# Release Notes

==========

| | |
|---|---|
| Product: | IBM Security Guardium |
| Release: | v10.1.4 |
| Version | Guardium v10.0 GPU p400 |
| Completion Date: | 2017-December-21 |

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 v10.1.4 Release Notes

## General note on upgrading to v10.1.4

v10.1.4 (v10.0 GPU p400) 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 v10.1.4 (v10.0 GPU p400). See the section below on Health Check patch.

v10.1.4 (v10.0 GPU p400) includes all previous v10.x fixpacks, security fixes, and sniffer updates, up to and including v10.0 p235 for fixpacks and v10.0 p4029 for sniffer updates. See the sections (starting on page 12) 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.

Depending on the size of the Guardium system being upgraded, MySQL 5.7 will enter into a recovery mode, which could take some extended time to complete.

During the 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 recovery mode.

If the MySQL upgrade needs to perform MySQL check table (which is known to be a very time-consuming process) and, depending on the size and number of tables, then this can delay the time it takes to upgrade.

## Health Check patch

v10.0 Health Check patch 9997 must be successfully installed before installing the Guardium v10.1.4 (v10.0 GPU p400). This release will not install without FIRST installing the Health Check patch. The name of this Health Check file is SqlGuard-10.0p9997_HealthCheck_2017_02_09.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

v10.1.4 (v10.0 GPU p400) will overwrite any v10.0 Sniffer update patch greater than v10.0 patch 4029.

Be sure to re-install any v10.0 Sniffer update patch greater than v10.0 patch 4029 after installing v10.1.4 (v10.0 GPU p400).

## Installing or upgrading to 10.1.4 Windows S-TAP

Fresh install of v10.1.4, no reboot required

Upgrading from v9 to v10.1.4, 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 10.1.4 features/functions and enhancements*

v10.1.4 introduces the following new capabilities, depending on the product you have installed:

- Cloud database protection service

  Cloud database protection service provides discovery, classification, vulnerability assessment, for all RDS AWS database engines, and activity monitoring for Oracle v.11. You manage all these functions in one page, which lists all the databases on our cloud DB service account and provides status of your monitored DBs. Once you set up a connection with a cloud DB service account, and discover its instances, you can assign classification and VA processes to individual instances. Use the classification results to enable activity monitoring (done though database auditing).

  The cloud functionality in previous Guardium versions (Amazon RDS discovery and vulnerability assessment) is combined with the new functionality, accessed via Discover > Database Discovery >Cloud DB Service Protection.

- Use the compliance monitoring tool to help meet compliance standards by quickly installing policies, populating groups, and running reports for monitoring database activity.
- The redesigned and enhanced 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.
- The redesigned GIM module installation tool streamlines software installation by identifying client-module incompatibility and simplifying parameter management.
- Rapid Response DPS - Uploads are used to keep information current and within industry best practices to protect against newly discovered vulnerabilities. Distribution of updates is done whenever a CVE is published with a scoring of 7.0 or greater. Rapid Response DPS is available only to customers with Guardium v10.1.4 release and higher.
- Additional languages added – French, Spanish and German.

Enhancements - new features and supported platforms that improve your overall Guardium experience.

- Enhance GDPR support with additional languages and patterns, new policies and reports, and support for DB2 for z/OS. You can find more information for compliance monitoring at:

  https://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc/monitor/compliance_monitoring.html

- Improve internal communications security by providing TLS 1.2 support and deprecating older TLS 1.0/1.1 protocols. See the separate article on this feature at the end of this bullet list.

