

# Let's Talk About Support Tools

## QRadar SIEM

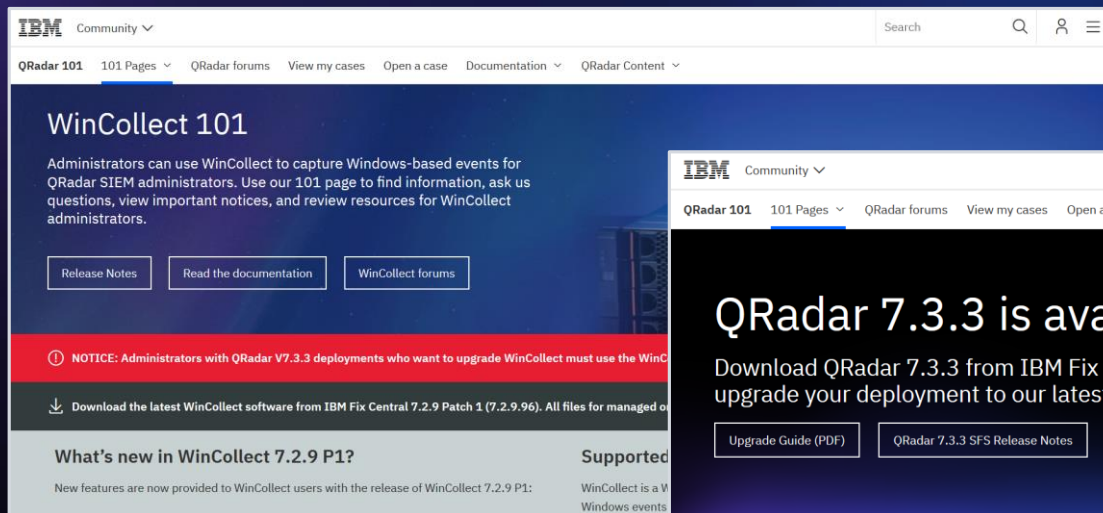
Joel Levesque  
QRadar Core Support Architect  
IBM Security  
joell@ca.ibm.com

Daniel Barriault  
QRadar Support Squad Lead  
IBM Security  
danielba@ca.ibm.com

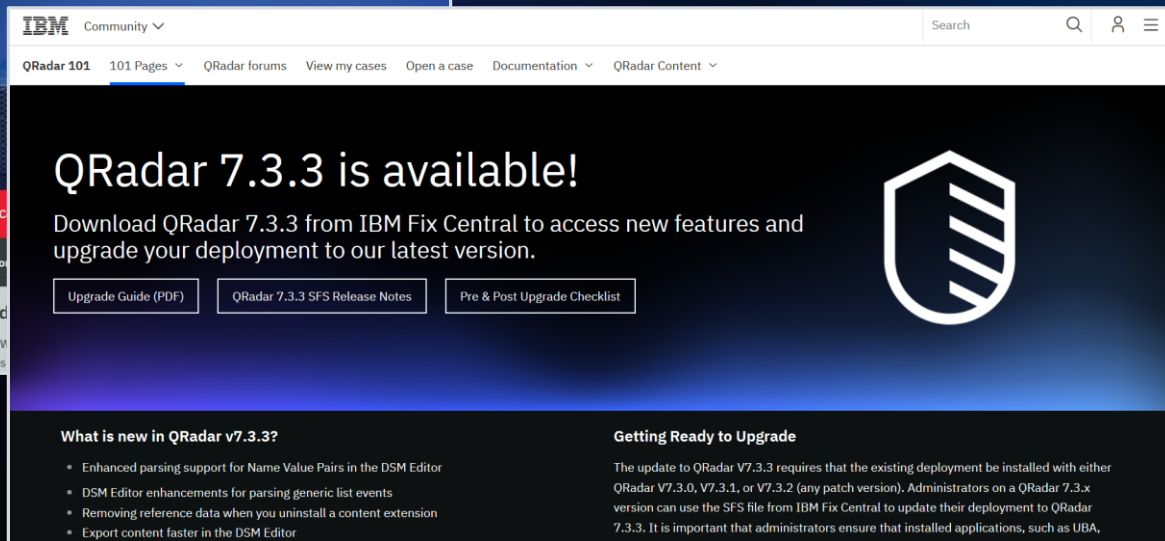
Jonathan Pechta  
QRadar Support Content Lead  
IBM Security  
jonathan.pechta1@ibm.com

# Announcements

- QRadar V7.3.3 is available on IBM Fix Central.
- WinCollect 7.2.9 Patch 1 is available on IBM Fix Central.



The screenshot shows the IBM Community website interface. The top navigation bar includes the IBM logo, a 'Community' dropdown menu, a search bar, and user profile icons. Below the navigation, there are tabs for 'QRadar 101', '101 Pages', 'QRadar forums', 'View my cases', 'Open a case', 'Documentation', and 'QRadar Content'. The main content area is titled 'WinCollect 101' and contains a paragraph of introductory text. Below the text are three buttons: 'Release Notes', 'Read the documentation', and 'WinCollect forums'. A red banner with a warning icon contains a notice about upgrading WinCollect for QRadar V7.3.3. Below the banner is a download link for the latest WinCollect software from IBM Fix Central. At the bottom, there are two sections: 'What's new in WinCollect 7.2.9 P1?' and 'Supported'.



