Genesys

Genesys Management Framework

Migration of Management Framework 8.x Components

Technical Paper

Version 1.0

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

About Genesys

Genesys is the world's leading provider of customer service and contact center software - with more than 4,000 customers in 80 countries. Drawing on its more than 20 years of customer service innovation and experience, Genesys is uniquely positioned to help companies bring their people, insights and customer channels together to effectively drive today's customer conversation. Genesys software directs more than 100 million interactions every day, maximizing the value of customer engagement and differentiating the experience by driving personalization and multichannel customer service - and extending customer service across the enterprise to optimize processes and the performance of customer-facing employees. Go to www.genesys.com for more information.

Each product has its own documentation for online viewing at the Genesys Customer Care website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc. cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System’s Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Table of Contents

Purpose

This document contains recommended steps for migrating Genesys Framework 8.x components to ensure minimal possible downtime and impact on a production environment.

Upgrading Configuration Server

Prerequisites

- A Configuration Server High Availability (HA) pair must be configured in the database that is being migrated. Both servers of the HA pair are installed and configured properly. All new Installation Packages have being delivered to the relevant hosts and ready to be installed.
- The latest version of LCA must be installed on the Configuration Server hosts.
- The latest version of SCS must be deployed in the environment before proceeding with Configuration Server upgrade.

Planning for Upgrade

Plan your upgrade to begin with the master Configuration Server (HA pair, if applicable) and extend to all Configuration Server Proxies (HA pairs). When the upgrade procedure is completed, Genesys recommends that you run the same version of server components deployed as master and proxy, unless stated otherwise in the Configuration Server Release Notes. Both Configuration Servers configured as an HA pair must have the same version. If there are requirements for related components (such as DB Server), upgrade those components first.

Procedure

1) Back up your configuration database.

2) Install the new master Configuration Server instance (**Note:** If you have an HA pair of master Configuration Servers, start with the backup) but do not start it. When installing via the Installation Package, select **Configuration Server Master Backup** installation mode. At the prompt to provide a name for the Application object, specify the same name as the Application object that is currently running in backup mode, but select a new folder for your installation. Confirm that, in the configuration file of the newly installed server, the section name corresponds to the name of the application object for which this instance has been installed, and matches the value of the –s option in the command line to start this instance.

3) If database schema migration is required (upgrade to major versions), use Configuration Conversion Wizard (CCW) to convert the legacy database to a new format:

   a) Create a new database.

   b) Launch CCW and specify the new database as a target for conversion. The legacy database will be left intact, allowing the existing server to run. The server will be brought into read-only mode for a conversion period. Follow the instructions of CCW.

   c) For the new instance installed in Step 2, in its configuration file, specify the configuration parameters to access the new database. Leave the other parameters as is.

   d) Make sure the newly created database is updated with the valid license file by using the standalone utility as described in the *Framework Deployment Guide*, otherwise, the server will not start on the upgraded database. Re-validation of the license file is the mandatory step during the upgrade.

   e) If you are not using an HA pair of master Configuration Servers, proceed to Step 4.

   f) Modify the configuration file of the newly installed Configuration Server instance to include the `upgrade-mode=1` option to enable side-by-side startup without contacting the configured peer server.

   g) Update the configuration of the current primary SCS to include the following option `[general]disable-switchover=true` . This will ensure that SCS will not attempt to switch over any application that is starting in primary mode; instead it will log message 43-10326. Alternatively, you can stop LCA on the host where the newly installed Configuration Server is located.

4) Force the currently running Configuration Server into Read-Only mode to prevent any changes being made to your configuration during the switchover by using Genesys Administrator or Configuration Manager, or by implementing any other mechanism you may have to accomplish the same result.

5) Start upgrade with the backup instance first. Using the Management Layer, shut down the backup instance you are replacing. Refer to the Release Notes to confirm that there are no particular issues that may prevent two versions (new and old) from being launched as an HA pair. If there are issues, shut down the primary instance. This will cause some downtime for Configuration Server clients.

6) Back up the folder of the instance that is currently being shut down (by changing the folder name to be version-specific), and replace it with content of the relevant folder, prepared in Step 2.