**Linux, Solaris, AIX, HP-UX S-TAP updates**

- S-TAP now supports up to ten collectors when configured for multi-threading (participate_in_load_balancing=4) and non-multi-threading (participate_in_load_balancing=1) modes.
- guard_monitor has two new parameters:
    - cpu_measurement_mode: You can measure CPU consumption per core or relative to total CPU capacity of the system
    - force_core_when: configure when to collect a core dump (always, limitsexceeded, nonresponsive)
- Guard-config-update new parameters
    - add-sqlguard: Adds SQLGuard_ID section to S-TAP config file
    - remove-sqlguard: removes SQLGuard_ID section from S-TAP config file
    - modify-sqlguard: used to modify many common S-TAP parameters
- guardctl commands:
    - two new commands: save-active-ataps and restore-active-ataps, Save and then restore the configurations of the currently active ATAPs in a single file. Useful when upgrading databases.
    - Repair command is automatically run during activate and deactivate when guardctl detects it to be necessary
- Add a SSH client's IP to the UID chain: enable with the S-TAP parameter uid_chain_ssh_ip
- Dedicated upload directory for uploading modules and diagnostics from database server:
    - Shell installation – guardium/guard_stap/.upload
    - GIM installation – modules/STAP/current/.upload
- Kerberos plugin: You can specify (colon separated) multiple paths to the Kerberos system cache files in the parameter KRB5_PLUGIN_CCACHE in the guardkerbplugin.conf and in optional parameter KRB5_PLUGIN_GSSAPI_LIBRARY

# *Disable TLS1.0/1.1, enable TLS 1.2*

To increase the security of the Guardium system, in Guardium release v10.1.4, 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 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 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 new for Guardium v10.1.4.

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`

# *Additional OS and Databases supported for v10.1.4*

## For Database Activity Monitoring (DAM)

MariaDB 10.1

## For Vulnerability Assessment

Oracle 12.2 STIG benchmark coverage. Version 1, Release 7.

## Platforms

Update support to SUSE:

SLES 11 PPC64 (Big Endian system only)

SLES 12 PPC64LE (Little Endian only)

CentOS 7 in Unix S-TAP

OpenSSL for UNIX S-TAP: OpenSSL1.0.2k

TLS 1.2

## 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).

In 10.1.4, 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/

## Change in default behavior

The default behavior of FAM_enabled parameter has been changed from ON by default to OFF by default. This will only affect new GIM installations. Upgraded environments will not be affected. In Shell S-TAP installations, FAM is still enabled ON by default. (GRD-13167)

The change of fam_enable=0 as default also changes the behavior of FAM crawler on UNIX. Previous behavior was, after install, the FAM crawler would start discovering files and sending the results to the Guardium System. After the recent change of fam_enable=0 upon installation, the FAM crawler, upon installation, is unable to connect to the Guardium system. The workaround is to turn on FAM_ENABLED=1 of S-TAP and the FAM crawler will work. (GRD-13890)

# *Bugs fixed in v10.1.4 (v10.0 GPU p400)*

The list below details many of the bugs fixed in v10.1.4. 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-5105 | GA16013 | Fix instance of guard_writer0 shmem" messages logged as LEVEL: Severe in db2diag.log |
| 2. | GRD-5870 | GA11393 | Fix instance of unknown message in database server syslog ("ktap_ioctl:Ioctl xxxx by non-daemon, I am xxxx, daemon is xxxx") |
| 3. | GRD-6469 | GA16108 | Fix instance of blank DB_USER with Kerberos Authentication enabled on Redhat Linux 6 DB server |
| 4. | GRD-6478 | GA16098 | Fix instance of roles assigned in Custom Workflow not reinforced |
| 5. | GRD-6499 | | Fix instance of Central Manager GUI requiring frequent restarts due to out-of-memory resulting from quick search components |
| 6. | GRD-6505 | GA16186 | Fix CLI command "store password disable" so it disables the passwords of inactive users |
| 7. | GRD-6510 | | Fix instance of classification job stopping after 8-minutes |
| 8. | GRD-6875 | | Fix instance of Deployment Health view from the Central Manager not reporting correctly after the customer renamed the hostname of the collector appliance. |
| 9. | GRD-6877 | GA16268 | Improve query performance for remotely invoked reports |
| 10. | GRD-6918 | | New alert template works as designed |
| 11. | GRD-6929 | IT23432 | Fix STAP service not starting automatically after reboot. |
| 12. | GRD-6943 | | Fix instance of CLI command, store system snif-thread-number automatically setting thread number different from given value |
| 13. | GRD-6948 | GA16161 | Clarify GIM installed modules confusion |
| 14. | GRD-6951 | GA16148 | After upgrading from V10.1 to V10.1.2 with Language = Japanese, fix GUI text strings appearing in English |
| 15. | GRD-6959 | GA16097 | Security-related fix. Fix instance of /guardhelp/advanced/print.jsp showing error information |
| 16. | GRD-7066 | GA16083 | Fix instance of sample size input field in the Classification Builder GUI not saved |
| 17. | GRD-7256 | | Add Query Builder new fields |
| 18. | GRD-7478 | GA16136 | Fix instances of STAP log contains multiple zone_getattr: Invalid argument |

