Framework Migration Guide

Upgrading Components

5/8/2025

Contents

- 1 Upgrading Components
  - 1.1 Interoperability
  - 1.2 Upgrading Local Control Agent
  - 1.3 Upgrading Management Layer Server Components
  - 1.4 Upgrading Configuration Server

Upgrading Components

This section defines the order of the steps necessary to upgrade software. You might also consider upgrading the database schema and/or reloading the locale, if necessary, as part of the software upgrade procedure. See the following sections for details of database-related activities.

Important

- You do not have to update both the software and the database schema at the same time, unless you want particular new features to work with new software.
- For Windows hosts, Genesys recommends that you select Windows as a generic type for all hosts running the Windows 2016 and later operating system. For Linux hosts, Genesys recommends that you select Linux as a generic type for all hosts running a Linux operating system other than Red Hat Enterprise Linux.

Interoperability

There are several items to consider regarding interoperability:

- When upgrading a configuration environment running in Distributed mode, first upgrade Configuration Server to the newer version, then upgrade all Configuration Server Proxies as soon as possible. Genesys does not support running different versions of Configuration Server components, except during the migration from one version to another. During this phase, different versions of Configuration Server can co-exist in the same environment to ensure minimal downtime; however, do not attempt to enable any new features until you remove older versions of Configuration Server from the environment.
- When upgrading Configuration Server in Disaster Recovery/Business Continuity mode, make sure you upgrade dormant copies of master Configuration Servers. If the Configuration Database was also upgraded, be sure to replicate the upgraded database before you start any of the dormant instances.
- License Reporting Manager (LRM) 8.5 is no longer integrated with Configuration Server. If you are upgrading from a configuration environment using LRM 8.5, you must uninstall it. Refer to the LRM Technical Advisory for more information.

Upgrading Local Control Agent

Use the following procedure to upgrade Local Control Agent (LCA).

Prerequisites

- LCA is installed and running on a host.

- SCS is controlling this host, has been upgraded to the latest version, and is connected to LCA.
- There are no active alarms on the host or any 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 (SCS) that is not configured in an HA pair. In this case, ensure that you shut down this SCS before upgrading LCA. Note that you will have no Management Layer control of this environment until SCS is back on line.

   This step should be repeated one host at a time.

   > **Warning**
   > If the upgrade of every host takes any longer than the value set for the **disconnect-switchover-timeout** option, an incorrect switchover could occur.

3. Upgrade LCA on the host that runs the primary SCS, as follows:
   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, as follows:
   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 HA components on the host where LCA being upgraded if any of them or their peers fail, until one of the following occurs:

- A new LCA is installed and running, or
- The timeout defined by the **disconnect-switchover-timeout** option has elapsed.

Upgrading Management Layer Server Components

Important

- When upgrading a Management Layer server component, you must stop it using the Management Layer (using Genesys Administrator), to prevent it from being restarted during the upgrade process.
- Use the Management Layer to prevent them from being restarted during the upgrade process to start the components, except when a single Solution Control Server (SCS) (not part of an HA pair) is being upgraded. In this case, start SCS using the appropriate operating system commands on its host, and then confirm that Genesys Administrator can reconnect to this SCS.

Use the following procedure to upgrade Management Layer Server Components.

For the SCS and Message Server components, the same sequence of steps applies.

Prerequisites

- All new Installation Packages (IPs) are delivered to the relevant hosts and are ready to be installed.

Procedure

1. Shut down the server to be upgraded. If the server is part of an HA pair, shut down the backup first.
2. Save the configuration options of the server shut down in Step 1 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 and metadata file into the configuration environment and associate the existing configuration object, originally associated with the shut-down server application, with the new Application Template. Select the option 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 server (updated in Step 3), using the same host where a previous backup has been installed. Follow deployment and configuration guidelines for the particular component.
5. (Message Server only) If the upgrade requires that the Log Database be updated, refer to the instructions in Updating the Centralized Log Database Schema.
6. Start the newly upgraded server component and, if a part of an HA pair, ensure it becomes backup for the currently running primary server.
7. (HA servers only) If the newly upgraded server component is part of an HA pair, 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 other component of the HA pair.

Limitations

Availability of the component being upgraded might be limited during the downtime of backing up, installing, and starting the new version.

Upgrading Configuration Server

> ### Warning
>
> - Do not enable any new features of Configuration Server until you finish upgrading all Configuration Server Proxies to the version that supports the new features.
> - Both Configuration Servers configured as an HA pair must be running the same version when migration is complete. If there are requirements for related components (such as DB Server), upgrade those components first.

Recommendation

Preserve the legacy Configuration 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 are not preserved between older and newer versions of servers when upgrading the database. There might be other cases when session restoration will not 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 to accommodate the startup of new Configuration Servers, or it might not be able to control applications on the host of the newly installed Configuration Server if LCA was shut down using the previous steps.

Prerequisites

- All new Installation Packages have been delivered to the relevant hosts and are ready to be installed.
- The latest version of LCA is installed on the Configuration Server hosts.
- The latest version of SCS is deployed in the environment.

