Release Notes

==========

Product:	IBM Security Guardium
Release version:	Guardium 11.5
Completion date:	15 September 2022
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 11.5

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 11.5

Guardium 11.5 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 11.5

You can upgrade to Guardium 11.5 from any Guardium system that is running on version 11.0 and up. 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.

Installing or upgrading to 11.5 S-TAP

Guardium 11.5 does not support some versions of Windows S-TAP when it's used with the enterprise load balancing feature. Using incompatible versions can lead to a loss of communication with S-TAPs. Before you upgrade your Guardium system to 11.5, you must upgrade your Windows S-TAPs to a version that is equal or higher than the following versions: 11.3 revision 11.3.0.321, 11.4 revision 11.4.0.267, or 11.5 revision 11.5.0.143. For more information about S-TAPs, see the Windows or UNIX S-TAP release notes.

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 the following format: **SqlGuard_11.0p9997_HealthCheck_<date>.zip**

The version 11.0 Health Check patch 9997 must be successfully installed in the last seven days before you install the Guardium 11.5 GPU. If the Health Check patch isn't installed as recommended, the 11.5 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 11.5 GPU, you must resolve it before installing the 11.5 GPU. If the 11.5 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, purges, backups, and imports.

Installation can fail when aggregation processes are still running 60 minutes after the patch install starts. The CLI command **show system patch installed** displays "ERROR: Patch Installation Failed - Aggregation process running". If this issue occurs, reinstall the upgrade patch after the aggregation processes are complete.

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: Guardium version 11.5 upgrades the internal database from MySQL 5.7 to 8.0. Due to the change in database engines that are required for internal database upgrade, the installation on aggregator or central manager appliances might take significantly more time than the installation of older Guardium versions. The duration of installation depends on the amount of dynamic audit data that exists in the database.

Central managers with no audit data are not affected by this change and collector appliances are not affected.

Don't manually restart the system during the internal database upgrade even if it appears to be stuck. 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. If you're concerned about the status of the installation, use the CLI commands **support must_gather patch_install_issues** and **support must_gather agg_issues** and contact Guardium support.

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 11.5, 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.

Note: If LDAP authentication is used, you must update LDAP configuration after you upgrade to 11.5. For more information, see the following support page: https://www.ibm.com/support/pages/node/6848599

New Features and Enhancements

Alerts
CSV files can be attached to emails generated by a threshold alert. You can set up this function when you configure the alert.

API parameters
Several new modifiable Guardium API parameters are added. For more information, see modify_guard_param.

Certificate management with Venafi
Several enhancements are added to the Venafi certificate management feature. You can now use grdAPI commands to propagate Venafi configurations and certificates from a central manager to some or all the managed units. For more information, see Managing certificates with Venafi.

CyberArk
Guardium now supports the CyberArk AIM agent version 12.4.1. After you install the new CyberArk patch, the Guardium system indicates that CyberArk version 12.04 is installed (Version 12.04 is the Guardium equivalent of CyberArk AIM agent 12.4.1). You need not reconfigure your datasources to connect to CyberArk. Test a datasource to ensure that your Guardium system can establish a connection and fetch the password from your CyberArk vault. For more information, see Managing datasource credentials with CyberArk.

Datasources for Vulnerability Assessment
Support is added for Snowflake, MariaDB, and Oracle 21c.
SSL support is added for Informix, SAP Hana, and Sybase IQ.
Entitlement support is added for Amazon Redshift, Snowflake, MySQL, and MariaDB.

To support Oracle 21c from Oracle Autonomous Cloud, we have added Oracle Wallet support. A new datasource type "Oracle (DataDirect - Cloud Wallet)" has been added to the datasource screen.

For Oracle and MSSQL, you can now change the driver from DataDirect to OpenSource by using the grdAPI command *grdapi change_to_opensource datasourceType=<datasource> opensourceDriver=<datasource/service name>*. Manually revert to DataDirect by using the datasource screen in the UI.

Discover sensitive data
You can now use the Guardium API *grdapi pause_or_resume_scenarios* to pause or resume scheduling of Discover Sensitive Data scenarios.

Enterprise load balancer

You can identify conflicting group assignments of managed units by using a new report and alert. The conflicting condition is triggered when a managed unit is assigned to both the primary group and failover group that is mapped to an S-TAP group.

External S-TAP

From the External S-TAP instances page:

- You can now add a comment for an External S-TAP.
- You can select and delete multiple External S-TAPs. However, you cannot delete a running External S-TAP.
- From the *View details* section of the **Actions menu**, you can now delete one or more inactive containers from a group.

For more information, see The External S-TAP user interface.

From the Kubernetes tab of the Deploy External S-TAP window:

- You can now select the **Use internal load balancer** checkbox to have External S-TAP use an internal load balancer for the selected cloud provider. For more information, see Kubernetes tab.

External S-TAP images are no longer hosted on the Docker Hub. They can now be accessed at the following container registry address: icr.io/guardium-insights/guardium_external_s-tap.

IBM Security Discover and Classify

Guardium now supports IBM Security Discover and Classify**,** also known as 1touch.io Inventa for data discovery and classification. Import data from 1touch into your Guardium custom table at a scheduled interval by using a .csv file. Use predefined reports to display data from your custom table or customize your views by using the 1touch classification data import custom domain in the Guardium Query-Report Builder. IBM Security Discover and Classify uses network analytics, AI, and machine learning to continuously find and catalog sensitive and protected data, of any type, anywhere. This tool is a powerful complement to IBM Security Guardium products and the entire IBM Security portfolio.

