Release Notes

==========

Product:	IBM Security Guardium
Release version:	Guardium 11.4
Completion date:	17 September 2021
Modified on:	21 March 2023

IBM Security Guardium is designed to help safeguard critical data.

Guardium is a comprehensive hybrid multi cloud data protection platform that enables security teams to automatically analyze and protect sensitive-data environments such as databases, data warehouses, big data platforms, cloud data sources, file systems, IBM Z® mainframes, IBM i platforms and so on.

Guardium minimizes risk, protects sensitive data from internal and external threats, and seamlessly adapts to IT changes that can impact data security. It ensures the integrity of information and automates compliance controls like GDPR, HIPAA, SOX, PCI, CCPA, and others, no matter where the data resides.

Guardium provides a suite of programs that are organized around components and modules:

- IBM Security Guardium Appliances
- IBM Security Guardium Data Security and Compliance
    - IBM Security Guardium Data Protection
    - IBM Security Guardium Data Activity Monitor
    - IBM Security Guardium Vulnerability Assessment
- IBM Security Guardium for Files
    - IBM Security Standard Activity Monitor for Files
    - IBM Security Advanced Activity Monitor for Files
- IBM Security Guardium Data Protection for NAS
- IBM Security Guardium Data Protection for SharePoint

Table of Contents

DOWNLOADING GUARDIUM 11.4 ..... **3**

INSTALLING GUARDIUM 11.4 ..... **3**

UPGRADING TO GUARDIUM 11.4 ..... **3**

NEW FEATURES AND ENHANCEMENTS IN GUARDIUM 11.4 ..... **5**

NEW FEATURES 5
KEY ENHANCEMENTS 5

SNIFFER UPDATES **8**

SUPPORT ADDED IN 11.4 ..... **8**

NEW PLATFORMS AND DATABASES 8
NEW BROWSERS 9
DATABASES SUPPORTED BY THE GUARDIUM UNIVERSAL CONNECTOR 9

DEPRECATED FUNCTIONS **9**

REPORTS 9
S-TAPS 9
CONFIGURATION AUDITING SYSTEM (CAS) 9
VULNERABILITY ASSESSMENT 9
BROWSERS 9

KNOWN LIMITATIONS AND WORKAROUNDS **10**

BUG FIXES **12**

SECURITY FIXES **22**

RESOURCES **23**

Downloading Guardium 11.4

Important:

The original Guardium internal MySQL certificate expires April 2, 2023. This re-released Guardium Patch Update (GPU) file contains an updated certificate. After installing or upgrading to Guardium version 11.4 by using this GPU file, you must install appliance patch 11.0p440 or later to retain the updated MySQL certificate. The latest appliance patch also remediates log4j vulnerabilities.

For more information, see https://www.ibm.com/support/pages/node/6839175

Passport Advantage:

http://ibm.com/software/howtobuy/passportadvantage/pao_customers.htm
On Passport Advantage (PA), find the Guardium Product Image - ISO file, licenses, product keys, and manuals. You can download only the products to which your site is entitled.
If you need assistance to find or download a product from the Passport Advantage site, contact the Passport Advantage team at 800-978-2246 (8:00 AM - 8:00 PM ET) or by email paonline@us.ibm.com.

Fix Central:

http://ibm.com/support/fixcentral
Find Upgrades, Guardium Patch Update files (GPUs), individual patches, and the current versions of S-TAP and GIM on Fix Central. If you need assistance to find a product on Fix Central, contact Guardium support.

Guardium patch types:

For more information on the types of Guardium patches and naming conventions, see Understanding Guardium patch types and patch names.

Installing Guardium 11.4

Guardium 11.4 is available as an ISO product image on Passport Advantage.

If the downloaded package is in .ZIP format, extract it outside the Guardium appliance before you upload or install it.

Install Guardium across all the appliances such as the central manager, aggregators, and collectors.

Upgrading to Guardium 11.4

You can upgrade to Guardium 11.4 from any Guardium system that is running on version 11.0 and above.

Before you upgrade, ensure that your appliance meets the minimum requirements. You must upgrade your firmware to the latest versions provided by your vendor. If you use a Guardium appliance, check the Fix Central website for the latest firmware.
You can’t upgrade a disk with custom partitions or disks with Encrypted Logical Volume Management (LVM). Use the backup-rebuild-restore procedure to upgrade these configurations.

Health Check patch

Before you upgrade, you must install the latest version of the Health Check patch that's available on the Fix Central website.

The Health Check file is a compressed file with the file name in this format:
SqlGuard_11.0p9997_HealthCheck_<date>.zip
The v11.0 Health Check patch 9997 must be successfully installed in the last seven days before you install the Guardium 11.4 GPU. If the Health Check patch isn't installed as recommended, the 11.4 installation fails with this error message: "Patch Installation Failed - Latest patch 11.0p9997 required".

If the Health Check patch identifies a problem specific to the 11.4 GPU, you must resolve it before installing the 11.4 GPU. If the 11.4 GPU is installed without resolving the health check warnings, the installation might fail with this error message: "Patch Installation Failed - check Health Check warning". For more information about troubleshooting health check warnings, see the Health Check patch release notes.

Any media (such as DVDs or USB disks) that is mounted on the physical appliance (either connected directly or with remote virtual mounting through systems such as IMM2 or iDRAC), must be unmounted before you upgrade. Mounted media might cause the upgrade to fail.

Back up, archive, and purge the appliance data as much as possible for an easier installation process.

Schedule the installation during a quiet time on the Guardium appliance to avoid conflicts with other long-running processes such as heavy reports, audit processes, backups, and imports.

During GPU upgrades, the appliance's internal database shuts down and the system restarts automatically. Depending on the size of the database, it might take an extended amount of time to restart. During this time, CLI access is available only in recovery mode.

