Release Notes

================

Product: IBM InfoSphere Guardium

Release: 9.0/9.1

Version   InfoSphere Guardium GPU v9.0, patch 300

Fix Completion Date: 2014-10-06

Description: InfoSphere Guardium GPU v9.0, patch 300

Finding the Fix/Patch

============================

This document is intended to provide a reference to the contents of this fix/patch. If applicable, the detailed description of each fix and instructions for applying this fix/patch are contained within the download package. The actual package is available for downloading from the IBM Fix Central web site at http://www.ibm.com/support/fixcentral/

Make the following selections on Fix Central:

Product Group: Information Management

Product: InfoSphere Guardium

Installed Version: 9.0/9.1

Platform: Linux

Heading: Appliance Patch (GPU and Ad-hoc)

Click "Continue", then select "Browse for fixes" and click "Continue" again.

============================

GPU V9.0/9.1 patch 300 Release Notes

Instead of using the CLI command, fileserver, to upload the patch, it is recommended to use the CLI command, store system patch install scp, to upload this patch. This is because the patch is over 2 GB in size. Using Fileserver may result in a timeout issue. Using the store system patch install scp CLI command is not subject to a timeout.

Note: The language pack is separate from GPU patch 300.

V9.0 patch 300 (September 2014) supersedes V9.0 patch 200 (April 2014).

Notes:

1. The GPU installer will automatically perform a reboot after successful installation of the patch.

Upgrade existing Guardium systems to version 9.0, patch 300 from any V9 release or from version 8.2, or install version 9.0 on a new system.

Choose the correct scenario:

- Upgrade an existing 32-bit Guardium system: download the 32-bit patch from Fix Central and apply it. Refer to the Upgrading section of the Guardium 9.0 Knowledge Center at http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.nex.igsec.doc/g91_welcome.html

- Upgrade an existing 32-bit Guardium system to a 64-bit Guardium system: (1) run system backup; (2) rebuild using the 64-bit .ISO image; and, (3) restore backup. Refer to the Upgrading section of the Guardium 9.0 Knowledge Center at http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.nex.igsec.doc/g91_welcome.html

- Install a new 32-bit Guardium system: download the 32-bit image from Passport Advantage. The file includes the 32-bit V9.0 image and patch 200. Install the image on the 32-bit hardware and then apply the patch 200. Then retrieve patch 300 from Fix Central and install patch 300. Refer to the Installing and Upgrading section of the Guardium 9.0 Knowledge Center at http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.nex.igsec.doc/g91_welcome.html

InfoSphere Guardium GPU v9.0/9.1 patch 300 release notes

- Install a new 64-bit Guardium system: download the 64-bit image from Passport Advantage. The image contains the 64-bit V9.0 product. Install the image on the 64-bit hardware. Then retrieve patch 300 from Fix Central and install patch 300. Refer to the Installing section of the Guardium 9.0 Knowledge Center at
http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.nex.igsec.doc/g91_welcome.html

Health check patch dependency

Health check patch 9997 must be installed before installing the v9.0 patch 300 (32-bit or 64-bit). The upgrade patch will not install without FIRST installing the Health Check patch. The name of this file is SqlGuard-9.0p9997.tgz.enc.

Note: V9.0 patch 300 is available as a 32-bit and 64-bit patch.

New Features and Enhancements

1. A Central Manager redundancy enhancement
2. More parameters for existing REST API commands
3. New CLI commands for certificate-related commands
4. Security patch 1036/ Security patch 1061
5. A list of ad-hoc released patches
6. A language pack.

See a summary of public URLs for the full number of Guardium v9.0 releases, located at the end of this document.

Central Manager redundancy enhancement

Guardium has added support to Central Manager redundancy for the following:

1. Backup Central Manager - Make Primary CM link will be available after Primary Central Manager loses connection.

2. User Layouts will be retained.

3. User and roles are in the synch backup and will not rely on user synch.

4. User Group Roles Data will be retained.

5. A GuardAPI function make_primary_cm, has been added to allow switch to Central Manager from CLI.

6. Data is retained from Audit Process Builder processes after switching Primary Central Manager to Backup Central Manager.

7. Central Management backup includes all the definitions (reports, queries, alerts, policies, audit processes etc.), users and roles as it did before.

8. It includes the schedules for enterprise reports, distributed reports and LDAP.

9. It includes schedules for all audit processes, schedules and settings for data management processes such as archive, export, backup, and import.