MySQL and Netezza Exit library

For Linux/UNIX, The MySQL Exit library enables S-TAP® to monitor any MySQL database activities, whether encrypted or not and whether local or remote. The Exit libraries do not require A-TAP or K-TAP. For more information, see Configuring MySQL Exit.

The Netezza Exit for Guardium will be available in a future release of Netezza Performance Server (NPS). Any documentation for this feature is provided by IBM Netezza.

Real-time trust evaluator improvements

There are improvements to the UI for the real-time trust evaluator, along with other updates. The documentation is reorganized to improve readability. For more information, see Real-time trust evaluator. You can now configure the trust evaluator to look for and track anomalous conditions. For more information, see Configuring the trust evaluator.

Reports

You can now share your reports dashboard with other users by assigning permissions to roles.

SAML support

The SAML feature is an authentication process that gives users access to multiple web-based applications by using one set of login credentials. To use this feature customers will need to have an identity provider metadata file that is provided by their company. This metadata file contains a public certificate that

communicates with the Guardium appliance and can be found on the companies help page. For more information, see Configuring authentication.

Security incident policies
Two new security incident policies are available to help provide out-of-the-box security incident protection. For more information, see Security anomalies policy and rules and Password spraying attack policy and rules.

System enhancements
Guardium internal database is upgraded from MySQL 5.7 to 8.0. The new database version includes improvements in several areas that are related to the internal functioning of MySQL. For example:

- MySQL undo log handling is improved. Large undo log files are handled automatically, without interaction from support
- Increased usage of InnoDB storage engine, including the in-database dictionary, result in fewer table corruption issues.
- Security enhancements including new authentication plug-in improves security internally on appliances.
- Guardium development team has ongoing support and updates for the latest MySQL versions.

Vulnerability Assessment (VA)

- You can now add custom comments to a vulnerability assessment test. These comments can be added to pre-defined or custom tests and can be exported or imported between Guardium systems.

- In the vulnerability assessment test results, you can choose to include or exclude test scores for databases that are not supported. When the vulnerability assessment test score is "Not Applicable for the DB version", the test results and recommendations now display the database versions that are supported.

- New improvements are added to the process of uploading and logging DPS reports. You can now use the dps_upgrade log to track the DPS upgrade process. The log file is at the following location: /opt/IBM/Guardium/log/DpsUpgrade.log

- Integration with ServiceNow: A certified ServiceNow application is available for clients who prefer to use ServiceNow as their response control center. The Guardium Vulnerability Assessment plug-in is available on the ServiceNow site and can “pull” data from Guardium Vulnerability Assessment via RestAPI. The app helps synchronize VA database type, database group, and test-result entries for tighter integration with ServiceNow Configuration Management Database (CMDB). Users can start scanning jobs and tests right from the ServiceNow user interface and the app shows all VA results within ServiceNow. Additionally, the app can be used to centrally manage all tools and can automatically assign tickets through ServiceNow. For clients who do not want to use ServiceNow as the front end, Guardium Vulnerability Assessment also provides more traditional integration with ServiceNow, helping operationalize and orchestrate VA remediation. This out-of-the-box integration allows users to send failed vulnerability scan results from the solution to ServiceNow.

Watson Knowledge Catalog integration
Integrate your Guardium® data with Watson™ Knowledge Catalog policies to help ensure that your Guardium data is protected through Watson Knowledge Catalog. An IBM Cloud Pak for Data license is required. For more information, see Configuring Watson Knowledge Catalog data protection.

Sniffer Updates

The following Sniffer patches are included in Guardium 11.5. The latest sniffer patch that is included in Guardium 11.5 is v11.0p4048.

Sniffer patch number	Issue key	Summary	APAR
11.0p4034		https://delivery04.dhe.ibm.com/sar/CMA/IMA/0a4v5/0/Guardium_v11_0_p4034_sniffer_update_release_notes.pdf	
11.0p4039		https://delivery04.dhe.ibm.com/sar/CMA/IMA/0acdx/0/Guardium_v11_0_p4039_sniffer_update_release_notes.pdf	
11.0p4042		https://download4.boulder.ibm.com/sar/CMA/IMA/0alne/0/Guardium_v11_0_p4042_sniffer_update_release_notes.pdf	
11.0p4043	GRD-61618	Add SERVER DESCRIPTION into DAM policy condition	
	GRD-60251	Fixing PARSER_ERRORs for MEMSQL sessions: unexpected token: /*! , unexpected token: ESTIMATE	GA17930
	GRD-57366	UC config - upload import files Oracle Postgres - CloudWatch	GA18023
11.0p4044	GRD-61955	Sniffer crashing with Cassandra Traffic	GA17981
11.0p4045	GRD-62091	Error when running db2_exit_health_check script	GA17980
	GRD-61955	Sniffer crashing with Cassandra Traffic	GA17981
	GRD-55019	Guardium is not capturing every instance of the same query from Oracle.	GA18010
11.0p4048	GRD-62091	Error when running db2_exit_health_check script	GA17980
	GRD-61955	Sniffer crashing with Cassandra Traffic	GA17981
	GRD-61910	Sniffer crashing with SGATE rules	GA18022
	GRD-61618	Add SERVER DESCRIPTION into DAM policy condition	
	GRD-60388	p4039 Snif crashing with unknown structure Mysql packets	GA17931
	GRD-60251	Fixing PARSER_ERRORs for MEMSQL sessions: unexpected token: /*! , unexpected token: ESTIMATE	GA17930
	GRD-57366	UC config - upload import files Oracle Postgres - CloudWatch	GA18023
	GRD-56752	sniffer crashing/segfault	GA18014
	GRD-55019	Guardium is not capturing every instance of the same query from Oracle.	GA18010
	GRD-47412	SAP batch job traffic randomly missed	GA18015