The screenshot shows the IBM Community website interface with a large announcement banner. The top navigation bar is identical to the previous screenshot. The main content area features a large heading 'QRadar 7.3.3 is available!' followed by a sub-heading 'Download QRadar 7.3.3 from IBM Fix Central to access new features and upgrade your deployment to our latest version.' To the right of the text is a large white shield icon with three diagonal stripes. Below the text are three buttons: 'Upgrade Guide (PDF)', 'QRadar 7.3.3 SFS Release Notes', and 'Pre & Post Upgrade Checklist'. At the bottom, there are two sections: 'What is new in QRadar v7.3.3?' and 'Getting Ready to Upgrade'.

# Let's Talk About Support Tools

Standard Support Tools	04
get_logs.sh - About	05
get_logs.sh – options	07
all_servers.sh	09
deployment_info.sh	10
partitionDiagnostic	11
partitionDiagnostic – options	12
ha_diagnosis	13
ha_diagnosis – options	15
iteam_support.sh	16
mod_log4j	17
WinCollectHealthCheck.sh	19
DrQ and Cliniq	21
collectGvStats.sh	22
Recon – application status	23
Common System Notifications	25
Support Tools 101	30

# Standard Support Tools

All standard support tools are available in `/opt/qradar/support/`. The weekly auto update (WAU) is responsible for updating support tools globally for QRadar (`supportability-tools.rpm`).

- `get_logs.sh`
- `all_servers.sh`
- `deployment_info.sh`
- `partitionDiagnostic`
- `ha_diagnosis.sh`
- `iteam_support.sh`
- `mod_log4j.pl`
- `WinCollectHealthCheck.sh`
- `collectGvStats.sh`
- `cliniq` (and `DrQ`)
- `recon`

# get\_logs.sh - About

The `get_logs` utility is available in the command-line or through the UI under Admin > System and License Management. This script is used for primary troubleshooting (log collection) from a QRadar system.

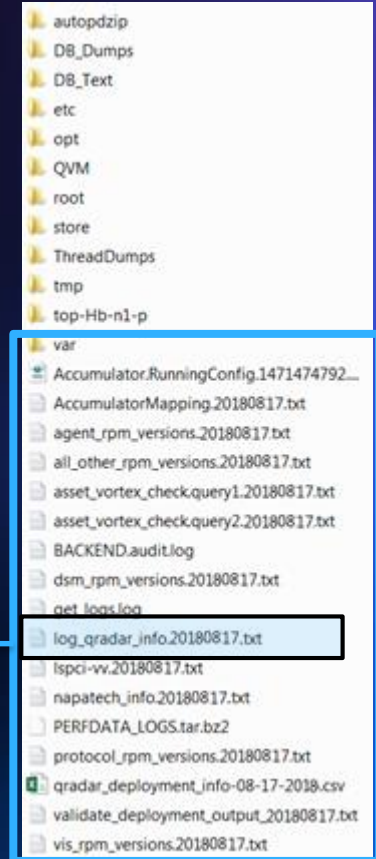
## What is captured?

- QRadar log files
  - DB config and stats
  - journalctl
  - Threaddumps
  - Performance monitoring
  - Setup and patch logs
  - QRadar config
  - Installed packages
  - Application framework logs
  - Optional (full setup folders, git history, system reports, `get_logs` from other hosts and asset data)
- Administrators can include the last `{#_of_days}` of old files in `/var/log/qradar.old/`.

For example, to collect logs from the last 7 days, type:

```
/opt/qradar/support/get_logs.sh -q 7
```

Start with  
`log_qradar_info`  
for a general  
review of your  
system



# get\_logs.sh – About (continued)

- Uses defect\_inspector to detect defects and display the APAR in log\_qradar\_info.txt log file
  - -D to include logs from defect-inspector --long /var/log/qradar.error
- Can include git history of config files in /opt/qradar/conf
- Pipeline Performance Output
  - Get\_logs\_dir/bin/CreatePipelinePerformanceCsvFiles.sh script runs during get\_logs and output to /var/log/setup-####/pipeline\_performance\_\*.csv
  - To display nicely in CLI:  
`column -t -s "," /var/log/setup-###/pipeline_performance_<name>.csv | less`
- Customer can encrypt the logs by using the -e option for encrypting
  - The password to use for decrypting is the date referenced in the file name
- To decrypt the file that gets created with the encryption option, use the following syntax:
  - `openssl enc -d -blowfish -in /var/log/filename.tar.gz.enc -out /var/log/filename.tar.gz -pass pass:<password>`

# get\_logs.sh – options

- -q {# of days}      • Include the last {#\_of\_days} of old files in /var/log/qradar.old/
- -s                    • Include /var/log/setup-(current version)/\*
- -S                    • Include /var/log/setup-(all versions)/\*
- -r                    • Include the SYSTEM REPORTS by Users
- -D                    • Include logs from defect-inspector --long /var/log/qradar.error
- -g {file}            • Include git history of file in /opt/qradar/conf (runs: git log --stat -p <file>)
- -l                    • Generate only the log\_qradar\_info.txt file.
- -i {files}           • Argument quoted and space separated files or directories to be included in tarball.
- -x {files}           • Argument quoted and space separated files or directories to be excluded in tarball.

