Release Notes

==========

Product:	IBM Security Guardium
Release version:	Guardium v11.2
Completion date:	12 June 2020

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 v11.2

Passport Advantage:

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 EST) or by email paonline@us.ibm.com.

Fix Central:

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 v11.2

Guardium V11.2 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.

Installation must be across all the appliances such as the central manager, aggregators, and collectors.

Upgrading to Guardium v11.2

You can upgrade to Guardium v11.2 from any Guardium system that is running on v10.0p11001 or 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.

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 v11.2 GPU. If the Health Check patch isn't installed as recommended, the v11.2 installation fails with this error message: Patch Installation Failed - Latest patch 11.0p9997 required.

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.

Backup, 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 is not fully functional and only a limited set of commands are available.

> Note:
>
> Do not 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.

Previously installed patches

When you upgrade to Guardium v11.x, the v10x patches that were previously installed are no longer visible in the "Installed Patches" screen in the GUI.

Installing or upgrading to v11.2 S-TAP

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

New Features and Enhancements

UI-Based Enhancements

Active Threat Analytics

Case Analysis drill down page. Case Analysis has three tabs for a deep dive into the context and details of each case: Source details and history, Case details, and Exploration. To open the Case Analysis page, click a case number in the Active Threat Analytics page. For more information, see Case Analysis page.

Failed logins case type: Active Threat Analytics now identifies threats that are posed by failed logins. For more information, see Failed logins.

Use policy rules to create a case type. You can add a threshold to a violation rule that has a severity of high in the rule definition, and the rule action is alert per match. If the threshold is exceeded in any 1 hour, an Active Threat Analytics case is created. For more information, see Creating threat categories from policy rules.

Advanced session-level policies UI

Install advanced session-level policy scripts from the Guardium UI. Advanced session level policies allow you to validate incoming packets and define actions based on the result, for example sending the request back to the S-TAP, transforming runtime data for the analyzer, or preparing the data for the parser or logger. For more information, see Create and install advanced session-level policies from the UI.

Alert Builder and Policy Builder support non-Guardium emails as receivers

In previous releases, only Guardium users were permitted as email receivers. Now you can define external email addresses. For more information, see Correlation Alerts and Alerting rule actions.

Asset reconciliation

Part of the Compliance Monitoring tools, asset reconciliation compares a user-provided list of databases with the databases that are known to a Guardium system. This offers a quick way to identify old or unknown databases and to verify that Guardium provides the desired coverage. For more information, see Reconcile database inventory.

Audit process builder

In the audit process builder, use the "Sync QUERY_FROM_DATE to the previous execution date" checkbox to prevent missing or duplicate data in scheduled audit processes.
Note:

- The audit process must run at least once before the setting takes effect.
- If an audit process did not run recently, disable the setting to avoid an excessive amount of data in the report.

Audit process to-do list

You can now filter the to-do list by selecting the user whose to-do list you want to open. You can do this by using the drop-down menu or by searching users. You can also filter by process name or by execution start and end date, and then clicking search.

Audit processes and tasks open in pop-up browsers, so you can open and compare multiple results simultaneously without exporting them to CSV.

Backup central manager can be defined and managed with API
Several new commands provide control over the backup central manager configuration. For more information, see the central manager APIs in Central management APIs.

CyberArk
The CyberArk SDK is no longer packaged with the Guardium® system. To install or upgrade CyberArk, download the CyberArk SDK patch from the IBM Fix Central website. For more information, see Managing datasource credentials with CyberArk.

Data Mart report page improvements
The Data Mart page now lists all data marts in the system, their type (file or table), the related query/report, and the domain. You can sort and filter data marts, and you can use the Actions menu to view the related queries, the extraction logs, and the configurations.

Database discovered instances rules
You can now configure the schedule for automatically creating inspection engines based on specified rules. In addition, the Discovered Instances Rules Report custom report and Discovered Instances Rules Alert predefined alert are now available for reporting on discovered instances. For more information, see Database discovered instances rules.

Datasources
Before v11.2, only 10 datasource connections could be tested at a time. In v11.2, you can test the connection for any number of datasources simultaneously in the Datasource Definitions page. You can also view the last test date, the error summary for the connection, if any, and the connection status for all Guardium systems in your environment that were last tested.

SSL authentication is added to MySQL and Sybase datasources.

For datasources that support SSL mutual authentication, upload a certificate in PEM (Privacy Enhanced Mail) format. If there is no PEM certificate available, Guardium connects by using the tomcat certificate.

You can now update the connection string `IFX_USE_STRENC=true` for all Informix Datasources by using a CLI command. For more information, see Parameters to configure an Informix Datasource.

When DNS settings are changed, Guardium datasources automatically connect to the new IP address after 60 seconds. A GUI restart is no longer necessary.

Deployment health views
Improvements to the deployment health views include advanced filtering support on the deployment health table and topology, the addition of a K-TAP health metric, a new S-TAP and GIM graphical dashboard, support for aliases, and improved performance offering near real-time status information. For more information, see Deployment health views.

Enterprise load balancing: additional failover groups
You can specify multiple failover groups and give each one a priority. When the load balancer needs to relocate an S-TAP®, it searches for a managed unit in the top priority group. If it does not find one, it continues in the next priority group, and so on. For more information, see Enterprise load balancing.

