Release Notes

==========

Product:	IBM Security Guardium
Release:	v10.5
Version	Guardium v10.0 GPU 500
Completion Date:	2018-April-27

IBM Guardium offers the most complete database protection solution for reducing risk, simplifying compliance and lowering audit cost.

The IBM Security Guardium data protection solutions covered by these release notes includes:

- IBM Security Guardium Database Activity Monitoring (DAM)
- IBM Security Guardium Vulnerability Assessment (VA)
- IBM Security Guardium File Activity Monitoring (FAM) - Use Guardium file activity monitoring to extend monitoring capabilities to file servers.

The IBM Guardium products provide a simple, robust solution for preventing data leaks from databases and files, helping to ensure the integrity of information in the data center and automating compliance controls.

Contents

Guardium v10.5 Release Notes

Read through this document before you begin installation.

.ISO or GPU

For this Guardium release v10.5, the software is available as a .ISO product image from Passport Advantage and as a GPU from Fix Central.

Passport Advantage

http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm

On Passport Advantage (PA), you will find the Guardium Product Image - ISO file, Licenses, Product Keys, Manuals, etc. You may only download products that you are entitled.

If you need assistance, locating and/or downloading a product from the Passport Advantage site you need to contact the Passport Advantage team at 800-978-2246 (8:00 AM - 8:00 PM EST) or via email paonline@us.ibm.com.

Fixcentral

http://www.ibm.com/support/fixcentral

On Fixcentral, you will find Guardium Patch Update (GPUs), individual patches and the latest versions of STAP, GIM, etc.

If you need assistance finding a product on Fixcentral, contact Guardium support.

General note on upgrading to v10.5

v10.5 (v10.0 GPU 500) can be installed on any v10.x system regardless of whether it was upgraded from v9.x or built from an earlier v10.x image.

The only dependency is that v10.0 Health Check patch 9997 must be successfully installed before installing the Guardium v10.5 (v10.0 GPU 500). See the section below on Health Check patch.

v10.5 (v10.0 GPU 500) includes all previous v10.x fixpacks, security fixes, and sniffer updates, up to and including v10.0 p403 for fixpacks and v10.0 p4032 for sniffer updates. See the sections (starting on page 17) later in this document listing v10.x fixpacks, security fixes and sniffer-related patches. Also check the list of Known Limitations that appears near the end of this document.

Internal database upgraded to MySQL 5.7

To speed up this upgrade, Guardium customers are strongly recommended to backup, archive and purge the appliance data as much as possible.

During GPU upgrades, appliance internal MySQL database will be shut down. Depending on the size of the database, it might take extended time to restart. During this time, CLI access will only be available in recovery mode.

In recovery mode, the following CLI message will display:

```
The internal database on the appliance is currently down and CLI
will be working in 'recovery mode'; only a limited set of
commands will be available.
```

Important: Do NOT reboot the system during the MySQL upgrade.

Use the CLI command, show system patch status, for real-time details on the system patch installation. For v10.5, this command can be run during the CLI recovery mode, but only after a certain point in the v10.0 GPU 500 installation when the CLI command gets added.

Health Check patch

v10.0 Health Check patch 9997 must be successfully installed in the last seven days prior to installing Guardium v10.5 (v10.0 GPU 500). This release will not install without FIRST installing the Health Check patch. The name of this Health Check file is SqlGuard-10.0p9997_HealthCheck_2018_01_16.zip.

Always use the latest and newest version of Health Check patch on Fixcentral, even if you have the Health Check patch from earlier GPUs.

General Notes

- This GPU patch will restart the appliance.
- Installation needs to be performed/scheduled during the "quiet" time on the Guardium appliance to avoid conflicts with other long-running processes (such as heavy reports, audit processes, backups, imports and so on).
- Purge as much unneeded data as possible to make installation easier.
- If the downloaded package is in .ZIP format, customers are required to unzip it outside Guardium appliance before uploading/ installing it.
- When this patch is installed on a collector appliance, make sure that the patch is also installed on the corresponding aggregator appliance. Do this to avoid aggregator merge issues.
- Installation should be across all the appliances: Central Manager, aggregators and collectors.

Note on Overwrite

v10.5 (v10.0 GPU 500) will overwrite any v10.0 Sniffer update patch greater than v10.0 patch 4032.

Be sure to re-install any v10.0 Sniffer update patch greater than v10.0 patch 4032 after installing v10.5 (v10.0 GPU 500).

Installing or upgrading to 10.5 Windows S-TAP

Fresh install of v10.5, no reboot required

Upgrading from v9 to v10.5, no reboot required

Upgrading from v10.0 and build lower than 83909, reboot is required

Upgrading from v10.1.x (revisions lower than Windows STAP v10.1.22.16), reboot is required

New for 10.5 features/functions and enhancements

v10.5 introduces the following new capabilities, depending on the product you have installed:

GUI changes

- The **GIM set up by client tool** streamlines software installation by identifying client-module incompatibility and simplifying parameter management.
  Manage > Module Installation > Set up by Client
- The **group builder** allows you to populate groups from a variety of new sources while providing at-a-glance information about group membership and where groups are used in policies and queries.

New features and enhancements

- Use the **Guardium Ecosystem** to extend and enhance your current Guardium deployment with new data and ready-to-use use cases.

  Guardium apps are the centerpiece of the ecosystem. A Guardium app is a means to augment and enrich your current Guardium system with new data and functionality. You can download and install other shared apps that are created by IBM, its Business Partners, and other Guardium customers.

