IBM Security Guardium

Health Check Patch Release Notes

Package name:

Health Check for GPU and Upgrade installations (Nov 7 2023)

Filename	**MD5Sum:**
SqlGuard-11.0p9997.tgz.enc.sig	6a446a3042eb48f4fc8b76b05ab651f0

Dependencies:

Overview:

==========

The purpose of the patch is to perform preliminary checks on the Guardium appliance before v11 GPU installation 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.<time_stamp>.log*.

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.

Output of each Health Check run is available in predefined UI Report “Health Check Log” and overall result of the patch is available in UI report “Installed Patches” or cli – “show system patch installed”

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.*

- Installed patch report will show the patch with status: *ERROR: Patch Installation Failed*

In case when validation is completed with a warning (validation has failed but it will not block 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.*
- Installed patch report will show the patch with status: *WARNING: Review health check log file.*

In this case the output should be checked, following steps in these release notes. Output might have to be sent to support to prevent potential issue during the upgrade.

In case no problem was found:

- The following message appears at the end of the log file: *Appliance is ready for GPU installation/upgrade.*
- Installed patch report will show the patch with status: *DONE: Patch installation Succeeded.*

On Guardium versions that do not include warning status functionality, p9997 will automatically re-install itself to add the warning status. No extra action is required when installing. You may notice p9997 moves from post install stage back to preparing to install stage before completing. Conditions where p9997 will re-install:

- Appliance is on Guardium bundle including and before - v11.4 p440, v11.3 p370, v11.2 p275, v11.1 p160, v11.0 p50
- P9997 check results in warning status
- P9997 from Aug 25 2022, or later has never been installed and generated warning status before

In cases where there is a re-install of p9997, there will be two sets of health check log files. Review the most recent one based on the date-time in the file.

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 30G of free space, the following message appears in the output file: ERROR:/var partition has less than 30G of free space.

- In case / partition has less than 2.5G of free space, the following message appear in the output file: ERROR: root partition has less than 2.5G of free space.

- Appliances built on earlier versions with 10G / partition should be rebuilt when upgrading to v11.5. This is to ensure sufficient / space for the appliance to work.

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.

Custom Entity Tables 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 entity table 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 entity table names 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.

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.

  Guardium support should investigate the issue before GPU installation.

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

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 Network Role

In order to prevent failure of upgrade because of wrong network configuration, the patch will verify rolemap file content

- In case configuration is correct, the following message will appear in the log file: “No need to rebuild rolemap”
- In case configuration is wrong but can be fixed by the patch, the following message will appear in the log file: "Rolemap was successfully rebuilt"
- In case configuration is wrong and the patch can not fix it, the patch will fail and the following message will appear in the log file: "ERROR: Please escalate the issue to Guardium support for fixing network configurations" and the patch will fail to prevent GPU installation failure

Check for existing TURBINE_USER_GROUP_ROLE table

TURBINE_USER_GROUP_ROLE table may be missing due to previous database crash problems.

- In case this table is missing, the following message will appear in the log file: “ERROR: TURBINE_USER_GROUP_ROLE table does not exist or is corrupted”. Guardium support should be contacted to correctly rebuild this table.
- In case the table exists, no message will be written to the log file.

Check for maximum purge age on Aggregator

Note - This check only requires action if upgrading to v11.5 or above.

In v11.5 and above there is a new maximum purge age on aggregators due to limitations of underlying MySQL table engines. The maximum age is linked to the maximum number of collectors allowed to export to the aggregator, which is 10 by default and configurable. For 10 collectors the maximum purge age is 759 days (2 years, 29 days).

In case the purge age is over the maximum on aggregators, the patch will show warning status in installed patch report. The following message will appear in log file:

- ERROR for v11.5 and above: Current purge age (<current age>) is too high to install p500 or above. Lower the purge age below <max allowed age> or reduce number of collectors. This only applies for upgrading to v11.5 or above.

In case purge age is not over the maximum on aggregators, the following message will appear in log file:

- No issue with purge age for v11.5 upgrade.

If the purge age is over the maximum and it cannot be reduced, the maximum number of collectors allowed to export to the aggregator can be reduced using store max_number_collector.