New platforms and databases supported

- Cassandra 4.0
- Cloudera 7.1.7
- CockroachDB 21.1.11
- Couchbase 7.0.2
- CouchDB 3.2
- Elasticsearch 7.15
- Greenplum 6.19
- MariaDB 10.7.3: Windows (non-SSL only) and Unix.
- MemSQL 7.8
- MongoDB 5.0
- MySQL 8.0.28: Windows (non-SSL only) and Unix.
- Neo4j 4.4.4
- Oracle 21c
- Postgres 14
- Redis 6.2
- SAP HANA 2.0 SPS06
- Teradata 17.10
- Vertica 10.1.1

Deprecated platforms, functions, and commands

Deprecated platforms in 11.5

Support for HP-UX 11.31 PA-RISC is deprecated (The only supported version of HP-UX version is 11.31 IA64).

Deprecated functions in 11.5

The Application Lifecycle ("Guardium ecosystem") interface and associated functionality is no longer supported.

Deprecated commands in 11.5

Ecosystem commands:

- `support must_gather eco_system_issues`
- `show system ecosystem`
- `store system ecosystem`
- `restart ecosystem`
- `stop ecosystem`
- `start ecosystem`

Inspection engine commands:

- `show inspection-engines all`
- `start inspection-engines all`
- `stop inspection-engines all`

Session level policy commands:

- `import session_rules`
- `support show session_rules`

- `support store session_rules`

Venafi certificate management commands:
- `store certificate gui venafi`

Deprecated platforms and functions in a future release

Platforms
HP-UX is no longer supported starting with Guardium version 12.0.

Functionality
The Exit interfaces for Db2 and Informix are preferred to using A-TAP for Db2 or Informix. The Exit interfaces offer several advantages:
– no need to install or use kernel modules (K-TAP)
– lower CPU utilization
– new database versions are supported sooner

A-TAP for Db2 and A-TAP for Informix are no longer supported starting with Guardium version 12.0.

For information about using Db2 Exit, see:
https://ibm.com/docs/en/SSMPHH_11.5.0/com.ibm.guardium.doc.stap/stap/db2_stap_integrate.html
For information about using Informix Exit, see:
https://ibm.com/docs/en/SSMPHH_11.5.0/com.ibm.guardium.doc.stap/stap/informix_exit_cfg.html

Known limitations and workarounds

Component	Issue key	Description
Active threat analytics	GRD-64434	When a case is added to a group, the UI becomes unresponsive. **Workaround:** Close the browser. Access the group builder, select the relevant group, and then add the Server IP, database, or DB user to the group.
	GRD-64391	When you select a case and open the case dashboard, the quick search page does not open. **Workaround:** Open the investigation dashboard and choose the “custom” option in the date range filter. Enter the case creation date as the “from date” and one hour later as the “to date”. Then, add the filters such as Server IP, database, DB user, or OS user according to the source field of the case.
Aggregation	GRD-63435	Some aggregation jobs might complete successfully but not display the completion time in the aggregation/archive log. **Workaround:** This issue can occur due to an intermittent problem with post-aggregation steps after the main job has finished. To confirm if this is the case for jobs with no end time, check the following items:

		1. Right click the job in aggregation/archive log and select "Aggregation/Archive debug log". At the top of the debug log, the "Aggregation Stage" column displays "<job> - END". Example: "IMPORT data – END". 2. Check whether the aggregation jobs that follow are successful and end time is displayed. If both are true, you can ignore the issue. If not, then there might be a problem with aggregation. Run the CLI command **support must_gather agg_issues** and contact Guardium support.
	GRD-55487	Data archive files from Guardium version 9.1 aggregators cannot be restored to Guardium version 11.5. This is due to the large difference in the version of the underlying MySQL database between version 9.1 and version 11.5. (Note: Data archives from version 9.1 collectors can be restored to version 11.5) **Workaround:** If you need the data archive on version 9.1 aggregators, build a new Guardium stand-alone version 11.4 system and restore the version 9.1 data. Then, upgrade to Guardium version 11.5.
Database discovered instances rules	GRD-64234	Group names are not supported for the Host parameter in the new filter rule for Database Discovered Instances. **Workaround:** Provide a comma-separated list of names or a hyphenated range of inclusive numbers. Example: If you previously created a group name called "my_host_group" with members 9.10.55.101 and 9.10.55.102, you cannot reference the group name. You must specify a comma-separated list of members. Similarly, for the 'Port range start' and 'Port range end' fields, specify an inclusive list of port numbers. Example: "1520-1530, 1621, 1622".
Discover sensitive data	GRD-64271	When a new discovery scenario is added, the page does not load immediately. A fix is available in an upcoming patch release.
GUI	GRD-64072	The GUI takes over 9 minutes to restart when the *restart gui* command is used. A fix is available in an upcoming patch release.
Policy builder	GRD-64420	An error occurs when you view the ad hoc analysis results. A fix is available in an upcoming patch release.
Query builder	GRD-63670	If you have previously copied and saved the predefined query "Installed patches" in which you created conditions that reference the fields [CREATION_DATE and/or UPLOAD_DATE], you must save the query again when you preview it after you upgrade to Guardium 11.5.
Risk spotter	GRD-48198	Risk spotter does not recognize an updated Dynamic Auditing Policy selection. **Workaround:** Restart Tomcat on the Guardium collector to refresh the Risk Spotter policy ID in watchdog.

