Release Notes

==========

Product:	IBM Security Guardium
Release:	v9.0/9.5
Version	Guardium GPU v9.5 (v9.0 patch 750)
Fix Completion Date:	2017-04-21
Description:	Guardium GPU v9.5 (v9.0 patch 750)
Filenames:	SqlGuard-9.0p1089_Language_Update_GPU_750_32-bit.tgz.enc
	SqlGuard-9.0p750_GPU_March_2017_32-bit.tgz.enc
	SqlGuard-9.0p1089_Language_Update_GPU_750_64-bit.tgz.enc
	SqlGuard-9.0p750_GPU_March_2017_64-bit.tgz.enc

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:	Security Systems
Product:	Guardium
Installed Version:	9.0/9.5
Platform:	Linux
Heading:	Appliance Patch (GPU and Ad-hoc)

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

==========

Version 9.5 (GPU v9.0 patch 750) Release Notes

Installation choices/upgrade/new installation

To upload this patch, use the CLI command, fileserver

In a slow network scenario, Guardium recommends the use of another CLI command, store system patch install scp. However, be mindful that using the CLI command, store system patch install scp, requires staging the patch on an FTP server.

Note: The language pack is separate from GPU patch 750.

V9.0 patch 750 (March 2017) supersedes V9.0 patch 700 (August 2016).

Notes:

1. V9.0 patch 750 is available as a 32-bit and 64-bit patch from Fix Central.
2. **The GPU installer will automatically perform a reboot after successful installation of the patch.**

Upgrade existing Guardium systems to version 9.0, patch 750 from any V9 release.

Upgrade IBM Guardium appliances in following required top-down order:

1. Central Manager
2. Aggregator
3. Collector
4. GIM agent
5. S-TAP agent

Please make sure that each step in the sequence above successfully completed before proceeding to the next step.

The upgrade process usually cannot be done simultaneously on all appliances (Central Manager, Aggregator, Collector and Managed Units) and all S-TAPs at the same time. During the upgrade transition, the customer will have a hybrid version of different v9.x Guardium systems. While this "hybrid mode" is supported by Guardium, many functions are limited until all components are at the same version. Therefore, it is strongly recommended to complete the upgrade in a timely manner and have all Guardium components at the same version and the same patch level.

Choose the correct upgrade scenario:

- Upgrade an existing 32-bit Guardium system: download the 32-bit GPU p750 patch from Fix Central and apply it.
  Refer to the Upgrading section of the Guardium 9.5 Knowledge Center at
  http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.nex.igsec.doc/g95_welcome.html
- Upgrade an existing 32-bit Guardium system to a 64-bit Guardium system: (1) run system backup; (2) rebuild using the latest v9.5 64-bit .ISO image; (3) apply the GPU p750 64-bit patch; and, (4) restore backup. Refer to the Upgrading section of the Guardium 9.5 Knowledge Center at
  http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.nex.igsec.doc/g95_welcome.html

- Install a new 32-bit Guardium system: download the latest v9.5 32-bit image from Passport Advantage, which includes the 32-bit V9.0 image and an older GPU, and the latest GPU p750 patch from FixCentral. The image contains the 32-bit V9.5 product. Install the .iso image on the 32-bit hardware, then apply GPU p750 patch. Refer to the Installing and Upgrading section of the Guardium 9.0 Knowledge Center at
  http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.nex.igsec.doc/g95_welcome.html
- Install a new 64-bit Guardium system: download the latest v9.5 64-bit image from Passport Advantage, the latest GPU p750 patch from FixCentral, and apply GPU p750 patch. . The image contains the 64-bit V9.5 product. Install the .iso image on the 64-bit hardware. Refer to the Installing section of the Guardium 9.0 Knowledge Center at
  http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.nex.igsec.doc/g95_welcome.html

Health check patch dependency

Health check patch 9997 must be installed before installing the v9.0 patch 750 (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. Use the latest version of health check patch - at least April 3, 2017 or newer.

Note: Health check patch 9997 installed for an earlier GPU (for example, v9.0/9.5 GPU patch 500) needs to be installed again for v9.0/9.5 GPU patch 750 (make sure to download and install the latest version of Health check patch 9997 prior to running GPU patch). Use the latest version of health check patch - at least April 3, 2017 or newer.