In the recovery mode, the system isn't fully functional and only a limited set of commands are available.

Note: Don't manually restart the system during the internal database upgrade. The patch automatically restarts the system. For real-time details on the system patch installation, use the CLI command **show system patch status**. You can run this command in the CLI recovery mode, but only after a certain point in the installation when the CLI command gets added.

When you use the GUI (fileserver method) to upload the patch, a slow network connection might cause a timeout because of the large file size. Use the CLI command **store system patch install**. For more information, see Store system patch install.

After you upgrade to Guardium 11.4, apply all relevant maintenance patches. You must also apply the latest quarterly DPS patch and rapid response DPS patch even if these patches were applied before the upgrade.

Previously installed patches

When you upgrade to any version of Guardium 11.0 and above, the Guardium 10.0 patches that were previously installed are no longer visible in the "Installed Patches" screen in the GUI.

Installing or upgrading to 11.4 S-TAP

See Windows or UNIX S-TAP release notes for more information.

New Features and Enhancements in Guardium 11.4

New features

Custom properties for datasources
By configuring custom properties, you can better manage your datasources, organize your workflow, and efficiently accomplish complex processes. For more information, see Configuring custom properties for your datasources.

HashiCorp integration
Integrate your Guardium® system with HashiCorp to securely store, manage, rotate, and retrieve credentials for all supported datasources. For more information, see Managing datasource credentials with HashiCorp.

Real-time trust evaluator
The real-time trust evaluator monitors and evaluates your Guardium S-TAP connections to determine whether connections can be trusted and to identify anomalies.
The real-time trust evaluator uses machine learning and a probability engine through both a primary and secondary training period. After the training period, the trust evaluator uses that information to detect and act on anomalies and untrusted connections. For more information about the real-time trust evaluator, see Real-time trust evaluator.

Security incident policies
Guardium provides several session level policy templates that encapsulate security problems that are frequently found at run time. Each of the security incident policies contains rules that find and report on a specific type of security incident. For more information about the security incident policies, see Security incident policies.

Key enhancements

Certificate management with Venafi
Guardium now supports MySQL and Sniffer certificate management with Venafi.

Classifier
You can now overwrite the classifier policy when you import a data set by selecting the checkbox for "Overwrite Classifier Policy" in the Definition Import page in the UI.

Entitlement reports
Guardium now supports entitlement reporting for Azure SQL, DataStax Cassandra, and Neo4j.

External S-TAP
- Tooltips are now available for most UI elements.
- You can now deploy External S-TAPs using Kubernetes Helm charts. For more information, see Deploying External S-TAP with Helm.
- You can use certificate mirroring to allow an External S-TAP® to automatically generate copies of client and server key pairs from an existing signing key pair. For more information, see Certificate CLI Commands.
- You can use Kubernetes Security Policies with External S-TAPs. You need to ensure that pod user can access files and mounted volumes. for more information, see Advanced tab.

- External S-TAP supports Query Rewrite (QRW) and load balancer node affinity. For more information, see TAP tab.

File transfer without passwords for data archive, data backup, export results, and data marts
The SSH key support provides a new solution for password management for data archive, data backup, export results, and data marts. The Guardium system generates SSH keys specific to the transfer and propagates them to remote hosts that support SCP connections. At the central manager level, you can generate SSH keys across the deployment and propagate them to remote hosts. For more information, see Enabling SSH key pairs for data archive, data export, data mart, export_transfer_key, and the store system public_transfer_key and store system scp-ssh-key-mode CLI commands.

GIM
GIM listeners are activated after the GIM certificates on the appliance is changed. For more information, see What to do next in Creating and managing custom GIM certificates.

LDAP support
- Guardium can now import LDAP users from multiple LDAP servers. For this change, the access manager now handles LDAP configuration in a new access manager window. For more information, see Importing users from LDAP and Configuring local, RADIUS, or LDAP authentication.

Manage access to the Guardium system
- You can now limit access to the Guardium UI, CLI (via SSH), or both for specified IP addresses. For more information, see Managing access by IP address.
- Guardium now supports nine guardcli accounts (guardcli1 - guardcli9)
- You can disable the password for one user or configure a password to expire after a designated number of days. For more information, see User account security.

Multi-factor authentication RSA SecurID support
Multi-factor authentication now supports RSA SecurID with either a hardware or software token. For more information, see Configuring multi-factor configuration.

Response length in policies, reports, and alerts
When you define policy rules, you can now include the response length threshold under **Other Criteria** for access policies. For alerts, you can now add the *%%ResponseLength* variable to the alert message template. For more information about using response length, see Rule definition fields and The alert message template.
Note: Response length is not supported for z/OS.

Smart card authentication
Import users from LDAP and update the smart card username without losing related settings. Admin and accessmgr users can now authenticate without smart cards by using a separate login page. Use the CLI command `store system websmartcard-admin-only` to enable or disable smart card authentication without using a smart card. For more information, see System CLI Commands.

S-TAPs
For S-TAP enhancements, see the UNIX and Windows S-TAP release notes.

To-do list enhancements: manage multiple processes, compare classifier results
The to-do list now supports taking actions on multiple processes at once, for example marking several items as viewed or as signed. For more information about working with multiple processes, see Audit process to-do list.

In addition, the to-do list also allows you to compare discovery and classification results across multiple runs of the same job. For more information about comparing classifier results, see Comparing discovery and classification results.

Vulnerability Assessment (VA)
- Vulnerability Assessment has updated the method of storing test result details. In addition to storing the detailed results into one record, VA now creates a separate record for each detailed finding. When the test results are exported to an external location, you can normalize each detailed finding into a record of its own. You can disable writing all detailed test results into one record by using an API command. For more information, see disable_test_result_detail_string_setting.
- You can now export a custom query-based or CAS-based test to another Guardium system. If a test with the same name exists, it's overwritten. If not, a new test is created.
- Sync one or more security assessments based on one selected assessment.
- Supported added for Oracle 19c CIS Benchmark, SQL Server 2019 CIS Benchmark, and MongoDB 3.x STIG benchmark.
- Support added for scans on MySQL version 8.0, all versions of Cloudera 7, Teradata 17.0, Neo4j, Amazon Redshift, MongoDB 4.4, and PostgreSQL 13.0.

