Release Notes

==========

Product:	IBM Security Guardium
Release version:	Guardium 12.0
Completion date:	22 September 2023
Updated:	28 July 2025

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 12.0

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.

Installing Guardium 12.0

Guardium 12.0 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 12.0

Before you upgrade, ensure that your appliance meets the minimum requirements. 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 upgrade to Guardium 12.0 from Guardium systems that are running on version 11.5 and up.

A direct upgrade to 12.0 is not supported for these configurations: disks with custom partitions, and disks with Encrypted Logical Volume Management (LVM), and Guardium systems that are deployed in cloud environments. Use the backup-rebuild-restore procedure to upgrade these configurations.

Before you upgrade, use the disable_deprecated_protocols GuardAPI to disable TLS 1.0 and TLS 1.1 and upgrade to TLS 1.2 on your 11.5 systems. Use TLS 1.2 on all of your 11.0 appliances so the communications are not lost when the central manager is upgraded to version 12.0. For more information about managing TLS in Guardium 12.0 and later, see Managing the TLS version.

Version 12.0 uses GIM certificates with SHA256. For more information, see Updating Guardium Data Protection GIM clients with SHA256 certificates.

The upgrade patch creates and sends an upgrade backup file to a remote server. The patch uses the current appliance system backup configuration as the location to send the file. System backup must be set with SCP or SFTP option on all appliances that are upgraded, even if system backup was never configured on those appliances.

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_11.0p9998_HealthCheck_<date>.zip

The version 11.0 Health Check patch 9998 must be successfully installed in the last seven days before you install the Guardium 12.0 GPU. If the Health Check patch isn't installed as recommended, the 12.0 installation fails with this error message: Patch Installation Failed - Latest patch 11.0p9998 required.

If the Health Check patch identifies a problem specific to the 12.0 GPU, you must resolve it before you install the 12.0 GPU. If the 12.0 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.

During upgrade, the system restarts to install the version 12.0 OS and software. Expect the system to take an extended amount of time to restart. During this time, the progress can be seen only on the VM or hardware console. After the system is up, it upgrades the data and configuration. During this time CLI access is available only in recovery mode. In recovery mode, the system isn't fully functional and only a limited set of commands are available.

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.

Note: Don't restart the system at any time during the upgrade even if it appears to be stuck. For real-time details on the system patch installation, different commands can be used at different phases. Before the system restarts, use the CLI command **show system patch status**. After the system restarts, use the CLI command **show upgrade-status**. If you're concerned about the status of the installation, use the CLI command **support must_gather patch_install_issues** and contact Guardium support. Depending on the phase of the upgrade, **support must_gather patch_install_issues** might not work, or the fileserver might not be accessible to collect the file. If you run into this scenario, contact Guardium support.

For more information about upgrading to Guardium 12.0, see Upgrading your Guardium system.

Post-upgrade
After you upgrade, 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.

To restore pre-12.0 backups, disable FIPS mode, restore your backup, and then enable FIPS mode.

To run Configuration Auditing System (CAS) with FIPS mode enabled, CAS server requires TLS 1.2 to be enabled, and CAS client requires IBM Java 8 SR7 or above.
To use S-TAP for z/OS with TLS 1.3, z/OS 2.04 is required.

New Features and Enhancements

Access management
Guardium 12.0 adds "password last changed" and "password expired" dates to the access management page and to the list_users API output to better support proactive password management.

Active threat analytics
You can now optimize resources and reduce false positives by excluding certain sources such as test data and activities that are performed by automated processes.

Audit process
The audit process to-do list adds the ability to quickly change the classification result sets being compared directly from the results-comparison view itself. For more information, see Comparing discovery and classification results.

You can now modify the receivers list for active audit processes, including deleting and rearranging existing users. Changes are tracked in the "User activity audit trail" report. For more information, see Audit process receivers.

Certificate management
- Support added for automatic retrieval of existing certificates from Venafi using the Guardium CLI.
- The number of SAN (subject alternative name) slots have increased from nine to 99.
- The date format in the warning message under the notification icon for expiring certificates has changed from `d-m-yyyy` to `yyyy-mm-dd`.

Classifier
Support added for the following:
- Fire with marker option for catalog search rules. For more information, see Classification rule handling.
- New custom properties, including maximum length for large-text data types with Microsoft SQL Server and new data-cardinality methods for Oracle. For more information, see MS SQL Server (DataDirect), and Oracle (Data Direct - Service Name).

Central management
The cross-central-manager health view (cross-CM health view) is a new Guardium unit type that provides aggregated health views for an entire Guardium deployment. These views include health information for all available central managers, aggregators, collectors, and S-TAPs in your environment. For more information, see Viewing deployment health data from multiple central managers.

You can now define S-TAP clusters for environments with multiple S-TAPs assigned to clusters of database servers. S-TAP clusters allow Guardium to detect traffic at the cluster level, meaning that if one S-TAP in the cluster is active, all S-TAPs assigned to the cluster are also marked as active. S-TAP clusters also support automatic removal of inactive S-TAP connections for active-passive cluster configurations. For more information, see Create and manage S-TAP clusters.

Database discovered instances rules
Support added for the following:
- Ability to specify existing Guardium groups for filter and exclude rules
- Ability to delete discovered instances and existing inspection engines that match specified criteria and standard operators.

For more information, see database discovered instances rules.

Datasources
Support added for creating new groups with username and host name or IP address criteria.

External ticketing
Event Management is now integrated with the ServiceNow. For more information, see Configuring an external ticketing system.

GIM
Guardium now uses SHA256 GIM client certificates. For more information, see GIM clients with SHA256 certificates.

IBM Knowledge Catalog integration
Integration with IBM Knowledge Catalog is not currently supported in Guardium Data Protection 12.0. If you require support, please submit an idea on the IBM Product Support portal at ideas.ibm.com.

Investigation dashboard
Support added for monitoring and automatic recovery to identify and recover issues in the investigation dashboard. For more information, see Monitoring and automatic recovery for the investigation dashboard.