ServiceNow	GRD-63725	No Vulnerable items are displayed in the page *Vulnerability Response -> Vulnerable item.* **Workaround:** From the IBM Guardium UI, access Configuration > Preferences. Then, click “Update”. After the preferences are saved, any future synchronization of "Test Result Details" for CVE tests adds the failed test results into Vulnerable Item table.
Session level policy	GRD-61760	You cannot save a service map entry that does not include a port number.
Smart card authentication	GRD-64483	Smart card authentication does not work as expected with Guardium 11.5. The fix for this issue is available in an upcoming patch release. Meanwhile, you can contact IBM support to obtain an interim fix to enable the smart card functionality.
ECS	GRD-59770 GRD-64496	ECS 3.6 cannot run the *support clean centera_files* command because Centera is not supported.
Solr	GRD-64444	Solr does not work as expected on some managed units. **Workaround:** Run the grdAPI commands *grdapi restart_solr* and *grdapi get_solr_status*. If the status is “Solr not running”, run the *clean solr upgrade* command.
	GRD-64471	If Quick Search (solr) appears to be unstable on the collector, use the CLI command *restart stopped_services*.
Risk spotter	GRD-64435	When a new DB user or Server IP is added, the group is not updated immediately. **Workaround:** Wait for a few minutes and try again to see the updated list. A resolution is available in an upcoming release.
Universal connector	GRD-63379 GRD-54393	When you upgrade from 11.4 to 11.5 by using the backup and restore method, the universal connector status is not retained. **Workaround:** Upload missing plug-ins, re-enable the universal connector.
User management	GRD-64382	When you log in as *accessmgr* and edit a user, you might encounter an error when you use the “back” button. **Workaround:** After you edit a user, refresh the page and then click on the next page of users. The page loads as expected.
Windows S-TAP with enterprise load balancing	GRD-64080	Guardium 11.5 does not support some versions of Windows S-TAP when it's used with the enterprise load balancing feature. Using incompatible versions can lead to a loss of communication with S-TAPs. **Workaround:** Before you upgrade your Guardium system to 11.5, you must upgrade your Windows S-TAPs to a version that is equal or higher than the following versions: 11.3 revision 11.3.0.321, 11.4 revision 11.4.0.267, or 11.5 revision 11.5.0.143.

Bug Fixes

Issue key	Summary	APAR
GRD-63513	Patch p370 fails to install in CM with EFI Boot option.	GA18079
GRD-62758	Login fails when connecting to MSSQL via External S-TAP with ODBC	GA18034
GRD-57688	Can't install Windows S-TAP V11.3.0.219 via GIM because the module download fails	GA18039
GRD-63381	Db2 EXIT causing SQL delays	GA18037
GRD-62956	Discovery is not configuring Scan_Listener for socket marker	
GRD-60434	Corner case between Failover and rebalancing in ELB environment causing STAP using unusual High CPU workload	GA18062
GRD-62091	Error when running db2_exit_health_check script	GA17980
GRD-56223	Performance for FAMforNAS activities	
GRD-59918	toad Db2 client hangs and Db2 server process is high until 200% after applying query rewrite	GA17935
GRD-61618	Add SERVER DESCRIPTION into DAM policy condition	N/A
GRD-60415	ORACLE DB username blank: database username was listed as a carriage return character	GA17914
GRD-59421	Guardium datastreams cannot support assume-role for multiple roles when using instance-profile.	GA17898
GRD-57314	v11.4 Collectors filling /opt/IBM/Guardium/tomcat/dump/ directory disabling appliance.	GA17873
GRD-54956	Discovery not working on AIX box with numerous instances.	GA17848
GRD-57417	CVE-2021-44228 log4j vulnerability	
GRD-54641	11.5: Qualys Scan Vulnerability || Port 8447 and Port 16019 || After Patch 315 and 320	GA17768
GRD-55172	After applying v11.3 325 CM GUI/tomcat keeps crashing due to Exception in thread "elasticsearchxxx"	GA17754
GRD-57949	Post upgrade to p400 unable to set LDAP guiuser from CLI	GA17918
GRD-56339	Flatten Hierarchical Groups not working	GA17802
GRD-47633	MySQL crashed and created huge core files after installing truncate undo files patch	GA17628
GRD-57586	Log4j patch stuck restarting Solr	GA17819
GRD-61623	Add DB_PROTOCOL into DAM Policy condition	N/A
GRD-60445	Audit process not writing results to SYSLOG p410	GA18017
GRD-62439	Editing Groups in Group Builders it's giving a timeout	GA18018