External ticketing support for audit processes
You can configure audit processes to generate external tickets to track incidents, problems, and tasks discovered by Guardium. For more information, see Configure an external ticketing system.

Hadoop monitoring with Ranger integration supports HTTPS connection with Ambari
For more information, see Linux-UNIX: Configure Guardium and Ranger communication, add_ranger_config, update_ranger_config.

LDAP import into custom tables
Enrich Guardium tables with LDAP data by using an LDAP server as a datasource. Retrieve and configure LDAP attributes that can be used to customize reports. For more information, see Configure an LDAP datasource and import data.

Multi-factor (two-factor) authentication for Guardium GUI and CLI
To provide an extra layer of security for Guardium user accounts, you can enable multi-factor authentication with the DUO authentication engine. For more information, see Portal configuration.

Oracle Unified Audit Activity new report
This new report presents the server, client, and database details for the logged Oracle traffic.

Outliers detection clustering
User clustering divides the system's users into clusters based on their activity. It compares the activity of the users in a group as part of the outliers scoring process. Analyzing groups of users increases the accuracy of the results and decreases the number of false positives. For more information, see Outliers detection clustering.

Outliers detection OS user
For systems that need tracking by OS user, you can switch outliers detection (on the central manager level) to track activity by OS user. For more information, see Switching DB and OS users.

Outlier mining
Outlier mining alerts on process failure
The new predefined alert, Outlier Analysis Failure, sends notifications if the outlier mining process fails. For more information, see Predefined alerts.

Query rewrite: handling large SQL statements from an MSSQL Server database
Query rewrite does not mask the data when the overwritten SQL is larger than the negotiated packet size. In these cases, Guardium issues an alert. The alert fires once per session when the query returns more than the negotiated packet size. Use the new predefined alert QWR Exceptions Alert to be notified of this situation. For more information, see Handling large SQL statements from an MSSQL Server database.

Remote syslog test
You can check the Guardium communication with the remote syslog. For more information, see remote syslog.

Session-level policy tuple parameters
Combine several session-level policy parameters into a single parameter that is known as a tuple. Compared to using multiple single parameters, where each parameter matches any value in a group,

tuple parameters allow finer control by defining only specific combinations of values to match. For more information, see Create tuple parameters for session-level policies.

Smart card Authentication
If you import Guardium user definitions from an LDAP server, you can continue to import these definitions when you use the smart card authentication feature.
The regular expression (regex) values for smart card authentication in the Guardium Portal page can be updated by using the API modify_guard_param. For more information, see Smart card modifiable parameter.

Smart card authentication supports OCSP validation. For more information, see Guardium UI login using a Smart card.

S-TAP and GIM dashboard
The new S-TAP and GIM dashboard provides graphical charts displaying health and deployment information. The dashboard makes it easy to see the health of S-TAPs and identify both are system-wide and one-off problems. For more information, see S-TAP and GIM dashboard.

Threat Detection Analytics supports MSSQL databases
For more information, see Threat Detection Analytics.

External S-TAP

You can now configure External S-TAPs to automatically generate certificate signing requests (CSRs). By storing an intermediate certificate on a Guardium central manager or collector, Guardium can use that certificate to automatically generate certificates for every External S-TAP container.

File Activity

File Activity Monitoring (FAM) for network-attached storage (NAS) and SharePoint
Use the comprehensive criteria and rule actions of Data Activity monitoring (DAM) policy to monitor FAM for NAS and SharePoint in deeper granularity. Create alerts on a subset of users, audit all or a set of users, and optionally ignore a set of users or operations. For more information, see Creating a DAM access policy to monitor files on NAS and SharePoint.

In the FAM installer, you can now enter a list of Guardium hostnames or IP addresses. If there is a failover, the FAM agent connects to the next appliance on the list.

In the FAM configuration utility, you can now enter a list of semicolon or comma-separated appliance hostnames or IP addresses. The connection to all appliances can be tested simultaneously.

If you have multiple network interfaces, the IP version of the local host must match the IP version of the Guardium system.

The path prefix for object names in the NAS file activity report is no longer included by default. You can now manually include the path prefix, if required.

FAM now supports multiple services that are pointed to the same monitored host.

File Discovery, Entitlement, and Classification (FDEC) for NAS and SharePoint
In the FDEC scan configuration utility, you can now enter a list of Guardium appliances and test the connection of each appliance. If there is a failover, the FDEC agent connects to the next appliance on the list.

You can now select, add, or remove site collections to the scan configuration. You can also create a farm-wide scan by not specifying a scan path.

View the status and progress of a scan by creating a FAM progress report on the dashboard.

FamMonitor installation on Windows
The FamMonitor installation wizard has a new field: Appliance Address(es). Use it to add more Guardium® hostnames or IP addresses. If there is a failover, the FAM agent attempts to connect to the next appliance on the list. See Install the FamMonitor installation package with the wizard.

FAM Policy Builder supports non-Guardium emails as receivers
In previous releases, only Guardium users were permitted as email receivers. Now you can define external email addresses. For more information, see Using rules for file activity policies.

Guardium Installation Manager (GIM)

GIM bundle and module lists
The Upload Modules page now has full details about the uploaded modules. For more information, see Uploading and installing GIM modules

The new Centralized Module View lists all GIM bundles present on the entire system. For more information, see Centralized Module View.

