Framework Deployment Guide

Distributed Solution Control Servers

5/8/2025

Contents

Distributed Solution Control Servers

Multiple Solution Control Servers operating in Distributed mode (referred to as *Distributed Solution Control Servers*) distribute management-related tasks among the sites in a distributed enterprise that uses a single Genesys Configuration Database.

What are Distributed Solution Control Servers?

In these installations, each SCS controls its own subset (defined by you) of the Hosts, Applications, and Solutions, and communicates with the others through a dedicated Message Server.

Specifically, a Distributed Solution Control Server performs the following functions:

- Performs the same functions of monitoring, control, alarm detection, and alarm processing as the SCS in non-Distributed mode, but on a subset of Hosts, Applications, and Solutions explicitly assigned to this SCS in the Configuration Database.
- Communicates all the updates to statuses of the assigned objects to other Distributed Solution Control Servers, using a dedicated Message Server.
- Receives notifications about updates to the status of non-assigned objects (that is, objects assigned to other Solution Control Servers) from Message Server.
- When receiving a control command on an object not assigned to this SCS, forwards this command via Message Server to the appropriate SCS.

Because Distributed Solution Control Servers communicate with each other, they all have the same information about all hosts, applications, and solutions. Thus, you can connect the interface object associated with Genesys Administrator to any Distributed SCS and monitor and control the whole environment as a single entity (given appropriate permissions). When a Distributed SCS receives a control command for an object that this SCS does not control, it forwards this command to the appropriate SCS and passes any further notifications back to the requestor.

Using Distributed Solution Control Servers helps you resolve some problems common to distributed installations:

- It eliminates false switchovers that occur when SCS disconnects from LCA at a remote site because of the slow network connection between sites or because of temporary network problems.
- It prevents a single point of failure. A failure of one Distributed SCS only means a temporary loss of control over a subset of Hosts, Applications, and Solutions; other Distributed Solution Control Servers continue to control the rest of the environment.

Limitation

In distributed mode, Solution Control Server reports host statistics (such as CPU, User Time, Kernel Time, and Non-IDLE Time) for only the host it controls when Genesys Administrator or Genesys Administrator Extension (GAX) is connected to SCS. It does not provide host information for other hosts that are controlled by other Solution Control Servers in distributed mode.

For example, assume the following distributed SCS environment:

host_a
host_b
SCS_a is located on, and controls, host_a
SCS_b is located on, and controls, host_b
GAX can be connected to either SCS_a or SCS_b

When GAX is connected to SCS_a, it reports host statistics for only host_a.
When GAX is connected to SCS_b, it reports host statistics for only host_b.

Deploying Distributed Solution Control Servers

Warning

- Do not use Solution Control Servers in Distributed and non-Distributed modes simultaneously within the same Configuration environment. If you plan to use Distributed SCS in your installation, turn on Distributed mode for all Solution Control Servers you install.
- When using Distributed Solution Control Servers, always ensure that each Solution Control Server, either by itself or as part of a high-availability pair, is running on the host which it controls. Failure to do so can, in some cases, result in unpredictable behavior of the Solution Control Servers in the Distributed configuration. For example, different Solution Control Servers may start competing for control over Applications on the Host.
- When working with applications in HA pairs, the same distributed SCS must be configured to control both applications working in each HA pair.

1. Configure Distributed Solution Control Servers in Distributed mode.

a. Configure as many Solution Control Server Application objects as necessary, as described in Solution Control Server.

b. Turn on Distributed mode for each Solution Control Server Application object, by setting the following configuration options in the **[general]** section:

   - **distributed_mode=**`on`
   - **distributed_rights=**`default`

c. If you are planning to leave any of the Host, Application, or Solution objects unassigned—that is, without specifying which SCS is to control them—dedicate one SCS to the control of all unassigned hosts, applications, and solutions. To instruct one SCS to work in this mode, set the following values for configuration options in the **[general]** section for that particular SCS application:

   - **distributed_mode=**`on`

- **distributed_rights=**`main`

> **Important**
>
> Only one of the Distributed Solution Control Servers can have the value `main` for the **distributed_rights** configuration option.

2. Divide your configuration environment between the Solution Control Servers.

When you are using Distributed Solution Control Servers, you must explicitly configure the servers' ownership of Hosts, Applications, and Solutions. That is, you must associate each Host, Application, and Solution object with a particular SCS by changing the object's properties:

> **Important**
>
> To distribute control over the primary and backup servers in a redundant pair between different Distributed Solution Control Servers, all Solution Control Servers in the configuration must be running release 7.6 or later.

