Genesys Security Deployment Guide

Application Redundancy

5/6/2025

Application Redundancy

Contents

Redundant applications, normally server applications, provide backup capability in the event that an application fails. That is, if one server (the primary server) goes out of service for some reason, such as lost connectivity, the other server (the backup server) can act as the primary server, with little or no loss of service.

Security Benefits

The use of redundant applications greatly reduces the loss of functionality and data if an application is out of service because of a security-related attack, such as a denial-of-service attack.

Supporting Components

Refer to documentation for your product to determine if it supports redundancy, and the redundancy types that it supports.

Feature Description

Redundant applications address the potential loss of functionality and data in the event of an application failure.

A complete application failure can be the result of either an internal defect (for example, an infinite loop) or an external event (for example, a power failure). It can manifest itself either as no response from a process, or as termination. Typically, if a solution component stops working, the solution is no longer available to process customer interactions.

Because the application that fails cannot perform any functions, you must employ an external mechanism for both detection and correction of faults of this type. The Management Layer serves as such a mechanism. To detect an application failure, the Management Layer employs a simple monitoring component called Local Control Agent (LCA), which continuously maintains a connection with the application, confirming both its existence and its ability to communicate. To ensure that an application failure is never confused with a connection failure, the LCA that monitors a specific application always resides on the computer where the application itself is running.

LCA is installed on a one-per-host basis, and can connect to all Genesys applications located on the host. When a connection is broken, LCA generates a message to Solution Control Server (SCS), where an appropriate recovery action is chosen and executed according to the system configuration. SCS uses the Advanced Disconnect Detection Protocol (ADDP) to recognize a loss of connection with LCA. A loss of connection is interpreted as a failure of the host (that is, as failures of all Genesys components running on that host).

If a backup application is configured and running, the Management Layer automatically switches operations over to that application, provided that you have a so-called *high-availability (HA) license* . If the application is a server, the clients automatically connect to the backup server.

The Management Layer provides more robust switchover capabilities. In particular, it enables detection of situations when a running application is unable to provide service, and treats this situation as an application failure. The Service Unavailable application status serves this purpose.

When an application reports that its status has changed to Service Unavailable, if a backup server for this application is configured and running, the Management Layer automatically switches operations over to the backup server. When both the primary and backup applications are running with the Service Unavailable status, the backup application might report that it can now provide the service (that is, the status of the backup application changes to Started). In this case, the Management Layer automatically switches operations over to the backup application. As with a switchover resulting from an application failure, you must have an HA license to perform a switchover related to service unavailability.

> **Important**
>
> Although some applications support the Service Unavailable status and report it under appropriate circumstances, others do not. (For example, when T-Server loses its connection to the CTI Link, T-Server changes its status to Service Unavailable). The Management Layer bases its operation on the information supplied by an application, and cannot automatically detect an application's inability to provide service. Refer to application-specific documentation to determine whether the Service Unavailable status is supported on the application side.

Redundancy Types

There are two types of redundancy in Genesys software-warm standby and hot standby.

Warm Standby

Genesys uses the term *warm standby* to describe the redundancy type in which a backup server application remains initialized and ready to take over the operations of the primary server. The Warm standby redundancy type minimizes the inability to process interactions that might have originated during the time it took to detect the failure. It also eliminates the need to bring a backup server online, thereby increasing solution availability.

The backup server does not process client requests until its role is changed to primary by the Management Layer. When a connection is broken between the primary server and the LCA running on the same host, a failure of the primary process is reported. As a result, the Management Layer instructs the backup process to switch its role from backup to primary, and the former backup starts processing all new requests for service.

> **Important**
>
> To switch to Primary mode, the backup Configuration Server must have an active connection to the Configuration Database during the failure of the primary

> Configuration Server.

Although normal operations are restored as soon as the backup process takes over, the fault management effort continues. This consists of repeated attempts to restart the process that failed. Once it is restarted successfully, the process is assigned the backup role.

If SCS detects a loss of connection with the LCA of a host, it performs switchover for all applications located on the host, provided that backup applications are configured. There are two exceptions to this:

- A Configuration Server in backup mode ignores the switchover command if it detects another Configuration Server in primary mode. In other words, if the LCA residing on a host with a Configuration Server in primary mode goes down, the SCS requests that a Configuration Server in backup mode, on another host with an available LCA, switch over to primary mode. When it receives the request, this Configuration Server checks whether the Configuration Server in primary mode is down, as indicated by a lost connection between the two Configuration Servers. The Configuration Server in backup mode switches over to primary mode only if this connection is down. If the connection still exists, no switchover occurs.
- An SCS in backup mode does not try to switch itself over if it can still detect the SCS that is in primary mode. In other words, if an SCS in backup mode loses its connection to an LCA residing on a remote host with an SCS in primary mode—either because the LCA went down or a network timeout caused the SCS to drop its connection—the SCS in backup mode checks whether it is still connected to the remote SCS in primary mode. If that connection is also lost, the SCS switches over to primary mode.

Hot Standby

Genesys uses the term *hot standby* to describe the redundancy type in which a backup server application remains initialized, clients connect to both the primary and the backup servers at startup, and the backup server data is synchronized with the primary server. Data synchronization and existing client connections to the backup guarantee higher availability of a component.

Feature Configuration

The configuration of redundant Genesys applications can vary, depending on application type, and requires that you do the following steps:

1. Create an Application object for the primary application.
2. Install the primary application.
3. Configure an Application object for the backup application.
4. Install the backup application.
5. In the primary Application object, add the backup Application object and specify the supported redundancy type.

For more information, and for detailed instructions for setting up redundant applications in your environment, refer to product-specific documentation.