For further information on health check patch 9997, refer to

http://www-01.ibm.com/support/docview.wss?uid=swg21650612

Reinstall security patches

All security patches up to and including 6022 are included in v9.5 GPU p750. Security patches greater than 6022 must be reinstalled after installing this GPU.

Central Manager and SSLv3 behavior with v9.5 (patch 750)

Guardium and SSLv3 protocol vulnerability

POODLE ("Padding Oracle On Downgraded Legacy Encryption") is a SSLv3 protocol vulnerability. It allows attackers to downgrade SSL/TLS protocol to version SSLv3, and then break the cryptographic security (for example, decrypt the traffic, hijack sessions, etc.)

The vulnerability is detailed in Java Advisory 2311 and Oct 2014 CPU for Java including CVE-2014-3566, SSLv3 POODLE Attack.

Vulnerable Guardium products: GPU versions prior to 9.0p500, 32-bit and 64-bit (for example, GPU p300, 32-bit and 64-bit or without p9501/p9502.)

Vulnerable components: RedHat OpenSSL library, Java 6, Tomcat Server configuration

If conditions

Upgrade GPU	
Upgrade managed units (MU)	SSLv3 disabled
Upgrade Central Manager (CM)	If SSLv3 enabled, keep enabled If SSLv3 disabled, keep disabled
.ISO installation, with the unit type of Manager	
Managed units	SSLv3 disabled
Central Manager	SSLv3 enabled
Backup Central Manager	If SSLv3 enabled, keep enabled If SSLv3 disabled, keep disabled

Notes:

1. Guardium recommends that SSLv3 be disabled.
2. However, in dealing with older versions that do not have patch 750 installed, if SSLv3 is disabled, the Central Management functionality will be impaired between the Central Manager and the managed units.
3. To ensure connectivity and limited downtime, the actions listed above will enable SSLv3. Recommendation - After all systems are patched to v9.0 patch 750, then run the CLI command, store sslv3 off

4. To see if SSLv3 is enabled, run the CLI command, show sslv3.
5. When switching from backup Central Manager to primary Central Manager, SSLv3 will be enabled from the source.

The following screenshot displays a system message on SSLv3 enabled or disabled.

Security updates since v9.0/9.5 GPU p700 (August 2016)

Patch name	
6022	Includes Patches: 9.0p6007, 9.0p6008, 9.0p6009, 9.0p6010, 9.0p6011, 9.0p6012, 9.0p6014, 9.0p6015, 9.0p6017, 9.0p6019, 9.0p6020

Security bug fixes

Bug#	**PSIRT #**	**Description**
55048	PSIRT 83837	Open Source Oracle MySQL Vulnerabilities
55087	PSIRT 82898	Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN
55146	PSIRT 85581	Linux kernel privesc: Dirty COW
55299	p6022	secure_file_priv is causing error with extraction of data for Enterprise Search

Guardium Patch Update (GPU) 9.0 p750 patches/ bugs fixed

Appliance Patch (Fixcentral heading)

Includes patches since GPU p700 (August 2016): 701, 702, 703, 1087, 704, 705, 1088, 706, 707, 708, 709, 710, 711, 712, 713

Includes one Security Update since GPU p700 (August 2016): 6022

(*see table on previous page*)

Includes eight Sniffer Updates since GPU p700 (August 2016): 4067 to 4074

(*see separate Sniffer Update table after patch table*)

Fix #	Ad-hoc patch#	Guardium Bugzilla#	APAR	Description of Fix
1.	701	54175		Allow multiple targets for distributed reports
		54998		Fix import of query with computed attribute
2.	702	55006	GA15902	Fix SAP OBSERVED method
3.	703	50786		Add functionality to modify distributed report definition
		54175		Allow multiple targets for distributed reports
		54927	GA15890	Fix error "problem connecting to server" when naming an Audit Task with # in the name
		54998		Fix import of query with computed attribute
		55066	GA15902	Fix SAP OBSERVED method
4.	1087	55004	GA15907	Correct change in Turkey time zone
5.	704	55188		Fix DPS file not decrypting when loading
6.	705	54876	GA15915	Fix instance of Last ping status is not showing the correct time
7.	1088	55196		Fix instance of inability to link RULE and RULE ACTION Entities
8.	706	54695	GA16000	Enhance CLI Host Name Cache Handling

