Release Notes

==========

Product:	IBM Security Guardium
Release version:	Guardium 11.3
Completion date:	7 December 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 11.3

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 11.3

Guardium 11.3 is available as an ISO product image on Passport Advantage.

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

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

Upgrading to Guardium 11.3

You can upgrade to Guardium 11.3 from any Guardium system that is running on version 11.0 and above.

Before you upgrade, ensure that your appliance meets the minimum requirements. You must upgrade your firmware to the latest versions provided by your vendor. If you use a Guardium appliance, check the Fix Central website for the latest firmware.

You cannot upgrade a disk with custom partitions or disks with Encrypted Logical Volume Management (LVM). Use the backup-rebuild-restore procedure to upgrade these configurations.

Health Check patch

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

The Health Check file is a compressed file with the file name in this format:
SqlGuard_11.0p9997_HealthCheck_<date>.zip

The v11.0 Health Check patch 9997 must be successfully installed in the last seven days before you install the Guardium 11.3 GPU. If the Health Check patch isn't installed as recommended, the 11.3 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.

After you upgrade to Guardium 11.3, apply all relevant maintenance patches. You must also apply the latest quarterly DPS patch and rapid response DPS patch even if these patches were applied before the upgrade.

Previously installed patches

When you upgrade to any version of Guardium 11.0, 11.1, 11.2, or 11.3, the Guardium 10.0 patches that were previously installed are no longer visible in the "Installed Patches" screen in the GUI.

Installing or upgrading to 11.3 S-TAP

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

New Features and Enhancements in Guardium 11.3

New features

Guardium universal connector
The Guardium universal connector enables Guardium to get data from potentially any data source's native activity logs without using S-TAPs. The Guardium Universal Connector ships with support for MongoDB and Amazon S3, requiring minimal configuration. Users can easily develop plug-ins for additional data sources and install them in Guardium. For more information, see Universal connector.

Hadoop with ranger HDFS
The S-TAP can consume Ranger audits from HDFS. For more information, see Hadoop integration with Ranger HDFS.

Manage datasource credentials with Amazon Web Services (AWS) Secrets Manager
Integrate your Guardium system with the Amazon Web Services (AWS) Secrets Manager to securely store, manage, rotate, and retrieve credentials for your datasources that use the Amazon Relational Database Service (RDS). For more information, see Managing datasource credentials with AWS Secrets Manager.

Manage GUI and GIM certificates with Venafi
Use the Venafi certificate management system to generate, install, and manage GUI and GIM certificates automatically in your stand-alone or central manager environment. For more information, see Managing certificates by using Venafi.

Tagging for policy rules
Guardium now provides predefined policy rule tags and supports custom tagging of rules. Use tags to quickly create and manage policies aligned with specific compliance standards, reporting and auditing requirements, and geographies. For more information, see Tagging policy rules.

Key enhancements

Data mart backup host
If the file transfer to a primary destination fails, Data mart sends the files to the failover host.

Data streams
Support added for AWS RDS Aurora MySQL databases.

Deployment health views
The deployment health table and topology views add support for a traffic metric, data streams, and universal connector. The deployment health dashboard adds a new *central manager limits* chart showing central manager connections and processes. The chart values are expressed as a percentage of configurable thresholds. For more information, see Deployment health views.

Discovery and classification
- Discover Sensitive Data now includes support for document-type datasources like MongoDB. For more information, see Discover Sensitive Data.
- You can now view the creator of the datasource in the Datasource Definitions page and in the datasources report.

- You can now calculate a confidence score during scanning. For more information, see Rule Criteria.
- Classifier now supports Amazon Web Services (AWS) RDS PostgreSQL and AWS RDS MySQL.

Encryption keys for Logical Volume Management (LVM) disks
If you use encrypted LVM disks, you can now set up a tang server that automatically unlocks each volume of your encrypted disks when you restart your system. You are no longer required to manually enter the encryption key for each disk. For more information, see Encrypted LVMs.

Enterprise load balancing
When the Enterprise load balancer relocate S-TAPs from loaded managed unit to a less loaded unit, the data from the S-TAP buffers is not lost. This is controlled by the **restartMode** parameter of the API **restart_stap**.

External ticketing
- You can now configure Guardium to automatically create incident or problem tickets in both IBM Resilient and ServiceNow platforms. For more information, see External ticketing.
- An audit trail is automatically created when a ServiceNow ticket is created. You can now store and retrieve comments from ServiceNow tickets.

Gather I/O metrics
Use the gather_io_metrics CLI command to manage the gather_io_metrics service, which collects information about I/O statistics on the Guardium appliance when you run the command. Guardium now includes the gather_io_metrics.txt file with the output of any must_gather command. For more information, see support gather_io_metrics in Support CLI Commands.

Guardcli accounts
You can now enable or disable guardcli1 to guardcli5 accounts from the User Browser page in the Access management GUI, by using the store guarduser_state CLI command, or from the update user API. For more information, see Managing users and User account, password, and authentication CLI commands.

Job history
The new job history view provides a Gantt chart showing when jobs have run and for how long. The chart supports audit, aggregation, and data mart jobs and includes information about start and stop times, duration (current, shortest, longest, and average), and task count. For more information, see Viewing job history.

LDAP import into custom tables
The LDAP configurations dialog now includes a column to display the LDAP filter that is applied to the imported data.