Vulnerability assessment (VA)

VA users can run VA assessments on SQL DB Azure datasources. For parameters to configure an SQL DB Azure datasource on your Guardium system, see SQL DB Azure.

When a DPS (Database Protection Subscription Service) update file is uploaded, Guardium now validates the version of the file. View the upgrade history and the status of the DPS upload by using the CLI command `show dps`.

The Test Results entity in the Security Assessment Result domain now displays the start and end time for all VA tests.

Guardium now includes a mechanism to recognize Db2 special fixes for CVE (Common Vulnerability and Exposure) tests. If applicable, the recommendation to patch the vulnerability is displayed in the results for the security assessment.

You can now run a VA scan with the latest SQL Server 2016 STIG benchmark.

VA now provides recommendations that are related to Db2 special fixes in the UI.

There are 16 new query-based tests and 1 new CAS-based test for SAP HANA.

Before v11.2, if a halt was caused by a test that takes over 30 minutes to execute, it was terminated by the nanny OS process. Users were required to rerun the assessment. In v11.2, VA resumes the scan, skips the test, and continues to the next test in the same datasource. The test that was skipped is assigned a score and error message. However, if the halt is caused by a multi-threaded assessment, or by a reboot of the OS, GUI, or classifier, VA resumes the scan without skipping the test.

You can now add and update roles to datasources by adding a column called “Role” to the CSV file when you use the upload CSV feature. You can also add multiple roles for each datasource separated by a semicolon.

Other enhancements

Windows S-TAP software is more efficient with no firewall timeout issues. The SQL command latency is significantly reduced.

The ANTLR3 parser supports Sybase versions up to V16.0.

In an MSSQL custom table upload, the datasource now includes results from all accessible databases when there is no database specified. The results are aggregated on each accessible database.

The IBM Spectrum Protect client version on the Guardium Appliance was upgraded from v8.1.7 to v8.1.9.

You can now purge must_gather files by using the command
`store must_gather_file_max_age <number of days>`
For more information, see Purging must_gather files.

You can now identify when the encryption ciphers that are used by the Guardium system are changed or updated. For more information see, Cipher suites.

The following new and updated variables are available for the alert message template:

- %%AnalyzedClientIp (new)
- %%BindVarVal (new, available in v10.6 and later releases)
- %%DBName and %%DBProtocolVersion are now populated for AS400 Db2 iSeries
- %%ImsPartArea (new, available in v10.6 and later releases)
- %%SenderIP (new, available in v10.6 and later releases)
- %%succeeded is now populated for Db2 for z/OS and Hadoop traffic.

Known limitations and workarounds

Guardium component	Issue key	Summary
Active Threat Analytics	GRD-41965	The active threat analytics page does not work as expected in the Internet Explorer browser. **Workaround:** Use a different browser.
	GRD-42079	Cases that were created before upgrading to v11.2 are missing some details in the exploration tab. The "not connected" message can be ignored. **Workaround:** Resolution is available in an upcoming patch release.
	GRD-41060 GRD-41061	The DB protocol and the DB name are presented incorrectly for MS-SQL.
Alert builder	GRD-41881	An error occurs when the Alert Builder is launched after distributing updated utilization threshold from central manager to the managed unit. **Workaround:** Restart the GUI after changing utilization thresholds. Resolution is planned in an upcoming patch release.
Archive/backup	GRD-40235	IBM Cloud (formerly Softlayer) configuration is not supported for system backup.
Backup CM	GRD-41993	On a backup central manager, the backup process occasionally stops running after first sync backup completed. **Workaround:** Run the “show local_cm_sync_file” command on the backup central manager’s server. If the backup process is not verified, and the second backup and timestamp is not updated as expected, reinitiate the backup central manager process from the primary central manager.
	GRD-41494	When you switch to a backup central manager, the outlier user mode is not retained. **Workaround:** If the outlier user mode is OS: after switching to the backup CM, set the outlier user mode to OS again, using grdapi set_outliers_user_detection_mode mode=OS
Deployment health	GRD-42076	If you hover on an S-TAP with red K-TAP status, the tooltip continues to display the message “KTAP not loaded” for all S-TAPs, even if it points to an S-TAP with green or blue K-TAP status. **Workaround:** Refresh the browser.
Deployment Topology	GRD-41167	Verification status of the inspection engine is not accurate. A “passed” status can mean: (a) verification is scheduled and it passed successfully or