Runtime sensitive-object identifier
The Runtime Sensitive Object Identifier is redesigned. You can now manage runtime sensitive object identification by using the new Runtime Sensitive Object Identifier session level policy and report.
For more information, see Runtime sensitive-object identifier.

Policies
Session-level policy adds support for SQL criteria, extrusion rules through criteria server data, and ability to use regex in groups and custom tuples.

S-TAP
Unix S-TAP and External S-TAP support OpenSSL v3.1 and FIPS140-3.
External S-TAP supports MongoDB Atlas with MongoDB Compass.

Universal connector
The universal connector now offers a troubleshooting tool. For more information, see universal connectors.

Universal connector plug-ins are now preinstalled. When newer versions of the plug-ins become available, you can choose to upload them manually or wait for the next Guardium patch release to get them automatically updated.

Vulnerability Assessment

- Ability to display both alias and non-alias value in a report.
- Ability to find an existing vulnerability assessment by using the Security Assessment Finder screen.
- Support for uploading MS SQL opensource driver through custom uploads.
- Ability to export vulnerability assessment results through external feed.
- Support added for Oracle MySQL enterprise edition 8.0 CIS benchmark version 1.2.0, MongoDB 4.0 and MongoDB 5.0 CIS benchmark version 1.0.0, latest CIS benchmark for DB2, CIS benchmark for PostgreSQL version 15.
- Support added for Oracle MySQL enterprise edition 8.0 STIG benchmark, ver 1 rel 1, Oracle 19c benchmark.
- SSL encryption for Oracle 11.x, 12.x, and 19.
- Support added for Apache Cassandra, Percona MySQL datasources.
- Support added for Apache Cassandra, PostgreSQL, and PostgreSQL EDB entitlement reports.
- For a complete list of tests and groups added or updated in version 12.0, see https://www.ibm.com/support/pages/node/7031317. Tests and groups that are added after the release of Guardium version 12.0 will be available in upcoming quarterly DPS reports.

System enhancements

- RHEL is upgraded from RHEL 7 to RHEL 9
- The output of all CLI commands (including Guardium API commands) that modify a component of the user's system now includes the timestamp after the command finishes running.
- Network Time Protocol (NTP) daemon is now replaced by Chrony daemon.
- Support added for TLS 1.3.
- Ability to mark updates as "read" from the notification icon in the UI.
- View patch installation status of managed units from central managers.

Sniffer Updates

The following Sniffer patches are included in Guardium 12.0. The latest sniffer patch that is included in Guardium 12.0 is version 11.0p4067.

Sniffer patch number	Issue key	Summary	APAR
11.0p4053		https://download4.boulder.ibm.com/sar/CMA/IMA/0b18n/0/Guardium_v11_0_p4053_sniffer_update_release_notes.pdf	
11.0p4054		https://download4.boulder.ibm.com/sar/CMA/IMA/0b2h6/0/Guardium_v11_0_p4054_sniffer_update_release_notes.pdf	
11.0p4055		https://download4.boulder.ibm.com/sar/CMA/IMA/0bak0/0/Guardium_v11_0_p4055_sniffer_update_release_notes.pdf	
11.0p4057		https://download4.boulder.ibm.com/sar/CMA/IMA/0bblm/0/Guardium_v11_0_p4057_sniffer_update_release_notes.pdf	
11.0p4062		https://download4.boulder.ibm.com/sar/CMA/IMA/0bgoq/1/Guardium_v11_0_p4062_sniffer_update_release_notes.pdf	
11.0p4067	GRD-72872	p4062 - Sniffer crash	GA18353

	GRD-72489	Postgres collate parser error	GA18348
	GRD-72481	POSTGRESQL PARSER_ERROR related to DATE and POSITION functions	GA18340
	GRD-72381	session is never terminated leaving db users locked on db side when using S-GATE TERMINATE with firewall_default_state=1 and snif.log shows "Session doesn't exist"	GA18357
	GRD-72376	Guardium captures password in clear text	GA18356
	GRD-72273	"ZOS Audit" Rule Action No longer reported in snif.log in Guardium V11.x	GA18352
	GRD-72182	Some Oracle SQL commands are incorrectly logged as the SHUTDOWN command reopen.	GA18341
	GRD-70831	Sniffer becomes unstable, reports parser errors, segmentation faults and generates coredump files	GA18297
	GRD-70588	Unable to filter in policy using the Application User attribute	GA18310
	GRD-70226	Improvements to Failover mechanism	N/A
	GRD-69605	Query Rewrite when TOAD used connect to Oracle 19.15 resulted in ORA-03120	GA18354
	GRD-66624	No DB User Name in Guardium Activity Logs for Teradata Exit with no exception	N/A

New platforms and databases supported

Windows S-TAP

- EDB Postgres 15.2
- PostgreSQL 15
- MSSQL Azure MI 2022
- Couchbase 7.1
- Elasticsearch v.8.6
- MongoDB v.6.0

Unix S-TAP

- EDB Postgres 15.2
- PostgreSQL 15
- Teradata 17.2
- Vertica 12
- Redis 6.2
- Couchbase 7.1
- CockroachDB 22.2.0
- Elasticsearch 8.6
- Neo4j 5.6
- DataStax 6.8.20

- MongoDB 6.0
- Red Hat 9
- Ubuntu 22.04 LTS

Deprecated commands, platforms, and functionality

Deprecated CLI commands

Old command	New command
- show runtime_sensitive_object_identifier - show runtime_sensitive_object_identifier_hits - show runtime_sensitive_object_identifier_hits_with_signature - store runtime_sensitive_object_identifier - store runtime_sensitive_object_identifier_hits - store runtime_sensitive_object_identifier_hits_with_signature	None. Commands are replaced with the template session level policy. For more information, see Runtime sensitive-object identification.
show/store ssl_ciphers	show/store ssl_configuration
delete ntp-server	delete time_server
show system ntp all	show system time_server all
show system ntp diagnostics	show system time_server diagnostics
show system ntp server	show system time_server hostnames
show system ntp state	show system time_server state
store system ntp server	store system time_server hostnames
store system ntp state	store system time_server state

Deprecated GuardAPI and REST API commands

Old API	New API
- disable_deprecated_protocols - enable_deprecated_protocols - local_disable_deprecated_protocols	These APIs were available to upgrade TLS 1.0 and 1.1 to TLS 1.2. For Guardium 12.0, you can use the following new APIs to enable and disable TLS 1.2 and 1.3 as needed: - enable_all_tls - enable_fips_tls - enable_latest_tls For more information, see Managing the TLS version.