Recommendations

- Do not distribute control over the primary and backup servers in a redundant pair between different Distributed Solution Control Servers if any SCS in the configuration environment is running a pre-7.5 release. Genesys recommends that you configure the same SCS to control both the primary and backup servers in a redundant pair.
- When you are distributing control over the configuration objects among Distributed Solution Control Servers, ensure that the same SCS that controls a solution also controls all applications included in this solution. Although one SCS can technically control a solution while other servers control applications included in that solution, avoiding this configuration helps minimize network traffic between Solution Control Servers.
- Genesys strongly recommends that you not assign each component in an HA pair to different Solution Control Servers in a distributed environment. In this configuration, the functionality of each Solution Control Server in the HA pair might be limited to handling simple application failures only (the failure of an application within the pair). In addition, the state of each component in the monitored HA pair might become inconsistent if network failures occur between the Distributed Solution Control Servers.

Assigning a Distributed Solution Control Server

- To control a Host: In the Host object, specify the SCS Application in the **Solution Control Server** field in the **General** section of the **Configuration** tab.
- To control an Application: Do not make any changes to the Application object. Specifying SCS ownership of the Application's Host is enough. The Distributed SCS automatically controls any Applications assigned to the Host this SCS controls.
- To control a Solution: In the Solution object, specify the SCS Application in the **Solution Control Server** field in the **General** section of the **Configuration** tab.

3. Configure a dedicated Message Server through which the Distributed Solution Control Servers will communicate with each other.

Recommendations

Distributed Solution Control Servers communicate with each other through Message Server. Genesys recommends that you use a dedicated Message Server for this purpose.

Prerequisites

- An Application object exists for each Distributed SCS in the configuration environment.
- You are logged in to Genesys Administrator.

Configuring a Dedicated Message Server

a. Configure a Message Server Application object with appropriate configuration parameters. Refer to Message Server.

b. Double-click the Message Server Application object, and click the **Options** tab.

c. Create a new configuration options section called **[MessageServer]**.

d. In this section, create a new configuration option called **signature** and set its value to `scs_distributed`. Each Distributed SCS will process this option to determine which of the Message Servers specified in its **Connections** to use for communications with other Solution Control Servers.

e. In the Application object for each Distributed Solution Control Server, add a connection to this Message Server, as follows:

1. Enter ADDP as the **Connection protocol**.
2. Set the **ADDP Local Timeout** and **Remote Timeout** to values that are less than half the minimum **alive_timeout** values of all Distributed Solution Control Servers in the configuration environment.
   In other words:
   $T_{addp} < T_{scs} * 0.5$
   where:
   T_{addp} = ADDP timeout
   T_{scs} = minimum `alive_timeout` of all Distributed Solution Control Servers
   Refer to the *Framework Configuration Options Reference Manual* for a detailed description of the **alive_timeout** option.

4. (Optional) Configure a Message Server for centralized logging at each site with Distributed Solution Control Servers.

For distributed environments using a single Configuration Database, Genesys recommends using a dedicated Message Server for centralized logging at each site. In most cases, you have to configure as many Message Servers as there are Distributed Solution Control Servers.

> **Important**
> You can configure as many Message Servers for centralized logging as you need per site. These are in addition to the Message Server dedicated to handle communications between the distributed servers.

After you have installed the Message Servers, you should verify that each Message Server used for centralized logging is configured and connected to a Solution Control Server and to each of the applications controlled by that Solution Control Server as follows:

Prerequisites

- Distributed Solution Control Servers are set up in the configuration environment.

- The Message Server used for centralized logging in this environment is installed.
- You are logged in to Genesys Administrator.

Verifying Configuration of Message Servers used for Centralized Logging

a. Go to **Provisioning > Applications**, and double-click a Solution Control Server Application object to open its Configuration tab.

b. In the **General** section, make sure that a connection to the Message Server that is providing the centralized logging is added to the list of **Connections**.

c. For each Application object that this particular Solution Control Server controls:

   i. Open the **Configuration** tab of the Application object.

   ii. In the **General** section, make sure that a connection to that same Message Server is added to the list of **Connections**.

5. (Optional) Configure redundant Application objects for Distributed Solution Control Servers.

Distributed Solution Control Servers support the Warm Standby redundant configuration in the same way as other Genesys servers, with the added benefit that the backup maintains data synchronization with the primary. That is, you can configure a primary and a backup pair of Distributed Solution Control Servers to operate with Warm Standby redundancy. Refer to Redundant Solution Control Servers for more information.

6. After you are finished with the configuration tasks, physically install all instances of Solution Control Server and Message Server to match the configuration.

Starting Distributed Solution Control Servers

> **Important**
>
> Starting a Solution Control Server in Distributed mode requires a special license. Refer to the *Genesys Licensing Guide* for more information.

Start each Distributed Solution Control Server in the same way as you would start a non-distributed SCS. See Starting SCS and Starting a Backup SCS for more information.