IBM Security Guardium

Health Check Patch Release Notes

Package name:

Health Check for v12 upgrade installation (Jan 30 2024)

Filename	**MD5Sum:**
SqlGuard-11.0p9998.tgz.enc.sig	f52ff9b59ca51fa8402f24480fc0e981

Dependencies:

Overview:

==========

The purpose of the patch is to perform preliminary checks on the Guardium appliance before v12 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*.

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.

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

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 20% and 80%, the following message appears in the output file:

- WARNING: DB is more than 20% full. Consider reducing size of your DB and run Health Check again.

In this case we do not fail the patch, but recommend to consider reducing database used space as much as possible before upgrade. Reduce space by decreasing the purge age. Reducing space used in the appliance database reduces time to complete the upgrade.

Check there is no issue with disk space.

In case there are old files in /boot partition that can be moved, the health check does it automatically and the following message appears in the output file:

- Old initramfs files moved from /boot to /var/tmp/p9998_initramfs_files

After automatically moving files, in case /boot partition does not have enough space to start the upgrade, the following message appears in the output file:

- ERROR: Not enough space in /boot for upgrade. Contact Guardium support and attach support must_gather patch_install_issues and system_db_info.

In case /var partition does not have enough space to start the upgrade, the following message appears in the output file:

- ERROR: Not enough space in /var for upgrade. Estimated space required - xMB. Actual space available – yMB

In case /var partition is more than 45% used, the following message appears in the output file:

- WARNING: /var disk usage is over 45%. Consider reducing /var disk usage before upgrade.

Reducing space used on the appliance /var partition reduces time to complete the upgrade. It is recommended to reduce space by purging as much data as possible.

In case swap partition has less than 11G of free space, the following message appears in the output file:

- ERROR: swap partition has less than 11G of free space.

In case swap partition size cannot be found by the health check, swap may be in an unexpected configuration. The following message appears in the output file:

- ERROR: Can not identify swap partition size.

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 upgrade, 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.

Check Hardware Version

To prevent failure of upgrade because of firmware version, verify that the version of firmware 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 is M4, the patch will fail and the following message will appear in the log:

- ERROR: M4 hardware is not supported by v12

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 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 cannot 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 v12 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 v12 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 v12 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 v12 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 v12 APPLIANCE SHOULD BE REBUILT - multi-disk installation is not supported

In case any other kind of custom partition setting is found, the following message will appear in the log file:

- ERROR: FOR UPGRADE TO v12 APPLIANCE SHOULD BE REBUILT - Custom partitions flag found.

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

- No custom partitions found

Check latest GPU

In case the highest GPU installed on the appliance is 11.4 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 500.

Check backup configured

V12 upgrade requires an external SCP or SFTP location to send data to. The GUI system backup configuration is used for this. In case system backup is not configured with SCP or SFTP options, the following message will appear in log file:

- ERROR: System backup is not configured correctly. It must be set in GUI System Backup page using SCP or SFTP options.

In case system backup is configured, but a test file failed to send to the location, the following message will appear in log file:

- ERROR: System backup is configured correctly but test connection failed. Confirm system backup settings in GUI.

In case system backup is configured and test connection works, the following message will appear in log file:

- System backup is configured correctly and test connection succeeded.

Check TLS version

V12 does not support TLS version below v1.2. In case TLS v1.2 is not available on the appliance, the following message will appear in log file:

- ERROR: TLS version is not correct for v12 upgrade.

In case TLS v1.2 is available, the following message will appear in log file:

- TLS version 1.2 is available

To manage the TLS version on appliances, see - https://www.ibm.com/docs/en/guardium/11.5?topic=system-managing-tls-version

Check Network Role

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 cannot 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

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 old partitions

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

- WARNING: 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

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 following message will appear in the log file:

- WARNING: 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 v12 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

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

Because v10.5 and earlier Unix and Windows S-TAPs are not supported in v12, 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.

10.6 is the minimum allowed version, but it is recommended to upgrade to v11.5

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 p9998 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

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

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

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

In case bad jar files are 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 GIM certificates

It is not possible to push new GIM bundles in v12 if the GIM certificates are using SHA1 certificates, including the default certificate on appliances. The GIM certificate must be updated to use custom SHA256. This can be done before or after v12 upgrade.

In case GIM certificates using SHA1 are found, the following message will appear in log file:

- WARNING: Non SHA256 GIM certificates found. To resolve install new SHA256 GIM certificates from cli.

In case there is no issue with the certificates, the following message will appear in log file:

- No issue with GIM certificates.

To install custom GIM certificates see - https://www.ibm.com/docs/en/guardium/11.5?topic=management-creating-managing-custom-gim-certificates

Check for aggregator flag

In case the unit type is aggregator, but an internal aggregator flag was missing, the flag will be created and the following message will appear in the log file:

- Missing aggregator flag automatically recreated.