Deprecated functionality

Starting with Guardium 12.0, A-TAP support for Db2 and Informix is deprecated. Use the Db2 and Informix Exit interfaces instead. 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.

For information about using Db2 Exit, see:
https://ibm.com/docs/en/SSMPHH_12.0.0/com.ibm.guardium.doc.stap/stap/db2_stap_integrate.html

For information about using Informix Exit, see:
https://ibm.com/docs/en/SSMPHH_12.0.0/com.ibm.guardium.doc.stap/stap/informix_exit_cfg.html

Platforms and software that are no longer supported
- HP-UX 11.31
- Centera is no longer supported for backups.

Platforms that will not be supported in Guardium versions 12.1 and up
- Ubuntu 14
- AIX 7.1
- SuSe 11
- Debian 9
- Windows Server 2012
- Windows Server 2012 R2
- SQL Server 2012

Guardium functionality that will be deprecated in versions 12.1 and up

FAM crawler

Guardium versions that will reach EOS

Guardium version 11.3 will reach end of servicing in April 2024. For more information on how to upgrade your Guardium system, see https://ibmdocs-test.dcs.ibm.com/docs/en/SSMPHH_12.0.0_test?topic=upgrading-your-guardium-system.

Known limitations and workarounds

Component	Issue key	Description
Active threat analytics (ATA)	GRD-74185	Users with either "user" role or "admin" role have the permission to view reports from ATA case details. If the "user" role access is removed from a user, report links are disabled unless the user is assigned the "admin" role. **Workaround:** Add the "user" role back to the user to allow access from the Active Threat Analytics case.
	GRD-69359	In the new Exclude function for ATA, items that were added to the Exclude list before 12.0 will not be included during the 12.0 upgrade or backup and restore. **Workaround:** These items will need to be re-added to the exclude list using any of the usual methods.
	GRD-74154	After upgrading to Guardium 12.0, you might encounter the following error message when you click on 'View profile' in the active threat analytics dashboard: “Operation couldn't complete due to database error.” **Workaround:** Install the Guardium 12.0 database protection subscription service package.

	GRD-69930	If you clicked a link that opened the Investigation Dashboard on a new window, you might experience faster browsing experience if you left the window open while investigating different potential risky users from Risk Spotter or Active Threat Analytics cases. However, the links may appear broken if you minimize the Investigation dashboard window or switch to a different one. **Workaround:** Click the Investigation dashboard window to return focus to it or ensure that it is always visible.
	GRD-68513	The available reports in case details view are usually filtered by either service name or database name, depending on the server type of the case source. However, the following four case types are filtered by service name regardless of the server type: • Brute-force attack • New grants • Malicious stored procedures • SQL Injection **Workaround:** You can manually adjust the filter settings to filter these cases by database name instead.
	GRD-73256	The source activities chart in the Source details and History tabs for the following case types: brute-force attack, new grants, malicious stored procedures, and SQL Injection are not available for these server types: MySQL, Db2, MongoDB, MS SQL Server, and S3. **Workaround:** Fix is available in an upcoming patch release.
	GRD-75135	An incorrect period end date is displayed in Active Threat Analytic (ATA) cases that were generated before upgrading to 12.0. The ATA page does not display new ATA cases that are generated from managed units on Guardium versions lower than 12.0. **Workaround**: Install ad-hoc patch 12.0p4.
Central management	GRD-73612 GRD-72134	Unregistered systems still appear on the aggregated health views of the cross-CM health view system, but their data is no longer updated, and their status may not be listed accurately. **Workaround:** A fix is available in an upcoming patch release.
Custom reports	GRD-74601	If any previously created custom report uses the following attribute, that report will fail to execute after you upgrade to Guardium version 12.0: `Test Result  Datasource/Severity` **Workaround:** Edit the report definition by using the Custom Query-Report Builder, remove the `Datasource/Severity attribute,` and then save the cloned report. If needed, these attributes can be manually added back to your cloned report.
FIPS mode	GRD-74155	You cannot restore pre-12.0 backups with FIPS mode enabled. **Workaround:** Disable FIPS mode, restore your backup, and then enable FIPS mode.
	GRD-74651	Running the CLI command `store system ssh secure` with FIPS mode enabled might limit access to the Guardium system.