GRD-57924	Intermittent Tomcat "java/lang/OutOfMemoryError" caused QuickStartJobGroup.QuickStartJobError	GA17880
GRD-61607	SNMP traps with invalid format on 11.4 with Netcool/OMNlbus monitor system. The Error said "No rule found in the Enterprise ID OID .1.3.6.1.4.1"	GA17990
GRD-62120	v11.4 CyberArk Installation Fails	GA18020
GRD-62432	Invalid Shared Secret	GA18032
GRD-62483	v11.4 p440 Breaks SmartCard Authentication	GA17987
GRD-62762	Db2 TOAD/DBEAVER hang if Query Rewrite Applied on SQLs with long WHERE clause	GA18067
GRD-59128	CVE-2017-13098 vulnerability on port 16019 for Guardium v10.6	GA18012
GRD-54648	Kernel Panic Solaris 11.4.30.88.3 with STAP 11.3.0.0_r109764	GA18064
GRD-59547	File "failover.isam" is filling up servers with STAP agent V11.4.0.179	GA17955
GRD-55293	Failing Backup jobs in Guardium - ERROR: Backup file was not copied. Method=TSM	GA17822
GRD-63344	Oracle Unified Audit (OUA) DB instance information lost after OS reboot with GIM	GA18052
GRD-63301	ELB: STAP retry mechanism during installation with groups defined and ELB map locked	GA18066
GRD-61165	Require documentation on how to implement multiple roles when using instance-profiles in Cloud Database Discovery	
GRD-62585	FAM not visible on GUI || FAM config gets disabled	
GRD-51041	KTAP loads automatically after reboot	
GRD-60891	S-TAP Installation creates directory "C:\Guardium" unexpectedly when setting non C: drive with no directory in INSTALLERLOGPTH (V11.3.0.219, using local silent install)	
GRD-62903	Windows OS crash, caused by WfpMonitor.sys V10.6.0.333 (BugCheck 0xD1)	GA18041
GRD-60844	Can't set directory to WINSTAP_WER_DUMP_FOLDER from GUI	GA17928
GRD-60861	GIM Installation creates directory "C:\Guardium" unexpectedly when setting non C: drive with no directory in INSTALLERLOGPTH (V11.3.0.256, using local install wizard)	GA17927
GRD-56568	GimConnector.exe hangs in OpenSSL TLS negotiation	GA17820
GRD-61309	SQL Dropping TCP connections (in WFP driver) after upgrading Window STAP to 11.4.0.220 (V7 protocol)	GA17975
GRD-58884	Guardium ETAP "locks up" while handling the data transfer	
GRD-54887	Guardium is not capturing a specific type of data	GA17770
GRD-59562	Problem with patch p405 notification on CM	GA18058

GRD-62618	Blank "Last Connect" field in "Data-Sources" report for CouchDB datasources	GA18016
GRD-58575	Guardium Assessment - SQL concurrent connections (Test ID 2589)	
GRD-58849	Documentation needs to mention WINSTAP_CMD_LINE should be used for parameters not editable via the GUI	Doc Defect
GRD-50588	Manage units are not showing on the CM after DST (java.sql.SQLException: HOUR_OF_DAY: 2 -> 3)	GA17908
GRD-58984	The default value of MEM_USAGE_LIMIT is too small (PINK S-TAP)	GA17977
GRD-61910	Sniffer crashing with SGATE rules	GA18022
GRD-59846	Patch installation failure due to missing RPMs	
GRD-61104	NANNY_TEST_RSYSLOG generates email every 5 minutes even after the test flag is set to 0	GA18013
GRD-58995	Solaris 11.4 DB: Oracle 19.x - Dtrace conflict.	
GRD-60075	All Audit Processes with blank results via GUI only.	GA18001
GRD-59369	Active Threat Analytics case closure error	GA17905
GRD-60516	GIM / S-TAP on Solaris db zone does not start in Solaris 11.4	GA18028
GRD-58576	Guardium External Ticketing System	GA17889
GRD-52448	Unipol - aggr02 outliers do not appear on CM	GA17758
GRD-56393	Every 5mins smtp guard-sender services stopped running	GA17812
GRD-53629	Several DB2 started tasks did not re-connect after IPL	GA17891
GRD-60493	Add SESSION_ERROR exception type to possible value table	GA17999
GRD-49718	Improvement on ELB's effort to remove leftover STAP.	GA17669
GRD-55281	v11.3 Patch Issues promoting Backup CM	GA17800
GRD-55442	Promotion to Backup CM does not copy test detail exceptions or datasource groups	GA17760
GRD-59778	Add to VA Test 2572 - Oracle DBMS application object ownership	GA18004
GRD-60498	Performance issue with ATAP on due to an issue with Db_request_handler	GA17960
GRD-51707	Intermittent false negatives with CM Deployment Health Table S-TAPs Connectivity Status	GA17771
GRD-57553	Plug-in developed by customer - Universal connector plug-in: file not found	
GRD-56903	Servlet [SwaggerInitializationServletV1] in web application [/guardhelp_kc] threw load() exception	
GRD-58472	Guardium Appliance ran out of space (98% used) on / partition due to core dump	
GRD-57353	After installing patch p340, Cannot SSH to IBM Cloud Guardium Appliance. Access only via Rescue Mode	