| | Bug# | APAR | Description |
|---|---|---|---|
| 19. | GRD-7546 | | Enable GUI aliasing, then use GuardAPI command to schedule Hostname aliasing |
| 20. | GRD-7613 | GA16239 | Fix blank Teradata "OS User" and "Source Program" when connecting using ODBC |
| 21. | GRD-7627 | GA16147 | Fix OOM exception just after midnight that affects Tomcat |
| 22. | GRD-7699 | | Fix "Escalate" an Audit results |
| 23. | GRD-7706 | GA16262 | Clear alert in WAIT state with RCA |
| 24. | GRD-7717 | GA16137 | Fix CLI command, support clean DAM_data, so that it purges old GDMS files |
| 25. | GRD-7818 | | Fix orphan cleanup for GDM_ACCESS on Aggregator |
| 26. | GRD-7931 | GA16194 | Fix default filenames for any report export to PDF |
| 27. | GRD-8024 | | Obfuscate root, accessmgr password reset, and passkey cryptography, so that the clear text is not visible or present in emails. |
| 28. | GRD-8171 | GA16171 | Fix restore data from a TSM server |
| 29. | GRD-8205 | GA16143 | Fix "Allow purge without exporting or archiving" checkbox remaining checked after effort to uncheck it and save. |
| 30. | GRD-8253 | GA16159 | Fix stopping of Tomcat with Enterprise Quick Search and Enterprise Load Balancer disabled |
| 31. | GRD-8258 | GA16208 | Fix instance of reports sent to a NAS server and the timestamp in the report adds 'z' at the end indicating GMT/Zulu time. |
| 32. | GRD-8379 | GA16265 | Fix instance of error message "Please contact your system administrator." when moved to "Support Information Gathering Results" page |
| 33. | GRD-8459 | | Fix instance of /etc/init/guard-sender.conf not automatically restarting -n run of guard_sender |
| 34. | GRD-8656 | GA16180 | Fix support execute with ERROR : No Such File, Check the correct script is installed: Code Point (103) |
| 35. | GRD-8927 | | Fix CLI diag SNMP test using enterprises.18708 instead of enterprises.18000 |
| 36. | GRD-9014 | GA16168 | Fix instance of store certificate keystore for SSL cert failing with certificate not imported, alias <-trustcacerts> already exists |
| 37. | GRD-9052 | | Fix patch recovery |
| 38. | GRD-9079 | | Update RHEL tzdata* to 2017b |
| 39. | GRD-9098 | | Fix instance of Inspection Engines Discovery missing MS-SQL ports due to peculiar configuration of MS-SQL |