  You create your own apps from Guardium by using the Guardium GUI Application Framework software development kit (SDK). You can then package the app and reuse it in other Guardium deployments. You can share your app on the IBM Guardium App Exchange portal (https://exchange.xforce.ibmcloud.com/hub/).

  Notes:

  - Use one app on the Central Manager and one app on the collector.
  - Use the CLI command, store system ecosystem off, to turn off Ecosystem. Use this command if it is suspected that Ecosystem is overloading the Guardium system. To turn on Ecosystem, use the CLI command, store system ecosystem on
  - The Guardium SDK does not support apps in non-English Guardium systems, nor filenames in non-English languages.
  - Hardware requirement for developer machine when Investigation Dashboard is enabled is 34 GB minimum (and not 32 GB as written in Knowledge Center).

For more information, go to https://www.ibm.com/support/knowledgecenter/SSMPHH_10.5.0/com.ibm.guardium.doc.admin/ecosystem/ecosystem.html

- **FAM enhancements allow classification of files on NAS and SharePoint**

  FAM for NAS and SharePoint is a new Guardium product that can be used for scanning NAS or SharePoint servers or server farms for file entitlement and classification of instances of PII and other sensitive data, which may be related to regulatory laws (for example, GDPR or HIPAA).

  NAS or network-attached storage is a file-level storage system based on networked appliances containing multiple storage devices. SharePoint is a web-based collaborating platform and a document management and storage system.

  This Guardium product includes a Windows-based service performing scheduled scans of either NAS or SharePoint, and a configuration application for configuring the scan's targets, schedule, and classification criteria. For more information please follow the link below.

  https://www.ibm.com/support/knowledgecenter/SSMPHH_10.5.0/com.ibm.guardium.doc/discover/fam_for_nas_sp.html

- **Blocking on z/OS** has been expanded to allow for blocking by Client IP.

  Single Client IP blocking is possible by entering client IP and 255.255.255.0 in netmask.

  To block a range of Client IPs, enter 255.255.255.255 in netmask field.

  To block more than one Client IP:

  Best practice is to create a group (say zosblock) and enter the Client IP addresses. Then, in blocking policy, for field Client IP, use the dropdown key and select item zosblock. You can also have values in the Client IP and netmask, and a blocked group of Client IP addresses.

- **Amazon RDS Oracle v12 native auditing support** has been added in v10.5 (GRD-8500).

- **Manage SSH public keys** – Add three CLI commands (store system public key authorized [reset], show system public key authorized, delete system public key authorized) to give users the ability to add and manage SSH public keys in the Guardium appliance, so that they can script commands without specifying a password.

UNIX S-TAP

- **ATAP instances can now be managed without root access.** To enable this, configure the new IE new parameter db_user = <DB process owner>. This method doesn't require authorizing the user to the 'guardium' group. The root user has more control. The user cannot deactivate an A-TAP activated by root, but the root user can deactivate A-TAP activated by the user. The guard-config-update script is updated with this new functionality. It is not currently supported by GIM.
- **Improved handling of STAP configuration errors.** When you modify parameters in the GUI or GIM, S-TAP performs a check before saving the parameter values. Any value identified as erroneous is not saved. When you change values in the guard_tap.ini, S-TAP performs a check and tries to correct values it identifies as erroneous. For example, if the port range start is greater than the port range end, it sets the actual end as the start. It also logs configuration errors to the S-TAP event log as CONF_ERROR, so you can quickly identify and rectify the problem. The status in the S-TAP Control window is yellow when there is a CONF_ERROR. The S-TAP creates a backup guard_tap.ini when it corrects the configuration. It is saved as guard_tap.ini.bak under the S-TAP directory.
- **New script to identify DB2 shared memory parameter**. Run **find_db2_shmem_parameters.sh <instance name>** to make connections to DB2 over SHMEM, detect the SHMEM parameters, and list them so they can be added to the .INI. This replaces the previous calculations with ASLHEAPSZ… and db2sysc.
- **ktap_fast_tcp_verdict** now has value of 1 on S-TAP upgrade: KTAP decides itself whether or not to intercept traffic, without checking with S-TAP, giving a much faster connection.
- New **firewall default state** supported. When set to 2, all sessions start with a default watch enabled and the sniffer sends either a WATCH or UNWATCH verdict within the priority_count packets. This is useful for cases where only sessions created by a certain user need to be firewalled.
- **Improved STAP messages**. Messages are now coalesced based on message ID so even if the text strings differ, the messages are collapsed.
- **Discovery improvements:**
    - Supports enterprise PostgreSQL
    - Pfiles on Solaris are killed if it takes more than 30 seconds
- **Delayed S-TAP upgrade.** Use the new configurator.sh parameter, --delayed_bundle_deployment enable, to delay S-TAP upgrade until you verify that no A-TAP users are active, and DBs are not undergoing maintenance.

