Release Notes

==========

Product: IBM Security Guardium

Release version: Guardium v11.1

Completion date: 3 December 2019

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, mainframes, IBM Z®, 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

Download Guardium v11.1

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 that 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 STAP and GIM on Fix Central. If you need assistance to find a product on Fix Central, contact Guardium support.

Installing Guardium v11.1

Guardium V11.1 is available as an ISO product image on Passport Advantage.

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

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

Upgrading to Guardium v11.1

You can upgrade to Guardium v11.1 from any Guardium system that is running on v10.0p11001 or above.

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

Health Check patch

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

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

The v11.0 Health Check patch 9997 must be successfully installed in the last seven days before you install the Guardium v11.1 GPU. If the Health Check patch isn't installed as recommended, the v11.1 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 directly connected or through 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. 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 restart the system during the internal database upgrade. For real-time details on the system patch installation, use the CLI command **show system patch status**. For v11.1, you can run this command in the CLI recovery mode, but only after a certain point in the installation when the CLI command gets added.

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

Previously installed patches

When you upgrade from a Guardium v10.x GPU (such as v10.1.3 or later) to Guardium v11.0, the v10 patches that were previously installed are no longer visible in the "Installed Patches" screen in the GUI.

New Features and Enhancements

UI-Based Enhancements

Active Threat Analytics

Active threat analytics identifies many more potential security breaches than in V11.0. You can now assign cases directly to ServiceNow from the Active threat analytics page. For more information, see Active threat Analytics.

Active Threat Analytics Setup

You can enable Active Threat Analytics across your entire system with one click in the new Active Threat Analytics Setup page. The Setup page incorporates the previous Outlier mining status and adds the new Threat finder configuration. When required, you can also enable on individual Guardium systems. New functions in the DAM outlier mining table include: an indication of the remaining training time; free-text filter of the units; new Outlier mining enable or disable history window, selecting all visible rows on one click. For more information, see Active threat analytics setup.

Application Data Monitoring

The smart assistant for application data monitoring adds support for hierarchically grouping databases into applications and industries. This feature enables you to organize databases into meaningful applications and quickly configure those applications for monitoring. Support is provided both for predefined monitoring policies that are aligned with industry standards like GDPR and for custom monitoring user-defined policies. For more information, see Smart assistant for compliance monitoring.

Basic Data Security Monitoring Policy

The basic data security monitoring policy monitors SQL traffic right out of box. Using predefined groups of privileged users, privileged commands, and error codes for some of the most common use cases, the basic monitoring policy provides rules that address common data access and attack patterns. For more information, see Basic data security monitoring policy.

Compliance monitoring

The Smart Assistant for Compliance Monitoring adds support for custom policies and the California Consumer Privacy Act (CCPA). For more information, see Smart assistant for compliance monitoring.

Database discovered instances rules

You can configure Guardium to discover databases that are created on both Windows and UNIX systems. In many cases, you want Guardium to create and run inspection engines on all newly discovered databases. However, there are scenarios in which you want control when and how Guardium creates new inspection engines. In these cases, **Database Discovered Instances Rules** provides a way to manage inspection engine creation. For more information, see Database discovered instances rules.

External Ticketing Systems

Integrate Guardium with ticketing systems like Service Now to help run your service desk operations. This integration allows Guardium to open tickets, send information that is related to tickets, and close tickets on the external ticketing system. For more information, see Configure an external ticketing system.

Group builder
The group builder grid now indicates the children of hierarchical groups, which are used in the policies and queries that their parent groups are used in. This feature enables you to get a complete view of dependencies and group usage across your environment.

Investigation dashboard: Sankey diagram
The investigation dashboard has a new chart: the Sankey diagram, introducing a new paradigm for viewing data. It is a useful graph for investigating filtered data, for example, of a specific alert, outlier, report, or threat. For more information, see Using the Sankey chart.

Policy analyzer
Policy analyzer supports drill down into each rule to view sql log details or policy violation details. You can quickly see the values (such as client ip, db user, source program, server ip and db type) that caused it to fire. Additionally, ad hoc process scheduling enables you to view and cancel scheduled ad hoc analyses.

Policy builder
New tuples for Service/Object and Db/Object are now supported for data activity monitoring policy access rules. You can use tuples to separate environments and databases with sensitive objects from those with non-sensitive objects.

