Framework Deployment Guide

Disaster Recovery / Business Continuity

4/4/2026

Contents

Disaster Recovery / Business Continuity

This section describes a recommended architecture to ensure successful disaster recovery, or business continuity, following a scenario in which the main site was rendered inoperable because of some natural or other disaster.

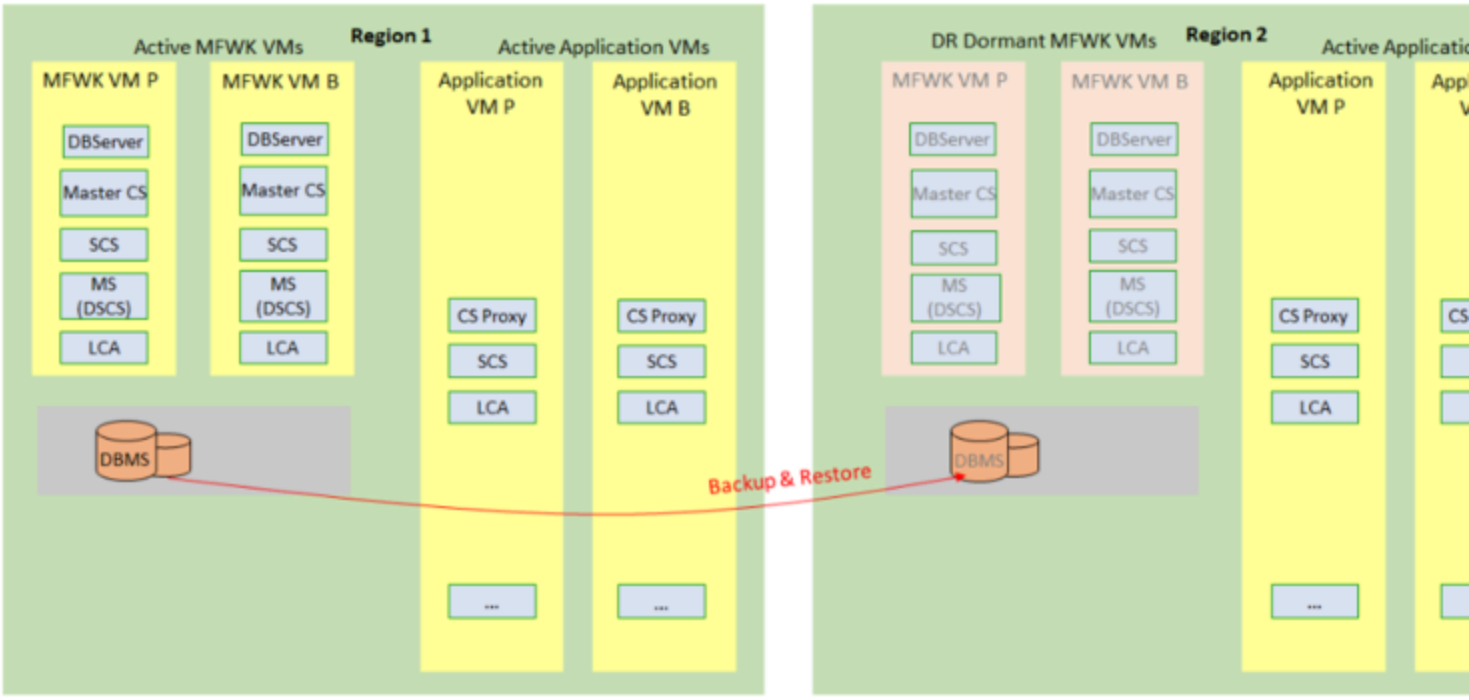
> **Warning**
>
> The information provided herein is a reference architecture and not a step-by-step deployment procedure. The main focus of this chapter is to highlight major requirements when deploying Genesys software in Disaster Recovery mode. Actual deployment may require additional steps and/or configuration that is beyond the scope of this document.

Overview

The Genesys system configuration is stored in a single database, and can be accessed by only one primary master Configuration Server connection at a time. The Configuration Database is constantly modified by Configuration Server clients, and is archived periodically to prevent the loss of data. However, database maintenance and periodic backup can cause significant downtime. It cannot prevent partial or whole loss of configuration data if a major disaster occurs, such as one in which the Configuration Database and all updates and modifications made since the last backup is completely lost. To improve the robustness of the Management Framework solution and to reduce downtime for system maintenance, this architecture replicates a secondary standby database.

Architecture

The following diagram illustrates the disaster recovery architecture for a multi-site configuration operating under normal conditions.



MFWK – Management FrameWorK
Master CS – Master Configuration Server
SCS – Genesys Solution Control Server
LCA – Genesys Local Control Agent
MS(DSCS) – Genesys Message Server for Distributed SCS
CS Proxy – Genesys Configuration Server Proxy
RDS Multi Zone – Relational Database Server configured for multi zone operation
DBMS – DataBase Management System (MSSQL/Postgres/Oracle)
MFWK VM P – Management Framework Virtual Machine Primary
MFWK VM B – Management Framework Virtual Machine Backup
Application VM P – Application Virtual Machine Primary
Application VM B – Application Virtual Machine Backup

- Failed part
- Dormant MFWK Instanc
- Active Instances
- Genesys Component

Components

> **Important**
> Genesys recommends deployment of components on Virtual Machines (VMs). It is recommended that Framework VMs be cloned, to have identical copies across sites, and then make targeted adjustments.