- **S-TAP GIM parameter for FAM monitoring**: STAP_FAM_ENABLED, enables the FAM monitoring service that is part of the S-TAP installation. On a fresh install, the default value is 0 which translates to the service being stopped, decoupling the S-TAP from FAM monitoring. When upgrading from earlier versions, STAP_FAM_ENABLED is persistent. STAP_FAM_ENABLED maps directly to the guard_tap.ini parameter FAM_ENABLE

Windows S-TAP

- Windows S-TAP drivers are now compliant with new **Microsoft driver signing requirements** for Windows 2016 and later versions of the Windows operating system.
- **S-TAP GIM parameter for FAM monitoring**: WSTAP_FAM_ENABLED, enables the FAM monitoring service that is part of the S-TAP installation. On a fresh install, the default value is 0 which translates to the service being stopped, decoupling the S-TAP from FAM monitoring. When upgrading from earlier versions, WSTAP_FAM_ENABLED is persistent. WSTAP_FAM_ENABLED maps directly to the guard_tap.ini parameter FAM_ENABLE.
- S-TAPs, using the **Grid load balancing** option, can now send log files and results of running diagnostics to the active collector as well as the associated central manager. For more information on Grid type load balancing please refer to the link below.

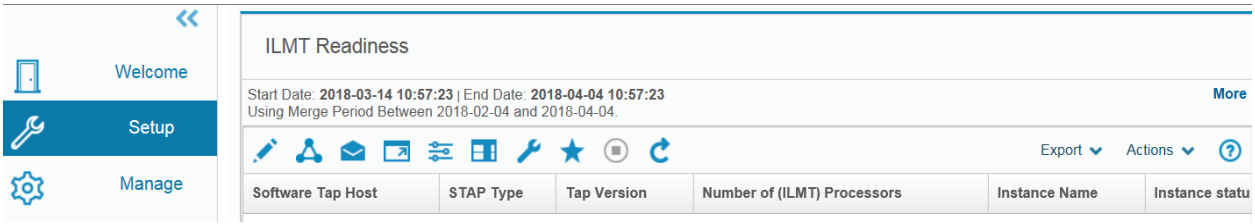
  https://www.ibm.com/support/knowledgecenter/SSMPHH_10.5.0/com.ibm.guardium.doc.stap/stap/load_balancing_types.html
- Windows S-TAP saves database related traffic into an **internal circular buffer** before sending it to Guardium collectors. To reduce the S-TAP memory footprint and to handle large database traffic spikes without having to restart S-TAP, two new enhancements have been added in 10.5:
  - When the buffer reaches 75% of the current maximum, S-TAP goes into 'ignore server reply' mode and no longer logs server reply packets. Similarly, when buffer reaches 90% of current maximum, only login packets are logged to reduce the buffer size.
  - If the first feature is insufficient, a new parameter DYNAMIC_BUFFER_INCREASE enables the dynamic buffer allocation. This allows the buffer size to increase incrementally by 50 MB when the buffer gets to 75% full in the current S-TAP session. Buffer size will continue to be impacted by limiting the number of packets logged as described above and will increase until it hits the BUFFER_FILE_MAX_SIZE. Review the relevant parameters below for more information.

Parameter	Default value	Description
BUFFER_FILE_SIZE	50	Advanced. The initial size of the buffer. The range is 5 to 1000.
BUFFER_FILE_NAME		Deprecated in v10.5. The full path of the memory mapped file if BUFFER_MMAP_FILE=1. Default is WSTAP working folder/StapBuffer/STAP_buffer.dtx
BUFFER_MMAP_FILE	0	1=memory mapped file option. 0=virtual memory allocation
BUFFER_FILE_MAX_SIZE	250	Advanced. The maximum size that the Memory commit will expand to, in MB. Maximum value is 1000.
BUFFER_FILE_MEM_FOOTPRINT	8	Advanced. The maximum fraction of the total memory that is allocated for the dynamic buffer increase. The default value of 8 translates to 1/8 of the total memory. The minimum parameter value is 2, meaning that you cannot allocate more than 1/2 of the total memory.
DYNAMIC_BUFFER_INCREASE	0	Advanced. Enables the dynamic buffer feature: when the buffer gets to 75% full in the current S-TAP session, the buffer size increases incrementally by 50MB. The feature is controlled by buffer_file_size, buffer_file_max_size, buffer_file_mem_footprint. 0: disabled; 1: enabled

- **Add pre-defined report for ILMT readiness** - For v10.5, an ILMT readiness report has been added. This pre-defined Guardium report will extract the number of processors from ILMT in the database server when ILMT is installed.

  The following attributes have been added to the S-TAP Info domain and are available for custom reporting: Instance Name; STAP Type; Number of (ILMT) Processors; and, Alternate IPs.

  Access the report by following the path Setup > Reports > ILMT Readiness



- The **Data Set Event** field allows the user to capture various event types for the data sets being monitored. The DSCL type Data Set Event captures Data Set Close events. Add two additional Data Set events:

  DSCLI – Data Set Close IN

  DSCLO – Data Set Close OUT

- **GBDI data readback** into Guardium was added in v10.5. Before this, data flow was one directional from Guardium to GBDI, now we can pull the data back from GBDI into Guardium Appliance for reporting, etc. For further information on Guardium Big Data Intelligence, click on https://www.ibm.com/us-en/marketplace/guardium-big-data-intelligence

Additional OS and Databases supported for v10.5

For Database Activity Monitoring (DAM)

Oracle 12.2 including Oracle RAC

MongoDB 3.6

MemSQL v6

Cassandra support enhancements: Cassandra Compression; Cassandra 3.11

PostgreSQL bind variables

Ubuntu 16.04

Red Hat Enterprise Linux 6.9

For Vulnerability Assessment

Amazon RDS data sources, SAP HANA V2, and the latest SAP HANA and Oracle 12.2 CVEs

Microsoft SQL Server 2014 Database STIG - Ver 1, Rel 5

Note: VA on Amazon RDS

See the following IBM link for guidance on deployment of VA on Amazon RDS.

