High-Availability Deployment

This chapter describes the general steps for setting up a high-availability (HA) environment for your T-Server. The high-availability architecture implies the existence of redundant applications, a primary and a backup. These are monitored by a management application so that, if one application fails, the other can take over its operations without any significant loss of contact center data.

Every switch/T-Server combination offers different high-availability options. The Framework Management Layer currently supports two types of redundant configurations: `warm standby` and `hot standby`. All T-Servers offer the `warm standby` redundancy type and, starting with release 7.1, the `hot standby` redundancy type is implemented in T-Servers for most types of switches. Some T-Servers support a switch's ability to provide two CTI links to two T-Servers or even one CTI link to two T-Servers.

This chapter describes the redundant architecture and how to configure T-Server so that it operates with either type. Information in this chapter is divided into the following sections:

Warm Standby Redundancy Type

Genesys uses the expression *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 reduces to a minimum the inability to process interactions that may have

originated during the time it took to detect the failure. It also eliminates the need to bring a standby server online, thereby increasing solution availability.

Warm Standby Redundancy Architecture

Figure 5 illustrates the warm standby architecture. The standby server recognizes its role as a backup and does not process client requests until the Management Layer changes its role to primary. When a connection is broken between the primary server and the Local Control Agent (LCA, not shown in the diagram) running on the same host, a failure of the primary process is reported, and the switchover occurs; or, if the host on which the T-Server is running fails, the switchover also occurs. (See the *Framework 8.1 Deployment Guide* for information on LCA.) As a result:

1. The Management Layer instructs the standby process to change its role from backup to primary.

2. A client application reconnects to the new primary.

3. The new primary (former backup) starts processing all new requests for service.
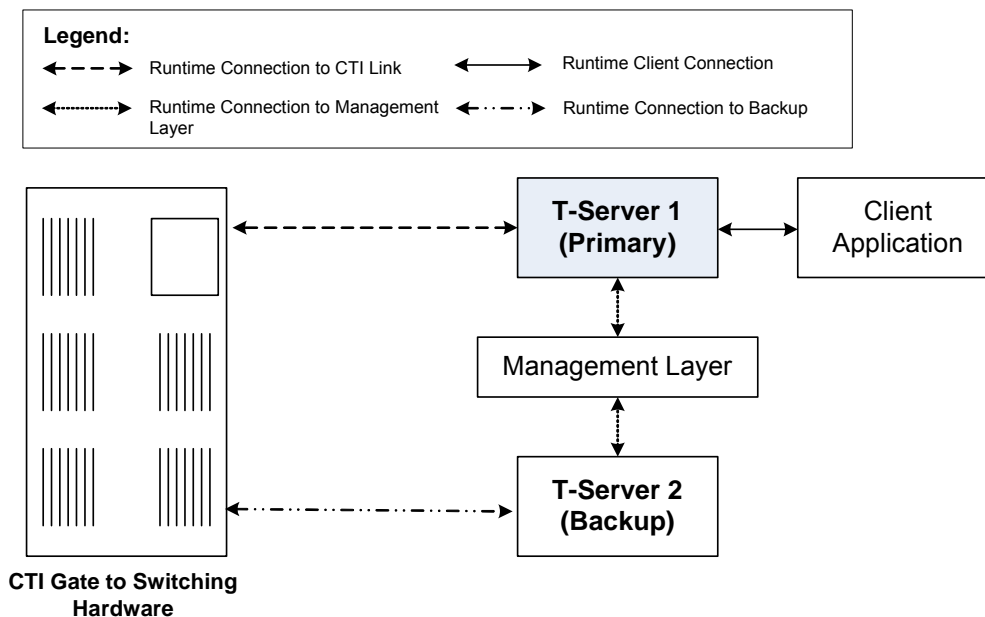

Figure 5: Warm Standby Redundancy Architecture

Although normal operations are restored as soon as the backup process takes over, the fault management effort continues. That effort consists of repeated

attempts to restart the process that failed. Once successfully restarted, the process is assigned the backup role.

Note: You can find full details on the role of the Management Layer in redundant configurations in the *Framework 8.1 Deployment Guide*.

Hot Standby Redundancy Type

Genesys uses the expression *hot standby* to describe the redundancy type in which a backup server application remains initialized, clients connect to both the primary and backup servers at startup, and the backup server data is synchronized from the primary server. Data synchronization and existing client connections to the backup guarantee higher availability of a component. (See Figure 6 on .)