Link status of a network interface
You can now display the physical link status of a network interface by using the CLI command `show network interface status <NIC>`. For more information, see Network Configuration CLI commands.

Network Time protocol (NTP) server synchronization:
If the IP address of an NTP Server that is used to set the time of a Guardium system is changed, the system will continue to stay synchronized to the NTP server.

Predefined reports
New predefined reports are added to list days that are not archived or exported, new attributes in FAM for NAS and SharePoint, and available security assessment tests. For more information, see Predefined admin reports.

S-TAP and GIM dashboard
The S-TAP and GIM dashboard now offers interactive filtering, historical charts, and configurable traffic metrics. For more information, see S-TAP and GIM dashboard.

System backup
Support added for Amazon S3 Glacier.

File Activity
You can no longer configure FAM for Network-attached Storage (NAS) devices or SharePoint using the configuration app. Any manual change to the configuration file triggers an alert. After you establish a connection between your monitoring agent and the Guardium system, you can configure FAM for NAS or SharePoint by creating and installing a policy. For more information, see File activity policies for NAS and SharePoint.

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

Vulnerability Assessment (VA)
- There are 4 new Vulnerability Assessment tests for Db2.
- Support added for PostgreSQL 12.x and CIS benchmark for PostgreSQL 12.
- In the Assessment test selections screen in the UI, you can now choose to select from either CIS tests or STIG tests. You can also select CVE tests that are greater than or equal to a specific CVSS score.
- In the query-based test builder, a return value of 1 from the "Pre test check SQL" codes indicates that the pre-test passed and the test's SQL statement continues to run. A value of -1 indicates "Not applicable". The test stops running and the text from the "Pre test fail message" is displayed in the recommendation. Any value other than 1 or -1 indicates "Pre Test Check Failed. Test not executed". The test stops running and the text from the "Pre test fail message" is displayed in the recommendation.
- You can now create datasources and CAS database instances for Couchbase versions 6.0.4, 6.5.x and 6.6.0. For more information, see Couchbase datasource configuration.

Other enhancements
- When you log in as a CLI user, Guardium now checks to ensure that all components are running. If successful, the following message displays: System is now operational in CLI regular mode.
- When you install Guardium from a CD or DVD media on a system that's already on the same version, you will now be prompted to confirm or reboot to remove the ISO/DVD.

New platforms and databases supported in 11.3

Cassandra Apache 3.11.6
Cassandra Datastax 6.8
CDP 7.0
Cloudera 6.3.3
Cockroach DB
Couchbase 6.5
Greenplum 6.7.1
Greenplum 6.9
Google Cloud SQL
MariaDB 10.5
MongoDB 4.2.8
MongoDB 4.4
MySQL 8.0.20
PostgreSQL 12.3
Redis 6.x
SAP HANA 2 SPS04
Sybase ASE 16.0 SP2 PL08 and SP03 PL08

Known limitations and workarounds

Component	Issue key	Description
Audit process builder	GRD-46564	Some audit results not written to syslog. **Workaround:** Restart the GUI.
Deployment health topology	GRD-45881	If import is not scheduled on a backup central manager, a red node is displayed for that aggregator. But the node does not turn green even after the failover happens and the aggregator turns into a central manager. **Workaround:** After a failover, run the following command on the central manager to reset the change tracker: `grdapi change_tracker_reset host="CM hostname”`.
External S-TAP	GRD-47572	External S-TAP V11.3 is affected by CVE-2020-8177, which includes known vulnerabilities to the curl and libcurl packages, and by CVE-2019-20907, which includes known vulnerabilities to the python-libs and python packages. **Workaround:** Upgrade curl and libcurl to 7.29.0-59.el7_9.1 or later, and upgrade python-libs and python to 2.7.5-90.el7 or later.
	GRD-45918	Shared memory is not allocated on IBM Cloud k8 cluster **Workaround:** Install External S-TAP in IBM cloud with OpenShift instead of Kubernetes cluster.
	GRD-43912	External S-TAP may hang when importing or exporting non-TLS data. **Workaround:** If all traffic is non-TLS, you can either delete any certificates that are installed on the collector or reinstall External S-TAP without using certificates. For example, from the installation script, set --proxy-secret to null, or, from Kubernetes set the STAP_CONFIG_PROXY_SECRET environment variable to null.
Guardium universal connector	GRD-46471	You cannot upgrade the pre-installed plugins for MongoDB to a newer version. **Resolution:** Available in an upcoming release.
	GRD-46314	Full SQL report shows server IP and client IP as an IPV4 address when traffic is sent over IPV6 or dual collector via filebeat.
	GRD-44481	Universal Connector in 11.3 only supports either IPv4 or IPv6 traffic. It doesn't support a mix of IPv4 and IPv6 traffic. **Resolution:** available in an upcoming release.
	GRD-43262	DB server is listed on the S-TAP control page even after the host entry is removed from the rsyslog.conf file or from the filebeat.yml file. **Resolution:** available in an upcoming release.
	GRD-43764	Shell installation does not check for the mandatory parameter: GUC_GUARD_HOSTS.

