IBM Security Guardium

Health Check Patch Release Notes

Package name:

Health Check for v11 upgrade installation (Mar 1 2023)

Filename	**MD5Sum:**
SqlGuard-10.0p9998.tgz.enc.sig	e55f8ead91a753d1b8a05243f5da8eea

Dependencies:

Overview:

==========

The purpose of the patch is to perform preliminary checks on the Guardium appliance before v11 upgrade installation in order to prevent potential issues during the upgrade.

This patch can be installed more than once.

The health check generates a log file named *health_check_9998.<time_stamp>.log*.

In order to view the log file, perform the following actions:

1. type *fileserver* command in cli
2. open the fileserver in web browser
3. go to *Sqlguard logs->diag->current* folder and open the log file

The log file will contain a status of each validation.

In case any one of these validations has failed, the status of the failed validation will start with an "ERROR:" prefix and the following message will appear at the end of the log file:

Please send this log file and <file_name> file to support team.

In case when validation is completed with a warning (validation has failed but it will not fail the upgrade), the status of the failed validation will be “DONE”, but the following message will appear at the end of the log file:

Please send this log file and <file_name> file to support team.

In this case the output has to be sent to support in order to prevent potential issue during the upgrade.

If no problem was found, the following message appears at the end of the log file:

Appliance is ready for GPU installation/upgrade.

Since GPU 10.6 output of each Health Check run is available in predefined UI Report “Health Check Log”.

The following will be checked by the patch:

Appliance Configuration Check:

- There is NO issue with DB size (used DB space is less than 80%).
- In case DB used space is greater than 80%, the following message appears in the output file:
  ERROR:DB is more than 80% full.
  Please reduce size of your DB and run Health Check again.
- In case DB used space is between 50% and 80%, the following message appears in the output file: WARNING:DB is more than 50% full.
  Please reduce size of your DB and run Health Check again.

  In this case we do not fail the patch, but strongly recommend to ask support to investigate the issue before GPU installation.
- There is NO issue with disk space
- In case /var partition has less than 9G of free space, the following message appears in the output file: ERROR:/var partition has less than 9G of free space.
- In case / partition has less than 1.5G of free space, the following message appears in the output file: ERROR: root partition has less than 1.5G of free space..

Note: Health Check will delete unnecessary metadata files from root partition.

Custom Query Check :

- In case customer has custom queries with the same name that are going to be added by GPU, the following message will appear in log file:
  ERROR: Duplicate query names found.

- In case no custom queries found with the same name that are going to be added by upgrade, the following message will appear in log file:
  No duplicate queries found.

MySQL Table Corruption Check:

- In case there are any crashed tables found in the main databases, the following message will appear in the log file:
  ERROR: Crashed tables have been found.

- In case no crashed tables are found, the following message will appear in the log file:
  No crashed tables found.

Custom Domain ID Check

- This patch finds and resolves Domain ID contentions in Custom Domain meta data and prints the following message in the log file:

  Updating domain entity id completed

Create Tivoli link

- In order to save space on / partition, we move tivoli directory to /var partition and create link to it. In case link already exists or successfully created by this patch, the following message will appear in the log file: “tivoli link points to /var/local/tivoli”

- In case there is no /opt/tivoli directory on the appliance, it not need to be removed and linked. The following message will appear in the log file “/opt/tivoli does not exist, no need to link it.”

- In case the /opt/tivoli link exists but not valid, the following message will appear in the log file: “WARNING: link /opt/tivoli points to not existing directory.”. This should not prevent GPU installation, but is recommended to check with support the possible reason for the warning.

Create solr7 link

- In case solr7 directory already exists, the following message will appear in the log file: **“**/var/IBM/Guardium/data/guard-solr7 exists, no need to create it.”
- In case solr7 directory does not exist, the following message will appear in the log file: **“**/var/IBM/Guardium/data/guard-solr7 was created and linked .”
- In both cases the status of the Health Check will not be affected

Check VALIDATE_CERTIFICATE_HOST parameter

- In case the parameter was set before GPU 600 or higher installation, it should be reset to default value 0 (disabled) in this case the following message appears in the log file: “VALIDATE_CERTIFICATE_HOST was set to 'disable' (default).”
- In case the value is not set or GPU 600 or higher is installed, the value of the parameter will not be updated and the following message appears in the log file: “VALIDATE_CERTIFICATE_HOST parameter was checked.”

Handle GDM_SESSION_PARTITIONS table.

- In Case there are records with session_apartition value ‘NONE’, such records should be delete and the following message appears in the log file: “GDM_SESSION_PARTITIONS table has been updated.”
- In Case there are NO records with session_apartition value ‘NONE’, the following message appears in the log file: GDM_SESSION_PARTITIONS is up to date.