		Workaround: If this issue occurs, run the CLI command `store system ssh default` to restore ssh connectivity.
GIM	GRD-74548	GIM cannot be upgraded directly from version 10.6 to version 12.0 because version 10.6 does not support custom GIM certificates. **Workaround:** Upgrade to version 11.4 or 11.5 before you deploy custom certificates with SHA256 and then upgrade to version 12.0.
	GRD-74281	GIM transitional bundles (SHA1) cannot be uploaded to Guardium version 12.0 when FIPS mode is on. **Workaround:** Turn off FIPS mode to upload SHA1 GIM bundles.
	GRD-75006	When you upgrade from Guardium version 11.5 to 12.0, all GIM packages that were imported before the upgrade are removed.
Installing Guardium by using ISO	GRD-64163	If you are using the ISO to install Guardium on physical hardware that has serial ports and you are not connected to those serial ports, some console messages such as system output and start up messages will be redirected to the unused serial ports. These messages are not sent and cannot be viewed in the remote console. **Workaround:** If you are having problems when the system starts and are not seeing messages or output in your remote console, connect a terminal to the serial port in order to see if the additional messages are being directed there.
	GRD-80726	The following warning message is displayed during ISO installation: "Warning: Deprecated Driver is detected: "iptables" will not be maintained in a future major release and may be disabled. **Resolution:** Ignore the warning message. Guardium 12.0 uses "iptables" even though it's deprecated in RHEL9.
MySQL server upgrade	GRD-73148	When logging in to the CLI the following warning appears: "WARNING: MYSQL_OPT_RECONNECT is deprecated and will be removed in a future version." The same warning might appear in other CLI command output or logs. Guardium functionality is not affected by this warning. **Workaround:** A fix is available in an upcoming patch release.
Risk events	GRD-74537	Cannot access the action button in the 'DB User Behavioral Analytics' window when it's opened from Risk indicator.
Real-time sensitive object identifier	GRD-74412	Predefined pattern codes in RSOI session level policies can be corrupted. Runtime sensitive object identifier session level policy rules include predefined patterns that represent frequently used sensitive objects such as credit card data. These predefined patterns include a code (for example, *$(10100001-)$*) that represents selected Server Data criteria flags in the options menu.

		If you clone a policy rule, click on the options menu, and then click OK, when you re-open the cloned rule, the settings are cleared from the options menu and the code is deleted from the pattern. **Workaround:** If you are working with a cloned rule in the runtime sensitive object identifier session level policy, either do not click on the options menu, or before you open the menu, copy the code so that you can paste it back into the pattern so it can be added back if it is cleared.
	GRD-76113	The Runtime Sensitive Object Identifier policy template contains a regex error in the pattern for PCI Track data. This policy will be updated in an upcoming bundle. **Workaround:** After you create a copy of the Runtime Sensitive Object Identifier policy template, replace the criteria for PCI Track (Rule 8) with the following regex: (101000010)GUARDIUM://REGEXP/[%B[0-9]{15,19}[A-Za-z0-9.]\/[A-Za-z0-9.][0-9]?[0-9]?|\;[0-9]{15,19}=[0-9]?[0-9]?
SAML authentication	GRD-74144	SAML does not work after upgrading to version 12.0 from a Guardium system with patch 11.0p530 or below. **Workaround:** If single sign-on is enabled, you must access the upgraded central manager, download the metadata again and upload the new metadata to IdP (Identity Provider). For more information on uploading the metadata, see Configuring authentication.
Session-level policies	GRD-74346	When installing a policy rule with FIELD, OBJECT or COMMAND in rule with value *Every Member in Group*, the flag is the database is not set. **Workaround:** A fix is available in an upcoming patch release.
	GRD-74087	When a UI session-level policy is imported to advanced session-level policy, the advanced session-level policy does not recognize the operator “ALL”. **Workaround:** A fix is available in an upcoming patch release.
	GRD-74086	When a UI session-level policy is imported to advanced session-level policy and there is more than one rule, the first rule is not imported. **Workaround:** A fix is available in an upcoming patch release.
SMTP Alerter	GRD-76375	The SMTP alerter might restart every 5 minutes if SMTP is not configured. **Workaround:** Use the *modify_guard_param* GrdAPI to turn off the SMTP alerter (or set it to a very long interval). For example, the following command turns the SMTP alerter off. `> grdapi modify_guard_param paramName=NANNY_TEST_SMTP_ALERTER paramValue=0 ID=0`

TLS	GRD-73681	AWS Secrets Manager does not work as expected when the IAM Role uses TLS 1.3 authentication. **Workaround:** The Amazon IAM role requires that TLS 1.2 is enabled. For more information about managing the TLS protocol, see Managing the TLS version.
		Before you upgrade, disable TLS 1.0 and TLS 1.1. Use TLS 1.2 or TLS 1.3 on all your 11.0 appliances so the communications are not lost when the central manager is upgraded to version 12.0. For more information, see Managing the TLS version.
Upgrade	GRD-72744	The scp-ssh-key-mode is disabled after upgrade. **Workaround:** Turn on scp-ssh-key-mode by using the CLI command `store system scp-ssh-key-mode on` and then create a new "public-transfer-key" by using the command `store system public-transfer-key create`.
	GRD-66984	When you upgrade to Guardium 12.0 after installing 11.5 the GUI does not restart when the non-default port (8443) is used. **Workaround:** After installing 11.5, run the CLI command `restart gui` before upgrading to 12.0.
	GRD-75004	If upgrade patch 11.0p12000 (12.0 upgrade) fails before rebooting to version 12.0, the upgrade patch is not available to reinstall version 12.0. **Workaround:** reupload and reinstall health check patch 11.0p9998, which will retrieve the missing upgrade patch file. Or re-upload and re-install patch 11.0p12000.
	GRD-75007	If upgrade patch 11.0p12000 (12.0 upgrade) fails before rebooting to version 12.0 and you reinstall p12000, you the following warning even though the install failed: “Patch 11.0 12000 has already installed successfully. Don't need to install it again.” Do you really want to install again (yes or no)? **Workaround:** Type “yes”.
	GRD-75059	The custom uploaded Oracle driver and Db2 license is missing in Guardium systems that were upgraded from 11.0p530 (version 11.5 with patch 530) to version 12.0. **Workaround:** After upgrading, manually upload the custom Oracle driver and Db2 license, and restart the GUI.