		Workaround: Install by using GUI, GIM, or from the command line. Then, update the GUC_GUARD_HOSTS parameter using the command line utility "configurator.sh".
	GRD-45618	A connector is fully configured to connect with the Guardium universal connector, but it does not show in the S-TAP or central manager pages. **Workaround:** Check that the database has activity. The universal connector displays in the pages only when there is active traffic.
	GRD-46069	When you restore an environment to version 11.3 by using the backup and restore method, the Guardium universal connector status is not retained after restore.
	GRD-46137	Parameters are not updated when you install and configure the GIM Guardium universal connector bundle on the datasources. **Workaround:** Update an additional Guardium universal connector parameter by using the GIM Set up by Client.
	GRD-46835	If an SSL certificate is not reloaded, generate an SSL key and certificate by using the command `grdapi generate_ssl_key_universal_connector hostname="<hostname or a wildcard>" overwrite="true"`
	GRD-46865	In Full SQL reports, the runtime parameter DB username might not appear in the search results because an extra space is appended to the end of the username. **Workaround:** Add a space at the end of the username when you query it. Resolution is available in an upcoming release.
	GRD-46937	The S-TAP status page displays an incorrect primary host name in dual and IPv6 environments.
Quick start compliance monitoring	GRD-46159	"View details" shows red S-TAP and AWS PostgreSQL "Ready for policy" displays "Need agents installed" even though the datastream is assigned to a collector and monitoring is enabled.
	GRD-46156	IP address shows up as 0.0.0.0 for Aurora PostgreSQL
Risk spotter	GRD-46278	Reports cannot be viewed by a user after an upgrade. **Workaround:** 1. Log in to Guardium as accessmgr or another role with permissions to modify roles. 2. Click **Role Browser** and **Manage Permissions** of the user. 3. From the drop-down list, select Reports. 4. If "Active Risk Spotter - Risky User" is listed in the filter of Inaccessible items, move it to Accessible items. 5. Save the permissions.
	GRD-46274	When you upgrade Guardium sequentially from 11.1 to 11.2 and then to 11.3, risky users that are assigned to a user role before the upgrade, appear as 'Not Assigned' after the upgrade. **Resolution:** Available in an upcoming release.

Sniffer	GRD-41797	For Amazon Aurora MySQL and PostgreSQL Database Activity Streams, when there is a SQL error, the SQL statement is not available and shows up as "ERROR" for "Exception"."SQL_STRING". **Resolution:** This issue is expected to be fixed by Amazon in a future release.
	GRD-47303	You must add the updated Microsoft Azure TLS certificates to the tomcat keystore to avoid encountering an “Unknown issue” status error in your Insights Azure connection. Add the certificates by using the CLI command `store certificate keystore trusted`. For more information, see Certificate CLI commands.
S-TAP and GIM dashboard	GRD-46457	The filter value is not removed during a refresh. **Workaround:** Before the refresh, manually remove the filter by clicking on "Remove" link.
Upgrade	GRD-46219	When you upgrade from Guardium 11.0 or 11.1 to 11.3, the following command line parameters are restored to default values: fipsmode, gui session timeout, and disable_deprecated_protocols. **Workaround:** use the following CLI or API commands to reset the values: - store system fipsmode on - store gui session_timeout 1800 - grdapi disable_deprecated_protocols force=true Note: The values are preserved if you upgrade from 11.2 to 11.3 using the backup and restore method. After you restore to 11.3, reboot your Guardium system for the FIPS mode to stay enabled.
	GRD-45858	Active threat analytics cases that are assigned to a user role before upgrade are not escalated after an upgrade.
	GRD-45771	Guardium Insights is compatible with Guardium versions 10.6, v11.1 and above. When you upgrade from Guardium version 10.6 to 11.0, 11.1, or 11.2, the Guardium Insights export datamart parameters are lost and datamarts are not exported. **Workaround:** After you upgrade to Guardium 11.0, continue the upgrade process until you are at version 11.1 or 11.2. Then install the corresponding ad-hoc patch with the fixes for Guardium Insights v2.5. After the ad-hoc patch is installed, disable streaming from Guardium Insights and then re-enable streaming. The Insights export datamart parameters are then repopulated and datamarts are exported. Note: This issue does not occur when you upgrade your Guardium 11.1 or 11.2 systems with the latest patch to 11.3.
	GRD-46681	After switching to backup central manager, the new central manager’s, GUI is sometimes inaccessible indefinitely. **Workaround:** Restart the central manager to resolve the issue. Note: During the process of switching to a new central manager, the GUI restarts and is inaccessible briefly. This is expected behavior and is not an indication of the issue described above.
Vulnerability Assessment	GRD-46854	When a security assessment uses a user-defined datasource group which is criteria-based and the Datasource type is "All", the security

		assessment and its datasources associations are not displayed on the "Assessment Datasources" report. **Workaround:** Add the datasource group "All datasources" to the security assessment to display the security assessment and its associated datasources.
z/OS	GRD-43135	S-TAP errors occur if all recent maintenance patches are not applied to your z/OS systems versions 2.03 and 2.02.
	GRD-28847	Deployment Health Topology and table for S-TAPs for z/OS sometimes show as red. **Workaround:** Manually track the S-TAPs for z/OS that are disconnected. If you bring down an S-TAP and do not want to see the connectivity in the health calculation, then use the customize option to remove the connectivity.

