This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

SIP Server HA Deployment Guide

SIP Server 8.1.0

1/14/2022

Table of Contents

SIP Server High-Availability Deployment Guide

This guide introduces you to the concepts, terminology, and procedures that are relevant to SIP Server high-availability (HA) deployment.

Find the information you need from the topics below.

About the HA Methods

Find descriptions of the different ways you can set up HA SIP Server instances.

IP Address Takeover

Windows NLB

Network Device-Based HA

Deploying on Windows

Find procedures for the different ways to deploy SIP Server HA on Windows servers.

IP Address Takeover on Windows

Windows NLB

Business Continuity

Find information about setting up Business Continuity in your environment.

Architecture

Deployment

Deploying on UNIX

Find procedures for the different ways to deploy SIP Server HA on UNIX-based servers.

Deploying on AIX

Deploying on Solaris

Deploying on Linux

Overview

Welcome to the *Framework 8.1 SIP Server High-Availability Deployment Guide*. These topics introduce you to the concepts, terminology, and procedures that are relevant to SIP Server high-availability (HA) deployment.

The information includes, but is not limited to, an overview of SIP Server HA architecture, HA workflows, and SIP Server HA-deployment procedures for Windows and UNIX operating systems.

This document can be used together with the Framework 8.1 SIP Server Deployment Guide during your deployment planning.

About SIP Server

SIP Server is the Genesys software component that provides an interface between your telephony hardware and the rest of the Genesys software components in your enterprise. It translates and keeps track of events and requests that come from, and are sent to, the telephony device. SIP Server is an IP"based server that can also act as a messaging interface between SIP Server clients. It is the critical point in allowing your Genesys solution to facilitate and track the contacts that flow through your enterprise.

Intended Audience

These topics primarily intended for system architects or administrators who are responsible for ensuring that systems, including SIP Server, are highly available. It has been written with the assumption that you have a basic understanding of:

- High-availability architecture
- Network design and operation
- Genesys Framework architecture and functions
- Your own network architecture and configurations

Reading Prerequisites

You must read the Framework 8.1 SIP Server Deployment Guide before you use these topics. Those topics contain information about the SIP Server deployment in general.

SIP Server HA Architecture

A high-availability (HA) architecture implies the existence of redundant applications: a primary and a backup. These applications are configured so that if one fails, the other can take over its operations without significant loss of data or impact to business operations.

SIP Server supports several high-availability deployment options:

- IP Address Takeover
- Windows NLB Cluster
- Network device-based HA

IP Address Takeover and Windows NLB Cluster HA options utilize the concept of a Virtual IP address. In a Virtual IP interface"based architecture, primary and backup SIP Servers are located on the same subnet, and SIP endpoints and gateways are configured to send SIP messages to SIP Server by using this single Virtual IP address. The Virtual IP address is preserved during switchover occurrences, and messages that are sent to the Virtual IP address are delivered to the SIP Server that is currently running in primary mode.

When the Management Layer detects failure of a primary SIP Server, it executes a set of corrective actions, which allows SIP messages that are destined for the failed primary SIP Server to be delivered to the backup SIP Server that has just started running in primary mode.

While SIP endpoints and gateways use a single Virtual IP address to communicate with SIP Server, Management Layer and Configuration Layer components, and T-Library clients must use a unique IP address for communication with the SIP Server and Local Control Agent (LCA) that is installed at each SIP Server host.

On Windows and UNIX, an IP Address Takeover configuration is implemented by using Virtual IP address control scripts to enable and disable Virtual IP addresses. The Windows NLB configuration uses Cluster control scripts to enable and disable Virtual IP ports.

A network device-based HA is an alternative to software-based HA configurations. The SIP Server and F5 Networks BIG-IP Local Traffic Manager (LTM) integration solution supports this type of HA configuration.

Each of these configurations is described in more detail in the following sections.

The following table summarizes SIP Server HA options, their benefits and limitations, and supported operating systems (Windows, Linux, Solaris, or AIX).