		(b) verification is not scheduled, and the status is not verified. **Workaround:** Resolution is planned in an upcoming patch release.
File Activity policies for NAS	GRD-40540	When FAM for NAS is upgraded to v11.2 or later, the existing policies that are installed on v11.0 or v11.1 do not work due to a change in the format of the datasource name. In Guardium v11.2 and later, the NAS datasources appear in the following format: <The name of the server where the agent is installed>:<the monitored host>_<type of NAS device>:FAM-NAS. **Workaround:** Update the name of the NAS datasource, save, and reinstall the policy.
IPv6	GRD-41148	IBM Cloud Object Storage (Formerly Cleversafe) is not supported in an IPV6 environment.
	GRD-39251	When managed units are registered to the central manager and then patched to v11.2, the IP mode of each managed unit is not displayed. **Workaround:** Click the refresh button to see the IP mode.
	GRD-41767	When the central manager is not on the same internet protocol as a Windows S-TAP, then the S-TAP diagnostics are not communicated to the central manager.
	GRD-41774	When you upgrade to v11.2, risky users are not generated in the IPv6 environment.
	GRD-40700	Query Rewrite Operations do not work as expected in an IPv6 environment **Workaround:** Resolution available in an upcoming sniffer patch.
Network	GRD-41747	If the appliance is a central manager, both the primary and secondary IP address must resolve to the same hostname that is set for the appliance. Otherwise, a network failure might occur in the communication between the central manager and managed unit.
Outliers detection	GRD-42136	Outlier data may not be displayed sometimes even though outliers are generated. **Workaround:** Restart the GUI.
Policy Builder	GRD-41513	If some fields are empty when you add and save a member to the tuple, the values appear out of order when you edit the tuple. **Workaround:** Delete and add the member again to the tuple.
	GRD-41947	When you install a policy after an import definition, the policy may not get installed. **Workaround:** If there are issues when installing policy from the Policy Installation page, then user log out and log in again and try to install policy or install policy from Policy Builder for Data page.

Risk Spotter	GRD-29475	“User Risk Indicator” does not work in Internet Explorer. **Workaround:** Use a different browser.
	GRD-36584	Risk spotter Risk details modal does not open in Internet Explorer. **Workaround:** Use a different browser.
Smart Assistant	GRD-35587	Compliance policies GDPR and CCPA for z/OS cannot be installed from Smart Assistant. **Workaround:** Install the ‘Default - Ignore Data Activity for Unknown Connections [template]' before restarting compliance monitoring. To do this, you must clone the policy before installing it. The name of the cloned policy must include 'Default - Ignore Data Activity for Unknown Connections [template]' to install and override the policy. Otherwise it may result in failure of policy installation.
Sniffer	GRD-39699	ANALYZED_CLIENT is not updated for Oracle SSL encryption type.
Upgrading in a mixed environment	GRD-41525	When the central manager is upgraded to v11.2 and managed units operate on v10.6, Guardium components such as Active Threat Analytics, Risk Spotter, Data Protection Dashboard, and Enterprise Search may not work as expected. **Workaround:** Upgrade all managed units to v11.2.
	GRD-41341	When upgrading to v11.2, and one or more of your Guardium systems are running a v11.1 version prior to v11.0p115, you might experience unusual behavior in Active Threat Analytics, Enterprise Search, RiskSpotter and Data Protection Dashboard until all of the units are upgraded to V11.2. **Workarounds:** • When Guardium is upgraded to v11.2, upgrade all managed units to v11.2 (or) • Upgrade all units to V11.0p115 before upgrading to V11.2
z/OS	GRD-42069	IMS Definitions cannot be updated from Guardium user interface. **Workaround:** Create an IMS definition rather than update the existing one.

Bug Fixes

Issue key	Summary	APAR
GRD-24491	V10.5 || CUSTOM TABLE UPLOAD from GUI shows many insert and actual table content is just five rows.	GA16649, GA16888
GRD-34084	Pipe sign character is not permitted in username field	GA16852
GRD-33092	show local_cm_sync_file throws Use of uninitialized value $name[6] error	GA16872
GRD-32374	Add a section to the must_gather(s) to show MIN(TIMESTAMP)	GA16873
GRD-35259	HTTP500 error on Support Information Gathering Results	GA16885
GRD-36442	STAP does not failover to secodary collector	GA16929
GRD-37803	SAP sybase ASE instance terminates with signal 11 when ATAP is activated.	GA16933
GRD-39531	Issue with STAP v11.1 r107670 support for Encryption in Transit for Sybase ASE 16 installations	GA16933
GRD-40289	Patch Distribution failed with "Patch file scp failed:" after Primary CM applied V11.1 P105	GA16934
GRD-39657	v10.6/v11 Unable to save the query when "Count" and "Add condition group/parentheses" are used	GA16936
GRD-34346	Request to change file permissions	GA16942
GRD-35211	"support must_gather system_db_info" returns "Note: This output shows SysV services only" etc- not needed and confuses customers.	GA16965
GRD-35358	cli "support check tables" does not filter out messages like "...is deprecated and will be removed ....etc" and "....Please use native partitioning instead." - confusing for customer who can;t do anything anyway	GA16966
GRD-34065	Syslog to Arcsight is not capturing SQL statements correctly if there are multiple "=" symbols	GA16968
GRD-36138	Tuple group with values containing plus (+) sign can't be used in policy	GA16986
GRD-36088	Values in a tuple group entries don't work with a + (plus) sign	GA16987
GRD-36422	2611 - Oracle Database Vault is installed	GA16996
GRD-35484	Datamart Error - Malformed query built by datamart process, not a customer creation	GA16997
GRD-35734	GIM Setup by Client Filtering not clearing after patch p630	GA16998
GRD-36588	CLONE - Doc: Missing description In 'S-TAP/Z files domain'	GA16999
GRD-36731	Upload Datasource Definition error: Unknown column name	GA17003
GRD-36286	Audit process runs in TURBINE DB, that has hundreds of partitions and doesn't use 2 stage	GA17007
GRD-33090	v11 GUI TLS Vulnerability Improvements	GA17015