Bug Fixes

Issue key	Summary	APAR
GRD-45487	StealthBits - FDEC for NetApp huge memory usage	GA17419
GRD-40840	Conflict between Dtrace and S-TAP on Solaris server leading to OS crash	GA17301
GRD-46160	Unable to start S-TAP on TERADATA node after upgrade to TERADATA – S-TAP PID issue	GA17397
GRD-45435	K-TAP.log and K-TAP_install.log filling up /var	GA17389
GRD-45095	In Guardium 11.0p106, the GUI stops working daily because of too many HTTP connections.	GA17398
GRD-44937	Request root cause S-TAP 11.1 on HP 11.31 coredump filling file system	GA17395
GRD-43473	K-TAP 10.6.0.4_r108055 stops capturing the traffic with error: "ktap query handler <HID> stopped running: Bad address"	GA17372
GRD-43127	Exit Library Upgrade from 10.6.0.2_r106973 to 10.6.0.4_r108055 caused DB2 Crash	GA17316
GRD-42399	v10.6 S-TAP ktap_request_hander thread got bad address and traffic stop being captured	GA17093
GRD-45643	Message filling syslog: update_callback_platform: old_softstate 3040238da2000	GA17390
GRD-42731	NPE for all Informix classification jobs following 11.2 upgrade	GA17285
GRD-41313	App Debug is turned on by java classes without customer awareness	
GRD-41673	FULL_SQL for SESSION from SOURCE_PROGRAM: ORACLE 64-Bit Client are not captured	GA17255
GRD-42034	IBM Security Guardium v11.1: openssl connection does not display the full CA trust chain after installing patch P106	GA17296
GRD-42973	Windows S-TAP parameter "ADDITIONAL_SQLGUARD_IPS" not updated at the GIM Server GUI when Managed Units are allocated by the Enterprise Load Balancer	GA17295
GRD-45323	A-TAP stop monitoring bequeath traffic after reboot.	GA17417
GRD-37281	How to Unload K-TAP without uninstalling S-TAP	GA17125
GRD-45732	Fixed an issue where not all Guardium hosts are displayed in S-TAP control when WINSTAP_LOAD_BALANCER_NUM_MUS has a large value	GA17405
GRD-41969	TLS 1.1 or lower is not disabled at port 8983	GA17305
GRD-42604	Unable to login via GUI	GA17351
GRD-41037	Adhoc DB is missing GDM_SESSION	GA16978
GRD-42381	Oracle Database slow logins	GA17284
GRD-40756	Instance discovery fails to discover on AIX/Oracle	GA17263
GRD-43601	Local build failure - ktap_108838: Unknown symbol _mcount (err 0)	

GRD-43701	11.2 Squid HTTP Proxy available exposure on some Guardium appliances	GA17338
GRD-42243	New installation of Win S-TAP V11.0.1.68 fails due to a file under 'Staging' is used by another process	GA17328
GRD-44391	FDEC for NAS - Scan doesn’t finish	GA17348
GRD-42894	Inconsistent results for 'Task Description' in the Job Queue Log	GA17277
GRD-41536	NO_AUTH and SYSTEM__ users randomly, very often for MongoDB	GA17361
GRD-37874	V11 || CONFIG RESTORE || GUI certificate is not restored	GA17306
GRD-43557	v11.2 PostgreSQL custom database field resets to PostgreSQL before a scan	GA17307
GRD-46033	Guardium gdmmonitor-mss.sql error on SQL 2014	GA17396
GRD-45328	WARNING: attaching to shmem[10] of 20 failed Error opening shared memory area errno=2 err=8	GA17367
GRD-43561	V11.1 Hardware Appliances || Unable to setup HA port ens2f1	GA17194
GRD-43652	Backslash prohibited in 11.2 FTP Username field	GA17317
GRD-45419	SmartCard enabled, actively working and get a popup message to extend session or terminate session.	GA17370
GRD-45420	Instance discovery fails to discover on AIX/Oracle (TS003601394/STAPLES INC.)	GA17263
GRD-45422	v11.2 Test_Exceptions and Test_Detail Exceptions Truncate Explanation Column	GA17386
GRD-45717	STAP 10.6.0.6_r109098 - after db2 failover No db2 shared memory traffic captured, unless STAP restarted	GA17187
GRD-41912	Erroneous message in jobqueue.log stating tomcat memory use at the time nanny restarts classifier process	GA17350
GRD-44055	java.lang.NoClassDefFoundError: javax.xml.rpc.Service error in GuardiumFAM.log (Windows FAM Crawler V11.2.0.134)	GA17406
GRD-44700	Empty OSUser on FAM Activities	GA17402
GRD-42385	K-TAP lock may cause delay when there is too many threads configured on DB2 side	GA17280
GRD-41166	GIM client doesn't switch to GIM secondary server (where certificate is valid) when Primary GIM server certificate expires	GA17326
GRD-42208	S-TAP Autokill Doesn't Disable S-TAP After Reaching Threshold of Kills in Hour	GA17331
GRD-43785	High System CPU usage while running stress test.	GA17378
GRD-44511	V11.x || GIM module upload cannot be imported || absolute path included in the uploaded module	GA17356
GRD-45579	Big Number of Database Connections since Guardium Oracle Unified Audit	