7) Launch the new version of the Configuration Server instance from the replaced folder and wait for it to initialize. This initiated instance will become the backup server. Make sure it completes initialization before continuing.

- If you are not using an HA pair or have both Configuration Servers down, the time when the server instance completes initialization will end the downtime window for Configuration Server clients. It also completes the upgrade of the master Configuration Server and you do not need to continue with the rest of the steps unless you are upgrading the database schema. In that case, proceed to Step 12.

- If you are working with an HA pair, this newly initiated instance will become the backup if you are not upgrading the database, or the primary if you are running the database schema upgrade procedure. In both cases, make sure it completes initialization in the expected mode before continuing.

- If you are upgrading from a pre-8.5 environment, an additional LRM deployment step must be performed before the newly installed Configuration Server can be accessed by regular clients. Follow the *Framework* and *LRM Deployment Guides* to make sure LRM is installed (against the server running on the new 8.5 database in primary mode) and started before proceeding to the next step.

- If you are upgrading the database schema and a disaster recovery (DR) deployment is in place, set up replication from the migrated database to a remote DR site where the corresponding new database should be created. Follow the same guidelines as discussed in the *Framework 8.5 Deployment Guide*.

8) Continue with the primary instance. Use the Management Layer to shut down the primary instance that you are replacing. This will cause a temporary loss of connectivity for Configuration Server clients. The first (already upgraded) instance will be brought into primary mode momentarily, and clients should be able to restore their sessions. Confirm that another instance successfully entered primary mode. If there are issues with the new instance taking over the load, restart the instance that you have just stopped and, when initialization is finished, stop the first instance allowing clients to connect back. Perform troubleshooting steps before moving forward, or roll back as discussed in the subsequent section.

9) Back up the folder of the instance that is currently being shut down and replace it with content of the relevant folder, prepared in Step 2.

10) Install another master Configuration Server instance as described in Step 2, above. This time, select another Application object that corresponds to an instance, currently not running, that was a primary server before you started the upgrade procedure. Select **Configuration Server Master Backup** when prompted by the Installation Package. Confirm that, in the configuration file of the newly installed server, the section name

corresponds to the name of the application object for which this instance has been installed, and matches the value of the –s option in the command line to start this instance.

11) Launch the second (new) instance and wait for it to initialize completely as a backup server. Verify that you specified the locations (installation folders) of new instances correctly in the configuration database (in respective Application objects) as well as in any external scripts and/or Windows service definitions that you may have set up previously. Back up and disable any external scripts and/or Windows service instances that are being used to deal with the old instances.

12) If you performed the database upgrade and you did not use the `disable-switchover` option for SCS, then restart LCA on the host where new Configuration Servers are running.

13) If you performed the database upgrade, remove the line `upgrade-mode=1` from the configuration file of the currently running primary server to avoid future interference from side-by-side startup.

14) To ensure that the same (configured) instance is running after upgrade, using the Management Layer, shut down the current primary instance, the backup server will be switched into primary mode momentarily and clients should be able to restore connections. Restart another instance that will become a backup.

15) This completes the upgrade of a master Configuration Server HA pair. Proceed with the upgrade of Configuration Server Proxy instances, if any. The procedure is similar to that described above with a few exceptions:

    - You do not need to put the configuration environment into read-only mode, but Genesys strongly recommends that you ensure no updates are pending and/or scheduled.

    - You do not need to copy any *.conf files from one folder to another when preparing new instances.

    - You may want to back up Application options of individual Configuration Server objects using Genesys Administrator, by selecting Application object's options and exporting them into XML.

    - When installing the new Configuration Server Proxy instance for upgrade purposes, you must specify the same Application object name as that of the instance being replaced, and perform all configuration (using the master Configuration Server) using the options of that Application object.

16) Install the new version of the remaining server in the HA pair (on the host where the original server from that pair was installed). Ensure that the same Application name has

been used (use the `confserv` predefined name if the remaining server is configured as primary, or use the name of the actual object if it is configured as backup) and provide the new server with the reference to an upgraded database.