System enhancements
- The Guardium system now runs on Red Hat Enterprise Linux version 7.9 (RHEL7.9).
- Support added for Network File System (NFS) for SCP, SFTP, Amazon S3, Centera, IBM COS, and TSM. Note: NFS drive configuration is limited to one mounting point and currently supports only system backup and restore. Data archive backup and restore isn't supported.
- SNMP version 3 support added
- The passkeys for your Guardium system are updated. You can access the new passkeys by using the CLI command `support show passkey [accessmgr| cloudsupport | root]`. Passkeys are confidential and must be shared only with the IBM Security Guardium support team when access to your system is required to troubleshoot.
- Patches that failed installation were previously deleted from the Guardium system. You can now preserve a failed patch by using the CLI command `store system patch preservation on` to enable patch preservation. The default setting is `off`. View the patches in the directory by using the command `show system patch staged`. Delete the preserved patches by using the CLI command `store system patch cleanup`.
- Solr engine is upgraded to version 8.4
- Support added for Suse 12 VCS FS late mount with GIM

Sniffer Updates

The following is a list of Sniffer patches that are included in Guardium 11.4. The latest sniffer patch that is included in Guardium 11.4 is v11.0p4031.

Sniffer patch number	Issue key	Summary	APAR
11.0p4022		https://delivery04.dhe.ibm.com/sar/CMA/IMA/09k0n/0/Guardium_v11_0_p4022_sniffer_update_release_notes.pdf	
11.0p4024		https://delivery04.dhe.ibm.com/sar/CMA/IMA/09npe/1/Guardium_v11_0_p4024_sniffer_update_release_notes.pdf	
11.0p4028		https://delivery04.dhe.ibm.com/sar/CMA/IMA/09s01/1/Guardium_v11_0_p4028_sniffer_update_release_notes.pdf	
11.0p4031		https://download4.boulder.ibm.com/sar/CMA/IMA/09ylo/0/Guardium_v11_0_p4031_sniffer_update_release_notes.pdf	
	GRD-54025	Snif doesn't receive SPAN Port Oracle Traffic	
	GRD-53249	Incorrect, "partial" or blank "Exception Description" in report for MSSQL	GA17718
	GRD-53080	Oracle Unified Audit enabled S-TAP: Sessions captured report "Session End Time" prior "Session Start Time"	GA17716
	GRD-52457	The number of SQL errors recorded after the upgrade to version 10.6 has increased significantly	GA17707
	GRD-48030	Informix EXIT traffic is being ignored with S-TAP Ignore Response enabled.	GA17497

Support added in 11.4

New platforms and databases

- Neo4J 4
- GreenPlum DB 6.10.1
- Teradata 17.0
- SAP HANA SP205
- Vertica 10.0
- CouchDB 3.0
- MemSQL 7.1
- PostgreSQL 13.0
- Couchbase 6.6
- Maria 10.1.3 on Windows 2012
- CockroachDB 20.2.3
- GoogleBigQuery

New browsers

- Microsoft Edge
- Version 93.0.961.38 (64-bit)

Databases supported by the Guardium universal connector

The Guardium universal connector supports several platforms, including:

- Amazon AWS S3
- Hadoop Distributed File System
- MongoDB
- MySQL
- Snowflake

New platform support is added regularly, with support for the following coming soon:

- Dynamo AWS
- Microsoft SQL Server
- Neo4J
- Postgres AWS

To see if your platform is supported by universal connector, use the Guardium supported platforms database at the Security Learning
Academy: https://www.securitylearningacademy.com/mod/data/view.php?d=12&mode=asearch

Deprecated functions

Reports

Old report name	New report name
Available Security Assessment tests	Available VA Tests - Detailed

S-TAPs

- All versions of RHEL 5
- AIX 6

Configuration Auditing System (CAS)

CAS requires Java runtime environment (JRE) 1.8 or later.

Vulnerability Assessment

- Cloudera Data Platform (CDP) scan isn't supported on all versions of Cloudera 5.0. The latest Cloudera driver doesn't support older Cloudera releases.
- MongoDB versions below 3.6 aren't supported.

Browsers

Internet Explorer 11

Functionality

Application Lifecycle ("Guardium ecosystem") will be removed in an upcoming release. For more information, see https://www.ibm.com/support/pages/node/6553922

Known limitations and workarounds

Component	Issue key	Description
Active threat analytics	GRD-45975	The Outlier mining history doesn't display results for outliers on the central manager.
	GRD-45858	Active threat analytics cases that are assigned to a user role before upgrade are not escalated after an upgrade.
	GRD-41965	Full SQL Report link displays an error on Internet Explorer. **Workaround:** use a different browser.
Backup and restore	GRD-55087	When you upgrade Guardium versions 11.1 and 11.2 to version 11.4 using the backup and restore method in an AWS environment, the test connection is successful. However, the system backup and data archive fail. **Workaround:** Before you run Test Connect, enter the AWS secret access key from the Guardium version that you're upgrading from. Archive data and backup your system after the upgrade to 11.4 is complete.
Certificates	GRD-54643	You might encounter an error while importing Venafi MySQL certificates. The error occurs when several certificates are imported at the same time. **Workaround:** Clear certificates on the Venafi portal and try again.
File transfer by using the TSM server	GRD-54760	If you import the dsm.sys file with the *import tsm config* CLI command, the command fails if the *passwordaccess generate* parameter isn't in uppercase text. **Workaround:** Within the dsm.sys file, make sure that the PASSWORDACCESS GENERATE parameter is in uppercase before you import the file.
Guardium GUI and CLI	GRD-54344	Always assign one or more IP addresses to the *allowlist* from which you can access Guardium. If you restrict access to all IP addresses available to users, you'll permanently lock all users (and yourself) out of Guardium.
	GRD-55246	When you unregister a managed unit from the CLI, you can't log in to the managed unit by using the GUI. **Workaround:** restart the GUI and try again. To avoid the error, unregister from the GUI of the central manager or managed unit.
Guardium universal connector	GRD-55044	Filebeat can't be installed during a GUC shell installation. **Workaround:** Uninstall GUC that's installed via shell and install via GIM GUI, with GUC_INSTALL_FILEBEAT=true
	GRD-54990	When you add a connector configuration on your managed unit, the GUI displays instructions to run the grdAPI command: `restart_universal_connector overwrite_instance=true`, which is incorrect.