Starting with release 7.1, the `hot standby` redundancy type is implemented in T-Servers for most types of switches. However, for some switches, you must compensate for the lack of link redundancy by using an additional Genesys component called *HA Proxy*.

Hot Standby Redundancy Architecture

Figure 6 illustrates the switch-independent side of a `hot standby` implementation. Here, T-Servers start simultaneously and connect to the switch. At T-Server startup, the Management Layer assigns the role of the primary server to T-Server 1, and the role of backup to T-Server 2. T-Server clients register with both T-Servers, but only the primary T-Server handles client requests other than the registration requests. The internal T-Server information, such as a DN status, `ConnID`, `UserData`, and `Call Type`, is synchronized between the primary and backup T-Servers. Therefore, the backup T-Server has the same information as the primary T-Server.

If T-Server 1 fails, the Management Layer makes T-Server 2 the new primary server, and it starts processing client requests. The Management Layer attempts to restart T-Server 1, and if it is successful, it makes T-Server 1 the new backup server.

The details of `hot standby` redundancy implementation between T-Servers and their switches vary depending on switch support for multiple CTI links.
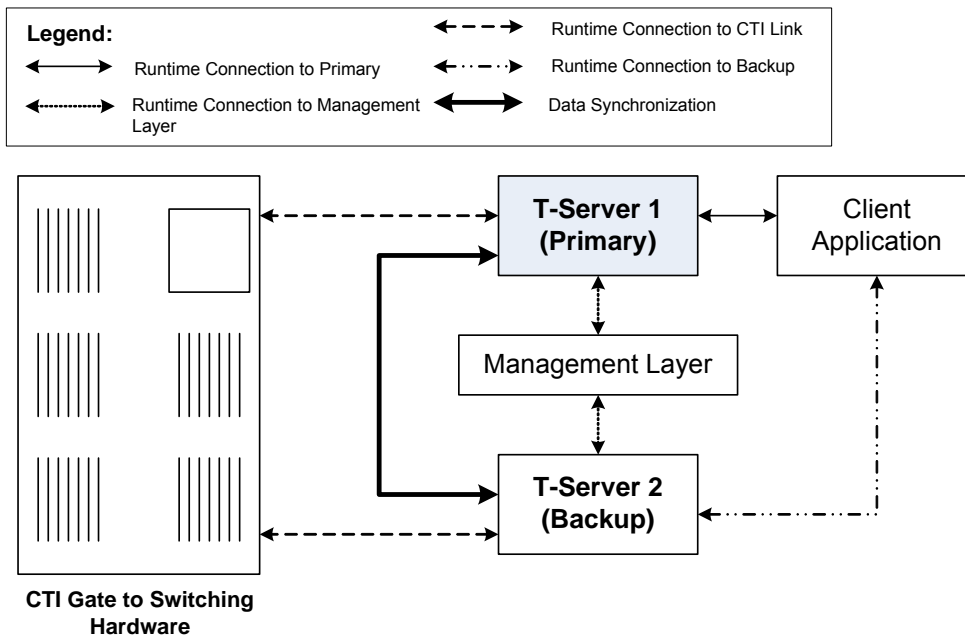
Figure 6: Hot Standby Redundancy Architecture

Benefits of Hot Standby Redundancy

The `hot standby` redundancy type provides the following benefits over the `warm standby` type:

- Using `hot standby` ensures the processing of interactions in progress if a failure occurs. After the primary T-Server (T-Server 1) fails, T-Server 2 handles all new interactions and takes over the processing of interactions that are currently in progress.

- T-Servers perform one-way (from primary to backup) synchronization of call-associated data, including, but not limited to:
  - Connection IDs.
  - Attached user data.
  - Inter Server Call Control (ISCC; formerly called External Routing) call references to another site in a multi-site environment (to support the ISCC/COF feature).

  Note: Refer to "ISCC Call Data Transfer Service" on page 41 for ISCC feature descriptions.

- When mirrored links are not available, HA Proxy helps T-Server synchronize the current states of agents, calls, parties, and devices between the primary and backup T-Servers.

However, keep the following `hot standby` limitations in mind:

- Client requests sent during the failure and switchover may be lost.
- Routing requests sent by the switch during the failure and switchover may be lost.
- T-Server does not synchronize interactions that begin before it starts, including incomplete ISCC-related transactions.
- Some T-Library events might be duplicated or lost.
- Reference IDs from client requests can be lost in events.

