system-warning-00515: Admin
user expect has logged on via Telnet from 10.12.2.5:37314 (2012-07-25 11:50:21)
```

Table 682. Highlighted fields

QRadar field name	Highlighted payload field name
Source IP	**10.12.2.5**
Source Port	**37314**
Event Category	**NetScreen device_id**
Event Name	**Admin** + **logged on via Telnet**
Event ID	**Admin** + **user** + **logged on via Telnet**

Juniper Networks Junos OS

The Juniper Junos OS Platform DSM for IBM QRadar accepts events that use syslog, structured-data syslog, or PCAP (SRX Series only). QRadar records all valid syslog or structured-data syslog events.

About this task

The Juniper Junos OS Platform DSM supports the following Juniper devices that are running Junos OS:

- Juniper M Series Multiservice Edge Routing
- Juniper MX Series Ethernet Services Router
- Juniper T Series Core Platform
- Juniper SRX Series Services Gateway

For information on configuring PCAP data that uses a Juniper Networks SRX Series appliance, see "Configure the PCAP Protocol" on page 1079.

Note: For more information about structured-data syslog, see RFC 5424 at the Internet Engineering Task Force: http://www.ietf.org/

Before you configure QRadar to integrate with a Juniper device, you must forward data to QRadar using syslog or structured-data syslog.

Procedure

1. Log in to your Juniper platform command-line interface (CLI).
2. Include the following syslog statements at the `set system` hierarchy level:

```
[set system] syslog {host (hostname) {facility <severity>; explicit-
priority; any any; authorization any; firewall any;
```

```
} source-address source-address; structured-data {brief;} }
```

The following table lists and describes the configuration setting variables to be entered in the syslog statement.

List of Syslog Configuration Setting Variables	
Parameter	**Description**
host	Type the IP address or the fully qualified host name of your QRadar.
Facility	Define the severity of the messages that belong to the named facility with which it is paired. Valid severity levels are: • Any • None • Emergency • Alert • Critical • Error • Warning • Notice • Info Messages with the specified severity level and higher are logged. The levels from emergency through info are in order from highest severity to lowest.
Source-address	Type a valid IP address configured on one of the router interfaces for system logging purposes. The source-address is recorded as the source of the syslog message send to QRadar. This IP address is specified in the **host** host name statement `set system syslog` hierarchy level; however, this is not for messages directed to the other routing engine, or to the TX Matrix platform in a routing matrix.
structured-data	Inserts structured-data syslog into the data.

You can now configure the log source in QRadar.

The following devices are auto discovered by QRadar as a Juniper Junos OS Platform devices:

- Juniper M Series Multiservice Edge Routing
- Juniper MX Series Ethernet Services Router
- Juniper SRX Series
- Juniper EX Series Ethernet Switch
- Juniper T Series Core Platform

Note: Due to logging similarities for various devices in the JunOS family, expected events might not be received by the correct log source type when your device is automatically discovered. Review the automatically created log source for your device and then adjust the configuration manually. You can add any missed log source type or remove any incorrectly added log source type.

Related concepts

"TLS Syslog protocol configuration options" on page 227

Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Syslog log source parameters for Juniper Junos OS

If QRadar does not automatically detect the log source, add a Juniper Junos OS log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Juniper Junos OS:

Table 683. Syslog log source parameters for the Juniper Junos OS DSM

Parameter	Value
Log Source type	• **Juniper JunOS Platform** • **Juniper M-Series Multiservice Edge Routing** • **Juniper MX-Series Ethernet Services Router** • **Juniper SRX-series** • **Juniper T-Series Core Platform**
Protocol Configuration	Syslog

For more information about your Juniper device, see your vendor documentation.

Related tasks

"Adding a log source" on page 5

Configure the PCAP Protocol

The Juniper SRX Series appliance supports forwarding of packet capture (PCAP) and syslog data to IBM QRadar.

Syslog data is forwarded to QRadar on port 514. The IP address and outgoing PCAP port number are configured on the Juniper Networks SRX Series appliance interface. The Juniper Networks SRX Series appliance must be configured in the following format to forward PCAP data:

<IP Address>:*<Port>*

Where,

- *<IP Address>* is the IP address of QRadar.
- *<Port>* is the outgoing port address for the PCAP data.

Note:

QRadar supports receiving PCAP data only from a single Juniper Networks SRX Series appliance for each event collector.

For more information about Configuring Packet Capture, see your *Juniper Networks Junos OS documentation*.

You are now ready to configure the new Juniper Networks SRX Log Source with PCAP protocol in QRadar.

Related concepts

"PCAP Syslog Combination log source parameters for Juniper SRX Series" on page 1080

PCAP Syslog Combination log source parameters for Juniper SRX Series

If QRadar does not automatically detect the log source, add a Juniper SRX Series log source on the QRadar Console by using the PCAP Syslog Combination protocol.

QRadar detects the syslog data and adds the log source automatically. The PCAP data can be added to QRadar as Juniper SRX Series Services Gateway log source by using the PCAP Syslog combination protocol. Adding the PCAP Syslog Combination protocol after QRadar auto discovers the Junos OS syslog data adds a log source to your existing log source limit. Deleting the existing syslog entry, then adding the PCAP Syslog Combination protocol adds both syslog and PCAP data as single log source.

When using the PCAP Syslog Combination protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect PCAP Syslog Combination events from Juniper SRX Series:

Table 684. PCAP Syslog Combination log source parameters for the Juniper SRX Series DSM

Parameter	Value
Log Source type	Juniper SRX-series Services Gateway

For a complete list of PCAP Syslog Combination protocol parameters and their values, see c_logsource_PCAPprotocol.dita.

Related tasks

"Adding a log source" on page 5

Juniper Junos OS sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Juniper MX-Series Ethernet Services Router sample message when you use the Syslog protocol

The following sample event message shows that a member is successfully added to a group.

```
<166>Oct 14 10:16:59 juniper.mxseries.test (FPC Slot 5, PIC Slot 2) 2019-10-14
08:16:59: WifiAuleU5{WifiAuleU5A}JSERVICES_SESSION_CLOSE: application:none, domain.2051
10.253.200.191:39718 [10.253.203.241:2268] ->  10.255.78.72:80 (TCP)
```

Table 685. Highlighted fields

QRadar field name	Highlighted payload field name
Log Source Time	**Oct 14 10:16:59**
Event ID	**JSERVICES_SESSION_CLOSE**
IP address	**10.253.200.191**
Source Port	**39718**

Juniper Networks Network and Security Manager

The Juniper Networks Network and Security Manager (NSM) DSM for IBM QRadar accepts Juniper Networks NSM and Juniper Networks Secure Service Gateway (SSG) logs. All Juniper SSG logs must

be forwarded through Juniper NSM to QRadar. All other Juniper devices logs can be forwarded directly to QRadar.

For more information on advanced filtering of Juniper Networks NSM logs, see your *Juniper Networks* vendor documentation.

To integrate a Juniper Networks NSM device with QRadar, you must complete the following tasks:

- "Configuring Juniper Networks NSM to export logs to syslog" on page 1081
- "Juniper NSM log source parameters for Juniper Networks Network and Security Manager" on page 1081

Configuring Juniper Networks NSM to export logs to syslog

Juniper Networks NSM uses the syslog server to export qualified log entries to syslog.

About this task

Configuring the syslog settings for the management system defines only the syslog settings for the management system. It does not export logs from the individual devices. You can enable the management system to export logs to syslog.

Procedure

1. Log in to the **Juniper Networks NSM** user interface.
2. From the **Action Manager** menu, select **Action Parameters**.
3. Type the IP address for the syslog server that you want to send qualified logs.
4. Type the syslog server facility for the syslog server to which you want to send qualified logs.
5. From the **Device Log Action Criteria** node, select the **Actions** tab.
6. Select **Syslog Enable** for **Category**, **Severity**, and **Action**.

   You are now ready to configure the log source in IBM QRadar.

Juniper NSM log source parameters for Juniper Networks Network and Security Manager

If QRadar does not automatically detect the log source, add a Juniper Networks Network and Security Manager log source on the QRadar Console by using the Juniper NSM protocol.

When using the Juniper NSM protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Juniper NSM events from Juniper Networks Network and Security Manager:

Table 686. Juniper NSM log source parameters for the Juniper Networks Network and Security Manager DSM

Parameter	Value
Log Source Type	Juniper Networks Network and Security Manager
Protocol Configuration	Juniper NSM
Log Source Identifier	Type the IP address or host name for the log source. The **Log Source Identifier** must be unique for the log source type.
IP	Type the IP address or host name of the Juniper Networks NSM server.

Table 686. Juniper NSM log source parameters for the Juniper Networks Network and Security Manager DSM (continued)	
Parameter	**Value**
Inbound Port	Type the **Inbound Port** to which the Juniper Networks NSM sends communications. The valid range is 0 - 65536. The default is 514.
Redirection Listen Port	Type the port to which traffic is forwarded. The valid range is 0 - 65,536. The default is 516.
Use NSM Address for Log Source	Select this check box to use the Juniper NSM management server IP address instead of the log source IP address. By default, the check box is selected.

Note: In the QRadar interface, the Juniper NSM protocol configuration provides the option to use the Juniper Networks NSM IP address by selecting the **Use NSM Address for Log Source** check box. If you wish to change the configuration to use the originating IP address (clear the check box), you must log in to your QRadar Console, as a root user, and restart the Console (for an all-in-one system) or the Event Collector hosting the log sources (in a distributed environment) by using the **shutdown -r now** command.

For a complete list of Juniper NSM parameters and their values, see c_logsource_NSMprotocol.dita.

Related tasks

"Adding a log source" on page 5

Juniper Networks Secure Access

Juniper Networks Secure Access is now known as Pulse Secure Pulse Connect Secure.

Related concepts

"Pulse Secure Pulse Connect Secure" on page 1379

The IBM QRadar DSM for Pulse Secure Pulse Connect Secure collects syslog and WebTrends Enhanced Log File (WELF) formatted events from Pulse Secure Pulse Connect Secure mobile VPN devices.

Juniper Networks Security Binary Log Collector

The Juniper Security Binary Log Collector DSM for IBM QRadar can accept audit, system, firewall, and intrusion prevention system (IPS) events in binary format from Juniper SRX or Juniper Networks J Series appliances.

The Juniper Networks binary log file format is intended to increase performance when large amounts of data are sent to an event log. To integrate your device with QRadar, you must configure your Juniper appliance to stream binary formatted events, then configure a log source in QRadar.

Configuring the Juniper Networks Binary Log Format

The binary log format from Juniper SRX or J Series appliances are streamed to IBM QRadar by using the UDP protocol. You must specify a unique port for streaming binary formatted events, because the standard syslog port for QRadar cannot understand binary formatted events.

About this task

The default port that is assigned to QRadar for receiving streaming binary events from Juniper appliances is port 40798.

Note: The Juniper Binary Log Collector DSM supports only events that are forwarded in Streaming mode. The Event mode is not supported.

Procedure

1. Log in to your Juniper SRX or J Series by using the command-line interface (CLI).
2. Type the following command to edit your device configuration:

   ```
   configure
   ```
3. Type the following command to configure the IP address and port number for streaming binary formatted events:

   ```
   set security log stream <Name> host <IP address> port <Port>
   ```

   Where:

   - <*Name*> is the name that is assigned to the stream.
   - <*IP address*> is the IP address of your QRadar Console or Event Collector.
   - <*Port*> is a unique port number that is assigned for streaming binary formatted events to QRadar. By default, QRadar listens for binary streaming data on port 40798. For a list of ports that are used by *QRadar*, see the IBM QRadar *Common Ports List technical note*.
4. Type the following command to set the security log format to binary:

   ```
   set security log stream <Name> format binary
   ```

   Where: <*Name*> is the name that you specified for your binary format stream in "Configuring the Juniper Networks Binary Log Format" on page 1082.
5. Type the following command to enable security log streaming:

   ```
   set security log mode stream
   ```
6. Type the following command to set the source IP address for the event stream:

   ```
   set security log source-address <IP address>
   ```

   Where: <*IP address*> is the IP address of your Juniper SRX Series or Juniper J Series appliance.
7. Type the following command to save the configuration changes:

   ```
   commit
   ```
8. Type the following command to exit the configuration mode:

   ```
   exit
   ```

What to do next

The configuration of your Juniper SRX or J Series appliance is complete. You can now configure a log source in QRadar.

Juniper Security Binary Log Collector log source parameters for Juniper Networks Security Binary Log Collector

If QRadar does not automatically detect the log source, add a Juniper Security Binary Log Collector log source on the QRadar Console by using the Juniper Security Binary Log Collector protocol.

When using the Juniper Security Binary Log Collector protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Juniper Security Binary Log Collector events from Juniper Security Binary Log Collector:

Table 687. Juniper Security Binary Log Collector log source parameters for the Juniper Security Binary Log Collector DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	Juniper Security Binary Log Collector
Protocol Configuration	Juniper Security Binary Log Collector
Log Source Identifier	Type an IP address or host name to identify the log source. The identifier address is the Juniper SRX or J Series appliance that generates the binary event stream.
Binary Collector Port	Specify the port number that is used by the Juniper Networks SRX or J Series appliance to forward incoming binary data to QRadar. The UDP port number for binary data is the same port that is configured in "Configuring the Juniper Networks Binary Log Format" on page 1082, "Configuring the Juniper Networks Binary Log Format" on page 1082. If you edit the outgoing port number for the binary event stream from your Juniper Networks SRX or J Series appliance, you must also edit your Juniper log source and update the **Binary Collector Port** parameter in QRadar. To edit the port: 1. In the **Binary Collector Port** field, type the new port number for receiving binary event data. 2. Click **Save**. The port update is complete and event collection starts on the new port number.

For a complete list of Juniper Networks Security Binary Log Collector parameters and their values, see c_logsource_JuniperSBLCprotocol.dita.

Related tasks

"Adding a log source" on page 5

Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

QRadar records all successful and unsuccessful login attempts. You can integrate Juniper Networks Steel-Belted Radius with QRadar by using one of the following methods:

- Configure Juniper Steel Belted-Radius to use WinCollect on Microsoft Windows operating systems. For more information, go to Configuring Juniper Networks Steel-Belted Radius to forward Windows events to QRadar.
- Configure Juniper Steel-Belted Radius on Linux-based operating systems.

- Configuring Juniper Steel-Belted Radius by using the Syslog protocol.
- Configuring Juniper Steel-Belted Radius by using the TLS syslog protocol.
- Configuring Juniper Steel-Belted Radius by using the Log file protocol.

Related concepts

Configure Juniper Networks Steel-Belted Radius to forward Windows events to QRadar
You can forward Windows events to IBM QRadar by using WinCollect.

Related tasks

Configuring Juniper Networks Steel-Belted Radius to forward Syslog events to QRadar
Before you can add a log source in QRadar, configure your Juniper Networks Steel-Belted Radius device to send Syslog events to QRadar.

Configuring a Juniper Steel-Belted Radius log source by using the Syslog protocol
If you want to collect Juniper Steel-Belted Radius logs from a Juniper Steel-Belted Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Syslog protocol.

Configuring a Juniper Networks Steel-Belted Radius log source by using the TLS syslog protocol
If you want to collect Juniper Steel Belted-Radius logs from a Juniper Steel Belted-Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the TLS syslog protocol.

Configuring a Juniper Steel-Belted Radius log source by using the Log File protocol
If you want to collect Juniper Steel-Belted Radius logs from Juniper Steel-Belted Radius, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Log File protocol.

Related reference

Juniper Networks Steel-Belted Radius DSM specifications
The following table describes the specifications for the Juniper Steel-Belted Radius DSM.

Juniper Networks Steel-Belted Radius DSM specifications

The following table describes the specifications for the Juniper Steel-Belted Radius DSM.

Table 688. Juniper Networks Steel-Belted Radius DSM specifications

Specification	**Value**
Manufacturer	Juniper Networks
DSM name	Juniper Steel-Belted Radius
RPM file name	`DSM-JuniperSteelBeltedRadius-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	5.x
Protocol	Syslog, TLS Syslog, Log File, and WinCollect Juniper SBR
Event format	
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	Yes

Related concepts

Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

Configure Juniper Networks Steel-Belted Radius to forward Windows events to QRadar

You can forward Windows events to IBM QRadar by using WinCollect.

To forward Windows events by using WinCollect, install WinCollect agent on a Windows host. Download the WinCollect agent setup file from the IBM Support website (https://www.ibm.com/support). Add a Juniper Steel-Belted Radius log source and assign it to the WinCollect agent.

The following table describes the parameters that require specific values for the WinCollect log source parameters.

Table 689. Juniper Steel-Belted Radius WinCollect Juniper SBR log source parameters

Parameter	Value
Log Source type	**Juniper Steel-Belted Radius**
Protocol Configuration	**WinCollect Juniper SBR**
Log Source Identifier	The IP address or host name of the Windows device from which you want to collect Windows events. The log source identifier must be unique for the log source type.
Local System	Select the **Local System** check box to disable the remote collection of events for the log source. The log source uses local system credentials to collect and forward logs to QRadar. You need to configure the **Domain**, **Username**, and **Password** parameters if remote collection is required.
Polling Interval	The interval, in milliseconds, between times when WinCollect polls for new events.
Enable Active Directory Lookups	Do not select the check box.
WinCollect**Agent**	Select your WinCollect agent from the list.
Target Internal Destination	Use any managed host with an event processor component as an internal destination.

For more information about WinCollect log source parameters, see the Common WinCollect log source parameters documentation (https://www.ibm.com/docs/en/SS42VS_SHR/com.ibm.wincollect.doc/r_ug_wincollect_comon_parameters.html).

Related concepts

Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring Juniper Networks Steel-Belted Radius to forward Syslog events to QRadar

Before you can add a log source in QRadar, configure your Juniper Networks Steel-Belted Radius device to send Syslog events to QRadar.

Procedure

1. Use SSH to log in to your Juniper Steel-Belted Radius device, as a root user.
2. Edit the following file:

   `/etc/syslog.conf`
3. Add the following information:

   <*facility*>.<*priority*>@<*IP address*>

   Where:

   - <*facility*> is the syslog facility, for example, local3.
   - <*priority*> is the syslog priority, for example, info.
   - <*IP address*> is the IP address of QRadar.
4. Save the file.
5. From the command-line, type the following command to restart syslog:

   `service syslog restart`

What to do next

You are now ready to add a log source in QRadar.

Related concepts

Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

Related tasks

“Configuring a Juniper Steel-Belted Radius log source by using the Syslog protocol” on page 1087

If you want to collect Juniper Steel-Belted Radius logs from a Juniper Steel-Belted Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Syslog protocol.

Configuring a Juniper Steel-Belted Radius log source by using the Syslog protocol

If you want to collect Juniper Steel-Belted Radius logs from a Juniper Steel-Belted Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Syslog protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.

   - DSMCommon RPM
   - Juniper Steel Belt Radius DSM RPM
   -
   -
2. Configure your Juniper Steel-Belted Radius device to send syslog events to QRadar.

3. Add a Syslog log source on the QRadar Console.

   The following table describes the parameters that require specific values to collect Syslog events from Juniper Steel-Belted Radius by using the Syslog protocol:

Table 690. Syslog protocol log source parameters	
Parameter	**Description**
Log Source Type	Juniper Steel-Belted Radius
Protocol Configuration	Syslog

Related concepts

Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring a Juniper Networks Steel-Belted Radius log source by using the TLS syslog protocol

If you want to collect Juniper Steel Belted-Radius logs from a Juniper Steel Belted-Radius device, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the TLS syslog protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - TLS Syslog protocol RPM
   - JuniperSteelBeltedRadius DSM RPM
2. Add a TLS Syslog log source on the QRadar Console.

   The following table describes the parameters that require specific values to collect events from Juniper Steel-Belted Radius by using the TLS syslog protocol:

Table 691. TLS syslog protocol log source parameters	
Parameter	**Description**
Log Source Type	**Juniper Steel-Belted Radius**
Protocol Configuration	**TLS Syslog**

Related concepts

Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

"TLS Syslog protocol configuration options" on page 227

Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring a Juniper Steel-Belted Radius log source by using the Log File protocol

If you want to collect Juniper Steel-Belted Radius logs from Juniper Steel-Belted Radius, configure a log source on the QRadar Console so that Juniper Steel-Belted Radius can communicate with QRadar by using the Log File protocol.

Procedure

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Log File protocol RPM
   - JuniperSteelBeltedRadius DSM RPM
2. Add a Log File protocol log source on the QRadar Console.

   The following table describes the parameters that require specific values to collect Juniper Steel-Belted Radius events from Juniper Steel-Belted Radius by using the Log File protocol:

Table 692. Log File protocol log source parameters

Parameter	Description
Log Source Type	**Juniper Steel-Belted Radius**
Protocol Configuration	**Log File**
Service Type	**FTP**
Remote Directory	The default directory is `/opt/JNPRsbr/radius/authReports/`
FTP File Pattern	`.*\.csv`
Event Generator	**Juniper SBR**

Related concepts

Juniper Networks Steel-Belted Radius

The Juniper Steel-Belted Radius DSM for IBM QRadar accepts syslog forwarded events from Windows when you run the WinCollect agent. You can also collect events from Linux-based operating systems by using the Syslog, TLS syslog, or the Log File protocol.

"Log File protocol configuration options" on page 155

To receive events from remote hosts, configure a log source to use the Log File protocol.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Juniper Steel Belted Radius sample event message

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Juniper Steel Belted Radius sample message when you use the Syslog protocol

The following sample event message shows a successful authentication.

```
<13>Oct 30 18:13:36 juniper.sbr.test AgentDevice=JuniperSBR    AgentLogFile=accepts
Date=2007-10-30    Time=12:25:53    RADIUS-Client=Testt    Full-Name=Test T
User-Name=Test    Nas-IP-Address=10.100.10.3    Calling-Station-Id=192.168.2.1    NAS-Port-
Type=1115551213
```

Table 693. Highlighted fields in the Juniper Steel Belted Radius sample event

QRadar field name	Highlighted values in the event payload
Event ID	accepts
Event Category	JuniperSBR
Source IP	10.100.10.3

Juniper Networks vGW Virtual Gateway

The Juniper Networks vGW Virtual Gateway DSM for IBM QRadar accepts events by using syslog and NetFlow from your vGW management server or firewall.

The Juniper Networks vGW Virtual Gateway product is end of life (EOL), and is no longer supported by Juniper.

About this task

QRadar records all relevant events, such as admin, policy, IDS logs, and firewall events. Before you configure a Juniper Networks vGW Virtual Gateway in QRadar, you must configure vGW to forward syslog events.

Procedure

1. Log in to your Juniper Networks vGW user interface.
2. Select **Settings**.
3. From **Security Settings**, select **Global**.
4. From **External Logging**, select one of the following options:
   - **Send Syslog from vGW management server** - Central logging with syslog event provided from a management server.
   - **Send Syslog from Firewalls** - Distribute logging with each Firewall Security VM providing syslog events.

   If you select the option **Send Syslog from vGW management server**, all events that are forwarded to QRadar contain the IP address of the vGW management server.
5. Type values for the following parameters:

Table 694. Syslog parameters	
Parameter	**Description**
Syslog Server	Type the IP address of your vGW management server if you selected to **Send Syslog from vGW management server**. Or, type the IP address of QRadar if you selected **Send Syslog from Firewalls**.
Syslog Server Port	Type the port address for syslog. This port is typically port 514.

6. From the **External Logging** pane, click **Save**.

   Only the changes that are made to the **External Logging** section are stored when you click **Save**. Any changes that are made to NetFlow require that you save by using the button within **NetFlow Configuration** section.

7. From the **NetFlow Configuration** pane, select the **enable** check box.

   NetFlow does not support central logging from a vGW management server. From the **External Logging** section, you must select the option **Send Syslog from Firewalls**.

8. Type values for the following parameters:

Table 695. Netflow parameters	
Parameter	**Description**
NetFlow collector address	Type the IP address of QRadar.
Syslog Server Port	Type a port address for NetFlow events.

   Note: QRadar typically uses port 2055 for NetFlow event data on QFlow Collectors. You must configure a different NetFlow collector port on your Juniper Networks vGW Series Virtual Gateway for NetFlow.

9. From the **NetFlow Configuration**, click **Save**.
10. You can now configure the log source in QRadar.

    QRadar automatically detects syslog events that are forwarded from Juniper Networks vGW. If you want to manually configure QRadar to receive syslog events:

    From the **Log Source Type** list, select **Juniper vGW**.

    For more information, see your *Juniper Networks vGW* documentation.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Juniper Networks Junos WebApp Secure

The Juniper WebApp Secure DSM for IBM QRadar accepts events that are forwarded from Juniper Junos WebApp Secure appliances by using syslog.

Juniper Junos WebApp Secure provides incident logging and access logging events to QRadar. Before you can receive events in QRadar, you must configure event forwarding on your Juniper Junos WebApp Secure, then define the events that you want to forward.

Configuring syslog forwarding

To configure a remote syslog server for Juniper Junos WebApp Secure, you must use SSH to connect to a configuration interface. You can use the configuration interface to set up or configure core settings on your Juniper Junos WebApp Secure appliance.

Procedure

1. Use SSH on port 2022 to log in to your Juniper Junos WebApp device.

   `https://<IP address>:<port>`

   Where:

   - <*IP address*> is the IP address of your Juniper Junos WebApp Secure appliance.
   - <*Port*> is the port number of your Juniper Junos WebApp Secure appliance configuration interface.

   The default SSH configuration port is 2022.
2. From the **Choose a Tool** menu, select **Logging**.
3. Click **Run Tool**.
4. From the **Log Destination** menu, select **Remote Syslog Server**.
5. In the **Syslog Server** field, type the IP address of your QRadar Console or Event Collector.
6. Click **Save**.
7. From the **Choose a Tool** menu, select **Quit**.
8. Type `Exit` to close your SSH session.

What to do next

You are now ready to configure event logging on your Juniper Junos WebApp Secure appliance.

Configuring event logging

The Juniper Junos WebApp Secure appliance must be configured to determine which logs are forwarded to IBM QRadar.

Procedure

1. Using a web browser, log in to the configuration site for your Juniper Junos WebApp Secure appliance.

   `https://<IP address>:<port>`

   Where:

   - <*IP address*> is the IP address of your Juniper Junos WebApp Secure appliance.
   - <*Port*> is the port number of your Juniper Junos WebApp Secure appliance.

     The default configuration uses a port number of 5000.
2. From the navigation menu, select **Configuration Manager**.
3. From the configuration menu, select **Basic Mode**.
4. Click the **Global Configuration** tab and select **Logging**.
5. Click the link **Show Advanced Options**.
6. Configure the following parameters:

Table 696. Juniper Junos WebApp Secure logging parameters	
Parameter	**Description**
Access logging: Log Level	Click this option to configure the level of information that is logged when access logging is enabled. The options include the following levels: • **0** - Access logging is disabled. • **1** - Basic logging. • **2** - Basic logging with headers. • **3** - Basic logging with headers and body. **Note:** Access logging is disabled by default. It is suggested that you enable access logging only for debugging purposes. For more information, see your *Juniper Junos WebApp Secure documentation*.
Access logging: Log requests before processing	Click this option and select **True** to log the request before it is processed, then forward the event to QRadar.
Access logging: Log requests to access log after processing	Click this option and select **True** to log the request after it is processed. After Juniper Junos WebApp Secure processes the event, then it is forwarded to QRadar.
Access logging: Log responses to access log after processing	Click this option and select **True** to log the response after it is processed. After Juniper Junos WebApp Secure processes the event, then the event is forwarded to QRadar.
Access logging: Log responses to access log before processing	Click this option and select **True** to log the response before it is processed, then forward the event to QRadar.
Incident severity log level	Click this option to define the severity of the incident events to log. All incidents at or above the level that is defined are forwarded to QRadar. The options include the following levels: • **0** - Informational level and later incident events are logged and forwarded. • **1** - Suspicious level and later incident events are logged and forwarded. • **2** - Low level and later incident events are logged and forwarded. • **3** - Medium level and later incident events are logged and forwarded. • **4** - High level and later incident events are logged and forwarded.
Log incidents to the syslog	Click this option and select **Yes** to enable syslog forwarding to QRadar.

The configuration is complete. The log source is added to QRadar as Juniper Junos WebApp Secure events are automatically discovered. Events that are forwarded to QRadar by Juniper Junos WebApp Secure are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Juniper Networks Junos WebApp Secure

If QRadar does not automatically detect the log source, add a Juniper Networks Junos WebApp Secure log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Juniper Networks Junos WebApp Secure:

Table 697. Syslog log source parameters for the Juniper Networks Junos WebApp Secure DSM

Parameter	Value
Log Source type	Type a name for your log source.
Log Source type	Type a description for the log source.
Log Source type	Juniper Junos WebApp Secure
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Juniper Junos WebApp Secure appliance.

Related tasks

"Adding a log source" on page 5

Juniper Junos WebApp Secure sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Juniper Junos WebApp Secure sample message when you use the Syslog protocol

The following sample event message shows a failed login.

```
Jun 8 23:55:56 demo [INFO][mws-security-alert][Thread-4336050] MKS_Category="Security
Incident" MKS_Type="Missing Host Header" MKS_Severity="2" MKS_ProfileName="profile_name"
MKS_SrcIP="10.154.42.194" MKS_pubkey="YRnxm8SHts7mlQPIYFGk" MKS_useragent="" MKS_url="http://
localhost:80/" MKS_count="1"
```

Table 698. Highlighted fields in the Juniper Junos WebApp Secure sample event

QRadar field name	Highlighted payload field name
Event ID	MKS_Type
Event Category	In QRadar, the value is **JuniperMykonosWebSecurity**.
Source IP	MKS_SrcIP
Username	MKS_ProfileName

Juniper Networks WLC Series Wireless LAN Controller

IBM QRadar can collect and categorize syslog events from Juniper Networks WLC Series Wireless LAN Controllers.

To collect syslog events, you must configure your Juniper Networks Wireless LAN Controller to forward syslog events to QRadar. Administrators can use either the RingMaster interface or the command-line interface to configure syslog forwarding for their Juniper Networks Wireless LAN Controller appliance.

QRadar automatically discovers and creates log sources for syslog events that are forwarded from Juniper Networks WLC Series Wireless LAN Controllers. QRadar supports syslog events from Juniper WLAN devices that run on Mobility System Software (MSS) V7.6.

To integrate Juniper WLC events with QRadar, administrators can complete the following tasks:

1. On your Juniper WLAN appliance, configure syslog server.
2. Use one of the following methods:
   - To use the RingMaster user interface to configure a syslog server, see "Configuring a syslog server from the Juniper WLC user interface" on page 1095.
   - To use the command-line interface to configure a syslog server, see "Configuring a syslog server with the command-line interface for Juniper WLC" on page 1095.
3. On your QRadar system, verify that the forwarded events are automatically discovered.

Configuring a syslog server from the Juniper WLC user interface

To collect events, you must configure a syslog server on your Juniper WLC system to forward syslog events to IBM QRadar.

Procedure

1. Log in to the RingMaster software.
2. From the **Organizer** panel, select a Wireless LAN Controller.
3. From the **System** panel, select **Log**.
4. From the **Task** panel, select **Create Syslog Server**.
5. In the **Syslog Server** field, type the IP address of your QRadar system.
6. In the **Port** field, type 514.
7. From the **Severity Filter** list, select a severity.

   Logging debug severity events can negatively affect system performance on the Juniper WLC appliance. It is a good practice for administrators to log events at the error or warning severity level and slowly increase the level to get the data you need. The default severity level is error.
8. From the **Facility Mapping** list, select a facility between local 0 - local 7.
9. Click **Finish**.

   As events are generated by the Juniper WLC appliance, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded to QRadar. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console. The **Log Activity** tab displays events from the Juniper WLC appliance.

Configuring a syslog server with the command-line interface for Juniper WLC

To collect events, configure a syslog server on your Juniper WLC system to forward syslog events to IBM QRadar.

Procedure

1. Log in to the command-line interface of the Juniper WLC appliance.
2. To configure a syslog server, type the following command:

```
set log server <ip-addr> [port 514 severity <severity-level> local-facility
<facility-level>]
```

Example:

set log server 1.1.1.1 port 514 severity error local-facility local0.

3. To save the configuration, type the following command:

   ```
   save configuration
   ```

   As events are generated by the Juniper WLC appliance, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded to QRadar. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created. The **Log Activity** tab displays events from the Juniper WLC appliance.

Chapter 90. Kisco Information Systems SafeNet/i

The IBM QRadar DSM for Kisco Information Systems SafeNet/i collects event logs from IBM i systems.

The following table identifies the specifications for the Kisco Information Systems SafeNet/i DSM:

Table 699. Kisco Information Systems SafeNet/i DSM specifications

Specification	**Value**
Manufacturer	Kisco Information Systems
DSM name	Kisco Information Systems SafeNet/i
RPM file name	`DSM-KiscoInformationSystemsSafeNetI-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V10.11
Protocol	Log File
Recorded event types	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Kisco Information Systems website (http://www.kisco.com/safenet/summary.htm)

To collect Kisco Information Systems SafeNet/i events, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Log File Protocol RPM
   - Kisco Information Systems SafeNet/i DSM RPM
2. Configure your Kisco Information Systems SafeNet/i device to communicate with QRadar.
3. Add a Kisco Information Systems SafeNet/i log source on the QRadar Console. The following table describes the parameters that require specific values for Kisco Information Systems SafeNet/i event collection:

Table 700. Kisco Information Systems SafeNet/i log source parameters

Parameter	**Value**
Log Source type	Kisco Information Systems SafeNet/i
Protocol Configuration	Log File
Service Type	FTP
Remote IP or Hostname	The IP or host name of Kisco Information systems SafeNet/i device.
Remote Port	21
Remote User	The IBM i User ID that you created for QRadar in Kisco Information Systems SafeNet/i.

Table 700. Kisco Information Systems SafeNet/i log source parameters (continued)	
Parameter	**Value**
Remote Directory	Leave this field empty.
FTP File Pattern	`.*`
FTP Transfer Mode	BINARY
Processor	NONE
Event Generator	LINEBYLINE
File Encoding	US-ASCII

Related tasks

Adding a DSM

Configuring Kisco Information Systems SafeNet/i to communicate with QRadar

To collect SafeNet/i events, configure your IBM i system to accept FTP GET requests from your QRadar through Kisco Information Systems SafeNet/i.

Adding a log source

Configuring Kisco Information Systems SafeNet/i to communicate with QRadar

To collect SafeNet/i events, configure your IBM i system to accept FTP GET requests from your QRadar through Kisco Information Systems SafeNet/i.

About this task

Use the following table when you configure the FTP access settings:

Table 701. FTP access settings	
Parameter	**Value**
Initial Name Format	*PATH
Initial List Format	*UNIX
Initial Library	*USRPRF
Initial Home Directory Path	The IFS directory

Procedure

1. Create an IFS directory on your IBM i system.
   a) Log in to your IBM i system.
   b) Create an IFS Directory to hold the Kisco Information Systems SafeNet/i QRadar alert files.

      Example: `/SafeNet/QRadar/`
   c) Set up a user profile for QRadar to use to FTP into the IFS Directory through SafeNet/i.

      Example: QRADARUSER
2. Configure FTP access for the QRadar user profile.
   a) Log in to Kisco Information Systems SafeNet/i.
   b) Type **GO SN7** and select **Work with User to Server Security**.
   c) Type the user profile name that you created for QRadar, for example, QRADARUSER.

d) Type 1 for the **FTP Server Request Validation *FTPSERVER** and **FTP Server Logon *FTPLOGON3** servers.

e) Press F3 and select **Work with User to FTP Statement Security** and type the user profile name again.

f) Type 1 for the **List Files** and **Receiving Files** FTP operations.

g) Press F4 and configure FTP access parameters for the user. See Table 701 on page 1098.

h) Press F3 and select **Work with User to Long Paths**.

i) Press F6 and provide the path to the IFS directory.

Ensure that the path is followed by an asterisk, for example, `/SafeNet/QRadar/*`

j) Type X under the **R** column.

k) Press F3 to exit.

3. Type `CHGRDRSET` and then press F4.
4. Configure the following parameters:

Paramter	Value
Activate QRADAR Integration	Yes
This Host Identifier	The IP address or host name of the IBM i system.
IFS Path to QRADAR Alert File	Use the following format: `/SafeNet/QRadar/`

5. Type `CHGNOTIFY` and press F4.
6. Configure the following parameters:

Parameter	Value
Alert Notification Status	On
Summarized Alerts?	Yes

Chapter 91. Kubernetes Auditing

The IBM QRadar DSM for Kubernetes collects auditing events from a Kubernetes master node Kube-apiserver.

To integrate Kubernetes with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Kubernetes Auditing DSM RPM
2. Configure your Kubernetes master node Kube-apiserver to send events to QRadar.
3. Create a copy of the audit policy file. For more information, see Kubernetes documentation about Audit Policy (https://kubernetes.io/docs/tasks/debug-application-cluster/audit/#audit-policy).
4. Configure rsyslog on your Kubernetes master hosted Linux system. For more information about configuring rsyslog, see Configuring rsyslog on a logging server (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/ch-viewing_and_managing_log_files#s1-configuring_rsyslog_on_a_logging_server).
5. If QRadar does not automatically detect the log source, add a Kubernetes Auditing log source on the QRadar Console.

Note: The Kubernetes auditing event payload can be over 32,000 bytes. The default QRadar syslog payload length is 4,096 bytes. You can increase the QRadar syslog payload size to 32,000 bytes. For more information about increasing the QRadar maximum payload size, see QRadar: TCP Syslog Maximum Payload Message Length for QRadar Appliances (https://www.ibm.com/support/pages/qradar-tcp-syslog-maximum-payload-message-length-qradar-appliances).

If Kubernetes audit events are larger than 32,000 bytes, the events are truncated by QRadar. To keep the events from being truncated, tune your Kubernetes audit polity to return less data.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5
“Configuring Kubernetes Auditing to communicate with QRadar” on page 1102
To collect all events from Kubernetes Auditing, you must specify IBM QRadar as the syslog server.

Kubernetes Auditing DSM specifications

When you configure Kubernetes Auditing, understanding the specifications for the Kubernetes Auditing DSM can help ensure a successful integration. For example, knowing what the supported version of Kubernetes is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Kubernetes Auditing DSM.

Table 702. Kubernetes Auditing DSM specifications

Specification	**Value**
Manufacturer	Kubernetes
DSM name	Kubernetes Auditing
RPM file name	DSM-*KubernetesAuditing-QRadar_version-build_number*.noarch.rpm
Supported version	Kubernetes API 1.19

Table 702. Kubernetes Auditing DSM specifications (continued)	
Specification	**Value**
Protocol	Syslog
Event format	JSON
Recorded event types	RequestReceived, ResponseStarted, ResponseComplete
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	Yes
More information	https://kubernetes.io/docs/tasks/debug-application-cluster/audit/

Configuring Kubernetes Auditing to communicate with QRadar

To collect all events from Kubernetes Auditing, you must specify IBM QRadar as the syslog server.

Before you begin

A Kubernetes cluster must be running on your system. For more information, see Kubernetes documentation about Creating a single control-plane cluster with kubeadm (https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/create-cluster-kubeadm/).

Create a copy of the Kubernetes audit policy file. For more information, see Kubernetes documentation about Audit Policy (https://kubernetes.io/docs/tasks/debug-application-cluster/audit/#audit-policy).

If you are using the Container or the Kubernetes content extensions, you need the QRadar audit policy file. For more information about the Container content extension, see Container (https://www.ibm.com/docs/en/qradar-common?topic=extensions-container). For more information about the Kubernetes content extension, see Kubernetes (https://www.ibm.com/docs/en/qradar-common?topic=extensions-kubernetes).

Make sure that rsyslog is installed and running on your system. For more information, see the rsyslog documentation (https://www.rsyslog.com).

About this task

Procedure

1. Use SSH to log in to your Kubernetes Auditing console.
2. In the `/etc/Kubernetes/maifests/kube-apiserver.yaml` file, define the **`audit-policy-file`** and **`audit-log-path`** parameters.

```
apiVersion: v1kind: Podmetadata:  creationTimestamp: null  labels:    component: kube-
apiserver    tier: control-plane  name: kube-apiserver  namespace: kube-systemspec:
containers:  - command:    - kube-apiserver    ...       - --audit-policy-file=/etc/kubernetes/
audit-policy.yaml    - --audit-log-path=/var/log/apiserver/audit.log    ...
```

3. Configure the `rsyslog /etc/rsyslog.conf` file to forward events that are logged in the `audit.log` file to QRadar.

```
#### MODULES ####…$ModLoad imfile# ### begin forwarding rule
###$InputFileName /var/log/apiserver/audit.log$InputFileSeverity notice$InputFileFacility
local0$InputRunFileMonitorlocal0.* @@QRADAR_EVENT_COLLECTOR_IP:514
```

4. Restart rsyslog by typing the following command: `service rsyslog restart`.

Kubernetes Auditing log source parameters

When you add a Kubernetes Auditing log source on the QRadar Console by using the Syslog protocol, there are specific parameters you must use.

The following table describes the parameters that require specific values to collect Syslog events from Kubernetes Auditing:

Table 703. Kubernetes Auditing Syslog log source parameters for the Kubernetes Auditing DSM

Parameter	Value
Log Source type	Kubernetes Auditing
Protocol Configuration	Syslog
Log Source Identifier	IP address or host name

Related tasks

"Adding a DSM" on page 4

Related information

"Adding a log source" on page 5

Kubernetes Auditing sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when you use the Syslog protocol for the Kubernetes Auditing DSM.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Table 704. Kubernetes Auditing sample message supported by the Kubernetes Auditing DSM

Event name	Low-level category	Sample log message
Read the specified endpoints	Read Activity Succeeded	<133>Oct 21 10:37:55 test.example.com k8s-audit: {"kind":"Event","apiVersion": "audit.k8s.io/ v1","level":"RequestResponse","auditID":"d30b40b8-4f6a-4219-9828-a7f732518541", "stage":"ResponseComplete","requestURI":"/api/v1/namespaces/default/endpoints/kubernetes", "verb":"get","user":{"username":"system:apiserver","uid":"0f440c21-a1c6-4ec3-84a4-50cd5dee2eb7", "groups":["system:masters"]},"sourceIPs":["::1"],"userAgent":"kube-apiserver/v1.15.2 (linux/amd64) kubernetes/f627830","objectRef": {"resource":"endpoints","namespace":"default","name":"kubernetes", "apiVersion":"v1"},"responseStatus":{"metadata": {},"code":200},"responseObject":{"kind":"Endpoints", "apiVersion":"v1","metadata": {"name":"kubernetes","namespace":"default","selfLink":"/api/v1/namespaces /default/endpoints/ kubernetes","uid":"1104e39a-46d2-4c35-92d2-5206dc6be4d2","resource Version":"156","creationTimestamp":"2019-10-21T13:18:48Z"},"subsets": [{"addresses":[{"ip":"192.0.2.0/24"}], "ports": [{"name":"https","port":6443,"protocol":"TCP"}]}],"requestReceived Timestamp":"2019-10-21T14:37:53.788926Z","stageTimestamp": "2019-10-21T14:37:53.789945Z","annotations":{"authorization.k8s.io/decision":"allow", "authorization.k8s.io/reason":""}} <133>Oct 21 10:37:55 test.example.com k8s-audit: {"kind":"Event","apiVersion":"audit.k8s.io/ v1","level":"RequestResponse","auditID":"d30b40b8-4f6a-4219-9828-a7f732518541","stage":"ResponseComplete","requestURI":"/api/v1/ namespaces/default/endpoints/kubernetes","verb":"get","user": {"username":"system:apiserver","uid":"0f440c21-a1c6-4ec3-84a4-50cd5dee2eb7","groups": ["system:masters"]},"sourceIPs":["::1"],"userAgent":"kube-apiserver/v1.15.2 (linux/amd64) kubernetes/f627830","objectRef": {"resource":"endpoints","namespace":"default","name":"kubernetes","apiVersion":"v1"},"responseStatus":{"metadata": {},"code":200},"responseObject": {"kind":"Endpoints","apiVersion":"v1","metadata": {"name":"kubernetes","namespace":"default","selfLink":"/api/v1/ namespaces/default/endpoints/ kubernetes","uid":"1104e39a-46d2-4c35-92d2-5206dc6be4d2","resourceVersion":"156","creationTimestamp":"2019-10-21T13:18:48Z"},"subsets" :[{"addresses":[{"ip":"192.0.2.0/24"}],"ports": [{"name":"https","port":6443,"protocol":"TCP"}]}],"requestReceived Timestamp":"2019-10-21T14:37:53.788926Z","stageTimestamp":"2019-10-21T14:37:53.789945Z","annotations":{"authorization.k8s.io/decision":"allow","authorization.k8s.io/reason":""}}

Chapter 92. Lastline Enterprise

The IBM QRadar DSM for Lastline Enterprise receives anti-malware events from Lastline Enterprise systems.

The following table identifies the specifications for the Lastline Enterprise DSM:

Table 705. Lastline Enterprise DSM specifications

Specification	**Value**
Manufacturer	Lastline
DSM name	Lastline Enterprise
RPM file name	`DSM-LastlineEnterprise-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	6.0
Protocol	LEEF
Recorded event types	Anti-malware
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Lastline website (http://www.lastline.com)

To send Lastline Enterprise events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Lastline Enterprise DSM RPM
2. Configure your Lastline Enterprise device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Lastline Enterprise log source on the QRadar Console. The following table describes the parameters that require specific values that are required for Lastline Enterprise event collection:

   Table 706. Lastline Enterprise log source parameters

Parameter	**Value**
Log Source type	Lastline Enterprise
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring Lastline Enterprise to communicate with QRadar

On the Lastline Enterprise system, use the SIEM settings in the notification interface to specify a SIEM appliance where Lastline can send events.

Adding a log source

Configuring Lastline Enterprise to communicate with QRadar

On the Lastline Enterprise system, use the SIEM settings in the notification interface to specify a SIEM appliance where Lastline can send events.

Procedure

1. Log in to your Lastline Enterprise system.
2. On the sidebar, click **Admin**.
3. Click **Reporting > Notifications**.
4. To add a notification, click the **Add a notification** (+) icon.
5. From the **Notification Type** list, select **SIEM**.
6. In the **SIEM Server Settings** pane, configure the parameters for your QRadar Console or Event Collector. Ensure that you select **LEEF** from the **SIEM Log Format** list.
7. Configure the triggers for the notification:
   a) To edit existing triggers in the list, click the **Edit trigger** icon, edit the parameters, and click **Update Trigger**.
   b) To add a trigger to the list, click the **Add Trigger** (+) icon, configure the parameters, and click **Add Trigger**.
8. Click **Save**.

Chapter 93. Lieberman Random Password Manager

The Lieberman Random Password Manager DSM gives the option to integrate IBM QRadar with Lieberman Enterprise Random Password Manager and Lieberman Random Password Manager software by using syslog events in the Log Event Extended Format (LEEF).

About this task

The Lieberman Random Password Manager uses Port 514 to forward syslog events to QRadar. QRadar records all relevant password management events. For information on configuring syslog forwarding, see your vendor documentation.

QRadar automatically detects syslog events that are forwarded from Lieberman Random Password Manager and Lieberman Enterprise Random Password Manager devices. However, if you want to manually configure QRadar to receive events from these devices:

Procedure

From the **Log Source Type** list, select **Lieberman Random Password Manager**.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Chapter 94. LightCyber Magna

The IBM QRadar DSM for LightCyber Magna collects events from a LightCyber Magna device.

The following table describes the specifications for the LightCyber Magna DSM:

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Table 707. LightCyber Magna DSM specifications

Specification	**Value**
Manufacturer	LightCyber
DSM name	LightCyber Magna
RPM file name	`DSM-LightCyberMagna-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	3.9
Protocol	Syslog
Event format	LEEF
Recorded event types	C&C Exfilt Lateral Malware Recon
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	LightCyber website (https://www.lightcyber.com)

To integrate LightCyber Magna with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - LightCyber Magna DSM RPM
2. Configure your LightCyber Magna device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a LightCyber Magna log source on the QRadar Console. The following table describes the parameters that require specific values to collect events from LightCyber Magna:

Table 708. LightCyber Magna log source parameters

Parameter	**Value**
Log Source type	LightCyber Magna
Protocol Configuration	Syslog

Table 708. LightCyber Magna log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	Type a unique identifier for the log source.

4. To verify that QRadar is configured correctly, review the following table to see an example of a normalized audit event message.

   The following table shows a sample event message from LightCyber Magna:

Table 709. LightCyber Magna sample message		
Event name	**Low level category**	**Sample log message**
Suspicious Riskware	Misc Malware	LEEF:2.0|LightCyber|Magna |3.7.3.0|New indicator|type=Riskware sev=7 devTime=Sep 18 2016 08:26 :08 devTimeFormat=MMM dd yyyy HH:mm:ss devTimeEnd=Sep 29 2016 15:26:47 devTimeEndFormat=MMM dd yyyy HH:mm:ss msg=Riskware alert (0) app= dstPort= usrName= shostId=xxxxxxxx- xxxx-xxxx-xxxx-xxxxxxxxxxxx shost=PC04 src=<Source_IP_address> srcMAC=<Source_MAC_address> status=Suspicious filePath=c:\program files\ galaxy must\galaxy must.exe malwareName=W32.HfsAutoB.3DF2 fileHash=d836433d538d864d21a4e 0f7d66e30d2 externalId=16100 sdeviceExternalId=32373337 -3938-5A43-4A35-313030303336 LEEF:2.0|LightCyber|Magna|3.7.3.0|New indicator|type=Riskware sev=7 devTime=Sep 18 2016 08:26:08 devTimeFormat=MMM dd yyyy HH:mm:ss devTimeEnd=Sep 29 2016 15:26:47 devTimeEndFormat=MMM dd yyyy HH:mm:ss msg=Riskware alert (0) app= dstPort= usrName= shostId=xxxxxxxx-xxxx- xxxx-xxxx-xxxxxxxxxxxx shost=PC04 src=<Source_IP_address> srcMAC=<Source_MAC_address> status=Suspicious filePath=c:\program files\galaxy must\galaxy must.exe malwareName=W32.HfsAutoB.3DF2 fileHash=d836433d538d864d21a4e0f7d66e3 0d2 externalId=16100 sdeviceExternalId=32373337-3938-5A43-4 A35-313030303336

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring LightCyber Magna to communicate with QRadar

To collect LightCyber Magna events, configure your LightCyber Magna device to send syslog events to QRadar.

Procedure

1. Log in to the LightCyber Magna interface as administrator.
2. Click **Configuration** > **Syslog**.

3. Enable **Yes**.
4. Configure the following parameters:

Table 710. LightCyber Magna configuration parameters

Parameter	Value
Host	The IP address or host name of the QRadar Event Collector.
Port	514
Protocol	TCP
Format	LEEF

5. Click **Save**.

Chapter 95. Linux

IBM QRadar supports the a range of Linux DSMs.

Linux DHCP Server

The Linux DHCP Server DSM for IBM QRadar collects DHCP events by using syslog.

To integrate Linux DHCP Server with IBM QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (http://www.ibm.com/support).
   - DSM Common RPM
   - GNU Linux DHCP DSM RPM
   - Protocol Common RPM
2. Configure your Linux DHCP server to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Linux DHCP Server logsource log source on the QRadar Console. For more information about configuring your Linux DHCP Server, consult the Linux man pages or associated documentation for your DHCP daemon.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Linux DHCP Server DSM specifications

When you configure Linux DHCP Server, understanding the specifications for the Linux DHCP Server DSM can help ensure a successful integration. For example, knowing what the supported version of Linux DHCP Server is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Linux DHCP Server DSM.

Table 711. Linux DHCP DSM specifications

Specification	Value
Manufacturer	Linux
DSM name	Linux DHCP Server
RPM file name	DSM-*GNULinuxDHCP-QRadar_version-build_number*.noarch.rpm
Supported version	Linux DHCP Server 2.4
Protocol	Syslog
Recorded event types	All events from a DHCP server
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	DHCP documentation (https://docs.box.com/docs/configuring-box-platform)

Syslog log source parameters for Linux DHCP

If QRadar does not automatically detect the log source, add a Linux DHCP log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Linux DHCP servers:

Table 712. Syslog log source parameters for the Linux DHCP DSM

Parameter	Value
Log Source type	Linux DHCP Server
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Linux DHCP Server.

Related tasks

Adding a log source

Linux DHCP Server sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Linux DHCP Server sample message when you use the Syslog protocol

The following sample event message shows the client determined that the offered configuration parameters are invalid and the client must begin the lease process again.

```
The following sample event message shows that the client has determined that the offered
configuration parameters are invalid, the client must begin the lease process again.
<30>Sep 25 15:23:34 gnu.linuxdhcp.test dhcpd[28894]: DHCPDECLINE of 192.0.2.0 from
00-00-5E-00-53-00 (broker) via 192.0.2.1: abandoned
```


```
The following sample event message shows that the client has determined that the offered
configuration parameters are invalid, the client must begin the lease process again.
<30>Sep 25 15:23:34 gnu.linuxdhcp.test dhcpd[28894]: DHCPDECLINE of 192.0.2.0 from
00-00-5E-00-53-00 (broker) via 192.0.2.1: abandoned
```


Table 713. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**DHCPDECLINE**
Source IP	**192.0.2.0**
Source MAC	**00-00-5E-00-53-00**
Device Time	**Sep 25 15:23:34**

Linux IPtables

The Linux IPtables DSM for IBM QRadar accepts firewall IPtables events by using syslog.

QRadar records all relevant from Linux IPtables where the syslog event contains any of the following words: Accept, Drop, Deny, or Reject. Creating a customized log prefix in the event payload enables QRadar to easily identify IPtables behavior.

Configuring IPtables

IPtables is a powerful tool, which is used to create rules on the Linux kernel firewall for routing traffic.

About this task

To configure IPtables, you must examine the existing rules, modify the rule to log the event, and assign a log identifier to your IPtables rule that can be identified by IBM QRadar. This process is used to determine which rules are logged by QRadar. QRadar includes any logged events that include the words: accept, drop, reject, or deny in the event payload.

Procedure

1. Using SSH, log in to your Linux Server as a root user.
2. Edit the IPtables file in the following directory:

   `/etc/iptables.conf`

   Note: The file that contains the IPtables rules can vary according to the specific Linux operating system you are configuring. For example, a system using Red Hat Enterprise has the file in the `/etc/sysconfig/iptables` directory. Consult your *Linux operating system documentation* for more information about configuring IPtables.
3. Review the file to determine the IPtables rule you want to log.

   For example, if you want to log the rule that is defined by the entry, use:

   ```
   -A INPUT -i eth0 --dport 31337 -j DROP
   ```
4. Insert a matching rule immediately before each rule you want to log:

   ```
   -A INPUT -i eth0 --dport 31337 -j DROP
   ```

   ```
   -A INPUT -i eth0 --dport 31337 -j DROP
   ```
5. Update the target of the new rule to LOG for each rule you want to log,For example:

   ```
   -A INPUT -i eth0 --dport 31337 -j LOG
   ```

   ```
   -A INPUT -i eth0 --dport 31337 -j DROP
   ```
6. Set the log level of the LOG target to a SYSLOG priority level, such as info or notice:

   ```
   -A INPUT -i eth0 --dport 31337 -j LOG --log-level info
   ```

   ```
   -A INPUT -i eth0 --dport 31337 -j DROP
   ```
7. Configure a log prefix to identify the rule behavior. Set the log prefix parameter to :

   `Q1Target=<rule>`

   Where <*rule*> is one of the following IPtable firewall actions: **`fw_accept`**, **`fw_drop`**, **`fw_reject`**, or **`fw_deny`**.

   For example, if the rule that is logged by the firewall targets dropped events, the log prefix setting is:

   `Q1Target=fw_drop`

   ```
   -A INPUT -i eth0 --dport 31337 -j LOG --log-level info --log-prefix "Q1Target=fw_drop " -A
   INPUT -i eth0 --dport 31337 -j DROP
   ```

   Note: You must have a trailing space before the closing quotation mark.
8. Save and exit the file.
9. Restart IPtables using the following command:

   `/etc/init.d/iptables restart`
10. Open the `syslog.conf` file.
11. Add the following line:

```
kern.<log level>@<IP address>
```

Where:

- <*log level*> is the previously set log level.
- <*IP address*> is the IP address of QRadar.

12. Save and exit the file.
13. Restart the syslog daemon by using the following command:

```
/etc/init.d/syslog restart
```

After the syslog daemon restarts, events are forwarded to QRadar. IPtable events that are forwarded from Linux Servers are automatically discovered and displayed in the **Log Activity** tab of QRadar.

Syslog log source parameters for Linux IPtables

If QRadar does not automatically detect the log source, add a Linux IPtables log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Linux IPtables firewalls:

Table 714. Syslog log source parameters for the Linux IPtables DSM

Parameter	Value
Log Source type	Linux IPtables Firewall
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Linux IPtables firewall.

Related tasks

Adding a log source

Linux OS

The Linux OS DSM for IBM QRadar records Linux operating system events and forwards the events using syslog or syslog-ng.

If you are using syslog on a UNIX host, upgrade the standard syslog to a more recent version, such as, syslog-ng.

Note: Do not run both syslog and syslog-ng at the same time.

To integrate Linux OS with QRadar, select one of the following syslog configurations for event collection:

- “Configuring syslog on Linux OS” on page 1117
- “Configuring syslog-ng on Linux OS” on page 1117

You can also configure your Linux operating system to send audit logs to QRadar. For more information, see “Configuring Linux OS to send audit logs” on page 1118.

Supported event types

The Linux OS DSM supports the following event types:

- cron
- HTTPS

- FTP
- NTP
- Simple Authentication Security Layer (SASL)
- SMTP
- SNMP
- SSH
- Switch User (SU)
- Pluggable Authentication Module (PAM) events.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Configuring syslog on Linux OS

Configuring Linux OS to forward events by using the syslog protocol.

Procedure

1. Log in to your Linux OS device, as a root user.
2. Open the `/etc/syslog.conf` file and add the following facility information:

   ```
   authpriv.* @<ip_address>
   ```

   where:

   <ip_address> is the IP address of IBM QRadar.
3. Save the file.
4. Restart syslog by typing the following command:

   `service syslog restart`
5. Log in to the QRadar Console.
6. Add a Linux OS log source on the QRadar Console.

   For more information about syslog, see the Linux documentation (https://www.linux.com/what-is-linux/).

Configuring syslog-ng on Linux OS

If you are using syslog on a UNIX host to forward events, upgrade the standard syslog to syslog-ng, which is a more recent version.

Procedure

1. Log in to your Linux OS device, as a root user.
2. Open the `/etc/syslog-ng/syslog-ng.conf` file and add the following facility information:

   ```
   source qr_source {
       internal();
       system();
   };
   filter qr_filter {
       facility(auth, authpriv);
   };
   destination qr_destination {
       tcp("<qradar_ip_address>" port(514));
   };
   log{
       source(qr_source);
       filter(qr_filter);
   ```

```
    destination(qr_destination);
};
```

where:

<qradar_ip_address> is the IP address of IBM QRadar.

3. Save the file.
4. Restart syslog-ng by typing the following command:

   service syslog-ng restart
5. Log in to the QRadar Console.
6. Add a Linux OS log source on the QRadar Console.

   For more information about syslog-ng, see the Linux documentation (https://www.linux.com/what-is-linux/).

Related tasks

"Adding a log source" on page 5

Configuring Linux OS to send audit logs

Configure Linux OS to send audit logs to QRadar.

About this task

This task applies to Red Hat Enterprise Linux (RHEL) v6 to v8 operating systems.

If you use a SUSE, Debian, or Ubuntu operating system, see your vendor documentation for specific steps for your operating system.

Procedure

1. Log in to your Linux OS device, as a root user.
2. Type the following commands:

   yum install audit

   service auditd start

   chkconfig auditd on
3. Optional: If you are using RHEL v6 to v7.9, open the `/etc/audisp/plugins.d/syslog.conf` file and verify that the parameters match the following values:

   ```
   active = yes
   direction = out
   path = builtin_syslog
   type = builtin
   args = LOG_LOCAL6
   format = string
   ```
4. Optional: If you are using RHEL v8, open the `/etc/audit/plugins.d/syslog.conf` file and verify that the parameters match the following values:

   ```
   active = yes
   direction = out
   path = builtin_syslog
   type = builtin
   args = LOG_LOCAL6
   ```

format = string

5. Open the /etc/rsyslog.conf file and add the following line at the end of the file:
   local6.* @@<*QRadar_Collector_IP_address*>
6. Type the following commands:
   service auditd restart
   service syslog restart
7. Log in to the QRadar Console.
8. Add a Linux OS log source on the QRadar Console.

Related tasks

"Adding a log source" on page 5

Linux OS Sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Linux OS sample event messages when you use the syslog protocol

Sample 1: The following sample event message shows a PAM authentication failure for a user.

```
<118>Jul 7 15:54:13 kernel: Jul 7 15:54:13 gnu.linuxserver.test sshd[708]: error: PAM:
authentication error for root from 172.16.197.55
```

```
<118>Jul 7 15:54:13 kernel: Jul 7 15:54:13 gnu.linuxserver.test sshd[708]: error: PAM:
authentication error for root from 172.16.197.55
```

Table 715. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	authentication error
Source IP	172.16.197.55
Username	root

Sample 2: The following sample event message show that an incorrect or failed password was received from an invalid user.

```
<38>2015-06-24T14:15:51Z sshd[12239959]: Failed password for invalid user test from 192.168.8.75
port 57436 ssh2
```

```
<38>2015-06-24T14:15:51Z sshd[12239959]: Failed password for invalid user test from
192.168.8.75 port 57436 ssh2
```

Table 716. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	Failed password
Source IP	192.168.8.75
Source Port	57436
Username	test

Chapter 96. LOGbinder

Configure your LOGbinder system to send event logs to IBM QRadar.

The following LOGbinder systems are supported:

- LOGbinder EX event collection from Microsoft Exchange Server.
- LOGbinder SP event collection from Microsoft SharePoint.
- LOGbinder SQL event collection from Microsoft SQL Server.

LOGbinder EX event collection from Microsoft Exchange Server

The IBM QRadar DSM for Microsoft Exchange Server can collect LOGbinder EX V2.0 events.

The following table identifies the specifications for the Microsoft Exchange Server DSM when the log source is configured to collect LOGbinder EX events:

Table 717. LOGbinder for Microsoft Exchange Server

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft Exchange Server
RPM file name	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
Supported versions	LOGbinder EX V2.0
Protocol type	Syslog LEEF
QRadar recorded event types	Admin Mailbox
Automatically discovered?	Yes
Included identity?	No
More information	Microsoft Exchange website (http://www.office.microsoft.com/en-us/exchange/)

The Microsoft Exchange Server DSM can collect other types of events. For more information on how to configure for other Microsoft Exchange Server event formats, see the Microsoft Exchange Server topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft Exchange Server, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM Support Website:
   - DSMCommon RPM
   - Microsoft Exchange Server DSM RPM
2. Configure your LOGbinder EX system to send Microsoft Exchange Server event logs to QRadar.
3. If the log source is not automatically created, add a Microsoft Exchange Server DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder EX event collection:

Table 718. Microsoft Exchange Server log source parameters for LOGbinder event collection	
Parameter	**Value**
Log Source type	Microsoft Exchange Server
Protocol Configuration	Syslog

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring your LOGbinder EX system to send Microsoft Exchange event logs to QRadar

To collect Microsoft Exchange LOGbinder events, you must configure your LOGbinder EX system to send events to IBM QRadar.

Before you begin

Configure LOGbinder EX to collect events from your Microsoft Exchange Server. For more information, see your LOGbinder EX documentation.

Procedure

1. Open the **LOGbinder EX Control Panel**.
2. Double-click **Output** in the Configure pane.
3. Choose one of the following options:
   - Configure for Syslog-Generic output:
     a. In the Outputs pane, double-click **Syslog-Generic**.
     b. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
   - Configure for Syslog-LEEF output:
     a. In the Outputs pane, double-click **Syslog-LEEF**.
     b. Select the **Send output to Syslog-LEEF** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
4. Click **OK**.
5. To restart the LOGbinder service, click the **Restart** icon.

LOGbinder SP event collection from Microsoft SharePoint

The IBM QRadar DSM for Microsoft SharePoint can collect LOGbinder SP events.

The following table identifies the specifications for the Microsoft SharePoint DSM when the log source is configured to collect LOGbinder SP events:

Table 719. LOGbinder for Microsoft SharePoint specifications	
Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft SharePoint
RPM file name	`DSM-MicrosoftSharePoint-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	LOGbinder SP V4.0

Table 719. LOGbinder for Microsoft SharePoint specifications (continued)	
Specification	**Value**
Protocol type	Syslog LEEF
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	No
More information	*http://office.microsoft.com/en-sg/sharepoint/* (http://office.microsoft.com/en-sg/sharepoint/) *http://www.logbinder.com/products/logbindersp/* (http://www.logbinder.com/products/logbindersp/)

The Microsoft SharePoint DSM can collect other types of events. For more information about other Microsoft SharePoint event formats, see the Microsoft SharePoint topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft SharePoint, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM Support Website:
   - DSMCommon RPM
   - Microsoft SharePoint DSM RPM
2. Configure your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar.
3. If the log source is not automatically created, add a Microsoft SharePoint DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder event collection:

Table 720. Microsoft SharePoint log source parameters for LOGbinder event collection	
Parameter	**Value**
Log Source type	Microsoft SharePoint
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar

To collect Microsoft SharePoint LOGbinder events, you must configure your LOGbinder SP system to send events to IBM QRadar.

Related information

Adding a log source

Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar

To collect Microsoft SharePoint LOGbinder events, you must configure your LOGbinder SP system to send events to IBM QRadar.

Procedure

1. Open the **LOGbinder SP Control Panel**.
2. Double-click **Output** in the Configure pane.

3. Choose one of the following options:
   - Configure for Syslog-Generic output:
     a. In the Outputs pane, double-click **Syslog-Generic**.
     b. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
   - Configure for Syslog-LEEF output:
     a. In the Outputs pane, double-click **Syslog-LEEF**.
     b. Select the **Send output to Syslog-LEEF** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
4. Click **OK**.
5. To restart the LOGbinder service, click the **Restart** icon.

LOGbinder SQL event collection from Microsoft SQL Server

The IBM QRadar DSM for Microsoft SQL Server can collect LOGbinder SQL events.

The following table identifies the specifications for the Microsoft SQL Server DSM when the log source is configured to collect LOGbinder SQL events:

Table 721. LOGbinder for Microsoft SQL Server specifications

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft SQL Server
RPM file name	`DSM-MicrosoftSQL-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	LOGBinder SQL V2.0
Protocol type	Syslog
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	Yes
More information	LogBinder SQL website (http://www.logbinder.com/products/logbindersql/) Microsoft SQL Server website (http://www.microsoft.com/en-us/server-cloud/products/sql-server/)

The Microsoft SQL Server DSM can collect other types of events. For more information about other Microsoft SQL Server event formats, see the Microsoft SQL Server topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft SQL Server, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM Support Website:
   - DSMCommon RPM
   - Microsoft SQL Server DSM RPM
2. Configure your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar.

3. If the log source is not automatically created, add a Microsoft SQL Server DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder event collection:

Table 722. Microsoft SQL Server log source parameters for LOGbinder event collection

Parameter	Value
Log Source type	Microsoft SQL Server
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar

To collect Microsoft SQL Server LOGbinder events, you must configure your LOGbinder SQL system to send events to IBM QRadar.

Before you begin

Configure LOGbinder SQL to collect events from your Microsoft SQL Server. For more information, see your LOGbinder SQL documentation.

Procedure

1. Open the **LOGbinder SQL Control Panel**.
2. Double-click **Output** in the Configure pane.
3. Choose one of the following options:
   - Configure for Syslog-Generic output:
     a. In the Outputs pane, double-click **Syslog-Generic**.
     b. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
   - Configure for Syslog-LEEF output:
     a. In the Outputs pane, double-click **Syslog-LEEF**.
     b. Select the **Send output to Syslog-LEEF** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
4. Click **OK**.
5. To restart the LOGbinder service, click the **Restart** icon.

Chapter 97. McAfee

IBM QRadar supports a range of McAfee products.

JDBC log source parameters for McAfee Application/Change Control

If QRadar does not automatically detect the log source, add a McAfee Application/Change Control log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from McAfee Application/Change Control:

Table 723. JDBC log source parameters for the McAfee Application/Change Control DSM

Parameter	Description
Log Source Type	**McAfee Application/Change Control**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Table Name	Type `SCOR_EVENTS` as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if it's needed for your configuration. The list must contain the field that is defined in the **Compare Field** parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type `AutoID` as the compare field. The compare field is used to identify new events added between queries to the table.

For a complete list of Syslog protocol parameters and their values, see “JDBC protocol configuration options” on page 147.

Related tasks

Adding a log source

McAfee ePolicy Orchestrator

The IBM QRadar DSM for McAfee ePolicy Orchestrator collects events from a McAfee ePolicy Orchestrator device.

The following table identifies the specifications for the McAfee ePolicy Orchestrator DSM:

Table 724. McAfee ePolicy Orchestrator

Specification	**Value**
Manufacturer	McAfee
DSM name	McAfee ePolicy Orchestrator
RPM file name	DSM-McAfeeEpo-*QRadar_version-build_number*.noarch.rpm
Supported versions	3.5 to 5.10
Protocol	JDBC- supports versions 3.5 to 5.9 SNMPv1 - supports versions 3.5 to 5.9 SNMPv2 - supports versions 3.5 to 5.9 SNMPv3 - supports versions 3.5 to 5.9 TLS Syslog - supports version 5.10
Recorded event types	AntiVirus events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	McAfee website (http://www.mcafee.com/enterprise/en-us/products/epolicy-orchestrator.html)

To integrate McAfee ePolicy Orchestrator with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console.
   - JDBC Protocol RPM
   - SNMP Protocol RPM
   - TLS Syslog Protocol RPM
   - DSMCommon RPM
   - McAfee ePolicy Orchestrator DSM RPM
2. Configure your McAfee ePolicy Orchestrator device to send events to QRadar.
   a. Add a registered server. If you are using the JDBC protocol, you don't need to add a registered server. For more information about registering servers, see the following procedures:
      - Register syslog servers (https://docs.trellix.com/bundle/trellix-epolicy-orchestrator-on-prem-5.10.0-product-guide/page/GUID-5C5332B3-837A-4DDA-BE5C-1513A230D90A.html)
      - Register SNMP servers (https://docs.trellix.com/bundle/trellix-epolicy-orchestrator-on-prem-5.10.0-product-guide/page/GUID-F37CFF4C-B227-4545-8BC5-2DDC46504F90.html)

b. Configure SNMP notifications. If you are using the JDBC protocol or the TLS Syslog protocol, no further configuration is required. For more information about configuring SNMP notifications, see Configuring SNMP notifications on McAfee ePolicy Orchestrator.

c. Install the Java Cryptography Extension for high-level SNMP decryption algorithms. For more information, see the following procedures:

- Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator
- Installing the Java Cryptography Extension on QRadar

3. Add a McAfee ePolicy Orchestrator log source on the QRadar Console. The following tables describe the SNMPv1, SNMPv2, SNMPv3, JDBC, and TLS syslog protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

   The following table describes the SNMPv1 protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

Table 725. McAfee ePolicy Orchestrator SNMPv1 log source parameters	
Parameter	**Value**
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	**McAfee ePolicy Orchestrator**
Protocol Configuration	**SNMPv1**
Log Source Identifier	Type a unique identifier for the log source.

   The following table describes the SNMPv2 protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

Table 726. McAfee ePolicy Orchestrator SNMPv2 log source parameters	
Parameter	**Value**
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	**McAfee ePolicy Orchestrator**
Protocol Configuration	**SNMPv2**
Log Source Identifier	Type a unique identifier for the log source.

   For a complete list of SNMPv2 protocol log source parameters and their values, see SNMPv2 protocol configuration options.

   The following table describes the SNMPv3 protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

Table 727. McAfee ePolicy Orchestrator SNMPv3 log source parameters	
Parameter	**Value**
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	**McAfee ePolicy Orchestrator**
Protocol Configuration	**SNMPv3**
Log Source Identifier	Type a unique identifier for the log source.

For a complete list of SNMPv3 protocol log source parameters and their values, see SNMPv3 protocol configuration options.

The following table describes the JDBC protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

Table 728. McAfee ePolicy Orchestrator JDBC log source parameters

Parameter	Value
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	**McAfee ePolicy Orchestrator**
Protocol Configuration	**JDBC**
Database Type	Select **MSDE** from the list.
Table Name	A table or view that includes the event records as follows: • For ePolicy Orchestrator 3.x, type `Events`. • For ePolicy Orchestrator 4.x, type `EPOEvents`. • For ePolicy Orchestrator 5.x, type `EPOEvents`.

For a complete list of JDBC protocol log source parameters and their values, see JDBC protocol configuration options.

The following table describes the TLS syslog protocol log source parameters that require specific values to collect events from McAfee ePolicy Orchestrator.

Table 729. McAfee ePolicy Orchestrator TLS syslog log source parameters

Parameter	Value
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	**McAfee ePolicy Orchestrator**
Protocol Configuration	**TLS Syslog**

For a complete list of TLS syslog log source parameters and their values, see TLS syslog protocol configuration options.

Related concepts

"SNMPv2 protocol configuration options" on page 216
You can configure a log source to use the SNMPv2 protocol to receive SNMPv2 events.

"SNMPv3 protocol configuration options" on page 217
You can configure a log source to use the SNMPv3 protocol to receive SNMPv3 events.

"TLS Syslog protocol configuration options" on page 227
Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

"McAfee ePolicy Orchestrator sample event messages" on page 1133
Use these sample event messages to verify a successful integration with QRadar.

Related tasks

"Adding a log source" on page 5

"Adding a DSM" on page 4

"Configuring SNMP notifications on McAfee ePolicy Orchestrator" on page 1131
To send SNMP events from McAfee ePolicy Orchestrator to IBM QRadar, you must configure SNMP notifications on your McAfee ePolicy Orchestrator device.

"Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator" on page 1132
The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your McAfee ePolicy Orchestrator (McAfee ePO) device.

Related information

c_logsource_JDBCprotocol.dita

Configuring SNMP notifications on McAfee ePolicy Orchestrator

To send SNMP events from McAfee ePolicy Orchestrator to IBM QRadar, you must configure SNMP notifications on your McAfee ePolicy Orchestrator device.

Before you begin

You must add a registered server to McAfee ePolicy Orchestrator before you complete the following steps. For more information, see Register syslog servers (https://docs.mcafee.com/bundle/epolicy-orchestrator-5.10.0-product-guide/page/GUID-5C5332B3-837A-4DDA-BE5C-1513A230D90A.html).

Procedure

1. Select **Menu** > **Automation** > **Automatic Responses**.
2. Click **New Responses**, and then configure the following values.
   a. Type a name and description for the response.
   b. From the **Event group** list, select **ePO Notification Events**.
   c. From the **Event type** list, select **Threats**.
   d. From the **Status** list, select **Enabled**.
3. Click **Next**.
4. From the **Value** column, type a value to use for system selection, or click the ellipsis icon.
5. Optional: From the **Available Properties** list, select more filters to narrow the response results.
6. Click **Next**.
7. Select **Trigger this response for every event** and then click **Next**.

   When you configure aggregation for your McAfee ePolicy Orchestrator responses, do not enable throttling.
8. From the **Actions** list, select **Send SNMP Trap**.
9. Configure the following values:
   a. From the list of SNMP servers, select the SNMP server that you registered when you added a registered server.
   b. From the **Available Types** list, select **List of All Values**.
   c. Click **>>** to add the event type that is associated with your McAfee ePolicy Orchestrator version. Use the following table as a guide:

Available Types	Selected Types	ePolicy Orchestrator Version
Detected UTC	{listOfDetectedUTC}	4.5, 5.9
Received UTC	{listOfReceivedUTC}	4.5, 5.9
Detecting Product IPv4 Address	{listOfAnalyzerIPV4}	4.5, 5.9
Detecting Product IPv6 Address	{listOfAnalyzerIPV6}	4.5, 5.9

Available Types	Selected Types	ePolicy Orchestrator Version
Detecting Product MAC Address	{listOfAnalyzerMAC}	4.5, 5.9
Source IPv4 Address	{listOfSourceIPV4}	4.5, 5.9
Source IPv6 Address	{listOfSourceIPV6}	4.5, 5.9
Source MAC Address	{listOfSourceMAC}	4.5, 5.9
Source User Name	{listOfSourceUserName}	4.5, 5.9
Target IPv4 Address	{listOfTargetIPV4}	4.5, 5.9
Target IPv6 Address	{listOfTargetIPV6}	4.5, 5.9
Target MAC	{listOfTargetMAC}	4.5, 5.9
Target Port	{listOfTargetPort}	4.5, 5.9
Threat Event ID	{listOfThreatEventID}	4.5, 5.9
Threat Event ID	{listOfThreatEventID}	4.5, 5.9
Threat Severity	{listOfThreatSeverity}	4.5, 5.9
SourceComputers		4.0
AffectedComputerIPs		4.0
EventIDs		4.0
TimeNotificationSent		4.0

10. Click **Next**, and then click **Save**.

What to do next

1. Add a log source in QRadar.
2. Install the Java Cryptography Extension for high-level SNMP decryption algorithms.

Related tasks

"Adding a log source" on page 5

"Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator" on page 1132
The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your McAfee ePolicy Orchestrator (McAfee ePO) device.

"Installing the Java Cryptography Extension on QRadar" on page 1133
The Java Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your QRadar appliance.

Installing the Java Cryptography Extension on McAfee ePolicy Orchestrator

The Java™ Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your McAfee ePolicy Orchestrator (McAfee ePO) device.

Procedure

1. Download the latest version of the JavaTM Cryptography Extension from the following website:

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

The JavaTM Cryptography Extension version must match the version of the Java™ installed on your McAfee ePO device.

2. Copy the JCE compressed file to the following directory on your McAfee ePO device:

```
<installation path to McAfee ePO>/jre/lib/security
```

Installing the Java Cryptography Extension on QRadar

The Java Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your QRadar appliance.

Procedure

1. Optional: If you are using QRadar 7.2x, 7.3.0, or 7.31, complete the following steps:
   a) Download the latest version of the Java Cryptography Extension from the IBM website (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).

      The Java Cryptography Extension version must match the version of the Java that is installed on QRadar.

   b) Extract the JCE file.

      The following Java archive (JAR) files are included in the JCE download:

      - `local_policy.jar`
      - `US_export_policy.jar`

   c) Log in to your QRadar Console or QRadar Event Collector as a root user.

   d) Copy the JCE JAR files to the following directory on your QRadar Console or Event Collector:

      `/store/configservices/staging/globalconfig/java_security`

      Note: The JCE JAR files are only copied to the system that receives the AES192 or AE256 encrypted files.

   e) Restart the QRadar services by typing one of the following commands:

      - If you are using QRadar 7.2.x, type `service ecs-ec restart`.
      - If you are using QRadar 7.3.0, type `systemctl restart ecs-ec.service`.
      - If you are using QRadar 7.3.1, type `systemctl restart ecs-ec-ingress.service`.

2. Optional: If you are using QRadar 7.4.3 Fix Pack 4 or earlier, complete the Installing unrestricted SDK JCE policy files procedure (https://www.ibm.com/docs/en/qsip/7.4?topic=authentication-installing-unrestricted-sdk-jce-policy-files).

   Important: If you are using QRadar 7.4.3 Fix Pack 5 or later, do not install these files.

McAfee ePolicy Orchestrator sample event messages

Use these sample event messages to verify a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

McAfee ePolicy Orchestrator sample event message when you use the JDBC protocol

The following sample event message shows that a host intrusion was detected, but not handled.

```
AutoID: "231426750" AutoGUID: "995F348A-4CA3-4CEF-B259-5E678106884E" ServerID: "QRADARSERVER1"
ReceivedUTC: "2014-07-23 08:02:13.553" DetectedUTC: "2014-07-23 07:55:11.0" AgentGUID:
"2AB7C0C3-23C5-4FBD-B0A6-9A3A9B802A9E" Analyzer: "HOSTIPS_8000" AnalyzerName: "McAfee Host
Intrusion Prevention" AnalyzerVersion: "8.0.0" AnalyzerHostName: "QRADARANALYZER" AnalyzerIPV4:
```

```
"739325208" AnalyzerIPV6: "[B@e00e408" AnalyzerMAC: "001cc4e0e79e" AnalyzerDATVersion:
"null" AnalyzerEngineVersion: "null" AnalyzerDetectionMethod: "null" SourceHostName:
"null" SourceIPV4: "739325208" SourceIPV6: "[B@7d03cef5" SourceMAC: "00005E005300"
SourceUserName: "QRADAR\SYSTEM" SourceProcessName: "C:\WINNT\SYSTEM32\SERVICES.EXE" SourceURL:
"file:///C:\WINNT\SYSTEM32\SERVICES.EXE" TargetHostName: "QRADAR" TargetIPV4: "739325208"
TargetIPV6: "[B@cf5e07d2" TargetMAC: "00005E005300" TargetUserName: "null" TargetPort: "null"
TargetProtocol: "null" TargetProcessName: "null" TargetFileName: "null" ThreatCategory:
"hip.Registry" ThreatEventID: "18000" ThreatSeverity: "2" ThreatName: "915" ThreatType:
"modify" ThreatActionTaken: "hip.reaction.permit" ThreatHandled: "false" TheTimestamp:
"[B@6d04e225"
```


McAfee ePolicy Orchestrator sample message when you use the TLS Syslog protocol

The following sample event message shows that an infected file was deleted.


```
<29>1 2018-06-29T10:53:33.0Z mcafee.epo.test EPOEvents - EventFwd [agentInfo@3401 tenantId="1"
bpsId="1" tenantGUID="{00000000-0000-0000-0000-000000000000}" tenantNodePath="1\2"] <?
xml version="1.0" encoding="UTF-8"?><EPOEvent><MachineInfo><MachineName>mcafee.epo.test</
MachineName><AgentGUID>{890cc45c-7b89-11e8-1cd6-005056afc747}</
AgentGUID><IPAddress>10.254.35.131</IPAddress><OSName>Windows Server
2012 R2</OSName><UserName>SYSTEM</UserName><TimeZoneBias>-330</
TimeZoneBias><RawMACAddress>00-00-5E-00-53-00 through 00-00-5E-00-53-
FF</RawMACAddress></MachineInfo><SoftwareInfo ProductName="McAfee Endpoint
Security" ProductVersion="10.6.0" ProductFamily="TVD"><CommonFields><Analyzer>ENDP_AM_1060</
Analyzer><AnalyzerName>McAfee Endpoint Security</
AnalyzerName><AnalyzerVersion>10.6.0</AnalyzerVersion><AnalyzerHostName>mcafee.epo.test</
AnalyzerHostName><AnalyzerEngineVersion>5900.7806</
AnalyzerEngineVersion><AnalyzerDetectionMethod>On-Access
Scan</AnalyzerDetectionMethod><AnalyzerDATVersion>3389.0</AnalyzerDATVersion></
CommonFields><Event><EventID>1027</EventID><Severity>3</Severity><GMTTime>2018-06-29T10:52:58</
GMTTime><CommonFields><ThreatCategory>av.detect</ThreatCategory><ThreatEventID>1027</
ThreatEventID><ThreatSeverity>2</ThreatSeverity><ThreatName>Elspy.worm</
ThreatName><ThreatType>virus</ThreatType><DetectedUTC>2018-06-29T10:52:58Z</
DetectedUTC><ThreatActionTaken>IDS_ALERT_ACT_TAK_DEL</ThreatActionTaken><ThreatHandled>True</
ThreatHandled><SourceHostName>mcafee.epo.test</SourceHostName><SourceProcessName>c:\Program
Files\QRadar\file1.ext</SourceProcessName><TargetHostName>mcafee.epo.test</
TargetHostName><TargetUserName>domain\admin</TargetUserName><TargetFileName>c:\Program
Files\QRadar_v1\91</TargetFileName></CommonFields><CustomFields
target="EPExtendedEventMT"><BladeName>IDS_BLADE_NAME_SPB</
BladeName><AnalyzerContentCreationDate>2018-06-28T02:04:00Z</
AnalyzerContentCreationDate><AnalyzerGTIQuery>False</
AnalyzerGTIQuery><ThreatDetectedOnCreation>True</ThreatDetectedOnCreation><TargetName>91</
TargetName><TargetPath>c:\Program
Files\QRadar_v2\Desktop</TargetPath><TargetHash>ed066136978a05009cf30c35de92e08e</
TargetHash><TargetFileSize>70</TargetFileSize><TargetModifyTime>2018-06-29T10:52:57Z</
TargetModifyTime><TargetAccessTime>2018-06-29T10:52:57Z</
TargetAccessTime><TargetCreateTime>2018-06-29T10:52:57Z</TargetCreateTime><Cleanable>True</
Cleanable><TaskName>IDS_OAS_TASK_NAME</TaskName><FirstAttemptedAction>IDS_ALERT_THACT_ATT_CLE</
FirstAttemptedAction><FirstActionStatus>True</
FirstActionStatus><SecondAttemptedAction>IDS_ALERT_THACT_ATT_DEL</
SecondAttemptedAction><SecondActionStatus>False</
SecondActionStatus><AttackVectorType>4</AttackVectorType><DurationBeforeDetection>1</
DurationBeforeDetection><NaturalLangDescription>IDS_NATURAL_LANG_OAS_DETECTION_DEL|
TargetName=91|TargetPath=c:\Program Files\QRadar_v2\Desktop|
ThreatName=Elspy.worm|SourceProcessName=c:\Program Files\QRadar\file1.ext|
ThreatType=virus|TargetUserName=domain\admin</NaturalLangDescription><AccessRequested></
AccessRequested><DetectionMessage>IDS_OAS_DEFAULT_THREAT_MESSAGE</
DetectionMessage><AMCoreContentVersion>3389.0</AMCoreContentVersion></CustomFields></Event></
SoftwareInfo></EPOEvent>
```


McAfee MVISION Cloud (formerly known as Skyhigh Networks Cloud Security Platform)

The IBM QRadar DSM for McAfee MVISION Cloud collects logs from a McAfee MVISION Cloud Platform.

McAfee MVISION Cloud is formerly known as Skyhigh Networks Cloud Security Platform.

The following table identifies the specifications for the McAfee MVISION Cloud DSM:

Table 730. McAfee MVISION Cloud DSM specifications

Specification	Value
Manufacturer	McAfee

Table 730. McAfee MVISION Cloud DSM specifications (continued)	
Specification	**Value**
DSM name	McAfee MVISION Cloud
RPM file name	DSM-SkyhighNetworksCloudSecurityPlatform-*QRadar_version-build_number*.noarch.rpm
Supported versions	2.4 and 3.3
Protocol	Syslog
Event format	LEEF
Recorded event types	Privilege Access, Insider Threat, Compromised Account, Access, Admin, Data, Policy, and Audit
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	McAfee MVision Cloud (https://www.mcafee.com/enterprise/en-ca/products/mvision-cloud.html)

To integrate McAfee MVISION Cloud with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Skyhigh Networks Cloud Security Platform DSM RPM
   - DSMCommon RPM
2. Configure your McAfee MVISION Cloud device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a McAfee MVISION Cloud log source on the QRadar Console. The following table describes the parameters that require specific values for McAfee MVISION Cloud event collection:

Table 731. McAfee MVISION Cloud log source parameters	
Parameter	**Value**
Log Source type	McAfee MVISION Cloud
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the McAfee MVISION Cloud that sends events to QRadar.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring McAfee MVISION Cloud to communicate with QRadar

Procedure

1. Log in to the McAfee Enterprise Connector administration interface.
2. Select **Enterprise Integration** > **SIEM Integration**.
3. Configure the following **SIEM SYSLOG SERVICE** parameters:

Parameter	Value
SIEM server	ON
Format	Log Event Extended Format (LEEF)
Syslog Protocol	TCP
Syslog Server	*<QRadar IP or hostname>*
Syslog Port	514
Send to SIEM	new anomalies only

4. Click **Save**.

McAfee MVISION Cloud sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

McAfee MVISION Cloud sample message when you use the Syslog protocol

The following sample event message shows that a CAP incident occurred.

```
<14>Dec 21 18:00:47 mcafee.mvision.test LEEF:1.0|McAfee|MVISION Cloud|4.0.2.1-SNAPSHOT|
Incident|cat=Alert.Policy.CloudAccess    devTimeFormat=MMM dd yyyy HH:mm:ss.SSS zzz
devTime=Sep 18 2018 03:28:08.000 UTC    usrName=user@user.example.com    sev=10
activityName=[Created]  actorIdType=USER        incidentId=35227        riskSeverity=high
collaborationSharedLink=false   contentItemHierarchy=Confidential.docx  contentItemId=AAAAAAAA1
contentItemName=Confidential.docx       informationContentItemParent=Confidential.docx
FileSize=29344  contentItemType=FILE    externalCollaborators=[]        policyId=1
policyName=Enterprise DLP       totalMatchCount=0       instanceId=4008 instanceName=Default
response=[Deleted]      serviceNames=[Slack]    status=new      updatedOn=Sep 25 2018
09:19:51.480 UTC
```

```
<14>Dec 21 18:00:47 mcafee.mvision.test LEEF:1.0|McAfee|MVISION Cloud|4.0.2.1-SNAPSHOT|
Incident|cat=Alert.Policy.CloudAccess    devTimeFormat=MMM dd yyyy HH:mm:ss.SSS zzz
devTime=Sep 18 2018 03:28:08.000 UTC    usrName=user@user.example.com    sev=10
activityName=[Created]  actorIdType=USER        incidentId=35227        riskSeverity=high
collaborationSharedLink=false   contentItemHierarchy=Confidential.docx  contentItemId=AAAAAAAA1
contentItemName=Confidential.docx       informationContentItemParent=Confidential.docx
FileSize=29344  contentItemType=FILE    externalCollaborators=[]        policyId=1
policyName=Enterprise DLP       totalMatchCount=0       instanceId=4008 instanceName=Default
response=[Deleted]      serviceNames=[Slack]    status=new      updatedOn=Sep 25 2018
09:19:51.480 UTC
```

Table 732. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**Incident**
Event Category	**Alert.Policy.CloudAccess**
Username	**user@user.example.com**
Device Time	**Sep 18 2018 03:28:08.000 UTC** (extracted from the date and time fields)

McAfee Network Security Platform (formerly known as McAfee Intrushield)

The IBM QRadar McAfee Network Security Platform DSM collects syslog events from a McAfee Network Security Platform device. QRadar records all relevant events.

To integrate McAfee Network Security Platform with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - McAfee Network Security Platform, DSM RPM
2. To configure your McAfee Network Security Platform device to send events to QRadar, select your McAfee Network Security Platform device version.
   - "Configuring alert events for McAfee Network Security Platform 2.x - 5.x" on page 1138.
   - Configuring alert events for McAfee Network Security Platform 6.x - 7.x.
   - Configuring alert events for McAfee Network Security Platform v8x - 10x.
   - Configuring fault notification events for McAfee Network Security Platform 6.x - 7.x.
   - Configuring fault notification events for McAfee Network Security Platform 8.x - 10.x.
3. If QRadar does not automatically detect the log source, add a McAfee Network Security Platform log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

McAfee Network Security Platform DSM specifications

When you configure the McAfee Network Security Platform, understanding the specifications for the McAfee Network Security Platform DSM can help ensure a successful integration. For example, knowing what the supported version of McAfee Network Security Platform is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the McAfee Network Security Platform DSM.

Table 733. McAfee Network Security Platform DSM specifications

Specification	**Value**
Manufacturer	McAfee
DSM name	McAfee Network Security Platform
RPM file name	DSM-*McAfeeNetworkSecurityPlatform -QRadar_version-build_number*.noarch.rpm
Supported version	2.x - 10.x
Protocol	Syslog
Recorded event types	• Alert notification events (McAfee Network Security Platform 2.x - 5.x) • Alert and fault notification events (McAfee Network Security Platform 6.x - 10.x) **Important:** Supported alert notification events do not include custom events with IDs that begin with 0xc, 0xcc, 0xe, or 0xee.
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No

Table 733. McAfee Network Security Platform DSM specifications (continued)	
Specification	**Value**
More information	McAfee Network Security Platform documentation (https://docs.mcafee.com/bundle/network-security-platform-9.2.x-product-guide/page/GUID-EAE8264B-F9B4-4DA4-9F10-479CCF277F3A.html)

Configuring alert events for McAfee Network Security Platform 2.x - 5.x

To collect alert notification events from McAfee Network Security Platform, administrators must configure a syslog forwarder to send events to IBM QRadar.

Before you begin

To collect alert notification events from McAfee Network Security Platform, you need McAfee Network Security Platform Manager.

Procedure

1. Log in to the **McAfee Network Security Platform Manager** user interface.
2. On the **Network Security Manager** dashboard, click **Configure**.
3. From the **Resource Tree**, click **root** node (Admin-Domain-Name).
4. Click **Alert Notification** > **Syslog Forwarder**.
5. Configure the **Syslog Server** details parameters.

Parameter	Value
Enable Syslog Forwarder	Yes
Port	514

6. Click **Edit**.
7. Select one of the following versions:

Table 734. McAfee Network Security Platform 2.x - 5.x custom message formats	
Version	**Description**
Unpatched McAfee Network Security Platform 2.x systems	`|$ALERT_ID$|$ALERT_TYPE$|$ATTACK_TIME$|"$ATTACK_NAME$"|$ATTACK_ID$| $ATTACK_SEVERITY$|$ATTACK_SIGNATURE$|$ATTACK_CONFIDENCE$| $ADMIN_DOMAIN$|$SENSOR_NAME$|$INTERFACE$|$SOURCE_IP$|$SOURCE_PORT$| $DESTINATION_IP$|$DESTINATION_PORT$|`
McAfee Network Security Platform that has patches applied to update to 3.x - 5.x.	`|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"| $IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$| $IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$| $IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$| $IV_DESTINATION_PORT$|`

Note: The custom message string must be entered as a single line without carriage returns or spaces. McAfee Network Security Platform appliances that do not have software patches applied, use different message strings from patched systems. The format of the custom message must contain a dollar sign ($) as a delimiter before and after each alert element. If you are missing a dollar sign for an element, the alert event might not be formatted properly.

If you are not sure which event message format to use, contact McAfee customer support.

8. Click **Save**.

When alert events are generated by McAfee Network Security Platform, they are forwarded to the syslog destination that you specified. The log source is automatically discovered after enough events are forwarded by the McAfee Network Security Platform appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console and that the **Log Activity** tab displays events from the McAfee Network Security Platform appliance.

Configuring alert events for McAfee Network Security Platform 6.x - 7.x

To collect alert notification events from McAfee Network Security Platform, administrators must configure a syslog forwarder to send events to IBM QRadar

Before you begin

To collect alert notification events from McAfee Network Security Platform, you need McAfee Network Security Platform Manager.

Procedure

1. Log in to the **McAfee Network Security Platform Manager** user interface.
2. On the **Network Security Manager** dashboard, click **Configure**.
3. Expand the **Resource Tree** and then click **IPS Settings** node.
4. Click the **Alert Notification** tab.
5. On the **Alert Notification** menu, click the **Syslog** tab.
6. Configure the following parameters to forward alert notification events:

Table 735. McAfee Network Security Platform 6.x - 7.x alert notification parameters

Parameter	Description
Enable Syslog Notification	Select **Yes** to enable syslog notifications for McAfee Network Security Platform. You must enable this option to forward events to QRadar.
Admin Domain	Select any of the following options: • **Current** - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default. • **Children** - Select this check box to send syslog notifications for alerts in any child domains within the current domain.
Server Name or IP Address	The IP address of your QRadar Console or Event Collector. This field supports both IPv4 and IPv6 addresses.
UDP Port	Type 514 as the UDP port for syslog events.
Facility	Select a syslog facility value.

Table 735. McAfee Network Security Platform 6.x - 7.x alert notification parameters (continued)	
Parameter	**Description**
Severity Mapping	Select a value to map the **informational**, **low**, **medium**, and **high** alert notification levels to a syslog severity. The options include the following levels: • **Emergency** - The system is down or unusable. • **Alert** - The system requires immediate user input or intervention. • **Critical** - The system should be corrected for a critical condition. • **Error** - The system has non-urgent failures. • **Warning** - The system has a warning message that indicates an imminent error. • **Notice** - The system has notifications, no immediate action required. • **Informational** - Normal operating messages.
Send Notification If	Select the following check boxes: • **The attack definition has this notification option explicitly enabled** • **The following notification filter is matched**, and From the list, select **Severity Informational and later**.
Notify on IPS Quarantine Alert	Select **No** as the notify on IPS quarantine option.
Message Preference	Select the **Customized** option.

7. From the **Message Preference** field, click **Edit** to add a custom message filter.
8. To ensure that alert notifications are formatted correctly, type the following message string:

```
|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"|$IV_ATTACK_ID$|
$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|
$IV_SENSOR_NAME$|$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$|
$IV_DESTINATION_PORT$|$IV_DIRECTION$|$IV_SUB_CATEGORY$
```

   Note: The custom message string must be entered as a single line without carriage returns or spaces. McAfee Network Security Platform expects the format of the custom message to contain a dollar sign ($) as a delimiter before and after each alert element. If you are missing a dollar sign for an element, then the alert event might not be formatted properly.

   You might require a text editor to properly format the custom message string as a single line.
9. Click **Save**.

   As alert events are generated by McAfee Network Security Platform, they are forwarded to the syslog destination you specified. The log source is automatically discovered after enough events are forwarded by the McAfee Network Security Platform appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console and that the **Log Activity** tab displays events from the McAfee Network Security Platform appliance.

Configuring alert events for McAfee Network Security Platform 8.x - 10.x

To collect alert notification events from McAfee Network Security Platform, administrators must configure a syslog forwarder to send events to IBM QRadar

Before you begin

To collect alert notification events from McAfee Network Security Platform, you need McAfee Network Security Platform Manager.

Procedure

1. Log in to the **McAfee Network Security Platform Manager** user interface.
2. Click the **Manager** tab.
3. From the navigation menu, select **Setup** > **Notification** > **IPS Events** > **Syslog**.
4. In the **Enable Syslog Notification** pane, select **Yes**
5. Click **Save**.
6. On the **Syslog** page, Click **New**. If you are using version 10.x, click the **+** sign.
7. On the **Add a Syslog Notification Profile** page, configure the following parameters:

Table 736. McAfee Network Security Platform 8.x - 10.x syslog notification profile parameters

Parameter	Description
Admin Domain	Select any of the following options: • **Current** - Send syslog notifications for alerts in the current domain. This option is selected by default. • **Children** - Include alerts for all child domains within the current domain. (Not applicable to NTBA)
Notification Profile Name	The name of the profile where notifications are sent from.
Target Server	Add a server profile: a. Click **Add**. b. Type the target server profile name. c. Type the IP address of your QRadar Console or Event Collector d. From the **Protocol** list, select **UDP**. e. Type 514 in the **Port** field. f. Click Save.
Facility	Select a syslog facility value from the list.

Table 736. McAfee Network Security Platform 8.x - 10.x syslog notification profile parameters (continued)

Parameter	Description
Severity Mapping	Select a value to map the **informational**, **low**, **medium**, and **high** alert notification levels to a syslog severity. • **Emergency** - The system is down or unusable. • **Alert** - The system requires immediate user input or intervention. • **Critical** - The system should be corrected for a critical condition. • **Error** - The system has non-urgent failures. • **Warning** - The system has a warning message that indicates an imminent error. • **Notice** - The system has notifications, no immediate action required. • **Informational** - Normal operating messages. • **Debug** - Debug level messages.
Notify for All Alerts	Enable this option.
Notify on Quarantine Events	Disable this option.
Message	To ensure that alert notifications are formatted correctly, type the following message string: `|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"|` `$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|` `$IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|` `$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$|` `$IV_DESTINATION_PORT$|$IV_DIRECTION$|$IV_SUB_CATEGORY$` **Note:** The custom message string must be entered as a single line without carriage returns or spaces. McAfee Network Security Platform expects the format of the custom message to contain a dollar sign ($) as a delimiter before and after each alert element. If you are missing a dollar sign for an element, then the alert event might not be formatted properly. You might require a text editor to properly format the custom message string as a single line.

8. Click **Save**.

   The new notification profile displays on the **Syslog** page. As alert events are generated by McAfee Network Security Platform, they are forwarded to the syslog destination that you specified. The log source is automatically discovered in QRadar after enough events are forwarded by the McAfee Network Security Platform appliance. It typically takes a minimum of 25 events to automatically discover a log source.

What to do next

Administrators can log in to the QRadar Console and verify that the log source is created on the QRadar Console and that the **Log Activity** tab displays events from the McAfee Network Security Platform appliance.

Configuring fault notification events for McAfee Network Security Platform 6.x - 7.x

To integrate fault notifications with McAfee Network Security Platform, you must configure your McAfee Network Security Platform to forward fault notification events.

Procedure

1. Log in to the **McAfee Network Security Platform Manager** user interface.
2. On the **Network Security Manager** dashboard, click **Configure**.
3. Expand the **Resource Tree**, and then click **IPS Settings** node.
4. Click the **Fault Notification** tab.
5. From the **Alert Notification** menu, click the **Syslog** tab.
6. Configure the following parameters to forward fault notification events:

Table 737. McAfee Network Security Platform 6.x - 7.x fault notification parameters

Parameter	Description
Enable Syslog Notification	Select **Yes** to enable syslog notifications for McAfee Network Security Platform. You must enable this option to forward events to QRadar.
Admin Domain	Select any of the following options: • **Current** - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default. • **Children** - Select this check box to send syslog notifications for alerts in any child domains within the current domain.
Server Name or IP Address	Type the IP address of your QRadar Console or Event Collector. This field supports both IPv4 and IPv6 addresses.
Port	Type **514** as the port for syslog events.
Facilities	Select a syslog facility value.
Severity Mapping	Select a value to map the **`informational`**, **`low`**, **`medium`**, and **`high`** alert notification level to a syslog severity. The options include the following levels: • **Emergency** - The system is down or unusable. • **Alert** - The system requires immediate user input or intervention. • **Critical** - The system should be corrected for a critical condition. • **Error** - The system has non-urgent failures. • **Warning** - The system has a warning message that indicates an imminent error. • **Notice** - The system has notifications, no immediate action required. • **Informational** - Normal operating messages.
Forward Faults with severity level	Select **Informational and later**.

7. From the **Message Preference** field, click **Edit** to add a custom message filter.
8. To ensure that fault notifications are formatted correctly, type the following message string:

```
|%INTRUSHIELD-FAULT|$IV_FAULT_NAME$|$IV_FAULT_TIME$|
```

Note: The custom message string must be entered as a single line with no carriage returns. McAfee Network Security Platform expects the format of the custom message syslog information to contain a dollar sign ($) delimiter before and after each element. If you are missing a dollar sign for an element, the event might not parse properly.

9. Click **Save**.

   As fault events are generated by McAfee Network Security Platform, they are forwarded to the syslog destination that you specified.

What to do next

You can log in to the QRadar Console and verify that the **Log Activity** tab contains fault events from the McAfee Network Security Platform appliance.

Configuring fault notification events for McAfee Network Security Platform 8.x - 10.x

To integrate fault notifications with McAfee Network Security Platform, you must configure your McAfee Network Security Platform to forward fault notification events.

Procedure

1. Log in to the **McAfee Network Security Platform Manager** user interface.
2. Click the **Manager** tab.
3. From the navigation menu, select **Setup** > **Notification** > **Faults** > **Syslog**.
4. On the **Syslog** page, configure the following parameters to forward fault notification events:

Table 738. McAfee Network Security Platform 8.x - 10.x fault notification parameters

Parameter	Description
Enable Syslog Notification	Select **Yes** to enable syslog notifications for McAfee Network Security Platform. You must enable this option to forward events to QRadar.
Admin Domain	Select any of the following options: • **Current** - Select this check box to send syslog notifications for alerts in the current domain. This option is selected by default. • **Children** - Select this check box to send syslog notifications for alerts in any child domains within the current domain.
Server Name or IP Address	Type the IP address of your QRadar Console or Event Collector. This field supports both IPv4 and IPv6 addresses.
Port	Type **514** as the port for syslog events.
Facilities	Select a syslog facility value.

Table 738. McAfee Network Security Platform 8.x - 10.x fault notification parameters (continued)	
Parameter	**Description**
Severity Mapping	Select a value to map the **informational**, **low**, **medium**, and **high** alert notification level to a syslog severity. The options include the following levels: • **Emergency** - The system is unusable. • **Alert** - The system requires immediate user input or intervention. • **Critical** - The system should be corrected for a critical condition. • **Error** - The system has non-urgent failures. • **Warning** - The system displays a warning message that indicates an imminent error. • **Notice** - The system has notifications, no immediate action required. • **Informational** - Normal operating messages. • **Debug** - Debug level messages
Forward Faults	Select **Informational and later**.

5. From the **Message Preference** field, click **Edit** to add a custom message filter.
6. To ensure that fault notifications are formatted correctly, type the following message string:

   ```
   |%INTRUSHIELD-FAULT|$IV_FAULT_NAME$|$IV_FAULT_TIME$|
   ```

   Note: The custom message string must be entered as a single line with no carriage returns. McAfee Network Security Platform expects the format of the custom message syslog information to contain a dollar sign ($) delimiter before and after each element. If you are missing a dollar sign for an element, the event might not parse properly.
7. Click **Save**.

   As fault events are generated by McAfee Network Security Platform, they are forwarded to the syslog destination that you specified.

What to do next

You can log in to the QRadar Console and verify that the **Log Activity** tab contains fault events from the McAfee Network Security Platform appliance.

McAfee Network Security Platform sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

McAfee Network Security Platform sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that an HTTP login brute force is detected.

```
<116>Feb 7 11:06:51 SyslogAlertForwarder: |5915530749831189905|Signature|2014-02-07 11:06:49
EST|"HTTP: HTTP Login Bruteforce Detected"|0x0040256b|Medium|Unknown|High|My Company|USILSS501|
G3/2|192.168.0.5|0|10.0.1.2|80|Unknown|brute-force
```

Table 739. Highlighted QRadar fields and highlighted payload data	
QRadar field name	**Highlighted payload data**
Date	**2014-02-07 11:06:49 EST**
Event ID	**0x0040256b**
Source IP	**192.168.0.5**
Destination IP	**10.0.1.2**
Destination Port	**80**

Sample 2: The following sample event message shows that a user account is created.

```
<109>Mar 26 07:48:49 mcafee.test: User Account Creation succeeded at 2020-03-26 07:48:49 CET
```

Table 740. Highlighted QRadar fields and highlighted payload data	
QRadar field name	**Highlighted payload data**
Date	**2020-03-26 07:48:49 CET**
Event ID	**User Account Creation succeeded**

McAfee Web Gateway

You can configure McAfee Web Gateway to integrate with IBM QRadar.

Use one of the following methods:

- "Configuring McAfee Web Gateway to communicate with QRadar (syslog)" on page 1147
- "Configuring McAfee Web Gateway to communicate with IBM QRadar (log file protocol)" on page 1148

Note: McAfee Web Gateway is formerly known as McAfee WebWasher.

The following table identifies the specifications for the McAfee Web Gateway DSM:

Table 741. McAfee Web Gateway DSM specifications	
Specification	**Value**
Manufacturer	McAfee
DSM	McAfee Web Gateway
RPM file name	DSM-McAfeeWebGateway-*qradarversion-buildnumber*.noarch
Supported versions	v6.0.0
Protocol	Syslog protocol Log file protocol
Event format	Log Extended Event Format (LEEF)
Recorded event types	All events
Automatically discovered	Yes
Includes identity	No

Table 741. McAfee Web Gateway DSM specifications (continued)	
Specification	**Value**
More information	McAfee website (http://www.mcafee.com)

McAfee Web Gateway DSM integration process

You can integrate McAfee Web Gateway DSM with IBM QRadar.

Use the following procedure:

- Download and install the most recent version of the McAfee Web Gateway DSM RPM from the IBM Support Website onto your QRadar Console.
- For each instance of McAfee Web Gateway, configure your McAfee Web Gateway VPN system to enable communication with QRadar.
- If QRadar does not automatically discover the log source, for each McAfee Web Gateway server you want to integrate, create a log source on the QRadar Console.
- If you use McAfee Web Gateway v7.0.0 or later, create an event map.

Related tasks

"Configuring McAfee Web Gateway to communicate with QRadar (syslog)" on page 1147

"Configuring McAfee Web Gateway to communicate with IBM QRadar (log file protocol)" on page 1148

"Creation of an event map for McAfee Web Gateway events" on page 1150

Configuring McAfee Web Gateway to communicate with QRadar (syslog)

To collect all events from McAfee Web Gateway, you must specify IBM QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your McAfee Web Gateway console.
2. On the **Toolbar**, click **Configuration**.
3. Click the **File Editor** tab.
4. Expand the **Appliance Files** and select the file `/etc/rsyslog.conf`.

   The file editor displays the `rsyslog.conf` file for editing.
5. Modify the `rsyslog.conf` file to include the following information:

```
# send access log to qradar *.info;
daemon.!=info;
mail.none;authpriv.none;
cron.none -/var/log/messages *.info;mail.none;
authpriv.none;
cron.none
@<IP Address>:<Port>
```

   Where:

   - <*IP Address*> is the IP address of QRadar.
   - <*Port*> is the syslog port number, for example 514.
6. Click **Save Changes**.

   You are now ready to import a policy for the syslog handler on your McAfee Web Gateway appliance. For more information, see "Importing the Syslog Log Handler" on page 1148.

Importing the Syslog Log Handler

About this task

To Import a policy rule set for the syslog handler:

Procedure

1. From the support website, download the following compressed file:

   `log_handlers-1.1.tar.gz`
2. Extract the file.

   The extract file provides XML files that are version dependent to your McAfee Web Gateway appliance.

Table 742. McAfee Web Gateway required log handler file	
Version	**Required XML file**
McAfee Web Gateway V7.0	syslog_loghandler_70.xml
McAfee Web Gateway V7.3	syslog_loghandler_73.xml

3. Log in to your McAfee Web Gateway console.
4. Using the menu toolbar, click **Policy**.
5. Click **Log Handler**.
6. Using the menu tree, select **Default**.
7. From the **Add** list, select **Rule Set from Library**.
8. Click **Import from File** button.
9. Navigate to the directory containing the syslog_handler file you downloaded and select **syslog_loghandler.xml** as the file to import.

   Note: If the McAfee Web Gateway appliance detects any conflicts with the rule set, you must resolve the conflict. For more information, see your *McAfee Web Gateway documentation*.
10. Click **OK**.
11. Click **Save Changes**.
12. You are now ready to configure the log source in QRadar.

    QRadar automatically discovers syslog events from a McAfee Web Gateway appliance.

    If you want to manually configure QRadar to receive syslog events, select McAfee Web Gateway from the **Log Source Type** list.

Related tasks

"Adding a log source" on page 5

Configuring McAfee Web Gateway to communicate with IBM QRadar (log file protocol)

The McAfee Web Gateway appliance gives the option to forward event log files to an interim file server for retrieval by QRadar.

Procedure

1. From the support website, download the following file:

log_handlers-1.1.tar.gz

2. Extract the file.

   This gives you the access handler file that is needed to configure your McAfee Web Gateway appliance.

   access_log_file_loghandler.xml

3. Log in to your McAfee Web Gateway console.
4. Using the menu toolbar, click **Policy**.

   Note: If there is an existing access log configuration in your McAfee Web Gateway appliance, you must delete the existing access log from the **Rule Set Library** before you add the access_log_file_loghandler.xml.

5. Click **Log Handler**.
6. Using the menu tree, select **Default**.
7. From the **Add** list, select **Rule Set from Library**.
8. Click **Import from File** button.
9. Navigate to the directory that contains the access_log_file_loghandler.xml file you downloaded and select syslog_loghandler.xml as the file to import.

   When the rule set is imported for access_log_file_loghandler.xml, a conflict can occur stating the Access Log Configuration exists already in the current configuration and a conflict solution is presented.

10. If the McAfee Web Gateway appliance detects that the Access Log Configuration exists already, select the **Conflict Solution**: **Change name** option that is presented to resolve the rule set conflict.

    For more information on resolving conflicts, see your *McAfee Web Gateway vendor documentation*.

    You must configure your access.log file to be pushed to an interim server on an auto rotation. It does not matter if you push your files to the interim server based on time or size for your access.log file. For more information on auto rotation, see your *McAfee Web Gateway vendor documentation*.

    Note: Due to the size of access.log files that are generated, it is suggested that you select the option GZIP files after rotation in your McAfee Web Gate appliance.

11. Click **OK**.
12. Click **Save Changes**.

    Note: By default McAfee Web Gateway is configured to write access logs to the /opt/mwg/log/user-defined-logs/access.log/ directory.

What to do next

You are now ready to configure QRadar to receive access.log files from McAfee Web Gateway. For more information, see "Pulling data by using the log file protocol" on page 1149.

Pulling data by using the log file protocol

A log file protocol source allows IBM QRadar to retrieve archived log files from a remote host. The McAfee Web Gateway DSM supports the bulk loading of access.log files by using the log file protocol source. The default directory for the McAfee Web Gateway access logs is the /opt/mwg/log/user-defined-logs/access.log/ directory.

About this task

You can now configure the log source and protocol in QRadar.

Procedure

1. To configure QRadar to receive events from a McAfee Web Gateway appliance, select **McAfee Web Gateway** from the **Log Source Type** list.
2. To configure the protocol, you must select the **Log File** option from the **Protocol Configuration** list.
3. To configure the **File Pattern** parameter, you must type a regex string for the `access.log` file, such as access[0-9]+\.log.

   Note: If you selected to **GZIP** your `access.log` files, you must type `access[0-9]+\.log\.gz` for the **FIle Pattern** field and from the **Processor** list, select **GZIP**.

Creation of an event map for McAfee Web Gateway events

Event mapping is needed for events that are collected from McAfee Web Gateway v7.0.0 and later, which are identified as Unknown and not covered by the base QID map.

You can individually map each event for your device to an event category in IBM QRadar. Mapping events allows QRadar to identify, coalesce, and track recurring events from your network devices. Until you map an event, some events that are displayed in the **Log Activity** tab for McAfee Web Gateway are categorized as Unknown, and some events might be already assigned to an existing QID map. Unknown events are easily identified as the **Event Name** column and **Low Level Category** columns display Unknown.

Discovering unknown events

This procedure ensures that you map all event types and that you do not miss events that are not generated frequently, repeat this procedure several times over a period.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select the log source group or **Other**.

   Log sources that are not assigned to a group are categorized as **Other**.
6. From the **Log Source** list, select your McAfee Web Gateway log source.
7. Click **Add Filter**.

   The **Log Activity** tab is displayed with a filter for your log source.
8. From the **View** list, select **Last Hour**.

   Any events that are generated by the McAfee Web Gateway DSM in the last hour are displayed. Events that are displayed as Unknown in the **Event Name** column or **Low Level Category** column require event mapping.

   Note: You can save your existing search filter by clicking **Save Criteria**.

   You are now ready to modify the event map.

Modifying the event map

Modify an event map to manually categorize events to a QRadar Identifier (QID) map.

About this task

Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

Note: Events that do not have a defined log source cannot be mapped to an event. Events without a log source display `SIM Generic Log` in the **Log Source** column.

Procedure

1. On the **Event Name** column, double-click an unknown event for McAfee Web Gateway.

   The detailed event information is displayed.
2. Click **Map Event**.
3. From the Browse for QRadar Identifier pane, select any of the following search options to narrow the event categories for a QRadar Identifier (QID):

   - From the **High-Level Category** list, select a high-level event categorization.
   - From the **Low-Level Category** list, select a low-level event categorization.
   - From the **Log Source Type** list, select a log source type.

   The **Log Source Type** list gives the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, McAfee Web Gateway provides policy events, you might select another product that likely captures similar events.

   To search for a QID by name, type a name in the **QID/Name** field.

   The **QID/Name** field gives the option to filter the full list of QIDs for a specific word, for example, policy.
4. Click **Search**.

   A list of QIDs are displayed.
5. Select the QID that you want to associate to your unknown event.
6. Click **OK**.

   QRadar maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.

   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

McAfee Web Gateway sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

McAfee Web Gateway sample message when you use the Syslog protocol

The following sample event message shows that web access is verified.