GRD-36393	Rule to ignore STAP session is getting triggered incorrectly	GA17016
GRD-32035	GIM/STAP Install places "local0.err,kern.debug /var/log/ktap.log" line in the /etc/syslog.conf on AIX servers	GA17019
GRD-36208	V10 & V11 || SMART CARD Authentication Allows Login via GUI after INACTIVITY	GA17021
GRD-36952	make "Purge" a separate "Activity Type" in the main Aggregation/Archive Log report - this would make the overall Aggregation/Archive Log report much better to view from GUI etc	GA17023
GRD-32965	DB User value is being cut off from syslog alert	GA17024
GRD-37587	V11.1 || LOGIN ID displayed incorrectly in report on GUI	GA17027
GRD-36771	cli commands return incorrect DATABASE eg - "du: cannot access `/var/IBM/Guardium/data/mysql/GDMS/AGG_RELEVANT_DAYS*': No such file or directory"	GA17028
GRD-37401	VA TEST_ID=2168 does not check for Db2 11 and Db2 12 sample databases	GA17030
GRD-36993	V11.1 || Missing HSTS Headers	GA17032
GRD-36944	V11.1 || grdapi grant_role commands not working properly for BULK execution	GA17033
GRD-37019	DBMS source code encoding or encryption requires encryption or encoding of source code	GA17035
GRD-36007	Repeated "DecryptMessage failed" with "The context has expired and can no longer be used" for Windows S-TAP 10.6.0.193	GA17036
GRD-37140	SQL Verb comes up incorrect in Splunk syslog	GA17038
GRD-37290	Win S-TAP install via GIM sets CORRELATION_TIMEOUT=5, which should be 300	GA17042
GRD-37361	Not able to clone Datamart Extraction Log report	GA17043
GRD-33941	Guardium triggered server reboot STAP-10.6.0.2_r106401 with Trendimicro installed	GA17046
GRD-37614	Netwok Must gather is throwing the follwoing Error in V11.1 Undefined subroutine &main::show_net_resolver_all called at /opt/IBM/Guardium/cli/subs_supp_must_gather.pl line 1877.	GA17047
GRD-37397	* character not handled correctly in health check duplicate query check	GA17051
GRD-37303	The Disk and Database Health Analyzer feature sends Alerts to Guardium inactive/disabled admin users	GA17053
GRD-37615	in v11.1 cli commands "store network interface map" and "store network interface remap" is giving errors.	GA17054
GRD-37765	v11.1 || Restore Backup Doesn't properly handle version check between GPU and bundle	GA17055

GRD-37369	V11.1 || GUI Issue || Customer Uploads || "Upload CSV to Create/Update Datasources "	GA17056
GRD-36263	Error while saving the Classification job : The following suggested jobs are not set as a runnable jobs. Therefore, are not going to be executed immediately when AuditTriggerxxxxxxx is fired	GA17060
GRD-32929	Discovery is not finding Oracle instance on Solaris	GA17068
GRD-37479	"Object / Field group In group" Policy rule fails to log MS SQL SERVER "SET" and "DECLARE" statements , however it does log them when the rule does not exist	GA17070
GRD-37539	Delete running without limit in GUI archive/export purge	GA17071
GRD-37613	cli command "store network interface inventory" is missing!	GA17072
GRD-37746	Windows-STAP-V10.6.0.177 return code 1 on success?	GA17077
GRD-37470	Request changes to Unified Auditing and standard Auditing Tests	GA17086
GRD-37876	Missing 'HELP SESSION' in Teradata traffic collection when 'S-TAP TERMINATE' policy action configured	GA17096
GRD-37927	Need a 'cli' command to check an ethernet port status on the physical appliance	GA17098
GRD-35342	Restoring appliance from configuration backup does not retain deprecated TLS 1.2 disabled	GA17102
GRD-37834	GIM 10.5 client certificate alerts after installing on CM patch 100	GA17104
GRD-38245	PSIRT 210352: We connect to solr dashboard on port 8983	GA17112
GRD-36967	Sensitive data in long SQL statements is not always masked	GA17114
GRD-37943	snmpwalk causes timeout on Guardium snmpd V11	GA17115
GRD-38439	Teradata EXIT node not sending traffic to collector	GA17116
GRD-38400	"Query SQL Statement Invalid or Not defined" when creating distributed report	GA17118
GRD-38627	Cassandra integration does not allow use of multiple custom query handlers	GA17119
GRD-38279	Guardium CM upgrade from 10.6 p635 to v11 failed. GUARDIUM_V11_UPGRADE_PHASEMSG:4.7:FAIL:Failed running mysql_upgrade_meta_data.sql	GA17121
GRD-37980	Report "Primary Guardium Host Change Log" has the "Guardium Primary Host" keeps changing when STAP load balancing=1 used	GA17122
GRD-38419	guard_gsvr.service has executable permission on RHEL7	GA17123
GRD-37302	Upgrading stap from older versions to 10.1.4 on AIX	GA17127
GRD-38254	MariaDB Inspection engines are not being automatically generated on running Guardium installation shell scripts	GA17129
GRD-38449	How to install Windows GIM client without using SSL (i.e. GIM_USE_SSL=0)?	GA17130