GRD-58606	ATAP activation doesn't preserve stickybit and causes inability to connect to DB	GA17910
GRD-55670	Investigate use of a single GIM cert across multiple GIM servers	GA17792
GRD-56943	11.4 upgrade failure due to CLS_LOG table crash	GA17892
GRD-56464	ELB constantly tries to delete STAPs that are not there	GA17961
GRD-59375	Import from LDAP in group builder times out resulting not fetching all members	GA17967
GRD-60742	Server HKL25xxxx19 Supervisor service is inactive after upgrade	GA17994
GRD-61535	Product folder (for example, "$IBM Windows GIM$") is created under %SystemRoot%\. Need to have an option not to create any file under C:	GA17991
GRD-55963	Vulnerability detected , tls v1.0 allowed in port16019	GA17863
GRD-55276	v11.2 Frequent sniffer restarts	GA17779
GRD-56701	CAGS - Real-time trust evaluator (RTTE)	GA17841
GRD-60607	Real-time trust evaluator || Confusing feature introduction in documentation	
GRD-58753	Oracle VA Test 128 "The SYSTEM and SYS user account status is Open or Expired" should be deprecated	GA17944
GRD-60294	Back up Configuration export from CM to Backup CM failed as the user's (username: aggregator) password has expired.	GA17925
GRD-59552	V11.4 "support reset-managed-cli" returned "Error decoding root passkey!"	GA18104
GRD-59934	KTAP request 4.18.0-348.12.2.el8_5, x86_64 STAP v11.3	
GRD-59875	KTAP request 4.18.0-305.25.1.el8_4, x86_64 STAP v11.2	
GRD-59429	KTAP 4.18.0-348.12.2.el8_5.x86_64 STAP 11.2	
GRD-59876	KTAP request 4.18.0-305.25.1.el8_4, x86_64 STAP v11.3	
GRD-58129	KTAP request 4.18.0-348.7.1.el8_5.x86_64 STAP v11.3	
GRD-57658	Valid SQL (with comma in numbers) in DB2 for iSeries generated PARSER_ERROR	GA17869
GRD-62936	K-TAP Module request for 3.10.0-1160.66.1.el7.x86_64 on V11.3	
GRD-58635	Removing IBM Docker Network Interface	GA17878
GRD-55625	v11.4 - Custom Datasource Properties: The field cannot contain non-BMP characters	GA17786
GRD-59156	Classification Scans errors in SAP HANA BW system	GA17896
GRD-62102	Import of large policy definition fails with java.lang.ArrayStoreException	GA18011
GRD-57700	Violation Timestamp in Incident report	GA17963
GRD-60042	Unable to authenticate at the CLI using SET GUIUSER command and GUI user	

GRD-59667	oracle ownership and permission changed unexpectedly after ATAP activation	GA17910
GRD-55501	Error while resetting MU CLI password on CM	GA17782
GRD-55698	Error <guardium_audit> is already created. However, there is no record for this database in your DATASOURCE table when use Value Change Audit	GA17806
GRD-57629	KTAP request 4.18.0-348.2.1.el8_5.x86_64 for STAP v11.3	
GRD-56275	STAP Verification Exception: Column 'DATASOURCE_NAME' cannot be null	GA17877
GRD-58595	Guardium S-TAP Failure "Can't Start K-TAP"	GA17947
GRD-55915	Managed appliance down during 11.4 upgrade stuck in the "POST: Starting mysql." step for almost 12 hours.	GA17803
GRD-52639	S-TAP Verification is failing on Db2 EXIT IE	GA17780
GRD-56449	WINSTAP upgrade from v10.6 to v11.4 aborted because some dlls are being used by another process	GA17850
GRD-57421	Venafi Integration errors	GA17886
GRD-56974	V11.4 snmptrap cannot send message - "Cannot find TrapOID in TRAP2 PDU"	GA17831
GRD-56289	Guardium sending excessive rsyslog service status emails (No response from remotelog host) when remotelog host is a cluster	GA17808
GRD-46227	QID-38695 TLS 1.2 vuln on scanned appliances	
GRD-56290	Error "Unexpected error has occurred. Please contact your System Administrator" when opening Compliance Monitoring.	GA17814
GRD-56022	v11.4 MS SQL SSIS enabled significantly expands findings in VA	GA17826
GRD-58127	"KeyError: 'interface-name'" message is displayed while trying to run CLI network commands	GA17881
GRD-59151	The Synchronize Security Assessments feature does not sort datasources alphabetically	GA17874
GRD-57747	Three VA test values deprecation for Oracle 11g R2 and later releases	GA17825
GRD-54204	Error update cli password by "accessmgr" in GUI	GA17778
GRD-59127	PostgreSQL tests 308 and 309 not passing newer patch versions	GA17899
GRD-56967	After applying V10.6 P680 - Hadoop Monitoring page is stuck	GA17817
GRD-56572	V10.6 SFTP mode not preserved after system reboot	GA17804
GRD-53994	grdapi run_clean_solr7_upgrade run on version 11.315	GA17763
GRD-56542	Query Report Builder - Failed to save query that includes field "App User Name"	GA17801
GRD-54938	Request detailed steps to store mysql client/server certificate	GA17781
GRD-54099	grdapi Process Doesn't Update the Flat Log Process Schedule Correctly	GA17787

GRD-54040	Double forward slash in /var/IBM/Guardium/TSM/guard_filetransfer_log || === IN logCatalog ====== filename = /var/tmp/archive//7	GA17627
GRD-54579	Cannot upload data to CUSTOM table via grdapi upload_custom_data: "ERR=2003 Could not complete the operation"	GA17735
GRD-56004	Possible Field not in 11.4 Report Test Result entity DETAIL_TEXT	GA17788
GRD-54588	Vulnerability Assessment SQL request for TEST IDs (656,657,658, 669 and 670)	GA17776
GRD-56806	S-TAP error: "guard: [TAG] - ERR: Problem in traversal"	
GRD-58952	Azure Data Stream "Red Status" "Namespace Unreachable" and "Unknown Issue, contact support" errors	GA18000
GRD-60343	Analyze Solr in Datamining must gather	N/A
GRD-58900	v11.4 Custom Table Builder - shows blank values for custom table fields of type varchar larger than 255	GA18024
GRD-62555	Authentication Logic Flaws with 205 - SQL OLEDB disabled (DisallowAdhocAccess registry key)	GA18027
GRD-61879	Compliance Monitoring creates too many records for a single Oracle OUA DB	GA17992
GRD-61656	Oracle Test "CONNECT_TIME is limited" does not have ability to add group exception	GA17973
GRD-62080	"Operation could not complete due to database error" after removing the “Group Builder” application in roles in 11.4	GA17986
GRD-60537	Unexpected status of chart while creating graph report based on Sniffer Buffer Usage Monitor.	GA18044
GRD-54635	Data Mart extraction is adding another backslash to the SQL Server user name when it included the domain name	GA17919
GRD-60733	NOT RECEIVING ALERTS OF TYPE="MAIL" FROM POLICY (TYPE="SYSLOG" are logged fine)	GA18021
GRD-62880	Standard menu options not available on Aggregation/Archive log - 11.4	GA18030
GRD-57807	VA Scan Failing but No Details Indicated (No Privileges With The Grant Option)	GA17911
GRD-60386	Vulnerability detected on CyberArk credential provider	GA17923
GRD-60327	V11.0 MySQL certificate extension request + extended support contract customer.	GA17954
GRD-59091	Running 'store certificate gim client console' with 'r' and 'a' option is not generating keystore for clients	GA17929
GRD-63526	11.4 FAMMONITOR continuously crashing and restarting	GA18054
GRD-59970	Is Solr Query a parameter that can be modified on RestAPI calls?	