Fix #	Ad-hoc patch#	Guardium Bugzilla#	APAR	Description of Fix
9.	707			Shell injection in CLI command CVE-2016-6065
10.	708	55234	GA15940	Fix disk space calculation
11.	709	55126		Add GuardAPIs For Archive Purge Aggregation
12.	710	50029	GA15849	Fix UID Chain Scheduled Job Exception
13.	711	55310	GA15997	Fix instance of Custom alert using Java class stopped working after applying patch p700
14.	712	55398		Fix instance of Application logging timing out
15.	713	55332		Fix instance of failure in importing a custom domain built on a computed timestamp attribute

Sniffer Updates since GPU p700

Sniffer Updates since GPU p700 (August 2016): 4067 to 4074

	Sniffer update	Guardium Bug #	APAR	Description
1.	4067	52785	GA10827	Application Username missing for some traffic
		54276		Access rule EVERY checkbox on object field not working
		54881	GA15889	Records affected is incorrect
		54915	GA15893	70K length SQL was truncated
		54996		Show 4-byte UTF-8 characters
2.	4068	54034	GA15806	Traffic is not hitting rule that it should
		54070	GA15884	iSTAP reports wrong OSUSER
		54586	IT17275	Buffer usage monitor report showing 0 for eth-0 column on V9
		54817	GA15910	Sometimes GuardApp event fields Event Type 0 and Event Value Str blank in Entity Policy Rule Violation but are with Entity SQL
		54851	GA15992	Teradata - some SQL errors are being logged as both Login_Failed and sql_error
		55012	GA16010	Only the first one of three SQLS executed in a JDBC batch are captured
3.	4069	54174	GA15817	.NET application executes store procedures and either we see sp(null,null) as values or we see meaningless information as parameter values
		54625	GA16006	STAP in DB server causing the Oracle database to have performance issues and the eviction of nodes as well as use High CPU.

	Sniffer update	Guardium Bug #	APAR	Description
		54823	GA15998	Mainframe policy pushdown not successful
		55081	GA15911	Parser errors with SQL Server and Oracle
		55140	GA15952	Garbled Source Program in Teradata traffic collection
4.	4070	54695	GA16000	Server Host Name is Blank in report and capturing data from wrong database in a load balancing
		55089	IT18087	Guardium does not mask/escape character \= (equal) in the SQLNonString value of default alert message template
		55190	GA16001	Policy not capturing after installing GPU 700
5.	4071	52246	GA16002	Combine DDL alters to speed up patch installation (aggregators)
		55248	GA15936	Select statement is logged as with SQL Verb
6.	4072	52420	GA15970	IGNORE STAP SESSION rule appearing to ignore traffic inconsistently
		54851	GA15992	Teradata - some SQL errors are being logged as both Login_Failed and sql_error
		55186	GA15980	Failure to capture INSERT statements while running script in SQL
		55309	GA16009	Mainframe DBs timestamps are not converted to local Time zone of the collector
		55365	GA15969	Oracle EBS application user translation not capturing SYSADMIN user
		55370	GA15971	Additional check for binary traffic to prevent sniffer crash condition.
		55377	GA15976	Sniffer stops related to Oracle prepared statements and bind variables

	Sniffer update	Guardium Bug #	APAR	Description
		55390	GA15977	Guardium is capturing user passwords in DB User field 'Cassandra'
7.	4073	55380	GA16005	DB user appearing as ? occasionally
8.	4074	55367	GA16033	Policy might misfire when using 5- or 7-tuple policy rule and number of group members exceeding 32
		55477	GA16032	DB_USER field recorded incorrectly in syslog