Bug Fixes

Issue key	Summary	APAR
GRD-52978	SOFTWARE_TAP_PROPERTY_HISTORY table crashing multiple times on multiple appliance (Need RCA)	GA18216
GRD-56003	Quick Search shows enabled in GUI and CLI but Investigation DB says it's not enabled	GA17763
GRD-59362	New Guardium installation (Oracle Cloud OCI image) on the Cloud: can't change system domain nor ping the appliance by hostname	GA18069
GRD-59398	Aggregation processes are failing due to stuck queries from threat detection analytics (11.3)	GA18092
GRD-59736	v11.4 Please update MS SQL Custom Driver capability from jTDS to Microsoft's JDBC Driver	RFE
GRD-59740	Custom query based on a distributed report gets scrambled if the columns order of the distributed report is changed	GA17617
GRD-59907	java.sql.SQLException: HOUR_OF_DAY: 2 -> 3	GA18314
GRD-60592	Wrong solr path used when data mart post extraction process checks for disk usage	N/A
GRD-60921	Unable to update ETAP parameters from UI	N/A
GRD-61254	IEs "has different ASLHEAPSZ with but they are sharing the same executables	GA17757
GRD-61728	Error creating Distributed Report: two records same attribute	GA18019
GRD-62057	S-TAP verification failed even the datasource test connection is successful	GA18102
GRD-62115	Audit results export sending template not data to external location	GA18038
GRD-62182	Missing ATAP info in the "S-TAP and External S-TAP Statistics" report	GA18025
GRD-62803	Calling gim_client_params RESTAPI fails for Windows GIM client	GA18116
GRD-62983	Backup CONFIG Failed on p440 Upgraded Appliances	GA18075
GRD-63100	Import is failing with the error "Error opening /etc/adsm/TSM.sth encryption key file"	GA18106
GRD-63330	12.0: "store system strong shared secret enable" does not check for pre-existing secret key validity	GA18036
GRD-63441	v11.4 Additional SSIS Vulnerabilities Appearing after installing SSIS	GA18108
GRD-63603	Is there any plan (workaround, or fix) on the roadmap to address the limitation only on Linux that the Guardium K-TAP agent cannot co-exist with Vormetric LDT policies?	GA18158
GRD-63634	License key exposed in browser debug HTTP request	GA18375
GRD-63693	ATA: Case Details - Full SQL Report won’t open when selected in case details	GA18097

GRD-63722	Cannot create Snowflake datasource; receive an error	N/A
GRD-63831	request to add us-go-east-1 region for AWS Secretes Manager for data source definition	N/A
GRD-63869	12.0: Guardium - need to disable diffie-hellman ciphers	GA18077
GRD-64052	Unable to Open Ticket to Resilient	GA18123
GRD-64216	Server may become unstable if STAP is upgraded twice while a session is open and KTAP_INSTALLED=0 during the second upgrade	GA18139
GRD-64524	Login banner is not shown when authenticating to the GUI using SAML	GA18136
GRD-64548	Datasource Test Connection message "You must save the datasource before testing the connection" despite the datasource was saved	GA18138
GRD-64553	custom alerting class	N/A
GRD-64573	Error during classification scan: Cursors are not supported on a table which has a clustered columnstore index	GA18140
GRD-64646	GI connection issues to GDP CM due to faulty insights-cert	GA18217
GRD-64672	Guardium ssl_gui_ciphers missing after Restoring System Config Backup	GA18171
GRD-64794	Unable to remove hostnames/entries from the Traffic Ignore List	GA18159
GRD-64883	Guardium Memory utilization SNMP MIBs	GA18241
GRD-64885	Cannot create a report with TotalAccess field in condition	N/A
GRD-64902	Schedule job Exception after applying patch 11.0p450	GA18132
GRD-64977	No EXIT libraries for Netezza and MySQL in STAP 11.5.0 r113097 in GIM package (RH8)	GA18204
GRD-64986	Wrong zoo.cfg included in must gather	N/A
GRD-65037	Guardium Authentication via SSO with Microsoft Azure AD fails: "AADSTS750032: SAML protocol response cannot be sent via bindings other than HTTP POST"	GA18130
GRD-65081	Query-Report Builder takes a lot of time to save queries	GA18209
GRD-65119	Errors in discovery data	GA18231
GRD-65180	The value of NUMBER_OF_PROCESSORS is not sent to the collector in V8 Protocol	GA18179
GRD-65189	Multiple Scheduled Audit Processes Not being executed	GA18188
GRD-65278	Error performing any action on page Audit Process Status on the GUI	GA18127
GRD-65280	Include all rolled-over ELB logs in ELB must gather	N/A
GRD-65312	Custom Table Scheduling section missing with Datasource using Cyberark	GA17811
GRD-65342	grdapi create_datasource does not store secret name	GA18143
GRD-65541	Need MIB file for SNMP Traps	GA18206

GRD-65632	QID 38738 vulnerability reoccurs after restart	GA18279
GRD-65640	Distributed Report does not complete for one date with a lot of traffic	GA18173
GRD-65668	Fileserver doesn't work after setting "store cipher java secure"	GA18149
GRD-65689	STAP 'Missing parameters' in 'Run diagnostics' of 'Module Installation/Set up by Client'	GA18194
GRD-65705	Custom Table upload query setting 'Column Id Type' to 'String' reverts it to 'Number' upon 'Apply'	GA18312
GRD-65718	Quick Search was disabled on one MU	N/A
GRD-65746	Issues identified post Event Hub implementation in Azure environment	GA18166
GRD-65757	HostName IP Alias creation: An error occured java.lang.RuntimeException due to Communications link failure	GA18234
GRD-65772	Active Threat Analytics - Source Behavioral Analysis is EMPTY in all incidents	GA18189
GRD-65798	STAP may become unstable if it sends traffic to between 6 and 9 collectors	GA18164
GRD-65836	Guardium Aggregator Import fails - Error:1030; Message:Got error 1 - 'Operation not permitted' from storage engine ; SQL:alter table TURBINE.GDM_CONSTRUCT_INSTANCE	GA18160
GRD-65851	Unix S-TAP Agent not capturing SQL for Oracle	GA18249
GRD-65873	"Warning: Unable to connect to GUI" login to cli if GUI port has been changed from the default 8443	GA18175
GRD-65890	Ability to copy a custom K-TAP module from one GIM server environment to a different GIM server environment	GA18407
GRD-65923	Classification timeout repeating more times on same object	GA18165
GRD-66283	Aggregation/Archive report indicates success when purge fails	N/A
GRD-66321	To remove GIM module with partial package name, then import again get "This bundle already exists in the guardium system"	GA18168
GRD-66752	Old data in GDM_SESSION table is not purged, and partitions are not deleted	N/A
GRD-66761	ELB is not functioning properly - Windows STAP	GA18199
GRD-66858	System Data Backup error: mysqldump: Error 1412: Table definition has changed, please retry transaction when dumping table `TURBINE_USER_GROUP_ROLE`	GA18151
GRD-66878	ServiceNow is not loading Assignment group, Category Subcategory Affected CI and Environment fields for a new ticket created in Guardium Threat Analytics integration	GA18224
GRD-66895	mongod-guard-or process is killed abruptly by OOM	GA18370
GRD-66915	Session Level Policy with filter on 7-tuple including Analyzed CLient IP and other fields, does not work correctly	GA18413