Comparing High-Availability Options

HA Option	Benefits	Limitations
IP Address Takeover	• Supported on all operating systems • Supports multiple NICs	• Supports a single subnet • Operations on both servers, backup and primary, must succeed

HA Option	Benefits	Limitations
	• 100% Genesys components • HA option of choice for reliability ratings and tests	• Subnet equipment to accept gratuitous ARP
Windows NLB Cluster	• Widely deployed • Thoroughly documented • Supports multiple NICs	• Supports a single subnet • Complexity/Prerequisites • Dedicated switch/VLAN
F5 Networks BIG-IP LTM	• Reliability • Flexibility (HA and Load balancing) • Supports multiple NICs	• Additional equipment cost • Additional network element

SIP Server also supports HA configurations in which both primary and backup SIP Server instances reside on a single host server. In this case, IP interface virtualization is not required.

HA Redundancy Types

When you deploy a SIP Server HA configuration, you can choose a hot-standby or warm-standby redundancy type, both are supported for the Virtual IP interface–based HA configuration.

The redundancy-type selection is made in the Configuration Layer or Genesys Administrator when you configure the primary SIP Server.

When you deploy a hot-standby configuration, there are additional steps for enabling data synchronization between the primary and backup SIP Servers. Configuration steps for both hot- and warm-standby redundancy types are included in the deployment procedures that are provided in SIP Server HA Deployment.

Hot-Standby Redundancy Type

Genesys uses the expression *hot standby* to describe the high-availability configuration 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 server guarantee a higher degree of availability. Data synchronization includes information about calls, device states, monitoring subscriptions, and agent states.

SIP Server supports Hot Standby mode for established calls, calls that are in the ringing state, and calls that are parked on a Routing Point. All telephony functions can be performed on synchronized calls after a switchover.

While the hot-standby redundancy type provides a higher degree of availability than the warm-standby redundancy type, hot standby has limitations that include the following:

- Client requests that are sent during the time in which a failure occurs until switchover completes might be lost.
- IP requests that are sent by SIP endpoints during the failure and switchover might be lost.
- SIP Server does not synchronize interactions that begin before it starts.
- Some T-Library events might be duplicated or lost.
- The Client request `Reference ID` might be lost for client requests that are received just before a failure occurs and processed after the switchover completes.

When you deploy an HA configuration of the hot-standby redundancy type, Genesys recommends that Advanced Disconnect Detection Protocol (ADDP) be configured on the connection between the primary and backup SIP Servers. The primary SIP Server uses this connection to deliver synchronization updates.

Warm-Standby Redundancy Type

Genesys uses the expression *warm standby* to describe the high-availability configuration in which a backup-server application remains initialized and ready to take over the operations of the primary server.

Unlike the hot-standby redundancy type, there is no propagation or synchronization of information from the primary SIP Server to the backup SIP Server about calls, devices, monitoring subscriptions, and agent states.