```
<30>Oct 13 15:59:02 WebGatewayHost mwg: LEEF:1.0|McAfee|Web Gateway|8.2.9|0|devTime=1602597542000|
src=10.10.10.10|usrName=user1|httpStatus=204|dst=10.20.10.20|urlCategories=Messaging|blockReason=|
url=https://www.example.com/rt-pub/node/hub/negotiate?
appId=180&sId=4A87EE607A615896&cId=8B1D&dev=Personal%20computer&br=Chrome&os=Windows&cc=IT&rc=RM&v
=0.1
```

```
<30>Oct 13 15:59:02 WebGatewayHost mwg: LEEF:1.0|McAfee|Web Gateway|8.2.9|0|
devTime=1602597542000|src=10.10.10.10|usrName=user1|httpStatus=204|dst=10.20.10.20|
urlCategories=Messaging|blockReason=|url=https://www.example.com/rt-pub/node/hub/negotiate?
appId=180&sId=4A87EE607A615896&cId=8B1D&dev=Personal%20computer&br=Chrome&os=Windows&cc=IT&rc=RM
&v=0.1
```

Table 743. Highlighted values in the McAfee Web Gateway sample event

QRadar field name	Highlighted values in the event payload
Event ID	**0**

Table 743. Highlighted values in the McAfee Web Gateway sample event (continued)

QRadar field name	Highlighted values in the event payload
Event Category	This DSM doesn't have a category field to key from for the device in the payloads. QRadar provides the *value* as a static category.
Source IP	**src**
Destination IP	**dst**
Username	**usrName**

Chapter 98. Syslog log source parameters for MetaInfo MetaIP

If QRadar does not automatically detect the log source, add a MetaIP log source on the QRadar Console by using the syslog.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Metadata appliances:

Table 744. Syslog log source parameters for the MetaInfo MetaIP DSM

Parameter	Value
Log Source type	MetaInfo MetaIP
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your MetaInfo MetaIP appliances.

Related tasks

Adding a log source

Chapter 99. Microsoft

IBM QRadar supports a range of Microsoft products.

Microsoft 365 Defender

The IBM QRadar Microsoft 365 Defender DSM collects events from a Microsoft 365 Defender service by using the Microsoft Azure Event Hubs protocol to collect Streaming API data. You can use the Defender for Endpoint SIEM REST API protocol to collect alerts and device events from a Microsoft 365 Defender service.

The Microsoft 365 Defender DSM also collects alerts from the Microsoft Defender for Endpoint Service Alerts V2 API by using the Microsoft Graph API protocol.

Important:

- The Microsoft Windows Defender ATP DSM name is now the Microsoft 365 Defender DSM. The DSM RPM name remains as Microsoft Windows Defender ATP in QRadar.
- Due to a change in the Microsoft Defender API suite as of 25 November 2021, Microsoft no longer allows the onboarding of new integrations with their SIEM API. For more information, see Deprecating the legacy SIEM API (https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/deprecating-the-legacy-siem-api/ba-p/3139643).

  The Streaming API can be used with the Microsoft Azure Event Hubs protocol to provide event and alert forwarding to QRadar. For more information about the service and its configuration, see Configure Microsoft 365 Defender to stream Advanced Hunting events to your Azure Event Hub (https://docs.micosoft.com/en-us/microsoft-365/security/defender/streaming-api-event-hub?view=o365-worldwide)

Integrate a Microsoft 365 Defender service when you use the Microsoft Azure Event Hubs protocol

If you want to integrate Microsoft 365 Defender service with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (http://www.ibm.com/support).
   - Protocol Common RPM
   - Microsoft Azure Event Hubs Protocol RPM
   - DSM Common RPM
   - Microsoft 365 Defender DSM RPM
2. Optional: Create a storage account. For more information, see Create a storage account.

   Important: You must have a storage account to connect to an event hub. For more information, see Microsoft Azure Event Hubs protocol FAQ.
3. Optional: Create an event hub. For more information, see Quickstart: Create an event hub using Azure portal.
4. Configure Microsoft 365 Defender to send advanced hunting events to a Microsoft Azure Event Hub. For more information, see Configure Microsoft Defender to stream Advanced Hunting events to your Azure Event Hub.
5. If QRadar does not automatically detect the log source, add a Microsoft 365 Defender log source that uses the Microsoft Azure Event Hubs protocol on the QRadar Console. For more information about the protocol, see Microsoft Azure Event Hubs log source parameters for Microsoft 365 Defender.

Integrate a Microsoft 365 Defender service when you use the Microsoft Defender for Endpoint SIEM REST API protocol

If you want to integrate a Microsoft 365 Defender service with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website.
   - Protocol Common RPM
   - Microsoft Defender for Endpoint SIEM REST API Protocol RPM
   - DSMCommon RPM
   - Microsoft 365 Defender DSM RPM
2. Add a Microsoft 365 Defender log source that uses the Microsoft Defender for Endpoint SIEM REST API protocol on the QRadar Console. QRadar does not automatically detect the Microsoft Defender for Endpoint SIEM REST API. For more information, see Microsoft Defender for Endpoint SIEM REST API log source parameters for Microsoft 365 Defender.

Integrate a Microsoft Defender for Endpoint service when you use the Microsoft Graph Security API protocol

If you want to integrate a Microsoft Defender for Endpoint service with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website.
   - Protocol Common RPM
   - Microsoft Graph Security API Protocol RPM
   - DSMCommon RPM
   - Microsoft 365 Defender DSM RPM
2. Add a Microsoft 365 Defender log source that uses the Microsoft Graph Security API protocol on the QRadar Console. QRadar does not automatically detect the Microsoft Graph Security API. For more information, see Microsoft Graph Security API log source parameters for Microsoft 365 Defender.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Microsoft 365 Defender DSM Specifications

The following table describes the specifications for the Microsoft 365 Defender DSM.

Important:

- The Microsoft Windows Defender ATP DSM name is now the Microsoft 365 Defender DSM. The DSM RPM name remains as Microsoft Windows Defender ATP in QRadar.
- Due to a change in the Microsoft Defender API suite as of 25 November 2021, Microsoft no longer allows the onboarding of new integrations with their SIEM API. For more information, see Deprecating the legacy SIEM API (https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/deprecating-the-legacy-siem-api/ba-p/3139643).

  The Streaming API can be used with the Microsoft Azure Event Hubs protocol to provide event and alert forwarding to QRadar. For more information about the service and its configuration, see Configure Microsoft 365 Defender to stream Advanced Hunting events to your Azure Event Hub (https://docs.micosoft.com/en-us/microsoft-365/security/defender/streaming-api-event-hub?view=o365-worldwide)

Table 745. Microsoft 365 Defender DSM specifications	
Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft 365 Defender
RPM file name	`DSM-MicrosoftWindowsDefenderATP-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocols	Microsoft Defender for Endpoint SIEM REST API Microsoft Azure Event Hubs Microsoft Graph Security API
Event format	JSON
Recorded event types when you use the Microsoft Azure Event Hubs protocol.	The Microsoft 365 Defender DSM supports the following events when you use the Microsoft Azure Event Hubs protocol: Alerts (Alerts are supported only for Microsoft Defender for Endpoint.): • AlertInfo • AlertEvidence Device: • DeviceInfo • DeviceNetworkInfo • DeviceProcessEvents • DeviceNetworkEvents • DeviceFileEvents • DeviceRegistryEvents • DeviceLogonEvents • DeviceEvents • DeviceFileCertificateInfo • DeviceImageLoadEvents Email: • EmailEvents • EmailAttachmentInfo • EmailPostDeliveryEvents • EmailUrlInfo
Recorded event types when you use the Microsoft Defender for Endpoint SIEM REST API protocol.	Windows Defender ATP Windows Defender AV Third party TI Customer TI Bitdefender

Table 745. Microsoft 365 Defender DSM specifications (continued)	
Specification	**Value**
Recorded event types when you use the Microsoft Graph Security API protocol.	Microsoft Defender for Endpoint Alerts V2 Microsoft Defender for Cloud App Security Alerts V2 Microsoft Defender for Identity Alerts V2 Microsoft Defender for Office 365 Alerts V2 Microsoft Defender for Azure AD Identity Protection Alerts V2 Microsoft Defender for Data Loss Prevention Alerts V2
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Microsoft 365 Defender documentation (https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide)

Microsoft Defender for Endpoint SIEM REST API log source parameters for Microsoft 365 Defender

If IBM QRadar does not automatically detect the log source, add a Microsoft 365 Defender log source on the QRadar Console by using Microsoft Defender for Endpoint SIEM REST API protocol.

When you use the Microsoft Defender for Endpoint SIEM REST API protocol, there are specific parameters that you must use.

Important:

- The Microsoft Windows Defender ATP DSM name is now the Microsoft 365 Defender DSM. The DSM RPM name remains as Microsoft Windows Defender ATP in QRadar.
- Due to a change in the Microsoft Defender API suite as of 25 November 2021, Microsoft no longer allows the onboarding of new integrations with their SIEM API. For more information, see Deprecating the legacy SIEM API (https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/deprecating-the-legacy-siem-api/ba-p/3139643).

  The Streaming API can be used with the Microsoft Azure Event Hubs protocol to provide event and alert forwarding to QRadar. For more information about the service and its configuration, see Configure Microsoft 365 Defender to stream Advanced Hunting events to your Azure Event Hub (https://docs.micosoft.com/en-us/microsoft-365/security/defender/streaming-api-event-hub?view=o365-worldwide)

The following table describes the parameters that require specific values to collect Microsoft Defender for Endpoint SIEM REST API events from Microsoft 365 Defender:

Table 746. Microsoft Defender for Endpoint SIEM REST API log source parameters for the Microsoft 365 Defender DSM	
Parameter	**Value**
`Log Source type`	Microsoft 365 Defender

Table 746. Microsoft Defender for Endpoint SIEM REST API log source parameters for the Microsoft 365 Defender DSM (continued)	
Parameter	**Value**
Protocol Configuration	Microsoft Defender for Endpoint SIEM REST API

For a complete list of Microsoft Defender for Endpoint SIEM REST API log source protocol parameters and their values, see Microsoft Defender for Endpoint SIEM REST API protocol configuration options.

Related tasks
Adding a log source

Microsoft Azure Event Hubs log source parameters for Microsoft 365 Defender

If IBM QRadar does not automatically detect the log source, add a Microsoft 365 Defender log source on the QRadar Console by using the Microsoft Azure Event Hubs protocol.

When you use the Microsoft Azure Event Hubs protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Microsoft Azure Event Hubs events from Microsoft 365 Defender:

Table 747. Microsoft Azure Event Hubs log source parameters for the Microsoft 365 Defender DSM	
Parameter	**Value**
Log Source type	Microsoft 365 Defender
Protocol Configuration	Microsoft Azure Event Hubs
Log Source Identifier	Use an identifiable name or IP address for the log source. When the **Use as a Gateway Log Source** parameter is enabled, the **Log Source Identifier** value is not used.

For a complete list of Microsoft Azure Event Hubs protocol parameters and their values, see Microsoft Azure Event Hubs protocol configuration options.

Related tasks
Adding a log source

Microsoft Graph Security API log source parameters for Microsoft 365 Defender

If IBM QRadar does not automatically detect the log source, add a Microsoft 365 Defender log source on the QRadar Console by using the Microsoft Graph Security API protocol.

When you use the Microsoft Graph Security API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Microsoft Graph Security API events from Microsoft 365 Defender:

Table 748. Microsoft Graph Security API log source parameters for the Microsoft 365 Defender DSM	
Parameter	**Value**
Log Source type	Microsoft 365 Defender
Protocol Configuration	Microsoft Graph Security API

Table 748. Microsoft Graph Security API log source parameters for the Microsoft 365 Defender DSM (continued)	
Parameter	**Value**
Log Source Identifier	Use a unique name for the log source.
API	**Alerts V2 (/alerts_v2)**

For a complete list of Microsoft Graph Security API protocol parameters and their values, see Microsoft Graph Security API protocol configuration options.

Related tasks

Adding a log source

Microsoft 365 Defender sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important:

- The Microsoft Windows Defender ATP DSM name is now the Microsoft 365 Defender DSM. The DSM RPM name remains as Microsoft Windows Defender ATP in QRadar.
- Due to a change in the Microsoft Defender API suite as of 25 November 2021, Microsoft no longer allows the onboarding of new integrations with their SIEM API. For more information, see Deprecating the legacy SIEM API (https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/deprecating-the-legacy-siem-api/ba-p/3139643).

  The Streaming API can be used with the Microsoft Azure Event Hubs protocol to provide event and alert forwarding to QRadar. For more information about the service and its configuration, see Configure Microsoft 365 Defender to stream Advanced Hunting events to your Azure Event Hub (https://docs.micosoft.com/en-us/microsoft-365/security/defender/streaming-api-event-hub?view=o365-worldwide)

Microsoft 365 Defender sample messages when you use the Microsoft Azure Event Hubs protocol

Sample 1: The following sample event message shows a successful scheduled task update.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.


```
"{"time":"2021-07-21T00:57:23.0186119Z","tenantId":"abc12345-123a-123a-456b-
abcdefg12345","operationName":"Publish","category":"AdvancedHunting-DeviceEvents","properties":
{"AccountSid":null,"AccountDomain":null,"AccountName":null,"LogonId":null,"FileName":null,"Folde
rPath":null,"MD5":null,"SHA1":null,"FileSize":null,"SHA256":null,"ProcessCreationTime":null,"Pro
cessTokenElevation":null,"RemoteUrl":null,"RegistryKey":null,"RegistryValueName":null,"RegistryV
alueData":null,"RemoteDeviceName":null,"FileOriginIP":null,"FileOriginUrl":null,"LocalIP":null,"
LocalPort":null,"RemoteIP":null,"RemotePort":null,"ProcessId":null,"ProcessCommandLine":null,"Ad
ditionalFields":"{\"TaskName\":\"\\\\Microsoft\\\\Windows\\\\UpdateOrchestrator\\\\Schedule
Maintenance
Work\"}","ActionType":"ScheduledTaskUpdated","InitiatingProcessVersionInfoCompanyName":null,"Ini
tiatingProcessVersionInfoProductName":null,"InitiatingProcessVersionInfoProductVersion":null,"In
itiatingProcessVersionInfoInternalFileName":null,"InitiatingProcessVersionInfoOriginalFileName":
null,"InitiatingProcessVersionInfoFileDescription":null,"InitiatingProcessFolderPath":null,"Init
iatingProcessFileName":null,"InitiatingProcessFileSize":null,"InitiatingProcessMD5":null,"Initia
tingProcessSHA256":null,"InitiatingProcessSHA1":null,"InitiatingProcessLogonId":999,"InitiatingP
rocessAccountSid":"S-1-5-18","InitiatingProcessAccountDomain":"m365defender","InitiatingProcessA
ccountName":"client-
pc$","InitiatingProcessAccountUpn":null,"InitiatingProcessAccountObjectId":null,"InitiatingProce
ssCreationTime":null,"InitiatingProcessId":null,"InitiatingProcessCommandLine":null,"InitiatingP
rocessParentCreationTime":null,"InitiatingProcessParentId":null,"InitiatingProcessParentFileName
":null,"DeviceId":"11112222333344445555666677778888999aaaa","AppGuardContainerId":"","MachineGr
oup":null,"Timestamp":"2021-07-21T00:55:44.2280946Z","DeviceName":"client-
pc.example.net","ReportId":60533}}" );
```

Table 749. Highlighted fields in the Microsoft 365 Defender event	
QRadar field name	**Highlighted payload field name**
Event Category	category
Event ID	ActionType
Device Time	Timestamp

Sample 2: The following sample event message shows an alert to possible keylogging activity.


```
{"time":"2021-09-09T00:40:17.7066896Z","tenantId":"abc12345-123a-123a-456b-
abcdefg12345","operationName":"Publish","category":"AdvancedHunting-AlertInfo","properties":
{"AlertId":"da637667448174310467_1631502683","Timestamp":"2021-09-09T00:39:17.1650944Z","Title":
"Possible keylogging activity","ServiceSource":"Microsoft Defender for
Endpoint","Category":"Collection","Severity":"High","DetectionSource":"EDR","MachineGroup":null,
"AttackTechniques":"[\"Input Capture (T1056)\"]"}}
```


Table 750. Highlighted fields in the Microsoft 365 Defender event	
QRadar field name	**Highlighted payload field name**
Event Category	category
Event ID	Title
Device Time	Timestamp

Microsoft 365 Defender sample messages when you use the Microsoft Defender for Endpoint SIEM REST API protocol

Sample 1: The following sample event message shows suspicious activity.


```
{"AlertTime":"2017-12-27T03:54:41.1914393Z","ComputerDnsName":"<ComputerDnsName>","AlertTitle":"
<AlertTitle>","Category":"CommandAndControl","Severity":"<Severity>","AlertId":"<AlertId>","Acto
r":"<Actor>","LinkToWDATP":"<LinkToWDATP>","IocName":"<IocName>","IocValue":"<IocValue>","Creato
rIocName":"<CreatorIocName>","CreatorIocValue":"<CreatorIocValue>","Sha1":"<Sha1>","FileName":"<
FileName>","FilePath":"<FilePath>","IpAddress":"192.0.2.0","Url":"<Url>","IoaDefinitionId":"<Ioa
DefinitionId>","UserName":"qradar1","AlertPart":"<AlertPart>","FullId":"<FullId>","LastProcessed
TimeUtc":"2017-12-27T07:16:34.1412283Z","ThreatCategory":"<ThreatCategory>","ThreatFamily":"<Thr
eatFamily>","ThreatName":"<ThreatName>","RemediationAction":"<RemediationAction>","RemediationIs
Success":"<RemediationIsSuccess>","Source":"WindowsDefenderAtp","Md5":"<Md5>","Sha256":"<Sha256>
","WasExecutingWhileDetected":"<WasExecutingWhileDetected>","UserDomain":"<UserDomain>","LogOnUs
ers":"<LogOnUsers>","MachineDomain":"<MachineDomain>","MachineName":"<MachineName>","InternalIPv
4List":"192.0.2.0;127.0.0.1","InternalIPv6List":"2001:0DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF","FileH
ash":"<FileHash>","ExternalId":"<ExternalId>","IocUniqueId":"IocUniqueId"}
```


Table 751. Highlighted fields in the Microsoft 365 Defender sample event	
QRadar field name	**Highlighted payload field name**
Device Time	AlertTime
Event ID	Category
Source IP	IpAddress
Source IP v6	InternalIPv6List
Username	UserName

Sample 2: The following sample event message shows that a backdoor access is detected.


```
{"AlertTime":"2017-11-22T18:01:32.1887775Z","ComputerDnsName":"<ComputerDnsName>","AlertTitle":"
<AlertTitle>","Category":"Backdoor","Severity":"<Severity>","AlertId":"<AlertId","Actor":"<Actor
>","LinkToWDATP":"<LinkToWDATP>","IocName":"<IocName>","IocValue":"<IocValue>","CreatorIocName":
"<CreatorIocName>","CreatorIocValue":"<CreatorIocValue>","Sha1":"<Sha1>","FileName":"<FileName>"
,"FilePath":"<FilePath>","IpAddress":"192.0.2.0","Url":"<Url>","IoaDefinitionId":"<IoaDefinition
```

Id>","**UserName**":"qradar1","AlertPart":"<AlertPart>","FullId":"<FullId>","LastProcessedTimeUtc":"
2017-11-22T18:01:49.8739015Z","ThreatCategory":"<ThreatCategory>","ThreatFamily":"<ThreatFamily>
","ThreatName":"<ThreatName>","RemediationAction":"<RemediationAction>","RemediationIsSuccess":"
<RemediationIsSuccess>","Source":"WindowsDefenderAtp","Md5":"<Md5>","Sha256":"<Sha256>","WasExec
utingWhileDetected":"<WasExecutingWhileDetected>","UserDomain":"<UserDomain>","LogOnUsers":"<Log
OnUsers>","MachineDomain":"<MachineDomain>","MachineName":"<MachineName>","InternalIPv4List":"19
2.0.2.0;127.0.0.1","**InternalIPv6List**":"2001:0DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF","FileHash":"<Fil
eHash>","ExternalId":"<ExternalId>","IocUniqueId":"IocUniqueId"}

Table 752. Highlighted fields in the Microsoft 365 Defender sample event

QRadar field name	Highlighted payload field name
Device Time	AlertTime
Event ID	Category
Source IP	IpAddress
Source IP v6	InternalIPv6List
Username	UserName

Microsoft 365 Defender sample messages when you use the Microsoft Graph Security API protocol

The following sample event message shows that a lateral movement on another device was observed in close time proximity to a suspicious network event on this device. This could mean that an attacker is attempting to move laterally across devices to gather data or elevate privileges. This alert was triggered based on a Microsoft Defender for Endpoint alert.

{"id":"da637789431774501659_-1621338217","providerAlertId":"da637789431774501659_-1621338217","i
ncidentId":"5","status":"resolved","severity":"medium","classification":null,"determination":nul
l,"serviceSource":"microsoftDefenderForEndpoint","detectionSource":"microsoft365Defender","detec
torId":"ab3e5834-3d38-42c5-aaa6-
c1cfc6c02882","tenantId":"24d3dca4-61f8-4b86-8e22-612b71d65386","title":"Possible lateral
movement","description":"Lateral movement on another device was observed in close time
proximity to a suspicious network event on this device. This could mean that an attacker is
attempting to move laterally across devices to gather data or elevate privileges. This alert
was triggered based on a Microsoft Defender for Endpoint alert.","recommendedActions":"A.
Validate the alert.\r\n1. Investigate the process, its behaviors, and the endpoint involved in
the original alert for suspicious activity.\r\n2. Check for other suspicious activities in the
device timeline.\r\n3. Locate unfamiliar processes in the process tree. Check files for
prevalence, their locations, and digital signatures.\r\n4. Submit relevant files for deep
analysis and review file behaviors.\r\n5. Identify unusual system activity with system
owners.\r\n\r\nB. Scope the incident. Find related device, network addresses, and files in the
incident graph.\r\n\r\nC. Contain and mitigate the breach. Stop suspicious processes, isolate
affected devices, decommission compromised accounts or reset passwords, block IP addresses and
URLs, and install security updates.\r\n\r\nD. Contact your incident response team, or contact
Microsoft support for investigation and remediation
services.","**category**":"LateralMovement","**assignedTo**":"testUser@testUser@example.test","alertWebU
rl":"https://security.microsoft.com/alerts/da637789431774501659_-1621338217?
tid=24d3dca4-61f8-4b86-8e22-612b71d65386","incidentWebUrl":"https://security.microsoft.com/
incidents/5?
tid=24d3dca4-61f8-4b86-8e22-612b71d65386","actorDisplayName":null,"threatDisplayName":null,"thre
atFamilyName":null,"mitreTechniques":
["T1570","T1021.002","T1021.003","T1021.004","T1021.006"],"**createdDateTime**":"2022-01-28T05:06:17
.4503018Z","lastUpdateDateTime":"2022-01-28T07:11:29.6933333Z","resolvedDateTime":"2022-01-28T05
:21:32.5866667Z","firstActivityDateTime":"2022-01-28T04:53:35.0699463Z","lastActivityDateTime":"
2022-01-28T04:53:35.0699463Z","comments":[],"evidence":
[{"@odata.type":"#microsoft.graph.security.deviceEvidence","**createdDateTime**":"2022-01-28T05:06:1
7.51Z","evidenceRole":"impacted","verdict":"unknown","remediationStatus":"none","remediationStat
usDetails":null,"firstSeenDateTime":"2022-01-28T01:15:01.628Z","mdeDeviceId":"12345testmdeDevice
id","azureAdDeviceId":null,"deviceDnsName":"testHost.test","osPlatform":"Windows10","osBuild":17
763,"version":"1809","healthStatus":"active","riskScore":"high","rbacGroupId":0,"rbacGroupName":
null,"onboardingStatus":"onboarded","defenderAvStatus":"updated","loggedOnUsers":
[{"accountName":"testUser","domainName":"MPRTDEV"}]},
{"@odata.type":"#microsoft.graph.security.processEvidence","**createdDateTime**":"2022-01-28T05:06:1
7.51Z","evidenceRole":"related","verdict":"unknown","remediationStatus":"none","remediationStatu
sDetails":null,"processId":4,"parentProcessId":0,"processCommandLine":"","processCreationDateTim
e":"2022-01-28T01:01:49.3539999Z","parentProcessCreationDateTime":null,"detectionStatus":null,"m
deDeviceId":null,"parentProcessImageFile":null,"imageFile":
{"sha1":"3791cf139c5f9e5c97e9c091f73e441b6a9bbd30","sha256":"e2f1857de3560a5237ca7ea661fc3688715
bbbf6baa483511d49baac4ce1acf9","fileName":"System","filePath":"c:\\windows\\system32\
\ntoskrnl.exe","fileSize":null,"filePublisher":null,"signer":null,"issuer":null},"userAccount":

```
{"accountName":"system","domainName":null,"userSid":"S-1-1-1","azureAdUserId":null,"userPrincipa
lName":null}},
{"@odata.type":"#microsoft.graph.security.ipEvidence","createdDateTime":"2022-01-28T05:06:17.51Z
","evidenceRole":"related","verdict":"unknown","remediationStatus":"none","remediationStatusDeta
ils":null,"ipAddress":"10.0.0.5"},
{"@odata.type":"#microsoft.graph.security.urlEvidence","createdDateTime":"2022-01-28T05:06:17.51
Z","evidenceRole":"related","verdict":"unknown","remediationStatus":"none","remediationStatusDet
ails":null,"url":"mprtdev-win10b"},
{"@odata.type":"#microsoft.graph.security.userEvidence","createdDateTime":"2022-01-28T05:06:17.5
1Z","evidenceRole":"impacted","verdict":"unknown","remediationStatus":"none","remediationStatusD
etails":null,"userAccount":
{"accountName":null,"domainName":null,"userSid":null,"azureAdUserId":null,"userPrincipalName":nu
ll}}]}
```


Table 753. Highlighted fields in the Microsoft 365 Defender sample event

QRadar field name	Highlighted payload field name
Device Time	createdDateTime
Event ID	Category
Event Category	detectionSource
Source IP	ipAddress
Username	assignedTo

Microsoft Entra ID

The IBM QRadar DSM for Microsoft Entra ID Audit logs collects events such as user creation, role assignment, and group assignment events. The Microsoft Entra ID Sign-in logs collects user sign-in activity events.

Important: The **Microsoft Azure Active Directory DSM** name is now the **Microsoft Entra ID DSM**. The DSM RPM name remains as **Microsoft Azure Active Directory** in QRadar.

To integrate Microsoft Entra ID with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website. Download and install the most recent version of the following RPMs on your QRadar Console.
   - Protocol Common RPM
   - DSM Common
   - Microsoft Azure Event Hubs Protocol RPM
   - Microsoft Azure Platform DSM RPM
   - Microsoft Azure Active Directory DSM RPM
2. If you do not have an existing storage account, create a storage account. For more information, see Create a storage account.

   Important: You must have a storage account to connect to an event hub. For more information, see Microsoft Azure Event Hubs protocol FAQ.
3. If you do not have an existing event hub, create an event hub. For more information, see Quickstart: Create an event hub using Azure portal.
4. Configure Microsoft Entra ID to forward events to an Azure Event Hub by streaming events through diagnostic logs. For more information, see Tutorial: Stream Azure Active Directory logs to an Azure Event Hub.
5. If QRadar does not automatically detect the log source, add a Microsoft Entra ID log source on the QRadar Console by using the Microsoft Azure Event Hubs protocol. For more information about configuring the protocol, see Microsoft Active Directory log source parameters.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Microsoft Entra ID DSM specifications

When you configure the Microsoft Entra ID DSM, understanding the specifications for the Microsoft Entra ID DSM can help ensure a successful integration. For example, knowing what protocol to use before you begin can help reduce frustration during the configuration process.

Table 754. Microsoft Entra ID DSM specifications

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft Entra ID
RPM file name	`DSM-MicrosoftAzureActiveDirectory-`*`QRadar_version-build_number`*`.noarch.rpm`
Protocol	Microsoft Azure Event Hubs
Event format	JSON
Recorded event types	Sign-In logs, Audit logs
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Azure Active Directory documentation (https://docs.microsoft.com/en-ca/azure/active-directory/) Azure Event Hubs documentation (https://docs.microsoft.com/en-us/azure/event-hubs/)

Microsoft Entra ID log source parameters

When you add an Entra ID log source on the QRadar Console by using the Microsoft Azure Event Hubs protocol, there are specific parameters you must use.

The following table describes the parameters that require specific values to retrieve Microsoft Entra ID events from Microsoft Entra ID:

Table 755. Microsoft Azure Event Hubs protocol log source parameters for the Microsoft Entra ID DSM

Parameter	Value
`Log Source type`	Microsoft Entra ID
`Protocol Configuration`	Microsoft Azure Event Hubs
`Log Source Identifier`	The Log Source Identifier can be any valid value, including the same value as the Log Source Name parameter, and doesn't need to reference a specific server. If you configured multiple Microsoft Entra ID log sources, you might want to identify the first log source as `EntraID-1`, the second log source as `EntraID-2`, and the third log source as `EntraID-3`.

For a complete list of Microsoft Entra ID protocol parameters and their values, see Microsoft Azure Event Hubs protocol configuration options.

Related concepts

"Microsoft Entra ID" on page 1163

Related information

"Adding a log source" on page 5

Microsoft Entra ID sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides sample event messages for the Microsoft Entra ID DSM:

Important: Due to formatting, paste the message formats into a text editor and then remove any carriage return or line feed characters.

Table 756. Microsoft Entra ID sample event message supported by Microsoft Entra ID

Event name	Low level category	Sample log message
Add member to group-success	Group Member Added	{"time":"2019-09-03T20:01:53.7619661Z","resourceId":"/tenants/1111a11a-111a-11a1-1111-111a1a2aa11a/providers/Microsoft.aadiam","operationName":"Add member to group","operationVersion":"1.0","category":"AuditLogs","tenantId":"1111a11a-111a-11a1-1111-111a1a2aa11a","resultSignature":"None","durationMs":0,"correlationId":"1111a11a-111a-11a1-1111-111a1a2aa11a","level":"Informational","properties":{"id":"Directory_AAA11_11111","category":"GroupManagement","correlationId":"111a11a-111a-11a1-1111-111a1a2aa11a","result":"success","resultReason":"","activityDisplayName":"Add member to group","activityDateTime":"2019-09-03T20:01:53.7619661+00:00","loggedByService":"Core Directory","operationType":"Assign","initiatedBy":{"user":{"id":"111a11a-111a-11a1-1111-111a1a2aa11a","displayName":null,"userPrincipalName":"username","ipAddress":null}},"targetResources":[{"id":"111a11a-111a-11a1-1111-111a1a2aa11a","displayName":null,"type":"User","userPrincipalName":"username","modifiedProperties":[{"displayName":"Group.ObjectID","oldValue":null,"newValue":"\"111a11a-111a-11a1-1111-111a1a2aa11a\""},{"displayName":"Group.DisplayName","oldValue":null,"newValue":"\"AD_Roadmap\""},{"displayName":"Group.WellKnownObjectName","oldValue":null,"newValue":null}]},{"id":"111a11a-111a-11a1-1111-111a1a2aa11a","displayName":null,"type":"Group","groupType":"azureAD","modifiedProperties":[]}],"additionalDetails":[]}}

Table 756. Microsoft Entra ID sample event message supported by Microsoft Entra ID (continued)		
Event name	**Low level category**	**Sample log message**
Sign-in activity fail	User Login Failure	{"eventHubsAzureRecord": {"time":"2018-08-08T12:41:15.3163732Z","resourceId":"/tenants/g1111111-1aaa-11a1-1111-1111aa1a1111/providers/Microsoft.aadiam","operationName":"Sign-in activity","operationVersion":"1.0","category":"SignInLogs","tenantId":"h1111111-1aaa-11a1-1111-1111aa1a1111","resultType":"50074","resultSignature":"None","resultDescription":"User did not pass the MFA challenge.","durationMs":0,"callerIpAddress":"192.0.2.0","correlationId":"g1111111-1aaa-11a1-1111-1111aa1a1111","identity":"fname, lname","Level":4,"location":"NL","properties": {"id":"ia1111111-1aaa-11a1-1111-1111aa1a1111","createdDateTime":"2018-08-08T12:41:15.3163732+00:00","userDisplayName":"fname, lname","userPrincipalName":"user@example.com","userId":"j1111111-1aaa-11a1-1111-1111aa1a1111","appId":"k1111111-1aaa-11a1-1111-1111aa1a1111","appDisplayName":"Microsoft App Access Panel","ipAddress":"192.0.2.0","status": {"errorCode":50074,"failureReason":"User did not pass the MFA challenge.","additionalDetails":"MFA required in Azure AD"},"clientAppUsed":"Browser","deviceDetail":"...","location":"...","mfaDetail": {"authMethod":"Text message"},"correlationId":"l1111111-1aaa-11a1-1111-1111aa1a1111","conditionalAccessStatus":2,"conditionalAccessPolicies":"...","isRisky":false}}}

Microsoft Azure Platform

The IBM QRadar DSM for Microsoft Azure Platform parses events from the Microsoft Azure Activity log.

The Microsoft Azure Platform DSM collects events that occur at the platform level; such as resource creation, modification, or deletion. For a list of supported event types, see Microsoft Azure Platform DSM specifications.

To integrate Microsoft Azure Platform with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website. Download and install the most recent version of the following RPMs on your QRadar Console.
   - Protocol Common RPM
   - Protocol Event Hubs RPM
   - DSM Common RPM
   - Microsoft Azure Platform DSM RPM
2. Optional: Create a storage account. For more information, see Create a storage account.

   Important: You must have a storage account to connect to an event hub. For more information, see Microsoft Azure Event Hubs protocol FAQ.
3. Optional: Create an event hub. For more information, see Quickstart: Create an event hub using Azure portal.
4. Configure the Microsoft Azure Activity Logs to send events to a Microsoft Azure Event Hub. For more information see, Export Azure Activity log to storage or Azure Event Hubs.
5. Configure QRadar to collect events from Microsoft Azure Event Hubs by using the Microsoft Azure Event Hubs protocol. For more information about the protocol, see “Microsoft Azure log source parameters for Microsoft Azure Event Hubs” on page 1167.

Note: Microsoft Azure Log Integration service is no longer used to send events to QRadar. Microsoft Azure Log Integration service is deprecated and no longer supported by Microsoft.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Microsoft Azure Platform DSM specifications

When you configure the Microsoft Azure Platform DSM, understanding the specifications for the Microsoft Azure Platform DSM can help ensure a successful integration. For example, knowing what event format is supported before you begin can help reduce frustration during the configuration process.

Table 757. Microsoft Azure Platform DSM specifications

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft Azure Platform
RPM file name	`DSM-MicrosoftAzurePlatform-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Microsoft Azure Event Hubs
Event format	JSON
Recorded event types	Platform level activity logs For more information about Platform level activity logs, see Azure Resource Manager resource provider operations (https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations).
Automatically discovered?	Yes **Note:** This DSM automatically discovers only Activity Log Events that are forwarded directly from the Activity Log to the Event Hub.
Includes identity?	No
Includes custom properties?	No
More information	Microsoft Azure Information page (https://azure.microsoft.com/en-us/services/event-hubs) Microsoft Azure Portal (https://portal.azure.com)

Microsoft Azure log source parameters for Microsoft Azure Event Hubs

If QRadar does not automatically detect the log source, add a Microsoft Azure Event Hubs log source on the QRadar Console by using the Microsoft Azure protocol.

When using the Microsoft Azure protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Microsoft Azure events from Microsoft Azure Event Hubs:

Table 758. Microsoft Azure log source parameters for the Microsoft Azure Event Hubs DSM	
Parameter	**Description**
Log Source type	Microsoft Azure
Protocol Configuration	Microsoft Azure Event Hubs
Log Source Identifier	An identifiable name or IP address for the log source. When the **Use as Gateway Log Source** field is selected, the **Log Source Identifier** value is not used.

For a complete list of Microsoft Azure Event Hubs protocol parameters and their values, see "Microsoft Azure Event Hubs protocol configuration options" on page 159.

Related tasks

Adding a log source

Microsoft Azure Platform sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft Azure sample event messages when you use the Microsoft Azure Event Hubs protocol

Sample 1: The following sample event message shows a restart of a virtual machine.

```
LEEF:1.0|Microsoft|Azure Resource Manager|1.0|MICROSOFT.CLASSICCOMPUTE/VIRTUALMACHINES/RESTART/
ACTION|devTime=Jun 07 2016 17:04:26    devTimeFormat=MMM dd yyyy HH:mm:ss
cat=MICROSOFT.CLASSICCOMPUTE    src=10.0.0.2    usrName=name@example.com        sev=4
resource=testvm    resourceGroup=Test Resource Group    description=Restart a Virtual Machine
```

Table 759. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	The LEEF header Event ID field. For example, **MICROSOFT.CLASSICCOMPUTE/VIRTUALMACHINES/ RESTART/ ACTION**.
Event category	**cat**
Severity	**sev**
Source IP	**src**
Username	**usrName**
Device Time	**devTime**

Sample 2: The following sample event message shows the return of the access keys for the specified storage account.

```
{ "time": "2017-09-14T11:47:36.3237658Z", "resourceId": "/SUBSCRIPTIONS//RESOURCEGROUPS//
PROVIDERS/MICROSOFT.STORAGE/STORAGEACCOUNTS/", "operationName": "MICROSOFT.STORAGE/
STORAGEACCOUNTS/LISTKEYS/ACTION", "category": "Action", "resultType": "Success",
"resultSignature": "Succeeded.OK", "durationMs": 125, "callerIpAddress": "<IP_address>",
"correlationId": "", "identity": {"authorization":{"scope":"/subscriptions//resourceGroups//
providers/Microsoft.Storage/storageAccounts/","action":"Microsoft.Storage/storageAccounts/
listKeys/action","evidence":{"role":"Insights Management Service Role","roleAssignmentScope":"/
subscriptions/","roleAssignmentId":"","roleDefinitionId":"","principalId":"","principalType":"Se
```

```
rvicePrincipal"}},"claims":{"aud":"https://management.azure.com/","iss":"https://
sts.windows.net/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/","iat":"1505389356","nbf":"1505389356","exp":"1505393256","aio":"Y2VgYBBQEA5y0vTd4
PVnSpSp9qVwAA==","appid":"","appidacr":"2","e_exp":"262800","http://schemas.microso ft.com/
identity/claims/identityprovider":"https://sts.windows.net//","http://schemas.microsoft.com/
identity/claims/objectidentifier":"","http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
nameidentifier":"","http://schmas.microsoft.com/identity/claims/
tenantid":"","uti":"xxxxxx__xxxxxxxxxxxxxx","ver":"1.0"}}, "level": "Information", "location":
"global", "properties": {“statusCode":"OK","serviceRequestId":""}}
```


Table 760. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**operationName**
Event category	The **Event category** is located in the **resourceId** field after the **PROVIDERS** keyword. For example, **MICROSOFT.STORAGE**.
Source IP	**callerIpAddress**
Device Time	**time**

Sample 3: The following sample event message shows that a specified secret is retrieved from a given key vault.


```
{"eventHubsAzureRecord":{"time": "2016-03-02T 04:31:28.6127743Z","resourceId": "/
SUBSCRIPTIONS//RESOURCEGROUPS//PROVIDERS/MICROSOFT.KEYVAULT/VAULTS/AZLOGTEST","operationName":
"SecretGet","operationVersion": "2015-06-01","category": "AuditEvent","resultType":
"Success","resultSignature": "OK" ,"resultDescription": "","durationMs": "18
7","callerIpAddress": "","correlationId": "","identity": {"claim": {"http://schemas.
microsoft.com/identity/claims/objectidentifier": "","appid": "","http://schemas.xmlsoap.org/ws/
2005/05/identity/claims/upn": ""}},"properties": {"clientInfo": "","requestUri": "","id":
"https://.vault.azure.ne t/secrets/testsecret/","httpStatusCode": 200}}}
```


Table 761. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**operationName**
Event category	The **Event category** is located in the **resourceId** field after the **PROVIDERS** keyword. For example, **MICROSOFT.KEYVAULT**.
Device Time	**time**
Source IP	**callerIpAddress**

Sample 4: The following sample event message shows that a user successfully logged in to Microsoft SQL Server.


```
{"LogicalServerName":"servername","SubscriptionId":"42061870-6656-472f-9297-6a8f48a5e8b0","Resou
rceGroup":"RESOURCEGROUP","package":"SecAudit","event":"au-
dit_event_shoebox","sessionName":"audit_session_for_shoebox","originalEventTimestamp":"2020-07-1
9T05:26:01.5293718Z","time":"2020-07-19T05:26:01.5260341Z","resourceId":"/SUBSCRIPTIONS/ACCOUNT/
RESOURCEGROUPS/RESOURCEGROUP/PROVIDERS/MICROSOFT.SQL/MANAGEDINSTANCES/SERVER-
NAME","category":"SQLSecurityAuditEvents","operationName":"AuditEvent","properties":
{"audit_schema_version":1,"event_time":"2020-07-19T05:26:01.166Z","sequence_number":1,"action_id
":"LGIS","action_name":"LOGIN
SUCCEEDED","succeeded":"true","is_column_permission":"false","session_id":184,"server_principal_
id":286,"database_principal_id":0,"target_server_principal_id":0,"target_database_princi-
pal_id":0,"object_id":0,"user_defined_event_id":0,"transaction_id":0,"class_type":"LX","class_ty
pe_description":"LOGIN","securable_class_type":"LOGIN","duration_milliseconds":0,"response_rows"
:0,"affected_rows":0,"client_ip":"10.242.142.140","permission_bitmask":"0000000000000000000000000
00000000","sequence_group_id":"0AB33370-A776-485A-AD98-
FBB08D58A684","session_server_principal_name":"LoginName","server_principal_name":"LoginName","s
erver_principal_sid":"782fa7bb4f95374ba7fb6f346ccdafa6","database_principal_name":"","target_ser
ver_principal_name":"","target_server_principal_sid":"","target_database_principal_name":"","ser
ver_instance_name":"servername","database_name":"","schema_name":"","object_name":"","statement"
:"-- network protocol: TCP/IP\r\nset quoted_identifier on\r\nset arithabort off\r\nset
numeric_roundabort off\r\nset ansi_warnings on\r\nset ansi_padding on\r\nset ansi_nulls
on\r\nset con-cat_null_yields_null on\r\nset cursor_close_on_commit off\r\nset
```

```
implicit_transactions off\r\nset language us_english\r\nset dateformat mdy\r\nset datefirst
7\r\nset transac-tion isolation level read
committed\r\n","additional_information":"<action_info xmlns=\"http://schemas.microsoft.com/
sqlserver/2008/sqlaudit_data\"><pooled_connection>1</
pooled_connection><client_options>0x28000020</client_options><client_options1>0x0001f438</
client_options1><connect_options>0x00000001</connect_options><packet_data_size>8000</
packet_data_size><address>10.153.63.59</address><is_dac>0</is_dac></
action_info>","user_defined_information":"","application_name":".Net SqlClient Data
Provider","connection_id":"284D6271-94AD-4719-BA5A-
A2834CA24F82","data_sensitivity_information":"","host_name":"HOSNAME","session_context":"","is_s
erver_level_audit":"true","event_id":"F4FBD375-7F97-40F7-8C40-833D59CCC3D1"}}
```


Table 762. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	The **Event ID** is comprised from the **`category`** and **`action_name`** field values. For example, "**`category`**":"**`SQLSecurityAuditEvents`**" and "**`action_name`**":"**`LOGIN SUCCEEDED`**" results in an **Event ID** value of "`sqlsecurityauditevents_login succeeded`".
Event category	The **Event category** is located in the **`resourceId`** field after the **`PROVIDERS`** keyword. For example, **`MICROSOFT.SQL`**.
Device Time	**`time`**
Username	**`server_principal_name`**
Source IP	**`client_ip`**

Microsoft Defender for Cloud

The IBM QRadar DSM for Microsoft Defender for Cloud collects JSON events from a Microsoft Defender for Cloud. Events can be collected by using the Microsoft Graph Security API protocol and the Microsoft Azure Event Hubs protocol.

Important:

The Microsoft Azure Security Center DSM name is now the Microsoft Defender for Cloud DSM. The DSM RPM name remains as Microsoft Azure Security Center in QRadar.

To integrate Microsoft Defender for Cloud with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Microsoft Defender for Cloud DSM RPM
   - Microsoft Graph Security API Protocol DSM (If you want to add a log source by using the Microsoft Graph Security API protocol, download this RPM.)
   - Microsoft Azure Event Hubs Protocol RPM (If you want to add a log source by using the Microsoft Azure Event Hubs protocol, download this RPM.)
2. Optional: Configure Microsoft Defender for Cloud to send events to QRadar when you use Microsoft Graph Security API. For more information, see Export security alerts and recommendations https://docs.microsoft.com/en-us/azure/security-center/continuous-export).
3. Optional: Configure Microsoft Defender for Cloud to send events to QRadar when you use Microsoft Azure Event Hub. For more information, see Stream alerts to QRadar (https://learn.microsoft.com/en-us/azure/defender-for-cloud/export-to-siem#stream-alerts-to-qradar-and-splunk)
4. Add a Microsoft Defender for Cloud log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

“Adding a log source” on page 5

Microsoft Defender for Cloud DSM specifications

When you configure Microsoft Defender for Cloud, understanding the specifications for the Microsoft Defender for Cloud DSM can help ensure a successful integration. For example, knowing what event format is supported for Microsoft Defender for Cloud before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Microsoft Defender for Cloud DSM.

Table 763. Microsoft Defender for Cloud DSM specifications

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft Defender for Cloud
RPM file name	DSM-*MicrosoftAzureSecurityCenter-QRadar_version-build_number*.noarch.rpm
Protocol	Microsoft Graph Security API Microsoft Azure Event Hubs
Event format	JSON
Recorded event types	Security alert
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Security alerts - a reference guide (https://docs.microsoft.com/en-us/azure/security-center/alerts-reference)

Microsoft Graph Security API protocol log source parameters for Microsoft Defender for Cloud

Add a Microsoft Defender for Cloud log source on the QRadar Console by using the Microsoft Graph Security API protocol.

The following table describes the parameters that require specific values to collect Microsoft Graph Security API events from Microsoft Defender for Cloud:

Table 764. Microsoft Graph Security API log source parameters for the Microsoft Defender for Cloud DSM

Parameter	Value
Log Source type	Microsoft Defender for Cloud
Protocol Configuration	Microsoft Graph Security API

Table 764. Microsoft Graph Security API log source parameters for the Microsoft Defender for Cloud DSM (continued)	
Parameter	**Value**
Log Source Identifier	An identifiable name for the log source. The Log Source Identifier can be any valid value, including the same value as the Log Source Name parameter, and doesn't need to reference a specific server. If you configured multiple Microsoft Defender for Cloud log sources, you might want to identify the first log source as `MASC-1` the second log source as `MASC-2`, and the third log source as `MASC-3`.
Tenant ID	To find the **Tenant ID** parameter value, log in to Microsoft Defender for Cloud, and then select **Azure Active Directory** > **Overview** or select **Azure Active Directory** > **App registration** > **Microsoft Graph Security App** > **Overview**.
Client ID	To find the **Client ID** parameter value, log in to Microsoft Defender for Cloud, and then select **Azure Active Directory** > **App registration** > **Microsoft Graph Security App** > **Overview**.
Client Secret	To find the **Client Secret** parameter value, log in to Microsoft Defender for Cloud, and then select **Azure Active Directory** > **App registration** > **Microsoft Graph Security App** > **Certificates and secrets** > **Client secrets**. If no client secret exists, you can create one there.

For a complete list of Microsoft Graph Security API protocol parameters and their values, see Microsoft Graph Security API protocol configuration options.

Related tasks

Adding a log source

Microsoft Azure Event Hubs protocol log source parameters for Microsoft Defender for Cloud

Add a Microsoft Defender for Cloud log source on the QRadar Console by using the Microsoft Azure Event Hubs protocol.

The following table describes the parameters that require specific values to collect Microsoft Azure Event Hubs events from Microsoft Defender for Cloud:

Table 765. Microsoft Azure Event Hubs log source parameters for the Microsoft Defender for Cloud DSM	
Parameter	**Value**
Log Source type	Microsoft Defender for Cloud
Protocol Configuration	Microsoft Azure Event Hubs

Table 765. Microsoft Azure Event Hubs log source parameters for the Microsoft Defender for Cloud DSM (continued)	
Parameter	**Value**
Log Source Identifier	An identifiable name or IP address for the log source. When the **Use as Gateway Log Source** parameter is selected, the **Log Source Identifier** value is not used

For a complete list of Microsoft Azure Event Hubs protocol parameters and their values, see Microsoft Azure Event Hubs protocol configuration options Microsoft Azure Event Hubs protocol configuration options.

Related tasks

Adding a log source

Microsoft Defender for Cloud sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft Defender for Cloud sample message when you use the Microsoft Graph Security API protocol

The following sample shows that a user attempted to access resources by using a suspicious IP address.


```
{ "id": "1111d111-fa11-111a-11b1-c1e11c111a11", "azureTenantId":
"00000001-0001-0001-0001-000000000001", "azureSubscriptionId": "", "riskScore": null, "tags":
[], "activityGroupName": null, "assignedTo": "", "category": "Malicious_IP", "closedDateTime":
null, "comments": [], "confidence": 0, "createdDateTime": "2020-01-11T14:36:57.2738949Z",
"description": "Network traffic analysis indicates that your devices communicated with
what might be a Command and Control center for a malware of type Dridex. Dridex
is a banking trojan family that steals credentials of online banking websites. Dridex
is typically distributed via phishing emails with Microsoft Word and Excel document
attachments. These Office documents contain malicious macro code that downloads and installs
Dridex on the affected system.", "detectionIds": [], "eventDateTime": "2020-01-09T11:02:01Z",
"feedback": null, "lastModifiedDateTime": "2020-01-11T14:37:05.1157187Z", "recommendedActions":
[ "1. Escalate the alert to your security administrator.", "2. Add the source IP
address to your local FW block list for 24 hours. For more information, see
Plan virtual networks (https://sub.domain.test/en-us/documentation/articles/virtual-networks-
nsg/).", "3. Make sure your devices are completely updated and have updated antimalware
installed.", "4. Run a full anti-virus scan and verify that the threat was
removed.", "5. Install and run Microsoftâ€™s Malicious Software Removal Tool (https://
www.domain.test/en-us/security/pc-security/malware-removal.aspx).", "6. Run Microsoftâ€™s
Autoruns utility and try to identify unknown applications that are configured to
run when you sign in. For more information, see Autoruns for Windows (https://
technet.domain.test/en-us/sysinternals/bb963902.aspx).", "7. Run Process Explorer and try
to identify any unknown processes that are running. For more information, see Process
Explorer (https://technet.domain.test/en-us/sysinternals/bb896653.aspx)." ], "severity":
"high", "sourceMaterials": [], "status": "newAlert", "title": "Network communication with a
malicious IP", "vendorInformation": { "provider": "Azure Security Center", "providerVersion":
"3.0", "subProvider": null, "vendor": "Microsoft" }, "cloudAppStates": [], "fileStates":
[], "hostStates": [ { "fqdn": "abc-TestName.AAA111.ondomain.test", "isAzureAdJoined": null,
"isAzureAdRegistered": null, "isHybridAzureDomainJoined": false, "netBiosName": "abc-TestName",
"os": "", "privateIpAddress": null, "publicIpAddress": "172.16.37.125", "riskScore": "0" } ],
"historyStates": [], "malwareStates": [ { "category": "Trojan", "family": "Dridex", "name":
"", "severity": "", "wasRunning": true } ], "networkConnections": [], "processes": [],
"registryKeyStates": [], "triggers": [], "userStates": [ { "aadUserId": "", "accountName":
"TestName", "domainName": "AAA111.ondomain.test", "emailRole": "unknown", "isVpn": null,
"logonDateTime": null, "logonId": "0", "logonIp": null, "logonLocation": null, "logonType":
null, "onPremisesSecurityIdentifier": "", "riskScore": "0", "userAccountType": null,
"userPrincipalName": "TestName@AAA111.ondomain.test" } ], "vulnerabilityStates": []}
```

Table 766. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event Category	**category**
Log Source Time	**eventDateTime**
Username	**accountName**
Source IP	**publicIpAddress**

Microsoft Defender for Cloud sample message when you use the Microsoft Azure Event Hubs protocol

The following sample shows that a user attempted to manipulate WordPress theme by code injection.

```
{ "id": "/subscriptions/f57e6412-aaaa-1234-bbbb-11653c15d2b8/resourceGroups/Sample-RG/providers/
Microsoft.Security/locations/centralus/alerts/72cd4617-1234-1234-1234-ed28e3ed4124", "name":
"72cd4617-1234-1234-1234-ed28e3ed4124", "type": "Microsoft.Security/Locations/alerts",
"properties": { "status": "Active", "timeGeneratedUtc": "2022-12-13T09:39:40.4643132Z",
"processingEndTimeUtc": "2022-12-13T09:39:39.9451937Z", "version": "2022-01-01.0",
"vendorName": "Microsoft", "productName": "Microsoft Defender for Cloud",
"alertType": "SIMULATED_APPS_WpThemeInjection", "startTimeUtc": "2022-12-13T09:39:37.9451937Z",
"endTimeUtc": "2022-12-13T09:39:37.9451937Z", "severity": "High", "isIncident":
false, "systemtestId": "72cd4617-1234-1234-1234-ed28e3ed4124", "intent": "Unknown",
"resourceIdentifiers": [ { "$id": "centralus_1", "azureResourceId": "/SUBSCRIPTIONS/f57e6412-
aaaa-1234-bbbb-11653c15d2b8/RESOURCEGROUPS/Sample-RG/providers/Microsoft.Web/sites/Sample-App",
"type": "AzureResource", "azureResourceTenantId": "7106186f-1234-1234-1234-9d6431c4a909" } ],
"compromisedEntity": "Sample-App", "alertDisplayName": "[SAMPLE ALERT] Suspicious WordPress
theme invocation detected", "description": "THIS IS A SAMPLE ALERT: The Azure App
Service activity log indicates a possible code injection activity on your App Service
resource.\r\nThe suspicious activity detected resembles that of a manipulation of WordPress
theme to support server side execution of code, followed by a direct web request
to invoke the manipulated theme file.\r\nThis type of activity was seen in the
past as part of an attack campaign over WordPress.", "remediationSteps": [ "1. If
WordPress is installed, make sure that the application is up to date and automatic
updates are enabled.", "2. If only specific IP addresses should be allowed to
access the web app, set IP restrictions (https://example.com) for it." ], "entities":
[ { "$id": "centralus_2", "hostName": "Sample-App", "azureID": "/SUBSCRIPTIONS/f57e6412-
aaaa-1234-bbbb-11653c15d2b8/RESOURCEGROUPS/Sample-RG/providers/Microsoft.Web/sites/Sample-App",
"type": "host" } ], "alertUri": "https://example.com" } }
```

Table 767. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**alertType**
Log Source Time	**StartTimeUtc**

The following is a sample event when you use the Microsoft Azure Event Hubs protocol.

```
{
    "VendorName": "Microsoft",
    "AlertType": "SIMULATED_K8S_SensitiveMount",
    "ProductName": "Microsoft Defender for Cloud",
    "StartTimeUtc": "2023-07-20T11:53:23.7354152Z",
    "EndTimeUtc": "2023-07-20T11:53:23.7354152Z",
    "TimeGenerated": "2023-07-20T11:53:39.7354152Z",
    "ProcessingEndTime": "2023-07-20T11:53:39.7354152Z",
    "Severity": "Medium",
    "Status": "New",
    "ProviderAlertStatus": null,
    "ConfidenceLevel": null,
    "ConfidenceScore": null,
    "ConfidenceReasons": null,
    "IsIncident": false,
    "SystemAlertId": "1213123123123123_Test837912479-222222222",
    "CorrelationKey": null,
    "Intent": "PrivilegeEscalation",
    "AzureResourceId": "/subscriptions/aaaaaa-bbbb-4ccc-dddd-eeeeeee7/resourceGroups/
test/providers/Microsoft.Security/securityConnectors/gcp-connector/testdata/gcp-clusters-sample-
```

```
cluster-test-c",
    "WorkspaceId": null,
    "WorkspaceSubscriptionId": null,
    "WorkspaceResourceGroup": null,
    "AgentId": null,
    "CompromisedEntity": "Sample-Cluster",
    "AlertDisplayName": "[SAMPLE ALERT] Container with a sensitive volume mount detected
(Preview)",
    "Description": "THIS IS A SAMPLE ALERT: Kubernetes audit log analysis detected a new
container with a sensitive volume mount. The volume that was detected is a hostPath type
which mounts a sensitive file or folder from the node to the container. If the container gets
compromised, the attacker can use this mount for gaining access to the node.",
    "Entities": [
        {
            "$id": "4",
            "ImageId": "sample-image:v1",
            "Asset": false,
            "Type": "container-image"
        },
        {
            "$id": "5",
            "CloudResource": {
                "$id": "6",
                "ResourceId": "/subscriptions/950b61bf-99cc-49dc-aaea-2222222222222/
resourceGroups/Sample-RG/providers/Microsoft.Security/securityConnectors/gcp-connector/testdata/
gcp-clusters-sample-cluster-Test-c",
                "ResourceType": "Test1 Test Cluster",
                "Asset": false,
                "Type": "azure-resource"
            },
            "Asset": false,
            "Type": "K8s-cluster"
        },
        {
            "$ref": "6"
        },
        {
            "$id": "7",
            "Name": "Sample-namespace",
            "Cluster": {
                "$ref": "5"
            },
            "Asset": false,
            "Type": "K8s-namespace"
        },
        {
            "$id": "8",
            "Name": "sample-pod",
            "Namespace": {
                "$ref": "7"
            },
            "Asset": false,
            "Type": "K8s-pod"
        },
        {
            "$id": "9",
            "Name": "sample-container",
            "Image": {
                "$ref": "4"
            },
            "Pod": {
                "$ref": "8"
            },
            "Asset": false,
            "Type": "container"
        },
        {
            "$id": "10",
            "ProjectId": "012345678901",
            "ResourceType": "Test1 Test Cluster",
            "ResourceName": "Sample-Cluster",
            "Location": "Test-c",
            "LocationType": "Tester",
            "Metadata": {
                "IsGraphCenter": true
            },
            "Asset": true,
            "Type": "gcp-resource",
            "RelatedAzureResourceIds": {
                "MulticloudResourceMDCAzureId": "/subscriptions/aaaaa-bbbb-4ccc-
dddd-eeeeeee7/resourceGroups/test/providers/Microsoft.Security/securityConnectors/gcp-connector/
securityentitydata/gcp-clusters-sample-cluster-test-c",
```

```
                "MdcConnectorResourceAzureId": "/subscriptions/aaaaa-bbbb-4ccc-
dddd-eeeeeee7/resourceGroups/test/providers/Microsoft.Security/securityConnectors/gcp-connector/
securityentitydata/gcp-clusters-sample-cluster-test-c"
            }
        }
    ],
    "ExtendedLinks": null,
    "RemediationSteps": [
        "Review the container and the path in the alert details.",
        "If possible, consider mounting only specific folders or files that are necessary to
the container operation.",
        "If the container is not legitimate, escalate the alert to the information security
team."
    ],
    "ExtendedProperties": {
        "Namespace": "Sample-namespace",
        "Container image": "sample-image",
        "Container name": "sample-container",
        "Pod name": "sample-pod",
        "Sensitive mount name": "sample-mount",
        "Sensitive mount path": "/Sample",
        "resourceType": "Test1 Test Cluster"
    },
    "ResourceIdentifiers": [
        {
            "$id": "2",
            "AzureResourceId": "/subscriptions/aaaaaa-bbbb-4ccc-
dddd-eeeeeee7/resourceGroups/test/providers/Microsoft.Security/securityConnectors/gcp-connector/
testdata/gcp-clusters-sample-cluster-test-c",
            "Type": "AzureResource",
            "AzureResourceTenantId": "aaaaaaaa-bbbbbb-cccc-b857-eeeeeeee"
        },
        {
            "$id": "3",
            "AadTenantId": "abababab-ccdcdcdc-efefefef-12121212",
            "Type": "AAD"
        }
    ],
    "AlertUri":
"https://portal.Test.com/#blade/Microsoft_Azure_Security_AzureDefenderForData/Alerttest/alertId/
123123123123_sadasdasd-ffff-4213213-cccc-123123123123213/subscriptionId/12121212-asasa-accaac-
aaea-eeeeeeeeee/resourceGroup/Sample-Test/referencedFrom/alerttestLink/location/testlocation"
}
```


Table 768. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**`AlertType`**
Log Source Time	**`StartTimeUtc`**

Microsoft DHCP Server

The Microsoft DHCP Server DSM for IBM QRadar accepts DHCP events by using the Microsoft DHCP Server protocol or WinCollect.

About this task

Before you can integrate your Microsoft DHCP Server with QRadar, you must enable audit logging.

To configure the Microsoft DHCP Server:

Procedure

1. Log in to the DHCP Server Administration Tool.
2. From the DHCP Administration Tool, right-click on the DHCP server and select **Properties**.

   The **Properties** window is displayed.
3. Click the **General** tab.

   The **General** pane is displayed.

4. Click **Enable DHCP Audit Logging**.

   The audit log file is created at midnight and must contain a three-character day of the week abbreviation.

Table 769. Microsoft DHCP log file examples	
Log Type	**Example**
IPv4	`DhcpSrvLog-Mon.log`
IPv6	`DhcpV6SrvLog-Wed.log`

   By default Microsoft DHCP is configured to write audit logs to the `%WINDIR%\system32\dhcp\` directory.
5. Restart the DHCP service.
6. You can now configure the log source and protocol in QRadar.
   a) To configure QRadar to receive events from a Microsoft DHCP Server, you must select the Microsoft **DHCP Server** option from the **Log Source Type** list.
   b) To configure the protocol, you must select the Microsoft DHCP option from the Protocol Configuration list.

      Note: To integrate Microsoft DHCP Server versions 2000/2003 with QRadar by using WinCollect, see the *IBM QRadar WinCollect User Guide*.

Related concepts

"Microsoft DHCP protocol configuration options" on page 177

To receive events from Microsoft DHCP servers, configure a log source to use the Microsoft DHCP protocol.

Related tasks

"Adding a log source" on page 5

Microsoft DHCP Server sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft DHCP Server sample message when you use the Syslog protocol

The following sample event message shows that Microsoft DHCP requested a DNS update to the named DNS server.

```
SourceIp=10.168.41.1 AgentLogFile=DhcpSrvLog-Mar AgentProtocol=WindowsDHCP ID de s=30 ceso
Significado=04/23/19
```

Table 770. Highlighted values in the Microsoft DHCP Server sample event message	
QRadar field name	**Highlighted values in the event payload**
Event ID	30
Event Category	MicrosoftDHCP
Source IP	10.168.41.1

Microsoft DNS Debug

The IBM QRadar DSM for Microsoft DNS Debug collects events from a Microsoft Windows system.

Note:

The following table describes the specifications for the Microsoft DNS Debug DSM:

Table 771. Microsoft DNS Debug DSM specifications

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft DNS Debug
RPM file name	DSM-MicrosoftDNS-*QRadar_version-build_number*.noarch.rpm
Supported versions	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Protocol	WinCollect Microsoft DNS Debug
Event format	LEEF
Recorded event types	All operational and configuration network events.
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	http://www.microsoft.com

To integrate Microsoft DNS Debug with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following files from the IBM Support Website in the order that they are listed on your QRadar Console:
   - .sfs file for WinCollect
   - DSMCommon RPM
   - Microsoft DNS Debug RPM
2. Configure WinCollect to forward Microsoft DNS Debug events to QRadar. For more information, go to Log Sources for WinCollect agents in the *IBM QRadar WinCollect User Guide*. (https://www.ibm.com/docs/en/SS42VS_SHR/com.ibm.wincollect.doc/c_ug_wincollect_log_sources.html).
3. If QRadar does not automatically detect the log source, add a Microsoft DNS Debug log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Enabling DNS debugging on Windows Server

Enable DNS debugging on Windows Server to collect information that the DNS server sends and receives.

Before you begin

The DNS role must be installed on the Windows Server.

Important: DNS debug logging can affect system performance and disk space because it provides detailed data about information that the DNS server sends and receives. Enable DNS debug logging only when you require this information.

Procedure

1. Open the **DNS Manager** with the following command:

   ```
   dnsmgmt.msc
   ```

2. Right-click the DNS server and click **Properties**.
3. Click the **Debug Logging** tab.
4. Select **`Log packets for debugging`**.
5. Enter the **`File path and name`**, and **`Maximum size`**.

   Important: The **`File path and name`**, need to align with the **`Root Directory`** and **`File Pattern`** you provided when the Microsoft DNS debug log source was created in QRadar .
6. Click **Apply** and **OK**.

Microsoft DNS Debug sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft DNS Debug sample message when you use the Syslog protocol

The following sample event shows a DNS type A query.

```
<13>Aug 01 07:46:17 microsoft.dns.test AgentDevice=WindowsDNS    AgentLogFile=dns.log
PluginVersion=192.168.63.93    Date=1/08/2019    Time=7:46:13    Thread ID=a.m. 0E40
Context=PACKET    Message=    Internal packet identifier=000000A018724240    UDP/TCP
indicator=UDP    Send/Receive indicator=Snd    Remote IP=192.168.113.142    Xid
(hex)=0f5f    Query/Response=Q    Opcode=Q    Flags (hex)=0001    Flags (char codes)=D
ResponseCode=NOERROR    Question Type=A    Question Name=d3hb14vkzrxvla.cloudfront.net
```

Table 772. Highlighted values in the Microsoft DNS Debug sample event

QRadar field name	Highlighted values in the payload
Event ID	Type
Category	WindowsDNS
Destination Address	Remote IP
Log Source TIME	Aug 01 07:46:17

Microsoft Endpoint Protection

The Microsoft Endpoint Protection DSM for IBM QRadar collects malware detection events.

QRadar collects malware detection events by using the JDBC protocol. Adding malware detection events to QRadar gives the capability to monitor and detect malware infected computers in your deployment.

Malware detection events include the following event types:

- Site name and the source from which the malware was detected.
- Threat name, threat ID, and severity.
- User ID associated with the threat.
- Event type, time stamp, and the cleaning action that is taken on the malware.

Configuration overview

The Microsoft Endpoint Protection DSM uses JDBC to poll an SQL database for malware detection event data. This DSM does not automatically discover. To integrate Microsoft Endpoint Protection with QRadar, take the following steps:

1. If your database is not configured with Predefined Query, create an SQL database view for QRadar with the malware detection event data.
2. Configure a JDBC log source to poll for events from the Microsoft Endpoint Protection database. For information about configuring JDBC log source parameters for Microsoft Endpoint Protection, see "Microsoft Endpoint Protection JDBC log source parameters for predefined database queries" on page 1181.
3. Ensure that no firewall rules are blocking communication between QRadar and the database that is associated with Microsoft Endpoint Protection.

Creating a database view

Microsoft EndPoint Protection uses SQL Server Management Studio (SSMS) to manage the EndPoint Protection SQL databases.

Procedure

1. Log in to the system that hosts your Microsoft EndPoint Protection SQL database.
2. From the **Start** menu, select **Run**.
3. Type the following command:

   ```
   ssms
   ```
4. Click **OK**.
5. Log in to your Microsoft Endpoint Protection database.
6. From the **Object Explorer**, select **Databases.**
7. Select your database and click **Views**.
8. From the navigation menu, click **New Query**.
9. In the **Query** pane, type the following Transact-SQL statement to create the database view:

   ```
   create view dbo.MalwareView as select n.Type , n.RowID , n.Name ,
   n.Description , n.Timestamp , n.SchemaVersion , n.ObserverHost , n.ObserverUser ,
   n.ObserverProductName , n.ObserverProductversion , n.ObserverProtectionType ,
   n.ObserverProtectionVersion , n.ObserverProtectionSignatureVersion , n.ObserverDetection ,
   n.ObserverDetectionTime , n.ActorHost , n.ActorUser , n.ActorProcess ,
   n.ActorResource , n.ActionType , n.TargetHost , n.TargetUser , n.TargetProcess ,
   n.TargetResource , n.ClassificationID , n.ClassificationType , n.ClassificationSeverity ,
   n.ClassificationCategory , n.RemediationType , n.RemediationResult ,
   n.RemediationErrorCode , n.RemediationPendingAction , n.IsActiveMalware , i.IP_Addresses0
   as 'SrcAddress'
   ```

   ```
   from v_AM_NormalizedDetectionHistory n, System_IP_Address_ARR i, v_RA_System_ResourceNames
   s, Network_DATA d where n.ObserverHost = s.Resource_Names0 and s.ResourceID = d.MachineID
   and d.IPEnabled00 = 1 and d.MachineID = i.ItemKey and i.IP_Addresses0 like '%.%.%.%';
   ```
10. From the **Query** pane, right-click and select **Execute**.

    If the view is created, the following message is displayed in the results pane:

    ```
    Command(s) completed successfully.
    ```

What to do next

You are now ready to configure a log source in IBM QRadar.

Microsoft Endpoint Protection JDBC log source parameters for predefined database queries

Administrators who do not have permission to create a database view because of policy restrictions can collect Microsoft Endpoint Protection events with a JDBC log source that uses predefined queries.

Predefined queries are customized statements that can join data from separate tables when the database is polled by the JDBC protocol. To successfully poll for audit data from the Microsoft Endpoint Protection database, create a new user or provide the log source with existing user credentials. For more information about creating a user account, see the Microsoft website (https://www.microsoft.com).

Restriction: If you use network segregation to separate networks, using a predefined query might cause duplicate events. Use your own query.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Microsoft Endpoint Protection:

Table 773. Microsoft Endpoint Protection JDBC parameters

Parameter	Description
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source Type	**Microsoft Endpoint Protection**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	**MSDE**
Database Name	The name of the database to which you want to connect.
IP or Hostname	Type the IP address or host name of the Microsoft Endpoint Protection SQL Server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft Endpoint Protection database. The Microsoft Endpoint Protection database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a **Database Instance** when MSDE is used as the database type, you must leave the **Port** field blank in your configuration.

Table 773. Microsoft Endpoint Protection JDBC parameters (continued)	
Parameter	**Description**
Username	Type the user name the log source can use to access the Microsoft Endpoint Protection database.
Password	Type the password the log source can use to access the Microsoft Endpoint Protection database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password that is used to access the database. The confirmation password must be identical to the password entered in the **Password** field.
Authentication Domain	If you did not select **Use Microsoft JDBC**, **Authentication Domain** is displayed. If you select **MSDE** as the **Database Type** and the database is configured for Windows Authentication, you must populate the **Authentication Domain** field. Otherwise, leave this field blank.
Database Instance	If you have multiple SQL server instances on your database server, type the database instance. If you use a non-standard port in your database configuration, or block access to port 1434 for SQL database resolution, you must leave the **Database Instance** parameter blank in your configuration.
Predefined Query	From the list, select **Microsoft Endpoint Protection**.
Table Name	The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**.
Compare Field	A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created.
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this checkbox requires you to use an alternative method of querying that does not use pre-compiled statements.
Start Date and Time (Optional)	Type the start date and time for database polling. The **Start Date and Time** parameter must be formatted as yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.

Table 773. Microsoft Endpoint Protection JDBC parameters (continued)	
Parameter	**Description**
Polling Interval	Type the polling interval, which is the amount of time between queries to the view you created. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values that are entered without an H or M poll in seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 20,000.
Use Named Pipe Communication	If you did not select **Use Microsoft JDBC**, **Use Named Pipe Communication** is displayed. MSDE databases require the username and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.
Database Cluster Name	If you selected the **Use Named Pipe Communication**, the **Database Cluster Name** parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.
Use NTLMv2	If you did not select **Use Microsoft JDBC**, **Use NTLMv2** is displayed. Select the **Use NTLMv2** check box. This option forces MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.
Use Microsoft JDBC	If you want to use the Microsoft JDBC driver, you must enable **Use Microsoft JDBC**.
Use SSL	If your connection supports SSL communication, select **Use SSL**. This option requires extra configuration on your Endpoint Protection database and also requires administrators to configure certificates on both appliances.
Microsoft SQL Server Hostname	If you selected **Use Microsoft JDBC** and **Use SSL**, the **Microsoft SQL Server Hostname** parameter is displayed. You must type the hostname for the Microsoft SQL server.

For a complete list of JDBC protocol parameters and their values, see c_logsource_JDBCprotocol.dita.

Related information

“Adding a log source” on page 5

Microsoft Exchange Server

The IBM QRadar DSM for Microsoft Exchange Server collects Exchange events by polling for event log files.

The following table identifies the specifications for the Microsoft Exchange Server DSM:

Table 774. Microsoft Exchange Server

Specification	Value
Manufacturer	Microsoft
DSM name	Exchange Server
RPM file name	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
Supported versions	Microsoft Exchange 2003 Microsoft Exchange 2007 Microsoft Exchange 2010 Microsoft Exchange 2013 Microsoft Exchange 2016 Microsoft Exchange 2019
Protocol type	WinCollect for Microsoft Exchange 2003 Microsoft Exchange protocol for Microsoft Exchange 2007, 2010, 2013, 2016 and 2019.
QRadar recorded event types	Outlook Web Access events (OWA) Simple Mail Transfer Protocol events (SMTP) Message Tracking Protocol events (MSGTRK)
Automatically discovered?	No
Included identity?	No
More information	Microsoft website (http://www.microsoft.com)

To integrate Microsoft Exchange Server with QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the Microsoft Exchange Server DSM RPM from the IBM Support Website.
2. Configure your Microsoft Exchange Server DSM device to enable communication with QRadar.
3. Create an Microsoft Exchange Server DSM log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Microsoft Exchange Server to communicate with QRadar

Before you begin

Ensure that the firewalls that are located between the Exchange Server and the remote host allow traffic on the following ports:

- TCP port 135 for Microsoft Endpoint Mapper.
- UDP port 137 for NetBIOS name service.
- UDP port 138 for NetBIOS datagram service.
- TCP port 139 for NetBIOS session service.
- TCP port 445 for Microsoft Directory Services to transfer files across a Windows share.

Procedure

1. Configure OWA logs.
2. Configure SMTP logs.
3. Configure MSGTRK logs.

Configuring OWA logs on your Microsoft Exchange Server

To prepare your Microsoft Exchange Server to communicate with IBM QRadar, configure Outlook Web Access (OWA) event logs.

Procedure

1. Log into your Microsoft Internet Information System (IIS) Manager.
2. On the desktop, select **Start** > **Run**.
3. Type the following command:

   ```
   inetmgr
   ```
4. Click **OK**.
5. In the menu tree, expand **Local Computer**.
6. If you use IIS 6.0 Manager for Microsoft Server 2003, complete the following steps:
   a) Expand **Web Sites**.
   b) Right-click **Default Web Site** and select **Properties**.
   c) From the **Active Log Format** list, select **W3C**.
   d) Click **Properties**.
   e) Click the **Advanced** tab.
   f) From the list of properties, select the **Method (cs-method)** and **Protocol Version (cs-version)** check boxes
   g) Click **OK**.
7. If you use IIS 7.0 Manager for Microsoft Server 2008 R2, or IIS 8.5 for Microsoft Server 2012 R2, complete the following steps:
   a) Click **Logging**.
   b) From the **Format** list, select **W3C**.
   c) Click **Select Fields**.
   d) From the list of properties, select the **Method (cs-method)** and **Protocol Version (cs-version)** check boxes
   e) Click **OK**.

Enabling SMTP logs on your Microsoft Exchange Server 2003, 2007, and 2010

To prepare your Microsoft Exchange Server 2003, 2007 and 2010 to communicate with IBM QRadar, enable SMTP event logs.

Procedure

1. Start the Exchange Management Console.
2. To configure your *receive connector*, choose one of the following options:
   - For edge transport servers, select **Edge Transport** in the console tree and click the **Receive Connectors** tab.
   - For hub transport servers, select **Server Configuration** > **Hub Transport** in the console tree, select the server, and then click the **Receive Connectors** tab.
3. Select your receive connector and click **Properties**.
4. Click the **General** tab.
5. From the **Protocol logging level** list, select **Verbose**.
6. Click **Apply**.
7. Click **OK**.
8. To configure your *send connector*, choose one of the following options:
   - For edge transport servers, select **Edge Transport** in the console tree and click the **Send Connectors** tab.
   - For hub transport servers, select **Organization Configuration** > **Hub Transport** in the console tree, select your server, and then click the **Send Connectors** tab.
9. Select your send connector and click **Properties**.
10. Click the **General** tab.
11. From the **Protocol logging level** list, select **Verbose**.
12. Click **Apply**.
13. Click **OK**.

Enabling SMTP logs on your Microsoft Exchange Server 2013, and 2016

To prepare your Microsoft Exchange Server 2013 and 2016 to communicate with IBM QRadar, enable SMTP event logs.

Procedure

1. Start the Exchange Administration Center.
2. To configure your *receive connector*, select **Mail Flow** > **Receive Connectors**.
3. Select your receive connector and click **Edit**.
4. Click the **General** tab.
5. From the **Protocol logging level** list, select **Verbose**.
6. Click **Save**.
7. To configure your *send connector*, select **Mail Flow** > **Send Connectors**
8. Select your send connector and click **Edit**.
9. Click the **General** tab.
10. From the **Protocol logging level** list, select **Verbose**.
11. Click **Save**.

Configuring MSGTRK logs for Microsoft Exchange 2003, 2007, and 2010

Message Tracking logs created by the Microsoft Exchange Server detail the message activity that takes place on your Microsoft Exchange Server, including the message path information.

About this task

MSGTRK logs are enabled by default on Microsoft Exchange 2007 or Exchange 2010 installations. The following configuration steps are optional.

To enable MSGTRK event logs:

Procedure

1. Start the Exchange Management Console.
2. Configure your receive connector based on the server type:
   - For edge transport servers - In the **console tree**, select **Edge Transport** and click **Properties**.
   - For hub transport servers - In the console tree, select **Server Configuration** > **Hub Transport**, and then select the server and click **Properties**.
3. Click the **Log Settings** tab.
4. Select the **Enable message tracking** check box.
5. Click **Apply**.
6. Click **OK**.

   MSGTRK events are now enabled on your Exchange Server.

Configuring MSGTRK logs for Exchange 2013 and 2016

Message Tracking logs created by the Microsoft Exchange Server detail the message activity that takes place on your Exchange Server, including the message path information.

Procedure

1. Start the Exchange Administration Center.
2. Click **Servers** > **Servers**.
3. Select the mailbox server that you want to configure, and then click **Edit**.
4. Click **Transport Logs**.
5. In the **Message tracking log** section, configure the following parameters:

Parameter	Description
Enable message tracking log	Enable or disable message tracking on the server.
Message tracking log path	The value that you specify must be on the local Exchange server. If the folder does not exist, it is created when you click **Save**.

6. Click **Save**.

Microsoft Exchange Server log source parameters for Microsoft Exchange

If QRadar does not automatically detect the log source, add a Microsoft Exchange log source on the QRadar Console by using the Microsoft Exchange Server protocol.

When using the Microsoft Exchange Server protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Microsoft Exchange Server events from Microsoft Exchange:

Table 775. Microsoft Exchange Server log source parameters for the Microsoft Exchange DSM	
Parameter	**Value**
Log Source type	Microsoft Exchange Server
Protocol Configuration	Microsoft Exchange
Log Source Identifier	The IP address or host name to identify the Windows Exchange event source in the QRadar user interface.
SMTP Log Folder Path	The directory path to access the SMTP log files. Use one of the following directory paths: • For Microsoft Exchange 2003, use `c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/ .` • For Microsoft Exchange 2007, use `c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/ProtocolLog/.` • For Microsoft Exchange 2010, use `c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/ProtocolLog/.` • For Microsoft Exchange 2013, use `c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/.` • For Microsoft Exchange 2016, use `c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/ProtocolLog/.`
OWA Log Folder Path	The directory path to access the OWA log files. Use one of the following directory paths: • For Microsoft Exchange 2003, use `c$/WINDOWS/system32/LogFiles/W3SVC1/ .` • For Microsoft Exchange 2007, use `c$/WINDOWS/system32/LogFiles/W3SVC1/ .` • For Microsoft Exchange 2010, use `c$/inetpub/logs/LogFiles/W3SVC1/.` • For Microsoft Exchange 2013, use `c$/inetpub/logs/LogFiles/W3SVC1/.` • For Microsoft Exchange 2016, use `c$/inetpub/logs/LogFiles/W3SVC1/.` • For Microsoft Exchange 2019, use `c$/inetpub/logs/LogFiles/W3SVC1/.`

Table 775. Microsoft Exchange Server log source parameters for the Microsoft Exchange DSM (continued)	
Parameter	**Value**
MSGTRK Log Folder Path	The directory path to access message tracking log files. Message tracking is only available on Microsoft Exchange 2007 servers assigned the Hub Transport, Mailbox, or Edge Transport server role. Use one of the following directory paths: • For Microsoft Exchange 2007, use `c$/Program Files/Microsoft/Exchange Server/TransportRoles/Logs/MessageTracking/`. • For Microsoft Exchange 2010, use `c$/Program Files/Microsoft/Exchange Server/V14/TransportRoles/Logs/MessageTracking/`. • For Microsoft Exchange 2013, use `c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/MessageTracking/`. • For Microsoft Exchange 2016, use `c$/Program Files/Microsoft/Exchange Server/V15/TransportRoles/Logs/MessageTracking/`.

For a complete list of Microsoft Exchange Server protocol parameters and their values, see "Microsoft Exchange protocol configuration options" on page 179.

Related tasks

Adding a log source

Microsoft Exchange Server sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Microsoft Exchange Server sample message when you use the Microsoft Exchange protocol

The following sample shows a send external event.

```
SourceIp=10.91.5.110 AgentDevice=WindowsExchange AgentLogFile=MSGTRK2018112722-1.LOG
AgentLogFormat=MSGTRK date-time=2018-11-27T22:40:02.966Z client-ip
=10.4.11.100 client-hostname=testHostName server-ip=192.168.25.195 server-hostname
=qradar.example.test source-context=;250 2.0.0 OK b139-v6si456977itb.104 -
gsmtp;ClientSubmitTime:
connector-id=Outbound Mail source=SMTP event-id=SENDEXTERNAL internal-message-
id=64441689310559 message-id=<admin4@qradar.domain.test> network-message-
id=0fd591fe-1cc4-47f0-0bbc
-08d654b944f3 recipient-address=admin3@qradar.domain.test recipient-status=250 2.1.5 OK b139-
v6si45
6977itb.104 - gsmtp total-bytes=7249 recipient-count=1 related-recipient-address= reference=
messag
e-subject=Receipt sender-address=admin1@qradar.domain.test return-path=admin2@
qradar.domain.test message-info=2018-11-27T22:40:02.194Z;SRV=testHostName.BLAH.BLAH.BLAH:TOTAL-FE=
0.006|SMR=0.004(SMRPI=0.002(SMRPI-FrontendProxyAgent=0.002))|SMS=0.001;SRV=testHostName.BLAH.BLAH.
BLAH:TOTAL-HUB=0.765|SMR=0.103(SMRDE=0.001|SMRC=0.101(SMRCL=0.101))|CAT=0.030(CATOS=0.005(CATSM=0.
005(CATSM-Unified Group Post Sent Item Routing Agent=0.004))|CATRESL=0.002|CATORES=0.020(CATRS=0.
020(CATRS-Transport Rule Agent=0.001(X-ETREX=0.001)|CATRS-Index Routing Agent=0.017)))|QDE=0.120|
SMSC=0.127(X-SMSDR=0.120)|SMS=0.382 directionality=Originating tenant-id= original-client-ip= ori
ginal-server-ip= custom-data=S:E2ELatency=0.771;S:ExternalSendLatency=0.141;S:ToEntity=Internet;S
:FromEntity=Internet;S:MsgRecipCount=1;S:IncludeInSla=True;S:Microsoft.Exchange.Transport.MailRec
ipient.RequiredTlsAuthLevel=Opportunistic;S:Microsoft.Exchange.Transport.MailRecipient.EffectiveT
lsAuthLevel=EncryptionOnly;S:IsSmtpResponseFromExternalServer=True;S:DeliveryPriority=Normal;S:Or
```

```
iginalFromAddress=admin1@qradar.domain.test;S:AccountForest=BLAH.BLAH.BLAH transport-traffic-type
=Email log-id=755ab09c-9c04-44aa-8b07-08d654b94568 schema-version=15.01.1261.039
```

```
SourceIp=10.91.5.110 AgentDevice=WindowsExchange AgentLogFile=MSGTRK2018112722-1.LOG
AgentLogFormat=MSGTRK date-time=2018-11-27T22:40:02.966Z client-ip=10.4.11.100 client-
hostname=testHostName server-ip=192.168.25.195 server-hostname=qradar.example.test source-
context=;250 2.0.0 OK b139-v6si456977itb.104 - gsmtp;ClientSubmitTime: connector-id=Outbound
Mail source=SMTP event-id=SENDEXTERNAL internal-message-id=64441689310559 message-
id=<admin4@qradar.domain.test> network-message-id=0fd591fe-1cc4-47f0-0bbc-08d654b944f3
recipient-address=admin3@qradar.domain.test recipient-status=250 2.1.5 OK b139-
v6si456977itb.104 - gsmtp total-bytes=7249 recipient-count=1 related-recipient-address=
reference= message-subject=Receipt sender-address=admin1@qradar.domain.test return-
path=admin2@qradar.domain.test message-
info=2018-11-27T22:40:02.194Z;SRV=testHostName.BLAH.BLAH.BLAH:TOTAL-FE=0.006|
SMR=0.004(SMRPI=0.002(SMRPI-FrontendProxyAgent=0.002))|
SMS=0.001;SRV=testHostName.BLAH.BLAH.BLAH:TOTAL-HUB=0.765|SMR=0.103(SMRDE=0.001|
SMRC=0.101(SMRCL=0.101))|CAT=0.030(CATOS=0.005(CATSM=0.005(CATSM-Unified Group Post Sent Item
Routing Agent=0.004))|CATRESL=0.002|CATORES=0.020(CATRS=0020(CATRS-Transport Rule Agent=0.001(X-
ETREX=0.001)|CATRS-Index Routing Agent=0.017)))|QDE=0.120|SMSC=0.127(X-SMSDR=0.120)|SMS=0.382
directionality=Originating tenant-id= original-client-ip= original-server-ip= custom-
data=S:E2ELatency=0.771;S:ExternalSendLatency=0.141;S:ToEntity=Internet;S:FromEntity=Internet;S:
MsgRecipCount=1;S:IncludeInSla=True;S:Microsoft.Exchange.Transport.MailRecipient.RequiredTlsAuth
Level=Opportunistic;S:Microsoft.Exchange.Transport.MailRecipient.EffectiveTlsAuthLevel=Encryptio
nOnly;S:IsSmtpResponseFromExternalServer=True;S:DeliveryPriority=Normal;S:OriginalFromAddress=ad
min1@qradar.domain.test;S:AccountForest=BLAH.BLAH.BLAH transport-traffic-type=Email log-
id=755ab09c-9c04-44aa-8b07-08d654b94568 schema-version=15.01.1261.039
```

Table 776. Highlighted fields

QRadar field name	Highlighted payload field name
Event ID	**AgentLogFormat** + **event-id**
Username	**sender-address**
Source IP	**client-ip**
Destination IP	**server-ip**

Microsoft Hyper-V

The IBM QRadar Microsoft Hyper-V DSM collects events from Microsoft Hyper-V servers.

The following table describes the specifications for the Microsoft Hyper-V Server DSM:

Table 777. Microsoft Hyper-V DSM specifications

Specification	Value
Manufacturer	Microsoft
DSM	Microsoft Hyper-V
RPM file name	DSM-MicrosoftHyperV-*QRadar_version-build_number*.rpm

Table 777. Microsoft Hyper-V DSM specifications (continued)	
Specification	**Value**
Supported versions	Windows Server 2016 Windows Server 2012 (most recent) Windows Server 2012 Core Windows Server 2008 (most recent) Windows Server 2008 Core Windows 10 (most recent) Windows 8 (most recent) Windows 7 (most recent) Windows Vista (most recent)
Protocol	WinCollect
QRadar recorded events	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	http://technet.microsoft.com/en-us/windowsserver/dd448604.aspx

Microsoft Hyper-V DSM integration process

You can integrate Microsoft Hyper-V DSM with IBM QRadar by using WinCollect.

Use the following procedures:

1. Download and install the DSM-MicrosoftHyperV RPM and the WinCollect RPM from the IBM support website (http://www.ibm.com/support).
2. Install a WinCollect agent on the Hyper-V system or on another system that has a route to the Hyper-V system. You can also use an existing WinCollect agent. For more information about WinCollect, see the WinCollect documentation (https://www.ibm.com/docs/en/qsip/7.5?topic=configuring-wincollect-7) .
3. If automatic updates are not enabled, download and install the DSM RPM for Microsoft Hyper-V on your QRadar Console. RPMs need to be installed only one time.
4. For each Microsoft Hyper-V server that you want to integrate, add a log source on the QRadar Console.

Related tasks

Adding a log source

WinCollect log source parameters for Microsoft Hyper-V

If QRadar does not automatically detect the log source, add a Microsoft Hyper-V log source on the QRadar Console by using the WinCollect protocol.

When using the WinCollect protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect WinCollect events from Microsoft Hyper-V:

Table 778. WinCollect log source parameters for the Microsoft Hyper-V DSM	
Parameter	**Value**
Log Source type	Microsoft Hyper-V
Protocol Configuration	WinCollect
Application or Service Log Type	Microsoft Hyper-V
WinCollect Agent	Select the WinCollect agent that accesses the Microsoft Hyper-V server.

For a complete list of WinCollect protocol parameters and their values, see the *WinCollect User Guide*.

Related tasks

Adding a log source

Microsoft IAS Server

The Microsoft IAS Server DSM for IBM QRadar accepts RADIUS events by using syslog.

About this task

You can integrate Internet Authentication Service (IAS) or Network Policy Server (NPS®) logs with QRadar by using WinCollect. For more information, see the *IBM QRadar WinCollect User Guide*.

You can now configure the log source in QRadar.

To configure QRadar to receive events from a Microsoft Windows IAS Server.

Procedure

From the **Log Source Type** list, select the Microsoft **IAS Server** option.

For more information about your server, see your vendor documentation.

Related tasks

"Adding a log source" on page 5

Microsoft IIS Server

The Microsoft Internet Information Services (IIS) Server DSM for IBM QRadar accepts FTP, HTTP, NNTP, and SMTP events using syslog.

You can integrate a Microsoft IIS Server with QRadar by using one of the following methods:

- Configure QRadar to connect to your Microsoft IIS Server by using the IIS Protocol which collects HTTP events from Microsoft IIS servers. For more information, see "Configuring Microsoft IIS by using the IIS Protocol" on page 1193.
- Configure WinCollect to forward IIS events to QRadar. For more information, go to Log Sources for WinCollect agents in the *IBM QRadar WinCollect User Guide* (https://www.ibm.com/docs/en/SS42VS_SHR/com.ibm.wincollect.doc/c_ug_wincollect_log_sources.html).

Table 779. Supported log types for Microsoft IIS 6.0 - IIS 10.0	
Method of Import	**Supported Log Type**
IIS Protocol	HTTP
WinCollect	SMTP, NNTP, FTP, HTTP

Configuring Microsoft IIS by using the IIS Protocol

You can configure Microsoft IIS Protocol to communicate with QRadar by using the IIS Protocol.

Before you begin

Before you configure IBM QRadar with the Microsoft IIS protocol, you must configure your Microsoft IIS Server to generate the correct log format.

About this task

The Microsoft IIS Protocol supports only the W3C Extended log file format.

Procedure

1. Log in to your Microsoft Information Services (IIS) Manager.
2. Expand **IIS Manager** > **Local Computer** > **Sites**.
3. Select **Web Site**.
4. Double-click the **Logging** icon.
5. Select **W3C** as the log file format from the **Log File** window.
6. Click **Select Fields**.
7. From the list of properties, select check boxes for the following W3C properties:

Table 780. Required Properties for IIS event logs

IIS 6.0 Required Properties	IIS 7.0/7.5 Required Properties	IIS 8.0/8.5 Required Properties	IIS 10 Required Properties
Date (date)	Date (date)	Date (date)	Date (date)
Time (time)	Time (time)	Time (time)	Time (time)
Client IP Address (c-ip)	Client IP Address (c-ip)	Client IP Address (c-ip)	Client IP Address (c-ip)
User Name (cs-username)	User Name (cs-username)	User Name (cs-username)	User Name (cs-username)
Server IP Address (s-ip)	Server IP Address (s-ip)	Server IP Address (s-ip)	Server IP Address (s-ip)
Server Port (s-port)	Server Port (s-port)	Server Port (s-port)	Server Port (s-port)
Method (cs-method)	Method (cs-method)	Method (cs-method)	Method (cs-method)
URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)	URI Stem (cs-uri-stem)
URI Query (cs-uri-query)	URI Query (cs-uri-query)	URI Query (cs-uri-query)	URI Query (cs-uri-query)
Protocol Status (sc-status)	Protocol Status (sc-status)	Protocol Status (sc-status)	Protocol Status (sc-status)
Protocol Version (cs-version)	User Agent (cs(User-Agent))	User Agent (cs(User-Agent))	User Agent (cs(User-Agent))
User Agent (cs(User-Agent))			

8. Click **OK**, and then click **Apply**.

What to do next

You are now ready to configure the log source in QRadar.

Microsoft IIS log source parameters for Microsoft IIS Server

If QRadar does not automatically detect the log source, add a Microsoft IIS Server log source on the QRadar Console by using the Microsoft IIS protocol.

When using the Microsoft IIS protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Microsoft IIS events from a Microsoft IIS Server:

Table 781. Microsoft IIS log source parameters for the Microsoft IIS Server DSM

Parameter	Value
Log Source type	Microsoft IIS Server
Protocol Configuration	Microsoft IIS
Log Source Identifier	Type the IP address or host name for the log source.
File Pattern	Type the regular expression (regex) that is needed to filter the file names. All matching files are included in the processing. The default is `(?:u_)?ex.*\.(?:log|LOG)` For example, to list all files that start with the word log, followed by one or more digits and ending with `tar.gz`, use the following entry: `log[0-9]+\.tar\.gz`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

For a complete list of Microsoft IIS protocol parameters and their values, see "Microsoft IIS protocol configuration options" on page 187.

Related tasks

Adding a log source

Syslog log source parameters for Microsoft IIS Server

If QRadar does not automatically detect the log source, add a Microsoft IIS Server log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Microsoft IIS Server:

Table 782. Syslog log source parameters for the Microsoft IIS Server DSM

Parameter	Value
Log Source type	Microsoft IIS Server
Protocol Configuration	Syslog

Table 782. Syslog log source parameters for the Microsoft IIS Server DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source.

Related tasks

Adding a log source

Microsoft IIS Server sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft IIS Server sample message when you use the Microsoft IIS protocol

The following sample event message shows that an HTTP 500 internal server error occurred.

```
SourceIp=10.232.192.155    AgentDevice=MSIIS    AgentLogFile=u_extend1220_x.log
AgentLogFormat=W3C    date=2018-06-19    time=06:27:41    s-sitename=W3SVC2    s-
computername=TESTTESTTEST012    s-ip=10.232.192.155    cs-method=GET    cs-uri-stem=/login.asp
cs-uri-query=-    s-port=444    cs-username=-    c-ip=10.142.129.147    cs-version=HTTP/1.0
cs(User-Agent)=-    cs(Cookie)==    cs(Referer)=-    cs-host=    sc-status=500    sc-
substatus=0    sc-win32-status=0    sc-bytes=3733    cs-bytes=90    time-taken=171    X-Forwarded-
For=-
```

```
SourceIp=10.232.192.155    AgentDevice=MSIIS    AgentLogFile=u_extend1220_x.log
AgentLogFormat=W3C    date=2018-06-19    time=06:27:41    s-sitename=W3SVC2    s-
computername=TESTTESTTEST012    s-ip=10.232.192.155    cs-method=GET    cs-uri-stem=/
login.asp    cs-uri-query=-    s-port=444    cs-username=-    c-ip=10.142.129.147    cs-
version=HTTP/1.0    cs(User-Agent)=-    cs(Cookie)==    cs(Referer)=-    cs-host=    sc-
status=500    sc-substatus=0    sc-win32-status=0    sc-bytes=3733    cs-bytes=90    time-
taken=171    X-Forwarded-For=-
```

Table 783. QRadar field names and highlighted values in the event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	**500**
Source IP	**10.142.129.147**
Destination IP	**10.232.192.155**
Destination Port	**444**

Microsoft IIS Server sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows a configuration error.

```
<13>Apr 17 08:55:56 microsoft.iis.test AgentDevice=WindowsLog    AgentLogFile=Microsoft-
IIS-Configuration/Administrative    PluginVersion=7.2.9.105    Source=Microsoft-Windows-IIS-
Configuration    Computer=microsoft.iis.test    OriginatingComputer=10.18.224.7    User=user
Domain=domain    EventID=12    EventIDCode=12    EventType=2    EventCategory=0
RecordNumber=380    TimeGenerated=1587124522    TimeWritten=1587124522    Level=Warning
Keywords=0x8000000000000000    Task=None    Opcode=Info    Message=Unable to find schema for
config section 'system.serviceModel/client'. This section will be ignored.
```

```
<13>Apr 17 08:55:56 microsoft.iis.test AgentDevice=WindowsLog    AgentLogFile=Microsoft-
IIS-Configuration/Administrative    PluginVersion=7.2.9.105    Source=Microsoft-Windows-IIS-
Configuration    Computer=microsoft.iis.test    OriginatingComputer=10.18.224.7    User=user
Domain=domain    EventID=12    EventIDCode=12    EventType=2    EventCategory=0
RecordNumber=380    TimeGenerated=1587124522    TimeWritten=1587124522    Level=Warning
Keywords=0x8000000000000000    Task=None    Opcode=Info    Message=Unable to find schema for
config section 'system.serviceModel/client'. This section will be ignored.
```

Table 784. QRadar field names and highlighted values in the event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	**12**
Username	**user**
Source IP	**10.18.224.7**
Device Time	**Apr 17 08:55:56** is extracted from **Date** and **Time** fields in QRadar.

Sample 2: The following sample event message shows that an HTTP 401 access denied error occurred.

```
<13>Oct 02 09:54:19 microsoft.iis.test IISWebLog    0    2020-10-02 14:53:31 10.0.10.51 CCM_POST /
ccm_system_windowsauth/request - 80 - 10.0.0.23 ccmhttp - 401 2 5 1509 1
```

```
<13>Oct 02 09:54:19 microsoft.iis.test IISWebLog    0    2020-10-02 14:53:31 10.0.10.51
CCM_POST /ccm_system_windowsauth/request - 80 - 10.0.0.23 ccmhttp - 401 2 5 1509 1
```

Table 785. QRadar field names and highlighted values in the event payload	
QRadar field name	**Highlighted values in the event payload**
Event ID	**401**
Source IP	**10.0.0.23**
Destination IP	**10.0.10.51**
Destination Port	**80**
Device Time	**Oct 02 09:54:19** is extracted from the **Date** and **Time** fields in QRadar.

Microsoft ISA

The Microsoft Internet and Acceleration (ISA) DSM for IBM QRadar accepts events by using syslog.

You can integrate Microsoft ISA Server with QRadar by using WinCollect. For more information, see the *IBM QRadar WinCollect User Guide*.

Note: The Microsoft ISA DSM also supports events from Microsoft Threat Management Gateway by using WinCollect.

Microsoft Office 365

The IBM QRadar DSM for Microsoft Office 365 collects events from Microsoft Office 365 online services.

Important: The Service Communications API endpoint is no longer available for use because it was deprecated by Microsoft. For more information, see APAR IJ37562 (https://www.ibm.com/support/pages/apar/IJ37562).

The following table describes the specifications for the Microsoft Office 365 DSM:

Table 786. Microsoft Office 365 DSM specifications	
Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft Office 365
RPM file name	DSM-MicrosoftOffice365-*QRadar_version-build_number*.noarch.rpm

Table 786. Microsoft Office 365 DSM specifications (continued)	
Specification	**Value**
Supported versions	N/A
Protocol	Office 365 REST API
Event format	JSON
Recorded event types	Exchange Audit, SharePoint Audit, Azure Active Directory Audit
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Microsoft website (https://www.microsoft.com)

To integrate Microsoft Office 365 with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - Office 365 REST API Protocol RPM
   - Microsoft Office 365 DSM RPM
2. Configure a Microsoft Office 365 account in the Microsoft Azure portal.
3. Add a Microsoft Office 365 log source on the QRadar Console. For more information about adding a log source, see the "Adding a log source" on page 5 topic. The following table describes the log source parameters that require specific values for Microsoft Office 365 event collection:

Table 787. Microsoft Office 365 log source parameters	
Parameter	**Value**
Log Source type	Microsoft Office 365
Protocol Configuration	Office 365 REST API
Log Source Identifier	A unique identifier for the log source. The **Log Source Identifier** can be any valid value and does not need to reference a specific server. The **Log Source Identifier** can be the same value as the **Log Source Name**. If you configured multiple Microsoft Office 365 log sources, you might want to identify the first log source as MSOffice365-1, the second log source as MSOffice365-2, and the third log source as MSOffice365-3.
Client ID	In your application configuration of Azure Active Directory, this parameter is under **Client ID**.
Client Secret	In your application configuration of Azure Active Directory, this parameter is under **Value**.
Tenant ID	Used for Azure AD authentication.

Table 787. Microsoft Office 365 log source parameters (continued)	
Parameter	**Value**
Event Filter	The type of audit events to retrieve from Microsoft Office. • Azure Active Directory • Exchange • SharePoint • General • DLP
Use Proxy	For QRadar to access the Office 365 Management APIs, all traffic for the log source travels through configured proxies. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, keep the **Proxy Username** and **Proxy Password** fields empty.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.
Show Advanced Options	Show optional advanced options for event collection. The **Advanced Options** values are in effect whether they are shown or not.
Management Activity API URL	Specify the Office 365 Management Activity API URL. Default is https://manage.office.com.
Azure AD Sign-in URL	Specify the Azure AD sign-in URL. Default is https://login.microsoftonline.com.

4. Test the connectivity to the Office365 log source. Follow the instructions in "Testing log sources" on page 12.

Related tasks

"Configuring a Microsoft Office 365 account in Microsoft Azure Active Directory" on page 1199
Before you can add a log source in QRadar, you must run the Azure Active Directory PowerShell cmdlet and then configure Azure Active Directory for Microsoft Office 365.

"Adding a DSM" on page 4
"Adding a log source" on page 5

Related information

Office 365 REST API protocol configuration options

Configuring a Microsoft Office 365 account in Microsoft Azure Active Directory

Before you can add a log source in QRadar, you must run the Azure Active Directory PowerShell cmdlet and then configure Azure Active Directory for Microsoft Office 365.

Procedure

1. Run the Azure Active Directory PowerShell cmdlet. For more information, see How to install and configure Azure PowerShell (https://azure.microsoft.com/en-us/documentation/articles/powershell-install-configure/).
2. Identify the **Tenant ID** of the tenant that is subscribed to Microsoft Office 365 by typing the following commands:

   ```
   import-module MSOnline

   $userCredential = Get-Credential

   Connect-MsolService -Credential $userCredential

   Get-MsolAccountSku | % {$_.AccountObjectID}
   ```

   Use the **Tenant ID** value for the **Tenant ID** value when you configure a log source in QRadar.
3. To use Azure Active Directory to register an application, log in to the Azure Management Portal (https://portal.azure.com) with the credentials of the tenant that is subscribed to Microsoft Office 365.
   a. From the navigation menu, select **Azure Active Directory**.
   b. From the **Overview** pane, select **App registrations**, and then click **New registration**.
   c. In the **Supported account types** section, select the type of account to use the application or to access the API.
   d. In the **Redirect URI (optional)** section, select **Web**, and type `http://localhost` in the **Web** field.
   e. Click **Register**, and then copy and store the **Application (client) ID** value. Use this value for the **Client ID** value when you configure a log source in QRadar.
4. Generate a client secret for the application.
   a. From the **Manage** pane, select **Certificates & secrets** > **New client secret**.
   b. Select an expiry period, and then click **Add**.
   c. Copy and store your client secret key value because it can't be retrieved later. Use this value for the **Client Secret** value when you configure a log source in QRadar.
5. Specify the permissions that the Microsoft Azure application must use to access Microsoft Office 365 Management APIs.
   a. From the **Manage** pane, select **API permissions**.
   b. Click **Add a permission** > from the API list, choose **Office 365 Management APIs** > **Delegated permissions**, and then select the following options:

   Table 788. Delegated permissions

Permission	Values
Activity Feed	ActivityFeed.Read ActivityFeed.ReadDlp
ServiceHealth	ServiceHealth.Read

   c. Click **Application permissions**, and then select the following options:

Table 789. Application permissions	
Permission	**Values**
Activity Feed	ActivityFeed.Read ActivityFeed.ReadDlp
ServiceHealth	ServiceHealth.Read

d. Click **Add permssions**.

e. In the **API permissions** window, go to the **Grant consent** section, click **Grant admin consent** > **Yes**.

What to do next

Adding a log source

Related concepts

"Microsoft Office 365" on page 1196

The IBM QRadar DSM for Microsoft Office 365 collects events from Microsoft Office 365 online services.

Microsoft Office 365 sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft Office 365 sample messages when you use the Office 365 REST API protocol

Sample 1: The following sample event message shows that a member is successfully added to a group.

{"**CreationTime**":"2020-01-10T15:07:31","Id":"aaaaaaaa4-bbbb-cccc-c664-qwerasdfzxcv","**Operation**":"Set-Mailbox","OrganizationId":"aaaaaaaaa-f5b4-5d43-8070-xxxxxxxxxxx","RecordType":1,"ResultStatus":"True","**UserKey**":"\"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/**iteamtesting.onmicrosoft.com/admin.user**\" on behalf of \"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/user1\"","UserType":2,"Version":1,"**Workload**":"Exchange","**ClientIP**":"10.10.1.21:7414","ObjectId":"user1","UserId":"\"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/admin.user\" on behalf of \"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/user1\"","AppId":"","ClientAppId":"","ExternalAccess":false,"OrganizationName":"iteamtesting.onmicrosoft.com","OriginatingServer":"SERVER1234 (10.20.30.40)","Parameters":[{"Name":"Identity","Value":"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/user1"},{"Name":"ForwardingSmtpAddress","Value":""},{"Name":"DeliverToMailboxAndForward","Value":"True"}],"SessionId":"aaaaaa-bbbb-cccc-dddd-bgh627392m"}

{"**CreationTime**":"2020-01-10T15:07:31","Id":"aaaaaaaa4-bbbb-cccc-c664-qwerasdfzxcv","**Operation**":"Set-Mailbox","OrganizationId":"aaaaaaaaa-f5b4-5d43-8070-xxxxxxxxxxx","RecordType":1,"ResultStatus":"True","**UserKey**":"\"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/**iteamtesting.onmicrosoft.com/admin.user**\" on behalf of \"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/user1\"","UserType":2,"Version":1,"**Workload**":"Exchange","**ClientIP**":"10.10.1.21:7414","ObjectId":"user1","UserId":"\"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/admin.user\" on behalf of \"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/user1\"","AppId":"","ClientAppId":"","ExternalAccess":false,"OrganizationName":"iteamtesting.onmicrosoft.com","OriginatingServer":"SERVER1234 (10.20.30.40)","Parameters":[{"Name":"Identity","Value":"host.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/iteamtesting.onmicrosoft.com/user1"},{"Name":"ForwardingSmtpAddress","Value":""},{"Name":"DeliverToMailboxAndForward","Value":"True"}],"SessionId":"aaaaaa-bbbb-cccc-dddd-bgh627392m"}

Table 790. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**Operation**
Event Category	**Workload**
Log Source Time	**CreationTime**
Username	**UserKey** Only the **iteamtesting.onmicrosoft.com/admin.user** portion of the **UserKey** is used for the **Username**.
Source IP	**ClientIP**

Sample 2: The following sample event message shows a Session Started audit event for Microsoft Teams.


```
{\"CreationTime\":\"2020-06-23T13:16:59\",\"Id\":\"22222222-4444-4444-4444-
aaaaaaaaaaaa\",\"Operation\":\"TeamsSessionStarted\",\"OrganizationId\":\"aaaaaaaa-bbbb-cccc-dddd-
aaaaaaaaaaaa\",\"RecordType\":25,\"UserKey\":\"aaaaaaaaa-aaaa-bbbb-cccc-
aaaaaaaaaaaa\",\"UserType\":0,\"Version\":1,\"Workload\":\"MicrosoftTeams\",\"ClientIP\":\"10.118.
199.208\",\"ObjectId\":\"Unknown (Unknown)\",\"UserId\":\"firstname.lastname@example.com\"}
```

```
{\"CreationTime\":\"2020-06-23T13:16:59\",\"Id\":\"22222222-4444-4444-4444-
aaaaaaaaaaaa\",\"Operation\":\"TeamsSessionStarted\",\"OrganizationId\":\"aaaaaaaa-bbbb-cccc-
dddd-aaaaaaaaaaaa\",\"RecordType\":25,\"UserKey\":\"aaaaaaaaa-aaaa-bbbb-cccc-
aaaaaaaaaaaa\",\"UserType\":0,\"Version\":1,\"Workload\":\"MicrosoftTeams\",\"ClientIP\":\"10.11
8.199.208\",\"ObjectId\":\"Unknown (Unknown)\",\"UserId\":\"firstname.lastname@example.com\"}
```


Table 791. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**Operation**
Event Category	**Workload**
Log Source Time	**CreationTime**
Username	**UserId**
Source IP	**ClientIP**

Microsoft Office 365 Message Trace

The IBM QRadar DSM for Microsoft Office 365 Message Trace collects JSON events from a Microsoft Office 365 Message Trace by using the Office 365 Message Trace API protocol.

To integrate Microsoft Office 365 Message Trace with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM support website (http://www.ibm.com/support):
   - Microsoft Office 365 Message Trace DSM RPM
   - Protocol Common RPM
   - Office 365 Message Trace API protocol RPM
2. Add a Microsoft Office 365 Message Trace log source by using the Office 365 Message Trace REST API protocol on the QRadar Console. The Office 365 Message Trace REST API protocol supports both modern and basic authentication. Modern authentication uses OAuth 2.0 to authenticate and authorize access to the resource, while basic authentication uses a username and password.

   Important: As of 1 January 2023, Microsoft will no longer support basic authentication. To continue receiving Message Trace events, you must use modern authentication. Modern authentication uses OAuth 2.0 to authenticate and authorize access to the events. For more information

about the deprecation of basic authentication, see Basic Authentication Deprecation in Exchange Online – September 2022 Update (https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-deprecation-in-exchange-online-september/ba-p/3609437).

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Microsoft Office 365 Message Trace DSM specifications

When you configure Microsoft Office 365 Message Trace, understanding the specifications for the Microsoft Office 365 Message Trace DSM can help ensure a successful integration. For example, knowing what the supported version of Microsoft Office 365 Message Trace is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Microsoft Office 365 Message Trace DSM.

Table 792. Microsoft Office 365 Message Trace DSM specifications

Specification	Value
Manufacturer	Microsoft
DSM name	Microsoft Office 365 Message Trace
RPM file name	`DSM-MicrosoftOffice365MessageTrace-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	N/A
Protocol	Office 365 Message Trace REST API
Event format	JSON
Recorded event types	Email security threat classification
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Message trace in the Security & Compliance Center (https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/message-trace-scc?view=o365-worldwide)

Microsoft Office Message Trace REST API log source parameters for Microsoft Office Message Trace

If QRadar does not automatically detect the log source, add a Microsoft Office Message Trace log source on the QRadar Console by using the Office 365 Message Trace REST API protocol.

When using the Microsoft Office 365 Message Trace REST API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Microsoft Office 365 Message Trace REST API events from Microsoft Office 365 Message Trace:

Table 793. Microsoft Office 365 Message Trace REST API log source parameters for the Microsoft Office 365 Message Trace DSM	
Parameter	**Value**
Log Source type	Microsoft Office 365 Message Trace
Protocol Configuration	Office 365 Message Trace REST API
Log Source Identifier	A unique name for the log source. The name can't include spaces and must be unique among all log sources of this type that are configured with the Office 365 Message Trace REST API protocol.

For a complete list of Office 365 Message Trace REST API protocol parameters and their values, see Office 365 Message Trace REST API protocol configuration options.

Related tasks

Adding a log source

Microsoft Office 365 Message Trace sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft Office 365 Message Trace sample message when you use the Office 365 Message Trace REST API protocol

The following sample event message shows that a message was successfully delivered to the intended destination.


```
{"Organization":"test.oncompany.test","MessageId":"<32A2AAA5SAA4.AAAA00A6A2AA@AA00155AA5A4A6>","
Received":"2020-06-02T01:29:06.3627033","SenderAddress":"username@domain.test","RecipientAddress
":"testRecep@test.oncompany.test","Subject":"Azure AD Identity Protection Weekly
Digest","Status":"Delivered","ToIP":null,"FromIP":"10.10.10.12","Size":76047,"MessageTraceId":"6
6f62cca-c8ce-4436-
f519-08d80694575d","StartDate":"2020-05-31T16:34:00Z","EndDate":"2020-06-02T16:34:00Z","Index":0
}
```



```
{"Organization":"test.oncompany.test","MessageId":"<32A2AAA5SAA4.AAAA00A6A2AA@AA00155AA5A4A6>",
"Received":"2020-06-02T01:29:06.3627033","SenderAddress":"username@domain.test","Reci
pientAddress":"testRecep@test.oncompany.test","Subject":"Azure AD Identity Protection Weekly
Digest","Status":"Delivered","ToIP":null,"FromIP":
"10.10.10.12","Size":76047,"MessageTraceId":"66f62cca-c8ce-4436-f519-08d80694575d",
"StartDate":"2020-05-31T16:34:00Z","EndDate":"2020-06-02T16:34:00Z","Index":0}
```


Table 794. Highlighted fields	
QRadar field name	**Highlighted payload field name**
Event ID	**Status**
Username	**SenderAddress**
Source IP	**FromIP**
Destination IP	**ToIP**
Device Time	**StartDate**

JDBC log source parameters for Microsoft Operations Manager

If QRadar does not automatically detect the log source, add a Microsoft Operations Manager log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Microsoft Operations Manager:

Table 795. JDBC log source parameters for the Microsoft Operations Manager DSM

Parameter	Value
Log Source type	Microsoft Operations Manager
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	From the list, select **MSDE**.
Database Name	Type `OnePoint` as the name of the Microsoft Operations Manager database.
IP or Hostname	Type the IP address or host name of the Microsoft Operations Manager SQL Server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft Operations Manager database. The Microsoft Operations Manager database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a **Database Instance** when MSDE is used as the database type, you must leave the **Port** parameter blank in your configuration.
Table Name	Type `SDKEventView` as the name of the table or view that includes the event records.
Compare Field	Type `TimeStored` as the compare field. The compare field is used to identify new events that are added between queries to the table.

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

Adding a log source

Microsoft SharePoint

The Microsoft SharePoint DSM for IBM QRadar collects audit events from the SharePoint database by using JDBC to poll an SQL database for audit events.

Audit events can track changes that are made to sites, files, and content that is managed by Microsoft SharePoint.

Microsoft SharePoint audit events include the following elements:

- Site name and the source from which the event originated
- Item ID, item name, and event location
- User ID associated with the event
- Event type, time stamp, and event action

Two log source configurations can be used to collect Microsoft SharePoint database events.

1. Create a database view in your SharePoint database to poll for events with the JDBC protocol. See Creating a database view for Microsoft SharePoint.
2. Create a JDBC log source and use predefined database queries to collect SharePoint events. This option does not require an administrator to create database view. See "JDBC log source parameters for Microsoft Share Point" on page 1207.

Note: The collection of Microsoft Sharepoint events now uses a predefined query, instead of requiring an administrator to create a database view. If you are an administrator, you might want to update existing Microsoft Sharepoint log sources so that they use the Microsoft Sharepoint predefined query.

Configuring Microsoft SharePoint audit events

The audit settings for Microsoft SharePoint give you the option to define what events are tracked for each site that is managed by Microsoft SharePoint.

Procedure

1. Log in to your Microsoft SharePoint site.
2. From the **Site Actions** list, select **Site Settings**.
3. From the **Site Collection Administration** list, click **Site collection audit settings**.
4. From the **Documents and Items** section, select a check box for each document and item audit event you want to audit.
5. From the **Lists, Libraries, and Sites** section, select a check box for each content audit event you want to enable.
6. Click **OK**.

What to do next

Create a database view for IBM QRadar to poll Microsoft SharePoint events.

Related tasks

"Creating a database view for Microsoft SharePoint" on page 1206

Microsoft SharePoint uses SQL Server Management Studio (SSMS) to manage the SharePoint SQL databases. To collect audit event data, you must create a database view on your Microsoft SharePoint server that is accessible to IBM QRadar.

Creating a database view for Microsoft SharePoint

Microsoft SharePoint uses SQL Server Management Studio (SSMS) to manage the SharePoint SQL databases. To collect audit event data, you must create a database view on your Microsoft SharePoint server that is accessible to IBM QRadar.

Before you begin

Do not use a period (.) in the name of your view, or in any of the table names. If you use a period in your view or table name, JDBC cannot access the data within the view and access is denied. Anything after a (.) is treated as a child object.

Procedure

1. Log in to the system that hosts your Microsoft SharePoint SQL database.
2. From the **Start** menu, select **Run**.
3. Type the following command:

   `ssms`
4. Click **OK**.

   The Microsoft SQL Server 2008 displays the **Connect to Server** window.
5. Log in to your Microsoft SharePoint database.
6. Click **Connect**.
7. From the **Object Explorer** for your SharePoint database, click **Databases** > **WSS_Logging** > **Views**.
8. From the navigation menu, click **New Query**.
9. In the **Query** pane, type the following Transact-SQL statement to create the AuditEvent database view:

   ```
   create view dbo.AuditEvent as select a.siteID
   ```

   ```
   ,a.ItemId ,a.ItemType ,u.tp_Title as
   "User" ,a.MachineName ,a.MachineIp ,a.DocLocation ,a.LocationType ,a.Occurred as
   "EventTime" ,a.Event as "EventID" ,a.EventName ,a.EventSource ,a.SourceName ,a.EventData
   ```

   ```
   from WSS_Content.dbo.AuditData a, WSS_Content.dbo.UserInfo u where a.UserId = u.tp_ID and
   a.SiteId = u.tp_SiteID;
   ```
10. From the **Query** pane, right-click and select **Execute**.

    If the view is created, the following message is displayed in the results pane:

    `Command(s) completed successfully.`

    The `dbo.AuditEvent` view is created. You are now ready to configure the log source in QRadar to poll the view for audit events.

Creating read-only permissions for Microsoft SharePoint database users

Restrict user access on the SharePoint database by granting read-only permissions on objects.

Procedure

1. From the **Object Explorer** in your SharePoint database, click **Security**. Expand the **Security** folder tree.
2. Right-click **Logins** and select **New Login**.

3. For Windows authentication, complete the following steps:
   a) On the **General** page, click **Search**.
   b) Click **Locations**. From the **Locations** page, select a location that the user belongs to and click **OK**.
   c) Enter the object name in the text-box, and click **Check Names** to validate the user.

      Note: Set the **Default database** to **WSS_Logging**.
   d) On the **Server Roles** page, select **public**.
   e) On the **User Mapping** page, select the **WSS_Content** and **WSS_Logging**. In the **`Default Schema`** column, click **...** > **Browse...** and select **db_datareader** as the default schema.
   f) On the **Status** page, select **Grant** permission to connect to the database engine and select **Enabled** login.
4. From the **Object Explorer** in your SharePoint database, click **Databases** > **WSS_Logging** > **Security** > **Users**.
   a) Double-click the Windows user that was created in step 3.
   b) On the **Securables** page, click **Search**.
   c) On the **Add Objects** page, select **Specific objects...** and click **OK**.
   d) Click **Object Types...** and select **Views**.
   e) For object names, click **Browse** and select the database view that you created. For example, **`[dbo].[AuditEvent]`**.
   f) For the permissions of the database view you select, grant **Select**.
   g) Click **OK**.
5. From the **Object Explorer** in your SharePoint database, click **Databases** > **WSS_Content** > **Security** > **Users**.
   a) Double-click the Windows user that was created in step 3.
   b) On the **Securables** page, click **Search**.
   c) On the **Add Objects** page, select **Specific objects...** and click **OK**.
   d) Click **Object Types...** and select **Tables**.
   e) For object names, click **Browse**. Select **[dbo].[AuditData]** and **[dbo].[UserInfo]**.
   f) For the permissions of the **`AuditData`** table, grant **Select**.
   g) For the permissions of the **`UserInfo`** table, grant **Select**.
   h) Click **OK**.

JDBC log source parameters for Microsoft Share Point

If QRadar does not automatically detect the log source, add a Microsoft SharePoint log source on the QRadar Console by using the JDBC protocol.

Tip: Ensure that firewall rules are not blocking the communication between QRadar and the database that is associated with Microsoft SharePoint.

The following table describes the parameters that require specific values to collect JDBC events from Microsoft SharePoint:

Table 796. JDBC log source parameters for the Microsoft SharePoint DSM

Parameter	Value
`Log Source type`	Microsoft SharePoint
`Protocol Configuration`	JDBC

Table 796. JDBC log source parameters for the Microsoft SharePoint DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	From the list, select **MSDE**.
Database Name	Type `WSS_Logging` as the name of the Microsoft SharePoint database.
IP or Hostname	Type the IP address or host name of the Microsoft SharePoint SQL Server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SharePoint database. The Microsoft SharePoint database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a **Database Instance** when you use **MSDE** as the database type, you must leave the **Port** parameter blank in your configuration.
Table Name	Type `AuditEvent` as the name of the table or view that includes the event records.
Compare Field	Type `EventTime` as the compare field. The compare field is used to identify new events added between queries to the table.

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

Adding a log source

JDBC log source parameters for Microsoft SharePoint with predefined database queries

Administrators who do not have permission to create a database view because of policy restrictions can collect Microsoft SharePoint events with a log source that uses predefined queries. If QRadar does not

automatically detect the log source, add a Microsoft SharePoint log source on the QRadar Console by using the JDBC protocol.

Predefined queries are customized statements that can join data from separate tables when the database is polled by the JDBC protocol.

Tip: Ensure that firewall rules are not blocking the communication between QRadar and the database that is associated with Microsoft SharePoint.

The following table describes the parameters that require specific values to collect JDBC events from Microsoft SharePoint:

Table 797. JDBC log source parameters for the Microsoft SharePoint DSM

Parameter	Value
Log Source type	Microsoft SharePoint
Protocol Configuration	JDBC
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: *<SharePoint Database>@<SharePoint Database Server IP or Host Name>* Where: • *<SharePoint Database>* is the database name, as entered in the Database Name parameter. • *<SharePoint Database Server IP or Host Name>* is the host name or IP address for this log source, as entered in the **IP or Hostname** parameter.
Database Type	From the list, select **MSDE**.
Database Name	Type `WSS_Logging` as the name of the Microsoft SharePoint database.
IP or Hostname	Type the IP address or host name of the Microsoft SharePoint SQL Server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SharePoint database. The Microsoft SharePoint database must have incoming TCP connections that are enabled to communicate with IBM QRadar. If you define a **Database Instance** when you use **MSDE** as the database type, you must leave the **Port** parameter blank in your configuration.
Predefined Query	From the list, select **Microsoft SharePoint**.

Table 797. JDBC log source parameters for the Microsoft SharePoint DSM (continued)	
Parameter	**Value**
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.
Use NTLMv2	Select the **Use NTLMv2** check box. This option forces MSDE connections to use the NTLMv2 protocol when they communicate with SQL servers that require NTLMv2 authentication. The default value of the check box is selected. If the **Use NTLMv2** check box is selected, it has no effect on MSDE connections to SQL servers that do not require NTLMv2 authentication.

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

Adding a log source

Microsoft SQL Server

The IBM QRadar DSM for Microsoft SQL Server collect SQL events by using the syslog, WinCollect Microsoft SQL, or JDBC protocol.

The following table identifies the specifications for the Microsoft SQL Server DSM:

Table 798. Microsoft SQL Server DSM	
Specification	**Value**
Manufacturer	Microsoft
DSM name	SQL Server
RPM file name	DSM-MicrosoftSQL-*QRadar-version-Build_number*.noarch.rpm
Supported versions	2012, 2014 (Enterprise editions only), 2016, 2017, and 2019
Event format	Syslog, JDBC, WinCollect
QRadar recorded event types	SQL error log events
Automatically discovered?	Yes
Includes identity?	Yes
More information	Microsoft website (http://www.microsoft.com/en-us/server-cloud/products/sql-server/)

You can integrate Microsoft SQL Server with QRadar by using one of the following methods:

Syslog
The IBM QRadar DSM for Microsoft SQL Server can collect LOGbinder SQL events. For information about configuring LOGbinder SQL to collect events from your Microsoft SQL Server, see "LOGbinder SQL event collection from Microsoft SQL Server" on page 1124

.

JDBC
Microsoft SQL Server Enterprise can capture audit events by using the JDBC protocol. The audit events are stored in a table view. Audit events are only available in Microsoft SQL Server 2012, 2014 Enterprise, and 2016.

WinCollect
You can integrate Microsoft SQL Server 2012, 2014, 2016, 2017, and 2019 with QRadar by using WinCollect to collect ERRORLOG messages from the databases that are managed by your Microsoft SQL Server. For more information about WinCollect, go to the WinCollect documentation (https://www.ibm.com/docs/en/qsip/7.5?topic=7-wincollect-overview).

To integrate the Microsoft SQL Server DSM with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Microsoft SQL Server RPM from the IBM Support Website onto your QRadar Console.
2. For each instance of Microsoft SQL Server, configure your Microsoft SQL Server appliance to enable communication with QRadar.
3. If QRadar does not automatically discover the Microsoft SQL Server log source, create a log source for each instance of Microsoft SQL Server on your network.

Related concepts

"LOGbinder SQL event collection from Microsoft SQL Server" on page 1124
The IBM QRadar DSM for Microsoft SQL Server can collect LOGbinder SQL events.

Related tasks

"Configuring your LOGbinder SQL system to send Microsoft SQL Server event logs to QRadar" on page 1125
To collect Microsoft SQL Server LOGbinder events, you must configure your LOGbinder SQL system to send events to IBM QRadar.

"Adding a DSM" on page 4
"Adding a log source" on page 5

Microsoft SQL Server preparation for communication with QRadar

To prepare Microsoft SQL Server for communication with QRadar, you must create an audit object, audit specification, and database view.

Creating a Microsoft SQL Server auditing object

Create an auditing object to store audit events.

Procedure

1. Log in to your Microsoft SQL Server Management Studio.
2. From the navigation menu, select **Security** > **Audits**.
3. Right-click **Audits** and select **New Audit**.
4. In the **Audit name** field, type a name for the new audit file.
5. From the **Audit destination** list, select **File**.
6. From the **File path** field, type the directory path for your Microsoft SQL Server audit file.
7. Click **OK**.

8. Right-click your audit object and select **Enable Audit**.

Creating a Microsoft SQL Server audit specification

Create an audit specification to define the level of auditing events that are written to an audit file.

Before you begin

You must create an audit object. For more information, see "Creating a Microsoft SQL Server auditing object" on page 1211.

About this task

You can create an audit specification at the server level or at the database level. Depending on your requirements, you might require both a server and database audit specification.

Procedure

1. From the Microsoft SQL Server Management Studio navigation menu, select one the following options:
   - **Security** > **Server Audit Specifications**
   - **<Database>** > **Security** > **Database Audit Specifications**
2. To enable Server or Database Audit, select one of the following options:
   - Right-click **Server Audit Specification**, then select **New Server Audit Specifications**
   - Right-click **Database Audit Specification**, then select **New Database Audit Specifications**
3. In the **Name** field, type a name for the new audit file.
4. From the **Audit** list, select the audit object that you created.
5. In the **Actions** pane, add actions and objects to the server audit.
6. Click **OK**.
7. Right-click your server audit specification and select one of the following options:
   - **Enable Server Audit Specification**
   - **Enable Database Audit Specification**

What to do next

Create a SQL Server database view.

Creating a Microsoft SQL Server database view

Create the dbo.AuditData database view to allow QRadar to poll for audit events from a database table by using the JDBC protocol. The database view contains the audit events from your server audit specification and database audit specification.

Procedure

1. From the Microsoft SQL Server Management Studio toolbar, click **New Query**.
2. Type the following Transact-SQL statement:

```
create view dbo.AuditData as      SELECT * FROM sys.fn_get_audit_file     ('<Audit File Path
and Name>',default,default);     GOa
```

   For example:

```
create view dbo.AuditData as      SELECT * FROM sys.fn_get_audit_file
('C:\inetpub\logs\SQLAudits*',default,default);     GO
```

3. From the Standard toolbar, click **Execute**.

JDBC log source parameters for Microsoft SQL Server

If QRadar does not automatically detect the log source, add a Microsoft SQL Server log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Microsoft SQL Server:

Table 799. JDBC log source parameters for the Microsoft SQL Server DSM

Parameter	Value
Log Source type	Microsoft SQL Server
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	From the list, select **MSDE**.
Database Name	Type `Master` as the name of the Microsoft SQL database.
IP or Hostname	Type the IP address or host name of the Microsoft SQL server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SQL database. The Microsoft SQL database must have incoming TCP connections that are enabled to communicate with QRadar. **Important:** If you define a **Database Instance** when you are using MSDE as the **Database Type**, you must leave the **Port** parameter blank in your configuration.
Table Name	Type `dbo.AuditData` as the name of the table or view that includes the audit event records.
Compare Field	Type `event_time` in the **Compare Field** parameter. The **Compare Field** identifies new events that are added between queries, in the table.

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

Adding a log source

Microsoft SQL Server sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft SQL Server sample message when you use the Syslog protocol

The following sample event message shows a Microsoft SQL Server Drop Login event.

event_time: "2019-02-11 13:17:32.0931454" sequence_number: "1" **action_id**: "DR"
succeeded: "true" permission_bitmask: "00000000000000000000000000000000" is_column_permission:
"false" session_id: "93" server_principal_id: "261" database_principal_id: "1"
target_server_principal_id: "0" target_database_principal_id: "0" object_id: "280"
class_type: "WL" **session_server_principal_name**: "test\testUser" server_principal_name:
"test\testUser" server_principal_sid: "0105000000000005150000000400A7B7284B93A98D9627B492A050000"
database_principal_name: "dbo" target_server_principal_name: "" target_server_principal_sid:
"null" target_database_principal_name: "" server_instance_name:
"testInstance" database_name: "master" schema_name: "" object_name:
"test\9testSIEMSQLread" statement: "DROP LOGIN [test\9testSIEMSQLread]"
additional_information: "" file_name: "L:\Audit\Audit-20190201-185847_AAD06900-8725-43A2-
A949-9F15D560395A_0_131938307626970000.sqlaudit" audit_file_offset: "35328"
user_defined_event_id: "0" user_defined_information: "" audit_schema_version: "1"
sequence_group_id: "8EDC9010D8D0294FB639D026C4CB2241" transaction_id: "1321291"

event_time: "2019-02-11 13:17:32.0931454" sequence_number: "1" **action_id**: "DR"
succeeded: "true" permission_bitmask: "00000000000000000000000000000000" is_column_permission:
"false" session_id: "93" server_principal_id: "261" database_principal_id: "1"
target_server_principal_id: "0" target_database_principal_id: "0" object_id: "280" **class_type**:
"WL" **session_server_principal_name**: "test\testUser" server_principal_name: "test\testUser"
server_principal_sid: "0105000000000005150000000400A7B7284B93A98D9627B492A050000"
database_principal_name: "dbo" target_server_principal_name: "" target_server_principal_sid:
"null" target_database_principal_name: "" server_instance_name:
"testInstance" database_name: "master" schema_name: "" object_name:
"test\9testSIEMSQLread" statement: "DROP LOGIN [test\9testSIEMSQLread]"
additional_information: "" file_name: "L:\Audit\Audit-20190201-185847_AAD06900-8725-43A2-
A949-9F15D560395A_0_131938307626970000.sqlaudit" audit_file_offset: "35328"
user_defined_event_id: "0" user_defined_information: "" audit_schema_version: "1"
sequence_group_id: "8EDC9010D8D0294FB639D026C4CB2241" transaction_id: "1321291"

Table 800. Highlighted values in the Microsoft SQL Server sample event

QRadar field name	Highlighted values in the event payload
Event ID	**action_id** + **class_type**
Category	When the Microsoft SQL Server DSM parses this type of event, the **Category** value in QRadar is always **MicrosoftSQL**.
Username	**session_server_principal_name**
Log Source Time	**event_time**

JDBC log source parameters for Microsoft System Center Operations Manager

If QRadar does not automatically detect the log source, add a Microsoft System Center Operations Manager (SCOM) log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from the Microsoft System Center Operations Manager:

Table 801. JDBC log source parameters for the Microsoft System Center Operations Manager DSM

Parameter	Value
Log Source type	Microsoft SCOM
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	From the list, select **MSDE**.
Database Name	The name of the Microsoft SCOM database.
IP or Hostname	Type the IP address or host name of the Microsoft SCOM SQL Server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Microsoft SCOM database. The Microsoft SCOM database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a **Database Instance** when MSDE is used as the database type, you must leave the **Port** parameter blank in your configuration.
Table Name	Type `EventView` as the name of the table or view that includes the event records.
Compare Field	Type **TimeAdded** as the compare field. The compare field is used to identify new events added between queries to the table.

For a complete list of JDBC protocol parameters and their values, see JDBC protocol configuration options.

Related tasks

Adding a log source

Microsoft Windows Security Event Log

The IBM QRadar DSM for Microsoft Windows Security Event Log accepts syslog events from Microsoft Windows systems. All events, including Sysmon and winlogbeats.json, are supported.

Important: Support for the Windows Event Log protocols ended on 31 October 2022. To continue collecting Windows Event Log events, you must select a new protocol type from the list of supported protocols. For more information about the end of support, see QRadar: End of life announcement for WMI-based Microsoft Windows Security Event Log protocols (31 Oct 2022) (https://www.ibm.com/support/pages/node/6616223).

For event collection from Microsoft operating systems, QRadar supports the following protocols:

- Syslog (Intended for Snare, BalaBit, and other third-party Windows solutions).
- Forwarded. For more information, see "Forwarded protocol configuration options" on page 117.
- TLS Syslog. For more information, see "TLS Syslog protocol configuration options" on page 227.
- TCP Multiline Syslog. For more information, see "TCP Multiline Syslog protocol configuration options" on page 222.
- MSRPC (Microsoft Security Event Log over MSRPC). For more information, see "Microsoft Security Event Log over MSRPC Protocol" on page 189.
- WinCollect. See the *IBM QRadar WinCollect User Guide*.
- WinCollect NetApp Data ONTAP. See the *IBM QRadar WinCollect User Guide*.
- Amazon Web Services protocol from AWS CloudWatch. For more information, see "Amazon Web Services protocol configuration options" on page 83 and How do I upload my Windows logs to CloudWatch? (https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-upload-windows-logs/).
- Microsoft Azure Event Hubs. For more information, see Microsoft Azure Event Hubs protocol configuration options and Install and configure Windows Azure diagnostics extension (WAD) - Azure Monitor (https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostics-extension-windows-install).

  Ensure that you have an Azure storage account and an Azure event hub.

  1. Optional: Create a storage account. For more information, see Create a storage account (https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal).

     Important: You must have a storage account to connect to an event hub. For more information, see Microsoft Azure Event Hubs protocol FAQ.
  2. Optional: Create an event hub. For more information, see Quickstart: Create an event hub using Azure portal (https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-create).

Related concepts

MSRPC parameters on Windows hosts
To enable communication between your Windows host and IBM QRadar over MSRPC, configure the Remote Procedure Calls (RPC) settings on the Windows host for the Microsoft Remote Procedure Calls (MSRPC) protocol.

WMI parameters on Windows hosts
Support for the Windows Event Log protocols ended on 31 October 2022.

Installing the MSRPC protocol on the QRadar Console

You must install the MSRPC protocol RPM on the QRadar Console before events can be collected from a Windows host.

Before you begin

Ensure that you download the MSRPC protocol RPM from the IBM Support Website onto your QRadar Console.

Procedure

1. Log in to the QRadar Console as a root user.
2. Copy the MSRPC protocol RPM to a directory on the QRadar Console.
3. Go to the directory where you copied the MSRPC protocol RPM by typing the following command:

```
cd <path_to_directory>
```

4. Install the MSRPC protocol RPM by typing the following command:

```
yum –y install PROTOCOL-WindowsEventRPC-<version_number>.noarch.rpm
```

5. From the **Admin** tab of the QRadar Console, select **Advanced** > **Deploy Full Configuration**.
6. After you deploy the configuration, select **Advanced** > **Restart Web Server**.

MSRPC parameters on Windows hosts

To enable communication between your Windows host and IBM QRadar over MSRPC, configure the Remote Procedure Calls (RPC) settings on the Windows host for the Microsoft Remote Procedure Calls (MSRPC) protocol.

You must be a member of the administrators group to enable communication over MSRPC between your Windows host and the QRadar appliance.

Based on performance tests on an IBM QRadar QRadar Event Processor 1628 appliance with 128 GB of RAM and 40 cores (Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80 GHz), a rate of 8500 events per second (eps) was achieved successfully, while simultaneously receiving and processing logs from other non-Windows systems. The log source limit is 500.

Specification	Value
Manufacturer	Microsoft
Protocol type	The operating system dependant type of the remote procedure protocol for collection of events. Select one of the following options from the **Protocol Type** list: **MS-EVEN6** The default protocol type for new log sources. The protocol type that is used by QRadar to communicate with Windows Vista and Windows Server 2008 and later. **MS-EVEN (for Windows XP/2003)** The protocol type that is used by QRadar to communicate with Windows XP and Windows Server 2003. Windows XP and Windows Server 2003 are not supported by Microsoft. The use of this option might not be successful. **auto-detect (for legacy configurations)** Previous log source configurations for the Microsoft Windows Security Event Log DSM use the **auto-detect (for legacy configurations)** protocol type. Upgrade to the **MS_EVEN6** or the **MS-EVEN (for Windows XP/2003)** protocol type.

Specification	Value
Supported versions	Windows Server 2022 (including Core) WinCollect v10.1.2 and above Windows Server 2019 (including Core) Windows Server 2016 (including Core) Windows Server 2012 (including Core) Windows 11 WinCollect v10.1.2 and above Windows 10
Intended application	Agentless event collection for Windows operating systems that can support 100 EPS per log source.
Maximum number of supported log sources	500 MSRPC protocol log sources for each managed host (16xx or 18xx appliance)
Maximum overall EPS rate of MSRPC	8500 EPS for each managed host
Special features	Supports encrypted events by default.
Required permissions	The log source user must be a member of the **Event Log Readers** group. If this group is not configured, then domain admin privileges are required in most cases to poll a Windows event log across a domain. In some cases, the **Backup operators** group can also be used depending on how Microsoft Group Policy Objects are configured. Windows XP and 2003 operating system users require read access to the following registry keys: • `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog` • `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language` • `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft Windows\CurrentVersion`
Supported event types	Application System Security DNS Server File Replication Directory Service logs
Windows service requirements	For Windows Server 2008 and Windows Vista, use the following services: • Remote Procedure Call (RPC) • RPC Endpoint Mapper For Windows 2003, use the Remote Registry and Server.

Specification	Value
Windows port requirements	Ensure that external firewalls between the Windows host and the QRadar appliance are configured to allow incoming and outgoing TCP connections on the following ports: For Windows Server 2008 and Windows Vista, use the following ports: • TCP port 135 • TCP port that is dynamically allocated for RPC, above 49152 For Windows 2003, use the following ports: • TCP port 445 • TCP port 139
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	A security content pack with Windows custom event properties is available on IBM Fix Central.
Required RPM files	`PROTOCOL-WindowsEventRPC-`*`QRadar_release-Build_number`*`.noarch.rpm` `DSM-MicrosoftWindows-`*`QRadar_release-Build_number`*`.noarch.rpm` `DSM-DSMCommon-`*`QRadar_release-Build_number`*`.noarch.rpm`
More information	Microsoft support (http://support.microsoft.com/)
Troubleshooting tool available	MSRPC test tool is part of the MSRPC protocol RPM. After installation of the MSRPC protocol RPM, the MSRPC test tool can be found in `/opt/qradar/jars`

Related concepts

Microsoft Windows Security Event Log

The IBM QRadar DSM for Microsoft Windows Security Event Log accepts syslog events from Microsoft Windows systems. All events, including Sysmon and winlogbeats.json, are supported.

Microsoft Security Event Log over MSRPC log source parameters for Microsoft Windows Security Event Log

If QRadar does not automatically detect the log source, add a Microsoft Windows Security Event Log log source on the QRadar Console by using the Microsoft Security Event Log over MSRPC protocol.

When using the Microsoft Security Event Log over MSRPC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Microsoft Security Event Log over MSRPC events from Microsoft Windows Security Event Log:

Table 802. Microsoft Security Event Log over MSRPC log source parameters for the Microsoft Windows Security Event Log DSM	
Parameter	**Value**
Log Source type	**Microsoft Windows Security Event Log**
Protocol Configuration	**Microsoft Security Event Log over MSRPC**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Microsoft Windows Security Event Log devices.

For a complete list of Microsoft Security Event Log over MSRPC protocol parameters and their values, see Microsoft Security Event Log over MSRPC Protocol.

Related tasks

Adding a log source

WMI parameters on Windows hosts

Support for the Windows Event Log protocols ended on 31 October 2022.

Important: Support for the Windows Event Log protocols ended on 31 October 2022. To continue collecting Windows Event Log events, you must select a new protocol type from the "Microsoft Windows Security Event Log" on page 1216 page. For more information, see QRadar: End of life announcement for WMI-based Microsoft Windows Security Event Log protocols (31 Oct 2022) (https://www.ibm.com/support/pages/node/6616223).

Related concepts

Microsoft Windows Security Event Log

The IBM QRadar DSM for Microsoft Windows Security Event Log accepts syslog events from Microsoft Windows systems. All events, including Sysmon and winlogbeats.json, are supported.

Microsoft Security Event Log log source parameters for Microsoft Windows Security Event Log

Support for the Windows Event Log protocols ended on 31 October 2022.

Important: Support for the Windows Event Log protocols ended on 31 October 2022. To continue collecting Windows Event Log events, you must select a new protocol type from the "Microsoft Windows Security Event Log" on page 1216 page. For more information, see QRadar: End of life announcement for WMI-based Microsoft Windows Security Event Log protocols (31 Oct 2022) (https://www.ibm.com/support/pages/node/6616223).

Installing Winlogbeat and Logstash on a Windows host

To retrieve Winlogbeat JSON formatted events in QRadar, you must install Winlogbeat and Logstash on your Microsoft Windows host.

Before you begin

Ensure that you are using the Oracle Java Development Kit V8 for Windows x64 and later.

Procedure

1. Install Winlogbeat 7.7 by using the default values. For more information, see Getting Started With Winlogbeat (https://www.elastic.co/guide/en/beats/winlogbeat/7.7/winlogbeat-getting-started.html).
2. Start the Winlogbeat service.

Note: For Windows services, the service name is Winlogbeat. After installation, the service is set to STOPPED, and then must be started for the first time. Any configuration changes beyond this point require a service restart.

3. Optional. For more flexibility when you configure Winlogbeat, see Set up Winlogbeat (https://www.elastic.co/guide/en/beats/winlogbeat/7.7/configuration-winlogbeat-options.html).
4. Install Logstash by downloading the package and saving it to a file location of your choice.
5. To ensure that Winlogbeat communicates properly with QRadar, see Configure Winlogbeat to use Logstash (https://www.elastic.co/guide/en/beats/winlogbeat/7.7/config-winlogbeat-logstash.html).

   The following basic sample configuration file can be used in the *<logstash_install_directory>*/config file.