For more information see - https://www.ibm.com/support/pages/node/6615287

Check for import file sizes on Aggregator

Note - This check only requires action if upgrading to v11.5 or above.

Time taken for v11.5 and above import jobs might be longer than previous versions due to underlying MySQL database changes. The time taken is dependent on the number of rows in import files. Longer time to run aggregation jobs is only a problem if it causes impact other scheduled jobs. For example, audit processes on aggregator might start before import is finished, resulting in missing data in the reports.

When installed on a central manager, p9997 runs checks on all managed aggregators to collect aggregation and schedule information for later analysis. The root passkey must be set on the managed aggregators to run the remote checks. There is also a local check on each aggregator or central manager p9997 is installed on.

In case there are days where total imported rows exceed 100 million, this is a strong indictor the schedule will need to be updated. The patch will show warning status in installed patch report. The following message will appear in log file:

- WARNING for v11.5 and above: Import of large number of rows found locally on this unit. Impact on aggregation job duration in v11.5 is likely. See health check release notes for more information and Fileserver->Sqlguard logs->diag->current->agg_schedule_check_results_<datetime>.tgz for details of scheduled jobs.

When patch is run on the CM, in case there are days where total imported rows exceed 100 million on any managed aggregator. Message like above appears with list of logs for managed aggregators that exceeded threshold.

In case there are no days where total imported rows exceed 100 million, there is still a chance the schedule will need to be updated. The following message will appear in log file:

- INFORMATION for v11.5 and above: Impact on aggregation job duration in v11.5 is possible. See health check release notes for more information.

A set of log files is created in Sqlguard logs->diag->current->agg_schedule_check_results_<dateime>.tgz. On the central manager this contains results from all managed aggregators.

If p9997 shows a warning for this check, follow this technote to resolve potential problems - https://www.ibm.com/support/pages/node/6612043

Check for non-standard MyISAM partitioned tables

Note - This check only requires action if upgrading to v11.5 or above.

In v11.5 and above, MySQL database version does not allow MyISAM partitioned tables. Known standard tables are converted by GPU installation. In case there are any non-standard MyISAM partitioned tables they need to be altered or removed by Guardium support before upgrade to v11.5 and above.

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

- ERROR for v11.5 and above: Non standard MyISAM partitioned tables found. Contact support to remove or alter these tables to InnoDB. List of tables and schema: <table names>

In case no non-standard tables are found, the following message will appear in log file:

- No issue with non standard MyISAM partitioned tables.

Check for Windows S-TAP and Enterprise Load Balancer compatibility

Note - This check only requires action if upgrading to v11.5 or above.

Enterprise Load Balancer (ELB) on v11.5 and above Central Manager (CM) is not compatible with Windows S-TAPS with versions:

- v10.6, v11.0, v11.1, v11.2 – All versions
- v11.4 – Before 11.4.0.267
- v11.3 – Before 11.3.0.321

Windows S-TAP versions 11.3.0.321, 11.4.0.267 and all 11.5 and above are not affected. All other S-TAP types are not affected. Windows S-TAPs should be upgraded to the latest versions before upgrading CM to v11.5 and above.

In case ELB is active with Windows S-TAPS on affected versions, the following message will appear in log file on the CM only:

- WARNING for v11.5 and above: Windows S-TAP versions not compatible with Enterprise Load Balancer found. Upgrade S-TAPs before upgrading appliances. Problem S-TAPs, versions and collector they report to can be found in elb_windows_stap_check.log.

In case ELB is not active, or Windows S-TAPs on affected versions not found, the following message will appear in log file on the CM only:

- No issue with Windows S-TAP ELB compatibility.

If affected S-TAPs are found, elb_windows_stap_check.log is available from fileserver *Sqlguard logs->diag->current* folder. The log file lists all affected S-TAPs, their version and collector they report to.

Check for orphaned MySQL temporary files

Note - This check only requires action if upgrading to v11.5 or above.

If internal MySQL database shut down unexpectedly during alter table operations, orphaned temporary files might exist. The files can cause a problem for Guardium v11.0p500 installation. P9997 attempts to clean up these files automatically, but in some cases the cleanup might not be possible.