IP Address Takeover

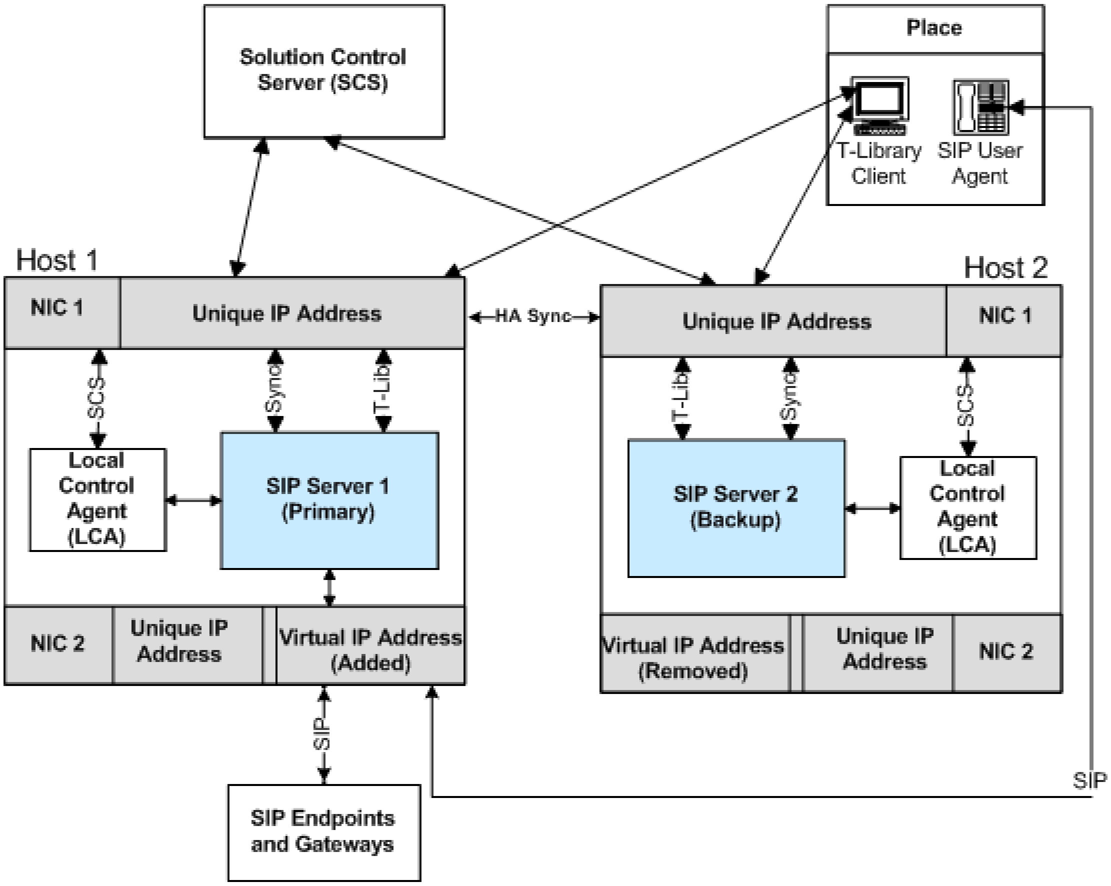
Windows and UNIX Platforms

High availability of the service for SIP communications requires that the IP address of SIP Server is always accessible by other SIP components, is operational on the SIP Server currently running in primary mode, and is transferred to the other server in case of failover or switchover.

There are two approaches for the IP Address Takeover HA configuration:

- Linux and Solaris platforms use the Virtual IP address as the IP address configured on a logical sub-interface on the network interface card (NIC).
    - Logical sub-interface with the Virtual IP address is enabled on the server that is running in primary mode.
    - Logical sub-interface with the Virtual IP address is disabled on the server that is running in backup mode.
- Windows and AIX platforms use the Virtual IP address as an additional (or alias) IP address configured on the NIC.
    - Virtual IP address is added to the NIC configuration on the server that is running in primary mode.
    - Virtual IP address is deleted from the NIC configuration on the server that is running in backup mode.

The **HA Configuration with One NIC** figure shows an IP Address Takeover configuration on the Linux or Solaris platform using one NIC.



HA Configuration with One NIC

There are two SIP Server hosts on the same subnet, each of them has two logical IP interfaces set up on the NIC connected to the subnet. Each host has a unique IP address that is configured on the main logical IP interface. The second IP interface (a sub-interface) is configured with the IP address that is shared by the hosts and called the Virtual IP address. The second IP interface is enabled only on one host at a time.