List of bugs fixed, v9.x GPU p750

Bug #	APAR	Description
45386	GA16043	Results archive: "Create TURBINE_TMP_DB - Clone Failed"
48980		Invalid Query error when using Custom table joins on Dataset fields
50387		Use 64-bit key sent by UNIX STAP for session management
50401		Add possibility to use different regex libraries in logger rules.
50786		Add functionality to modify distributed report definition
51637		Add MySQL Data Types support Phase II
52246		Combine DDL alters to speed up patch installation (aggregators)
52420	GA15970	IGNORE STAP SESSION rule appearing to ignore traffic inconsistently
52785	GA10827	Fix instance of Application Username Missing for some traffic
53645		Allow customers to check/repair tables in major databases
54034	GA15806	Fix instance of traffic is not hitting rule that it should
54082		Fix memory leak in RestAPI
54174	GA15817	.NET application executes store procedures and either we see sp(null null) as values or we see meaningless information as parameter values
54175		Need to allow multiple targets for distributed reports
54276		Fix instance of checkbox for object field not working on Access rule
54625	GA16006	STAP in DB server causing the Oracle database to have performance issues and the eviction of nodes as well as use High CPU.
54695	GA16000	Server Host Name is Blank in report and capturing data from wrong database in a load balancing
54708		Regression in Analyzer Rule for pattern
54817	GA15910	Sometimes GuardApp event fields Event Type 0 and Event Value Str blank in Entity Policy Rule Violation but are with Entity SQL
54823	GA15998	Fix instance of mainframe policy pushdown not responded
54828		Export USER_ROLE DM
54839		v9 RPM installations printing "warning: user guard does not exist - using root"
54851	GA15992	Teradata - some SQL errors are being logged as both Login_Failed and sql_error
54856		Investigation dashboard refreshes without returning data when applying certain filters
54873		Access queries failing in GPU700 that work in GPU600
54876	GA15915	Fix instance of last ping status is not showing the correct time
54881	GA15889	Records affected is incorrect

Bug #	APAR	Description
54885		Fix instance of dynamic tables on the Central Manager /Aggregator are corrupted by Aggregation
54905	GA15923	TSM restore giving error ANS2039E Invalid destination file specification '/var/dump/TURBINE/736528-dam1.intra.ca.ma-w20160719.050002-d2016-07-18.dbdump.enc' entered
54915	GA15893	70K length SQL was truncated
54918		GPU 700: "store certificate alias" command fails to accept certificate after storing root certificate in keystore
54920		GPU 700: "restore certificate sniffer backup" results in :error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_lib.c:647:Expecting: TRUSTED CERTIFICATE
54923		Fix instance of thread idx in tuple group
54927	GA15890	Error "problem connecting to server" when naming an Audit Task with # in the name
54930		DLS doesn't work for custom domain on Managed Unit
54950		Computed attribute is created with wrong type
54953	GA16042	Invalid Custom Query Error
54954	GA15988	Aggregation/archive log incomplete for Managed Units
54956		Restore database from Managed Unit/collector overwrites MANAGER_IP value
54979		Fix instance of Informix parser errors
54990		Running VA causes java.lang.NoClassDefFoundError: org/apache/commons/lang/StringEscapeUtils
54996		Could not show 4-byte UTF-8 characters
54998		Import of query with computed attribute failed
55004	GA15907	Turkey change in time zone
55006	GA15902	Fix instance of SAP OBSERVED method not working in recent v9 patches
55012	GA16010	Only the first one of three SQLs executed in a JDBC batch are captured
55032		MongoDB: User traffic with SSL and LDAP has no db_user
55045		PSIRT 82343 - OpenSource Spring Source/Pivotal Spring Framework Vulnerability
55048		PSIRT 83837- Open Source Oracle MySQL Vulnerabilities
55051		Backport changes from v10 to improve logger performance after the fixes to bug 54915
55055		Fix Datamart CSV export and Unit type
55063		packet_run slon fails on packet 97760 - parser problem for bind variable in Oracle