In case orphaned MySQL temporary files found but are actively in use by MySQL, the cleanup cannot run. P9997 should be reinstalled when no MySQL processes are running. In this case, the following message will appear in log file:

- ERROR for p500 Install: MySQL #sql- temporary files are actively in use. Reinstall p9997 during a quiet time when no MySQL processes are running. If p9997 repeatedly fails with this error, contact Guardium support and attach support must_gather patch_install_issues and system_db_info.

In case orphaned MySQL temporary files found and could not be cleaned up for any other reason, one of the following message will appear in log file:

- ERROR for p500 Install: Cleanup of MySQL #sql- temporary files found files that could not be automatically removed. Contact Guardium support and attach support must_gather patch_install_issues and system_db_info.

- ERROR for p500 Install: Cleanup of MySQL #sql- temporary files ran with errors. Contact Guardium support and attach support must_gather patch_install_issues and system_db_info.
- ERROR for p500 Install: MySQL #sql- temporary tables found in data dictionary but not filesystem. Contact Guardium support and attach support must_gather patch_install_issues and system_db_info.

In case orphaned MySQL temporary files found and were successfully cleaned up, the following message will appear in log file:

- Cleanup of MySQL #sql- temporary files succeeded.

In case no orphaned MySQL temporary files found, the following message will appear in log file:

- No issue with orphaned MySQL temporary files.

For more information and steps to follow see – https://www.ibm.com/support/pages/node/6827635

Check for GDMS tables older than the purge age

Note – This check only requires action if installing v11.0p500

Aggregator appliances use GDMS database if purge age is over 90 days or more than 10 collectors are used. If GDMS is in use and tables exist older than the purge period, p500 can fail when converting data. Purge should be run successfully and p9997 installed again before installing p500.

In case data older than purge period found in GDMS database, the following message will appear in log file:

- ERROR for p500 install: Tables found in GDMS database older than purge age. Run purge again to remove old data. If p9997 fails after running purge again contact Guardium support and attach support must_gather agg_issues.

In case no data older than purge period found, the following message will appear in log file:

- No issue with GDMS old tables

In case GDMS is not in use or appliance is collector, no message will appear in log file.

Check for GDMS older data in new table

Note – This check only requires action if installing v11.0p500

Aggregator appliances use GDMS database if purge age is over 90 days or more than 10 collectors are used. If GDMS is in use and there is data older than the purge period in a GDMS table that is within the purge period, p500 can fail.

In case older data is found in newer table, the following message will appear in log file:

• ERROR for p500 install: Old data found in GDMS tables within purge age. Check p9997 release notes for steps to resolve.

In case older data is not found, the following message will appear in log file: • No issue with old data in GDMS tables within purge age

If this error is seen, contact Guardium support to help investigate the issue.

Check for empty GDMS tables

Note – This check only requires action if installing v11.0p500

Aggregator appliances use GDMS database if purge age is over 90 days or more than 10 collectors are used. If GDMS is in use and some GDMS tables are empty, p500 can fail.

In case empty GDMS tables are found, the following message will appear in log file:

- ERROR for p500 install: Empty GDMS tables found. Check p9997 release notes for steps to resolve.

In case no empty GDMS tables are found, the following message will appear in log file:

- No issue with empty GDMS tables

For steps to resolve the problem see – https://www.ibm.com/support/pages/node/6847391

Check for multiple collector IDs in GDMS tables

Note – This check only requires action if installing v11.0p500

Aggregator appliances use GDMS database if purge age is over 90 days or more than 10 collectors are used. If GDMS is in use and some GDMS tables have multiple collector ID, where one of those IDs is -1, p500 can fail.

In case multiple collector IDs are found, the following message will appear in log file:

• ERROR for p500 install: Multiple collector IDs including ID -1 found in GDMS table. Check p9997 release notes for steps to resolve.

In case multiple collectors IDs are not found, the following message will appear in log file: • No issue with multiple GDMS collector IDs including ID -1

If this error is seen, contact Guardium support to help investigate the issue.

Check for p375 and kpatch-patch rpm

Note – This check only requires action if installing v11.0p400 or v11.0p500

V11.0p400 and v11.0p500 installation will fail if installed on an appliance where v11.0p375 was previously installed and a specific kpatch-patch rpm is present. The problem appears regardless of any sniffer patches installed.