GRD-37079	Custom bundle STAP failed to upload	GA17131
GRD-38590	V11.1 || LDAP User Import disables the built-in users	GA17132
GRD-38870	tusc process triggered by guard_diag was not terminated because of a wrong pid	GA17134
GRD-38486	'zdiag' command to collect SLON and TCPDUMP for z/OS traffic functionality failure	GA17135
GRD-38252	v11.1 Data Import from IP doesn't work if DNS-Resolver is not set	GA17137
GRD-36743	GUI is not responsive infrequently on managed unit of v11 (non-English env)	GA17138
GRD-38739	Network Must Gather runs indefinitely post V11.1 + workaround	GA17139
GRD-37235	CEF events, logged in syslog with additional space, are not parsable from ArcSight	GA17140
GRD-39073	create_computed_attribute throws ERR=2410 when using GBDI related entity	GA17141
GRD-33215	Enabling SmartCard authentication breaks LDAP User Import	GA17144
GRD-39244	v11.1 VA - SQL Server must prevent unauthorized info transfer	GA17145
GRD-37620	GIM/STAP Directory Ownership Changed where "STAP_RUN_AS_ROOT=0" After Reboot of Server	GA17149
GRD-37723	v10.6 CM was down due to disk full (/var 100% used) most of which is used by kafka	GA17150
GRD-39318	Archive Data Restore Fails in v11.1 with an error "<Port>:Exit value = 1"	GA17152
GRD-39200	V11.1 Q1 2020 DPS MS SQL Missing Permissions	GA17156
GRD-36994	V11.1 || CACHEABLE SSL pages found	GA17157
GRD-38666	"Designate Backup CM" is failing in the MS Azure cloud environment	GA17158
GRD-39217	Missing SCP port from the output of grdapi get_datamart_info	GA17160
GRD-32175	Disabling weak cipher CBC_SHA on the TLSV1.2	GA17163
GRD-39410	v11.1 Expired Test_2454 - Check Parameter LOCAL_LISTENER Setting	GA17165
GRD-37757	security sia-db2-2019.10-1 and security siadb2-2018.10-1 appearing after UI58950	GA17166
GRD-37639	Audit job when runs from the 'Audit Builder' keeps failing	GA17170
GRD-37722	Import of Policy is failing	GA17171
GRD-34030	Existing report is not picking up newly added REGEXP condition	GA17172
GRD-38219	Cleversafe configuration no longer works in v11	GA17173
GRD-39445	Orphans cleanup fails for some days, on aggregators that are used as backup appliances, restores done on them.	GA17174

GRD-39670	FAM on Windows drops policies because it cannot access user information (Access Denied)	GA17175
GRD-39569	Q1 2020 DPS has test with grammatical error	GA17176
GRD-36184	Mongodb restarts due to memory deallocation by Guardium STAP	GA17177
GRD-39149	Check box disappears after editing Classification rule under the discover sensitive data / discovery scenarios	GA17178
GRD-39404	v11.1 Failed to set secondary IP address and reason: invalid interface name docker0	GA17179
GRD-39599	Network Role mismatch after upgrading from v10.6 to v11.1	GA17179
GRD-38313	Upgrade to v11.1 disabled existing LDAP users	GA17182
GRD-37304	Sniffer restarts frequently by SEGV signal because of size mismatch in the LRU internal two containers (list and map)	GA17183
GRD-40077	The VA test "SSL FIPS Mode Enabled" is failing even though this is incorrect	GA17189
GRD-39776	Local accounts get incorrect password error for set guiuser after v11 upgrade	GA17191
GRD-40259	VA Scans Halting due to Table Lock	GA17192
GRD-38981	Certificate chain failure with CleverSafe after upgrading Appliance from 10.5 to 11.1	GA17193
GRD-39434	All network interfaces default to BRIDGED causing spanning tree issues	GA17194
GRD-40579	Unit network.service entered failed state [release 11.1.0_r107671] system x3550 M5	GA17194
GRD-40440	Displaying "Unit guard_utap.service entered failed state" when running "systemctl stop"	GA17195
GRD-40355	MongoDB datasources for v11.1 are not accepting special characters (@ or :) on password	GA17196
GRD-38275	Test connection" returns "snmp trap sink host is unreachable.	GA17206
GRD-39182	API client registration don't have a way to know what has been registered	GA17207
GRD-38387	CCB - Problem restoring data from AWS	GA17209
GRD-34825	FAM installation failing with CIS hardening	GA17211
GRD-39352	docker0 interface caused store net resolver not updating /etc/resolv.conf file with DNS info.	GA17212
GRD-40367	LDAP Group import doesn't import anything if using LDAP Server's hostname instead of ip address	GA17216
GRD-40468	S-TAP on standby AIX lpar flipping Yellow-Green after HA Database Failover on AIX	GA17220
GRD-37371	High 'MySQL memory usage' on almost all Collectors even though traffic collection is light	GA17221