17) Start the second installed server, either manually or using Management Layer, to ensure uninterrupted operations in the future.

18) Preserve the legacy database for some period of time to ensure rollback is possible, if needed. Rollback can be carried out using the same sequence of steps if the legacy Configuration Server was 8.5; for older servers, it is required to shut down both currently running servers in the master Configuration Server pair before starting any previous version .

Limitations

- Client sessions cannot be preserved between older and newer versions of servers when using database upgrade. There might be other cases when session restoration won't work during upgrade – refer to the Release Notes of the particular version.
- During the upgrade procedure, the Configuration Server environment remains read-only and the master Configuration Server is not redundant until the new server is fully initialized.
- During upgrade, SCS might not be able to switch over applications as long as it is configured that way to accommodate the startup of new Configuration Servers, or it may not be able to control applications on the host of the newly installed Configuration Server if LCA was shut down using the previous steps.

Rolling Back to the Previous Version of Configuration Server

If you need to return to a previously stable version of Configuration Server, an installed but inactive old instance should be used to boot up the stable version.
If roll back of both master and Configuration Server Proxy are required, the roll back order depends on the operational state of the master, as follows:

- If the master is fully operational, roll back the Configuration Server Proxy instances first.
- If the master is not operational, roll back the master instance first.

Procedure: Rolling Back the Master Configuration Server

1) If you determine that immediate rollback is needed after unsuccessful execution of the upgrade procedure, follow these steps:

a) Shut down the newly installed second instance that is having problems (if it is still running) and restart the first (old) instance that was shut down at first when you started the upgrade.

   There will be intermittent downtime until the old instance is fully initialized.

b) When the old instance takes over as primary, log into the configuration environment and manually reset the startup parameters of the second instance (that was replaced by the new installation of the upgrade procedure) to point to a location of the original target installation folder for that instance before the upgrade.

c) Restart the second instance.

This completes the immediate rollback procedure. You do not need to continue with other steps.

2) If you performed the database upgrade, the old database is still available. You have to follow the same procedure as described in Step 1 above, except that you launch the old instance against the old database. You do not need to continue with future steps.

3) If the database rollback is needed to restore the normal operation and you have a database backup, do the following:

   a) Shut down any DB Server instances that have being used by master Configuration Servers. This will initiate a rollback window.

   b) Take DBMS offline and restore DBMS to the previous state.

   c) Proceed to Step 6 of the rollback procedure.

4) If the database rollback is not performed, log into the configuration environment and manually reset startup parameters of all to point to the location of the original target installation folder for each instance before the upgrade.

5) If the database rollback is not performed, force the currently running master Configuration Server into read-only mode, or ensure there are no pending changes to the configuration. This will initiate a rollback window.

6) Using the Management Layer, shut down the currently running backup instance and replace the folder with the backup copy from the previous version.

7) If the database rollback is performed, make sure the DBMS is online and start any DB Servers that are being used by the master Configuration Servers.

8) Start the corresponding old instance of Configuration Server from the restored folder and wait for it to initialize as backup. If you are not using an HA pair, this will end the downtime\rollback window. You do not need to continue with the rest of the steps.

9) Using the Management Layer, shut down the remaining instance you want to roll back. This will cause a temporary loss of connectivity for Configuration Server clients. The second (already downgraded) instance will be brought into primary mode momentarily and clients should be able to reconnect. Confirm that this second instance successfully entered primary mode before you continue.

10) Replace the folder with the backup copy from the previous version for the instance that is currently down, and launch the second old instance. Wait until it is initialized and enters backup mode.

11) Verify that you have correctly specified locations (installation folders) of old instances in the configuration database (in respective Application objects) as well as in any external scripts and/or Windows service definitions that you may have set up previously. Back up and disable any external scripts and/or Windows service instances that are being used to deal with recently instances that were rolled back. This will end your rollback window.

Procedure: Rolling Back the Configuration Server Proxy

1) Using the Management Layer, shut down the currently running backup instance. This will begin your rollback window. If there is no HA pair, shut down the currently running instance; this will start a downtime window.