```
    input {     beats {        port => 5044      }    }    output {      tcp {        host
=> ["172.16.199.22"]        port => 514        mode => "client"        codec =>
"json_lines"      }      stdout { codec => rubydebug }    }
```

   Notes:

   - If you are using rubydebug, debugging must be enabled in the `logstash.yml` file. Uncomment the line `# log.level: info`, and replace `info` with `debug`. Restarting the service is required after any configuration changes.
   - The `codec` in output must be set to `json_lines` to ensure that each event is sent separately to QRadar.
   - If you want to send Kafka output to an existing Kafka server, see Configure the Kafka output (https://www.elastic.co/guide/en/beats/winlogbeat/7.7/kafka-output.html).

6. Ensure that Logstash is set up correctly by verifying that the `config` file for Logstash is working. Run the following command from the Logstash `bin` directory:

```
logstash --config.test_and_exit -f <path_to_config_file>
```

7. Ensure that Winlogbeat is configured correctly.
   a) Verify that the config file is working by running the following command from the `winlogbeat` directory:

```
./winlogbeat test config
```

   b) Verify that Winlogbeat can access the Logstash server by running the following command from the `winlogbeat` directory:

```
./winlogbeat test output
```

   If the output of the `./winlogbeat test output` command is successful, it might break any existing connection to Logstash. If the connection breaks, restart the Logstash service.

What to do next

Add a log source in QRadar and use the parameters that are listed in "Microsoft Windows Security Event Log log source parameters" on page 1221.

Microsoft Windows Security Event Log log source parameters

When you add a Microsoft Windows Security Event Log log source on the QRadar Console by using the Syslog protocol, there are specific parameters you must use.

The following table describes the parameters that require specific values to collect Syslog events from Microsoft Windows Security Event Log:

Table 803. Microsoft Windows Security Event Log Syslog log source parameters for the Microsoft Windows Security Event Log DSM	
Parameter	**Value**
Log Source type	Microsoft Windows Security Event Log
Protocol Configuration	Syslog
Log Source Identifier	The host ID of the logstash server.

For a complete list of Syslog protocol parameters and their values, see "Adding a log source" on page 5.

Configuring which usernames QRadar considers to be system users in events that are collected from Microsoft Windows Security Event Log

By default, all user names in Microsoft Windows Security Event Log events that end with a dollar sign ($) are considered as system users and are excluded from event parsing. If you want to change the way that IBM QRadar parses events, you can use the DSM Editor to include system users.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click **DSM Editor**.
3. From the **Select Log Source Type** window, select **Windows Security Event Log** from the list, and click **Select**.
4. On the **Configuration** tab, set **Display DSM Parameters Configuration** to on.
5. From the **Event Collector** list, select the event collector for the log source.
6. If you want usernames that end with a dollar sign ($) to *always* be considered as system users, set the **System User Criteria** parameter value to **Usernames Ending With A Dollar Sign Are Considered As System Users**.
7. If you want usernames that end with a dollar sign ($) as system users *only when they match with the computer name*, set the **System User Criteria** parameter value to **Usernames Ending With a Dollar Sign If It Matches Computer Name Are Considered As System Users**.

   Tip: A username is considered to match the computer name when the username (excluding the dollar sign) is equal to the computer name or, if the computer name is a fully-qualified domain name, the host component of the computer name. Letter case is ignored. For example, if the username is **HOST$** and the computer name is **host** or **host.example.com**, then the username is considered to match the computer name.
8. If you want usernames that end with a dollar sign ($) to *never* be considered as system users, set the **System User Criteria** parameter value to **Usernames Ending With a Dollar Sign Are Not Considered As System Users**.
9. Click **Save** and close out the DSM Editor.

   Tip: If the **Include System User With (No) Identity** parameter value is set to **Include System User With No Identity** or **Include System User With Identity**, all system users are included in parsing, regardless of the **System User Criteria** parameter value.

Configuring QRadar to parse the XML Level tag for application events that are collected from Microsoft Windows Security Event Log

By default, Microsoft Windows Security Event Log does not parse the level tag when it determines the QID for XML formatted application events. If you want to enable parsing of the Level tag for the Microsoft Windows Security Event Log DSM, use the DSM Editor to enable mapping.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click **DSM Editor**.
3. From the **Select Log Source Type** window, select **Microsoft Windows Security Event Log** from the list, and click **Select**.
4. On the **Configuration** tab, set **Display DSM Parameters Configuration** to **on**.
5. From the **Event Collector** list, select the event collector for the log source.
6. Set **Enable XML Tag For XML Application events** to **on**.
7. Click **Save** and close out the DSM Editor.

Microsoft Windows Security Event Log sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Microsoft Windows Security Event Log sample messages when you use WinCollect

The following sample has an event ID of 4624 that shows a successful login for the *<account_name>* user that has a source IP address of 10.0.0.1 and a destination IP of 10.0.0.2.

```
<13>May 08 10:45:44 microsoft.windows.test AgentDevice=WindowsLog
AgentLogFile=Security   PluginVersion=7.2.9.108 Source=Microsoft-Windows-Security-Auditing
Computer=microsoft.windows.test OriginatingComputer=10.0.0.2    User=   Domain=
EventID=4624    EventIDCode=4624    EventType=8 EventCategory=12544 RecordNumber=649155826
TimeGenerated=1588945541    TimeWritten=1588945541  Level=Log Always    Keywords=Audit Success
Task=SE_ADT_LOGON_LOGON Opcode=Info Message=An account was successfully logged on.
Subject:  Security ID:  NT AUTHORITY\SYSTEM  Account Name:  account_name$  Account Domain:
account_domain  Logon ID:  0x3E7  Logon Information:  Logon Type:  10  Restricted Admin
Mode: No  Virtual Account:  No  Elevated Token:  Yes  Impersonation Level:  Impersonation
New Logon:  Security ID:  account_domain\account_name  Account Name:  account_name  Account
Domain:  domain_name  Logon ID:  0x9A4D3C17  Linked Logon ID:  0x9A4D3CD6  Network Account
Name: -  Network Account Domain: -  Logon GUID:  {00000000-0000-0000-0000-000000000000}
Process Information:  Process ID:  0x3e4  Process Name:  C:\Windows\System32\svchost.exe
Network Information:  Workstation Name: workstation_name  Source Network Address: 10.0.0.1
Source Port:  0  Detailed Authentication Information:  Logon Process:  User32   Authentication
Package: Negotiate  Transited Services: -  Package Name (NTLM only): -  Key Length:  0  This
event is generated when a logon session is created. It is generated on the computer that was
accessed.  The subject fields indicate the account on the local system which requested the
logon. This is most commonly a service such as the Server service, or a local process such as
Winlogon.exe or Services.exe.  The logon type field indicates the kind of logon that occurred.
The most common types are 2 (interactive) and 3 (network).  The New Logon fields indicate
the account for whom the new logon was created, i.e. the account that was logged on.  The
network fields indicate where a remote logon request originated. Workstation name is not always
available and may be left blank in some cases.  The impersonation level field indicates the
extent to which a process in the logon session can impersonate.  The authentication information
fields provide detailed information about this specific logon request.  - Logon GUID is a
unique identifier that can be used to correlate this event with a KDC event.  - Transited
services indicate which intermediate services have participated in this logon request.  -
Package name indicates which sub-protocol was used among the NTLM protocols.  - Key length
indicates the length of the generated session key. This will be 0 if no session key was
requested.
```

The following sample has an event ID of 4624 that shows a successful login for the *<target_user_name>* user that has a source IP address of 10.0.0.1.

```
<13>May 08 14:54:03 microsoft.windows.test AgentDevice=NetApp
AgentLogFile=Security PluginVersion=7.2.9.108 Source=NetApp-Security-Auditing
Computer=00000000-0000-000000005-000000000000/11111111-1111-1111-1111-111111111111
OriginatingComputer=00000000-0000-0000-0000-000000000000/11111111-1111-1111-1111-111111111111
User= Domain= EventID=4624 EventIDCode=4624 EventType=8 EventCategory=0
RecordNumber=6706 TimeGenerated=1588960308 TimeWritten=1588960308 Level=LogAlways
Keywords=AuditSuccess Task=None Opcode=Info Message=IpAddress=10.0.0.1 IpPort=49155
TargetUserSID=S-0-0-00-00000000-0000000000-0000000000-0000 TargetUserName=target_user_name
TargetUserIsLocal=false TargetDomainName=target_domain_name AuthenticationPackageName=NTLM_V2
LogonType=3 ObjectType=(null) HandleID=(null) ObjectName=(null) AccessList=(null)
AccessMask=(null) DesiredAccess=(null) Attributes=(null)
```

Microsoft Windows Security Event Log sample message when you use Syslog to collect logs in Snare format

The following sample has an event ID of 4724 that shows that an attempt was made to reset an account's password, and that the attempt was made by the account name Administrator.

Important: The logs that you send to QRadar must be tab-delimited. If you cut and paste the code from this sample, make sure that you press the tab key where indicated by the *<tab>* variables, then remove the variables.

```
<133>Aug 15 23:12:08 microsoft.windows.test MSWinEventLog<tab>1<tab>Security<tab>839<tab>Wed
Aug 15 23:12:08 2012<tab>4724<tab>Microsoft-Windows-Security-Auditing<tab>user<tab>N/
A<tab>Success Audit<tab>w2k8<tab>User Account Management<tab>An attempt was made to reset
an account's password.    Subject:   Security ID:  subject_security_id   Account Name:
Administrator   Account Domain:  DOMAIN   Logon ID:  0x5cbdf    Target Account:   Security ID:
target_security_id   Account Name:  target_account_name   Account Domain:  DOMAIN  355
```

Microsoft Windows Security Event Log sample message when you use Syslog to collect logs in LEEF format

The following sample has an event ID of 8194 that shows that the event generated a Volume Shadow Copy Service error that was initiated by the *<user_name>* user.

```
<131>Apr 04 10:03:18 microsoft.windows.test LEEF:1.0|Microsoft|Windows|2k8r2|8194|
devTime=2019-04-04T10:03:18GMT+02:00  devTimeFormat=yyyy-MM-dd'T'HH:mm:ssz    cat=Error
sev=2   resource=microsoft.windows.test usrName=domain_name\user_name   application=Group
Policy Registry   message=domain_name\user_name: Application Group Policy Registry: [Error]
The client-side extension could not apply computer policy settings for '00 - C - Domain -
Baseline (Enforced) {00000000-0000-0000-0000-000000000000}' because it failed with error code
'0x80070002 The system cannot find the file specified.' See trace file for more details.
(EventID 8194)
```

Microsoft Windows Security Event Log sample message when you use Syslog to collect logs in CEF format

The following sample has an event ID of 7036 Service Stopped that shows that a service entered the stopped state.

```
CEF:0|Microsoft|Microsoft Windows||Service Control Manager:7036|Service entered
the stopped state|Low| eventId=132 externalId=7036 categorySignificance=/Normal
categoryBehavior=/Execute/Response categoryDeviceGroup=/Operating System catdt=Operating System
categoryOutcome=/Success categoryObject=/Host/Application/Service art=1358378879917 cat=System
deviceSeverity=Information act=stopped rt=1358379018000 destinationServiceName=Portable
Device Enumerator Service cs2=0 cs3=Service Control Manager cs2Label=EventlogCategory
cs3Label=EventSource cs4Label=Reason or Error Code ahost=192.168.0.31 agt=192.168.0.31
agentZoneURI=/All Zones/example System/Private Address Space Zones/RFC1918:
192.168.0.0-192.168.255.255 av=5.2.5.6395.0 atz=Country/City_Name aid=00000000000000000000000\
\=\\= at=windowsfg dvchost=host.domain.test dtz=Country/City_Name _cefVer=0.1
ad.Key[0]=Portable Device Enumerator Service ad.Key[1]=stopped ad.User=
ad.ComputerName=host.domain.test ad.DetectTime=2013-1-16 15:30:18 ad.EventS
```

Microsoft Windows Security Event Log sample message when you use Syslog to collect logs by using Winlogbeats

The following sample has an event ID of System that shows that NtpClient was unable to set a manual peer to use as a time source.

```
{"@timestamp":"2017-02-13T01:54:07.745Z","beat":
{"hostname":"microsoft.windows.test","name":"microsoft.windows.test","version":"5.6.3"},"compute
r_name":"microsoft.windows.test","event_data":
{"DomainPeer":"time.windows.test,0x9","ErrorMessage":"No such host is known.
(0x80072AF9)","RetryMinutes":"15"},"event_id":134,"level":"Warning","log_name":"System","message
":"NtpClient was unable to set a manual peer to use as a time source because of DNS resolution
error on 'time.windows.test,0x9'. NtpClient will try again in 15 minutes and double the
reattempt interval thereafter. The error was: No such host is known.
(0x80072AF9)","opcode":"Info","process_id":996,"provider_guid":"{00000000-0000-0000-0000-0000000
00000}","record_number":"40292","source_name":"Microsoft-Windows-Time-
Service","thread_id":3312,"type":"wineventlog","user":{"domain":"NT
AUTHORITY","identifier":"user_identifier","name":"LOCAL SERVICE","type":"Well Known Group"}}
```

Microsoft Windows Security Event Log sample message when you use Syslog to collect logs by using Azure Event Hubs

The following sample has an event ID of 5061 that shows that there was a cryptographic operation that is completed by the *<subject_user_name>* user.

```
{"time":"2019-05-07T17:53:30.0648172Z","category":"WindowsEventLogsTable","level":"Informational
","properties":
{"DeploymentId":"00000000-0000-0000-0000-000000000000","Role":"IaaS","RoleInstance":"_role_insta
nce","ProviderGuid":"{00000000-0000-0000-0000-000000000000}","ProviderName":"Microsoft-Windows-
Security-
Auditing","EventId":5061,"Level":0,"Pid":700,"Tid":1176,"Opcode":0,"Task":12290,"Channel":"Secur
ity","Description":"Cryptographic operation.\r\n\r\nSubject:\r\n\tSecurity
ID:\t\tsecurity_id\r\n\tAccount Name:\t\taccount_name\r\n\tAccount
Domain:\t\tWORKGROUP\r\n\tLogon ID:\t\t0x3E7\r\n\r\nCryptographic Parameters:\r\n\tProvider
Name:\tMicrosoft Software Key Storage Provider\r\n\tAlgorithm Name:\tRSA\r\n\tKey
Name:\t{11111111-1111-1111-1111-111111111111}\r\n\tKey Type:\tMachine key.\r\n\r\nCryptographic
Operation:\r\n\tOperation:\tOpen Key.\r\n\tReturn Code:\t0x0","RawXml":"<Event xmlns='http://
schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-
Security-Auditing' Guid='{22222222-2222-2222-2222-222222222222}'/><EventID>5061</
EventID><Version>0</Version><Level>0</Level><Task>12290</Task><Opcode>0</
Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated
SystemTime='2019-05-07T17:53:30.064817200Z'/><EventRecordID>291478</EventRecordID><Correlation
ActivityID='{33333333-3333-3333-3333-333333333333}'/><Execution ProcessID='700' ThreadID='1176'/
><Channel>Security</Channel><Computer>computer_name</Computer><Security/></
System><EventData><Data Name='SubjectUserSid'>subject_user_sid</Data><Data
Name='SubjectUserName'>subject_user_name</Data><Data Name='SubjectDomainName'>WORKGROUP</
Data><Data Name='SubjectLogonId'>0x3e7</Data><Data Name='ProviderName'>Microsoft Software Key
Storage Provider</Data><Data Name='AlgorithmName'>RSA</Data><Data
Name='KeyName'>{44444444-4444-4444-4444-444444444444}</Data><Data Name='KeyType'>%%2499</
Data><Data Name='Operation'>%%2480</Data><Data Name='ReturnCode'>0x0</Data></EventData></
Event>"}}
```

Chapter 100. Motorola Symbol AP

The Motorola Symbol AP DSM for IBM QRadar records all relevant events forwarded from Motorola Symbol AP devices using syslog.

Syslog log source parameters for Motorola SymbolAP

If QRadar does not automatically detect the log source, add a Motorola SymbolAP log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Motorola SymbolAP:

Table 804. Syslog log source parameters for the Motorola SymbolAP DSM

Parameter	Value
Log Source type	Motorola SymbolAP
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name for the log source as an identifier for events from your Motorola SymbolAP appliance.

Related tasks

Adding a log source

Configure syslog events for Motorola Symbol AP

You can configure the device to forward syslog events to IBM QRadar.

Procedure

1. Log in to your Symbol AP device user interface.
2. From the menu, select **System Configuration > Logging Configuration**.

   The Access Point window is displayed.
3. Using the **Logging Level** list, select the desired log level for tracking system events. The options are:

   0 - Emergency

   1- Alert

   2 - Critical

   3 - Errors

   4 - Warning

   5 - Notice

   6 - Info. This is the default.

   7 - Debug
4. Select the Enable logging to an external syslog server check box.
5. In the **Syslog Server IP Address** field, type the IP address of an external syslog server, such as QRadar.

This is required to route the syslog events to QRadar.

6. Click **Apply**.
7. Click **Logout**.

   A confirmation window is displayed.
8. Click **OK** to exit the application.

   The configuration is complete. Events forwarded to QRadar are displayed on the **Log Activity** tab.

Chapter 101. Name Value Pair

The Name Value Pair DSM gives you the option to integrate IBM QRadar with devices that might not normally send syslog logs.

The Name Value Pair DSM provides a log format that gives you the option to send logs to QRadar. For example, for a device that does not export logs natively with syslog, you can create a script to export the logs from a device that QRadar does not support, format the logs in the Name Value Pair log format, and send the logs to QRadar using syslog.

The Name Value Pair DSM log source that is configured in QRadar then receives the logs and is able to parse the data since the logs are received in the Name Value Pair log format.

Tip: Events for the Name Value Pair DSM are not automatically discovered by QRadar.

The Name Value Pair DSM accepts events by using syslog. QRadar records all relevant events. The log format for the Name Value Pair DSM must be a tab-separated single-line list of `Name=Parameter`. The Name Value Pair DSM does not require a valid syslog header.

Note: The Name Value Pair DSM assumes an ability to create custom scripts or thorough knowledge of your device capabilities to send logs to QRadar using syslog in Name Value Pair format.

The Name Value Pair DSM is able to parse the following tags:

Table 805. Name Value Pair log format tags

Tag	Description
DeviceType	Type `NVP` as the **DeviceType**. This identifies the log formats as a Name Value Pair log message. This is a required parameter and `DeviceType=NVP` must be the first pair in the list.
EventName	Type the event name that you want to use to identity the event in the Events interface when using the Event Mapping functions. For more information on mapping events, see the *IBM QRadar User Guide*. This is a required parameter.
EventCategory	Type the event category that you want to use to identify the event in the Events interface. If this value is not included in the log message, the value `NameValuePair` value is used.
SourceIp	Type the source IP address for the message.
SourcePort	Type the source port for the message.
SourceIpPreNAT	Type the source IP address for the message before Network Address Translation (NAT) occurred.
SourceIpPostNAT	Type the source IP address for the message after NAT occurs.
SourceMAC	Type the source MAC address for the message.
SourcePortPreNAT	Type the source port for the message before NAT occurs.

Table 805. Name Value Pair log format tags (continued)	
Tag	**Description**
SourcePortPostNAT	Type the source port for the message after NAT occurs.
DestinationIp	Type the destination IP address for the message.
DestinationPort	Type the destination port for the message.
DestinationIpPreNAT	Type the destination IP address for the message before NAT occurs.
DestinationIpPostNAT	Type the IP address for the message after NAT occurs.
DestinationPortPreNAT	Type the destination port for the message before NAT occurs.
DestinationPortPostNAT	Type the destination port for the message after NAT occurs.
DestinationMAC	Type the destination MAC address for the message.
DeviceTime	Type the time that the event was sent, according to the device. The format is: YY/MM/DD hh:mm:ss. If no specific time is provided, the syslog header or **DeviceType** parameter is applied.
UserName	Type the user name that is associated with the event.
HostName	Type the host name that is associated with the event. Typically, this parameter is only associated with identity events.
GroupName	Type the group name that is associated with the event. Typically, this parameter is only associated with identity events.
NetBIOSName	Type the NetBIOS name that is associated with the event. Typically, this parameter is only associated with identity events.
Identity	Type TRUE or FALSE to indicate whether you want this event to generate an identity event. An identity event is generated if the log message contains the **SourceIp** (if the **IdentityUseSrcIp** parameter is set to TRUE) or **DestinationIp** (if the **IdentityUseSrcIp** parameter is set to FALSE) and one of the following parameters: **UserName**, **SourceMAC**, **HostName**, **NetBIOSName**, or **GroupName**.
IdentityUseSrcIp	Type TRUE or FALSE (default). TRUE indicates that you want to use the source IP address for identity. FALSE indicates that you want to use the destination IP address for identity. This parameter is used only if the Identity parameter is set to TRUE.

Use these sample event messages to verify a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Example 1

The following example parses all fields:

```
DeviceType=NVP EventName=Test
DestinationIpPostNAT=<IP_address>
DeviceTime=2007/12/14 09:53:49
SourcePort=1111 Identity=FALSE SourcePortPostNAT=3333
DestinationPortPostNAT=6666 HostName=testhost
DestinationIpPreNAT=<IP_address> SourcePortPreNAT=2222
DestinationPortPreNAT=5555 SourceMAC=<MAC_address>
SourceIp=<IP_address> SourceIpPostNAT=<IP_address>
NetBIOSName=<BIOS_name> DestinationMAC=<MAC_address>
EventCategory=Accept DestinationPort=4444
GroupName=testgroup SourceIpPreNAT=<IP_address>
UserName=<Username> DestinationIp=<IP_address>
```

```
DeviceType=NVP EventName=Test DestinationIpPostNAT=<IP_address> DeviceTime=2007/12/14
09:53:49 SourcePort=1111 Identity=FALSE SourcePortPostNAT=3333
DestinationPortPostNAT=6666 HostName=testhost DestinationIpPreNAT=<IP_address>
SourcePortPreNAT=2222 DestinationPortPreNAT=5555 SourceMAC=<MAC_address> SourceIp=<IP_address>
SourceIpPostNAT=<IP_address> NetBIOSName=<BIOS_name> DestinationMAC=<MAC_address>
EventCategory=Accept DestinationPort=4444 GroupName=testgroup SourceIpPreNAT=<IP_address>
UserName=<Username> DestinationIp=<IP_address>
```

Example 2

The following example provides identity by using the destination IP address:

```
<133>Apr 16 12:41:00 192.0.2.1 namevaluepair:
DeviceType=NVP EventName=Test EventCategory=Accept
Identity=TRUE SourceMAC=<MAC_address>
SourceIp=<Source_IP_address> DestinationIp=<Destination_IP_address>
UserName=<Username>
```

```
<133>Apr 16 12:41:00 192.0.2.1 namevaluepair: DeviceType=NVP EventName=Test
EventCategory=Accept Identity=TRUE SourceMAC=<MAC_address> SourceIp=<Source_IP_address>
DestinationIp=<Destination_IP_address> UserName=<Username>
```

Example 3

The following example provides identity by using the source IP address:

```
DeviceType=NVP EventName=Test
EventCategory=Accept DeviceTime=2007/12/14 09:53:49
SourcePort=5014 Identity=TRUE IdentityUseSrcIp=TRUE
SourceMAC=<MAC_address> SourceIp=<Source_IP_address>
DestinationIp=<Destination_IP_address>
DestinationMAC=<MAC_address> UserName=<Username>
```

```
DeviceType=NVP EventName=Test EventCategory=Accept DeviceTime=2007/12/14
09:53:49 SourcePort=5014 Identity=TRUE IdentityUseSrcIp=TRUE
SourceMAC=<MAC_address> SourceIp=<Source_IP_address> DestinationIp=<Destination_IP_address>
DestinationMAC=<MAC_address> UserName=<Username>
```

Example 4

The following example provides an entry with no identity:

```
DeviceType=NVP EventName=Test
EventCategory=Accept DeviceTime=2007/12/14 09:53:49
SourcePort=5014 Identity=FALSE
SourceMAC=<MAC_address>
SourceIp=<Source_IP_address>
DestinationIp=<Destination_IP_address>
DestinationMAC=<MAC_address>
UserName=<Username>
```

```
DeviceType=NVP EventName=Test
EventCategory=Accept DeviceTime=2007/12/14 09:53:49
SourcePort=5014 Identity=FALSE
SourceMAC=<MAC_address>
SourceIp=<Source_IP_address>
DestinationIp=<Destination_IP_address>
```

```
DestinationMAC=<MAC_address>
UserName=<Username>
```

Chapter 102. NCC Group DDoS Secure

The IBM QRadar DSM for NCC Group DDoS Secure collects events from NCC Group DDoS Secure devices.

The following table describes the specifications for the NCC Group DDoS Secure DSM:

Table 806. NCC Group DDoS Secure DSM specifications

Specification	**Value**
Manufacturer	NCC Group
DSM name	NCC Group DDoS Secure
RPM file name	`DSM-NCCGroupDDoSSecure-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	5.13.1-2s to 5.16.1-0
Protocol	Syslog
Event format	LEEF
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	NCC Group website (https://www.nccgroup.trust/uk/)

To integrate NCC Group DDoS Secure with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - NCC Group DDoS Secure DSM RPM
2. Configure your NCC Group DDoS Secure device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an NCC Group DDoS Secure log source on the QRadar Console. The following table describes the parameters that require specific values to collect event from NCC Group DDoS Secure:

   Table 807. NCC Group DDoS Secure log source parameters

Parameter	**Value**
Log Source type	NCC Group DDoS Secure
Protocol Configuration	Syslog

4. To verify that QRadar is configured correctly, review the following table to see an example of a normalized event message.

   The following table shows a sample event message from NCC Group DDoS Secure:

   Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Table 808. NCC Group DDoS Secure sample message

Event name	Low level category	Sample log message
TCP Attack - Port Scan - END	Host Port Scan	<134>LEEF:1.0|NCCGroup|DDoS Secure |5.16.2-1|4078|desc=TCP Attack - Port Scan sev=4 myip=<IP_address proto=TCP scrPort =0 dstPort=0 src=<Source_IP_address> dst=<Destination_IP_address> cat= END devTime=2017-06-05 11: 26:00 devTimeFormat=yyyy-MM -dd HH:mm:ss end=2017-06-05 11:34:33 CurrentPps=0 PeakPps=14 totalPackets=243 realm=<Domain> action=DROP <134>LEEF:1.0|NCCGroup|DDoS Secure| 5.16.2-1|4078|desc=TCP Attack - Port Scan sev=4 myip=<IP_address proto=TCP scrPort=0 dstPort=0 src=<Source_IP_address> dst=<Destination_IP_address> cat=END devTime=2017-06-05 11:26:00 devTimeFormat=yyyy-MM- dd HH:mm:ss end=2017-06-05 11:34:33 CurrentPps=0 PeakPps=14 totalPackets=243 realm=<Domain> action=DROP

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring NCC Group DDoS Secure to communicate with QRadar

The NCC Group DDoS Secure DSM for IBM QRadar receives events from NCC Group DDoS Secure devices by using syslog in Log Event Extended Format (LEEF) format. QRadar records all relevant status and network condition events.

Procedure

1. Log in to NCC Group DDoS Secure.
2. Go to the **Structured Syslog Server** window.
3. In the **Server IP Address(es)** field, type the IP address of the QRadar Console.
4. From the **Format** list, select **LEEF**.
5. Optional: If you do not want to use the default of `local0` in the **Facility** field, type a syslog facility value.
6. From the **Priority** list, select the syslog priority level that you want to include. Events that meet or exceed the syslog priority level that you select are forwarded to QRadar.
7. In the **Log Refresh (Secs)** field, specify a refresh update time for structured logs. The refresh update time is specified in seconds.
8. In the **Normal Peak Bandwith** field, specify the expected normal peak bandwidth of the appliance.

Chapter 103. NetApp Data ONTAP

IBM QRadar accepts events from a Windows host by using the WinCollect NetApp Data ONTAP plug-in.

For more information about NetApp Data ONTAP source parameters in WinCollect 10, see Netapp Data ONTAP source.

For more information about configuring the WinCollect 7 plug-in for NetApp ONTAP, see NetApp Data ONTAP configuration options.

Chapter 104. Netgate pfSense

The IBM QRadar DSM for Netgate pfSense collects syslog events from a pfSense device.

To integrate Netgate pfSense with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Netgate pfSense DSM RPM
   - Linux DHCP DSM RPM (only if DHCP event logging is enabled)
   - Sourcefire Snort DSM RPM (only if the Snort package for Netgate pfSense is installed and event logging is enabled)

     Suricata events are not officially supported by the Sourcefire Snort DSM. However, they might be parsed by the Snort DSM.
2. Configure your Netgate pfSense device to send events to QRadar. For more information, see Configuring Netgate pfSense to communicate with QRadar.

   If you send Snort or Suricata events to QRadar, and the log source is not automatically detected, add a Snort log source on the QRadar Console For more information, see Syslog log source parameters for Open Source SNORT.
3. If QRadar does not automatically detect the log source, add a Netgate pfSense Syslog log source on the QRadar Console. For more information, see Syslog log source parameters for Netgate pfSense.

   If you send Snort or Suricata events to QRadar and QRadar does not automatically detect the log source, add a Snort log source on the QRadar Console For more information, see Syslog log source parameters for Open Source SNORT.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Netgate pfSense DSM specifications

When you configure Netgate pfSense, understanding the specifications for the Netgate pfSense DSM can help ensure a successful integration. For example, knowing what the supported version of Netgate pfSense is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Netgate pfSense DSM.

Table 809. Netgate pfSense DSM specifications

Specification	Value
Manufacturer	Netgate
DSM name	Netgate pfSense
RPM file name	`DSM-NetgatePfSense-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported version	2.4.4
Protocol	Syslog
Event format	CSV, Syslog

Table 809. Netgate pfSense DSM specifications (continued)	
Specification	**Value**
Recorded event types	System Firewall DNS DHCP (when you use the Linux DHCP DSM)
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	pfSense website (https://www.pfsense.org) pfSense documentation (https://docs.netgate.com/pfsense/en/latest/)

Configuring Netgate pfSense to communicate with QRadar

To send syslog messages to IBM QRadar, the Netgate pfSense remote logging options must be configured to specify a remote log server.

Before you begin

If you want to send Snort IDS events to QRadar, ensure that the Snort package for Netgate pfSense is installed and configured. Snort is an open source network intrusion detection and prevention system.

Procedure

1. Log in to your Netgate pfSense device.
2. Configure remote logging options for Netgate pfSense.
   a) Select **Status** > **System Logs**.
   b) Click the **Settings** tab and then go to the **Remote Logging Options** section.
   c) Select a **Source Address**, or use the default.
   d) Select an **IP Protocol** or use the default.
   e) In the **Remote log servers** options section, enable **System Events**, **Firewall Events**, **DNS Events**, and **DHCP Events**.

Important: If the **System Events** logging option is enabled, **Unknown** or **Stored** events might occur because extra services that are installed by packages for Netgate pfSense can output log messages to the system log. Due to the large number of packages available for Netgate pfSense, the DSM was developed to support the base installation of the device. The DSM Editor can be used in this case to create custom parsing for any **Unknown** or **Stored** events that result from user installed packages. For more information about the DSM Editor, see the *IBM QRadar Administration Guide*.

Important: If DHCP events are enabled, you must create a Linux DHCP log source in QRadar to normalize the DHCP events. The Linux DHCP log source must be placed after Netgate pfSense log source in the parsing order. For more information, see Syslog log source parameters for Linux DHCP and Adding a log source parsing order.

Important: If you send Snort or Suricata events to QRadar and the log source is not automatically detected, add a Snort log source on the QRadar Console For more information, see Syslog log source parameters for Open Source SNORT.

Important: For DNS logs to be properly send to QRadar, complete the following steps. These steps apply only for the Unbound DNS Resolver, the default DNS service configured on Netgate pfSense. If you're running BIND instead of Unbound, these steps do not apply.

a. Go to **Services** > **DNS Resolver**.

b. On the General Settings tab, scroll down to Custom Options.

c. Add the following lines in custom options.

```
server:
     log-replies:yes
```

d. Click **Save**.

e. To confirm that Netgate pfSense is generating DNS logs, go to **Status** > **System logs**.

3. Optional: Configure the Snort service to output logs to the Netgate pfSense system log.

a) Select **Service** > **Snort**.

b) On the **Snort Interface** tab, click **Edit this Snort interface mapping** (pencil icon).

c) In the **Alert Settings** section, enable **Send Alerts to System Log**.

d) Click **Save**.

e) On the **Snort Interface** tab, click **Restart Snort on this interface**.

Syslog log source parameters for Netgate pfSense

If QRadar does not automatically detect the log source, add a Netgate pfSense log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Netgate pfSense:

Table 810. Syslog log source parameters for the Netgate pfSense DSM

Parameter	Value
Log Source type	Netgate pfSense
Protocol Configuration	Syslog

For a list of common protocol parameters and their values, see Adding a log source..

Related tasks

Adding a log source

Netgate pfSense sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Netgate pfSense sample message when you use the Syslog protocol: name server DNS query

The following sample event message shows that the event indicates that a name server DNS query was made.

<30>Mar 17 00:35:02 unbound: [33068:6] info: **192.168.1.222** hostname.test. **NS** IN

```
<30>Mar 17 00:35:02 unbound: [33068:6] info: 192.168.1.222 hostname.test. NS IN
```

Table 811. Highlighted fields in the Netgate pfSense sample event	
QRadar field name	**Highlighted payload field name**
Event Name	**NS**
Source IP	**192.168.1.222**

Netgate pfSense sample message when you use the Syslog protocol: firewall permit event

The following sample event message shows a firewall permit event.

<134>Mar 10 08:43:23 filterlog: 100,,,1581299744,hn0,match,**pass**,out,4,0x0,,127,46462,0,DF,**6**,
tcp,52,**192.168.0.10**,**192.168.2.3**,**10945**,**443**,0,S,1283715954,,64240,,mss;nop;wscale;
nop;nop;sackOK

<134>Mar 10 08:43:23 filterlog:
100,,,1581299744,hn0,match,**pass**,out,4,0x0,,127,46462,0,DF,**6**,tcp,52,**192.168.0.10**,**192.168.2.3**,**1094
5**,**443**,0,S,1283715954,,64240,,mss;nop;wscale;nop;nop;sackOK

Table 812. Highlighted fields in the Netgate pfSense sample event	
QRadar field name	**Highlighted payload field name**
Event Name	**pass**
Protocol	**6** (TCP)
Source IP	**192.168.0.10**
Destination IP	**192.168.2.3**
Source Port	**10945**
Destination Port	**443**

Chapter 105. Netskope Active

The IBM QRadar DSM for Netskope Active collects events from your Netskope Active servers.

Important: The IBM QRadar DSM for Netskope Active is deprecated.

To continue taking advantage of this integration, please download the Netskope Security Cloud DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/ff97aaadc10ed96b0e05d1a1f24af2f7).

The following table identifies the specifications for the Netskope Active DSM:

Table 813. Netskope Active DSM specifications

Specification	**Value**
Manufacturer	Netskope
DSM name	Netskope Active
RPM file name	DSM-NetskopeActive-*Qradar_version-build_number*.noarch.rpm
Protocol	Netskope Active REST API
Recorded event types	Alert, All
Automatically discovered?	No
Includes identity?	Yes
More information	Netskope Active website (www.netskope.com)

To integrate Netskope Active DSM with QRadar complete the following steps:

Note: If multiple DSM RPMs are required, the integration sequence must reflect the DSM RPM dependency.

1. If automatic updates are not enabled, download and install the most recent version of the following DSMs from the IBM Support Website onto your QRadar Console.
   - Netskope Active DSM RPM
   - Netskope Active REST API Protocol RPM
   - PROTOCOL-Common RPM
2. Configure the required parameters, and use the following table for the Netskope Active log source specific parameters:

   Table 814. Netskope Active log source parameters

Parameter	**Value**
Log Source type	Netskope Active
Protocol Configuration	Netskope Active REST API

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Netskope Active REST API log source parameters for Netskope Active

If QRadar does not automatically detect the log source, add a Netskope Active log source on the QRadar Console by using the Netskope Active REST API protocol.

Important: The IBM QRadar DSM for Netskope Active is deprecated.

To continue taking advantage of this integration, please download the Netskope Security Cloud DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/ff97aaadc10ed96b0e05d1a1f24af2f7).

When using the Netskope Active REST API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Netskope Active REST API events from Netskope Active:

Table 815. Netskope Active REST API log source parameters for the Netskope Active DSM

Parameter	Value
Log Source type	Netskope Active
Protocol Configuration	Netskope Active REST API
IP or Hostname	`<customer_tenant_name>.goskope.com`
Authentication Token	The authentication token is generated in the Netskope WebUI and is the only credential that is required for **Netskope Active REST API** usage. To access the token generation option in the Netskope WebUI, select **Settings** > **REST API**.
Automatically Acquire Server Certificates	If you choose **Yes** from the list, QRadar automatically downloads the certificate and begins trusting the target server. The correct server must be entered in the **IP or Hostname** field.
Throttle	The maximum number of events per second. The default is 5000.
Recurrence	You can specify when the log source attempts to obtain data. The format is M/H/D for Minutes/Hours/Days. The default is 1 M.
Collection Type	**All Events** Select to collect all events. **Alerts Only** Select to collect only alerts.

Related tasks

Adding a log source

Netskope Active sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: The IBM QRadar DSM for Netskope Active is deprecated.

To continue taking advantage of this integration, please download the Netskope Security Cloud DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/ff97aaadc10ed96b0e05d1a1f24af2f7).

Netskope Active sample messages when you use the Netskope Rest API protocol

Tip: Due to formatting, paste the message formats into a text editor and then remove any carriage return or line feed characters.

Sample 1: The following sample event message shows an anomaly collaboration event.

```
{"dstip":"XXXXX","dst_location":"XXXXX","last_timestamp":1436237104,"latency_total":74,"app"
:"Google Hangouts","profile_id":"XXXX","last_country":"XX","device":"Windows
Device","src_location":"N/A"
,"alert_type":"anomaly","id":66483,"app_session_id":XXXXX,"event_type":"proximity","risk_level":
"high","client_bytes":3109,"last_location":XXXX],"dst_region":"XXX","last_device":"Windows
Device","conn_durat
ion":XXX,"dst_country":"XXX","resp_cnt":3,"ccl":"high","src_zipcode":"N/
A","req_cnt":3,"src_timezone":
"unknown","server_bytes":2012,"type":"connection","access_method":"Client","latency_min":24,
"organization_unit":"","dst_latitude":XXXX,"timestamp":1436237457,"src_region":"N/
A","src_latitude":XX,
"connection_id":XXX,"dst_longitude":-XXX,"alert":"yes","app_action_cnt":0,"last_app":"Google
Hangouts","user"
:"XXX","src_longitude":-
XX,"srcip":"XXXXX","src_country":"XX","last_region":"CO","appcategory":"Collaboration
","conn_endtime":1436237457,"count":1,"acked":"false","_id":"XXXX","dst_zipcode":"XXX","risk
_level_id":2,"sv":"unknown","latency_max":25,"numbytes":5121,"alert_name":"proximity","conn_
starttime":1436237210,"userip":"XXXX","telemetry_app":"","browser":"Chrome","os":"Windows 8.1"}
```

Sample 2: The following sample event message shows a successful user login audit event.

```
{"supporting_data":{"data_values":["XXX","XXXX],"data_type":"user"},"severity_level":2,"time
stamp":1419922155,"organization_unit":"","ccl":"unknown","user":"XXXXXX","audit_log_event":"Logi
n Succes
sful","_id":"XXXXXX","type":"admin_audit_logs","appcategory":"n/a"}
```

Chapter 106. NGINX HTTP Server

The IBM QRadar DSM for NGINX HTTP Server collects Syslog events from an NGINX HTTP Server device.

To integrate NGINX HTTP Server with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Apache HTTP Server DSM RPM
   - NGINX HTTP Server DSM RPM
2. Configure your NGINX HTTP Server device to send events to QRadar.
3. If QRadar does not automatically detect the log source, add an NGINX HTTP Server log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from NGINX HTTP Server:

Table 816. NGINX HTTP Server Syslog log source parameters

Parameter	Value
Log Source type	NGINX HTTP Server
Protocol Configuration	Syslog
Log Source Identifier	The IPv4 address or host name that identifies the log source. If your network contains multiple devices that are attached to a single management console, specify the IP address of the individual device that created the event. A unique identifier, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

NGINX HTTP Server DSM specifications

The following table describes the specifications for the NGINX HTTP Server DSM.

Table 817. NGINX HTTP Server DSM specifications

Specification	Value
Manufacturer	NGINX
DSM name	NGINX HTTP Server
RPM file name	DSM-*NginxWebserver-QRadar_version-build_number*.noarch.rpm
Supported versions	1.15.5
Protocol	Syslog
Event format	LEEF, Standard syslog
Recorded event types	Error log, Access log

Table 817. NGINX HTTP Server DSM specifications (continued)	
Specification	**Value**
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	NGINX HTTP Server product information (https://nginx.com)

Configuring NGINX HTTP Server to communicate with QRadar

To collect events from NGINX HTTP Server, configure your NGINX HTTP Server device to forward Syslog events to QRadar.

Procedure

1. Log in to your NGINX HTTP Server device.
2. Open the `nginx.conf` file.
3. Add the following LEEF format string under `http block`. For more information about configuring logging, see https://docs.nginx.com/nginx/admin-guide/monitoring/logging/.

```
LEEF:1.0|NGINX|NGINX|$nginx_version|$status|devTime=$time_local\tdevTimeFormat=dd/MMM/
yyyy:HH:mm:ss
Z\tsrc=$remote_addr\tdst=$server_addr\tdstPort=$server_port\tproto=$server_protocol\tusrName=
$remote_user\trequest=$request\tbody_bytes_sent=$body_bytes_sent\thttp_referer=$http_referer\
thttp_true_client_ip=$http_true_client_ip\thttp_user_agent=$http_user_agent\thttp_x_header=$h
ttp_x_header\thttp_x_forwarded_for=$http_x_forwarded_for\trequest_time=$request_time\tupstrea
m_response_time=$upstream_response_time\tpipe=$pipe\turi_query=$query_string\turi_path=$uri\t
cookie=$http_cookie
```

4. Add the following syslog server configuration under `http block`.

```
access_log syslog:server=QRadar_Server_IP:514,facility=Facility_Parameter qradar;
```

5. Save the configuration.
6. To verify the configuration, type the following command:

```
nginx -t
```

7. If NGINX is running, reload the configuration by typing the following command:

```
nginx -s reload
```

NGINX HTTP Server sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides sample event messages when you use the Syslog protocol for the NGINX HTTP Server DSM:

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Table 818. NGINX HTTP Server sample message supported by NGINX HTTP Server.

Event name	Low-level category	Sample log message
404	System Status	LEEF:1.0|NGINX|NGINX|1.15.5|404|devTime= 29/Oct/2018:15:36:58 -0300 src=127.0.0.1 dst=127.0.0.1 dstPort=80 proto=HTTP/1.1 usrName=- request=GET /nginx_status HTTP/1.1 body_bytes_sent=153 http_referer=- http_true _client_ip=- http_user_agent=curl/7.29.0 htt p_x_header=- http_x_forwarded_for=- request_ time=0.000 upstream_response_time=- pipe =. uri_query=- uri_path=/nginx_status cookie=- LEEF:1.0|NGINX|NGINX|1.15.5|404|devTime=29/Oct/ 2018:15:36:58 -0300 src=127.0.0.1 dst=127.0.0.1 dstPort=80 proto=HTTP/1.1 usrName=- request=GET /nginx_status HTTP/1.1 body_bytes_sent=153 http_referer=- http_true_client_ip=- http_user_agent=curl/7.29.0 http_x_header=- http_x_forwarded_for=- request_time=0.000 upstream_response_time=- pipe=. uri_query=- uri_path=/nginx_status cookie=-
Connection refused	Firewall Deny	<187>Sep 19 07:46:27 company3-hst ng inx: 2018/09/19 07:46:27 [error] 24881#24881 : *416 connect() failed (111: Connection ref used) while connecting to upstream, client: 198.51.100.111, server: ute-hst.company.com , request: "POST /api/v1/view/bill HTTP/1.1" , upstream: "http://198.51.100.225:9000/v1/ view/bill", host: "198.51.100.25:8080", ref errer: "https://www.hst.company.com/web/totes/" <187>Sep 19 07:46:27 company3-hst ng inx: 2018/09/19 07:46:27 [error] 24881#24881 : *416 connect() failed (111: Connection ref used) while connecting to upstream, client: 198.51.100.111, server: ute-hst.company.com , request: "POST /api/v1/view/bill HTTP/1.1" , upstream: "http://198.51.100.225:9000/v1/ view/bill", host: "198.51.100.25:8080", ref errer: "https://www.hst.company.com/web/totes/"

Chapter 107. Niksun

The Niksun DSM for IBM QRadar records all relevant Niksun events by using the syslog protocol.

You can integrate NetDetector/NetVCR2005, version 3.2.1sp1_2 with QRadar. Before you configure QRadar to integrate with a Niksun device, you must configure a log source and then enable syslog forwarding on your Niksun appliance. For more information about configuring Niksun, see your *Niksun appliance documentation*.

Syslog log source parameters for Niksun

If QRadar does not automatically detect the log source, add a Niksun log source on the QRadar Console by using the syslog protocol.

The following table describes the parameters that require specific values to collect syslog events from Niksun:

Table 819. Syslog log source parameters for the Niksun DSM

Parameter	Value
Log Source type	Niksun 2005 v3.5
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Niksun appliance.

Related tasks

Adding a log source

Chapter 108. Nokia Firewall

The Check Point Firewall-1 DSM allows IBM QRadar to accept Check Point-based Firewall events sent from Nokia Firewall appliances by using syslog or OPSEC protocols.

Integration with a Nokia Firewall by using syslog

This method gives you the option to configure your Nokia Firewall to accept Check Point syslog events that are forwarded from your Nokia Firewall appliance.

To configure IBM QRadar to integrate with a Nokia Firewall device, take the following steps:

1. Configure iptables on yourQRadar Console or Event Collector to receive syslog events from Nokia Firewall.
2. Configure your Nokia Firewall to forward syslog event data.
3. Configure the events that are logged by the Nokia Firewall.
4. Optional. Configure a log source in QRadar.

Configuring IPtables

Nokia Firewalls require a TCP reset (`rst`) or a TCP acknowledge (`ack`) from IBM QRadar on port 256 before they forward syslog events.

About this task

The Nokia Firewall TCP request is an online status request that is designed to ensure that QRadar is online and able to receive syslog events. If a valid reset or acknowledge is received from QRadar, then Nokia Firewall begins forwarding events to QRadar on UDP port 514. By default, QRadar does not respond to any online status requests from TCP port 256.

You must configure IPtables on your QRadar Console or any Event Collector that receives Check Point events from a Nokia Firewall to respond to an online status request.

Procedure

1. Using SSH, log in to QRadar as the root user.

   Login: `root`

   Password: <*password*>
2. Type the following command to edit the IPtables file:

   ```
   vi /opt/qradar/conf/iptables.pre
   ```

   The IPtables configuration file is displayed.
3. Type the following command to instruct QRadar to respond to your Nokia Firewall with a TCP reset on port 256:

   ```
   -A INPUT -s <IP address> -p tcp --dport 256 -j REJECT --reject-with tcp-reset
   ```

   Where <*IP address*> is the IP address of your Nokia Firewall. You must include a TCP reset for each Nokia Firewall IP address that sends events to your QRadar Console or Event Collector, for example,

   - -A INPUT -s <IP_address1>/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset
   - -A INPUT -s <IP_address2>/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset
   - -A INPUT -s <IP_address3>/32 -p tcp --dport 256 -j REJECT --reject-with tcp-reset
4. Save your IPtables configuration.

5. Type the following command to update IPtables in QRadar:

   ```
   ./opt/qradar/bin/iptables_update.pl
   ```

6. Repeat steps 1 - 5 to configure any additional QRadar Event Collectors that receive syslog events from a Nokia Firewall.

   You are now ready to configure your Nokia Firewall to forward events to QRadar.

Configuring syslog

To configure your Nokia Firewall to forward syslog events to IBM QRadar:

Procedure

1. Log in to the Nokia Voyager.
2. Click **Config**.
3. In the **System Configuration** pane, click **System Logging**.
4. In the **Add new remote IP address to log to** field, type the IP address of your QRadar Console orEvent Collector.
5. Click **Apply**.
6. Click **Save**.

   You are now ready to configure which events are logged by your Nokia Firewall to the logger.

Configuring the logged events custom script

To configure which events are logged by your Nokia Firewall and forwarded to IBM QRadar, you must configure a custom script for your Nokia Firewall.

Procedure

1. Using SSH, log in to Nokia Firewall as an administrative user.

   If you cannot connect to your Nokia Firewall, check that SSH is enabled. You must enable the command-line by using the Nokia Voyager web interface or connect directly by using a serial connection. For more information, see your *Nokia Voyager documentation*.

2. Type the following command to edit your Nokia Firewall `rc.local` file:

   ```
   vi /var/etc/rc.local
   ```

3. Add the following command to your `rc.local` file:

   ```
   $FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
   ```

4. Save the changes to your `rc.local` file.

   The **terminal** is displayed.

5. To begin logging immediately, type the following command:

   ```
   nohup $FWDIR/bin/fw log -ftn | /bin/logger -p local1.info &
   ```

   You can now configure the log source in QRadar.

Syslog log source parameters for Nokia Firewall

If QRadar does not automatically detect the log source, add a Nokia Firewall log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Nokia Firewall:

Table 820. Syslog log source parameters for the Nokia Firewall DSM	
Parameter	**Value**
Log Source type	Check Point
Protocol Configuration	Syslog
Log Source Identifier	Use the IP address or host name for the log source as an identifier for events from your Nokia Firewall devices.

Related tasks

Adding a log source

Integration with a Nokia Firewall by using OPSEC

IBM QRadar can accept Check Point FireWall-1 events from Nokia Firewalls using the Check Point FireWall-1 DSM configured using the OPSEC/LEA protocol.

Before you configure QRadar to integrate with a Nokia Firewall device, you must:

1. Configure Nokia Firewall using OPSEC, see "Configuring a Nokia Firewall for OPSEC" on page 1253.
2. Configure a log source in QRadar for your Nokia Firewall using the OPSEC LEA protocol, see "OPSEC/LEA log source parameters for Nokia FireWall" on page 1254.

Configuring a Nokia Firewall for OPSEC

You can configure Nokia Firewall by using OPSEC.

Procedure

1. To create a host object for your IBM QRadar, open up the **Check Point SmartDashboard** GUI, and select **Manage** > **Network Objects** > **New** > **Node** > **Host**.
2. Type the Name, IP address, and an optional comment for your QRadar.
3. Click **OK**.
4. Select **Close**.
5. To create the OPSEC connection, select **Manage** > **Servers and OPSEC Applications** > **New** > **OPSEC Application Properties**.
6. Type the Name and an optional comment.

   The name that you type must be different from the name in "Configuring a Nokia Firewall for OPSEC" on page 1253.
7. From the **Host drop-down** menu, select the QRadar host object that you created.
8. From **Application Properties**, select **User Defined as the Vendor Type**.
9. From **Client Entries**, select **LEA**.
10. Select **Communication** and enter an activation key to configure the Secure Internal Communication (SIC) certificate.
11. Select **OK** and then select **Close**.
12. To install the policy on your firewall, select **Policy** > **Install** > **OK**.

    For more information on policies, see your vendor documentation. You can now configure a log source for your Nokia Firewall in QRadar.

OPSEC/LEA log source parameters for Nokia FireWall

If QRadar does not automatically detect the log source, add a Nokia FireWall log source on the QRadar Console by using the OPSEC/LEA protocol.

When using the OPSEC/LEA protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect OPSEC/LEA events from a Nokia FireWall:

Table 821. OPSEC/LEA log source parameters for the Nokia FireWall DSM

Parameter	Value
Log Source type	Check Point FireWall-1
Protocol Configuration	OPSEC/LEA
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names are better because they enable QRadar to match a log file to a unique event source.

For a complete list of OPSEC/LEA protocol parameters and their values, see "OPSEC/LEA protocol configuration options" on page 201.

Related tasks

Adding a log source

Chapter 109. Nominum Vantio

Note: The Nominum Vantio DSM for QRadar is deprecated.

Chapter 110. Nortel Networks

Several Nortel Networks DSMs can be integrated with IBM QRadar.

Nortel Multiprotocol Router

The Nortel Multiprotocol Router DSM for IBM QRadar records all relevant Nortel Multiprotocol Router events by using syslog.

About this task

Before you configure QRadar to integrate with a Nortel Multiprotocol Router device, you must:

Procedure

1. Log in to your Nortel Multiprotocol Router device.
2. At the prompt, type the following command:

   ```
   bcc
   ```

   The Bay Command Console prompt is displayed.

   ```
   Welcome to the Bay Command Console!
   * To enter configuration mode, type config
   * To list all system commands, type ?
   * To exit the BCC, type exit
   bcc>
   ```
3. Type the following command to access configuration mode:

   ```
   config
   ```
4. Type the following command to access syslog configuration:

   ```
   syslog
   ```
5. Type the following commands:

   ```
   log-host address <IP address>
   ```

   Where <*IP address*> is the IP address of your QRadar.
6. View current default settings for your QRadar:

   ```
   info
   ```

   For example:

   ```
   log-host/<IP_address># info
   address <IP_address>
   log-facility local0
   state enabled
   ```
7. If the output of the command entered in “Nortel Multiprotocol Router” on page 1257 indicates that the state is not enabled, type the following command to enable forwarding for the syslog host:

   ```
   state enable
   ```
8. Configure the log facility parameter:

   ```
   log-facility local0
   ```

9. Create a filter for the hardware slots to enable them to forward the syslog events. Type the following command to create a filter with the name WILDCARD:

   ```
   filter name WILDCARD entity all
   ```

10. Configure the slot-upper bound parameter:

    ```
    slot-upper bound <number of slots>
    ```

    Where <*number of slots*> is the number of slots available on your device. This parameter can require different configuration which depends on your version of Nortel Multiprotocol Router device, which determines the maximum number of slots available on the device.

11. Configure the level of syslog messages you want to send to your QRadar.

    ```
    severity-mask all
    ```

12. View the current settings for this filter:

    ```
    info
    ```

    For example:

    ```
    filter/<IP_address>/WILDCARD# info
    debug-map debug
    entity all
    event-lower-bound 0
    event-upper-bound 255
    fault-map critical
    info-map info
    name WILDCARD
    severity-mask {fault warning info trace debug}
    slot-lower-bound 0
    slot-upper-bound 1
    state enabled
    trace-map debug
    warning-map warning
    ```

13. View the currently configured settings for the syslog filters:

    ```
    show syslog filters
    ```

    When the syslog and filter parameters are correctly configured, the Operational State indicates up.

    For example:

    ```
    syslog# show syslog filters
    show syslog filters Sep 15, 2008 18:21:25 [GMT+8]
    ```

    Table 822. Syslog filters

Host IP address	Filter Name	Entity Name	Entity Code	Configured State	Operational State
<IP_address1>	WILDCARD	all	255	enabled	up
<IP_address2>	WILDCARD	all	255	enabled	up

14. View the currently configured syslog host information:

```
show syslog log-host
```

The host log displays the number of packets that are going to the various syslog hosts.

For example:

```
syslog# show syslog log-host
show syslog log-host Sep 15, 2008 18:21:32 [GMT+8]
```

Table 823. Syslog host log

Host IP address	Configured State	Operational State	Time Sequencing	UDP Port	Facility Code	#Messages Sent
<IP_address 1>	enabled	up	disabled	514	local0	1402
<IP_address 2>	enabled	up	disabled	514	local0	131

15. Exit the command line interface:
    a) Exit the current command line to return to the bcc command line:

    ```
    exit
    ```

16. Exit the bbc command line:

    ```
    exit
    ```

17. Exit the command-line session:

    ```
    logout
    ```

18. You can now configure the log source in QRadar.

    To configure QRadar to receive events from a Nortel Multiprotocol Router device:

    a) From the **Log Source Type** list, select the **Nortel Multiprotocol Router** option.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Nortel Application Switch

Nortel Application Switches integrate routing and switching by forwarding traffic at layer 2 speed by using layer 4-7 information.

About this task

The Nortel Application Switch DSM for IBM QRadar accepts events by using syslog. QRadar records all relevant status and network condition events. Before you configure a Nortel Application Switch device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Nortel Application Switch command-line interface (CLI).
2. Type the following command:

   ```
   /cfg/sys/syslog/host
   ```

3. At the prompt, type the IP address of your QRadar:

Enter new syslog host: <*IP address*>

Where <*IP address*> is the IP address of your QRadar.

4. Apply the configuration:

   `apply`

5. After the new configuration is applied, save your configuration:

   `save`

6. Type y at the prompt to confirm that you want to save the configuration to flash.
   See the following example:

   ```
   Confirm saving to FLASH [y/n]: y
   New config successfully saved to FLASH
   ```

   Next you will need to configure QRadar to receive events from a Nortel Application Switch:

7. Configure the log source in QRadar. From the **Log Source Type** list, select the **Nortel Application Switch** option.

   For more information about the Nortel Application Switch, see your vendor documentation.

Related tasks

"Adding a log source" on page 5

Nortel Contivity

A QRadar Nortel Contivity DSM records all relevant Nortel Contivity events by using syslog.

About this task

Before you configure QRadar to integrate with a Nortel Contivity device, take the following steps:

Procedure

1. Log in to the Nortel Contivity command-line interface (CLI).
2. Type the following command:

   enable <*password*>

   Where <*password*> is the Nortel Contivity device administrative password.

3. Type the following command:

   `config t`

4. Configure the logging information:

   `logging <IP address> facility-filter all level all`

   Where <*IP address*> is the IP address of the QRadar.

5. Type the following command to exit the command-line:

   `exit`

   Next you will need to configure QRadar to receive events from a Nortel Contivity device.

6. You can now configure the log source in QRadar. From the **Log Source Type** list, select the **Nortel Contivity VPN Switch**

   For more information about your Nortel Contivity device, see your vendor documentation.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Nortel Ethernet Routing Switch 2500/4500/5500

The IBM QRadar Nortel Ethernet Routing Switch (ERS) 2500/4500/5500 DSM records all relevant routing switch events by using syslog.

About this task

Before configuring a Nortel ERS 2500/4500/5500 device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Nortel ERS 2500/4500/5500 user interface.
2. Type the following commands to access global configuration mode:

   ```
   ena
   config term
   ```
3. Type `informational` as the severity level for the logs you want to send to the remote server.

   For example, `logging remote level {critical|informational|serious|none}`

   ```
   logging remote level informational
   ```

   Where a severity level of `informational` sends all logs to the syslog server.
4. Enable the host:

   ```
   host enable
   ```
5. Type the remote logging address:

   ```
   logging remote address <IP address>
   ```

   Where <*IP address*> is the IP address of the QRadar system.
6. Ensure that remote logging is enabled:

   ```
   logging remote enable
   ```

   You can now configure the log source in QRadar.
7. To configure to receive events from a Nortel ERS 2500/4500/5500 device: From the **Log Source Type** list, select the **Nortel Ethernet Routing Switch 2500/4500/5500** option.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Nortel Ethernet Routing Switch 8300/8600

The IBM QRadar Nortel Ethernet Routing Switch (ERS) 8300/8600 DSM records all relevant events by using syslog.

About this task

Before you configure a Nortel ERS 8600 device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Nortel ERS 8300/8600 command-line interface (CLI).

2. Type the following command:

   `config sys syslog host <ID>`

   Where <*ID*> is the ID of the host you wish to configure to send syslog events to QRadar.

   For the syslog host ID, the valid range is 1 - 10.
3. Type the IP address of your QRadar system:

   address <*IP address*>

   Where <IP address> is the IP address of your QRadar system.
4. Type the facility for accessing the syslog host.

   `host <ID> facility local0`

   Where <*ID*> is the ID specified in "Nortel Ethernet Routing Switch 8300/8600" on page 1261.
5. Enable the host:

   `host enable`
6. Type the severity level for which syslog messages are sent:

   `host <ID> severity info`

   Where <*ID*> is the ID specified in "Nortel Ethernet Routing Switch 8300/8600" on page 1261.
7. Enable the ability to send syslog messages:

   `state enable`
8. Verify the syslog configuration for the host:

   `sylog host <ID> info`

   For example, the output might resemble the following:

   ```
   ERS-8606:5/config/sys/syslog/host/1# info Sub-Context: Current Context:
   address : 192.0.2.1 create : 1 delete : N/A facility : local6 host : enable
   mapinfo : info mapwarning : warning maperror : error mapfatal : emergency
   severity : info|warning|error|fatal udp-port : 514 ERS-8606:5/config/sys/
   syslog/host/1#
   ```

   You can now configure the log source in QRadar.
9. To configure QRadar to receive events from a Nortel ERS 8300/8600 device: From the **Log Source Type** list, select the **Nortel Ethernet Routing Switch 8300/8600** option.

Related tasks

"Adding a log source" on page 5

Nortel Secure Router

The IBM QRadar Nortel Secure Router DSM records all relevant router events by using syslog.

About this task

Before you configure a Nortel Secure Router device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Nortel Secure Router command line interface (CLI).
2. Type the following to access global configuration mode:

   `config term`

3. Type the following command:

   ```
   system logging syslog
   ```
4. Type the IP address of the syslog server (QRadar system):

   ```
   host_ipaddr <IP address>
   ```

   Where <*IP address*> is the IP address of the QRadar system.
5. Ensure that remote logging is enabled:

   ```
   enable
   ```
6. Verify that the logging levels are configured correctly:

   ```
   show system logging syslog
   ```

   The following code is an example of the output:

   ```
   ---------------------------------- Syslog Setting
   ---------------------------------- Syslog:
   Enabled Host IP Address: <IP_address> Host UDP Port: 514
   Facility Priority Setting:
   facility priority
   ======== ========
   auth: info
   bootp: warning
   daemon: warning
   domainname: warning
   gated: warning
   kern: info
   mail: warning
   ntp: warning
   system: info
   fr: warning
   ppp: warning
   ipmux: warning
   bundle: warning
   qos: warning
   hdlc: warning
   local7: warning
   vpn: warning
   firewall: warning
   ```

   You can now configure the log source in QRadar.
7. To configure QRadar to receive events from a Nortel Secure Router device: From the **Log Source Type** list, select the **Nortel Secure Router** option.

Related tasks

"Adding a log source" on page 5

Nortel Secure Network Access Switch

The IBM QRadar Nortel Secure Network Access Switch (SNAS) DSM records all relevant switch events by using syslog.

About this task

Before you configure a Nortel SNAS device in QRadar, take the following steps:

Procedure

1. Log in to the Nortel SNAS user interface.
2. Select the **Config** tab.
3. Select **Secure Access Domain and Syslog** from the **Navigation** pane.

   The **Secure Access Domain** window is displayed.
4. From the **Secure Access Domain** list, select the **secure access domain**. Click **Refresh**.
5. Click **Add**.

   The **Add New Remote Server** window is displayed.
6. Click **Update**.

   The server is displayed in the secure access domain table.
7. Using the toolbar, click **Apply** to send the current changes to the Nortel SNAS.

   You are now ready to configure the log source in QRadar.
8. To configure QRadar to receive events from a Nortel SNAS device: From the **Log Source Type** list, select the **Nortel Secure Network Access Switch (SNAS)** option.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Nortel Switched Firewall 5100

A IBM QRadar Nortel Switched Firewall 5100 DSM records all relevant firewall events by using either syslog or OPSEC.

Before you configure a Nortel Switched Firewall device in QRadar, you must configure your device to send events to QRadar.

See information about configuring a Nortel Switched Firewall by using one the following methods:

- "Integrating Nortel Switched Firewall by using syslog" on page 1264
- "Integrate Nortel Switched Firewall by using OPSEC" on page 1265

Integrating Nortel Switched Firewall by using syslog

This method ensures the IBM QRadar Nortel Switched Firewall 5100 DSM accepts events by using syslog.

About this task

To configure your Nortel Switched Firewall 5100:

Procedure

1. Log into your Nortel Switched Firewall device command-line interface (CLI).
2. Type the following command:

```
/cfg/sys/log/syslog/add
```

3. Type the IP address of your QRadar system at the following prompt:

   ```
   Enter IP address of syslog server:
   ```

   A prompt is displayed to configure the severity level.
4. Configure **info** as the severity level.

   For example, `Enter minimum logging severity`

   `(emerg | alert | crit | err | warning | notice | info | debug): info`

   A prompt is displayed to configure the facility.
5. Configure **auto** as the local facility.

   For example, `Enter the local facility (auto | local0-local7): auto`
6. Apply the configuration:

   ```
   apply
   ```
7. Repeat for each firewall in your cluster.

   You are now ready to configure the log source in QRadar.
8. To configure QRadar to receive events from a Nortel Switched Firewall 5100 device by using syslog: From the **Log Source Type** list, select the **Nortel Switched Firewall 5100** option.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Integrate Nortel Switched Firewall by using OPSEC

This method ensures the IBM QRadar Nortel Switched Firewall 5100 DSM accepts Check Point FireWall-1 events by using OPSEC.

Depending on your Operating System, the procedures for the Check Point SmartCenter Server can vary. The following procedures are based on the Check Point SecurePlatform Operating system.

To enable Nortel Switched Firewall and QRadar integration, take the following steps:

1. Reconfigure Check Point SmartCenter Server.
2. Configure the log source in QRadar.

Configuring a log source

Configure the log source in QRadar.

Procedure

1. To configure QRadar to receive events from a Nortel Switched Firewall 5100 device that uses OPSEC, you must select the **Nortel Switched Firewall 5100** option from the **Log Source Type** list.
2. To configure QRadar to receive events from a Check Point SmartCenter Server that uses OPSEC LEA, you must select the **LEA** option from the **Protocol Configuration** list when you configure your protocol configuration.

Related concepts

"OPSEC/LEA protocol configuration options" on page 201
To receive events on port 18184, configure a log source to use the OPSEC/LEA protocol.

Related tasks

"Adding a log source" on page 5

Nortel Switched Firewall 6000

A IBM QRadar Nortel Switched Firewall 6000 DSM records all relevant firewall events by using either syslog or OPSEC.

Before you configure a Nortel Switched Firewall device in QRadar, you must configure your device to send events to QRadar.

The following information is about configuring a Nortel Switched Firewall 6000 device with QRadar by using one of the following methods:

- “Configuring syslog for Nortel Switched Firewalls” on page 1266
- “Configuring OPSEC for Nortel Switched Firewalls ” on page 1267

Configuring syslog for Nortel Switched Firewalls

This method ensures the IBM QRadar Nortel Switched Firewall 6000 DSM accepts events by using syslog.

About this task

To configure your Nortel Switched Firewall 6000:

Procedure

1. Log into your Nortel Switched Firewall device command-line interface (CLI).
2. Type the following command:

   `/cfg/sys/log/syslog/add`
3. Type the IP address of your QRadar system at the following prompt:

   `Enter IP address of syslog server:`

   A prompt is displayed to configure the severity level.
4. Configure **`info`** as the severity level.

   For example, `Enter minimum logging severity`

   `(emerg | alert | crit | err | warning | notice | info | debug): info`

   A prompt is displayed to configure the facility.
5. Configure **`auto`** as the local facility.

   For example, `Enter the local facility (auto | local0-local7): auto`
6. Apply the configuration:

   `apply`

   You can now configure the log source in QRadar.
7. To configure QRadar to receive events from a Nortel Switched Firewall 6000 using syslog: From the Log Source Type list, select the **Nortel Switched Firewall 6000** option.

Related tasks

“Adding a log source” on page 5

Configuring OPSEC for Nortel Switched Firewalls

This method ensures the IBM QRadar Nortel Switched Firewall 6000 DSM accepts Check Point FireWall-1 events by using OPSEC.

About this task

Depending on your Operating System, the procedures for the Check Point SmartCenter Server can vary. The following procedures are based on the Check Point SecurePlatform Operating system.

To enable Nortel Switched Firewall and QRadar integration, take the following steps:

Procedure

1. Reconfigure Check Point SmartCenter Server. See "Reconfiguring the Check Point SmartCenter Server" on page 1267.
2. Configure the OPSEC LEA protocol in QRadar.

   To configure QRadar to receive events from a Check Point SmartCenter Server that uses OPSEC LEA, you must select the **LEA** option from the **Protocol Configuration** list when you configure LEA.
3. Configure the log source in QRadar.

   To configure QRadar to receive events from a Nortel Switched Firewall 6000 device using OPSEC you must select the **Nortel Switched Firewall 6000** option from the **Log Source Type** list.

Related concepts

"OPSEC/LEA protocol configuration options" on page 201
To receive events on port 18184, configure a log source to use the OPSEC/LEA protocol.

Related tasks

"Adding a log source" on page 5

Reconfiguring the Check Point SmartCenter Server

In the Check Point SmartCenter Server, you can create a host object that represents the IBM QRadar system. The *leapipe* is the connection between the Check Point SmartCenter Server and QRadar.

About this task

To reconfigure the Check Point SmartCenter Server:

Procedure

1. To create a host object, open the Check Point SmartDashboard user interface and select **Manage** > **Network Objects** > **New** > **Node** > **Host**.
2. Type the Name, IP address, and type a comment for your host if you want.
3. Click **OK**.
4. Select **Close**.
5. To create the OPSEC connection, select **Manage** > **Servers and OPSEC applications** > **New** > **OPSEC Application Properties**.
6. Type the Name, and type a comment if you want.

   The name that you type must be different from the name in "Reconfiguring the Check Point SmartCenter Server" on page 1267.
7. From the **Host** drop-down menu, select the host object that you have created in "Reconfiguring the Check Point SmartCenter Server" on page 1267.
8. From **Application Properties**, select **User Defined** as the vendor.
9. From **Client Entries**, select **LEA**.

10. Click **Communication** to generate a Secure Internal Communication (SIC) certificate and enter an activation key.
11. Click **OK** and then click **Close**.
12. To install the Security Policy on your firewall, select **Policy** > **Install** > **OK**.

    The configuration is complete.

Nortel Threat Protection System (TPS)

The IBM QRadar Nortel Threat Protection System (TPS) DSM records all relevant threat and system events by using syslog.

About this task

Before you configure a Nortel TPS device in QRadar, take the following steps:

Procedure

1. Log in to the Nortel TPS user interface.
2. Select **Policy & Response** > **Intrusion Sensor** > **Detection & Prevention**.

   The **Detection & Prevention** window is displayed.
3. Click **Edit** next to the intrusion policy you want to configure alerting option.

   The **Edit Policy** window is displayed.
4. Click **Alerting**.

   The **Alerting** window is displayed.
5. Under **Syslog Configuration**, select **on next to State** to enable *syslog alerting*.
6. From the list, select the facility and priority levels.
7. Optional: In the **Logging Host** field, type the IP address of your QRadar system. This configures your QRadar system to be your logging host. Separate multiple hosts with commas.
8. Click **Save**.

   The *syslog alerting* configuration is saved.
9. Apply the policy to your appropriate detection engines.

   You can now configure the log source in QRadar.
10. To configure QRadar to receive events from a Nortel TPS device: From the **Log Source Type** list, select the **Nortel Threat Protection System (TPS) Intrusion Sensor** option.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Nortel VPN Gateway

The IBM QRadar Nortel VPN Gateway DSM accepts events by using syslog.

About this task

QRadar records all relevant operating system (OS), system control, traffic processing, startup, configuration reload, AAA, and IPsec events. Before you configure a Nortel VPN Gateway device in QRadar, you must configure your device to send syslog events to QRadar.

To configure the device to send syslog events to QRadar:

Procedure

1. Log in to the Nortel VPN Gateway command-line interface (CLI).
2. Type the following command:

   ```
   /cfg/sys/syslog/add
   ```
3. At the prompt, type the IP address of your QRadar system:

   ```
   Enter new syslog host: <IP address>
   ```

   Where <*IP address*> is the IP address of your QRadar system.
4. Apply the configuration:

   ```
   apply
   ```
5. View all syslog servers currently added to your system configuration:

   ```
   /cfg/sys/syslog/list
   ```

   You can now configure the log source in QRadar.
6. To configure QRadar to receive events from a Nortel VPN Gateway device: From the **Log Source Type** list, select the **Nortel VPN Gateway** option.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Chapter 111. Novell eDirectory

The Novell eDirectory DSM for IBM QRadar accepts audit events from Novell eDirectory using syslog.

To use the Novell eDirectory DSM, you must have the following components installed:

- Novell eDirectory v8.8 with service pack 6 (sp6)
- Novell Audit Plug-in
- Novell iManager v2.7
- XDASv2

To configure Novell eDirectory with QRadar, you must:

1. Configure the XDASv2 property file to forward events to QRadar.
2. Load the XDASv2 module on your Linux or Windows Operating System.
3. Install the Novell Audit Plug-in on the Novell iManager.
4. Configure auditing using Novell iManager.
5. Configure QRadar.

Related tasks
"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring XDASv2 to forward events

By default, XDASv2 is configured to log events to a file. To forward events from XDASv2 to QRadar, you must edit the `xdasconfig.properties.template` and configure the file for syslog forwarding.

About this task

Audit events must be forwarded by syslog to QRadar, instead of being logged to a file.

To configure XDASv2 to forward syslog events:

Procedure

1. Log in to the server hosting Novell eDirectory.
2. Open the following file for editing:
   - Windows - `C:\Novell\NDS\xdasconfig.properties.template`
   - Linux or Solaris - `etc/opt/novell/eDirectory/conf/xdasconfig.properties.template`
3. To set the root logger, remove the comment marker (#) from the following line:

   ```
   log4j.rootLogger=debug, S, R
   ```
4. To set the appender, remove the comment marker (#) from the following line:

   ```
   log4j.appender.S=org.apache.log4j.net.SyslogAppender
   ```
5. To configure the IP address for the syslog destination, remove the comment marker (#) and edit the following lines:

   ```
   log4j.appender.S.Host=<IP address> log4j.appender.S.Port=<Port>
   ```

   Where,

   `<IP address>` is the IP address or hostname of QRadar.

   `<Port>` is the port number for the UDP or TCP protocol. The default port for syslog communication is port **514** for QRadar or Event Collectors.

6. To configure the syslog protocol, remove the comment marker (#) and type the protocol (UDP, TCP, or SSL) use in the following line:

   ```
   log4j.appender.S.Protocol=TCP
   ```

   The encrypted protocol SSL is not supported by QRadar.
7. To set the severity level for logging events, remove the comment marker (#) from the following line:

   ```
   log4j.appender.S.Threshold=INFO
   ```

   The default value of INFO is the correct severity level for events.
8. To set the facility for logging events, remove the comment marker (#) from the following line:

   ```
   log4j.appender.S.Facility=USER
   ```

   The default value of USER is the correct facility value for events.
9. To set the facility for logging events, remove the comment marker (#) from the following line:

   ```
   log4j.appender.R.MaxBackupIndex=10
   ```
10. Save the `xdasconfig.properties.template` file.

    After you configure the syslog properties for XDASv2 events, you are ready to load the XDASv2 module.

Loading the XDASv2 Module

Before you can configure events in Novell iManager, you must load the changes that you made to the XDASv2 module.

About this task

To load the XDASv2 module, select your operating system:

- To load the XDASv2 in Linux, see "Loading the XDASv2 on a Linux Operating System" on page 1272.
- To load the XDASv2 in Windows, see "Loading the XDASv2 on a Windows Operating System" on page 1273.

Important: If your Novell eDirectory has Novell Module Authentication Service (NMAS) installed with NMAS auditing enabled, the changes made to XDASv2 modules are loaded automatically. If you have NMAS installed, you should configure event auditing. For information on configuring event auditing, see "Configuring event auditing using Novell iManager" on page 1273.

Loading the XDASv2 on a Linux Operating System

You can load XDASv2 on a Linux Operating System.

Procedure

1. Log in to your Linux server hosting Novell eDirectory, as a root user.
2. Type the following command:

   ```
   ndstrace -c "load xdasauditds"
   ```

What to do next

You are now ready to configure event auditing in Novell eDirectory. For more information, see "Configuring event auditing using Novell iManager" on page 1273.

Loading the XDASv2 on a Windows Operating System

You can load XDASv2 on a Windows Operating System.

Procedure

1. Log in to your Windows server hosting Novell eDirectory.
2. On your desktop, click **Start > Run**.

   The Run window is displayed.
3. Type the following:

   `C:\Novell\NDS\ndscons.exe`

   This is the default installation path for the Windows Operating System. If you installed Novell eDirectory to a different directory, then the correct path is required.
4. Click **OK**.

   The Novell Directory Service console displays a list of available modules.
5. From the **Services** tab, select **xdasauditds**.
6. Click **Start**.

   The xdasauditds service is started for Novell eDirectory.
7. Click **Startup**.

   The Service window is displayed.
8. In the **Startup Type** panel, select the **Automatic** check box.
9. Click **OK**.
10. Close the Novell eDirectory Services window.

What to do next

You are now ready to configure event auditing in Novell eDirectory. For more information, see "Configuring event auditing using Novell iManager" on page 1273.

Configuring event auditing using Novell iManager

You can configure event auditing for XDASv2 in Novell iManager.

Procedure

1. Log in to your Novell iManager console user interface.
2. From the navigation bar, click **Roles and Tasks**.
3. In the left-hand navigation, click **eDirectory Auditing** > **Audit Configuration**.

   The Audit Configuration panel is displayed.
4. In the **NPC Server name** field, type the name of your NPC Server.
5. Click **OK**.

   The Audit Configuration for the NPC Server is displayed.
6. Configure the following parameters:
   a) On the **Components** panel, select one or both of the following:

      DS - Select this check box to audit XDASv2 events for an eDirectory object.

      LDAP - Select this check box to audit XDASv2 events for a Lightweight Directory Access Protocol (LDAP) object.
7. On the **Log Event's Large Values** panel, select one of the following:

Log Large Values - Select this option to log events that are larger than 768 bytes.

Don't Log Large Values - Select this option to log events less than 768 bytes. If a value exceeds 768 bytes, then the event is truncated.

8. On the **XDAS Events Configuration**, select the check boxes of the events you want XDAS to capture and forward to IBM QRadar.
9. Click **Apply**.
10. On the **XDAS** tab, click **XDASRoles**.

    The XDAS Roles Configuration panel is displayed.
11. Configure the following role parameters:
    a) Select a check box for each object class to support event collection.
12. From the **Available Attribute(s)** list, select any attributes and click the **arrow** to add these to the **Selected Attribute(s)** list.
13. Click **OK** after you have added the object attributes.
14. Click **Apply**.
15. On the **XDAS** tab, click **XDASAccounts**.

    The XDAS Accounts Configuration panel is displayed.
16. Configure the following account parameters:
    a) From the **Available Classes** list, select any classes and click the **arrow** to add these to the **Selected Attribute(s)** list.
17. Click **OK** after you have added the object attributes.
18. Click **Apply**.

What to do next

You are now ready to add a log source in QRadar.

Related tasks

"Adding a log source" on page 5

Configuring a log source

IBM QRadar automatically detects syslog events from Novell eDirectory. If the log source is not automatically detected, add a log source in QRadar.

Procedure

From the Log Source Type list, select Novell eDirectory.

For more information about Novell eDirectory, Novell iManager, or XDASv2, see your vendor documentation.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Novell eDirectory sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Novell eDirectory sample message when you use the Syslog protocol

The following sample event message shows that an account security token modification failed.

```
eDirectory: INFO {"Source" : "eDirectory#DS","Observer" : {"Account" :
{"Domain" : "DOMAIN-EXAMPLE-TEST","Name" : "CN=ws,OU=SRV,O=COMPANY"},"Entity" : {"SysAddr" :
"172.16.20.1","SysName" : "ws.domain.example.test"}},"Initiator" : {"Account" : {"Domain" :
"DOMAIN-EXAMPLE-TEST","Name" : "CN=ws,OU=SRV,O=COMPANY"},"Entity" : {"SysAddr" :
"172.16.20.1"}},"Target" : {"Data" : {"ClassName" : "User","Version" : "2"},"Account" :
{"Domain" : "DOMAIN-EXAMPLE-TEST","Name" : "CN=TEST,OU=usr,O=ORG","Id" : "11111111"}},"Action" :
{"Event" : {"Id" : 0.0.0.6","Name" : "MODIFY_ACCOUNT_SECURITY_TOKEN","CorrelationID" :
"eDirectory#0#","SubEvent" : "DSE_CHGPASS"},"Time" : {"Offset" : 1567083869},"Log" :
{"Severity" : 7},"Outcome" : "1.10","ExtendedOutcome" : "-215"}}
```


```
eDirectory: INFO {"Source" : "eDirectory#DS","Observer" : {"Account" :
{"Domain" : "DOMAIN-EXAMPLE-TEST","Name" : "CN=ws,OU=SRV,O=COMPANY"},"Entity" : {"SysAddr" :
"172.16.20.1","SysName" : "ws.domain.example.test"}},"Initiator" : {"Account" :
{"Domain" : "DOMAIN-EXAMPLE-TEST","Name" : "CN=ws,OU=SRV,O=COMPANY"},"Entity" :
{"SysAddr" : "172.16.20.1"}},"Target" : {"Data" : {"ClassName" :
"User","Version" : "2"},"Account" : {"Domain" : "DOMAIN-EXAMPLE-TEST","Name" :
"CN=TEST,OU=usr,O=ORG","Id" : "11111111"}},"Action" : {"Event" : {"Id" : 0.0.0.6","Name" :
"MODIFY_ACCOUNT_SECURITY_TOKEN","CorrelationID" : "eDirectory#0#","SubEvent" :
"DSE_CHGPASS"},"Time" : {"Offset" : 1567083869},"Log" : {"Severity" : 7},"Outcome" :
"1.10","ExtendedOutcome" : "-215"}}
```


Table 824. Highlighted values in the Novell eDirectory sample event

QRadar field name	Highlighted values in the event payload
Event ID	**MODIFY_ACCOUNT_SECURITY_TOKEN** - FAILED is extracted from the Event.Name and Outcome fields in Action object. If Outcome = 0, then eventID = Event.Name. Otherwise, eventID = Event.Name + "-FAILED", as shown in this sample event.
Device Category	**eDirectory**
Username	**TEST**
Source IP	**172.16.20.1**
Device Time	**1567083869** (which is Aug 29, 2019, 10:04:29 AM)

Chapter 112. Observe IT JDBC

The IBM QRadar DSM for ObserveIT JDBC collects JDBC events from ObserveIT.

The following table identifies the specifications for the ObserveIT JDBC DSM:

Table 825. ObserveIT JDBC DSM specifications

Specification	**Value**
Manufacturer	ObserveIT
Product	ObserveIT JDBC
DSM RPM name	`DSM-ObserveIT-`*`QRadar_Version-Build_Number`*`.noarch.rpm`
Supported versions	V5.7
Protocol	ObserveIT JDBC Log File Protocol
QRadar recorded events	The following event types are supported by ObserveIT JDBC: • Alerts • User Activity • System Events • Session Activity • DBA Activity The Log File Protocol supports user activity in LEEF logs.
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	ObserveIT website (http://www.observeit-sys.com)

To collect ObserveIT JDBC events, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs from the IBM Support Website onto your QRadar Console:
   - ObserveIT JDBC DSM RPM
   - DSMCommon DSM RPM
   - ObserveIT JDBC PROTOCOL RPM
   - JDBC PROTOCOL RPM
2. Make sure that your ObserveIT system is installed and the SQL Server database is accessible over the network.
3. For each ObserveIT server that you want to integrate, create a log source on the QRadar Console. Configure all the required parameters. Use these tables to configure ObserveIT specific parameters:

Table 826. ObserveIT JDBC log source parameters	
Parameter	**Description**
Log Source type	ObserveIT
Protocol Configuration	ObserveIT JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database name	ObserveIT
IP or Hostname	The IP address or host name of the ObserveIT system.
Port	The port on the ObserveIT host. The default is 1433.
Username	The user name that is required to connect to the ObserveIT MS SQL database
Password	The password that is required to connect to the ObserveIT MS SQL database.
Start Date and Time	Use the yyyy-MM-dd HH: mm format.
Polling Interval	The frequency by which to poll the database.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.

Table 827. Log file protocol parameters	
Parameter	**Description**
Protocol Configuration	Log file
Log Source Identifier	The IP address for the log source. This value must match the value that is configured in the **Remote IP or Hostname** parameter. The **Log Source Identifier** value must be unique for the log source type.

Table 827. Log file protocol parameters (continued)

Parameter	Description
Service Type	From the list, select the protocol that you want to use when retrieving log files from a remote server. The default is SFTP. SFTP - SSH File Transfer Protocol FTP - File Transfer Protocol SCP - Secure Copy The underlying protocol that retrieves log files for the SCP and SFTP service type requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	The IP address or host name of the device that stores your event log files.
Remote Port	If the remote host uses a non-standard port number, you must adjust the port value to retrieve events.
Remote User	The user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in Length.
Remote Password	The password that is necessary to log in to the host.
Confirm Password	Confirmation of the password that is necessary to log in to the host.
SSH Key File	The path to the SSH key, if the system is configured to use key authentication. When an SSH key file is used, the **Remote Password** field is ignored.
Remote Directory	For FTP, if the log files are in the remote user's home directory, you can leave the remote directory blank. A blank **remote directory** field supports systems where a change in the working directory (CWD) command is restricted.
SCP Remote File	If you selected **SCP** as the **Service Type**, you must type the file name of the remote file.
Recursive	This option is ignored for SCP file transfers.
FTP File Pattern	The regular expression (regex) required to identify the files to download from the remote host.
FTP Transfer Mode	For ASCII transfers over FTP, you must select **NONE** in the **Processor** field and **LINEBYLINE** in the **Event Generator** field.

Table 827. Log file protocol parameters (continued)

Parameter	Description
Start Time	The time of day when you want the processing to begin. For example, type `12:00 AM` to schedule the log file protocol to collect event files at midnight. This parameter functions with the **Recurrence value** to establish when and how often the **Remote Directory** is scanned for files. Type the **start time**, based on a 12-hour clock, in the following format: `HH:MM` *<AM/PM>*.
Recurrence	The time interval to determine how frequently the remote directory is scanned for new event log files. The time interval can include values in hours (H), minutes (M), or days (D). For example, a recurrence of 2H scans the remote directory every 2 hours.
Run On Save	Starts the log file import immediately after you save the log source configuration. When selected, this check box clears the list of previously downloaded and processed files. After the first file import, the log file protocol follows the start time and recurrence schedule that is defined by the administrator.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle.
Processor	Processors allow QRadar to expand event file archives, and to process contents for events. QRadar processes files only after they are downloaded. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.
Ignore Previously Processed File(s)	Tracks and ignores files that were processed by the log file protocol. QRadar examines the log files in the remote directory to determine whether a file was processed previously by the log file protocol. If a previously processed file is detected, the log file protocol does not download the file for processing. All files that were not processed previously are downloaded. This option applies only to FTP and SFTP Service Types.
Change Local Directory?	Changes the local directory on the Target Event Collector to store event logs before they are processed.
Local Directory	The local directory on the Target Event Collector. The directory must exist before the log file protocol attempts to retrieve events.

Table 827. Log file protocol parameters (continued)	
Parameter	**Description**
File Encoding	The character encoding that is used by the events in your log file.
Folder Separator	The character that is used to separate folders for your operating system. Most configurations can use the default value in **Folder Separator** field. This field is intended for operating systems that use a different character to define separate folders. For example, periods that separate folders on mainframe systems.

Related tasks

Adding a DSM

Adding a log source

Chapter 113. Okta

The IBM QRadar DSM for Okta collects Okta REST API events from an Okta device.

The following table identifies the specifications for the Okta DSM:

Table 828. Okta DSM specifications

Specification	**Value**
Manufacturer	Okta
DSM name	Okta
RPM file name	`DSM-OktaIdentityManagement-`*`QRadar_version-build_number`*`.noarch.rpm`
Protocol	Okta REST API
Event format	JSON
Recorded event types	All
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Okta website (https://www.okta.com/)

To integrate Okta with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol Common
   - Okta REST API Protocol RPM
   - Okta DSM RPM

   If multiple DSM RPMs are required, the integration sequence must reflect the DSM RPM dependency.
2. Add an Okta log source on the QRadar Console:

   Table 829. Okta DSM log source parameters

Parameter	**Value**
Log Source type	Okta
Protocol type	Okta REST API
Name	A name for the log source
Description (optional)	A description for the log source

For a list of Okta REST API protocol parameters and their values, see Okta REST API protocol configuration options.

The following table provides a sample event message for the Okta DSM:

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Table 830. Okta sample message supported by the Okta device

Event name	Low level category	Sample log message
Core-User Auth-Login Success	User Login Success	{"eventId":"xxxxxxxxxxxxxx xxxxx-xxxxxxxxxxxxxxx","sessionId":"xxxxxxxxxxxxxxxx xxxxxxx","requestId":"xxxxx xxxxxxxxxxxxxxxxxxx", "published":"2016-04-06T16:16:40.000Z","action":{ "message":"Sign-in successful","categories":["Sign-in Success"],"objectType":"core.user_auth.login_success","requestUri":"/api/v1/authn"},"actors":[{"id":"xxxxxxxxxxxxxxxxxx", "displayName":"User","login":"username@example.com", "objectType":"User"},{"id":"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0", "displayName":"FIREFOX", "ipAddress":"<IP_address>", "objectType":"Client"}], "targets":[{"id":"xxxxxxxx xxxxxxxxxxx","displayName":"User","login":"username@example.com","objectType":"User"}]}

{"eventId":"xxxxxxxxxxxxxxxxxxxx-xxxxxxxxxxxxxxxx","sessionId":"xxxxxxxxxxxxxxxxxx","requestId":"xxxxxxxxxxxxxxxxxx","published":"2016-04-06T16:16:40.000Z","action":{"message":"Sign-in successful","categories":["Sign-in Success"],"objectType":"core.user_auth.login_success","requestUri":"/api/v1/authn"},"actors":[{"id":"xxxxxxxxxxxxxxxxxxx","displayName":"User","login":"username@example.com","objectType":"User"},{"id":"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0","displayName":"FIREFOX","ipAddress":"<IP_address>","objectType":"Client"}],"targets":[{"id":"xxxxxxxxxxxxxxxxxxx","displayName":"User","login":"username@example.com","objectType":"User"}]}

Table 830. Okta sample message supported by the Okta device (continued)

Event name	Low level category	Sample log message
Core-User Auth-Login Failed	User Login Failure	{"eventId":"xxxxxxxxxxxxxxx_ xxxxxxxxxxxxxxxxxxxxx","sessionId" :"","requestId":"xxxxxxxxxxxxxxxxxx -xxxxxx","published":"2015-08- 19T17:08:37.000Z","action": {"message":"Sign-in Failed - Not Specified","categories":["Sign-in Failure","Suspicious Activity"], "objectType":"core.user_auth. login_failed","requestUri":"/ login/do-login"},"actors":[{"id" :"Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko","displayName":"x x", "ipAddress":"<IP_address>","objectType" :"Client"}],"targets":[{"id":"", "objectType":"User"}]} {"eventId":"xxxxxxxxxxxxxxx_xxxxxxxxxx xxxxxxxxxx","sessionId":"","requestId": "xxxxxxxxxxxxxxxxxx- xxxxxx","published":"2015-08-19T17:08:3 7.000Z","action":{"message":"Sign-in Failed - Not Specified","categories": ["Sign-in Failure","Suspicious Activity"],"objectType":"core.user_auth. login_failed","requestUri":"/login/do- login"},"actors":[{"id":"Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko","displayName":"x x","ipAddress":"<IP_address>","objectTyp e":"Client"}],"targets": [{"id":"","objectType":"User"}]}

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Chapter 114. Onapsis Security Platform

The IBM QRadar DSM for Onapsis Security Platform collects logs from an Onapsis Security Platform device.

The following table describes the specifications for the Onapsis Security Platform DSM:

Table 831. Onapsis Security Platform DSM specifications

Specification	**Value**
Manufacturer	Onapsis
DSM name	Onapsis Security Platform
RPM file name	`DSM-OnapsisIncOnapsisSecurityPlatform-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	1.5.8 and later
Event format	Log Event Extented Format (LEEF)
Recorded event types	Assessment Attack signature Correlation Compliance
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Onapsis website (https://www.onapsis.com)

To integrate Onapsis Security Platform with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Onapsis Security Platform DSM RPM
   - DSM Common RPM
2. Configure your Onapsis Security Platform device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add an Onapsis Security Platform log source on the QRadar Console. The following table describes the parameters that require specific values for Onapsis Security Platform event collection:

   Table 832. Onapsis Security Platform log source parameters

Parameter	**Value**
Log Source type	Onapsis Security Platform
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Onapsis Security Platform to communicate with QRadar

To collect events from Onapsis Security Platform, you must add a connector and an alarm profile.

About this task

Alarm profiles configure the Onapsis Security Platform to automatically take action when an incident is observed.

Procedure

1. Log in to Onapsis Security Platform.
2. Click the **Gear** icon.
3. Click **Settings**.
4. From **Connectors Settings**, click **Add** to include a new connector.
5. Click **Respond** > **Alarm Profiles**.
6. Add new alarm profile.
   a) Select **Alarm Type** and **Severity**.
   b) Type the name and the description.
   c) Select the target from the **Assets List** or **Tags List**.
      The lists are mutually exclusive.
   d) Add a condition for when the alarm is triggered
   e) To add an action that runs when the alarm is triggered, click **Action**.
   f) Select the QRadar connector that was created in step 4.

Chapter 115. OpenBSD

The OpenBSD DSM for IBM QRadar accepts events by using syslog.

QRadar records all relevant informational, authentication, and system level events that are forwarded from OpenBSD operating systems.

Syslog log source parameters for OpenBSD

If QRadar does not automatically detect the log source, add a OpenBSD log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from OpenBSD:

Table 833. Syslog log source parameters for the OpenBSD DSM

Parameter	Value
Log Source type	Open BSD OS
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your OpenBSD appliance.

Related tasks

Adding a log source

Configuring syslog for OpenBSD

You can configure OpenBSD to forward syslog events.

Procedure

1. Use SHH, to log in to your OpenBSD device, as a root user.
2. Open the `/etc/syslog.conf` file.
3. Add the following line to the top of the file. Make sure that all other lines remain intact:

   `*.* @<IP address>`

   Where <*IP address*> is the IP address of your IBM QRadar.
4. Save and exit the file.
5. Send a hang-up signal to the syslog daemon to ensure that all changes are applied:

   ```
   kill -HUP `cat /var/run/syslog.pid`
   ```

   Note: This command line uses the back quotation mark character (`), which is located to the left of the number one on most keyboard layouts.

   The configuration is complete. Events that are forwarded to QRadar by OpenBSD are displayed on the **Log Activity** tab.

Chapter 116. Open LDAP

The Open LDAP DSM for IBM QRadar accepts UDP Multiline syslog events from Open LDAP installations that are configured to log stats events by using logging level 256.

Open LDAP events are forwarded to QRadar by using port 514. The events must be redirected to the port that is configured for the UDP Multiline syslog protocol. QRadar does not support UDP Multiline syslog on the standard listen port 514.

Note: UDP Multiline Syslog events can be assigned to any available port that is not in use, other than port 514. The default port that is assigned to the UDP Multiline Syslog protocol is port 517. If port 517 is already being used in your network, see the *QRadar port usage* topic in the *IBM QRadar Administration Guide* or the IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_common_ports.html?pos=2) for a list of ports that are used by QRadar.

Important: Forward the UDP Multiline syslog events directly to the chosen port (default 517) from your Open LDAP device. If you can't send events to this port directly, you can use the backup method of configuring IPtables for UDP Multiline Syslog events.

Related concepts

"UDP multiline syslog protocol configuration options" on page 233
To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

UDP Multiline Syslog log source parameters for Open LDAP

If QRadar does not automatically detect the log source, add a Open LDAP log source on the QRadar Console by using the UDP Multiline Syslog protocol.

When using the UDP Multiline Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect UDP Multiline Syslog events from Open LDAP:

Table 834. UDP Multiline Syslog log source parameters for the Open LDAP DSM

Parameter	Value
Log Source type	Open LDAP Software
Protocol Configuration	UDP Multiline Syslog
Log Source Identifier	

Table 834. UDP Multiline Syslog log source parameters for the Open LDAP DSM (continued)	
Parameter	**Value**
Listen Port	Type the port number that is used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65536. The default UDP Multiline Syslog listen port is 517. If you do not see the **Listen Port** field, you must restart Tomcat on QRadar. To edit the **Listen Port** number: Update IPtables on your QRadar Console or Event Collector with the new UDP Multiline Syslog port number. For more information, see "Configuring IPtables for UDP Multiline Syslog events" on page 1292. 1. In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events. 2. Click **Save**. The port update is complete and event collection starts on the new port number.
Message ID Pattern	Type the regular expression (regex) that is needed to filter the event payload messages. All matching events are included when processing Open LDAP events. The following regular expression is suggested for Open LDAP events: `conn=(\d+)` For example, Open LDAP starts connection messages with the word *conn*, followed by the rest of the event payload. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/

For a complete list of UDP Multiline Syslog protocol parameters and their values, see "UDP multiline syslog protocol configuration options" on page 233.

Related tasks

Adding a log source

Configuring IPtables for UDP Multiline Syslog events

To collect UDP Multiline Syslog events in IBM QRadar, if you are unable to send the events directly to the standard UDP Multiline port of 517 or any other available port that is not already in use by QRadar, then you must redirect events from port 514 to the default port 517 or your chosen alternate port by using IPTables as outlined below. You must configure IPtables on your QRadar Console or for each QRadar Event Collector that receives UDP Multiline Syslog events from an Open LDAP server, and then complete the configuration for each Open LDAP server IP address that you want to receive logs from.

Before you begin

Important: Complete this configuration method only if you can't send UDP Multiline Syslog events directly to the chosen UDP Multiline port on QRadar from your Open LDAP server, and you are restricted to only sending to the standard syslog port 514.

Procedure

1. Using SSH, log in to QRadar as the root user.

   Login: <*root*>

   Password: <*password*>
2. Type the following command to edit the IPtables file:

   `vi /opt/qradar/conf/iptables-nat.post`

   The IPtables NAT configuration file is displayed.
3. Type the following command to instruct QRadar to redirect syslog events from UDP port 514 to UDP port 517:

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>
   ```

   Where:

   <*IP address*> is the IP address of your Open LDAP server.

   <*New port*> is the port number that is configured in the UDP Multiline protocol for Open LDAP.

   You must include a redirect for each Open LDAP IP address that sends events to your QRadar Console or Event Collector. Example:

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s <IP_address>
   ```
4. Save your IPtables NAT configuration.

   You are now ready to configure IPtables on your QRadar Console or Event Collector to accept events from your Open LDAP servers.
5. Type the following command to edit the IPtables file:

   `vi /opt/qradar/conf/iptables.post`

   The IPtables configuration file is displayed.
6. Type the following command to instruct QRadar to allow communication from your Open LDAP servers:

   ```
   -I QChain 1 -m udp -p udp --src <IP_address> --dport <New port> -j ACCEPT
   ```

   Where:

   <*IP address*> is the IP address of your Open LDAP server.

   <*New port*> is the port number that is configured in the UDP Multiline protocol for Open LDAP.

   You must include a redirect for each Open LDAP IP address that sends events to your QRadar Console or Event Collector. Example:

   ```
   -I QChain 1 -m udp -p udp --src <IP_address> --dport 517 -j ACCEPT
   ```
7. Type the following command to update IPtables in QRadar:

   `./opt/qradar/bin/iptables_update.pl`

Example

If you need to configure another QRadar Console or Event Collector that receives syslog events from an Open LDAP server, repeat these steps.

What to do next

Configure your Open LDAP server to forward events to QRadar.

Configuring event forwarding for Open LDAP

Configure syslog event forwarding for Open LDAP:

Procedure

1. Log in to the command line interface for your Open LDAP server.
2. Edit the following file:

   `/etc/syslog.conf`
3. Add the following information to the syslog configuration file:

   `<facility>@<IP address>`

   Where:

   <facility> is the syslog facility, for example local4.

   <IP address> is the IP address of your QRadar Console or Event Collector.

   For example,

   ```
   #Logging for SLAPD local4.debug /var/log/messages local4.debug @<IP_address>
   ```

   Note: If your Open LDAP server stores event messages in a directory other than `/var/log/messages`, you must edit the directory path.
4. Save the syslog configuration file.
5. Type the following command to restart the syslog service:

   `/etc/init.d/syslog restart`

   The configuration for Open LDAP is complete. UDP Multiline Syslog events that are forwarded to QRadar are displayed on the **Log Activity** tab.

Configuring QRadar for users to use OP code instead of connection number

By default, Open LDAP events are combined on the operation code. If you want to change the way that IBM QRadar maps events, you can use the DSM Editor to combine events on connection number.

Procedure

1. Click the **Admin** tab.
2. In the **Data Sources** section, click **DSM Editor**.
3. From the **Select Log Source Type** window, select **Open LDAP Software** from the list, and click **Select**.
4. On the **Configuration** tab, set **Display DSM Parameters Configuration** to **on**.
5. From the **Event Collector** list, select the event collector for the log source.
6. Set **Allow User to use OP code rather than Connection number** to **on**.
7. Click **Save** and close out the DSM Editor.

Chapter 117. Open Source SNORT

The Open Source SNORT DSM for IBM QRadar records all relevant SNORT events using syslog.

The SourceFire VRT certified rules for registered SNORT users are supported. Rule sets for Bleeding Edge, Emerging Threat, and other vendor rule sets might not be fully supported by the Open Source SNORT DSM.

Configuring Open Source SNORT

To configure syslog on an Open Source SNORT device:

About this task

The following procedure applies to a system that runs Red Hat Enterprise. The following procedures can vary for other operating systems.

Procedure

1. Configure SNORT on a remote system.
2. Open the `snort.conf` file.
3. Uncomment the following line:

   ```
   output alert_syslog:LOG_AUTH LOG_INFO
   ```
4. Save and exit the file.
5. Open the following file:

   ```
   /etc/init.d/snortd
   ```
6. Add a `-s` to the following lines, as shown in the example:

   ```
   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE -i $i -s -u $USER -g
   $GROUP $CONF -i $LOGIR/$i $PASS_FIRST
   ```

   ```
   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE $INTERFACE -s -u $USER -g
   $GROUP $CONF -i $LOGDIR
   ```
7. Save and exit the file.
8. Restart SNORT by typing the following command:

   ```
   /etc/init.d/snortd restart
   ```
9. Open the `syslog.conf` file.
10. Update the file to reflect the following code:

    `auth.info@<`*`IP Address`*`>`

    Where <*IP Address*> is the system to which you want logs sent.
11. Save and exit the file.
12. Restart syslog:

    ```
    /etc/init.d/syslog restart
    ```

What to do next

You can now configure the log source in QRadar.

Syslog log source parameters for Open Source SNORT

If QRadar does not automatically detect the log source, add a Open Source SNORT log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Open Source SNORT:

Table 835. Syslog log source parameters for the Open Source SNORT DSM

Parameter	Value
Log Source type	Open Source IDS
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for your Open Source SNORT events.

Related tasks

Adding a log source

Chapter 118. OpenStack

The IBM QRadar DSM for OpenStack collects event logs from your OpenStack device.

The following table identifies the specifications for the OpenStack DSM:

Table 836. OpenStack DSM specifications

Specification	**Value**
Manufacturer	OpenStack
DSM name	OpenStack
RPM file name	`DSM-OpenStackCeilometer-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V2015.1
Protocol	HTTP Receiver
Recorded event types	Audit event
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	OpenStack website (http://www.openstack.org/)

To send events from OpenStack to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - PROTOCOL-HTTPReceiver RPM
   - OpenStack DSM RPM
2. Add an OpenStack log source on the QRadar Console. The following table describes the parameters that are required to collect OpenStack events:

   Table 837. OpenStack log source parameters

Parameter	**Value**
Log Source type	**OpenStack**
Log Source Identifier	The IP address of the OpenStack server, and not the host name.
Protocol Configuration	**HTTPReceiver**
Communication Type	**HTTP**
Listen Port	The port number that OpenStack uses to communicate with QRadar. **Important:** Do not use Port 514. Port 514 is used by the standard Syslog listener.
Message Pattern	`^\{"typeURI`
3. Configure your OpenStack device to communicate with QRadar.

The following table provides a sample event message for the OpenStack DSM:

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Table 838. OpenStack sample message supported by the OpenStack device

Event name	Low level category	Sample log message
Lists details for all servers	Read activity attempted	{"typeURI": "http://schemas .dmtf.org/cloud/audit/1.0/event", "eventTime": "2014-12-09T00:18:52. 063878+0000", "target": {"typeURI": "service/compute/servers/detail", "id": "openstack:xxxxxxxxxxxxxxxx xxxxxxxxxxxxxx", "name": "nova", "addresses": [{"url": "http:// <IP_address>:8774/v2/xxxxxxxxxxxxxxxx xxxxxxxxxxxxxxx", "name": "admin"}, {"url": "http://<IP_address>:8774/v2/ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx", "name": "private"}, {"url": "http: //<IP_address>:8774/v2/xxxxxxxxxxxxxx xxxxxxxxxxxxxxx", "name": "public"}]}, "observer": {"id": "target"}, "tags": ["correlation_ id?value=openstack:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx"], "eventType": "activity", "initiator": {"typeURI": "service/security/account/user", "name": "admin", "credential": {"token": "xxxx xxxxxxxx xxxx", "identity_status": "Confirmed"}, "host": {"agent": "python-novaclient", "address": "<IP_address>"}, "project_id": "openstack:xxxxxxxx xxxxxxxxxxxxxxxxxxxxxx", "id": "openstack:xxxxxxxxxxxxxxxxxxxx xxxxxxxxxx"}, "action": "read/list", "outcome": "pending", "id": "openstack:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx", {"typeURI": "http://schemas.dmtf.org/cloud/ audit/1.0/event", "eventTime": "2014-12-09T00:18:52.063878+0000", "target": {"typeURI": "service/compute/servers/detail", "id": "openstack:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx", "name": "nova", "addresses": [{"url": "http:// <IP_address>:8774/v2/ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx", "name": "admin"}, {"url": "http://<IP_address>:8774/v2/ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx", "name": "private"}, {"url": "http:// <IP_address>:8774/v2/ xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx", "name": "public"}]}, "observer": {"id": "target"}, "tags": ["correlation_id? value=openstack:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx"], "eventType": "activity", "initiator": {"typeURI": "service/security/ account/user", "name": "admin", "credential": {"token": "xxxx xxxxxxxx xxxx", "identity_status": "Confirmed"}, "host": {"agent": "python-novaclient", "address": "<IP_address>"}, "project_id": "openstack:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx", "id": "openstack:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"}, "action": "read/list", "outcome": "pending", "id": "openstack:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",

Related tasks

Configuring OpenStack to communicate with QRadar

Adding a log source

Configuring OpenStack to communicate with QRadar

To collect OpenStack events, you must configure your OpenStack device to allow connections from QRadar.

Important: OpenStack is an open source product with many different distributions that can be set up on many different operating systems. This procedure might vary in your environment.

Procedure

1. Log in to your OpenStack device.
2. Edit the `/etc/nova/api-paste.ini` file.
3. At the end of the file, add the following text:

```
[filter:audit] paste.filter_factory = pycadf.middleware.audit:AuditMiddleware.factory
audit_map_file = /etc/nova/api_audit_map.conf
```

4. Review the `[composite:openstack_compute_api_v2]` settings and verify that the values match the following sample:

```
[composite:openstack_compute_api_v2] use = call:nova.api.auth:pipeline_factory noauth =
faultwrap sizelimit noauth ratelimit osapi_compute_app_v2 keystone = faultwrap sizelimit
authtoken keystonecontext ratelimit audit osapi_compute_app_v2 keystone_nolimit = faultwrap
sizelimit authtoken keystonecontext audit osapi_compute_app_v2
```

5. Copy the `api_audit_map.conf` file to the `/etc/nova/` directory.
6. Restart the api service.

   The command to restart the API service depends on what operating system your OpenStack node is hosted on. On Redhat Enterprise Linux systems, the command is `service openstack-nova-api restart`.
7. Open the `entry_points.txt` file in the `egg-info` subdirectory of your OpenStack installation directory.

   For PackStack installations, the file path resembles the following path: `/usr/lib/python2.7/site-packages/ceilometer-2014.2-py2.7.egg-info/entry_points.txt`.
8. Add the http dispatcher to the `[ceilometer.dispatcher]` section.