GRD-41128	IBM Guardium v11.1 Data Classification Process Tasks Finishing with Errors: java.lang.NullPointerException	GA17248
GRD-43318	Missing root shell activity from the Guardium user activity domain for V11.x	GA17309
GRD-40560	Uploading data into ENTERPRISE_NO_TRAFFIC errors when using IPv6	GA17261
GRD-41405	VA Scan report shows the DB Name as blank	GA17234
GRD-41537	v11.1 || Group created is not visible in Query-Report Builder	GA17254
GRD-42157	Unable to run any network related cli command on Collector - COLL05GUARDIUM	GA17290
GRD-43166	set guiuser doesn't support radius authentication	GA17313
GRD-43938	Error when integrating ServiceNow with Guardium v11.1	GA17323
GRD-44820	v11.2 SmartCard Login Repeats Splash Screen on MCs	GA17422
GRD-38387	CCB - Problem restoring data from AWS	GA17209
GRD-43600	Entitlement report don't populate results.	GA17335
GRD-36065	Exclusion list not working	GA17155
GRD-44727	V11.2 || "Guardium Job Queue" || "Stop Job" not working as expected	GA17357
GRD-44825	Documentation: For MongoDB, OS User is not sent as part of the login packet	
GRD-40495	Compliance Summary Page hangs in version 11.1	GA17219
GRD-41552	Command "revoke all privileges on DB from User" in Oracle not captured	GA17253
GRD-28887	VA Scan of particular MS SQL Test sometimes is Halted	GA16957
GRD-38690	Unit Util status -1	GA17278
GRD-42471	Excluding SELECT statement from nest queries	GA17336
GRD-42689	Audit Result PDF in email does not show DIFF output	GA17333
GRD-46775	Predefined Database Disk Space Alert incorrectly uses 'per report' threshold	GA17324
GRD-42566	Include entire LOAD_BALANCER_EVENTS table dump in enterprise_load_balancer_issues must gather	
GRD-45937	Documentation: Supported methods to download records for Distributed-Immediate reports	
GRD-41404	11.1 False Positive - 2614 - Ensure the Windows OS Network Time Protocol (NTP) is enabled	GA17245
GRD-44717	No alerts are sent when Users get added from Scheduled LDAP Job	GA17403
GRD-42209	Allow overriding Guardium user role membership when users are exported VIA LDAP	GA17270
GRD-40525	Issues with Guardium VA for DataStax Cassandra	GA17262
GRD-44189	MUs and STAPs that have different time zone with CM showing blue status (unavailable) in Deployment Health Topology	GA17337

GRD-46187	Adding SQLGUARD_IP by "Set Up by Client" / "S-TAP Control" may fail when Windows GIM and S-TAP were installed using consolidated installer	GA17409
GRD-43502	Guardium 11 the datetime change is lost after restart system	GA17308
GRD-45073	v11.2 Assessment Datasources Report is missing Datasource Type for Group Datasources	GA17411
GRD-43791	v11.2 mysql disk notification configured incorrectly by default	GA17324
GRD-45228	Unable to restore data from FTP - Invalid username	GA17375
GRD-45064	Can't save a cloned query when deleting the IN GROUP condition, "error in query condition section, please fill all the fields"	GA17363
GRD-44593	Guardium defined roles NOT to be overridden for users imported from LDAP	
GRD-44047	FSAAConfig.xml parameter MaxFileSizeLimitValue doesn't exist in config file	GA17399
GRD-41268	Failures of import and other aggregator jobs don't alert, if another aggregator process is running	GA17320
GRD-44542	Guardium No traffic received from a particular S-TAP (force_tap_ip does not work)	GA17387
GRD-42053	Documentatiom: Add clarity to the "Ignore S-TAP Session" section about how "Session Ignored" is interpreted.	
GRD-41243	Guardium S-TAP does not work if there are more than 50 DB instances	GA17246
GRD-43613	Confirmation of v11 DB2-Exit procedures	
GRD-42558	Document parameters allowed during STAP upgrade	
GRD-41511	STAP_TAP_IP changed from hostname to a link-local address after upgrade	GA17366
GRD-41379	Db2 exit health check script generates error with correct db2 exit setup	GA17238
GRD-43274	Improve documentation for wait_for_db_exec	
GRD-42904	The width of the "version" columns for GIM modules may not be sufficient for custom bundles.	GA17302
GRD-41370	Support GIM Installation in non-English environment - Spanish	
GRD-45621	UNIX-STAP - details regarding buffer_nmap_file	GA17382
GRD-42302	Error "Host error: invalid host" happened when configuring more than 1 Alternative IP in STAP control	GA17265
GRD-45066	Add ATAP activation for Oracle on Linux cluster to KC	
GRD-38388	Guardium running Zone Transfer against DNS	GA17289
GRD-38867	Error encountered when trying to install GUI Certificate	GA17230
GRD-39983	Customer request support for modified gdmmonitor-ora.sq script for AWS RDS Oracle database	GA17388
GRD-24755	Restore config is not restoring configuration for remote log	
GRD-43856	Domain user not passed to drill-down reports	GA17365