This link is useful for customers when hardening the database on RDS.

http://www-01.ibm.com/support/docview.wss?uid=swg27050667

Disable TLS1.0/1.1, enable TLS 1.2

Repeat of information from v10.1.4 release (December 2017) with v10.5 added

Note: The v10.5 Guardium appliance ships with the same TLS settings as previous releases. No default settings were changed. A customer that wishes to have stronger TLS encryption must manually execute the specific CLI command to disable old protocols.

To increase the security of the Guardium system, in Guardium release v10.1.4 and later GPUs, communications protocols TLS1.0/1.1 can optionally be disabled in support of using communications protocol TLS1.2.

The Guardium customer must disable TLS1.0/1.1 and enable TLS1.2 from their Central Manager or standalone unit using the command line interface. Customer's Guardium appliances, S-TAP agents, CAS and GIM clients must be at specific versions to enable this new feature.

The enablement of TLS1.2 will automatically check to make sure managed units and S-TAPs are at specific versions, but cannot check CAS client versions so customers using CAS will need to make sure their CAS clients are at least on version 10.1.4 and their database servers have Java 7 enabled. Lack of doing this will result in the inability to see CAS connections to database servers.

Customers must also make sure all managed units have version 10.1.4 or later GPUs installed, and GIM Clients and S-TAPs are at a minimum version of 10.1.2. Failure to meet all requirements will mean that TLS1.0/1.1 will not be disabled.

Steps to enable this feature

Guardium users with admin role need to input the following GuardAPI commands at the CLI prompt. These commands are included in Guardium v10.1.4 and later GPUs.

To get information about and to disable TLS1.0/1.1 on all units in a managed environment, (Central Manager, Aggregator, Managed units), the following commands should be run on the Central Manager.

1. `grdapi get_secured_protocols_info`
2. `grdapi disable_deprecated_protocols`

Running these commands from a Central Manager will propagate down to all managed units.

`grdapi get_secured_protocols_info`

This GuardAPI command will list the enabled protocols (TLS1.0/1.1 and TLS1.2) and will indicate if the deprecated protocols can be disabled.

`grdapi disable_deprecated_protocols`

This GuardAPI command will first run the version check described above. If the result is positive for changes, then this command will change the configuration settings for each module on Central Manager and all managed units to disable the deprecated protocols and then restart the modules.

If the check result is negative for changes, then this command will indicate deprecated protocols are enabled and must be kept until all managed units are upgraded.

`grdapi enable_deprecated_protocols`

Running `grdapi enable_deprecated_protocols` on the Central Manager will ONLY enable deprecated protocols on the Central Manager. To enable deprecated protocols and have the Central Manager propagate the changes down to the managed units, the following command needs to be used, `grdapi enable_deprecated_protocols all=true`

This GuardAPI command is a fallback that will change back the configuration settings for each module on Central Manager and all managed units to enable the deprecated protocols and restart the modules.

After all the configuration changes are made, Guardium users with admin role should check that communications between Central Managers are stable and working properly.

For any managed unit that was offline during the GuardAPI command execution, Guardium users with admin role must manually start a command line session on the managed unit and execute the following command to make the configuration changes:

`grdapi local_disable_deprecated_protocols`

How to access the VA, Entitlement, and Classification scripts using fileserver

Guardium provides scripts to make it easier for DBAs to provide the minimum set of privileges required to run Vulnerability Assessment tests, Entitlements, and Classifications (sensitive data finder).

Use the same scripts for both Entitlement Reporting and Vulnerability Assessment tests.

Important: Each DBMS script has very specific instructions in the script header that must be followed.

From the CLI, run the following command:

fileserver <your desktop IP:port> 3600

Then go to a browser and enter the URL for the type of scripts you want to upload and choose the file that matches your database type.

Vulnerability Assessment and Entitlements:

https://<appliance ip:port>/log/debug-logs/gdmmonitor_scripts/

Classification:

https://<appliance ip:port>/log/debug-logs/classification_role/

Bugs fixed in v10.5 (v10.0 GPU 500)

The list below details many of the bugs fixed in v10.5. However, if you are looking for a certain bug, that is not listed, check with your Guardium support team member.

	Bug#	APAR	Description
1.	GRD-10471		Fixed instance of backslashes in report query condition not working as expected
2.	GRD-10819	GA16232	Fixed horizontal axis of CPU usage graph in GUI not showing the whole period.
3.	GRD-10956		ANS1708E Backup operation stopped. Only a root user can do this operation.
4.	GRD-11438	GA16229	Fixed instance of Central Manager not operational because of STAP association query
5.	GRD-11721		Fixed instance of remote must_gather run from the Central Manager not producing logs
6.	GRD-11776	GA16234	Fixed instance of column for 7 tuple "Client IP/Src App./DB User/Server IP/Svc. Name/OS User/DB Name" missing from CM's "Installed Policy Details"
7.	GRD-11883		Fixed instance of scheduled Job stuck in ARRIVED state
8.	GRD-12212	GA16246	Fixed instance of disk space calculation running slow on Aggregators
9.	GRD-12381	GA16249	Fixed instance of Alert sent to only a few users in a privileged group
10.	GRD-12383		Fixed instance of IP to Hostname aliasing working on some appliances but not on others.
11.	GRD-12674		Fixed display_stap_config so that it is REST API enabled
12.	GRD-12704		Fixed instance of Aggregator GID CID table missing entries from collectors
13.	GRD-12774	GA16144	Fixed instance of restore from TSM not working
14.	GRD-12879		Fixed instance of SKIP_LOGGING action on Exception rules with unexpected behavior
15.	GRD-12921	GA16296	Fixed instance of "Guardium Hosts" view in "Edit STAP parameter" section of GUI not working correctly
16.	GRD-13112	GA16278	Fixed instance of dashboard definition import/export not populating in another user's login.
17.	GRD-13262	GA16309	QID 11827 || CWE-693 ||Title: HTTP Security Header Not Detected