		Workaround: Use the correct grdAPI command: `run_universal_connector overwrite_instance=true`.
	GRD-49646	If you add a connector when the universal connector is disabled, the connector is added, but universal connector doesn't get enabled automatically. **Workaround:** Manually enable the universal connector.
	GRD-52782	The universal connector doesn't capture AWS PostgreSQL events on IPv6.
	GRD-46069 GRD-54393	After a backup and restore from Guardium version 11.3 to 11.4, the Universal connector status isn't retained. **Workaround:** Enable universal connector after upgrading to Guardium 11.4
Quick search	GRD-48991	For some databases (including MySQL), Guardium doesn't display the correct DATABASE NAME in Quick Search (Investigation Dashboard).
Real-time trust evaluator	GRD-54439	If the training time for real-time trust evaluator is modified, the progress indicator may not be accurate.
Real-time trust evaluator and security incident policies	GRD-55094	The members in the predefined tuple group "Empty client IP and analyzed client IP values" are overwritten. **Workaround:** To avoid false positives, manually add the following members in the group builder: guardium://empty+0.0.0.0 guardium://empty+0000:0000:0000:0000:0000:0000:0000:0000 Member values are separated by the + sign. The resolution for this issue is available in an upcoming patch.
Risk spotter	GRD-50761	The risk score isn't updated for existing users who are in a watchlist group. Trusted users are identified as risky when their usernames are entered in lowercase letters when they are added into the group. **Workaround:** Add users to the relevant groups in uppercase.
	GRD-46278	Reports can't be viewed by a user after an upgrade. **Workaround:** 1. Log in to Guardium as accessmgr or another role with permissions to modify roles. 2. Click **Role Browser** and **Manage Permissions** of the user. 3. From the drop-down list, select Reports. 4. If "Active Risk Spotter -Risky User" is listed in the filter of Inaccessible items, move it to Accessible items. 5. Save the permissions.
Upgrade	GRD-54546	After upgrading to 11.4, you can't query an LDAP connection. This issue occurs because a new field for the domain name was created in 11.4.

		Workaround: You must manually populate the domain field in the Import Config tab after you upgrade to Guardium 11.4
	GRD-54452	When you upgrade from Guardium 11.0 or 11.1 to 11.4, the command-line parameter *FIPSmode* is restored to the default value. **Workaround:** Use the CLI command `store system fipsmode on` to reset the value. Note: The value is preserved if you upgrade from 11.2 to 11.4 using the backup and restore method. After you restore to 11.4, restart your Guardium system for the FIPSmode to stay enabled.
	GRD-54393	The universal connector status is disabled after upgrading to Guardium 11.4 **Workaround:** enable universal connector after upgrading to Guardium 11.4
zS-TAP	GRD-52671	Deployment topology reporting is inaccurate for zS-TAPs. **Workaround:** Remove inactive z STAP information in Health Topology by manually logging into the MU and removing inactive S-TAPS for z.

Bug Fixes

Issue key	**Summary**	**APAR**
GRD-51738	V10.6_r108055 S-TAP crashing on Db2 prod database server (AIX)	GA17667
GRD-47165	Teradata Database Restart due to TD Exit	GA17457
GRD-47407	S-TAP crashes causing high CPU when sqlguard_ip is set to loopback IP	GA17447
GRD-52653	Teradata system restart - Suspect of Guardium	GA17722
GRD-47869	S-TAP keeps crashing in fsmon thread calling SSL_library_init() when S-TAP starts	GA17481
GRD-46177	Error messages flooding the syslog for fsmon on servers for FAM enabled	GA17439
GRD-48909	KTAP module for 3.8.x family is causing a Kernel panic in loop with v11.3 (3.8.13 - 4.18)	
GRD-52818	GUI crashing (opens for barely 1 minute after a restart gui, then crashes) after p315 was installed	GA17713
GRD-47340	Guardium not collecting SQL statements greater than 256 characters	GA17453
GRD-50727	GIM Supervisor is terminating PDE on the server where Teradata Exit is configured	GA17605
GRD-49082	WinS-TAP v11.2.0.194 is Installing Successfully on Some Windows Servers, but Not on Others	GA17708
GRD-51960	"Failed to save Query" when trying to copy or save a report	GA17703
GRD-51093	Win S-TAP may fail to connect to collector after restart if DNS takes time to work.	GA17640