10. It includes settings for Alerter and Sender.

11. User's GUI customization's, custom classes and uploaded JDBC drivers are included.

See complete information in the help topic for Central Management.

Additional functions, REST API

Use an optional fetchSize parameter in the online_report REST API.

If this parameter is empty, the default is 20 records so API operates as it did before this change.

If parameter is larger than 30000, an error message is returned.

For any other number, this parameter determines the max number of records returned by the API request.

Additional REST API parameters are sortColumn and sortType.

Changes in certificate-related CLI commands

Changes in Commands
Some commands have been changed involving certificates and certificate keys.

- csr is now create csr gui.
- create system csr is now create csr sniffer.
- restore keystore is now restore certificate keystore backup.
- restore system-certificate is now restore certificate sniffer default.
- show system certificate is now show certificate sniffer.
- store system certificate is now store certificate sniffer.
- store trusted certificate is now store certificate keystore.
- store certificate console is now store certificate gui.

New Commands

- create csr alias
- restore cert_key sniffer backup
- restore cert_key sniffer default
- restore certificate keystore default
- restore certificate sniffer backup
- store cert_key sniffer
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server
- show certificate summary
- show certificate warn_expired

Deprecated Commands

The following commands have been deprecated. These older CLI commands are not supported in V9.0/9.1 patch 300 and their use will result in an error message. However, these older CLI commands will still work in v9.0/9.1 patch 200 and lower.

- csr
- store certificate console
- store system key
- show system key
- store system certificate
- show system certificate

Full List of Certificate-related CLI commands

- create csr gui
- create csr alias
- create csr sniffer
- restore cert_key sniffer backup
- restore cert_key sniffer default
- restore certificate keystore default
- restore certificate keystore backup
- restore certificate sniffer backup
- restore certificate sniffer default
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server
- show certificate sniffer
- show certificate summary
- show certificate warn_expired
- store cert_key sniffer
- store certificate keystore
- store certificate sniffer
- store certificate gui

Backup and Default Options

You can choose to restore certificates and certificate keys with the backup or default parameter. Use the backup parameter to restore a certificate to the last saved certificate. Use the default parameter to restore a certificate to the original certificate that Guardium supplied.

Certificate Expiration Dates and Summary Commands

Run the show certificate warn_expire command periodically. This command warns you of certificates that will expire in six months and displays a list of expired certificates. For more information, see the show certificate CLI command. To show a summary of all certificates, run the CLI command show certificate summary. Run the commands periodically to review certificate expiration dates.

Language Pack

SqlGuard-9.0p1059_Language_Update_GPU_300

Separate versions for 32-bit and 64-bit

      SqlGuard-9.0p1059_Language_Update_GPU_300_32-bit.tgz.enc

      SqlGuard-9.0p1059_Language_Update_GPU_300_64-bit.tgz.enc

The language pack is separate from GPU 300.

There are changes to some of the JAR files to enable them to be translated. Therefore, the language pack contains some updated JAR files.

Since these may conflict with newer versions of the JAR files in later patches (for example, after GPU patch 300), it is important that Guardium users install the language pack before installing any other patches on a system that has GPU patch 300 or the v9.0 ISO.

If Guardium users install the language pack after the other patches, they may need to re-install the other patches.

On a non-English Guardium system, the language pack must be installed before upgrading to GPU patch 300.

Note: The language pack is not needed to install GPU patch 300 on an English Guardium system, but the language pack must be installed on a non-English Guardium system.

Question #1: Should V9.0 patch 300 be applied again after the language pack is installed?

Answer:

No, do not apply V9.0 patch 300 twice. If upgrading a Guardium English system with v9.0 GPU patch 300, install the GPU, then install the language pack, and then run the CLI command, store language, to change the language on what was previously a Guardium English system. On a Guardium non-English system, the language pack must be installed before the GPU.

Question #2: Is the language pack dependent on installing the Health Check patch 9997?

Answer:

No, the language pack is NOT dependent on first installing the Health Check patch 9997.

Question #3: What happens if a user installs GPU patch 300 before the language pack on a non-English system?

Answer:

V9.0/9.1 GPU patch 300 will not install on a non-English system that does not have the language pack installed beforehand.