| | Bug# | APAR | Description |
|---|---|---|---|
| 40. | GRD-9128 | GA16182 | Fix 'tap_min_heartbeat_interval' parameter |
| 41. | GRD-9477 | GA16166 | Fix instance of LDAP authentication not working after GPU 230+p4027 installed. |
| 42. | GRD-9495 | GA16263 | Fix blank Teradata "OS User" and "Source Program" when connecting using ODBC |
| 43. | GRD-9519 | GA16266 | Fix instance of user credentials storage randomness |
| 44. | GRD-9550 | GA16220 | Fix instance of network bonding configuration resulted in warning messages |
| 45. | GRD-9568 | GA16179 | Add support for Maria Enterprise 10.1.22 |
| 46. | GRD-9631 | GA16219 | Fix instance of Central Manager patch installation status issue |
| 47. | GRD-9651 | GA16175 | Fix instance of activating ATAP for Sybase ASE 15.7 environment not opening shared object file |
| 48. | GRD-9778 | | Fix instance of table column attributes with incorrect display flag setting |
| 49. | GRD-10175 | | Expose GIM_MODULES_HEARTBITS Entity |
| 50. | GRD-10176 | IT22670 | Fix instance of GIM.pm location in @INC for new GIM install |
| 51. | GRD-10188 | GA16175 | Fix instance of V10 STAP of causing Sybase DB Server to stop |
| 52. | GRD-10226 | GA16247 | Fix instance of AutoDiscovery emptying list of hosts after v10p230 upgrade |
| 53. | GRD-10233 | | Fix instance of Classifier stopped and jobqueue restarting |
| 54. | GRD-10401 | GA16201 | Fix instance of Datamart consolidation intermittently stopping |
| 55. | GRD-10420 | GA16206 | Fix instance of Result Archive and Result Export configuration (FTP) intermittently disappearing |
| 56. | GRD-10494 | GA16206 | Fix instance of oauth_access_token issues |
| 57. | GRD-10670 | PI91374 | Fix instance of running guard_diag for STAP 10.1.3 r101342 stopping AIX 7.1 DB server |
| 58. | GRD-10775 | | Fix instance of DB2 Inspection engine created by auto discovery not collecting local traffic |
| 59. | GRD-10977 | | Change instance not checking EXPRESS_DAM license at CLI start, but on demand |
| 60. | GRD-10978 | GA16226 | 1000s of UNIX S-TAP messages - Fix instance of unrecognized address family for current server in heartbeat reply |
| 61. | GRD-10982 | GA16263 | Fix instance of blank Teradata "OS User" and "Source Program" when connecting using ODBC |

| | Bug# | APAR | Description |
|---|---|---|---|
| 62. | GRD-11012 | | Fix instance of common name invalid warning on GUI |
| 63. | GRD-11317 | | Fix instance of re-running failed DM consolidation duplicates activity if successful on secondary node (or vice versa) |
| 64. | GRD-11603 | | Fix instance of CLI command "support ping stap_hosts all" prompting for hostname and causing e command to fail if not entered correctly |
| 65. | GRD-11654 | GA16226 | 1000s of UNIX S-TAP messages - Fix instance of unrecognized address family for current server in heartbeat reply |
| 66. | GRD-11710 | GA16261 | Fix instance of Must gather slow log function not checking all slow log files |
| 67. | GRD-11725 | | Fix diag.pl inserts 0 for MESSAGE_TEXT_ID, which caused test emails not to send. |
| 68. | GRD-11731 | GA16203 | Fix instance of Unit Utilization Statistics not populated if no CONSTRUCT INSTANCE |
| 69. | GRD-11779 | GA16240 | Fix instance of blank/white screen when Definitions Export> Datasource Export With "Export to API file" selected |
| 70. | GRD-12250 | PI89781 | Fix instance of V10.1.3 UNIX S-TAP failover to secondary collector not occurring when primary collector is down |
| 71. | GRD-12317 | PI89838 | Fix semaphore increase leak on Guardium AIX 7.1 DB2 v10 STAP 10.1.3 with DB2 Exit |
| 72. | GRD-12448 | | Security-related fix. CVE-2017-15265 |
| 73. | GRD-12459 | GA16264 | Fix instance of DB2_EXIT causing high number of opened files and memory utilization increase on AIX 7.1 |
| 74. | GRD-12568 | | Security-related fix. Fix instance of CLI security options not preserved at customer site for GUI security settings |
| 75. | GRD-12592 | | Fix instance of Datamart export / import not carrying over IDs properly |
| 76. | GRD-12875 | | Fix instance of DB2 database stopping with Exit configured, DB2 started, and STAP issue activity |