GRD-49748	MongoDB activities aren’t captured by External S-TAP from containerized DB from specific client	
GRD-46991	The bind value for a specific column (PARTNER_GUID) is truncated	GA17416
GRD-50854	Db2 Exit isn’t collecting traffic	
GRD-48844	S-TAP starts before K-TAP is loaded after restart	GA17534
GRD-48030	Informix EXIT traffic is being ignored with S-TAP Ignore Response enabled.	GA17497
GRD-50120	V10.6 - Teradata EXIT Agent - PROD DB Restarted after changing S-TAP_DB_IGNORE_RESPONSE=ALL using GIM	GA17604
GRD-49411	Incorrect Oracle Service Name captured by S-TAP using Oracle Unified Auditing interception method	GA17611
GRD-47785	Need to document GUI option "Restart mode" in S-TAP Control	
GRD-50071	Obsolete entries in GIM_CERTIFICATE_DISTRIBUTION_INFO table after GIM client removal	
GRD-47687	Add documentation about the <install dir>/modules/UTILS/current/files/bin/configurator.sh script	
GRD-49856	S-TAP LOG_WARNING: ktap query handler <HID> stopped running: Bad address; ktap query handler <HID> stopped running: No such file or directory	GA17575
GRD-43996	Can’t register a new GIM client to a GIM server that implements custom GIM certificates	GA17344
GRD-45655	Irrelevant Session Failover message is causing DB user extraction mismatch	GA17518
GRD-53080	Oracle Unified Audit enabled S-TAP: Sessions captured report "Session End Time" prior "Session Start Time"	GA17716
GRD-41589	S-TAP not deleted from S-TAP Control after failover and then S-TAP restarts and ELB assigns new MU(s)	GA17286
GRD-48179	FAM error messages are logged in to dmesg at boot time	GA17511
GRD-53997	S-TAP Cores generated in Solaris	GA17732
GRD-48148	ELB not relocating S-TAPs as expected	GA17482
GRD-50722	Db2_exit_health_check.sh produces incorrect output if db_install_dir includes capital letters	GA17597
GRD-51038	Db2 Exit - WARNING: attaching to shmem[10] of 20 failed Error opening shared memory area errno=2 err=8	GA17670
GRD-46742	Query from threat detection analytics constantly stuck (v11.2)	GA17507
GRD-49632	DB User missing from Oracle Kerberos Authenticated session from Windows client talking to a Solaris server	GA17561
GRD-49524	Distributed report result has different number of rows than the normal report result	GA17596

GRD-50349	CA Certificates failing to install after appliance upgrade	
GRD-52870	TURBINE_USER.LOGIN_NAME field blank in reports.	GA17696
GRD-49185	Active Threat Analytics report - Analytic case "Closed By" attribute for blank value has both values, NULL and '0'	GA17404
GRD-50285	Stealthbits[58568] - FDEC - ERROR - Scanner: GetScanResults failed: [2] on FDECforNAS-V11.1.0.224	GA17726
GRD-49265	Compliance Monitoring Dashboard errors after changing smart policies	GA17548
GRD-50650	Can't grant privileges to a role on all Guardium reports due error: "Unable to connect to UI server. Verify that server is operational and try again."	GA17588
GRD-53031	Group builder issues handling duplicated entries (with alias defined)	GA17706
GRD-48837	Suspicious LOGIN_FAILED from 00:00 until 00:50 || 5-7 attempts.	GA17571
GRD-50532	When replaying msg_dump, the following errors are being frequently observed in the sniffer log: <<<<Unknown error: No such node (type) >>>	
GRD-52683	Failure to create trigger for a table in "Value Change Auditing Builder"	GA17730
GRD-51649	GUI is failing on Custom Class update and delete when ACCESS_RULE or ACCESS_RULE_SET is missing	
GRD-44668	Issues with Active Threat Analytics dashboard - solr_test shows SSL exceptions on MUs	GA17675
GRD-51200	System backup and Archive failing after Upgrade from V11.2 to V11.3	GA17682
GRD-52135	Azure Data Stream DAM Reports information not expected	GA17680
GRD-49826	Extra Character needed on VA Test ID 445 fail statement as in version 11.2	GA17637
GRD-49367	GDM V11.3 || PostgreSQL DB datasource resets to (pre-upgrade from V11.2) original value in custom database field	GA17562
GRD-48570	After upgrading to 11p300 management units are indicating "Attention: disk almost full"	GA17528
GRD-46132	v11.0p215 Oracle 19c HPUX 11.31 with S-TAP-11.2.0.10_r109349 - bind variables not showing properly - "null" is shown	GA17401
GRD-50582	Cannot search for all the procedures in MS SQL ("analysis on datasource using stored procedures")	GA17678
GRD-50959	GIM: S-TAP Upgrade from v11.2 to v11.3 with Exit caused Db2 to crash because exit_lib parameters are removed	GA17610
GRD-52004	Create Procedure statement not captured from Mainframe Db2	GA17657
GRD-52018	v11 sniffer 4024 - Sniffer Segfault Message and core files	GA17681
GRD-53249	Incorrect, "partial" or blank "Exception Description" in report for MSSQL	GA17718
GRD-54025	Snif does NOT receive SPAN Port Oracle Traffics	
GRD-52063	v11.3 DB auditing status in Cloud DB Service Accounts page showing Active for deleted instance	GA17692