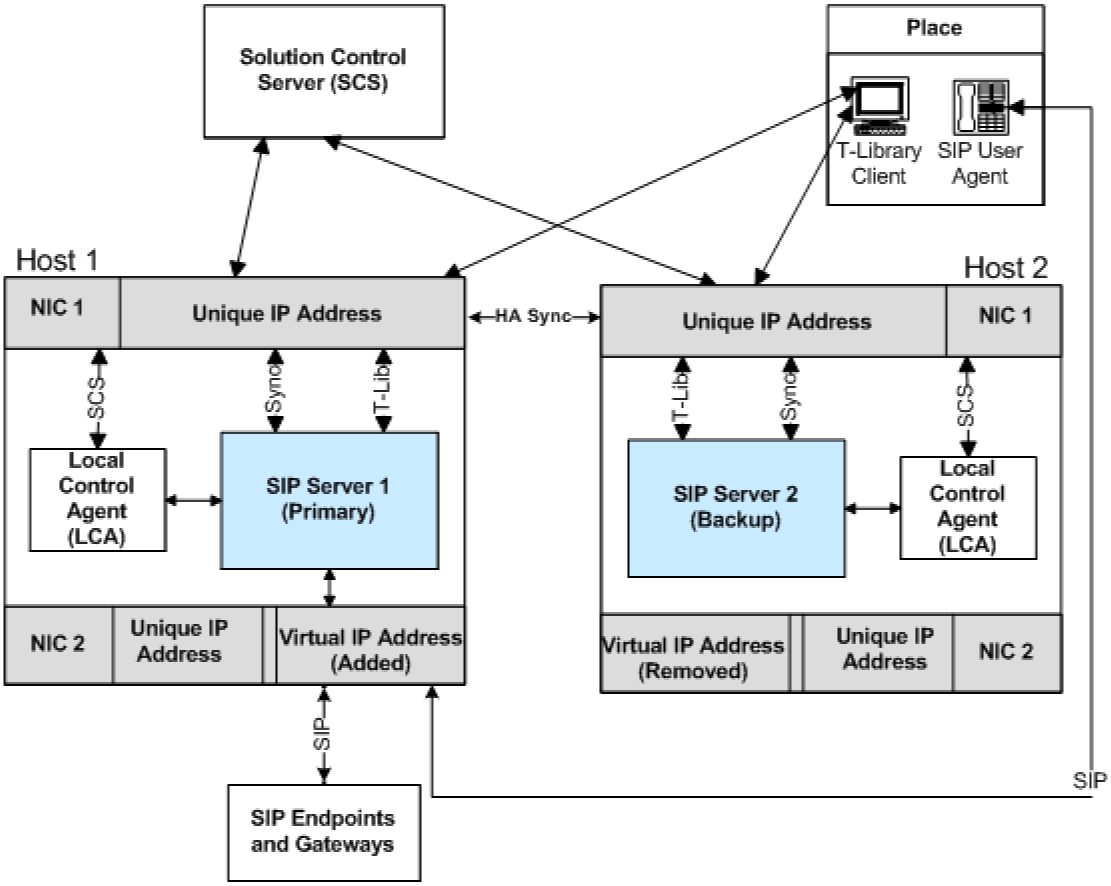
The IP interface with the unique IP address is always active. Management Layer and Configuration Layer components, and T-Library clients use the unique IP address for communication with the SIP Server and LCA.

SIP endpoints and gateways use the Virtual IP address to send SIP messages to SIP Server. The IP interface with the Virtual IP address is only enabled on the host on which SIP Server is running in primary mode. The IP interface with the Virtual IP address is disabled on the host on which SIP Server is running in backup mode.

In the IP Address Takeover configuration, the IP interface with the Virtual IP address is enabled and disabled by using the Virtual IP address control scripts.

The IP Address Takeover HA can be configured using either one network interface card (NIC), or multiple NICs.

The **HA Configuration with Two NICs** figure shows an IP Address Takeover configuration using two NICs on the Windows platform.



HA Configuration with Two NICs

In a deployment with two NICs, one NIC (NIC 2 in the above figure) is used for the SIP communication, while the second NIC (NIC 1 in the above figure) is used for other kinds of communication with various components"for example, Management Layer and Configuration Layer components, as well as any T-Library clients. Solution Control Server (SCS) manages and monitors the SIP Server application through NIC 1 (dedicated to other non-SIP communication).

Although, the unique IP address of NIC 2 is not used, the Virtual IP address is configured on NIC 2 or its sub-interface. Monitoring of the connectivity through NIC 2 can be done by means of the SIP traffic monitoring feature. (See SIP Traffic Monitoring.)