	Bug#	APAR	Description
18.	GRD-13351	GA16256	Fixed instance of "Returned SQL errors" getting an error in Japanese GUI
19.	GRD-13626	GA16301	Fixed instance of GUI user role will run a security assessment but editing privileges for datasource were not included
20.	GRD-13706		Block KTAP IOCTLS until KTAP is fully initialized and STAP is connected
21.	GRD-14123	GA16300	Fixed instance of v10, Exception rules "continue to next" even though "continue to next" is not checked
22.	GRD-14260		Fixed instance of Call Statements dropping parameters
23.	GRD-14282		Fixed memory leak on Guardium system where DB2_exit is configured
24.	GRD-14317	GA16294	Fixed error from command, grdapi enable_outliers_detection_agg, "Could not get the datasource factory for the connection"
25.	GRD-14431		Fixed instance of SQL Statements having latency returning results when QRW enabled
26.	GRD-14633		Fixed instance of core dumping after upgrading S-TAP to 10.1.5
27.	GRD-14681		Fixed instance of DB2_EXIT not capturing encrypted traffic
28.	GRD-14699	GA16315	Policy evaluation of regular expression has changed after v10.0p4029
29.	GRD-14904		Fixed instance of RedHat Enterprise Linux 6 database server stuck in boot mode after GIM v10.1.4 Upgrade
30.	GRD-15033		Fixed instance of Entitlement stopping if just one database is unavailable and returns no data even for the available ones.
31.	GRD-15079	GA16303	Fixed instance of policy violation alerts unable to sort
32.	GRD-15227		Fixed instance of v10.1.4 p400 not installing
33.	GRD-15763/ GRD-15769/ GRD-15770/ GRD-15771/ GRD-15780/ GRD-16089		Add support of logging timestamp in format of millisecond of event to syslog alert; syslog alert on policy; for all types of real time policy alert Create CLI commands, set alert_timestamp_unit value, and show alert_timestamp_unit value. Value 0 = second Value 1 = millisecond
34.	GRD-15955	GA16304	Fixed instance of store sniffer certificate errors
35.	GRD-16025		Fixed instance of overwrite per datasource not working
36.	GRD-16083		Fixed instance of Session Inference UID Chain Error

	Bug#	APAR	Description
37.	GRD-16335		Fix instance of runtime parameter order in GUI different than Query Builder and param name no longer displayed
38.	GRD-16477		Fix instance of STAP Live update failing if initially installed as "root"
39.	GRD-16534		Fix REST API command issue
40.	GRD-16656		Fix instance of GIM Module version not showing in the GIM process monitor
41.	GRD-16701		Fix instance of upgrading Windows STAP to 10.1.4 not removing GuardiumDC Connector service
42.	GRD-16932		Fix documentation on Flat Log Process
43.	GRD-4673	GA15943	Fixed instance of STAP install or upgrade on AIX TL3 SP3 changing ownership of /usr/sbin/lsof to root:guardium (was root:system)
44.	GRD-4686	GA15918	Fixed instance of audit processes taking much longer after upgrade
45.	GRD-4855		Fixed constant "-W- System is in boot run level ... will skip any checks" due to "who -r" returning blank when attempting STAP install from GIM
46.	GRD-4863	IT21138	Fixed Orphans Cleanup improvement
47.	GRD-4877		Fixed instance of GUI error with large Managed Unit selection on the Central Manager page with Patch Installation Status
48.	GRD-4890		Cloning Guardium VMs no longer requires manually updating GID (GLOBAL_ID)
49.	GRD-4923		Fixed instance of Group getting emptied daily
50.	GRD-4962		Fixed instance of FAM: Alert and Audit setting lost in Japanese and Chinese setting.
51.	GRD-4963		Add index on AUDIT_PROCESS_RESULT and REPORT_RESULT_HEADER
52.	GRD-5087		Fixed instance of Report Query Start Of <DAY/WEEK/MONTH> showing 23:59:59 of the day prior to the date.
53.	GRD-5861		Add Guardium support for MongoDB version 3.2
54.	GRD-6573		Fixed instance of If you have several API functions mapped to a report, and then you delete one API function mapping, it deletes ALL API function mappings
55.	GRD-6876		Fixed instance of reports running from Central Manager on remote source using group members from Central Manager instead of managed unit
56.	GRD-7796		Fixed instance of v10.0p1121 persistence changing for gsys-securing.sh

	Bug#	APAR	Description
57.	GRD-7973	GA16173	Fixed DATA Archive failing with AmazonServiceException "Your proposed upload exceeds the maximum allowed size"
58.	GRD-9200		InfoSec - Fixed instance of Guardium appliance displaying SQL errors
59.	GRD-9532		Fixed instance of Oracle traffic collection not logged