```
[ceilometer.dispatcher] file = ceilometer.dispatcher.file:FileDispatcher
database = ceilometer.dispatcher.database:DatabaseDispatcher http =
ceilometer.dispatcher.http:HttpDispatcher
```

9. Copy the supplied `http.py` script to the dispatcher subdirectory of the Ceilometer installation directory.

   The exact location depends on your operating system and OpenStack distribution. On the Redhat Enterprise Linux Distribution of OpenStack, the directory is `/usr/lib/python2.7/site-packages/ceilometer/dispatcher/`.
10. Edit the `/etc/ceilometer/ceilometer.conf` file.
11. Under the `[default]` section, add `dispatcher=http`.
12. At the bottom of the file, add this section:

```
[dispatcher_http] target = http://<QRadar-IP>:<QRadar-Port> cadf_only = True
```

    Use the port that you configured for OpenStack when you created the log source on your QRadar system.
13. Restart the ceilometer collector and notification services.

The command to restart the ceilometer collector and notification services depends on what operating system your OpenStack device is hosted on. On devices that use the Redhat Enterprise Linux operating system, use the following commands:

```
service openstack-ceilometer-collector restart
```

```
service openstack-ceilometer-notification restart
```

Chapter 119. Oracle

IBM QRadar supports a number of Oracle DSMs.

Oracle Acme Packet Session Border Controller

You can use IBM QRadar to collect events from Oracle Acme Packet Session Border Controller (SBC) installations in your network.

The Oracle Acme Packet SBC installations generate events from syslog and SNMP traps. SNMP trap events are converted to syslog and all events are forwarded to QRadar over syslog. QRadar does not automatically discover syslog events that are forwarded from Oracle Communications SBC. QRadar supports syslog events from Oracle Acme Packet SBC V6.2 and later.

To collect Oracle Acme Packet SBC events, you must complete the following tasks:

1. On your QRadar system, configure a log source with the Oracle Acme Packet Session Border Controller DSM.
2. On your Oracle Acme Packet SBC installation, enable SNMP and configure the destination IP address for syslog events.
3. On your Oracle Acme Packet SBC installation, enable syslog settings on the media-manager object.
4. Restart your Oracle Acme Packet SBC installation.
5. Optional. Ensure that firewall rules do not block syslog communication between your Oracle Acme Packet SBC installation and the QRadar Console or managed host that collects syslog events.

Supported Oracle Acme Packet event types that are logged by IBM QRadar

The Oracle Acme Packet SBC DSM for QRadar can collect syslog events from the authorization and the system monitor event categories.

Each event category can contain low-level events that describe the action that is taken within the event category. For example, authorization events can have low-level categories of `login success` or `login failed`.

Syslog log source parameters for Oracle Acme Packet SBC

If QRadar does not automatically detect the log source, add a Oracle Acme Packet SBC log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Oracle Acme Packet SBC:

Table 839. Syslog log source parameters for the Oracle Acme Packet SBC DSM

Parameter	Value
`Log Source type`	Oracle Acme Packet SBC
`Protocol Configuration`	Syslog
`Log Source Identifier`	Type the IP address or host name as an identifier for events from your Oracle Acme Packet SBC installation. The log source identifier must be unique value.

Related tasks

Adding a log source

Configuring SNMP to syslog conversion on Oracle Acme Packet SBC

To collect events in a format compatible with IBM QRadar, you must enable SNMP to syslog conversion and configure a syslog destination.

Procedure

1. Use SSH to log in to the command-line interface of your Oracle Acme Packet SBC installation, as an administrator.
2. Type the following command to start the configuration mode:

   ```
   config t
   ```
3. Type the following commands to start the system configuration:

   ```
   (configure)# system (system)# (system)# system-config (system-config)# sel
   ```

   The **sel** command is required to select a single-instance of the system configuration object.
4. Type the following commands to configure your QRadar system as a syslog destination:

   ```
   (system-config)# syslog-servers (syslog-config)# address <QRadar IP address>
   (syslog-config)# done
   ```
5. Type the following commands to enable SNMP traps and syslog conversion for SNMP trap notifications:

   ```
   (system-config)# enable-snmp-auth-traps enabled (system-config)# enable-snmp-syslog-notify
   enabled (system-config)# enable-snmp-monitor-traps enabled (system-config)# ids-syslog-
   facility 4 (system-config)# done
   ```
6. Type the following commands to return to configuration mode:

   ```
   (system-config)# exit (system)# exit (configure)#
   ```

Enabling syslog settings on the media manager object

The media-manager object configuration enables syslog notifications when the Intrusion Detection System (IDS) completes an action on an IP address. The available action for the event might depend on your firmware version.

Procedure

1. Type the following command to list the firmware version for your Oracle Acme Packet SBC installation:

   ```
   (configure)# show ver

   ACME Net-Net OSVM Firmware SCZ 6.3.9 MR-2 Patch 2 (Build 465) Build
   Date=03/12/13
   ```

   You may see underlined text which shows the major and minor version number for the firmware.
2. Type the following commands to configure the media-manager object:

   ```
   (configure)# media-manager (media-manager)# (media-manager)# media-manager
   (media-manager)# sel (media-manager-config)#
   ```

   The **sel** command is used to select a single-instance of the media-manager object.
3. Type the following command to enable syslog messages when an IP is demoted by the Intrusion Detection System (IDS) to the denied queue.

   ```
   (media-manager-config)# syslog-on-demote-to-deny enabled
   ```
4. For firmware version C6.3.0 and later, type the following command to enable syslog message when sessions are rejected.

```
(media-manager-config)# syslog-on-call-reject enabled
```

5. For firmware version C6.4.0 and later, type the following command to enable syslog messages when an IP is demoted to the untrusted queue

   ```
   (media-manager-config)# syslog-on-demote-to-untrusted enabled
   ```

6. Type the following commands to return to configuration mode:

   ```
   (media-manager-config)# done (media-manager-config)# exit (media-manager)#
   exit (configure)# exit
   ```

7. Type the following commands to save and activate the configuration:

   ```
   # save Save complete # activate
   ```

8. Type `reboot` to restart your Oracle Acme Packet SBC installation.

   After the system restarts, events are forwarded to IBM QRadar and displayed on the **Log Activity** tab.

Oracle Audit Vault

The IBM QRadar DSM for Oracle Audit Vault collects events from an Oracle Audit Vault server.

The following table describes the specifications for the Oracle Audit Vault DSM:

Table 840. Oracle Audit Vault DSM specifications

Specification	**Value**
Manufacturer	Oracle
DSM name	Oracle Audit Vault
RPM file name	`DSM-OracleAuditvault-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	10.3 and 12.2
Protocol	JDBC
Event format	name-value pair (NVP)
Recorded event types	All audit records from the AVSYS.AV$ALERT_STORE table for V10.3, or from the custom AVSYS.AV_ALERT_STORE_V view for V12.2. For more information about audit records, see Configuring Oracle Audit Vault to communicate with QRadar.
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Oracle website (https://www.oracle.com/index.html)

To integrate Oracle Audit Vault with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:

   - JDBC Protocol RPM
   - DSMCommon RPM

- Oracle Audit Vault DSM RPM

2. Obtain the database information for your Oracle Audit Vault server and then configure your Oracle Audit Vault database to allow incoming TCP connections.
3. For each instance of Oracle Audit Vault, add an Oracle Audit Vault log source on the QRadar Event Collector. The following table describes the parameters that require specific values to collect events from Oracle Audit Vault:

Table 841. Oracle Audit Vault JDBC log source parameters

Parameter	Value
Log Source type	**Oracle Audit Vault**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	**Oracle**
Database Name	The name of the Oracle Audit Vault database.
IP or Hostname	The IP address or host name of the Oracle Audit Vault server.
Port	The port from where the Oracle Audit Vault database is listening.
Username	Any user with the AV_AUDITOR permission. For example, AVAUDITOR.
Password	The password for the database user.
Predefined Query	None
Table Name	For Oracle Audit Vault Version 10.3, the **Table Name** value is AVSYS.AV$ALERT_STORE. For Oracle Audit Vault Version 12.2, the **Table Name** value is AVSYS.AV_ALERT_STORE_V.
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**.

Table 841. Oracle Audit Vault JDBC log source parameters (continued)	
Parameter	**Value**
Compare Field	For Oracle Audit Vault Version 10.3, the **Compare Field** value is `ALERT_SEQUENCE` For Oracle Audit Vault Version 12.2, the **Compare Field** value is `RECORD_ID`.
Use Prepared Statements	You must select the **Use Prepared Statements** option.
Start Date and Time (Optional)	The initial date and time for the JDBC retrieval.
Use Oracle Encryption	*Oracle Encryption and Data Integrity settings* is also known as *Oracle Advanced Security*. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.

For more information about configuring JDBC protocol parameters, see c_logsource_JDBCprotocol.dita.

4. Verify that QRadar is configured correctly.

   The following table shows a sample parsed audit event message from Oracle Audit Vault:

   Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Table 842. Oracle Audit Vault sample message

Event name	Low level category	Sample log message
LOGON-success	3075	ALERT_SEQUENCE: "25" AV_ALERT_TIME: "2010-01- 11 13:02:13.30702" ACTUAL_ALERT_TIME: "2010-01-11 12:19:36.0" TIME_CLEARED: "null" ALERT_NAME: "testing2" TARGET_OWNER: "null" TARGET_OBJECT: "null" ASSOCIATED_OBJECT_OW NER: "null" ASSOCIATED_OBJECT_NA ME: "null" ALERT_SEVERITY: "1" CLIENT_HOST: "host.domain.lab" CLIENT_HOSTIP: "<client_host_IP_address>" SOURCE_HOST: "<source_host_IP_address>" SOURCE_HOSTIP: "<source_host_IP_address>" PROCESS#: "3428" OSUSER_NAME: "null" USERNAME: "<os_user_name>" INSTANCE_NAME: "null" INSTANCE_NUMBER: "null" EVENT_STATUS: "0" CONTEXTID: "1561" SUB_CONTEXTID: "null" PARENT_CONTEXTID: "null" SOURCE_NAME: "XE" RECORD_ID: "23960" MSG_NUMBER: "0" CAT_ID: "2" EVENT_ID: "95" MSG_ARG_1: "null" MSG_ARG2: "null" MSG_ARG3: "null" MSG_ARG4: "null" MSG_ARG5: "null" ALERT_SEQUENCE: "25" AV_ALERT_TIME: "2010-01-11 13:02:13.30702" ACTUAL_ALERT_TIME: "2010-01-11 12:19:36.0" TIME_CLEARED: "null" ALERT_NAME: "testing2" TARGET_OWNER: "null" TARGET_OBJECT: "null" ASSOCIATED_OBJECT_OWNER: "null" ASSOCIATED_OBJECT_NAME: "null" ALERT_SEVERITY: "1" CLIENT_HOST: "host.domain.lab" CLIENT_HOSTIP: "<client_host_IP_address>" SOURCE_HOST: "<source_host_IP_address>" SOURCE_HOSTIP: "<source_host_IP_address>" PROCESS#: "3428" OSUSER_NAME: "null" USERNAME: "<os_user_name>" INSTANCE_NAME: "null" INSTANCE_NUMBER: "null" EVENT_STATUS: "0" CONTEXTID: "1561" SUB_CONTEXTID: "null" PARENT_CONTEXTID: "null" SOURCE_NAME: "XE" RECORD_ID: "23960" MSG_NUMBER: "0" CAT_ID: "2" EVENT_ID: "95" MSG_ARG_1: "null" MSG_ARG2: "null" MSG_ARG3: "null" MSG_ARG4: "null" MSG_ARG5: "null"

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

"Configuring Oracle Audit Vault to communicate with QRadar" on page 1307

If you are using Oracle Audit Vault V12.2, you must create a database view. If you are using Oracle Audit Vault V10.3, no further configuration is required.

Configuring Oracle Audit Vault to communicate with QRadar

If you are using Oracle Audit Vault V12.2, you must create a database view. If you are using Oracle Audit Vault V10.3, no further configuration is required.

Procedure

1. Log in to your Oracle Audit Vault V12.2 database as the AVSYS user.
2. To create the database view, type the following query:

```
create or replace view AVSYS.AV_ALERT_STORE_V as select
RECORD_ID, USER_NAME, SECURED_TARGET_ID, SECURED_TARGET_NAME,
SECURED_TARGET_TYPE, EVENT_TIME, OSUSER_NAME, COMMAND_CLASS,
nvl(to_number(decode(EVENT_STATUS,'SUCCESS','0','FAILURE','1','1')),1)
EVENT_STATUS, EVENT_NAME EVENT_ID, nvl(ERROR_CODE,0) ERROR_CODE,
ERROR_MESSAGE, AV_TIME, TARGET_TYPE, TARGET_OBJECT, TARGET_OWNER,
CLIENT_HOST_NAME, CLIENT_IP, AUDIT_TRAIL_ID, MONITORING_POINT_ID, MARKER,
ALERT_RAISED, ACTION_TAKEN, NETWORK_CONNECTION, LOGFILE_ID, SERVICE_NAME,
POLICY_NAME, THREAT_SEVERITY, LOG_CAUSE, CLUSTER_ID, CLUSTER_TYPE,
GRAMMAR_VERSION, CLIENT_PROGRAM, COMMAND_TEXT, COMMAND_PARAM, EXTENSION,
SECURED_TARGET_CLASS, LOCATION, TERMINAL, CLIENT_ID from avsys.EVENT_LOG el
where el.alert_raised = 1;
```

3. To allow a user that has AV_AUDITOR permission to read the view that you created, type the following query:

```
grant select on AVSYS.AV_ALERT_STORE_V to AV_AUDITOR;
```

Oracle BEA WebLogic

The Oracle BEA WebLogic DSM allows IBM QRadar to retrieve archived server logs and audit logs from any remote host, such as your Oracle BEA WebLogic server.

About this task

QRadar uses the log file protocol to retrieve events from your Oracle BEA WebLogic server and provides information on application events that occur in your domain or on a single server.

QRadar supports Oracle events by using the Log File protocol from Oracle BEA Weblogic v12.2.1.3.0.

To integrate Oracle BEA WebLogic events, take the following steps:

1. Enable auditing on your Oracle BEA WebLogic server.
2. Configure *domain logging* on your Oracle BEA WebLogic server.
3. Configure *application logging* on your Oracle BEA WebLogic server.
4. Configure an audit provider for Oracle BEA WebLogic.
5. Configure QRadar to retrieve log files from Oracle BEA WebLogic.

Enabling event logs

By default, Oracle BEA WebLogic does not enable event logging.

About this task

To enable event logging on your Oracle WebLogic console:

Procedure

1. Log in to your Oracle WebLogic console user interface.
2. Select **Domain** > **Configuration** > **General**.
3. Click **Advanced**.
4. From the **Configuration Audit Type** list, select **Change Log and Audit**.
5. Click **Save**.

What to do next

You can now configure the collection of domain logs for Oracle BEA WebLogic.

Configuring domain logging

Oracle BEA WebLogic supports multiple instances. Event messages from instances are collected in a single domain-wide log for the Oracle BEA WebLogic server.

About this task

To configure the log file for the domain:

Procedure

1. From your Oracle WebLogic console, select **Domain** > **Configuration** > **Logging**.
2. From the **Log file name** parameter, type the directory path and file name for the domain log.

   For example, `OracleDomain.log`.
3. Optional: Configure any additional domain log file rotation parameters.
4. Click **Save**.

What to do next

You can now configure *application logging* for the server.

Configuring application logging

You can configure application logging for Oracle BEA WebLogic:

Procedure

1. From your Oracle WebLogic console, select **Server** > **Logging** > **General**.
2. From the **Log file name** parameter, type the directory path and file name for the application log.

   For example, `OracleDomain.log`.
3. Optional: Configure any additional application log file rotation parameters.
4. Click **Save**.

What to do next

You can now configure an audit provider for Oracle BEA WebLogic.

Configuring an audit provider

You can configure an audit provider:

Procedure

1. Select **Security Realms** > **Realm Name** > **Providers** > **Auditing**.

2. Click **New**.
3. Configure an audit provider by typing a name for the audit provider that you are creating.
4. From the **Type** list, select **DefaultAuditor**.
5. Click **OK**.

   The **Settings** window is displayed.
6. Click the auditing provider that you created in "Configuring an audit provider" on page 1308.
7. Click the **Provider Specific** tab.
8. Add any **Active Context Handler Enteries** that are needed.
9. From the **Severity** list, select **Information**.
10. Click **Save**.

What to do next

You can now configure IBM QRadar to pull log files from Oracle BEA WebLogic.

Log file log source parameters for Oracle BEA WebLogic

If QRadar does not automatically detect the log source, add a Oracle BEA WebLogic log source on the QRadar Console by using the Log file protocol.

When using the Log file protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect log file events from Oracle BEA WebLogic:

Table 843. Log file log source parameters for the Oracle BEA WebLogic DSM

Parameter	Value
Log Source type	Oracle BEA WebLogic
Protocol Configuration	Log file
Log Source Identifier	Type the IP address or host name for the log source. This value must match the value that is configured in the **Remote Host IP or Hostname** parameter. The log source identifier must be unique for the log source type.
Event Generator	From the **Event Generator** list, select **Oracle BEA WebLogic**.

For a complete list of Log file protocol parameters and their values, see "Log File protocol configuration options" on page 155.

Related tasks

Adding a log source

Oracle BEA WebLogic sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Oracle BEA WebLogic sample messages when you use the Log File protocol

Sample 1: The following sample event shows that the server has successfully established a connection with the domain level diagnostic service.

```
####<Oct 15, 2012 4:27:41 PM MST> <Notice> <Log Management> <qradarTesting.qradar.test>
<sgss_ManagedServer_1> <[STANDBY] ExecuteThread: &apos;1&apos; for queue:
&apos;weblogic.kernel.Default (self-tuning)&apos;> <<WLS Kernel>> <> <> <1350343661416>
<BEA-170027> <The Server has established connection with the Domain level Diagnostic Service
successfully.>
```

```
####<Oct 15, 2012 4:27:41 PM MST> <Notice> <Log Management> <qradarTesting.qradar.test>
<sgss_ManagedServer_1> <[STANDBY] ExecuteThread: &apos;1&apos; for queue:
&apos;weblogic.kernel.Default (self-tuning)&apos;> <<WLS Kernel>> <> <> <1350343661416>
<BEA-170027> <The Server has established connection with the Domain level Diagnostic Service
successfully.>
```

Sample 2: The following sample event shows that the NetUIx container is initializing.

```
####<Dec 17, 2012 1:51:34 PM MST> <Info> <netuix> <qradarTesting.qradar.test> <AdminServer>
<[ACTIVE] ExecuteThread: &apos;0&apos; for queue: &apos;weblogic.kernel.Default (self-
tuning)&apos;> <<anonymous>> <> <> <1355777494726> <BEA-423101> <[consolehelp] Initializing the
NetUIx container>
```

```
####<Dec 17, 2012 1:51:34 PM MST> <Info> <netuix> <qradarTesting.qradar.test> <AdminServer>
<[ACTIVE] ExecuteThread: &apos;0&apos; for queue: &apos;weblogic.kernel.Default (self-
tuning)&apos;> <<anonymous>> <> <> <1355777494726> <BEA-423101> <[consolehelp] Initializing the
NetUIx container>
```

Sample 3: The following sample event shows that a node manager command has failed.

```
####<Oct 15, 2012 4:19:42 PM MST> <Error> <NodeManager> <qradarTesting.qradar.test>
<AdminServer> <[ACTIVE] ExecuteThread: &apos;0&apos; for queue: &apos;weblogic.kernel.Default
(self-tuning)&apos;> <weblogic> <> <> <1350343182323> <BEA-300033> <Could not execute command
"getVersion" on the node manager. Reason: "Connection refused. Could not connect to NodeManager.
Check that it is running at localhost:5556.".>
```

```
####<Oct 15, 2012 4:19:42 PM MST> <Error> <NodeManager> <qradarTesting.qradar.test>
<AdminServer> <[ACTIVE] ExecuteThread: &apos;0&apos; for queue: &apos;weblogic.kernel.Default
(self-tuning)&apos;> <weblogic> <> <> <1350343182323> <BEA-300033> <Could not execute command
"getVersion" on the node manager. Reason: "Connection refused. Could not connect to
NodeManager. Check that it is running at localhost:5556.".>
```

Oracle RDBMS Audit Record

The IBM QRadar DSM for Oracle RDBMS Audit Record collects logs from an Oracle database.

The following table describes the specifications for the Oracle RDBMS Audit Record DSM:

Table 844. Oracle RDBMS Audit Record DSM specifications

Specification	**Value**
Manufacturer	Oracle
DSM name	Oracle RDBMS Audit Record
RPM file name	DSM-OracleDbAudit-*QRadar_version-build_number*.noarch.rpm
Supported versions	9i, 10g, 11g, 12c (includes unified auditing)
Protocol	JDBC, Syslog
Event format	Name-Value Pair
Recorded event types	Audit records
Automatically discovered?	Yes
Includes identity?	Yes

Table 844. Oracle RDBMS Audit Record DSM specifications (continued)	
Specification	**Value**
Includes custom properties?	No
More information	Oracle website (https://www.oracle.com)

To integrate Oracle RDBMS Audit Record with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol JDBC RPM
   - DSMCommon RPM
   - Oracle RDBMS Audit Record DSM RPM
2. Configure your Oracle RDBMS Audit Record device to write audit logs.
3. If QRadar does not automatically detect the log source, add an Oracle RDBMS Audit Record log source on the QRadar Console. The following tables describe the parameters that require specific values to collect audit events from Oracle RDBMS Audit Record:

Table 845. Oracle RDBMS Audit Record Syslog log source parameters	
Parameter	**Value**
Log Source type	Oracle RDBMS Audit Record
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

Table 846. Oracle RDBMS Audit Record JDBC log source parameters	
Parameter	**Value**
Log Source type	**Oracle RDBMS Audit Record**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	**Oracle**
Database Name	The name of the database from where you collect audit logs.
IP or Hostname	The IP or host name of the Oracle database.

Table 846. Oracle RDBMS Audit Record JDBC log source parameters (continued)

Parameter	Value
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix - 9088 • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the **Port** field blank.
Username	A user account to connect to the database. The user must have **AUDIT_ADMIN** or **AUDIT_VIEWER** permissions.
Password	The password that is required to connect to the database.
Predefined Query	Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the **none** option.
Table Name	The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**.
Compare Field	For Oracle 9i or Oracle 10g Release 1, type `Qradar_time`. For Oracle 10g Release 2, Oracle 11g, or Oracle 12c (non-unified auditing), type `extended_timestamp`. For Oracle 12c (unified auditing), type `event_timestamp`.

Table 846. Oracle RDBMS Audit Record JDBC log source parameters (continued)	
Parameter	**Value**
Use Oracle Encryption	*Oracle Encryption and Data Integrity settings* is also known as *Oracle Advanced Security*. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.

For more information about configuring JDBC parameters, see JDBC protocol configuration options.

4. Verify that QRadar is configured correctly.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

The following table shows a sample normalized event message from Oracle RDBMS Audit Record:

Table 847. Oracle RDBMS Audit Record sample message		
Event name	**Low level category**	**Sample log message**
SELECT succeeded	System Action Allow	OS_USERNAME: "os_username" USERNAME: "username" USERHOST: "userhost" TERMINAL: "terminal" TIMESTAMP: "2017-04-05 21:04:02.0" OWNER: "owner" OBJ_NAME: "PARTIAL_ALERT" ACTION: "3" ACTION_NAME: "SELECT" NEW_OWNER: "null" NEW_NAME: "null" OBJ_PRIVILEGE: "null" SYS_PRIVILEGE: "null" ADMIN_OPTION: "null" GRANTEE: "null" AUDIT_OPTION: "null" SES_ACTIONS: "null" LOGOFF_TIME: "null" LOGOFF_LREAD: "null" LOGOFF_PREAD: "null" LOGOFF_LWRITE: "null" LOGOFF_DLOCK: "null" COMMENT_TEXT: "null" SESSIONID: "xxxxxx" ENTRYID: "2" STATEMENTID: "2" RETURNCODE: "0" PRIV_USED: "null" CLIENT_ID: "null" ECONTEXT_ID: "null" SESSION_CPU: "null" EXTENDED_TIMESTAMP: "2017-04-05 21:04:02.318133 America/Halifax" PROXY_SESSIONID: "null" GLOBAL_UID: "null" INSTANCE_NUMBER: "0" OS_PROCESS: "9276" TRANSACTIONID: "null" SCN: "3842851" SQL_BIND: "null" SQL_TEXT: "null" OBJ_EDITION_NAME: "null" DBID: "xxxxxxxxxx" OS_USERNAME: "os_username" USERNAME: "username" USERHOST: "userhost" TERMINAL: "terminal" TIMESTAMP: "2017-04-05 21:04:02.0" OWNER: "owner" OBJ_NAME: "PARTIAL_ALERT" ACTION: "3" ACTION_NAME: "SELECT" NEW_OWNER: "null" NEW_NAME: "null" OBJ_PRIVILEGE: "null" SYS_PRIVILEGE: "null" ADMIN_OPTION: "null" GRANTEE: "null" AUDIT_OPTION: "null" SES_ACTIONS: "null" LOGOFF_TIME: "null" LOGOFF_LREAD: "null" LOGOFF_PREAD: "null" LOGOFF_LWRITE: "null" LOGOFF_DLOCK: "null" COMMENT_TEXT: "null" SESSIONID: "xxxxxx" ENTRYID: "2" STATEMENTID: "2" RETURNCODE: "0" PRIV_USED: "null" CLIENT_ID: "null" ECONTEXT_ID: "null" SESSION_CPU: "null" EXTENDED_TIMESTAMP: "2017-04-05 21:04:02.318133 America/Halifax" PROXY_SESSIONID: "null" GLOBAL_UID: "null" INSTANCE_NUMBER: "0" OS_PROCESS: "9276" TRANSACTIONID: "null" SCN: "3842851" SQL_BIND: "null" SQL_TEXT: "null" OBJ_EDITION_NAME: "null" DBID: "xxxxxxxxxx"

Table 847. Oracle RDBMS Audit Record sample message (continued)

Event name	Low level category	Sample log message
AUDIT failed	Failed Configuration Modification	AUDIT_TYPE: "Standard" SESSIONID: "xxxxxxxxxx" PROXY_SESSIONID: "0" OS_USERNAME: "os_username" USERHOST: "userhost" TERMINAL: "terminal" INSTANCE_ID: "1" DBID: "xxxxxxxxxx" AUTHENTICATION_TYPE: "(TYPE=(DATABASE));" DBUSERNAME: "dbusername" DBPROXY_USERNAME: "null" EXTERNAL_USERID: "null" GLOBAL_USERID: "null" CLIENT_PROGRAM_NAME: "client_program_name" DBLINK_INFO: "null" XS_USER_NAME: "null" XS_SESSIONID: "00000000000000000000000000000000000000000000000000000000000000000000" ENTRY_ID: "3" STATEMENT_ID: "11" EVENT_TIMESTAMP: "2017-04-05 20:44:21.29604" ACTION_NAME: "AUDIT" RETURN_CODE: "1031" OS_PROCESS: "1749" TRANSACTION_ID: "0000000000000000" SCN: "3841187" EXECUTION_ID: "null" OBJECT_SCHEMA: "null" OBJECT_NAME: "null" SQL_TEXT: "audit all" SQL_BINDS: "null" APPLICATION_CONTEXTS: "null" CLIENT_IDENTIFIER: "null" NEW_SCHEMA: "null" NEW_NAME: "null" OBJECT_EDITION: "null" SYSTEM_PRIVILEGE_USED: "null" SYSTEM_PRIVILEGE: "null" AUDIT_OPTION: "CREATE SESSION" OBJECT_PRIVILEGES: "null" ROLE: "null" TARGET_USER: "null" EXCLUDED_USER: "null" EXCLUDED_SCHEMA: "null" EXCLUDED_OBJECT: "null" ADDITIONAL_INFO: "null" UNIFIED_AUDIT_POLICIES: "null" FGA_POLICY_NAME: "null" XS_INACTIVITY_TIMEOUT: "0" XS_ENTITY_TYPE: "null" XS_TARGET_PRINCIPAL_NAME: "null" XS_PROXY_USER_NAME: "null" XS_DATASEC_POLICY_NAME: "null" XS_SCHEMA_NAME: "null" XS_CALLBACK_EVENT_TYPE: "null" XS_PACKAGE_NAME: "null" XS_PROCEDURE_NAME: "null" XS_ENABLED_ROLE: "null" XS_COOKIE: "null" XS_NS_NAME: "null" XS_NS_ATTRIBUTE: "null" XS_NS_ATTRIBUTE_OLD_VAL: "null" XS_NS_ATTRIBUTE_NEW_VAL: "null" DV_ACTION_CODE: "0" DV_ACTION_NAME: "null" DV_EXTENDED_ACTION_CODE: "0" DV_GRANTEE: "null" DV_RETURN_CODE: "0" DV_ACTION_OBJECT_NAME: "null" DV_RULE_SET_NAME: "null" DV_COMMENT: "null" DV_FACTOR_CONTEXT: "null" DV_OBJECT_STATUS: "null" OLS_POLICY_NAME: "null" OLS_GRANTEE: "null" OLS_MAX_READ_LABEL: "null" OLS_MAX_WRITE_LABEL: "null" OLS_MIN_WRITE_LABEL: "null" OLS_PRIVILEGES_GRANTED: "null" OLS_PROGRAM_UNIT_NAME: "null" OLS_PRIVILEGES_USED: "null" OLS_STRING_LABEL: "null" OLS_LABEL_COMPONENT_TYPE: "null" OLS_LABEL_COMPONENT_NAME: "null" OLS_PARENT_GROUP_NAME: "null" OLS_OLD_VALUE: "null" OLS_NEW_VALUE: "null" RMAN_SESSION_RECID: "0" RMAN_SESSION_STAMP: "0" RMAN_OPERATION: "null" RMAN_OBJECT_TYPE: "null" RMAN_DEVICE_TYPE: "null" DP_TEXT_PARAMETERS1: "null" DP_BOOLEAN_PARAMETERS1: "null" DIRECT_PATH_NUM_COLUMNS_LOADED: "0"

Table 847. Oracle RDBMS Audit Record sample message (continued)

Event name	Low level category	Sample log message
		AUDIT_TYPE: "Standard" SESSIONID: "xxxxxxxxxx" PROXY_SESSIONID: "0" OS_USERNAME: "os_username" USERHOST: "userhost" TERMINAL: "terminal" INSTANCE_ID: "1" DBID: "xxxxxxxxxx" AUTHENTICATION_TYPE: "(TYPE=(DATABASE));" DBUSERNAME: "dbusername" DBPROXY_USERNAME: "null" EXTERNAL_USERID: "null" GLOBAL_USERID: "null" CLIENT_PROGRAM_NAME: "client_program_name" DBLINK_INFO: "null" XS_USER_NAME: "null" XS_SESSIONID: "00000000000000000000000000000000000000000000000000000000000000000000000000" ENTRY_ID: "3" STATEMENT_ID: "11" EVENT_TIMESTAMP: "2017-04-05 20:44:21.29604" ACTION_NAME: "AUDIT" RETURN_CODE: "1031" OS_PROCESS: "1749" TRANSACTION_ID: "0000000000000000" SCN: "3841187" EXECUTION_ID: "null" OBJECT_SCHEMA: "null" OBJECT_NAME: "null" SQL_TEXT: "audit all" SQL_BINDS: "null" APPLICATION_CONTEXTS: "null" CLIENT_IDENTIFIER: "null" NEW_SCHEMA: "null" NEW_NAME: "null" OBJECT_EDITION: "null" SYSTEM_PRIVILEGE_USED: "null" SYSTEM_PRIVILEGE: "null" AUDIT_OPTION: "CREATE SESSION" OBJECT_PRIVILEGES: "null" ROLE: "null" TARGET_USER: "null" EXCLUDED_USER: "null" EXCLUDED_SCHEMA: "null" EXCLUDED_OBJECT: "null" ADDITIONAL_INFO: "null" UNIFIED_AUDIT_POLICIES: "null" FGA_POLICY_NAME: "null" XS_INACTIVITY_TIMEOUT: "0" XS_ENTITY_TYPE: "null" XS_TARGET_PRINCIPAL_NAME: "null" XS_PROXY_USER_NAME: "null" XS_DATASEC_POLICY_NAME: "null" XS_SCHEMA_NAME: "null" XS_CALLBACK_EVENT_TYPE: "null" XS_PACKAGE_NAME: "null" XS_PROCEDURE_NAME: "null" XS_ENABLED_ROLE: "null" XS_COOKIE: "null" XS_NS_NAME: "null" XS_NS_ATTRIBUTE: "null" XS_NS_ATTRIBUTE_OLD_VAL: "null" XS_NS_ATTRIBUTE_NEW_VAL: "null" DV_ACTION_CODE: "0" DV_ACTION_NAME: "null" DV_EXTENDED_ACTION_CODE: "0" DV_GRANTEE: "null" DV_RETURN_CODE: "0" DV_ACTION_OBJECT_NAME: "null" DV_RULE_SET_NAME: "null" DV_COMMENT: "null" DV_FACTOR_CONTEXT: "null" DV_OBJECT_STATUS: "null" OLS_POLICY_NAME: "null" OLS_GRANTEE: "null" OLS_MAX_READ_LABEL: "null" OLS_MAX_WRITE_LABEL: "null" OLS_MIN_WRITE_LABEL: "null" OLS_PRIVILEGES_GRANTED: "null" OLS_PROGRAM_UNIT_NAME: "null" OLS_PRIVILEGES_USED: "null" OLS_STRING_LABEL: "null" OLS_LABEL_COMPONENT_TYPE: "null" OLS_LABEL_COMPONENT_NAME: "null" OLS_PARENT_GROUP_NAME: "null" OLS_OLD_VALUE: "null" OLS_NEW_VALUE: "null" RMAN_SESSION_RECID: "0" RMAN_SESSION_STAMP: "0" RMAN_OPERATION: "null" RMAN_OBJECT_TYPE: "null" RMAN_DEVICE_TYPE: "null" DP_TEXT_PARAMETERS1: "null" DP_BOOLEAN_PARAMETERS1: "null" DIRECT_PATH_NUM_COLUMNS_LOADED: "0"

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Enabling Unified Auditing in Oracle 12c

To enable Unified Auditing in Oracle 12c, you must shut down the Oracle database, stop the Oracle listener service and then restart the Oracle database and Oracle Listener service.

Before you begin

You must have the AUDIT_SYSTEM system privilege or the AUDIT_ADMIN role to complete the following steps.

Procedure

1. Shut down the Oracle database by connecting to the database with SQLplus, and then type the following command:

   ```
   shutdown immediate
   ```
2. Stop the Oracle listener service by typing the following command:

   ```
   lsnrctl stop
   ```
3. If applicable, stop the Enterprise Manager by typing the following commands:

   ```
   cd /u01/app/oracle/product/middleware/oms
   ```

   ```
   export OMS_HOME=/u01/app/oracle/product/middleware/oms
   ```

   ```
   $OMS_HOME/bin/emctl stop oms
   ```
4. Relink Oracle DB with the *uniaud* option by typing the following commands:

   ```
   cd $ORACLE_HOME/rdbms/lib
   ```

   ```
   make -f ins_rdbms.mk uniaud_on ioracle
   ```
5. Restart the Oracle database by connecting to the database with SQLplus, and then type the following command:

   ```
   startup
   ```
6. Restart the Oracle *listener* service by typing the following command:

   ```
   lsnrctl start
   ```
7. If applicable, restart the Enterprise Manager by typing the following commands:

   ```
   cd /u01/app/oracle/product/middleware/oms
   ```

   ```
   export OMS_HOME=/u01/app/oracle/product/middleware/oms
   ```

   ```
   $OMS_HOME/bin/emctl start oms
   ```
8. To verify that unified auditing is enabled, connect to the Oracle database with SQLplus, and then type the following command:

   ```
   select * from v$option where PARAMETER = 'Unified Auditing';
   ```

   Verify that the command returns one row with **`VALUE equal to "TRUE"`**.

Configuring an Oracle database server to send audit logs to QRadar

Configure your Oracle device to send audit logs to IBM QRadar.

Procedure

1. Log in to the Oracle host as an Oracle user.
2. Ensure that the *ORACLE_HOME* and *ORACLE_SID* environment variables are configured properly for your deployment.
3. Open the following file:

   ```
   ${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora
   ```

4. Choose one of the following options:
   a) For database audit trails, type the following command:

      ```
      *.audit_trail='DB'
      ```

   b) For syslog, type the following commands:

      ```
      *.audit_trail='os'
      ```

      ```
      *.audit_syslog_level='local0.info'
      ```

      You must ensure that the syslog daemon on the Oracle host is configured to forward the audit log to QRadar. For systems that run Red Hat Enterprise, the following line in the `/etc/syslog.conf` file affects the forwarding:

      `local0.info @ qradar.domain.tld`

      Where *qradar.domain.tld* is the hostname of QRadar that receives the events. The syslog configuration must be reloaded for the command to be recognized. On a system that runs Red Hat Enterprise, type the following line to reload the syslog configuration:

      ```
      kill -HUP /var/run/syslogd.pid
      ```

5. Save and exit the file.
6. To restart the database, connect to SQLplus and log in as sysdba:

   Example: `Enter user-name: sys as sysdba`
7. Shut down the database by typing the following line:

   ```
   shutdown immediate
   ```

8. Restart the database by typing the following line:

   ```
   startup
   ```

9. If you are using Oracle v9i or Oracle v10g Release 1, you must create a view that uses SQLplus to enable the QRadar integration. If you are using Oracle 10g Release 2 or later, you can skip this step:

   ```
   CREATE VIEW qradar_audit_view AS SELECT CAST(dba_audit_trail.timestamp AS TIMESTAMP) AS
   qradar_time, dba_audit_trail.* FROM dba_audit_trail;
   ```

   If you are using the JDBC protocol, when you configure the JDBC protocol within QRadar, use the following specific parameters:

   Table 848. Configuring log source parameters

Parameter Name	Oracle v9i or 10g Release 1 Values	Oracle v10g Release 2 and v11g Values
Table Name	QRadar_audit_view	dba_audit_trail
Select List	*	*
Compare Field	QRadar_time	extended_timestamp
Database Name	For all supported versions of Oracle, the **Database Name** must be the exact service name that is used by the Oracle *listener*. You can view the available service names by running the following command on the Oracle host: **`lsnrctl status`**	

   Note: Ensure that the database user that QRadar uses to query events from the audit log table has the appropriate permissions for the Table Name object.
10. You can now configure QRadar to receive events from an Oracle database: From the **Log Source Type** list, select the **Oracle RDBMS Audit Record** option.

Related tasks
"Adding a log source" on page 5

Oracle DB Listener

The Oracle Database Listener application stores logs on the database server.

To integrate IBM QRadar with Oracle DB Listener, select one of the following methods for event collection:

- "Oracle Database Listener log source parameters" on page 1318
- "Collecting Oracle database events by using Perl " on page 1318

Related tasks
"Adding a DSM" on page 4
"Adding a log source" on page 5

Oracle Database Listener log source parameters

If QRadar does not automatically detect the log source, add a Oracle Database Listener log source on the QRadar Console by using the Oracle Database Listener protocol.

When using the Oracle Database Listener protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect events from Oracle Database Listener:

Table 849. Oracle Database Listener log source parameters for the Oracle Database Listener DSM

Parameter	Value
Log Source type	Oracle Database Listener
Protocol Configuration	Oracle Database Listener
Log Source Identifier	Type the IP address or host name for the Oracle Database Listener log source.

For a complete list of Oracle Database Listener protocol parameters and their values, see "Oracle Database Listener protocol configuration options" on page 203.

Related tasks
Adding a log source

Collecting Oracle database events by using Perl

The Oracle Database Listener application stores logs on the database server. To forward these logs from the Oracle server to IBM QRadar, you must configure a Perl script on the Oracle server. The Perl script monitors the listener log file, combines any multi-line log entries in to a single log entry, and sends the logs, by using syslog (UDP), to QRadar.

About this task

Before the logs are sent to QRadar, they are processed and reformatted so that they are not forwarded line-by-line, as they are in the log file. All of the relevant information is retained.

Note: Perl scripts that are written for Oracle DB listener work on Linux/UNIX servers only. Windows Perl script is not supported. You must make sure Perl 5.8 is installed on the device that hosts the Oracle server.

To install and configure the Perl script:

Procedure

1. Go to the following website to download the files that you need:

   http://www.ibm.com/support
2. From the **Downloads** list, click **Fix Central**.
3. Click **Select product** tab.
4. Select **IBM Security** from the **Product Group** list.
5. Select **IBM Security QRadar SIEM** from the **Select from IBM Security** list.
6. Select the **Installed Version** of QRadar.
7. Select **Linux** from the **Platform** list and click **Continue**.
8. Select **Browse for fixes** and click **Continue**.
9. Select **Script**.
10. Click *<QRadar_version>*-oracle_dblistener_fwdr-*<version_number>*.pl.tar.gz to download the Oracle DB Listener Script.
11. Copy the Oracle DB Listener Script to the server that hosts the Oracle server.
12. Log in to the Oracle server by using an account that has read/write permissions for the `listener.log` file and the `/var/run` directory.
13. Extract the Oracle DB Listener Script file by typing the following command:

    `tar -xvzf oracle_dblistener_fwdr-`*`<version_number>`*`.pl.tar.gz`
14. Type the following command and include any additional command parameters to start monitoring the Oracle DB Listener log file:

    `oracle_dblistener_fwdr.pl -h <`*`IP address`*`> -t "tail -F <`*`absolute_path_to_listener_log`*`>/listener.log"`

    where *<IP address>* is the IP address of your QRadar Console or Event Collector, and *<absolute_path_to_listener_log>* is the absolute path of the listener log file on the Oracle server.

Table 850. Command parameters

Parameters	Description
-D	The **-D** parameter defines that the script is to run in the foreground. Default is to run as a daemon and log all internal messages to the local syslog service.
-t	The **-t** parameter defines that the command-line is used to tail the log file (monitors any new output from the listener). The location of the log file might be different across versions of the Oracle database. For examples, Oracle 9i: `<install_directory>/product/9.2/network/log/listener.log` Oracle 10g: `<install_directory>/product/10.2.0/db_1/network/log /listener.log` Oracle 11g: `<install_directory>/diag/tnslsnr/qaoracle11/listener /trace/listener.log`
-f	The **-f** parameter defines the **syslog facility.priority** to be included at the beginning of the log. If nothing is specified, `user.info` is used.

Table 850. Command parameters (continued)	
Parameters	**Description**
-g	The **-g** parameter defines the language pack file. For example, `./oracle_dblistener_fwdr.pl -h <IP_address> -g /root/OracleDBListener/languagepacks/localization.french -t "tail -f /root/smbtest/listener_vali.log"` This parameter is optional.
-H	The **-H** parameter defines the host name or IP address for the syslog header. It is suggested that is the IP address of the Oracle server on which the script is running.
-h	The **-h** parameter defines the receiving syslog host (the Event Collector host name or IP address that is used to receive the logs).
-p	The **-p** parameter defines the receiving UDP syslog port. If a port is not specified, 514 is used.
-r	The **-r** parameter defines the directory name where you want to create the `.pid file`. The default is `/var/run`. This parameter is ignored if **-D** is specified.
-l	The **-I** parameter defines the directory name where you want to create the lock file. The default is `/var/lock`. This parameter is ignored if **-D** is specified.

For example, to monitor the listener log on an Oracle 9i server with an IP address of 192.0.2.10 and forward events to QRadar with the IP address of 192.0.2.20, type the following code:

```
oracle_dblistener_fwdr.pl -t "tail -f <install_directory>/product/9.2/
network/log/listener.log" -f user.info -H 192.0.2.10 -h 192.0.2.20 -p 514
```

A sample log from this setup would appear as follows:

```
<14>Apr 14 13:23:37 192.0.2.10 AgentDevice=OracleDBListener
Command=SERVICE_UPDATE DeviceTime=18-AUG-2006 16:51:43 Status=0 SID=qora9
```

Note: The **kill** command can be used to stop the script if you need to reconfigure a script parameter or stop the script from sending events to QRadar. For example,

```
kill -QUIT `cat /var/run/oracle_dblistener_fwdr.pl.pid`
```

The example command uses the *backquote* character (`), which is located to the left of the number one on most keyboard layouts.

What to do next

You can now configure the Oracle Database Listener within QRadar.

Configuring the Oracle Database Listener within QRadar.

You can configure the Oracle Database Listener within IBM QRadar.

Procedure

1. From the **Log Source Type** list, select **Oracle Database Listener**.
2. From the **Protocol Configuration** list, select **syslog**.
3. In the **Log Source Identifier** field, type the IP address of the Oracle Database you specified using the -H option in “Collecting Oracle database events by using Perl ” on page 1318.

The configuration of the Oracle Database Listener protocol is complete. For more information on Oracle Database Listener, see your vendor documentation.

Oracle Directory Server overview

Oracle Directory Server is formerly known as Sun ONE LDAP.

Related concepts

"Sun ONE LDAP" on page 1491

Oracle Enterprise Manager

The IBM QRadar DSM for Oracle Enterprise Manager collects events from an Oracle Enterprise Manager device. The Real-time Monitoring Compliance feature of Oracle Enterprise Manager generates the events.

The following table lists the specifications for the Oracle Enterprise Manager DSM:

Table 851. Oracle Enterprise Manager DSM specifications

Specification	**Value**
Manufacturer	Oracle
DSM name	Oracle Enterprise Manager
RPM file name	`DSM-OracleEnterpriseManager-`*`QRadar_version-Buildbuild_number`*`.noarch.rpm`
Supported versions	Oracle Enterprise Manager Cloud Control 12c
Protocol	JDBC
Recorded event types	Audit Compliance
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Oracle Enterprise Manager (https://www.oracle.com/enterprise-manager/). The original format of the events are rows in an Oracle Enterprise Manager database view (`sysman.mgmt$ccc_all_observations`). QRadar polls this view for new rows and uses them to generate events. For more information, see Compliance Views (http://docs.oracle.com/cd/E24628_01/doc.121/e57277/ch5_complianceviews.htm#BABBIJAA)

To collect events from Oracle Enterprise Manager, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Oracle Enterprise Manager DSM RPM from the IBM Support Website onto your QRadar Console.
2. Ensure that the Oracle Enterprise Manager system is configured to accept connections from external devices.
3. Add an Oracle Enterprise Manager log source on the QRadar Console. The following table describes the parameters that require specific values for Oracle Enterprise Manager event collection:

Table 852. Oracle Enterprise Manager JDBC log source parameters	
Parameter	**Description**
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	Oracle Enterprise Manager
Protocol Configuration	JDBC
Database Type	Oracle
Database Name	The Service Name of Oracle Enterprise Manager database. To view the available service names, run the `lsnrctl status` command on the Oracle host.
IP or Hostname	The IP address or host name of the Oracle Enterprise Manager database server.
Port	The port that is used by the Oracle Enterprise Manager database.
Username	The user name of the account that has rights to access the `sysman.mgmt$ccc_all_observations` table.
Password	The password that is required to connect to the database.
Predefined Query (Optional)	none
Table Name	`sysman.mgmt$ccc_all_observations`
Select List	*
Compare Field	ACTION_TIME
Use Prepared Statements	True
Start Date and Time (Optional)	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value The maximum polling interval is one week.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 20,000.

Table 852. Oracle Enterprise Manager JDBC log source parameters (continued)	
Parameter	**Description**
Use Oracle Encryption	*Oracle Encryption and Data Integrity settings* is also known as *Oracle Advanced Security*. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.

For more information about configuring JDBC parameters, see c_logsource_JDBCprotocol.dita

Related tasks

Adding a DSM

Adding a log source

"Adding a DSM" on page 4

"Adding a log source" on page 5

Oracle Fine Grained Auditing

The Oracle Fine Grained Auditing DSM can poll for database audit events from Oracle 9i and later by using the Java Database Connectivity (JDBC) protocol.

To collect events, administrators must enable fine grained auditing on their Oracle databases. Fine grained auditing provides events on select, update, delete, and insert actions that occur in the source database and the records that the data changed. The database table `dba_fga_audit_trail` is updated with a new row each time a change occurs on a database table where the administrator enabled an audit policy.

To configure Oracle fine grained auditing, administrators can complete the following tasks:

1. Configure on audit on any tables that require policy monitoring in the Oracle database.
2. Configure a log source for the Oracle Fine Grained Auditing DSM to poll the Oracle database for events.
3. Verify that the events polled are collected and displayed on the **Log Activity** tab of IBM QRadar.

JDBC log source parameters for Oracle Fine Grained Auditing

If QRadar does not automatically detect the log source, add a Oracle Fine Grained Auditing log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Oracle Fine Grained Auditing:

Table 853. JDBC log source parameters for the Oracle Fine Grained Auditing DSM	
Parameter	**Value**
`Log Source type`	Oracle Fine Grained Auditing
`Protocol Configuration`	JDBC

Table 853. JDBC log source parameters for the Oracle Fine Grained Auditing DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	Oracle
Predefined Query	From the list, select **None**.
Table Name	Type `dba_fga_audit_trail` as the name of the table that includes the event records. If you change the value of this field from the default, events cannot be properly collected by the JDBC protocol.
Compare Field	Type `extended_timestamp` to identify new events added between queries to the table by their time stamp.
Use Prepared Statements	Select the **Use Prepared Statements** check box. Prepared statements allow the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clearing this check box requires you to use an alternative method of querying that does not use pre-compiled statements.

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

Adding a log source

Oracle RDBMS OS Audit Record

The IBM QRadar DSM for Oracle RDBMS OS Audit Record collects events from an Oracle device.

To integrate Oracle RDBMS OS Audit Record with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:

- DSM Common RPM
- OracleOSAudit DSM RPM

2. Configure your Oracle RDBMS OS Audit Record device to send events to QRadar. For more information, see Configuring Oracle RDBMS OS Audit Record to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add an Oracle RDBMS OS Audit Record log source on the QRadar Console by using the Syslog or Log File protocol. For more information, see Syslog log source parameters for Oracle RDBMS OS Audit Record or Log File log source parameters for Oracle RDBMS OS Audit Record.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Oracle RDBMS OS Audit Record DSM specifications

When you configure the Oracle RDBMS OS Audit Record DSM, understanding the specifications for the Oracle RDBMS OS Audit Record DSM can help ensure a successful integration. For example, knowing what the supported version of Oracle RDBMS OS Audit Record is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Oracle RDBMS OS Audit Record DSM.

Table 854. Oracle RDBMS OS Audit Record DSM specifications

Specification	**Value**
Manufacturer	Oracle
DSM name	**Oracle RDBMS OS Audit Record**
RPM file name	DSM-*OracleOSAudit-QRadar_version-build_number*.noarch.rpm
Supported versions	9i, 10g, 11g
Protocol	Syslog Log File protocol
Event format	name-value pair (NVP)
Recorded event types	Oracle events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Oracle website (https://docs.oracle.com)

Configuring Oracle RDBMS OS Audit Record to communicate with QRadar

When using the Oracle RDBMS OS Audit Record DSM for IBM QRadar, you can monitor the audit records that are stored in the local operating system file.

About this task

When audit event files are created or updated in the local operating system directory, a Perl script detects the change and then forwards the data to QRadar. The Perl script monitors the Audit log file, and combines any multi-line log entries into a single log entry to make sure that the logs are not forwarded line-by-line. This format matches the format in the log file. The logs are then sent by using Syslog to

QRadar. Perl scripts that are written for Oracle RDBMS OS Audit Record work only on Linux or UNIX servers. Windows - based Perl installations are not supported.

Procedure

1. Go to the IBM Support website (https://www.ibm.com/support/fixcentral) and download the following script:

   QRadar 7.4.0 - 7.4.0-QRADAR-SCRIPT-oracle_osauditlog_fwdr_5.3.tar.gz (https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=All&platform=All&function=fixId&fixids=7.4.0-QRADAR-SCRIPT-oracle_osauditlog_fwdr_5.3.tar.gz&includeSupersedes=0)
2. Type the following command to extract the file:

   ```
   tar -zxvf oracle_osauditlog_fwdr_5.3.tar.gz
   ```
3. Copy the Perl script to the server that hosts the Oracle server.

   Note: Perl 5.8 must be installed on the device that hosts the Oracle server. If you don't have Perl 5.8 installed, you might be prompted that library files are missing when you attempt to start the Oracle OS Audit script. Verify that Perl 5.8 is installed before you continue.
4. Log in to the Oracle host as an Oracle user that has SYS or root privilege.
5. Make sure the *ORACLE_HOME* and *ORACLE_SID* environment variables are configured properly for your deployment.
6. Open the following file:

   ```
   ${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora
   ```
7. For syslog, add the following lines to the file:

   ```
   *.audit_trail=os *.audit_syslog_level=local0.info
   ```
8. Verify that account has read/write permissions for the following directory:

   ```
   /var/lock/ /var/run/
   ```
9. Restart the Oracle database instance.
10. Start the OS Audit DSM script:

    ```
    oracle_osauditlog_fwdr_5.3.pl -t target_host -d logs_directory
    ```

    If you restart your Oracle server, you must restart the script:

    ```
    oracle_osauditlog_fwdr.pl -t target_host -d logs_directory
    ```

    For more information about Oracle OS Audit command parameters, see Oracle RDBMS OS Audit Record command parameters.

What to do next

Configure a log source in QRadar. For more information about Oracle OS Audit log source parameters, see Syslog log source parameters for Oracle RDBMS OS Audit Record or Log File log source parameters for Oracle RDBMS OS Audit Record.

Related tasks

"Adding a log source" on page 5

Oracle RDBMS OS Audit Record command parameters

When you use Oracle RDBMS OS Audit Record commands, there are specific parameters that you must use.

The following table describes the Oracle RDBMS OS Audit Record command parameters for Oracle RDBMS OS Audit Record:

Table 855. Oracle RDBMS OS Audit Record command parameters	
Parameter	**Description**
-t	Defines the remote host that receives the audit log files.
-d	Defines directory location of the DDL and DML log files. The directory location that you specify must be the absolute path from the root directory.
-H	Defines the host name or IP address for the syslog header. It is suggested that is the IP address of the Oracle server on which the script is running.
-D	The **-D** parameter defines that the script is to run in the foreground. The default is to run as a daemon (in the background) and log all internal messages to the local syslog service.
-n	Processes new logs, and monitors existing log files for changes to be processed. If the **-n** option string is absent, all existing log files are processed during script execution.
-u	Defines UDP.
-f	Defines the **syslog facility.priority** to be included at the beginning of the log. If you do not type a value, `user.info` is used.
-r	Defines the directory name where you want to create the `.pid` file. The default is `/var/run`. This parameter is ignored if **-D** is specified.
-l	Defines the directory name where you want to create the lock file. The default is `/var/lock`. This parameter is ignored if **-D** is specified.
-h	Displays the help message.
-v	Displays the version information for the script.

Related tasks

“Configuring Oracle RDBMS OS Audit Record to communicate with QRadar” on page 1325
When using the Oracle RDBMS OS Audit Record DSM for IBM QRadar, you can monitor the audit records that are stored in the local operating system file.

Syslog log source parameters for Oracle RDBMS OS Audit Record

When you add an Oracle RDBMS OS Audit Record log source on the QRadar Console by using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Oracle RDBMS OS Audit Record:

Table 856. Syslog log source parameters for the Oracle RDBMS OS Audit Record DSM	
Parameter	**Value**
Log Source type	**Oracle RDBMS OS Audit Record**
Protocol Configuration	Syslog

Table 856. Syslog log source parameters for the Oracle RDBMS OS Audit Record DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the address that is specified when you use the **-H** option in Oracle RDBMS OS Audit Record command parameters.

For more common log source parameters and their values, see Adding a log source..

Log File log source parameters for Oracle RDBMS OS Audit Record

If QRadar does not automatically detect the log source, add an Oracle RDBMS OS Audit Record log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from Oracle RDBMS OS Audit Record:

Table 857. Log File log source parameters for the Oracle RDBMS OS Audit Record DSM	
Parameter	**Value**
Log Source type	Oracle RDBMS OS Audit Record
Protocol Configuration	Log File
Log Source Identifier	Type the address that is specified when you use the **-H** option in Oracle RDBMS OS Audit Record command parameters.

For a complete list of Log File protocol parameters and their values, see Log File protocol configuration options.

Related tasks

Adding a log source

Sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Oracle OS Audit sample event message when you use the syslog protocol

The following sample event message shows that a DML procedure was run.

```
<14>Nov 07 18:57:35 oracle.osaudit.test AgentDevice=OracleOSAudit
SourceFile=ora_1234567.aud    DeviceTime=Thu Nov  7 18:57:33 2013    DatabaseUser='/'
Privilege='SYSDBA'    ClientUser='oracle'    ClientTerminal='pts/2'    Status='0'
Action=LENGTH : '193''UPDATE user_type4.people set CREATE_DATE = sysdate WHERE NUM=1'
```


```
<14>Nov 07 18:57:35 oracle.osaudit.test AgentDevice=OracleOSAudit
SourceFile=ora_1234567.aud    DeviceTime=Thu Nov  7 18:57:33 2013    DatabaseUser='/'
Privilege='SYSDBA'    ClientUser='oracle'    ClientTerminal='pts/2'    Status='0'
Action=LENGTH : '193''UPDATE user_type4.people set CREATE_DATE = sysdate WHERE NUM=1'
```


Table 858. Highlighted values in the Oracle RDBMS OS Audit Record sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**UPDATE**
Username	**oracle**

Table 858. Highlighted values in the Oracle RDBMS OS Audit Record sample event (continued)	
QRadar field name	**Highlighted values in the event payload**
Device Time	**Thu Nov 7 18:57:33 2013**

Chapter 120. osquery

The IBM QRadar DSM for osquery receives JSON formatted events from devices that use a Linux operating system. The osquery DSM is available for QRadar V7.3.0 and later.

The osquery DSM supports rsyslog and the following queries that are included in the `qradar.pack.conf` file for osquery V3.3.2:

- container_processes
- docker_container_mounts
- docker_containers
- listening_ports
- process_open_sockets
- sudoers
- users
- file_events

Important: The supported osquery queries run on a 10 second interval, and only capture data that is available at that moment. For example, if a new process starts and finishes between queries of container_processes, that information is not captured by osquery. For information about osquery differential logs, see the osquery documentation (https://osquery.readthedocs.io/en/stable/deployment/logging/#results-logs).

The following supported queries only capture data that is available at the 10 second querying interval:

- container_processes
- docker_container_mounts
- docker_containers
- listening_ports
- process_open_sockets
- sudoers
- users

To integrate osquery with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - osquery DSM RPM
   - TCP Multiline Syslog protocol RPM
   - Protocol Common RPM
2. Ensure that the TCP port you want to use on your QRadar Console to receive events is open. For more information, see QRadar: Managing IPtables firewall ports using the User Interface. (https://www.ibm.com/support/pages/qradar-managing-iptables-firewall-ports-using-user-interface)
3. Configure rsyslog on your Linux system. For more information about configuring rsyslog, see “Configuring rsyslog on your Linux system” on page 1332.
4. Configure osquery on your Linux system. For more information about configuring osquery, see “Configuring osquery on your Linux system” on page 1333.
5. Add an osquery log source on the QRadar Console to use the TCP multiline syslog protocol. For information about osquery log source parameters, see “osquery log source parameters” on page 1334.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Related information

osquery's integration with QRadar

osquery DSM specifications

When you configure osquery, understanding the specifications for the osquery DSM can help ensure a successful integration. For example, knowing what the supported version of osquery is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the osquery DSM

Table 859. osquery DSM specifications

Specification	Value
DSM name	osquery
RPM file name	DSM-*osquery-QRadar_version-build_number*.noarch.rpm
Supported versions	3.3.2
Protocol	Syslog TCP Multiline Syslog
Event format	JSON
Recorded event types	Access Audit Authentication System
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	Yes
More information	osquery website (https://osquery.io)

Configuring rsyslog on your Linux system

Before you can add a log source in QRadar, you need to configure rsyslog on your Linux system.

Before you begin

Rsyslog must be installed on your Linux system. For more information, go to the rsyslog website (https://www.rsyslog.com).

Procedure

1. On your Linux system, open the /etc/rsyslog.conf file, and then add the following entry at the end of the file:

   ```
   local3.info @@<QRadar_IP_address>:12468
   ```

   where <QRadar_IP_address> is the IP address of the QRadar Event Collector that you want to send events to.
2. You must be able to send rsyslog on a non-traditional TCP port. A potential challenge is that SELinux might block TCP port 12468. For more information, see Configuring rsyslog on

a logging server (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/s1-configuring_rsyslog_on_a_logging_server).

3. Restart the rsyslog service.

What to do next

Configure osquery on your Linux system. For more information, see "Configuring osquery on your Linux system" on page 1333.

Related concepts

"osquery" on page 1331

Configuring osquery on your Linux system

Before you can add a log source in QRadar, you must configure osquery on your Linux device.

Before you begin

Osquery V3.3.2 must be installed and running on your Linux system. For more information about installing osquery for Linux, see Downloading and Installing Osquery (https://osquery.io/downloads/official/3.3.2).

Procedure

1. Download the `qradar.pack.conf` file from IBM Fix Central (https://www.ibm.com/support/fixcentral).
2. Copy the `qradar.pack.conf` file to your osquery host. For example, `<location_of_pack_file>/qradar.pack.conf`
3. Edit the `osquery.conf` file. The default file location is `/etc/osquery/osquery.conf`.
   a) Ensure the following options are included in the `osquery.conf` file.

```
"disable_logging": "false"
 "disable_events" : "false"
 "logger_plugin": "filesystem,syslog"
```

   b) Add `qradar.pack.conf` to the `osquery.conf` file.

```
"qradar": "/<path_to_packs>/qradar.pack.conf"
```

   Example *<osquery>*.conf file:

```
{ // Configure the daemon below: "options": {    "disable_logging": "false",
"disable_events" : "false",    "logger_plugin": "filesystem,syslog",    "utc": "true" },
"packs": {   "qradar": "<location_of_pack_file>/qradar.pack.conf" }}
```

   Note: The `qradar.pack.conf` file contains a "`file_paths`" section that defines default file integrity monitoring for the QRadar pack. "`file_paths`" that are defined inside customer *<osquery>*`.conf` files take precedent over the `qradar.pack.conf` file.

4. Restart the osquery daemon.

What to do next

To get the parameter values that you need to add a log source in QRadar, see "osquery log source parameters" on page 1334.

Related concepts

"osquery" on page 1331

osquery log source parameters

When you add an osquery log source on the QRadar Console by using the TCP multiline syslog protocol, there are specific parameters you must use.

Note: You might need to restart rsyslog after you add the log source in QRadar.

The following table describes the parameters that require specific values to collect TCP multiline syslog events from osquery:

Table 860. TCP multiline syslog log source parameters for the osquery DSM

Parameter	Value
Log Source type	osquery
Protocol Configuration	TCP Multiline Syslog
Log Source Identifier	osquery
Listen Port	12468
Aggregation Method	Id-Linked
Message ID Pattern	"Unique_ID":\"(.*?)"
Event Formatter	No Formatting
Show Advanced Options	Yes
Use As A Gateway Log Source	Select this option. When selected, events that flow through the log source can be routed to other log sources based on the source name tagged on the events.
Retain Entire Lines During Event Aggregation	Select this option. When this option is selected, you can either discard or keep the part of the events that come before **Message IDPattern** when you concatenate events with the same ID pattern together.
Time Limit	5
Enabled	Select this option to enable the log source.

For a complete list of TCP multiline syslog protocol parameters and their values, see "TCP Multiline Syslog protocol configuration options" on page 222.

Related concepts

"osquery" on page 1331

Related tasks

"Adding a DSM" on page 4

osquery sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the TCP multiline syslog protocol for the osquery DSM:

Table 861. osquery DSM sample message supported by osquery.

Event name	Low-level category	Sample log message
User Added	User Account Added	<158>Sep 23 08:48:48 osquery.test osqueryd[16768]: {"name":"pack_qradar_users","hostIdentifier":"osquery.test.localdomain","calendarTime":"Mon Sep 23 12:48:48 2019 UTC","unixTime":1569242928,"epoch":0,"counter":21041,"decorations":{"host_uuid":"dd4b2142-1fa2-e1cd-c755-6bfb3cc33b55","last_logged_in_user":"root","username":"root"},"columns":{"Unique_ID":"1030-","description":"","directory":"/home/username6001","gid":"1030","gid_signed":"1030","query_name":"users","shell":"/bin/bash","uid":"1030","uid_signed":"1030","username":"username6001","uuid":""},"action":"added"}

Chapter 121. OSSEC

The OSSEC DSM for IBM QRadar accepts events that are forwarded from OSSEC installations by using syslog.

OSSEC is an open source Host-based Intrusion Detection System (HIDS) that can provide intrusion events to QRadar. If you have OSSEC agents that are installed, you must configure syslog on the OSSEC management server. If you have local or stand-alone installations of OSSEC, then you must configure syslog on each stand-alone OSSEC to forward syslog events to QRadar.

Configuring OSSEC

You can configure syslog for OSSEC on a stand-alone installation or management server:

Procedure

1. Use SSH to log in to your OSSEC device.
2. Edit the OSSEC configuration `ossec.conf` file.

   `<installation directory>/ossec/etc/ossec.conf`
3. Add the following syslog configuration:

   Note: Add the syslog configuration after the **`alerts`** entry and before the **`localfile`** entry.

   ```
   </alerts>

   <syslog_output> <server>(QRadar IP Address)</server> <port>514</port> </
   syslog_output>

   <localfile>
   ```

   For example,

   ```
   <syslog_output> <server><IP_address></server> <port>514</port> </
   syslog_output>
   ```
4. Save the OSSEC configuration file.
5. Type the following command to enable the syslog daemon:

   `<installation directory>/ossec/bin/ossec-control enable client-syslog`
6. Type the following command to restart the syslog daemon:

   `<installation directory>/ossec/bin/ossec-control restart`

   The configuration is complete. The log source is added to IBM QRadar as OSSEC events are automatically discovered. Events that are forwarded to QRadar by OSSEC are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for OSSEC

If QRadar does not automatically detect the log source, add an OSSEC log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from OSSEC:

Table 862. Syslog parameters log source parameters for the OSSEC DSM	
Parameter	**Description**
Log Source type	OSSEC
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from your OSSEC installation.

Related tasks

"Adding a log source" on page 5

Chapter 122. Palo Alto Networks

IBM QRadar supports a range of Palo Alto Network devices.

Palo Alto Endpoint Security Manager

The IBM QRadar DSM for Palo Alto Endpoint Security Manager (Traps) collects events from a Palo Alto Endpoint Security Manager (Traps) device.

The following table describes the specifications for the Palo Alto Endpoint Security Manager DSM:

Table 863. Palo Alto Endpoint Security Manager DSM specifications

Specification	**Value**
Manufacturer	Palo Alto Networks
DSM name	Palo Alto Endpoint Security Manager
RPM file name	`DSM-PaloAltoEndpointSecurityManager-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	3.4.2.17401
Protocol	Syslog
Event format	Log Event Extended Format (LEEF) Common Event Format (CEF). CEF:0 is supported.
Recorded event types	Agent Config Policy System Threat
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Palo Alto Networks website (https://www.paloaltonetworks.com)

To integrate Palo Alto Endpoint Security Manager with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (http://www.ibm.com/support).
   - DSMCommon RPM
   - Palo Alto Endpoint Security Manager DSM RPM
2. Configure your Palo Alto Endpoint Security Manager device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Palo Alto Endpoint Security Manager log source on the QRadar Console. The following table describes the parameters that require specific values for Palo Alto Endpoint Security Manager event collection:

Table 864. Palo Alto Endpoint Security Manager log source parameters	
Parameter	**Value**
Log Source type	Palo Alto Endpoint Security Manager
Protocol Configuration	Syslog
Log Source Identifier	A unique identifier for the log source.

4. To verify that QRadar is configured correctly, review the following table to see an example of a parsed event message.

   The following table shows a sample event message for Palo Alto Endpoint Security Manager:

Table 865. Palo Alto Endpoint Security Manager sample message		
Event name	**Low level category**	**Sample log message**
New Hash Added	Successful Configuration Modification	`LEEF:1.0|Palo Alto Networks|Traps ESM|3.4.2.17401| New Hash Added|cat=Policy subtype=New Hash Added devTimeFormat= MMM dd yyyy HH:mm:ss devTime=Nov 03 2016 18:43:57 src=<Source_IP_address> shost=hostname suser= fileHash= xxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxx NewVerdict=Benign msg=New hash added sev=6`  `LEEF:1.0|Palo Alto Networks|Traps ESM| 3.4.2.17401|New Hash Added| cat=Policysubtype=New HashAdded devTimeFormat=MMM dd yyyy HH:mm:ss devTime=Nov 03 2016 18:43:57 src=<Source_IP_address> shost=hostname suser= fileHashxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx NewVerdict=Benign msg=New hash added sev=6`

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Palo Alto Endpoint Security Manager to communicate with QRadar

Before IBM QRadar can collect events from Palo Alto Endpoint Security Manager, you must configure Palo Alto Endpoint Security Manager to send events to QRadar.

Procedure

1. Log in to the Endpoint Security Manager (ESM) Console.
2. Click **Settings** > **ESM**.
3. Click **Syslog**, and then select **Enable Syslog**.
4. Configure the syslog parameters:

Parameter	**Value**
Syslog Server	Host name or IP address of the QRadar server.
Syslog Port	514

Parameter	Value
Syslog Protocol	LEEF
Keep-alive-timeout	0
Send reports interval	Frequency (in minutes), in which Traps sends logs from the endpoint. The default is 10. The range is 1 - 2,147,483,647.
Syslog Communication Protocol	Transport layer protocol that the ESM Console uses to send syslog reports by using UDP, TCP, or TCP with SSL.

5. In the **Logging Events** area, select the types of events that you want to send to QRadar.
6. Click **Check Connectivity**. The ESM Console sends a test communication to the syslog server by using the information on the **Syslog** page. If the test message is not received, verify that the settings are correct, and then try again.

Palo Alto Networks PA Series

Use the IBM QRadar DSM for Palo Alto PA Series to collect events from Palo Alto PA Series, Next Generation Firewall logs, and Prisma Access logs, by using Cortex Data Lake.

To send events from Palo Alto PA Series to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM support website (https://www.ibm.com/support).
   - DSMCommon RPM
   - TLS Syslog Protocol RPM
   - Palo Alto PA Series DSM RPM
2. Configure your Palo Alto PA Series device to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a Palo Alto PA Series log source on the QRadar Console.

Related concepts

"TLS Syslog log source parameters for Palo Alto PA Series" on page 1354

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Palo Alto PA DSM specifications

The following table identifies the specifications for the Palo Alto PA Series DSM:

Table 866. DSM specifications for Palo Alto PA Series

Specification	Value
Manufacturer	Palo Alto Networks
DSM name	Palo Alto PA Series
RPM file name	`DSM-PaloAltoPaSeries-`*`QRadar_version-build_number`*`.noarch.rpm`
Event format	LEEF for PAN-OS v3.0 to v10.2, and Prisma Access v2.1 CEF for PAN-OS v4.0 to v6.1. (CEF:0 is supported)

Table 866. DSM specifications for Palo Alto PA Series (continued)	
Specification	**Value**
QRadar recorded log types	Traffic Threat Config System HIP Match Data WildFire Authentication Tunnel Inspection Correlation URL Filtering User-ID SCTP File Data GTP HIP Match IP-Tag Global Protect **Important:** To use the Global Protect log type, you must enable the **EventStatus/Status** field in Palo Alto. Decryption
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Palo Alto Networks website (http://www.paloaltonetworks.com)

Configuring Syslog or LEEF formatted events on your Palo Alto PA Series device

To send Palo Alto PA Series events to IBM QRadar, create a Syslog destination (Syslog or LEEF event format) on your Palo Alto PA Series device.

About this task

Palo Alto can send only one format to all Syslog devices. By modifying the Syslog format, any other device that requires Syslog must support that same format.

Procedure

1. Log in to Palo Alto Networks.

2. On the **Device** tab, click **Server Profiles** > **Syslog**, and then click **Add**.
3. Create a Syslog destination by following these steps:
   a) In the **Syslog Server Profile** dialog box, click **Add**.
   b) Specify the name, server IP address, port, and facility of the QRadar system that you want to use as a Syslog server.
   c) If you are using Syslog, set the **Custom Format** column to **Default** for all log types.
4. Configure LEEF events by following these steps:

   Important: Due to formatting issues, copy the text into a text editor, remove any carriage return or line feed characters, and then paste it into the appropriate field.

   a) Click the **Custom Log Format** tab in the **Syslog Server Profile** dialog.
   b) Click **Config**, copy one of the following texts applicable to the version you are using, and paste it in the **Config Log Format** field for the **Config** log type. If your version is not listed, omit this step.

   PAN-OS 3.0 - 6.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|4.0|$result|x7C|cat=$type|usrName=$admin|src=$host|devTime=$cef-
formatted-receive_time|client=$client|sequence=$seqno|serial=$serial|msg=$cmd
```

   PAN-OS 7.1 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$result|
x7C|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|devTime=$cef-formatted-
receive_time|src=$host|VirtualSystem=$vsys|msg=$cmd|usrName=$admin|client=$client|
Result=$result|ConfigurationPath=$path|sequence=$seqno|ActionFlags=$actionflags|
BeforeChangeDetail=$before-change-detail|AfterChangeDetail=$after-change-detail|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name
```

   PAN-OS 10.0

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$result|
x7C|TimeReceived=$receive_time|DeviceSN=$serial|cat=$type|devTime=$cef-formatted-
receive_time|src=$host|VirtualSystem=$vsys|msg=$cmd|usrName=$admin|client=$client|
Result=$result|ConfigurationPath=$path|sequence=$seqno|ActionFlags=$actionflags|
BeforeChangeDetail=$before-change-detail|AfterChangeDetail=$after-change-detail|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name
```

   c) Click **System**, then copy one of the following texts applicable to the version you are using, and paste it in the **System Log Format** field for the **System** log type. If your version is not listed, omit this step.

   PAN-OS 3.0 - 6.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|4.0|$eventid|x7C|cat=$type|Subtype=$subtype|devTime=$cef-formatted-
receive_time|sev=$severity|Severity=$number-of-severity|msg=$opaque|Filename=$object
```

   PAN-OS 7.1 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$eventid|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_time|
VirtualSystem=$vsys|Filename=$object|Module=$module|sev=$number-of-severity|
Severity=$severity|msg=$opaque|sequence=$seqno|ActionFlags=$actionflags|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name
```

   PAN-OS 10.0

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$eventid|x7C|TimeReceived=$receive_time|
```

```
DeviceSN=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_time|
VirtualSystem=$vsys|Filename=$object|Module=$module|sev=$number-of-severity|
Severity=$severity|msg=$opaque|sequence=$seqno|ActionFlags=$actionflags|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name
```

d) Click **Threat**, copy one of the following texts applicable to the version you are using, and paste it in the **Threat Log Format** field for the **Threat** log type. If your version is not listed, omit this step.

PAN-OS 3.0 - 6.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|4.0|$threatid|x7C|cat=$type|
Subtype=$subtype|src=$src|dst=$dst|srcPort=$sport|dstPort=$dport|proto=$proto|
usrName=$srcuser|SerialNumber=$serial|srcPostNAT=$natsrc|dstPostNAT=$natdst|
RuleName=$rule|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$fromDestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags|
URLCategory=$category|sev=$severity|Severity=$number-of-severity|Direction=$direction|
ContentType=$contenttype|action=$action|Miscellaneous=$misc
```

PAN-OS 7.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$threatid|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-
receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
usrName=$srcuser|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|Miscellaneous=$misc|
ThreatID=$threatid|URLCategory=$category|sev=$number-of-severity|Severity=$severity|
Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|
DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|
FileDigest=$filedigest|Cloud=$cloud|URLIndex=$url_idx|UserAgent=$user_agent|
FileType=$filetype|identSrc=$xff|Referer=$referer|Sender=$sender|Subject=$subject|
Recipient=$recipient|ReportID=$reportid|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name
```

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$threatid|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-
receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
usrName=$srcuser|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|
Miscellaneous=$misc|ThreatID=$threatid|URLCategory=$category|sev=$number-of-severity|
Severity=$severity|Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|
SourceLocation=$srcloc|DestinationLocation=$dstloc|ContentType=$contenttype|
PCAP_ID=$pcap_id|FileDigest=$filedigest|Cloud=$cloud|URLIndex=$url_idx|
RequestMethod=$http_method|Subject=$subject|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|MonitorTag=$monitortag|
ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|
TunnelType=$tunnel|ThreatCategory=$thr_category|ContentVer=$contentver
```

PAN-OS 10.0

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$threatid|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-
receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
usrName=$srcuser|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|
Miscellaneous=$misc|ThreatID=$threatid|URLCategory=$category|sev=$number-of-severity|
Severity=$severity|Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|
```

```
SourceLocation=$srcloc|DestinationLocation=$dstloc|ContentType=$contenttype|
PCAP_ID=$pcap_id|FileDigest=$filedigest|Cloud=$cloud|URLIndex=$url_idx|
RequestMethod=$http_method|Subject=$subject|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|MonitorTag=$monitortag|
ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|
TunnelType=$tunnel|ThreatCategory=$thr_category|ContentVer=$contentver
```

e) Click **Traffic**, copy one of the following texts applicable to the version you are using, and paste it in the **Traffic Log Format** field for the **Traffic** log type. If your version is not listed, omit this step.

PAN-OS 3.0 - 6.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|4.0|$action|x7C|cat=$type|src=$src|dst=$dst|srcPort=$sport|
dstPort=$dport|proto=$proto|usrName=$srcuser| SerialNumber=$serial|
Type=$type|Subtype=$subtype|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags|
totalBytes=$bytes|totalPackets=$packets|ElapsedTime=$elapsed|URLCategory=$category|
dstBytes=$bytes_received|srcBytes=$bytes_sent|action=$action
```

PAN-OS 7.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$action|x7C|
cat=$type|ReceiveTime=$receive_time|SerialNumber=$serial|Type=$type|Subtype=$subtype|
devTime=$cef-formatted-receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|
dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|SourceUser=$srcuser|
DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from|
DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|
LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|
srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|
Flags=$flags|proto=$proto|action=$action|totalBytes=$bytes|dstBytes=$bytes_received|
srcBytes=$bytes_sent|totalPackets=$packets|StartTime=$start|ElapsedTime=$elapsed|
URLCategory=$category|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|
DestinationLocation=$dstloc|dstPackets=$pkts_received|srcPackets=$pkts_sent|
SessionEndReason=$session_end_reason|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
ActionSource=$action_source
```

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$action|x7C|cat=$type|ReceiveTime=$receive_time|
SerialNumber=$serial|Type=$type|Subtype=$subtype|devTime=$cef-formatted-
receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
usrName=$srcuser|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|totalBytes=$bytes|
dstBytes=$bytes_received|srcBytes=$bytes_sent|totalPackets=$packets|
StartTime=$start|ElapsedTime=$elapsed|URLCategory=$category|sequence=$seqno|
ActionFlags=$actionflags|SourceLocation=$srcloc|DestinationLocation=$dstloc|
dstPackets=$pkts_received|srcPackets=$pkts_sent|SessionEndReason=$session_end_reason|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|ActionSource=$action_source|
SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|MonitorTag=$monitortag|
ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|
TunnelType=$tunnel
```

PAN-OS 10.2

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$action|x7C|
cat=$type|devTime=$cef-formatted-receive_time|SerialNumber=$serial|Subtype=$subtype|
src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
usrName=$srcuser|DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|
SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|Flags=$flags|proto=$proto|totalBytes=$bytes|
srcBytes=$bytes_sent|dstBytes=$bytes_received|totalPackets=$packets|
```

```
dstPackets=$pkts_received|srcPackets=$pkts_sent|start=$cef-formatted-time_generated|
ElapsedTime=$elapsed|URLCategory=$category|sequence=$seqno|
SessionEndReason=$session_end_reason|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
vSrcName=$vsys_name|DeviceName=$device_name|ActionSource=$action_source|
ActionFlags=$actionflags|SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|
MonitorTag=$monitortag|ParentSessionID=$parent_session_id|
ParentStartTime=$parent_start_time|TunnelType=$tunnelRuleUUID=$rule_uuid|
PolicyID=$policy_id|LinkDetail=$link_switches|SDWANCluster=$sdwan_cluster|
SDWANDevice=$sdwan_device_type|SDWANClustype=$sdwan_cluster_type|
SDWANSite=$sdwan_site|DynamicUsrgrp=$dynusergroup_name|XFFIP=$xff_ip|
SrcDeviceCat=$src_category|SrcDeviceProf=$src_profile|SrcDeviceModel=$src_model|
SrcDeviceVendor=$src_vendor|SrcDeviceOS=$src_osfamily|SrcDeviceOSv=$src_osversion|
SrcHostname=$src_host|SrcMac=$src_mac|DstDeviceCat=$dst_category|
DstDeviceProf=$dst_profile|DstDeviceModel=$dst_model|DstDeviceVendor=$dst_vendor|
DstDeviceOS=$dst_osfamily|DstDeviceOSv=$dst_osversion|DstHostname=$dst_host|
DstMac=$dst_mac|ContainerName=$container_id|PODNamespace=$pod_namespace|
PODName=$pod_name|SrcEDL=$src_edl|DstEDL=$dst_edl|GPHostID=$hostid|
EPSerial=$serialnumber|SrcDAG=$src_dag|DstDAG=$dst_dag
```

f) If you are using versions other than PAN-OS 3.0 - 6.1, click **HIP Match**, copy one of the following texts applicable to the version you are using, and paste it in the **HIP Match Log Format** field for the **HIP Match** log type.

PAN-OS 7.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|
$sender_sw_version|$matchname|x7C|ReceiveTime=$receive_time|SerialNumber=$serial|
cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_time|usrName=$srcuser|
VirtualSystem=$vsys|identHostName=$machinename|OS=$os|identSrc=$src|HIP=$matchname|
RepeatCount=$repeatcnt|HIPType=$matchtype|sequence=$seqno|ActionFlags=$actionflags|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name
```

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|
$sender_sw_version|$matchname|x7C|ReceiveTime=$receive_time|SerialNumber=$serial|
cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_time|usrName=$srcuser|
VirtualSystem=$vsys|identHostName=$machinename|OS=$os|identsrc=$src|HIP=$matchname|
RepeatCount=$repeatcnt|HIPType=$matchtype|sequence=$seqno|ActionFlags=$actionflags|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|srcipv6=$srcipv6|
startTime=$cef-formatted-time_generated
```

PAN-OS 10.2

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|
$matchname|x7C|ProfileToken=$actionflags|TimeReceived=$receive_time|DeviceSN=$serial|
cat=$type|SubType=$subtype|ConfigVersion=$sender_sw_version|devTime=$cef-formatted-
receive_time|usrName=$srcuser|VirtualLocation=$vsys|identHostName=$machinename|
EndpointOSType=$os|iOSsrc=$src|CountOfRepeats=$repeatcnt|SequenceNo=$seqno|
DGHierarchyLevel1=$dg_hier_level_1|DGHierarchyLevel2=$dg_hier_level_2|
DGHierarchyLevel3=$dg_hier_level_3|DGHierarchyLevel4=$dg_hier_level_4|
VirtualSystemName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|
SourceIPv6=$srcipv6|HostID=$hostid|EndpointSerialNumber=$serialnumber|
SourceDeviceCategory=$reclassified|SourceDeviceModel=$matchtype|
SourceDeviceMac=$mac|TimestampDeviceIdentification=$time_generated|
TimeGeneratedHighResolution=$high_res_timestamp|devTimeFormat=$cef-formatted-
time_generated
```

g) Copy one of the following texts applicable to the version you are using and paste it in the **Custom Format** column for the log type. If you are using **PAN-OS 8.0 - 9.1**, copy and paste the text for the **URL Filtering** log type. If you are using **PAN-OS 10.0**, copy and paste the text for the **URL** log type. If your version is not listed, omit this step.

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$threatid|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-
receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
usrName=$srcuser|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
```

```
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|Miscellaneous=$misc|
ThreatID=$threatid|URLCategory=$category|sev=$number-of-severity|Severity=$severity|
Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|SourceLocation=$srcloc|
DestinationLocation=$dstloc|ContentType=$contenttype|PCAP_ID=$pcap_id|
FileDigest=$filedigest|Cloud=$cloud|URLIndex=$url_idx|RequestMethod=$http_method|
UserAgent=$user_agent|identSrc=$xff|Referer=$referer|Subject=$subject|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|SrcUUID=$src_uuid|DstUUID=$dst_uuid|
TunnelID=$tunnelid|MonitorTag=$monitortag|ParentSessionID=$parent_session_id|
ParentStartTime=$parent_start_time|TunnelType=$tunnel|ThreatCategory=$thr_category|
ContentVer=$contentver
```

PAN-OS 10.0

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$threatid|
x7C|ProfileToken=$actionflags|TimeReceived=$receive_time|DeviceSN=$serial|cat=$type|
SubType=$subtype|ConfigVersion=$sender_sw_version|devTime=$cef-formatted-receive_time|
src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|Rule=$rule|usrName=$srcuser|
DestinationUser=$dstuser|Application=$app|VirtualLocation=$vsys|FromZone=$from|
ToZone=$to|InboundInterface=$inbound_if|OutboundInterface=$outbound_if|
LogSetting=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPort=$sport|
dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|proto=$proto|
Action=$action|URL=$file_url|VendorSeverity=$severity|DirectionOfAttack=$direction|
SequenceNo=$seqno|SourceLocation=$srcloc|DestinationLocation=$dstloc|
ContentType=$contenttype|PacketID=$pcap_id|URLCounter=$url_idx|UserAgent=$user_agent|
identSrc=$xff|Referer=$referer|DGHierarchyLevel1=$dg_hier_level_1|
DGHierarchyLevel2=$dg_hier_level_2|DGHierarchyLevel3=$dg_hier_level_3|
DGHierarchyLevel4=$dg_hier_level_4|VirtualSystemName=$vsys_name|
DeviceName=$device_name|SourceUUID=$src_uuid|DestinationUUID=$dst_uuid|
HTTPMethod=$http_method|IMSI=$imsi|IMEI=$imei|ParentSessionID=$parent_session_id|
ParentStarttime=$parent_start_time|Tunnel=$tunnelid|ContentVersion=$contentver|
SigFlags=$sig_flags|HTTPHeaders=$http_headers|URLCategoryList=$url_category_list|
RuleUUID=$rule_uuid|HTTP2Connection=$http2_connection|
DynamicUserGroupName=$dynusergroup_name|X-Forwarded-ForIP=$xff_ip|
SourceDeviceCategory=$src_category|SourceDeviceProfile=$src_profile|
SourceDeviceModel=$src_model|SourceDeviceVendor=$src_vendor|
SourceDeviceOSFamily=$src_osfamily|SourceDeviceOSVersion=$src_osversion|
SourceDeviceHost=$src_host|SourceDeviceMac=$src_mac|
DestinationDeviceCategory=$dst_category|DestinationDeviceProfile=$dst_profile|
DestinationDeviceModel=$dst_model|DestinationDeviceVendor=$dst_vendor|
DestinationDeviceOSFamily=$dst_osfamily|DestinationDeviceOSVersion=$dst_osversion|
DestinationDeviceHost=$dst_host|DestinationDeviceMac=$dst_mac|
ContainerID=$container_id|ContainerNameSpace=$pod_namespace|ContainerName=$pod_name|
SourceEDL=$src_edl|DestinationEDL=$dst_edl|HostID=$hostid|
EndpointSerialNumber=$serialnumber|SourceDynamicAddressGroup=$src_dag|
DestinationDynamicAddressGroup=$dst_dag|
TimeGeneratedHighResolution=$high_res_timestamp|NSSAINetworkSliceType=$nssai_sst|
devTimeFormat=$cef-formatted-time_generated
```

h) If you are using **PAN-OS 8.0 - 9.1**, copy the following text and paste it in the **Custom Format** column for the **Data** log type.

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|
$sender_sw_version|$threatid|x7C|ReceiveTime=$receive_time|SerialNumber=$serial|
cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_time|src=$src|dst=$dst|
srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|SourceUser=$srcuser|
DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from|
DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|
LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPort=$sport|
dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|Flags=$flags|
proto=$proto|action=$action|Miscellaneous=$misc|ThreatID=$threatid|URLCategory=$category|
sev=$number-of-severity|Severity=$severity|Direction=$direction|sequence=$seqno|
ActionFlags=$actionflags|SourceLocation=$srcloc|DestinationLocation=$dstloc|
ContentType=$contenttype|PCAP_ID=$pcap_id|FileDigest=$filedigest|
Cloud=$cloud|URLIndex=$url_idx|RequestMethod=$http_method|Subject=$subject|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|SrcUUID=$src_uuid|DstUUID=$dst_uuid|
TunnelID=$tunnelid|MonitorTag=$monitortag|ParentSessionID=$parent_session_id|
ParentStartTime=$parent_start_time|TunnelType=$tunnel|ThreatCategory=$thr_category|
ContentVer=$contentver
```

i) Copy one of the following texts applicable to the version you are using and paste it in the **Custom Format** column for the **WildFire** log type. If your version is not listed, omit this step.

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$threatid|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-
receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|RuleName=$rule|
usrName=$srcuser|SourceUser=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|IngressInterface=$inbound_if|
EgressInterface=$outbound_if|LogForwardingProfile=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|Flags=$flags|proto=$proto|action=$action|
Miscellaneous=$misc|ThreatID=$threatid|URLCategory=$category|sev=$number-of-severity|
Severity=$severity|Direction=$direction|sequence=$seqno|ActionFlags=$actionflags|
SourceLocation=$srcloc|DestinationLocation=$dstloc|ContentType=$contenttype|
PCAP_ID=$pcap_id|FileDigest=$filedigest|Cloud=$cloud|URLIndex=$url_idx|
RequestMethod=$http_method|FileType=$filetype|Sender=$sender|Subject=$subject|
Recipient=$recipient|ReportID=$reportid|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
SrcUUID=$src_uuid|DstUUID=$dst_uuid|TunnelID=$tunnelid|MonitorTag=$monitortag|
ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|
TunnelType=$tunnel|ThreatCategory=$thr_category|ContentVer=$contentver
```

PAN-OS 10.2

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|
$threatid|x7C|ProfileToken=$actionflags|TimeReceived=$receive_time|DeviceSN=$serial|
cat=$type|SubType=$subtype|ConfigVersion=$sender_sw_version|devTime=$cef-formatted-
receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|Rule=$rule|
usrName=$srcuser|DestinationUser=$dstuser|Application=$app|VirtualLocation=$vsys|
FromZone=$from|ToZone=$to|InboundInterface=$inbound_if|OutboundInterface=$outbound_if|
LogSetting=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPort=$spor|
dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|proto=$proto|
Action=$action|FileName=$misc|VendorSeverity=$severity|DirectionOfAttack=$direction|
SequenceNo=$seqno|SourceLocation=$srcloc|DestinationLocation=$dstloc|
PacketID=$pcap_id|FileHash=$filedigest|ApplianceOrCloud=$cloud
```

j) Copy one of the following texts applicable to the version you are using and paste it in the **Custom Format** column for the **Authentication** log type. If your version is not listed, omit this step.

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|$sender_sw_version|$event|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|Subtype=$subtype|devTime=$cef-formatted-receive_time|
ServerProfile=$serverprofile|LogForwardingProfile=$logset|VirtualSystem=$vsys|
AuthPolicy=$authpolicy|ClientType=$clienttype|NormalizeUser=$normalize_user|
ObjectName=$object|FactorNumber=$factorno|AuthenticationID=$authid|src=$ip|
RepeatCount=$repeatcnt|usrName=$user|Vendor=$vendor|msg=$event|sequence=$seqno|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|AdditionalAuthInfo=$desc|
ActionFlags=$actionflags
```

PAN-OS 10.0

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|
$event|x7C|ProfileToken=$actionflags|TimeReceived=$receive_time|DeviceSN=$serial|
cat=$type|SubType=$subtype|ConfigVersion=$sender_sw_version|devTime=$cef-
formatted-receive_time|VirtualLocation=$vsys|src=$ip|User=$normalize_user|
usrName=$user|Object=$object|object2AuthenticationPolicy=$authpolicy|
CountOfRepeats=$repeatcnt|MFAAuthenticationID=-$authid|MFAVendor=$vendor|
LogSetting=$logset|AuthServerProfile=$serverprofile|AuthenticationDescription=$desc|
ClientType=$clienttype|AuthFactorNo=$factorno|SequenceNo=$seqno|
DGHierarchyLevel1=$dg_hier_level_1|DGHierarchyLevel2=$dg_hier_level_2|
DGHierarchyLevel3=$dg_hier_level_3|DGHierarchyLevel4=$dg_hier_level_4|
VirtualSystemName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|
AuthenticationProtocol=$authproto|RuleMatchedUUID=$rule_uuid|
TimeGeneratedHighResolution=$high_res_timestamp|SourceDeviceCategory=$src_category|
SourceDeviceProfile=$src_profile|SourceDeviceModel=$src_model|
SourceDeviceVendor=$src_vendor|SourceDeviceOSFamily=$src_osfamily|
SourceDeviceOSVersion=$src_osversion|SourceDeviceHost=$src_host|
SourceDeviceMac=s$src_mac|AuthCacheServiceRegion=$region|UserAgentString=$user_agent|
SessionID=$sessionid|devTimeFormat=$cef-formatted-time_generated
```

k) Copy one of the following texts applicable to the version you are using and paste it in the **Custom Format** column for the **User-ID** log type. If your version is not listed, omit this step.

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$subtype|
x7C|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|
devTime=$cef-formatted-receive_time|FactorType=$factortype|VirtualSystem=$vsys|
DataSourceName=$datasourcename|DataSource=$datasource|DataSourceType=$datasourcetype|
FactorNumber=$factorno|VirtualSystemID=$vsys_id|TimeoutThreshold=$timeout|
src=$ip|srcPort=$beginport|dstPort=$endport|RepeatCount=$repeatcnt|usrName=$user|
sequence=$seqno|EventID=$eventid|FactorCompletionTime=$factorcompletiontime|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|ActionFlags=$actionflags
```

PAN-OS 10.2

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$subtype|x7C|
ProfileToken=$actionflags|TimeReceived=$receive_time|DeviceSN=$serial|cat=$type|
ConfigVersion=$sender_sw_version|devTime=$cef-formatted-receive_time|
VirtualLocation=$vsys|src=$ip|usrName=$user|MappingDataSourceName=$datasourcename|
EventIdName=$eventid|CountofRepeats=$repeatcnt|MappingTimeout=$timeout|
srcPort=$beginport|dstPort=$endport|MappingDataSource=$datasource|
MappingDataSourceType=$datasourcetype|SequenceNo=$seqno|
DGHierarchyLevel1=$dg_hier_level_1|DGHierarchyLevel2=$dg_hier_level_2|
DGHierarchyLevel3=$dg_hier_level_3|DGHierarchyLevel4=$dg_hier_level_4|
VirtualSystemName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|
MFAFactorType=$factortype|AuthCompletionTime=$factorcompletiontime|
AuthFactorNo=$factorno|UGFlags=$ugflags|UserIdentifiedBySource=$userbysource|
Tag=$tag_name|TimeGeneratedHighResolution=$high_res_timestamp|devTimeFormat=$cef-
formatted-time_generated
```

l) Copy one of the following texts applicable to the version you are using and paste it in the **Custom Format** column for the log type. If you are using **PAN-OS 8.0 - 9.1**, copy and paste the text for the **Tunnel Inspection** log type. If you are using **PAN-OS 10.0**, copy and paste the text for the **Tunnel** log type. If your version is not listed, omit this step.

PAN-OS 8.0 - 9.1

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|
$action|x7C|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|Subtype=$subtype|
devTime=$cef-formatted-receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|
dstPostNAT=$natdst|RuleName=$rule|usrName=$srcuser|SourceUser=$srcuser|
DestinationUser=$dstuser|Application=$app|VirtualSystem=$vsys|SourceZone=$from|
DestinationZone=$to|IngressInterface=$inbound_if|EgressInterface=$outbound_if|
LogForwardingProfile=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|
srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|
Flags=$flags|proto=$proto|action=$action|sequence=$seqno|ActionFlags=$actionflags|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|TunnelID=$tunnelid|MonitorTag=$monitortag|
ParentSessionID=$parent_session_id|ParentStartTime=$parent_start_time|
TunnelType=$tunnel|totalBytes=$bytes|dstBytes=$bytes_received|srcBytes=$bytes_sent|
totalPackets=$packets|dstPackets=$pkts_received|srcPackets=$pkts_sent|
MaximumEncapsulation=$max_encap|UnknownProtocol=$unknown_proto|
StrictChecking=$strict_check|TunnelFragment=$tunnel_fragment|
SessionsCreated=$sessions_created|SessionsClosed=$sessions_closed|
SessionEndReason=$session_end_reason|ActionSource=$action_source|startTime=$start|
ElapsedTime=$elapsed
```

PAN-OS 10.0

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$action|x7C|
ProfileToken=$actionflags|TimeReceived=$receive_time|DeviceSN=$serial|cat=$type|
SubType=$subtype|ConfigVersion=$sender_sw_version|devTime=$cef-formatted-receive_time|
src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|Rule=$rule|usrName=$srcuser|
DestinationUser=$dstuse|Application=$app|VirtualLocation=$vsys|FromZone=$from|
ToZone=$to|InboundInterface=$inbound_if|OutboundInterface=$outbound_if|
LogSetting=$logset|SessionID=$sessionid|RepeatCount=$repeatcnt|srcPort=$sport|
dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|proto=$proto|
SequenceNo=$seqno|SourceLocation=$srcloc|DestinationLocation=$dstloc|
DGHierarchyLevel1=$dg_hier_level_1|DGHierarchyLevel2=$dg_hier_level_2|
DGHierarchyLevel3=$dg_hier_level_3|DGHierarchyLevel4=$dg_hier_level_4|
VirtualSystemName=$vsys_name|DeviceName=$device_name|
ParentSessionID=$parent_session_id|ParentStarttime=$parent_start_time|Tunnel=$tunnel|
Bytes=$bytes|srcBytes=$bytes_sent|dstBytes=$bytes_received|totalPackets=$packets|
srcPackets=$pkts_sent|dstPackets=$pkts_received|
TunnelSessionsCreated=$sessions_created|TunnelSessionsClosed=$sessions_closed|
SessionEndReason=$session_end_reason|ActionSource=$action_source|startTime=$start|
```

```
SessionDuration=$elapsed|RuleUUID=$rule_uuid|DynamicUserGroupName=$dynusergroup_name|
ContainerID=$container_id|ContainerNameSpace=$pod_namespace|ContainerName=$pod_name|
SourceEDL=$src_edl|DestinationEDL=$dst_edl|SourceDynamicAddressGroup=$src_dag|
DestinationDynamicAddressGroup=dst_dag|
TimeGeneratedHighResolution=$high_res_timestamp|
NSSAINetworkSliceDifferentiator=$nssai_sd|NSSAINetworkSliceType=$nssai_sst|
ProtocolDataUnitsessionID=$pdu_session_id|devTimeFormat=$cef-formatted-time_generated
```

m) If you are using **PAN-OS 8.0 - 9.1**, copy the following text and paste it in the **Custom Format** column for the **Correlation** log type.

```
LEEF:2.0|Palo Alto Networks|PAN-OS
Syslog Integration|8.0|$category|x7C|ReceiveTime=$receive_time|
SerialNumber=$serial|cat=$type|devTime=$cef-formatted-receive_time|startTime=$cef-
formatted-time_generated|Severity=$severity|VirtualSystem=$vsys|VirtualSystemID=$vsys_id|
src=$src|SourceUser=$srcuser|msg=$evidence|DeviceGroupHierarchyL1=$dg_hier_level_1|
DeviceGroupHierarchyL2=$dg_hier_level_2|DeviceGroupHierarchyL3=$dg_hier_level_3|
DeviceGroupHierarchyL4=$dg_hier_level_4|vSrcName=$vsys_name|DeviceName=$device_name|
ObjectName=$object_name|ObjectID=$object_id
```

n) If you are using **PAN-OS 8.1 - 9.1**, copy the following text, and paste it in the **Custom Format** column for the **SCTP** log type.

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$action|
x7C|ReceiveTime=$receive_time|SerialNumber=$serial|cat=$type|genTime=$time_generated|
src=$src|dst=$dst|VirtualSystem=$vsys|SourceZone=$from|DestinationZone=$to|
IngressInterface=$inbound_if|EgressInterface=$outbound_if|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|proto=$proto|action=$action|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vsysName=$vsys_name|DeviceName=$device_name|sequence=$seqno|AssocID=$assoc_id|
PayloadProtoID=$ppid|sev=$num_of_severity|SCTPChunkType=$sctp_chunk_type|
SCTPVerTag1=$verif_tag_1|SCTPVerTag2=$verif_tag_2|SCTPCauseCode=$sctp_cause_code|
DiamAppID=$diam_app_id|DiamCmdCode=$diam_cmd_code|DiamAVPCode=$diam_avp_code|
SCTPStreamID=$stream_id|SCTPAssEndReason=$assoc_end_reason|OpCode=$op_code|
CPSSN=$sccp_calling_ssn|CPGlobalTitle=$sccp_calling_gt|SCTPFilter=$sctp_filter|
SCTPChunks=$chunks|SrcSCTPChunks=$chunks_sent|DstSCTPChunks=$chunks_received|
Packets=$packets|srcPackets=$pkts_sent|dstPackets=$pkts_received
```

o) Copy one of the following texts applicable to the version you are using and paste it in the **Custom Format** column for the **IP-Tag** log type. If your version is not listed, omit this step.

PAN-OS 9.x

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|
$event_id|x7C|cat=$type|devTime=$cef-formatted-receive_time|ReceiveTime=$receive_time|
SerialNumber=$serial|Subtype=$subtype|GenerateTime=$time_generated|
VirtualSystem=$vsys|src=$ip|TagName=$tag_name|EventID=$eventid|RepeatCount=$repeatcnt|
TimeoutThreshold=$timeout|DataSourceName=$datasourcename|DataSource=$datasource_type|
DataSourceType=$datasource_subtype|sequence=$seqno|ActionFlags=$actionflags|
DeviceGroupHierarchyL1=$dg_hier_level_1|DeviceGroupHierarchyL2=$dg_hier_level_2|
DeviceGroupHierarchyL3=$dg_hier_level_3|DeviceGroupHierarchyL4=$dg_hier_level_4|
vSrcName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id
```

PAN-OS 10.2

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|
$sender_sw_version|$event_id|x7C|ProfileToken=$actionflags|TimeReceived=$receive_time|
DeviceSN=$serial|cat=$type|SubType=$subtype|ConfigVersion=$sender_sw_version|
devTime=$cef-formatted-receive_time|VirtualLocation=$vsys|src=$ip|
TagName=$tag_name|CountOfRepeats=$repeatcnt|MappingTimeout=$timeout|
MappingDataSource=$datasourcename|MappingDataSourceType=$datasource_type|
MappingDataSourceSubType=$datasource_subtype|SequenceNo=$seqno|
DGHierarchyLevel1=$dg_hier_level_1|DGHierarchyLevel2=$dg_hier_level_2|
DGHierarchyLevel3=$dg_hier_level_3|DGHierarchyLevel4=$dg_hier_level_4|
VirtualSystemName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|
IPSubnetRange=$ip_subnet_range|TimeGeneratedHighResolution=$high_res_timestamp|
devTimeFormat=$cef-formatted-time_generated
```

p) If you are using **PAN-OS 10.2**, copy the following text, and paste it in the **Custom Format** column for the **GlobalProtect** log type.

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|
$eventid|x7C|TimeReceived=$receive_time|DeviceSN=$serial|cat=$type|SubType=$subtype|
ConfigVersion=$sender_sw_version|devTime=$cef-formatted-receive_time|VirtualSystem=$vsys|
```

```
Stage=$stage|AuthMethod=$auth_method|TunnelType=$tunnel_type|usrName=$srcuser|
SourceRegion=$srcregion|EndpointDeviceName=$machinename|PublicIPv4=$public_ip|
PublicIPv6=$public_ipv6|PrivateIPv4=$private_ip|PrivateIPv6=$private_ipv6|
HostID=$hostid|EndpointSN=$serialnumber|GlobalProtectClientVersion=$client_ver|
EndpointOSType=$client_os|EndpointOSVersion=$client_os_ver|CountOfRepeats=$repeatcnt|
QuarantineReason=$reason|ConnectionError=$error|Description=$opaque|EventStatus=$status|
GlobalProtectGatewayLocation=$location|LoginDuration=$login_duration|
ConnectionMethod=$connect_method|ConnectionErrorID=$error_code|Portal=$portal|
SequenceNo=$seqno|TimeGeneratedHighResolution=$high_res_timestamp|
GatewaySelectionType=$selection_type|SSLResponseTime=$response_time|
GatewayPriority=$priority|AttemptedGateways=$attempted_gateways|Gateway=$gateway|
DGHierarchyLevel1=$dg_hier_level_1|DGHierarchyLevel2=$dg_hier_level_2|
DGHierarchyLevel3=$dg_hier_level_3|DGHierarchyLevel4=$dg_hier_level_4|
VirtualSystemName=$vsys_name|DeviceName=$device_name|VirtualSystemID=$vsys_id|
devTimeFormat=$cef-formatted-time_generated
```

q) If you are using **PAN-OS 10.2**, copy the following text, and paste it in the **Custom Format** column for the **Decryption** log type.

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|$sender_sw_version|$proxy_type|
x7C|ProfileToken=$actionflags|TimeReceived=$receive_time|DeviceSN=$serial|cat$type|
SubType=$subtype|ConfigVersion=$sender_sw_version|devTime=$cef-formatted-receive_time|
src=$src|dst=$dst|srcPostNAT=$natsrc|dstPostNAT=$natdst|Rule=$rule|usrName=$srcuser|
DestinationUser=$dstuser|Application=$app|VirtualLocation=vsys1|FromZone=$from|ToZone=$to|
InboundInterface=$inbound_if|OutboundInterface=$outbound_if|LogSetting=$logset|
TimeReceivedManagementPlane=$time_received|SessionID=$sessionid|CountOfRepeat=$repeatcnt|
srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|dstPostNATPort=$natdport|
proto=$proto|Action=$action|Tunnel=$tunnel|SourceUUID=$src_uuid|DestinationUUID=$dst_uuid|
RuleUUID=$rule_uuid|TLSVersion=$tls_version|TLSKeyExchange=$tls_keyxchg|
TLSEncryptionAlgorithm=$tls_enc|TLSAuth=$tls_auth|PolicyName=$policy_name|
EllipticCurve=$ec_curve|ErrorIndex=$err_index|RootStatus=$root_status|
ChainStatus=$chain_status|CertificateSerial=$cert_serial|Fingerprint=$fingerprint|
TimeNotBefore=$notbefore|TimeNotAfter=$notafter|CertificateVersion=$cert_ver|
CertificateSize=$cert_size|CommonNameLength=$cn_len|IssuerNameLength=$issuer_len|
RootCNLength=$rootcn_len|SNILength=$sni_len|CertificateFlags=$cert_flags|CommonName=$cn|
IssuerCommonName=$issuer_cn|RootCommonName=$root_cn|ServerNameIndication=$sni|
ErrorMessage=$error|ContainerID=$container_id|ContainerNameSpace=$pod_namespace|
ContainerName=$pod_name|SourceEDL=$src_edl|DestinationEDL=$dst_edl|
SourceDynamicAddressGroup=$src_dag|DestinationDynamicAddressGroup=$dst_dag|
TimeGeneratedHighResolution=$high_res_timestamp|SourceDeviceCategory=$src_category|
SourceDeviceProfile=$src_profile|SourceDeviceModel=$src_model|
SourceDeviceVendor=$src_vendor|SourceDeviceOSFamily=$src_osfamily|
SourceDeviceOSVersion=$src_osversion|SourceDeviceHost=$src_host|SourceDeviceMac=$src_mac|
DestinationDeviceCategory=$dst_category|DestinationDeviceProfile=$dst_profile|
DestinationDeviceModel=$dst_model|DestinationDeviceVendor=$dst_vendor|
DestinationDeviceOSFamily=$dst_osfamily|DestinationDeviceOSVersion=$dst_osversion|
DestinationDeviceHost=$dst_host|DestinationDeviceMac=$dst_mac|SequenceNo=$seqno|
devTimeFormat=$cef-formatted-time_generated
```

r) If you are using **PAN-OS 10.0**, copy the following text, and paste it in the **Custom Format** column for the **File Data** log type.

```
LEEF:2.0|Palo Alto Networks|PAN-OS Syslog Integration|
$sender_sw_version|$action|x7C|ProfileToken=$actionflags|TimeReceived=$receive_time|
DeviceSN=$serial|cat=$type|SubType=$subtype|ConfigVersion=$sender_sw_version|
devTime=$cef-formatted-receive_time|src=$src|dst=$dst|srcPostNAT=$natsrc|
dstPostNAT=$natdst|Rule=$rule|usrName=$srcuser|DestinationUser=$dstuser|Application=$app|
VirtualLocation=$vsys|FromZone=$from|ToZone=$to|InboundInterface=$inbound_if|
OutboundInterface=$outbound_if|LogSetting=$logset|SessionID=$sessionid|
RepeatCount=$repeatcnt|srcPort=$sport|dstPort=$dport|srcPostNATPort=$natsport|
dstPostNATPort=$natdport|proto=$proto|Bytes=$bytes|srcBytes=$bytes_sent|
dstBytes=$bytes_received|totalPackets=$packets|SessionStartTime=$start|
SessionDuration=$elapsed|URLCategory=$category|SequenceNo=$seqno|SourceLocation=$srcloc|
DestinationLocation=$dstloc|srcPackets=pkts_sent|dstPackets=$pkts_received|
SessionEndReason=$session_end_reason|DGHierarchyLevel1=$dg_hier_level_1|
DGHierarchyLevel2=$dg_hier_level_2|DGHierarchyLevel3=$dg_hier_level_3|
DGHierarchyLevel4=$dg_hier_level_4|VirtualSystemName=$vsys_name|DeviceName=$device_name|
ActionSource=$action_source|SourceUUID=$src_uuid|DestinationUUID=$dst_uuid|IMSI=$imsi|
IMEI=$imei|ParentSessionID=$parent_session_id|ParentStarttime=parent_start_time|
Tunnel=$tunnel|EndpointAssociationID=-$assoc_id|ChunksTotal=$chunks|
ChunksSent=$chunks_sent|ChunksReceived=$chunks_received|RuleUUID=$rule_uuid|
HTTP2Connection=$http2_connection|LinkChangeCount=$link_change_count|
SDWANPolicyName=$sdwan_ec_applied|LinkSwitches=$link_switches|SDWANCluster=$sdwan_cluster|
SDWANDeviceType=$sdwan_device_type|SDWANClusterType=$sdwan_cluster_type|
SDWANSite=$sdwan_site|DynamicUserGroupName=$dynusergroup_name|
X-Forwarded-ForIP=$xff_ip|SourceDeviceCategory=$src_category|
SourceDeviceProfile=$src_profile|SourceDeviceModel=$src_model|
SourceDeviceVendor=$src_vendor|SourceDeviceOSFamily=$src_osfamily|
SourceDeviceOSVersion=$src_osversion|SourceDeviceHost=$src_host|SourceDeviceMac=$src_mac|
```

```
DestinationDeviceCategory=$dst_category|DestinationDeviceProfile=$dst_profile|
DestinationDeviceModel=$dst_model|DestinationDeviceVendor=$dst_vendor|
DestinationDeviceOSFamily=$dst_osfamily|DestinationDeviceOSVersion=$dst_osversion|
DestinationDeviceHost=$dst_host|DestinationDeviceMac=$dst_mac|ContainerID=$container_id|
ContainerNameSpace=$pod_namespace|ContainerName=$pod_name|SourceEDL=$src_edl|
DestinationEDL=$dst_edl|GPHostID=$hostid|EndpointSerialNumber=$serialnumber|
SourceDynamicAddressGroup=$src_dag|DestinationDynamicAddressGroup=$dst_dag|
HASessionOwner=$session_owner|TimeGeneratedHighResolution=$high_res_timestamp|
NSSAINetworkSliceType=$nssai_sst|NSSAINetworkSliceDifferentiator=$nssai_sd|
devTimeFormat=$cef-formatted-time_generated
```

5. Click **OK**.
6. To specify the severity of events that are contained in the Syslog messages, click **Log Settings**.
   a) For each severity that you want to include in the Syslog message, click the **Severity** name and select the Syslog destination from the **Syslog** menu.
   b) Click **OK**.
7. Click **Commit**.

What to do next

To enable communication between your Palo Alto Networks device and QRadar create a forwarding policy. For more information, see Creating a forwarding policy on your Palo Alto PA Series device.

Forwarding Palo Alto Cortex Data Lake (Next Generation Firewall) LEEF events to IBM QRadar

To send Palo Alto Cortex Data Lake events to QRadar, you must add a TLS Syslog log source in QRadar and configure Cortex Data Lake to forward logs to a Syslog server.

Procedure

1. Add a log source in QRadar by using the TLS Syslog protocol. For more information, see TLS Syslog log source parameters for Palo Alto PA Series.

   Important: If your log source is dedicated only to Cortex Data Lake events, then you must disable **Use as a Gateway Log Source** and set the DSM type to **Palo Alto PA Series**. If the log source is shared with multiple integrations, and you already enabled **Use as a Gateway Log Source**, then the **Log Source Identifier** must use the following regex structure:

   ```
   <Log Source Identifier>=stream-logfwd.*?logforwarder
   ```

2. Forward logs from Cortex Data Lake to QRadar. For more information, see your Palo Alto documentation (https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-log-forwarding-app/forward-logs-from-logging-service-to-syslog-server.html).

   Important:

   - When forwarding logs from Cortex Data Lake, choose the LEEF log format.
   - You must enable the **cat** and **EventStatus/Status** fields in Palo Alto. The **EventStatus/Status** field is required to parse **Global Protect** events in QRadar.

Creating a forwarding policy on your Palo Alto PA Series device

If your IBMQRadar Console or Event Collector is in a different security zone than your Palo Alto PA Series device, create a forwarding policy rule.

Procedure

1. Log in to Palo Alto Networks.
2. Click **Policies** > **Policy Based Forwarding**.

3. Click **Add**.
4. Configure the parameters. For descriptions of the policy-based forwarding values, see your *Palo Alto Networks Administrator's Guide*.

Configuring ArcSight CEF formatted Syslog events on your Palo Alto PA Series Networks Firewall device

Configure your Palo Alto Networks firewall to send ArcSight CEF formatted Syslog events to IBM QRadar.

Procedure

1. Log in to the Palo Alto Networks interface.
2. Click the **Device** tab.
3. Select **Server Profiles** > **Syslog**.
4. Click **Add**.
5. Specify the name, server IP address, port, and facility of the QRadar system that you want to use as a Syslog server:
   a) The **Name** is the Syslog server name.
   b) The **Syslog Server** is the IP address for the Syslog server.
   c) The **Transport** default is **UDP**.
   d) The **Port** default is **514**.
   e) The **Faculty** default is **LOG_USER**.
6. To select any of the listed log types that define a custom format, based on the ArcSight CEF for that log type, complete the following steps:
   a) Click the **Custom Log Format** tab and select any of the listed log types to define a custom format based on the ArcSight CEF for that log type. The listed log types are **Config**, **System**, **Threat**, **Traffic**, and **HIP Match**.
   b) Click **OK** twice to save your entries, then click **Commit**.
7. To define your own CEF-style formats that use the event mapping table that is provided in the ArcSight document, *Implementing ArcSight CEF*, you can use the following information about defining CEF style formats:
   a) The **Custom Log Format** tab supports escaping any characters that are defined in the CEF as special characters. For example, to use a backslash to escape the backslash and equal characters, enable the **Escaping** check box, specify `\=` as the **Escaped Characters** and `\` as the **Escape Character**.
   b) The following list displays the CEF-style format that was used during the certification process for each log type. These custom formats include all of the fields, in a similar order, that the default format of the Syslogs display.

      Important: Due to PDF formatting, do not copy and paste the message formats directly into the PAN-OS web interface. Instead, paste into a text editor, remove any carriage return or line feed characters, and then copy and paste into the web interface.

      Traffic

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type|1|rt=$cef-formatted-receive_time
deviceExternalId=$serial src=$src dst=$dst sourceTranslatedAddress=$natsrc
destinationTranslatedAddress=$natdst cs1Label=Rule cs1=$rule suser=$srcuser
duser=$dstuser app=$app cs3Label=Virtual System cs3=$vsys
cs4Label=Source Zone cs4=$from cs5Label=Destination Zone
cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if
cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid
cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport
destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags
proto=$proto act=$action flexNumber1Label=Total bytes flexNumber1=$bytes
in=$bytes_sent out=$bytes_received cn2Label=Packets cn2=$packets
PanOSPacketsReceived=$pkts_received PanOSPacketsSent=$pkts_sent start=$cef-formatted-
```

```
time_generated cn3Label=Elapsed time in seconds cn3=$elapsed cs2Label=URL Category
cs2=$category externalId=$seqno
```

Threat

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type|$number-of-severity|rt=$cef-
formatted-receive_time deviceExternalId=$serial src=$src dst=$dst
sourceTranslatedAddress=$natsrc destinationTranslatedAddress=$natdst cs1Label=Rule
cs1=$rule suser=$srcuser duser=$dstuser app=$app cs3Label=Virtual System
cs3=$vsys cs4Label=Source Zone cs4=$from cs5Label=Destination Zone
cs5=$to deviceInboundInterface=$inbound_if deviceOutboundInterface=$outbound_if
cs6Label=LogProfile cs6=$logset cn1Label=SessionID cn1=$sessionid
cnt=$repeatcnt spt=$sport dpt=$dport sourceTranslatedPort=$natsport
destinationTranslatedPort=$natdport flexString1Label=Flags flexString1=$flags
proto=$proto act=$action request=$misc cs2Label=URL Category
cs2=$category flexString2Label=Direction flexString2=$direction externalId=$seqno
requestContext=$contenttype cat=$threatid filePath=$cloud fileId=$pcap_id
fileHash=$filedigest
```

Config

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$result|$type|1|rt=$cef-formatted-receive_time
deviceExternalId=$serial dvchost=$host cs3Label=Virtual System cs3=$vsys act=$cmd
duser=$admin destinationServiceName=$client msg=$path externalId=$seqno
```

Optional:

```
cs1Label=Before Change Detail cs1=$before-change-detail cs2Label=After Change Detail
cs2=$after-change-detail
```

System

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$subtype|$type|$number-of-severity|rt=$cef-
formatted-receive_time deviceExternalId=$serial cs3Label=Virtual System
cs3=$vsys fname=$object flexString2Label=Module flexString2=$module msg=$opaque
externalId=$seqno cat=$eventid
```

HIP Match

```
CEF:0|Palo Alto Networks|PAN-OS|6.0.0|$matchtype|$type|1|rt=$cef-formatted-
receive_time deviceExternalId=$serial suser=$srcuser cs3Label=Virtual System
cs3=$vsys shost=$machinename src=$src cnt=$repeatcnt externalId=$seqno cat=$matchname
cs2Label=Operating System cs2=$os
```

What to do next

For more information about Syslog configuration, see the *PAN-OS Administrator's Guide* on the Palo Alto Networks website (https://www.paloaltonetworks.com).

TLS Syslog log source parameters for Palo Alto PA Series

If IBM QRadar does not automatically detect the log source, add a Palo Alto PA Series log source on the QRadar Console by using the TLS Syslog protocol.

When you use the TLS Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect TLS Syslog events from Palo Alto PA Series:

Table 867. TLS Syslog log source parameters for the Palo Alto PA Series DSM

Parameter	Value
Log Source type	Palo Alto PA Series
Protocol Configuration	TLS Syslog
Log Source Identifier	An IP address or hostname to identify the log source.

For a complete list of TLS Syslog protocol parameters and their values, see TLS Syslog protocol configuration options.