See the IP Address Takeover HA Workflows for step-by-step descriptions of manual switchover, primary SIP Server failure, and primary SIP Server disconnect workflows. For deployment procedures, see:

- Deploying HA on Windows
- Deploying HA on AIX
- Deploying HA on Solaris
- Deployng HA on Linux

IP Address Takeover HA Notes

- In an IP Address Takeover configuration, the Virtual IP address control scripts are used to add and delete the Virtual IP address to achieve a switchover. On Windows platform, the scripts use a Netsh command. Improper execution of this command may impact the SIP Server switchover time, as follows:
    - If the Netsh command fails to execute on either SIP Server host, the switchover will fail. For example, the `Netsh` command fails if any NIC properties are opened.
    - The `Netsh` command may take up to five seconds to execute. The execution time depends on the hardware and software characteristics of the host.With some network adapters the execution time can be significantly longer.
- Some hosts on the subnet may not be able to connect to the primary SIP Server after a switchover. Disabling the Virtual IP address at one host and enabling it at another changes the relationship between the MAC address and Virtual IP address. If an Address Resolution Protocol (ARP) announcement fails, the ARP table on some hosts on the subnet is not updated.

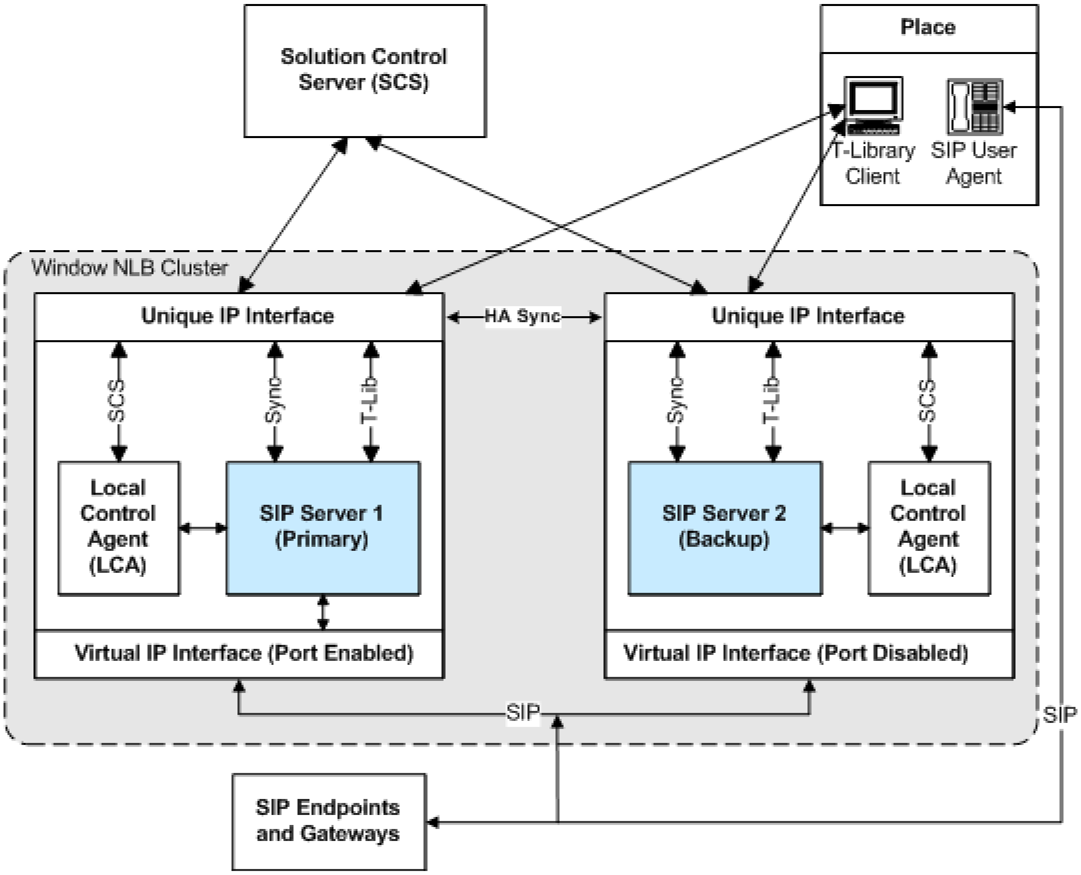
See the Prerequisites section for information about basic requirements and recommendations for deploying an IP Address Takeover HA configuration in a particular operating system.