Check Hardware Version

In order to prevent failure of upgrade because of firmware version, we want to verify that current version of it will not cause upgrade issues.

- In case when hardware is not 3550 M4 or 3550 M5 or SR630 (M6), patch will NOT fail and the following message will appear in the log file: “Hardware is not a recognized type. Skipping version check.”
- In case hardware version need to be checked and the check passes, the patch will NOT fail and the following message will appear in the log: “<Hardware version info>. Hardware version check passed.”

For each of the supported models/types, the health check verifies the following:
x3550 M4 – Type 7914:
· DSA: >= 9.54
· IMM: >= 7.40
· UEFI: >= 3.10
x3550 M5 – Type 8869/5463
· DSA: >= 10.5
· IMM2: >= 5.40
· UEFI: >= 3.11
SR630 (M6) – Type 7X02:
· BMC/XCC: >= 4.20
· LXPM: >= 1.90
· UEFI: >= 2.61

- In case hardware version does not pass the verification, the patch will fail and the following message will appear in the log file: "ERROR: Hardware version check failed. Please apply the latest firmware patch from IBM Fix Central"

Check Custom Partitions

Appliance with custom partitions can not be upgraded and should be rebuilt.

- In case /boot partition is missing, the following message will appear in the log file:

  ERROR: FOR UPGRADE TO v11 APPLIANCE SHOULD BE REBUILT - no boot partition.

- In case / partition is missing, the following message will appear in the log file:

  ERROR: FOR UPGRADE TO v11 APPLIANCE SHOULD BE REBUILT - no root partition.

- In case /var partition is missing, the following message will appear in the log file:

  ERROR: FOR UPGRADE TO v11 APPLIANCE SHOULD BE REBUILT - no var partition.

- In case any non-standard partition is found, the following message will appear in the log file:

  ERROR: FOR UPGRADE TO v11 APPLIANCE SHOULD BE REBUILT - non-standard partition

- In case multi-disk installation is found, the following message will appear in the log file:

  ERROR: FOR UPGRADE TO v11 APPLIANCE SHOULD BE REBUILT - multi-disk installation is not supported

- In case no custom partitions are found, the following message will appear:

No custom partitions found

Drop obsolete columns

In order to prevent failure during insertion of analytic data collected from collector, an obsolete column AVG_EXECUTION_TIME should be dropped from the AGG_ANALYTIC_INPUT table in DATAMART DB.

In case the column is found, the following message will appear in log file:

Obsolete column DATAMART.AGG_ANALYTIC_INPUT.AVG_EXECUTION_TIME has been dropped.

In case the column was not found, the following message will appear in log file:

Obsolete column DATAMART.AGG_ANALYTIC_INPUT.AVG_EXECUTION_TIME was not found.

Find Default Routes

Default route is not allowed in Guardium v11 and should be removed.

In case default routs are found, the following message will appear in log file:

ERROR: Default route is not allowed in Guardium v11, please remove it or use the gateway settings after that will appear the list of found default routes

Check latest GPU

In case the highest GPU installed on the appliance is 10.5 or lower, the Health Check fails, and the following message will appear in log file:

ERROR: The latest installed GPU is <number of the highest installed GPU>. Please upgrade to at least 600.

Check whether any 10.5 or earlier version STAP is used by the appliance

Because v10.5 and earlier Unix and Windows S-TAPs are not supported in v11.3, if Health Check finds any of those, for each one the following message will appear in log file.

ERROR:<tap type> on <tap host> should be upgrade to version 10.6 or higher.

Check for old partitions

In case partitions older than purge age plus 60 days exist, the health check fails and following message will appear in the log file:

> ERROR: Old partitions found. The oldest partition is <date> while expected oldest date is <date>. Please run support must_gather patch_install_issues and contact support to clean up old partitions

In case old partitions exist, but only in GDM_SESSION table and the oldest partition contains active sessions, the health check passes and following message will appear in log file:

> Old partitions found only in GDM_SESSION containing active or recently closed sessions. The oldest partition is <date>

Old partitions have multiple causes. The correct course of action to clean them up should be determined in consultation with Guardium support. Old partitions diagnostic file from patch must gather diag/current directory will help to determine the next steps. For more information check https://www.ibm.com/support/pages/node/6564421

Check for old data

In case data older than purge age plus 60 days exists in the oldest partition, the health check fails and following message will appear in the log file:

> ERROR: Data older than purge period + 60 days found in oldest partition. Please run support must_gather patch_install_issues and contact support to clean up old data

If old data is existing on the appliance oldest partition, upgrade to v11.0 will recreate partitions based on this data, causing old partitions problems after upgrade. The correct course of action to clean them up should be determined in consultation with Guardium support. For more information check https://www.ibm.com/support/pages/node/6564421

Note: This list is subject to change/expand with later versions of the Health Check patch to include additional checks, if required.