Related tasks

Adding a log source

Palo Alto PA Series Sample event message

Use these sample event messages to verify a successful integration with QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Palo Alto PA Series sample message when you use the Syslog protocol

Sample 1: The following sample event message shows PAN-OS events for a trojan threat event.

```
<180>May  6 16:43:53 paloalto.paseries.test LEEF:1.0|
Palo Alto Networks|PAN-OS Syslog Integration|8.1.6|trojan/
PDF.gen.eiez(268198686)|ReceiveTime=2019/05/06 16:43:53|SerialNumber=001801010877|cat=THREAT|
Subtype=virus|devTime=May 06 2019 11:13:53 GMT|src=10.2.75.41|dst=192.168.178.180|
srcPostNAT=192.168.68.141|dstPostNAT=192.168.178.180|RuleName=Test-1|usrName=qradar\\user1|
SourceUser=qradar\\user1|DestinationUser=|Application=web-browsing|VirtualSystem=vsys1|
SourceZone=INSIDE-ZN|DestinationZone=OUTSIDE-ZN|IngressInterface=ethernet1/1|
EgressInterface=ethernet1/3|LogForwardingProfile=testForwarder|SessionID=3012|RepeatCount=1|
srcPort=63508|dstPort=80|srcPostNATPort=31539|dstPostNATPort=80|Flags=0x406000|proto=tcp|
action=alert|Miscellaneous=\"qradar.example.test/du/uploads/08052018_UG_FAQ.pdf\"|
ThreatID=trojan/PDF.gen.eiez(268198686)|URLCategory=educational-institutions|sev=3|
Severity=medium|Direction=server-to-client|sequence=486021038|ActionFlags=0xa000000000000000|
SourceLocation=10.0.0.0-10.255.255.255|DestinationLocation=testPlace|ContentType=|
PCAP_ID=0|FileDigest=|Cloud=|URLIndex=5|RequestMethod=|Subject=|DeviceGroupHierarchyL1=12|
DeviceGroupHierarchyL2=0|DeviceGroupHierarchyL3=0|DeviceGroupHierarchyL4=0|vSrcName=|
DeviceName=testName|SrcUUID=|DstUUID=|TunnelID=0|MonitorTag=|ParentSessionID=0|ParentStartTime=|
TunnelType=N/A|ThreatCategory=pdf|ContentVer=Antivirus-2969-3479
```

Table 868. Highlighted fields in the sample event

QRadar field name	Highlighted payload fields
Event ID	The Event ID value is 268198686. **Note:** Usually the Event ID field from the LEEF header is used. However, for certain event types, more LEEF fields or custom fields such as **Subtype**, and **action** might be used to form a unique event ID.
Category	PA Series Threat **Note:** The value of the **cat** field is not used directly as the **Category** of the event. The value of this field is used to determine a predefined set of category values. For certain event types, more LEEF fields or custom fields can be used to form a unique event **Category**.
Device Time	devTime
Source IP	src
Destination IP	dst
Source Port	srcPort
Destination Port	dstPort
Post NAT Source IP	srcPostNAT
Post NAT Destination IP	dstPostNAT
Post NAT Soure Port	srcPostNATPort

Table 868. Highlighted fields in the sample event (continued)	
QRadar field name	**Highlighted payload fields**
Post NAT Destination Port	dstPostNATPort
Protocol	proto

Sample 2: The following sample event message shows a Prisma event where a session is allowed by a policy.

```
<14>1 2021-10-26T13:56:21.887Z paloalto.paseries.test logforwarder -
panwlogs - LEEF:2.0|Palo Alto Networks|Prisma Access|2.1|allow|    |
TimeReceived=2021-10-26T13:56:20.000000Z   DeviceSN=no-serial  cat=traffic SubType=start
ConfigVersion=10.0  devTime=2021-10-26T13:56:17.000000Z src=192.168.21.100  dst=172.16.0.3
srcPostNAT=172.16.0.4   dstPostNAT=172.16.0.5   Rule=CG-RN-Guest-to-Internet    usrName=
DestinationUser=    Application=web-browsing    VirtualLocation=vsys1   FromZone=FromZone
ToZone=untrust  InboundInterface=tunnel.101 OutboundInterface=ethernet1/1   LogSetting=to-
Cortex-Data-Lake  SessionID=49934 RepeatCount=1   srcPort=59532   dstPort=80
sr=49718    dstPostNATPort=80   proto=tcp   Bytes=374   srcBytes=300    dstBytes=74
totalPackets=4  SessionStartTime=2021-10-26T13:56:15.000000Z    SessionDuration=0
URLCategory=any SequenceNo=13336648 SourceLocation=192.168.0.0-192.168.255.255
DestinationLocation=CA  srcPackets=3    dstPackets=1    SessionEndReason=n-
a    DGHierarchyLevel1=62    DGHierarchyLevel2=38    DGHierarchyLevel3=53
DGHierarchyLevel4=0 VirtualSystemName=  DeviceName=DeviceName   ActionSource=from-
policy    SourceUUID= DestinationUUID=    IMSI=0  IMEI=   ParentSessionID=0
ParentStarttime=1970-01-01T00:00:00.000000Z Tunnel=N/A  EndpointAssociationID=0 ChunksTotal=0
ChunksSent=0    ChunksReceived=0    RuleUUID=00000000-0000-0000-0000-000000000000
HTTP2Connection=0   LinkChangeCount=0   SDWANPolicyName=    LinkSwitches=   SDWANCluster=
SDWANDeviceType=    SDWANClusterType=   SDWANSite=  DynamicUserGroupName=   X-
Forwarded-ForIP=  SourceDeviceCategory=   SourceDeviceProfile=    SourceDeviceModel=
SourceDeviceVendor= SourceDeviceOSFamily=   SourceDeviceOSVersion=  SourceDeviceHost=
SourceDeviceMac=    DestinationDeviceCategory=  DestinationDeviceProfile=
DestinationDeviceModel= DestinationDeviceVendor=    DestinationDeviceOSFamily=
DestinationDeviceOSVersion= DestinationDeviceHost=  DestinationDeviceMac=   ContainerID=
ContainerNameSpace= ContainerName=  SourceEDL=  DestinationEDL= GPHostID=
EndpointSerialNumber=   SourceDynamicAddressGroup=  DestinationDynamicAddressGroup=
HASessionOwner= TimeGeneratedHighResolution=2021-10-26T13:56:17.911000Z NSSAINetworkSliceType=
NSSAINetworkSliceDifferentiator=    devTimeFormat=YYYY-MM-DD'T'HH:mm:ss.SSSZ
```

Table 869. Highlighted fields in the sample event	
QRadar field name	**Highlighted payload fields**
Event ID	The **Event ID** value is **allow**.
Event Category	PA Series Traffic **Note:** The value of the **cat** field is not used directly as the **Category** of the event. The value of this field is used to determine a predefined set of category values. For certain event types, more LEEF fields or custom fields can be used to form a unique event **Category**.
Device Time	devTime
Source IP	src
Destination IP	dst
Source Port	srcPort
Destination Port	dstPort
Post NAT Source IP	srcPostNAT
Post NAT Destination IP	dstPostNAT
Post NAT Soure Port	sr
Post NAT Destination Port	dstPostNATPort

Table 869. Highlighted fields in the sample event (continued)	
QRadar field name	**Highlighted payload fields**
Protocol	proto

Palo Alto PA Series sample message when you use the TLS Syslog protocol

The following sample event message shows Next Generation Firewall events for version 10.1.

```
<14>1 2021-08-09T14:00:26.364Z paloalto.paseries.test logforwarder - panwlogs
- LEEF:2.0|Palo Alto Networks|Next Generation Firewall|10.1|drop-all| |
TimeReceived=2021-08-09T14:00:25.000000Z DeviceSN=001011000011111 cat=gtp SubType=end
ConfigVersion=10.1 devTime=2021-08-09T14:00:22.000000Z src=fc00:0:e426:5678:b202:b3ff:fe1e:8329
dst=fc00:5678:90aa:cc33:f202:b3ff:fe1e:8329 srcPostNAT=10.5.5.5 dstPostNAT=192.168.178.180
Rule=allow-all-employees usrName=paloaltonetwork\testUser DestinationUser=paloaltonetwork\tUser
Application=adobe-cq VirtualLocation=aaaa1 FromZone=corporate ToZone=corporate
InboundInterface=ethernet1/1 OutboundInterface=ethernet1/3 LogSetting=rs-logging
SessionID=1111111 RepeatCount=1 srcPort=10273 dstPort=27624 srcPostNATPort=26615
dstPostNATPort=6501 proto=tcp TunnelEventType=51 MobileSubscriberISDN=
AccessPointName= RadioAccessTechnology=11 TunnelMessageType=0 MobileIP=
TunnelEndpointID1=0 TunnelEndpointID2=0 TunnelInterface=0 TunnelCauseCode=0
VendorSeverity=Unused MobileCountryCode=0 MobileNetworkCode=0 MobileAreaCode=0
MobileBaseStationCode=0 TunnelEventCode=0 SequenceNo=1111111111111111111 SourceLocation=NB
DestinationLocation=saint john DGHierarchyLevel1=12 DGHierarchyLevel2=0 DGHierarchyLevel3=0
DGHierarchyLevel4=0 VirtualSystemName= DeviceName=PA-VM IMSI=28 IMEI=datacenter
ParentSessionID=1111111 ParentStarttime=1970-01-01T00:00:00.000000Z Tunnel=tunnel
Bytes=741493 srcBytes=277595 dstBytes=463898 totalPackets=1183 srcPackets=554
dstPackets=629 PacketsDroppedMax=58 PacketsDroppedProtocol=34 PacketsDroppedStrict=171
PacketsDroppedTunnel=773 TunnelSessionsCreated=537 TunnelSessionsClosed=206
SessionEndReason=unknown ActionSource=unknown startTime=2021-08-09T13:59:51.000000Z
SessionDuration=35 TunnelInspectionRule=gtp TunnelRemoteUserIP= TunnelRemoteIMSIID=0
RuleUUID=11a111aa-1a11-1a1a-11a1-1a11a11111a1 DynamicUserGroupName=dynug-4 ContainerID=
ContainerNameSpace= ContainerName= SourceEDL= DestinationEDL= SourceDynamicAddressGroup=
DestinationDynamicAddressGroup= TimeGeneratedHighResolution=2021-08-09T14:00:22.079000Z
NSSAINetworkSliceDifferentiator=0 NSSAINetworkSliceType=0 ProtocolDataUnitsessionID=0
devTimeFormat=YYYY-MM-DDTHH:mm:ss.SSSSSSZ
```

Table 870. Highlighted fields in the sample event	
QRadar field name	**Highlighted payload fields**
Event ID	drop-all (LEEF header **Event ID** field) **Note:** Usually the **Event ID** field from the LEEF header is used. However, for certain event types, more LEEF fields or custom fields such as **Subtype**, and **action** might be used to form a unique event ID.
Category	PA Series GTP **Note:** The value of the **cat** field is not used directly as the **Category** of the event. The value of this field is used to determine a predefined set of category values. For certain event types, more LEEF fields or custom fields can be used to form a unique event **Category**.
Device Time	devTime
Source IPv6	src
Destination IPv6	dst
Source Port	SrcPort
Destination Port	dstPort
Post NAT Source IP	srcPostNAT
Post NAT Destination IP	dstPostNAT

Table 870. Highlighted fields in the sample event (continued)	
QRadar field name	**Highlighted payload fields**
Post NAT Soure Port	srcPostNATPort
Post NAT Destination Port	dstPostNATPort
Protocol	tcp
Username	usrName **Tip:** If a username contains the domain as part of its value, the domain portion is removed and only the actual username portion is used.

Chapter 123. PingFederate

The IBM QRadar DSM for PingFederate collects CEF events from a PingFederate server.

To integrate PingFederate with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from IBM support. Download and install the most recent version of the PingFederateRPM on your QRadar Console.
2. Configure your PingFederate device to send events to QRadar. For more information, see Configuring PingFederate to communicate with IBM QRadar.
3. If QRadar does not automatically detect the log source, add a PingFederate log source on the QRadar Console. For more information, see Syslog log source parameters for PingFederate.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

PingFederate DSM specifications

The IBM QRadar DSM for PingFederate supports events that are collected from PingFederate with the help of the Syslog protocol.

The following table lists the specifications for the PingFederate DSM.

Table 871. PingFederate DSM specifications

Specification	Value
Manufacturer	Ping Identity
DSM name	PingFederate
RPM file name	DSM-*PingFederate-QRadar_version-Build_number*.noarch.rpm
Supported protocols	Syslog
Event format	CEF
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	PingFederate Server

Configuring PingFederate to communicate with IBM QRadar

To collect PingFederate events, configure your PingFederate to send CEF events to QRadar.

The IBM QRadar DSM for PingFederate supports events that are collected from PingFederate with the help of the Syslog protocol.

Procedure

1. Configure PingFederate to communicate with QRadar by following the configuration steps in the PingFederate writing audit log.
2. Edit `log4j2.xml` file present at the location - `<pf_install>/pingfederate/server/default/conf/log4j2.xml`.

3. Add the below details to `log4j2.xml`.

```
<Socket name="SecurityAuditToCEFSyslog" host="<Qradar_host>" port="514" protocol="TCP"
ignoreExceptions="false">            <PingSyslogLayout>
    <PatternLayout>
       <pattern>%escape{CEF}{CEF:0|Ping Identity|PingFederate|%X{pfversion}|%X{event}|
%X{event}|0|rt=%d{MMM dd yyyy HH:mm:ss.SSS} duid=%X{subject} src=%X{ip} msg=%X{status}
cs1Label=Target Application URL cs1=%X{app} cs2Label=Connection ID cs2=%X{connectionid}
cs3Label=Protocol cs3=%X{protocol} dvchost=%X{host} cs4Label=Role cs4=%X{role}
externalId=%X{trackingid} cs5Label=SP Local User ID cs5=%X{localuserid} cs6Label=Attributes
cs6=%X{attributes} %n}</pattern>
     </PatternLayout>
</PingSyslogLayout>
</Socket>
```

What to do next

Add a PingFederate - Syslog log source in QRadar. For more information, see Syslog log source parameters for PingFederate.

Syslog log source parameters for PingFederate

The IBM QRadar DSM for PingFederate collects security audit logging events from a PingFederate server.

If QRadar does not automatically detect the log source, add a PingFederate log source on the QRadar Console by using the Syslog protocol.

Configure specific parameters when you are using the Syslog protocol.

The following table describes the parameters that require specific values to collect the security audit logging events from PingFederate:

Table 872. PingFederate log source parameters

Parameter	Value
Log Source type	PingFederate
Protocol Configuration	Syslog
Log Source Identifier	Type a unique name for the log source.

For more information about the protocol parameters and their values, see Adding a log source.

PingFederate sample event message

Use these sample event messages to verify a successful integration with IBM QRadar.

PingFederate sample message when you use the Syslog protocol: Authentication Attempt

The following sample event message shows that the event indicates an authentication attempt against an identity provider (IdP) adapter instance, and also an authentication request sent to another identity provider instance through an identity provider connection.

```
CEF:0|Ping Identity|PingFederate|12.0|AUTHN_ATTEMPT|AUTHN_ATTEMPT|0|rt=Feb 02 2024 15:49:12.139
duid= src=127.0.0.1 msg=inprogress cs1Label=Target Application URL cs1= cs2Label=Connection
ID cs2=IAMShowcase cs3Label=Protocol cs3=SAML20 dvchost=ip-127-0-0-1.ec2.internal cs4Label=Role
cs4=IdP externalId=tid:x7PBlk1Y1ZA0vnTest_iRSN1Q cs5Label=SP Local User ID cs5=
cs6Label=Attributes cs6=
```

Table 873. Highlighted values in the PingFederate sample event

QRadar field name	Highlighted payload field name
Event ID	The value in QRadar is **AUTHN_ATTEMPT_inprogress**

Table 873. Highlighted values in the PingFederate sample event (continued)	
QRadar field name	**Highlighted payload field name**
Source IP	**src**
Device Time	**rt**

PingFederate sample message when you use the Syslog protocol: Single Sign-On (SSO)

The following sample event message shows that the event indicates the process of authenticating an identity (sign-on) at a website (with a user ID and a password), and then accessing resources secured by other domains without re-authentication.

```
CEF:0|Ping Identity|PingFederate|12.0|SSO|SSO|0|rt=Feb 02 2024 15:49:15.178 duid=testuser
src=127.0.0.1 msg=success cs1Label=Target Application URL cs1= cs2Label=Connection ID
cs2=IAMShowcase cs3Label=Protocol cs3=SAML20 dvchost=ip-127-0-0-1.ec2.internal cs4Label=Role
cs4=IdP externalId=tid:x7PBlk1Y1ZATest_iRSN1Q cs5Label=SP Local User ID cs5=
cs6Label=Attributes cs6=SAML_SUBJECT\=testuser, email\=testuser@example.com
```

Table 874. Highlighted values in the PingFederate sample event	
QRadar field name	**Highlighted payload field name**
Event ID	The value in QRadar is **SSO_success**
Source IP	**src**
Device Time	**rt**

Chapter 124. Pirean Access: One

The Pirean Access: One DSM for IBM QRadar collects events by polling the DB2 audit database for access management, and authentication events.

QRadar supports Pirean Access: One software installations at v2.2 that use a DB2 v9.7 database to store *access management* and *authentication* events.

Before you begin

Before you configure QRadar to integrate with Pirean Access: One, you can create a database user account and password for QRadar. Creating a QRadar account is not required, but is beneficial as it secures your *access management* and *authentication* event table data for the QRadar user.

Your QRadar user needs read permission access for the database table that contains your events. The JDBC protocol allows QRadar to log in and poll for events from the database based on the time stamp to ensure that the most recent data is retrieved.

Note: Ensure that firewall rules do not block communication between your Pirean Access: One installation and the QRadar Console or managed host responsible for event polling with JDBC.

JDBC log source parameters for Pirean Access: One

If QRadar does not automatically detect the log source, add a Pirean Access: One log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Pirean Access: One:

Parameter	Description
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source Type	**Pirean Access: One**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	**DB2**
Database Name	Type the name of the database to which you want to connect. The default database name is LOGINAUD.

Parameter	Description
IP or Hostname	Type the IP address or host name of the database server.
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix - 9088 • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the **Port** field blank.
Username	A user account for QRadar in the database.
Password	The password that is required to connect to the database.
Confirm Password	The password that is required to connect to the database.
Table Name	Type AUDITDATA as the name of the table or view that includes the event records. The table name can be up to 255 alphanumeric characters in length. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Select List	Type * to include all fields from the table or view. You can use a comma-separated list to define specific fields from tables or views, if it is needed for your configuration. The list must contain the field that is defined in the **Compare Field** parameter. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type **TIMESTAMP** to identify new events added between queries to the table. The compare field can be up to 255 alphanumeric characters in length. The list can include the special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Use Prepared Statements	Select this check box to use prepared statements, which allows the JDBC protocol source to set up the SQL statement one time, then run the SQL statement many times with different parameters. For security and performance reasons, it is suggested that you use prepared statements. Clear this check box to use an alternative method of querying that does not use pre-compiled statements.

Parameter	Description
Start Date and Time (Optional)	Optional. Configure the start date and time for database polling. The **Start Date and Time** parameter must be formatted as yyyy-MM-dd HH: mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values without an H or M designator poll in seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 20,000 EPS.
Security Mechanism	From the list, select the security mechanism that is supported by your DB2 server. If you don't want to select a security mechanism, select **None**. The default is **None**. For more information about security mechanisms that are supported by DB2 environments, see the IBM Support website (https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html)
Enabled	Select this check box to enable the Pirean Access: One log source.

For a complete list of JDBC protocol parameters and their values, see “JDBC protocol configuration options” on page 147.

Related tasks

“Adding a log source” on page 5

Chapter 125. PostFix Mail Transfer Agent

IBM QRadar can collect and categorize syslog mail events from PostFix Mail Transfer Agents (MTA) installed in your network.

To collect syslog events, you must configure PostFix MTA installation to forward syslog events to QRadar. QRadar does not automatically discover syslog events that are forwarded from PostFix MTA installations as they are multiline events. QRadar supports syslog events from PostFix MTA V2.6.6.

To configure PostFix MTA, complete the following tasks:

1. On your PostFix MTA system, configure `syslog.conf` to forward mail events to QRadar.
2. On your QRadar system, create a log source for PostFix MTA to use the UDP multiline syslog protocol.
3. On your QRadar system, configure IPtables to redirect events to the port defined for UDP multiline syslog events.
4. On your QRadar system, verify that your PostFix MTA events are displayed on the **Log Activity** tab.

If you have multiple PostFix MTA installations where events go to different QRadar systems, you must configure a log source and IPtables for each QRadar system that receives PostFix MTA multiline UDP syslog events.

Configuring syslog for PostFix Mail Transfer Agent

To collect events, you must configure syslog on your PostFix MTA installation to forward mail events to IBM QRadar.

Procedure

1. Use SSH to log in to your PostFix MTA installation as a root user.
2. Edit the following file:

   `/etc/syslog.conf`
3. To forward all mail events, type the following command to change `-/var/log/maillog/` to an IP address. Make sure that all other lines remain intact:

   `mail.*@<IP address>`

   Where <*IP address*> is the IP address of the QRadar Console, Event Processor, or Event Collector, or all-in-one system.
4. Save and exit the file.
5. Restart your syslog daemon to save the changes.

UDP Multiline Syslog log source parameters for PostFix MTA

If QRadar does not automatically detect the log source, add a PostFix MTA log source on the QRadar Console by using the UDP Multiline Syslog protocol.

When using the UDP Multiline Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect UDP Multiline Syslog events from PostFix MTA:

Table 875. UDP Multiline Syslog log source parameters for the PostFix MTA DSM	
Parameter	**Description**
Log Source Identifier	Type the IP address, host name, or name to identify your PostFix MTA installation.
Listen Port	Type **517** as the port number used by QRadar to accept incoming UDP Multiline Syslog events. The valid port range is 1 - 65535. To edit a saved configuration to use a new port number: 1. In the **Listen Port** field, type the new port number for receiving UDP Multiline Syslog events. 2. Click **Save**. 3. On the **Admin** tab toolbar, click **Deploy Changes** to make this change effective. The port update is complete and event collection starts on the new port number.
Message ID Pattern	Type the following regular expression (regex) needed to filter the event payload messages. `postfix/.*?[ \[]\d+[ \]](?:- - |: )([A-Z0-9]{8,})`
Enabled	Select this check box to enable the log source.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

For a complete list of UDP Multiline Syslog protocol parameters and their values, see "UDP multiline syslog protocol configuration options" on page 233.

Related tasks

"Adding a log source" on page 5

Configuring IPtables for multiline UDP syslog events

To collect events, you must redirect events from the standard PostFix MTA port to port 517 for the UDP multiline protocol.

Procedure

1. Use SSH to log in to IBM QRadar as the root user.
2. To edit the IPtables file, type the following command:

   ```
   vi /opt/qradar/conf/iptables-nat.post
   ```
3. To instruct QRadar to redirect syslog events from UDP port 514 to UDP port 517, type the following command:

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>
   ```

   Where:

   - <*IP address*> is the IP address of your PostFix MTA installation.
   - <*New port*> is the port number that is configured in the UDP Multiline protocol for PostFix MTA.

   For example, if you had three PostFix MTA installations that communicate to QRadar, you can type the following code:

   ```
   -A PREROUTING -p udp --dport 514 -j
   REDIRECT --to-port 517 -s <IP_address1> -A PREROUTING -p udp --dport 514 -j
   REDIRECT --to-port 517 -s <IP_address2> -A PREROUTING -p udp --dport 514 -j
   REDIRECT --to-port 517 -s <IP_address3>
   ```
4. Save your IPtables NAT configuration.

   You are now ready to configure IPtables on your QRadar Console or Event Collector to accept events from your PostFix MTA installation.
5. Type the following command to edit the IPtables file:

   ```
   vi /opt/qradar/conf/iptables.post
   ```
6. Type the following command to instruct QRadar to allow communication from your PostFix MTA installations:

   ```
   -I QChain 1 -m udp -p udp --src <IP address> --dport <New port> -j ACCEPT
   ```

   Where:

   - <*IP address*> is the IP address of your PostFix MTA installation.
   - <*New port*> is the port number that is configured in the UDP Multiline protocol.

   For example, if you had three PostFix MTA installations that communicate with an Event Collector, you can type the following code:

   ```
   -I QChain 1 -m udp -p udp --src <IP_address1>
   --dport 517 -j ACCEPT -I QChain 1 -m udp -p udp
   --src <IP_address2> --dport 517 -j ACCEPT -I QChain 1 -m udp -p udp
   --src <IP_address3> --dport 517 -j ACCEPT
   ```
7. To save the changes and update IPtables, type the following command:

   ```
   ./opt/qradar/bin/iptables_update.pl
   ```

PostFix Mail Transfer Agent sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

PostFix Mail Transfer Agent sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that an email is sent successfully.

```
<22>Mar 5 13:09:45 postfix.mailtransferagent.test postfix/smtpd[7609]: B83C6210AB:
client=unknown[192.168.0.14] message-id=<27914646.772901551755385716.JavaMail.root@testsrv1>
from=<user4@exampledomain.test>, size=564564, nrcpt=1 (queue active)
to=<user01@host.example.test>, relay=apc.olc.protection.server.test[192.168.126.33]:25,
delay=3.4, delays=0.03/0/0.62/2.7, dsn=2.6.0, status=sent (250
2.6.0 <27914646.772901551755385716.JavaMail.root@testsrv1> [InternalId=19877108654932,
Hostname=SERVER.PROD.EXAMPLE.TEST] 570417 bytes in 2.113, 263.513 KB/sec Queued mail for delivery
-> 250 2.1.5) removed
```

```
<22>Mar 5 13:09:45 postfix.mailtransferagent.test postfix/smtpd[7609]: B83C6210AB:
client=unknown[192.168.0.14] message-id=<27914646.772901551755385716.JavaMail.root@testsrv1>
from=<user4@exampledomain.test>, size=564564, nrcpt=1 (queue active)
to=<user01@host.example.test>, relay=apc.olc.protection.server.test[192.168.126.33]:25,
delay=3.4, delays=0.03/0/0.62/2.7, dsn=2.6.0, status=sent (250
2.6.0 <27914646.772901551755385716.JavaMail.root@testsrv1> [InternalId=19877108654932,
Hostname=SERVER.PROD.EXAMPLE.TEST] 570417 bytes in 2.113, 263.513 KB/sec Queued mail for
delivery -> 250 2.1.5) removed
```

Table 876. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**B83C6210AB**
Number of Recipients (custom property)	**1**
Username	**user4@+exampledomain.test**
Originating Host (custom property)	**exampledomain.test**
Originating User (custom property	**user4@+exampledomain.test**
Recipient Host (custom property)	**host.example.test**
Recipient User (custom property)	**user01@+host.example.test**
Source IP	**192.168.0.14**
Destination Port	**192.168.126.33**
Destination Port	**25**

Sample 2: The following sample event message shows that an email is received.

```
<22>Jun 19 15:41:12 postfix.mailtransferagent.test postfix/qmgr[12345]: FFFFFFF:
from=<User.Name@domain1.test>, size=3806, nrcpt=1 (queue active)
```

```
<22>Jun 19 15:41:12 postfix.mailtransferagent.test postfix/qmgr[12345]: FFFFFFF:
from=<User.Name@domain1.test>, size=3806, nrcpt=1 (queue active)
```

Table 877. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**qmgr**
Username	**User.Name@domain1.test**
Message Size (custom property)	**3806**
MessageID (custom property)	**FFFFFFF**

Tip:

Use the *IBM® QRadar® Custom Properties for Postfix* to closely monitor your Custom Properties for Postfix deployment. The Postfix custom event properties expand your QRadar searches and reports by normalizing specific event data from a log source. If the *IBM QRadar Custom Properties for Postfix* content pack is not installed on your system, download it from the IBM X-Force® Exchange website (https://exchange.xforce.ibmcloud.com/hub).

Chapter 126. ProFTPd

IBM QRadar can collect events from a ProFTP server through syslog.

By default, ProFTPd logs authentication related messages to the local syslog using the **auth** (or **authpriv**) facility. All other logging is done using the daemon facility. To log ProFTPd messages to QRadar, use the SyslogFacility directive to change the default facility.

Configuring ProFTPd

You can configure syslog on a ProFTPd device:

Procedure

1. Open the `/etc/proftd.conf` file.
2. Below the LogFormat directives add the following line:

   `SyslogFacility <facility>`

   Where <*facility*> is one of the following options: **AUTH** (or **AUTHPRIV**), **CRON**, **DAEMON**, **KERN**, **LPR**, **MAIL**, **NEWS**, **USER**, **UUCP**, **LOCAL0**, **LOCAL1**, **LOCAL2**, **LOCAL3**, **LOCAL4**, **LOCAL5**, **LOCAL6**, or **LOCAL7**.
3. Save the file and exit.
4. Open the `/etc/syslog.conf` file
5. Add the following line at the end of the file:

   `<facility> @<QRadar host>`

   Where:

   <*facility*> matches the facility that is chosen in "Configuring ProFTPd" on page 1373. The facility must be typed in lowercase.

   <*QRadar host*> is the IP address of your QRadar Console or Event Collector.
6. Restart syslog and ProFTPd:

   `/etc/init.d/syslog restart`

   `/etc/init.d/proftpd restart`

What to do next

You can now configure the log source in QRadar.

Syslog log source parameters for ProFTPd

If QRadar does not automatically detect the log source, add a ProFTPd log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from ProFTPd:

Table 878. Syslog log source parameters for the ProFTPd DSM

Parameter	Value
Log Source type	ProFTPd Server
Protocol Configuration	Syslog

Table 878. Syslog log source parameters for the ProFTPd DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ProFTPd installation.

Related tasks

“Adding a log source” on page 5

Chapter 127. Proofpoint Enterprise Protection and Enterprise Privacy

The IBM QRadar DSM for Proofpoint Enterprise Protection and Enterprise privacy can collect events from your Proofpoint Enterprise Protection and Enterprise Privacy DSM servers.

The following table identifies the specifications for the Proofpoint Enterprise Protection and Enterprise Privacy DSM:

Table 879. Proofpoint Enterprise Protection and Enterprise Privacy DSM specifications

Specification	**Value**
Manufacturer	Proofpoint
DSM name	Proofpoint Enterprise Protection/Enterprise Privacy
RPM file name	`DSM-Proofpoint_Enterprise_Protection/Enterprise_Privacy-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V7.02 V7.1 V7.2 V7.5 V8.0
Protocol	Syslog Log File
Recorded event types	System Email security threat classification Email audit and encryption
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Proofpoint website (https://www.proofpoint.com/us/solutions/products/enterprise-protection)

To integrate the Proofpoint Enterprise Protection and Enterprise Privacy DSM with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Proofpoint Enterprise Protection and Enterprise Privacy DSM RPM from the IBM Support Website onto your QRadar Console.
2. For each instance of Proofpoint Enterprise Protection and Enterprise Privacy, configure your Proofpoint Enterprise Protection and Enterprise Privacy DSM appliance to enable communication with QRadar.
3. Add a Proofpoint Enterprise Protection and Enterprise Privacy log source on your QRadar Console.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Proofpoint Enterprise Protection and Enterprise Privacy DSM to communicate with IBM QRadar

To collect all audit logs and system events from your Proofpoint Enterprise Protection and Enterprise Privacy DSM, you must add a destination that specifies IBM QRadar as the Syslog server.

Procedure

1. Log in to the Proofpoint Enterprise interface.
2. Click **Logs and Reports**.
3. Click **Log Settings.**
4. From the **Remote Log Settings** pane, configure the following options to enable Syslog communication:
   a) Select **Syslog** as the communication protocol.
5. Type the IP address of the QRadar Console or Event Collector.
6. In the **Port** field, type 514 as the port number for Syslog communication.
7. From the **Syslog Filter Enable** list, select **On**.
8. From the **Facility** list, select **local1**.
9. From the **Level** list, select **Information**.
10. From the **Syslog MTA Enable** list, select **On**.
11. Click **Save**

Syslog log source parameters for Proofpoint Enterprise Protection and Enterprise Privacy

If QRadar does not automatically detect the log source, add a Proofpoint Enterprise Protection and Enterprise Privacy log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Proofpoint Enterprise Protection and Enterprise Privacy:

Table 880. Syslog log source parameters for the Proofpoint Enterprise Protection and Enterprise Privacy DSM

Parameter	Value
Log Source type	Proofpoint Enterprise Protection/Enterprise Privacy
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name for the log source as an identifier for events from Proofpoint Enterprise Protection and Enterprise Privacy installations. For each additional log source that you create when you have multiple installations, include a unique identifier, such as an IP address or host name

Related tasks

"Adding a log source" on page 5

Proofpoint Enterprise Protection and Enterprise Privacy sample event messages

Use the sample event messages to verify a successful integration with the QRadar product.

Proofpoint Enterprise Protection and Enterprise Privacy sample event message using Syslog protocol

Important: Due to formatting issues, paste the message into a text editor and remove any carriage return or line feed characters.

Sample 1: Example of a 'sent' email log message is given below.

```
<22>Feb 11 08:22:26 proofpoint.enterpriseprotection.test sendmail[31248]: s1BDHmHc028570:
to=<user_test@proof.point.test>, delay=00:00:00, xdelay=00:00:00, mailer=esmtp, pri=186258,
relay=[172.16.10.32] [172.16.10.32], dsn=2.0.0, stat=Sent (a1AAAAAa111111 Message accepted for
delivery)
```

Table 881. Highlighted fields in the Proofpoint Enterprise Protection and Enterprise Privacy event

QRadar product field name	Highlighted payload field name
Event ID	info MESSAGE SENT from **to=**
Category	**Proofpoint**
Device Time	From payload header
Source IP	**relay=**
Username(s)	**to=**

Sample 2: Example of a 'received' email log message is given below.

```
<22>Feb 11 08:22:26 proofpoint.enterpriseprotection.test sendmail[28570]: s1BDHmHc028570:
from=<user.1234@proof.point.test>, size=66258, class=0, nrcpts=1,
msgid=<USER.TEST.0@proof.point.test>, proto=SMTP, daemon=MTA, relay=proofpoint.test [127.0.0.1]
```

Table 882. Highlighted fields in the Proofpoint Enterprise Protection and Enterprise Privacy event

QRadar product field name	Highlighted payload field name
Event ID	info MESSAGE RECEIVED based on **from=**
Category	**Proofpoint**
Device Time	From payload header
Source IP	From **relay=**
Username(s)	From **from=**, **msgid=**

Chapter 128. Pulse Secure

IBM QRadar supports a range of Pulse Secure DSMs.

Pulse Secure Infranet Controller

The Pulse Secure Infranet Controller DSM for IBM QRadar accepts DHCP events by using syslog. QRadar records all relevant events from a Pulse Secure Infranet Controller.

Before you configure QRadar to integrate with a Pulse Secure Infranet Controller, you must configure syslog in the server. For more information on configuring your Pulse Secure Infranet Controller, consult your vendor documentation.

Syslog log source parameters for Pulse Secure Infranet Controller

If QRadar does not automatically detect the log source, add a Pulse Secure Infranet Controller log source on the QRadar Console by using the syslog protocol.

When using the syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect syslog events from Pulse Secure Infranet Controller:

Table 883. Syslog log source parameters for the Pulse Secure Infranet Controller DSM

Parameter	Value
Log Source type	Juniper Networks Infranet Controller
Protocol Configuration	Syslog

After you configure syslog for your Pulse Secure Infranet Controller, you are now ready to configure the log source in QRadar.

Related tasks

"Adding a log source" on page 5

Pulse Secure Pulse Connect Secure

The IBM QRadar DSM for Pulse Secure Pulse Connect Secure collects syslog and WebTrends Enhanced Log File (WELF) formatted events from Pulse Secure Pulse Connect Secure mobile VPN devices.

The following table describes the specifications for the Pulse Secure Pulse Connect Secure DSM:

Table 884. Pulse Secure Pulse Connect Secure DSM specifications

Specification	Value
Manufacturer	Pulse Secure
DSM name	Pulse Secure Pulse Connect Secure
RPM file name	`DSM-PulseSecurePulseConnectSecure-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	8.2R5
Protocol	Syslog, TLS Syslog

Table 884. Pulse Secure Pulse Connect Secure DSM specifications (continued)	
Specification	**Value**
Recorded event types	Admin Authentication System Network Error
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	Yes
More information	Pulse Secure website (https://www.pulsesecure.net)

To integrate Pulse Secure Pulse Connect Secure with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the Pulse Secure Pulse Connect Secure DSM RPM on your QRadar Console.
2. Configure your Pulse Secure Pulse Connect Secure device to send WebTrends Enhanced Log File (WELF) formatted events to QRadar.
3. Configure your Pulse Secure Pulse Connect Secure device to send syslog events to QRadar.
4. If QRadar does not automatically detect the log source, add a Pulse Secure Pulse Connect Secure log source on the QRadar Console. The following tables describe the parameters that require specific values to collect Syslog events from Pulse Secure Pulse Connect Secure:

Table 885. Pulse Secure Pulse Connect Secure Syslog log source parameters	
Parameter	**Value**
Log Source type	Pulse Secure Pulse Connect Secure
Protocol Configuration	Syslog
Log Source Identifier	Type a unique identifier for the log source.

5. Optional. To add a Pulse Secure Pulse Connect Secure log source to receive syslog events from network devices that support TLS Syslog event forwarding, configure the log source on the QRadar Console to use the TLS Syslog protocol.

   The following table describes the parameters that require specific values to collect TLS Syslog events from Pulse Secure Pulse Connect Secure:

Table 886. Pulse Secure Pulse Connect Secure TLS Syslog log source parameters	
Parameter	**Value**
Log Source type	Pulse Secure Pulse Connect Secure
Protocol Configuration	TLS Syslog
Log Source Identifier	Type a unique identifier for the log source.
TLS Protocols	Select the version of TLS that is installed on the client.

Related concepts

"TLS Syslog protocol configuration options" on page 227
Configure a TLS Syslog protocol log source to receive encrypted syslog events from network devices that support TLS Syslog event forwarding for each listener port.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring a Pulse Secure Pulse Connect Secure device to send WebTrends Enhanced Log File (WELF) events to IBM QRadar

Before you can send WebTrends Enhanced Log File (WELF) formatted events to QRadar, you must configure syslog server information for events, user access, administrator access and client logs on your Pulse Secure Pulse Connect Secure device.

Procedure

1. Log in to your Pulse Secure Pulse Connect Secure device administration user interface on the web:

   `https://<IP_address>/admin`
2. Configure syslog server information for events.
   a) Click **System** > **Log/Monitoring** > **Events** > **Settings**.
   b) From the **Select Events to Log** pane, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) From the **Facility list**, select a syslog server facility level.
   e) From the **Filter** list, select **WELF:WELF**.
   f) Click **Add**, and then click **Save Changes**.
3. Configure syslog server information for user access.
   a) Click **System** > **Log/Monitoring** > **User Access** > **Settings**.
   b) From the **Select Events to Log pane**, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) From the **Facility** list, select the facility.
4. Configure syslog server information for Administrator access.
   a) Click **System** > **Log/Monitoring** > **Admin Access** > **Settings**.
   b) From the **Select Events to Log** pane, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) From the **Facility** list, select the facility.
   e) From the **Filter** list, select **WELF:WELF**.
   f) Click **Add**, then click **Save Changes**.
5. Configure syslog server information for client logs.
   a) Click **System** > **Log/Monitoring** > **Client Logs** > **Settings**.
   b) From the **Select Events to Log pane**, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) From the **Facility** list, select the facility.
   e) From the **Filter** list, select **WELF:WELF**.
   f) Click **Add**, then click **Save Changes**.

Results

You are now ready to configure a log source in QRadar.

Configuring a Pulse Secure Pulse Connect Secure device to send syslog events to QRadar

To forward syslog events to QRadar, you need to configure syslog server information for events, user access, administrator access and client logs on your Pulse Secure Pulse Connect Secure device.

Procedure

1. Log in to your Pulse Secure Pulse Connect Secure device administration user interface on the web:

   `https://<IP_address>/admin`
2. Configure syslog server information for events.
   a) Click **System** > **Log/Monitoring** > **Events** > **Settings**.
   b) From the **Select Events to Log** section, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) Click **Add**, and then click **Save Changes**.
3. Configure syslog server information for user access.
   a) Click **System** > **Log/Monitoring** > **User Access** > **Settings**.
   b) From the **Select Events to Log** section, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) Click **Add**, and then click **Save Changes**.
4. Configure syslog server information for Administrator access.
   a) Click **System** > **Log/Monitoring** > **Admin Access** > **Settings**.
   b) From the **Select Events to Log** section, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) Click **Add**, and then click **Save Changes**.
5. Configure syslog server information for client logs.
   a) Click **System** > **Log/Monitoring** > **Client Logs** > **Settings**.
   b) From the **Select Events to Log** section, select the events that you want to log.
   c) In the **Server name/IP** field, type the name or IP address of the syslog server.
   d) Click **Add**, and then click **Save**.

Results

You are now ready to configure a log source in QRadar.

Pulse Secure Pulse Connect Secure sample event message

Use this sample event message as a way of verifying a successful integration with QRadar.

The following table provides a sample event message for the Pulse Secure Pulse Connect Secure DSM:

Table 887. Pulse Secure Pulse Connect Secure sample message

Event name	Low level category	Sample log message
VlanAssigned	Information	id=firewall time="2009-10-01 22:26:39" pri=6 fw=<IP_address> vpn=ic user=user realm="<Domain>" roles="Employee, Remediation" proto= src=<Source_IP_address> dst= dstname= type=vpn op= arg=""result= sent= rcvd= agent="" duration= msg="EAM24459: User assigned to vlan (VLAN='16')"

Chapter 129. Radware

IBM QRadar supports a range of Radware devices.

Radware AppWall

The IBM QRadar DSM for Radware AppWall collects logs from a Radware AppWall appliance.

The following table describes the specifications for the Radware AppWall DSM:

Table 888. Radware AppWall DSM specifications	
Specification	**Value**
Manufacturer	Radware
DSM name	Radware AppWall
RPM file name	`DSM-RadwareAppWall-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	6.5.2 8.2
Protocol	Syslog
Recorded event types	Administration Audit Learning Security System
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	For more information, see the Radware link to public site website (https://www.radware.com).

To integrate Radware AppWall with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Radware AppWall DSM RPM from the IBM Support Website onto your QRadar Console:
2. Configure your Radware AppWall device to send logs to QRadar.
3. If QRadar does not automatically detect the log source, add a Radware AppWall log source on the QRadar Console. The following table describes the parameters that require specific values for Radware AppWall event collection:

Table 889. Radware AppWall log source parameters	
Parameter	**Value**
Log Source type	Radware AppWall
Protocol Configuration	Syslog

Important: Your RadWare AppWall device might have event payloads that are longer than the default maximum TCP Syslog payload length of 4096 bytes. This overage can result in the event payload being split into multiple events by QRadar. To avoid this behavior, increase the maximum TCP Syslog payload length. To optimize performance, start by configuring the value to 8192 bytes. The maximum length for RadWare AppWall events is 14,019 bytes.

The maximum QRadar syslog payload size is 32,000 bytes. For more information about increasing the QRadar maximum payload size, see QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances (https://www.ibm.com/support/pages/qradar-tcp-and-udp-syslog-maximum-payload-message-length-qradar-appliances).

You can verify that QRadar is configured to receive events from your Radware AppWall device when you complete Step 6 of the Configuring Radware AppWall to communicate with QRadar procedure.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

"Configuring Radware AppWall to communicate with QRadar" on page 1386
Configure your Radware AppWall device to send logs to IBM QRadar. You integrate AppWall logs with QRadar by using the Vision Log event format.

"Increasing the maximum TCP Syslog payload length for Radware AppWall" on page 1387
Increase the maximum TCP Syslog payload length for your RadWare AppWall appliance in IBM QRadar for payloads that are longer than the default maximum TCP Syslog payload length.

Configuring Radware AppWall to communicate with QRadar

Configure your Radware AppWall device to send logs to IBM QRadar. You integrate AppWall logs with QRadar by using the Vision Log event format.

Procedure

1. Log in to your Radware AppWall Console.
2. Select **Configuration View** from the menu bar.
3. In the Tree View pane on the left side of the window, click **appwall Gateway** > **Services** > **Vision Support**.
4. From the **Server List** tab on the right side of the window, click the add icon (**+**) in the Server List pane.
5. In the **Add Vision Server** window, configure the following parameters:

Parameter	Value
Address	The IP address for the QRadar Console.
Port	514
Version	Select the most recent version from the list. It is the last item in the list.

6. Click **Check** to verify that the AppWall can successfully connect to QRadar.
7. Click **Submit** and **Save**.
8. Click **Apply** > **OK**.

Increasing the maximum TCP Syslog payload length for Radware AppWall

Increase the maximum TCP Syslog payload length for your RadWare AppWall appliance in IBM QRadar for payloads that are longer than the default maximum TCP Syslog payload length.

Before you begin

Important: Your RadWare AppWall device might have event payloads that are longer than the default maximum TCP Syslog payload length of 4096 bytes. This overage can result in the event payload being split into multiple events by QRadar. To avoid this behavior, increase the maximum TCP Syslog payload length. To optimize performance, start by configuring the value to 8192 bytes. The maximum length for RadWare AppWall events is 14,019 bytes.

The maximum QRadar syslog payload size is 32,000 bytes. For more information about increasing the QRadar maximum payload size, see QRadar: TCP and UDP Syslog Maximum Payload Message Length for QRadar Appliances (https://www.ibm.com/support/pages/qradar-tcp-and-udp-syslog-maximum-payload-message-length-qradar-appliances).

Procedure

1. Login to the QRadar Console as an administrator.
2. From the **Admin** tab, click **System Settings** > **Advanced**.
3. In the **Max TCP Syslog Payload Length** field, type 8192, and then click **Save**.
4. From the **Admin** tab, click **Deploy Changes**.

Radware AppWall sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Radware AppWall sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that a service is stopped.

```
OLF6 appwall    2.1    date="05/27/2019 06:01:24 +00"    milli.1=92
et=Initialization    sev=notice    subj="Subsystem stopped"    evtid=1558936884-109
hostname=testHostName    hostip=10.22.126.18    module=SystemType    devtype="Stand Alone
Gateway"    cmip=10.22.126.18    msg="The subsystem was stopped."
```

Table 890. Highlighted values in the Radware AppWall sample event

QRadar field name	Highlighted values in the event payload
Event ID	**1558936884-109**
Source IP	**10.22.126.18**
Device Time	**05/27/2019 06:01:24 +00**

Sample 2: The following sample event message shows a reverse DNS lookup failure.

```
OLF6 appwall    2.1    date="05/27/2019 09:00:33 +00"    milli.1=244    et=Initialization
sev=warning    subj="Reverse DNS Lookup Initialization Error"    evtid=1558947633-294
hostname=testHostName    hostip=10.22.126.18    module=WebApp_SubSys    devtype="Stand Alone
Gateway"    cmip=10.22.126.18    msg="Reverse DNS Lookup operation failed to initialize.Dig
Init Check failed: ;; connection timed out; no servers could be reached\n\nPrimary DNS Server:
10.22.14.135:53"
```

Table 891. Highlighted values in the Radware AppWall sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**1558947633-294**
Source IP	**10.22.126.18**
Device Time	**05/27/2019 09:00:33 +00**

Radware DefensePro

The Radware DefensePro DSM for IBM QRadar accepts events by using syslog. Event traps can also be mirrored to a syslog server.

Before you configure QRadar to integrate with a Radware DefensePro device, you must configure your Radware DefensePro device to forward syslog events to QRadar. You must configure the appropriate information by using the **Device > Trap and SMTP option**.

Any traps that are generated by the Radware device are mirrored to the specified syslog server. The current Radware Syslog server gives you the option to define the status and the event log server address.

You can also define more notification criteria, such as Facility and Severity, which are expressed by numerical values:

- **Facility** is a user-defined value that indicates the type of device that is used by the sender. This criteria is applied when the device sends syslog messages. The default value is 21, meaning Local Use 6.
- Severity indicates the importance or impact of the reported event. The Severity is determined dynamically by the device for each message sent.

In the **Security Settings** window, you must enable security reporting by using the **connect** and **protect/security** settings. You must enable security reports to syslog and configure the severity (syslog risk).

You are now ready to configure the log source in QRadar.

Tip: If you have custom events that display as unknown in QRadar, see the IBM Support article about QRadar: Custom events for Radware DefensePro display 'parsed, but not mapped' (https://www.ibm.com/support/pages/node/6960301).

Syslog log source parameters for Radware DefensePro

If QRadar does not automatically detect the log source, add a Radware DefensePro log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Radware DefensePro:

Table 892. Syslog log source parameters for the Radware DefensePro DSM	
Parameter	**Value**
Log Source type	Radware DefensePro
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Radware DefensePro installation.

Related tasks

“Adding a log source” on page 5

Chapter 130. Raz-Lee iSecurity

IBM QRadar collects and parses Log Event Extended Format (LEEF) events that are forwarded from Raz-Lee iSecurity installations on IBM i. The events are parsed and categorized by the IBM i DSM.

QRadar supports events from Raz-Lee iSecurity installations for iSecurity Firewall V15.7 and iSecurity Audit V11.7.

The following table describes the specifications for the IBM i DSM for Raz-Lee iSecurity installations:

Table 893. IBM i DSM specifications for Raz-Lee iSecurity

Specification	**Value**
Manufacturer	IBM
DSM name	IBM i
RPM file name	`DSM-IBMi-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	iSecurity Firewall V15.7 iSecurity Audit V11.7
Protocol	Syslog
Event format	LEEF
Recorded event types	All security, compliance, firewall, and audit events.
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	IBM website (http://www.ibm.com)

Configuring Raz-Lee iSecurity to communicate with QRadar

To collect security, compliance, and audit events, configure your Raz-Lee iSecurity installation to forward Log Event Extended Format (LEEF) syslog events to IBM QRadar.

Procedure

1. Log in to the IBM i command-line interface.
2. From the command line, type STRAUD to access the **Audit** menu options.
3. From the **Audit** menu, select **81. System Configuration**.
4. From the **iSecurity/Base System Configuration** menu, select **32. SIEM 1**.
5. Configure the **32.SIEM 1** parameter values.

   Learn more about 32. SIEM 1 parameter values:

   Table 894. 32.SIEM 1 parameter values

Parameter	**Value**
SIEM 1 name	Type `QRadar`.

Table 894. 32.SIEM 1 parameter values (continued)	
Parameter	**Value**
Port	Type the port that is used to send syslog messages. The default port is 514, which is the syslog standard.
SYSLOG type	Type 1 for UDP.
Destination address	Type the IP address for QRadar.
Severity range to auto send	Type a severity message level in the range of 0 - 7. For example, type **7** to send all syslog messages.
Facility to use	Type a syslog facility level in the range of 0 - 23.
Message structure	Type *LEEF.
Convert data to CCSID	Type 0 in the **Convert data to CCSID** field. This is the default character conversion.
Maximum length	Type 1024.

6. From the **iSecurity/Base System Configuration** menu, select **31. Main Control**.
7. Configure the **31. Main Control** parameter values.

   Learn more about 31. Main Control parameter values:

*Table 895. **31. Main Control** parameter values*	
Parameter	**Value**
Run rules before sending	To process the events that you want to send, type Y. To send all events, type N.
SIEM 1: QRadar	Type Y.
Send JSON messages (for DAM)	Type N.
As only operation	Type N.

8. From the command line, to configure the **Firewall** options, type STRFW to access the menu options.
9. From the **Firewall** menu, select **81. System Configuration**.
10. From the **iSecurity (part 1) Global Parameters:** menu, select **72. SIEM 1**.
11. Configure the **72.SIEM 1** parameter values.

    Learn more about 72. SIEM 1 parameter values:

*Table 896. **72.SIEM 1** parameter values*	
Parameter	**Value**
SIEM 1 name	Type QRadar.
Port	Type the port that is used to send syslog messages. The default port is 514, which is the Syslog standard.
SYSLOG type	Type 1 for UDP syslog type.
Send in FYI mode	Type N.

*Table 896. **72.SIEM 1** parameter values (continued)*	
Parameter	**Value**
Destination address	Type the IP address for the QRadar console.
Severity range to auto send	Type a severity level in the range 0 - 7.
Facility to use	Type a facility level.
Message structure	Type *LEEF.
Convert data to CCSID	Type 0.
Maximum length	Type 1024.

12. From the **iSecurity (part 1) Global Parameters:** menu, select **71. Main Control**.
13. Configure the **71. Main Control** parameter values.

    Learn more about 71. Main Control parameter values:

*Table 897. **71. Main Control** parameter values*	
Parameter	**Value**
SIEM 1: QRadar	Type 2.
Send JSON messages (for DAM)	Type 0.

Results

Syslog LEEF events that are forwarded by Raz-Lee iSecurity are automatically discovered by the QRadar DSM for IBM i. In most cases, the log source is automatically created in QRadar after a few events are detected.

If the event rate is low, you can manually configure a log source for Raz-Lee iSecurity in QRadar. Until the log source is automatically discovered and identified, the event type displays as Unknown on the **Log Activity** tab.

Syslog log source parameters for Raz-Lee iSecurity

If QRadar does not automatically detect the log source, add a Raz-Lee iSecurity log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Raz-Lee iSecurity:

Table 898. Syslog log source parameters for the Raz-Lee iSecurity DSM	
Parameter	**Value**
Log Source type	Raz-Lee iSecurity
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name of the log source that sends events from the Raz-Lee iSecurity device.
Enabled	By default, the check box is selected.

Table 898. Syslog log source parameters for the Raz-Lee iSecurity DSM (continued)	
Parameter	**Value**
Credibility	The **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Coalescing Events	By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Payload Encoding	Select **Incoming Payload Encoder** for parsing and storing the logs.
Store Event Payload	By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the **System Settings** in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related tasks

"Adding a log source" on page 5

Chapter 131. Redback ASE

The Redback ASE DSM for IBM QRadar accepts events by using syslog.

The Redback ASE device can send log messages to the Redback device console or to a log server that is integrated with QRadar to generate deployment-specific reports. Before you configure a Redback ASE device in QRadar, you must configure your device to forward syslog events.

Configuring Redback ASE

You can configure the device to send syslog events to IBM QRadar.

Procedure

1. Log in to your Redback ASE device user interface.
2. Start the CLI configuration mode.
3. In global configuration mode, configure the default settings for the security service:

   ```
   asp security default
   ```
4. In ASP security default configuration mode, configure the IP address of the log server and the optional transport protocol:

   ```
   log server <IP address> transport udp port 9345
   ```

   Where <*IP address*> is the IP address of the QRadar.
5. Configure the IP address that you want to use as the source IP address in the log messages:

   ```
   log source <source IP address>
   ```

   Where <*source IP address*> is the IP address of the loopback interface in context local.
6. Commit the transaction.

   For more information about Redback ASE device configuration, see your vendor documentation.

   For example, if you want to configure:

   - Log source server IP address <IP_address>
   - Default transport protocol: UDP
   - Default server port: 514

   The source IP address that is used for log messages is <IP_address>. This address must be an IP address of a *loopback* interface in context local.

   ```
   asp security default log server <IP_address1> log source <IP_address2>
   ```

What to do next

You can now configure the log sources in QRadar.

Syslog log source parameters for Redback ASE

If QRadar does not automatically detect the log source, add a Redback ASE log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Redback ASE:

Table 899. Syslog log source parameters for the Redback ASE DSM	
Parameter	**Value**
Log Source type	Redback ASE
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Redback ASE appliance.

Related tasks

"Adding a log source" on page 5

Chapter 132. Red Hat Advanced Cluster Security for Kubernetes

The IBM QRadar DSM for Red Hat Advanced Cluster Security for Kubernetes collects HTTP Receiver events from a Red Hat Advanced Cluster Security for Kubernetes application.

To integrate Red Hat Advanced Cluster Security for Kubernetes with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - DSM Common RPM
   - Red Hat Advanced Cluster Security for Kubernetes DSM RPM
2. Configure your Red Hat Advanced Cluster Security for Kubernetes application to send events to QRadar. For more information, see Configuring Red Hat Advanced Cluster Security for Kubernetes to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a Red Hat Advanced Cluster Security for Kubernetes log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Red Hat Advanced Cluster Security for Kubernetes DSM specifications

When you configure Red Hat Advanced Cluster Security for Kubernetes, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported protocol for Red Hat Advanced Cluster Security for Kubernetes is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Red Hat Advanced Cluster Security for Kubernetes DSM.

Table 900. Red Hat Advanced Cluster Security for Kubernetes DSM specifications

Specification	**Value**
Manufacturer	Red Hat
DSM name	Red Hat Advanced Cluster Security for Kubernetes
RPM file name	DSM-*RedhatKubernetes-QRadar_version-build_number*.noarch.rpm
Protocol	HTTP Receiver
Event format	JSON
Recorded event types	audit and alert events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No

Configuring Red Hat Advanced Cluster Security for Kubernetes to communicate with QRadar

To send events to IBM QRadar, you must add a new Generic Webhook integration.

Before you begin

You must have permission to access Generic Webhook Integrations in the Red Hat Advanced Cluster for Kubernetes application.

Procedure

1. Log in to the Red Hat Advanced Cluster Security for Kubernetes application.
2. From the navigation menu, select **Platform Configuration** > **Integrations**.
3. In the **Integrations** window, click **StackRox Generic Webhook**.
4. In the **CONFIGURE GENERIC WEBHOOK NOTIFIER INTEGRATIONS** window, click **+ NEW INTEGRATION**.
5. Type your integration name and endpoint in the **Integration Name** field.

   Use the following example as a guide:

   ```
   <URL to QRadar Box:<Port of Integration>
   ```
6. Click **Create**.

What to do next

HTTP Receiver log source parameters for Red Hat Advanced Cluster Security for Kubernetes

HTTP Receiver log source parameters for Red Hat Advanced Cluster Security for Kubernetes

If QRadar does not automatically detect the log source, add a Red Hat Advanced Cluster Security for Kubernetes log source on the QRadar Console by using the HTTP Receiver.

When using the HTTP Receiver protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect HTTP Receiver events from Red Hat Advanced Cluster Security for Kubernetes:

Table 901. HTTP Receiver log source parameters for the Red Hat Advanced Cluster Security for Kubernetes DSM

Parameter	Value
Log Source type	Red Hat Advanced Cluster Security for Kubernetes
Protocol Configuration	HTTP Receiver
Log Source Identifier	The IP address, hostname, or any name to identify the source of the payloads. Must be unique for the log source type.
Communication Type	HTTP or HTTPs - The value is determined by the open port and the StackRox Generic Webhook integration that you completed.
Listen Port	The port that you specified when you completed the StackRox Generic Webhook integration.

For a complete list of HTTP Receiver protocol parameters and their values, see HTTP Receiver protocol configuration options.

Related tasks

"Adding a log source" on page 5

Red Hat Advanced Cluster Security for Kubernetes sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Red Hat Advanced Cluster Security for Kubernetes sample message when you use the HTTP receiver protocol

Sample 1: The following sample event message shows that a container uses a read/write root file system.


```
{"alert": {"id":"f92601a5-83ec-47b3-856b-1000cd381b0d","policy":{"id":"8ac93556-4ad4-4220-
a275-3f518db0ceb9","name":"Container using read-write root filesystem","description":"Alert on
deployments with containers with read-write root filesystem","rationale":"Containers running
with read-write root filesystem represent greater post-exploitation risk by allowing an
attacker to modify important files in the container.","remediation":"Use a read-only root
filesystem, and use volume mounts to allow writes to specific sub-directories depending on your
application's needs.","categories":["Privileges","Docker CIS"],"lifecycleStages":
["DEPLOY"],"exclusions":[{"name":"Don't alert on kube-system namespace","deployment":{"scope":
{"namespace":"kube-system"}}},{"name":"Don't alert on istio-system namespace","deployment":
{"scope":{"namespace":"istio-system"}}},{"name":"Don't alert on openshift-node
namespace","deployment":{"scope":{"namespace":"openshift-node"}}},{"name":"Don't alert on
openshift-sdn namespace","deployment":{"scope":{"namespace":"openshift-sdn"}}},{"deployment":
{"name":"mastercard-processor"}},{"deployment":{"name":"community-
operators-884t8"}}],"severity":"MEDIUM_SEVERITY","notifiers":["58c8b9ba-0d96-4dd4-a3fe-
d9b9931ab788","e892ed00-de0f-40b7-
b309-45fc6de7bcfa"],"lastUpdated":"2021-04-29T14:45:56.095158050Z","SORTName":"Container using
read-write root
filesystem","SORTLifecycleStage":"DEPLOY","policyVersion":"1.1","policySections":
[{"policyGroups":[{"fieldName":"Read-Only Root Filesystem","values":
[{"value":"false"}]}]}]},"deployment":{"id":"47e90a53-3aeb-4e0b-a4cd-
bf7819f3a2b5","name":"community-operators-kbw79","type":"Pod","namespace":"openshift-
marketplace","namespaceId":"23ab4c01-9553-40f7-871b-d9a39317bb90","labels":
{"catalogsource.operators.coreos.com/update":"community-
operators","olm.catalogSource":""},"clusterId":"916b38c2-
fa71-45cf-9726-1d6b227858b3","clusterName":"production","containers":[{"image":{"name":
{"registry":"registry.redhat.io","remote":"redhat/community-operator-
index","tag":"v4.7","fullName":"registry.redhat.io/redhat/community-operator-
index:v4.7"}},"name":"registry-server"}],"annotations":{"openshift.io/
scc":"anyuid"}},"violations":[{"message":"Container 'registry-server' uses a read-write root
filesystem"}],"time":"2021-05-05T15:16:15.612525111Z","firstOccurred":"2021-05-05T15:16:15.61703
4472Z"}}
```


Table 902. Highlighted fields in the Red Hat Advanced Cluster for Kubernetes event

QRadar field name	Highlighted values in the payload
Device Time	**2021-05-05T15:16:15.612525111Z**

Sample 2: The following sample event message shows that an administrator requested a read/write access.


```
{"audit": {"time":"2021-05-06T18:53:37.725743614Z","status":"REQUEST_SUCCEEDED","user":
{"friendlyName":"admin","permissions":
{"name":"Admin","globalAccess":"READ_WRITE_ACCESS"},"roles":
[{"name":"Admin","globalAccess":"READ_WRITE_ACCESS"}],"role":
{"name":"Admin","globalAccess":"READ_WRITE_ACCESS"}},"request":{"endpoint":"/v1/networkbaseline/
ebaf8cc8-6dce-46a6-931d-c98d1ecad26f/status","method":"POST","payload":
{"@type":"v1.NetworkBaselineStatusRequest","deploymentId":"ebaf8cc8-6dce-46a6-931d-
c98d1ecad26f","peers":[{"entity":{"id":"dd550035-
eb16-45be-80e0-45d4993358fc","type":"DEPLOYMENT"},"port":7777,"protocol":"L4_PROTOCOL_TCP","ingr
ess":true},{"entity":
```

{"id":"f2eed5c7-7a19-4863-8b64-9257416917be","type":"DEPLOYMENT"},"port":8080,"protocol":"L4_PROTOCOL_TCP"},{"entity":{"id":"5951f034-ca72-4613-bf11-dd5659882a3a","type":"DEPLOYMENT"},"port":8080,"protocol":"L4_PROTOCOL_TCP"}]},"method":"UI","interaction":"CREATE"}}

Table 903. Highlighted fields in the Red Hat Advanced Cluster for Kubernetes sample event

QRadar field name	Highlighted values in the event payload
Device Time	**2021-05-06T18:53:37.725743614Z**
Username	**admin**

Chapter 133. Resolution1 CyberSecurity

Resolution1 CyberSecurity is formerly known as AccessData InSight. The Resolution1 CyberSecurity DSM for IBM QRadar collects event logs from your Resolution1 CyberSecurity device.

The following table identifies the specifications for the Resolution1 CyberSecurity DSM:

Table 904. Resolution1 CyberSecurity DSM specifications

Specification	**Value**
Manufacturer	Resolution1
DSM name	Resolution1 CyberSecurity
RPM file name	`DSM-Resolution1CyberSecurity-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V2
Event format	Log file
QRadar recorded event types	Volatile Data Memory Analysis Data Memory Acquisition Data Collection Data Software Inventory Process Dump Data Threat Scan Data Agent Remediation Data
Automatically discovered?	No
Included identity?	No

To send events from Resolution1 CyberSecurity to QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs from the IBM Support Website.
   - LogFileProtocol
   - DSMCommon
   - Resolution1 CyberSecurity DSM
2. Configure your Resolution1 CyberSecurity device to communicate with QRadar.
3. Create a Resolution1 CyberSecurity log source on the QRadar Console.

Related concepts

Log file log source parameters for Resolution1 CyberSecurity

Related tasks

Adding a DSM

Configuring your Resolution1 CyberSecurity device to communicate with QRadar

To collect Resolution1 CyberSecurity events, you must configure your third-party device to generate event logs in LEEF format. You must also create an FTP site for Resolution1 CyberSecurity to transfer the LEEF files. QRadar can then pull the logs from the FTP server.

Configuring your Resolution1 CyberSecurity device to communicate with QRadar

To collect Resolution1 CyberSecurity events, you must configure your third-party device to generate event logs in LEEF format. You must also create an FTP site for Resolution1 CyberSecurity to transfer the LEEF files. QRadar can then pull the logs from the FTP server.

Procedure

1. Log in to your Resolution1 CyberSecurity device.
2. Open the `ADGIntegrationServiceHost.exe.config` file, which is in the `C:\Program Files\AccessData\eDiscovery\Integration Services` directory.
3. Change the text in the file to match the following lines:

```
<Option Name="Version" Value="2.0" />
<Option Name="Version" Value="2.0" />
<Option Name="OutputFormat" Value="LEEF" />
<Option Name="LogOnly" Value="1" />
<Option Name="OutputPath" Value="C:\CIRT\logs" />
```

4. Restart the Resolution1 Third-Party Integration service.
5. Create an FTP site for the `C:\CIRT\logs` output folder:
   a) Open Internet Information Services Manager (IIS).
   b) Right-click the **Sites** tab and click **Add FTP Site**.
   c) Name the FTP site, and enter `C:\CIRT\logs` as the location for the generated LEEF files.
   d) Restart the web service.

Log file log source parameters for Resolution1 CyberSecurity

If QRadar does not automatically detect the log source, add a Resolution1 CyberSecurity log source on the QRadar Console by using the Log file.

When using the Log file protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log file events from Resolution1 CyberSecurity:

Table 905. Log file log source parameters for the Resolution1 CyberSecurity DSM

Parameter	Value
Log Source type	Resolution1 CyberSecurity
Protocol Configuration	Log file
Log Source Identifier	Type the IP address or host name of the Resolution1 CyberSecurity device

For a complete list of Log File protocol parameters and their values, see "Log File protocol configuration options" on page 155.

Related tasks

"Adding a log source" on page 5

Chapter 134. Riverbed

IBM QRadar supports a number of Riverbed DSMs:

Riverbed SteelCentral NetProfiler (Cascade Profiler) Audit

The IBM QRadar DSM for Riverbed SteelCentral NetProfiler Audit collects audit logs from your Riverbed SteelCentral NetProfiler system. This product is also known as *Cascade Profiler*.

The following table identifies the specifications for the Riverbed SteelCentral NetProfiler DSM:

Table 906. Riverbed SteelCentral NetProfiler specifications

Specification	**Value**
Manufacturer	Riverbed
DSM name	SteelCentral NetProfiler Audit
RPM file name	`DSM-RiverbedSteelCentralNetProfilerAudit-`*`Qradar_version-build_number`*`.noarch.rpm`
Protocol	Log file
Recorded event types	Audit Events
Automatically discovered?	No
Includes identity?	Yes
Includes custom properties?	No
More information	Riverbed website (http://www.riverbed.com/)

To integrate Riverbed SteelCentral NetProfiler Audit with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol-LogFile RPM
   - Riverbed SteelCentral NetProfiler Audit RPM
2. Create an audit report template on your Riverbed host and then configure a third-party host to use the template to generate the audit file. See “Creating a Riverbed SteelCentral NetProfiler report template and generating an audit file” on page 1402.
3. Create a log source on the QRadar Console. The log source allows QRadar to access the third-party host to retrieve the audit file. Use the following table to define the Riverbed-specific parameters:

Table 907. Riverbed SteelCentral NetProfiler log source parameters

Parameter	**Description**
Log Source Type	Riverbed SteelCentral NetProfiler Audit
Protocol Configuration	LogFile
Remote IP or Hostname	The IP address or host name of the third-party host that stores the generated audit file
Remote User	The user name for the account that can access the host.
Remote Password	The password for the user account.
Remote Directory	The absolute file path on the third-party host that contains the generated audit file.
FTP File Pattern	A regex pattern that matches the name of the audit file.

Table 907. Riverbed SteelCentral NetProfiler log source parameters (continued)	
Parameter	**Description**
Recurrence	Ensure that recurrence matches the frequency at which the `SteelScript for Python` SDK script is run on the remote host.
Event Generator	Line Matcher
Line Matcher RegEx	`^\d+/\d+/\d+ \d+:\d+,`

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Creating a Riverbed SteelCentral NetProfiler report template and generating an audit file

To prepare for Riverbed SteelCentral NetProfiler integration with QRadar, create a report template on the Riverbed SteelCentral NetProfiler and then use a third-party host to generate an audit file. The third-party host must be a system other than the host you use for Riverbed SteelCentral NetProfiler or QRadar.

Before you begin

Ensure that the following items are installed on a third-party host that you use to run the audit report:

Python

Download and install Python from the Python website (https://www.python.org/download/).

SteelScript for Python

Download and install the `SteelScript for Python` SDK from the Riverbed SteelScript for Python website (https://support.riverbed.com/apis/steelscript/index.html). The script generates and downloads an audit file in CSV format. You must periodically run this script.

Procedure

1. Define the audit file report template.
   a) Log in to your Riverbed SteelCentral NetProfiler host user interface.
   b) Select **System** > **Audit Trail**.
   c) Select the criteria that you want to include in the audit file.
   d) Select a time frame.
   e) On the right side of the window, click **Template**.
   f) Select **Save As/Schedule**.
   g) Type a name for the report template.
2. To run the report template and generate an audit file, complete the following steps
   a) Log in to the third-party host on which you installed Python.
   b) Type the following command:

```
$ python ./get_template_as_csv.py  <riverbed_host_name>  -u admin -p admin -t
"<report_template_name>"  -o <absolute_path_to_target file>
```

   Tip: Record the report template name and file path. You need to use the name to run the report template and when you configure a log source in the QRadarinterface.

Riverbed SteelCentral NetProfiler (Cascade Profiler) Alert

The IBM QRadar DSM for Riverbed SteelCentral NetProfiler collects alert logs from your Riverbed SteelCentral NetProfiler system. This product is also known as *Cascade Profiler*.

The following table identifies the specifications for the Riverbed SteelCentral NetProfiler DSM:

Table 908. Riverbed SteelCentral NetProfiler specifications

Specification	Value
Manufacturer	Riverbed
DSM name	SteelCentral NetProfiler
RPM file name	`DSM-RiverbedSteelCentralNetProfiler-`*`QRadar_version-build_number`*`.noarch.rpm`
Protocol	JDBC
Recorded event types	Alert Events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Riverbed website (http://www.riverbed.com/)

To integrate Riverbed SteelCentral NetProfiler with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol-JDBC RPM
   - Riverbed SteelCentral NetProfiler RPM
2. Configure your Riverbed SteelCentral NetProfiler system to enable communication with QRadar.
3. Create a log source on the QRadar Console. Use the following table to define the Riverbed-specific JDBC parameters:

Table 909. Riverbed SteelCentral NetProfiler JDBC log source parameters

Parameter	Description
Log Source Type	**Riverbed SteelCentral NetProfiler**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	Postgres
Database Name	You can type the actual name of the Riverbed database. For most configurations, the database name is `mazu`. **Tip:** Confirm the actual name of the Riverbed database.
IP or Hostname	The IP address or host name of the database server.

Table 909. Riverbed SteelCentral NetProfiler JDBC log source parameters (continued)	
Parameter	**Description**
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix - 9088 • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the **Port** field blank.
Table Name	`events.export_csv_view`
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**.
Username	The user name for the account that is configured to access the PostgreSQL database on the Riverbed SteelCentral NetProfiler system.
Password	The password that is required to connect to the database.
Compare Field	`start_time`
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Start Date and Time (Optional)	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	**5M**
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 20,000.

For more information about configuring JDBC protocol parameters, see c_logsource_JDBCprotocol.dita

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Configuring your Riverbed SteelCentral NetProfiler system to enable communication with QRadar

To collect Riverbed SteelCentral NetProfiler alert events, you must configure your Riverbed SteelCentral NetProfiler system to allow QRadar to retrieve events from the PostgreSQL database.

Procedure

1. Log in to your Riverbed SteelCentral NetProfiler host user interface.
2. Select **Configuration** > **Appliance Security** > **Security Compliance**.
3. Check the **Enable ODBC Access** check box.
4. Select **Configuration** > **Account Management** > **User Accounts**.
5. Add an account that QRadar can use to access to the PostgreSQL database.

Chapter 135. RSA Authentication Manager

You can use an RSA Authentication Manager DSM to integrate IBM QRadar with an RSA Authentication Manager 6.x or 7.x by using syslog or the log file protocol. RSA Authentication Manager 8.x uses syslog only.

Before you configure QRadar to integrate with RSA Authentication Manager, select your configuration preference:

- "Configuration of syslog for RSA Authentication Manager 6.x, 7.x and 8.x" on page 1407
- "Configuring the log file protocol for RSA Authentication Manager 6.x and 7.x" on page 1408

Note: You must apply the most recent hot fix on RSA Authentication Manager 7.1 primary, replica, node, database, and radius installations before you configure syslog.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuration of syslog for RSA Authentication Manager 6.x, 7.x and 8.x

The procedure to configure your RSA Authentication Manager 6.x, 7.x and 8.x using syslog depends on the operating system version for your RSA Authentication Manager or SecureID 3.0 appliance.

If you are using RSA Authentication Manager on Linux, see "Configuring Linux" on page 1407.

If you are using RSA Authentication Manager on Windows, see "Configuring Windows" on page 1408.

Configuring Linux

You can configure RSA Authentication Manager for syslog on Linux based operating systems.

Procedure

1. Using SSH, log in to the RSA Security Console as root user.
2. Open one of the following files for editing based on your version of RSA Authentication Manager:

   Versions earlier than version 8
   `/usr/local/RSASecurity/RSAAuthenticationManager/utils/resources/ims.properties`

   Version 8
   `/opt/rsa/am/utils/resources/ims.properties`
3. Add the following entries to the `ims.properties` file:

   ```
   ims.logging.audit.admin.syslog_host = <IP address>
   ims.logging.audit.admin.use_os_logger = true
   ims.logging.audit.runtime.syslog_host = <IP address>
   ims.logging.audit.runtime.use_os_logger = true
   ims.logging.system.syslog_host = <IP address>
   ims.logging.system.use_os_logger = true
   ```

   Where <*IP address*> is the IP address or host name of IBM QRadar.
4. Save the `ims.properties` file.
5. Open the following file for editing:

   `/etc/syslog.conf`
6. Type the following command to add QRadar as a syslog entry:

```
*.* @<IP address>
```

Where <*IP address*> is the IP address or host name of QRadar.

7. Type the following command to restart the syslog services for Linux.

```
service syslog restart
```

For more information on configuring syslog forwarding, see your *RSA Authentication Manager documentation*.

What to do next

Configure the log source and protocol in QRadar. To receive events from RSA Authentication Manager, from the **Log Source Type** list, select the **RSA Authentication Manager** option.

Configuring Windows

To configure RSA Authentication Manager for syslog using Microsoft Windows.

Procedure

1. Log in to the system that hosts your RSA Security Console.
2. Open the following file for editing based on your operating system:

```
/Program Files/RSASecurity/RSAAuthenticationManager/utils/ resources/
ims.properties
```

3. Add the following entries to the `ims.properties` file:

```
ims.logging.audit.admin.syslog_host = <IP address>
ims.logging.audit.admin.use_os_logger = true
ims.logging.audit.runtime.syslog_host = <IP address>
ims.logging.audit.runtime.use_os_logger = true
ims.logging.system.syslog_host = <IP address>
ims.logging.system.use_os_logger = true
```

Where <*IP address*> is the IP address or host name of QRadar.

4. Save the `ims.properties` files.
5. Restart RSA services.

You are now ready to configure the log source in QRadar.

6. To configure QRadar to receive events from your RSA Authentication Manager: From the **Log Source Type** list, select the **RSA Authentication Manager** option.

For more information on configuring syslog forwarding, see your *RSA Authentication Manager documentation*.

Related concepts

"Log File log source parameters for RSA Authentication Manager" on page 1409

Configuring the log file protocol for RSA Authentication Manager 6.x and 7.x

The log file protocol allows IBM QRadar to retrieve archived log files from a remote host. The RSA Authentication Manager DSM supports the bulk loading of log files using the log file protocol source.

The procedure to configure your RSA Authentication Manager using the log file protocol depends on the version of RSA Authentication Manager:

- If you are using RSA Authentication Manager v6.x, see "Configuring RSA Authentication Manager 6.x" on page 1409.

- If you are using RSA Authentication Manager v7.x, see "Configuring RSA Authentication Manager 7.x" on page 1410.

Log File log source parameters for RSA Authentication Manager

If QRadar does not automatically detect the log source, add a RSA Authentication Manager log source on the QRadar Console by using Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from RSA Authentication Manager:

Table 910. Log File log source parameters for the RSA Authentication Manager DSM

Parameter	Value
Log Source type	RSA Authentication Manager
Protocol Configuration	Log File

For a complete list of Log File protocol parameters and their values, see "Log File protocol configuration options" on page 155.

Related tasks

"Adding a log source" on page 5

Configuring RSA Authentication Manager 6.x

You can configure your RSA Authentication Manager 6.x device.

Procedure

1. Log in to the RSA Security Console.
2. Log in to the RSA Database Administration tool:
3. Click the **Advanced** tool.

   The system prompts you to log in again.
4. Click **Database Administration**.

   For complete information on using **SecurID**, see your vendor documentation.
5. From the **Log** list, select **Automate Log Maintenance**.

   The **Automatic Log Maintenance** window is displayed.
6. Select the **Enable Automatic Audit Log Maintenance** check box.
7. Select **Delete and Archive**.
8. Select **Replace files**.
9. Type an archive file name.
10. In the **Cycle Through Version(s)** field, type a value.
11. For example 1, Select **Select all Logs**.
12. Select a frequency.
13. Click **OK**.

Related concepts

"Log File log source parameters for RSA Authentication Manager" on page 1409

Related tasks

"Adding a log source" on page 5

Configuring RSA Authentication Manager 7.x

You can configure your RSA Authentication Manager 7.x device.

Procedure

1. Log in to the RSA Security Console.
2. Click **Administration** > **Log Management** > **Recurring Log Archive Jobs**.
3. In the Schedule section, configure values for the **Job Starts**, **Frequency**, **Run Time**, and **Job Expires** parameters.
4. For the **Operations** field, select **Export Only** or **Export and Purge** for the following settings: **Administration Log Settings**, **Runtime Log Settings**, and **System Log Settings**.

   Note: The **Export and Purge** operation exports log records from the database to the archive and then purges the logs form the database. The **Export Only** operation exports log records from the database to the archive and the records remain in the database.
5. For **Administration**, **Runtime**, and **System**, configure an `Export` Directory to which you want to export your archive files.

   Ensure that you can access the Administration Log, Runtime Log, and System Log by using FTP before you continue.
6. For Administration, Runtime, and System parameters, set the Days Kept Online parameter to 1. Logs older than 1 day are exported. If you selected **Export and Purge**, the logs are also purged from the database.
7. Click **Save**.

Related concepts

"Log File log source parameters for RSA Authentication Manager" on page 1409

"Log File protocol configuration options" on page 155

To receive events from remote hosts, configure a log source to use the Log File protocol.

Related tasks

"Adding a log source" on page 5

Chapter 136. SafeNet DataSecure

The IBM QRadar DSM for SafeNet DataSecure collects syslog events from a SafeNet DataSecure device.

DataSecure maintains activity, such as, record administrative actions, network activity, and cryptography requests. QRadar supports SafeNet DataSecure V6.3.0.

SafeNet DataSecure creates the following event logs:

Activity Log
Contains a record of each request that is received by the key server.

Audit Log
Contains a record of all configuration changes and user input errors that are made to SafeNet KeySecure, whether through the management console or the command-line interface.

Client Event Log
Contains a record of all client requests that have the <RecordEventRequest> element.

System Log
Contains a record of all system events, such as the following events:

- Service starts, stops, and restarts
- SNMP traps
- Hardware failures
- Successful or failed cluster replication and synchronization
- Failed log transfers

To integrate SafeNet DataSecure with QRadar, complete the following steps:

1. Enable syslog on the SafeNet DataSecure device.
2. QRadar automatically detects SafeNet DataSecure after your system receives 25 events and configures a log source. If QRadar does not automatically discover SafeNet DataSecure, add a log source.

Related tasks
"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring SafeNet DataSecure to communicate with QRadar

Before you can add the DSM for SafeNet DataSecure, enable syslog on your SafeNet DataSecure device.

Procedure

1. Log in to the SafeNet DataSecure management console as an administrator with logging access control.
2. Select **Device** > **Log Configuration**.
3. Select the **Rotation & Syslog** tab.
4. Select a log in the **Syslog Settings** section and click **Edit**.
5. Select **Enable Syslog**.
6. Configure the following parameters:

Parameter	Description
Syslog Server #1 IP	The IP address or host name of the target QRadar. Event Collector.

Parameter	Description
Syslog Server #1 Port	The listening port for QRadar. Use Port 514.
Syslog Server #1 Proto	QRadar can receive syslog messages by using either UDP or TCP.

7. Optional. Type an IP address port, and protocol for a Syslog Server #2. When two servers are configured, SafeNet DataSecure sends messages to both servers.
8. Type the Syslog Facility or accept the default value of local1.
9. Click **Save**.

Chapter 137. Salesforce

IBM QRadar supports a range of Salesforce DSMs for the Salesforce Service type.

Salesforce Security

The IBM QRadar DSM for Salesforce Security collects Salesforce Security Auditing audit trail logs and Salesforce Security Monitoring event logs from your Salesforce console by using a RESTful API.

The following table identifies the specifications for the Salesforce Security DSM:

Table 911. Salesforce Security DSM specifications

Specification	**Value**
Manufacturer	Salesforce
DSM	Salesforce Security
RPM file name	DSM-SalesforceSecurity-QRadar_Version-Build_Number.noarch.rpm
Protocol	Salesforce REST API Protocol
QRadar recorded events	Login History, Account History, Case History, Entitlement History, Service Contract History, Contract Line Item History, Contract History, Contact History, Lead History, Opportunity History, Solution History, Salesforce Security Auditing audit trail
Automatically discovered	No
Includes identity	Yes
More information	Salesforce website (http://www.salesforce.com/)

Salesforce Security DSM integration process

To integrate Salesforce Security DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs from the IBM Support Website onto your QRadar Console.
   - Protocol Common RPM
   - SalesforceRESTAPI Protocol RPM
   - DSMCommon RPM
   - Salesforce Security Auditing RPM
   - Salesforce Security RPM
2. Configure the Salesforce Security server to communicate with QRadar.
3. Obtain and install a certificate to enable communication between Salesforce Security and QRadar. The certificate must be in the `/opt/QRadar/conf/trusted_certificates` folder and be in `.DER` format.
4. For each instance of Salesforce Security, create a log source on the QRadar Console.

Configuring the Salesforce Security Monitoring server to communicate with QRadar

To allow QRadar communication, you need to configure Connected App on the Salesforce console and collect information that the Connected App generates. This information is required for when you configure the QRadar log source.

Before you begin

If the RESTful API isn't enabled on your Salesforce server, contact Salesforce support.

Procedure

1. Configure and collect information that is generated by the Connected App.
   a) Log in to your Salesforce Security Monitoring server.
   b) Click the **Setup** button.
   c) In the navigation pane, click **Create** > **Apps** > **New**.
   d) Type the name of your application.
   e) Type the contact email information.
   f) Select **Enable OAuth Settings**.
   g) From the **Selected OAuth Scopes** list, select **Access and manage your data (api)**.
   h) In the **Info URL** field, type a URL where the user can go for more information about your application.
   i) Configure the remaining optional parameters.
   j) Click **Save**.
2. Turn on **Entitlement History**.
   a) Click the **Setup** button.
   b) In the navigation pane, select **Build** > **Customize** > **Entitlement Management** > **Enablement Settings**.
   c) From the **Entitlement Management Settings** window, select the **Enable Entitlement Management** check box.
   d) Click **Save**.

What to do next

The Connected App generates the information that is required for when you to configure a log source on QRadar. Record the following information:

Consumer Key
Use the **Consumer Key** value to configure the **Client ID** parameter for the QRadar log source.

Consumer Secret
You can click the link to reveal the consumer secret. Use the **Consumer Secret** value to configure the **Secret ID** parameter for the QRadar log source.

Important: The **Consumer Secret** value is confidential. Don't store the consumer secret as plain text.

Security token
A security token is sent by email to the email address that you configured as the contact email.

Salesforce REST API log source parameters for Salesforce Security

If QRadar does not automatically detect the log source, add a Salesforce Security log source on the QRadar Console by using the Salesforce REST API protocol.

When you use the Salesforce REST API protocol, you must configure specific parameters.

The following table describes the parameters that require specific values to collect Salesforce REST API events from Salesforce Security:

Table 912. Salesforce REST API log source parameters for the Salesforce Security DSM	
Parameter	**Value**
Log Source type	Salesforce Security
Protocol Configuration	Salesforce REST API
Login URL	The URL of the Salesforce security console. For example, `https://test.my.salesforce.com`.
Username	The user name of the Salesforce security console.
Security Token	The security token that was sent to the email address configured as the contact email for the Connected App on the Salesforce security console.
Client ID	The Consumer Key that was generated when you configured the Connected App on the Salesforce security console.
Secret ID	The Consumer Secret that was generated when you configured the Connected App on the Salesforce security console.
Use Proxy	When a proxy is configured, all traffic for the log source travels through the proxy for QRadar to access the Salesforce Security buckets. Configure the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** fields. If the proxy does not require authentication, you can leave the **Proxy Username** and **Proxy Password** fields blank.
Advanced Options	By default the Salesforce REST API collects Audit Trail and Security Monitoring events. Configure available options as required.

Related tasks

"Adding a log source" on page 5

Salesforce Security Auditing

The IBM QRadar DSM for Salesforce Security Auditing can collect Salesforce Security Auditing audit trail logs that you copy from the cloud to a location that QRadar can access.

The following table identifies the specifications for the Salesforce Security Auditing DSM:

Table 913. Salesforce Security Auditing DSM specifications	
Specification	**Value**
Manufacturer	Salesforce
DSM	Salesforce Security Auditing
RPM file name	DSM-SalesforceSecurityAuditing-*QRadar_Version-Build_Number*.noarch.rpm

Table 913. Salesforce Security Auditing DSM specifications (continued)	
Specification	**Value**
Protocol	Log File
QRadar recorded events	Setup Audit Records
Automatically discovered	No
Includes identity	No
More information	Salesforce web site (http://www.salesforce.com/)

Salesforce Security Auditing DSM integration process

To integrate Salesforce Security Auditing DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Log File Protocol RPM
   - Salesforce Security Auditing RPM
2. Download the Salesforce audit trail file to a remote host that QRadar can access.
3. For each instance of Salesforce Security Auditing, create a log source on the QRadar Console.

Downloading the Salesforce audit trail file

To collect Salesforce Security Auditing events, you must download the Salesforce audit trail file to a remote host that QRadar can access.

About this task

You must use this procedure each time that you want to import an updated set of audit data into QRadar. When you download the audit trail file, you can overwrite the previous audit trail CSV file. When QRadar retrieves data from the audit trail file, QRadar processes only audit records that were not imported before.

Procedure

1. Log in to your Salesforce Security Auditing server.
2. Go to the **Setup** section.
3. Click **Security Controls**.
4. Click **View Setup Audit Trail**.
5. Click **Download setup audit trail for last six months (Excel.csv file)**.
6. Copy the downloaded file to a location that QRadar can reach by using Log File Protocol.

Log File log source parameters for Salesforce Security Auditing

If QRadar does not automatically detect the log source, add a Salesforce Security Auditing log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events fromSalesforce Security Auditing:

Table 914. Log File log source parameters for the Salesforce Security Auditing DSM	
Parameter	**Value**
Log Source type	Salesforce Security Auditing

Table 914. Log File log source parameters for the Salesforce Security Auditing DSM (continued)	
Parameter	**Value**
Protocol Configuration	Log File
Event Generator	RegEx Based Multiline
Start Pattern	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w+)
End Pattern	Ensure that this parameter remains empty.
Date Time RegEx	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w+)
Date Time Format	dd/MM/yyyy hh:mm:ss z

For a complete list of Log File protocol parameters and their values, see "Log File protocol configuration options" on page 155.

Related tasks

"Adding a log source" on page 5

Chapter 138. Samhain Labs

The Samhain Labs Host-Based Intrusion Detection System (HIDS) monitors changes to files on the system.

The Samhain HIDS DSM for IBM QRadar supports Samhain version 2.4 when used for File Integrity Monitoring (FIM).

You can configure the Samhain HIDS DSM to collect events by using syslog or JDBC.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring syslog to collect Samhain events

Before you configure IBM QRadar to integrate with Samhain HIDS using syslog, you must configure the Samhain HIDS system to forward logs to your QRadar system.

About this task

The following procedure is based on the default samhainrc file. If the samhainrc file is modified, some values might be different, such as the syslog facility,

Procedure

1. Log in to Samhain HIDS from the command-line interface.
2. Open the following file:

   `/etc/samhainrc`
3. Remove the comment marker (*#*) from the following line:

   `SetLogServer=info`
4. Save and exit the file.

   Alerts are sent to the local system by using syslog.
5. Open the following file:

   `/etc/syslog.conf`
6. Add the following line:

   `local2.* @<IP Address>`

   Where <*IP Address*> is the IP address of your QRadar.
7. Save and exit the file.
8. Restart syslog:

   `/etc/init.d/syslog restart`

   Samhain sends logs by using syslog to QRadar.

   You are now ready to configure Samhain HIDS DSM in QRadar. To configure QRadar to receive events from Samhain:
9. From the **Log Source Type** list, select the **Samhain HIDS** option.

Related tasks

"Adding a log source" on page 5

JDBC log source parameters for Samhain

If QRadar does not automatically detect the log source, add a Samhain log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Samhain:

Table 915. JDBC log source parameters for the Samhain DSM

Parameter	Value
Log Source type	Samhain HIDS
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	Select **Oracle**, **PostgresSQL**, or **MySQL**
Database Name	*<Samhain SetDBName>*
IP or Hostname	*<Samhain SetDBHost>*
Username	*<Samhain SetDBUser>*
Password	*<Samhain SetDBPassword>*
Table Name	*<Samhain SetDBTable>*

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

"Adding a log source" on page 5

JDBC protocol configuration options

QRadar uses the JDBC protocol to collect information from tables or views that contain event data from several database types.

The JDBC protocol is an outbound/active protocol. QRadar does not include a MySQL driver for JDBC. If you are using a DSM or protocol that requires a MySQL JDBC driver, you must download and install the *platform-independent* `MySQL Connector/J` from http://dev.mysql.com/downloads/connector/j/.

1. Copy the Java archive (JAR) file to `/opt/qradar/jars` and `/opt/ibm/si/services/ecs-ec-ingress/eventgnosis/lib/q1labs/`.
2. Restart Tomcat service by typing the following command:

```
systemctl restart tomcat
```

3. Restart event collection services by typing the following command:

```
systemctl restart ecs-ec-ingress
```

The following table describes the protocol-specific parameters for the JDBC protocol:

Table 916. JDBC protocol parameters

Parameter	Description
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source Type	Select your Device Support Module (DSM) that uses the JDBC protocol from the **Log Source Type** list.
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or hostname, use the IP address or hostname of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or hostname, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	Select the type of database that contains the events.
Database Name	The name of the database to which you want to connect.
Schema (Snowflake only)	This parameter specifies either the default schema to be used for the specified database post connection, or an empty string. The specified schema must be an existing schema for which the specified default role has privileges.
IP or Hostname	The IP address or hostname of the database server.
Warehouse (Snowflake only)	This parameter specifies the virtual warehouse to use post connection, or an empty string. The specified warehouse must be an existing warehouse for which the specified default role has privileges.

Table 916. JDBC protocol parameters (continued)	
Parameter	**Description**
Role (Snowflake only)	This parameter specifies the default access control role to be used in the Snowflake session initiated by the driver. The specified role must be an existing role that is already assigned to the specified user for the driver. If the specified role is not assigned to the user, then the role is not used during the session initiation by the driver.
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • Db2 - 50000 • Informix - 9088 • MSDE - 1433 • MySQL - 3306 • Oracle - 1521 • Postgres - 5432 • Sybase - 5000 • Snowflake - 443 If you configure the **Database Instance** parameter and have an MSDE database type, leave the **Port** parameter blank.
Username	A user account for QRadar in the database.
Password	The password that is required to connect to the database.
Confirm Password	The password that is required to connect to the database.
Authentication Domain (MSDE only)	If you disable **Use Microsoft JDBC**, the **Authentication Domain** parameter is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance (MSDE or Informix only)	The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When you use a different port number from the default for SQL database resolution, leave this parameter blank.
Predefined Query (Optional)	Select a predefined database query for the log source. If a predefined query is not available for the log source type, you can select the **None** option. If the configuration guide for a specific integration states to use a predefined query, choose it from the list. Otherwise, select **None** and populate the remaining required values.
Table Name	The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).

Table 916. JDBC protocol parameters (continued)	
Parameter	**Description**
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If you defined a comma-separated list, the list must contain the field that is defined in the **Compare Field** parameter.
Compare Field	A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. When you set this parameter value, the protocol identifies events that were previously pulled by the protocol to ensure that duplicate events are not created.
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Start Date and Time (Optional)	Select or enter the start date and time for database polling. The format is yyyy-mm-dd HH:mm, where HH is specified by using a 24-hour clock. If this parameter is empty, polling begins immediately and repeats at the specified polling interval. This parameter is used to set the time and date at which the protocol connects to the target database to initialize event collection. It can be used along with the **Polling Interval** parameter to configure specific schedules for the database polls. For example, use these parameters to ensure that the poll happens at five minutes past the hour, every hour, or to ensure that the poll happens at exactly 1:00 AM each day. This parameter cannot be used to retrieve older table rows from the target database. For example, if you set the parameter to **Last Week**, the protocol does not retrieve all table rows from the previous week. The protocol retrieves rows that are newer than the maximum value of the **Compare Field** on initial connection.
Polling Interval	Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value. The maximum polling interval is one week.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 20,000.

Table 916. JDBC protocol parameters (continued)	
Parameter	**Description**
Security Mechanism (Db2 only)	From the list, select the security mechanism that is supported by your Db2 server. If you don't want to select a security mechanism, select **None**. The default is **None**. For more information about security mechanisms that are supported by Db2 environments, see the IBM Support website (https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_cjvjcsec.html)
Use Named Pipe Communication (MSDE only)	If you disable **Use Microsoft JDBC**, the **Use Named Pipe Communication** parameter is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.
Database Cluster Name	If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly. This parameter is required if you enable **Use Named Pipe Communication** and select the MSDE database type option.
Use NTLMv2 (MSDE only)	If you disable **Use Microsoft JDBC**, the **Use NTLMv2** parameter is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use Microsoft JDBC (MSDE only)	If you want to use the Microsoft JDBC driver, you must enable **Use Microsoft JDBC**. This parameter is enabled by default.
Use SSL (MSDE only)	Enable this option if your MSDE connection supports SSL.
SSL Certificate Hostname	This field is required when both **Use Microsoft JDBC** and **Use SSL** are enabled. This value must be the fully qualified domain name (FQDN) for the host. The IP address is not permitted. For more information about SSL certificates and JDBC, see the procedures at the following links: • QRadar: Configuring JDBC Over SSL with a Self-signed certificate (https://www.ibm.com/support/pages/node/246077) • Configuring JDBC Over SSL with an Externally-signed Certificate (https://www.ibm.com/support/pages/node/246079)

Table 916. JDBC protocol parameters (continued)	
Parameter	**Description**
Use Oracle Encryption(Oracle only)	*Oracle Encryption and Data Integrity settings* is also known as *Oracle Advanced Security*. If selected, Oracle JDBC connections require the server to support similar Oracle Data Encryption settings as the client.
Database Locale (Informix only)	For multilingual installations, specify the language to use for the installation process (or software?). After you choose a language, you can then choose the character set that is used in the installation in the **Code-Set** parameter.
Code-Set (Informix only)	The **Code-Set** parameter displays after you choose a language for multilingual installations. Use this field to specify the character set to use.
Enabled	Select this checkbox to enable the log source. By default, the checkbox is selected.
Credibility	From the list, select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select the **Coalescing Events** checkbox to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select the **Store Event Payload** checkbox to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Enable Advanced Options	Select this checkbox to enable advanced options. When disabled, the default value is used.
Use With (No Lock) in SQL statements	Enable this option to append the tables in all SQL statements with "WITH (NOLOCK)".

Chapter 139. SAP Enterprise Threat Detection

The IBM QRadar DSM for SAP Enterprise Threat Detection collects events from an SAP Enterprise Threat Detection server. SAP Enterprise Threat Detection enables real-time security intelligence to help protect against cybersecurity threats and help ensure data loss prevention.

To integrate SAP Enterprise Threat Detection with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol-Common RPM
   - SAP ETD Alert API Protocol RPM
   - SAP Enterprise Threat Detection DSM RPM
2. Configure QRadar to receive events from SAP Enterprise Threat Detection. See "SAP Enterprise Threat Detection Alert API log source parameters for SAP Enterprise Threat Detection" on page 1428.
3. Configure SAP Enterprise Threat Detection to communicate with QRadar. See the Enterprise ThreatMonitor Integration documentation. (https://www.enterprise-threat-monitor.com/sap-qradar-enterprise-threat-detection-siem-integration/)
4. If QRadar does not automatically detect the log source, add an SAP Enterprise Threat Detection log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Related reference

"SAP Enterprise Threat Detection DSM specifications" on page 1427

The following table describes the specifications for the SAP Enterprise Threat Detection DSM.

SAP Enterprise Threat Detection DSM specifications

The following table describes the specifications for the SAP Enterprise Threat Detection DSM.

Table 917. SAP Enterprise Threat Detection DSM specifications

Specification	Value
Manufacturer	SAP
DSM name	SAP Enterprise Threat Detection
RPM file name	`DSM-SAPEnterpriseThreatDetection-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	SAP Enterprise Threat Detection V1.0 SP6 to V2.0 SP5
Protocol	SAP Enterprise Threat Detection Alert API
Event format	LEEF
Recorded event types	Alerts
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No

Table 917. SAP Enterprise Threat Detection DSM specifications (continued)	
Specification	**Value**
More information	SAP Help Portal (https://www.sap.com/products/enterprise-threat-detection.html#why-sap)

SAP Enterprise Threat Detection Alert API log source parameters for SAP Enterprise Threat Detection

If QRadar does not automatically detect the log source, add a SAP Enterprise Threat Detection log source on the QRadar Console by using the SAP Enterprise Threat Detection Alert API protocol.

When using the SAP Enterprise Threat Detection Alert API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SAP Enterprise Threat Detection Alert API events from SAP Enterprise Threat Detection:

Table 918. SAP Enterprise Threat Detection Alert API log source parameters for the SAP Enterprise Threat Detection DSM	
Parameter	**Value**
Log Source type	SAP Enterprise Threat Detection
Protocol Configuration	SAP Enterprise Threat Detection Alert API
Log Source Identifier	A unique identifier for the log source. The Log Source Identifier can be any valid value, including the same value as the Log Source Name, and doesn't need to reference a specific server. If you configured multiple SAP Enterprise Threat Detection Alert API log sources, you might want to identify the first log source as SAPETD-1, the second log source as SAPETD-2, and the third log source as SAPETD-3.
Server URL	Specify the URL used to access the SAP Enterprise Threat Detection Alert API, including the port. For example, “http://192.0.2.1:8003” or “https://192.0.2.1:9443”.s
Username/Password	Enter the user name and password that are required to access the SAP ETD server, and then confirm that you entered the password correctly. The confirmation password must be identical to the password you typed for the *password* parameter. **Important:** SAP Enterprise Threat Detection has a login attempt limit of three attempts. If your account is locked because of multiple login attempts, you cannot connect QRadar to the SAP Enterprise Threat Detection Server until the account is unlocked. Contact SAP Support for assistance.

Table 918. SAP Enterprise Threat Detection Alert API log source parameters for the SAP Enterprise Threat Detection DSM (continued)

Parameter	Value
Use Pattern Filter	Select this option to limit the query to only a specific pattern filter. Leave the field cleared to query for all the events.
Pattern Filter ID	The pattern filter Id that is used to filter the query. The field accepts a UUID that is created when a pattern filter is made. The **Filter ID** is the UUID mentioned in the protocol parameters table for parameter **Pattern Filter Id**.
Use Proxy	If QRadar accesses the SAP Enterprise Threat Detection Alert API by using a proxy, enable Use Proxy. If the proxy requires authentication, configure the **Proxy Hostname or IP**, **Proxy Port**, **Proxy Username**, and **Proxy** fields. If the proxy does not require authentication, configure the **Proxy Hostname or IP** and **Proxy Port**.
Automatically Acquire Server Certificates	If you choose **Yes** from the list, QRadar automatically downloads the certificate and begins trusting the target server. If **No** is selected, QRadar does not attempt to retrieve any server certificates. **Note:** If the SAP Enterprise Threat Detection Server is configured for HTTPS, a valid certificate is required. Either set this value to **Yes** or manually retrieve a certificate for the Log Source.
Recurrence	The time interval between log source queries to the SAP Enterprise Threat Detection Alert API for new events. The time interval can be in hours (H), minutes (M), or days (D). The default is 5 minutes (5M).
Throttle	The maximum number of events per second. The default is 5000.

Related tasks

"Adding a log source" on page 5

Creating a pattern filter on the SAP server

A **Pattern Filter** is a user configured setting that can be used to limit queries to specific events. When a **Pattern Filter** is generated on the SAP server, a **Filter Id** is provided. The **Filter Id** can then be entered into the **Pattern Filter Id** field of the QRadar log source to filter the patterns that are retrieved.

Procedure

1. To create the **Pattern Filter** on the SAP Server, use the following steps:
   a) Log in into the SAP server by using the administrator user name and password.

b) Go to **Administration** > **Settings**.

c) Select **Pattern Filter** and click **Add**.

d) Enter a name for the **Pattern Filter**. This name is only used for identification purposes.

Note: The name appears in the **Name Column** with a corresponding **Filter Id** (UUID). Record the **Filter Id** for future reference.

e) Click the pattern filter name to see a new table with **Namespace** as a column header.

f) To add patterns to the **Pattern Filter**, click **Add**.

Note: A new window appears called **Pattern**.

g) Select any **Pattern** you want to filter on and click **OK**.

h) Refresh the page and ensure that the **Pattern** was added to the table with the **Namespace** header.

2. To use a **Pattern Filter** with QRadar, use the following steps:

a) Either select or create an SAP ETD Alert API log source.

b) Find the **Use Pattern Filter Id** check box and select it.

c) Enter the **Filter Id** obtained in step 1d and enter it in the **Patter Filter Id** field.

d) Save the log source.

Note: If you receive a 500 Internal Server Error after you save the log source with the **Filter Id**, double check that there is at least one pattern that is being filtered for.

Troubleshooting the SAP Enterprise Threat Detection Alert API

The SAP Enterprise Threat Detection DSM relies on the default pattern names of alerts to identify the events. Modifying the default patterns might result in events that appear as "Unknown".

Procedure

1. Verify that the SAP Enterprise Threat Detection server login credentials are valid by following these steps:

a) In a Web browser, enter the IP address or domain name of your SAP Enterprise Threat Detection server. For example, `http://192.0.2.1:8003`.

b) Enter your user name and password.

2. Query the SAP Enterprise Threat Detection server to verify that QRadar can receive events. Use the following example as a starting point to create your query:

```
<Server_URL>/sap/secmon/services/Alerts.xsjs?$
query=AlertCreationTimestamp%20ge%20<Date>T15:00:00.00Z&$format=LEEF&$batchSize=10
```

In the example, replace the following parameters with your own values:

<Server_URL>
The address of the SAP Enterprise Threat Detection server you are trying to access.

<Date>
The current day's date in the YYYY-MM-DD format. Choose a date where you know that events came in; for example, 2017-10-15.

The resulting query might look like this example:

```
http://192.0.2.1:8003/sap/secmon/services/Alerts.xsjs?$query=AlertCreationTimestamp
%20ge%202017-10-15T15:00:00.00Z&$format=LEEF&$batchSize=10
```

If a problem exists with the query, it's unlikely that QRadar can successfully connect with SAP Enterprise Threat Detection.

3. Check that the server port is not blocked by a firewall.

Note: If the port is blocked, contact your security or network administrator to open the port.

Related concepts

"SAP Enterprise Threat Detection V1.0 SP6 sample event messages" on page 1431
Use these sample event messages as a way of verifying a successful integration with QRadar. Replace the sample IP addresses, and so on with your own content.

Related reference

"SAP Enterprise Threat Detection DSM specifications" on page 1427
The following table describes the specifications for the SAP Enterprise Threat Detection DSM.

SAP Enterprise Threat Detection V1.0 SP6 sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar. Replace the sample IP addresses, and so on with your own content.

The following table provides sample event messages for the SAP Enterprise Threat Detection DSM.

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM

Event name	Low-level category	Sample log message
Blacklisted function modules	Potential Misc. Exploit	LEEF:1.0|SAP|ETD|1.0 SP5|Blacklisted function modules (http://sap.com/secmon/basis)| devTime=2017-04-03T08:12:01.931Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Access to Critical Resource PatternId=55824E7FE1B0FE2BE10000000A4CF109 PatternType=FLAB AlertId=2888 sev=7 MinResultTimestamp=2017-04-03T08:10:05.000Z MaxResultTimestamp=2017-04-03T08:10:05.000Z Text=Measurement 1 reached threshold 1 for ('Event, Scenario Role Of Actor' = 'Server' / 'Network, Hostname, Initiator' = '<hostname>' / 'Network, IP Address, Initiator' = '<IP_address>' / 'Service, Function Name' = 'RFC_READ_TABLE' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Acting' = '<username>') Measurement=1 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> EventScenarioRoleOfActor=Server NetworkHostnameInitiator=<hostname> NetworkIPAddressInitiator=192.0.2.* ServiceFunctionName=RFC_READ_TABLE SystemIdActor=<computer name> UserPseudonymActing=<username> usrName=<username>

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Blacklisted transactions	Potential Misc. Exploit	LEEF:1.0|SAP|ETD|1.0 SP5|Blacklisted transactions (http://sap.com/secmon/basis)| devTime=2017-04-06T12:39:01.834Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Access to Critical Resource PatternId=55824E81E1B0FE2BE10000000A4CF109 PatternType=FLAB AlertId=3387 sev=7 MinResultTimestamp=2017-04-06T12:38:04.000Z MaxResultTimestamp=2017-04-06T12:38:25.000Z Text=Measurement 4 exceeded threshold 1 for ('Network, Hostname, Initiator' = '<hostname>' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Acting' = '<username>') Measurement=4 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> NetworkHostnameInitiator=<hostname> SystemIdActor=<computer name> UserPseudonymActing=<username> usrName=<username>
Brute force attack	Brute force attack	LEEF:1.0|SAP|ETD|1.0 SP5|Brute force attack (http://sap.com/secmon/basis)| devTime=2017-03-16T00:10:01.891Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Brute Force Attack PatternId=55827776E1B0FE2BE10000000A4CF109 PatternType=FLAB AlertId=1303 sev=4 MinResultTimestamp=2017-03-15T23:24:38.000Z MaxResultTimestamp=2017-03-16T00:08:47.000Z Text=Measurement 16 exceeded threshold 12 for 'Network, Hostname, Initiator' = 'null' Measurement=16 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> NetworkHostnameInitiator=null

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Data Exchange by System ID with Third-Party Systems	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Data Exchange by System Id with Third Party Systems (http://sap.com/secmon/basis)| devTime=2017-08-22T15:03:12.158Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=System PatternId=22610959E8B5F1499E4CFCCB1422C3D3 PatternType=ANOMALY AlertId=12279 sev=7 MinResultTimestamp=2017-08-22T13:00:00.000Z MaxResultTimestamp=2017-08-22T14:00:00.000Z Text=Anomaly score is 73 for ('System ID, Actor' = '<computer name>' / 'System Type, Actor' = 'https://www.expedia.ca/Kenoza-Lake-Hotels-Kenoza-Lake-View-Manor.h19660605.Hotel-Information?chkin=15%2F06%2F2018&chkout=16%2F06%2F2018&rm1=a2&regionId=0&hwrqCacheKey=557055a7-9bd8-4191-8044-1a9072ac2b76HWRQ1522171541587&vip=false&c=e6079ffc-cd41-477f-aaed-c2d9e1df2fa9&mctc=10&exp_dp=218.48&exp_ts=1522171542334&exp_curr=CAD&swpToggleOn=false&exp_pg=HSR') Measurement=73 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> SystemIdActor=<computer name> SystemTypeActor=ABAP
Data Exchange by Technical User	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Data Exchange by Technical User (http://sap.com/secmon/basis)| devTime=2017-03-28T14:02:26.154Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Technical Users,Users PatternId=7CCB9FFD5249FC4AA2B83D4BC5C8EA06 PatternType=ANOMALY AlertId=2490 sev=10 MinResultTimestamp=2017-03-28T12:00:00.000Z MaxResultTimestamp=2017-03-28T13:00:00.000Z Text=Anomaly score is 100 for 'User Pseudonym, Acting' = '<username>' Measurement=100 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> UserPseudonymActing=<username> usrName=<username>

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Debugging in systems assigned to critical roles	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Debugging in systems assigned to critical roles (http://sap.com/secmon/basis)| devTime=2017-04-03T08:06:06.370Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Debugging PatternId=937627F31E37524F837F9374804DE234 PatternType=FLAB AlertId=2880 sev=7 MinResultTimestamp=2017-04-03T08:06:04.752Z MaxResultTimestamp=2017-04-03T08:06:04.752Z Text=Measurement 1 reached threshold 1 for ('Network, Hostname, Initiator' = '<hostname>' / 'System ID, Actor' = '<computer name>' / 'System Type, Actor' = 'ABAP' / 'User Pseudonym, Acting' = '<username>') Measurement=1 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> NetworkHostnameInitiator=<hostname> SystemIdActor=<computer name> SystemTypeActor=ABAP UserPseudonymActing=<username> usrName=<username>
Failed logon by RFC/CPIC call	User Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Failed logon by RFC/CPIC call (http://sap.com/secmon/basis)| devTime=2016-12-27T11:58:24.588Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Failed Logon PatternId=5582D941F02EFE2BE10000000A4CF109 PatternType=FLAB AlertId=177 sev=7 MinResultTimestamp=2016-12-27T11:54:42.000Z MaxResultTimestamp=2016-12-27T11:55:01.000Z Text=Measurement 3 reached threshold 3 for ('System ID, Actor' = '<computer name>' / 'User Pseudonym, Targeted' = 'null') Measurement=3 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> SystemIdActor=<computer name> UserPseudonymTargeted=null

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Failed logon with too many attempts	User Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Failed logon with too many attempts (http://sap.com/secmon/basis)| devTime=2017-06-07T17:33:02.029Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Failed Logon PatternId=5582D942F02EFE2BE10000000A4CF109 PatternType=FLAB AlertId=6287 sev=7 MinResultTimestamp=2017-06-07T16:33:01.000Z MaxResultTimestamp=2017-06-07T17:32:59.000Z Text=Measurement 39193 exceeded threshold 3 for ('Event (Semantic)' = 'User, Logon, Failure' / 'System ID, Actor' = '<username>' / 'User Pseudonym, Targeted' = '<username>') Measurement=39193 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> EventSemantic=User, Logon, Failure SystemIdActor=<username> UserPseudonymTargeted=<username>
Generic access to critical database tables	Database Exploit	LEEF:1.0|SAP|ETD|1.0 SP5|Generic access to critical database tables (http://sap.com/secmon/basis)| devTime=2017-03-29T15:50:10.291Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Data Manipulation PatternId=DF3F93F156DAAA408C1512168E16F2B0 PatternType=FLAB AlertId=2558 sev=7 MinResultTimestamp=2017-03-29T15:48:12.000Z MaxResultTimestamp=2017-03-29T15:48:12.000Z Text=Measurement 1 reached threshold 1 for ('Generic, Action' = '03' / 'Resource Name' = '<computer name>' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Acting' = '<username>') Measurement=1 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> GenericAction=03 ResourceName=<computer name> SystemIdActor=<computer name> UserPseudonymActing=<username> usrName=<username>

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Log Volume by System Group	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Log Volume by System Group (http://sap.com/secmon/basis)| devTime=2016-12-27T13:02:32.321Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=System,Test PatternId=7A8D37B77AF8CF4096B9EB49BA932ACD PatternType=ANOMALY AlertId=196 sev=10 MinResultTimestamp=2016-12-27T11:00:00.000Z MaxResultTimestamp=2016-12-27T12:00:00.000Z Text=Anomaly score is 100 for ('System Group, ID, Actor' = 'null' / 'System Group, Type, Actor' = 'null') Measurement=100 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> SystemGroupIdActor=null SystemGroupTypeActor=null
Logon and Communication by System ID	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Logon and Communication by System Id (http://sap.com/secmon/basis)| devTime=2017-06-08T14:03:13.156Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=System PatternId=B09BED65105D4D4C9EE82FBCCFAD6647 PatternType=ANOMALY AlertId=6634 sev=7 MinResultTimestamp=2017-06-08T12:00:00.000Z MaxResultTimestamp=2017-06-08T13:00:00.000Z Text=Anomaly score is 70 for ('System ID, Actor' = '<computer name>' / 'System Type, Actor' = 'ABAP') Measurement=70 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> SystemIdActor=<computer name> SystemTypeActor=ABAP

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Logon success same user from different Terminal IDs	User Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Logon success same user from different Terminal IDs (http://sap.com/secmon/basis)| devTime=2016-10-24T11:13:04.589Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Suspicious Logon PatternId=5582A320E1B0FE2BE10000000A4CF109 PatternType=FLAB AlertId=2 sev=7 MinResultTimestamp=2016-10-24T07:17:36.000Z MaxResultTimestamp=2016-10-24T08:40:34.000Z Text=Measurement 2 reached threshold 2 for ('System ID, Actor' = '<username>' / 'User Pseudonym, Targeted' = 'null') Measurement=2 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> SystemIdActor=<username> UserPseudonymTargeted=null
Logon with SAP standard users	User Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Logon with SAP standard users (http://sap.com/secmon/basis)| devTime=2017-03-13T21:05:01.494Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Suspicious Logon PatternId=5582A31CE1B0FE2BE10000000A4CF109 PatternType=FLAB AlertId=1000 sev=4 MinResultTimestamp=2017-03-13T13:32:04.000Z MaxResultTimestamp=2017-03-13T21:02:10.000Z Text=Measurement 1 reached threshold 1 for ('Event (Semantic)' = 'User, Logon' / 'Network, Hostname, Initiator' = 'null' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Targeted' = '<username>') Measurement=1 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> EventSemantic=User, Logon NetworkHostnameInitiator=null SystemIdActor=<computer name> UserPseudonymTargeted=<username>

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
New Service Calls by Technical Users	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|New Service Calls by Technical Users (http://sap.com/secmon/basis)| devTime=2017-02-16T23:02:22.157Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Technical Users,Users PatternId=5F852070B8645C42907C90C27864E20D PatternType=ANOMALY AlertId=251 sev=7 MinResultTimestamp=2017-02-16T21:00:00.000Z MaxResultTimestamp=2017-02-16T22:00:00.000Z Text=Anomaly score is 74 for ('System ID, Actor' = '<computer name>' / 'System Type, Actor' = 'ABAP' / 'User Pseudonym, Acting' = '<computer name>') Measurement=74 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> SystemIdActor=<computer name> SystemTypeActor=ABAP UserPseudonymActing=<computer name> usrName=<computer name>
Security relevant configuration changes	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Security relevant configuration changes (http://sap.com/secmon/basis)| devTime=2017-06-30T19:28:56.835Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Configuration PatternId=558292A9E1B0FE2BE10000000A4CF109 PatternType=FLAB AlertId=9273 sev=7 MinResultTimestamp=2017-06-30T19:26:34.000Z MaxResultTimestamp=2017-06-30T19:26:34.000Z Text=Measurement 1 reached threshold 1 for ('Event (Semantic)' = 'System Admin, Audit Policy, Alter' / 'Network, Hostname, Initiator' = 'null' / 'System ID, Actor' = '<username>' / 'System Type, Actor' = 'ABAP' / 'User Pseudonym, Acting' = 'null') Measurement=1 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> EventSemantic=System Admin, Audit Policy, Alter NetworkHostnameInitiator=null SystemIdActor=<username> SystemTypeActor=ABAP UserPseudonymActing=null usrName=null

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Service Calls by System ID	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|Service Calls by System Id (http://sap.com/secmon/basis)| devTime=2017-03-22T13:03:40.160Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=System PatternId=8CF6323786DE674691BB716CAEA1111D PatternType=ANOMALY AlertId=1892 sev=10 MinResultTimestamp=2017-03-22T11:00:00.000Z MaxResultTimestamp=2017-03-22T12:00:00.000Z Text=Anomaly score is 99 for ('System ID, Actor' = '<computer name>' / 'System Type, Actor' = 'ABAP') Measurement=99 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> SystemIdActor=<computer name> SystemTypeActor=ABAP
User acts under created user	User Activity	LEEF:1.0|SAP|ETD|1.0 SP5|User acts under created user (http://sap.com/secmon/basis)| devTime=2017-04-03T08:17:03.529Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=User Maintenance PatternId=76560A14DBEC9C4A9EA502EFD6EA3BCC PatternType=FLAB AlertId=2893 sev=7 MinResultTimestamp=2017-04-03T08:07:34.000Z MaxResultTimestamp=2017-04-03T08:10:05.000Z Text=Measurement 2 exceeded threshold 1 for ('Network, Hostname, Initiator' = '<hostname>' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Targeted' = '<username>') Measurement=2 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> NetworkHostnameInitiator=<hostname> SystemIdActor=<computer name> UserPseudonymTargeted=<username>

Table 919. SAP Enterprise Threat Detection V1.0 SP6 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
User role changed	Suspicious Activity	LEEF:1.0|SAP|ETD|1.0 SP5|User role changed (http://sap.com/secmon/basis)| devTime=2017-04-06T12:40:42.056Z devTimeFormat=YYYY-MM-dd'T'HH:mm:ss.SSSX cat=Authorization Critical Assignment PatternId=305166E4E6C11B4593B31CFBB6BABD44 PatternType=FLAB AlertId=3390 sev=4 MinResultTimestamp=2017-04-06T12:40:22.000Z MaxResultTimestamp=2017-04-06T12:40:22.000Z Text=Measurement 3 exceeded threshold 1 for ('Event (Semantic)' = 'User Admin, Role, Create' / 'Network, Hostname, Initiator' = 'null' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Acting' = '<username>') Measurement=3 UiLink=http://192.0.2.*/sap/hana/uis/clients/ushell-app/shells/fiori/FioriLaunchpad.html?siteId=sap.secmon.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show\?alert=<Alert Id> EventSemantic=User Admin, Role, Create NetworkHostnameInitiator=null SystemIdActor=<computer name> UserPseudonymActing=<username> usrName=<username>

SAP Enterprise Threat Detection V2.0 SP5 sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar. Replace the sample IP addresses, and so on with your own content.

The following table provides sample event messages for the SAP Enterprise Threat Detection DSM.

Table 920. SAP Enterprise Threat Detection V2.0 SP5 sample message supported by the SAP Enterprise Threat Detection DSM

Event name	Low-level category	Sample log message
Logon success same user from different Terminal IDs	Suspicious Logon	LEEF:1.0|SAP|ETD|2.0 SP5|Logon success same user from different Terminal IDs (http://example.com/qradar/basis)| devTime=2023-06-01T13:10:15.119Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Suspicious Logon PatternId=10000000000000000012345678912345 6 PatternType=FLAB AlertId=2382283 sev=7 MinResultTimestamp=2023-06-01T13:01:50.980Z MaxResultTimestamp=2023-06-01T13:01:51.378Z Text=Measurement 2 reached threshold 2 for ('System ID, Actor' = '<computer name>' / 'User Pseudonym, Target' = '<username>') Measurement=2 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html?siteId=exp.com.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show?alert=<Alert Id> SystemIdActor=<computer name> UserPseudonymTargeted=<username>

Table 920. SAP Enterprise Threat Detection V2.0 SP5 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Calls between a non-productive and a productive system	Cross Communication	LEEF:1.0|SAP|ETD|2.0 SP5|Calls between a non-productive and a productive system (http://example.com/qradar/basis)| devTime=2023-06-01T13:25:29.714Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Cross Communication PatternId=20000000000000000001234567891234567 PatternType=FLAB AlertId=2382291 sev=4 MinResultTimestamp=2023-06-01T13:16:08.000Z MaxResultTimestamp=2023-06-01T13:25:08.120Z Text=Measurement 228 exceeded threshold 1 for ('Correlation ID' = '<correlation Id>' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Actor' = '<username>') Measurement=228 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html?siteId=exp.com.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show?alert=<Alert Id> CorrelationId=<correlation Id> SystemIdActor=<computer name> UserPseudonymActing=<username> usrName=<username>
Logon success same Terminal ID with different users	Suspicious Logon V1	LEEF:1.0|SAP|ETD|2.0 SP5|Logon success same Terminal ID with different users (http://demo)| devTime=2023-06-01T13:20:12.146Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Suspicious Logon V1 PatternId=70000000000000000001234567891234567 PatternType=FLAB AlertId=2382287 sev=4 MinResultTimestamp=2023-06-01T12:51:06.000Z MaxResultTimestamp=2023-06-01T13:20:06.941Z Text=Measurement 2 reached threshold 2 for ('Network, Hostname, Initiator' = '<hostname>' / 'System ID, Actor' = '<computer name>') Measurement=2 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html?siteId=exp.com.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show?alert=<Alert Id> NetworkHostnameInitiator=<hostname> SystemIdActor=<computer name>

Table 920. SAP Enterprise Threat Detection V2.0 SP5 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
SAP HANA Partitioning unsuccessful Heath Check	Health Checks	LEEF:1.0|SAP|ETD|2.0 SP5|SAP HANA Partitioning unsuccessful Health Check (http://exm.com/qradar)| devTime=2023-05-30T12:05:50.176Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Health Checks PatternId=500000000000000001234567891234567 PatternType=FLAB AlertId=2381877 sev=7 MinResultTimestamp=2023-05-30T12:05:28.000Z MaxResultTimestamp=2023-05-30T12:05:28.000Z Text=Measurement 5 exceeded threshold 1 for 'System ID' = 'ABC' Measurement=5 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html?siteId=exp.com.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show?alert=<Alert Id> systemId=ABC
Security relevant policy changes	Security relevant policy changes	LEEF:1.0|SAP|ETD|2.0 SP5|Security relevant policy changes (http://example.com/qradar/basis)| devTime=2023-05-30T12:11:30.015Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Configuration PatternId=300000000000000001234567891234567 PatternType=FLAB AlertId=2381879 sev=7 MinResultTimestamp=2023-05-30T12:07:05.000Z MaxResultTimestamp=2023-05-30T12:07:05.000Z Text=Measurement 1 reached threshold 1 for ('Event (Semantic)' = 'System Admin, Audit Policy, Alter' / 'Network, Hostname, Initiator' = '<hostname>' / 'System ID, Actor' = '<computer name>' / 'System Type, Actor' = 'ABCD') Measurement=1 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html?siteId=exp.com.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show?alert=<Alert Id> EventSemantic=System Admin, Audit Policy, Alter NetworkHostnameInitiator=<hostname> SystemIdActor=<computer name> SystemTypeActor=<computer name>

Table 920. SAP Enterprise Threat Detection V2.0 SP5 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
Audit Slot deactivated in critical system Roles	Audit Configuration Changes	LEEF:1.0|SAP|ETD|2.0 SP5|Audit Slot deactivated in critical system Roles (http://demo)| devTime=2023-05-30T12:12:06.402Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Audit Configuration Changes PatternId=40000000000000000012345678912345 67 PatternType=FLAB AlertId=2381889 sev=10 MinResultTimestamp=2023-05-30T12:07:05.0 00Z MaxResultTimestamp=2023-05-30T12:07:05.0 00Z Text=Measurement 1 reached threshold 1 for ('Network, Hostname, Initiator' = '<hostname>' / 'Network, IP Address, Initiator' = 'null' / 'Parameter Name' = 'Audit Slot' / 'Parameter Value, String' = '4' / 'System Group, Role, Actor' = 'Production' / 'System ID, Actor' = '<computer name>') Measurement=1 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html? siteId=exp.com.ui.mobile.launchpad| ETDLaunchpad#AlertDetails-show? alert=<Alert Id> NetworkHostnameInitiator=<hostname> NetworkIPAddressInitiator=null ParameterName=Audit Slot ParameterValueString=4 SystemGroupRoleActor=Production SystemIdActor=<computer name>
Low Log Amount per system	Log Failure	LEEF:1.0|SAP|ETD|2.0 SP5|Low Log Amount per system (http://demo)| devTime=2023-05-30T12:20:15.280Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Log Failure PatternId=92408893B4EED249A21219D645F55C 77 PatternType=FLAB AlertId=2381894 sev=4 MinResultTimestamp=2023-05-30T12:11:26.5 46Z MaxResultTimestamp=2023-05-30T12:15:52.5 30Z Text=Measurement 9 exceeded threshold 50 for ('Event, Log Type' = 'Indicator' / 'System ID, Actor' = '<computer name>') Measurement=9 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html? siteId=exp.com.ui.mobile.launchpad| ETDLaunchpad#AlertDetails-show? alert=<Alert Id> EventLogType=Indicator SystemIdActor=<computer name>

Table 920. SAP Enterprise Threat Detection V2.0 SP5 sample message supported by the SAP Enterprise Threat Detection DSM (continued)

Event name	Low-level category	Sample log message
RFC calls from non-productive systems	Cross Communication	LEEF:1.0|SAP|ETD|2.0 SP5|RFC calls from non-productive to productive systems (http://exm.com/qradar/basis)| devTime=2023-06-01T13:25:12.896Z devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSX cat=Cross Communication PatternId=10000000000000000012345678912345 6 PatternType=FLAB AlertId=2382290 sev=4 MinResultTimestamp=2023-06-01T13:16:08.000Z MaxResultTimestamp=2023-06-01T13:23:08.000Z Text=Measurement 8 exceeded threshold 1 for ('Service, Function Name' = 'SUSR_SUIM_API_NAME' / 'System ID, Actor' = '<computer name>' / 'User Pseudonym, Actor' = '<username>') Measurement=8 UiLink=null/sap/hana/uis/clients/ushell-app/shells/xxxx/xxxxLaunchpad.html?siteId=exp.com.ui.mobile.launchpad|ETDLaunchpad#AlertDetails-show?alert=<Alert Id> ServiceFunctionName=SUSR_SUIM_API_NAME SystemIdActor=<computer name> UserPseudonymActing=<username> usrName=<username>

Chapter 140. Seculert

The IBM QRadar DSM for Seculert collects events from the Seculert cloud service.

The following table describes the specifications for the Seculert DSM:

Table 921. Seculert DSM specifications

Specification	Value
Manufacturer	Seculert
DSM name	Seculert
RPM file name	`DSM-SeculertSeculert-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	v1
Protocol	Seculert Protection REST API Protocol
Recorded event types	All malware communication events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	Seculert website (http://www.seculert.com)

To integrate Seculert with QRadar, complete the following steps:

1. Download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol-Common
   - DSM-DSMCommon
   - Seculert DSM RPM
   - SeculertProtectionRESTAPI PROTOCOL RPM
2. Add a Seculert log source on the QRadar Console. The following table describes the parameters that require specific values for Seculert event collection:

   Table 922. Seculert log source parameters

Parameter	Value
Log Source type	Seculert
Protocol Configuration	Seculert Protection REST API
API Key	32 character UUID For more information about obtaining an API key, see “Seculert Protection REST API protocol configuration options” on page 208.

   For more information about this protocol, see “Seculert Protection REST API protocol configuration options” on page 208.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Chapter 141. Sentrigo Hedgehog

You can integrate a Sentrigo Hedgehog device with IBM QRadar.

About this task

A Sentrigo Hedgehog device accepts LEEF events by using syslog. Before you configure QRadar to integrate with a Sentrigo Hedgehog device, take the following steps:

Procedure

1. Log in to the Sentrigo Hedgehog command-line interface (CLI).
2. Open the following file for editing:

   <*Installation directory*>/conf/sentrigo-custom.properties

   Where <*Installation directory*> is the directory that contains your Sentrigo Hedgehog installation.
3. Add the following *log.format* entries to the custom properties file:

   Note: Depending on your Sentrigo Hedgehog configuration or installation, you might need to replace or overwrite the existing *log.format* entry.