GRD-40361	Network is unreachable - after v11p105 and p4005 install	GA17222
GRD-41204	Alert for ATAP enabled DB executable override scenario	GA17224
GRD-40898	S-TAP v11.1 installation using GIM fails with 'Unable to determine OS version'	GA17225
GRD-40995	S-TAP 11.0.0.2_r108051 replaces tap_ip to host FQDN instead of set alias FQDN	GA17226
GRD-38546	11.1 Linux STAP fails goes inactive in collector using hostname	GA17228
GRD-17427	DNS resolution is cached and doesn't get refreshed in UI	GA17229
GRD-41132	java.lang.NumberFormatException on Guardium v11.1	GA17231
GRD-41236	Unnecessary popup for Classification run in case of CyberArk integration	GA17233
GRD-41374	ELB not deleting Red Windows STAPs from original MU upon failover	GA17236
GRD-40906	Missing doc on snif cache related CLI commands in KC	GA17237
GRD-41379	Issue while installing S-Tap on AIX Db2 system with db2exit.	GA17238
GRD-39646	Datasource caching IP causes connection failure in cloud	GA17239
GRD-41079	RFE: Ability to bulk update connection strings for Informix Datasources	GA17240
GRD-41371	v11 RH7 upgrade failure -guard_ktap_loader: Update failed: cannot get old khash content	GA17241
GRD-29991	V10.6 || Smart Card and Cert revocation status (via OCSP or CRL download)	
GRD-41718	Oracle Exadata DB server restarted after following the work around provided in the technote (1170778)	
GRD-41643	Guardium unable to collect DB activity from Cloudera Navigator via Kafka	
GRD-41673	FULL_SQL for SESSION from SOURCE_PROGRAM: ORACLE 64-Bit Client are not captured	
GRD-41119	The SSH Client IP is not shown in the UID chain for FAM entries	
GRD-35341	'Download as pdf' results in empty report for all reports. 'Full printable report' displays ok.	
GRD-37480	EXIT traffic is not compressed when STAP compression is enabled, or "long" is 8 bytes on the system.	
GRD-38861	Inconsistent logging of failed login attempts- Informix Exit	
GRD-39016	Exclude networks is not working for Informix Exit- SUSE 11,12	
GRD-37500	Bundle STAP does not allow to skip discovery when run via shell	
GRD-39035	Database discovered instances rules documentation	
GRD-34168	DB Instance discovery not working for customer's Oracle VCS cluster configuration	
GRD-38146	Support Ktap for 4.18.0-147.3.1.el8_1.x86_64	

GRD-41230	Improve documentation for UID chain	
GRD-34589	Add a grdapi command to remove invalid stap	
GRD-41280	GIM failover documentation	
GRD-39792	add limit for the number of verbs displayed in the alert message	
GRD-41369	Need to clarify private_tap_ip documentation	
GRD-40363	upgrade STAP through GIM will not link the libraries	
GRD-37596	WAIT_FOR_DB_EXEC parameter behavior needs to be changed to allow more frequent stat() of DB process name	
GRD-36648	Consolidated_installer script not filtering out invalid ip 0.0.0.0	
GRD-39393	Detect AVG_EXECUTION_TIME column in AGG_ANALYTIC_INPUT table in dataming must gather	
GRD-34261	Need to document Kernel signing - Secure boot	
GRD-37592	Documentation for WAIT_FOR_DB_EXEC parameter is incorrect	
GRD-35868	Restore specific certificates from backup or default	
GRD-34538	Add /var/IBM/Guardium/log/cmDataUpload.log to mastGather related to custom Uploads and UnitUtilization.	
GRD-37031	ATAP documentation incorrect regarding authorize db_user for GIM based installs	
GRD-35420	Add CRON_EXPRESSION to must gather schedule outputs	
GRD-34156	Enhance deployment must gather	
GRD-37724	system_db_info must gather	
GRD-39109	Document ATAP activation on RAC	
GRD-35570	Guardium v11.0 documentation revision about "Configure Apache Cassandra auditing": Inspection Engines setup, Multi-tenant architecture and Datastax support	

Security Fixes

Issue key	CVEs	Summary
GRD-38475	CVE-2019-4732 CVE-2020-2583 CVE-2020-2593 CVE-2020-2604 CVE-2020-2659	Upgrade IBM Java
GRD-37699	CVE-2019-5736	Update docker to latest version

Sniffer Updates

The latest sniffer patch that is included in v11.2 is v11.0p4007

Installation of sniffer patches must be scheduled during a quiet time on the Guardium appliance to avoid conflicts with other long-running processes (such as heavy reports, audit processes, backups, imports etc.).

Universal sniffer patch can be installed on top of any GPU starting with v10.0 patch 100 or higher.
If there's a failure to install, the following error message is displayed:
ERROR: Patch Installation Failed - Incompatible GPU level. GPU p100 or higher required.

If the downloaded package is in .zip format, extract it outside the Guardium appliance before installation.
The sniffer patch must be installed across all the appliances: central manager, aggregators and collectors to avoid aggregator merge issues.

Important:
Any superseding sniffer or security patches must be reinstalled after you install v11.2.
Installation of sniffer patches will automatically restart the sniffer process.