GRD-44873	Not able to export dashboard when dashboard name includes single quote (')	GA17373
GRD-37027	Add 'Days not archived or exported' predefined report	
GRD-40049	"Use of uninitialized value $ENV{"TERM"}..." when running CLI commands	GA17202
GRD-32731	Application User Translation not working for an Oracle EBS Cluster with multiple VIPs	GA17001
GRD-44340	User Interface Tab and "Search for Data Activity" Appear in MU GUI when QS is disabled in v11.2	GA17349
GRD-41818	grdapi schedule_job InstallPolicy does not install the specified policy	GA16971
GRD-42019	Failure to upload Oracle datasources from CSV	GA17325
GRD-41877	Custom Tables related to entitlement reports for Oracle need fields enlarged to 128 characters	GA17304
GRD-43725	Include "show system ipmode" in must_gather diagnostics	GA17321
GRD-41814	GIM needs to automatic fill timestamp for conf file if missing	
GRD-43007	Ability to bulk update connection strings for Informix Datasources	
GRD-44333	Include guard-outliers_detection.log in must gather datamining_issues	
GRD-44207	patch_install issues must gather should include dmidecode.txt file	
GRD-38535	System Monitor - eg Request Rate "Graphical View" does not show correct data points after login and pick "Graphical View" (if the main view is "Report Type : Chart" to start with)	GA17167
GRD-42807	Test Expression Button in Query Builder Always returns Expression Invalid	GA16991
GRD-45731	Data Integrity issue while modifying Classification Rules in Classification Policy under Discovery Scenarios	GA17394
GRD-30799	GIM uninstall doesn't clean GIM services properly	GA16953
GRD-38414	Request Rate "Tabular view" does not "order by" when click on Timestamp if the main view is "Report Type: Chart”	GA17167

Security Fixes

Issue key	Summary	CVEs
GRD-46003	PSIRT: 203123, 143943, 203931, 209643, 213856, 216342, 220564, 221974, 222039, 223217, 224170	CVE-2019-15807 CVE-2019-19046 CVE-2019-19055 CVE-2019-19056 CVE-2019-19062 CVE-2019-19524 CVE-2019-20636 CVE-2020-8647 CVE-2020-8649 CVE-2020-10690 CVE-2020-10732 CVE-2020-10751 CVE-2020-10942 CVE-2020-12653 CVE-2020-12654 CVE-2020-12826
GRD-44276	PSIRT: 222102 - IBM SDK, Java Technology Edition Quarterly CPU - July 2020	CVE-2019-17639 CVE-2020-14556 CVE-2020-14577 CVE-2020-14578 CVE-2020-14579 CVE-2020-14581 CVE-2020-14583 CVE-2020-14593 CVE-2020-14621
GRD-43941	PSIRT: 232566 Shell injection vulnerability in guard_filetransfer.pl with ftp command	CVE-2020-4688
GRD-43478	PSIRT: 232791, 232792, 232794, 232796, 234182 - SE - Customer Pen Test	CVE-2020-4678 CVE-2020-4679 CVE-2020-4680 CVE-2020-4681 CVE-2020-4689
GRD-40895	PSIRT: 215639 Oracle MySQL April 2020 CPU - connector update needed	CVE-2020-2934
GRD-40894	PSIRT: 215639, 215870 Oracle MySQL April 2020 CPU v10_6	CVE-2019-1547 CVE-2019-15601 CVE-2019-5482 CVE-2020-2752 CVE-2020-2760 CVE-2020-2763 CVE-2020-2765 CVE-2020-2780 CVE-2020-2790 CVE-2020-2804 CVE-2020-2806 CVE-2020-2812

		CVE-2020-2814
GRD-36635	PSIRT: 205875 SE - Pen Testing 2019 - Information Exposure	CVE-2020-4189
GRD-43179	SE - Nessus scanning 11.2 - upgrade emacs-filesystem	CVE-2017-1000476 CVE-2017-11166 CVE-2017-12805 CVE-2017-12806 CVE-2017-18251 CVE-2017-18252 CVE-2017-18254 CVE-2017-18271 CVE-2017-18273 CVE-2018-10177 CVE-2018-10804 CVE-2018-10805 CVE-2018-11656 CVE-2018-12599 CVE-2018-12600 CVE-2018-13153 CVE-2018-14434 CVE-2018-14435 CVE-2018-14436 CVE-2018-14437 CVE-2018-15607 CVE-2018-16328 CVE-2018-16749 CVE-2018-16750 CVE-2018-18544 CVE-2018-20467 CVE-2018-8804 CVE-2018-9133 CVE-2019-10131 CVE-2019-10650 CVE-2019-11470 CVE-2019-11472 CVE-2019-11597 CVE-2019-11598 CVE-2019-12974 CVE-2019-12975 CVE-2019-12976 CVE-2019-12978 CVE-2019-12979 CVE-2019-13133 CVE-2019-13134 CVE-2019-13135 CVE-2019-13295 CVE-2019-13297 CVE-2019-13300 CVE-2019-13301 CVE-2019-13304 CVE-2019-13305

		CVE-2019-13306 CVE-2019-13307 CVE-2019-13309 CVE-2019-13310 CVE-2019-13311 CVE-2019-13454 CVE-2019-14980 CVE-2019-14981 CVE-2019-15139 CVE-2019-15140 CVE-2019-15141 CVE-2019-16708 CVE-2019-16709 CVE-2019-16710 CVE-2019-16711 CVE-2019-16712 CVE-2019-16713 CVE-2019-17540 CVE-2019-17541 CVE-2019-19948 CVE-2019-19949 CVE-2019-7175 CVE-2019-7397 CVE-2019-7398 CVE-2019-9956
GRD-43147	SE - Nessus scanning 11.2 - upgrade file	CVE-2018-10360
GRD-43146	SE - Nessus scanning 11.2 - upgrade gettext	CVE-2018-18751
GRD-43145	SE - Nessus scanning 11.2 - upgrade glibc	CVE-2016-10739
GRD-43144	SE - Nessus scanning 11.2 - upgrade dhcp	CVE-2019-6470
GRD-43143	SE - Nessus scanning 11.2 - upgrade bind	CVE-2018-5742
GRD-43140	SE - Nessus scanning 11.2 - upgrade ntp	CVE-2018-12327
GRD-43139	SE - Nessus scanning 11.2 - upgrade libicu	CVE-2020-10531
GRD-43138	SE - Nessus scanning 11.2 - upgrade libjpeg-turbo	CVE-2016-3616 CVE-2018-11212 CVE-2018-11213 CVE-2018-11214 CVE-2018-11813 CVE-2018-14498
GRD-43137	SE - Nessus scanning 11.2 - upgrade libcgroup	CVE-2018-14348
GRD-43136	SE - Nessus scanning 11.2 - upgrade libarchive	CVE-2017-14503 CVE-2018-1000877 CVE-2018-1000878 CVE-2019-1000019 CVE-2019-1000020
GRD-43102	SE - Nessus scanning 11.2 - upgrade libssh2	CVE-2019-3855 CVE-2019-3856 CVE-2019-3857 CVE-2019-3863