Prerequisites

This section presents basic requirements and recommendations for configuring and using redundant T-Servers.

Requirements

You must install the Management Layer if you are installing redundant T-Server applications. In particular, install Local Control Agent (LCA) on each computer that runs T-Server.

Warning!   Genesys strongly recommends that you install the backup and primary T-Servers on different host computers.

Synchronization Between Redundant T-Servers

When T-Servers operate in a high-availability environment, the backup T-Server must be ready to take on the primary role when required. For this purpose, both T-Servers must be running and must have the same information. When you configure redundant T-Servers to operate with the `hot standby` type, the primary T-Server uses the connection to the backup to deliver synchronization updates. Genesys recommends that you enable the Advanced Disconnect Detection Protocol (ADDP), described in Chapter 1, for this connection. Do so using the configuration options in the "Backup-Synchronization Section" section. Refer to the "T-Server Common Configuration Options" chapter for option descriptions.

Configuration Warnings

When configuring T-Servers to support either the `warm standby` or `hot standby` redundancy type, remember:

1. When at least one of the two T-Servers that operate in a redundant mode is running, do not change a redundancy type, host, or port in either T-Server configuration.

2. When both the primary and backup T-Servers are running, do not remove the backup T-Server `Application` object from the configuration.

You are responsible for the option synchronization in the configuration of the primary and backup T-Servers; Configuration Server does not synchronize either options or their values in different T-Server `Application` objects. That is, you must configure both T-Servers to have the same options with the same values. If you change a value in one T-Server configuration, you must change it in the other T-Server configuration manually. The log options in the primary T-Server can differ from those in the backup T-Server configuration. The link configuration options in the primary T-Server can also differ from those in the backup T-Server configuration.

Warm Standby Deployment

This section describes how to configure redundant T-Servers to work with the `warm standby` redundancy type, including details on their connections and settings.

General Order of Deployment

The general guidelines for T-Server `warm standby` configuration are:

1. Configure two T-Server `Application` objects as described in "Configuration of T-Server" on .

2. Make sure the `Switch` object is configured for the switch these T-Servers should serve, as described in "Configuration of T-Server" on .

3. Modify the configuration of the primary and backup T-Servers as instructed in the following sections.

After completing the configuration steps, ensure that both T-Servers are installed (see).

Modification of T-Servers for Warm Standby

Modify the configuration of both the primary and backup T-Server `Application` objects as described in the following sections.

Note: Starting with release 7.5, you can configure multiple ports for any application of type `server`. When multiple ports are configured for a server in a `warm standby` redundancy pair, the number of ports, their `Port IDs,` and the `Listening Mode` settings of the primary and backup servers must match respectively.

Procedure:
Modifying the primary T-Server configuration for warm standby

Start of procedure

1. Stop both the primary and backup T-Servers if they are already running.

2. Open the Configuration Manager main window.

3. Open the `Properties` dialog box of the `Application` object for the T-Server that you want to configure as a primary server.

4. Click the `Switches` tab.

5. Ensure that it specifies the Switch that this T-Server `Application` should serve. If necessary, select the correct `Switch` using the `Browse` button.

6. Click `Apply` to save the configuration changes.

7. Click the `Server Info` tab.

8. Specify the T-Server `Application` you want to use as the backup server. Use the `Browse` button next to the `Backup Server` field to locate the backup T-Server `Application` object.

9. Select `Warm Standby` as the `Redundancy Type`.

10. Click `Apply` to save the configuration changes.

11. Click the `Start Info` tab.

12. Select `Auto-Restart`.

13. Click `Apply` and `OK` to save the configuration changes.

End of procedure

Next Steps

- Procedure: Modifying the backup T-Server configuration for warm standby, on page 34

Procedure:
Modifying the backup T-Server configuration for warm standby

Start of procedure

1. Make sure the two T-Servers are *not* running.

2. Open the Configuration Manager main window.

3. Open the `Properties` dialog box of the `Application` object for the T-Server that you want to configure as a backup server.

4. Click the `Switches` tab.

5. Using the `Browse` button, select the same `Switch` object you associated with the primary T-Server `Application` object.

6. Click `Apply` to save the configuration changes.

7. Click the `Start Info` tab.

8. Select `Auto-Restart`.

9. Click `Apply` and `OK` to save the configuration changes.

End of procedure

Warm Standby Installation of Redundant T-Servers

The installation of a redundant T-Server is the same as that for the stand-alone T-Server. If you have not installed the primary and backup T-Servers yet, follow the instructions in "Installation of T-Server" on for both installations.