GRD-66920	'Data-Sources' Report takes long to display the list of datasources	GA18281
GRD-66956	Password expiration for GUI is reset to default 90 days after applying patch	GA18181
GRD-66966	Unable to reset an accessmgr account that is disabled.	GA18185
GRD-66984	After GPU 500 installation the GUI is not started when uses non-default port (8443)	GA18232
GRD-67023	PSIRT: PVR0412782 - Guardium V11.5 affected by "Reverse Tabnabbing" Vulnerability	GA18239
GRD-67028	Getting error "Invalid argument resultSetType, use TYPE_FORWARD_ONLY " when trying to get a roles assigned report in a SAP HANA DB	GA18215
GRD-67067	DOCUMENTATION REQUEST CLI COMMANDS	GA18402
GRD-67093	Report Color Indication Rule with 'In Group'/'Not In Group' Not Working Properly	GA18240
GRD-67119	Data Source Username field is limited to 50 characters	GA18155
GRD-67150	CAS Server Control	N/A
GRD-67175	No bequeath traffic after A-tap re-configured and DB reboot due to device minor number calculation	GA18294
GRD-67250	store sync_solr_certificate sets expiration date to 01/23/2023 causing alert on GUI	GA18156
GRD-67261	VA Error in Test logic for all MS SQL Audit Record Tests	GA18190
GRD-67267	QUERY REWRITE POLICY NOT BEING APPLIED CORRECTLY BY EXTERNAL S-TAP	GA18197
GRD-67338	Connection to Microsoft Azure SQL Datasource on Cloud fails	GA18229
GRD-67346	Show service state for 8444 erroneously shows enabled, even if disabled	GA18220
GRD-67358	Missing db username on 2 Oracle DBs without exceptions	GA18247
GRD-67420	KTAP not loading after system reboot (AIX 7.2; STAP 10.6 release r112157)	GA18425
GRD-67534	FILESERVER WITH TLS ENABLED (PORT 8445) STOPS WORKING IF GIM IS NOT RUNNING AND APPLIANCE WAS UPGRADED FROM p400 DIRECTLY TO p460	GA18285
GRD-67616	SESSION FOR MSSQL DATABASE MISSING DB USERNAME IF THERE WAS NO SQL ISSUED FOR A WHILE AFTER THE DATABASE CONNECTION WAS OPENED	GA18251
GRD-67699	"show network verify" command on Microsoft Azure hosted Guardium appliance does not work.	GA18237
GRD-67714	KTAP request for 5.14.21-150400.24.38.86_64 STAP v11.3 (suse-15 sp4)	N/A
GRD-67723	Microsoft SQL Server 2022 needs supported in DPS update	GA18401
GRD-67799	MySQL Certificate Extension Ad hoc patch - V9.5	GA18389

GRD-67825	Hadoop Ranger HA Connectivity Failure using HDFS NamedNode	N/A
GRD-67936	Active Risk Spotter and Active Threat analytics not showing data in quick search when choosing to investigate.	GA18378
GRD-67946	hadoop hdfs (High Availbility) only collects traffic for one day then stops until Hadoop services are restarted.	GA18306
GRD-68013	Generate GUI CSR without the OU field	GA18213
GRD-68063	Large number of packets dropped when DB2 Exit is configured	GA18305
GRD-68072	AWS PostgreSQL - Experian - filter out irrelevant empty data	N/A
GRD-68163	Documentation required about deprecated protocols enabled, disabled and feature scope	N/A
GRD-68210	The date format in the Warning for Certificates about to expire, displayed under Bell icon in GUI	GA18420
GRD-68213	Flat Log Process Not working on Collectors since applying v11p460	GA18272
GRD-68214	Guardium log in error for IBM i servers	
GRD-68235	VA Test 2264 - NOTIFYLEVEL parameter Is 3 Or Greater	GA18371
GRD-68249	MISSING DB USER IN KERBEROS AUTHENTICATION FOR NAMED PIPES CONNECTION	GA18226
GRD-68338	Database crashing after applying RHEL 8.7 KTAP bundle(4.18.0-425.10.1.el8_7.x86_64).	GA18424
GRD-68523	CLASSIFICATION JOB ON ORACLE DATABASE FAILS WITH ORACLE SYNTAX RELATED ERRORS	GA18266
GRD-68541	Alerter process did not start after mysql cert patch installation, v11.0p1018	GA18419
GRD-68574	Account lockout setting is reset to default after applying patch	GA18236
GRD-68584	VA job can't connect to datasources configured to be authenticated by external vaults	GA18286
GRD-68626	Health check Patch installation error (Ghost eth1 not removing)	GA18384
GRD-68667	NET_PROTOCOL is logged as TCP instead of TAP_DECRYPTED	GA18253
GRD-68725	Data Restore using SFTP with Windows path (backslash in it) Failed to Work	GA18270
GRD-68750	Custom Table Upload job for “PostgreSQL Sys Privs Granted To User And Role” custom table fails	GA18283
GRD-68756	DB_USER missing for local and remote sessions using NETEZZA_EXIT	GA18250
GRD-68765	Problem with DB2 z/OS VA tests	GA18397
GRD-68794	Active Threat analytics FullSQL report empty	GA18336
GRD-68813	Documentation required about "store service" CLI command	N/A
GRD-68831	Active Threat Reports are missing db_user name	GA18403