# get\_logs.sh – options list (continued)

- H {hosts} • Requires an argument of quoted and comma separated IPs or hostnames. Will collect logs from the hosts and store them in ./GETLOGS\_YYYYMMDD. Always includes the console.
- e • Encrypt the resulting tarball
- v • Display revision information
- t • Collect additional asset information and db tables
- h,--help • Displays this dialog



# all\_servers.sh

- A deployment aware CLI tool for information gathering and command execution on MHs.
- Can be used to copy files, running a command on multiple hosts or viewing deployment information.
- Must be executed from the console.
- This is a very powerful tool but can also cause system downtime if not used properly.
- Filter on appliance type, ip address, hostname
- Useful for:
  - Staging patches on all hosts:  
`/opt/qradar/support/all_servers.sh -Ckp /storetmp/731_QRadar-7.3.1.20171206222136.sfs`
  - Operational queries (storage space, load, installed versions, et cetera)  
`/opt/qradar/support/all_servers.sh -Ck df -Th`  
`/opt/qradar/support/all_servers.sh -Ck "umount /media/updates"`
  - Getting files from all hosts  
`/opt/qradar/support/all_servers.sh -Ckg /var/log/qradar.error`

# deployment\_info.sh

- A wrapper for all\_servers.sh that gathers operational information from each appliance in a deployment
- Must be executed from the Console appliance
- By default, gathers all of the following information:
  - Hardware Information (e.g. #CPUs, #Disks, Model, Serial #)
  - Firmware Information
  - Storage Information for the /store partition
  - Memory Information (Full 24 hour average from previous day)
  - Pipeline Related Stats (Record and Payload sizes average since last service restart)
  - Performance Related Stats (Full 24 hour average from previous day)
- All information is stored in a .csv file with an option to display information on the screen:

```
[root@732vm]# ./deployment_info.sh -A -J
```

```
INFO: Gathering deployment information. This may take a while...
```

```
{
  "/store % Used": "40%",
  "/store Available (GB)": "84",
  "/store Size (GB)": "140",
  "/store Used (GB)": "55",
  "Appliance": "3199",
  "Average /dev/sda util %": "1.49",
  "Average /dev/sdb util %": "N/A",
  "Average 5m Load": "2.59",
  "Average CPU System %": "5.65",
  "Average CPU Wait %": "0.08",
  "Average RAM Cached (MB)": "17850",
  "Average RAM Free (MB)": "10393",
  "Average RAM Used (MB)": "19890",
  "Average Swap Free (MB)": "24562",
  "Average Swap Used (MB)": "13",
  "BIOS FW Version": "6.00",
  "Build": "2019.14.0.20191031163225",
  "CPUs": "8 x Intel(R) Xeon(R) CPU E5-4650L 0 @ 2.60GHz",
  "DSA FW Version": "N/A",
  "Disks": "0 x ",
  "Event Coalesce%": "0.80",
  "Event Payload Size (KB)": "0.00",
  "Event Record Size (KB)": "0.00",
  "Flow Payload Size (KB)": "0.00",
  "Flow Record Size (KB)": "0.00",
  "HA Status": "N/A",
  "HD FW Version": "N/A",
  "Hardware": " VMware Virtual Platform",
  "Hostname": "pechtaj-qr732-3199-5732",
  "IMM FW Version": "N/A",
  "IP": "9.55.219.230",
  "RAID Controller FW Version": "N/A",
  "RAM Total (MB)": "48138",
  "Raw EPS": "129.89",
  "Raw FPS": "6.57",
  "Serial #": "VMware-42 24 0f f6 22 21 b3 9b-df f4 50 5a 37 41 30 8c",
  "Stored EPS": "0.00",
  "Stored FPS": "0.00",
  "Swap Total (MB)": "24575"
}
```

# partitionDiagnostic

- This partitionDiagnostic tool is designed to clean up unused event collection service (ecs-ec and ecs-ec-ingress) versions and free up partition space
- In addition, moves /opt/qradar/dca (scaserver) to /store by creating a symlink
- It is strongly recommended that this script first be run with -n to highlight changes, and then -s to backup and remove the services. This is safest procedure.
- The -d deletes without making backups of the services.
- When running with the -s parameter, the services are backed up under /store/support/ directory
- Future feature will scan partitions for large unused files

```
[root@SupportLAB]# opt/qradar/support/partitionDiagnostic -n
2019/01/23 10:07:31 ----- ecs-ec -----
2019/01/23 10:07:33 Not loading "xhnplugin" plugin, as it is disabled
Loading "product-id" plugin
Loading "search-disabled-repos" plugin
Loading "subscription-manager" plugin
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered with an entitlement server. You can use
subscription-manager to register.
Config time: 0.123
Yum version: 3.4.3
rpmdb time: 0.000
Resolving Dependencies
--> Running transaction check
--> Package ecs-ec-0.0.804.noarch 0:0.0.804-1 will be erased
Checking deps for ecs-ec-0.0.804.noarch 0:0.0.804-1 - e
--> Finished Dependency Resolution
Dependency Process ending
Depsolve time: 1.311
Dependencies Resolved
=====
Package                Arch      Version      Repository      Size
=====
Removing:
ecs-ec-0.0.804         noarch    0.0.804-1    @local          149 M
Transaction Summary
=====
Remove 1 Package
Installed size: 149 M
Exiting on user command
2019/01/23 10:07:39 Moving: /opt/qradar/dca/ To: /store/dca/ & Creating a
symlink
2019/01/23 10:07:39 Services that will be shutdown: scaserver
```

# partitionDiagnostic - Options

- `-n, --dry-run` Don't actually remove anything, just show what would be done.
- `-d, --delete` Delete the files and folders
- `-p, --dir string` Scan partition for large unused files :: future feature not available yet (default `"/opt/"`)
- `-s, --save-delete` Backup all the Files and Folders, before the deletion, will fail if the backups do NOT complete
- `-h, --help` Help for partitionDiagnostic

# ha\_diagnosis.sh

ha\_diagnosis is a summary utility which completes a series of HA tests to output a summary of HA appliance checks to the administrator. New in 7.3.x is the Verbose (-V) flag which will hide the success messages and only print failure messages.