GRD-55252	Failure to save "Distributed Report Configuration" due to a failure to modify data mart definition	GA17790
GRD-55058	Issue with continuously disconnecting latest STAPs on RHEL and Win platform	GA18072
GRD-60036	(Documentation) Need document of Pink S-TAP parameters for Win S-TAP V11.4	Doc Defect
GRD-62987	Auto discovery does not create all inspection engines when MS SQL Server instance has multiple ports, should not create 0-value port based inspection engines	GA18050
GRD-57272	Guardium Central Manager FileServer utility Not working.	GA17882
GRD-56917	Win S-TAP V11.3.0.131 process crash caused by internal dump buffer	GA17838
GRD-51561	Investigation Dashboard is not working from GBDI and Guardium Appliance	GA18068
GRD-61273	Guardium displays 3 backslash characters before double quotes when extracting Full SQL via rest API	GA17971
GRD-63014	Custom properties on data source definitions add to data sources does not work if done for more than 750 sources.	GA18080
GRD-62251	DB2 Exit generated "Error detaching from shmbox" in db2diag.log when db2start/db2stop	GA18047
GRD-52120	Unable to run ImpFrmQuery job due to db error	GA18057
GRD-55906	SNMP "Test Connection" Button throws "SNMP trap sink host is unreachable" However, ports are opened and alerts are reaching the SNMP server.	GA18063
GRD-63064	Can’t fully accept License without UI access – cant access UI accessmgr without License	GA18060
GRD-54338	Bug identified in Schedule for Distributed Reports improper	GA18059
GRD-59427	Incorrect message in the report about merge period for distributed reports	GA18056
GRD-62787	Guardium add user issue	GA18087
GRD-56069	v11.3 p325 unable to modify datasources for non admin or owners	GA17789
GRD-59957	Document review request - Oracle-specific guardctl parameters	Doc Defect
GRD-59956	Documentation check required - Running database entitlement reports	Doc Defect
GRD-56328	Current Alert value is higher than average threat activity	GA17875
GRD-63504	Add groups has Errors in the Database	
GRD-54518	Teradata Classification - Could not access column(s)	GA17756
GRD-56468	Datamart doesn't extract expected data if run covers multiple days	
GRD-59031	UTF-8 4-byte characters specified in the host variable of the SQL statement are garbled	GA17915
GRD-53594	Guardium - Reports duplicating API mapping	GA17775

GRD-58561	'NOT IN PERIOD' condition not working properly in query	Doc Defect
GRD-53062	v11.3 - grdapi register_oauth_client - need explanation for parameters	
GRD-63231	Expose PatchType in Installed Patches entity	
GRD-56405	Documentation - using wildcards within groups for Vulnerability Assessment	
GRD-58771	VA Test Deprecate - 2561 Oracle storage use privileges	
GRD-59581	Guardium appliances for OCI Government Cloud	
GRD-56385	Missing data on the discovery scenarios screen	GA17797
GRD-60145	Update third party health check control parameter and message	
GRD-62911	Add ADMINCONSOLE.txt to enterprise_load_balancer_issues must gather	
GRD-54928	Minor ELB enhancement	
GRD-58206	KTAP request 4.18.0-305.19.1.el8_4.x86_64 for STAP v11.4	
GRD-59405	After CM upgrade to v11.3.0.347 GUI not loading and many inserts/deletes on CHANGE_TRACKER_STAP_PROPERTIES waiting for lock	GA17950
GRD-59955	v11.4 Test 154 No Individual User Privileges	GA17952
GRD-57443	Errors during TSM config file import	GA17872
GRD-60947	CLI Command system scp-ssh-key-mode not working for data archive	GA17964
GRD-56782	Slowness on the discovery scenario	GA17941
GRD-60867	IGNORE SESSION rule action in SLP is missing	GA17970
GRD-58130	1st Installed Policy changed to "Default - Ignore Data Activity for Unknown Connections [template]" after applying log4j patch	GA17903
GRD-62058	Error in connection to Oracle Database using OUA causing production database outage	GA17978
GRD-54459	Guardium Collector outbound SSH	
GRD-59718	Bug in CLI and Online KB for command - store disable_sha1_passwords true	GA17943
GRD-60419	V11.4 Data Restore Failed to Import Archive File using SCP when there's backslash in scp user name	GA17939
GRD-54776	Extend expiration number when delete datasources with "grdapi delete_datasource_by_name"	GA17777
GRD-60848	Unable to restore Archive data with SFTP from Windows Server.	GA17969
GRD-61097	Guardium Appliance Discovery by CMDB without OS root Access	GA17962
GRD-55632	Pre-defined 'Groups Usage Report' doesn't list Groups used in Query with 'NOT LIKE GROUP' operator	GA17795
GRD-56769	Restore failed - Error: Table 'TURBINE.SRC_DB_SCHEMA_TABLES' doesn't exist	