# *Security fixes, v10.1.4*

| PSIRT ID | Description | Issue ID |
|---|---|---|
| 93714 | Information Exposure | GRD-6505 |
| 93716 | Password in Clear Text | GRD-6197, GRD-6196, GRD-6198, GRD-2557, GRD-2501 |
| 93719 | Information Exposure Through Log Files | GRD-5456, GRD-4024 |
| 93720 | HTTP Response Splitting | GRD-6193 |
| 93724 | Incorrect Permission Assignment for Critical Resource | GRD-3179 |
| 93727 | SQL Injection | GRD-3750 |
| 93728 | Session Identifier Not Updated | GRD-6505 |
| 93729 | Selection of Less-Secure Algorithm During Negotiation | GRD-4447 |
| 96966 | Using Components with Known Vulnerabilities | GRD-6445, GRD-6447, GRD-6417 |
| 97227 | Open Source GNU glibc Vulnerabilities | GRD-8563 |
| 99243 | IBM SDK, Java Technology Edition Quarterly CPU | GRD-9990 |
| 100323 | SQL Injection in GIM Servlet | GRD-10395 |
| 101224 | Use of a Broken or Risky Cryptographic Algorithm | GRD-10395 |
| 101225 | Sensitive Information Leakage | GRD-10117 |
| 101226 | Password Returned in HTTP Response | GRD-10081 |
| 101227 | Lack or Misconfiguration of Browser Security Header | GRD-10108 |
| 105195 | Multiple Open Source packages vulnerable in Guardium Appliance | GRD-12198 |

# *UNIX S-TAP bugs fixed, v10.1.4*

| Bug# | APAR | Description |
|---|---|---|
| GRD-3865 | | Fix instance of server message logged in Db2 diag when DB2 exit is loaded and S-TAP is down |
| GRD-5104 | GA15941 | Fix instance of S-TAP restarting Teradata. |
| GRD-5105 | GA16013 | Fix instance of the "Attached /.guard_writer0 shmem" messages logged as LEVEL: Severe in db2diag.log |
| GRD-5870 | GA11393 | Fix instance of unknown message in DB server syslog ("ktap_ioctl:Ioctl xxxx by non-daemon, I am xxxx, daemon is xxxx") |
| GRD-6469 | GA16108 | Fix instance of blank DB_USER with Kerberos Authentication enabled on Redhat Linux 6 DB server |
| GRD-6948 | GA16161 | Fix instance of incorrect GIM installed modules |
| GRD-7478 | GA16136 | Fix instances of S-TAP log containing multiple zone_getattr: Invalid argument |
| GRD-7613 | GA16229 | Fix instance of blank Teradata "OS User" and "Source Program" when connecting using ODBC |
| GRD-8246 | GA16183 | Fix instance of embedded SQL traffic not captured by Java application |
| GRD-8248 | | Fix instance of DB2 lockout occurring after ATAP activation was done on z/Linux |
| GRD-8448 | | Fix instance of S-TAP 10.1.2 r100595 causing RHEL 7 server to stop |
| GRD-8784 | | Fix instance of UNIX S-TAP for DB2 shared memory only passing unsigned short length of data to collector |
| GRD-9128 | GA16182 | Fix instance of 'tap_min_heartbeat_interval' parameter not working |
| GRD-9492 | GA16213 | Fix Instance discovery not discovering inspection engine for Oracle correctly on Solaris |

| Bug# | APAR | Description |
|---|---|---|
| GRD-9495 | GA16263 | Fix instance of blank Teradata "OS User" and "Source Program" when connecting using ODBC |
| GRD-9651 | GA16175 | Fix instance of activating ATAP for Sybase ASE 15.7 environment not opening shared object file |
| GRD-9931 | GA16175 | Fix instance of activating ATAP for Sybase ASE 15.7 environment not opening shared object file |
| GRD-10176 | IT22670 | Fix instance of GIM.pm not located in @INC for new GIM install |
| GRD-10188 | GA16175 | Fix instance of V10 S-TAP causing Sybase DB Server to stop |
| GRD-10311 | | Connect to IP fields get truncated (?) and throws invalid format exception |
| GRD-10350 | | Fix instance of UID chain showing up only for the DB2 instance configured in the first Inspection Engine |
| GRD-10474 | GA16212 | Fix instances of too many [guardctl] <defunct> process existing without other error messages |
| GRD-10670 | PI91374 | Fix instance of Running guard_diag for S-TAP 10.1.3 r101342 led to AIX 7.1 DB server stop. |
| GRD-10775 | | Fix instance of DB2 Inspection engine created by auto discovery not collecting local traffic |
| GRD-10974 | | Fix instance of blank DB User and Source Program for SSL Encrypted Remote Traffic for Sybase |
| GRD-10978 | GA16226 | Fix instance of unrecognized address family for current server in heartbeat reply |
| GRD-10982 | GA16263 | Fix instance of blank Teradata "OS User" and "Source Program" when connecting using ODBC |
| GRD-11229 | | Fix instance of no HADOOP traffic collection |
| GRD-11404 | | Fix instance of encrypted Mongo DB traffic creating too many rows in GDM_CONSTRUCT table |