Understanding the output:

- HA manager is running. The ha\_diagnosis utility runs `/opt/qradar/ha/bin/ha check` to make certain HA manager is running
- Defines the system roles. You are on HA <Role:Primary|Secondary> Uses the `/opt/qradar/ha/bin/ha cstate` to determine the Role of the appliance.
- Checks the HA heartbeat `/opt/qradar/ha/bin/ha cstate` to determine the HBC (or heart beat) between hosts
- Checks HA Virtual IP with `/opt/qradar/ha/init.d/ha_ipaddr status` to determine is the VIP is on the system
- Checks the HA State using `/opt/qradar/ha/bin/ha cstate` to determine the State of the system (i.e Active/Standby)

```
[support_lab]# /opt/qradar/support/ha_diagnosis.sh

HA manager is running
Currently, You are on HA primary.
Check the HA State
  > Currently, local HA state reaches ACTIVE state
  > Currently, remote HA state reaches STANDBY state
Check the HA heartbeat [OK]
Checking HA Virtual IP
  > HA Virtual Interface is UP
Checking QRadar Services [OK]
Checking HA Mount
  > HA Mount service is running
Checking HA DRBD
  > Local DRBD Role is primary
  > HA DRBD Connection Status is Connected
Checking DRBD configuration files [OK]
Checking 'drbdadm show-gi store' fields [OK]
Check the hidden token [OK]

Diagnosis Summary:
  > All the HA check is PASSED [OK]
```

# ha\_diagnosis.sh (continued)

- Checking QRadar Services
  - Checks the status of services (hostservices, hostcontext, tomcat (where applicable))
- Checking HA Mount
  - `/opt/qradar/ha/init.d/ha_mount` status to see if the proper HA filesystems are mounted
- Checking HA DRBD (This section does a lot. Looks for split brain scenarios, etc...)
  - `/opt/qradar/ha/init.d/ha_drbd` status to determine sync role
  - `cat /proc/drbd` to determine connection state (cs)
- Checking DRBD configuration files
  - diffs the drbd.conf files between local and remote hosts
  - Looks for keyboards in the config files to make certain the file hasn't been truncated
- Checking 'drbdadm show-gi store' fields
  - Runs `drbdadm show-gi store` to check data consistency and status
- Check the hidden token
  - Looks for hidden files in `/opt/qradar/ha` for failures in patching or HA in general
- Checking HA Gluster Filesystem Status
  - Check to make certain the glusterd daemon is running and the peer is connected

# ha\_diagnosis.sh - options

```
/opt/qradar/support/ha_diagnosis.sh -h  
ha_diagnosis v1.2
```

```
Usage: ha_diagnosis.sh [-h] [-t] [-i] [-f] [-s] [-d] [-v] [-V] [-S] [-a] [-c]
```

- a :: Apply all the checks
- S :: Check HA State from HA Manager
- s :: Check QRadar Service status
- f :: Check HA mount status
- d :: Check HA DRBD status
- i :: Check HA virtual interface status
- t :: Check HA hidden tokens
- V :: Verbose output
- c :: Skip all the check if in synchronization state
- v :: Display revision information
- h,--help :: Displays this dialog

# iteam\_support.sh

A CLI and menu driven script that assist customer and support troubleshoot problems.

- Display last Auto Update date
- Display Managed Host related information
- Find QidMap, DSM, Protocol and Scanner related information
- Can identify RPM versions
- Can check jar check sum
- Can check Log Source and Log Source Protocols
- Can collect DSM Performance Data
- Can collect Getlog Data
- Can Enable/Disable Debug

```
[root@pechtaj/]# /opt/qradar/support/iteam_support.sh
iteam_support.sh: v1.0
-----
Last Auto Update Date: 2019-11-28
-----
*****
** 1) Find Managed Host Information
** 2) QidMap / DSM / Protocol / Scanner Menu
** 3) Log Source Menu
** 4) Advanced Menu
** 5) Clear Screen
** 6) Quit
*****
Please enter a menu option and enter or enter to exit.
4
*****
** 1) Collect DSM Performance Data
** 2) Collect Getlog Data
** 3) Enable/Disable Debug
** 4) Clear Screen
** 5) Go To Previous Menu
** 6) Quit
*****
```



# mod\_log4j.pl

- A CLI and menu driven script that assists the user in properly enabling/disabling debug loggers in /opt/qradar/conf/log4j.xml
- Primarily used to toggle debugging
- Any changes written to it are picked up automatically, thus no service restarts are required
- Advanced menu - most common use case for this menu is to restore defaults
- Logs to /var/log/qradar.java.debug
- All classpaths you're likely to add should start with **com.q1labs**.
- The classname can be found in qradar.log

```
Sep  4 16:28:05 ::ffff:xxx.xxx.xxx.xxx [ecs-ec-ingress.ecs-ec-ingress] [OFFICE365]
com.q1labs.semsources.sources.office365restapi.api.query.Office365RESTAPIQueryBase: [ERROR]
[NOT:0000003000][xxx.xxx.xxx.xxx/- -] [-/- -]Unable to start a content subscription.
```

## Steps to enable debugging

- 0) Toggle Debugging
- A) Add a new logger
- Enter the classname

**IMPORTANT:** Always disable/restore defaults before you exit your SSH session to the appliance unless you intend to continue to troubleshoot issues.