Bug #	APAR	Description
55074		Merged from trunk: Failing Test Case "1.1 check GUI elements are editable only on appropriate selection" when executing Test Execution Record "1.1 check GUI elements are editable only on appropriate selection_Firefox
55078		Password logged in clear text in Guardium User Activity Audit
55081	GA15911	Fix instance of parser errors with SQL Server and Oracle
55084		Prepare to migrate guard_agg_keys.dir and guard_agg_keys
55087		PSIRT 82898- Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN
55088		Add info to system must gather for "Too many connections" investigation
55091		CSV Export: define Classification Process Log Datamart
55097		Allow to change Datamart initial start for File type DM via grdapi
55120		CSV Export:Modify "Export:User - Role" datamart
55122	GA15960	grdapi set_expiration_date_for_restored_day only change one restore from a group of restores
55126		Add GuardAPIs for archive purge aggregation RFE 32094 32092 33248
55127		Postgres parser errors for array types
55131	GA15925	Fix instance of cm_sync_file.tgz Failed ERROR: backup failed 2.
55140	GA15932	Garbled Source Program in Teradata traffic collection
55146		PSIRT 85581 - Linux kernel privesc: Dirty COW
55147		HP Vertica statements cause parser errors
55162		Backport RTC 39656: after failover one report has Central Manager as both primary and secondary target
55167	GA15919	ALERT_LOG growing large and affecting the Central Manager performance
55182	GA16044	Failed to Generate Utilization records for LOCAL Host - Central Manager missing from Unit Utilization Report
55186	GA15980	Fix instance of failure to capture INSERT statements while running script in SQR
55188		The DPS file will not decrypt when attempting to load it
55190	GA16001	Policy not capturing after installing GPU 700
55196		Fix instance of cannot link RULE and RULE ACTION Entities
55202	GA15932	Data from JDBC connection not logged- possible parser error
55212		Aster (Postgres) parser errors
55213	GA15961	UI stops when patch p4067 is selected and tried to schedule
55216		Fix instance of problem with PostgreSQL custom id procedures
55217		Fix instance of MYSQL Parser Error
55218		Fix instance of DB2 Parser Errors
55220		Fix instance of Oracle Parser Errors
55234	GA15940	Fix instance of slow v9 p700 Central Manager/Aggregator

Bug #	APAR	Description
55238	GA15926	Oracle 'audit grant xxxx' sql always has 'audit grant type' as construct
55248	GA15936	Select statement is logged as with SQL Verb = (
55250		Regression: create table cannot be captured as alert in specific policy
55252		Regression: Extrusion rule cannot work with defined sql pattern and data pattern together
55255		Change the error in the nanny.pl, refer to documentation
55258		Update Redhat and IBM Java time zone files/RPMs
55286		No Server Host Name / Group in GDM_INSTALLED_POLICY_RULES
55291		V10 P120 - App User Name truncate user
55299		Fix instance of secure_file_priv is causing error with extraction of data for Enterprise Search
55309	GA16009	Mainframe DBs timestamps are not converted to local Time zone of the collector
55310	GA15997	Custom alert using java class stopped working after applying patch p700
55321	GA15981	Failure to schedule policy installation via "grdapi schedule_job" command
55327		MySQL bind variables problems
55332		Fix instance of failure in importing a custom domain built on a computed timestamp attribute
55334		Back port v10 empty tuple group behavior to v9
55358		File Server: Absolute path to patch in file server upload directory is incorrect resulting in patch registration failure
55360		Improve classifier policy and rule delete performance
55361		Add checking for crashed/corrupted tables into the migration as a pre-requisite.
55364		Datamart CSV export modifications
55365	GA15969	Oracle EBS app user translation not capturing SYSADMIN user
55369		guard_filetransfer.pl doesn't return error code when it should
55370	GA13971	Fix instance of Sniffer stopping
55374		Only the first one of three SQLs executed in a JDBC batch are captured
55386		QUERY_DOMAIN_ENTITY gets wrong IDs when importing definitions of custom domain
55390	GA15977	Guardium is capturing user passwords in DB User field 'Cassandra'
55397		Fix instance of Netezza parser error
55398		Application logging times out randomly - Porting from v10.1
55403		GDM_SESSION_LIVE is missing two columns (SESSION_KEY CALLER_ID)
55422		File Server: Implement a non-SSL option for file server to allow for communication over port 80
55442		COPY_FILE_BUNDLE_NAME cannot be null" error on creating a datamart RTC 40837

Bug #	APAR	Description
55446		Upload to Guardium system locally-built bundle STAP with _801
55448		Add CLI command to find crashed tables
55474	GA15028	Regression of bug# 46808 seen in GPU p600 for support clean CENTERA_FILES

Known issues, V9.0/v9.5 GPU p750

1. V9.x UNIX S-TAP does not support a kernel ≥ 3.19.

2.