In case flag already existed, the following will appear in log file:

- No issue with missing aggregator flag.

Check for import file sizes on Aggregator

Time taken for v12 import jobs might be longer than versions before v11.5 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, p9998 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 p9998 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: Import of large number of rows found locally on this unit. Impact on aggregation job duration 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: Impact on aggregation job duration 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 p9998 shows a warning for this check, follow this technote to resolve potential problems. The technote refers to v11.5, but the same applies on v12 - https://www.ibm.com/support/pages/node/6612043

Check for expired cli password

If cli user's password is expired, or the password is set to never expire, upgrade can fail. In case cli user password is set to never expire, the following message will appear in the log file:

- ERROR: Password for user cli never expires. The expiration must be set to a valid number of days and password reset

To resolve, the cli password expiry must be set to a valid number of days (1-60) using cli "store password expiration cli". The cli password must then be changed using cli "store user password", because it may

be older than the number of days just set. The password and expiry can be propagated from CM to all MUs using cli “support reset-managed-cli”.

In case cli user password is expired, the following message will appear in the log file:

- ERROR: Password has expired for user cli

To resolve, the cli password must be changed using cli “store user password”, or when prompted on cli login. The password can be propagated from CM to all MUs using cli “support reset-managed-cli”.

In case cli user password is not expired, the following message will appear in the log file:

- Password has not expired for user cli

Check for p12000 file in migration directory

If p12000 was previously installed and failed, the patch file is no longer available in the patches directory. P9998 health check will recover the p12000 patch file if it exists, so p12000 can be re-installed after resolving the cause of the failure. This means p12000 does not need to be re-uploaded to the appliance. If p9998 detects p12000 file to recover, the following message will appear in the log file:

- Patch restored from previous p12000 upgrade failure.

Otherwise, no message will appear in the log file.

Check for active threat analytics (ATA) cases

After upgrade to v12, existing ATA cases will appear with an incorrect Period End date. New ATA cases will not be visible. To resolve the problem after upgrade, install ad-hoc patch v12.0p4. In case ATA cases exist, the following message will appear in the log file:

- WARNING: Appliance might be using Active Threat Analytics (ATA). After upgrade to v12, existing ATA cases will appear with an incorrect Period End date, and new ATA cases will not be visible. To correct that, install ad-hoc patch 12.0p4.

It is possible to receive this warning, even if ATA is not actively used. If ATA is not used in the environment, v12.0p4 is not required after upgrade.

Check for system backup password decryption

There is a known issue with p12000 upgrade patch where some system backup passwords cannot be decrypted mid-way through the upgrade. This check detects if the current password will trigger the known issue on upgrade.

In case the password will trigger known issue, the following message will appear in the log file:

- ERROR: System backup password could not be decrypted and is invalid

In this case, the password on the backup server and GUI system backup must be changed. At the time of release of this check the exact triggering condition for the failure is not known, however one of the following can be tried:

  - Remove all special characters from the password
  - Reduce the number of special characters in the password
  - Move the location of special characters, for example change Pass!word to P!assword

Each time the password is changed, reinstall p9998 to verify if it is now valid. If there is any concern, contact Guardium support.

In case the password check cannot confirm the known issue, contact Guardium support. The following message will appear in the log file:

- WARNING: Could not confirm backup password validity

In case the password is valid for upgrade, the following message will appear in the log file:

- No issue with system backup password decryption

Check for system backup password with backslash

Backslash character "\" is not allowed in the password for backup server for p12000 upgrade patch. System data and config will work in v11, but p12000 will fail due to a known issue with password handling.

In case system backup password contains a backslash, the following message will appear in the log file:

- ERROR: System backup password contains backlash, it must be removed

In case there is no backslash in the password, the following message will appear in the log file:

- No issue with backslash in password

To resolve the problem, the password for the backup server must be changed to remove backslash characters.

Check for old host key algorithm on backup server

In v12, ssh communication with ssh-rsa host key algorithm is not allowed for security reasons. This is due to the underlying Redhat 9 OS in v12. Communication with backup servers with older OS e.g. Redhat 6 will fail. During upgrade, backup to an older server will succeed on v11 but upgrade patch will fail when v12 appliance restores from that server.

In case incompatible host key algorithm is found on the backup server, the following message will appear in the log file:

- ERROR: Backup server host key algorithm is not compatible with Redhat 9

In case the backup server algorithm is ok, the following message will appear in log file:

- No issue with backup server host key algorithm

In case the backup server algorithm could not be found, upgrade will not be blocked and the following message will appear in the log file:

- WARNING: Could not confirm if backup servers host key algorithm is compatible with Redhat 9

To resolve, use a backup server OS that can communicate with Redhat 9 via ssh.

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