Framework components for all Framework VMs should be set up identically in this architecture.

Framework components on Application VMs are set up as required to provide service in each region, and include other details listed in this section and keeping in mind future requirements if necessary. Application components are set up as needed, and must use Configuration Server Proxy in the given region, instead of the master Configuration Server, to obtain their configuration. There must be two FQDNs that can be resolved globally for Framework VMs. Each pair of Framework VMs (Active and Dormant) must have the same pair of FQDNs and different IP Addresses.

Region 1

- A primary DBMS, containing the Configuration Database and the optional Log Database.
- An active redundant master Configuration Server primary/backup (HA) pair in the Framework Virtual Machine (VM).
- An active DB Server HA pair in the Framework VM, which is required for Configuration Server (8.1 only) to connect to Configuration Database.
- An active Solution Control Server (SCS) in distributed mode; as the main SCS, it is required to control the main master Configuration Server pair in the Framework VM.
- An active Message Server HA pair configured in distributed mode in the Framework VM to support communication between the Solution Control Servers that are controlling components such as Configuration Server Proxy pairs, and Log Message Servers.
- A Local Control Agent in each VM.
- A Configuration Server Proxy HA pair in the Application VM and connected to the currently active primary Configuration Server.
- A Solution Control Server HA pair in distributed mode set as `default` in the Application VM, to control other components.
- (Optional) A Log Message Server HA pair in both the Framework and Application VMs for network logging, and connected to the Log Database.

Region 2

- A secondary DBMS, containing the replicated Configuration Database and the optional replicated Log Database, which gets updated by the primary instance in case of any changes.
- A dormant (non-active) redundant master Configuration Server primary/backup (HA) pair in the Framework VM.
- A dormant DB Server HA pair in the Framework VM, which is required for Configuration server (8.1 only) to connect to the Configuration Database.
- A dormant Solution Control Server (SCS) in distributed mode; as the main SCS, it is required to control the main master Configuration Server pair in Framework VM.
- A dormant Message Server HA pair configured in distributed mode in the Framework VM to support communication between Solution Control Servers controlling components, such as Configuration Server Proxy pairs and Log Message Servers.
- A Local Control Agent in each VM.
- Configuration Server Proxy HA pair in the Application VM and connected to the currently active primary Configuration Server.
- A Solution Control Server HA pair in distributed mode set as `default` in the Application VM, to control

other components.

- (Optional) A Log Message Server HA Pair in both the Framework and Application VMs for network logging, and connected to the Log Database.

Solution Control Servers

All Solution Control Servers used in this deployment are configured in Distributed SCS mode. They should all be configured in HA pairs in each Region.

In each Region, one SCS is deployed on the Framework VMs, and is dedicated to management applications, specifically Configuration Server and the dedicated Message Server for the distributed Solution Control Servers, described below.

For distributed Solution Control Servers to communicate with each other, a Message Server dedicated for use by the distributed Solution Control Servers (**[MessageServer].signature**=`scs_distributed`) is also installed in each Framework VM.

Each Region also has an SCS HA pair deployed on the Application VMs.

All Solution Control Servers in all VMs must always connect to the main Configuration Server, not to the Configuration Server Proxies. Solution Control Servers must be provisioned to start using a configuration file (use the `-f` command line option) that points to the FQDNs of master Configuration Servers.

Depending on the number of applications, it is possible to deploy additional distributed Solution Control Servers for load balancing.

Message Servers

An HA pair of Message Servers is dedicated for communications between the distributed Solution Control Servers deployed in the Framework VM.

Optionally, each Region can have its own instance of a Log Message Server to be used for network logging by applications running at the same site. One pair of Message Servers is installed on the Framework VM, and handles logging for all components in this VM. Likewise, a Message Server pair is also installed on the Application VM, is managed by the SCS in that VM, and handles logging for all components in this region. If a Log Message Server is configured, a dedicated Log Database is required at each site, one as active primary and the other as dormant replicated secondary.

Configuration Server Proxies

In each region, a Configuration Server Proxy HA pair is deployed in one pair of Application VMs that connects to the active pair of Master Configuration Server.

All applications deployed in all Application VMs, except SCS, must connect only to the Configuration Server Proxy in the corresponding region for any read/write operation.

DB Server

DB Server HA pairs should be deployed in the Framework VMs to connect with the corresponding

database, but only if required by the master Configuration Server.

Replicating DBMS

The DB Server must be replicated in Region 2 for the Configuration and Log Databases. This is required so that, after failover, the secondary Configuration Server and Log Message Servers can connect with the replicated DBMS and continue working.

If a major disaster occurs, the secondary database can be accessed by a secondary master Configuration Server that is brought online from the dormant state, and changing the IP address name resolution for Configuration Server Proxies to the host running that secondary master Configuration Server. Operations at sites will continue uninterrupted, but in limited mode, without a configuration change until the secondary master Configuration Server is brought online and restored to normal mode after the proxy servers reconnect to the secondary master Configuration Server.