Bugzilla	RTC	APAR	Description
55419/ 49156		GA15982	Alerts can't be disabled/enabled from the list in Anomaly detection panel v9.x GPU p600 or later - Alerts can be disabled/enabled locally from the alert definition GUI page in the Guardium application, either standalone or Central Manager. If the environment is centrally managed, alerts must be disabled/enabled from the alert definition GUI page for the Central Manager

3. **Functionality: Distributed reports**

Issue: Report error for reports where Central Manager was target after failover.

Description: "Error in generating report/monitor, Table does not exist"

For a scheduled report with Central Manager as target, after Central Manager has been failed over to secondary Central Manager (which was not a target before the failover), user will see report showing an error message "Error in generating report/monitor, Table does not exist". This message will be resolved when the report runs on its next schedule.

For immediate report, after the Central Manager has failed over to backup Central Manager and you see the error "Error in generating report/monitor, Table does not exist", please re-create the immediate report.

4. **After restoring the backup, manually restart guard_sender**

The CLI command, restart stopped services only restarts Tomcat, Classifier, snif, snif_buf, and sql_session. After restoring the backup, the user can start guard_sender manually if needed.

5. Policies Rule Acton - **Quick Parse No Fields** - Do not parse fields in the SQL statement. All quick parse rules are only applied if SQL string is greater than 100 characters.

6. CAS TLS port(port 16019) is not in listening mode.

Database Access Format

In v9.0 GPU 700, Guardium changed the internal database access format. As a result, older ad-hoc patches may not be compatible with the Guardium system on v9.0 GPU 700 or higher.

If an older patch is not compatible with v9.0 GPU 750, during patch installation, an error message will appear.

In CLI, the error message is:

> Patch not compatible with this appliance. This patch contains an old access format.

In the GUI, the error message is:

> Patch Installation Failed - Patch not compatible with this appliance (access format)

In case the functionality from an incompatible patch is not included in v9.0 GPU 750, and is still required, request Guardium Customer Support to provide a new patch.

Language Pack

SqlGuard-9.0p1089_Language_Update_GPU_750

Separate versions for 32-bit and 64-bit

SqlGuard-9.0p1089_Language_Update_GPU_750_32-bit.tgz.enc

SqlGuard-9.0p1089_Language_Update_GPU_750_64-bit.tgz.enc

The language pack is separate from GPU p750.

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 750), it is important that Guardium users install the language pack before installing any other patches on a system that has GPU patch 750 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 750.

Note: The language pack is not needed to install GPU patch 750 on an English Guardium system, but the language pack must be installed on a non-English Guardium system.

Question #1: Should V9.0 patch 750 be applied again after the language pack is installed?

Answer:

No, do not apply V9.0 patch 750 twice. If upgrading a Guardium English system with v9.0 GPU patch 750, 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 750 before the language pack on a non-English system?

Answer:

V9.0/9.5 GPU patch 750 will not install on a non-English system that does not have the language pack installed beforehand.

Online help available via Web

The online help is included in the Guardium 9.0/9.5 Knowledge Center on the Web at:

http://www-01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.nex.igsec.doc/g95_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.

Use this link to retrieve a list of all public URLs for V9.0/9.5:

http://www-01.ibm.com/support/docview.wss?&uid=swg27045362

Links to System requirements/ Technical requirements for v9.5

V9.5 System Requirements (Platforms Supported) (June 2016)

32-bit and 64-bit

http://www-01.ibm.com/support/docview.wss?&uid=swg27045286

V9.5 Software Appliance Technical Requirements (August 2015)

32-bit and 64-bit

New hardware configurations (6)

http://www-01.ibm.com/support/docview.wss?&uid=swg27045285

2017 April 21