In case p375 was installed and the rpm is present, the following message will appear in log file:

- ERROR for p400 and p500 install: p400 and p500 install will fail if specific kpatch-patch rpm is present. Other bundles will succeed. Check p9997 release notes for steps to resolve.

In case p375 was not installed or kpatch-patch is not present, no message will appear in log file.

For detailed steps to resolve the problem see – https://www.ibm.com/support/pages/node/6952241

In case device-mapper-multipath rpm is found on the appliance, the following message will appear in the log file:

- ERROR for p500 install: p500 install will fail if specific device-mapper-multipath rpm is present. Other bundles will succeed. Check p9997 release notes for steps to resolve.

In order to resolve the issue, patch SqlGuard-11.0p9990.tgz.enc.sig need to be installed.

Check for largest partitioned table

Note – This check only requires action if installing v11.0p500

V11.0p500 installation alters table engines on partitioned tables on aggregator type appliances. During the alter operation, temporary files are created. If the total size of the temporary files and the existing table files exceeds the remaining disk space, the alter will fail and p500 installation will fail. This is more likely to happen if one table is significantly larger than others on the appliance.

In case the largest partitioned table files will exceed remaining disk space when altered, the following message will appear in log file:

- ERROR for p500 install: Largest partitioned table will fill up /var space on upgrade. Reduce size of the largest table by purging data.

In case the largest partitioned table files will not exceed remaining disk space when altered, or appliance is already at v11.5 or above, the following message will appear in log file:

- No issue with largest partitioned table.

To resolve the problem, reduce the purge age so that the largest table is reduced in size. The issue can also be avoided by rebuilding the appliance to v11.5 and restoring a backup. If neither option is possible, contact Guardium support.

Check for xorg rpm conflict

Note – This check only requires action if installing v11.0p400 or v11.0p500

Ad-hoc patch v11.0p1020 contains an xorg rpm version that conflicts with the version in v11.0p400 and v11.0p500. The conflict causes the p400 and p500 install to fail.

In case the problematic rpm is found on the appliance, the following message will appear in log file:

- ERROR for p400 and p500 install: Rpm conflict with xorg rpm detected. Check p9997 release notes for steps to resolve.

In case the problematic rpm is not found, the following message will appear in log file:

- No issue with xorg rpm conflict.

For steps to resolve the problem see – https://www.ibm.com/support/pages/node/6960603

Check for duplicate alias entries

Due to a previous defect, duplicates might exist in ALIAS table. The defect is resolved in latest bundles, but the leftover alias entries might remain.

In case duplicate alias entries found, the following message will appear in log file:

- ERROR: There are duplicates in ALIAS table. Check p9997 release notes for steps to resolve.

In case no duplicate alias entries are found, the following message will appear in log file:

- No duplicates in ALIAS table found.

For steps to resolve the problem see – https://www.ibm.com/support/pages/node/7008419

Check for bad uploaded jar files

Note – This check only requires action if installing v11.0p500

Jar files for some functionality can be uploaded from GUI customer uploads page. If these files are not valid jar files they can cause v11.0p500 install to fail.

In case bad jar files are found, the following message will appear in log file, followed by a list of files:

- ERROR for p500 install: Bad jar files found in customer uploads directory. Contact Guardium support to resolve. Bad jar files:

In case the problematic rpm is not found, the following message will appear in log file:

- No bad jar files found.

To resolve the problem, contact Guardium support. If the files are not needed, they can be removed by support. The files would have to be inspected on a case-by-case basis

Check for old guard parameter name

Guard parameter with name 'cm_of_cms_hostname' is no longer valid as it has been renamed.

In case the old parameter name is found on the appliance, it is removed and the following message will appear in the log file:

- Old guard_parameter removed.

In case the old parameter was not found, no action is taken and no message appears in the log file.

Check for corrupt trigger files

Database trigger files may become corrupted in rare cases, which can block patch installation.

In case corrupted trigger files are found, the following message will appear in the log file:

- WARNING: Possible trigger file corruption. Contact Guardium support for further investigation

In case no corrupted trigger files are found, the following message will appear in the log file:

- No issue with trigger file corruption

Contact Guardium support to investigate possible corruption of the trigger files.