Block any accidental connection between the dormant DBMS VM and either active and dormant Framework VMs by running the `iptables` command (on Linux) or creating firewall rules (on Windows) on the dormant DBMS host.

To block an active Configuration Server from accessing a dormant DBMS:

- On Linux:

```
sudo iptables -A INPUT -p tcp --dport <DBMS PORT> --src <Framework VM IP>/24   -j
REJECT
```

- On Windows, create firewall rules that block any connection to a DBMS port from the Framework VMs.

After the replicated dormant DBMS become active, and after the previously active DBMS instance is stopped or failover has occurred, use the `iptables` command or remove the firewall rules to restore the connection with the Framework VMs.

Use the same `iptables`/firewall rules to block connections for the currently dormant DBMS VM. To restore access:

- On Linux:

```
sudo iptables -D INPUT -p tcp --dport <DBMS PORT>…
```

- On Windows, remove the firewall rules for Framework VMs.

For more information about replicating Framework databases for Disaster Recovery using MS SQL Server and Oracle, refer to the following:

- Framework Database Replication for Disaster Recovery Using MS SQL Cluster with AlwaysOn
- Framework Database Replication for Disaster Recovery Oracle GoldenGate

Deploying Genesys Components

Deploy Genesys components as follows:

1. Using the initialization scripts in the Installation Package, create the database objects for the Configuration Database and if you want, the Log Message Server Database.
2. In one Region, deploy the initial set of Framework VMs, including the following components in HA pairs, as services to be started when the Framework VMs start:
    - Master Configuration Server
    - DB Server (if required for the selected master Configuration Server deployment mode)
    - Local Control Agent
    - Main Solution Control Server
3. On active Framework machines, deploy an HA pair of Message Servers. In the Annex of the Message Server objects, set the **[sml].autostart** option to `true`.
4. In both Regions (1 and 2), deploy the following components in HA pairs as services to be started when the Application VMs start:
    - Configuration Server Proxy
    - Local Control Agent
    - Solution Control Server
5. If required, deploy Log Message Server HA pairs as services in the Application VMs. Set the **[sml].autostart** option to `true` in the Annex of the Application objects, so the application will be started automatically by Management Layer when the system is started.
6. Clone Framework VMs to another site and start them as not connected, using a firewall or the `iptables` command to make sure that no connections can be made from components running on the closed machines to anywhere within the environment. Adjust the local VM configuration files as needed (typically, you have to point to Region-specific DBMS endpoints), and then stop the cloned VMs.

DNS-based Disaster Recovery

Both Full and Partial Failovers can be done with the help of DNS.

The DNS Server configures a record type (call it type *A* for purposes of this discussion) to resolve the IP address of the host running the live master Configuration Server HA pair. It resolves the IP address to the main host in normal mode, and to the secondary host in failover mode.

To avoid false situations, name resolution from this record of type A in the **/etc/hosts** file on the main and secondary hosts points to the IP Address of the local host.

Within each set of Framework VMs, all fully-qualified domain names (FQDNs) of Framework components are resolved using the **hosts** file in IPs on these VMs. This is required because the DNS service resolves Management Framework FQDNs to VMs running in the active Region and currently serves other VMs of this environment.

The DNS TTL (Time To Leave) on type A records for Framework FQDNs must be set according to the

expected period of time after which components running on Application VMs are expected to automatically reconnect to newly introduced instances of Framework VMs during the Disaster Recovery event.

Operation

1. Start the Framework VM pair in Region 2.
2. Run the necessary procedure to switch the cfgmaster host name IP resolution to a MAIN live system.
3. On the host running Configuration Server Proxies, run the necessary procedure to clean out the DNS cache.

Failover Scenarios

This section describes the various failover scenarios that are handled by this architecture.

Full Failover

Region 1, hosting the currently active Framework components, goes down completely so no VM in this region is up and running. The Region goes through Full Failover.

The DBMS in Region 2 becomes active after the previously active DBMS is stopped or is going through failover. Set the iptables command or firewall rules, as described in Replicating DBMS.

In Region 2, restart the Framework VMs to bring the dormant Framework components back into service. These reactivated components will connect to the corresponding databases in the currently active DBMS (in Region 2).

Change the IP address name resolution for Configuration Server Proxies in all Application VMs to the host where the secondary master Configuration Server is running.

Partial Failover

This scenario is the case in which only one (not both) of the Framework VMs or the DBMS VM, which are currently active in Region 1, go down.

Framework VMs Failover

In Region 2, restart the Framework VMs to bring the dormant Framework components back into service. These reactivated components will connect to the corresponding databases in the currently active DBMS (in Region 2).

Change the IP address name resolution for Configuration Server Proxies in all Application VMs to the host where the secondary master Configuration Server is running.

DBMS Failover

The DBMS in Region 2 becomes active after the previously active DBMS is stopped or is going through failover. Use the `iptables` command or firewall rules, as described in Replicating DBMS.

Active Framework components will connect to the corresponding databases in the currently active DBMS (in Region 2).