Guardium checks and warns of common errors during policy creation and editing. The new checks include warnings for continue to next rule, conflicting actions, and extrusion rule prerequisites.

Risk Spotter
The Risk Spotter UI has a number of enhancements. The risk indicators include the Threat Analytics score. Configuring and enabling the Risk Spotter Dynamic Auditing policy is simplified. For more information, see Risk Spotter.

Oracle Unified Auditing
Use Oracle Unified Auditing to audit Oracle traffic without installing K-TAP or A-TAP on the database. For more information, see Configuring an SQL connection for Oracle Unified Auditing.

Query-Report builder enhancements
When you open the Query-Report builder, and no domain is selected, the query list includes all queries in all the domains. You can search for a query using the free text filter. See Using the Query-Report Builder.

Cloud Deployment

Event hub streaming for Azure
Use database activity monitoring to provide cloud database service protection for Azure event hubs. Guardium u event hub monitoring for SQL Azure and Cosmos data stores. For more information, see Cloud database service protection Azure setup.

Cloud database service protection for Amazon AWS
When you use database activity monitoring with Amazon, you can specify consumer groups to determine whether multiple consumers have a shared or separate view of this data stream. For more information, see Discover and configure AWS data streams.

AWS authentication
Guardium supports three types of AWS authentication. Security Credentials, IAM Role, and IAM Instance Profile. For more information, see Define a Guardium cloud DB service account.

External S-TAP
External S-TAP now supports failover, firewalls, and many S-TAP policies, including S-GATE and S-TAP Terminate. In addition, External S-TAP is supported under TLS 1.3. You can use External S-TAPs with several new databases, including Db2 Warehouse, MongoDB Atlas, and RedShift.

Guardium Installation Manager (GIM)

Windows GIM interactive installer supports custom certificates
When you install the GIM client in both standard mode and in listener mode on a Windows server, you can specify a custom key, certificate, and CA. In the Setup Type window, select Customized certificates. Then, in the optional GIM listener mode configuration, enter the Key, Certificate, and CA File names. For more information, see Installing the GIM client on a Windows server and Create and manage custom GIM certificates.

Vulnerability assessment

Vulnerability Assessment (VA) supports DataStax Enterprise (DSE) Cassandra for NoSQL databases. VA can be deployed to detect and correct vulnerabilities on all nodes for DSE clusters. New Configuration Auditing System (CAS) tests and Java-based tests are available on the Guardium system. New Common Vulnerabilities and Exposures (CVE) and query-based tests are available through quarterly DPS reports.

The severity of Guardium Common Vulnerabilities and Exposures (CVE) tests are updated to reflect the severity score of the Common Vulnerability Scoring System (CVSS) v3.0. CVE severity is classified into critical, major, minor, caution, and info.

A security assessment can be exported without the datasource. An assessment can be deleted even it is used by an audit task or has results that are attached. For more information, see Deleting an assessment.

You can set up an audit process to run automatically upon the completion of a security assessment. For more information, see Creating an assessment.

There are three new VA reports that list assessment tests, datasources, and roles allowed. For more information, see Predefined admin reports.

VA supports the Oracle 12c and the SQL server 2016 CIS benchmark.

Other enhancements

IPV6 support

Guardium supports IPv6 addresses, or both IPv4 and IPv6 addresses for industries that use both protocols in parallel. For more information, see Internet Protocol modes and Enable IPv6.

Hyper-V integration

Support added for Hyper-V integration toolkit. For more information, see Hyper-V virtual machine.

CLI accounts

Guardium CLI users can now authenticate by using LDAP. For more information, see User Account, Password, and Authentication CLI commands.

You can now set the passwords for cli and guardcli1 - guardcli5 users from the accessmgr User Browser page. For more information, see How to create a user with the proper entitlements to log in to CLI.

Reports

Guardium adds SAP Hana entitlement reporting and updates to predefined IBM License Metric Tool (ILMT) reports.

Autodiscovery

Autodiscovery now covers all database types that are supported by Windows. New database types include MySQL, PostgreSQL, and Sybase.

Datasources

You can now add connection properties for MongoDB, if required.