GRD-49640	IBM i S-TAP Upgrade document/ instructions	
GRD-50936	V11.3 Snif-debug can’t generate Snif-debug coredump	GA17607
GRD-51291	Need a way to remove weak ciphers in port 8444	
GRD-42074	Can’t Restore Data Archive from TSM Server between different appliances	GA17599
GRD-48763	Policy change alert isn’t consistent	GA17652
GRD-49996	Query Rewrite Definition. Limit rows selected on Oracle 11 by using "ROWNUM" produces syntactically incorrect SELECT statements	GA17568
GRD-51750	Request to backport GRD-50384 to v11.3 - QRW_DEFAULT_STATE=2 parameter not available on GUI.	GA17687
GRD-50208	Active Threat Analytics Case - Full SQL report incorrectly populating the condition	
GRD-53148	Can’t collect DAM traffic from Azure PaaS Instance due to issues with the Datastreams	GA17712
GRD-49593	Scheduled policy installation isn’t stored in GUARD_USER_ACTIVITY_AUDIT	
GRD-51214	Missing Service Name in the VA reports	GA17701
GRD-50763	Report is adding a forward slash character when datamart sends data to SIEM.	GA17627
GRD-51454	After CM upgrade to V11.3- GUI not loading and many inserts/deletes on CHANGE_TRACKER_S-TAP_PROPERTIES waiting for lock	GA17685
GRD-53066	Hierarchical Group not saving members or groups with backslash	GA17714
GRD-51275	Insert/Update Group Member in Policy	GA17612
GRD-51368	The "list_health_node" GRDAPI command's output is incomplete: details are null	GA17623
GRD-51986	v11.3 Detail Test Exception and Test Exception Problems	GA17690
GRD-52225	v11.3 Duplicate entries in Result Details Column	GA17686
GRD-49354	v11.3 | "Test Exceptions" Default Report & deleted assessments	GA17530
GRD-53157	Request for document update to avoid GIM installation to go into listener mode unconsciously.	GA17731
GRD-51487	GIM server report bundles having "_0" as the bundle name suffix	
GRD-52724	Distributed report (immediate) is not returning data	GA17710
GRD-50037	Failure to retrieve "Unit utilization timechart" information on CM for all registered MUs at once	GA17689
GRD-48195	FIREWALL is always enabled, even in FIREWALL_INSTALLED=0	GA17572
GRD-53078	V11.2 and V11.3 || Active Threat analytics shows threats but doesn't show supported data (MS-SQL)	GA17729
GRD-49816	StealthBits | FAM for NAS stops all monitoring	GA17727

GRD-49596	Performance issue on Oracle DB server when A-TAP enabled and K-TAP not loaded	GA17529
GRD-46618	Aggregator Import Fails into GDMS	GA17454
GRD-46393	Data Classification Process Objects Definitions Export doesn’t properly relate changes to Exclusion Groups at Definitions Import execution	GA17536
GRD-47234	WINTAP receives empty collector from ELB and tries to use it. Also removes collector entry on S-TAP ini file, which will make upgrades fail	GA17452
GRD-53141	V11.3 Can’t Save Password in Results Export (Files)	GA17720
GRD-47094	Records affected count returns incorrect result	GA17570
GRD-49662	Upgrading v11.3 WINS-TAP failed due to couldn't copy PrcMonitorMsgs.dll or DbMonitorMsgs.dll	GA17666
GRD-53216	"K-TAP status" is green in the "Deployment Health Table" when the S-TAP EXIT is configured	GA17715
GRD-47529	Windows GIM Upgrade from CM consistently throws ERR=1309 Read time-out	GA17531
GRD-37739	Appliance backup doesn’t retain public keys/cert	
GRD-47685	Win S-TAP may send failover request to ELB with DISCOVERY_INTERVAL>0 and Discovery times out	GA17509
GRD-33280	MS SQL SERVER Data Restore using NetBackup while S-TAP is running means a file transfer speed of 1 Gbps - without S-TAP running is 4-5 Gbps	GA16946
GRD-49440	Cron job for Scheduler skips increment	GA17665
GRD-46215	Incident Generation Process execution throws exception: "java.sql.SQLSyntaxErrorException: Unknown column '<ID>' in 'where clause'"	GA17431
GRD-46628	Alerter keeps sending emails for the same alert event every minute	GA17553
GRD-47266	LDAP import failing with SocketTimeout	GA17487
GRD-49855	Kernel Panic with Kernel 4.1.12-61.1.28.el6uek.x86_64 while installing S-TAP v11.3	GA17559
GRD-42239	CVE-2020-9484 Apache Tomcat 7.0.0 < 7.0.104 Remote Code Execution	GA17460
GRD-49580	Custom table data upload is failing for all Db2 datasources after upgrade to v11.3	GA17619
GRD-49004	Cyberark Integration version question	GA17549
GRD-45902	Tomcat keeps shutting down within a minute if a custom alert class that uses JDBC is triggered during startup.	GA17521
GRD-47737	Sniffer must_gather doesn’t complete without collector reboot	GA17502
GRD-47653	Report CAS Saved Data not displaying request information	GA17490
GRD-47841	Snowflake and other plugins do not work (Logstash JDBC plug-in issue)	

GRD-47018	LDAP users import failure	
GRD-49651	OS upgrade procedure for different platforms with S-TAPs installed isn't clear	
GRD-51088	Spot large ELB failover offenders in must gather	
GRD-48069	K-TAP dropping even with multithreading enabled	GA17603
GRD-53005	Teradata Database Error Code and Database Error Text show N/A in V11.3 p315 in Teradata	GA17721
GRD-48201	Add Clarification to the KC to differentiate between ELB and S-TAP Load Balancing	
GRD-53349	PostgreSQL Datasource Falsely Shows Test Connection as Successful	GA17741
GRD-50628	GIM certificate CLI, unable to select range of servers (not specific one, or 'all')	
GRD-46485	VCS Filesystem loading delays causing Guardium agents (GIM & S-TAP) to fail as they can't find directory	GA17624
GRD-47173	"Resource Deployment" information show "GIM Installed"=no if GIM is Installed but S-TAP/WINS-TAP had been installed for the first time and failed.	GA17466
GRD-47713	Documentation improvements	
GRD-47120	Guardium File Policies (FAM) don't allow to share policies with Guardium Roles	GA17449
GRD-46420	Upgrading KTAP through GIM on AIX is failing due to using rsyslogd	GA17437
GRD-53325	Be able to turn mini level ELB debugging on/off through Cli command	
GRD-44452	KTAP loader messages not appearing correctly in GIM Events list	GA17465
GRD-46475	When the custom bundle number reaches revision number 1000 the following bundles keep getting generated with revision number 1000 and GIM server refuses to register them as duplicates	GA17423
GRD-48951	Discovery is creating false IEs causing Oracle DB performance issues high Disk I/O	
GRD-45437	Request KTAP 4.18.0-147.el8.s390x	
GRD-51186	Request documentation update concerning "auto_install_on_db_server_os_upgrade" parameter	
GRD-46673	Connect to IP isn't being evaluated with default fast TCP verdict	GA17428
GRD-49281	Db2 Debug log isn't being disabled correctly after being enabled.	
GRD-49960	Support for VM level live backup	
GRD-52778	2310 - PASSWORD_LOCK_TIME Testing	GA17699
GRD-51794	MongoDB - Incorrect Data	
GRD-48147	Risk Spotter Watch list Population	GA17476