# mod\_log4j.pl (continued)

## Useful class paths list:

com.q1labs.vis.scanners.eEye [Retina eEye scanners]  
com.q1labs.semsources.sources.estreamer [Sourcefire/Firesight]  
com.q1labs.vis.scanners.qualys [Qualys Vulnerability Scanners]  
com.q1labs.vis.scanners.mcafee.vulnerabilitymanager [McAfee Vulnerability Manager]  
com.q1labs.core.shared.ldap [LDAP]  
com.q1labs.semsources.sources.jdbc  
com.q1labs.uiframeworks.auth [Authentication]  
com.q1labs.semsources.sources.windowseventlog  
com.q1labs.configservices.capabilities.AddHost  
com.q1labs.semsources.cre  
com.q1labs.hostcontext.backup  
com.q1labs.semsources.sources.remote [FTP & SFTP remote connections]  
com.q1labs.ariel.ui.UIArielServices [Useful for Dashboard issues]  
com.q1labs.semsources.sources.jdbc  
com.q1labs.semsources.sources.jdbc.JdbcEventConnector  
com.q1labs.frameworks.crypto.Q1X509TrustManager  
com.q1labs.semsources.sources.LEA  
com.q1labs.vis.scanners.ip360  
com.q1labs.cve.resultset  
com.q1labs.reporting.charts  
com.q1labs.reporting.ReportServices  
com.q1labs.sem.semsources.wincollectconfigserver

```
TOGGLE DEBUGGING
```

```
Please select from the following options:
```

```
-----  
0) INFO com.eventgnosis.ecs  
1) INFO com.ibm.gradar.forensics.indexer  
2) INFO com.ibm.gradar.forensics.tika  
3) INFO com.ibm.si  
4) INFO com.ibm.si.mpc.magi.contrib.ModelPersister  
5) ERROR com.ibm.si.mpc.magi.contrib.commands.CredibilityCollector  
6) ERROR com.ibm.si.mpc.magi.contrib.commands.RelevanceCollector  
7) INFO com.ibm.si.mpc.magi.statistics  
8) ERROR com.ibm.si.mpc.magi.tasks.TargetEventAnalyzer  
9) INFO com.q1labs  
10) INFO com.q1labs.aleremotemanagement  
11) INFO com.q1labs.ariel  
12) DEBUG com.q1labs.ariel.ext.QueryStats  
13) INFO com.q1labs.assetprofile.changelistener.impl.audit  
14) INFO com.q1labs.configservices  
15) INFO com.q1labs.configservices  
16) ERROR com.q1labs.core.platform.PlatformConfiguration  
17) INFO com.q1labs.core.ui.servlet.WinCollect  
18) WARN com.q1labs.frameworks.resources.jms  
19) ERROR com.q1labs.frameworks.session.transaction  
20) INFO com.q1labs.hostcontext  
21) INFO com.q1labs.qrm  
22) ERROR com.q1labs.qvm.workflow.util.DecryptPropertyConfigurer  
23) INFO com.q1labs.resolveragent  
24) INFO com.q1labs.resolveragent  
25) INFO com.q1labs.sem.monitors.EPMonitor  
26) INFO com.q1labs.sem.monitors.SourceMonitor  
27) INFO com.q1labs.sem.reporting  
28) INFO com.q1labs.sem.semsources.wincollectconfigserver  
29) INFO com.q1labs.semsources.filters.ReportingDestination  
30) INFO com.q1labs.semsources.filters.ReportingEventGenerator  
31) DEBUG com.q1labs.semsources.sources.jdbc  
32) INFO com.q1labs.semsources.sources.jdbc  
33) INFO com.q1labs.uiframeworks.servlet.RequestLoggingFilter  
34) ERROR mx4j.tools.adaptor.http.HttpAdaptor  
35) ERROR net.sf  
36) INFO net.sf.hibernate.SQL  
37) INFO net.sf.hibernate.cache  
38) ERROR net.sf.hibernate.cfg.Configuration  
39) INFO org.quartz  
40) ERROR org.quartz  
A) Add a new logger
```

```
INFO: Created DEBUG logger for com.q1labs.semsources.sources.jdbc  
Choice (q returns you to the main menu): █
```

# WinCollectHealthCheck.sh

This script run through a series of tests to help reduce support times by automating basic checks, identifying common problems, and facilitating the extraction of data. Understanding the output:

- Last Heartbeat Test (Agent Heartbeats)
  - Test will fail if heart beats are older than 30 mins, are not there or agents are not deployed
- Version Test (Agent versions information, NOTE: 7.2.9 agents fail due to a logged issue)
- Log Source Test (Log Source Heartbeats) - Passes when all log sources have reported in the last 720 minutes
- Status Test (Agent Status: Not Communicating, Running, Stopped, Unavailable)
  - Will only pass if all agents are running, and no agent is Dirty
- RPM Test (Currently passes only for 7.2.8 RPM files)
  - Compares the RPM files to the names of the required files for each version
- Type YES at the end of the utility to view a table of agents that failed test conditions.

```
Last Heartbeat Test :
  Failed : There are      0 WinCollect Agents that have a heartbeat within the last 30 minutes
  Passed : There are      0 WinCollect Agents whose last heartbeats are beyond 30 minutes
  Failed : There are      1 WinCollect Agents that have no heartbeat
  Passed : There are      0 WinCollect Agents that have not been deployed

-----
HeartBeat Test Failed

Version Test :
  Passed : There are      0 WinCollect Agents that are version 7.2.5
  Passed : There are      0 WinCollect Agents that are version 7.2.6
  Passed : There are      0 WinCollect Agents that are version 7.2.7
  Passed : There are      0 WinCollect Agents that are version 7.2.8
  Passed : There are      0 WinCollect Agents that are version 7.2.8 patch 1
  Passed : There are      0 WinCollect Agents that are version 7.2.8 patch 2
  Passed : There are      0 WinCollect Agents that are version 7.2.9
  Failed : There are      0 WinCollect Agents that are version 7.2.9 patch 1

-----
Version Test Failed

LogSource Test :
  Failed : There are      0 Log Sources whose last event times are less than 720 minutes
  Passed : There are      0 Log Sources whose last event times are beyond 720 minutes

-----
Log Source Test Failed

Status Test :
  Failed : There are      1 WinCollect Agents that are not communicating.
  Failed : There are      0 WinCollect Agents running.
  Passed : There are      0 WinCollect Agents in "Stopped" status.
  Passed : There are      0 WinCollect Agents that are Unavailable.
  Passed : There are      0 Dirty WinCollect Agents.

-----
Status Test Failed

RPM Test :
  Passed : WinCollect 7.2.5 RPM files were not found
  Passed : WinCollect 7.2.6 RPM files were not found
  Passed : WinCollect 7.2.7 RPM files were not found
  Passed : WinCollect 7.2.8 RPM files were not found
  Passed : WinCollect 7.2.8 Patch 1 RPM files were not found
  Passed : WinCollect 7.2.8 Patch 2 RPM files were not found
  Passed : WinCollect 7.2.9 RPM files were not found
  Passed : WinCollect 7.2.9 patch 1 RPM files were found

-----
RPM Test Passed

=====
Overall Results : At Least 1 Test Failed
Would you like further information on the components that failed the tests?
Please answer yes or no : no
```

# WinCollectHealthCheck.sh (continued)

Within this tool, tuning tests can also be run to see if the WinCollect deployment is within supported tuning parameters.

- Tuning Test (-t option, can take a few minutes depending on the size of the deployment)
  - Checks that the managed hosts have less than 500 agents each
  - Checks that each agent does not have more than 500 log sources
  - Checks that the polling channels divided by their respective polling interval is below 30
  - Checks that there are no more than 30 Xpath queries (2 per agents)
  - For this test to pass all elements of the tuning must be within the supported range

```
[root@pechtaj support]# ./WinCollectHealthCheck.sh -t

Tuning Test :
  Passed : The managed host with the most agents is at  with 1 agents.
  Passed : The agent(s) with the most logsources has
  Passed : Generating a maximum of  of the 30 supported WinCollect channels per second on a single agent.
  Passed : Generating a maximum of 0 of the 10 supported XPath channels per second on a single agent.
  Passed : Generating a maximum of 0 of the 30 supported channels per second on a single agent.

Tuning Test Passed
```

# DrQ and Cliniq

- These tools are designed to test for particular conditions and provide remediation steps
  - Extensible health check tool for QRadar
- DrQ is a standalone binary that lives in /opt/qradar/bin/
  - Cliniq is a packaged version of DrQ
  - Cliniq is a binary that includes the DrQ framework and tests
- Cliniq and DrQ are packaged with different tests
  - Traefik Install and Config Check (app framework)
  - Available Space Check in /var/log/
  - Log Rotate Check for unzipped rolled files
  - Deployment.xml In Global Config Check
  - HA Recovery Token Check
  - S4 Folder Check
  - Workload/service/container check
  - Vault Install and Config Check
- Tests can be updated or enhanced through QRadar Weekly Auto Updates (WAU)

```
[root@pechtaj/]# drq
DrQ version 1.2.0 (mode: 'checkup', tag(s): <none>, verbosity: summary)

Workload, Service and Container Checks
Checks which workloads are available, what services are available, what
containers should exist and that they have functionality.
[FAILURE]
Failed to decode workloads: parameter check: endpoint not specified
[REMEDIATION]
<none provided>

[SUMMARY] 10 successful checkups
[SUMMARY] 1 failed checkup
[SUMMARY] 0 invalid files
[SUMMARY] 1 skipped file
```

# collectGvStats.sh

- Useful to troubleshooting accumulated data issue, used by reports and time series graphs
- Enables you to get the timing on Event Processors to help identify which global view is falling behind
- Accumulator runs every 60 seconds
  - Total amount of time to load all GVs must be less than 60 seconds
- Accumulator rollup runs every hour and every morning (HOURLY and DAILY rollups)
- GVs can get expensive when large number of 'unique values' in the GV or search is not optimized
  - No filters - <criteria>
  - Payload searches
- When to use the utility (the customer may see the following system notifications)
  - "The accumulator was unable to aggregate all events or flows for this interval."
  - "The accumulator has fallen behind. See Aggregated Data Management for details."
  - "Interval processing time (XX seconds) exceeded threshold (60 seconds)"
- Most common switches are -c, -s and -M
  - -c prints the accumulator's running config to a file
  - -s option to print the Stats Report. This includes timings for all global views in the last interval.
  - -M option to view all GV ids, saved search and report title