The number of concurrent HTTP requests have increased from 150 to 300 for all Guardium web applications

Known limitations and workarounds

Guardium component	Issue key	Description
Backup and restore	GRD-36172	When you restore only DATA or CONFIG, or select not to "preserve the CM to MU relationship" when restoring the central manager: The unit groups are restored from the backup files successfully, but the managed units will be lost. This is expected behavior. The communication will be established when you register the managed units to the central manager.
CAS	GRD-26257	Issues upgrading CAS using GIM from v10.6 or earlier releases. If your site installed CAS by using GIM in v10.6 or earlier, and then you upgrade CAS using GIM, you must delete and then re-create the Template/Datasource mapping after you upgrade, as described in CAS Hosts.
Compliance policies		Compliance policies and basic security policies cannot be installed in the same collector because compliance policies are selective. But Audit trail and other policies are not.
Datamart	GRD-36591	Launching a mapped API from any report menu fails when you use Internet Explorer. **Workaround:** Use Chrome, Firefox, or Edge
	GRD-36204	When you use GBDI on IPv6, you must configure datamarts manually. For more information, see Setting up GBDI with IPv6.
Data set event	GRD-30336	On the Chrome browser, the dropdown might close when you select or deselect a checkbox in the “Dataset event” subfiltering criteria. **Workaround:** Open the dropdown again and continue selecting. The previously selected checkboxes remain checked. The selections are not erased.
Datastreams	GRD-35737	There might be instances in which Azure uses an older TLS protocol for communication. In this case, the event hub cannot connect to Azure and Azure returns an error.

		Workaround: In the Guardium CLI for the central manager, call the GuardAPI enable_deprecated_protocols command. For more information, see the enable_deprecated_protocols API.
Deployment health topology	GRD-35863	When you click the "reset view" link, the nodes sometimes move to the far-right corner and cannot be viewed. **Workaround:** Log out, clear the cache, and log in again to view the nodes.
Ecosystem	GRD-35895	When a backup from v10.6 is restored to v11.1, the applications in the Ecosystem do not get restored. **Workaround:** After you restore the system to v11.1, use the GUI to remove the applications that are currently installed and reinstall them.
	GRD-16690	Guardium apps do not support non-ASCII characters in application name and filenames within the app. **Workaround:** Use ASCII characters only
External S-TAP	GRD-33063	If you run a vulnerability scan on the External S-TAP, the scan might display a number of vulnerabilities that are related to some libraries which are part of the Linux base image. Because External S-TAP does not link to or load those libraries during runtime, those vulnerabilities are false positives and can be ignored.
FAM	GRD-28914	Exception is thrown while enabling FAM deep analysis **Workaround:** install libstdc+.so.5 libraries for 32-bit as described in Requirements for IBM Content Classification Version 8.8: https://www-01.ibm.com/support/docview.wss?uid=swg27020838.
IPv6	GRD-36268	Using a hostname in S-TAPs on IPv6: If the network configuration information on a Guardium collector does not match your DNS information, then you may experience issues when you specify a hostname for the sqlguard_ip parameter during S-TAP installation. **Workarounds:** 1) Correct the network configuration on the DNS and the collector. 2) Do not use a hostname. Instead, specify an IP address for sqlguard_ip.

		The following Guardium features are not compatible with IPv6: Active threat analytics Guardium apps Cloud database protection services The following third-party features and applications might not be compatible with IPv6. For more information, see the official website of the third-party. CyberArk Centera ECS 3.x or later ServiceNow
		Supported back up types: TSM, FTP, SCP, and Amazon S3. Centera is not supported yet.
	GRD-36329	Outlier detection: In an IPV6 or dual environment, distributed reports do not work. Outliers do not work on aggregators running IPv6.
	GRD-36721	External S-TAP: For Guardium v11.0 and v11.1, the External S-TAP server IP can be erroneously reported as the Docker container IP address. Resolution: Planned for an upcoming maintenance bundle
	GRD-36465	IPv6 is not compatible with z/OS versions earlier than 2.3
Outlier mining	GRD-36476	When restoring data from an aggregator to a new system with a different hostname, the new system shows collectors from the source aggregator *and* the collectors on new system. The list of collectors can be seen in the Active threat Analytics Setup>outlier mining. **Workaround:** 1. On each of the old collectors define a data export to a new aggregator 2. Delete the data export (that you just defined). It is not recommended to use restore to a system with a different hostname.
Outliers detection	GRD-36475	When you use backup from a pre v11.0 system and restore to a v11.0 or v11.1 system, a properties file is overwritten with an older version.