```
sentrigo.comm.ListenAddress=1996
log.format.body.custom=usrName=$osUser:20$|duser=$execUser:20$|
severity=$severity$|identHostName=$sourceHost$|src=$sourceIP$|
dst=$agent.ip$|devTime=$logonTime$|
devTimeFormat=EEE MMM dd HH:mm:ss z yyyy|
cmdType=$cmdType$|externalId=$id$|
execTime=$executionTime.time$|
dstServiceName=$database.name:20$|
srcHost=$sourceHost:30$|execProgram=$execProgram:20$|
cmdType=$cmdType:15$|oper=$operation:225$|
accessedObj=$accessedObjects.name:200$
```

```
log.format.header.custom=LEEF:1.0|
Sentrigo|Hedgehog|$serverVersion$|$rules.name:150$|
log.format.header.escaping.custom=\\|
log.format.header.seperator.custom=,
log.format.header.escape.char.custom=\\
log.format.body.escaping.custom=\=
log.format.body.escape.char.custom=\\
log.format.body.seperator.custom=|
log.format.empty.value.custom=NULL
log.format.length.value.custom=10000
log.format.convert.newline.custom=true
```

4. Save the custom properties file.
5. Stop and restart your Sentrigo Hedgehog service to implement the `log.format` changes.

   You can now configure the log source in QRadar.
6. To configure QRadar to receive events from a Sentrigo Hedgehog device: From the **Log Source Type** list, select the **Sentrigo Hedgehog** option.

   For more information about Sentrigo Hedgehog see your vendor documentation.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Chapter 142. Snowflake

The IBM QRadar DSM for Snowflake collects events from a Snowflake database.

To integrate Snowflake with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from IBM support. Download and install the most recent version of the following RPM on your QRadar Console.
   a. Snowflake DSM RPM
   b. JDBC Protocol RPM
2. Configure your Snowflake device to send events to QRadar. For more information, see JDBC protocol configuration options.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Snowflake DSM specifications

The IBM QRadar DSM for Snowflake supports events (Login history, Query history, and Snowalerts) that are collected from the Snowflake database.

The following table lists the specifications for the Snowflake DSM.

Table 923. Snowflake DSM specifications

Specification	**Value**
Manufacturer	Snowflake
DSM name	Snowflake
RPM file name	DSM-*Snowflake-QRadar_version-Build_number*.noarch.rpm
Supported protocols	JDBC Syslog
Event format	Name value pair (NVP)
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	Snowflake Database - Account Usage

Snowflake sample event message

The following sample events are from Snowflake database when you use the JDBC protocol.

Login History View event

In the following sample event message, the event indicates the results of a query that returns the login attempt details of the Snowflake users.

```
EVENT_ID: "1111111111111111xx" EVENT_TIMESTAMP: "2024-03-26 16:24:57.936"
EVENT_TYPE: "LOGIN" USER_NAME: "TEST" CLIENT_IP: "10.0.x.x"
```

```
REPORTED_CLIENT_TYPE: "JDBC_DRIVER" REPORTED_CLIENT_VERSION: "3.14.x"
FIRST_AUTHENTICATION_FACTOR: "PASSWORD" SECOND_AUTHENTICATION_FACTOR: "null"
IS_SUCCESS: "YES" ERROR_CODE: "null" ERROR_MESSAGE: "null" RELATED_EVENT_ID: "0" CONNECTION:
"null
```

Table 924. Highlighted values in the Snowflake: Login History View sample event

QRadar field name	Highlighted payload field name
Event ID	**EVENT_TYPE + IS_SUCCESS** [SUCCESS / (FAIL + ERROR_CODE)] **Important:** If the value of **IS_SUCCESS** is 'Yes', then the system appends **SUCCESS**, else **FAIL** with an **ERROR_CODE**.
Username	**USER_NAME**
Source IP	**CLIENT_IP**
Device Time	**EVENT_TIMESTAMP**

Query History View event

The following sample event message shows the results of a Snowflake query by different dimensions (time range, session, user, warehouse, and so on).

```
QUERY_ID: "11111111-1111-1111-1111-111111111111" QUERY_TEXT: "select max(SESSION_ID) from
QUERY_HISTORY"
DATABASE_ID: "1" DATABASE_NAME:"SNOWFLAKE" SCHEMA_ID: "3" SCHEMA_NAME: "ACCOUNT_USAGE"
QUERY_TYPE: "SELECT" SESSION_ID: "1111111111111" USER_NAME: "TEST" ROLE_NAME:"ACCOUNTADMIN"
WAREHOUSE_ID: "1" WAREHOUSE_NAME: "COMPUTE_WH" WAREHOUSE_SIZE: "X-Small" WAREHOUSE_TYPE:
"STANDARD"
CLUSTER_NUMBER:"1" QUERY_TAG: "" EXECUTION_STATUS: "SUCCESS" ERROR_CODE: "null" ERROR_MESSAGE:
"null"
START_TIME: "2024-04-03 11:41:36.358" END_TIME: "2024-04-03 11:41:36.95" TOTAL_ELAPSED_TIME:
"592"
BYTES_SCANNED: "35994112" PERCENTAGE_SCANNED_FROM_CACHE: "1.0"
BYTES_WRITTEN: "0" BYTES_WRITTEN_TO_RESULT: "306" BYTES_READ_FROM_RESULT: "0" ROWS_PRODUCED:
"1"
ROWS_INSERTED: "0" ROWS_UPDATED: "0" ROWS_DELETED: "0" ROWS_UNLOADED: "0" BYTES_DELETED: "0"
PARTITIONS_SCANNED: "33" PARTITIONS_TOTAL: "196285" BYTES_SPILLED_TO_LOCAL_STORAGE: "0"
BYTES_SPILLED_TO_REMOTE_STORAGE: "0" BYTES_SENT_OVER_THE_NETWORK: "0" COMPILATION_TIME: "437"
EXECUTION_TIME: "155" QUEUED_PROVISIONING_TIME: "0" QUEUED_REPAIR_TIME: "0"
QUEUED_OVERLOAD_TIME: "0"
TRANSACTION_BLOCKED_TIME: "0" OUTBOUND_DATA_TRANSFER_CLOUD: "null"
OUTBOUND_DATA_TRANSFER_REGION: "null"
OUTBOUND_DATA_TRANSFER_BYTES: "0" INBOUND_DATA_TRANSFER_CLOUD: "null"
INBOUND_DATA_TRANSFER_REGION: "null"
INBOUND_DATA_TRANSFER_BYTES: "0" LIST_EXTERNAL_FILES_TIME: "0" CREDITS_USED_CLOUD_SERVICES:
"6.7E-5"
RELEASE_VERSION: "8.13.1" EXTERNAL_FUNCTION_TOTAL_INVOCATIONS: "0"
EXTERNAL_FUNCTION_TOTAL_SENT_ROWS: "0"
EXTERNAL_FUNCTION_TOTAL_RECEIVED_ROWS: "0" EXTERNAL_FUNCTION_TOTAL_SENT_BYTES: "0"
EXTERNAL_FUNCTION_TOTAL_RECEIVED_BYTES: "0" QUERY_LOAD_PERCENT: "100"
IS_CLIENT_GENERATED_STATEMENT: "false"
QUERY_ACCELERATION_BYTES_SCANNED: "0" QUERY_ACCELERATION_PARTITIONS_SCANNED: "0"
QUERY_ACCELERATION_UPPER_LIMIT_SCALE_FACTOR: "0" TRANSACTION_ID: "0" CHILD_QUERIES_WAIT_TIME:
"0"
ROLE_TYPE: "ROLE" QUERY_HASH: "11111111111111111111111111111111" QUERY_HASH_VERSION:"2"
QUERY_PARAMETERIZED_HASH: "11111111111111111111111111111111" QUERY_PARAMETERIZED_HASH_VERSION:
"1"
SECONDARY_ROLE_STATS:"{"roleNames":[],"roleCount":0,"roleIds":[]}" ROWS_WRITTEN_TO_RESULT: "1"
QUERY_RETRY_TIME: "null" QUERY_RETRY_CAUSE: "null" FAULT_HANDLING_TIME:"null"
```

Table 925. Highlighted values in the Snowflake: Query History View sample event

QRadar field name	Highlighted payload field name
Event ID	**QUERY_TYPE + EXECUTION_STATUS** **Important:** If the status is **FAIL**, then append the **ERROR_CODE**.

Table 925. Highlighted values in the Snowflake: Query History View sample event (continued)	
QRadar field name	**Highlighted payload field name**
Username	**USER_NAME**
Device Time	**START_TIME**

Snowalert event

The following sample event message shows the snow alert for a particular view. **Snowalert** is a security analytics framework that uses the Snowflake Cloud Data Platform to identify security incidents across diverse data sources and time ranges.

```
TABLE_CATALOG: "SNOWALERT" TABLE_SCHEMA: "DATA" TABLE_NAME: "DATA_CONNECTOR_RUN_ERRORS"
TABLE_OWNER: "ACCOUNTADMIN"VIEW_DEFINITION: "CREATE OR REPLACE VIEW
data.data_connector_run_errors COPY GRANTS AS SELECT day ,
COUNT(DISTINCT SUBSTR(exc, 0, 50)) ASnum_distinct_exceptions ,
SUM(IFF(exc IS NOT NULL, 1, 0)) AS num_errors FROM ( SELECT slice_start::DATE AS day FROM
TABLE(data.time_slices_before_t(30,60*60*24)) ) d
RIGHT OUTER JOIN ( SELECT v:START_TIME::DATE AS day , v:ERROR.EXCEPTION_ONLY AS exc FROM
results.ingestion_metadata ) e
USING(day) GROUP BY day ORDER BY day DESC ;" CHECK_OPTION: "NONE" IS_UPDATABLE: "NO"
INSERTABLE_INTO: "NO"
IS_SECURE: "NO" CREATED : "2024-02-2914:56:14.88" LAST_ALTERED: "2024-02-29 14:56:15.005"
LAST_DDL: "2024-02-29 14:56:14.88" LAST_DDL_BY: "TEST" COMMENT: "Errors recorded during DCruns"
```

Table 926. Highlighted values in the Snowflake: Snowalert sample event	
QRadar field name	**Highlighted payload field name**
Event ID	**TABLE_CATALOG + TABLE_NAME**
Username	**LAST_DDL_BY**

Chapter 143. SolarWinds Orion

The IBM QRadar DSM for SolarWinds Orion collects events from a SolarWinds Orion appliance.

The following table describes the specifications for the SolarWinds Orion DSM:

Table 927. SolarWinds Orion DSM specifications

Specification	**Value**
Manufacturer	SolarWinds
DSM name	SolarWinds Orion
RPM file name	`DSM-SolarWindsOrion-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	2013.2.0
Protocol	SNMPv2 SNMPv3
Event format	name-value pair (NVP)
Recorded event types	All events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No
More information	For more information, see the SolarWinds Orion link to public site website (https://www.solarwinds.com/orion).

To integrate SolarWinds Orion with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the SolarWinds Orion DSM RPM on your QRadar Console:
2. Configure your SolarWinds Orion device to send events to QRadar.
3. Add a SolarWinds Orion log source on the QRadar Console.
4. Verify that QRadar is configured correctly.

   The following table shows a normalized sample event message from SolarWinds Orion:

Table 928. SolarWinds Orion sample message		
Event name	**Low level category**	**Sample log message**
Domain controller UnManaged	Warning	1.3.6.1.2.1.1.3.0=0:00:00.00 1.3.6.1.6.3.1.1.4.1.0=1.3.6.1.4.1.11307.10 1.3.6.1.6.3.1.1.4.3.0=1.3.6.1.4.1.11307 1.3.6.1.4.1.11307.10.2=hostname 1.3.6.1.4.1.11307.10.3=127.0.0.1 1.3.6.1.4.1.11307.10.4=2466 1.3.6.1.4.1.11307.10.5=hostname 1.3.6.1.4.1.11307.10.6=Node 1.3.6.1.4.1.11307.10.7=2466 1.3.6.1.4.1.11307.10.1=InfoSec - EMAIL ONLY - Domain Controller UnManaged - hostname - Status = Unknown 1.3.6.1.4.1.11307.10.8=InfoSec -EMAIL ONLY - Domain Controller UnManaged hostname is Unknown.

Related concepts

"SNMP log source parameters for SolarWinds Orion" on page 1456

Related tasks

"Adding a DSM" on page 4

Configuring SolarWinds Orion to communicate with QRadar

To collect events in IBM QRadar from SolarWinds Orion, you must configure your SolarWinds Orion Alert Manager device to create SNMP traps.

Procedure

1. Log in to your SolarWinds Orion Alert Manager device.
2. Select **Start** > **All Programs** > **SolarWinds Orion** > **Alerting, Reporting, and Mapping** > **Advanced Alert Manager**.
3. In the **Alert Manager Quick Start** window, click **Configure Alerts**.
4. In the **Manage Alerts** window, select an existing alert and then click **Edit**.
5. Click the **Triggered Actions** tab.
6. Click **Add New Action**.
7. In the **Select an Action** window, select **Send an SNMP Trap** and then click **OK**.
8. To configure **SNMP Trap Destinations**, type the IP address of the QRadar Console or QRadar Event Collector.
9. To configure the **Trap Template**, select **ForwardSyslog**.
10. To configure the **SNMP Version**, select the SNMP version that you want to use to forward the event:

    SNMPv2c - Type the **SNMP Community String** to use for SNMPv2c authentication. The default **SNMP Community String** value is public.

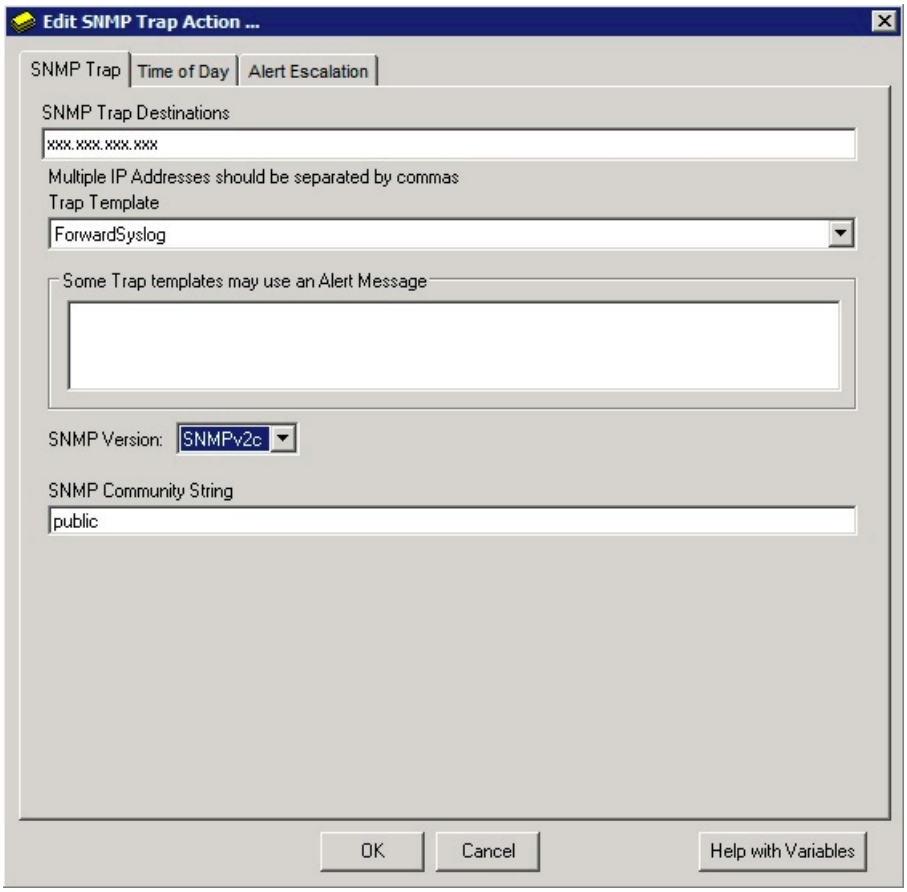


Figure 46. Edit SNMP Trap Action configuration for SNMPv2c

Note: To verify that your SNMP trap is configured properly, select an alert that you edited and click **Test**. This action triggers and forwards the events to QRadar.

SNMPv3 - Type the **Username** and then select the **Authentication Method** to use for SNMPv3.

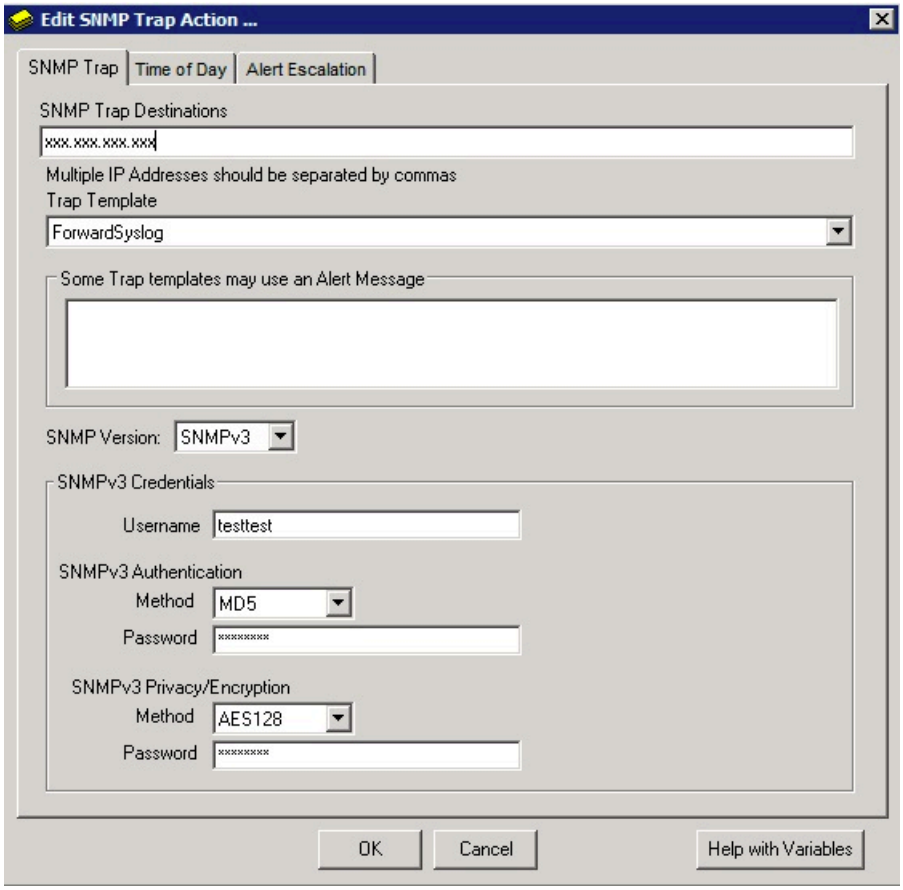


Figure 47. Edit SNMP Trap Action configuration for SNMPv3

Note: To verify that your SNMP trap is configured properly, select an alert that you edited and click **Test**. This action triggers and forwards the events to QRadar.

11. Click **OK**.

What to do next

Repeat these steps to configure the SolarWinds Orion Alert Manager with all of the SNMP trap alerts that you want to monitor in QRadar.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

SNMP log source parameters for SolarWinds Orion

If QRadar does not automatically detect the log source, add a SolarWinds Orion log source on the QRadar Console by using the SNMP protocol.

When using the SNMP protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMP events from SolarWinds Orion:

Table 929. SNMP log source parameters for the SolarWinds Orion DSM

Parameter	Value
Log Source type	SolarWinds Orion
Protocol Configuration	SNMPv2 or SNMPv3

Table 929. SNMP log source parameters for the SolarWinds Orion DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or the hose name of your SolarWinds Orion appliance to use as the identifier.

For a complete list of SNMPv2 protocol parameters and their values, see SNMPv2 protocol configuration options.

For a complete list of SNMPv3 protocol parameters and their values, see SNMPv3 protocol configuration options.

Related tasks

"Adding a log source" on page 5

Installing the Java Cryptography Extension on QRadar

The Java Cryptography Extension (JCE) is a Java framework that is required for IBM QRadar to decrypt advanced cryptography algorithms for AES192 or AES256. The following information describes how to install Oracle JCE on your QRadar appliance.

Procedure

1. Optional: If you are using QRadar 7.2x, 7.3.0, or 7.31, complete the following steps:
   a) Download the latest version of the Java Cryptography Extension from the IBM website (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk).

      The Java Cryptography Extension version must match the version of the Java that is installed on QRadar.

   b) Extract the JCE file.

      The following Java archive (JAR) files are included in the JCE download:

      - `local_policy.jar`
      - `US_export_policy.jar`

   c) Log in to your QRadar Console or QRadar Event Collector as a root user.

   d) Copy the JCE JAR files to the following directory on your QRadar Console or Event Collector:

      `/store/configservices/staging/globalconfig/java_security`

      Note: The JCE JAR files are only copied to the system that receives the AES192 or AE256 encrypted files.

   e) Restart the QRadar services by typing one of the following commands:

      - If you are using QRadar 7.2.x, type `service ecs-ec restart`.
      - If you are using QRadar 7.3.0, type `systemctl restart ecs-ec.service`.
      - If you are using QRadar 7.3.1, type `systemctl restart ecs-ec-ingress.service`.

2. Optional: If you are using QRadar 7.4.3 Fix Pack 4 or earlier, complete the Installing unrestricted SDK JCE policy files procedure (https://www.ibm.com/docs/en/qsip/7.4?topic=authentication-installing-unrestricted-sdk-jce-policy-files).

   Important: If you are using QRadar 7.4.3 Fix Pack 5 or later, do not install these files.

Solar Winds Orion sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Solar Winds Orion sample message when you use the Syslog protocol

The following sample event message shows that a network device is up.

```
1.3.6.1.2.1.1.3.0=0:00:00.00    1.3.6.1.6.3.1.1.4.1.0=1.3.6.1.4.1.11307.10
1.3.6.1.6.3.1.1.4.3.0=1.3.6.1.4.1.11307    1.3.6.1.4.1.11307.10.2=host.domain.test
1.3.6.1.4.1.11307.10.3=10.64.1.10    1.3.6.1.4.1.11307.10.4=1953
1.3.6.1.4.1.11307.10.5=host.domain.test    1.3.6.1.4.1.11307.10.6=Node
1.3.6.1.4.1.11307.10.7=1953    1.3.6.1.4.1.11307.10.1=    1.3.6.1.4.1.11307.10.8=Network Device
is down host.domain.test is Up.
```

Table 930. Hghlighted values in the Solar Winds Orion sample event

QRadar field name	Highlighted values in the event payload
Event ID	**Network Device is down host.domain.test is Up**
Source IP	**10.64.1.10**

Chapter 144. SonicWALL

The SonicWALL SonicOS DSM accepts events by using syslog.

IBM QRadar records all relevant syslog events that are forwarded from SonicWALL appliances by using SonicOS firmware. Before you can integrate with a SonicWALL SonicOS device, you must configure syslog forwarding on your SonicWALL SonicOS appliance.

Configuring SonicWALL to forward syslog events

SonicWALL captures all SonicOS event activity. The events can be forwarded to IBM QRadar by using SonicWALL's default event format.

Procedure

1. Log in to your SonicWALL web interface.
2. From the navigation menu, select **Log** > **Syslog**.
3. From the **Syslog Servers** pane, click **Add**.
4. In the **Name or IP Address** field, type the IP address of your QRadar Console or Event Collector.
5. In the **Port** field, type 514.

   SonicWALL syslog forwarders send events to QRadar by using UDP port 514.
6. Click **OK**.
7. From the **Syslog Format** list, select **Default**.
8. Click **Apply**.

   Syslog events are forwarded to QRadar. SonicWALL events that are forwarded to QRadar are automatically discovered and log sources are created automatically. For more information on configuring your SonicWALL appliance or for information on specific events, see your vendor documentation.

Syslog log source parameters for SonicWALL

If QRadar does not automatically detect the log source, add a SonicWALL log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from SonicWALL:

Table 931. Syslog log source parameters for the SonicWALL DSM

Parameter	Value
Log Source type	SonicWALL SonicOS
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from SonicWALL appliances. Each log source that you create for your SonicWALL SonicOS appliance ideally includes a unique identifier, such as an IP address or host name.

Related tasks

"Adding a log source" on page 5

SonicWALL sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

SonicWALL sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that a probable port scan is detected.

```
<1>    id=firewall sn=01234567ABCD time="2018-11-07 11:16:02" fw=10.0.0.2 pri=1 c=32
m=83 msg="Probable port scan detected" n=2 src=10.0.0.3:443:X1 dst=172.16.194.2:47379:X1
srcMac=00:00:5E:00:53:ff dstMac=00:00:5E:00:53:00 proto=tcp/1 note="TCP scanned port list, 14551,
61968, 53577, 27976, 29050, 25330, 21761, 23903, 7412, 47379" fw_action="NA"
```


```
<1>    id=firewall sn=01234567ABCD time="2018-11-07 11:16:02" fw=10.0.0.2 pri=1 c=32
m=83 msg="Probable port scan detected" n=2 src=10.0.0.3:443:X1 dst=172.16.194.2:47379:X1
srcMac=00:00:5E:00:53:ff dstMac=00:00:5E:00:53:00 proto=tcp/1 note="TCP scanned port list,
14551, 61968, 53577, 27976, 29050, 25330, 21761, 23903, 7412, 47379" fw_action="NA"
```


Table 932. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	83
Source IP	10.0.0.3
Source Port	443
Source Mac	00:00:5E:00:53:ff
Destination IP	172.16.194.2
Destination Port	47379
Destination Mac	00:00:5E:00:53:00
Device Time	2018-11-07 11:16:02

Sample 2: The following sample event message shows that NTP updated successfully.

```
<133>  id=firewall sn=12345678123 time="2018-11-13 00:26:12" fw=10.0.0.253 pri=5 c=128 m=1231
msg="Time update from NTP server was successful" sess="None" n=1104 src=10.0.2.3:123:X0
dst=10.0.5.6:123:X1 proto=0/ntp note="Received reply from NTP server 10.2.2.5. Update system time
from 11/13/2018 00:26:12.624 to 11/13/2018 00:26:12.736"
```


```
<133>  id=firewall sn=12345678123 time="2018-11-13 00:26:12" fw=10.0.0.253 pri=5 c=128 m=1231
msg="Time update from NTP server was successful" sess="None" n=1104 src=10.0.2.3:123:X0
dst=10.0.5.6:123:X1 proto=0/ntp note="Received reply from NTP server 10.2.2.5. Update system
time from 11/13/2018 00:26:12.624 to 11/13/2018 00:26:12.736"
```


QRadar field name	Highlighted values in the event payload
Event ID	1231
Source IP	10.0.2.3
Source Port	123
Destination IP	10.0.5.6
Destination Port	123
Device Time	2018-11-13 00:26:12

Chapter 145. Sophos

IBM QRadar supports a number of Sophos DSMs.

Sophos Enterprise Console

The IBM QRadar DSM for Sophos Enterprise Console provides two options for gathering events by using Java database connectivity (JDBC).

QRadar records all relevant anti-virus events.

To use the Sophos Enterprise Console JDBC protocol, the Sophos Reporting Interface must be installed with your Sophos Enterprise Console. If you do not have the Sophos Reporting Interface installed, configure QRadar by using the JDBC protocol. For information about installing the Sophos Reporting Interface, go to the Sophos Enterprise Console documentation (https://www.sophos.com/en-us/support/documentation/enterprise-console.aspx).

To integrate Sophos Enterprise Console with QRadar, complete the following steps:

1. Configure the database view for Sophos Enterprise Console .
2. **Optional:** If the Sophos Reporting Interface is installed on your Sophos Enterprise console, use the Sophos Enterprise Console JDBC log source to collect events. For more information, see "Sophos Enterprise Console JDBC log source parameters for Sophos Enterprise Console" on page 1462.
3. **Optional:** If the Sophos Reporting Interface is not installed on your Sophos Enterprise Console, use the standard JDBC protocol to collect events. For more information, see "JDBC log source parameters for Sophos Enterprise Console" on page 1463.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Sophos Enterprise Console DSM specifications

When you configure the Sophos Enterprise DSM, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported version of Sophos Enterprise Console is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Sophos Enterprise Console DSM.

Table 933. Sophos Enterprise Console DSM specifications

Specification	**Value**
Manufacturer	Sophos
DSM name	Sophos Enterprise Console
RPM file name	DSM-*SophosEntepriseConsole-QRadar_version-build_number*.noarch.rpm
Supported version	4.5.1 and 5.1
Protocols	Sophos Enterprise Console JDBC JDBC
Event format	JDBC
Recorded event types	all relevant anti-virus events
Automatically discovered?	No

Table 933. Sophos Enterprise Console DSM specifications (continued)	
Specification	**Value**
Includes identity?	No
Includes custom properties?	No
More information	Sophos Enterprise Console documentation (https://www.sophos.com/en-us/support/documentation/enterprise-console.aspx)

Configuring the database view for Sophos Enterprise Console

To collect events in IBM QRadar, you need to configure a database view on your Sophos Enterprise Console device.

Procedure

1. Log in to your Sophos Enterprise Console device command-line interface (CLI).
2. Type the following command to create a custom view in your Sophos database to support QRadar:

```
CREATE VIEW threats_view AS SELECT t.ThreatInstanceID, t.ThreatType, t.FirstDetectedAt,
c.Name, c.LastLoggedOnUser, c.IPAddress, c.DomainName, c.OperatingSystem, c.ServicePack,
t.ThreatSubType, t.Priority, t.ThreatLocalID, t.ThreatLocalIDSource, t.ThreatName,
t.FullFilePathCheckSum, t.FullFilePath, t.FileNameOffset, t.FileVersion, t.CheckSum,
t.ActionSubmittedAt, t.DealtWithAt, t.CleanUpable, t.IsFragment, t.IsRebootRequired,
t.Outstanding, t.Status, InsertedAt FROM <Database Name>.dbo.ThreatInstancesAll t, <Database
Name>.dbo.Computers c WHERE t.ComputerID = c.ID;
```

Where <*DatabaseName*> is the name of the Sophos database.

Important: The database name must not contain any spaces.

What to do next

After you create your custom view, you must configure QRadar to receive event information that uses the JDBC protocol or the Sophos Enterprise Console JDBC protocol.

Related concepts

"JDBC log source parameters for Sophos Enterprise Console" on page 1463

"Sophos Enterprise Console JDBC log source parameters for Sophos Enterprise Console" on page 1462

Sophos Enterprise Console JDBC log source parameters for Sophos Enterprise Console

If QRadar does not automatically detect the log source, add a Sophos Enterprise Console log source on the QRadar Console by using the Sophos Enterprise Console JDBC protocol.

When using the Sophos Enterprise Console JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Sophos Enterprise Console JDBC events from Sophos:

Table 934. Sophos Enterprise Console JDBC log source parameters for the Sophos Enterprise Console DSM	
Parameter	**Value**
Log Source type	Sophos Enterprise Console
Protocol Configuration	Sophos Enterprise Console JDBC

Table 934. Sophos Enterprise Console JDBC log source parameters for the Sophos Enterprise Console DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: *<Sophos Database>@<Sophos Database Server IP or Host Name>* Where: • *<Sophos Database>* is the database name, as entered in the **Database Name** parameter. • *<Sophos Database Server IP or Host Name>* is the host name or IP address for this log source, as entered in the **IP or Hostname** parameter. When you define a name for your log source identifier, you must use the values of the Sophos Database and Database Server IP address or host name from the Management Enterprise Console.

For a complete list of Sophos Enterprise Console JDBC protocol parameters and their values, see "Sophos Enterprise Console JDBC protocol configuration options" on page 218.

Related tasks

"Adding a log source" on page 5

JDBC log source parameters for Sophos Enterprise Console

If the Sophos Enterprise Console does not have the Sophos Reporting Interface installed, use the standard JDBC protocol to collect events in QRadar.

If QRadar does not automatically detect the log source, add a Sophos Enterprise Console log source on the QRadar Console.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Sophos Enterprise Console:

Table 935. JDBC log source parameters for the Sophos Enterprise Console DSM	
Parameter	**Value**
Log Source type	**Sophos Enterprise Console**
Protocol Configuration	**JDBC**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Sophos Enterprise Console devices.

For a complete list of JDBC protocol parameters and their values, see JDBC protocol configuration options.

Related tasks

Adding a log source

Sophos PureMessage

The Sophos PureMessage DSM for IBM QRadar accepts events by using Java Database Connectivity (JDBC).

QRadar records all relevant quarantined email events. This document provides information about configuring QRadar to access the Sophos PureMessage database by using the JDBC protocol.

QRadar supports the following Sophos PureMessage versions:

- Sophos PureMessage for Microsoft Exchange - Stores events in a Microsoft SQL Server database that is specified as `savexquar`.
- Sophos PureMessage for Linux - Stores events in a PostgreSQL database that is specified as `pmx_quarantine`.

Here's information on integrating QRadar with Sophos:

- “Integrating QRadar with Sophos PureMessage for Microsoft Exchange” on page 1464
- “Integrating QRadar with Sophos PureMessage for Linux” on page 1465

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Integrating QRadar with Sophos PureMessage for Microsoft Exchange

You can integrate QRadar with Sophos PureMessage for Microsoft Exchange.

Procedure

1. Log in to the Microsoft SQL Server command-line interface (CLI):

   ```
   osql -E -S localhost\sophos
   ```

2. Type which database you want to integrate with QRadar:

   ```
   use savexquar; go
   ```

3. Type the following command to create a SIEM view in your Sophos database to support QRadar:

   ```
   create view siem_view as select
   'Windows PureMessage' as application, id, reason,
   timecreated, emailonly as sender, filesize, subject,
   messageid, filename from dbo.quaritems,
   dbo.quaraddresses where ItemID = ID and Field = 76;
   ```

What to do next

After you create your SIEM view, you must configure QRadar to receive event information by using the JDBC protocol. To configure the Sophos PureMessage DSM with QRadar, see “JDBC log source parameters for Sophos PureMessage” on page 1464.

JDBC log source parameters for Sophos PureMessage

If QRadar does not automatically detect the log source, add a Sophos PureMessage log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Sophos:

Table 936. JDBC log source parameters for the Sophos PureMessage DSM	
Parameter	**Value**
Log Source type	Sophos PureMessage
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	MSDE
Database Name	Type `savexquar`.
Table Name	Type `siem_view` as the name of the table or view that includes the event records.
Compare Field	Type `ID`.

Note: You must refer to the database configuration settings on your Sophos PureMessage device to define the parameters that are required to configure the Sophos PureMessage DSM in QRadar.

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

"Adding a log source" on page 5

Integrating QRadar with Sophos PureMessage for Linux

You can integrate IBM QRadar with Sophos PureMessage for Linux.

Procedure

1. Navigate to your Sophos PureMessage PostgreSQL database directory:

   ```
   cd /opt/pmx/postgres-8.3.3/bin
   ```

2. Access the `pmx_quarantine` database SQL prompt:

   ```
   ./psql -d pmx_quarantine
   ```

3. Type the following command to create a SIEM view in your Sophos database to support QRadar:

   ```
   create view siem_view as select 'Linux PureMessage' as application, id, b.name, m_date,
   h_from_local, h_from_domain, m_global_id, m_message_size, outbound, h_to, c_subject_utf8
   from message a, m_reason b where a.reason_id = b.reason_id;
   ```

What to do next

After you create your database view, you must configure QRadar to receive event information by using the JDBC protocol.

JDBC log source parameters for Sophos PureMessage for Microsoft Exchange

If QRadar does not automatically detect the log source, add a Sophos PureMessage log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Sophos:

Table 937. JDBC log source parameters for the Sophos PureMessage for Microsoft Exchange DSM

Parameter	Value
Log Source type	Sophos PureMessage
Protocol Configuration	JDBC
Log Source Identifier	Type the identifier for the log source. Type the log source identifier in the following format: *<Sophos PureMessage Database>@<Sophos PureMessage Database Server IP or Host Name>* Where: • *<Sophos PureMessage Database>* is the database name, as entered in the Database Name parameter. • *<Sophos PureMessage Database Server IP or Host Name>* is the hostname or IP address for this log source, as entered in the IP or Hostname parameter. When defining a name for your log source identifier, you must use the values of the Database and Database Server IP address or host name of the Sophos PureMessage device.
Database Type	Postgres
Database Name	Type `pmx_quarantine`.
Table Name	Type `siem_view` as the name of the table or view that includes the event records.
Compare Field	Type `ID`.

Note: You must refer to the **Configure Database Settings** on your Sophos PureMessage to define the parameters required to configure the Sophos PureMessage DSM in QRadar.

For a complete list of JDBC protocol parameters and their values, see "JDBC protocol configuration options" on page 147.

Related tasks

"Adding a log source" on page 5

Sophos Astaro Security Gateway

The Sophos Astaro Security Gateway DSM for IBM QRadar accepts events by using syslog, enabling QRadar to record all relevant events.

About this task

To configure syslog for Sophos Astaro Security Gateway:

Procedure

1. Log in to the Sophos Astaro Security Gateway console.
2. From the navigation menu, select **Logging** > **Settings**.
3. Click the **Remote Syslog Server** tab.

   The **Remote Syslog Status** window is displayed.
4. From **Syslog Servers** panel, click the **+** icon.

   The **Add Syslog Server** window is displayed.
5. Configure the following parameters:
   a) **Name** - Type a name for the syslog server.
   b) **Server** - Click the folder icon to add a pre-defined host, or click **+** and type in new network definition
   c) **Port** - Click the folder icon to add a pre-defined port, or click **+** and type in a new service definition.
   By default, QRadar communicates by using the syslog protocol on UDP/TCP port 514.
   d) Click Save.
6. From the **Remote syslog log selection** field, you must select check boxes for the following logs:
   a) **POP3 Proxy** - Select this check box.
   b) **Packet Filter** - Select this check box.
   c) **Packet Filter** - Select this check box.
   d) **Intrusion Prevention System** - Select this check box
   e) **Content Filter(HTTPS)** - Select this check box.
   f) **High availability** - Select this check box
   g) **FTP Proxy** - Select this check box.
   h) **SSL VPN** - Select this check box.
   i) **PPTP daemon**- Select this check box.
   j) **IPSEC VPN** - Select this check box.
   k) **HTTP daemon** - Select this check box
   l) **User authentication daemon** - Select this check box.
   m) **SMTP proxy** - Select this check box.
   n) Click **Apply**.
   o) From **Remote syslog status** section, click **Enable**

   You can now configure the log source in QRadar.
7. To configure QRadar to receive events from your Sophos Astaro Security Gateway device: From the **Log Source Type** list, select **Sophos Astaro Security Gateway**.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Sophos Astaro Security Gateway sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Sophos Astaro Security Gateway sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that a web request is blocked.

```
<30>2019:06:20-04:12:39 sophos.astaro.test httpproxy[7917]: id="0002" severity="info"
sys="SecureWeb" sub="http" name="web request blocked" action="block" method="GET"
srcip="10.112.47.87" dstip="10.112.48.88" user="testUser" group="" ad_domain=""
statuscode="502" cached="0" profile="REF_DefaultHTTPProfile (Default Web Filter Profile)"
filteraction="REF_DefaultHTTPCFFAction (Default content filter action)" size="2521"
request="0x93368600" url="http://ipv6.qradar.example.test/connecttest.txt" referer="" error="Host
not found" authtime="0" dnstime="4743" cattime="180" avscantime="0" fullreqtime="5295"
device="0" auth="0" ua="Microsoft NCSI" exceptions="" category="178" reputation="neutral"
categoryname="Internet Services"
```

```
<30>2019:06:20-04:12:39 sophos.astaro.test httpproxy[7917]: id="0002" severity="info"
sys="SecureWeb" sub="http" name="web request blocked" action="block" method="GET"
srcip="10.112.47.87" dstip="10.112.48.88" user="testUser" group="" ad_domain=""
statuscode="502" cached="0" profile="REF_DefaultHTTPProfile (Default Web Filter
Profile)" filteraction="REF_DefaultHTTPCFFAction (Default content filter action)"
size="2521" request="0x93368600" url="http://ipv6.qradar.example.test/connecttest.txt"
referer="" error="Host not found" authtime="0" dnstime="4743" cattime="180" avscantime="0"
fullreqtime="5295" device="0" auth="0" ua="Microsoft NCSI" exceptions="" category="178"
reputation="neutral" categoryname="Internet Services"
```

Table 938. Highlighted values in the Sophos Astaro Security Gateway event

QRadar field name	Highlighted values in the event payload
Event ID	0002
Source IP	10.112.47.87
Destination IP	10.112.48.88
Username	testUser
Device Time	2019:06:20-04:12:39

Sample 2: The following sample event message shows that a packet is dropped by the packet filter.

```
<30>2019:06:20-04:12:39 sophos.astaro.test ulogd[7117]: id="2001" severity="info" sys="SecureNet"
sub="packetfilter" name="Packet dropped" action="drop" fwrule="60001" initf="eth0"
mark="0x307c" app="124" srcmac="00:00:5E:00:53:2A" dstmac="00:00:5E:00:53:66" srcip="10.112.2.39"
dstip="10.112.47.75" proto="17" length="1071" tos="0x00" prec="0x00" ttl="62" srcport="53"
dstport="29366"
```

```
<30>2019:06:20-04:12:39 sophos.astaro.test ulogd[7117]: id="2001" severity="info"
sys="SecureNet" sub="packetfilter" name="Packet dropped" action="drop" fwrule="60001"
initf="eth0" mark="0x307c" app="124" srcmac="00:00:5E:00:53:2A" dstmac="00:00:5E:00:53:66"
srcip="10.112.2.39" dstip="10.112.47.75" proto="17" length="1071" tos="0x00" prec="0x00"
ttl="62" srcport="53" dstport="29366"
```

Table 939. Highlighted values in the Sophos Astaro Security Gateway event

QRadar field name	Highlighted values in the event payload
Event ID	2001
Source IP	10.112.2.39
Source Port	53
Destination IP	10.112.47.75

Table 939. Highlighted values in the Sophos Astaro Security Gateway event (continued)	
QRadar field name	**Highlighted values in the event payload**
Destination Port	**29366**
Device Time	**2019:06:20-04:12:39**

Sample 3: The following sample event message shows that an IPS signature is detected.

```
<188>device="SFW" date=2020-07-31 time=09:45:51 timezone="CEST" device_name="device_name"
device_id=ABCDEFGH1234567 log_id=020803407001 log_type="IDP" log_component="Signatures"
log_subtype="Detect" priority=Warning idp_policy_id=13 fw_rule_id=9 user_name=""
signature_id=15888 signature_msg="SERVER-OTHER SAPLPD 0x31 command buffer overflow attempt"
classification="Attempted Administrator Privilege Gain" rule_priority=2 src_ip=10.0.0.1
src_country_code= dst_ip=10.0.0.2 dst_country_code= protocol="TCP" src_port=50392 dst_port=515
platform="Windows" category="server-other" target="Server"
```


```
<188>device="SFW" date=2020-07-31 time=09:45:51 timezone="CEST" device_name="device_name"
device_id=ABCDEFGH1234567 log_id=020803407001 log_type="IDP" log_component="Signatures"
log_subtype="Detect" priority=Warning idp_policy_id=13 fw_rule_id=9 user_name=""
signature_id=15888 signature_msg="SERVER-OTHER SAPLPD 0x31 command buffer overflow attempt"
classification="Attempted Administrator Privilege Gain" rule_priority=2 src_ip=10.0.0.1
src_country_code= dst_ip=10.0.0.2 dst_country_code= protocol="TCP" src_port=50392 dst_port=515
platform="Windows" category="server-other" target="Server"
```


Table 940. Highlighted values in the Sophos Astaro Security Gateway event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Detect**
Event Category	**IDP**
Source IP	**10.0.0.1**
Source Port	**50392**
Destination IP	**10.0.0.2**
Destination Port	**515**
Device Time	The value in QRadar is **31 July 2020 9:45:51 CEST**. (Extracted from the **date** +**time** +**timezone** fields in the event payload.)

Sophos Web Security Appliance

The Sophos Web Security Appliance (WSA) DSM for IBM QRadar accepts events using syslog.

About this task

QRadar records all relevant events forwarded from the transaction log of the Sophos Web Security Appliance. Before configuring QRadar, you must configure your Sophos WSA appliance to forward syslog events.

To configure your Sophos Web Security Appliance to forward syslog events:

Procedure

1. Log in to your Sophos Web Security Appliance.
2. From the menu, select **Configuration** > **System** > **Alerts & Monitoring**.
3. Select the **Syslog** tab.
4. Select the **Enable syslog transfer of web traffic** check box.
5. In the **Hostname/IP** text box, type the IP address or host name of QRadar.
6. In the **Port** text box, type 514.

7. From the **Protocol** list, select a protocol. The options are:
   - **TCP** - The TCP protocol is supported with QRadar on port 514.
   - **UDP** - The UDP protocol is supported with QRadar on port 514.
   - **TCP - Encrypted** - TCP Encrypted is an unsupported protocol for QRadar.
8. Click **Apply**.
   You can now configure the Sophos Web Security Appliance DSM in QRadar.
9. QRadar automatically detects syslog data from a Sophos Web Security Appliance. To manually configure QRadar to receive events from Sophos Web Security Appliance: From the **Log Source Type** list, select **Sophos Web Security Appliance**.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Chapter 146. Sourcefire Intrusion Sensor

The Sourcefire Intrusion Sensor DSM for IBM QRadar accepts Snort based intrusion and prevention syslog events from Sourcefire devices.

Configuring Sourcefire Intrusion Sensor

To configure your Sourcefire Intrusion Sensor, you must enable policy alerts and configure your appliance to forward the event to QRadar.

Procedure

1. Log in to your Sourcefire user interface.
2. On the navigation menu, select **Intrusion Sensor** > **Detection Policy** > **Edit**.
3. Select an active policy and click **Edit**.
4. Click **Alerting**.
5. In the **State** field, select on to enable the syslog alert for your policy.
6. From the Facility list, select **Alert**.
7. From the Priority list, select **Alert**.
8. In the **Logging Host** field, type the IP address of the QRadar Console or Event Collector.
9. Click **Save**.
10. On the navigation menu, select **Intrusion Sensor** > **Detection Policy** > **Apply**.
11. Click **Apply**.

What to do next

You are now ready to configure the log source in QRadar.

Syslog log source parameters for Sourcefire Intrusion Sensor

If QRadar does not automatically detect the log source, add a Sourcefire Intrusion Sensor log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Sourcefire Intrusion Sensor:

Table 941. Syslog log source parameters for the Sourcefire Intrusion Sensor DSM

Parameter	Value
Log Source type	Snort Open Source IDS
Protocol Configuration	Syslog

Related tasks

"Adding a log source" on page 5

Chapter 147. Splunk

IBM QRadar accepts and parses multiple event types that are forwarded from Splunk appliances.

For Check Point events that are forwarded from Splunk, see Chapter 38, “Check Point,” on page 597.

Collecting Windows events that are forwarded from Splunk

To collect events, you can configure your Windows end points to forward events to your QRadar Console and your Splunk indexer.

Forwarding Windows events from aggregation nodes in your Splunk deployment is not recommended. Use Splunk forwarder to send Windows event data to IBM QRadar. Splunk indexers that forward events from multiple Windows end points to QRadar can obscure the true source of the events with the IP address of the Splunk indexer. To prevent a situation where an incorrect IP address association might occur in the log source, you can update your Windows end-point systems to forward to both the indexer and your QRadar Console.

Splunk events are parsed by using the Microsoft Windows Security Event Log DSM with the TCP multiline syslog protocol. The regular expression that is configured in the protocol defines where a Splunk event starts or ends in the event payload. The event pattern allows QRadar to assemble the raw Windows event payload as a single-line event that is readable by QRadar. The regular expression that is required to collect Windows events is outlined in the log source configuration.

To configure event collection for Splunk syslog events, you must complete the following tasks:

1. On your QRadar appliance, configure a log source to use the Microsoft Windows Security Event Log DSM.

   Note: You must configure 1 log source for Splunk events. QRadar can use the first log source to autodiscover more Windows end points.

2. On your Splunk appliance, configure each Splunk Forwarder on the Windows instance to send Windows event data to your QRadar Console or Event Collector.

   To configure a Splunk Forwarder, you must edit the `props.conf`, `transforms.conf`, and `output.conf` configuration files. For more information on event forwarding, see your Splunk documentation.

3. Ensure that no firewall rules block communication between your Splunk appliance and the QRadar Console or managed host that is responsible for retrieving events.
4. On your QRadar appliance, verify the **Log Activity** tab to ensure that the Splunk events are forwarded to QRadar.

TCP Multiline Syslog log source parameters for Splunk

If QRadar does not automatically detect the log source, add a Splunk log source on the QRadar Console by using the TCP Multiline Syslog protocol.

When using the TCP Multiline Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect TCP Multiline Syslog events from Splunk:

Table 942. TCP Multiline Syslog log source parameters for the Splunk DSM

Parameter	Value
Log Source type	Microsoft Windows Security Event Log
Protocol Configuration	TCP Multiline Syslog

Table 942. TCP Multiline Syslog log source parameters for the Splunk DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Splunk appliance. The log source identifier must be unique value.

For a complete list of TCP Multiline Syslog protocol parameters and their values, see “TCP Multiline Syslog protocol configuration options” on page 222.

Related tasks

“Adding a log source” on page 5

Chapter 148. Squid Web Proxy

The IBM QRadar DSM for Squid Web Proxy records all cache and access log events by using syslog.

To integrate QRadar with Squid Web Proxy, you must configure your Squid Web Proxy to forward your cache and access logs by using syslog.

Configuring syslog forwarding

You can configure Squid to use syslog to forward your access and cache events.

Procedure

1. Use SSH to log in to the Squid device command line interface.
2. Open the following file:

   `/etc/rc3.d/S99local`

   Note: If `/etc/rc3.d/S99local` does not exist, use `/etc/rc.d/rc.local`.
3. Add the following line:

   `tail -f /var/log/squid/access.log | logger -p <facility>.<priority> &`

   - <facility> is any valid syslog facility, which is written in lowercase such as `authpriv`, `daemon`, `local0` to `local7`, or `user`.
   - <*priority*> is any valid priority that is written in lowercase such as `err`, `warning`, `notice`, `info`, `debug`.
4. Save and close the file.

   Logging begins the next time that the system is restarted.
5. To begin logging immediately, type the following command:

   ```
   nohup sh -c "tail -f /var/log/squid/access.log | logger -p
   <facility>.<priority>" &
   ```

   The <*facility*> and <*priority*> options are the same values that you entered.
6. Open the following file:

   `/etc/syslog.conf`

   Note: When using rsyslog, open `/etc/rsyslog.conf` instead of `/etc/syslog.conf`.
7. Add the following line to send the logs to QRadar:

   `<facility>.<priority> @<QRadar_IP_address>`

   The following example shows a priority and facility for Squid messages and a QRadar IP address:

   `local4.info @<IP_address>`
8. Confirm that `access_log` format ends in `common`.

   Example:

   ```
   access_log /path/to/access.log common
   ```

   If the `access_log` format end value is `squid`, change `squid` to `common`, as displayed in the example.

   If the `access_log` format does not have an ending value, add the following line to the Squid `conf` file to turn on `httpd` log file emulation:

   ```
   emulate_httpd_log on
   ```

9. Choose one of the following options:
   - To restart the Squid service, type the following command:

     ```
     service squid restart
     ```
   - To reload the configuration without restarting the service, type the following command:

     ```
     /usr/sbin/squid -k reconfigure
     ```
10. Save and close the file.
11. Type the following command to restart the syslog daemon:

    ```
    /etc/init.d/syslog restart
    ```

    For more information about configuring Squid, see your vendor documentation.

Results

After you configure syslog forwarding for your cache and access logs, the configuration is complete. QRadar can automatically discover syslog events that are forwarded from Squid.

Syslog log source parameters for Squid Web Proxy

If QRadar does not automatically detect the log source, add a Squid Web Proxy log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Squid Web Proxy:

Table 943. Syslog log source parameters for the Squid Web Proxy DSM

Parameter	Value
Log Source type	Squid Web Proxy
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from the Squid Web Proxy.

Related tasks

"Adding a log source" on page 5

Squid Web Proxy sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Squid Web Proxy sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that a client issued a no-cache pragma.

```
<14>Apr 29 10:23:13 user2: Info: 1556526193.765 100020 172.16.0.1 TCP_CLIENT_REFRESH_MISS/-50
4499 GET http://www.test.test/xx/test "TEST\userx@test" DIRECT/test.test text/html
DEFAULT_CASE_12-ASI_HTTP_Test-PSA_HTTP_NTLM-NONE-NONE-NONE-DefaultGroup
<IW_fnnc,-3.0,0,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-","-","-",-,-,IW_fnnc,-,"-","-","Unknown","Unknown","-
","-",0.36,0,-,"Unknown","-",-,"-",-,-,"-","-",-,-,"-"> - 795 user2
```

```
<14>Apr 29 10:23:13 user2: Info: 1556526193.765 100020 172.16.0.1 TCP_CLIENT_REFRESH_MISS/-50
4499 GET http://www.test.test/xx/test "TEST\userx@test" DIRECT/test.test text/html
```

```
DEFAULT_CASE_12-ASI_HTTP_Test-PSA_HTTP_NTLM-NONE-NONE-NONE-DefaultGroup
<IW_fnnc,-3.0,0,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-","-",-,-,IW_fnnc,-,"-","-","Unknown","Unknown",
"-","-",0.36,0,-,"Unknown","-",-,"-",-,-,"-","-",-,-,"-"> - 795 user2
```

Table 944. Highlighted values in the Squid Web Proxy sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**TCP_CLIENT_REFRESH_MISS**
Source IP	**172.16.0.1**
Username	**TEST\userx@test**
Device Time	**Apr 29 10:23:13**

Sample 2: The following sample event message shows that access is denied.

```
<166>Jan 05 15:45:39 remotelogger: 1515079800.000 10.146.139.172 TCP_DENIED/407 2052 CONNECT
phone.clients.example.com:443 - NONE/192.168.121.158 text/html
```

```
<166>Jan 05 15:45:39 remotelogger: 1515079800.000 10.146.139.172 TCP_DENIED/407 2052 CONNECT
phone.clients.example.com:443 - NONE/192.168.121.158 text/html
```

Table 945. Highlighted values in the Squid Web Proxy sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**TCP_DENIED**
Source IP	**10.146.139.172**
Destination IP	**192.168.121.158**
Device Time	**Jan 05 15:45:39**

Chapter 149. SSH CryptoAuditor

The IBM QRadar DSM for SSH CryptoAuditor collects logs from an SSH CryptoAuditor.

The following table identifies the specifications for the SSH CryptoAuditor DSM.

Table 946. SSH CryptoAuditor DSM specifications

Specification	Value
Manufacturer	SSH Communications Security
Product	CryptoAuditor
DSM Name	SSH CryptoAuditor
RPM filename	`DSM-SSHCryptoAuditor-`*`QRadar_release-Build_number`*`.noarch.rpm`
Supported versions	1.4.0 or later
Event format	Syslog
QRadar recorded event types	Audit, Forensics
Log source type in QRadar UI	SSH CryptoAuditor
Auto discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	SSH Communications Security website (http://www.ssh.com/)

To send events from SSH CryptoAuditor to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - SSH CryptoAuditor RPM
2. For each instance of SSH CryptoAuditor, configure your SSH CryptoAuditor system to communicate with QRadar.
3. If QRadar does not automatically discover SSH CryptoAuditor, create a log source on the QRadar Console for each instance of SSH CryptoAuditor. Use the following SSH CryptoAuditor specific parameters:

Parameter	Value
Log Source Type	SSH CryptoAuditor
Protocol Configuration	Syslog

Related tasks

Configuring an SSH CryptoAuditor appliance to communicate with QRadar
To collect SSH CryptoAuditor events, you must configure your third-party appliance to send events to IBM QRadar.

Adding a DSM

Configuring an SSH CryptoAuditor appliance to communicate with QRadar

To collect SSH CryptoAuditor events, you must configure your third-party appliance to send events to IBM QRadar.

Procedure

1. Log in to SSH CryptoAuditor.
2. Go to the syslog settings in **Settings** > **External Services** > **External Syslog Servers**.
3. To create server settings for QRadar, click **Add Syslog Server**.
4. Type the QRadar server settings: address (IP address or FQDN) and port in which QRadar collects log messages.
5. To set the syslog format to Universal LEEF, select the **Leef format** check box.
6. To save the configuration, click **Save**.
7. Configure SSH CryptoAuditor alerts in **Settings** > **Alerts**. The SSH CryptoAuditor alert configuration defines which events are sent to external systems (email or SIEM/syslog).
   a) Select an existing alert group, or create new alert group by clicking **Add alert group**.
   b) Select the QRadar server that you defined earlier in the **External Syslog Server** drop box.
   c) If you created a new alert group, click **Save**. Save the group before binding alerts to the group.
   d) Define which alerts are sent to QRadar by binding alerts to the alert group. Click **[+]** next to the alert that you want to collect in QRadar, and select the alert group that has QRadar as external syslog server. Repeat this step for each alert that you want to collect in QRadar.
   e) Click **Save**.
8. Apply the pending configuration changes. The saved configuration changes do not take effect until you apply them from pending state.

Chapter 150. Configuring Starent Networks device to forward syslog events to QRadar

The Starent Networks DSM for IBM QRadar accepts Event, Trace, Active, and Monitor events.

About this task

Before you configure a Starent Networks device in QRadar, you must configure your Starent Networks device to forward syslog events to QRadar.

Procedure

1. Log in to your Starent Networks device.
2. Configure the syslog server:

   ```
   logging syslog <IP address> [facility <facilities>] [<rate value>] [pdu-
   verbosity <pdu_level>] [pdu-data <format>] [event-verbosity <event_level>]
   ```

   The following table provides the necessary parameters:

Table 947. Syslog server parameters

Parameter	Description
syslog <*IP address*>	Type the IP address of your QRadar
facility <*facilities*>	Type the local facility for which the logging options are applied. The options are as follows: • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 The default is local7.
rate value	Type the rate that you want log entries to be sent to the system log server. This value must be an integer 0 - 100000. The default is 1000 events per second.
pdu-verbosity <*pdu-level*>	Type the level of verboseness you want to use in logging the Protocol Data Units (PDUs). The range is 1 - 5 where 5 is the most detailed. This parameter affects only protocol logs.

Table 947. Syslog server parameters (continued)	
Parameter	**Description**
pdu-data <*format*>	Type the output format for the PDU when logged as one of following formats: • none - Displays results in raw or unformatted text. • hex - Displays results in hexadecimal format. • hex-ascii - Displays results in hexadecimal and ASCII format similar to a main frame dump.
event-verbosity <*event_level*>	Type the level of detail you want to use in logging of events, that includes: • min - Provides minimal information about the event, such as, event name, facility, event ID, severity level, data, and time. • concise - Provides detailed information about the event, but does not provide the event source. • full - Provides detailed information about the event and includes the source information that identifies the task or subsystem that generated the event.

3. From the root prompt for the Exec mode, identify the session for which the trace log is to be generated:

   `logging trace {callid <call_id> | ipaddr <IP address> | msid <ms_id> | name <username>}`

   The following table provides the necessary parameters:

Table 948. Trace log parameters	
Parameter	**Description**
callid <*call_id*>	Indicates a trace log is generated for a session that is identified by the call identification number. This value is a 4-byte hexadecimal number.
ipaddr <*IP address*>	Indicates a trace log is generated for a session that is identified by the specified IP address.
msid <*ms_id*>	Indicates a trace log is generated for a session that is identified by the mobile station identification (MSID) number. This value must be 7 - 16 digits, which are specified as an IMSI, MIN, or RMI.
name <*username*>	Indicates a trace log is generated for a session that is identified by the username. This value is the name of the subscriber that was previously configured.

4. To write active logs to the active memory buffer, in the config mode:

   `logging runtime buffer store all-events`

5. Configure a filter for the active logs:

   `logging filter active facility <facility> level <report_level> [critical-info | no-critical-info]`

   The following table provides the necessary parameters:

Table 949. Active log parameters

Parameter	Description
facility <facility>	Type the facility message level. A facility is a protocol or task that is in use by the system. The local facility defines which logging options are applied for processes that run locally. The options are as follows: • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 The default is local7.
level <*report_level*>	Type the log severity level, including: • critical - Logs only those events that indicate a serious error is occurring and that is causing the system or a system component to cease functioning. Critical is the highest level severity. • error - Logs events that indicate an error is occurring that is causing the system or a system component to operate in a degraded state. This level also logs events with a higher severity level. • warning - Logs events that can indicate a potential problem. This level also logs events with a higher severity level. • unusual - Logs events that are unusual and might need to be investigated. This level also logs events with a higher severity level. • info - Logs informational events and events with a higher severity level. • debug - Logs all events regardless of the severity. It is suggested that a level of error or critical can be configured to maximize the value of the logged information and lower the quantity of logs that are generated.
critical-info	The critical-info parameter identifies and displays events with a category attribute of critical information. Examples of these types of events can be seen at bootup when system processes or tasks are being initiated.
no-critical-info	The no-critical-info parameter specifies that events with a category attribute of critical information are not displayed.

6. Configure the monitor log targets:

   `logging monitor {msid <ms_id>|username <username>}`

   The following table provides the necessary parameters:

Table 950. Monitor log parameters	
Parameter	**Description**
msid <*md_id*>	Type an msid to define that a monitor log is generated for a session that is identified by using the Mobile Station Identification (MDID) number. This value must be 7 - 16 digits that are specified as a IMSI, MIN, or RMI.
username <*username*>	Type user name to identify a monitor log generated for a session by the user name. The user name is the name of the subscriber that was previously configured.

7. You are now ready to configure the log source in QRadar.

   To configure QRadar to receive events from a Starent device:

   a) From the **Log Source Type** list, select the **Starent Networks Home Agent (HA)** option.

      For more information about the device, see your vendor documentation.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Chapter 151. STEALTHbits

IBM QRadar supports a range of STEALTHbits DSMs.

STEALTHbits StealthINTERCEPT

The IBM QRadar DSM for STEALTHbits StealthINTERCEPT can collect event logs from your STEALTHbits StealthINTERCEPT and File Activity Monitor services.

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT DSM.

Table 951. STEALTHbits StealthINTERCEPT DSM specifications

Specification	**Value**
Manufacturer	STEALTHbits Technologies
DSM	STEALTHbits StealthINTERCEPT
RPM file name	`DSM-STEALTHbitsStealthINTERCEPT-`*`QRadar_Version-build_number`*`.noarch.rpm`
Supported versions	3.3
Protocol	Syslog
Event format	LEEF
QRadar recorded events	Active Directory Audit Events, File Activity Monitor Events
Automatically discovered	Yes
Includes identity	No
More information	http://www.stealthbits.com/resources

Syslog log source parameters for STEALTHbits StealthINTERCEPT

If QRadar does not automatically detect the log source, add a STEALTHbits StealthINTERCEPT log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events fromSTEALTHbits StealthINTERCEPT:

Table 952. Syslog log source parameters for the STEALTHbits StealthINTERCEPT DSM

Parameter	**Value**
`Log Source type`	STEALTHbits StealthINTERCEPT
`Protocol Configuration`	Syslog

Related tasks

"Adding a log source" on page 5

Configuring your STEALTHbits StealthINTERCEPT to communicate with QRadar

To collect all audit logs and system events from STEALTHbits StealthINTERCEPT, you must specify IBM QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration** > **Syslog Server**.
4. Configure the following parameters:

Table 953. Syslog parameters	
Parameter	**Description**
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the `SyslogLeefTemplate.txt` file and press Enter.
7. Click **Save**.
8. On the **Administration Console**, click **Actions**.
9. Select the mapping file that you imported, and then select the **Send to Syslog** check box.

   Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.
10. Click **Add**.

Configuring your STEALTHbits File Activity Monitor to communicate with QRadar

To collect events from STEALTHbits File Activity Monitor, you must specify IBM QRadar as the Syslog server and configure the message format.

Procedure

1. Log in to the server that runs STEALTHbits File Activity Monitor.
2. Select the **Monitored Hosts** tab.
3. Select a monitored host and click **Edit** to open the host's properties window.
4. Select the Syslog tab and configure the following parameters:

Parameter	**Description**
Bulk Syslog server in SERVER[:PORT] format	<*QRadar event collector IP address*>:514 Example: 192.0.2.1:514 <*qradarhostname*>:514
Syslog message template file path	`SyslogLeefTemplate.txt` The template is stored in the STEALTHbits File Activity Monitor Install Directory

5. Click **OK**.

Syslog log source parameters for STEALTHbits File Activity Monitor

If QRadar does not automatically detect the log source, add a STEALTHbits StealthINTERCEPT log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from STEALTHbits File Activity Monitor:

Table 954. Syslog log source parameters for the STEALTHbits File Activity Monitor DSM

Parameter	Value
Log Source type	STEALTHbits StealthINTERCEPT
Protocol Configuration	Syslog

Related tasks

"Adding a log source" on page 5

STEALTHbits StealthINTERCEPT Alerts

IBM QRadar collects alerts logs from a STEALTHbits StealthINTERCEPT server by using STEALTHbits StealthINTERCEPT Alerts DSM

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT Alerts DSM:

Table 955. STEALTHbits StealthINTERCEPT Alerts DSM specifications

Specification	Value
Manufacturer	STEALTHbits Technologies
DSM name	STEALTHbits StealthINTERCEPT Alerts
RPM file name	`DSM-STEALTHbitsStealthINTERCEPTAlerts-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	3.3
Protocol	Syslog LEEF
Recorded event types	Active Directory Alerts Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	StealthINTERCEPT (http://www.stealthbits.com/products/stealthintercept)

To integrate STEALTHbits StealthINTERCEPT with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - `DSMCommon` RPM
   - `STEALTHbitsStealthINTERCEPT` RPM
   - `STEALTHbitsStealthINTERCEPTAlerts` RPM
2. Configure your STEALTHbits StealthINTERCEPT device to send syslog events to QRadar.

3. If QRadar does not automatically detect the log source, add a STEALTHbits StealthINTERCEPT Alerts log source on the QRadar Console. The following table describes the parameters that require specific values for STEALTHbits StealthINTERCEPT Alerts event collection:

Table 956. STEALTHbits StealthINTERCEPT Alerts log source parameters	
Parameter	**Value**
Log Source type	STEALTHbits StealthINTERCEPT Alerts
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Collecting alerts logs from STEALTHbits StealthINTERCEPT

To collect all alerts logs from STEALTHbits StealthINTERCEPT, you must specify IBM QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration** > **Syslog Server**.
4. Configure the following parameters:

Parameter	Description
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the **SyslogLeefTemplate.txt** file and press Enter.
7. Click **Save**.
8. On the Administration Console, click **Actions**.
9. Select the mapping file that you imported, and then select the **Send to Syslog** check box.

   Tip: Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.
10. Click **Add**.

STEALTHbits StealthINTERCEPT Analytics

IBM QRadar collects analytics logs from a STEALTHbits StealthINTERCEPT server by using STEALTHbits StealthINTERCEPT Analytics DSM.

The following table identifies the specifications for the STEALTHbits StealthINTERCEPT Analytics DSM:

Table 957. STEALTHbits StealthINTERCEPT Analytics DSM specifications	
Specification	**Value**
Manufacturer	STEALTHbits Technologies
DSM name	STEALTHbits StealthINTERCEPT Analytics

Table 957. STEALTHbits StealthINTERCEPT Analytics DSM specifications (continued)	
Specification	**Value**
RPM file name	DSM-STEALTHbitsStealthINTERCEPTAnalytics-*Qradar_version-build_number*.noarch.rpm
Supported versions	3.3
Protocol	Syslog LEEF
Recorded event types	Active Directory Analytics Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	StealthINTERCEPT (http://www.stealthbits.com/products/stealthintercept)

Integrate STEALTHbits StealthINTERCEPT with QRadar by completing the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console in the order that they are listed:
   - DSMCommon RPM
   - STEALTHbitsStealthINTERCEPT RPM
   - STEALTHbitsStealthINTERCEPTAnalytics RPM
2. Configure your STEALTHbits StealthINTERCEPT device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a STEALTHbits StealthINTERCEPT Analytics log source on the QRadar Console. The following table describes the parameters that require specific values for STEALTHbits StealthINTERCEPT Analytics event collection:

Table 958. STEALTHbits StealthINTERCEPT Analytics log source parameters	
Parameter	**Value**
Log Source type	STEALTHbits StealthINTERCEPT Analytics
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Collecting analytics logs from STEALTHbits StealthINTERCEPT" on page 1489
To collect all analytics logs from STEALTHbits StealthINTERCEPT, you must specify IBM QRadar as the syslog server and configure the message format.

"Adding a log source" on page 5

Collecting analytics logs from STEALTHbits StealthINTERCEPT

To collect all analytics logs from STEALTHbits StealthINTERCEPT, you must specify IBM QRadar as the syslog server and configure the message format.

Procedure

1. Log in to your STEALTHbits StealthINTERCEPT server.
2. Start the Administration Console.
3. Click **Configuration** > **Syslog Server**.

4. Configure the following parameters:

Parameter	Description
Host Address	The IP address of the QRadar Console
Port	514

5. Click **Import mapping file**.
6. Select the **SyslogLeefTemplate.txt** file and press Enter.
7. Click **Save**.
8. On the Administration Console, click **Actions**.
9. Select the mapping file that you imported, and then select the **Send to Syslog** check box.

   Tip: Leave the **Send to Events DB** check box selected. StealthINTERCEPT uses the events database to generate reports.
10. Click **Add**.

Chapter 152. Sun

IBM QRadar supports a range of Sun DSMs.

Sun ONE LDAP

The Sun ONE LDAP DSM for QRadar accepts multiline UDP access and LDAP events from Sun ONE Directory Servers.

Sun ONE LDLAP is known as Oracle Directory Server.

QRadar retrieves access and LDAP events from Sun ONE Directory Servers by connecting to each server to download the event log. The event file must be written to a location accessible by the log file protocol of QRadar with FTP, SFTP, or SCP. The event log is written in a multiline event format, which requires a special event generator in the log file protocol to properly parse the event. The ID-Linked Multiline event generator is capable of using regex to assemble multiline events for QRadar when each line of a multiline event shares a common starting value.

The Sun ONE LDAP DSM also can accept events streamed using the UDP Multiline Syslog protocol. However, in most situations your system requires a 3rd party syslog forwarder to forward the event log to QRadar. This can require you to redirect traffic on your QRadar Console to use the port defined by the UDP Multiline protocol.

Related concepts

"UDP multiline syslog protocol configuration options" on page 233
To create a single-line syslog event from a multiline event, configure a log source to use the UDP multiline protocol. The UDP multiline syslog protocol uses a regular expression to identify and reassemble the multiline syslog messages into single event payload.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Enabling the event log for Sun ONE Directory Server

To collect events from your Sun ONE Directory Server, you must enable the event log to write events to a file.

Procedure

1. Log in to your Sun ONE Directory Server console.
2. Click the **Configuration** tab.
3. From the navigation menu, select **Logs**.
4. Click the **Access Log** tab.
5. Select the **Enable Logging** check box.
6. Type or click **Browse** to identify the directory path for your Sun ONE Directory Server access logs.
7. Click **Save**.

What to do next

You are now ready to configure a log source in QRadar.

Log File log source parameters for Sun ONE LDAP

If QRadar does not automatically detect the log source, add a Sun ONE LDAP log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from Sun ONE LDAP:

Table 959. Log File log source parameters for the Sun ONE LDAP DSM

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	**Sun ONE LDAP**
Protocol Configuration	**Log File**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. IP addresses or host names enable QRadar to identify a log file to a unique event source. For example, if your network contains multiple devices, such as a management console or a file repository, specify the IP address or host name of the device that created the event. This enables events to be identified at the device level in your network, instead of identifying the event for the management console or file repository.
Service Type	Type the TCP port on the remote host that is running the selected Service Type. The valid range is 1 - 65535. The options include: **FTP** TCP Port 21. **SFTP** TCP Port 22. **SCP** TCP Port 22. **Important:** If the host for your event files is using a non-standard port number for FTP, SFTP, or SCP, you must adjust the port value.
Remote User	Type the user name necessary to log in to the host that contains your event files. The user name can be up to 255 characters in length.
Confirm Password	Confirm the password necessary to log in to the host.
SSH Key File	If you select SCP or SFTP as the **Service Type**, this parameter enables you to define an SSH private key file. When you provide an SSH Key File, the **Remote Password** field is ignored.

Table 959. Log File log source parameters for the Sun ONE LDAP DSM (continued)

Parameter	Value
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. **Important:** For FTP only. If your log files are in the remote user's home directory, you can leave the remote directory blank. This is to support operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Enable this check box to allow FTP or SFTP connections to recursively search sub folders of the remote directory for event data. Data that is collected from sub folders depends on matches to the regular expression in the FTP File Pattern. The **Recursive** option is not available for SCP connections.
FTP File Pattern	For example, if you want to list all files that start with the word log, followed by one or more digits and ending with tar.gz, use the following entry: log[0-9]+\.tar\.gz. Use of this parameter requires knowledge of regular expressions (regex). For more information about regular expressions, see the Oracle website (http://docs.oracle.com/javase/tutorial/essential/regex/) If you select SFTP or FTP as the Service Type, this option enables you to configure the regular expression (regex) that is required to filter the list of files that are specified in the Remote Directory. All matching files are included in the processing.
FTP Transfer Mode	From the list box, select the transfer mode that you want to apply to this log source: **Binary** Select **Binary** for log sources that require binary data files or compressed zip, gzip, tar, or tar+gzip archive files. **ASCII** Select **ASCII** for log sources that require an ASCII FTP file transfer. **Important:** You must select **NONE** for the **Processor** parameter and **LINEBYLINE** the **Event Generator** parameter when you use ASCII as the FTP Transfer Mode. This option only appears if you select FTP as the Service Type. The FTP Transfer Mode parameter enables you to define the file transfer mode when you retrieve log files over FTP.
SCP Remote File	If you select SCP as the **Service Type** you must type the file name of the remote file.

Table 959. Log File log source parameters for the Sun ONE LDAP DSM (continued)	
Parameter	**Value**
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, 2H if you want the directory to be scanned every 2 hours. The default is 1H.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the **Run On Save** completes, the log file protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the Ignore Previously Processed File parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	If the files on the remote host are stored in a zip, gzip, tar, or tar+gzip archive format, select the processor that allows the archives to be expanded and contents to be processed.
Ignore Previously Processed File(s)	This only applies to FTP and SFTP Service Types. Select this check box to track files that were processed and you do not want the files to be processed a second time.
Change Local Directory?	Select this check box to define the local directory on your QRadar that you want to use for storing downloaded files during processing. Most configurations can leave this check box clear. When you select the check box, the **Local Directory** field is displayed, which enables you to configure a local directory to use for temporarily storing files.

Table 959. Log File log source parameters for the Sun ONE LDAP DSM (continued)	
Parameter	**Value**
Event Generator	The ID-Linked Multiline format processes multiline event logs that contain a common value at the start of each line in a multiline event message. This option displays the **Message ID Pattern** field that uses regex to identify and reassemble the multiline event in to single event payload. Select **ID-Linked Multiline** to process to the retrieved event log as multiline events.
Folder Separator	Most configurations can use the default value in the **Folder Separator** field. This field is only used by operating systems that use an alternate character to define separate folders. For example, periods that separate folders on mainframe systems. Type the character that is used to separate folders for your operating system. The default value is /.

Related tasks
"Adding a log source" on page 5

UDP Multiline Syslog log source parameters for Sun ONE LDAP

If QRadar does not automatically detect the log source, add a Sun ONE LDAP log source on the QRadar Console by using the UDP Multiline Syslog protocol.

When using the UDP Multiline Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect UDP Multiline Syslog events from Sun ONE LDAP:

Table 960. UDP Multiline Syslog log source parameters for the Sun ONE LDAP DSM	
Parameter	**Value**
Log Source type	**Sun ONE LDAP**
Protocol Configuration	**UDP Multiline Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Sun ONE LDAP devices.

For a complete list of UDP Multiline Syslog protocol parameters and their values, see UDP multiline syslog protocol configuration options.

Related tasks
Adding a log source

Configuring IPtables for UDP Multiline Syslog events

You might be unable to send events directly to the standard UDP Multiline port 517 or any unused available ports when you collect UDP Multiline Syslog events in IBM QRadar. If this error occurs, then you must redirect events from port 514 to the default port 517 or your chosen alternative port by using IPTables. You must configure IPtables on your QRadar Console or for each QRadar Event Collector

that receives UDP Multiline Syslog events from an SunOne LDAP server. Then, you must complete the configuration for each SunOne LDAP server IP address that you want to receive logs from.

Before you begin

Important: Complete this configuration method when you can't send UDP Multiline Syslog events directly to the chosen UDP Multiline port on QRadar from your SunOne LDAP server. Also, you must complete this configuration when you are restricted to send only to the standard syslog port 514.

Procedure

1. Using SSH, log in to QRadar as the root user.

   Login: *root*

   Password: *password*
2. Type the following command to edit the IPtables file:

   `vi /opt/qradar/conf/iptables-nat.post`

   The IPtables NAT configuration file is displayed.
3. Type the following command to instruct QRadar to redirect syslog events from UDP port 514 to UDP port 517:

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port <new-port> -s <IP address>
   ```

   Where:

   IP address is the IP address of your SunOne LDAP server.

   New port is the port number that is configured in the UDP Multiline protocol for SunOne LDAP.

   You must include a redirect for each SunOne LDAP IP address that sends events to your QRadar Console or Event Collector. Example:

   ```
   -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 517 -s <IP_address>
   ```
4. Save your IPtables NAT configuration.

   You are now ready to configure IPtables on your QRadar Console or Event Collector to accept events from your SunOne LDAP servers.
5. Type the following command to edit the IPtables file:

   `vi /opt/qradar/conf/iptables.post`

   The IPtables configuration file is displayed.
6. Type the following command to instruct QRadar to allow communication from your SunOne LDAP servers:

   ```
   -I QChain 1 -m udp -p udp --src <IP_address> --dport <New port> -j ACCEPT
   ```

   Where:

   IP address is the IP address of your SunOne LDAP server.

   New port is the port number that is configured in the UDP Multiline protocol for SunOne LDAP.

   You must include a redirect for each SunOne LDAP IP address that sends events to your QRadar Console or Event Collector. Example:

   ```
   -I QChain 1 -m udp -p udp --src <IP_address> --dport 517 -j ACCEPT
   ```
7. Type the following command to update IPtables in QRadar:

   `./opt/qradar/bin/iptables_update.pl`

Example

If you need to configure another QRadar Console or Event Collector that receives syslog events from an SunOne LDAP server, repeat these steps.

What to do next

Configure your SunOne LDAP server to forward events to QRadar.

Sun Solaris Basic Security Mode (BSM)

Sun Solaris Basic Security Mode (BSM) is an audit tracking tool for the system administrator to retrieve detailed auditing events from Sun Solaris systems.

IBM QRadar retrieves Sun Solaris BSM events by using the log file Protocol. For you to configure QRadar to integrate with Solaris Basic Security Mode, take the following steps:

1. Enable Solaris Basic Security Mode.
2. Convert audit logs from binary to a human-readable format.
3. Schedule a cron job to run the conversion script on a schedule.
4. Collect Sun Solaris events in QRadar by using the log file protocol.

Enabling Basic Security Mode in Solaris 10

To configure Sun Solaris BSM in Solaris 10, you must enable Solaris Basic Security Mode and configure the classes of events the system logs to an audit log file.

About this task

Configure Basic Security Mode and enable auditing in Sun Solaris 10.

Procedure

1. Log in to your Solaris console as a superuser or root user.
2. Enable single-user mode on your Solaris console.
3. Type the following command to run the `bsmconv` script and enable auditing:

   ```
   /etc/security/bsmconv
   ```

   The `bsmconv` script enables Solaris Basic Security Mode and starts the auditing service `auditd`.
4. Type the following command to open the audit control log for editing:

   ```
   vi /etc/security/audit_control
   ```
5. Edit the audit control file to contain the following information:

   ```
   dir:/var/audit flags:lo,ad,ex,-fw,-fc,-fd,-fr naflags:lo,ad
   ```
6. Save the changes to the `audit_control` file, and then reboot the Solaris console to start `auditd`.
7. Type the following command to verify that `auditd` starts :

   ```
   /usr/sbin/auditconfig -getcond
   ```

   If the `auditd` process is started, the following string is returned:

   ```
   audit condition = auditing
   ```

What to do next

You can now convert the binary Solaris Basic Security Mode logs to a human-readable log format.

Enabling Basic Security Mode in Solaris 11

To configure Sun Solaris BSM in Solaris 11, you must enable Solaris Basic Security Mode and configure the classes of events the system logs to an audit log file.

Procedure

1. Log in to Solaris 11 console as a superuser or root.
2. Start the audit service by typing the following command:

   ```
   audit -s
   ```
3. Set up the attributable classes by typing the following command:

   ```
   auditconfig -setflags lo,ps,fw
   ```
4. Set up the non-attributable classes by typing the following command:

   ```
   auditconfig -setnaflags lo,na
   ```
5. To verify that audit service starts, type the following command:

   ```
   /usr/sbin/auditconfig -getcond
   ```

   If the `auditd` process is started, the following string is returned:

   ```
   audit condition = auditing
   ```

Converting Sun Solaris BSM audit logs

IBM QRadar doesn't process binary files directly from Sun Solaris BSM. You must convert the audit log from the existing binary format to a human-readable log format by using `praudit` before the audit log data can be retrieved by QRadar.

Procedure

1. Type the following command to create a new script on your Sun Solaris console:

   ```
   vi /etc/security/newauditlog.sh
   ```
2. Add the following information to the `newauditlog.sh` script:

```
#!/bin/bash
#
# newauditlog.sh - Start a new audit file and expire the old logs
#
AUDIT_EXPIRE=30
AUDIT_DIR="/var/audit"
LOG_DIR="/var/log/"
/usr/sbin/audit -n
cd $AUDIT_DIR
# Get a listing of the files based on creation date that are not current in use
FILES=$(ls -lrt | tr -s " " | cut -d" " -f9 | grep -v "not_terminated")
# We created a new audit log so that the last file in the list is the latest archived binary log file.
lastFile=""
for file in $FILES; do
 lastFile=$file
done
# Extract a human-readable file from the binary log file
echo "Beginning praudit of $lastFile"
praudit -l $lastFile > "$LOG_DIR$lastFile.log"
echo "Done praudit, creating log file at: $LOG_DIR$lastFile.log"
/usr/bin/find . $AUDIT_DIR -type f -mtime +$AUDIT_EXPIRE \ -exec rm {} > /dev/null 2>&1 \;
# End script
```

   The script outputs log files in the <*starttime*>.<*endtime*>.<*hostname*>.log format.

   For example, the log directory in `/var/log` contains a file with the following name:

   ```
   20111026030000.20111027030000.qasparc10.log
   ```
3. Optional: Edit the script to change the default directory for the log files.

   a) `AUDIT_DIR="/var/audit"` - The Audit directory must match the location that is specified by the audit control file you configured in “Enabling Basic Security Mode in Solaris 10” on page 1497.

4. `LOG_DIR="/var/log/"` - The log directory is the location of the human-readable log files of your Sun Solaris system that are ready to be retrieved by QRadar.
5. Save your changes to the `newauditlog.sh` script.
6. Optional: If you want to make the script executable, type the following command:

   ```
   chmod +x /etc/security/newauditlog.sh
   ```

What to do next

If this script is executable, you can automate it by using CRON to convert the Sun Solaris Basic Security Mode log to human-readable format.

Creating a cron job

Cron is a Solaris daemon utility that automates scripts and commands to run system-wide on a scheduled basis.

About this task

The following steps provide an example for automating newauditlog.sh to run daily at midnight. If you need to retrieve log files multiple times a day from your Solaris system, you must alter your cron schedule.

Procedure

1. Type the following command to create a copy of your cron file:

   ```
   crontab -l > cronfile
   ```
2. Type the following command to edit the `cronfile`:

   ```
   vi cronfile
   ```
3. Add the following information to your `cronfile`:

   ```
   0 0 * * * /etc/security/newauditlog.sh
   ```
4. Save the change to the `cronfile`.
5. Type the following command to add the `cronfile` to `crontab`:

   ```
   crontab cronfile
   ```
6. You can now configure the log source in IBM QRadar to retrieve the Sun Solaris BSM audit log files.

What to do next

You are now ready to configure a log source in QRadar.

Log File log source parameters for Sun Solaris BSM

If QRadar does not automatically detect the log source, add a Sun Solaris BSM log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from Sun Solaris BSM:

Table 961. Log File log source parameters for the Sun Solaris BSM DSM

Parameter	Value
Log Source type	**Solaris BSM**
Protocol Configuration	**Log File**

Table 961. Log File log source parameters for the Sun Solaris BSM DSM (continued)	
Parameter	**Value**
Log Source Identifier	Type the IP address or host name for the log source. The log source identifier must be unique for the log source type.
Service Type	From the list, select the protocol that you want to use when retrieving log files from a remove server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy The underlying protocol that is used to retrieve log files for the SCP and SFTP service types requires that the server specified in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the Sun Solaris BSM system.
Remote Port	Type the TCP port on the remote host that is running the selected Service Type. If you configure the Service Type as FTP, the default is 21. If you configure the Service Type as SFTP or SCP, the default is 22. The valid range is 1 - 65535.
Remote User	Type the user name necessary to log in to your Sun Solaris system. The user name can be up to 255 characters in length.
Remote Password	Type the password necessary to log in to your Sun Solaris system.
Confirm Password	Confirm the **Remote Password** to log in to your Sun Solaris system.
SSH Key File	If you select **SCP** or **SFTP** from the **Service Type** field you can define a directory path to an SSH private key file. The SSH Private Key File gives the option to ignore the **Remote Password** field.
Remote Directory	Type the directory location on the remote host from which the files are retrieved. By default, the newauditlog.sh script writes the human-readable logs files to the `/var/log/` directory.
Recursive	Select this check box if you want the file pattern to also search sub folders. The Recursive parameter is not used if you configure SCP as the Service Type. By default, the check box is clear.

Table 961. Log File log source parameters for the Sun Solaris BSM DSM (continued)

Parameter	Value
FTP File Pattern	If you select **SFTP** or **FTP** as the **Service Type**, this gives the option to configure the regular expression (regex) that is needed to filter the list of files that are specified in the **Remote Directory**. All matching files are included in the processing. For example, if you want to retrieve all files in the `<starttime>.<endtime>.<hostname>.log` format, use the following entry: `\d+\.\d+\.\w+\.log`. Use of this parameter requires knowledge of regular expressions (regex). For more information, see the following website: http://download.oracle.com/javase/tutorial/essential/regex/
FTP Transfer Mode	This option appears only if you select FTP as the Service Type. The **FTP Transfer Mode** parameter gives the option to define the file transfer mode when you retrieve log files over FTP. From the list, select the transfer mode that you want to apply to this log source: • `Binary` - Select Binary for log sources that require binary data files or compressed `.zip`, `.gzip`, `.tar`, or `.tar+gzip` archive files. • **ASCII** - Select ASCII for log sources that require an ASCII FTP file transfer. You must select **NONE** for the **Processor** field and **LINEBYLINE** the **Event Generator** field when you use the ASCII as the transfer mode.
SCP Remote File	If you select **SCP** as the Service Type, you must type the file name of the remote file.
Start Time	Type the time of day you want the processing to begin. This parameter functions with the Recurrence value to establish when and how often the Remote Directory is scanned for files. Type the start time, based on a 24-hour clock, in the following format: HH: MM.
Recurrence	Type the frequency, beginning at the Start Time, that you want the remote directory to be scanned. Type this value in hours (H), minutes (M), or days (D). For example, type 2H if you want the directory to be scanned every 2 hours. The default is 1H.

Table 961. Log File log source parameters for the Sun Solaris BSM DSM (continued)	
Parameter	**Value**
Run On Save	Select this check box if you want the log file protocol to run immediately after you click Save. After the Run On Save completes, the log file protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the **Ignore Previously Processed File(s)** parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	If the files on the remote host are stored in a `.zip`, `.gzip`, `.tar`, or `tar+gzip` archive format, select the processor that allows the archives to be expanded and contents processed.
Ignore Previously Processed File(s)	Select this check box to track files that are processed already, and you do not want the files to be processed a second time. This applies only to FTP and SFTP Service Types.
Change Local Directory?	Select this check box to define the local directory on your QRadar system that you want to use for storing downloaded files during processing. It is suggested that you leave the check box clear. When the check box is selected, the **Local Directory** field is displayed, which gives you the option to configure the local directory to use for storing files.
Event Generator	From the **Event Generator** list, select **LINEBYLINE**.

Related tasks

"Adding a log source" on page 5

Sun Solaris DHCP

The IBM QRadar DSM for Sun Solaris DHCP collects Syslog events from a Sun Solaris DHCP system.

To integrate Sun Solaris DHCP with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common Rational Portfolio Manager

- Sun Solaris DHCP DSM RPM

2. Configure your Sun Solaris DHCP system to send events to QRadar. For more information about configuring Sun Solaris DHCP to communicate with QRadar, see Configuring Sun Solaris DHCP.
3. If QRadar does not automatically detect the log source, add a Sun Solaris DHCP log source on the QRadar Console. For more information about configuring Syslog log source parameters, see Syslog log source parameters for Sun Solaris DHCP.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Syslog log source parameters for Sun Solaris DHCP

If QRadar does not automatically detect the log source, add a Sun Solaris DHCP log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Syslog events from Sun Solaris DHCP:

Table 962. Syslog log source parameters for the Sun Solaris DHCP DSM

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	**Solaris Operating System DHCP Logs**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from Sun Solaris installations. Each additional log source that you create when you have multiple installations ideally includes a unique identifier, such as an IP address or host name.

Related tasks

"Adding a log source" on page 5

Configuring Sun Solaris DHCP to communicate with QRadar

The Sun Solaris DHCP DSM for IBM QRadar records all relevant DHCP events by using syslog.

About this task

To collect events from Sun Solaris DHCP, you must configure syslog to forward events to QRadar.

Procedure

1. Log in to the Sun Solaris command-line interface.
2. Edit the `/etc/default/dhcp` file.
3. Enable logging of DHCP transactions to syslog by adding the following line:

   ```
   LOGGING_FACILITY=X
   ```

Where X is the number corresponding to a local syslog facility, for example, a number 0 - 7.

4. Save and exit the file.
5. Edit the `/etc/syslog.conf` file.
6. To forward system authentication logs to QRadar, add the following line to the file:

   `localX.notice @<IP address>`

   Where:

   X is the logging facility number that you specified in "Configuring Sun Solaris DHCP to communicate with QRadar" on page 1503.

   <IP address> is the IP address of your QRadar. Use tabs instead of spaces to format the line.
7. Save and exit the file.
8. Type the following command:

   ```
   kill -HUP `cat /etc/syslog.pid`
   ```

What to do next

You are now ready to configure the log source in QRadar.

Sun Solaris OS

The IBM QRadar DSM for Sun Solaris OS collects Syslog events from a Sun Solaris OS system.

To integrate Sun Solaris OS with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Sun Solaris OS DSM RPM
2. Configure your Sun Solaris OS system to send events to QRadar. For more information, see Configuring Sun Solaris OS to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a Sun Solaris OS log source on the QRadar Console. For more information, see Syslog log source parameters for Sun Solaris OS.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Sun Solaris OS DSM specifications

When you configure the Sun Solaris OS, understanding the specifications for the Sun Solaris OS DSM can help ensure a successful integration. For example, knowing what the supported version of Sun Solaris OS is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Sun Solaris OS DSM.

Table 963. Sun Solaris OS DSM specifications

Specification	Value
Manufacturer	Sun
DSM name	Sun Solaris OS
RPM file name	DSM-*SunSolarisOS-QRadar_version-build_number*.noarch.rpm
Supported version	Sun OS 5.8, 5.9

Table 963. Sun Solaris OS DSM specifications (continued)	
Specification	**Value**
Protocol	Syslog
Event format	All events
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No

Configuring Sun Solaris OS to communicate with QRadar

The Sun Solaris OS DSM for IBM QRadar records all relevant Solaris Operating System Authentication Messages events by using the Syslog protocol.

About this task

To collect events from Sun Solaris OS, you must configure syslog to forward events to QRadar.

Procedure

1. Log in to the Sun Solaris command-line interface (CLI).
2. Open the `/etc/syslog.conf` file.
3. To forward system authentication logs to QRadar, add the following line to the file:

   ```
   *.err;auth.notice;auth.info@<IP_address>
   ```

   Where *<IP_address>* is the IP address of your QRadar Console or Event Collector. Use tabs instead of spaces to format the line.

   Tip: Depending on your version of Sun Solaris, you might need to add more log types to the file. Contact your system administrator for more information.
4. Save and exit the file.
5. Type the following command:

   ```
   kill -HUP `cat /etc/syslog.pid`
   ```

What to do next

Configure a log source in QRadar. For more information, see Syslog log source parameters for Sun Solaris OS.

Important: If a Linux log source is created for the Solaris System that is sending events, disable the Linux log source, and then adjust the parsing order. Ensure that the Sun Solaris OS DSM is listed first.

Syslog log source parameters for Sun Solaris OS

If QRadar does not automatically detect the log source, add a Sun Solaris OS log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Syslog events from Sun Solaris OS:

Table 964. Syslog log source parameters for the Sun Solaris OS DSM	
Parameter	**Value**
Log Source type	**Sun Solaris Operating System Authentication Messages**
Protocol Configuration	Syslog
Log Source Identifier	A unique name for the log source. The Log Source Identifier can be any valid value and does not need to reference a specific server. **The Log Source Identifier** can be the same value as the log source **Name**. If you have more than one Sun Solaris OS log source that is configured, you might want to identify the first log source as `solarisos1`, the second log source as `solarisos2`, and the third log source as `solarisos3`.

Related tasks

Adding a log source

Sun Solaris OS sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Sun Solaris OS sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows that a session to the authentication server was opened in Sun Solaris OS.

```
<38>Oct  6 10:35:59 sshd[16942]: [ID 800047 auth.info] Accepted keyboard-interactive for testuser
from 2001:DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF port 51730 ssh2
```

```
<38>Oct  6 10:35:59 sshd[16942]: [ID 800047 auth.info] Accepted keyboard-interactive for
testuser from 2001:DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF port 51730 ssh2
```

Table 965. Highlighted values in the Sun Solaris OS sample event message	
QRadar field name	**Highlighted values in the event payload**
Event ID	login (inferred from the event content)
Source IPv6	**2001:DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF**
Source Port	**51730**
Username	**testuser**
Identity Username	**testuser**
Device Time	**Oct 6 10:35:59** (extracted from date and time fields)

Sample 2: The following sample event message shows mail information events in Sun Solaris OS.

```
<38>Mar 1 17:32:05 10.10.25.2 <22>Mar 1 17:32:00 sendmail[14359]: [ID 801593 mail.info]
a1AA111: to=envmgr, ctladdr=envmgr (11011/111100), delay=00:00:00, xdelay=00:00:00, mailer=abcde,
pri=11111, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent (a1AA111 Message accepted for
delivery)
```

```
<38>Mar 1 17:32:05 10.10.25.2 <22>Mar 1 17:32:00 sendmail[14359]: [ID 801593
mail.info] a1AA111: to=envmgr, ctladdr=envmgr (11011/111100), delay=00:00:00, xdelay=00:00:00,
mailer=abcde, pri=11111, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent (a1AA111 Message
accepted for delivery)
```

Table 966. Highlighted values in the Sun Solaris OS sample event message

QRadar field name	Highlighted values in the event payload
Event ID	**mail.info**
Source IP	**10.10.25.2**
Destination IP	**10.10.25.2**
Device Time	**Mar 1 17:32:05** (extracted from date and time fields)

Sun Solaris Sendmail

The Sun Solaris Sendmail DSM for IBM QRadar accepts Solaris authentication events by using syslog and records all relevant sendmail events.

About this task

To collect events from Sun Solaris Sendmail, you must configure syslog to forward events to QRadar.

Procedure

1. Log in to the Sun Solaris command-line interface.
2. Open the `/etc/syslog.conf` file.
3. To forward system authentication logs to QRadar, add the following line to the file:

   `mail.*; @<IP address>`

   Where <*IP address*> is the IP address of your QRadar. Use tabs instead of spaces to format the line.

   Note: Depending on the version of Solaris, you are running, you might need to add more log types to the file. Contact your system administrator for more information.
4. Save and exit the file.
5. Type the following command:

   `kill -HUP 'cat /etc/syslog.pid'`

   You are now ready to configure the log source QRadar.

Syslog log source parameters for Sun Solaris Sendmail

If QRadar does not automatically detect the log source, add a Sun Solaris Sendmail log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Sun Solaris Sendmail.

Table 967. Syslog log source parameters for the Sun Solaris Sendmail DSM

Parameter	Value
Log Source name	Type a name for your log source.
Log Source description	Type a description for the log source.
Log Source type	**Solaris Operating System Sendmail Logs**

Table 967. Syslog log source parameters for the Sun Solaris Sendmail DSM (continued)	
Parameter	**Value**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from Sun Solaris Sendmail installations Each additional log source that you create when you have multiple installations ideally includes a unique identifier, such as an IP address or host name.

Related tasks

"Adding a log source" on page 5

Chapter 153. Suricata

The IBM QRadar DSM for Suricata collects Syslog events from a Suricata device.

To integrate Suricata with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (https://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - TLS Syslog Protocol RPM
   - Suricata DSM RPM
2. Configure your Suricata device to send events to QRadar. For more information, see "Configuring Suricata to communicate with QRadar" on page 1510.
3. If QRadar does not automatically detect the log source, add a Suricata log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Suricata DSM specifications

When you configure the Suricata device, understanding the specifications for the Suricata DSM can help ensure a successful integration. For example, knowing what the supported version of Suricata is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Suricata DSM.

Table 968. Suricata DSM specifications

Specification	**Value**
Manufacturer	Open Information Security Foundation
DSM name	Suricata
RPM file name	DSM-*Suricata-QRadar_version-build_number*.noarch.rpm
Supported version	6.0.3 and earlier
Protocol	Syslog TLS Syslog
Event format	JSON
Recorded event types	Alerts
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	https://suricata.io/

Configuring Suricata to communicate with QRadar

To send events to IBM QRadar, you must configure a Syslog integration.

Before you begin

You must have access to the Suricata device and have the permissions to write to configuration files and to restart services. You need a username and password, such as Windows or Linux login information, for the system where you installed Suricata.

Ensure that rsyslog is installed on the system where you installed Suricata. For more information, see the rsyslog website (https://www.rsyslog.com).

Procedure

1. Log in to the Suricata device.
2. Open the Suricata configuration file called `suricata.yaml`, located in the Suricata installation directory. Update the `eve-log` entry under the `outputs` header.
   Use the following example as a guide:

```
outputs:
  - eve-log:
    enabled: yes
    filetype: syslog
    identity: "suricata"
    facility: <facility>
    types:
      - alert:
```

   The <*facility*> variable is a Syslog facility name between `local0` and `local7`, such as `local5`.
3. Open the rsyslog configuration file called `/etc/rsyslog.conf` and add a forwarding rule to send the alerts to QRadar.
   Use the following example as a guide:

   <*facility*>.* @@<*QRadar IP/hostname*>:514

   The <*facility*> variable is the same Syslog facility that you configured in the previous step. The <*QRadar IP/hostname*> is the IP or hostname of the QRadar Console or managed host that you want to forward Suricata alerts to.
4. Restart the Suricata and rsyslog services.

What to do next

"Syslog log source parameters for Suricata" on page 1510

Syslog log source parameters for Suricata

If IBM QRadar does not automatically detect the log source, add a Suricata log source on the QRadar Console by using the Syslog protocol.

The following table describes the parameters that require specific values to collect Syslog events from Suricata:

Table 969. Syslog log source parameters for the Suricata DSM

Parameter	Value
Log Source type	Suricata
Protocol Configuration	Syslog
Log Source Identifier	A unique identifier for the log source.

Related tasks

"Adding a log source" on page 5

TLS Syslog log source parameters for Suricata

If IBM QRadar does not automatically detect the log source, add a Suricata log source on the QRadar Console by using the TLS Syslog protocol.

The following table describes the parameters that require specific values to collect Syslog events from Suricata:

Table 970. TLS Syslog log source parameters for the Suricata DSM

Parameter	Value
Log Source type	Suricata
Protocol Configuration	TLS Syslog
Log Source Identifier	A unique identifier for the log source.
TLS Protocols	Select the version of TLS that is installed on the client.

For a complete list of TLS Syslog protocol parameters and their values, see "TLS Syslog protocol configuration options" on page 227.

Related tasks

"Adding a log source" on page 5

Suricata sample event message

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Suricata sample message when you use the Syslog protocol

The following sample event message shows that Suricata detected that malware was being downloaded by an HTTP request.


```
{"timestamp":"2008-10-13T09:55:36.806000-0400","flow_id":1111111111111111,"pcap_cnt":62,"event_t
ype":"alert","src_ip":"10.0.0.1","src_port":80,"dest_ip":"192.168.0.1","dest_port":8282,"proto":
"TCP","tx_id":0,"alert":
{"action":"allowed","gid":1,"signature_id":2014435,"rev":15,"signature":"ET MALWARE
Infostealer.Banprox Proxy.pac Download","category":"A Network Trojan was
detected","severity":1,"metadata":{"updated_at":["2019_08_06"],"created_at":
["2012_02_28"]}},"http":{"hostname":"hostname","url":"\/file2pcap\/
home%2fsuricata%2fpcap","http_user_agent":"Mozilla\/5.0 (X11; U; Linux i686; en-US;
rv:1.8.1.17) Gecko\/20081007 Firefox\/2.0.0.17","http_content_type":"application\/octet-
stream","http_method":"GET","protocol":"HTTP\/
1.1","status":200,"length":31730},"app_proto":"http","flow":
{"pkts_toserver":31,"pkts_toclient":31,"bytes_toserver":2102,"bytes_toclient":33757,"start":"200
8-10-13T09:55:36.013000-0400"},"payload":"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=","stream":1}
```

Table 971. Highlighted fields in the Suricata event	
QRadar field name	**Highlighted payload field name**
Event ID	**gid + ":" + signature_id**
Source IP	**src_ip**
Source Port	**src_port**
Destination IP	**dest_ip**
Destination Port	**dest_port**
Protocol	**proto**
Device Time	**timestamp**

Chapter 154. Sybase ASE

You can integrate a Sybase Adaptive Server Enterprise (ASE) device with IBM QRadar SIEM to record all relevant events by using JDBC.

About this task

To configure a Sybase ASE device:

Procedure

1. Configure Sybase auditing.

   For information about configuring Sybase auditing, see your *Sybase documentation*.
2. Log in to the Sybase database as a sa user:

   `isql -Usa -P<password>`

   Where <*password*> is the password necessary to access the database.
3. Switch to the security database:
   - `use sybsecurity`
   - `go`
4. Create a view for IBM QRadar SIEM.
   - `create view audit_view`
   - `as`
   - `select audit_event_name(event) as event_name, * from <audit_table_1>`
   - `union`
   - `select audit_event_name(event) as event_name, * from <audit_table_2>`
   - `go`
5. For each additional audit table in the audit configuration, make sure that the **`union select`** parameter is repeated for each additional audit table.

   For example, if you want to configure auditing with four audit tables (`sysaudits_01`, `sysaudits_02`, `sysaudits_03`, `sysaudits_04`), type the following commands:
   - `create view audit_view as select audit_event_name(event) as event_name, * from sysaudits_01`
   - `union select audit_event_name(event) as event_name, * from sysaudits_02,`
   - `union select audit_event_name(event) as event_name, * from sysaudits_03,`
   - `union select audit_event_name(event) as event_name, * from sysaudits_04`

What to do next

You can now configure the log source IBM QRadar SIEM.

Related tasks

"Adding a DSM" on page 4

JDBC log source parameters for Sybase ASE

If QRadar does not automatically detect the log source, add a Sybase ASE log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Sybase ASE:

Table 972. JDBC log source parameters for the Sybase ASE DSM

Parameter	Value
Log Source Name	Type a unique name for the log source.
Log Source Description	Type a description for the log source.
Log Source Type	**Sybase ASE**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	Sybase
Database Name	The name of the database to which you want to connect.
IP or Hostname	The IP address or host name of the database server.
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix - 9088 • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the **Port** field blank.
Username	A user account for QRadar in the database.
Password	The password that is required to connect to the database.

Table 972. JDBC log source parameters for the Sybase ASE DSM (continued)	
Parameter	**Value**
Confirm Password	The password that is required to connect to the database.
Predefined Query	Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the **none** option.
Table Name	The name of the table or view that includes the event records. The table name can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period (.).
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**.
Compare Field	A numeric value or time stamp field from the table or view that identifies new events that are added to the table between queries. Enables the protocol to identify events that were previously polled by the protocol to ensure that duplicate events are not created.
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Start Date and Time	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value The maximum polling interval is one week.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 20,000.

Table 972. JDBC log source parameters for the Sybase ASE DSM (continued)	
Parameter	**Value**
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the **Credibility** of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select the **Coalescing Events** check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Store Event Payload	Select the **Store Event Payload** check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related tasks

"Adding a log source" on page 5

Chapter 155. Symantec

IBM QRadar supports a number of Symantec DSMs.

Symantec Critical System Protection

The IBM QRadar DSM for Symantec Critical System Protection can collect event logs from Symantec Critical System Protection systems.

The following table identifies the specifications for the Symantec Critical System Protection DSM.

Table 973. Symantec Critical System Protection DSM specifications

Specification	**Value**
Manufacturer	Symantec
DSM Name	Critical System Protection
RPM file name	`DSM-SymantecCriticalSystemProtection-`*`QRadar_version_build number`*`.noarch.rpm`
Supported versions	5.1.1
Event format	DB Entries
QRadar recorded event types	All events from the 'CSPEVENT_VW ' view
Log source type in QRadar UI	Symantec Critical System Protection
Auto discovered?	No
Includes identity?	No
Includes custom properties	No
For more information	Symantec Web Page (http://www.symantec.com/)

To integrate Symantec Critical System Protection with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most current version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Protocol-JDBC RPM
   - Symantec Critical System Protection RPM
2. For each Symantec Critical System Protection instance, configure Symantec Critical System Protection to enable communication with QRadar.

   Ensure that QRadar can poll the database for events by using TCP port 1433 or the port that is configured for your log source. Protocol connections are often disabled on databases and extra configuration steps are required in certain situations to allow connections for event polling. Configure firewalls that are located between Symantec Critical System Protection and QRadar to allow traffic for event polling.
3. If QRadar does not automatically discover Symantec Critical System Protection, create a log source for each Symantec Critical System Protection instance on the QRadar Console. The following table describes the parameters that require specific values to collect events from Symantec Critical System Protection:

Parameter	**Description**
Log Source Type	Symantec Critical System Protection

Parameter	Description
Protocol Configuration	JDBC
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	MSDE
Database Name	SCSPDB
IP or Hostname	The IP address or host name of the database server.
Port	Enter the JDBC port. The JDBC port must match the listener port that is configured on the remote database. The database must permit incoming TCP connections. The valid range is 1 - 65535. The defaults are: • MSDE - 1433 • Postgres - 5432 • MySQL - 3306 • Sybase - 1521 • Oracle - 1521 • Informix - 9088 • DB2 - 50000 If a database instance is used with the MSDE database type, you must leave the **Port** field blank.
Username	A user account for QRadar in the database.
Password	The password that is required to connect to the database.
Authentication Domain	If you did not select **Use Microsoft JDBC**, **Authentication Domain** is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance	SCSP

Parameter	Description
Predefined Query (Optional)	Select a predefined database query for the log source. If a predefined query is not available for the log source type, administrators can select the **none** option.
Table Name	CSPEVENT_VW
Select List	The list of fields to include when the table is polled for events. You can use a comma-separated list or type an asterisk (*) to select all fields from the table or view. If a comma-separated list is defined, the list must contain the field that is defined in the **Compare Field**.
Compare Field	EVENT_ID
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Start Date and Time (Optional)	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Enter the amount of time between queries to the event table. To define a longer polling interval, append H for hours or M for minutes to the numeric value The maximum polling interval is one week.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 20,000.
Use Named Pipe Communication	If you did not select **Use Microsoft JDBC**, **Use Named Pipe Communication** is displayed. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database.

Parameter	Description
Database Cluster Name	If you selected **Use Named Pipe Communication**, the **Database Cluster Name** parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure named pipe communication functions properly.
Use NTLMv2	If you did not select **Use Microsoft JDBC**, **Use NTLMv2** is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use Microsoft JDBC	If you want to use the Microsoft JDBC driver, you must enable **Use Microsoft JDBC**.
Use SSL	Select this option if your connection supports SSL. This option appears only for MSDE.
Microsoft SQL Server Hostname	If you selected **Use Microsoft JDBC** and **Use SSL**, the **Microsoft SQL Server Hostname** parameter is displayed. You must type the host name for the Microsoft SQL server.

For more information about configuring the JDBC protocol parameters, see c_logsource_JDBCprotocol.dita

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Symantec Data Loss Prevention (DLP)

The Symantec Data Loss Protection (DLP) DSM for IBM QRadar accepts events from a Symantec DLP appliance by using syslog.

Before you configure QRadar, you must configure response rules on your Symantec DLP. The response rule allows the Symantec DLP appliance to forward syslog events to QRadar when a data loss policy violation occurs. Integrating Symantec DLP requires you to create two protocol response rules (SMTP and None of SMTP) for QRadar. These protocol response rules create an action to forward the event information, using syslog, when an incident is triggered.

To configure Symantec DLP with QRadar, take the following steps:

1. Create an SMTP response rule.
2. Create a None of SMTP response rule.
3. Configure a log source in QRadar.
4. Map Symantec DLP events in QRadar.

Creating an SMTP response rule

You can configure an SMTP response rule in Symantec DLP.

Procedure

1. Log in to Symantec DLP user interface.
2. From the menu, select the **Manage** > **Policies** > **Response Rules**.
3. Click **Add Response Rule**.
4. Select one of the following response rule types:
   - **Automated Response** - Automated response rules are triggered automatically as incidents occur. It is the default value.
   - **Smart Response** - Smart response rules are added to the Incident Command screen and handled by an authorized Symantec DLP user.
5. Click **Next**.

   Configure the following values:
6. **Rule Name** - Type a name for the rule that you are creating. This name is descriptive enough for policy authors to identify the rule.

   For example, `QRadar Syslog SMTP`.
7. **Description** - Optional. Type a description for the rule that you are creating.
8. Click **Add Condition**.
9. On the **Conditions** panel, select the following conditions:
   - From the first list, select **Protocol or Endpoint Monitoring**.
   - From the second list, select **Is Any Of**.
   - From the third list, select **SMTP**.
10. On the **Actions** pane, click **Add Action**.
11. From the **Actions** list, select **All: Log to a Syslog Server**.
12. Configure the following options:
    a) **Host** - Type the IP address of your IBM QRadar.
13. **Port** - Type 514 as the syslog port.
14. **Message** -Type the following string to add a message for SMTP events.

```
LEEF:2.0|Symantec|DLP|2:medium|$POLICY$|||usrName=$SENDER$|duser=$RECIPIENTS$|
rules=$RULES$|matchCount=$MATCH_COUNT$|blocked=$BLOCKED$|incidentID=$INCIDENT_ID$|
incidentSnapshot=$INCIDENT_SNAPSHOT$|subject=$SUBJECT$|fileName=$FILE_NAME$|
parentPath=$PARENT_PATH$|path=$PATH$|quarantineParentPath=$QUARANTINE_PARENT_PATH$|
scan=$SCAN$|target=$TARGET${color}
```

15. **Level** - From this list, select **6 - Informational**.
16. Click **Save**.

What to do next

You can now configure your None Of SMTP response rule.

Creating a None Of SMTP response rule

You can configure a None Of SMTP response rule in Symantec DLP:

Procedure

1. From the menu, select the **Manage** > **Policies** > **Response Rules**.
2. Click **Add Response Rule**.

3. Select one of the following response rule types:
   - **Automated Response** - Automated response rules are triggered automatically as incidents occur. This is the default value.
   - **Smart Response** - Smart response rules are added to the Incident Command screen and handled by an authorized Symantec DLP user.
4. Click **Next**.

   Configure the following values:
5. **Rule Name** - Type a name for the rule you are creating. This name ideally is descriptive enough for policy authors to identify the rule. For example, `QRadar Syslog None Of SMTP`
6. **Description** - Optional. Type a description for the rule you are creating.
7. Click **Add Condition**.
8. On the **Conditions** pane, select the following conditions:
   - From the first list, select **Protocol or Endpoint Monitoring**.
   - From the second list, select **Is Any Of**.
   - From the third list, select **None Of SMTP**.
9. On the **Actions** pane, click **Add Action**.
10. From the **Actions** list, select **All: Log to a Syslog Server**.
11. Configure the following options:
    a) **Host** - Type the IP address of your QRadar.
12. `Port` - Type 514 as the syslog port.
13. **Message** -Type the following string to add a message for *None Of SMTP* events.

```
LEEF:1.0|Symantec|DLP|2:medium|$POLICY$|src=$SENDER$|dst=$RECIPIENTS$|
rules=$RULES$|matchCount=$MATCH_COUNT$|blocked=$BLOCKED$|incidentID=$INCIDENT_ID$|
incidentSnapshot=$INCIDENT_SNAPSHOT$|subject=$SUBJECT$|fileName=$FILE_NAME$|
parentPath=$PARENT_PATH$|path=$PATH$|quarantineParentPath=$QUARANTINE_PARENT_PATH$|
scan=$SCAN$|target=$TARGET$
```

14. **Level** - From this list, select **6 - Informational**.
15. Click **Save**.

What to do next

You are now ready to configure IBM QRadar.

Configuring a log source

You can configure the log source in IBM QRadar to receive events from a Symantec DLP appliance.

About this task

QRadar automatically detects syslog events for the SMTP and None of SMTP response rules that you create. However, if you want to manually configure QRadarto receive events from a Symantec DLP appliance:

Procedure

From the **Log Source Type** list, select the **Symantec DLP** option.

For more information about Symantec DLP, see your vendor documentation.

Related tasks

“Adding a log source” on page 5

Event map creation for Symantec DLP events

Event mapping is required for a number of Symantec DLP events. Due to the customizable nature of policy rules, most events, except the default policy events do not contain a predefined QRadar Identifier (QID) map to categorize security events.

You can individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track reoccurring events from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for Symantec DLP are categorized as unknown. *Unknown* events are easily identified as the **Event Name** column and **Low Level Category** columns display *Unknown*.

Discovering unknown events

As your device forwards events to IBM QRadar, it can take time to categorize all of the events for a device, as some events might not be generated immediately by the event source appliance or software.

About this task

It is helpful to know how to quickly search for *unknown* events. When you know how to search for *unknown* events, it is suggested you repeat this search until you are comfortable that you can identify most of your events.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select the log source group or **Other**.

   Log sources that are not assigned to a group are categorized as *Other*.
6. From the **Log Source** list, select your Symantec DLP log source.
7. Click **Add Filter**.

   The **Log Activity** tab is displayed with a filter for your log source.
8. From the **View** list, select **Last Hour**.

   Any events that are generated by the Symantec DLP DSM in the last hour are displayed. Events that are displayed as *unknown* in the **Event Name** column or **Low Level Category** column require event mapping in QRadar.

   Note: You can save your existing search filter by clicking **Save Criteria**.

What to do next

You can now modify the event map.

Modifying the event map

Modifying an event map gives you the option to manually categorize events to a QRadar Identifier (QID) map.

About this task

Any event that is categorized to a log source can be remapped to a new QRadar Identifier (QID).

Note: Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the **Log Source** column.

Procedure

1. On the **Event Name** column, double-click an *unknown* event for Symantec DLP.

   The detailed event information is displayed.
2. Click **Map Event**.
3. From the **Browse for QID** pane, select any of the following search options to narrow the event categories for a IBM QRadar Identifier (QID):
   a) From the **High-Level Category** list, select a high-level event categorization.

      For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *IBM QRadar Administration Guide*.
4. From the **Low-Level Category** list, select a low-level event categorization.
5. From the **Log Source Type** list, select a log source type.

   The **Log Source Type** list gives you the option to search for QIDs from other log sources. Searching for QIDs by log source is useful when events are similar to another existing network device. For example, Symantec provides policy and data loss prevention events, you might select another product that likely captures similar events.
6. To search for a QID by name, type a name in the **QID/Name** field.

   The **QID/Name** field gives you the option to filter the full list of QIDs for a specific word, for example, policy.
7. Click **Search**.

   A list of QIDs are displayed.
8. Select the QID you want to associate to your unknown event.
9. Click **OK**.

   Maps any additional events that are forwarded from your device with the same QID that matches the event payload. The event count increases each time that the event is identified by QRadar.