Security fixes, v10.5

PSIRTs and v10.0p6024

PSIRT ID	Description	Issue ID
93721	User of Hard coded credentials	GRD-4444
96966	Using components with known vulnerabilities (commons-fileupload)	GRD-7108
101243	User Enumeration vulnerability - CLI	GRD-14055
105200	Multiple vulnerabilities in gnutls	GRD-12419
105527	Open Source OpenSSL vulnerabilities	GRD-13729
n/a	Using components with known vulnerabilities (commons-collections)	GRD-13963
n/a	Using components with known vulnerabilities (MySQL Connector)	GRD-13958
n/a	Using components with known vulnerabilities (ntp)	GRD-13905
n/a	Cross-Site scripting vulnerability	GRD-16798

	Bug#	APAR	Description
V10.0p6024	GRD-14285		Fixes for Meltdown and Spectre: CVE-2017-5754 CVE-2017-5753 CVE-2017-5715 Note: RedHat has issued a note that some degradation in performance is expected related to the new kernel from RedHat specifically compiled to fix Meltdown / Spectre vulnerability.

Releases for v10.0 since V10.1.4 (December 2017)

v10.0 p402, v10.0p403, V10.0 p1009, v10.0 p404, v10.0 p405, v10.0 p406, v10.0 p407

Release		Guardium GRD- #	APAR	Description
V10.0 p402	V10.0 p402	GRD-15938		Fixed instance of not being able to modify GIM client parameter or GIM version from GUI.
		GRD-15937	GA16305	Fixed instance of older versions of GIM clients losing connection to GIM server after upgrade to v10.1.4
		GRD-15724		Fixed instance of GIM Client NOT connecting to 10.1.4 GIM Server
		GRD-14483		Fixed instance of GPU 400 (10.1.4) installation causing Windows GIMs on 10.0_r85602_1 to disconnect from the GIM Server
		GRD-13916		PSIRT 106102 & PSIRT 109463 - Open Source Apache Struts 2.5 Vulnerability
		GRD-13728	GA16291	Fixed GRDAPI update_assessment_test ERR=880
		GRD-13547		PSIRT 104636 - IBM SDK, Java Technology Edition Quarterly CPU - Oct 2017 - Includes Oracle Oct 2017 CPU
		GRD-13410		Fixed instance (v10.1.3) of exclude group members box not working as expected. **Known Limitation**: Patch V10.0p402 introduces ERD change that will not allow importing Guardium Definition exports on appliances with patch level below patch v10.0p402. Customers

Release		Guardium GRD- #	APAR	Description
				advised to import definitions exported at v10.0p402 level only on the systems with patch v10.0p402 or above. Change will be included in GPU 10.5 or above. This limitation does not affect data restores.
		GRD-13112	GA16278	Fixed instance of dashboard definition import/export not populating in another user login.
		GRD-12617	GA16252	Fixed instance of Logging Collectors Report Showing a "1" for the Collector Name
		GRD-12921	GA16296	Fixed instance of "Guardium Hosts" view in "Edit STAP parameter" section of GUI not working correctly
		GRD-12881 and GRD-14819		PSIRT 104275- Open Source Oracle MySQL Server Vulnerabilities
		GRD-11769	GA16230	Fixed instance of restore v9 archive files not working with error message: Failed decrypting file (suffix=decrypt_failed)
V10.0 p403	V10.0p403	GRD-16106		Fixed Load Balancer
V10.0 p1009	V10.0 p1009	GRD-16603		Adjust database configuration
10.0p404	10.0p404	GRD-16455	GA16320	CSRF Same-Origin Validation Fix
10.0p405	10.0p405	GRD-15935		Group Builder Prototype Fix
10.0p406	10.0p406	GRD-16335		Runtime Parameter Fix
10.0p407	10.0p407	GRD-14996		Audit Process Fix

Sniffer Updates since V10.1.4 (December 2017)

4030, 4031, 4032 Sniffer Update

Notes:

- Installation of sniffer patches need to be performed/scheduled during the "quiet" time on the Guardium appliance to avoid conflicts with other long-running processes (such as heavy reports, audit processes, backups, imports and so on).
- Installation of sniffer patches will automatically restart the sniffer process.
- If the downloaded package is in .ZIP format, customers are required to unzip it outside Guardium appliance before uploading/ installing it.
- Universal sniffer patch can be installed on top of any GPU starting with v10.0 patch 100 or higher.

  If there is a failure to install, the following error message will display:

  ERROR: Patch Installation Failed - Incompatible GPU level. GPU p100 or higher required.

- This sniffer patch should be installed across all the appliances: Central Manager, Aggregators and Collectors. Do this to avoid aggregator merge issues.
- On Aggregators, it is recommended to turn off the GUI before installation of the patch, for the duration of the installation.

4030, 4031, 4032 Sniffer Update / Bugs that were fixed:

	Sniffer update	Guardium GRD- #	APAR	Description
1.	4030	9851	GA16222	Exhibits meaningless redundant "DB2_COMMAND" SQL construct in reports
		10429	GA16204	Cannot get 2 Alert Actions in the same Rule to use different templates
		10672		Improved F5 traffic handling
		10682	GA16237	Some of the Oracle ASO traffic cannot be captured
		10831	GA16255	UID chain not captured encrypted DB2_exit
		12381	GA16249	Alert sent for a few users in a privileged group
		12879		SKIP_LOGGING action on Exception rules have unexpected behavior
		12922	GA16286	Long INSERT statement is not logged
		13059	GA16274	DB user comes as "@@" followed by a sequence of numbers and letters
2.	4031	7373		Oracle 12.2.0.1.0 support
		12375/ 16055	GA16311	Intermittent loss of data db2_exit
		12922	GA16282 GA16286	Long INSERT statement is not logged
		13320	GA16285	Failed login exception with no ORA error code
		13703	GA16292	Alert CEF template variable values need to escape backslash
		14022	GA16298	Increase in Flat Log Requests
		14123	GA16300	Exception rules "continue to next" even though "continue to next" is not checked
		14205	GA16297	Encrypted Oracle: no exceptions captured
		14260		Call Statements dropping the parameters
		14431		SQL Statements have latency returning results when QRW enabled
		14463	GA16287	App user name truncate, only show 100 bytes
		14699	GA16315	Policy evaluation of reg-exp has changed after 4029
		16055	GA16314	SSL handling issue

	Sniffer update	Guardium GRD- #	APAR	Description
3.	4032	15638	GA16310	MongoDB reports showing values not expected
		16401		RETURNED_DATA in GDM_CONSTRUCT_TEXT table is always getting masked with default Regex library
		16057		Decrease the lower boundary of snif memory percentage from 33% to 25%
		Note: Sniffer update to 10.0p4032 was not built as a separate patch. This sniffer patch is specific to the v10.5 release.		

Notice - Deprecation and removal of functionality

In Guardium release v10.5, the following capabilities are deprecated:

- Legacy interface to setup by client in GIM. The new GIM user interface is much easier to use and provides a better user experience.

With the next major Guardium release after v10.5, an enhanced version of the Discover Sensitive Data tool will replace the classification policy and process builders. Begin familiarizing yourself with discovery scenarios now. Note: due to a limitation of the Discover Sensitive Data tool in V10.5, customers using many classification rules are advised to continue using the classification policy and process builders until the next major Guardium release.

Notice - End of Service

As of March 2018, Guardium will no longer support LHMON drivers. This is due to the new Windows Signing requirement for Windows 2016 support.

Monitoring CIFS/SMB

DAM support for monitoring CIFS/SMB ended with version 2.0. FAM supports CIFS/SMB in version 2.0 and beyond.

Notice – Platform deprecation

The following Guardium-supported platforms will be deprecated in 10.5. This deprecation applies to both DAM and VA.

Database	Deprecated versions
Microsoft SQL Server	2005, 2008, 2008 R2
IBM DB2	9.7
IBM DB2 Purescale	9.8
Sybase IQ	15.4
Teradata	13
Cloudera	4, 4.1
Hortonworks	2.3, 2.4
IBM BigInsights	4, 4.1
Cassandra	3.5
Windows File Share (WFS)	

Known Issues and Limitations

Issue No.	Description	Guardium Component	Bug #
1.	Traffic will not be captured for Sybase for pre-existing session when upgrading S-TAP from version 9 to version 10.5.	UNIX S-TAP	GRD-15006
2.	Purge object age definitions not saved after Backup CM switch	Backup CM	GRD-15456
3.	%RecordsAffected is not supported in Custom-Alert (same as SYSLOG restriction).	Policy and Realtime Alerts	GRD-16672
4.	Redaction rule action does not work on compressed SQL traffic.	Sniffer	GRD-16332
5.	Starting 10.5, FAM monitor will not be enabled by default for new installations. This is applicable for both UNIX S-TAP and Windows S-TAP. For upgrade installation, the existing value is inherited and won't be changed during upgrade.	FAM monitor	GRD-16967 GRD-15019 GRD-15675
6.	There are two issues for GBDI: 1. On a managed unit search window, user might not see the drop down to select GBDI for search. Workaround is to go to datasources on this managed unit and run a test connection for GBDI DS. When you open search page again, the drop down will be visible. 2. If search is disabled on a unit either because the unit is underpowered or disabled using API, and GBDI datasource is added, data search box will be available, but search does not work. when you open the search, it will show an error message and ask to close the window.	Guardium Big Data Intelligence	GRD-17032
7.	Two Hadoop auditing configuration settings are missing from documentation. Add the following steps to the install manual: Configure Ranger plugin to write audit logs to log4j HDFS In section “Custom ranger-hdfs-audit” add: xasecure.audit.destination.log4j=true xasecure.audit.destination.log4j.logger=xaaudit	Hadoop auditing configuration	GRD-16903

Issue No.	Description	Guardium Component	Bug #
	Hive In section "Advanced ranger-hive-audit.xml" add: xasecure.audit.destination.log4j=true xasecure.audit.destination.log4j.logger=xaaudit For further information, click on the link to this technote, Configuring Guardium to capture Apache Ranger auditing events for Hortonworks Hadoop (http://www-01.ibm.com/support/docview.wss?uid=swg21987893&aid=3) Configuring Ranger using the Python scripts is recommended over configuring Ranger from the GUI.		
8.	The Guardium SDK does not support apps on non-English Guardium systems, nor filenames in non-English languages.	SDK on non-English Guardium systems	GRD_16741
9.	Error message pops up when trying to save discovery scenario even though it is saved.	Discovery Agent	GRD-17005
10.	Data Set reports missing from the 'Based on Report' on Distributed Report Configuration. If you have cloned reports from "DATA SET Access" or "DATA SET Detailed Access" before v10.1.4 and you want to create a distributed report, you need to clone the reports again. In v10.1.4, Guardium made those two reports eligible for distributed reports.	Distributed Report	GRD-12279
11.	When creating or updating a group and editing the Client Name or Client IP address of GIM clients, the name and address must reflect valid values for a GIM client connected to the Guardium system. If an invalid name or address is specified, the edited client will no longer appear as a member of the client group.	Set up by Client	GRD-17110