| Bug# | APAR | Description |
|---|---|---|
| GRD-11654 | GA16226 | Fix instance of Unrecognized address family for current server in heartbeat reply |
| GRD-11727 | | Fix instance of Guardium KTAP R84814 led to AIX server stop |
| GRD-12250 | PI89781 | Fix instance of V10.1.3 UNIX S-TAP failover to secondary collector not occurring when primary collector is down |
| GRD-12317 | PI89838 | Fix instance of Guardium AIX 7.1 DB2 v10 S-TAP 10.1.3 with DB2 Exit causing semaphore increase leak |
| GRD-12459 | GA16264 | Fix instance of DB2_EXIT causing high number of opened files and memory utilization increase on AIX 7.1 |
| GRD-12875 | | Fix instance of DB2 database stopping with DB2 Exit configured, DB2 started, and SAP issue activity with S-TAP down |
| GRD-13115 | | Fix instance of S-TAP not capturing traffic via DB2 exit after reboot on AIX |
| GRD-13226 | | Fix instance of S-TAP 10.1.3_r101342 diag rebooting AIX 6.1 |
| GRD-13350 | | Fix instance of KTAP module request for 3.10.0-693.el7.s390x in S-TAP 10.1.3_r102091 |

# *Releases for v10.0 since V10.1.3 (June 2017)*

v10.0 p231, v10.0p232, v10.0 p233, v10.0 p234, v10.0p235

| Release | | Guardium GRD- # | APAR | Description |
|---|---|---|---|---|
| V10.0 p231 | V10.0 p231 | GRD-6889 | GA16174 | Fix Internet Explorer compatibility |
| V10.0 p232 bundle | | GRD-4914 | | Fix instance of Enterprise reports using Central Manager time to run remote queries on managed units in different time zones |
| | | GRD-6498 | GA16172 | Fix system backup using tomcat public key working for password-less system backups via SCP |
| | | GRD-6887 | GA16075 | Fix instance of a transfer-failed archive file isn't resent on the next run after 10.1 (p100). |
| | | GRD-6937 | GA16087 | Fix instance of admin user deleting a report which caused other roles' Navigation Menus to get reset to default |
| | | GRD-6959 | GA16097 | Fix Guardium Help showing error information |
| | | GRD-8171 | GA16171 | Fix TSM import file for nodenames that are short hostnames |
| | | GRD-9014 | GA16168 | Fix instance of store certificate keystore for SSL certificate failing with certificate not imported |
| V10.0 p233 | V10.0 p233 | GRD-10148 | GA16198 | Fix instance when cannot upgrade 10.1.2 AIX 7 STAP and GIM agents to 10.1.3 |
| V10.0 p234 | | GRD-10977 | | Defer CLI license check to run only during protected commands |
| | | GRD-10401 | GA16201 | Fix instance of Datamart consolidation intermittently stopping |
| | | GRD-9666 | GA16202 | Fix instance of "Ignore STAP Session" marking the Session Ignored but has SQL associated to it. |
| | | GRD-9151 | GA16181 | CLI security fix |
| | | GRD-8258 | GA16208 | Fix when reports are sent to a NAS server, the timestamp in the report adds 'z' at the end indicating GMT/Zulu time. |

| Release | | Guardium GRD- # | APAR | Description |
|---|---|---|---|---|
| | | GRD-8253 | GA16159 | Fix Tomcat heap size computation for memory utilization. |
| | | GRD-7096 | | Fix instance of when saving a report, large DataMart alters may stop and cause schema mismatch |
| | | GRD-6505 | GA16186 | Fix instance of the CLI command "store password disable" not disabling the passwords of inactive users |
| V10.0 p235 | | GRD-10311 | | Fix instance of connection to IP fields gets truncated and results in an invalid format exception |

# *Sniffer Updates since V10.1.3 (June 2017)*

4027, 4028, 4029 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.