GRD-57959	Windows Server Agent turns into sync state (the default HANDLE_COUNT_LIMIT is too small)	GA17977
GRD-58860	Guardium 11.4 stap agent is not letting windows smartcard login	
GRD-60342	KTAP request 4.14.35-2047.511.5.7.el7uek.x86_64 STAP v11.3	
GRD-57533	KTAP request for 5.4.0-90-generic STAP v11.4	
GRD-60533	KTAP request 5.3.18-150300.59.49-default s390x for STAP v11.4	
GRD-58722	K-TAP request for kernel 4.12.14-122.71-default on V11.3	
GRD-58720	KTAP request 4.12.14-122.74-default.X86_64 STAP v11.3	
GRD-58726	KTAP request for 4.18.0-193.28.1.el8_2.x86_64 on V11.3	
GRD-58723	KTAP request 4.12.14-122.60-default.x86_64 STAP V11.3	
GRD-58724	KTAP request 4.12.14-122.57-default.x86_64 STAP v11.3	
GRD-58719	KTAP request 4.12.14-122.46-default.x86_64 STAP v11.3	
GRD-59698	KTAP Request for kernel 3.10.0-693.el7.x86_64 for V11.2	
GRD-58725	KTAP request 4.12.14-122.103-default.x86_64 STAP v11.3	
GRD-57549	LDAPS users not able to authenticate via set guiuser command.	GA17900
GRD-60509	User Activity of Template modification does not get logged in GUARD_USER_ACTIVITY_AUDIT	GA18009
GRD-59674	Two fields with this same in name in one report entity (VA Tests)	GA17995
GRD-57545	Failure to complete installation of patch 11.0p404_CVE-2021-44228	GA17819
GRD-58844	"Pink STAP" guard_tap.ini params missing in 11.4 Doc.	
GRD-59273	Correlation Alert configuration: unable to add email addresses with special character for Alert Receiver of type email	GA17904
GRD-55675	Access denied for user 'root'@'localhost' at 01:50 am everyday	GA17785
GRD-50119	6 sessions (1 second apart) are reported when STAP Verification is executed	GA17827
GRD-56827	Errors observing in every 5 minutes event logs (sending file to gimserver failed)	GA17902
GRD-57544	Oracle Unified Auditing debug messages shown in STAP Event log unexpectedly	GA17867
GRD-58428	Data restore failure	GA17916
GRD-55889	STAP OUA Error: could not open .SQLC_PASSWORD after upgrade to 11.3.0.0_r110195 in GIM env	GA17796
GRD-58140	Any length limit in setting firewall_force_unwatch parameter?	GA17879
GRD-55259	S-TAP and GIM Dashboard displaying wrong information for STAPs	GA17823
GRD-55489	V11.3 Patch 325 || "Test Exceptions" Report sort order issue	GA17762
GRD-54929	Auto shut off debug in Cli command "support store debug on"	

GRD-49915	Mail Certificate stops working after a certain time.	GA17864
GRD-56758	V11.3 || "Test Detail Exceptions" || The field cannot contain non-BMP characters	GA17810
GRD-57324	In GUI Alerter page, the "Test Connection" of SMTP failed to send email even when other alert emails could be successfully sent	GA17866
GRD-57267	Error opening /opt/IBM/Guardium/log/certificate_expired_warning when show certificate warn_expired run	GA17833
GRD-60517	Parameter to Encrypt Functionality dropdown is missing	GA17957
GRD-56467	Datamart doesn't extract expected data after schedule pause	GA17897
GRD-59431	Grammatical errors in VA TestID 128 description	GA17895
GRD-54636	"support reset-managed-cli" exits if any one unit fails	GA17737
GRD-54804	Active Audit Process deleted	GA17739
GRD-60074	Enhance datamining must gather with additional ATA info	
GRD-57306	Guardium VA Security Assessment Builder Roles error	GA17883
GRD-58226	v11.4 ReOrder Does Not Work As Expected || Audit Task list in the Audit process	
GRD-53566	Data source import using GRD API commands does not validate mandatory fields (Eg. Database in PostgreSQL)	
GRD-55273	Format issue for CSR creation	GA17815
GRD-55736	GUI Certificate warning(6months) spams in alert popup window	GA17764
GRD-56240	Group having tuple members does NOT appear in Groups Usage Report	GA17793
GRD-49960	Do we support VM level live backup?	GA17765
GRD-56488	"Allow" rule action cannot be selected when GUI page v11.4 only	GA17807
GRD-54634	'grdapi create_ad_hoc_audit_and_run_with_name' failed to find ServiceNow user	GA17734
GRD-52187	SFTP protocol could not send test file in GUI backup	GA17794
GRD-59423	KTAP 5.4.0-99-generic.#112-Ubuntu x86_64 Ubuntu STAP v11.4	
GRD-54927	IBM Guardium Installation Manager installation fails in SE Linux but reports successfully	GA17805
GRD-54993	Guardium VA external References (CIS)	GA17885
GRD-59286	Postgres VA - Test category	GA17893
GRD-56498	Typo in GIM Events List error	

Resources

IBM Security Guardium documentation 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 11.5
https://www.ibm.com/support/pages/node/6613461

Appliance technical requirements 11.5
https://www.ibm.com/support/pages/node/6599135

IBM Security Learning Academy
securitylearningacademy.com

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