GRD-68858	The SESSION_TRUST_DETAILS table is not being purged properly	GA18394
GRD-68881	Documentation for grdapi set_outliers_detection_parameter	N/A
GRD-68904	MSSQL: empty db_user for server *.163 and service name YKE0-P12* - TDS	N/A
GRD-68918	support must_gather network_issues output shows errors in console	GA18320
GRD-68944	Long sql queries are not captured for SYBASE IQ connections using the CMDSEQ protocol	GA18304
GRD-69047	Patch p370 installation stuck in POST: Running VA Reset Assessment Threshold Script step and GUI down.	GA18382
GRD-69093	Variable 'sql_mode' can't be set to the value of 'NO_AUTO_CREATE_USER' during restoring a v10.6 data backup	GA18316
GRD-69095	Guardium SSO integration Issues	GA18280
GRD-69107	when installing STAP with consolidated installer, if adding value for KTAP_allow_module_combos, need a meanigful warning message	GA18396
GRD-69133	AWS RDS Oracle Datasource connection issues: "NoSuchMethodError"	GA18256
GRD-69163	2586 - DBMS Data Encryption (Recommendation Update)	GA18408
GRD-69182	WINDOWS STAP CONSUMES HIGH MEMORY AND MAY BECOME UNSTABLE IF AUTO DISCOVERY IS ENABLED	GA18259
GRD-69230	Classification count (*) causing timeouts	GA18257
GRD-69252	Strict username after login	GA18398
GRD-69274	Update documentation for cli command store ssl_ciphers custom	N/A
GRD-69330	DB UserName may be blank for DB2 z/OS sessions	GA18296
GRD-69346	installing Named Pipes Driver is not friendly position in the install screen.	GA18423
GRD-69369	Buffer overflow errors in Windows STAP are not logged to the collector STAP Events (STAP_EVENT table)	GA18258
GRD-69397	Non-existent IPV6 IPs logged by Guardium for Elasticsearch traffic	GA18293
GRD-69474	PSIRT: PVR0442868 - SQLMAP Reported Guardium appliance with SQL Injection Vulnerabilities against "archiveRestorexxxx"	GA18326
GRD-69487	Unable to edit inspection engines after adding with DB2 exit auto creation	GA18416
GRD-69493	DB Users logged as "1" and "?" Oracle	N/A
GRD-69495	Cannot edit policies or report Error: Mismatched parenthesis in regular expression.	GA18374
GRD-69529	2574 - Oracle DBMS Administrative Data Restrict Access to Views and Objects Owned by sys.	GA18388
GRD-69555	After Venafi sniffer certificate import, not taking sniffer common name	GA18358
GRD-69571	Audit Process executing Immediate Distributed Report returns zero rows	GA18260

GRD-69605	Query Rewrite when TOAD used connect to Oracle 19.15 resulted in ORA-03120	GA18354
GRD-69607	How to config ATAP for ElasticSearch	GA18392
GRD-69634	Missing session information after windows S-TAP upgrade for server .90 and .215/217 MSSQL	GA18431
GRD-69674	Clean Static Orphans fails with "Orphans cleanup had already run today" if the process from previous day finished the next day	GA18282
GRD-69706	SQLMAP SCANNING TOOL REPORTED GUARDIUM APPLIANCE WITH SQL INJECTION VULNERABILITIES AGAINST "NEWQUERYBUILDER"	GA18368
GRD-69707	PSIRT: PVR0442868 - SQLMAP Reported Guardium appliance with SQL Injection Vulnerabilities against "customDomain"	GA18300
GRD-69709	SQLMAP Reported Guardium appliance with SQL Injection Vulnerabilities against "definitionsExport"	GA18325
GRD-69710	PSIRT: PVR0442868 - SQLMAP Reported Guardium appliance with SQL Injection Vulnerabilities against "health"	GA18324
GRD-69795	2616 - Grantees with user defined Database Roles with DDL privileges	GA18385
GRD-69879	HDFS Ranger integration is not properly load balanced by STAP	GA18399
GRD-69902	Update datamining MG to include new zookeeper log files	N/A
GRD-69907	Windows STAP Discovery AD_Db2: Registry path not found	GA18376
GRD-69931	Tomcat services fail to start after Adhoc patch p1018 (Mysql certificate update) deployment	GA18268
GRD-69946	System Restore Process fails in v11.5: Backup file is not a packaged file	GA18415
GRD-69999	Disk usage issues if using Universal Connector due to the /var/lib/docker/overlay2/<hex str>/merged partition growing fast	GA18317
GRD-70013	VA - All Encryption at rest tests need verbiage to support 3rd party solutions per STIG Guidance	GA18395
GRD-70029	Db-user=6 or K for Oracle traffic	GA18417
GRD-70038	After Selective policy installed once, switching to non-selective policy has no effect	GA18263
GRD-70043	Installing v11 GPU patch p500 on top of v11 patch p380 fails	GA18273
GRD-70117	Custom Table Upload Stops Processing Datasources after multiple errors.	GA18333
GRD-70155	GUARDIUM APPLIANCE UNEXPECTED BEHAVIOR AFTER DAYLIGHT SAVING TIME CHANGES IN EGYPT	GA18267
GRD-70156	KTAP request 5.15.0-3.60.5.1.el8uek.x86_64 STAP for v11.4	GA18372
GRD-70158	Test 2572 and 2573 Issues	GA18377