   If you update an event with a new QRadar Identifier (QID) map, past events that are stored in QRadar are not updated. Only new events are categorized with the new QID.

Symantec Endpoint Protection

The IBM QRadar DSM for Symantec Endpoint Protection collects events from a Symantec Endpoint Protection system.

The IBM® QRadar® DSM for Symantec Endpoint Protection parses events from Symantec Endpoint Protection System in the following languages: English, French, German, Italian, Japanese, Russian, and Polish.

The following table describes the specifications for the Symantec Endpoint Protection DSM:

Table 974. Symantec Endpoint Protection DSM specifications

Specification	Value
Manufacturer	Symantec
DSM name	Symantec Endpoint Protection
RPM file name	`DSM-SymantecEndpointProtection-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	Endpoint Protection V11, V12, and V14
Protocol	Syslog
Event format	Syslog

Table 974. Symantec Endpoint Protection DSM specifications (continued)	
Specification	**Value**
Recorded event types	All Audit and Security Logs
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Symantec website (https://www.symantec.com)

To integrate Symantec Endpoint Protection with QRadar , complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Symantec Endpoint Protection DSM RPM
2. Configure your Symantec Endpoint Protection device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Symantec Endpoint Protection log source on the QRadar Console.
4. Verify that QRadar is configured correctly.

   The following table shows a sample normalized event message from Symantec Endpoint Protection:

Table 975. Symantec Endpoint Protection sample message		
Event name	**Low level category**	**Sample log message**
Blocked	Access Denied	<51>Mar 3 13:52:13 <Server> SymantecServer: USER,<IP_address>, Blocked,[AC13-1.5] Block from loading other DLLs - Caller MD5=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx,Load Dll,Begin: 2017-03-03 13:48:18,End: 2017-03-03 13:48:18,Rule: Corp Endpoint - Browser Restrictions | [AC13-1.5] Block from loading other DLLs, 6804,C:/Program Files (x86)/Microsoft Office/Office14/WINPROJ.EXE,0,No Module Name,C:/Users/USER /AppData/Local/assembly/dl3/DMD7K4QX.8GW/WQ9LV1W4.8HL/e705c114/006fef9d_f364d101/ProjectPublisher2010.DLL,User: USER,Domain: LAB,Action Type: ,File size (bytes): 4216832,Device ID: SCSI\Disk&Ven_ATA&Prod_SAMSUNG_SSD_PM83\4&27c82505&0&000000

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Symantec Endpoint Protection to Communicate with QRadar

Before you can add the Symantec Endpoint Protection log source in QRadar, you need to configure your Symantec Endpoint Protection device to forward syslog events.

Procedure

1. Log in to your Symantec Endpoint Protection Manager system.

2. In the left pane, click the **Admin** icon.
3. In the bottom of the **View Servers** pane, click **Servers**.
4. In the **View Servers** pane, click **Local Site**.
5. In the **Tasks** pane, click **Configure External Logging**.
6. From the **Generals** tab, select the **Enable Transmission of Logs to a Syslog Server** check box.
7. In the **Syslog Server** field, type the IP address of your QRadar that you want to parse the logs.
8. In the **UDP Destination Port** field, type 514.
9. In the **Log Facility** field, type 6.
10. In the **Log Filter** tab, under **Management Server Logs**, select the **Audit Logs** check box.
11. In the **Client Log** pane, select the **Security Logs** check box.
12. In the **Client Log** pane, select the **Risks** check box.
13. Click **OK**.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Symantec Endpoint Protection sample event messages

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Symantec Endpoint Protection sample message when you use the Syslog protocol

The following sample event message shows a firewall block.

```
<51>Oct 3 23:51:53 symantec.endpointprotection.english.test SymantecServer: 20-11111A111111,
Event Description: The client will block traffic from IP address 10.33.146.1 for
the next 60 seconds (from 03/10/2019 23:51:04 to 03/10/2019 23:52:04). ,Local:
10.246.162.238,Local Host MAC: 000000000000,Remote Host Name: ,Remote Host IP:
10.33.146.1,Remote Host MAC: 000000000000,Inbound,OTHERS,,Begin: 2019-10-03 23:51:04,End:
2019-10-03 23:52:04,Occurrences: 1,Application: ,Location: Test Loc - VPN,User: A1111111,Domain:
TESTDOMAIN,Local Port: 0,Remote Port: 0,CIDS Signature ID: 0,CIDS Signature string: ,CIDS
Signature SubID: 0,Intrusion URL: ,Intrusion Payload URL: ,SHA-256: ,MD-5:
```

```
<51>Oct 3 23:51:53 symantec.endpointprotection.english.test SymantecServer:
20-11111A111111,Event Description: The client will block traffic from IP address
10.33.146.1 for the next 60 seconds (from 03/10/2019 23:51:04 to 03/10/2019
23:52:04). ,Local: 10.246.162.238,Local Host MAC: 000000000000,Remote Host Name: ,Remote
Host IP: 10.33.146.1,Remote Host MAC: 000000000000,Inbound,OTHERS,,Begin: 2019-10-03
23:51:04,End: 2019-10-03 23:52:04,Occurrences: 1,Application: ,Location: Test Loc - VPN,User:
A1111111,Domain: TESTDOMAIN,Local Port: 0,Remote Port: 0,CIDS Signature ID: 0,CIDS Signature
string: ,CIDS Signature SubID: 0,Intrusion URL: ,Intrusion Payload URL: ,SHA-256: ,MD-5:
```

Table 976. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**Event Description** (firewall block is extracted)
Source IP	**10.33.146.1**
Destination IP	**10.246.162.238**
Username	**A1111111**
Device Time	**2019-10-03 23:51:04**

Symantec Encryption Management Server

The Symantec Encryption Management Server DSM for IBM QRadar collects syslog events from Symantec Encryption Management Servers.

Symantec Encryption Management Server is formerly known as Symantec PGP Universal Server.

QRadar collects all relevant events from the following categories:

- Administration
- Software updates
- Clustering
- Backups
- Web Messenger
- Verified Directory
- Postfix
- Client logs
- Mail
- Whole Disk Encryption logs

Before you can integrate Symantec Encryption Management Server events with QRadar, you must configure Symantec Encryption Management Server to communicate with QRadar.

Related concepts

"Syslog log source parameters for Symantec Encryption Management Servers" on page 1528

Related tasks

"Configuring Symantec Encryption Management Server to communicate with QRadar" on page 1527
Enable external logging to forward syslog events to IBM QRadar.

"Adding a DSM" on page 4

Configuring Symantec Encryption Management Server to communicate with QRadar

Enable external logging to forward syslog events to IBM QRadar.

Procedure

1. In a web browser, log in to your Encryption Management server's administrative interface.

   `https://<Encryption Management Server IP address>:9000`
2. Click **Settings**.
3. Select the **Enable External Syslog** check box.
4. From the **Protocol** list, select either **UDP** or **TCP**.

   By default, QRadar uses port 514 to receive UDP syslog or TCP syslog event messages.
5. In the **Hostname** field, type the IP address of your QRadar Console or Event Collector.
6. In the `Port` field, type 514.
7. Click **Save**.

   The configuration is complete. The log source is added to QRadar as Symantec Encryption Management Server events are automatically discovered. Events that are forwarded to QRadar by the Symantec Encryption Management Servers are displayed on the **Log Activity** tab of QRadar.

Syslog log source parameters for Symantec Encryption Management Servers

If QRadar does not automatically detect the log source, add a Symantec Encryption Management Servers log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Symantec Encryption Management Servers:

Table 977. Syslog log source parameters for the Symantec Encryption Management Servers DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	**Symantec Encryption Management Server**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Symantec Encryption Management Server.

Related tasks

"Adding a log source" on page 5

Symantec SGS

The IBM QRadar DSM for Symantec Gateway Security (SGS) Appliance collects events from a Symantec Gateway Security (SGS) device|appliance|service.

QRadar records all relevant events from SGS. Before you configure QRadar to integrate with an SGS, you must configure syslog within your SGS appliance. For more information on Symantec SGS, see your vendor documentation.

After you configure syslog to forward events to QRadar, the configuration is complete. Events forward from Symantec SGS to QRadar using syslog are automatically discovered.

Related concepts

"Syslog log source parameters for Symantec SGS" on page 1528

Related tasks

"Adding a DSM" on page 4

Syslog log source parameters for Symantec SGS

If QRadar does not automatically detect the log source, add a Symantec SGS log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Symantec SGS:

Table 978. Syslog log source parameters for the Symantec SGS DSM

Parameter	Value
Log Source Name	Type a name for your log source
Log Source Description	Type a description for the log source.
Log Source Type	**Symantec Gateway Security (SGS) Appliance**

Table 978. Syslog log source parameters for the Symantec SGS DSM (continued)	
Parameter	**Value**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source.

Related tasks

"Adding a log source" on page 5

Symantec System Center

The Symantec System Center (SSC) DSM for IBM QRadar retrieves events from an SSC database by using a custom view that is created for QRadar.

QRadar records all SSC events. You must configure the SSC database with a user that has read and write privileges for the custom QRadar view to be able to poll the view for information. Symantec System Center (SSC) supports only the JDBC protocol.

Configuring a database view for Symantec System Center

A database view is required by the JDBC protocol to poll for SSC events.

Procedure

In the Microsoft SQL Server database that is used by the SSC device, configure a custom default view to support IBM QRadar:

Note: The database name must not contain any spaces.

- `CREATE VIEW dbo.vw_qradar AS SELECT`
- `dbo.alerts.Idx AS idx,`
- `dbo.inventory.IP_Address AS ip,`
- `dbo.inventory.Computer AS computer_name,`
- `dbo.virus.Virusname AS virus_name,`
- `dbo.alerts.Filepath AS filepath,`
- `dbo.alerts.NoOfViruses AS no_of_virus,`
- `dbo.actualaction.Actualaction AS [action],`
- `dbo.alerts.Alertdatetime AS [date],`
- `dbo.clientuser.Clientuser AS user_name FROM`
- `dbo.alerts INNER JOIN`
- `dbo.virus ON dbo.alerts.Virusname_Idx = dbo.virus.Virusname_Idx INNER JOIN`
- `dbo.inventory ON dbo.alerts.Computer_Idx = dbo.inventory.Computer_Idx INNER JOIN`
- `dbo.actualaction ON dbo.alerts.Actualaction_Idx =`
- `dbo.actualaction.Actualaction_Idx INNER JOIN`
- `dbo.clientuser ON dbo.alerts.Clientuser_Idx = dbo.clientuser.Clientuser_Idx`

What to do next

After you create your custom view, you must configure QRadar to receive event information by using the JDBC protocol.

JDBC log source parameters for Symantec System Center

If QRadar does not automatically detect the log source, add a Symantec System Center log source on the QRadar Console by using the JDBC protocol.

When using the JDBC protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect JDBC events from Symantec System Center:

Table 979. JDBC log source parameters for the Symantec System Center DSM

Parameter	Value
Log Source Name	Type a unique name for the log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source Type	**Symantec System Center**
Protocol Configuration	**JDBC**
Log Source Identifier	Type a name for the log source. The name can't contain spaces and must be unique among all log sources of the log source type that is configured to use the JDBC protocol. If the log source collects events from a single appliance that has a static IP address or host name, use the IP address or host name of the appliance as all or part of the **Log Source Identifier** value; for example, 192.168.1.1 or JDBC192.168.1.1. If the log source doesn't collect events from a single appliance that has a static IP address or host name, you can use any unique name for the **Log Source Identifier** value; for example, JDBC1, JDBC2.
Database Type	**MSDE**.
Database Name	Type `Reporting` as the name of the Symantec System Center database.
IP or Hostname	Type the IP address or host name of the Symantec System Center SQL Server.
Port	Type the port number that is used by the database server. The default port for MSDE is 1433. The JDBC configuration port must match the listener port of the Symantec System Center database. The Symantec System Center database must have incoming TCP connections that are enabled to communicate with QRadar. If you define a **Database Instance** when you use MSDE as the database type, you must leave the **Port** field blank in your configuration.
Username	Type the user name that is required to access the database.
Password	Type the password that is required to access the database. The password can be up to 255 characters in length.
Confirm Password	Confirm the password that is required to access the database. The confirmation password must be identical to the password entered in the **Password** field.

Table 979. JDBC log source parameters for the Symantec System Center DSM (continued)	
Parameter	**Value**
Authentication Domain	If you did not select **Use Microsoft JDBC**, **Authentication Domain** is displayed. The domain for MSDE that is a Windows domain. If your network does not use a domain, leave this field blank.
Database Instance	The database instance, if required. MSDE databases can include multiple SQL server instances on one server. When a non-standard port is used for the database or access is blocked to port 1434 for SQL database resolution, the **Database Instance** parameter must be blank in the log source configuration.
Table Name	Type `vw_qradar` as the name of the table or view that includes the event records.
Select List	Type * for all fields from the table or view. You can use a comma-separated list to define specific tables or views, if you need it for your configuration. The comma-separated list can be up to 255 alphanumeric characters in length. The list can include the following special characters: dollar sign ($), number sign (#), underscore (_), en dash (-), and period(.).
Compare Field	Type `idx` as the compare field. The compare field is used to identify new events that are added between queries to the table.
Use Prepared Statements	Prepared statements enable the JDBC protocol source to set up the SQL statement, and then run the SQL statement numerous times with different parameters. For security and performance reasons, most JDBC protocol configurations can use prepared statements.
Start Date and Time(Optional)	Type the start date and time for database polling in the following format: yyyy-MM-dd HH:mm with HH specified by using a 24-hour clock. If the start date or time is clear, polling begins immediately and repeats at the specified polling interval.
Polling Interval	Type the polling interval, which is the amount of time between queries to the event table. The default polling interval is 10 seconds. You can define a longer polling interval by appending H for hours or M for minutes to the numeric value. The maximum polling interval is 1 week in any time format. Numeric values that are entered without an H or M poll in seconds.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The default is 20,000 EPS.

Table 979. JDBC log source parameters for the Symantec System Center DSM (continued)	
Parameter	**Value**
Use Named Pipe Communication	If you did not select **Use Microsoft JDBC**, **Use Named Pipe Communication** is displayed. Clear the **Use Named Pipe Communication** check box. MSDE databases require the user name and password field to use a Windows authentication user name and password and not the database user name and password. The log source configuration must use the default that is named pipe on the MSDE database
Database Cluster Name	If you selected the **Use Named Pipe Communication** check box, the **Database Cluster Name** parameter is displayed. If you are running your SQL server in a cluster environment, define the cluster name to ensure Named Pipe communication functions properly.
Use NTLMv2	If you did not select **Use Microsoft JDBC**, **Use NTLMv2** is displayed. Select this option if you want MSDE connections to use the NTLMv2 protocol when they are communicating with SQL servers that require NTLMv2 authentication. This option does not interrupt communications for MSDE connections that do not require NTLMv2 authentication. Does not interrupt communications for MSDE connections that do not require NTLMv2 authentication.
Use Microsoft JDBC	If you want to use the Microsoft JDBC driver, you must enable **Use Microsoft JDBC**.
Use SSL	Select this option if your connection supports SSL.
Microsoft SQL Server Hostname	If you selected **Use Microsoft JDBC** and **Use SSL**, the **Microsoft SQL Server Hostname** parameter is displayed. You must type the host name for the Microsoft SQL server.

For a complete list of JDBC protocol parameters and their values, see c_logsource_JDBCprotocol.dita.

Note: Selecting a value greater than 5 for the **Credibility** parameter weights your Symantec System Center log source with a higher importance compared to other log sources in QRadar.

Related tasks

"Adding a log source" on page 5

Chapter 156. SysFlow

The IBM QRadar DSM for SysFlow collects syslog events from a SysFlow agent.

To integrate SysFlow with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - SysFlow DSM RPM
2. Configure your SysFlow agent to send events to QRadar. For more information, see Configuring SysFlow agent to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a SysFlow log source on the QRadar Console. For more information, see Syslog log source parameters for SysFlow.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

SysFlow DSM specifications

When you configure SysFlow, understanding the specifications for the SysFlow DSM can help ensure a successful integration. For example, knowing what the supported version of SysFlow is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the SysFlow DSM.

Table 980. SysFlow DSM specifications

Specification	**Value**
Manufacturer	SysFlow is an open source project initiated by IBM.
DSM name	SysFlow
RPM file name	DSM-*SysFlow-QRadar_version-build_number*.noarch.rpm
Supported version	1.0
Protocol	Syslog
Event format	JSON
Recorded event types	SysFlow
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	SysFlow Telemetry Pipeline Documentation (https://sysflow.readthedocs.io/en/latest/)

Configuring SysFlow agent to communicate with QRadar

To forward events to IBM QRadar, you must install a SysFlow collector by using OpenShift or Kubernetes cluster.

About this task

The SysFlow installation uses the OpenShift or Kubernetes operator. The operator uses custom resources to manage the SysFlow agent and it's associated components. This installation deploys the operator pod and then applies custom resources. When the custom resources are created, the operator deploys SysFlow agent pods to all worker nodes in the cluster. During the installation process, OpenShift or Kubernetes cluster downloads container images from the internet.

Procedure

1. Use SSH to log in as administrator to the master node of your OpenShift or Kubernetes cluster.
2. Download the SysFlow installation package and then extract the files.
3. Go to the root folder `sf-operator` of the extracted installation package, and then go to the `/scripts/run` directory.
4. To run the script, type the following command:

   ```
   cd scripts/run/
   ```
5. To deploy the operator, type the following command:

   ```
   ./deployOperator.sh
   ```
6. To deploy the SysFlow agent, type the following command:

   ```
   ./applyCR.sh <QRadar_Console_IP_address > 514 tcp
   ```

What to do next

If QRadar does not automatically detect the log source, add a SysFlow log source on the QRadar Console.

Syslog log source parameters for SysFlow

If IBM QRadar does not automatically detect the log source, add a SysFlow log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Syslog events from SysFlow:

Table 981. Syslog log source parameters for the SysFlow DSM

Parameter	Value
Log Source type	SysFlow
Protocol Configuration	Syslog
Log Source Identifier	SysFlow

For a complete list of common protocol parameters and their values, see Adding a log source.

Related tasks

Adding a log source

SysFlow sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

SysFlow sample message when you use the Syslog protocol

The following sample event message shows that a network connection is established from the `sip:sport` port to the `dip:dport` port.


```
{"version":"2","type":"NF","opflags":
["CONNECT","CLOSE"],"ret":0,"ts":1606893550815035002,"endts":1606893550820977528,"schema":2,"pro
c":{"acmdline":["/bin/nc -N 10.11.9.73 8080","/home/test /events.sh ./events.sh","/bin/bash
","/usr/sbin/sshd    ","/usr/sbin/sshd   ","/usr/sbin/sshd -D"],"aexe":["/bin/nc","/home/test/
events.sh","/bin/bash","/usr/sbin/sshd","/usr/sbin/sshd","/usr/sbin/sshd"],"aname":
["nc","events.sh","bash","sshd","sshd","sshd"],"apid":
["30994","30973","28002","28001","27997","945"],"args":"-N 10.11.9.73 8080","cmdline":"/bin/nc
-N 10.11.9.73 8080","createts":1606893550811545514,"entry":false,"exe":"/bin/
nc","gid":1001,"group":"","name":"nc","oid":"dbe8ba0d16effeb6","pid":30994,"tid":30994,"tty":1,"
uid":1001,"user":""},"pproc":{"args":"./events.sh","cmdline":"/home/test/events.sh ./
events.sh","createts":1606893550765789258,"entry":false,"exe":"/home/test/
events.sh","gid":1001,"group":"","name":"events.sh","oid":"c208bed1b606ad31","pid":30973,"tty":t
rue,"uid":1001,"user":""},"net":{"dip":"10.11.9.73","dport":8080,"ip":
["10.11.22.176","10.11.9.73"],"port":
["42944","8080"],"proto":6,"sip":"10.11.22.176","sport":42944},"flow":
{"rbytes":0,"rops":0,"wbytes":0,"wops":0},"node":{"id":"local","ip":"127.0.0.1"},"policies":
[{"id":"Process Created a Network Connection","desc":"Process Created a Network
Connection","priority":0,"tags":[]}]}
```


Table 982. Highlighted fields

QRadar field name	Highlighted field name
Event Category	**type**
Command	**CONNECT** + **0**
Device Time	**ts**
Username	**proc** + **user** (if not empty)
Source IP	**net** + **sip**
Source Port	**net** + **sport**
Destination IP	**net** + **dip**
Destination Port	**net** + **dport**
Protocol	**net** + **proto**

Chapter 157. ThreatGRID Malware Threat Intelligence Platform

The ThreatGRID Malware Threat Intelligence Platform DSM for IBM QRadar collects malware events by using the log file protocol or syslog.

QRadarsupports ThreatGRID Malware Threat Intelligence Platform appliances with v2.0 software that use the QRadar Log Event Extended Format (LEEF) Creation script.

Supported event collection protocols for ThreatGRID Malware Threat Intelligence

ThreatGRID Malware Threat Intelligence Platform writes malware events that are readable by IBM QRadar.

The LEEF creation script is configured on the ThreatGRID appliance and queries the ThreatGRID API to write LEEF events that are readable by QRadar. The event collection protocol your log source uses to collect malware events is based on the script you install on your ThreatGRID appliance.

Two script options are available for collecting LEEF formatted events:

- `Syslog` - The syslog version of the LEEF creation script allows your ThreatGRID appliance to forward events directly to QRadar. Events that are forwarded by the syslog script are automatically discovered by QRadar.
- `Log file` - The log file protocol version of the LEEF creation script allows the ThreatGRID appliance to write malware events to a file. QRadar uses the log file protocol to communicate with the event log host to retrieve and parse malware events.

The LEEF creation script is available from ThreatGRID customer support. For more information, see the ThreatGRID website http://www.threatgrid.com or email ThreatGRID support at support@threatgrid.com.

ThreatGRID Malware Threat Intelligence configuration overview

You can integrate ThreatGRID Malware Threat Intelligence events with IBM QRadar.

You must complete the following tasks:

1. Download the QRadar Log Enhanced Event Format Creation script for your collection type from the ThreatGRID support website to your appliance.
2. On your ThreatGRID appliance, install and configure the script to poll the ThreatGRID API for events.
3. On your QRadar appliance, configure a log source to collect events based on the script you installed on your ThreatGRID appliance.
4. Ensure that no firewall rules block communication between your ThreatGRID installation and the QRadar Console or managed host that is responsible for retrieving events.

Syslog log source parameters for ThreatGRID Malware Threat Intelligence Platform

If QRadar does not automatically detect the log source, add a ThreatGRID Malware Threat Intelligence Platform log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from ThreatGRID Malware Threat Intelligence Platform:

Table 983. Syslog log source parameters for the ThreatGRID Malware Threat Intelligence Platform DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source
Log Source Description	Type a description for the log source.
Log Source Type	**ThreatGRID Malware Intelligence Platform**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your ThreatGRID Malware Intelligence Platform. The log source identifier must be unique for the log source type.
Enabled	Select this check box to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this check box to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this check box to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the System Settings in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related tasks

"Adding a log source" on page 5

Log File log source parameters for ThreatGRID Malware Threat Intelligence Platform

If QRadar does not automatically detect the log source, add a ThreatGRID Malware Threat Intelligence Platform log source on the QRadar Console by using the Log File protocol.

When using the Log File protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Log File events from ThreatGRID Malware Threat Intelligence Platform:

Table 984. Log File log source parameters for the ThreatGRID Malware Threat Intelligence Platform DSM

Parameter	Value
Log Source Name	Type a name for your log source
Log Source Description	Type a description for the log source.
Log Source Type	**ThreatGRID Malware Intelligence Platform**
Protocol Configuration	**Log File**
Log Source Identifier	Type an IP address, host name, or name to identify the event source. The log source identifier must be unique for the log source type.
Service Type	From the list, select the protocol that you want to use to retrieve log files from a remote server. The default is SFTP. • **SFTP** - SSH File Transfer Protocol • **FTP** - File Transfer Protocol • **SCP** - Secure Copy Protocol The SCP and SFTP service type requires that the host server in the **Remote IP or Hostname** field has the SFTP subsystem enabled.
Remote IP or Hostname	Type the IP address or host name of the ThreatGRID server that contains your event log files.
Remote Port	Type the port number for the protocol that is selected to retrieve the event logs from your ThreatGRID server. The valid range is 1 - 65535. The list of default service type port numbers: • **FTP** - TCP Port 21 • **SFTP** - TCP Port 22 • **SCP** - TCP Port 22
Remote User	Type the user name that is required to log in to the ThreatGRID web server that contains your audit event logs. The user name can be up to 255 characters in length.

Table 984. Log File log source parameters for the ThreatGRID Malware Threat Intelligence Platform DSM (continued)

Parameter	Value
Remote Password	Type the password to log in to your ThreatGRID server.
Confirm Password	Confirm the password to log in to your ThreatGRID server
SSH Key File	If you select **SCP** or **SFTP** as the **Service Type**, use this parameter to define an SSH private key file. When you provide an **SSH Key File**, the **Remote Password** field is ignored.
Remote Directory	Type the directory location on the remote host from which the files are retrieved, relative to the user account you are using to log in. For FTP only. If your log files are in the remote user's home directory, you can leave the remote directory blank. Blank values in the **Remote Directory** field support systems that have operating systems where a change in the working directory (CWD) command is restricted.
Recursive	Select this check box if you want the file pattern to search sub folders in the remote directory. By default, the check box is clear. The **Recursive** parameter is ignored if you configure SCP as the **Service Type**.
FTP File Pattern	Type the regular expression (regex) required to filter the list of files that are specified in the Remote Directory. All files that match the regular expression are retrieved and processed. The FTP file pattern must match the name that you assigned to your ThreatGRID event log. For example, to collect files that start with `leef` or LEEF and ends with a text file extension, type the following value: `(leef|LEEF)+.*\.txt` Use of this parameter requires knowledge of regular expressions (regex). This parameter applies to log sources that are configured to use FTP or SFTP.
FTP Transfer Mode	If you select **FTP** as the **Service Type**, from the list, select ASCII. ASCII is required for text-based event logs.
SCP Remote File	If you select **SCP** as the **Service Type**, type the file name of the remote file.

Table 984. Log File log source parameters for the ThreatGRID Malware Threat Intelligence Platform DSM (continued)

Parameter	Value
Start Time	Type a time value to represent the time of day you want the log file protocol to start. The start time is based on a 24 hour clock and uses the following format: HH:MM. For example, type `00:00` to schedule the Log File protocol to collect event files at midnight. This parameter functions with the **Recurrence** field value to establish when your ThreatGRID server is polled for new event log files.
Recurrence	Type the frequency that you want to scan the remote directory on your ThreatGRID server for new event log files. Type this value in hours (H), minutes (M), or days (D). For example, type 2H to scan the remote directory every 2 hours from the start time. The default recurrence value is 1H. The minimum time interval is 15M.
Run On Save	Select this check box if you want the log file protocol to run immediately after you click **Save**. After the save action completes, the log file protocol follows your configured start time and recurrence schedule. Selecting **Run On Save** clears the list of previously processed files for the **Ignore Previously Processed File** parameter.
EPS Throttle	The maximum number of events per second that QRadar ingests. If your data source exceeds the EPS throttle, data collection is delayed. Data is still collected and then it is ingested when the data source stops exceeding the EPS throttle. The valid range is 100 to 5000.
Processor	From the list, select **NONE**. Processors allow event file archives to be expanded and processed for their events. Files are processed after they are downloaded. QRadar can process files in `zip`, `gzip`, `tar`, or `tar+gzip` archive format.

Table 984. Log File log source parameters for the ThreatGRID Malware Threat Intelligence Platform DSM (continued)

Parameter	Value
Ignore Previously Processed File(s)	Select this check box to track and ignore files that are already processed. QRadar examines the log files in the remote directory to determine whether the event log was processed by the log source. If a previously processed file is detected, the log source does not download the file. Only new or unprocessed event log files are downloaded by QRadar. This option applies to **FTP** and **SFTP** service types.
Change Local Directory?	Select this check box to define a local directory on your QRadar appliance to store event log files during processing. In most scenarios, you can leave this check box not selected. When this check box is selected, the **Local Directory** field is displayed. You can configure a local directory to temporarily store event log files. After the event log is processed, the events added to QRadar and event logs in the local directory are deleted.
Event Generator	From the **Event Generator** list, select **LineByLine**. The **Event Generator** applies extra processing to the retrieved event files. Each line of the file is a single event. For example, if a file has 10 lines of text, 10 separate events are created.

Related tasks

"Adding a log source" on page 5

Chapter 158. TippingPoint

IBM QRadar supports aa number of TippingPoint DSMs.

TippingPoint Intrusion Prevention System

The TippingPoint Intrusion Prevention System (IPS) DSM for IBM QRadar collects TippingPoint events by using the Syslog protocol.

QRadar records all relevant events from either a Local Security Management (LMS) device or multiple devices with a Security Management System (SMS).

Before you configure QRadar to integrate with TippingPoint, you must configure your device based on type:

- If you are using SMS, see “Configuring remote syslog for SMS ” on page 1543.
- If you are using LSM, see “Configuring notification contacts for LSM” on page 1544.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Configuring remote syslog for SMS

To configure SMS you must enable and configure your TippingPoint device to send events to a remote host by using syslog.

Before you begin

TippingPoint SMS V5.2.0 is supported in IBM QRadar.

Procedure

1. Log in to the TippingPoint system.
2. On the **Admin** Navigation menu, select **Server Properties**.
3. Select the **Management** tab.
4. Click **Add**.

   The **Edit Syslog Notification** window is displayed.
5. Select the **Enable** check box.
6. Configure the following values:
   a) **Syslog Server** - Type the IP address of the QRadar to receive syslog event messages.
   b) **Port** - Type 514 as the port address.
   c) **Log Type** - Select **SMS 2.0 / 2.1 Syslog format** from the list.
   d) **Facility** - Select **Log Audit** from the list.
   e) **Severity** - Select **Severity in Event** from the list.
   f) **Delimiter** - Select **TAB** as the delimiter for the generated logs.
   g) **Include Timestamp in Header** - Select **Use original event timestamp**.
   h) Select the **Include SMS Hostname in Header** check box.
   i) Click **OK**.
   j) You are now ready to configure the log source in QRadar.
7. To configure QRadar to receive events from a TippingPoint device: From the **Log Source Type** list, select the **TippingPoint Intrusion Prevention System (IPS)** option.

For more information about your TippingPoint device, see your vendor documentation.

Related tasks

"Adding a log source" on page 5

Configuring notification contacts for LSM

If you are using an LSM device, you need to configure LSM notification contacts.

Procedure

1. Log in to the TippingPoint system.
2. From the **LSM** menu, select **IPS** > **Action Sets**.

   The **IPS Profile - Action Sets** window is displayed.
3. Click the **Notification Contacts** tab.
4. In the **Contacts List**, click **Remote System Log**.

   The **Edit Notification Contact** page is displayed.
5. Configure the following values:
   a) **Syslog Server** - Type the IP address of the QRadar to receive syslog event messages.
   b) **Port** - Type 514 as the port address.
   c) **Alert Facility** - Select none or a numeric value 0-31 from the list. Syslog uses these numbers to identify the message source.
   d) **Block Facility** - Select none or a numeric value 0-31 from the list. Syslog uses these numbers to identify the message source.
   e) **Delimiter** - Select **TAB** from the list.
   f) Click **Add to table below**.
   g) Configure a Remote system log aggregation period in minutes.
6. Click **Save**.

   Note: If your QRadar is in a different subnet than your TippingPoint device, you might have to add static routes. For more information, see your vendor documentation.

What to do next

You are now ready to configure the action set for LSM, see "Configuring an Action Set for LSM" on page 1544.

Configuring an Action Set for LSM

If you are using LSM, you need to configure an action set for your LSM.

Procedure

1. Log in to the TippingPoint system.
2. From the **LSM** menu, select **IPS Action Sets**.

   The **IPS Profile - Action Sets** window is displayed.
3. Click **Create Action Set**.

   The **Create/Edit Action Set** window is displayed.
4. Type the Action Set Name.
5. For Actions, select a flow control action setting:
   - **Permit** - Allows traffic.
   - **Rate Limit** - Limits the speed of traffic. If you select Rate Limit, you must also select the desired rate.

- **Block** - Does not permit traffic.
- **TCP Reset** - When this is used with the *Block action*, it resets the source, destination, or both IP addresses of an attack. This option resets blocked TCP flows.
- **Quarantine** - When this is used with the *Block action*, it blocks an IP address (source or destination) that triggers the filter.

6. Select the **Remote System Log** check box for each action you that you select.
7. Click **Create**.

   You are now ready to configure the log source in QRadar.
8. To configure QRadar to receive events from a TippingPoint device: From the **Log Source Type** list, select the **TippingPoint Intrusion Prevention System (IPS)** option.

   For more information about your TippingPoint device, see your vendor documentation.

Related tasks

"Adding a log source" on page 5

TippingPoint X505/X506 Device

The TippingPoint X505/X506 DSM for IBM QRadar collects events by using syslog.

QRadar records all relevant system, audit, VPN, and firewall session events.

Configuring your TippingPoint X506/X506 device to communicate with QRadar

To retriev events in IBM QRadar, you must configure your TippingPoint X505/X506 device to send events to QRadar.

Procedure

1. Log in to your TippingPoint X505/X506 device.
2. From the **LSM** menu, select **System** > **Configuration** > **Syslog Servers**.

   The **Syslog Servers** window is displayed.
3. For each log type you want to forward, select a check box and type the IP address of your QRadar.

   Note: If your QRadar is in a different subnet than your TippingPoint device, you might have to add static routes. For more information, see your vendor documentation.

   You are now ready to configure the log source in QRadar.
4. To configure QRadar to receive events from a TippingPoint X505/X506 device: From the **Log Source Type** list, select the **TippingPoint X Series Appliances** option.

   Note: If you have a previously configured TippingPoint X505/X506 DSM installed and configured on your QRadar, the TippingPoint X Series Appliances option is still displayed in the **Log Source Type** list. However, for any new TippingPoint X505/X506 DSM that you configure, you must select the **TippingPoint Intrusion Prevention System (IPS)** option.

Related tasks

"Adding a log source" on page 5

TippingPoint Intrusion Prevention System sample event message

Use this sample event message to verify a successful integration with QRadar.

TippingPoint Intrusion Prevention System (IPS) sample message when you use the Syslog protocol

Important: Due to formatting issues, paste the message formats into a text editor and then remove any carriage return or line feed characters.

The following sample detects an attempt to use a memory corruption vulnerability in vulnerable installations of Microsoft Excel. The specific flaw exists in the way that Microsoft Excel parses certain Binary Interchange File Format (BIFF) structures. An attacker might use the vulnerability to gain remote code execution in the privilege context of the current user. User interaction is required in that a user must download a malicious file. For more information, see the Microsoft Security Bulletin (https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-030).

```
<170>Jun  5 23:28:27 XXXX 8    4    af268b55-9e4b-11e1-0cf4-4fcf2efeb4af
00000001-0001-0001-0001-0000000123
11    12311: HTTP: Microsoft Excel ObjectLink Memory Corruption Vulnerability    12311
tcp    <IP>    <PORT>
    <IP>    <PORT>    1    2A    2B    4    0    XXXX 1338938885045         130277955
```

Chapter 159. Top Layer IPS

The Top Layer IPS DSM for IBM QRadar accepts Top Layer IPS events by using syslog.

QRadar records and processes Top Layer events. Before you configure QRadar to integrate with a Top Layer device, you must configure syslog within your Top Layer IPS device. For more information on configuring Top Layer, see your Top Layer documentation.

The configuration is complete. The log source is added to QRadar as Top Layer IPS events are automatically discovered. Events that are forwarded to QRadar by Top Layer IPS are displayed on the **Log Activity** tab of QRadar.

To configure QRadar to receive events from a Top Layer IPS device:

From the **Log Source Type** list, select the **Top Layer Intrusion Prevention System (IPS)** option.

For more information about your Top Layer device, see your vendor documentation.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Chapter 160. Townsend Security LogAgent

IBM QRadar can collect CEF format events from Townsend Security LogAgent installations on IBM i infrastructure.

QRadar supports CEF events from Townsend Security software that is installed on IBM i V5.1 and above.

Supported event types

Townsend Security LogAgent installations on IBM i can write to forward syslog events for security, compliance, and auditing to QRadar.

All syslog events that are forwarded by Raz-Lee iSecurity automatically discover and the events are parsed and categorized with the IBM i DSM.

Configuring Raz-Lee iSecurity

To collect security and audit events, you must configure your Raz-Lee iSecurity installation to forward syslog events to IBM QRadar.

Procedure

1. Log in to the IBM i command-line interface.
2. Type the following command to access the audit menu options:

   STRAUD
3. From the **Audit** menu, select **81. System Configuration**.
4. From the **iSecurity/Base System Configuration** menu, select **31. SYSLOG Definitions**.
5. Configure the following parameters:
   a) **Send SYSLOG message** - Select **Yes**.
   b) **Destination address** - Type the IP address of QRadar.
   c) **"Facility" to use** - Type a facility level.
   d) **"Severity" range to auto send** - Type a severity level.
   e) **Message structure** - Type any additional message structure parameters that are needed for your syslog messages.

What to do next

Syslog events that are forwarded by Raz-Lee iSecurity are automatically discovered by QRadar by the IBM i DSM. In most cases, the log source is automatically created in QRadar after a few events are detected. If the event rate is low, then you might be required to manually create a log source for Raz-Lee iSecurity in QRadar.

Until the log source is automatically discovered and identified, the event type displays as *Unknown* on the **Log Activity** tab of QRadar.

Syslog log source parameters for Raz-Lee i Security

If QRadar does not automatically detect the log source, add a Raz_Lee i Security log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Raz-Lee i Security:

Table 985. Syslog log source parameters for the Raz-Lee i Security: DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	**IBM i**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your IBM i system with Raz-Lee iSecurity.

Related tasks

"Adding a log source" on page 5

Chapter 161. Trend Micro

IBM QRadar supports several Trend Micro DSMs.

Trend Micro Apex Central

The IBM QRadar DSM for Trend Micro Apex Central collects Syslog or TLS syslog events from a Trend Micro Apex Central device.

To integrate Trend Micro Apex Central with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Trend Micro Apex Central DSM RPM
2. Configure your Trend Micro Apex Central device to send events to QRadar. For more information, see Configuring Trend Micro Apex Central to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a Trend Micro Apex Central log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Trend Micro Apex Central DSM specifications

When you configure the Trend Micro Apex Central, understanding the specifications for the Trend Micro Apex Central DSM can help ensure a successful integration. For example, knowing what the supported version of Trend Micro Apex Central is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Trend Micro Apex Central DSM.

Table 986. Trend Micro Apex Central DSM specifications

Specification	Value
Manufacturer	Trend Micro
DSM name	Trend Micro Apex Central
RPM file name	DSM-*TrendMicroApexCentral-QRadar_version-build_number*.noarch.rpm
Supported version	1
Protocol	Syslog, TLS syslog
Event format	CEF

Table 986. Trend Micro Apex Central DSM specifications (continued)	
Specification	**Value**
Recorded event types	Attack discovery detection logs Behavior monitoring logs C&C callback logs Content security logs Data loss prevention logs Device access control logs Endpoint application control logs Engine update status log Intrusion prevention logs Network content inspection logs Pattern Update Status Logs Predictive machine learning logs Sandbox detection logs Spyware/Grayware logs Suspicious file logs Virus/Malware logs Web security logs
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Trend Micro Apex Central website (https://www.trendmicro.com/en_ca/business/technologies/control-manager.html)

Configuring Trend Micro Apex Central to communicate with QRadar

Configure your Trend Micro Apex Central device to forward Common Event Format (CEF) events to IBM QRadar.

Procedure

1. Log in to your Apex Central console as Administrator.
2. Configure the syslog settings.
   a) Click **Detections** > **Notifications** > **Notifications Method Settings**.
   b) In the **Syslog Settings** section, configure the following parameters:

Table 987. Syslog Settings parameters	
Parameter	**Value**
Server IP address	The IPv4 or IPv6 address of your syslog server.
Port	The port number of your syslog server.

Table 987. Syslog Settings parameters (continued)	
Parameter	**Value**
Facility	Select the facility code.

c) Click **Save**.

3. Enable syslog forwarding.

a) Click **Administration** > **Settings** > **Syslog Settings**.

b) Select the **Enable syslog forwarding** checkbox.

c) To send events to QRadar, configure the following syslog forwarding parameters:

Table 988. Syslog forwarding parameters	
Parameter	**Value**
Server address	The IP address of your QRadar Console or Event Collector.
Port	• SSL/TLS - 6514 (default port) • TCP - 514 • UDP - 514
Protocol	• SSL/TLS • TCP • UDP
Format	CEF
Log type	Select **Security logs** from the list, and then select the types of events that you want to forward to QRadar.

d) To test the connection, click **Test Connection**.

e) Click **Save**.

For more information about configuring Trend Micro Apex Central, see the Trend Micro Technical Support documentation (https://success.trendmicro.com/solution/000152501-SIEM-solutions-integration-with-Apex-Central#collapseTwo).

Syslog log source parameters for Trend Micro Apex Central

If IBM QRadar does not automatically detect the log source, add a Trend Micro Apex Central log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Syslog events from Trend Micro Apex Central:

Table 989. Syslog log source parameters for the Trend Micro Apex Central DSM	
Parameter	**Value**
Log Source type	Trend Micro Apex Central
Protocol Configuration	Syslog
Log Source Identifier	The IP address or host name for the log source.

For more information about common protocols and their values, see Adding a log source.

Related tasks
Adding a log source

TLS Syslog log source parameters for Trend Micro Apex Central

If IBM QRadar does not automatically detect the log source, add a Trend Micro Apex Central log source on the QRadar Console by using the TLS syslog protocol.

When you use the TLS syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect TLS syslog events from Trend Micro Apex Central:

Table 990. TLS syslog log source parameters for the Trend Micro Apex Central DSM

Parameter	Value
Log Source type	Trend Micro Apex Central
Protocol Configuration	**TLS Syslog**
Log Source Identifier	A unique name to identify the log source.
TLS Protocols	Select the version of TLS that is installed on the client.

For a complete list of TLS syslog protocol parameters and their values, see TLS syslog protocol configuration options.

Related tasks
Adding a log source

Trend Micro Apex Central sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Trend Micro Apex Central sample messages when you use the TLS syslog protocol

Sample 1: The following sample event message shows that a call back from source 10.201.86.187 to destination 10.201.86.195 is detected and blocked.

```
CEF:0|Trend Micro|Apex Central|2019|CnC:Block|CnC Callback|3|deviceExternalId=12 rt=Oct 11
2017 06:34:09 GMT+00:00 cat=1756 deviceFacility=Apex One cs2Label=EI_ProductVersion
cs2=11.0 shost=ApexOneClient01 src=10.201.86.187 cs3Label=SLF_DomainName cs3=DOMAIN
act=Block cn1Label=SLF_CCCA_RiskLevel cn1=1 cn2Label=SLF_CCCA_DetectionSource cn2=1
cn3Label=SLF_CCCA_DestinationFormat cn3=1 dst=10.201.86.195 deviceProcessName=C:\\Program Files
(x86)\\Internet Explorer\\iexplore.exe
```


```
CEF:0|Trend Micro|Apex Central|2019|CnC:Block|CnC Callback|3|deviceExternalId=12 rt=Oct
11 2017 06:34:09 GMT+00:00 cat=1756 deviceFacility=Apex One cs2Label=EI_ProductVersion
cs2=11.0 shost=ApexOneClient01 src=10.201.86.187 cs3Label=SLF_DomainName cs3=DOMAIN
act=Block cn1Label=SLF_CCCA_RiskLevel cn1=1 cn2Label=SLF_CCCA_DetectionSource cn2=1
cn3Label=SLF_CCCA_DestinationFormat cn3=1 dst=10.201.86.195 deviceProcessName=C:\\Program Files
(x86)\\Internet Explorer\\iexplore.exe
```


Table 991. QRadar field names and highlighted values in the event payload

QRadar field name	Highlighted values in the event payload
Event ID	**CnC:Block**
Source IP	**10.201.86.187**
Destination IP	**10.201.86.195**

Table 991. QRadar field names and highlighted values in the event payload (continued)	
QRadar field name	**Highlighted values in the event payload**
Device Time	**Oct 11 2017 06:34:09 GMT+00:00**

Sample 2: The following sample event message shows that a suspicious connection has occurred.

```
CEF:0|Trend Micro|Apex Central|2019|NCIE:Pass|SuspiciousConnection|3|deviceExternalId=1 rt=Oct 11
2017 06:34:06 GMT+00:00 cat=1756
deviceFacility=Apex One deviceProcessName=C:\\Windows\\system32\\svchost-1.exe act=Pass
src=10.201.86.152 dst=10.69.81.64 spt=54594 dpt=80 deviceDirection=None cn1Label=SLF_PatternType
cn1=2 cs2Label=NCIE_ThreatName cs2=Malicious_identified_CnC_querying_on_UDP_detected reason=F
```

```
CEF:0|Trend Micro|Apex Central|2019|NCIE:Pass|SuspiciousConnection|3|deviceExternalId=1 rt=Oct
11 2017 06:34:06 GMT+00:00 cat=1756 deviceFacility=Apex One deviceProcessName=C:\
\Windows\\system32\\svchost-1.exe act=Pass src=10.201.86.152 dst=10.69.81.64 spt=54594
dpt=80 deviceDirection=None cn1Label=SLF_PatternType cn1=2 cs2Label=NCIE_ThreatName
cs2=Malicious_identified_CnC_querying_on_UDP_detected reason=F
```

QRadar field name	Highlighted values in the event payload
Event ID	**NCIE:Pass**
Source IP	**10.201.86.152**
Source Port	**54594**
Destination IP	**10.69.81.64**
Destination Port	**80**
Device Time	**Oct 11 2017 06:34:06 GMT+00:00**

Trend Micro Apex One

A Trend Micro Apex One DSM for IBM QRadar accepts events by using SNMPv2.

Trend Micro Apex One is formerly known as Trend Micro OfficeScan. The name remains the same in QRadar.

QRadar records events relevant to virus and spyware events. Before you configure a Trend Micro device in QRadar, you must configure your device to forward SNMPv2 events.

QRadar has several options for integrating with a Trend Micro device. The integration option that you choose depends on your device version:

- “Integrating with Trend Micro Apex One 8.x ” on page 1555
- “Integrating with Trend Micro Apex One 10.x ” on page 1556
- “Integrating with Trend Micro Apex One XG ” on page 1558

Related concepts

“SNMPv2 log source parameters for Trend Micro Apex One” on page 1560

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Integrating with Trend Micro Apex One 8.x

You can integrate a Trend Micro Apex One 8.x device with IBM QRadar.

Procedure

1. Log in to the Apex One Administration interface.

2. Select **Notifications**.
3. Configure the General Settings for SNMP Traps: In the **Server IP Address** field, type the IP address of the QRadar.

   Note: Do not change the community trap information.
4. Click **Save**.
5. Configure the Standard Alert Notification: Select **Standard Notifications**.
6. Click the **SNMP Trap** tab.
7. Select the **Enable notification via SNMP Trap for Virus/Malware Detections** check box.
8. Type the following message in the field (this should be the default):

   ```
   Virus/Malware: %v Computer: %s Domain: %m File: %p Date/Time: %y Result: %a
   ```
9. Select the **Enable notification via SNMP Trap for Spyware/Grayware Detections** check box.
10. Type the following message in the field (this should be the default):

    ```
    Spyware/Grayware: %v Computer: %s Domain: %m Date/Time: %y Result: %a
    ```
11. Click **Save**.
12. Configure Outbreak Alert Notifications: Select **Out Notifications**.
13. Click the **SNMP Trap** tab.
14. Select the **Enable notification via SNMP Trap for Virus/Malware Outbreaks** check box.
15. Type the following message in the field (this should be the default):

    ```
    Number of viruses/malware: %CV Number of computers: %CC Log Type Exceeded:
    %A Number of firewall violation logs: %C Number of shared folder sessions:
    %S Time Period: %T
    ```
16. Select the **Enable notification via SNMP Trap for Spyware/Grayware Outbreaks** check box.
17. Type the following message in the field (this should be the default):

    ```
    Number of spyware/grayware: %CV Number of computers: %CC Log Type Exceeded:
    %A Number of firewall violation logs: %C Number of shared folder sessions:
    %S Time Period: %T
    ```
18. Click **Save**.

What to do next

Configure a log source in QRadar by using the SNMPv2 protocol. For more information, see "SNMPv2 log source parameters for Trend Micro Apex One" on page 1560.

Integrating with Trend Micro Apex One 10.x

Several preparatory steps are necessary before you configure IBM QRadar to integrate with a Trend Micro Apex One 10.x device.

About this task

You must:

1. Configure the SNMP settings for Trend Micro Apex One 10.x.
2. Configure standard notifications.
3. Configure outbreak criteria and alert notifications.

Configuring General Settings in Trend Micro Apex One

You can integrate a Trend Micro Apex One 10.x device with IBM QRadar.

Procedure

1. Log in to the Apex One Administration interface.
2. Select **Notifications** > **Administrator Notifications** > **General Settings**.
3. Configure the General Settings for SNMP Traps: In the **Server IP Address** field, type the IP address of your QRadar.
4. Type a community name for your Trend Micro Apex One device.
5. Click **Save**.

What to do next

You must now configure the Standard Notifications for Apex One.

Configure Standard Notifications in Trend Micro Apex One

You can configure standard notifications.

Procedure

1. Select **Notifications** > **Administrator Notifications** > **Standard Notifications**.
2. Define the Criteria settings. Click the **Criteria** tab.
3. Select the option to alert administrators on the detection of virus/malware and spyware/grayware, or when the action on these security risks is unsuccessful.
4. To enable notifications: Configure the **SNMP Trap** tab.
5. Select the **Enable notification via SNMP Trap** check box.
6. Type the following message in the field:

   ```
   Virus/Malware: %v Spyware/Grayware: %T Computer: %s IP address: %i Domain:
   %m File: %p Date/Time: %y Result: %a User name: %n
   ```

7. Click **Save**.

What to do next

You must now configure Outbreak Notifications.

Configuring Outbreak Criteria and Alert Notifications in Trend Micro Apex One

You can configure outbreak criteria and alert notifications for your Trend Micro Apex One device.

Procedure

1. Select **Notifications** > **Administrator Notifications** > **Outbreak Notifications**.
2. Click the **Criteria** tab.
3. Type the number of detections and detection period for each security risk.

   Notification messages are sent to an administrator when the criteria exceeds the specified detection limit.

   Note: Trend Micro suggests that you use the default values for the detection number and detection period.
4. Select **Shared Folder Session Link** and enable Apex One to monitor for firewall violations and shared folder sessions.

Note: To view computers on the network with shared folders or computers currently browsing shared folders, you can select the number link in the interface.

5. Click the **SNMP Trap** tab.
   a) Select the **Enable notification via SNMP Trap** check box.
6. Type the following message in the field:

```
Number of virus/malware: %CV Number of computers: %CC Log Type Exceeded: %A
Number of firewall violation logs: %C Number of shared folder sessions: %S
Time Period: %T
```

7. Click **Save**.

What to do next

Configure a log source in QRadar by using the SNMPv2 protocol. For more information, see "SNMPv2 log source parameters for Trend Micro Apex One" on page 1560.

Integrating with Trend Micro Apex One XG

You can integrate a Trend Micro Apex One XG device with the QRadar system.

About this task

Before you can integrate a Trend Micro Apex One XG device with the QRadar system you must configure the following items:

- SNMP settings for Trend Micro Apex One XG
- Administrator notifications
- Outbreak notifications

Configuring General Settings in Trend Micro Apex One XG

You can integrate a Trend Micro Apex One XG device with IBM QRadar.

Procedure

1. Log in to the Apex One Administration interface.
2. Click **Administration** > **Notifications** > **General Settings**.
3. Configure the General Notification Settings for SNMP Traps.
4. In the **Server IP Address** field, type the IP address of the QRadar Console.
5. Type a community name for your Trend Micro Apex One device.
6. Click **Save**.

What to do next

You must now configure the Administrator Notifications for Apex One.

Configuring Administrator Notifications in Trend Micro Apex One XG

Administrators can be notified when certain security risks are detected by Trend Micro Apex One XG. Configure the device to send notifications through SNMP Trap.

Procedure

1. Click **Administration** > **Notifications** > **Administrator**.
2. Click the **Criteria** tab.
3. Select the following options for notification:
   - Virus/Malware Detection

- Spyware/Grayware Detection
- C&C Callbacks

4. Optional: To enable notifications, configure the **SNMP Trap** tab.
5. Select the **Enable notification via SNMP Trap** check box.
6. Type the following message in the field:

```
Virus/Malware: %v Spyware/Grayware: %T Computer: %s IP address: %i Domain:
%m File: %p Date/Time: %y Result: %a User name: %n

Spyware/Grayware: %v Endpoint: %s Domain: %m Date/Time: %y Result: %a

Compromised Host: %CLIENTCOMPUTER% IP Address: %IP% Domain: %DOMAIN% Date/
Time: %DATETIME% Callback address: %CALLBACKADDRESS% C&C risk level:
%CNCRISKLEVEL% C&C list source: %CNCLISTSOURCE% Action: %ACTION%
```

7. Click **Save**.

What to do next

You must now configure Outbreak Notifications.

Configuring Outbreak Notifications in Trend Micro Apex One XG

You can configure your Trend Micro Apex One XG device to notify you of security risk outbreaks. Define an outbreak by the number of detections and the detection period.

Procedure

1. Click **Administration** > **Notifications** > **Outbreak**.
2. Click the **Criteria** tab.
3. Type the number of detections and detection period for each security risk.

   Note: Notification messages are sent to an administrator when the criteria exceeds the specified detection limit.

   Tip: Trend Micro suggests that you use the default values for the detection number and detection period.
4. To enable notifications, click the **SNMP Trap** tab, and select the **Enable notification via SNMP Trap** check box.
5. Type the following message in the field:

```
Number of virus/malware: %CV Number of computers: %CC

Number of spyware/grayware: %CV Number of endpoints: %CC

C&C callback detected: Accumulated log count: %C in the last %T hour(s)
```

6. Click **Save**.

What to do next

Configure a log source in QRadar by using the SNMPv2 protocol. For more information, see "SNMPv2 log source parameters for Trend Micro Apex One" on page 1560.

Changing the date format in QRadar to match the date format for your Trend Micro Apex One device

If your Trend Micro Apex One device uses the dd/MM/yyyy date format, you can enable this date format in IBM QRadar by using the DSM Editor.

By default, the Trend Micro Apex One DSM uses the dd/MM/yyyy date format.

Procedure

1. On the **Admin** tab, in the **Data Sources** section, click **DSM Editor**.
2. From the **Select Log Source Type** window, select **Trend Micro Office Scan** from the log source type list.
3. Click the **Configuration** tab, and then set **Display DSM Parameters Configuration** to on.
4. From the **Event Collector** list, select the event collector for the log source.
5. Set Use dd/MM/yyyy date format to on.
6. Click **Save**.

What to do next

Configure a log source in QRadar by using the SNMPv2 protocol. For more information, see SNMPv2 logsource parameters for Trend Micro Apex One.

SNMPv2 log source parameters for Trend Micro Apex One

If QRadar does not automatically detect the log source, add a Trend Micro Apex One log source on the QRadar Console by using the SNMPv2 protocol.

When using the SNMPv2 protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMPv2 events from Trend Micro Apex One:

Table 992. SNMPv2 log source parameters for the Trend Micro Apex One DSM

Parameter	Value
Log Source type	**Trend Micro Office Scan**
Log Source Description	A description for the log source.
Protocol Configuration	SNMPv2
Log Source Identifier	The IP address or host name for the log source can be used as an identifier for events from your Trend Micro Apex One appliance.
Community	The SNMP community name that is required to access the system that contains SNMP events. The default is Public.
Include OIDs in Event Payload	If selected, clear the **Include OIDs in Event Payload** check box. This option allows the SNMP event payload to be constructed by using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.

For a complete list of SNMPv2 protocol parameters and their values, see SNMPv2 protocol configuration options.

Related tasks

Adding a log source

Trend Micro Control Manager

You can integrate a Trend Micro Control Manager device with IBM QRadar.

Trend Micro Control Manager accepts events using SNMPv1, SNMPv2 and SNMPv3. Before you configure QRadar to integrate with a Trend Micro Control Manager device, you must configure a log source, then configure SNMP trap settings for your Trend Micro Control Manager.

SNMPv1 log source parameters for Trend Micro Control Manager

If QRadar does not automatically detect the log source, add a log source on the QRadar Console by using the SNMPv1 protocol.

When you use the SNMPv1 protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMPv1 events from Trend Micro Control Manager:

Table 993. SNMPv1 log source parameters for the Trend Micro Control Manager DSM

Parameter	Value
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	**Trend Micro Control Manager**
Protocol Configuration	**SNMPv1**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Trend Micro Control Manager appliance.
Community	Type the SNMP community name required to access the system containing SNMP events. The default is Public.
Include OIDs in Event Payload	Clear the **Include OIDs in Event Payload** check box, if selected. This options allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.

Related tasks

"Adding a log source" on page 5

SNMPv2 log source parameters for Trend Micro Control Manager

If QRadar does not automatically detect the log source, add a Trend Micro Control Manager log source on the QRadar Console by using the SNMPv2 protocol.

When you use the SNMPv2 protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMPv2 events from Trend Micro Control Manager:

Table 994. SNMPv2 log source parameters for the Trend Micro Control Manager DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	**Trend Micro Control Manager**
Protocol Configuration	**SNMPv2**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Trend Micro Control Manager appliance.
Community	Type the SNMP community name required to access the system containing SNMP events. The default is Public.
Include OIDs in Event Payload	Clear the **Include OIDs in Event Payload** check box, if selected. This options allows the SNMP event payload to be constructed using name-value pairs instead of the standard event payload format. Including OIDs in the event payload is required for processing SNMPv2 or SNMPv3 events from certain DSMs.

Related tasks

"Adding a log source" on page 5

SNMPv3 log source parameters for Trend Micro Control Manager

If QRadar does not automatically detect the log source, add a Trend Micro Control Manager log source on the QRadar Console by using the SNMPv3 protocol.

When you use the SNMPv3 protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect SNMPv3 events from Trend Micro Control Manager:

Table 995. SNMPv3 log source parameters for the Trend Micro Control Manager DSM	
Parameter	**Value**
Log Source Name	Type a name for your log source.
Log Source Description	Type a description for the log source.
Log Source Type	**Trend Micro Control Manager**
Protocol Configuration	**SNMPv3**
Log Source Identifier	Type a unique name for the log source.

For more information about SNMPv3 log source parameters, see SNMPv3 protocol configuration options.

Related tasks

"Adding a log source" on page 5

Configuring SNMP traps

You can configure SNMP traps for Trend Micro Control Manager. Versions v5.5 and v6.0 are supported.

Procedure

1. Log in to the Trend Micro Control Manager device.
2. Choose one of the following options based on the Trend Micro Control Manager version you're using:
   a) For v5.5, select **Administration** > **Settings** > **Event Center Settings**.

      Note: Trend Micro Control Manager v5.5 requires hotfix 1697 or hotfix 1713 after Service Pack 1 Patch 1 to provide correctly formatted SNMPv2c events. For more information, see your vendor documentation.

   b) For v6.0 and v7.0, select **Administration** > **Event Center** > **General Event Settings**.
3. Set the SNMP trap notifications: In the **SNMP Trap Settings** field, type the Community Name.
4. Type the IBM QRadar server IP address.
5. Click **Save**.

   You are now ready to configure events in the Event Center.
6. Choose one of the following options based on the Trend Micro Control Manager version you're using:
   a) For v5.5, select **Administration** > **Event Center**.
   b) For v6.0, select **Administration** > **Event Center** > **Event Notifications**.
7. From the **Event Category** list, expand **Alert**.
8. Click **Recipients** for an alert.
9. In **Notification methods**, select the **SNMP Trap Notification** check box.
10. Click **Save**.

    The **Edit Recipients Result** window is displayed.
11. Click **OK**.
12. Repeat “Configuring SNMP traps ” on page 1563 for every alert that requires an SNMP Trap Notification.

    The configuration is complete. Events from Trend Micro Control Manager are displayed on the **Log Activity** tab of QRadar. For more information about Trend Micro Control Manager, see your vendor documentation.

Trend Micro Deep Discovery Analyzer

The IBM QRadar DSM for Trend Micro Deep Discovery Analyzer collects event logs from your Trend Micro Deep Discovery Analyzer console.

The following table identifies the specifications for the Trend Micro Deep Discovery Analyzer DSM:

Table 996. Trend Micro Deep Discovery Analyzer DSM specifications

Specification	**Value**
Manufacturer	Trend Micro
DSM name	Trend Micro Deep Discovery Analyzer
RPM file name	DSM-TrendMicroDeepDiscoveryAnalyzer-QRadar_version-*build_number*.noarch.rpm
Supported versions	5.0, 5.5, 5.8 and 6.0
Event format	LEEF
QRadar recorded event types	All events

Table 996. Trend Micro Deep Discovery Analyzer DSM specifications (continued)	
Specification	**Value**
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Trend Micro website (http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html)

To send Trend Micro Deep Discovery Analyzer events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs from the IBM Support Website.
   - DSMCommon RPM
   - Trend Micro Deep Discovery Analyzer DSM
2. Configure your Trend Micro Deep Discovery Analyzer device to communicate with QRadar.
3. If QRadar does not automatically detect Trend Micro Deep Discovery Analyzer as a log source, create a Trend Micro Deep Discovery Analyzer log source on the QRadar Console. Configure all required parameters and use the following table to determine specific values that are required for Trend Micro Deep Discovery Analyzer event collection:

Table 997. Trend Micro Deep Discovery Analyzer log source parameters	
Parameter	**Value**
Log Source type	Trend Micro Deep Discovery Analyzer
Protocol Configuration	Syslog

Related tasks

Adding a DSM

Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar

To collect Trend Micro Deep Discovery Analyzer events, configure your third-party instance to enable logging.

Related information

Adding a log source

Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar

To collect Trend Micro Deep Discovery Analyzer events, configure your third-party instance to enable logging.

Procedure

1. Log in to the Deep Discovery Analyzer web console.
2. To configure Deep Discovery Analyzer V5.0, follow these steps:
   a) Click **Administration** > **Log Settings**.
   b) Select **Forward logs to a syslog server**.
   c) Select **LEEF** as the log format.
   d) Select the protocol that you want to use to forward the events.

e) In the **Syslog server** field, type the host name or IP address of your QRadar Console or Event Collector.

f) In the **Port** field, type 514.

3. To configure Deep Discovery Analyzer V5.5, follow these steps:

a) Click **Administration** > **Log Settings**.

b) Select **Send logs to a syslog server**.

c) In the **Server** field, type the host name or IP address of your QRadar Console or Event Collector.

d) In the **Port** field, type 514.

e) Select the protocol that you want to use to forward the events.

f) Select **LEEF** as the log format.

4. To configure Deep Discovery Analyzer V5.8 or V6.0, follow these steps:

a) Click **Administration** > **Integrated Products/Services** > **Log Settings**.

b) Select **Send logs to a syslog server**.

c) In the **Server address** field, type the host name or IP address of your QRadar console or Event Collector.

d) In the **Port** field, type the port number.

Note: Trend Micro suggests that you use the following default syslog ports: UDP: 514; TCP: 601; and SSL: 443.

e) Select the protocol that you want to use to forward the events; UDP/TCP/SSL.

f) Select **LEEF** as the log format.

g) Select the **Scope** of logs to send to the syslog server.

h) Optional: Select the **Extensions** check box if you want to exclude any logs from sending data to the syslog server.

5. Click **Save**.

Trend Micro Deep Discovery Director

The IBM QRadar DSM for Trend Micro Deep Discovery Director collects LEEF formatted events from a Trend Micro Deep Discovery Director device.

To integrate Trend Micro Deep Discovery Director with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:

- Trend Micro Deep Discovery Inspector DSM RPM
- Trend Micro Deep Discovery Director DSM RPM

2. Configure your Trend Micro Deep Discovery Director device to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a Trend Micro Deep Discovery Director log source on the QRadar Console. The following table describes the parameters that require specific values to collect Syslog events from Trend Micro Deep Discovery Director:

Table 998. Trend Micro Deep Discovery Director Syslog log source parameters

Parameter	Value
Log Source type	Trend Micro Deep Discovery Director
Protocol Configuration	Syslog

Table 998. Trend Micro Deep Discovery Director Syslog log source parameters (continued)	
Parameter	**Value**
Log Source Identifier	The IPv4 address or host name that identifies the log source. If your network contains multiple devices that are attached to a single management console, specify the IP address of the individual device that created the event. A unique identifier, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Trend Micro Deep Discovery Director DSM specifications

The following table describes the specifications for the Trend Micro Deep Discovery Director DSM.

Table 999. Trend Micro Deep Discovery Director DSM specifications	
Specification	**Value**
Manufacturer	Trend Micro
DSM name	Trend Micro Deep Discovery Director
RPM file name	DSM-*TrendMicroDeepDiscoveryDirector-QRadar_version-build_number*.noarch.rpm
Supported versions	3.0
Protocol	Syslog
Event format	LEEF
Recorded event types	Trend Micro Deep Discovery Inspector Events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Trend Micro Deep Discovery Director product information (http://docs.trendmicro.com/en-us/enterprise/deep-discovery-director.aspx)

Configuring Trend Micro Deep Discovery Director to communicate with QRadar

To collect events from Trend Micro Deep Discovery Director, configure your Trend Micro Deep Discovery Director device to forward syslog events to QRadar.

Procedure

1. Log in to your Trend Micro Deep Discovery Director device.
2. Click **Administration** > **Integrated Products/Services** > **Syslog**.
3. Click **Add**, and then select **Enabled**.
4. Configure the parameters in the following table.

Parameter	Description
Profile name	The name for the Deep Discovery Director syslog server.
Server address	The IP address of your QRadar Console or Event Collector.
Port	• SSL/TLS - 6514 (default port) • TCP - 601 • UDP - 514
Protocol	• SSL/TLS • TCP • UDP
Log format	LEEF
Scope	The events that you want to forward to QRadar.

5. Click **Save**.

Trend Micro Deep Discovery Director sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides sample event messages when you use the Syslog protocol for the Trend Micro Deep Discovery Director DSM:

Table 1000. Trend Micro Deep Discovery Director sample message supported by Trend Micro Deep Discovery Director.

Event name	Low-level category	Sample log message
DENYLIST _CHANGE	Successful Configuration Modification	`Oct 24 12:37:32 ddd35-1.ddxqa.com LEEF:1.0|Trend Micro|Deep Discovery Director|3.5.0.1174|DENYLIST _CHANGE|devTime=Oct 24 2018 12:37:32 GMT+08:00 devTimeFormat=MMM dd yyyy HH:mm:ss z sev=3 dvc=198.51.100.88 dvchost=ddd35 -1.ddxqa.com deviceMacAddress=00-00-5E-00-5 3-00 deviceGUID=C4AC760E-8721-4B46-B966-47B D419376D8 end=Jan 19 2038 11:14:07 GMT+08:0 0 act=Add type=Deny List IP/Port dst=198.51.100.55 deviceExternalRiskType=High pComp=UDSO`

Table 1000. Trend Micro Deep Discovery Director sample message supported by Trend Micro Deep Discovery Director. (continued)

Event name	Low-level category	Sample log message
SECURITY _RISK_ DETECTION	Potential Misc Exploit	<156>LEEF:1.0|Trend Micro|Deep Discovery Director|2.0.0.1129|SECURITY_RISK_DETECTION| Origin=Inspector devTimeFormat=MMM dd yyyy HH:mm:ss z ptype=IDS dvc=198.51.10065 device MacAddress=00-00-5E-00-53-00 dvchost=localhost deviceGUID=E77B0BE4474D-4413AF2F-752E-5810-1B11 devTime=May 25 2017 05:59:53 GMT+00:00 sev=8 origin=Inspector protoGroup=SQL proto=UDP vLAN Id=4095 deviceDirection=1 dhost=hit-nxdomain.o pendns.com dst=198.51.100.9 dstPort=1207 dstMAC =00:00:0c:07:ac:0 shost=198.51.100.22 src=198. 55.100.7 srcPort=1060 srcMAC=00:00:0c:07:ac:0 malName=OPS_HTTP_SASFIS_REQUEST malType=FRAUD sAttackPhase=Data Exfiltration fname=controller. php fileType=458757 fsize=520704 ruleId=328 msg =WEMON - HTTP (Request) deviceRiskConfidenceLevel =1 duser=username@example.com suser=username@ex ample.com mailMsgSubject=Mail Subject botCommand =msblast.exe botUrl=0005 channelName=#Infected chatUserName=fhkvmxya url=http://1.alisiosanguer a.com.cn/cgi-bin/forms.cgi requestClientApplicat ion=Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) pComp=VSAPI riskType=0 com pressedFileName=test_inarc mitigationTaskId=48b 3d717-f30f-4890-8627-50bf75fbb6aa srcGroup=Defa ult srcZone=1 dstGroup=Default dstZone=1 detect ionType=2 act=not blocked threatType=1 interest edIp=198.51.100.35 peerIp=198.51.100.8 fileHash =F1C9FCF4B2F74E8EE53B6C006A4977F798A4D872 sUser1 =srcusername1 sUser1LoginTime=Mar 09 2017 12:34: 56 GMT+00:00 sUser2=srcusername2 sUser2LoginTime =Mar 09 2017 12:34:56 GMT+00:00 sUser3=srcuserna me3 sUser3LoginTime=Mar 09 2017 12:34:56 GMT+00: 00 dUser1=dstusername1 dUser1LoginTime=Mar 09 20 17 12:34:56 GMT+00:00 dUser2=dstusername2 dUser 2LoginTime=Mar 09 2017 12:34:56 GMT+00:00 dUser 3=dstusername3 dUser3LoginTime=Mar 09 2017 12: 34:56 GMT+00:00 suid=TsGh{USA-XP}803469 * 0 : (null) hostName=datingtipstricks.info cnt=4 sOS Name=Windows dOSName=Windows aggregatedCnt=1 ccc aDestinationFormat=URL cccaDetectionSource=RELE VANCE_RULE cccaRiskLevel=1 cccaDestination=xili .zerolost.org cccaDetection=1 evtCat=Malware ev tSubCat=Grayware aptRelated=1 hackerGroup=defau lt hackingCampaign=IXESHE malFamily=ZEUS pAtta ckPhase=0 oldFileSize=65530 oldFileType=15073 28 oldFileHash=5A272B7441328E09704B6D7EABDBD5 1B8858FDE4 oldFileName=attachment

Trend Micro Deep Discovery Email Inspector

The IBM QRadar DSM for Trend Micro Deep Discovery Email Inspector collects events from a Trend Micro Deep Discovery Email Inspector device.

The following table describes the specifications for the Trend Micro Deep Discovery Email Inspector DSM:

Table 1001. Trend Micro Deep Discovery Email Inspector DSM specifications

Specification	Value
Manufacturer	Trend Micro

Table 1001. Trend Micro Deep Discovery Email Inspector DSM specifications (continued)	
Specification	**Value**
DSM name	Trend Micro Deep Discovery Email Inspector
RPM file name	DSM-TrendMicroDeepDiscoveryEmailInspector-*Qradar_version-build_number*.noarch.rpm
Supported versions	V3.0
Event format	Log Event Extended Format (LEEF)
Recorded event types	Detections Virtual analyzer analysis logs System events Alert events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Trend Micro website (http://www.trendmicro.ca)

To integrate Trend Micro Deep Discovery Email Inspector with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Trend Micro Deep Discovery Email Inspector DSM RPM
   - DSM Common RPM
2. Configure your Trend Micro Deep Discovery Email Inspector device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Trend Micro Deep Discovery Email Inspector log source on the QRadar Console. The following table describes the parameters that require specific values for Trend Micro Deep Discovery Email Inspector event collection:

Table 1002. Trend Micro Deep Discovery Email Inspector log source parameters	
Parameter	**Description**
Log Source type	Trend Micro Deep Discovery Email Inspector
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Trend Micro Deep Discovery Email Inspector to communicate with QRadar

To collect events from Trend Micro Deep Discovery Email Inspector, configure a syslog server profile for the IBM QRadar host.

Procedure

1. Log in to the Trend Micro Deep Discovery Email Inspector user interface.

2. Click **Administration** > **Log Settings**.
3. Click **Add**.
4. Verify that **Enabled** is selected for **Status**. The default is **Enabled**.
5. Configure the following parameters:

Parameter	Description
Profile name	Specify a name for the profile.
Syslog server	The host name or IP of the QRadar server.
Port	514
Log format	LEEF

6. Select **Detections**, **Virtual Analyzer Analysis logs**, and **System events** for the types of events to send to QRadar.

Trend Micro Deep Discovery Inspector

The IBM QRadar DSM for Trend Micro Deep Discovery Inspector can receive event logs from your Trend Micro Deep Discovery Inspector console.

The following table identifies the specifications for the Trend Micro Deep Discovery Inspector DSM:

Table 1003. Trend Micro Deep Discovery Inspector DSM specifications

Specification	Value
Manufacturer	Trend Micro
DSM name	Trend Micro Deep Discovery Inspector
RPM file name	`DSM-TrendMicroDeepDiscovery-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V3.0 to V3.8, V5.0 and V5.1
Event format	LEEF
QRadar recorded event types	Malicious content Malicious behavior Suspicious behavior Exploit Grayware Web reputation Disruptive application Sandbox Correlation System Update
Automatically discovered?	Yes
Included identity?	No
Includes custom properties?	No

Table 1003. Trend Micro Deep Discovery Inspector DSM specifications (continued)	
Specification	**Value**
More information	Trend Micro website (https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/inspector.html)

To send Trend Micro Deep Discovery Inspector events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs from the IBM Support Website:
   - DSMCommon RPM
   - Trend Micro Deep Discovery Inspector DSM
2. Configure your Trend Micro Deep Discovery Inspector device to send events to QRadar.
3. If QRadar does not automatically detect Trend Micro Deep Discovery Inspector as a log source, create a Trend Micro Deep Discovery Inspector log source on the QRadar Console. The following table shows the protocol-specific values for Trend Micro Deep Discovery Inspector event collection:

Table 1004. Trend Micro Deep Discovery Inspector log source parameters	
Parameter	**Value**
Log Source type	Trend Micro Deep Discovery Inspector
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Trend Micro Deep Discovery Inspector V3.0 to send events to QRadar

To collect Trend Micro Deep Discovery Inspector events, configure the device to send events to IBM QRadar.

Procedure

1. Log in to Trend Micro Deep Discovery Inspector.
2. From the navigation menu, select **Logs > Syslog Server Settings**.
3. Select **Enable Syslog Server**.
4. Configure the following parameters:

Parameter	Description
IP address	The IP address of your QRadar Console or Event Collector.
Port	514
Syslog facility	The local facility, for example, **local 3**.
Syslog severity	The minimum severity level that you want to include.
Syslog format	LEEF

5. In the **Detections** pane, select the check boxes for the events that you want to forward to QRadar.

6. Click **Save**.

Configuring Trend Micro Deep Discovery Inspector V3.8, V5.0 and V5.1 to send events to QRadar

To collect Trend Micro Deep Discovery Inspector events, configure the device to send events to IBM QRadar.

Procedure

1. Log in to Trend Micro Deep Discovery Inspector.
2. Click **Administration** > **Integrated Products/Services** > **Syslog**.
3. Click **Add**, and then select **Enable Syslog Server**.
4. Configure the following parameters:

Parameter	Description
Server Name or IP address	The IP address of your QRadar Console or Event Collector.
Port	514
Protocol	TCP
Facility level	Select a facility level that specifies the source of a message.
Severity level	Select a severity level of the type of messages to be sent to the syslog server.
Log format	LEEF

5. In the **Detections** pane, select the check boxes for the events that you want to forward to QRadar.
6. If you need proxy servers for your connections, select **Connect through a proxy server**. The device uses the settings that are configured in the **Administrator** > **System Settings** > **Proxy** screen.

   Note: If you require the use of proxy servers for intranet connections, select this option.
7. Click **Save**.

Trend Micro Deep Security

The IBM QRadar DSM for Trend Micro Deep Security can collect logs from your Trend Micro Deep Security server.

The following table identifies the specifications for the Trend Micro Deep Security DSM:

Table 1005. Trend Micro Deep Security DSM specifications

Specification	Value
Manufacturer	Trend Micro
DSM name	Trend Micro Deep Security
RPM file name	`DSM-TrendMicroDeepSecurity-`*`Qradar_version-build_number`*`.noarch.rpm`
Supported versions	V9.6.1532 to V12.0
Event format	Log Event Extended Format

Table 1005. Trend Micro Deep Security DSM specifications (continued)	
Specification	**Value**
Recorded event types	Anti-Malware Deep Security Firewall Integrity Monitor Intrusion Prevention Log Inspection System Web Reputation
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Trend Micro website (https://www.trendmicro.com/us/)

To integrate Trend Micro Deep Security with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - Trend Micro Deep Security DSM RPM
   - DSMCommon RPM
2. Configure your Trend Micro Deep Security device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Trend Micro Deep Security DSM log source on the QRadar Console. The following table describes the parameters that require specific values for Trend Micro Deep Security DSM event collection:

Table 1006. Trend Micro Deep Security DSM log source parameters	
Parameter	**Value**
Log Source type	Trend Micro Deep Security
Protocol Configuration	Syslog

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Configuring Trend Micro Deep Security to communicate with QRadar

To collect all events from Trend Micro Deep Security, you must specify IBM QRadar as the Syslog server and configure the Syslog format on your Trend Micro Deep Security device.

Before you begin

Ensure that Deep Security Manager is installed and configured on your Trend Micro Deep Security Device.

Procedure

1. Click **Administration** > **System Settings** > **SIEM**.
2. From the **System Event Notification** pane in the Manager section, enable the **Forward System Events to remote computer (via Syslog)** option.
3. Type the host name or the IP address of the QRadar system.
4. Type **514** for the UDP port.
5. Select the **Syslog Facility** that you want to use.
6. Select **LEEF** for the **Syslog Format**.

   Note: Trend Micro Deep Security sends events only in LEEF format from the Deep Security Manager. If you select the **Direct forward** option on the **SIEM** tab, you can't select **Log Event Extended Format 2.0** for the **Syslog Format**.

Trend Micro Deep Security sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

Trend Micro Deep Security sample message when you use the Syslog protocol

The following sample event message shows an attempt to scan a computer, or that a network was detected.

```
<182>Jul 14 01:32:31 trendmicro.deepsecurity.test LEEF:2.0|Trend Micro|Deep Security Mana
ger|11.0.221|851|cat=System    name=Reconnaissance Detected: Network or Port Scan    desc=The A
gent/Appliance detected an attempt to scan a computer or a network. Check the Agent/Appliance
Events
to see the details of the scan.    sev=6    src=192.168.187.196    usrName=qradar    targe
t=testTarget6    msg=The Agent/Appliance detected an attempt to scan a computer or a network. Chec
k the Agent/Appliance Events to see the details of the scan.    TrendMicroDsTenant=Primary    T
rendMicroDsTenantId=0
```

```
<182>Jul 14 01:32:31 trendmicro.deepsecurity.test LEEF:2.0|Trend Micro|Deep Security Manager|
11.0.221|851|cat=System    name=Reconnaissance Detected: Network or Port Scan    desc=The
Agent/Appliance detected an attempt to scan a computer or a network. Check the Agent/
Appliance Events to see the details of the scan.    sev=6    src=192.168.187.196
usrName=qradar    target=testTarget6    msg=The Agent/Appliance detected an attempt to scan a
computer or a network. Chek the Agent/Appliance Events to see the details of the scan.
TrendMicroDsTenant=Primary    TrendMicroDsTenantId=0
```

Chapter 162. Tripwire

The Tripwire DSM accepts resource additions, removal, and modification events by using syslog.

Procedure

1. Log in to the Tripwire interface.
2. On the left navigation, click **Actions**.
3. Click **New Action**.
4. Configure the new action.
5. Select **Rules** and click the rule that you want to monitor.
6. Select the **Actions** tab.
7. Make sure that the new action is selected.
8. Click **OK**.
9. Repeat Chapter 162, “Tripwire,” on page 1575 to Chapter 162, “Tripwire,” on page 1575 for each rule you want to monitor.

   You are now ready to configure the log source in QRadar.
10. To configure QRadar to receive events from a Tripwire device: From the **Log Source Type** list, select the **Tripwire Enterprise** option.

    For more information about your Tripwire device, see your vendor documentation.

Related tasks

“Adding a DSM” on page 4

“Adding a log source” on page 5

Chapter 163. Tropos Control

The Tropos Control DSM for IBM QRadar accepts events by using syslog.

About this task

QRadar can record all fault management, login and logout events, provisioning events, and device image upload events. Before you configure QRadar, you must configure your Tropos Control to forward syslog events.

You can configure Tropos Control to forward logs by using syslog to QRadar.

Procedure

1. Use an SSH to log in to your Tropos Control device as a root user.
2. Open the following file for editing:

   `/opt/ControlServer/ems/conf/logging.properties`
3. To enable syslog, remove the comment marker (#) from the following line:

   `#log4j.category.syslog = INFO, syslog`
4. To configure the IP address for the syslog destination, edit the following line:

   `log4j.appender.syslog.SyslogHost = <IP address>`

   Where <*IP address*> is the IP address or host name of QRadar.

   By default, Tropos Control uses a facility of **USER** and a default log level of **INFO**. These default settings are correct for syslog event collection from a Tropos Control device.
5. Save and exit the file.
6. You are now ready to configure the Tropos Control DSM in QRadar.

   To configure QRadar to receive events from Tropos Control:

   a) From the **Log Source Type** list, select **Tropos Control**.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Chapter 164. Universal CEF

The IBM QRadar DSM for Universal CEF accepts events from any device that produces events in the Common Event Format (CEF).

The following table identifies the specifications for the Universal CEF DSM:

Table 1007. Universal CEF DSM specifications

Specification	Value
DSM name	Universal CEF
RPM file name	DSM-UniversalCEF-*Qradar_version-build_number*.noarch.rpm
Protocol	Syslog Log File
Event Format	Common Event Format (CEF). CEF:0 is supported.
Recorded event types	CEF-formatted events
Automatically discovered?	No
Includes identity?	No
Includes custom properties?	No

To send events from a device that generates CEF-formatted events to QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
   - DSMCommon RPM
   - Universal CEF RPM
2. Add a Universal CEF log source on the QRadar Console. Use the following values that are specific to Universal CEF:

Parameter	Description
Log Source Type	Universal CEF
Protocol Configuration	Syslog or Log File

3. Configure your third-party device to send events to QRadar. For more information about how to configure your third-party device, see your vendor documentation.
4. Configure event mapping for Universal CEF events.

Configuring event mapping for Universal CEF events

Universal CEF events do not contain a predefined QRadar Identifier (QID) map to categorize security events. You must search for unknown events from the Universal CEF log source and map them to high and low-level categories.

Before you begin

Ensure that you installed the Universal CEF DSM and added log source for it in QRadar.

About this task

By default, the Universal CEF DSM categorizes all events as unknown. All Universal CEF events display a value of **unknown** in the **Event Name** and **Low Level Category** columns on the **Log Activity** tab. You must modify the QID map to individually map each event for your device to an event category in QRadar. Mapping events allows QRadar to identify, coalesce, and track events from your network devices.

For more information about event mapping, see the *IBM QRadar User Guide*.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select **Other**.
6. From the **Log Source** list, select your Universal CEF log source.
7. Click **Add Filter**.
8. From the **View** list, select **Last Hour**.
9. Optional: Click **Save Criteria** to save your existing search filter.
10. On the **Event Name** column, double-click an unknown event for your Universal CEF DSM.
11. Click **Map Event**.
12. From the Browse for QID pane, select any of the following search options to narrow the event categories for a QRadar Identifier (QID):
    - From the **High-Level Category** list, select a high-level event category. For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *IBM QRadar Administration Guide*.
    - From the **Low-Level Category** list, select a low-level event category.
    - From the **Log Source Type** list, select a log source type.

      Tip: Searching for QIDs by log source is useful when the events from your Universal CEF DSM are similar to another existing network device. For example, if your Universal CEF provides firewall events, you might select Cisco ASA, as another firewall product that likely captures similar events.
    - To search for a QID by name, type a name in the **QID/Name** field.
13. Click **Search**.
14. Select the QID that you want to associate to your unknown Universal CEF DSM event and click **OK**.

Chapter 165. Universal LEEF

The Universal LEEF DSM for IBM QRadar collects events from devices that produce events that use the Log Event Extended Format (LEEF).

The LEEF event format is a proprietary event format, which allows hardware manufacturers and software product manufacturers to read and map device events specifically designed for QRadar integration.

LEEF formatted events sent to QRadar outside of the partnership program require you to have installed the Universal LEEF DSM and manually identify each event forwarded to QRadar by mapping unknown events. The Universal LEEF DSM can parse events forwarded from syslog or files containing events in the LEEF format polled from a device or directory using the Log File protocol.

To configure events in QRadar using Universal LEEF, you must:

1. Configure a Universal LEEF log source in QRadar.
2. Send LEEF formatted events from your device to QRadar. For more information on forwarding events, see your vendor documentation.
3. Map unknown events to QRadar Identifiers (QIDs).

Syslog protocol log source parameters for Universal LEEF

Add a Universal LEEF log source on the QRadar Console by using the Syslog protocol.

QRadar receives events from a real-time source by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Universal LEEF:

Table 1008. Syslog log source parameters for the Universal LEEF DSM

Parameter	Value
Log Source type	Universal LEEF
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for Universal LEEF events.

Related tasks

Adding a log source

Forwarding events to IBM QRadar

After you create your log source, you can forward or retrieve events for QRadar. Forwarding events by using syslog might require more configuration of your network device.

As events are discovered by QRadar, either using syslog or polling for log files, events are displayed in the **Log Activity** tab. Events from the devices that forward LEEF events are identified by the name that you type in the **Log Source Name** field. The events for your log source are not categorized by default in QRadar and they require categorization. For more information on categorizing your Universal LEEF events, see “Universal LEEF event map creation” on page 1582.

Universal LEEF event map creation

Event mapping is required for the Universal LEEF DSM, because Universal LEEF events do not contain a predefined QRadar Identifier (QID) map to categorize security events.

Members of the SIPP Partner Program have QID maps designed for their network devices, whereby the configuration is documented, and the QID maps are tested by IBM Corp.

The Universal LEEF DSM requires that you individually map each event for your device to an event category in IBM QRadar. Mapping events allows QRadar to identify, coalesce, and track events that recur from your network devices. Until you map an event, all events that are displayed in the **Log Activity** tab for the Universal LEEF DSM are categorized as unknown. Unknown events are easily identified as the **Event Name** column and **Low-Level Category** columns display *Unknown*.

Discovering unknown events

As your device forwards events to IBM QRadar, it can take time to categorize all of the events from a device, because some events might not be generated immediately by the event source appliance or software.

About this task

It is helpful to know how to quickly search for unknown events. When you know how to search for unknown events, you can repeat this search until you are happy that most of your Universal LEEF events are identified.

Procedure

1. Log in to QRadar.
2. Click the **Log Activity** tab.
3. Click **Add Filter**.
4. From the first list, select **Log Source**.
5. From the **Log Source Group** list, select the log source group or **Other**.

   Log sources that are not assigned to a group are categorized as Other.
6. From the **Log Source** list, select your Universal LEEF log source.
7. Click **Add Filter**.

   The **Log Activity** tab is displayed with a filter for your Universal LEEF DSM.
8. From the **View** list, select **Last Hour**.

   Any events that are generated by your Universal LEEF DSM in the last hour are displayed. Events that are displayed as *unknown* in the **Event Name** column or **Low Level Category** column require event mapping in QRadar.

   Note: You can save your existing search filter by clicking **Save Criteria**.

   You are now ready to modify the event map for your Universal LEEF DSM.

Modifying an event map

Modifying an event map allows you to manually categorize events to a IBM QRadar Identifier (QID) map.

About this task

Any event categorized to a log source can be remapped to a new QRadar Identifier (QID). By default, the Universal LEEF DSM categorizes all events as unknown.

Note: Events that do not have a defined log source cannot be mapped to an event. Events without a log source display SIM Generic Log in the Log Source column.

Procedure

1. On the Event Name column, double-click an unknown event for your Universal LEEF DSM.

   The detailed event information is displayed.
2. Click **Map Event**.
3. From the Browse for QID pane, select any of the following search options to narrow the event categories for a QRadar Identifier (QID):
   a) From the **High-Level Category** list, select a high-level event categorization.

      For a full list of high-level and low-level event categories or category definitions, see the Event Categories section of the *IBM QRadar Administration Guide*.
4. From the **Low-Level Category** list, select a low-level event categorization.
5. From the **Log Source Type** list, select a log source type.

   The **Log Source Type** list allows you to search for QIDs from other individual log sources. Searching for QIDs by log source is useful when the events from your Universal LEEF DSM are similar to another existing network device. For example, if your Universal LEEF DSM provides firewall events, you might select Cisco ASA, as another firewall product that likely captures similar events.
6. To search for a QID by name, type a name in the **QID/Name** field.

   The QID/Name field allows you to filter the full list of QIDs for a specific word, for example, MySQL.
7. Click **Search**.

   A list of QIDs is displayed.
8. Select the QID you want to associate to your unknown Universal LEEF DSM event.
9. Click **OK**.

   QRadar maps any additional events forwarded from your device with the same QID that matches the event payload. The event count increases each time the event is identified by QRadar.

   Note: If you update an event with a new QRadar Identifier (QID) map, past events stored in QRadar are not updated. Only new events are categorized with the new QID.

Chapter 166. Vectra Networks Vectra

The IBM QRadar DSM for Vectra Networks Vectra collects events from the Vectra Networks Vectra X-Series platform.

Important: The IBM QRadar DSM for Vectra Networks Vectra is deprecated.

To continue taking advantage of this integration, please download the Vectra Networks Vectra DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/47f3e9afff5e0281d6684bb633d769f2).

The following table describes the specifications for the Vectra Networks Vectra DSM:

Table 1009. Vectra Networks Vectra DSM specifications

Specification	**Value**
Manufacturer	Vectra Networks
DSM name	Vectra Networks Vectra
RPM file name	`DSM-VectraNetworksVectra-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	2.2
Protocol	Syslog
Event Format	Common Event Format (CEF). CEF:0 is supported.
Recorded event types	Host scoring, command and control, botnet activity, reconnaissance, lateral movement, exfiltration
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Vectra Networks Website (http://www.vectranetworks.com)

To integrate Vectra Networks Vectra with QRadar, complete the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website (onto your QRadar Console in the order that they are listed:
   - DSMCommon RPM
   - Vectra Networks Vectra DSM RPM
2. Configure your Vectra Networks Vectra device to send syslog events to QRadar.
3. If QRadar does not automatically detect the log source, add a Vectra Networks Vectra log source on the QRadar Console. The following table describes the parameters that require specific values for Vectra Networks Vectra event collection:

Table 1010. Vectra Networks Vectra log source parameters

Parameter	**Value**
Log Source type	Vectra Networks Vectra
Protocol Configuration	Syslog
Log Source Identifier	A unique identifier for the log source.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring Vectra Networks Vectra to communicate with QRadar

To collect Vectra Networks Vectra events, configure the QRadar syslog daemon listener.

Before you begin

Important: The IBM QRadar DSM for Vectra Networks Vectra is deprecated.

To continue taking advantage of this integration, please download the Vectra Networks Vectra DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/47f3e9afff5e0281d6684bb633d769f2).

Procedure

1. Log in to the Vectra web console.
2. Click **settings** > **Notifications**.
3. In the **Syslog** section, click **Edit**.
4. Configure the following QRadar syslog daemon listener parameters:

Option	Description
Destination	The QRadar Event Collector IP address.
Port	514
Protocol	UDP
Format	CEF

Vectra Networks Vectra sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: The IBM QRadar DSM for Vectra Networks Vectra is deprecated.

To continue taking advantage of this integration, please download the Vectra Networks Vectra DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/47f3e9afff5e0281d6684bb633d769f2).

Tip: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Vectra Networks Vectra sample messages when you use the Syslog protocol

Sample 1: The following sample event message shows when samba is exploited.

```
<13>Jul  9 07:54:46 vectranetworks.vectra.test vectra_cef -: CEF:0|Vectra Networks|X Series|
4.2|smb_brute_force|SMB Brute-Force|7|externalId=9481 cat=LATERAL MOVEMENT dvc=10.97.41.41
dvchost=10.97.41.41 shost=hostname123.example.com src=10.125.64.136 flexNumber1Label=threat
flexNumber1=70 flexNumber2Label=certainty flexNumber2=59 cs4Label=Vectra Event URL cs4=https://
www.Qradar.test/paths/resources1.ext cs5Label=triaged cs5=False dst=10.160.0.145 dhost= proto=
dpt=445 out=None in=None start=1531119062000 end=1531119099000
```


```
<13>Jul  9 07:54:46 vectranetworks.vectra.test vectra_cef -: CEF:0|Vectra Networks|X Series|
4.2|smb_brute_force|SMB Brute-Force|7|externalId=9481 cat=LATERAL MOVEMENT dvc=10.97.41.41
dvchost=10.97.41.41 shost=hostname123.example.com src=10.125.64.136 flexNumber1Label=threat
flexNumber1=70 flexNumber2Label=certainty flexNumber2=59 cs4Label=Vectra Event URL cs4=https://
www.Qradar.test/paths/resources1.ext cs5Label=triaged cs5=False dst=10.160.0.145 dhost= proto=
dpt=445 out=None in=None start=1531119062000 end=1531119099000
```

Table 1011. Highlighted values in the Vectra Networks Vectra sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**SMB Brute-Force**
Event Category	**LATERAL MOVEMENT**
Source IP	**10.125.64.136**
Destination IP	**10.160.0.145**
Destination Port	**445**

Sample 2: The following sample event message shows that there is suspicious activity.

```
<13>Oct 22 07:17:40 vectranetworks.vectra.test vectra_cef -: CEF:0|Vectra Networks|X Series|
4.5|kerberos_account_anomaly|Suspicious Kerberos Account|1|externalId=13841 cat=LATERAL MOVEMENT
dvc=10.97.41.41 dvchost=10.97.41.41 shost=spek006odc src=10.97.48.6 flexNumber1Label=threat
flexNumber1=10 flexNumber2Label=certainty flexNumber2=95 cs4Label=Vectra Event URL cs4=https://
www.Qradar.test/paths/resources1.ext cs5Label=triaged cs5=False dst=10.160.0.90 dhost= proto=
dpt=80 out=None in=None start=1540183389000 end=1540185634000
```


```
<13>Oct 22 07:17:40 vectranetworks.vectra.test vectra_cef -: CEF:0|Vectra Networks|X Series|4.5|
kerberos_account_anomaly|Suspicious Kerberos Account|1|externalId=13841 cat=LATERAL MOVEMENT
dvc=10.97.41.41 dvchost=10.97.41.41 shost=spek006odc src=10.97.48.6 flexNumber1Label=threat
flexNumber1=10 flexNumber2Label=certainty flexNumber2=95 cs4Label=Vectra Event URL cs4=https://
www.Qradar.test/paths/resources1.ext cs5Label=triaged cs5=False dst=10.160.0.90 dhost= proto=
dpt=80 out=None in=None start=1540183389000 end=1540185634000
```


Table 1012. Highlighted values in the Vectra Networks Vectra sample event	
QRadar field name	**Highlighted values in the event payload**
Event ID	**Suspicious Kerberos Account**
Event Category	**LATERAL MOVEMENT**
Source IP	**10.97.48.6**
Destination IP	**10.160.0.90**
Destination Port	**80**

Chapter 167. Venustech Venusense

The Venustech Venusense DSM for IBM QRadar can collect events from Venusense appliances by using syslog.

QRadar records all relevant unified threat, firewall, or network intrusion prevention events that are forwarded by using syslog on port 514.

The following Venustech appliances are supported by QRadar:

- Venustech Venusense Security Platform
- Venusense Unified Threat Management (UTM)
- Venusense Firewall
- Venusense Network Intrusion Prevention System (NIPS)

Venusense configuration overview

IBM QRadar can collect events from Venustech appliances that are configured to forward filtered event logs in syslog format to QRadar.

The following process outlines the steps that are required to collect events from a Venusense Venustech appliance:

1. Configure the syslog server on your Venusense appliance.
2. Configure a log filter on your Venusense appliance to forward specific event logs.
3. Configure a log source in QRadar to correspond to the filtered log events.

Configuring a Venusense syslog server

To forward events to IBM QRadar, you must configure and enable a syslog server on your Venusense appliance with the IP address of your QRadar Console or Event Collector.

Procedure

1. Log in to the configuration interface for your Venusense appliance.
2. From the navigation menu, select **Logs** > **Log Configuration** > **Log Servers**.
3. In the **IP Address** field, type the IP address of your QRadar Console or Event Collector.
4. In the **Port** field, type 514.
5. Select the **Enable** check box.
6. Click **OK**.

What to do next

You are ready to configure your Venusense appliance to filter which events are forwarded to QRadar.

Configuring Venusense event filtering

Event filtering determines which events your Venusense appliance forwards to IBM QRadar.

Procedure

1. From the navigation menu, select **Logs** > **Log Configuration** > **Log Filtering**.
2. In the **Syslog Log** column, select a check box for each event log you want to forward to QRadar.
3. From the list, select a syslog facility for the event log you enabled.

4. Repeat “Configuring Venusense event filtering” on page 1589 and “Configuring Venusense event filtering” on page 1589 to configure any additional syslog event filters.
5. Click **OK**.

What to do next

You can now configure a log source for your Venusense appliance in QRadar. QRadar does not automatically discover or create log sources for syslog events from Venusense appliances.

Syslog log source parameters for Venustech Venusense

If QRadar does not automatically detect the log source, add a Venustech Venusense log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Venustech Venusense:

Table 1013. Syslog log source parameters for the Venustech Venusense DSM

Parameter	Value
Log Source type	Select your Venustech Venusense appliance from the list. The type of log source that you select is determined by the event filter that is configured on your Venusense appliance. The options include the following types: • **Venustech Venusense Security Platform** - Select this option if you enabled all event filter options. • **Venustech Venusense UTM** - Select this option if you enabled unified filtering events. • **Venustech Venusense Firewall** - Select this option if you enabled filtering for firewall events. • **Venustech Venusense NIPS** - Select this option if you enabled filtering for firewall events.
Protocol Configuration	Syslog
Log Source Identifier	The IP address or hostname for your Venusense appliance. The log source identifier must be a unique value.

Related tasks

“Adding a log source” on page 5

Chapter 168. Verdasys Digital Guardian

The Verdasys Digital Guardian DSM for IBM QRadar accepts and categorizes all alert events from Verdasys Digital Guardian appliances.

Verdasys Digital Guardian is a comprehensive Enterprise Information Protection (EIP) *platform*. Digital Guardian serves as a cornerstone of policy driven, data-centric security by enabling organizations to solve the information risk challenges that exist in today's highly collaborative and mobile business environment. Digital Guardian's endpoint agent architecture makes it possible to implement a data-centric security framework.

Verdasys Digital Guardian allows business and IT managers to:

- Discover and classify sensitive data by context and content.
- Monitor data access and usage by user or process.
- Implement policy driven information protection automatically.
- Alert, block, and record high risk behavior to prevent costly and damaging data loss incidents.

Digital Guardian's integration with QRadar provides context from the endpoint and enables a new level of detection and mitigation for Insider Threat and Cyber Threat (Advanced Persistent Threat).

Digital Guardian provides QRadar with a rich data stream from the end-point that includes: visibility of every data access by users or processes that include the file name, file classification, application that is used to access the data and other contextual variables.

The following table describes the specifications for the Verdasys Digital Guardian DSM:

Specification	**Value**
Manufacturer	Verdasys Digital Guardian
DSM name	**Verdasys Digital Guardian**
RPM file name	`DSM-VerdasysDigitalGuardian-`*`QRadar_version-Build_number`*`.noarch.rpm`
Supported versions	V6.1.x and V7.2.1.0248 with the QRadar LEEF format V6.0x with the Syslog event format
Protocol	Syslog, LEEF
Event format	Syslog
Recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	Digital Guardian website (https://digitalguardian.com)

Configuring IPtables

Before you configure your Verdasys Digital Guardian to forward events, you must configure IPtables in IBM QRadar to allow ICMP requests from Verdasys Digital Guardian.

Procedure

1. Use an SSH to log in to QRadar as the root user.

   Login: `root`

   Password: <*password*>
2. Type the following command to edit the `IPtables` file:

   ```
   vi /opt/qradar/conf/iptables.post
   ```

   The IPtables configuration file is displayed.
3. Type the following commands to allow QRadar to accept ICMP requests from Verdasys Digital Guardian:

   ```
   -I QChain 1 -m icmp -p icmp --icmp-type 8 --src <IP address> -j ACCEPT
   -I QChain 1 -m icmp -p icmp --icmp-type 0 --src <IP address> -j ACCEPT
   ```

   Where <*IP address*> is the IP address of your Verdasys Digital Guardian appliance. For example,

   ```
   -I QChain 1 -m icmp -p icmp --icmp-type 8 --src <Source_IP_address> -j
   ACCEPT
   -I QChain 1 -m icmp -p icmp --icmp-type 0 --src <Source_IP_address> -j
   ACCEPT
   ```

   Note: Make sure that you specify "`--icmp-type`" in the commands to avoid failures when you're upgrading the IPTables.
4. Save your `IPtables` configuration.
5. Type the following command to update `IPtables` in QRadar:

   ```
   /opt/qradar/bin/iptables_update.pl
   ```
6. To verify that QRadar accepts ICMP traffic from your Verdasys Digital Guardian, type the following command:

   ```
   iptables --list --line-numbers
   ```

   The following output is displayed:

   ```
   [root@Qradar bin]# iptables --list --line-numbers
   ```

   ```
   Chain QChain (1 references)
   ```

   ```
   num  target  prot         opt              source      destination
   ```

   ```
   1    ACCEPT  icmp   --    <IP address>   anywhere    icmp echo-reply
   ```

   ```
   2    ACCEPT  icmp   --    <IP address>   anywhere    icmp echo-request
   ```

   ```
   3    ACCEPT  tcp    --    anywhere         anywhere    state NEW tcp dpt:https
   ```

   ```
   4    ACCEPT  tcp    --    anywhere         anywhere    state NEW tcp dpt:http
   ```

   The IPtables configuration for QRadar is complete.

Configuring a data export

Data exports give you the option to configure the events Verdasys Digital Guardian forwards to IBM QRadar.

Procedure

1. Log in to the Digital Guardian Management Console.
2. Select **Workspace** > **Data Export** > **Create Export**.
3. From the **Data Sources** list, select **Alerts** or **Events** as the data source.
4. From the **Export type** list, select QRadar **LEEF**.

   If your Verdasys Digital Guardian is v6.0.x, you can select **Syslog** as the **Export Type**. QRadar LEEF is the preferred export type format for all Verdasys Digital Guardian appliances with v6.1.1 and later.
5. From the **Type** list, select **UDP** or **TCP** as the transport protocol.

   QRadar can accept syslog events from either transport protocol. If the length of your alert events typically exceeds 1024 bytes, then you can select **TCP** to prevent the events from being truncated.
6. In the **Server** field, type the IP address of your QRadar Console or Event Collector.
7. In the **Port** field, type 514.
8. From the **Severity Level** list, select a severity level.
9. Select the **Is Active** check box.
10. Click **Next**.
11. From the list of available fields, add the following Alert or Event fields for your data export:
    - **Agent Local Time**
    - **Application**
    - **Computer Name**
    - **Detail File Size**
    - **IP Address**
    - **Local Port**
    - **Operation** (required)
    - **Policy**
    - **Remote Port**
    - **Rule**
    - **Severity**
    - **Source IP Address**
    - **User Name**
    - **Was Blocked**
    - **Was Classified**
12. Select a Criteria for the fields in your data export and click **Next**.

    By default, the Criterion is blank.
13. Select a group for the criteria and click **Next**.

    By default, the Group is blank.
14. Click **Test Query**.

    A Test Query ensures that the database runs properly.
15. Click **Next**.
16. Save the data export.

    The configuration is complete.

What to do next

The data export from Verdasys Digital Guardian occurs on a 5-minute interval. You can adjust this timing with the job scheduler in Verdasys Digital Guardian, if required. Events that are exported to QRadar by Verdasys Digital Guardian are displayed on the **Log Activity** tab.

Syslog log source parameters for Verdasys Digital Guardian

If QRadar does not automatically detect the log source, add a Verdasys Digital Guardian log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Verdasys Digital Guardian:

Table 1014. Syslog log source parameters for the Verdasys Digital Guardian DSM

Parameter	Value
Log Source Name (Optional)	Type a name for your log source.
Log Source Description (Optional)	Type a description for the log source.
Log Source type	**Verdasys Digital Guardian**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Verdasys Digital Guardian appliance.

Related tasks

"Adding a log source" on page 5

Chapter 169. Vericept Content 360 DSM

The Vericept Content 360 DSM for IBM QRadar accepts Vericept events by using syslog.

About this task

QRadar records all relevant and available information from the event. Before you configure a Vericept device in QRadar, you must configure your device to forward syslog. For more information about configuring your Vericept device, consult your vendor documentation.

After you configure syslog to forward events to QRadar, the configuration is complete. The log source is added to QRadar as Vericept Content 360 events are automatically discovered. Events that are forwarded to QRadar by your Vericept Content 360 appliance are displayed on the **Log Activity** tab.

To manually configure a log source for QRadar to receive events from a Vericept device:

Procedure

From the **Log Source Type** list, select the **Vericept Content 360** option.

Related tasks

“Adding a DSM” on page 4
“Adding a log source” on page 5

Chapter 170. VMware

IBM QRadar supports a range of VMware products.

VMware AppDefense

The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

To integrate VMware AppDefense with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - Protocol-Common RPM
   - VMWare AppDefense API Protocol RPM
   - DSMCommon RPM
   - VMware AppDefense DSM RPM
2. Configure your VMware AppDefense device to send events to QRadar.
3. Add a VMware AppDefense log source that uses the VMWare AppDefense API protocol on the QRadar Console.

Related concepts

VMWare AppDefense API log source parameters for VMware AppDefense

VMware AppDefense sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

Related tasks

Configuring VMware AppDefense to communicate with QRadar

To send events to QRadar from your VMware AppDefense system, you must create a new API key on your VMware AppDefense system.

Related reference

VMware AppDefense DSM specifications

The following table describes the specifications for the VMware AppDefense DSM.

VMware AppDefense DSM specifications

The following table describes the specifications for the VMware AppDefense DSM.

Table 1015. VMware AppDefense DSM specifications

Specification	Value
Manufacturer	VMware
DSM name	VMware AppDefense
RPM file name	`DSM-VMwareAppDefense-`*`QRadar_version-build_number`*`.noarch.rpm`
Supported versions	V1.0
Protocol	VMWare AppDefense API
Event format	JSON
Recorded event types	All
Automatically discovered?	No

Table 1015. VMware AppDefense DSM specifications (continued)	
Specification	**Value**
Includes identity?	No
Includes custom properties?	No
More information	VMware website (https://cloud.vmware.com/appdefense)

Related concepts

VMware AppDefense

The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

Configuring VMware AppDefense to communicate with QRadar

To send events to QRadar from your VMware AppDefense system, you must create a new API key on your VMware AppDefense system.

Before you begin

Ensure that you have access to the Integrations settings in the VMware AppDefense user interface so that you can generate the Endpoint URL and API Key that are required to configure a log source in QRadar. You must have the correct user permissions for the VMware AppDefense user interface to complete the following procedure:

Procedure

1. Log in to your VMware AppDefense user interface.
2. From the navigation menu, click the icon to the right of your user name, and then select **Integrations**.
3. Click **PROVISION NEW API KEY**.
4. In the **Integration Name** field, type a name for your integration.
5. Select an integration from the **Integration Type** list.
6. Click **PROVISION**, and then record and save the following information from the message in the window that opens. You need this information when you configure a log source in QRadar:
   - **EndPoint URL**
   - **API Key** - This is the **Authentication Token** parameter value when you configure a log source in QRadar.

   Note: If you click **OK** or close the window, the information in the message can't be recovered.

Related concepts

VMware AppDefense

The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

VMWare AppDefense API log source parameters for VMware AppDefense

If QRadar does not automatically detect the log source, add a VMware AppDefense log source on the QRadar Console by using the VMWare AppDefense API protocol.

When using the VMWare AppDefense API protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect VMWare AppDefense API events from VMware AppDefense:

Table 1016. VMWare AppDefense API log source parameters for the VMware AppDefense DSM	
Parameter	**Value**
Log Source type	**VMware AppDefense**
Protocol Configuration	**VMWare AppDefense API**
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your VMware AppDefense devices.
Endpoint URL	The endpoint URL for accessing VMware AppDefense. Example revision: `https://server_name.vmwaredrx.com/partnerapi/v1/orgs/<organization ID>`
Authentication Token	A single authentication token that is generated by the AppDefense console and must be used for all API transactions.
Use Proxy	If QRadar accesses the VMWare AppDefense API by using a proxy, enable **Use Proxy**. If the proxy requires authentication, configure the **Hostname**, **Proxy Port**, **Proxy Username**, and **Proxy** fields. If the proxy does not require authentication, configure the **Hostname** and **Proxy Port** fields.
Automatically Acquire Server Certificates	If you choose **Yes** from the drop down list, QRadar automatically downloads the certificate and begins trusting the target server. If **No** is selected QRadar does not attempt to retrieve any server certificates.
Recurrence	Beginning at the Start Time, type the frequency for how often you want the remote directory to be scanned. Type this value in hours(H), minutes(M), or days(D). For example, 2H if you want the directory to be scanned every 2 hours. The default is 5M.
Throttle	The maximum number of events per second. The default is 5000.

Related concepts

VMware AppDefense

The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

Related tasks

Adding a log source

VMware AppDefense sample event messages

Use these sample event messages as a way of verifying a successful integration with QRadar.

The following table provides a sample event message when using the VMWare AppDefense API protocol for the VMware AppDefense DSM:

Table 1017. VMware AppDefense sample message supported by VMware AppDefense.

Event name	Low-level category	Sample log message
Inbound Connection Rule Violation	Firewall Deny	{"id":1111111,"createdAt":1512009263.471000000,"remediation": {"id":1111111},"severity":"CRITICAL","lastReceivedAt":1516170726.957000000,"count":2,"status":"UNRESOLVED","violationDetails": {"processHashSHA256":"1000000000000000000000000000000000000000000000000000000000000000","processHash":"10000000000000000000000000000000","cli":"<cli>","localPort":"<24","processPath":"","alert":"INBOUND_CONNECTION_RULES_VIOLATION","localAddress":"192.0.2.0","ipProtocol":"tcp","preEstablishedConnection":"FALSE"},"violatingVirtualMachine": {"id":1111111,"vmToolsStatus":"TOOLS_NOT_RUNNING","vcenterUuid":"11111111-1111-1111-1111-111111111111","vmUuid":"11111111-1111-1111-1111-111111111111","ipAddress":"192.0.2.0”,"osType":"WINDOWS","vmManageabilityStatus":"HOST_MODULE_ENABLED_AND_GUEST_MODULE_MISSING","guestAgentVersion":"1.0.1.0","macAddress":"<MacAddress>","guestId":"windows8","healthStatus":"CRITICAL","service": {"id":00000},"vmId":"1","guestAgentStatus":"Disconnected","guestName":"Microsoft Windows","guestStatus":"POWERED_OFF","name":"<name>","hostName":"<Hostname>"},"violatingProcess": {"processReputationProfile":null,"fullPathName":"System","<System>":"<System>","process256Hash":"1000000000000000000000000000000000000000000000000000000000000000","processMd5Hash":"10000000000000000000000000000000"},"subRuleViolated":null,"ruleViolated":"INBOUND_CONNECTION"}

Table 1017. VMware AppDefense sample message supported by VMware AppDefense. (continued)

Event name	Low-level category	Sample log message
Outbound Connection Rule Violation	Firewall Deny	{"id":10101001,"createdAt":1512009263.495000000,"remediation":{"id":1551519},"severity":"CRITICAL","lastReceivedAt":1516224258.818000000,"count":00001,"status":"UNRESOLVED","violationDetails":{"processHashSHA256":"0000000000000000000000000000000000000000000000000000000000000000","processHash":"00000000000000000000000000000000","cli":"C:\\<path>,"alert":"OUTBOUND_CONNECTION_RULES_VIOLATION","localAddress":"192.0.2.0","remotePort":"24","ipProtocol":"udp","preEstablishedConnection":"FALSE","remoteAddress":"0000::0:0"},"violatingVirtualMachine":{"id":101010,"vmToolsStatus":"TOOLS_NOT_RUNNING","vcenterUuid":"11111111-1111-1111-1111-111111111111","vmUuid":"11111111-1111-1111-1111-111111111111","ipAddress":"192.0.2.0","osType":"WINDOWS","vmManageabilityStatus":"HOST_MODULE_ENABLED_AND_GUEST_MODULE_MISSING","guestAgentVersion":"1.0.1.0","macAddress":"<MacAddress>","guestId":"windows8","healthStatus":"CRITICAL","service":{"id":28486},"vmId":"1","guestAgentStatus":"Disconnected","guestName":"Microsoft Windows","guestStatus":"POWERED_OFF","name":"<name>","hostName":"<host>"},"violatingProcess":{"processReputationProfile":{"processFileInfo":{"md5":"00000000000000000000000000000000","sha256":"0000000000000000000000000000000000000000000000000000000000000000","container":false,"executable":true,"ssdeep":"100:THGFJFJFHJY7y86gHK7GHk7ghjgkghjk","fileSizeBytes":1,"peFormat":true,"firstSeenName":"<fileName>","sha1":"0000000000000000000000000000000000000000","crc32":null},"peHeaderMetadata":{"companyName":"Microsoft Corporation","productName":"Microsoft Windows,"version":null,"originalName":"<host>","description":"<description>","fileVersion":"192.0.2.0,"codePage":null,"productVersion":"6.3.9600.17415","language":"English (U.S.)"},"certificate":{"commonName":"Windows","certificateexinfo":{"thumbprint":"0000000000000000000000000000000000000000","issuerThumbprint":"0000000000000000000000000000000000000000","serialNumber":null,"validToDate":1437604140.000000000,"validFromDate":1398205740.000000000,"publisher":null,"name":null}},"trust":10,"threat":0},"fullPathName":"C:\\<path>","process256Hash":"0000000000000000000000000000000000000000000000000000000000000000","processMd5Hash":"00000000000000000000000000000000"},"subRuleViolated":null,"ruleViolated":"OUTBOUND_CONNECTION"}

Related concepts

VMware AppDefense

The IBM QRadar DSM for VMware AppDefense collects events from a VMware AppDefense system.

VMware Carbon Black App Control (formerly known as Carbon Black Protection)

The IBM QRadar DSM for VMware Carbon Black App Control collects Syslog events from a Carbon Black App Control device.

To integrate Carbon Black App Control with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs from the IBM support website (http://www.ibm.com/support).
   - DSM Common RPM
   - Carbon Black App Control DSM RPM
2. Configure your Carbon Black App Control device to send events to QRadar. For more information, see Configuring VMware Carbon Black App Control to communicate with QRadar.
3. If QRadar does not automatically detect the log source, add a Carbon Black App Control log source on the QRadar Console. For more information, see Syslog log source parameters for VMware Carbon Black App Control.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

VMware Carbon Black App Control DSM specifications

When you configure the Carbon Black App Control DSM, understanding the specifications for the Carbon Black App Control DSM can help ensure a successful integration. For example, knowing what the supported version of Carbon Black App Control is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Carbon Black App Control DSM.

Table 1018. Carbon Black App Control DSM specifications

Specification	**Value**
Manufacturer	VMware
DSM name	Carbon Black App Control
RPM file name	DSM-*CarbonBlackProtection-QRadar_version-build_number*.noarch.rpm
Supported version	8.0.x to 8.5.x
Protocol	Syslog
Event format	LEEF
Recorded event types	computer management, server management, session management, policy management, policy enforcement, internal events, general management, discovery
Automatically discovered?	Yes
Includes identity?	Yes
Includes custom properties?	No
More information	VMware Carbon Black App Control (https://www.carbonblack.com/products/app-control/

Configuring VMware Carbon Black App Control to communicate with QRadar

Configure your Carbon Black App Control console to forward events to IBM QRadar in LEEF format.

Procedure

1. Access the Carbon Black App Control console by entering the Carbon Black App Control server URL in your browser.

2. Log in to the Carbon Black App Control console. You must have Administrator or Power® User privileges.
3. From the navigation menu, select **Administration** > **System Configuration**.
4. On the **System Configuration page**, click the **Events** tab.
5. In the **External Events Logging** section, click **Edit** and then configure the following parameters.
   a) Type the IP address of the QRadar Event Collector in the **Syslog address** field.
   b) Type 514 in the **Syslog port** field.
6. From the **Syslog format** list, select **LEEF (Q1Labs)**.
7. Select the **Syslog Enabled** checkbox and then click **Update**.

Syslog log source parameters for VMware Carbon Black App Control

If QRadar does not automatically detect the log source, add a Carbon Black App Control log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must configure.

The following table describes the parameters that require specific values to collect Syslog events from Carbon Black App Control:

Table 1019. Syslog log source parameters for the Carbon Black App Control DSM

Parameter	Value
Log Source type	Carbon Black App Control
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source as an identifier for metric events from your Carbon Black App Control appliances.

Related tasks

Adding a log source

VMware Carbon Black App Control sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Carbon Black App Control sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that a user logged out of a console.

```
LEEF:1.0|Carbon_Black|Protection|8.0.0.2141|Console_user_logout|cat=Session Management  sev=4
devTime=Mar 09 2017 18:32:11.110 UTC   msg=User 'admin' logged out.   externalId=22272
src=192.168.0.23   usrName=admin  dstHostName=tesla  receivedTime=Mar 09 2017 18:32:1    1.110 UTC
```


```
LEEF:1.0|Carbon_Black|Protection|8.0.0.2141|Console_user_logout|cat=Session Management  sev=4
devTime=Mar 09 2017 18:32:11.110 UTC   msg=User 'admin' logged out.   externalId=22272
src=192.168.0.23   usrName=admin  dstHostName=tesla  receivedTime=Mar 09 2017 18:32:1    1.110
UTC
```


Table 1020. Highlighted fields

QRadar field name	Highlighted field name
Event ID	**Console_user_logout** (Extracted from the LEEF header **Event ID** field in QRadar)

Table 1020. Highlighted fields (continued)	
QRadar field name	**Highlighted field name**
Event Category	**cat**
Severity	**sev**
Source IP	**src**
Username	**usrName**
Device Time	**devTime**

Sample 2: The following sample event message shows that a server configuration was modified. This sample event is from Carbon Black App Control 8.5x.

```
Sep  3 15:42:17 carbonblack.appcontrol.test 1 2020-09-03T15:42:17.378058-04:00 AJW2019-1
Carbon Black App Control 7972 15 - LEEF:1.0|VMware_Carbon_Black|App_Control|8.5.0.37|
Server_config_modified|cat=Server Management  sev=5  devTime=Sep 03 2020 19:42:11.033
UTC   msg=Configuration property 'syslogFormat' was changed from 'cef' to 'leef' by
'admin'. externalId=52  src=10.1.17.139    usrName=admin  dstHostName=tst2019-1.test.domain.test
receivedTime=Sep03 2020 19:42:11.033 UTC
```

```
Sep  3 15:42:17 carbonblack.appcontrol.test 1 2020-09-03T15:42:17.378058-04:00 AJW2019-1
Carbon Black App Control 7972 15 - LEEF:1.0|VMware_Carbon_Black|App_Control|8.5.0.37|
Server_config_modified|cat=Server Management  sev=5  devTime=Sep 03 2020 19:42:11.033 UTC
msg=Configuration property 'syslogFormat' was changed from 'cef' to 'leef' by 'admin'.
externalId=52  src=10.1.17.139    usrName=admin  dstHostName=tst2019-1.test.domain.test
receivedTime=Sep03 2020 19:42:11.033 UTC
```

Table 1021. Highlighted fields	
QRadar field name	**Highlighted field name**
Event ID	**Server_config_modified** (Extracted from the LEEF header **Event ID** field in QRadar)
Event Category	**cat**
Severity	**sev**
Source IP	**src**
Username	**usrName**
Device Time	**devTime**

VMware ESX and ESXi

The EMC VMware DSM for IBM QRadar collects ESX and ESXi server events by using the VMware protocol or the syslog protocol.

When you use the VMware protocol, the EMC VMware DSM supports events from VMware ESX or ESXi 3.x, 4.x, 5.x and 6.x servers.

When you use the syslog protocol, the EMC VMware DSM supports events from VMware ESX or ESXi 3.x, 4.x, 5.x and 6.x and 7.x servers.

To collect VMware ESX or ESXi events, you can select one of the following event collection methods:

- “Configuring syslog on VMware ESX and ESXi servers” on page 1605
- “Configuring the EMC VMWare protocol for ESX or ESXi servers” on page 1607

Configuring syslog on VMware ESX and ESXi servers

To collect syslog events for VMware, you must configure the server to forward events by using syslogd from your ESXi server to IBM QRadar.

Procedure

1. Log in to your VMware vSphere Client.
2. Select the host that manages your VMware inventory.
3. Click the **Configuration** tab.
4. From the **Software** pane, click **Advanced Settings**.
5. In the navigation menu, click **Syslog**.
6. Configure values for the following parameters:

Table 1022. VMware syslog protocol parameters

Parameter	ESX version	Description
`Syslog.Local.DatastorePath`	ESX or ESXi 3.5.x or 4.x	Type the directory path for the local syslog messages on your ESXi server. The default directory path is `[] /scratch/log/messages`.
`Syslog.Remote.Hostname`	ESX or ESXi 3.5.x or 4.x	Type the IP address or host name of QRadar.
`Syslog.Remote.Port`	ESX or ESXi 3.5.x or 4.x	Type the port number the ESXi server uses to forward syslog data. The default is port 514.
`Syslog.global.logHost`	ESXi v5.x, ESXi v6.x or ESXi v7.x	Type the URL and port number that the ESXi server uses to forward syslog data. Examples: udp://<*QRadar IP address*>:514 tcp://<*QRadar IP address*>:514

7. Click **OK** to save the configuration.

   The default firewall configuration on VMware ESXi v5.x. VMware ESXi v6.x and VMware ESXi v7.x servers, disable outgoing connections by default. Outgoing syslog connections that are disabled restrict the internal syslog forwarder from sending security and access events to QRadar.