		Workaround: 3. Before restoring: Copy all the files from $GUARD_HOME/analytic/setups/, other than files with prefix "user" on the target machine to a location that won't get overwritten. 4. After restoring data from the backup, delete the files in the directory $GUARD_HOME/analytic/setups/, other than files with prefix "user" 5. Copy the files you saved in step 1 (V11.0 (or later) version) to the same directory: $GUARD_HOME/analytic/setups/.
	GRD-36170	Outlier parameters are not restored because they are not part of the backup.
Pre-defined policy	GRD-34491	Beginning v11.1, pre-defined policies or templates cannot be installed. These policies will not be available for installation in the "policy installation" screen. The installed policy must be a user-defined policy or a clone of one of the templates. These policies can be installed from the "security policies" screen. This feature enables the maintenance of pre-defined policies.
Restore backup	GRD-36049	The restore action must include both your data and configuration files. You cannot reinstall your configuration or data files separately. **Workaround:** You can restore your configuration or data files separately on a newly built system.
Risk spotter	GRD-36585	The Create ticket option in the Actions menu for creating a ServiceNow ticket does not function properly in Internet Explorer. **Workaround:** Use Chrome, Firefox, or Edge
	GRD-36443	When you assign a risky user (Actions > Assign risky user) for the first time, an error might occur if the process takes more than a few seconds to complete. An alert with the message "Failed saving results id" is displayed. **Workaround:** Assign the risky user again.

	GRD-36584	Hovering over Latest Risk and Max Risk of the Risky Users table in the Risk Spotter page does not give preview when using Internet Explorer. **Workaround:** Use a different browser.
	GRD-36587	The Policy and related modules section in the Risk Spotter page cannot be expanded, to configure Dynamic auditing policy and check the status of related modules in Internet Explorer. **Workaround:** Use Chrome, Firefox, or Edge
Sankey chart	GRD-36485	Sankey chart does not work on Internet Explorer. **Workaround:** Use Chrome, Firefox, or Edge
Smart assistant	GRD-35587	Compliance policies GDPR and CCPA for z/OS cannot be installed from Smart Assistant **Workaround:** Both GDPR and CCPA can be installed on the managed unit with the “Default - Ignore Data Activity for Unknown Connections” policy by using the install or override option. Install the default policy by going to “Policy Builder for Data”. Select “Default - Ignore Data Activity for Unknown Connections [template]” and clone the policy. Keep the default name and install it. Then go back to Smart Assistant and proceed.
Sniffer	GRD-32319	When you use an A-TAP with Oracle Exadata 18 to make a JDBC connection to the database, you might encounter a situation where the Oracle service name has the wrong value. **Workaround:** If possible, define and use session level rules.
Solr	GRD-30368	Solr is unstable after upgrade. **Workaround:** When upgrading from pre-V10.6 to a later version, run the CLI command *restart gui* on each managed unit.
Upgrade	GRD-36413	The message "Error running create_selfsigned_certificate.pl" is seen in the patch log after upgrading. **Workaround:** No action necessary since this is not an error and it does not impact the upgrade.

Notes on setting up GBDI with IPv6

If you are moving from IPv4 to IPv6 and already have a GBDI instance that is configured to run on IPv4, then, you must update the information for IPv6 by using the following GRDAPI command:

Example:
grdapi datamart_update_copy_file_info destinationHost=[<IPv6 address>]
destinationPassword=<password> destinationPath="/var/lib/sonargd/incoming"
destinationUser="sonargd" transferMethod="SCP" Name="<DataMartname>"

Note: Enclose your IPv6 address in [square brackets] and include the datamart names for each datamart export that was active on IPv4.

You must run this command only on the central manager. The central manager syncs with the managed unit on portal sync.