Upgrading a Standalone Configuration Server

Use the following procedure to upgrade a standalone Configuration Server.

Procedure

1. Back up your Configuration Database.
2. Install (but do not start) a new Configuration Server instance by selecting **Configuration Server Master Backup** installation mode when installing from the Installation Package. Note the following:
   - When prompted to provide a name for the Application object, enter the same name as the Application object that is being upgraded, but select a new folder for your installation.
   - Confirm that, in the configuration file of the newly upgraded server, the section name corresponds to both:
     - The name of the Application object for which this instance has been installed.
     - The value of the **–s** option in the command line to start this instance.
3. If the database schema of the Configuration Database must be upgraded, refer to Migrate the Database for detailed instructions.
4. Using Genesys Administrator, shut down the instance you are replacing. This will cause some downtime for Configuration Server clients.
5. Back up the folder of the instance that was shut down in the previous step. Change the folder name to be version-specific and replace it with the content of the relevant folder prepared in Step 2.
6. Launch the new version of the Configuration Server instance from the replaced folder and wait for it to initialize. Make sure it completes initialization before continuing. At this stage, note the following:
   - The time when the server instance completes initialization will end the downtime window for Configuration Server clients.
   - 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 Deployment Guide*.

Upgrading an HA Pair of Configuration Servers

If you want to upgrade to 8.5.101 an HA pair of Configuration Servers running version 8.1.3 against a Configuration Database with an 8.1.1 schema, you can upgrade the two servers without losing or interfering with any of the backup functionality. Use the following procedure:

Upgrading HA Configuration Servers, Using Same Configuration Database Schema 8.1.1, from 8.1.3 to 8.5.101

1. Back up your Configuration Database.
2. First, upgrade the backup Configuration Server. Deploy (but do not start) a new backup 8.5.1 Configuration Server instance by selecting **Configuration Server Master Backup** installation mode when installing from the Installation Package. Note the following:

- When prompted to provide a name for the Application object, enter the same name as the Application object that is being upgraded, but select a new folder for your installation.
- In the configuration file of the newly upgraded server, confirm that the section name corresponds to the name of the Application object for which this instance has been installed.

3. Stop the 8.1.3 backup instance using Genesys Administrator, then back up its folder. Change the folder name to be version-specific and replace it with the content of the relevant folder prepared in Step 2.
4. Launch the 8.5.101 Configuration Server instance from the replaced folder and wait for it to initialize. Standard-level log messages **21-25303** followed by **21-22172** should be generated, indicating that the 8.5.101 Configuration Server is running as backup to the 8.1.3 primary Configuration Server. If these log messages are not generated, you have to force the upgrade—use the other procedure for upgrading from 8.1 to 8.5.
5. After the new primary 8.5.101 Configuration Server has initialized, shut down the primary 8.1.3 Configuration Server. This forces the clients of the 8.1.3 server to try to connect to the primary 8.5.101 Configuration Server that will be brought into primary mode momentarily by Solution Control Server. Clients can restore their sessions.
6. After all clients are finished migrating to the primary 8.5.101 server instance (monitor this either by checking all client applications for successful reconnection messages or by the `total number of clients` message reported by both servers when the log level is set to debug), install an 8.5.101 version of of Configuration Server the on the host where the original 8.1.3 server from that pair was installed. Be sure to use the same Application name (use `confserv` if the remaining server is configured as primary).
7. Start the newly-installed 8.5.101 Configuration Server. Use the normal starting procedure; no special steps or options are required. The new Configuration Server recognizes that its HA peer (the primary 8.5.101 Configuration Server in upgrade mode) is already upgraded, and initializes as the backup server.
8. After the newly-installed 8.5.101 server has fully initialized as backup and generated log message **21-22172**, shut down the primary 8.5.101 backup Configuration Server that is in upgrade mode. SCS immediately promotes the backup 8.5.101 backup server to primary. Clients are able to restore their sessions normally, and they switch over to the new upgraded primary server.
9. Start the backup Configuration Server (formerly in upgrade mode), manually or using Genesys Administrator. The migration is complete. The only messages in the 8.5.101 log will be those relating to the migration.

If you just want to upgrade the HA pair to an 8.5 Configuration Server from an 8.1 version or an earlier 8.5 version, regardless of whether they are using the same Configuration Database schema, use the following procedure:

Upgrading HA Configuration Servers

1. Back up your Configuration Database.
2. First, upgrade the backup Configuration Server Install (but do not start) a new backup Configuration Server instance by selecting **Configuration Server Master Backup** installation mode when installing from the Installation Package. Note the following:
   - When prompted to provide a name for the Application object, enter the same name as the Application object that is being upgraded, but select a new folder for your installation.
   - Confirm that, in the configuration file of the newly upgraded server, the section name corresponds to the name of the Application object for which this instance has been installed.

3. Use Genesys Administrator or any other suitable tool or utility to force the currently running Configuration Server into Read-Only mode. This prevents any changes being made to your configuration during the switchover.
4. If you have upgraded the database, make sure that the new instance of Configuration Server is configured to start against the new database.

> **Important**
>
> 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 Deployment Guide*.