Security update, patch 1036

Fix #	Bug #	PSIRT	Description
1.	-	40054	MySQL 5.6.20 upgrade
2.	41335	40382	Java Update to correct CVE-2014-4263
3.	40549	39028	O/S OpenSSL, to correct CVE-2014-0224
4.	39251	39576	Upgrade Tomcat Version 7.0.54 on both 32 & 64 bit
5.	40532	39028	OpenSSL, to correct CVE-2014-0224

Security update, patch 1061

Fix #	Bug #	PSIRT	Description
1	42249	42770	V9.0, RedHat RHEL Bash vulnerability CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278
2	42248	42770	V8.2, RedHat RHEL Bash vulnerability CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278

InfoSphere Guardium GPU v9.0/9.1 patch 300 release notes

Guardium Patch Update 9.0 p300

Includes patches: 200, 1022, 1027, 1028, 1029, 202, 203, 210, 211, 212, 213, 215, 216. 217, 218, 219, 220, 1034, 221, 222, 223, 224, 226, 227, 1035, 1036, 1037, 1039, 229, 1042, 230, 231, 232, 233, 234, 235, 236, 238, 240, 242, 243,244, 1058, 1061

Fix #	Problem	Description
1.	33032	Update expired GUI certificates.
2.	37531	Update firewall parameters with the guardAPI command update_stap_config.
3.	37935	Improve response time due to packet loss between the S-TAP and sniffer.
4.	37978	Improve performance speed of show db-status command.
5.	38042	Increased protection against vulnerabilities found in BURP report, a vulnerability scanning tool.
6.	38166	Create index(es) in the custom tables builder.
7.	38713	Fix instance of installation failure involving Datamart.
8.	38815	Allow line wrapping in PDF audit reports when there are no spaces.
9.	38990	Disable auto discovery to add, edit, or delete Inspection Engines.
10.	39265	Fix incorrect database and operating system username.
11.	39339	Add support show snif_memory_max and support store snif_memory_max command to control memory usage.
12.	39340	Import a definition with a query containing a condition with a dynamic group.
13.	39344	Change patch number for the Distributed Status report check to return the correct message.
14.	39392	Restore certificate authentication in keystore.
15.	39394	Show records for report tasks in audit process result viewer.
16.	39394, 40549, 40550	Upgrade OpenSSL RHEL to strengthen security.
17.	39440	Disable quicksearch for aggregators and Central Managers.
18.	39535	Restore archived data due to time zone issues.
19.	39591, 38399	Fix client hostname after decryption/ fix database username
20.	39681	Fix instance of policy group import failure.
21.	39814	Fix instance of IP Alias job failure in scheduled job log.
22.	39822	Restart MySQL automatically after a system restart.
23.	39823	Fix enterprise buffer usage limitation.

Fix #	Problem	Description
24.	39889	Fix instance of CVE-2013-6245 test failure.
25.	40026	Fix invalid query messages from full SQL and Object/Field entities.
26.	40060	Fix instance of classifier process halting on views.
27.	40073	Fix Central Manager patch selection performance.
28.	40139	Capture SQL statements using host variables in DML report.
29.	40139	Capture SQL statements using host variables in DML report.
30.	40269	Reduce memory usage of GDM_Error table in MySQL database.
31.	40269	Reduce excessive growth of GDM_ERROR table.
32.	40394	Change internal Guardium method of parsing F5 data reports.
33.	40520, 40262	Fix instance of full SQL ID mapping to a different session ID.
34.	40744	Fix OpenSSL vulnerabilities for CVE-2014-0124.
35.	40917	Fix specification of more than three RECON files in IMS Definition.
36.	41095	Retrieve full Oracle version.
37.	41113	Make the backup Central Manager the primary CM when the primary CM is unavailable.
38.	41114, 41166	Restore audit process schedules in system backup.
39.	41257	Fix instance of LEEF template parsing and missing database name.
40.	41857	Fix extrusion values in GDM_POLICY_VIOLATIONS_LOG.
41.	42337	Fix instance of Failed login not recorded to GDM_EXCEPTION for Mongodb SSL.

Note: This table of ad-hoc patches and corresponding bugs lists the major appliance changes since GPU v9.0/9.1 patch 200 released in April 2014. For other minor fixes since GPU v9.0/9.1 patch 200, consult the corresponding PMR reporting system or contact Customer Support.