- 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.
- On Aggregators, it is recommended to turn off the GUI before installation of the patch, for the duration of the installation.
- This sniffer patch should be installed across all the appliances: Central Manager, aggregators and collectors.

v10.0 Sniffer Update patches 4027, 4028, 4029

The bugs that were fixed:

| | **Sniffer update** | **Guardium GRD- #** | **APAR** | **Description** |
|---|---|---|---|---|
| **1.** | 4027 | 7687 | GA16102 | Fixed sniffer segfault issue caused by race condition, applicable only to zOS STAP for DB2 customers, configured with TLS (encryption) on |
| 2. | 4028 | 8313 | IT22383 | Fix ALERT ONLY action writing to SYSLOG as well as MESSAGE and MESSAGE_TEXT table as opposed to SYSLOG only |
| | | 8214 | PI87260 | Fix frequent sniffer restarts for DB2 on z/OS |
| | | 8198 | GA16167 | Fix Sniffer Segment Fault - p4025 |
| | | 7938 | | Oracle - fix instance of select sysdate from dual not displayed correctly in the SQLfield |
| | | 7937 | | Teradata - fix instance of select current_timestamp not displayed correctly in the SQLfield |
| | | 7893 | GA16126 | Add additional masking of log content |
| | | 7749 | GA16086 | SQL Server - fix instance of grant statements not displayed correctly in the SQLfield |
| | | 7477 | GA16092 | Fix instance where Oracle Service Names sometimes are parsed in excessively long form |
| | | 7231 | GA16103 | Fix instance where running CREATE OR ALTER PROCEDURE command on MSSQL database gets a PARSER_ERROR on a v9/p700/p4074 Managed Unit |
| | | 7022 | GA16058 | Fix Sniffer restarts as the result of heavy POC stress test |
| | | 6940 | GA16200 | Fix instance of SQLs missing intermittently on collector in report based on COMMAND as main entity. Aggregator shows up no issue for the same report |
| | | 6893 | GA16164 | Fix instance where STAP Edit functionality goes away after page refresh |
| | | 6890 | GA15955 | Fix instance of MSSQL Objects logged including inline comments |
| | | 6503 | GA16165 | Fix instance where V10 Sniffer Dropping Packets \|\| DB_USER either missing or is "?" |

| | Sniffer update | Guardium GRD- # | APAR | Description |
|---|---|---|---|---|
| | | 6472 | GA16141 | Fix instance of Sniffer Restarts/STAP Buffer Errors and with Enterprise Load Balancing |
| | | 6469 | GA16108 | Fix instance of Blank DB_USER with Kerberos Authentication enabled on Redhat Linux 6 DB server |
| 3. | 4029 | 10498 | GA16193 | Fix instance of Selective audit policy and object/command and field tuples incorrectly logging constructs |
| | | 10205 | GA16191 | Fix instance of Sniffer stopping on p4028 |
| | | 9960 | GA16193 | Fix instance of a problem with group using object/command and logging "Full Details" and "Full Details with values" |
| | | 8329 | GA16189 | Fix instance where embedded SQL traffic not captured even for call - C application |
| | | 7990 | GA16178 | Fix instance of passed-in values for update statement are null in full SQL report |
| | | 7911 | GA16154 | Fix instance of DB User not logged for Oracle RAC environment when packets sent out of order |
| | | | | |

# *Notice - Deprecation and removal of functionality*

In Guardium release v10.1.4, the following capabilities are removed:

- Access Map - Use the Deployment Health view to understand the relationship between databases and appliances. Use the Data In-sight chart on the Investigation Dashboard to gain an understanding of database client-to-accesses with its interactive 3D visualizations. This YouTube video includes a demonstration of Data In-sight: https://www.youtube.com/watch?v=OsQbWMPyWL4
- Baseline: Use outlier detection capability to mine access data for anomalous behavior.
- AME Interface for Definition Builder- AME (Audit Management Expert) has not been used for z/OS support for many releases.