5. Stop the backup instance using Genesys Administrator, then back up its folder. Change the folder name to be version-specific and replace it with the content of the relevant folder prepared in Step 2.
6. Launch the new version of the Configuration Server instance from the replaced folder and wait for it to initialize. Monitor the new instance for any of the following Standard-level log messages:
   - The new Configuration Server should enter upgrade mode automatically when detecting another instance is not fully compatible. Log event **21-25301** is generated soon after the newly started Configuration Server is able to contact the current primary server in this case. If you don't see this message after log event **21-22911** but before event **21-22902**, and your primary Configuration server is older than 8.5, you must stop the new server and review Configuration Server Release Notes. You might need to force the new version into upgrade mode using the **upgrade-mode=1** option in the configuration file and/or in the command line.
   - There is no need for upgrade mode if you are replacing Configuration Servers that are fully compatible, and are running against the same Configuration Database. This is the case if you observe log event **21-22902**, followed by log event **21-22172**, from the newly installed server. In this case, you can ignore the rest of the steps in this procedure, which describe only situations where have to proceed with having one Configuration Server in upgrade mode.
   - This new instance will initialize as the primary Configuration Server in upgrade mode (that is, it detected upgrade mode automatically and generates log event **21-25301**, or it was started with the command-line parameter **-upgrade-mode1** or configuration option **upgrade-mode=1** and generates log event **21-25300**). It might compete with the original primary server for database access, if you are starting it against the same database (that is, you are not upgrading the database upgrade at the same time). Both servers will automatically enter Read Only mode during upgrade, when they share the same database.
   - Solution Control Server detects the presence of two primary Configuration Servers and tries to force the new server (in upgrade mode) into backup mode, but the new instance refuses these requests and continues to initialize. This is normal situation during upgrade. You might observe log event **21-25302** reported several times by Configuration Server in upgrade mode; this is not considered an error in this situation.
   - You must see that log event **21-22170** or **21-22171** has been generated by the new instance of Configuration Server before you can continue with the next steps.**21-22170** is generated when Configuration Server upgrade steps are performed in an environment with the same Configuration Database. **21-22171** will be generated if you are upgrading the database at the same time.
7. After the new primary Configuration Server, still in upgrade mode, has initialized, shut down the original primary Configuration Server. This forces the clients of the original server to try to connect to the new primary Configuration Server (the one in upgrade mode). The clients of the original Configuration see this as a temporary disconnection, and try to connect to the backup server (which is currently running as the new primary server, in upgrade mode). However, a backup server in upgrade mode does not

support session restoration, so clients must re-read the configuration to ensure they get the data in the appropriate schema.

8. After all clients are finished migrating to the new server instance (monitor this either by checking all client applications for successful reconnection messages or by the `total number of clients` message reported by both servers when the log level is set to debug), 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 `confserv` if the remaining server is configured as primary). If database upgrade was part of this migration, also provide the new server with the reference to the upgraded database.
9. Start the new Configuration Server. Use the normal starting procedure; no special steps or options are required. The new Configuration Server recognizes that its HA peer (the new primary Configuration Server in upgrade mode) is already upgraded, and initializes as the backup server.
10. After the new backup server has reported log event **21-22172** after becoming fully initialized , shut down the primary Configuration Server that is in upgrade mode. SCS immediately promotes the new backup server to primary. Clients are able to restore their sessions normally, and they switch over to the new upgraded primary server.
11. Start the backup Configuration Server (formerly in upgrade mode), manually or using Genesys Administrator, to ensure uninterrupted operations in the future.

Upgrading a Configuration Server Proxy

To upgrade Configuration Server Proxies, if any, use the previous procedures, depending on how they are configured—as standalone Configuration Server Proxies or in HA pairs. In either case, note the following exceptions to the referenced procedures:

- If the master Configuration Server 8.1.3 is using the Configuration Database in single-language mode, both primary and backup instances of Configuration Server Proxy 8.5 can, during migration, start and operate against Configuration Server 8.1.3. In all other cases, you must upgrade the master Configuration Server before any of its associated Configuration Server Proxies.
- 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 might want to back up configuration options of individual Configuration Server objects using Genesys Administrator, by selecting the 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.

Rolling Back 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 rollback of both the master and Configuration Server Proxy are required, the rollback 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.
  1. Using Genesys Administrator, shut down the currently running backup instance. This begins your rollback window. If there is no HA pair, shut down the currently running instance; this starts a downtime window.

2. Log into the configuration environment and manually reset the 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 Genesys Administrator, shut down the remaining instance you want to roll back. This causes a temporary loss of connectivity for Configuration Server clients. The second (already downgraded) instance is brought into primary mode momentarily and clients can 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 ends your rollback window.

- If the master is not operational, roll back the master instance first.
  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.
- If you performed the database upgrade, the old database is still available. Follow the same procedure as described in Step 1, but launch the old instance against the old database. You do not need to continue with future steps.
- 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 are 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.
- 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.
- 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.

- Using Genesys Administrator, shut down the currently running backup instance and replace the folder with the backup copy from the previous version.
- 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.
- 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.
- Using Genesys Administrator, 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.
- 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.
- 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.