Snif Update	Issue key	Summary	APAR
4003		https://delivery04.dhe.ibm.com/sar/CMA/IMA/08lpr/0/Guardium_v11_0_p4003_sniffer_update_release_notes.pdf	
4004	GRD-37994	Parser errors when performing DAM of a Sybase DB: 'unexpected token'	GA17103
	GRD-37876	Missing 'HELP SESSION' in Teradata traffic collection when 'S-TAP TERMINATE' policy action configured	GA17096
	GRD-37767	Snif logs cleartext passwords for some Oracle traffic	
	GRD-37759	'SQL Verb' parsed as '(' in the Informix traffic collection	GA17097
	GRD-37742	Query is not properly parsed by sniffer	
	GRD-37524	GuardAppEvent" sqls captured as Oracle prep/bind statements are not extracted properly when antlr3_cached_raw_context_count is enabled	GA17090
	GRD-37517	Records Affected of DB2 for z/OS is incorrect with sqlcode=-913	GA17022
	GRD-37479	"Object / Field group In group" Policy rule fails to log MS SQL SERVER "SET" and "DECLARE" statements, however it does log them when the rule does not exist	GA17070
	GRD-37423	Informix - Values are not masked when they are part of double quotes	GA17113
	GRD-37293	SAP HANA Parser errors unexpected token: "CURRENT"	GA17061
	GRD-37174	Table name with keyword 'ASC' is not parsed in the Informix traffic collection	GA17040
	GRD-37142	SQLs not logged after an apostrophe (')	

	GRD-37140	SQL Verb comes up incorrect in Splunk syslog	GA17038
	GRD-37121	ALTER QUEUE Service Broker statement for SQL SERVER 2017	
	GRD-36967	Sensitive data in long SQL statements in comments is not always masked	GA17114
	GRD-36910	snif.log growing fast filling up the file system	
	GRD-36810	Parser Error found for ORACLE Sniffer Version: p4048	
	GRD-36393	Rule to ignore STAP session is getting triggered incorrectly	GA17016
	GRD-36138	Tuple group with values containing plus (+) sign can't be used in policy	GA16986
	GRD-35854	Parser error for MS SQL Server	
	GRD-35289	V10.5 || SYBASE || Dynamic Stored Procedure || GDM_ERROR filling up with PARSER_ERROR	GA16980
	GRD-35055	Parser errors using Sniffer patch P4045 when performing DAM of a PostgreSQL database: "unexpected token" and "expecting RPAREN" errors	GA16992
	GRD-34786	Guardium does not always parse certain commands executed within a procedure or as dynamic statements.	GA17126
	GRD-34069	v10.6 Msg field with is blank for extrusion rules but Full SQL is logged	GA16927
	GRD-33883	No traffic after installing Sniffer patch p4046: snif.log filled up with hundreds of records like "INFO: TAP client <a.b.c.d> disconnected", where <a.b.c.d> is the same IP address as the Collector appliance	GA17004
	GRD-30806	support large packets for kafka	GA16979
	GRD-37894	Missing db user for mongodb kerberos + SSL traffic	
	GRD-28592	Failed login exceptions every time Db2 database is activated. Seen after sniffer patch p4040 is applied	GA16255
4005	GRD-39392	Query rewrite feature for MS SQL Server does not work	
4006	GRD-40890	IMS alert sending SQLError=bb messages	GA17210
	GRD-40414	IBM Security Guardium v10.6 Sniffer patch P4050 restarts: guard-snif main process (<guard-snif_PID>) terminated by SEGV signal	GA17203
	GRD-39934	Hadoop monitoring broke after upgrade from 10.6 to 11.1	GA17217
	GRD-39882	Failed SQL doesn't have exception logged	GA17201
	GRD-39050	DB2/Z LOGIN_FAILED exception logged as SQL_ERROR since Snif V10 P4044	GA17142
	GRD-37742	Query is not properly parsed by sniffer	GA17154

	GRD-37304	Sniffer restarts frequently by SEGV signal because of size mismatch in the LRU internal two containers (list and map)	GA17183
	GRD-35034	Access rule abnormal behavior using the Objects from previous rule	GA17168
	GRD-33042	SAP HANA Audit Logs vs Guardium does not match despite allow-all policy	GA17204
	GRD-32682	Under which circumstances would a client receive these alerts from an access rule?	GA17214
4007	GRD-41355	Constant Sniffer Restarts	GA17235
	GRD-41287	Sniffer failed to decompress messages from U-TAP	GA17227

New platforms and databases supported in v11.2

- Hortonworks v3.1
- CouchDB v2.3.1
- Vertica v9.2
- Informix v14
- Db2 v11.5
- MariaDB v10.4.8
- MemSQL v6.8
- Postgre v12
- Mongo DB v4.2.1
- MemSQL v7.0
- MariaDB v10.3.13
- Elastic Search v7.3 for S-TAP and AWS
- MySQL8.0.18
- Amazon DynamoDB (Supported only for External S-TAP)
- Vertica 9.3

Note: Hadoop is not supported in IPv6 mode.

Deprecated functionality

- IBM Cloud (formerly Softlayer) is deprecated and will be removed from the Guardium interface in an upcoming release.
- Cleversafe is renamed to IBM Cloud Object Storage.
- ttyS0 and ttyS1configurations for virtual machines are disabled in Guardium v11.2 and later. If your virtual machine supports a physical serial connection, enable serial tty by using the CLI command `store system serialtty`.
- Support for Ubuntu 12 ends in an upcoming release.

Resources

IBM Security Guardium IBM Knowledge Center and online help
http://www-01.ibm.com/support/knowledgecenter/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

System Requirements and Supported Platforms for Cloud and Vulnerability Assessment v11.2
https://www.ibm.com/support/pages/node/5736879

Supported platforms database for Data Activity Monitoring v11.2
https://www.securitylearningacademy.com/mod/data/view.php?id=19457

Appliance Technical Requirements v11.2
https://www.ibm.com/support/pages/node/5736891

IBM Security Learning Academy
securitylearningacademy.com

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