GRD-43101	SE - Nessus scanning 11.2 - upgrade expat	CVE-2015-2716
GRD-43100	SE - Nessus scanning 11.2 - upgrade elfutils	CVE-2018-16062 CVE-2018-16402 CVE-2018-16403 CVE-2018-18310 CVE-2018-18520 CVE-2018-18521 CVE-2019-7149 CVE-2019-7150 CVE-2019-7664
GRD-43099	SE - Nessus scanning 11.2 - upgrade bash component	CVE-2019-9924
GRD-43098	SE - Nessus scanning 11.2 - upgrade xorg-x11 and libX11 components	CVE-2018-14598 CVE-2018-14599 CVE-2018-14600 CVE-2018-15853 CVE-2018-15854 CVE-2018-15855 CVE-2018-15856 CVE-2018-15857 CVE-2018-15859 CVE-2018-15861 CVE-2018-15862 CVE-2018-15863 CVE-2018-15864
GRD-43097	SE - Nessus scanning 11.2 - upgrade SDL component	CVE-2019-14906
GRD-43095	SE - Nessus scanning 11.2 - upgrade systemd components	CVE-2018-15686 CVE-2018-16866 CVE-2018-16888
GRD-43093	SE - Nessus scanning 11.2 - Upgrade curl component	CVE-2018-16842
GRD-43074	SE - Nessus scanning 11.2 - upgrade binutils	CVE-2018-12641 CVE-2018-12697 CVE-2018-1000876
GRD-43071	SE - Nessus scanning 11.2 - upgrade kernel components	CVE-2018-9568 CVE-2018-17972 CVE-2018-18445
GRD-43070	SE - Nessus scanning 11.2 - upgrade http-parser	CVE-2019-15605
GRD-43069	SE - Nessus scanning 11.2 - upgrade ksh	CVE-2019-14868
GRD-43068	SE - Nessus scanning 11.2 - upgrade lftp	CVE-2018-10916
GRD-43067	SE - Nessus scanning 11.2 - upgrade patch	CVE-2018-20969 CVE-2019-13638
GRD-43066	SE - Nessus scanning 11.2 - upgrade polkit	CVE-2018-1116
GRD-43065	SE - Nessus scanning 11.2 - upgrade rsyslog	CVE-2019-17041 CVE-2019-17042
GRD-43064	SE - Nessus scanning 11.2 - upgrade squid	CVE-2020-11945 CVE-2019-12519 CVE-2019-12525
GRD-43063	SE - Nessus scanning 11.2 - upgrade sudo	CVE-2019-18634
GRD-43062	SE - Nessus scanning 11.2 - upgrade linux-firmware	CVE-2018-5383

GRD-43061	SE - Nessus scanning 11.3 - upgrade blktrace	CVE-2018-10689
GRD-43059	SE - Nessus scanning 11.2 - upgrade net-snmp	CVE-2018-18066
GRD-43058	SE - Nessus scanning 11.2 - upgrade nss	CVE-2019-11729 CVE-2019-11745
GRD-43041	SE - Nessus scanning 11.2 - upgrade openssh	CVE-2018-15473
GRD-43040	SE - Nessus scanning 11.2 - upgrade perl-Archive-Tar	CVE-2018-12015
GRD-43039	SE - Nessus scanning 11.2 - upgrade procps-ng	CVE-2018-1122
GRD-43037	SE - Nessus scanning 11.2 - upgrade python	CVE-2018-12207 CVE-2019-0154 CVE-2019-11135
GRD-43036	SE - Nessus scanning 11.2 - upgrade sqlite	CVE-2019-13734
GRD-43035	SE - Nessus scanning 11.2 - upgrade sssd	CVE-2018-16838 CVE-2019-3811
GRD-43034	SE - Nessus scanning 11.2 - upgrade tcpdump	CVE-2018-19519
GRD-43033	SE - Nessus scanning 11.2 - upgrade unzip	CVE-2018-18384
GRD-43032	SE - Nessus scanning 11.2 - upgrade telnet component	CVE-2020-10188
GRD-43031	SE - Nessus scanning 11.2 - upgrade GNOME component	CVE-2019-3820
GRD-42357	SE - OWASP - snakeyaml-1.18.jar need upgrade	CVE-2017-18640
GRD-42351	SE - OWASP - spring-security jars need upgrade	CVE-2020-5408
GRD-42345	SE - OWASP - HiveJDBC41.jar need upgrade	CVE-2019-12086
GRD-42342	SE - OWASP - MySQL Connector need upgrade	CVE-2020-2934
GRD-42340	SE - OWASP - MySQL Connector need upgrade	CVE-2020-2934
GRD-42339	SE - OWASP - KC jars need upgrade	CVE-2019-7611
GRD-42332	SE - OWASP - Kafka jars need upgrade	CVE-2017-5645 CVE-2018-10237 CVE-2020-11612 CVE-2019-17571

Sniffer Updates

The latest sniffer patch that is included in 11.3 is v11.0p4016.