Known Limitation in V9.0 patch 300

Multi-lingual versions of Guardium - multi-byte characters are displayed as "??" in Response Body of RESTAPI. This limitation will be corrected in a future ad-hoc patch release after the release of GPU V9.0/9.2 patch 300 (Bug #42413)

Online help available via Web

The online help is included in the Guardium 9.0/9.1 Knowledge Center on the Web at:

http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.1.0/com.ibm.nex.igsec.doc/g91_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.

InfoSphere Guardium GPU v9.0/9.1 patch 300 release notes

InfoSphere Guardium v9.0, v9.0p02, v9.0p50, v9.0p100, v9.0p150, v9.0p200, v9.0p300

V9.0/ 9.1 patch 300	**V9.0/9.1 patch 300 Detailed Release Notes (October 2014)** http://www-01.ibm.com/support/docview.wss?&uid=swg27043680
V9.1 V9.0 patch 200	**V9.0/9.1 patch 200 Detailed Release Notes (April 2014)** http://www-01.ibm.com/support/docview.wss?&uid=swg27041694
V9.1 V9.0 patch 150 Release notes; Technical reqs. System reqs.	**V9.0/9.1 patch 150 Detailed Release Notes (November 2013)** http://www-01.ibm.com/support/docview.wss?uid=swg27039700&aid=1 **V9.0/9.1 Software Appliance Technical Requirements (January 2014)** **32-bit and 64-bit** http://www-01.ibm.com/support/docview.wss?&uid=swg27039720 **V9.0/9.1 System Requirements (Platforms Supported) (modify date 2014-03-03)** **32-bit and 64-bit** http://www-01.ibm.com/support/docview.wss?&uid=swg27039049
V9.1 V9.0 patch 100 Release notes; Data sheet; Technical reqs; System reqs	**V9.0/9.1 GPU patch 100 Detailed Release Notes (October 2013)** http://www.ibm.com/support/docview.wss?&uid=swg27039700 **V9.0/9.1 Datasheet - IBM InfoSphere Guardium V9.0/9.1 helps you protect your high-value data and automate your compliance policies** http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS213-373&appname=USN **V9.0/9.1 Software Appliance Technical Requirements (October 2013)** **32-bit and 64-bit** http://www.ibm.com/support/docview.wss?&uid=swg27039720

InfoSphere Guardium GPU v9.0/9.1 patch 300 release notes

	V9.0/9.1 System Requirements (Platforms Supported) (October 2013) **32-bit and 64-bit** http://www.ibm.com/support/docview.wss?&uid=swg27039049
V9.0 patch 50	**V9.0 GPU patch 50 Detailed Release Notes (June 2013)** For new and enhanced features, see http://www.ibm.com/support/docview.wss?&uid=swg27038869
V9.0 patch 02	GPU for v9.0 patch 02 release notes (Nov. 2012) http://www.ibm.com/support/docview.wss?uid=swg27036839
V9.0	**V9.0 Release Notes (2-page with hyperlinks to V9.0 announcement documents) (Oct 2012)** http://www.ibm.com/support/docview.wss?&uid=swg27036230 **V9.0 Detailed release notes (Oct 2012)** For new and enhanced features, see http://www.ibm.com/support/docview.wss?&uid=swg27036227 **V9.0 Filenames and MD5SUMs (Oct 2012)** For S-TAP versions and MD5SUMs, see http://www.ibm.com/support/docview.wss?&uid=swg27036228 **V9.0 Software Appliance Technical Requirements (August 2013)** **32-bit and 64-bit** http://www.ibm.com/support/docview.wss?&uid=swg27036229 **V9.0 System Requirements (Platforms Supported) (August 2013)** **32-bit and 64-bit** http://www.ibm.com/support/docview.wss?&uid=swg27035836

	V9.0 Datasheet The IBM InfoSphere Guardium V9.0 announcement can be found at http://www.ibm.com/software/data/guardium/.

The "Deployment Guide for InfoSphere Guardium" has been released and is available for the general public at the IBM Redbooks link below:

> http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/sg248129.html

Other Helpful links
IBM Product Lifecycle: http://www-01.ibm.com/software/support/lifecycle/

IBM InfoSphere Guardium v9 Announcement:
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier=897&letternum=ENUSC13-042#213-373

Recorded tech talks for InfoSphere Guardium V9
bit.ly/guardwiki

InfoSphere Guardium GPU v9.0/9.1 patch 300 release notes