Hot Standby Deployment

This section describes how to configure redundant T-Servers to work with the `hot standby` redundancy type, including details on their connections and settings.

General Order of Deployment

The general guidelines for T-Server `hot standby` configuration are:

1. Configure two T-Server `Applications` objects as described in "Configuring T-Server" on .

2. Make sure the `Switch` object is configured for the switch these T-Servers should serve, as described in "Configuration of Telephony Objects" on page 18.

3. Modify the configuration of the primary and backup T-Servers as instructed in the following sections.

After completing the configuration steps, ensure that both T-Servers are installed (see page 37).

Modification of T-Servers for Hot Standby

Modify the configuration of both the primary and backup T-Server `Application` objects for `hot standby` redundancy as described in the following sections.

Note: Starting with release 7.5, you can configure multiple ports for any application of type `server`. When multiple ports are configured for a server in a `hot standby` redundancy pair, the number of ports, their `Port IDs`, and the `Listening Mode` settings of the primary and backup servers must match respectively.

Procedure:
Modifying the primary T-Server configuration for hot standby

Start of procedure

1. Stop both primary and backup T-Servers if they are already running.

2. Open the Configuration Manager main window.

3. Open the `Properties` dialog box of the `Application` object for the T-Server that you want to configure as a primary server.

4. Click the `Switches` tab.

5. Ensure that it specifies the `Switch` that this T-Server `Application` should serve. If necessary, select the correct `Switch` using the `Browse` button.

6. Click `Apply` to save the configuration changes.

7. Click the `Server Info` tab.

8. In the `Ports` section, select the port to which the backup server will connect for HA data synchronization and click `Edit Port`.

Note: For information on adding multiple ports, see "Configuring multiple ports" on page 22.

---

   a. In the `Port Properties` dialog box, on the `Port Info` tab, select the `HA sync` check box.

   b. Click `OK`.

Note: If the `HA sync` check box is not selected, the backup T-Server will connect to the *default* port of the primary T-Server.

---

9. Specify the T-Server `Application` you want to use as the backup server. Use the `Browse` button next to the `Backup Server` field to locate the backup T-Server `Application` object.

10. Select `Hot Standby` as the `Redundancy Type`.

11. Click `Apply` to save the configuration changes.

12. Click the `Start Info` tab.

13. Select `Auto-Restart`.

14. Click `Apply` to save the configuration changes.

15. To enable ADDP between the primary and backup T-Servers, click the `Options` tab. Open or create the `backup-sync` section and configure corresponding options.

16. Click `Apply` and `OK` to save the configuration changes.

End of procedure

Next Steps

Procedure:
Modifying the backup T-Server configuration for hot standby

Start of procedure

1. Make sure the two T-Servers are *not* running.

2. Open the Configuration Manager main window.

3. Open the `Properties` dialog box of the `Application` object for the T-Server that you want to configure as a backup server.

4. Click the `Switches` tab.

5. Using the `Browse` button, select the same `Switch` object you associated with the primary T-Server `Application`.

6. Click the `Server Info` tab.

7. In the `Ports` section, select the port to which the primary server will connect for HA data synchronization and click `Edit Port`.

Note: For information on adding multiple ports, see "Configuring multiple ports" on .

---

a. In the `Port Properties` dialog box, on the `Port Info` tab, select the `HA sync` check box.

b. Click `OK`.

Note: If the `HA sync` check box is not selected, the primary T-Server will connect to the *default* port of the backup T-Server.

---

8. Click `Apply` to save the configuration changes.

9. Click the `Start Info` tab.

10. Select `Auto-Restart`.

11. Click the `Options` tab.

12. Modify the values for all necessary configuration options. Genesys recommends that you set all configuration options for the backup T-Server to the same values as for the primary T-Server; the only exceptions are the log options and the `server-id` option.

13. Click `Apply` and `OK` to save the configuration changes.

End of procedure

Hot Standby Installation of Redundant T-Servers

The installation of a redundant T-Server is the same as that for the stand-alone T-Server. If you have not installed the primary and backup T-Servers yet, follow instructions in "Installation of T-Server" on for both installations.

Next Steps

At this point, you have learned how to configure and install redundant T-Servers. Go to Chapter 5, "Starting and Stopping T-Server and CSTA Connector," on page 97, to test your configuration and installation, or continue with Chapter 4, "Multi-Site Support," on page 39, for more possibilities.