Enabling syslog firewall settings on vSphere Clients

To forward syslog events from ESXi v5.x or ESXi v6.x servers, you must edit your security policy to enable outgoing syslog connections for events.

Procedure

1. Log in to your ESXi v5.x or ESXi v6.x server from a vSphere client.
2. From the **Inventory** list, select your ESXi Server.
3. Click the **Manage** tab and select **Security Profile**.
4. In the **Firewall** section, click **Properties**.
5. In the **Firewall Properties** window, select the **syslog** check box.

6. Click **OK**.

Enabling syslog firewall settings on vSphere Clients by using the esxcli command

To forward syslog events from ESXi v5.x or ESXi v6.x servers, as an alternative, you can configure ESXi Firewall Exception by using the esxcli command.

Note: To forward syslog logs, you might need to manually open the Firewall rule set. This firewall rule does not effect ESXi 5.0 build 456551. The UDP port 514 traffic flows.

To open outbound traffic through the ESXi Firewall on UDP port 514 and on TCP ports 514 and 1514, run the following commands:

```
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
```

```
esxcli network firewall refresh
```

Syslog log source parameters for VMware ESX or ESXi

If QRadar does not automatically detect the log source, add an EMC VMWare log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from VMware ESX or ESXi:

Table 1023. Syslog log source parameters for the EMC VMWare DSM

Parameter	Description
Log Source Name (Optional)	Type a name for your log source.
Log Source Type	**EMC VMWare**
Protocol Configuration	**Syslog**
Log Source Identifier	Type the IP address or hostname for the log source as an identifier for events from your EMC VMWare server.
Enabled	Select to enable the log source. By default, the check box is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the **System Settings** in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Table 1023. Syslog log source parameters for the EMC VMWare DSM (continued)	
Parameter	**Description**
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the **System Settings** in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

Related information

"Adding a log source" on page 5

Configuring the EMC VMWare protocol for ESX or ESXi servers

You can configure the EMC VMWare protocol to read events from your VMware ESXi server. The EMC VMWare protocol uses HTTPS to poll for ESX and ESXi servers for events.

About this task

Before you configure your log source to use the EMC VMWare protocol, it is suggested that you create a unique user to poll for events. This user can be created as a member of the root or administrative group, but you must provide the user with an assigned role of read-only permission. This ensures that IBM QRadar can collect the maximum number of events and retain a level of security for your virtual servers. For more information about user roles, see your VMware documentation.

To integrate EMC VMWare with QRadar, you must complete the following tasks:

1. Create an ESX account for QRadar.
2. Configure account permissions for the QRadar user.
3. Configure the EMC VMWare protocol in QRadar.

Creating a user who is not part of the root or an administrative group might lead to some events not being collected by QRadar. It is suggested that you create your QRadar user to include administrative privileges, but assign this custom user a read-only role.

Creating an account for QRadar in ESX

You can create a IBM QRadar user account for EMC VMWare to allow the protocol to properly poll for events.

Procedure

1. Log in to your ESX host by using the vSphere Client.
2. Click the **Local Users & Groups** tab.
3. Click **Users**.
4. Right-click and select **Add**.
5. Configure the following parameters:
   a) **Login** - Type a login name for the new user.
   b) **UID** - Optional. Type a user ID.
   c) **User Name** -Type a user name for the account.
   d) **Password** - Type a password for the account.

e) **Confirm Password** - Type the password again as confirmation.

f) **Group** - From the **Group** list, select **root**

6. Click **Add**.
7. Click **OK**.

Configuring read-only account permissions

For security reasons, configure your IBM QRadar user account as a member of your root or admin group, but select an assigned role of read-only permissions.

About this task

Read-only permission allows the QRadar user account to view and collect events by using the EMC VMWare protocol.

Procedure

1. Click the **Permissions** tab.
2. Right-click and select **Add Permissions**.
3. On the **Users and Groups** window, click **Add**.
4. Select your QRadar user and click **Add**.
5. Click **OK**.
6. From the **Assigned Role** list, select **Read-only**.
7. Click **OK**.

EMC VMWare log source parameters for VMware ESX or ESXi

If QRadar does not automatically detect the log source, add an EMC VMWare log source on the QRadar Console by using the EMC VMWare protocol.

When using the EMC VMWare protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect EMC VMWare events from VMware ESX or ESXi:

Table 1024. EMC VMWare protocol log source parameters for the EMC VMWare DSM

Parameter	Description
Log Source Name (Optional)	Type a name for your log source.
Log Source Type	**EMC VMWare**
Protocol Configuration	**EMC VMWare**
Log Source Identifier	Type the IP address or host name for the log source. This value must match the value that is configured in the **ESX IP** field.
VMware IP	Type the IP address of the VMware ESX or ESXi server. The VMware protocol *prepends* the IP address of your VMware ESX or ESXi server with HTTPS before the protocol requests event data.
User Name	Type the user name that is required to access the VMware server.
Password	Type the password that is required to access the VMware server.

For more information about the EMC VMWare protocol, see EMC VMware protocol configuration options.

Related information

"Adding a log source" on page 5

EMC VMWare sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

EMC VMWare sample message when you use the Syslog protocol

Sample 1: The following sample event messages shows that an event is generated by the *hostd* process on an ESXi/ESX host to report that a user is logged out.

```
<166>2019-05-21T19:27:32.479Z emc.vmware.test Hostd: info hostd[111111] [Originator@1111
sub=Vimsvc.ha-eventmgr opID=1a111a11 user=root] Event 136 : User root@10.21.120.237 logged
out (login time: Tuesday, 21 May, 2019 19:11:51, number of API invocations: 0, user agent:
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
10.0.3729.131 Safari/537.36)
```

Table 1025. Highlighted values in the EMC VMWare event

QRadar field name	Highlighted values in the event payload
Event ID	**User**
Source IP	**10.21.120.237**
Username	**root**
Identity IP	**10.21.120.237**
Identity Username	**root**

Sample 2: The following sample event message shows that a virtual machine (VM) is powered off.

```
1111111111111 emc.vmware.test LEEF:1.0|EMC|VMWare|1|VmPoweredOffEvent|usrName=userName
devTime=1369411554256    msg=example on  10.16.210.163 in company is powered off
```

Table 1026. Highlighted values in the EMC VMWare event

QRadar field name	Highlighted values in the event payload
Event ID	**VmPoweredOffEvent**
Source IP	**10.16.210.163**
Username	**userName**

Sample 3: The following sample event message shows that a user login session is in progress.

```
Dec 23 14:43:56 172.16.210.175 LEEF:1.0|EMC|VMWare|1|UserLoginSessionEvent|usrName=root
src=172.16.210.35    msg=User root@172.16.210.35 logged in
```

Table 1027. Highlighted values in the EMC VMWare event

QRadar field name	Highlighted values in the event payload
Event ID	**UserLoginSessionEvent**
Source	**172.16.210.35**
Destination IP	**172.16.210.175**

Table 1027. Highlighted values in the EMC VMWare event (continued)	
QRadar field name	**Highlighted values in the event payload**
Username	**root**

VMware vCenter

The VMware vCenter DSM for IBM QRadar collects vCenter server events by using the EMC VMWare protocol.

The EMC VMware protocol uses HTTPS to poll for vCenter appliances for events. You must configure a log source in QRadar to collect VMware vCenter events. For more information about configuring EMC VMWare log source parameters, see "EMC VMWare log source parameters for VMware vCenter" on page 1610.

Before you configure your log source to use the EMC VMWare protocol, it is suggested that you create a unique user to poll for events. This user can be created as a member of the Linux root or Windows administrative group, but you must provide the user with an assigned role of read-only permission in vSphere. This ensures that QRadar can collect the maximum number of events and retain a level of security for your virtual servers. For more information about user roles, see your VMware documentation.

EMC VMWare log source parameters for VMware vCenter

Add a VMware vCenter log source on the QRadar Console by using the EMC VMWare protocol.

When using the EMC VMWare protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect EMC VMWare events from VMware vCenter:

Table 1028. EMC VMWare log source parameters for the VMware vCenter DSM	
Parameter	**Description**
Log Source type	**VMware vCenter**
Protocol Configuration	**EMC VMWare**
Log Source Identifier	Type the IP address or host name for the log source. This value must match the value that is configured in the **ESX IP** field.
VMware IP	Type the IP address of the VMware vCenter server. The EMC VMWare protocol appends the IP address of your VMware vCenter server with HTTPS before the protocol requests event data.
User Name	Type the user name that is required to access the VMware vCenter server.
Password	Type the password that is required to access the VMware vCenter server.

For more information about EMC VMWare protocol parameters, see "EMC VMware protocol configuration options" on page 116.

Related information

"Adding a log source" on page 5

VMware vCenter sample event message

Use this sample event message to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage returns or line feed characters.

VMware vCenter sample message when you use the EMC VMWare protocol

Sample 1: The following sample event message shows that a user is granted access to the specified resource.

```
<142>Apr 14 08:33:05 vmware.vcenter.test - UserId : aaaaaa-111-111-1111-aaaa-
qqqqqq, UserName : admin, AuthSource : LOCAL, Session : aaaaaa-111-111-1111-aaaa-
qqqqqq::952f4613-9416-4769-9ba4-7ec5ce73ab85, Category : ACCESS_GRANTED - Access to
\"metadata.resourceKind.get\" is granted
```

Table 1029. Highlighted fields in the VMware vCenter event

QRadar field name	Highlighted values in the event payload
Event ID	**ACCESS_GRANTED**
Username	**admin**

Sample 2: The following sample event message shows a user login session event.

```
<14>1 2020-10-07T13:00:44.136034+02:00 vmware.vcenter.test vpxd 4188 - -  Event [420537] [1-1]
[2020-10-07T11:00:44.13551Z] [vim.event.UserLoginSessionEvent] [info] [TEST1.TEST\\vpxd-ext] []
[420537] [User TEST1.TEST\\vpxd-ext logged in as VMware vim-java 1.0]
```

Table 1030. Highlighted fields in the VMware vCenter event

QRadar field name	Highlighted values in the event payload
Event ID	**UserLoginSessionEvent**
Username	**TEST1.TEST\\vpxd-ext**

VMware vCloud Director

You can use the VMware vCloud Director DSM and the VMware vCloud Director protocol for IBM QRadar to poll the vCloud REST API for events.

QRadar supports polling for VMware vCloud Director events from vCloud Directory 5.1 appliances. Events that are collected by using the vCloud REST API are assembled as Log Event Extended Format (LEEF) events.

To integrate vCloud events with QRadar, you must complete the following tasks:

1. On your vCloud appliance, configure a public address for the vCloud REST API.
2. On your QRadar appliance, configure a log source to poll for vCloud events. For information about NMware vCloud Director log source protocol parameters, see “VMware vCloud Director log source parameters for VMware vCloud Director” on page 1612.
3. Ensure that no firewall rules block communication between your vCloud appliance and the QRadar Console or the managed host that is responsible for polling the vCloud REST API.

Configuring the vCloud REST API public address

IBM QRadar collects security data from the vCloud API by polling the REST API of the vCloud appliance for events. Before QRadar can collect any data, you must configure the public REST API base URL.

Procedure

1. Log in to your vCloud appliance as an administrator.
2. Click the **Administration** tab.
3. From the **Administration** menu, select **System Settings** > **Public Addresses**.
4. In the **VCD public REST API base URL** field, type an IP address or host name.

   The address that you specify becomes a publicly available address outside of the firewall or NAT on your vCloud appliance.
5. Click **Apply**.

   The public API URL is created on the vCloud appliance.

What to do next

You can now configure a log source in QRadar.

Supported VMware vCloud Director event types logged by IBM QRadar

The VMware vCloud Director DSM for QRadar can collect events from several categories.

Each event category contains low-level events that describe the action that is taken within the event category. For example, user events can have *user created* or *user deleted* as a low-level event.

The following list is the default event categories that are collected by QRadar from vCloud Director:

- User events
- Group events
- User role events
- Session events
- Organization events
- Network events
- Catalog events
- Virtual data center (VDC) events
- Virtual application (vApp) events
- Virtual machine (VM) events
- Media events
- Task operation events

VMware vCloud Director log source parameters for VMware vCloud Director

If QRadar does not automatically detect the log source, add a VMware vCloud Director log source on the QRadar Console by using the VMware vCloud Director protocol.

When using the VMware vCloud Director protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect VMware vCloud Director events from VMware vCloud Director:

Table 1031. VVMware vCloud Director log source parameters for the VMware vCloud Director DSM	
Parameter	**Description**
Log Source Name (Optional)	A unique name for your log source.
Log Source Description (Optional)	A description for your log source.
Log Source Type	**VMware vCloud Director**
Protocol Configuration	**VMware vCloud Director**
Enabled	Select this checkbox to enable the log source. By default, the checkbox is selected.
Credibility	From the list, select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	From the list, select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this checkbox to enable the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the **System Settings** in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	From the list, select the incoming payload encoder for parsing and storing the logs.
Store Event Payload	Select this checkbox to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the **System Settings** in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.

For a complete list of VMware vCloud Director protocol parameters and their values, see VMware vCloud Director protocol configuration options.

Related information

"Adding a log source" on page 5

VMware vShield

The IBM QRadar DSM for VMware vShield collects event logs from VMware vShield servers.

The following table identifies the specifications for the VMware vShield Server DSM:

Table 1032. VMware vShield DSM specifications	
Specification	**Value**
Manufacturer	VMware
DSM	VMware vShield
RPM file name	DSM-*VMwarevShield-QRadar_version-build_number*.noarch.rpm
Protocol	Syslog
QRadar recorded events	All events
Automatically discovered	Yes
Includes identity	No
More information	http://www.vmware.com/

VMware vShield DSM integration process

You can integrate VMware vShield DSM with IBM QRadar.

Use the following procedures:

1. If automatic updates are not enabled, download and install the most recent version of the VMware vShield RPM from the IBM Support Website onto your QRadar Console.
2. For each instance of VMware vShield, configure your VMware vShield system to enable communication with QRadar. This procedure must be completed for each instance of VMware vShield.
3. If QRadar does not automatically discover the log source, for each VMware vShield server that you want to integrate, create a log source on the QRadar Console. For more information about configuring VMware vShield log source parameters, see "Syslog log source parameters for VMware vShield" on page 1615.

Related tasks

"Configuring your VMware vShield system for communication with IBM QRadar" on page 1614

"Adding a log source" on page 5

Configuring your VMware vShield system for communication with IBM QRadar

To collect all audit logs and system events from VMware vShield, you must configure the vShield Manager. When you configure VMware vShield, you must specify IBM QRadar as the syslog server.

Procedure

1. Access your **vShield Manager inventory** pane.
2. Click **Settings & Reports**.
3. Click **Configuration** > **General**.
4. Click **Edit** next to the **Syslog Server** option.
5. Type the IP address of your QRadar Console.

6. Optional: Type the port for your QRadar Console. If you do not specify a port, the default UDP port for the IP address/host name of your QRadar Console is used.
7. Click **OK**.

Syslog log source parameters for VMware vShield

If QRadar does not automatically detect the log source, add a VMware vShield log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from VMware vShield:

Table 1033. Syslog log source parameters for the VMware vShield DSM

Parameter	Value
Log Source type	VMware vShield
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or hostname of the VMware device. The log source identifier must be unique value.

Related information

“Adding a log source” on page 5

Chapter 171. Vormetric Data Security

The Vormetric Data Security DSM for IBM QRadar can collect event logs from your Vormetric Data Security servers.

The following table identifies the specifications for the Vormetric Data Security DSM:

Vormetric Data Security DSM specifications	
Specification	**Value**
Manufacturer	Vormetric, Inc.
DSM	Vormetric Data Security
RPM file name	DSM-VormetricDataSecurity-7.1-804377.noarch.rpm DSM-VormetricDataSecurity-7.2-804381.noarch.rpm
Supported versions	Vormetric Data Security Manager v5.1.3 and later Vormetric Data Firewall FS Agent v5.2 and later
Protocol	Syslog (LEEF)
QRadar recorded events	Audit, Alarm, Warn, Learn Mode, System
Auto discovered	Yes
Includes identity	No
More information	Vormetric website (http://www.vormetric.com)

Vormetric Data Security DSM integration process

You can integrate Vormetric Data Security DSM with IBM QRadar.

Use the following procedures:

1. If automatic updates are not enabled, download and install the most recent version of the following RPMs from the IBM Support Website onto your QRadar Console:
2. • Syslog protocol RPM
   • DSMCommon RPM

   The minimum version of the DSMCommon RPM that you can use is the `DSM-DSMCommon-7.1-530016.noarch.rpm` or `DSM-DSMCommon-7.2-572972.noarch.rpm`

   • Vormetric Data Security RPM
3. For each instance of Vormetric Data Security, configure your Vormetric Data Security system to enable communication with QRadar.
4. If QRadar does not automatically discover the DSM, for each Vormetric Data Security server you want to integrate, create a log source on the QRadar Console.

Related tasks

"Configuring your Vormetric Data Security systems for communication with IBM QRadar" on page 1618

Configuring your Vormetric Data Security systems for communication with IBM QRadar

To collect all audit logs and system events from Vormetric Data Security, you must configure your Vormetric Data Security Manager to enable communication with QRadar.

About this task

Your Vormetric Data Security Manager user account must have System Administrator permissions.

Procedure

1. Log in to your Vormetric Data Security Manager as an administrator that is assigned System Administrator permissions.
2. On the navigation menu, click **Log** > **Syslog**.
3. Click **Add**.
4. In the **Server Name** field, type the IP address or host name of your QRadar system.
5. From the **Transport Protocol** list, select **TCP** or a value that matches the log source protocol configuration on your QRadar system.
6. In the **Port Number** field, type 514 or a value that matches the log source protocol configuration on your QRadar system.
7. From the **Message Format** list, select **LEEF**.
8. Click **OK**.
9. On the Syslog Server summary screen, verify the details that you have entered for your QRadar system. If the **Logging to SysLog** value is **OFF**, complete the following steps. On the navigation menu, click **System** > **General Preferences**
10. Click the **System** tab.
11. In the **Syslog Settings** pane, select the **Syslog Enabled** check box.

What to do next

"Configuring Vormetric Data Firewall FS Agents to bypass Vormetric Data Security Manager" on page 1618

Configuring Vormetric Data Firewall FS Agents to bypass Vormetric Data Security Manager

When the Vormetric Data Security Manager is enabled to communicate with IBM QRadar, all events from the Vormetric Data Firewall FS Agents are also forwarded to the QRadar system through the Vormetric Data Security Manager.

About this task

To bypass the Vormetric Data Security Manager, you can configure Vormetric Data Firewall FS Agents to send LEEF events directly to the QRadar system.

Your Vormetric Data Security Manager user account must have System Administrator permissions.

Procedure

1. Log in to your Vormetric Data Security Manager.
2. On the navigation menu, click **System** > **Log Preferences**.
3. Click the **FS Agent Log** tab.
4. In the **Policy Evaluation** row, configure the following parameters:

a) Select the **Log to Syslog/Event Log** check box.

5. Clear the **Upload to Server** check box.
6. From the **Level** list, select **INFO**.

   This set up enables a full audit trail from the policy evaluation module to be sent directly to a syslog server, and not to the Security Manager. Leaving both destinations enabled might result in duplication of events to the QRadar system.
7. Under the Syslog Settings section, configure the following parameters. In the **Server** field, use the following syntax to type the IP address or host name and port number of your QRadar system.

   qradar_IP address_or_host:*port*
8. From the **Protocol** list, select **TCP** or a value that matches the log source configuration on your QRadar system.
9. From the **Message Format** list, select **LEEF**.

What to do next

This configuration is applied to all hosts or host groups later added to the Vormetric Data Security Manager. For each existing host or host group, select the required host or host group from the **Hosts** list and repeat the procedure.

Syslog log source parameters for Vormetric Data Security

If QRadar does not automatically detect the log source, add a Vormetric Data Security log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Vormetric Data Security:

Table 1034. Syslog log source parameters for the Vormetric Data Security DSM

Parameter	Value
Log Source type	Vormetric Data Security
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or hostname of the Vormetric Data Security device. The log source identifier must be unique value.

Related information

“Adding a log source” on page 5

Chapter 172. WatchGuard Fireware OS

The IBM QRadar DSM for WatchGuard Fireware OS can collect event logs from your WatchGuard Fireware OS.

The following table identifies the specifications for the WatchGuard Fireware OS DSM:

Table 1035. WatchGuard Fireware DSM specifications

Specification	Value
Manufacturer	WatchGuard
DSM name	WatchGuard Fireware OS
RPM file name	DSM-WatchGuardFirewareOS-*QRadar-version-Build_number*.noarch.rpm
Supported versions	Fireware XTM OS v11.9 and later
Event format	syslog
QRadar recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
More information	WatchGuard Website (http://www.watchguard.com/)

To integrate the WatchGuard Fireware OS with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs from the IBM Support Website onto your QRadar Console.
   - DSMCommon RPM
   - WatchGuard Fireware OS RPM
2. For each instance of WatchGuard Fireware OS, configure your WatchGuard Fireware OS appliance to enable communication with QRadar. You can use one the following procedures:
   - "Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar" on page 1622
   - "Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar" on page 1622
3. If QRadar does not automatically discover the WatchGuard Fireware OS log source, create a log source for each instance of WatchGuard Fireware OS on your network. For more information about configuring the log source, see "Syslog log source parameters for WatchGuard Fireware OS" on page 1623.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar

To collect WatchGuard Fireware OS events, you can use the Policy Manager to configure your third-party appliance to send events to QRadar.

Before you begin

You must have Device Administrator access credentials.

Procedure

1. Open the WatchGuard System Manager.
2. Connect to your Firebox or XTM device.
3. Start the Policy Manager for your device.
4. To open the **Logging Setup** window, select **Setup > Logging**.
5. Select the **Send log messages to this syslog server** check box.
6. In the **IP address** text box, type the IP address for your QRadar Console or Event Collector.
7. In the **Port** text box, type 514.
8. From the **Log Format** list, select IBM **LEEF**.
9. Optional: Specify the details to include in the log messages.
   a) Click **Configure**.
   b) To include the serial number of the XTM device in the log message details, select the **The serial number of the device** check box.
   c) To include the syslog header in the log message details, select the **The syslog header** check box.
   d) For each type of log message, select one of the following syslog facilities:
      - For high-priority syslog messages, such as alarms, select **Local0**.
      - To assign priorities to other types of log messages, select an option from **Local1** through **Local7**. Lower numbers have greater priority.
      - To not send details for a log message type, select **NONE**.
   e) Click **OK**.
10. Click **OK**.
11. Save the configuration file to your device.

Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar

To collect WatchGuard Fireware OS events, you can use the Fireware XTM web user interface to configure your third-party appliance to send events to QRadar.

Before you begin

You must have Device Administrator access credentials.

Procedure

1. Log in to the Fireware XTM web user interface for your Fireware or XTM device.
2. Select **System > Logging**.
3. In the Syslog Server pane, select the **Send log messages to the syslog server at this IP address** check box.

4. In the **IP Address** text box, type the IP address for the QRadar Console or Event Collector.
5. In the **Port** text box, type 514.
6. From the **Log Format** list, select IBM **LEEF**.
7. Optional: Specify the details to include in the log messages.
   a) To include the serial number of the XTM device in the log message details, select the **The serial number of the device** check box.
   b) To include the syslog header in the log message details, select the **The syslog header** check box.
   c) For each type of log message, select one of the following syslog facilities:
      - For high-priority syslog messages, such as alarms, select **Local0**.
      - To assign priorities to other types of log messages, select an option from **Local1** through **Local7**. Lower numbers have greater priority.
      - To not send details for a log message type, select **NONE**.
8. Click **Save**.

Syslog log source parameters for WatchGuard Fireware OS

If QRadar does not automatically detect the log source, add a WatchGuard Fireware OS log source on the QRadar Console by using the Syslog protocol.

When using the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from WatchGuard Fireware OS:

Table 1036. Syslog log source parameters for the WatchGuard Fireware OS DSM

Parameter	Value
Log Source type	WatchGuard Fireware OS
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or hostname of the WatchGuard Fireware OS device. The log source identifier must be unique value.

Related information

“Adding a log source” on page 5

Chapter 173. Websense

Websense is now known as Forcepoint.

Related concepts

Forcepoint

IBM QRadar supports a range of Forcepoint DSMs.

Chapter 174. Zscaler Nanolog Streaming Service

The IBM QRadar DSM for Zscaler Nanolog Streaming Service (Zscaler NSS) collects Syslog events from either Web logs or Firewall logs.

To integrate Zscaler Streaming Service with QRadar, complete the following steps:

1. If automatic updates are not enabled, RPMs are available for download from the IBM support website (http://www.ibm.com/support). Download and install the most recent version of the following RPMs on your QRadar Console:
   - DSM Common RPM
   - Zscaler NSS DSM RPM
2. Configure your Zscaler NSS device to send events to QRadar. For more information about configuring Zscaler NSS, see the Zscaler and IBM QRadar Deployment Guide (https:/help.zscaler.com/zia/zscaler-ibm-qradar-deployment-guide).

   Important: When you configure your Zscaler NSS device, QRadar supports the following feeds:
   - Firewall logs. For more information about Firewall logs, see Adding NSS Feeds for Firewall logs (https://help.zscaler.com/zia/adding-nss-feeds-firewall-logs).
   - Web logs. For more information about Web logs, see Adding NSS Feeds for Web Logs (https://help.zscaler.com/zia/adding-nss-feeds-web-logs).

   Use the following LEEF output feed format for Web logs when you configure a Syslog feed in Zscaler NSS:

   ```
   %s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss} zscaler-nss:
   LEEF:1.0|Zscaler|NSS|4.1|%s{reason}|cat=%s{action}\tdevTime=%s{mon} %02d{dd}
   %d{yy} %02d{hh}:%02d{mm}:%02d{ss} %s{tz}\tdevTimeFormat=MMM dd
   yyyy HH:mm:ss z\tsrc=%s{cip}\tdst=%s{sip}\tsrcPostNAT=%s{cintip}\trealm=%s{location}
   \tusrName=%s{login}\tsrcBytes=%d{reqsize}\tdstBytes=%d{respsize}\trole=%s{dept}
   \tpolicy=%s{reason}\trecordid=%d{recordid}\tbwthrottle=%s{bwthrottle}\tuseragent=%s{ua}
   \treferer=%s{ereferer}\thostname=%s{ehost}\tappproto=%s{proto}\turlcategory=%s{urlcat}
   \turlsupercategory=%s{urlsupercat}\turlclass=%s{urlclass}\tappclass=%s{appclass}
   \tappname=%s{appname}\tmalwaretype=%s{malwarecat}\tmalwareclass=%s{malwareclass}
   \tthreatname=%s{threatname}\triskscore=%d{riskscore}\tdlpdict=%s{dlpdict}
   \tdlpeng=%s{dlpeng}\tfileclass=%s{fileclass}\tfiletype=%s{filetype}\treqmethod=%s{reqmethod}
   \trespcode=%s{respcode}\tbamd5=%s{bamd5}\turl=%s{eurl}
   ```

   Use the following LEEF output feed format for Firewall logs when you configure a Syslog feed in Zscaler NSS:

   ```
   %s{mon} %02d{dd} %02d{hh}:%02d{mm}:%02d{ss}
   zscaler-nss: LEEF:1.0|Zscaler|NSS-FW|6.0|%s{action}|usrName=%s{login}\trole=%s{dept}
   \trealm=%s{location}\tsrc=%s{csip}\tdst=%s{cdip}\tsrcPort=%d{csport}\tdstPort=%d{cdport}
   \tdstPreNATPort=%d{cdport}\tsrcPreNATPort=%d{csport}\tdstPostNATPort=%d{sdport}
   \tsrcPostNATPort=%d{ssport}\tsrcPreNAT=%s{csip}\tdstPreNAT=%s{cdip}\tsrcPostNAT=%s{ssip}
   \tdstPostNAT=%s{sdip}\ttsip=%s{tsip}\ttsport=%d{tsport}\tttype=%s{ttype}\tcat=nss-
   fw\tdnat=%s{dnat}\tstateful=%s{stateful}\taggregate=%s{aggregate}\tnwsvc=%s{nwsvc}
   \tnwapp=%s{nwapp}\tproto=%s{ipproto}\tipcat=%s{ipcat}\tdestcountry=%s{destcountry}
   \tavgduration=%ld{avgduration}\trulelabel=%s{rulelabel}\tdstBytes=%ld{inbytes}
   \tsrcBytes=%ld{outbytes}\tduration=%d{duration}\tdurationms=%d{durationms}
   \tnumsessions=%d{numsessions}\n
   ```

3. If QRadar does not automatically detect the log source, add a Zscaler NSS log source on the QRadar Console. For more information about adding a Sysog log source, see Syslog log source parameters for Zscaler NSS.
4. Optional: Configure your Zscaler NSS device to send HTTP receiver events to QRadar.

   Important: You need a certificate that is issued by a certificate authority (CA). It can't be a self-signed certificate because it must be validated by a CA. For more information about certificates and configuring the log source parameters for HTTP receiver, see HTTP Receiver protocol configuration options.

Related concepts

"Syslog log source parameters for Zscaler NSS" on page 1628
If IBM QRadar does not automatically detect the log source, add a Zscaler NSS log source on the QRadar Console by using the Syslog protocol.

"HTTP Receiver log source parameters for Zscaler NSS" on page 1629
If IBM QRadar does not automatically detect the log source, add a Zscaler NSS log source on the QRadar Console by using the HTTP Receiver protocol.

Related tasks

"Adding a DSM" on page 4
"Adding a log source" on page 5

Zscaler NSS DSM specifications

When you configure Zscaler NSS, understanding the specifications for the Zscaler NSS DSM can help ensure a successful integration. For example, knowing what the supported version of Zscaler NSS is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Zscaler NSS DSM.

Table 1037. Zscaler NSS DSM specifications

Specification	**Value**
Manufacturer	Zscaler
DSM name	Zscaler NSS
RPM file name	DSM-*ZscalerNSS-QRadar_version-build_number*.noarch.rpm
Supported version	6.0
Protocol	Syslog HTTP receiver
Event format	LEEF
Recorded event types	Weblog events, Firewall events (including DNS)
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	About Nanolog Streaming Service (NSS) (https://help.zscaler.com/zia/about-nanolog-streaming-service)

Syslog log source parameters for Zscaler NSS

If IBM QRadar does not automatically detect the log source, add a Zscaler NSS log source on the QRadar Console by using the Syslog protocol.

When you use the Syslog protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect Syslog events from Zscaler NSS:

Table 1038. Syslog log source parameters for the Zscaler NSS DSM	
Parameter	**Description**
Log Source type	Zscaler NSS
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address as an identifier for events from your Zscaler NSS installation. The log source identifier must be a unique value.
Enabled	By default, the check box is selected.
Credibility	Select the credibility of the log source. The range is 0 - 10. The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event. The default is 5.
Target Event Collector	Select the **Target Event Collector** to use as the target for the log source.
Coalescing Events	Select this option for the log source to coalesce (bundle) events. By default, automatically discovered log sources inherit the value of the **Coalescing Events** list from the **System Settings** in QRadar. When you create a log source or edit an existing log source configuration, you can override the default value by configuring this option for each log source.
Incoming Event Payload	Select the **Incoming Payload Encoder** option for parsing and storing the logs from the list.
Store Event Payload	Select this option to enable the log source to store event payload information. By default, automatically discovered log sources inherit the value of the **Store Event Payload** list from the **System Settings** in QRadar. When you create a log source or edit an existing configuration, you can override the default value by configuring this option for each log source.
Log Source Language	Select the language of the events that are generated by Zscaler NSS.

Related information

“Adding a log source” on page 5

HTTP Receiver log source parameters for Zscaler NSS

If IBM QRadar does not automatically detect the log source, add a Zscaler NSS log source on the QRadar Console by using the HTTP Receiver protocol.

When you use the HTTP Receiver protocol, there are specific parameters that you must use.

The following table describes the parameters that require specific values to collect HTTP Receiver events from Zscaler NSS:

Table 1039. HTTP Receiver log source parameters for the Zscaler NSS DSM	
Parameter	**Description**
Log Source type	Zscaler NSS
Protocol Configuration	HTTP Receiver
Log Source Identifier	Type the IP address as an identifier for events from your Zscaler NSS installation. The log source identifier must be a unique value.

Important: When you use the HTTP protocol, you must use a certificate that is issued by a certificate authority (CA). It can't be a self-signed certificate because it must be validated by a CA. For more information about certificates and configuring the log source parameters for HTTP receiver, see HTTP Receiver protocol configuration options.

Related information

"Adding a log source" on page 5

Zscaler NSS sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Sample 1: The following table provides a sample event message for Firewall logs feeds when you use the Syslog protocol for the Zscaler NSS DSM.

Table 1040. Zscaler NSS Syslog sample message for Firewall logs feeds supported by Zscaler NSS.		
Event name	**Low-level category**	**Sample log message**
Drop	Firewall Deny	Jun 02 16:34:55 zscaler-nss: LEEF:1.0|Zscaler|NSS-FW|5.5|Drop|usrName=GCL->SBL-1\trole=Default Department\trealm=GCL->SBL-1\tsrc=10.11.12.13\tdst=10.66.69.21\tsrcPort=30513\tdstPort=53\tdstPreNATPort=30512\tsrcPreNATPort=234\tdstPostNATPort=2345\tsrcPostNATPort=332\tsrcPreNAT=10.17.15.14\tdstPreNAT=10.66.69.111\tsrcPostNAT=10.66.54.105\tdstPostNAT=10.17.15.14\ttsip=10.66.54.105\t\ttsport=0\t\tttype=GRE\tcat=nss-fw\tdnat=No\tstateful=No\taggregate=No\tnwsvc=HTTP\tnwapp=adultadworld\tproto=TCP\tipcat=Miscellaneous or Unknown\tdestcountry=United States\tavgduration=115\trulelabel=Firewall_Adult\tdstBytes=898\tsrcBytes=14754\tduration=0\tdurationms=115\tnumsessions=1

Sample 2: The following table provides a sample event message for Web logs feeds when you use the Syslog protocol for the Zscaler NSS DSM.

Table 1041. Zscaler NSS Syslog sample message for Web logs feeds supported by Zscaler NSS.

Event name	Low-level category	Sample log message
Block	Network Threshold Policy Violation	<13>Feb 21 06:56:02 zscalar.nss.test zscaler-nss: LEEF:1.0|Zscaler|NSS|4.1|IPS block outbound request: adware/spyware traffic|cat=Blocked devTime=Feb 21 2019 06:56:02 GMT devTimeFormat=MMM dd yyyy HH:mm:ss z src=192.0.2.0 dst=192.0.2.11 srcPostNAT=192.0.2.14 realm=Location 1 usrName=User01 srcBytes=175 dstBytes=14798 role=Unauthenticated Transactions policy=IPS block outbound request: adware/spyware traffic url=qradar.example.test/?v=3.08&pcrc=123456789=CHECK recordid=6660343920943824897 bwthrottle=NO useragent=Unknown referer=None hostname=qradar.example.test appproto=HTTP urlcategory=Suspected Spyware or Adware urlsupercategory=Advanced Security urlclass=Advanced Security Risk appclass=General Browsing appname=generalbrowsing malwaretype=Clean Transaction malwareclass=Clean Transaction threatname=Win32.PUA.Jeefo riskscore=100 dlpdict=None dlpeng=None fileclass=None filetype=None reqmethod=POST respcode=40

Chapter 175. Zscaler Private Access

The IBM QRadar DSM for Zscaler Private Access (ZPA) collects syslog events from a Zscaler Private Access service.

To integrate Zscaler Private Access with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent versions of the RPMs from the IBM support website (https://www.ibm.com/support).
   - DSM Common RPM
   - ZscalerPrivateAccess DSM RPM
2. Configure your Zscaler Private Access service to send events to QRadar. For more information, see Configuring Zscaler Private Access to send events to QRadar.
3. If QRadar does not automatically detect the log source, add a Zscaler Private Access log source on the QRadar Console.

Related tasks

"Adding a DSM" on page 4

"Adding a log source" on page 5

Zscaler Private Access DSM specifications

When you configure the Zscaler Private Access DSM, understanding the specifications for the DSM can help ensure a successful integration. For example, knowing what the supported protocol is before you begin can help reduce frustration during the configuration process.

The following table describes the specifications for the Zscaler Private Access DSM.

Table 1042. Zscaler Private Access DSM specifications

Specification	Value
Manufacturer	Zscaler
DSM name	Zscaler Private Access
RPM file name	DSM-*ZscalerPrivateAccess-QRadar_version-build_number*.noarch.rpm
Protocol	Syslog
Event format	LEEF
Recorded event types	User Status App Connector Status Audit User Activity
Automatically discovered?	Yes
Includes identity?	No
Includes custom properties?	No
More information	ZScaler Private Access (https://www.zscaler.com/products/zscaler-private-access) Zscaler ZPA help (https://help.zscaler.com/zpa)

Configuring Zscaler Private Access to send events to QRadar

To send events to IBM QRadar, you must redirect the log stream for Zscaler Private Access. IBM supports user status, app connector status, and audit log types for Zscaler Private Access devices.

For more information about redirecting the log stream, see your Zscaler documentation about the Log Streaming Service (https://help.zscaler.com/zpa/about-log-streaming-service).

Procedure

1. To use the **User Status** log type, see your Zscaler documentation About User Status Log Fields (https://help.zscaler.com/zpa/about-user-status-log-fields).

   When you configure a Syslog format, use the following LEEF output log format for User Status logs:

   ```
   <166>%s{LogTimestamp:time} zpa-lss LEEF:1.0|Zscaler|ZPA|4.1|%s{SessionStatus}|cat=ZPA User
   Status\tCustomer=%s{Customer}\tusrName=%s{Username}\tSessionID=%s{SessionID}
   \tSessionStatus=%s{SessionStatus}\tVersion=%s{Version}\tZEN=%s{ZEN}
   \tCertificateCN=%s{CertificateCN}\tsrcPreNAT=%s{PrivateIP}\tsrc=%s{PublicIP}
   \tLatitude=%f{Latitude}\tLongitude=%f{Longitude}\tCountryCode=%s{CountryCode}
   \tTimestampAuthentication:iso8601=%s{TimestampAuthentication:iso8601}\tTimestampUnAuthenticat
   ion:iso8601=%s{TimestampUnAuthentication:iso8601}\tdstBytes=%d{TotalBytesRx}
   \tsrcBytes=%d{TotalBytesTx}\tIdp=%s{Idp}\tidentHostName=%s{Hostname}\tPlatform=%s{Platform}
   \tClientType=%s{ClientType}\tTrustedNetworks=%s(,){TrustedNetworks}
   \tTrustedNetworksNames=%s(,){TrustedNetworksNames}\tSAMLAttributes=%s{SAMLAttributes}
   \tPosturesHit=%s(,){PosturesHit}\tPosturesMiss=%s(,){PosturesMiss}
   \tZENLatitude=%f{ZENLatitude}\tZENLongitude=%f{ZENLongitude}
   \tZENCountryCode=%s{ZENCountryCode}\n
   ```

2. To use the **App Connector Status** log type, see your Zscaler documentation About App Connector Status Log Fields (https://help.zscaler.com/zpa/about-connector-status-log-fields).

   When you configure a Syslog format, use the following LEEF output log format for App Connector Status logs:

   ```
   <166>%s{LogTimestamp:time} zpa-lss LEEF:1.0|Zscaler|ZPA|4.1|%s{SessionStatus}|cat=Connector
   Status\tCustomer=%s{Customer}\tSessionID=%s{SessionID}\tSessionType=%s{SessionType}
   \tVersion=%s{Version}\tPlatform=%s{Platform}\tZEN=%s{ZEN}\tConnector=%s{Connector}
   \tConnectorGroup=%s{ConnectorGroup}\tsrcPreNAT=%s{PrivateIP}\tsrc=%s{PublicIP}
   \tLatitude=%f{Latitude}\tLongitude=%f{Longitude}\tCountryCode=%s{CountryCode}
   \tTimestampAuthentication:iso8601=%s{TimestampAuthentication:iso8601}\tTimestampUnAuthenticat
   ion:iso8601=%s{TimestampUnAuthentication:iso8601}\tCPUUtilization=%d{CPUUtilization}
   \tMemUtilization=%d{MemUtilization}\tServiceCount=%d{ServiceCount}
   \tInterfaceDefRoute=%s{InterfaceDefRoute}\tDefRouteGW=%s{DefRouteGW}
   \tPrimaryDNSResolver=%s{PrimaryDNSResolver}\tHostUpTime=%s{HostUpTime}
   \tConnectorUpTime=%s{ConnectorUpTime}\tNumOfInterfaces=%d{NumOfInterfaces}
   \tBytesRxInterface=%d{BytesRxInterface}\tPacketsRxInterface=%d{PacketsRxInterface}
   \tErrorsRxInterface=%d{ErrorsRxInterface}\tDiscardsRxInterface=%d{DiscardsRxInterface}
   \tBytesTxInterface=%d{BytesTxInterface}\tPacketsTxInterface=%d{PacketsTxInterface}
   \tErrorsTxInterface=%d{ErrorsTxInterface}\tDiscardsTxInterface=%d{DiscardsTxInterface}
   \tTotalBytesRx=%d{TotalBytesRx}\tTotalBytesTx=%d{TotalBytesTx}\n
   ```

3. To use the **Audit** log type, see your Zscaler documentation About Audit Log Fields (https://help.zscaler.com/zpa/about-audit-log-fields).

   When you configure a Syslog format, use the following LEEF output log format for Audit logs:

   ```
   <166>%s{modifiedTime:iso8601} zpa-lss LEEF:1.0|Zscaler|ZPA|4.1|%s{auditOperationType}|
   cat=ZPA_Audit_Log\tcreationTime=%s{creationTime:iso8601}\trequestId=%s{requestId}
   \tsessionId=%s{sessionId}\tauditOldValue=%s{auditOldValue}\tauditNewValue=%s{auditNewValue}
   \tauditOperationType=%s{auditOperationType}\tobjectType=%s{objectType}
   \tobjectName=%s{objectName}\tobjectId=%d{objectId}\taccountName=%d{customerId}
   \tusrName=%s{modifiedByUser}\n
   ```

4. To use the **User Activity** log type, see your Zscaler documentation about User Activity Log Fields (https://help.zscaler.com/zpa/about-user-activity-log-fields).

   When you configure a Syslog format, use the following LEEF output log format for User Activity logs:

   ```
   <166>%s{LogTimestamp:time} zpa-lss LEEF:1.0|Zscaler|ZPA|4.1|%s{ConnectionStatus}
   %s{InternalReason}|cat=ZPA User Activity\t\tCustomer=%s{Customer}\tSessionID=%s{SessionID}
   \tConnectionID=%s{ConnectionID}\tInternalReason=%s{InternalReason}
   \tConnectionStatus=%s{ConnectionStatus}\tproto=%d{IPProtocol}
   ```

```
\tDoubleEncryption=%d{DoubleEncryption}\tusrName=%s{Username}\tdstPort=%d{ServicePort}
\tsrc=%s{ClientPublicIP}\tsrcPreNAT=%s{ClientPrivateIP}\tClientLatitude=%f{ClientLatitude}
\tClientLongitude=%f{ClientLongitude}\tClientCountryCode=%s{ClientCountryCode}
\tClientZEN=%s{ClientZEN}\tpolicy=%s{Policy}\tConnector=%s{Connector}
\tConnectorZEN=%s{ConnectorZEN}\tConnectorIP=%s{ConnectorIP}\tConnectorPort=%d{ConnectorPort}
\tApplicationName=%s{Host}\tApplicationSegment=%s{Application}\tAppGroup=%s{AppGroup}
\tServer=%s{Server}\tdst=%s{ServerIP}\tServerPort=%d{ServerPort}
\tPolicyProcessingTime=%d{PolicyProcessingTime}\tServerSetupTime=%d{ServerSetupTime}
\tTimestampConnectionStart:iso8601=%s{TimestampConnectionStart:iso8601}\tTimestampConnectionE
nd:iso8601=%s{TimestampConnectionEnd:iso8601}\tTimestampCATx:iso8601=%s{TimestampCATx:iso8601
}
\tTimestampCARx:iso8601=%s{TimestampCARx:iso8601}\tTimestampAppLearnStart:iso8601=%s{Timestam
pAppLearnStart:iso8601}\tTimestampZENFirstRxClient:iso8601=%s{TimestampZENFirstRxClient:iso86
01}\tTimestampZENFirstTxClient:iso8601=%s{TimestampZENFirstTxClient:iso8601}\tTimestampZENLas
tRxClient:iso8601=%s{TimestampZENLastRxClient:iso8601}\tTimestampZENLastTxClient:iso8601=%s{T
imestampZENLastTxClient:iso8601}\tTimestampConnectorZENSetupComplete:iso8601=%s{TimestampConn
ectorZENSetupComplete:iso8601}\tTimestampZENFirstRxConnector:iso8601=%s{TimestampZENFirstRxCo
nnector:iso8601}\tTimestampZENFirstTxConnector:iso8601=%s{TimestampZENFirstTxConnector:iso860
1}\tTimestampZENLastRxConnector:iso8601=%s{TimestampZENLastRxConnector:iso8601}\tTimestampZEN
LastTxConnector:iso8601=%s{TimestampZENLastTxConnector:iso8601}\tZENTotalBytesRxClient=%d{ZEN
TotalBytesRxClient}\tZENBytesRxClient=%d{ZENBytesRxClient}
\tZENTotalBytesTxClient=%d{ZENTotalBytesTxClient}\tZENBytesTxClient=%d{ZENBytesTxClient}
\tZENTotalBytesRxConnector=%d{ZENTotalBytesRxConnector}
\tZENBytesRxConnector=%d{ZENBytesRxConnector}
\tZENTotalBytesTxConnector=%d{ZENTotalBytesTxConnector}
\tZENBytesTxConnector=%d{ZENBytesTxConnector}\tIdp=%s{Idp}\n
```

What to do next

Syslog log source parameters for Zscaler Private Access

Syslog log source parameters for Zscaler Private Access

If QRadar does not automatically detect the log source, add a Zscaler Private Access log source on the QRadar Console by using the Syslog protocol.

The following table describes the parameters that require specific values to collect Syslog events from Zscaler Private Access:

Table 1043. Syslog log source parameters for the Zscaler Private Access DSM

Parameter	Value
Log Source type	Zscaler Private Access
Protocol Configuration	Syslog
Log Source Identifier	Type the IP address or host name for the log source. The log source identifier must be unique for the log source type.

Related tasks

"Adding a log source" on page 5

Zscaler Private Access sample event messages

Use these sample event messages to verify a successful integration with IBM QRadar.

Important: Due to formatting issues, paste the message format into a text editor and then remove any carriage return or line feed characters.

Zscaler Private Access sample message when you use the Syslog protocol

Sample 1: The following sample event message shows that a user is successfully authenticated in Zscaler Private Access (ZPA).

```
<166>Tue Apr 20 22:23:25 2021 zscaler.privateaccess.test
LEEF:1.0|Zscaler|ZPA|4.1|ZPN_STATUS_AUTHENTICATED|cat=ZPA User Status
Customer=Zscaler Test    usrName=testuser2@domain.test    SessionID=VbPnANNR+Ua/
```

```
B2OHOMwx    SessionStatus=ZPN_STATUS_AUTHENTICATED    Version=2.1.2.81.225296
ZEN=BETA-CA-7987    CertificateCN=aaaaabbbbbccccceeeee1111122222=@domain.test
srcPreNAT=10.2.3.4    src=10.2.2.2    Latitude=44.972686    Longitude=-65.860879
CountryCode=CA    TimestampAuthentication:iso8601=2021-04-20T10:35:15.000Z
TimestampUnAuthentication:iso8601=    dstBytes=175590    srcBytes=109370    Idp=TestIdp
identHostName=ws1client1    Platform=windows    ClientType=zpn_client_type_zapp
TrustedNetworks=    TrustedNetworksNames=    SAMLAttributes={"FirstName":
["testuser2"],"LastName":["testuser2"],"Email":["testuser2@domain.test"]}    PosturesHit=
PosturesMiss=72057767984103498,72057767984103503,72057767984103590,72057767984103745
ZENLatitude=0.000000    ZENLongitude=0.000000    ZENCountryCode=
```

Table 1044. Highlighted fields in the Zscaler Private Access event

QRadar field name	Highlighted values in the event payload
Event ID	ZPN_STATUS_AUTHENTICATED
Event Category	ZPA User Status
Source IP	10.2.2.2
PreNat IP	10.2.3.4
Username	testuser2@domain.test
Device Time	Tue Apr 20 22:23:25 2021

Sample 2: The following sample event message shows that App Connector is successfully authenticated in ZPA.

```
<166>Tue Apr 20 22:23:19 2021 zscaler.privateaccess.test LEEF:1.0|
Zscaler|ZPA|4.1|ZPN_STATUS_AUTHENTICATED|cat=Connector Status    Customer=Zscaler
Test    SessionID=0FQhOAfbQ4yWYSAAUrUn    SessionType=ZPN_ASSISTANT_BROKER_CONTROL
Version=21.88.1    Platform=el7    ZEN=BETA-CA-1234    Connector=AWS
Connector account-1    ConnectorGroup=Connector Group1
srcPreNAT=10.3.4.3    src=192.168.2.2    Latitude=44.972686    Longitude=-65.860879
CountryCode=CA    TimestampAuthentication:iso8601=2021-04-20T13:19:19.154Z
TimestampUnAuthentication:iso8601=    CPUUtilization=1    MemUtilization=17
ServiceCount=2    InterfaceDefRoute=ens5    DefRouteGW=10.79.0.1
PrimaryDNSResolver=10.11.11.11    HostUpTime=1587783907    ConnectorUpTime=1618924759
NumOfInterfaces=2    BytesRxInterface=80385754338    PacketsRxInterface=824116164
ErrorsRxInterface=0    DiscardsRxInterface=0    BytesTxInterface=65456179168
PacketsTxInterface=683050042    ErrorsTxInterface=0    DiscardsTxInterface=0
TotalBytesRx=688700    TotalBytesTx=1101224
```

Table 1045. Highlighted fields in the Zscaler Private Access event

QRadar field name	Highlighted values in the event payload
Event ID	ZPN_STATUS_AUTHENTICATED
Event Category	Connector Status
Source IP	192.168.2.2
PreNat IP	10.3.4.3
Device Time	Tue Apr 20 22:23:19 2021

Chapter 176. QRadar supported DSMs

IBM QRadar can collect events from your security products by using a plug-in file that is called a Device Support Module (DSM).

QRadar can receive logs from systems and devices by using the Syslog protocol, which is a standard protocol. Supported DSMs can use other protocols, as mentioned in the Supported DSM table. You can try to configure third-party applications to send logs to QRadar through the Syslog protocol. For more information, see “Adding a log source” on page 5.

If you want to send logs by using a supported DSM that is not supported by the auto discovery feature in QRadar, you need to manually add a log source. For more information about adding a log source in QRadar, see “Adding a log source” on page 5.

Important: When you upgrade your IBM QRadar system, custom DSMs are not removed during the upgrade.

What do you do if the product version or device you have is not listed in the DSM Configuration Guide?

Sometimes a version of a vendor product or a device is not listed as supported. If the product or device is not listed, follow these guidelines:

Version not listed

If the DSM for your product is officially supported by QRadar, but your product version is not listed in the *IBM QRadar DSM Configuration Guide*, you have the following options:

- Try the DSM to see whether it works. The product versions that are listed in the guide are tested by IBM, but newer untested versions can also work.
- If you tried the DSM and it didn’t work, open a support ticket for a review of the log source to troubleshoot and rule out any potential issues.

  Tip: In most cases, no changes are necessary, or perhaps a minor update to the IBM QRadar Identifier (QID) Map might be all that is required. Software updates by vendors might on rare occasions add or change event formats that break the DSM, requiring an RFE for the development of a new integration. This is the only scenario where an RFE is required.

Device not listed

When a device is not officially supported, you have the following options:

- Open a request for enhancement (RFE) to have your device become officially supported.
  - Go to the QRadar SIEM RFE page (https://ibm.biz/BdRPx5).
  - Log in to the support portal page.
  - Click the **Submit** tab and type the necessary information.

    Tip: If you have event logs from a device, attach the event information and include the product version of the device that generated the event log.
- Write a log source extension to parse events for your device. For more information, see Chapter 4, “Log source extensions,” on page 19 and the DSM Editor.
- You can use content extensions for sending events to QRadar that are provided by some third-party vendors. They can be found on the IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub/). These third-party DSM integrations are supported by the vendor, not by IBM. For a list of available third-party DSMs, see Chapter 177, “DSMs supported by third-party vendors,” on page 1657.

The following table lists supported DSMs for third-party and IBM QRadar solutions.

Tip: To view all seven columns in the table, you might need to scroll to the right.

Table 1046. QRadar Supported DSMs

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
3Com	8800 Series Switch V3.01.30	Syslog	Status and network condition events	Yes	No	No
AhnLab	AhnLab Policy Center	AhnLabPolicy CenterJdbc	Spyware detection Virus detection Audit	No	Yes	No
Akamai	Akamai KONA	HTTP Receiver Akamai Kona REST API	Event format: JSON Recorded event types: All security events	No	No	No
Alibaba Cloud	Alibaba ActionTrail	Alibaba Cloud Object Storage Syslog	Event format: JSON	Yes	Yes	No
Amazon	Amazon AWS Application Load Balancer Access Logs	Amazon AWS S3 REST API	Event format: Space delimited pre-defined fields Recorded event types: Access logs	Yes	No	No
Amazon	Amazon AWS CloudTrail	Amazon AWS S3 REST API Amazon Web Services	Event versions 1.0, 1.02, 1.03, 1.04, 1.05, 1.06 and 1.08 events.	Yes	No	No
Amazon	Amazon AWS Config	Amazon AWS S3 REST API	Event format: JSON	Yes	No	No
Amazon	Amazon AWS Elastic Kubernetes Service Supported version: Kubernetes API 1.19	Amazon Web Services	Event format: JSON Recorded event types: Amazon AWS Kubernetes	Yes	No	No
Amazon	Amazon AWS Network Firewall	Amazon AWS S3 REST API	Event format: JSON Recorded event types: Firewall Alert logs, Firewall Flow logs	No	No	No
Amazon	Amazon AWS Route 53	• Amazon Web Services (Resolver and Public DNS query logs) • Amazon AWS S3 REST API (Resolver query logs only) • Syslog	Event format: • JSON (Resolver query logs) • Space delimited pre-defined fields (Public DNS query logs) Recorded event types: Event versions 1.0	Yes	No	No
Amazon	Amazon AWS Security Hub	Amazon Web Services	Event format: JSON Recorded event types: AWS Security Finding Format (ASFF)	No	No	No
Amazon	Amazon AWS WAFCentrif	Amazon AWS S3 REST API	Event format: JSON Recorded event types: Traffic allow, Traffic block	No	No	No
Amazon	Amazon CloudFront	Amazon Web Services	Event format: Tab Separated Value (TSV) Recorded event types: RealTime Log - TSV	Yes	No	No
Amazon	Amazon GuardDuty	Amazon Web Services	Amazon GuardDuty Findings JSON	No	No	No
Amazon	AWS Verified Access	Amazon AWS S3 REST API, Syslog	Event format: JSON	Yes	Yes	Yes
Ambiron	TrustWave ipAngel V4.0	Syslog	Snort-based events	No	No	No
Apache	HTTP Server V1.3+	Syslog, Syslog-ng	HTTP status	Yes	No	No
APC	UPS	Syslog	Smart-UPS series events	No	No	No
Apple	Apple Mac OS X version 10.12	Syslog	Firewall, web server access, web server error, privilege, and informational events	No	Yes	No
Application Security, Inc.	DbProtect V6.2, V6.3, V6.3sp1, V6.3.1, and v6.4	Syslog	All events	Yes	No	No
Arbor Networks	Arbor Networks Pravail APS V3.1+	Syslog, TLS Syslog	All events	Yes	No	No
Arbor Networks	Arbor Networks Peakflow SP V5.8 to V8.1.2	Syslog, TLS Syslog	Denial of Service (DoS) Authentication Exploit Suspicious activity System	Yes	No	No
Arpeggio Software	SIFT-IT V3.1+	Syslog	All events configured in the SIFT-IT rule set	Yes	No	No
Array Networks	SSL VPN ArraySP v7.3	Syslog	All events	No	Yes	Yes
Aruba Networks	Aruba ClearPass Policy Manager v6.5.0.71095 to v6.11.1	Syslog	Event format: LEEF Event types: session, audit, system, insight	Yes	Yes	No
Aruba Networks	Mobility Controllers v2.5 +	Syslog	All events	Yes	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Avaya Inc.	Avaya VPN Gateway v9.0.7.2	Syslog	All events	Yes	Yes	No
BalaBit IT Security	MicrosoftWindows Security Event Log V4.x	Syslog	Microsoft Event Log events	Yes	Yes	No
BalaBit IT Security	Microsoft ISA V\v4.x	Syslog and WinCollect	Microsoft Event Log vents	Yes	Yes	No
Barracuda Networks	Spam & Virus Firewall v5.x and later	Syslog	All events	Yes	No	No
Barracuda Networks	Web Application Firewall v7.0.x	Syslog	System, web firewall, access, and audit events	Yes	No	No
Barracuda Networks	Web Filter v6.0.x+	Syslog	Web traffic and web interface events	Yes	No	No
BlueCat Networks	Adonis v6.7.1-P2+	Syslog	DNS and DHCP events	Yes	No	No
Blue Coat	SG v4.x+	Syslog, Log File Protocol	All events	No	No	Yes
Blue Coat	Web Security Service		Blue Coat ELFF, Access	No	No	No
Box	Box	Box REST API	Event format: JSON RTC 256758 Event types: Administrator and enterprise events, Box Shield Alerts	No	Yes	No
Bridgewater Systems	AAA v8.2c1	Syslog	All events	Yes	Yes	No
Broadcom	CA Access Control Facility (ACF2) (Formerly known as CA Technologies ACF2)	Log File Protocol	All events	No	No	Yes
Broadcom	CA Top Secret (Formerly known as CA Technologies Top Secret)	Log File Protocol	All events	No	No	Yes
Broadcom	Symantec SiteMinder (Formerly known as CA SiteMinder)	Syslog, Log File	All events	No	Yes	No
Brocade	Fabric OS v7.x	Syslog	System and audit events	Yes	No	No
Carbon Black	Carbon Black v5.1 and later	Syslog	Watchlist hits	Yes	No	No
Carbon Black	Carbon Black Bit9 Parity	Syslog	LEEF	Yes		No
Carbon Black	Carbon Black Bit9 Security Platform v6.0.2	Syslog	All events	Yes	Yes	No
Centrify	Centrify Identity Platform Now known as CyberArk Identity					
Centrify	Centrify Infrastructure Services 2017	Syslog and WinCollect	WinCollect logs, Audit events	Yes	No	No
Check Point	Check Point versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R75, R77, R80, R81, and NGX	Syslog or OPSEC LEA	Event format: LEEF (versions R77.30, R80.10, R80.20, R81.10) Event types: All events	Yes	Yes	Yes
Check Point	VPN-1 versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, R80, R81, and NGX	Syslog or OPSEC LEA	Event format: LEEF (versions R77.30, R80.10, R80.20, R81.10) Event types: All events	Yes	Yes	No
Check Point	Check Point Multi-Domain Management (Provider-1) versions NG, FP1, FP2, FP3, AI R54, AI R55, R65, R70, R77, R80, R81, and NGX	Syslog or OPSEC LEA	Event format: LEEF (versions R77.30, R80.10, R80.20, R81.10) Event types: All events	Yes	Yes	No
Cilasoft	Cilasoft QJRN/400 v5.14.K+	Syslog	IBM audit events	Yes	Yes	No
Cisco	4400 Series Wireless LAN Controller V7.2	Syslog SNMPv2	All events	No	No	No
Cisco	Cisco CallManager 8.x, 11.5	Syslog	Application events	Yes	No	No
Cisco	ACS V4.1 and later if directly from ACS V3.x and later if using ALE	Syslog	Failed Access Attempts	Yes	Yes	No
Cisco	Aironet V4.x+	Syslog	Cisco Emblem Format	Yes	No	No
Cisco	ACE Firewall V12.2	Syslog	All events	Yes	Yes	No
Cisco	Cisco AMP	Cisco AMP	All security events For a detailed list of supported events, go to the Cisco AMP for Endpoints API documentation. (https://api-docs.amp.cisco.com/api_actions/details?api_action=GET+%2Fv1%2Fevent_types&api_host=api.amp.cisco.com&api_resource=Event+Type&api_version=v1) **Note:** Network traffic is supported only for Data Flow Control (DCF) events.	No	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Cisco	ASA V7.x and later	Syslog	All events	Yes	Yes	No
Cisco	ASA V7.x+	NSEL Protocol	All events	No	No	No
Cisco	CSA V4.x, V5.x and V6.x	Syslog SNMPv1 SNMPv2	All events	Yes	Yes	No
Cisco	CatOS for catalyst systems V7.3+	Syslog	All events	Yes	Yes	No
Cisco	Cloud Web Security (CWS)	Amazon AWS S3 REST API	W3C All web usage logs	No	No	No
Cisco	Cisco Stealthwatch V6.8	Syslog	Event format: LEEF Event types: Anomaly, Data Hoarding, Exploitation, High Concern, Index, High DDoS Source Index, High Target Index, Policy Violation, Recon, High DDoS Target Index, Data Exfilration, C&C	Yes	No	No
Cisco	IPS V7.1.10 and later, V7.2.x, V7.3.x	SDEE	All events	No	No	No
Cisco	• Cisco IronPort V5.5, V6.5, V7.1, V7.5 (adds support for access logs) • Cisco IronPort ESA: V10.0 • Cisco IronPort WSA: V10.0	Syslog, Log File protocol	Event format: All events Recorded event types: Mail (syslog) System (syslog) Access (syslog) Web content filtering (Log File) **Important:** Critical, Warning and Information logs are supported.	No	No	No
Cisco	Cisco Duo	Cisco Duo	Event format: JSON Event types: Authentication logs	Yes	Yes	No
Cisco	Cisco Firepower Management Center V5.2 to V6.4 (formerly known as Cisco FireSIGHT Management Center)	Cisco Firepower eStreamer protocol	Discovery events Correlation and White List events Impact Flag alerts User activity Malware events File events Connection events Intrusion events Intrusion Event Packet Data Intrusion Event Extra Data	No	No	No
Cisco	Cisco Firepower Threat Defense	Syslog	Event format: Syslog, Comma-separated values (CSV), Name-value pair (NVP) Recorded event types: Intrusion, Connection	Yes	Yes	No
Cisco	Cisco Firewall Service Module (FWSM) v2.1+	Syslog	All events	Yes	Yes	Yes
Cisco	Cisco Catalyst Switch IOS, 12.2, 12.5+	Syslog	All events	Yes	Yes	No
Cisco	Cisco Meraki	Syslog	Event format: Syslog Event types: Events Flows security_event_ids_alerted	Yes	No	No
Cisco	Cisco NAC Appliance v4.x +	Syslog	Audit, error, failure, quarantine, and infected events	No	No	No
Cisco	Cisco Nexus v6.x	Syslog	Nexus-OS events	Yes	No	No
Cisco	Cisco PIX Firewall v5.x, v6.3+	Syslog	Cisco PIX events	Yes	Yes	Yes
Cisco	Cisco Identity Services Engine V1.1 to V2.2	UDP Multiline Syslog	Event format: Syslog Event types: Device events	No	Yes	No
Cisco	Cisco IOS 12.2, 12.5+	Syslog	All events	Yes	Yes	No
Cisco	Cisco Secure Workload	Syslog	Event format: JSON	Yes	No	No
Cisco	Cisco Umbrella	Amazon AWS S3 REST API	Event format: Cisco Umbrella CSV Event types: DNS, Proxy, IP	No	No	No
Cisco	Cisco VPN 3000 Concentrator versions VPN 3005, 4.1.7.H	Syslog	All events	Yes	Yes	Yes
Cisco	Cisco Wireless Services Modules (WiSM) V 5.1+	Syslog	All events	Yes	No	No
Citrix	Citrix NetScaler V9.3 to V10.0	Syslog	All events	Yes	Yes	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Citrix	Citrix Access Gateway V4.5	Syslog	Access, audit, and diagnostic events	Yes	No	No
Cloudera	Cloudera Navigator	Syslog	Audit events for HDFS, HBase, Hive, Hue, Cloudera Impala, Sentry	Yes	No	No
Cloudflare	Cloudflare Logs	Amazon AWS S3 REST API HTTP Receiver	Event format: JSON Event types: HTTP events, Firewall events	Yes	No	No
CloudPassage	CloudPassage Halo	Syslog, Log file	All events	Yes	No	No
CrowdStrike	CrowdStrike Falcon	Syslog LEEF	Incident, Incident summary, Detection summary, Authentication, Detection status update, Uploaded IoCs, Network containment, IP whitelisting, Policy management, CrowdStrike store, Falcon firewall management, Real time response, Event streams	Yes	No	No
CrowdStrike	Falcon Data Replicator	Amazon AWS S3 REST API	Event format: JSON	Yes	No	No
CorreLog	CorreLog Agent for IBM z/OS	Syslog LEEF	All events	Yes	No	No
CRYPTOCard	CRYPTO- Shield V6.3	Syslog	All events	No	No	No
CyberArk	CyberArk Identity **Important:** The Centrify Identity Platform DSM name is now the CyberArk Identity DSM. The DSM RPM name remains as Centrify Identity Platform in QRadar.	Centrify Redrock REST API	Event format: JSON Event types: SaaS, Core, Internal and Mobile	No	No	No
CyberArk	CyberArk Privileged Threat Analytics V3.1	Syslog	Detected security events	Yes	No	No
CyberArk	CyberArk Vault V6.x	Syslog	All events	Yes	Yes	No
CyberGuard	Firewall/VPN KS1000 V5.1	Syslog	CyberGuard events	Yes	No	No
Damballa	Failsafe V5.0.2+	Syslog	All events	Yes	No	No
Digital China Networks	DCS and DCRS Series switches V1.8.7	Syslog	DCS and DCRS IPv4 events	No	No	No
DG Technology	DG Technology MEAS	Syslog LEEF	Mainframe events	Yes	No	No
ESET	ESET Remote Administrator V6.4.270	Syslog LEEF	Threat events Firewall Aggregated Event HIPS Aggregated Event Audit events	Yes	Yes	No
Extreme	Dragon V5.0, V6.x, V7.1, V7.2, V7.3, and V7.4	Syslog SNMPv1 SNMPv3	All relevant Extreme Dragon events	Yes	No	No
Extreme	800-Series Switch	Syslog	All events	Yes	No	No
Extreme	Matrix Router V3.5	Syslog SNMPv1 SNMPv2 SNMPv3	SNMP and syslog login, logout, and login failed events	Yes	No	No
Extreme	NetSight Automatic Security Manager V3.1.2	Syslog	All events	Yes	No	No
Extreme	Matrix N/K/S Series Switch V6.x, V7.x	Syslog	All relevant Matrix K-Series, N-Series and S-Series device events	Yes	No	No
Extreme	Stackable and Standalone Switches	Syslog	All events	Yes	Yes	No
Extreme	XSR Security Router V7.6.14.0002	Syslog	All events	Yes	No	No
Extreme	HiGuard Wireless IPS 2R2.0.30	Syslog	All events	Yes	No	No
Extreme	HiPath Wireless Controller 2R2.0.30	Syslog	All events	Yes	No	No
Extreme	NAC 3.2 and 3.3	Syslog	All events	Yes	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Enterprise-IT-Security.com	SF-Sherlock 8.1 and later	LEEF	All_Checks, DB2_Security_Configuration, JES_Configuration, Job_Entry_System_Attack, Network_Parameter, Network_Security, No_Policy, Resource_Access_Viol, Resource_Allocation, Resource_Protection, Running_System_Change, Running_System_Security, Running_System_Status, Security_Dbase_Scan, Security_Dbase_Specialty, Security_Dbase_Status, Security_Parm_Change, Security_System_Attack, Security_System_Software, Security_System_Status, SF-Sherlock, Sherlock_Diverse, Sherlock_Diverse, Sherlock_Information, Sherlock_Specialties, Storage_Management, Subsystem_Scan, Sysplex_Security, Sysplex_Status, System_Catalog, System_File_Change, System_File_Security, System_File_Specialty, System_Log_Monitoring, System_Module_Security, System_Process_Security, System_Residence, System_Tampering, System_Volumes, TSO_Status, UNIX_OMVS_Security, UNIX_OMVS_System, User_Defined_Monitoring, xx_Resource_Prot_Templ	Yes	No	No
Epic	Epic SIEM, Versions Epic 2014, Epic 2015, and Epic 2017	LEEF	Audit, Authentication	Yes	Yes	No
Exabeam	Exabeam 1.7 and 2.0	not applicable	Critical, Anomalous	Yes	No	No
Extreme Networks	Extreme Ware 7.7 and XOS 12.4.1.x	Syslog	All events	No	Yes	No
F5 Networks	F5 Networks BIG-IP AFM 11.3 and 12.x to 14.x	Syslog	Network, network DoS, protocol security, DNS, and DNS DoS events	Yes	Yes	No
F5 Networks	F5 Networks BIG-IP LTM 9.42 to 14.x	Syslog, CSV	All events	No	Yes	No
F5 Networks	F5 Networks BIG-IP ASM 10.1 to 16.x	Syslog	Event formats: CEF (CEF:0 is supported), JSON Recorded event types: All security events	Yes	Yes	No
F5 Networks	F5 Networks BIG-IP APM 10.x to 14.x	Syslog	All events	Yes	No	No
F5 Networks	FirePass 7.0	Syslog	All events	Yes	Yes	No
Fair Warning	Fair Warning 2.9.2	Log File Protocol	All events	No	No	No
Fasoo	Fasoo Enterprise DRM 5.0	JDBC	NVP event format Usage events	No	No	No
Fidelis Security Systems	Fidelis XPS 7.3.x	Syslog	Alert events	Yes	No	No
FireEye	FireEye CMS, MPS, EX, AX, NX, FX, and HX	Syslog, TLS Syslog	Event formats: CEF (CEF:0 is supported), LEEF Recorded event types: All relevant events	Yes	No	No
FreeRADIUS	FreeRADIUS 2.x	Syslog	All events	Yes	Yes	No
Forcepoint	Forcepoint Sidewinder 6.1 (formerly known as McAfee Firewall Enterprise 6.1)	Syslog	Forcepoint Sidewinder audit events	Yes	No	No
Forcepoint	Stonesoft Management Center 5.4 to 6.1	Syslog	Event format: LEEF Event types: Management Center, IPS, Firewall, and VPN events	Yes	No	No
Forcepoint	Forcepoint TRITON 7.7, and 8.2 (formerly known as Websense)	Syslog LEEF	Events for web content from several Forcepoint TRITON solutions, including Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series appliances. All events	Yes	No	No
Forcepoint	Forcepoint V-Series Data Security Suite (DSS) 7.1x (formerly known as Websense)	Syslog	All events	Yes	Yes	Yes

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Forcepoint	Forcepoint V-Series Content Gateway V7.1x (formerley known as Websense)	Log File Protocol	All events	No	No	No
ForeScout	CounterACT 7.x and later	Syslog	Denial of Service, system, exploit, authentication, and suspicious events	No	No	No
Fortinet	Fortinet FortiGate Security Gateway FortiOS 6.4 and earlier	Syslog Syslog Redirect	All events	Yes	Yes	Yes
Foundry	FastIron 3.x.x and 4.x.x	Syslog	All events	Yes	Yes	No
genua	genugate 8.2+	Syslog	General error messages High availability General relay messages Relay-specific messages genua programs/daemons EPSI Accounting Daemon - gg/src/acctd Configfw FWConfig ROFWConfig User-Interface Webserver	Yes	Yes	No
Google	Google Cloud Audit Logs	Google Cloud Pub/Sub	Supported services: • Google Compute Engine • Identity Access Management • Identity Platform • Cloud Storage Event format: JSON Event types: Storage, list, update	Yes	No	No
Google	Google Cloud Platform Firewall	Google Cloud Pub/Sub	Event format: JSON Event types: Firewall Allow, Firewall Deny	No	No	No
Google	Google G Suite Activity Reports	Google G Suite Activity Reports REST API	Event format: JSON Recorded event types: Admin, drive, login, user accounts	No	No	No
Great Bay	Beacon	Syslog	All events	Yes	Yes	No
H3C Technologies	H3C Comware Platform, H3C Switches, H3C Routers, H3C Wireless LAN Devices, and H3C IP Security Devices version 7 is supported	Syslog	NVP System	No	No	No
HBGary	Active Defense 1.2 and later	Syslog	All events	Yes	No	No
Hewlett Packard Enterprise	HPE Network Automation 10.11	Syslog LEEF	All operational and configuration network events.	Yes	Yes	No
Hewlett Packard Enterprise	HPE ProCurve K.14.52	Syslog	All events	Yes	No	No
Hewlett Packard Enterprise	HPE Tandem	Log File Protocol	Safe Guard Audit file events	No	No	No
Hewlett Packard Enterprise	HPE UX V11.x and later	Syslog	All events	No	Yes	No
Honeycomb Technologies	Lexicon File Integrity Monitor mesh service V3.1 and later	Syslog	integrity events	Yes	No	No
Huawei	S Series Switch S5700, S7700, and S9700 using V200R001C00	Syslog	IPv4 events from S5700, S7700, and S9700 Switches	No	No	No
Huawei	AR Series Router (AR150, AR200, AR1200, AR2200, and AR3200 routers using V200R002C00)	Syslog	IPv4 events	No	No	No
IBM	IBM AIX V6.1 and V7.1	Syslog, Log File protocol	Configured audit events	Yes	No	No
IBM	IBM AIX 5.x, 6.x, and v7.x	Syslog	Authentication and operating system events	Yes	Yes	No
IBM	IBM BigFixV8.2.x to 9.5.2 (formerly known as Tivoli EndPoint Manager)	IBM BigFix SOAP Protocol	Server events	No	Yes	No
IBM	IBM BigFix Detect **Note:** The IBM BigFix Detect DSM for QRadar is deprecated.					
IBM	IBM Bluemix Platform (now known as IBM Cloud Platform)					
IBM	IBM Cloud Activity Tracker	Apache Kafka protocol	Event format: JSON	Yes	No	No
IBM	IBM Cloud Identity (now known as IBM Security Verify					

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
IBM	IBM Cloud Platform (formerly known as IBM Bluemix Platform)	Syslog, TLS Syslog	All System (Cloud Foundry) events, some application events	Yes	No	No
IBM	IBM DLC Metrics	Syslog, Forwarded	Event format: LEEF Recorded event types: All DLC Metrics event types	Yes	No	No
IBM	IBM Federated Directory Server V7.2.0.2 and later	LEEF	FDS Audit	Yes	No	No
IBM	IBM Guardium 8.2p45	Syslog	Policy builder events	No	No	No
IBM	IBM Security Guardium Insights	Syslog	Out of Box Policy Violation Rules	Yes	No	No
IBM	IBM i DSM V5R4 and later (formerly known as AS/400iSeries)	Log File Protocol	Event format: • CEF (CEF:0 is supported.) • LEEF (LEEF:1.0 is supported.) Recorded event types: All security events	No	Yes	No
IBM	IBM i - Robert Townsend Security Solutions V5R1 and later (formerly known as AS/400iSeries)	Syslog	Event format: • CEF (CEF:0 is supported.) • LEEF (LEEF:1.0 is supported.) Recorded event types: All security events	Yes	Yes	No
IBM	IBM i - Powertech Interact V5R1 and later (formerly known as AS/400iSeries)	Syslog	Event format: • CEF (CEF:0 is supported.) • LEEF (LEEF:1.0 is supported.) Recorded event types: All security events	Yes	Yes	No
IBM	IBM ISS Proventia M10 v2.1_2004.1122_15.13.53	SNMP	All events	No	No	No
IBM	IBM Lotus Domino v8.5	SNMP	All events	No	No	No
IBM	IBM Proventia Management SiteProtector v2.0 and v2.9	JDBC	IPS and audit events	No	No	No
IBM	IBM RACF v1.9 to v1.13	Log File Protocol	All events	No	No	Yes
IBM	IBM CICS v3.1 to v4.2	Log File Protocol	All events	No	No	Yes
IBM	IBM DB2 v8.1 to v10.1	Log File Protocol	All events	No	No	Yes
IBM	IBM DataPower FirmwareV6 and V7 (formerly known as WebSphere DataPower)	Syslog	All events	Yes	No	No
IBM	IBM MaaS360 Security (formerly known as IBM Fiberlink MaaS360)	LEEF, JSON	Compliance rule events Device enrollment events Action history events	No	Yes	No
IBM	IBM QRadar Packet Capture IBM QRadar Packet Capture V7.2.3 to V7.2.8 IBM QRadar Network Packet Capture V7.3.0	Syslog, LEEF	All events	Yes	No	No
IBM	IBM Red Hat OpenShift V5.2.4	Syslog	Event format: JSON Event types: Audit and Infrastructure	Yes	No	Yes
IBM	IBM SAN Volume Controller	Syslog	CADF event format Activity, Control, and Monitor audit events	Yes	No	No
IBM	IBM z/OS v1.9 to v1.13	Log File Protocol	All events	No	No	Yes
IBM	IBM Informix v11	Log File Protocol	All events	No	No	No
IBM	IBM IMS	Log File Protocol	All events	No	No	No
IBM	Security Access Manager for Mobile (ISAM)	TLS Syslog	IBM_SECURITY_AUTHN IBM_SECURITY_TRUST IBM_SECURITY_RUNTIME IBM_SECURITY_CBA_AUDIT_MGMT IBM_SECURITY_CBA_AUDIT_RTE IBM_SECURITY_RTSS_AUDIT_AUTHZ IBM_SECURITY_SIGNING CloudOE Operations Usage IDaaS Appliance Audit IDaaS Platform Audit	Yes	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
IBM	Security Identity Governance (ISIG)	JDBC	NVP event format Audit event type	No	No	No
IBM	QRadar Network Security XGS v5.0 with fixpack 7 to v5.4	Syslog	System, access, and security events	Yes	No	No
IBM	Security Network IPS (GX) v4.6 and later	Syslog	Security, health, and system events	Yes	No	No
IBM	Security Privileged Identity Manager V1.0.0 to V2.1.1	JDBC	Audit, authentication and system events	No	No	No
IBM	Security Identity Manager 6.0.x and later	JDBC	Audit and recertification events	No	Yes	No
IBM	IBM Security Randori Recon	IBM Security Randori REST API	Event format: JSON Event types: Detections	Yes	No	No
IBM	IBM Security QRadar EDR v3.9.0 (formerly known as IBM Security ReaQta)	IBM Security ReaQta REST API	Event format: JSON Event types: Alerts	Yes	No	Yes
IBM	IBM Security Trusteer	HTTP Receiver	Event format: JSON Event types: Trusteer alerts	Yes	No	No
IBM	IBM Security Trusteer Apex Advanced Malware Protection	Syslog/LEEF Log File Protocol	Malware Detection Exploit Detection Data Exfiltration Detection Lockdown for Java Event File Inspection Event Apex Stopped Event Apex Uninstalled Event Policy Changed Event ASLR Violation Event ASLR Enforcement Event Password Protection Event	Yes	Yes	No
IBM	IBM Sense v1	Syslog	LEEF	Yes	No	No
IBM	IBM SmartCloud Orchestrator v2.3 FP1 and later	IBM SmartCloud Orchestrator REST API	Audit Records	No	Yes	No
IBM	IBM Security Verify (formerly known as IBM Cloud Identity)	JSON	Authentication SSO Management Threat	No	Yes	Yes
IBM	Tivoli Access Manager IBM Web Security Gateway v7.x	Syslog	audit, access, and HTTP events	Yes	Yes	No
IBM	Tivoli Endpoint Manager (now known asIBM BigFix)					
IBM	WebSphere Application Server v5.0 to v8.5	Log File Protocol	All events	No	Yes	No
IBM	WebSphere DataPower (now known as DataPower) WebSphere DataPower					
IBM	zSecure Alert v1.13.x and later	UNIX syslog	Alert events	Yes	Yes	No
IBM	Security Access Manager v8.1 and v8.2	Syslog	Audit, system, and authentication events	Yes	No	No
IBM	Security Verify Directory v6.3.1 and later (formerly known as Security Directory Server)	Syslog LEEF	All events	Yes	Yes	No
Illumio	Illumio Adaptive Security Platform	Syslog LEEF	Audit Traffic	Yes	No	No
Imperva	Incapsula	LEEF	Access events and Security alerts	Yes	No	No
Imperva	SecureSphere v6.2 and v7.x to v13 Release Enterprise Edition (Syslog) SecureSphere v9.5 to v13 (LEEF) cy	Syslog LEEF	Firewall policy events	Yes	No	No
Infoblox NIOS	Infoblox NIOS 6.x to 8.x	Syslog	ISC Bind Linux DHCP Linux Server Apache	No	Yes	No
Internet Systems Consortium (ISC)	ISC BIND 9.9, 9.11, 9.12	Syslog	All events	Yes	No	No
Intersect Alliance	SNARE Enterprise Windows Agent	Syslog	Microsoft Event Logs	Yes	Yes	No
iT-CUBE	agileSI 1.x	SMB Tail	AgileSI SAP events	No	Yes	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Itron	Openway Smart Meter	Syslog	All events	Yes	No	No
Juniper Networks	AVT	JDBC	All events	No	No	Yes
Juniper Networks	DDoS Secure Juniper Networks DDoS Secure is now known as NCC Group DDoS Secure.				No	No
Juniper Networks	DX The Juniper Networks DX Platform product is end of life (EOL), and is no longer supported by Juniper.	Syslog	Status and network condition events	Yes	No	Yes
Juniper Networks	Infranet Controller The Juniper Networks Infranet Controller DSM for IBM QRadar is now known as Pulse Secure Infranet Controller.					
Juniper Networks	Firewall and VPN v5.5r3 and later	Syslog	NetScreen Firewall events	Yes	Yes	Yes
Juniper Networks	Junos WebApp Secure v4.2.x	Syslog	Incident and access events	Yes	No	No
Juniper Networks	IDP v4.0, v4.1 & v5.0	Syslog	NetScreen IDP events	Yes	No	Yes
Juniper Networks	Network and Security Manager (NSM) and Juniper SSG v2007.1r2 to 2007.2r2, 2008.r1, 2009r1.1, 2010.x	Syslog	NetScreen NSM events	Yes	No	Yes
Juniper Networks	Junos OS 7.x to 10.x Ex Series Ethernet Switch DSM only supports 9.0 to 10.x	Syslog or PCAP Syslog***	All events	Yes**	Yes	Yes
Juniper Networks	Secure Access Juniper Networks Secure Access is now known as Pulse Secure Pulse Connect Secure.					Yes
Juniper Networks	Juniper Security Binary Log Collector SRX or J Series appliances at 12.1 or above	Binary	Audit, system, firewall, and IPS events	No	No	Yes
Juniper Networks	Steel-Belted Radius 5.x	Log File	All events	Yes	Yes	Yes
Juniper Networks	vGW Virtual Gateway 4.5 The Juniper Networks vGW Virtual Gateway product is end of life (EOL), and is no longer supported by Juniper.	Syslog	Firewall, admin, policy and IDS Log events	Yes	No	No
Juniper Networks	Wireless LAN Controller Wireless LAN devices with Mobility System Software (MSS) V7.6 and later	Syslog	All events	Yes	No	No
Kisco	Kisco Information Systems SafeNet/i 10.11	Log File	All events	No	No	No
Kubernetes	Kubernetes Auditing	Syslog	Event format: JSON Recorded event types: RequestReceived, ResponseStarted, ResponseComplete	Yes	No	Yes
Lastline	Lastline Enterprise 6.0	LEEF	Anti-malware	Yes	No	No
Lieberman	Random Password Manager 4.8x	Syslog	All events	Yes	No	No
LightCyber	LightCyber Magna 3.9	Syslog, LEEF	C&C, exfilt, lateral, malware and recon	Yes	No	No
Linux	Open Source Linux OS 2.4 and later	Syslog	Operating system events	Yes	Yes	No
Linux	DHCP Server 2.4 and later	Syslog	All events from a DHCP server	Yes	Yes	No
Linux	IPtables kernel 2.4 and later	Syslog	Accept, Drop, or Reject events	Yes	No	No
McAfee	McAfee Application / Change Control v4.5.x	JDBC	Change management events	No	Yes	No
McAfee	McAfee ePolicy Orchestrator 3.5 to 5.10	JDBC: 3.5 to 5.9 SNMPv1, SNMPv2, SNMPv3: 3.5 to 5.9 TLS Syslog: 5.10	AntiVirus events	No	No	No
McAfee	McAfee MVISION Cloud 2.4 and 3.3 (formerly known as Skyhigh Networks Cloud Security Platform)	Syslog	Event format: Log Event Extended Format (LEEF) Recorded event types: Privilege Access, Insider Threat, Compromised Account, Access, Admin, Data, Policy, and Audit	Yes	No	No
McAfee	McAfee Network Security Platform 2.x - 5.x (Formerly known as McAfee Intrushield)	Syslog	Alert notification events **Important:** Supported alert notification events do not include custom events with IDs that begin with Oxc, Oxcc, Oxe, or Oxee.	Yes	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
McAfee	McAfee Network Security Platform 6.x - 7.x and 8.x - 10.x (Formerly known as McAfee Intrushield)	Syslog	Alert and fault notification events **Important:** Supported alert notification events do not include custom events with IDs that begin with Oxc, Oxcc, Oxe, or Oxee.	Yes	No	No
McAfee	McAfee Web Gateway 6.0.0	Syslog Log File protocol	Event format: LEEF Recorded event types: All events	Yes	No	No
MetaInfo	MetaIP 5.7.00-6059	Syslog	All events	Yes	Yes	No
Microsoft	Microsoft 365 Defender **Important:** The Microsoft Windows Defender ATP DSM is now the Microsoft 365 Defender DSM. The DSM RPM name remains as Microsoft Windows Defender ATP in QRadar.	Microsoft Defender for Endpoint SIEM REST API Microsoft Azure Event Hubs Microsoft Graph Security API	**Event format:** JSON The Microsoft 365 Defender DSM supports the following events when you use the Microsoft Azure Event Hubs protocol: Alerts (Alerts are supported only for Microsoft Defender for Endpoint.): • AlertInfo • AlertEvidence Device: • DeviceInfo • DeviceNetworkInfo • DeviceProcessEvents • DeviceNetworkEvents • DeviceFileEvents • DeviceRegistryEvents • DeviceLogonEvents • DeviceEvents • DeviceFileCertificateInfo • DeviceImageLoadEvents Email: • EmailEvents • EmailAttachmentInfo • EmailPostDeliveryEvents • EmailUrlInfo The Microsoft 365 Defender DSM supports the following events when you use the Microsoft Defender for Endpoint REST API protocol: • Windows Defender ATP • Windows Defender AV • Third party TI • Customer TI • Bitdefender The Microsoft 365 Defender DSM supports the following events when you use the Microsoft Graph Security API protocol: • Microsoft Defender for Endpoint Alerts V2 • Microsoft Defender for Cloud App Security Alerts V2 • Microsoft Defender for Identity Alerts V2 • Microsoft Defender for Office 365 Alerts V2 • Microsoft Defender for Azure AD Identity Protection Alerts V2 • Microsoft Defender for Data Loss Prevention Alerts V2	Yes	Yes	No
Microsoft	Microsoft Entra ID (formerly Microsoft Azure Active Directory)	Microsoft Azure Event Hubs	Event format: JSON Recorded event types: Sign-In logs, Audit logs	Yes	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Microsoft	Microsoft Azure Platform	Microsoft Azure Event Hubs	Event format: JSON Recorded event types: Platform level activity logs For more information about Platform level activity logs, see Azure Resource Manager resource provider operations (https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations). **Note:** This DSM automatically discovers only Activity Log Events that are forwarded directly from the Activity Log to the Event Hub.	Yes	No	No
Microsoft	Microsoft Defender for Cloud **Important:** The Microsoft Azure Security Center DSM is now the Microsoft Defender for Cloud DSM. The DSM RPM name remains as Microsoft Azure Security Center in QRadar.	Microsoft Graph Security API Microsoft Azure Event Hubs	Event format: JSON Recorded event types: Security alert	No	No	No
Microsoft	DNS Debug Supported versions: Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2	WinCollect Microsoft DNS Debug	LEEF	Yes	Yes	No
Microsoft	IIS 6.0, 7.0 and 8.x	Syslog and WinCollect	HTTP status code events	Yes	No	No
Microsoft	Internet and Acceleration (ISA) Server or Threat Management Gateway 2006	Syslog and WinCollect	ISA or TMG events	Yes	No	No
Microsoft	Microsoft Exchange Server 2003, 2007, 2010, 2013, 2016 and 2019	Windows Exchange Protocol	Outlook Web Access events (OWA) Simple Mail Transfer Protocol events (SMTP Message Tracking Protocol events (MSGTRK)	No	No	No
Microsoft	Endpoint Protection 2012	JDBC	Malware detection events	No	No	No
Microsoft	Microsoft Hyper-V supported versions: Windows Server 2016 Windows Server 2012 (most recent) Windows Server 2012 Core Windows Server 2008 (most recent) Windows Server 2008 Core Windows 10 (most recent) Windows 8 (most recent) Windows 7 (most recent) Windows Vista (most recent)	WinCollect	All events	No	No	No
Microsoft	IAS Server v2000, 2003, and 2008	Syslog	All events	Yes	No	No
Microsoft	Microsoft Office 365	Office 365 REST API	JSON	No	No	No
Microsoft	Microsoft Office 365 Message Trace	Office 365 Message Trace REST API	Event format: JSON Event types: Email security threat classification	No	No	No
Microsoft	Microsoft Windows Defender ATP	Microsoft Defender for Endpoint REST API	Event format: JSON Event types: Windows Defender ATP Windows Defender AV Third Party TI Customer TI Bitdefender	No	No	No
Microsoft	Microsoft Windows Security Event Log supported versions: Windows Server 2016 Windows Server 2012 (most recent) Windows Server 2012 Core Windows Server 2008 (most recent) Windows Server 2008 Core Windows 10 (most recent) Windows 8 (most recent) Windows 7 (most recent) Windows Vista (most recent)	Syslog Forwarded TLS Syslog TCP Multiline Syslog Windows Event Log (WMI) Windows Event Log Custom (WMI) MSRPC WinCollect WinCollect NetApp Data ONTAP	All events, including Sysmon and winlogbeats.json	Yes	Yes	Yes
Microsoft	SQL Server 2008, 2012, 2014 (Enterprise editions only), and 2016	Syslog, JDBC and WinCollect	SQL Audit events	No	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Microsoft	SharePoint 2010 and 2013	JDBC	SharePoint audit, site, and file events	No	No	No
Microsoft	DHCP Server 2000/2003	Syslog and WinCollect	All events	Yes	Yes	No
Microsoft	Operations Manager 2005	JDBC	All events	No	No	No
Microsoft	System Center Operations Manager 2007	JDBC	All events	No	No	No
Motorola	Symbol AP firmware 1.1 to 2.1	Syslog	All events	No	No	No
NCC Group	NCC Group DDos 5.13.1-2s to 516.1-0	Syslog	Event format: LEEF Event types: All events	Yes	No	No
Niara	Niara 1.6	Syslog	Security System Internal Activity Exfiltration Infection Command & Control	Yes	No	Yes
NetApp	Data ONTAP	WinCollect NetApp Data ONTAP	CIFS events	Yes	Yes	No
Netgate	Netgate pfSense	Syslog	System Firewall DNS DHCP (when you use the Linux DHCP DSM)	Yes	Yes	No
Netskope	Netskope Active **Important:** The IBM QRadar DSM for Netskope Active is deprecated. To continue taking advantage of this integration, please download the Netskope Security Cloud DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/ff97aaadc10ed96b0e05d1a1f24af2f7).	Netskope Active REST API	Alert, All events	No	Yes	No
NGINX	NGINX HTTP Server 1.15.5	Syslog	Syslog, Standard syslog	Yes	No	No
Niksun	NetVCR 2005 v3.x	Syslog	Niksun events	No	No	No
Nokia	Firewall NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later	Syslog or OPSEC LEA	All events	Yes	Yes	No
Nokia	VPN-1 NG FP1, FP2, FP3, AI R54, AI R55, NGX on IPSO v3.8 and later	Syslog or OPSEC LEA	All events	Yes	Yes	No
Nominum	Vantio v5.3 **Note:** The Nominum Vantio DSM for QRadar is deprecated.					
Nortel	Contivity	Syslog	All events	Yes	No	No
Nortel	Application Switch v3.2 and later	Syslog	Status and network condition events	No	Yes	No
Nortel	ARN v15.5	Syslog	All events	Yes	No	No
Nortel*	Ethernet Routing Switch 2500 v4.1	Syslog	All events	No	Yes	No
Nortel*	Ethernet Routing Switch 4500 v5.1	Syslog	All events	No	Yes	No
Nortel*	Ethernet Routing Switch 5500 v5.1	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 8300 v4.1	Syslog	All events	No	Yes	No
Nortel	Ethernet Routing Switch 8600 v5.0	Syslog	All events	No	Yes	No
Nortel	VPN Gateway v6.0, 7.0.1 and later, v8.x	Syslog	All events	Yes	Yes	No
Nortel	Secure Router v9.3, v10.1	Syslog	All events	Yes	Yes	No
Nortel	Secure Network Access Switch v1.6 and v2.0	Syslog	All events	Yes	Yes	No
Nortel	Switched Firewall 5100 v2.4	Syslog or OPSEC	All events	Yes	Yes	No
Nortel	Switched Firewall 6000 v4.2	Syslog or OPSEC	All events	Yes	Yes	No
Nortel	Threat Protection System v4.6 and v4.7	Syslog	All events	No	No	No
Novell	eDirectory v2.7	Syslog	All events	Yes	No	No
ObserveIT	ObserveIT 5.7.x and later	JDBC	Alerts User Activity System Events Session Activity DBA Activity	No	Yes	No
Okta	Okta Identity Management	Okta REST API	JSON	No	Yes	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Onapsis	Onapsis Security Platform v1.5.8 and later	Log Event Extended Format (LEEF)	Assessment Attack signature Correlation Compliance	Yes	No	No
OpenBSD Project	OpenBSD v4.2 and later	Syslog	All events	No	Yes	No
Open Information Security Foundation (OISF)	Suratica v6.0.3 and earlier	Syslog TLS Syslog	Event format: JSON Recorded event types: Alerts	Yes	No	No
Open LDAP Foundation	Open LDAP 2.4.x	UDP Multiline Syslog	All events	No	No	No
Open Source	SNORT v2.x	Syslog	All events	Yes	No	No
OpenStack	OpenStack v2015.1	HTTP Reciever	Audit events	No	No	No
Oracle	Oracle RDBMS Audit Record versions 9i, 10g, 11g, 12c (includes unified auditing)	JDBC, Syslog	Event format: Name-Value Pair Recorded event types: Audit records	Yes	Yes	No
Oracle	Audit Vault V10.3 and V12.2	JDBC	All audit records from the AVSYS.AV$ALERT_STORE table for V10.3, or from the custom AVSYS.AV_ALERT_STORE_V view for V12.2.	No	Yes	No
Oracle	Oracle OS Audit 9i, 10g, and 11g	Syslog	Event format: name-value pair (NVP) Event types: Oracle events	Yes	Yes	No
Oracle	Oracle BEA WebLogic 12.2.1.3.0	Log File	Oracle events	No	No	No
Oracle	Oracle Database Listener 9i, 10g, and 11g	Syslog	Oracle events	Yes	No	No
Oracle	Oracle Directory Server (Formerly known as Sun ONE LDAP).					
Oracle	Oracle Fine Grained Auditing 9i and 10g	JDBC	Select, insert, delete, or update events for tables configured with a policy	No	No	No
N/A	osquery 3.3.2	Syslog TCP Multiline Syslog	Event format: JSON Event type: Access Audit Authentication System	No	No	Yes
OSSEC	OSSEC 2.6 and later	Syslog	All relevant	Yes	No	No
Palo Alto Networks	Palo Alto PA Series	Syslog TLS Syslog	**Event types:** Traffic Threat Config System HIP Match Authentication Tunnel Inspection (for PAN-OS 8.0 - 9.1) or Tunnel (for PAN-OS 10.0) Correlation SCTP File Data GTP HIP Match IP-Tag Global Protect - **Important:** To use this log type, you must enable the **EventStatus/ Status** field on your Palo Alto PA Series device. Decryption User ID URL Filtering (for PAN-OS 8.0 - 9.1) or URL (for PAN-OS 10.0) WildFire **Event Formats:** LEEF for PAN-OS v3.0 to v10.2, and Prisma Access v2.1 CEF for PAN-OS v4.0 to v6.1 (CEF:0 is supported)	Yes	Yes	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Palo Alto Networks	Palo Alto Endpoint Security Manager 3.4.2.17401	Syslog	Agent Config Policy System Threat Event formats: CEF (CEF:0 is supported), LEEF	Yes	No	No
Ping Identity	PingFederate	Syslog	Event format: CEF	Yes	No	No
Pirean	Access: One 2.2 with DB2 9.7	JDBC	Access management and authentication events	No	No	No
PostFix	Mail Transfer Agent 2.6.6 and later	UDP Multiline Protocol or Syslog	Mail events	No	No	No
ProFTPd	ProFTPd 1.2.x, 1.3.x	Syslog	All events	Yes	Yes	No
Proofpoint	Proofpoint Enterprise Protection and Enterprise Privacy versions 7.0.2, 7.1, 7.2, 7.5, 8.0	Syslog Log File	Event types: System Email security threat classification Email audit and encryption	No	No	No
Pulse Secure	Pulse Secure Infranet Controller 2.1, v3.1 and 4.0	Syslog	All events	No	Yes	Yes
Pulse Secure	Pulse Secure Pulse Connect Secure 8.2R5	Syslog TLS Syslog	Event types: Admin Authentication System Network Error	Yes	Yes	Yes
Radware	AppWall 6.5.2 and 8.2	Syslog	Event types: Administration Audit Learning Security System	Yes	No	No
Radware	DefensePro 4.23, 5.01, 6.x and 7.x	Syslog	All events (Event mapping is required when Event IDs are 300,000 or more.) **Tip:** If you have custom events that display as unknown in QRadar, see the IBM Support article about QRadar: Custom events for Radware DefensePro display 'parsed, but not mapped' (https://www.ibm.com/support/pages/node/6960301).	Yes	No	No
Raz-Lee iSecurity	IBM i Firewall 15.7 and Audit 11.7	Syslog	Security, compliance, firewall, and audit events	Yes	Yes	No
Redback Networks	ASE 6.1.5	Syslog	All events	Yes	No	No
Red Hat	Red Hat Advanced Cluster Security for Kubernetes	HTTP Receiver	JSON Recorded event types: audit and alert events	Yes	No	No
Resolution1	Resolution1 CyberSecurity Formerly known as AccessData InSight Resolution1 CyberSecurity.	Log file	Volatile Data, Memory Analysis Data, Memory Acquisition Data, Collection Data, Software Inventory, Process Dump Data, Threat Scan Data, Agent Remediation Data	No	No	No
Riverbed	SteelCentral NetProfiler	JDBC	Alert events	No	No	No
Riverbed	SteelCentral NetProfiler Audit	Log file protocol	Audit events	No	Yes	No
RSA	Authentication Manager 6.x, 7.x, and 8.x	v6.x and v7.x use Syslog or Log File Protocol v8.x uses Syslog only	All events	No	No	No
SafeNet	DataSecure 6.3.0 and later	Syslog	All events	Yes	No	No
Salesforce	Salesforce Security Auditing	Log File	Setup Audit Records	No	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Salesforce	Salesforce Security	Salesforce REST API Protocol	Login History Account History Case History Entitlement History Service Contract History Contract Line Item History Contract History Contact History Lead History Opportunity History Solution History Salesforce Security Auditing audit trail	No	Yes	No
Samhain Labs	HIDS 2.4	Syslog JDBC	All events	Yes	No	No
SAP	SAP Enterprise Threat Detection V1.0 SP6 to V2.0 SP5	SAP Enterprise Threat Detection Alert API	LEEF	No	No	No
Seculert	Seculert v1	Seculert Protection REST API Protocol	All malware communication events	No	No	No
Seculert	Seculert	Seculert protection REST API Protocol	All malware communication events	No	No	No
Sentrigo	Hedgehog 2.5.3	Syslog	All events	Yes	No	No
Snowflake	Snowflake	JDBC	Event format: Name value pair (NVP)	Yes	Yes	No
Skyhigh Networks (now known as McAfee)	Skyhigh Networks Cloud Security Platform 2.4 and 3.3 (now known as McAfee MVISION Cloud 2.4 and 3.3)					
SolarWinds	SolarWinds Orion 2011.2	Syslog	All events	No	No	No
SonicWALL	UTM/Firewall/VPN Appliance 3.x and later	Syslog	All events	Yes	No	No
Sophos	Sophos Astaro Security Gateway 17.x	Syslog	All events	Yes	No	No
Sophos	Sophos Enterprise Console 4.5.1 and 5.1	Sophos Enterprise Console protocol JDBC protocol	All relevant anti-virus events	No	No	No
Sophos	Sophos PureMessage 3.1.0.0 for Microsoft Exchange 5.6.0 for Linux	JDBC	Quarantined email events	No	No	No
Sophos	Sophos Web Security Appliance 3.x	Syslog	Transaction log events	Yes	No	No
Sourcefire	Sourcefire Intrusion Sensor IS 500, 2.x, 3.x, 4.x	Syslog	All events	Yes	No	No
Sourcefire	Sourcefire Defense Center (Now known as Cisco FireSIGHT Mangement Center)					
Splunk	MicrosoftWindows Security Event Log	Windows-based event provided by Splunk Forwarders	All events	No	Yes	No
Squid	Squid Web Proxy 2.5 and later	Syslog	All cache and access log events	Yes	No	No
Startent Networks	Startent Networks	Syslog	All events	Yes	No	No
STEALTHbits Technologies	STEALTHbits File Activity Monitor	Syslog LEEF	File Activity Monitor Events			
STEALTHbits Technologies	StealthINTERCEPT	Syslog LEEF	Active Directory Audit Events	Yes	No	No
STEALTHbits Technologies	STEALTHbits StealthINTERCEPT Alerts	Syslog LEEF	Active Directory Alerts Events	Yes	No	No
STEALTHbits Technologies	STEALTHbits StealthINTERCEPT Analytics	Syslog LEEF	Active Directory Analytics Events	Yes	No	No
Sun	Sun Solaris DHCP 2.8	Syslog	All events	Yes	Yes	No
Sun	Sun Solaris OS 5.8, 5.9	Syslog	All events	Yes	Yes	No
Sun	Sun Solaris Sendmail 2.x	Syslog Log File Protocol Proofpoint 7.5 and 8.0 Sendmail log	All events	Yes	No	No
Sun	Sun Solaris Basic Security Mode (BSM) 5.10 and 5.11	Log File Protocol	All events	No	Yes	No
Sun	Sun ONE LDAP v11.1 (Known as Oracle Directory Server)	Log File Protocol UDP Multiline Syslog	All relevant access and LDAP events	No	No	No
Sybase	Sybase ASE 15.0 and later	JDBC	All events	No	No	No
Symantec	Symantec Endpoint Protection 11, 12, and 14	Syslog	All Audit and Security Logs	Yes	No	Yes
Symantec	Symantec SGS Appliance 3.x and later	Syslog	All events	Yes	No	Yes

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Symantec	Symantec SSC 10.1	JDBC	All events	Yes	No	No
Symantec	Symantec Data Loss Prevention (DLP) 8.x	Syslog	All events	No	No	No
Symantec	Symantec Encryption Management Server 3.0x formerly known as PGP Universal Server	Syslog	All events	Yes	No	No
Symark	Symark PowerBroker 4.0	Syslog	All events	Yes	No	No
SysFlow is an open source project initiated by IBM.	SysFlow 1.0	Syslog	Event format: JSON Recorded event types: SysFlow	Yes	No	No
ThreatGRID	Malware Threat Intelligence Platform 2.0	Log file protocol Syslog	Malware events	No	No	No
TippingPoint	Intrusion Prevention System (IPS) 1.4.2 to 3.2.x TippingPoint SMS 5.2.0	Syslog	All events	No	No	No
TippingPoint	X505/X506 2.5 and later	Syslog	All events	Yes	Yes	No
Top Layer	IPS 5500 4.1 and later	Syslog	All events	Yes	No	No
Trend Micro	Trend Micro Apex Central (version 1)	Syslog, TLS syslog	Event format: CEF Event types: Attack discovery detection logs Behavior monitoring logs C&C callback logs Content security logs Data loss prevention logs Device access control logs Endpoint application control logs Engine update status logs Intrusion prevention logs Network content inspection logs Pattern Update Status Logs Predictive machine learning logs Sandbox detection logs Spyware/Grayware logs Suspicious file logs Virus/Malware logs Web security logs	Yes	No	No
Trend Micro	Trend Micro Apex One 8.x and 10.x Formerly known as Trend Micro Office Scan. The name remains the same in QRadar.	SNMPv2	All events	No	No	No
Trend Micro	Trend Micro Control Manager 5.0 or 5.5 with hotfix 1697 or hotfix 1713 after SP1 Patch 1; 6.0 and 7.0.	SNMPv1 SNMPv2 SNMPv3	All events	Yes	No	No
Trend Micro	Trend Micro Deep Discovery Analyzer 5.0, 5.5, 5.8 and 6.0	Syslog	Event format: LEEF Events: All events	Yes	No	No
Trend Micro	Trend Micro Deep Discovery Director 3.0	Syslog	Event format: LEEF Events: Trend Micro Deep Discovery Inspector events	Yes	No	No
Trend Micro	Trend Micro Deep Discovery Email Inspector 3.0	Syslog	Event format: LEEF Events: Detections, Virtual Analyzer Analysis logs, System events, Alert events	Yes	No	No
Trend Micro	Trend Micro Deep Discovery Inspector 3.0 to V3.8, 5.0 and 5.1	Syslog	Event format: LEEF Events: Malicious content Malicious behavior Suspicious behavior Exploit Grayware Web reputation Disruptive application Sandbox Correlation System Update	Yes	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Trend Micro	Trend Micro Deep Security 9.6.1532 to 12.0	Syslog	Event format: LEEF Events: Anti-Malware Deep Security Firewall Integrity Monitor Intrusion Prevention Log Inspection System Web Reputation	Yes	No	No
Tripwire	Tripwire Enterprise Manager 5.2 and later	Syslog	Event format: CEF (CEF:0 is supported) Event types: Resource additions, removal, and modification events	Yes	No	No
Tropos Networks	Tropos Control 7.7	Syslog	Fault management, login/ logout, provision, and device image upload events	No	No	No
Trusteer	Apex Local Event Aggregator 1304.x and later	Syslog	Malware, exploit, and data exfiltration detection events	Yes	No	No
Vectra Networks	Vectra Networks Vectra v2.2 **Important:** The IBM QRadar DSM for Vectra Networks Vectra is deprecated. To continue taking advantage of this integration, please download the Vectra Networks Vectra DSM from the IBM Security App Exchange website (https://exchange.xforce.ibmcloud.com/hub/extension/47f3e9afff5e0281d6684bb633d769f2).	Syslog	Host scoring, command and control, botnet activity, reconaissance, lateral movement, exfiltration Event format: CEF (CEF:0 is supported)	Yes	No	No
Verdasys	Digital Guardian 6.0.x (Syslog only) Digital Guardian 6.1.1 and 7.2 (LEEF only)	Syslog	Event format: LEEF Events: All events	Yes	No	No
Vericept	Content 360 up to 8.0	Syslog	All events	Yes	No	No
VMware	VMware AppDefense 1.0	JSON VMWare AppDefense API protocol	All events	No	No	No
VMware	Carbon Black App Control 8.0.x to 8.5.x (Formerly known as Carbon Black Protection)	Syslog	Event format: LEEF Event types: computer management, server management, session management, policy management, policy enforcement, internal events, general management, discovery	Yes	Yes	No
VMware	VMware ESX or ESXi 3.x, 4.x, 5.x and 6.x	Syslog EMC VMware protocol	Account Information Notice Warning Error System Informational System Configuration System Error User Login Misc Suspicious Event Access Denied License Expired Information Authentication Session Tracking	Yes if syslog	No	No
VMware	VMware vCenter v5.x and v6.x	EMC VMware protocol	Account Information Notice Warning Error System Informational System Configuration System Error User Login Misc Suspicious Event Access Denied License Expired Information Authentication Session Tracking	No	No	No
VMware	VMware vCloud Director 5.1 - 10.0	VMware vCloud Director protocol	All events	No	Yes	No
VMware	VMware vShield	Syslog	All events	Yes	No	No

Table 1046. QRadar Supported DSMs (continued)

Manufacturer	Device name and version	Protocol	Recorded events and formats	Auto discovered?	Includes identity?	Includes custom properties?
Vormetric, Inc.	Vormetric Data Security	Syslog (LEEF)	Audit Alarm Warn Learn Mode System	Yes	No	No
Watchguard	WatchGuard Fireware OS	Syslog	All events	Yes	No	No
Websense (now known as Forcepoint)						
Zscaler	Zscaler Nanolog Streaming Service (Zscaler NSS) 6.0	Syslog HTTP receiver **Important:** When you use the HTTP receiver protocol with Zscaler NSS, you need a certificate that is issued by a certificate authority (CA). It can't be a self-signed certificate because it must be validated by a CA. For more information about certificates and configuring the log source parameters for HTTP receiver, see HTTP Receiver protocol configuration options.	Event format: LEEF Event types: Web log events, Firewall events (including DNS)	Yes	No	No
Zscaler	Zscaler Private Access	Syslog	Event format: LEEF Event types: User Status, App Connector Status, Audit, User Activity	Yes	No	No

Chapter 177. DSMs supported by third-party vendors

Some content extensions on the IBM Security App Exchange are provided by third-party vendors and contain custom DSMs. These third-party DSM integrations are supported by the vendor, not by IBM.

The following table shows the third-party DSMs that are on the IBM Security App Exchange.

Important: New third-party DSMs are continually added to the IBM Security App Exchange, so the data in this table might be incomplete. If you don't see the vendor you're looking for in this table, go to IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub/), and search for the vendor. If you see a warning banner about QRadar CentOS 6 apps, do not install it.

Table 1047. Third-party DSMs that are available on the IBM Security App Exchange

DSM integration	IBM Security App Exchange link
Armis for QRadar - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/2637da558abd1b6253226a02b9bab4af
Armis for QRadar - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/ccf79f6d3a70af1075c233ffa0337ea0
Bitdefender DSM for Qradar	https://exchange.xforce.ibmcloud.com/hub/extension/de133797c363c03147a7acd194bf53e2
Bitglass \xe2\x80\x93 QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/2964681b93fa77e578af37945ba670b9
BlackBerry Extension for QRadar v7.3.3FP6+/7.4.1FP2+/7.4.2+	https://exchange.xforce.ibmcloud.com/hub/extension/63792efddec8f9d0346d7e059847d73a
BlackRidge App for QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/567c57baaa3fc5296b65d4451f3f752a
Canary	https://exchange.xforce.ibmcloud.com/hub/extension/6fee1138eac4f134676b65a5e9f46176
Check Point Dome9 for QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/903f975ff4e6b97c923fa1866be2ba43
Cisco Cloud Security - QRadar v7.4.2+	https://exchange.xforce.ibmcloud.com/hub/extension/ac62d16c6f8a6068424f896155d9ca3c
Cisco Cyber Vision	https://exchange.xforce.ibmcloud.com/hub/extension/32832b26fbcd39dd335bb3de2424854f
Cisco ISE pxGrid - QRadar v.7.3.3 FP6+/7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/4cfd7c7a39ec7df48dc3c56573d38f6e
Claroty CTD DSM	https://exchange.xforce.ibmcloud.com/hub/extension/b5134138c3d8f2780afd7d725c5c8695
Corelight App for IBM QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/cf253b7e3b242ab1d6a64fd397cb2a08
Cortex XDR for QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/d12c3794f142ee334b4bbdc83d10347f
CrowdStrike Falcon Endpoint \xe2\x80\x93 QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/0c71dc2bc326d7a5d535dc29bdc5605c

Table 1047. Third-party DSMs that are available on the IBM Security App Exchange (continued)	
DSM integration	**IBM Security App Exchange link**
CrowdStrike Falcon Intel \xe2\x80\x93 QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/f91001d90862533581024b3bbbb6d993
Cybereason Endpoint Protection Platform - QRadar 7.3.3 FP6+/7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/22cfaa426c5dd24a53e1684a0ebbc7cb
CyberInt Intelligence - 7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/54553b6cecdccb445532db4defaace81
Cybersixgill DVE Feed & Enrichment - QRadar v7.4.1/7.4.2+	https://exchange.xforce.ibmcloud.com/hub/extension/82c9821fae882131f173436827edfe08
Cylance Extension for QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/b7be703eb8dcd1750e5b7a37e74c289d
Cylera DSM	https://exchange.xforce.ibmcloud.com/hub/extension/9f221bbcd181d2a9588c8ce93ae95314
Cynerio DSM	https://exchange.xforce.ibmcloud.com/hub/extension/a1886526d68504b3aff1abb48889face
Darktrace QRadar DSM	https://exchange.xforce.ibmcloud.com/hub/extension/fc32e34c98165fdc3b9ff45f0ba66400
Deep Instinct DSM	https://exchange.xforce.ibmcloud.com/hub/extension/2e6368c3ecc891bca5bf93f9a14fe1f2
Digital Shadows App for QRadar \xe2\x80\x93 QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/544307ec43ed46b2fd34fe8badc33ebd
Dragos Platform QRadar Extension	https://exchange.xforce.ibmcloud.com/hub/extension/e049f59aa88dd568d3b96c41ce85d1b9
Ermes For Enterprise	https://exchange.xforce.ibmcloud.com/hub/extension/7a89255784208489536f3524295cd4ec
Expanse App for QRadar \xe2\x80\x93 QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/aa5d38404f1b7e5081d0ba4c389c3794
ExtraHop App for QRadar - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/0a684c8a09a664e7259bb7a5856f724a
FlowControl	https://exchange.xforce.ibmcloud.com/hub/extension/8c233f87025f5626a901726f27ad84fc
Flowmon ADS Content Pack	https://exchange.xforce.ibmcloud.com/hub/extension/ba24211f9f0de0f7503a4bf09f82dc16
Gigamon ThreatINSIGHT Add-on for QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/ac56691287484db72459e34a072c978c
Google SCC App For QRadar - QRadar v7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/e4644304db756c0113c9c65691bb4704
IBM QRadar Content Extension for Barac	https://exchange.xforce.ibmcloud.com/hub/extension/ab1e4f9f85672764d43fd48de36a7c9c

Table 1047. Third-party DSMs that are available on the IBM Security App Exchange (continued)

DSM integration	IBM Security App Exchange link
IBM Security Verify Privilege Vault (Thycotic Secret Server)	https://exchange.xforce.ibmcloud.com/hub/extension/445961bc985a3610d8b3e83a56b64af3
Illumio App for QRadar v7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/2df4cc0ea8e1c3138169c635c9c9df1d
Indegy Industrial Cyber Security Platform	https://exchange.xforce.ibmcloud.com/hub/extension/fb5525a64f5eec4aa1a63d5929b9266d
IntSights App For QRadar - QRadar v7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/f2f48af32f23ba6ee4e87dc97a29c690
Jeskell CyberSentinel Threat Detector	https://exchange.xforce.ibmcloud.com/hub/extension/Jeskell%20Systems:CyberSentinel
Keeper Security	https://exchange.xforce.ibmcloud.com/hub/extension/d6e6a1f5fbcef53d6440d81c42fb0e10
Lumu - QRadar v7.3.3FP6+/ 7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/a14a2f83281636260d660918b09a4a11
Mandiant Advantage App For QRadar - QRadar 7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/3a996a7812c185dea2bf3731347b8226
Mimecast for QRadar \xe2\x80\x93 QRadar v7.3.3FP8+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/c4723f2da1a832044aad17c7e8a4328f
MistNet	https://exchange.xforce.ibmcloud.com/hub/extension/ef1af12c4e7b5d5efe7f9d09d0591358
Netskope Security Cloud DSM	https://exchange.xforce.ibmcloud.com/hub/extension/ff97aaadc10ed96b0e05d1a1f24af2f7
NeuVector DSM	https://exchange.xforce.ibmcloud.com/hub/extension/f6dcde294cac1237ce08bcd4dfbc9142
NNT Change Tracker	https://exchange.xforce.ibmcloud.com/hub/extension/156bb35041924eace38c32f70edb36fa
Nozomi Networks Sensor - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/d459f6986e4c7a18550d80ed92cea4f5
Onapsis Content Pack	https://exchange.xforce.ibmcloud.com/hub/extension/cc8d1c7f6334b23a75d80faba605b9f9
Ordr SCE v742-1	https://exchange.xforce.ibmcloud.com/hub/extension/f63816ad5533746956e8c462326ebea0
Panda Adaptive Defense DSM	https://exchange.xforce.ibmcloud.com/hub/extension/aa9c0a5772877b6f09443690d5b628de
Prisma Cloud Compute for QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/46ede8c0299f5e4945fa664997f81521
Prisma Cloud DSM for QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/d249296e8dba167cc65eb0c38ee67ef1
Proofpoint on Demand Email Security App V2 - QRadar 7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/c4b4db25be30b5b3f2ec371f351705a2

Table 1047. Third-party DSMs that are available on the IBM Security App Exchange (continued)	
DSM integration	**IBM Security App Exchange link**
Qualys FIM for QRadar - QRadar 7.3.3 FP6+/7.4.1 FP2+/7.4.2 GA+	https://exchange.xforce.ibmcloud.com/hub/extension/1e7cea417eb72062f4803f36dd4336b8
Qualys VM for QRadar - QRadar 7.3.3 FP6+/7.4.1 FP2+/7.4.2 GA+	https://exchange.xforce.ibmcloud.com/hub/extension/624d1ac2d58d236a48e5614d42fab506
QVTI VirusTotal Integration - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/db73ab17547d28409303c2c2583a5160
radiflow iSID	https://exchange.xforce.ibmcloud.com/hub/extension/51efd311f963acbae48b1345094013e7
SCADAfence Platform Integration - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/a75c626aba4611c775ac3a5fd8e277a0
SecurityScorecard App For QRadar - QRadar 7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/b21f9ca87f1e25e3fce3c0426e68bbe9
Sentryo ICS CyberVision for QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/70d5aae95f1d5e0e9f162b4c345fb7fa
Snare E3	https://exchange.xforce.ibmcloud.com/hub/extension/e7ef0bec8315746eef631f36004658b6
Stormshield Network Security	https://exchange.xforce.ibmcloud.com/hub/extension/954b461580d81fa46929bbd04bf494d6
Symantec Email App For QRadar - QRadar v7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/5b14ada25f9af50c8bd14d68287d4b68
Symantec ICDx Content Pack For QRadar	https://exchange.xforce.ibmcloud.com/hub/extension/9bf92ae332571cac2476dfa8b1003ddc
Sysdig DSM	https://exchange.xforce.ibmcloud.com/hub/extension/01539d249fa273483fd1bed30906e7b2
Tenable app for QRadar - QRadar v7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/1184e189cb6489b8adb405075bbaca87
Trend Micro Vision One for QRadar (XDR) - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/57b6ef93cf6021dc14f098091b3c17e2
Virsec DSM for IBM QRadar v7.3.3FP6+	https://exchange.xforce.ibmcloud.com/hub/extension/1096c05fa58241ead5a6847220626695
VMRay Analyzer App for Qradar - 7.3.3FP6/7.4.1FP2/7.4.2+	https://exchange.xforce.ibmcloud.com/hub/extension/048b0db790cf0e62910ad069b6dfb7b5
VMware Carbon Black Cloud App - QRadar 7.3.3 FP6+/7.4.1 FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/e23310efdf0dce9d1631698748eed7b9
WALLIX Bastion DSM	https://exchange.xforce.ibmcloud.com/hub/extension/14f89315f1394c0bc69dcce0e34dee03
Wiz - QRadar 7.4.3+	https://exchange.xforce.ibmcloud.com/hub/extension/d4250fa56eb74aa1c4ba14adc033211f

Table 1047. Third-party DSMs that are available on the IBM Security App Exchange (continued)	
DSM integration	**IBM Security App Exchange link**
Wiz - QRadar 7.4.3+	https://exchange.xforce.ibmcloud.com/hub/extension/f85f68ddd53661cfd7f1004eeaada6a8
ZeroFox Alerts - QRadar v7.3.3FP6+/7.4.1FP2+	https://exchange.xforce.ibmcloud.com/hub/extension/c3eb82d50f75f2458e6284e310534665

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/ the section entitled “Cookies, Web Beacons and Other Technologies”.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing

advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

This glossary provides terms and definitions for the IBM QRadar SIEM software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

accumulator
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

active system
In a high-availability (HA) cluster, the system that has all of its services running.

Address Resolution Protocol (ARP)
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

administrative share
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

anomaly
A deviation from the expected behavior of the network.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

ARP
See Address Resolution Protocol.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN
See autonomous system number.

asset
A manageable object that is either deployed or intended to be deployed in an operational environment.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior
The observable effects of an operation or event, including its results.

bonded interface
See link aggregation.

burst
A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client
A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS
See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

DHCP
See Dynamic Host Configuration Protocol.

DNS
See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM
See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
An event or flow that the user can decide should not create an offense, or an offense that the user decides is not a security incident.

flow
A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.

H

HA
See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

I

ICMP
See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

IDS
See intrusion detection system.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)
An organization that provides access to the Internet.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP
See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS
See intrusion prevention system.

ISP
See Internet service provider.

K

key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L
See Local To Local.

L2R
See Local To Remote.

LAN
See local area network.

LDAP
See Lightweight Directory Access Protocol.

leaf
In a tree, an entry or node that has no children.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

live scan
A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.

log source
Either the security equipment or the network equipment from which an event log originates.

log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT
See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI
See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L
See Remote To Local.

R2R
See Remote To Remote.

recon
See reconnaissance.

reconnaissance (recon)
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report
In query management, the formatted data that results from running a query and applying a form to it.

report interval
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule
A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner
An automated security program that searches for software vulnerabilities within web applications.

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

SOAP
A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

T

TCP
See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file
A key database file that contains the public keys for a trusted entity.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.