# Recon – application status

- Used to investigate and identifying issues with installed applications and services
- Ranging from deployment issues to container environment and networking issues
- Require root access to run as it will need access to potentially modify the system
- Displays a unified view to help troubleshoot the apps
- Can also be used to connect and execute a command on a specific app
- Event or Flow data will not be touched directly, only indirectly by starting or correcting apps
- Commands include
  - recon ps
  - recon connect <app\_id>

# Recon – example

```
# /opt/qradar/support/recon ps
```

App-ID	Name	Managed Host ID	Workload ID	Service Name	AB	Container Name	CDEGH	Port	IJKL		
1103	Reference Data Import - LDAP	53		apps	++	qapp-1103	++	qapp-1103	+++++	5000	++++
1002	App Authorization Manager	53		apps	++	qapp-1002	++	qapp-1002	+++++	5000	++++
1111	Network Hierarchy Management	53		apps	++	qapp-1111	++	qapp-1111	+++++	5000	++++
1112	QRadar Assistant	53		apps	++	qapp-1112	++	qapp-1112	+++++	5000	++++
1109	Cloud Visibility	53		apps	++	qapp-1109	++	qapp-1109	+++++	5000	++++
1051	IBM QRadar on Cloud NPS	53		apps	++	qapp-1051	++	qapp-1051	+++++	5000	++++
1102	User Analytics	53		apps	++	qapp-1102	++	qapp-1102	+++++	5000	++++
1104	Machine Learning Analytics	53		apps	++	qapp-1104	++	qapp-1104	+++++	5000	++++
1110	Check Point SmartView	53		apps	++	qapp-1110	++	qapp-1110	+++++	5000	++++
1106	Deployment Intelligence	53		apps	++	qapp-1106	++	qapp-1106	+++++	5000	++++
1105	IBM QRadar DNS Analyzer	53		apps	++	qapp-1105	++	qapp-1105	+++++	5000	++++

Legend:

Symbols:

- n - Not Applicable
- - Failure
- \* - Warning
- + - Success

Checks:

Service:

- A - Service exists in the workload file
- B - Service is set to started

Container:

- C - Container is in ConMan workload file
- D - Container environment file exists
- E - Container image is in si-registry
- G - Container Systemd Units are started
- H - Container exists and is running in Docker

Port:

- I - Container IP are in firewall main filter rules
- J - Container IP and port is in iptables NAT filter rules
- K - Container port has routes through Traefik
- L - Container port is responsive on debug path



# QRadar Common System Notifications

- Accumulator is falling behind
- Disk Usage System Notification
- Active high-availability (HA) system failure

# Accumulator is falling behind

38750099 - The accumulator was unable to aggregate all events/flows for this interval.

## Sample message:

```
May 20 20:04:00 ::ffff:xxx.xxx.xxx.xxx [accumulator.accumulator] [AccumulationService]
com.q1labs.cve.accumulation.AccumulationService: [WARN] [NOT:0310004100][xxx.xxx.xxx.xxx/- -] [-/- -]
Interval processing time (85 seconds) exceeded threshold (60 seconds)
```

This message appears when the system is unable to accumulate data aggregations within a 60 seconds interval. Every minute, the system creates data aggregations for each aggregated search. The data aggregations are used in time-series graphs or reports. The notification will appear if the count of searches and unique values in the searches are too large or the time that is required to process the aggregations exceed 60 seconds. Time-series graphs or reports might be missing columns for the time period when the problem occurred. All raw data are still written to disk therefore you do not lose data when this problem occurs. Only the accumulations are incomplete which are data sets generated from stored data.

You may want to check the `/var/log/qradar/log` file to see if the message is repeatedly occurring. In this case, you should run the `/opt/qradar/support/collectGvStats.sh -s` to find out the amount of time each the global views are taking to create data aggregations and tune the GVs\Saved Searches that are taking too long.

# Disk Usage System Notification

38750076 - Disk Sentry: Disk Usage Exceeded Warning Threshold.

38750038 - Disk Sentry: Disk Usage Exceeded Max Threshold.

38750077 - Disk Sentry: System Disk Usage Back To Normal Levels.

## Sample message:

```
May 6 04:40:50 ::ffff:xxx.xxx.xxx.xxx[hostcontext.hostcontext] [595fdc09-5d4b-4757-b908-cc91560e92cb/SequentialEventDispatcher] com.qllabs.hostcontext.ds.DiskSpaceSentinel: [WARN] [NOT:0150064102][xxx.xxx.xxx.xxx/- -] [-/- -]System disk resources above warning threshold
```

```
May 6 04:43:50 xxx.xxx.xxx.xxx [db74f54b-656c-4a46-83d0-e2036676265a/SequentialEventDispatcher] com.qllabs.hostcontext.ds.DiskSpaceSentinel: [ERROR] [NOT:0150064100][xxx.xxx.xxx.xxx/- -] [-/- -]Disk usage on at least one disk has exceeded the maximum threshold level of 0.95. The following disks have exceeded the maximum threshold level: /opt. Processes are being shut down to prevent data corruption. To minimize the disruption in service, reduce disk usage on this system.
```

```
May 6 04:59:53 xxx.xxx.xxx.xxx [db74f54b-656c-4a46-83d0-e2036676265a/SequentialEventDispatcher] com.qllabs.hostcontext.ds.DiskSpaceSentinel: [INFO] [NOT:0150066100][xxx.xxx.xxx.xxx/- -] [-/- -]System disk resources back to normal levels
```

QRadar's disk sentry monitors the following partitions:

**/, /store, /transient, /storetmp, /opt, /var, /var/log, /var/log/audit, /tmp, and /home.**

# Disk Usage System Notification (Continued)

The first notification means that the disk usage on your system is greater than 90%. The operation of your QRadar system is not affected when the partition reaches this threshold.

