Framework Deployment Guide

Disaster Recovery Using DNS Failover and Oracle GoldenGate

4/12/2025

Disaster Recovery Using DNS Failover and Oracle GoldenGate

Contents

This section describes a recommended architecture to ensure successful disaster recovery, or business continuity, using Oracle GoldenGate, following a scenario in which the main site was rendered inoperable because of some natural or other disaster. For more information, including configuration details, see Configuring Disaster Recovery Using DNS Failover and Oracle GoldenGate.

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, is archived periodically to prevent the loss of data. 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 live database to a secondary live standby database. If a major disaster occurs, that secondary database can be accessed by a secondary master Configuration Server that is brought online from a dormant state, and changing IP address name resolution for Configuration Server Proxies to the host running that secondary master Configuration Server. Operations at sites can be continued uninterrupted 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.

Components

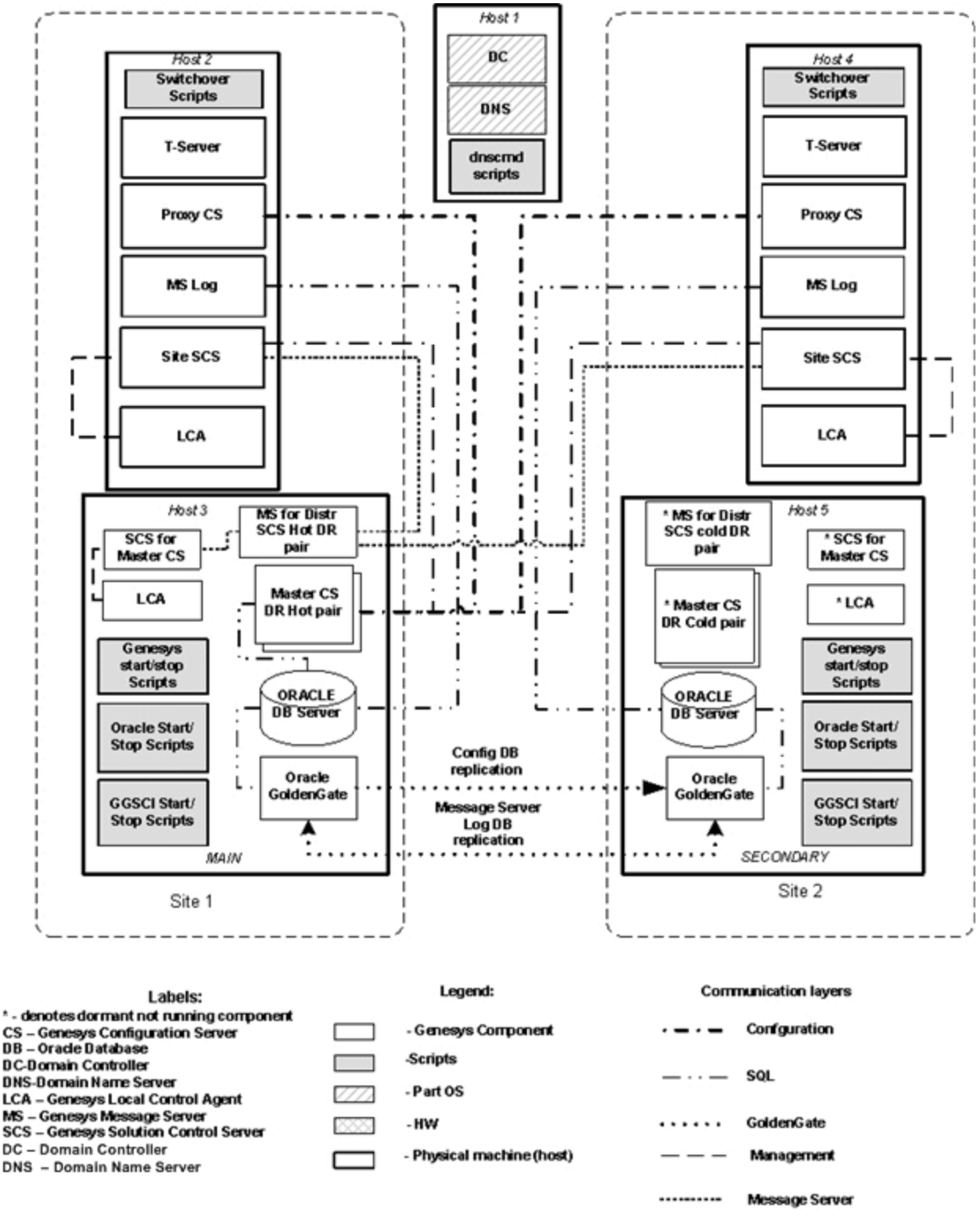
This architecture consists of the following components:

- Main live DBMS database server at Site 1.
- Secondary live DBMS at Site 2.
- DBMS solution to replicate the live Configuration Database to a secondary live standby database and log message databases cross sites replication.
- Main live redundant pair master Configuration Server primary/backup pair at Site 1.
- Secondary dormant (not running in normal operation mode) master Configuration Server primary/backup pair at Site 2.
- Main live Solution Control Server in distributed mode to control the main master Configuration Server pair at Site 1.
- Secondary dormant Solution Control Server in distributed mode to control the secondary Master Configuration Server pair at Site 2.
- Main Message Server at Site 1 to support communication between Solution Control Servers controlling site components, such as Configuration Server Proxy pairs, T-Servers, Log Message Servers.
- Secondary dormant (not running in normal operation mode) Message Server at Site 2 to support communication between Solution Control Servers controlling site components, such as Configuration Server Proxy pairs, T-Servers, and Log Message Servers.

- Live Configuration Server Proxy pair at Site 1.
- Live Configuration Server Proxy pair at Site 2.
- Live Solution Control Server at Site 1.
- Live Solution Control Server at Site 2.
- Live Message Server for network logging at Site 1, connected to the Log Database at Site 1.
- Live Message Server for network logging at Site 2, connected to the Log Database at Site 2.
- Scripts to start and stop the master Configuration Server primary/backup pair and master Solution Control Servers.
- DBMS scripts to enable and disable database access.
- DBMS solution scripts to start and stop replication processes.
- A script residing at the DNS server host to change IP address name resolution for the master Configuration Server host.
- A switchover script to push name resolution changes for Configuration Server Proxy hosts at Sites 1 and 2 after the IP address name resolution changes at the DNS server host.

Architecture

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



Labels:

* - denotes dormant not running component
CS – Genesys Configuration Server
DB – Oracle Database
DC-Domain Controller
DNS-Domain Name Server
LCA – Genesys Local Control Agent
MS – Genesys Message Server
SCS – Genesys Solution Control Server
DC – Domain Controller
DNS – Domain Name Server

Legend:

- Genesys Component
- Scripts
- Part OS
- HW
- Physical machine (host)

Communication layers

- Configuration
- SQL
- GoldenGate
- Management
- Message Server

Solution Control Server

The Solution Control Servers used in this deployment are configured in Distributed SCS mode. Some or all can also be configured in HA pairs at each site.

At each site, a Solution Control Server is deployed on the management host (Hosts 3 and 5 in the diagram above) and is dedicated to managing Applications on the management hosts, specifically Configuration Server and the dedicated Message Server for the Distributed Solution Control Servers, described below. Site Solution Control Server must always connect to the Main Configuration Server but not Site Configuration Server Proxies.

For Distributed Solution Control Servers to communicate with each other, a Message Server dedicated for distributed Solution Control Server use (that is, configured with **[MessageServer].signature=**`scs_distributed`) is also installed on each of the management hosts.

Each site also has a separate Solution Control Server deployed on the Application host configured to manage Genesys applications running on each site (that is, the site SCS in the diagram above).

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

For additional fault tolerance, Solution Control Servers can be deployed in high-availability (HA) pairs.

Message Server

Each site has its own instance of a Log Message Server to be used for network logging by applications running on the same site. Message Servers are installed on the application host and managed by the site Solution Control Server. A dedicated Log Database is used at each site. In a symmetrical setup, access to the database can use GEO DNS.

In addition, a Message Server is also dedicated to communications between the distributed Solution Control Servers. This requires two instances (or two HA pairs) of Message Servers to be deployed, one of which is dormant.

DNS Server Configuration and Switchover Scripts

The DNS Server configures a record type A to resolve the IP address of a host running the live master Configuration Server primary/backup pair. It resolves the IP address to the main host in normal mode, and to the secondary host in failover mode. It consists of two scripts setting the IP address resolution, one for the main host and the second for the secondary host.

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

DBMS Solution Replication Processes Configuration

The DBMS Solution must have replication processes designed to cross-replicate the Configuration and Log Databases, such as:

- From the database on the main system to that on the secondary system.

- From the database on the secondary system to that on the main system.

The following diagram illustrates the DBMS configuration in normal operating mode. In this mode, the Configuration Database replication process from the secondary system to the main system is in STOPPED state (marked *). It is started only when the secondary Configuration Database is switched from live standby to live mode and used for the initial data replication from the secondary to main database after the main system is restored.