Bug Fixes

Issue key	Summary	APAR
GRD-30599	TAP_IP will be changed to InfiniBand IP of Oracle Exadata automatically after restart the Oracle Exadata	GA16593
GRD-32791	Find possible cause why tap_ip changed from service IP to boot IP	GA16593
GRD-29592	Custom Query runtime error with DLS enabled	GA16596
GRD-31684	New query builder wouldn't allow to use same attribute twice in the report	GA16622
GRD-31782	Repeated 'populateAccessJob trigger: populateAccessJobGroup.populateAccessJob' alerts	GA16698
GRD-27771	Comment functionality is missing from Query-Report Builder in 10.6	GA16717
GRD-25749	V10.6 | VA_SUMMARY table is not consistent with CLS_PROCESS_RUN	GA16739
GRD-28862	Guardium SharePoint Discovery issue	GA16745
GRD-23382	SNMP test Connection for Alerter->SNMP settings ->Test Connection does not check for UDP connection	GA16820
GRD-25561	After you restart all STAPs, the STAPs connect to the collector or sniffer, but do NOT Appear in the GUI.	GA16824
GRD-31839	Oracle 18c with Solaris V11.4 is missing from Supported DB list in Guardium V11.	GA16829
GRD-33812	Query definition can be saved with invalid value	GA16832
GRD-32145	Customer changes to predefined custom table definitions not persisted after patch installation (DB upgrade)	GA16833
GRD-30293	Assessment Result header truncation	GA16836
GRD-32301	Unable to remove GIM Bundles generates ERR=1321	GA16840
GRD-31789	Changes to STAP directory permissions between V9.5 and V10	GA16841
GRD-32548	Query-Builder: RegEx condition not working in p620	GA16844
GRD-27554	VA assessment takes long time to save	GA16846
GRD-18898	Several issues with report background color behavior	GA16848
GRD-30479	Backup does not work when you use the GUI in Guardium 6 patch 620	GA16849
GRD-34084	Vertical line (pipe) is not available in FTP user	GA16852
GRD-28753	FAM module on CentOS 7.6 leads to system freeze	GA16856
GRD-27282	ATAP activation on Sybase 15.7 causes database timeout: Cannot Connect to Database	GA16860
GRD-29973	How to configure IE for Accumulo?	GA16862
GRD-27363	There is a mismatch in the execution of SQL statements timestamp and the timestamp that is reported	GA16863
GRD-26456	V10.5 | DB Instance Discovery not working as expected	GA16865
GRD-32060	Guardium Group Builder - GUI "Import by query" to get USERS does not give drop down for "IN DYNAMIC GROUP" (Server IP).. and in any case does not populate members when typing in the group name	GA16866

GRD-29681	guardctl gives "-gt: unary operator expected" and "too many arguments" but appears to install ok	GA16867
GRD-28702	ATAP: TERADATA reported a reboot caused for S-TAP agent	GA16868
GRD-29680	STAP r105601 atap_push_packet_append_data caused "signal: 11 SIGSEGV" "code: 2 SEGV_ACCERR" TPA restart initiated by this node, 001-11, for event 10416 gtwgateway Teradata 15.10.07.42 on Linux Suse 3.0.101-0.187.TDC.1.R.0-default	GA16868
GRD-10470	v10 (and v9) sniffer must_gather "Set Members" is BLANK for Policy import - this makes it impossible to know what the policy name is - difficult for Support Engineers	GA16869
GRD-30685	NullPointerException in 548 CLOUDERA MANAGER VA Test	GA16871
GRD-29136	S-TAP IP is changed between one of the host's IPs and host name without control	GA16875
GRD-32277	v10.6 Error 2007 - RestAPI gim_client_last_event	GA16876
GRD-28349	Not logging encrypted Sybase ASE 16.0 SP03	GA16877
GRD-30414	DB2 VA test "Authentication type configuration parameter"	GA16879
GRD-22993	PSIRT 120341 CVE-2018-15473	GA16882
GRD-32029	PSIRT 120341 CVE-2018-15473 for REHL 7	GA16883
GRD-30423	import rules with alert notification removes receiver from the source rule action	GA16886
GRD-30505	STAP Status stays yellow after install and fast_tcp_verdict disabled	GA16887
GRD-32233	Vmware tools can not be installed on v11	GA16889
GRD-32758	Session level policy GUI does not allow blank regex	GA16890
GRD-32558	V11 || CONFIG restore || What happens after restoring CONFIG file ?	GA16891
GRD-32756	V10.6 || SYBASE DB instance discovery not working as expected	GA16892
GRD-33233	XSS in investigation dashboard	GA16894
GRD-33073	Missing exception related attributes in query report builder for non-admin user	GA16895
GRD-35206	Auto Discovery is missing/skipping config on port 49125	GA16897
GRD-32269	STAP 11.0.0.0_r106780 - Database discovery failed to discover actual port for Oracle 18c	GA16897
GRD-30280	Snif thread for STAP properties	GA16898
GRD-33409	Rules in Installed Policy Details Sorted Alphabetically by Policy Description by default	GA16901
GRD-33330	STAP in Synchronize state - For Oracle Only	GA16902
GRD-33522	Incorrect Warning Message on Date Entry	GA16903
GRD-33653	Guardium API Command to Create Data Sources(DS) (grdapi create_datasource) does not contain a "Cluster Name" option for Cloudera Manager DS Type	GA16904
GRD-33885	Audit Process Execution in Guardium v11.0 fails with error: "Guard Report Generator Error: call AT_GET_ALL_FILTERS_CONDITION_OUT"	GA16905
GRD-33072	v8.2/v9/v10/v11 Data Archive failed to be restored into V11 Guardium	GA16909