2) Log into the configuration environment and manually reset startup parameters of the stopped instance to point to a location of the original target installation folder for this instance before the upgrade.

3) Start the corresponding old instance of Configuration Server and wait for it to initialize. If you are not using an HA pair, this will end the downtime\rollback window. You do not need to continue with the rest of the steps.

4) Using the Management Layer, shut down the remaining instance you want to roll back. This will cause a temporary loss of connectivity for Configuration Server clients. The second (already downgraded) instance will be brought into primary mode momentarily and clients should be able to reconnect. Confirm that this second instance successfully entered primary mode before continuing.

5) In the configuration environment, manually reset startup parameters of the stopped instance to point to the location of the original installation before the upgrade.

6) Launch the second old instance and wait until it is initialized and enters backup mode.

7) Verify that you have correctly specified locations (installation folders) of old instances in the configuration database (in respective Application objects) as well as in any external scripts and/or Windows service definitions that you may have set up previously. Back up and disable any external scripts and/or Windows service instances that are being used to deal with recently instances that were rolled back. This will end your rollback window.

Upgrading LCA

Prerequisites

LCA is installed and running on a host, SCS is controlling this host and has been upgraded to the latest version and connected to LCA. There are no active alarms on the host or are ready to be installed.

Procedure

1) In the options of all Solution Control Servers that control the hosts in which the LCA upgrade is performed, set the value of the `disconnect-switchover-timeout` option in the `general` section to, for example, `600` (10 minutes).

2) Upgrade LCA on those hosts in the environment that are running either:

- No Solution Control Servers, or
- One Solution Control Server that is not configured in an HA pair. In this case, ensure that you shut down SCS before upgrading LCA

This step should be repeated one host at a time.

Note: The upgrade of every host should not take any longer than the value set for the `disconnect-switchover-timeout` option, or an incorrect switchover could occur.

3) Upgrade LCA on the host that runs the primary SCS.

a) Shut down the primary SCS. Wait until the switchover is complete and the backup SCS is running in primary mode.
b) Upgrade LCA on the host.
c) Start the primary SCS. It should be running in backup mode.

4) Upgrade LCA on the host that runs the backup SCS in primary mode.

a) Shut down the backup SCS running in primary mode. Wait until the switchover is complete and the primary SCS is running in primary mode.
b) Upgrade LCA on the host.
c) Start the backup SCS. It should be running in backup mode.

5) In the Options of all Solution Control Servers in the environment, delete the `disconnect-switchover-timeout` option set in Step 1.

Limitations

There is no switchover of components that are running primary/backup on the host where LCA being upgraded if any of them or their peers fail, until either a new LCA is up or the timeout defined by the `disconnect-switchover-timeout` option has elapsed.

Upgrading Other Management Framework Server Components

Prerequisites

For the SCS and Message Server components, the same sequence of steps applies. Components should have HA pair configured and running. All new IPs are delivered to the relevant hosts and are ready to be installed.

Procedure

1) Shut down the backup server component.

2) Save configuration options of the backup configuration object to provide a rollback path if the older version must be restored. Use Genesys Administrator to export options into the XML file and save the file.

3) Using Genesys Administrator, upload a new Application Template/metadata file into the configuration environment and associate the existing configuration object, used for the backup server application being upgraded, with the new Application Template. Select to add new options from the template.

4) Install the new version of the component providing the same Application object name that was used by the former backup server (updated in the previous procedure), using the same host where a previous backup has been installed. Follow deployment/configuration guidelines for the particular component.

5) For Message Server only, if upgrade requires the database update (as specified in the Deployment Guide), shut down the primary Message Server, save the current database, and update the database schema if required according to the Deployment Guide.

6) Start the newly installed server component and ensure it becomes backup for the currently running primary server (if any).

7) Shut down the current primary server (if it is still running). Ensure that the newly installed component becomes primary and begins serving clients. Follow the same steps to upgrade the stopped component.

Limitations

High availability of the component being upgraded could be limited during the downtime of backing up, installing, and starting up the new version.