GRD-50702	Syslog filled with nanny messages	
GRD-47936	Unable to log in on several Managed units	GA17505
GRD-47373	Time Period isn’t showing the correct name in Query Summary	GA17442
GRD-47331	Using observed procedures isn’t working as expected on v11.1	GA17495
GRD-48911	Performance issues and missing data on the discovery scenarios screen	GA17676
GRD-51104	CVE-2004-2761 ssl certificate signed using weak hashing algorithm on port 8586	GA17608
GRD-51886	"CREATE" and "CREATE OR REPLACE" commands aren’t getting logged by collector.	GA17659
GRD-51535	False negatives in the "Deployment Health Table" for K-TAPs	GA17688
GRD-47641	Password change Rest API command error	GA17635
GRD-47228	Support show netstat grep not working properly	GA17459
GRD-46181	ReS-TAPi call to Windows S-TAP inspection engine returns ERROR 2007	GA17418
GRD-51884	Pausing Schedule of Auto discovery scan jobs not generating GUARD_USER_ACTIVITY_AUDIT record	GA17695
GRD-47562	AWS Secret Access Key disappears after changing to another tab or by signing off on v11.2	GA17467
GRD-47742	Data Classification Problem	GA17492
GRD-54717	Add note that only 'Tabular Report' is supported as Audit Task Report	
GRD-46814	Password not masked in Store procedure to change password "sp_password"	GA17424
GRD-51740	show remotelog test fails even when syslog might be successfully sent to the remote server	GA17719
GRD-48723	Error in slon looper with session tuple	
GRD-46860	11.2 store system snmp query community command not modifying /etc/snmp/snmpd.conf file	GA17435
GRD-49438	"restart gui clear" doesn’t work	GA17655
GRD-49528	Collectors in different timezone than CM stays in Pending status on Distributed Datamart status.	GA17626
GRD-49633	Data Archive over SCP in v11.3 iso fails due to permission issue	GA17633
GRD-50320	v11.3 VA tests stating unable to access when they're programmatically defined not to	GA17589
GRD-51690	v11.3 Test 58 - Oracle Patch Level has an error in its Short Description	GA17650
GRD-52047	Classification process progress status bar show zero percent progress and doesn’t change	GA17684
GRD-50894	Guardium - IAM Instance Profile Authentication - Fix privileges	GA17514

GRD-51515	Guardium 11.2 Report/Query Definition for Sort Order isn’t updating to show correct changes	GA17663
GRD-47602	CLS_LOG table isn’t getting purged	GA17656
GRD-50687	"Attribute type Date can't have Operator LIKE" isn’t checked when creating new query	GA17649
GRD-51793	Guardium: Analytic User Feedback - Failed to save the query	GA17642
GRD-49963	ACCESS_RULE_DESC size for GDM_INSTALLED_POLICY_RULES and GDM_CONSTRUCT_TEXT is different	GA17638
GRD-53264	Error When Enabling Risk Spotter	GA17740
GRD-46271	iS-TAP client ip showing 0.0.0.0	GA17567
GRD-47457	unencrypted iSeries traffic with TLS option marked	GA17554
GRD-53787	Win S-TAP V11.2.0.250 crashes by NmpSniffer	GA17733
GRD-49372	v11.3 Wrong Assessment Gets Deleted Between Double-Prompts	GA17644
GRD-49412	v11.3 Deleting audit process task through search disables save button	GA17540
GRD-50645	Delete certificate keystore doesn't allow multiple selections	GA17586
GRD-48128	Vulnerability detected in Guardium: SLOW HTTP HEADERS	GA17484
GRD-54414	GUI time falling behind actual time on appliance	GA17742
GRD-52071	Include guard_agg.out file into "support must_gather agg_issues"	GA17691
GRD-52189	MongoDB Compass access Replica-set Data Store only initial SQLs were captured	
GRD-52457	The number of SQL errors recorded after the upgrade to version 10.6 has increased significantly	GA17707
GRD-47446	Database discovery fails to discover variants of MySQL (example: wampmysql64)	GA17488
GRD-50044	Guardium for Z/OS (Steps to create an exception rule with the error code and the table)	GA17615
GRD-53907	My custom report failed to view when custom report renamed with display name from customization.	GA17725
GRD-51624	DISA STIG References and checks	GA17694
GRD-52911	Guardium VA Finding Language 2749	GA17700
GRD-49389	V11.2 : Must Gather -> Compliance_mon_issues -> QUERY_ENTITY : wrong output file (QUERY_HEADER)	
GRD-49395	V11.2 : Must Gather -> Compliance_mon_issues -> CLS_PROCESS table collection	
GRD-53727	Add CHANGE_TRACKER_CHANGE_HISTORY to deployment must gather	