The following capabilities are deprecated and are planned to be removed in a future release:

- Legacy Group Builder. The new Group Builder in 10.1.4 provides a much better user experience and improved capabilities.
- Legacy interface to setup by client in GIM. The new GIM user interface is much easier to use and provides a better user experience.
- Legacy classifier policy and process builder. Use the Discover Sensitive Data Scenario to create and edit policy rules and to create new classifier processes.

## 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.

## Notice – Platform deprecation

The following Guardium-supported platforms will be deprecated in the next release in 2018 (this will be a post-v10.1.4 release). 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. | The TSM file (dsm.sys) and the Centera (.pea) file do not get copied over to the new Central Manager after the Backup CM backup is restored. | Backup CM | GRD-13409 |
| 2. | On Guardium systems with v10.0p4029 and higher, the Blocking policy is not pushed down to S-TAP on z/OS. | z/OS | GRD-13271 |
| 3. | The LDAP certificate is not restored when using the restore db_from_previous_version command. | Backup | |
| 4. | Newly installed clients are not appearing in the Set up by Client> Choose clients list if the user is already logged into the Central Manager. It is not until the user logs out and then logs back in that the newly installed clients appear in the list.<br>Note: This issue does NOT occur with "Set up by Client (Legacy)". The user can install a new client and it will appear in the list.<br>Workaround: user can logout and then log back in to make the new clients appear. | Set up by Client | GRD-13267 |
| 5. | By default, Vormetric DSM server and, by default, GIM Listener are using port 8445.<br>Either change Vormetric DSM server port to a different port or install GIM listener with a different port, enable this port in firewall on both ends and use that port when discovering listeners and activating them. | GIM Listener port/ Vormetric DSM server | GRD-13525 |
| 6. | System Backup and Data Archive to Amazon S3 are limited to files that are less than 5 GB in size after compression. | System Backup/ Data Archive/ Amazon S3 | GRD-13659/ GRD-7973 |
| 7. | Property files return to their default value after upgrade. | Property files | GRD-7356 |
| 8. | Pre-defined access and classification policies cannot be modified | Pre-defined classification policies | GRD-8259 |
| | | | |
| | | | |

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

# *Additional Resources*

## Link to formal Guardium V10.1 product announcement

http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/9/760/ENUSJP16-0229/index.html&lang=en&request_locale=en

## Online help available via Web

The online help is included in the Guardium v10.1 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.

## V10.1.4 Detailed Release Notes (December 2017)

http://www-01.ibm.com/support/docview.wss?uid=swg27050547

## V10.1.3 Detailed Release Notes (June 2017)

http://www-01.ibm.com/support/docview.wss?uid=swg27049899

## V10.1.2 Detailed Release Notes (November 2016)

http://www-01.ibm.com/support/docview.wss?uid=swg27049019

## V10.1 Detailed Release Notes (June 2016)

http://www-01.ibm.com/support/docview.wss?uid=swg27047839

## Links to System requirements/ Technical requirements for v10.1/10.1.2/10.1.3/10.1.4

For a list of V10.1 databases and operating systems, go to:

**V10.1.x System Requirements (Platforms Supported) (December 2017)**

**64-bit**

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

**V10.1.x Software Appliance Technical Requirements (December 2017)**

**64-bit**

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

**V10.1.x and V10.1.4 S-TAP filenames and MD5Sums (December 2017)**

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

**v9.x to v10.1.3 Upgrade patch release notes/ known limitations (October 2017)**

http://www-01.ibm.com/support/docview.wss?uid=swg27050457

**Location of User Guide for the v9.x to v10.1.3 upgrade**

To access the user guide for the v9.x to v10.1.3 upgrade, go to the section on "Upgrading your Guardium system" in the v10.1.3 Knowledgecenter (September 2017).

http://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.install/upgrade/upgrade_guide.html

## V10.1 and Developerworks

For more information, see the Guardium V10.1 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

2017-December 21