GRD-70252	lsof: no pwd entry for UID <number> from support must_gather system_db_info command	GA18275
GRD-70254	lsof: no pwd entry for UID <number> from support must_gather system_db_info command	GA18275
GRD-70257	GIM client cannot connect to the GIM server anymore after it failed to connect once	GA18278
GRD-70276	FAM policy does not capture traffic if it is installed from CM	GA18386
GRD-70321	Update ATAP documentation is needed	N/A
GRD-70404	'Event User Name' is always blank in report based on the Policy Violation domain	GA18284
GRD-70411	DB2 DB crashing on db2-exit protocol	GA18404
GRD-70416	Sybase classification error - java.lang.OutOfMemoryError: Java heap space. V11.4	GA18299
GRD-70494	EI_GRANT table (CALL EI_COLLECT_GRANTS) run long time on one collector	GA18412
GRD-70607	Error - Failed to install module nvme when tried to install p470	GA18387
GRD-70645	Add ability to mark as read for available updates info	N/A
GRD-70693	MySQL DB Password appears in plaintext format during datasource save & update effort	N/A
GRD-70708	STAP is Red on STAP Control due to Deadlock	N/A
GRD-70784	Add support to CLIENT_OS=MACOS - Oracle	N/A
GRD-70870	Invalid count of "Known Databases" in Compliance Monitoring	GA18329
GRD-70901	S-TAP Log errors after 11.4 Upgrade - segfault at 381 ip code=killed, status=11/SEGV	GA18330
GRD-70917	Some SYBASE long sqls are not logged by the sniffer	GA18302
GRD-70948	ktap reader xxxx stopped running: Input/output error	GA18390
GRD-70952	Compliance Monitoring page shows "Needs agents installed" if applications connect using Virtual IPs	GA18313
GRD-71014	issue with Linux s-tap connection to OUA after upgrading s-tap to v11.5.2.0_r113723_1	GA18383
GRD-71017	S-Tap SAP HANA performance issue	N/A
GRD-71050	Not seeing database activity using the Universal Connector on a collector where the Universal Connector is running	GA18411
GRD-71159	V11.5 "store language" to Japanese completed with exceptions	GA18367
GRD-71166	Error saving query on the datastreams consumer status domain, after adding the status attribute to the report.	GA18366

GRD-71168	Regression - It returns error when adding Datasource from UI in upgraded CM	N/A
GRD-71221	LDAP Password visible clear text in the application debug	N/A
GRD-71278	RESTORE OF A BACKUP FAILS WITH: Can't kill a non-numeric process line 741.scripts/SQLGuard.pl	GA18318
GRD-71303	Z/os S-TAP V11.3 supported for Db2 V12 and DB2 v13	N/A
GRD-71364	db_user is logged as BAD_USER, but os_user is empty, client_os. server_os empty	GA18355
GRD-71396	Request for Documentation Update	N/A
GRD-71459	Include entire healthView and deployment logs in deployment issue must gather	N/A
GRD-71491	STAP v10.6.1.0_r113938 with fam_enabled=1 throws "FAM: ERROR: reading from K-TAP failed: -1 5 I/O error"	GA18393
GRD-71531	Documentation Jira - Linux-UNIX: Configuring Db2 Exit	GA18409
GRD-71537	Need to document the guard_tap.ini* files that get created in STAP directory	N/A
GRD-71545	resmon.ini default values for WSTAP are incorrect or missing in Documentation	GA18379
GRD-71558	Update analyze_limits.sh to reflect solr process change	N/A
GRD-71568	Oracle S-TAP Inactive Alerts triggered, stuck in Synchronizing	GA18426
GRD-71655	DB Utilization report error after installing patch P525: Unexpected error has occurred. Please contact your system administrator.	GA18309
GRD-71661	Guardium Netezza: no traffic from STAP on container	N/A
GRD-71699	Discovery does not work on Windows with Oracle DB v19	GA18414
GRD-71754	Entitlement Optimization - clicking 'Details' button under "New Users" section shows empty output	GA18339
GRD-71792	With "Password Never Expires" flag for a GUI user, the set guiuser says "Password has expired."	N/A
GRD-71810	Wrong IPv6 format is displayed for Client IP and Server IP addresses for Windows S-TAP	GA18319
GRD-71817	Sniffer crash - segfault at 10 ip 0000000003ac10ac	GA18405
GRD-71849	Query with "Test Results" main entity, fails to save after adding attribute "Datasource/Severity"	GA18327
GRD-71915	Allow 2 cloud accounts with same access key	N/A
GRD-72010	Need to confirm if given files can be ignored or not	GA18391
GRD-72037	"guard_ktap_loader retry" doesn't work properly	GA18406
GRD-72048	Test 2586 MS SQL Encryption At Rest does not check tempdb database but it should, as per the STIG	N/A

GRD-72140	Remove Security Guardium Vulnerability Assessment licenses from the product -Documentation	N/A
GRD-72171	"Updates are available" notification on the GUI lists older patches	GA18381
GRD-72227	Support matrix updates	N/A
GRD-72316	User Portal Sync can't deploy information into MUs	GA18373
GRD-72376	Guardium captures password in clear text	GA18356
GRD-72467	guardcli1-9 user passwords modified from GUI accessmgr stores cleartext password in TURBINE_USER	N/A
GRD-72489	Postgres COLLATE parser error	GA18348
GRD-72543	KTAP request 5.4.17-2011.6.2.el7uek.x86_64 STAP v11.4 (but v11.5 is needed after ticket is open)	N/A
GRD-72554	Hadoop Configuration does not appear after configuration	GA18345
GRD-72586	V11.5 iSTAP failover is not working when primary collector lost network connection	GA18349
GRD-72601	hadoop hdfs only collects traffic for one day then stops until Hadoop services are restarted.	GA18380
GRD-72822	GUI slow performance after applying p385	N/A
GRD-72847	Aggregator Data Archive Failed	GA18418
GRD-73671	Ability to shutdown snmp	N/A
GRD-73714	Improve process of updating Gim module running state	N/A
GRD-73805	Include gimserver logs in deploy_agents_issues must gather	N/A

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 12.0
https://www.ibm.com/support/pages/node/6955555

Appliance technical requirements 12.0
https://www.ibm.com/support/pages/node/7030249

IBM Security Learning Academy
securitylearningacademy.com

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