GRD-51959	QRW_DEFAULT_STATE=2 parameter doesn't work when using HeidiSQL connection to MSSQL due to the max limit of PRIORITY_COUNT	GA17661
GRD-51202	Clarification on Hadoop supported traffic and supported rule actions	
GRD-48178	Correlation DLLs not being injected into SQL Server	GA17477
GRD-48186	Guardium Archive and Back up to S3 - IAM Instance Profile Authentication	GA17514
GRD-51909	Include solr-addVA.log and solr-upgrade.log in datamining must gather	
GRD-51040	Incorrect %%analyzedClientIP & %%SessionID in msg template variable in v11.x KC	
GRD-47931	Activity on custom tables isn’t logged in Guardium user activity audit	GA17483
GRD-50956	Need instructions for the GIM consolidated installer on both Windows and UNIX	
GRD-47818	Kernel messages indicate AIX host crash due to K-TAP increasing credential reference count without properly decreasing it	GA17494
GRD-47017	CMDB import not working	GA17498
GRD-47880	V11.2 || Mainframe Db2 datasource/scan fails	GA17500
GRD-45343	Consistent 'customTableDataUpload_105' failure on Aggregator where 'Enterprise No Traffic' is irrelevant	GA17625
GRD-51110	Does Audit process for Data Classification support to send attachment with CSV format	GA17697
GRD-48261	(Documentation) Limitation in upgrading Win S-TAP V10.x to V11.x using GIM	
GRD-49998	Guardium allocating activity to the incorrect OS User	GA17594
GRD-47637	FDEC for NAS returns ERROR - Scanner: SqLite [near "s": syntax error]	GA17486
GRD-51016	v11.3 Deprecate DBMS source code encoding or encryption tests	GA17662
GRD-47591	GUI Certificate steps update	
GRD-51788	Include CHANGE_TRACKER_S-TAP_IE_PROPERTIES in deployment_issues must gather	
GRD-49546	CrowdStrike and BlueFringe setup on Guardium Cloud Appliance	GA17664
GRD-50041	Placement of reports in Dashboard altered when saved	GA17592
GRD-52223	Update External References for Test 308 and 309	GA17658
GRD-50077	Outliers API parameters need to be clarified	
GRD-49558	Incorrect definition of DISK_USAGE_ADJUSTMENT_FACTOR	
GRD-47846	Unit Utilization report failed on Aggregators 11p300	GA17634
GRD-46649	Datasource Definition shows wrong column name	GA17472
GRD-46249	GUI not retaining column name changes for TimeStamp Attribute in Report Definitions	GA17455

GRD-47541	Upload of DPS Patch Guardium_11.0_DPS-Update_Q3-2020 fails with a generic error message.	GA17480
GRD-47763	Can't add catalog record when username contains backslash	GA17470
GRD-47072	Japanese Environment Issue - Query's main entity of "Client/Server" changed to "Client/Server By Session" automatically	GA17441
GRD-47724	SNMP Trap is always sent as SNMP V1 regardless of the configured version (v2c or v3)	GA17499
GRD-47928	Test emails not sent	GA17621
GRD-49180	Guardium Vulnerability Assessment question/issue	GA17517
GRD-46164	Windows GIM doesn't notify parameter change event to GIM Event List	GA17412
GRD-50429	Policy criteria 'Trigger once per session' doesn't work properly if 'Time Period' is used in the same rule	GA17585
GRD-44405	"support clean servlets ?" || appending QUESTION MARK ? should show usage	GA17429
GRD-47701	SQL data pattern regex issue for policy - Basic Data Security Policy [template]	
GRD-49846	Incorrect %%SenderIP parameter in KnowledgeCenter	
GRD-49621	Audit processes shown in to do list when not required	GA17538
GRD-48922	Clarify messages generated by runing snif must gather : "Rules exported into file srules.exp" and "Rules do not exist"	GA17526
GRD-49380	Enhance Risk Spotter must gather	
GRD-48005	Guardium cli "support must_gather sniffer_issues" can return "Rules do not exist" , ""warning: unable to open /proc file", "ptrace: No such process"	GA17473
GRD-46184	Audit process definition imported from another appliance isn’t listed in Definitions to Export menu	GA17415
GRD-47335	Restore appliance question is confusing	GA17450
GRD-44213	Need Documentation for Splunk Integration App	
GRD-47483	V10.6 AGG MustGather can’t be generated from GUI while CLI can generate fine	GA17391

Security Fixes

Issue key	Summary	CVEs
GRD-43683, GRD-43682	PSIRT: 234185 - SE - Customer Pen Test - Bruteforcable Shared Secret	CVE-2020-4690
GRD-48544	PSIRT: 254743 - SE - Pen Test 2020 - Application Error in IBM Security Guardium	CVE-2021-20377
GRD-42337	PSIRT: 244970 - Solr jars need upgrade	CVE-2014-0114 CVE-2015-1832 CVE-2016-1000338 CVE-2017-1000190 CVE-2017-15095 CVE-2017-15691 CVE-2017-15713 CVE-2017-7656 CVE-2018-1000632 CVE-2018-10237 CVE-2018-11771 CVE-2018-11797 CVE-2019-0201 CVE-2019-10247 CVE-2019-12415 CVE-2019-16869 CVE-2019-17571 CVE-2020-1945 CVE-2020-1950 CVE-2020-26939 CVE-2020-9488

Resources

IBM Security Guardium IBM Knowledge Center and online help
https://www.ibm.com/docs/SSMPHH/SSMPHH_welcome.html

Guardium patch types and naming convention
https://www.ibm.com/support/pages/node/6195371

GuardAPI and REST API reference
Guardium API A-Z Reference

Guardium supported platforms database
https://www.securitylearningacademy.com/mod/data/view.php?d=12&mode=asearch

Supported Platforms and Requirements for Guardium Data Protection 11.4
https://www.ibm.com/support/pages/node/6441975

Appliance technical requirements 11.4
https://www.ibm.com/support/pages/node/6481035

IBM Security Learning Academy
securitylearningacademy.com

Flashes and Alerts for IBM Security Guardium
https://ibm.biz/BdY5fe