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 11.3.
Installation of sniffer patches will automatically restart the sniffer process.

Snif Update	Issue key	Summary	APAR
11.0p4007		https://delivery04.dhe.ibm.com/sar/CMA/IMA/08xnl/0/Guardium_v11_0_p4007_sniffer_update_release_notes.pdf	
11.0p4009	GRD-42786	After upgrading to p4052, sniffer stalls during policy validation.	GA17293
	GRD-42565	Sniffer consumes high CPU resources and crashes	GA17292
	GRD-42520	Session and log full details are not captured for Oracle Exadata	GA17291
	GRD-41928	Sniffer p4046 parser errors occur while executing alter view commands: "unexpected token: with" and "unexpected token: null"	GA17260
	GRD-41834	OS Username and DB Username not getting captured for HP-Vertica.	GA17276
11.0p4010	GRD-42786	After upgrading to 10.0p4052, sniffer stops during policy validation.	GA17293
	GRD-42565	Sniffer consumes high CPU resources and crashes	GA17292
	GRD-42520	Session and log full details are not captured for Oracle Exadata	GA17291
	GRD-41928	Sniffer p4046 parser errors occur while executing alter view commands: "unexpected token: with" and "unexpected token: null"	GA17260
	GRD-41834	OS Username and DB Username not getting captured for HP-Vertica.	GA17276
	GRD-44016	v11p4009 Sniffer restarting continuously	GA17330
	GRD-43505	TCP sessions are not logged by Guardium for Oracle Exadata	GA17327

	GRD-42471	Excluding SELECT statement from nest queries	GA17336
	GRD-38561	GDM_ERROR filling up with Sybase unexpected token parser errors	GA17190
	GRD-41174	Missing traffic for SAP Batch job	GA17256
	GRD-40803	DB Command "for row in" verb not getting recorded	GA17258
11.0p4016	GRD-44921	PostgreSQL bind variables are not logged	GA17381
	GRD-43568	Parser_error on Guardium 11.1	GA17315
	GRD-43542	WINSTAP 11.1.0.164 || Capturing strange characters in SQL Field	GA17393
	GRD-43505	TCP sessions are not logged by Guardium for Oracle Exadata	GA17327
	GRD-42520	Session and log full details are not getting captured for Oracle Exadata	GA17291
	GRD-41755	DB2 explain plan of a delete statement executed from Data Studio is being logged as a delete	GA17376
	GRD-41536	NO_AUTH and SYSTEM__ users randomly, very often for Mongodb.	GA17361
	GRD-41289	Guardium v11.1 - Unable to add z/OS ciphers	GA17379
	GRD-41213	Invalid DB Users captured for MongoDB	GA17339
	GRD-45479	Parser Error / Postgres CREATE ROLE with CONNECTION LIMIT -1	GA17188
	GRD-42874	Records affected showing -1 randomly	GA17383
	GRD-40396	The bind value for the column PARTNER_GUID has scrambled characters in SAP Oracle statement.	

Deprecated functionality

Platforms

- Ubuntu 10.04 is no longer supported.
- Support for HP-UX 11.11 and 11.23 ends in an upcoming release.
- Starting with Guardium V11.4, UNIX S-TAP no longer supports AIX 6.
- Red Hat extended support for RHEL 5 ended in November 2020. Guardium will continue supporting RHEL 5 until September 2021.

API Commands

- add_job_dependency
- delete_job_dependencies
- list_job_dependencies_tree
- list_suggested_job_dependencies
- modify_job_dependency
- show_job_dependency_execution_profile
- model_exposure

CLI parameters

The SoftLayer option is no longer available in the CLI command `import file`.

Protocols

Old	New
File Transfer Protocol (FTP)	Secure File Transfer Protocol (SFTP)

Vulnerability Assessment Tests

The “Weak Passwords Are Screened” Vulnerability Assessment test is replaced with five new tests to enforce password complexity for Oracle by using password verification.

Old test	New test
Weak Passwords Are Screened	The DBMS must support organizational requirements to enforce minimum password length
	The DBMS must support organizational requirements to enforce password complexity by the use of one or more lower-case characters
	The DBMS must support organizational requirements to enforce password complexity by the use of one or more numeric characters
	The DBMS must support organizational requirements to enforce password complexity by the use of one or more special characters
	The DBMS must support organizational requirements to enforce password complexity by the use of one or more upper-case characters

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 11.3
https://www.ibm.com/support/pages/node/6334261

Supported platforms database for Data Activity Monitoring 11.3
https://www.securitylearningacademy.com/mod/data/view.php?id=19457

Supported platforms for file discovery, classification, and monitoring 11.3
https://www.ibm.com/support/pages/node/6245402

Appliance Technical Requirements 11.3
https://www.ibm.com/support/pages/node/6335779

IBM Security Learning Academy
securitylearningacademy.com

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