GRD-32754	Can't delete GIM auto-discovery processes	GA16910
GRD-32642	After Configuring PAM, Key exchange wont allow appliance access	GA16913
GRD-31589	GuardiumSniffer[19177]: garbage collected when find port for |xxxxxxxxxxxxxxxxxxxxxx	GA16914
GRD-31610	Database Disk Space alerter not alerting when threshold is reached. Other alerts are working fine.	GA16915
GRD-35826	CLONE - Not able to use Total Access attribute in query condition	GA16917
GRD-33838	Not able to use Total Access attribute in query condition	GA16917
GRD-33915	Assessment Log - Details field truncating output	GA16922
GRD-34689	Modifications to the "gdmmonitor-mss.sql" script file to provide more meaningful content	GA16924
GRD-33851	gdmmonitor-mss.sql v10.6 and v11 deployment script missing a permission	GA16926
GRD-34069	v10.6 Msg field with is blank for extrusion rules but Full SQL is logged	GA16927
GRD-31951	Have Guardium be able to take a cipher from CLI and add it.	GA16928
GRD-34515	Cannot associate Exclusion Table for VA Scan Test "No OLE Automation Authorizations"	GA16935
GRD-34066	V11 || Vulnerability Assessment Results DIFFERENCE display is incorrect	GA16939
GRD-34625	WINTAP Became Inactive due to a potential GHOST records during ELB related Activity	GA16949
GRD-35489	V11 || Vulnerability Assessment || "Show Test Query" hyperlink pop-up does not have CLOSE (X) button on GUI	GA16951
GRD-35523	V11 || ENTITLEMENT TERADATA || java.sql.SQLException: Data truncation: Data too long for column 'Privilege_or_Role_Name' at row 1 on SQL statement	GA16952
GRD-34493	v10.6 - Policy installation failing with duplicate entry	GA16955
GRD-34666	API error code discrepancy for GIM Bundle install	GA16960
GRD-35028	Duplicate Test Showing Up in a CSV Report	GA16961
GRD-33994	snif process starts after installing patch 4002 on Aggregator unit	GA16962
GRD-35291	V11 || SQLException: [Teradata Database] [TeraJDBC 16.20.00.08] [Error 8028] [SQLState HY000] The LAN message Authentication is invalid. SqlState: HY000 Error Code: 8028	GA16964
GRD-33656	db2diag.log fills up with "OSERR : EMFILE (24) "Too many open files"" when Guardium DB2 Exit on AIX 7	GA16970
GRD-33005	Issue with large pages on s390x processors	
GRD-30743	Tracking concurrent number of HTTP requests in Oleg's threshold script.	
GRD-35551	Port Bug 56565 to v11.1 - STAP crashing with Exit	
GRD-35436	Need a facility to view/get the patch status of all the MUs from the CM	
GRD-30539	Invalid syntax for MSSQL in classifier scan	
GRD-30538	Classifier can't get the correct column name when column name as a space in the first character in MSSQL scan	