Issue No.	Description	Guardium Component	Bug #
12.	There is a default maximum size limitation of 2MB for classified files on target scan environments. To override this limit and open the scan to files greater than 2MB, the following files must be modified: For NAS: 1) Open the file <install directory>\Bin\FSAAConfig.xml 2) The value for MinFileSizeLimitValue should be set to 0 Example: <MinFileSizeLimitValue>0</MinFileSizeLimitValue> This will open the scan to all file sizes For SharePoint: 1) Open the file <install directory>\Bin\DLPConfig.xml 2) Set the value for MaxFileSizeLimigValue to the maximum size of the file you wish to classify in bytes. Example: <FileSizeLimitValue>10485760</FileSizeLimitValue> This will open the scan to all files up to the specified maximum size	FAM NAS SharePoint	GRD-17120
13.	There are missing and incorrect parameters in GDM_ACCESS and GDM_SESSION if you run only one query in Oracle 12 RDS session.	Native Auditing	GRD-17176
14.	Not able to install STAP V9 using GIM - Not all required fields are editable. Workaround – fill in all the required fields before installing the bundle.	GIM installer	GRD-17004
15.	If Hadoop monitoring service does not display port information and the status is “S-TAP not installed,” edit configuration and specify a valid S-TAP.	Hadoop monitoring	GRD-16841
16.	An error will result when user creates a custom domain if the domain name already exists in the "Domain Finder" list. If a new name is used each time, no error occurs.	Custom domain	GRD-17355

Issue No.	Description	Guardium Component	Bug #
17.	When a user installs CAS for Windows via GIM on an .ISO build, the last digit of the Client IP is dropped. This is causing the CAS status screen to show the incorrect IP and hostname. Notes: • Does NOT occur on a patched GPU environment. Only occurring on .ISO. • Does NOT occur when CAS is installed manually on the Windows machine. • Does NOT occur with CAS of Linux.	Windows S-TAP	GRD-17649
18.	In cases where Datamart extraction stops executing on a defined schedule, the user can restart the GUI on the affected unit. This should resolve the issue.	Datamart	GRD-17499
19.	The customer will not be able to run GIM Remote Activation and AWS Native Audit in parallel. AWS Native Audit will cause GIM Remote Activation to fail. Workaround options: Option 1. Don't use AWS Native Audit from the Central Manager. Run AWS Native Audit from an Managed Unit only. Option 2: If you want to run both AWS Native Audit and GIM Remote Activation on the Central Manager: (1) run AWS Native Audit; (2) restart the GUI; and, (3) run GIM Remote Activation. Option 3. Run GIM Remote Activation from the CLI.	AWS Native Audit/ GIM remote activation from Central Manager	GRD-17103
20.	grdapi update_stap_config is not allowing database types as value for DB_IGNORE_RESPONSE	S-TAP configuration	GRD-16491
21.	GIM uninstall not removing /usr/local/IBM/etc/guard from the database server	GIM uninstall	GRD-16677

Note: Important issues in this table will be addressed in future V10.x maintenance releases.

Additional Resources

Online help available via Web

The online help is included in the Guardium v10.5 Knowledge Center on the Web at:

http://www-01.ibm.com/support/knowledgecenter/SSMPHH/SSMPHH_welcome.html

Search all the product information together at that site. The Knowledge center is updated more frequently than the embedded online help and is the most up-to-date source of information.

V10.5 Detailed Release Notes (April 2018)

http://www-01.ibm.com/support/docview.wss?uid=swg27050791

Links to System requirements/ Technical requirements for v10.5

For a list of V10.5 databases and operating systems, go to:

V10.5 System Requirements (Platforms Supported) (April 2018)

64-bit

http://www-01.ibm.com/support/docview.wss?uid=swg27047801

V10.5 Software Appliance Technical Requirements (April 2018)

64-bit

http://www-01.ibm.com/support/docview.wss?uid=swg27047802

V10.1.5 S-TAP filenames and MD5Sums (April 2018)

http://www-01.ibm.com/support/docview.wss?&uid=swg27048065

Resources to help plan a migration from Guardium 9.x to 10.x

http://www-01.ibm.com/support/docview.wss?uid=swg22010717

V10.5 and Developerworks

For more information, see the Guardium V10.5 articles on IBM Developerworks:
https://www.ibm.com/developerworks/community/groups/service/html/communityview?communityUuid=432a9382-b250-4e55-98d7-8e9ee6cbf90e

IBM Security Learning Academy

See securitylearningacademy.com for further Guardium-related information.

ibm.biz/academy_datasec

IBM Data Security on the Security Learning Academy

Flashes and Alerts

https://www.ibm.com/support/home/search-results/E627144T24067U58/IBM_Security_Guardium?filter=DC.Type_avl:CT792,CT555,CT755&sortby=-dcdate_sortrange&ct=fab&acss=danl_4640_email

Listing all DCFs

https://www.ibm.com/search?lang=en&cc=us&q=GUARDIUM&tabType[0]=Support

Support resources

For more resources, access this support page:

http://www-01.ibm.com/support/docview.wss?uid=swg21984772

2018-April-27

IBM Guardium Version 10.x Licensed Materials - Property of IBM. © Copyright IBM Corp. 2018. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” (www.ibm.com/legal/copytrade.shtml)