The second notification means that the disk usage reaches 95% on any of the monitored partitions. QRadar data collection (ecs) and search processes (ariel) are shut down in order to protect the file system from reaching 100%. In this case, identify which partition is full and free some disk space by deleting files that are not needed or by changing your data retention policies.

The third notification means that the disk usage has returned back to below 90%. QRadar automatically restarts data collection and search processes

# Active high-availability (HA) system failure

## 38750081 - Active HA System Failure

### Sample Message:

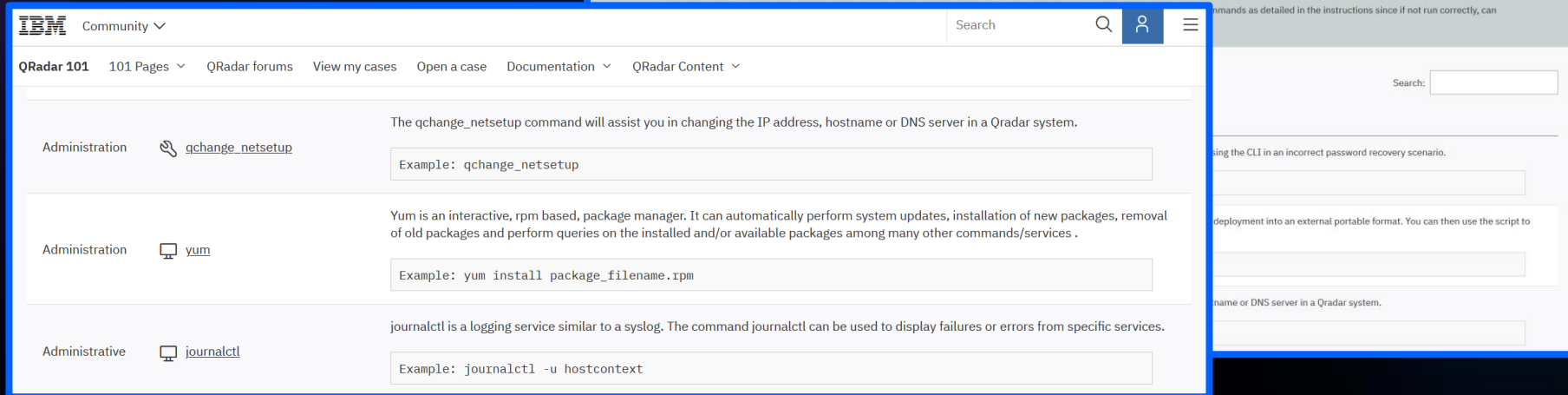
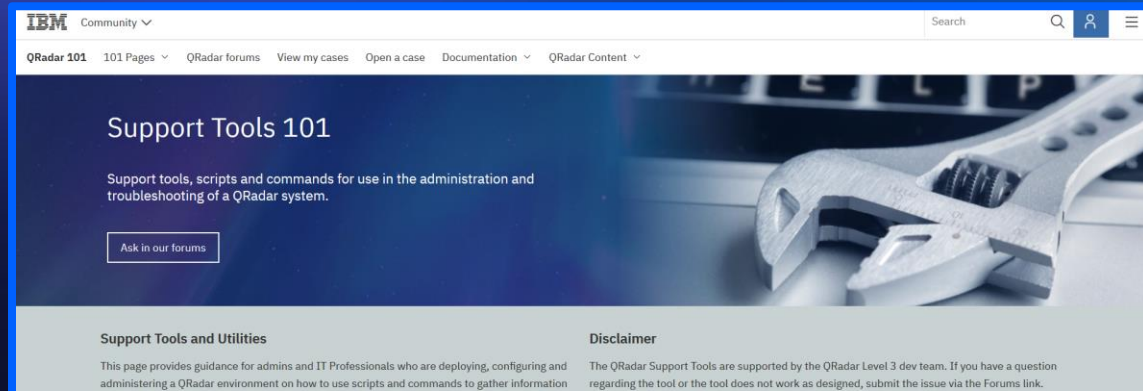
```
Mar 22 15:50:30 ::ffff:xxx.xxx.xxx.xxx [tomcat] [ServerHostServices_PersisterTimer]
com.qllabs.configservices.controller.IServerHostController: [INFO]
[NOT:0270004101][xxx.xxx.xxx.xxx/- -] [-/- -]Active system at xxx.xxx.xxx.xxx has failed.
Attempting fail over from xxx.xxx.xxx.xxx resources to xxx.xxx.xxx.xxx
```

This message appears when the active system cannot communicate with the standby system. This can be because the active system is unresponsive or failed. The standby system takes over operations from the failed active system.

In this case, you will want to inspect the active HA appliance to determine whether it is powered down or experienced a hardware failure. Otherwise you can run the `/opt/qradar/support/ha_diagnosis.sh` script on the failed system.

# Coming soon – Support Tools 101

- Support is building a reference page full of useful tools and commands.
- The goal of Support Tools 101 is to give advice on how to use tools and make helpful commands easier to locate.



# Questions?

Ask in the Q&A panel

# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.

**IBM Security**