GRD-30745	Add functionality for Nanny to trigger tomcat coredump (kill -3 pid) command	
GRD-32173	Win S-TAP keeps sending traffic after receiving Ignore S-TAP session	
GRD-29707	DEBUG_FILE_NAME can create only one directory	
GRD-30175	Previous Windows S-TAP installer log is not backed up	
GRD-28005	Upper case sensitive for STAP group members in Enterprise Load Balancer (ELB) env.	
GRD-29420	GIM Bundle S-TAP installation failing when STAP_TAP_IP configured as a hostname (aka grd-29188 issue)	
GRD-33540	Strip passphrase from private key for "store certificate privatekey"	
GRD-22654	Bundle GIM and bundle STAP installation with invalid failover_sqlguardip is not failing and no error message displayed using consolidated installer	
GRD-36284	MS SQL Datadirect Driver causes some version-based tests to fail	
GRD-36300	Modify DPS process error message to have the file name	GA16977
GRD-35368	v10 - AIX STAP - Causing AIX server crash	GA16994
GRD-36044		GA16984
GRD-32385	Inactive Windows STAP not deleted from old MU at failover	
GRD-36284	MS SQL Datadirect Driver causes some version-based tests to fail	GA16995
GRD-36409	Clarify the parameters required to install GIM client (documentation)	
GRD-35549	Port Bug 56565 to v10.6 - STAP crashing with Exit	
GRD-22642	How to activate ATAP in cluster environment (documentation)	
GRD-33036	Missing description in ‘S-TAP/Z files domain’ (documentation)	
GRD-34261	Kernel signing - Secure boot (documentation)	
GRD-32095	Make stap host name case insensitive in grdapi delete_inactive_stap	

Sniffer Updates

The latest sniffer patch that is included in v11.1 is 4003.

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

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

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

Important:
Any superseding sniffer or security patches must be reinstalled after you install v11.0.
Installation of sniffer patches will automatically restart the sniffer process.

Snif Update	Bug	Summary	APAR
4002		https://delivery04.dhe.ibm.com/sar/CMA/IMA/08fny/1/Guardium_v11_0_p4002_sniffer_update_release_notes.pdf	
4003	GRD-35670	Incorrect Analyzed Client IP reported for encrypted sessions that are connected via Oracle Connection Manager	GA16981
	GRD-35289	V10.5 || SYBASE || Dynamic Stored Procedure || GDM_ERROR filling up with PARSER_ERROR	GA16980
	GRD-33542	Exporting the session level policy. srules file placed under wrong directory	
	GRD-33048	SAP HANA parser errors in v11	GA16938
	GRD-32867	Netstat is showing more established connections from STAP than there are	GA16982
	GRD-32725	SQL captured in Guardium doesn't show HEBREW letters	GA16893
	GRD-31589	GuardiumSniffer[19177]: garbage collected when find port for |xxxxxxxxxxxxxxxxxxxxxx	GA16914
	GRD-30806	Need to know impact of changing kafka_message_max_bytes_settings	GA16979
	GRD-30280	Snif thread for STAP properties	GA16898
	GRD-32106	Some Oracle DatabaseLink SQL being captured as "###############"	GA16822
	GRD-34606	create invalid software tap entries when receive invalid stap config message	

New platforms and databases supported in v11.1

- Cloudera 6.2
- Greenplum 6
- Greenplum 5.19
- Vertica 9.2
- CouchDB 2.3.1
- Informix 14.0 (Not supported in Windows S-TAP)
- Redis
- DB2 11.5

Deprecated functionality

Cleversafe and Softlayer are being deprecated and replaced by IBM Object Storage.

Resources

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

GuardAPI and REST API reference
Guardium API A-Z Reference

System Requirements and Supported Platforms for Cloud and Vulnerability Assessment v11.1
https://www-01.ibm.com/support/docview.wss?uid=ibm11072124

Supported platforms database for Data Activity Monitoring v11.1
https://www.securitylearningacademy.com/mod/data/view.php?id=19457

Appliance Technical Requirements v11.1
https://www-01.ibm.com/support/docview.wss?uid=ibm11071936

IBM Security Learning Academy
securitylearningacademy.com

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