Windows NLB Cluster

A SIP Server HA configuration using Windows Network Load Balancing (NLB) configuration is an alternative to a Windows IP Address Takeover configuration.

Microsoft's NLB cluster technology allows you to configure cluster hosts to receive requests at a single Virtual IP address. SIP endpoints and gateways are configured to send all requests to SIP Server by using this single Virtual IP address. The Windows NLB cluster technology delivers the requests to the SIP Server that is running in primary mode and reroutes traffic to the backup SIP Server when a failure is detected.

The **HA Windows NLB Cluster Configuration** figure shows a SIP Server HA configuration that uses Windows NLB. SIP endpoints and gateways are configured to communicate with SIP Server by using a single Virtual IP address, and the SIP Server port is enabled only at the SIP Server that is running in primary mode. When a switchover to the backup SIP Server occurs, the port at the backup SIP Server host is enabled, and traffic is directed to the active SIP Server.


Solution Control Server (SCS)
Place
T-Library Client
SIP User Agent
Window NLB Cluster
Unique IP Interface
HA Sync
Unique IP Interface
SCS
Sync
T-Lib
Sync
T-Lib
SCS
Local Control Agent (LCA)
SIP Server 1 (Primary)
SIP Server 2 (Backup)
Local Control Agent (LCA)
Virtual IP Interface (Port Enabled)
Virtual IP Interface (Port Disabled)
SIP
SIP
SIP Endpoints and Gateways

HA Windows NLB Cluster Configuration

The Management Layer uses a Windows NLB utility (`wlbs.exe` or `nlb.exe`) to enable and disable ports that are occupied by SIP Server. The NLB utility is initiated by Cluster control scripts that are triggered by SIP Server Alarm Conditions that are configured for SIP Server log events that occur when a SIP Server changes its mode from primary to backup or from backup to primary.

Windows NLB can be configured to distribute incoming requests by using either the Unicast or the Multicast method. When you deploy a SIP Server HA configuration, you must define the method that you want to use.

Unicast and Multicast methods are described in the following sections.

See Windows NLB Cluster HA Workflows for step-by-step descriptions of manual switchover, primary SIP Server failure, and primary SIP Server disconnect workflows. For deployment procedures, see Windows NLB Cluster HA Deployment.

Unicast Method

In the Unicast method, all NLB cluster hosts share an identical unicast MAC address. NLB overwrites the original MAC address of the cluster adapter by using the unicast MAC address that is assigned to all of the cluster hosts. Unicast NLB nodes cannot communicate over an NLB-enabled network adapter. Considerations for the Unicast distribution method include the following:

- If you are using Windows Server 2003, you might require a second network adapter to provide peer-to-peer communication between cluster hosts. This limitation applies only to Windows Server 2003.
  Note: You can avoid the requirement for a second network adapter on Windows 2003 by applying a Windows Server 2003 Service Pack and performing a registry update. For instructions, see the following Microsoft Support article: [1].

- In the Unicast method, all switch ports are flooded with NLB traffic, including ports to which non-NLB servers are attached. A workaround for this issue is to place cluster hosts on separate VLANs.

Multicast Method

In a Multicast configuration, each NLB cluster host retains the original MAC address of the network adapter. In addition to the original MAC address of the adapter, the adapter is assigned a multicast MAC address that is shared by all cluster hosts. Client requests are sent to all cluster hosts at the multicast MAC address. Considerations for implementation of the Multicast distribution method include the following:

- Upstream routers might require a static Address Resolution Protocol (ARP) entry. Without an ARP entry, routers might not accept an ARP response that resolves unicast IP addresses to multicast MAC addresses.
- Without Internet Group Management Protocol (IGMP), switches might require additional configuration to define which ports the switch should use for multicast traffic.
- Upstream routers might not support mapping of a unicast IP address (the cluster IP address) to a multicast MAC address. In this case, you might be required to update or replace your router in order to use the Multicast method.

Network Device-Based HA

An alternative to software-based Virtual IP interface configurations is a hardware-based Virtual IP configuration that uses an external network device.

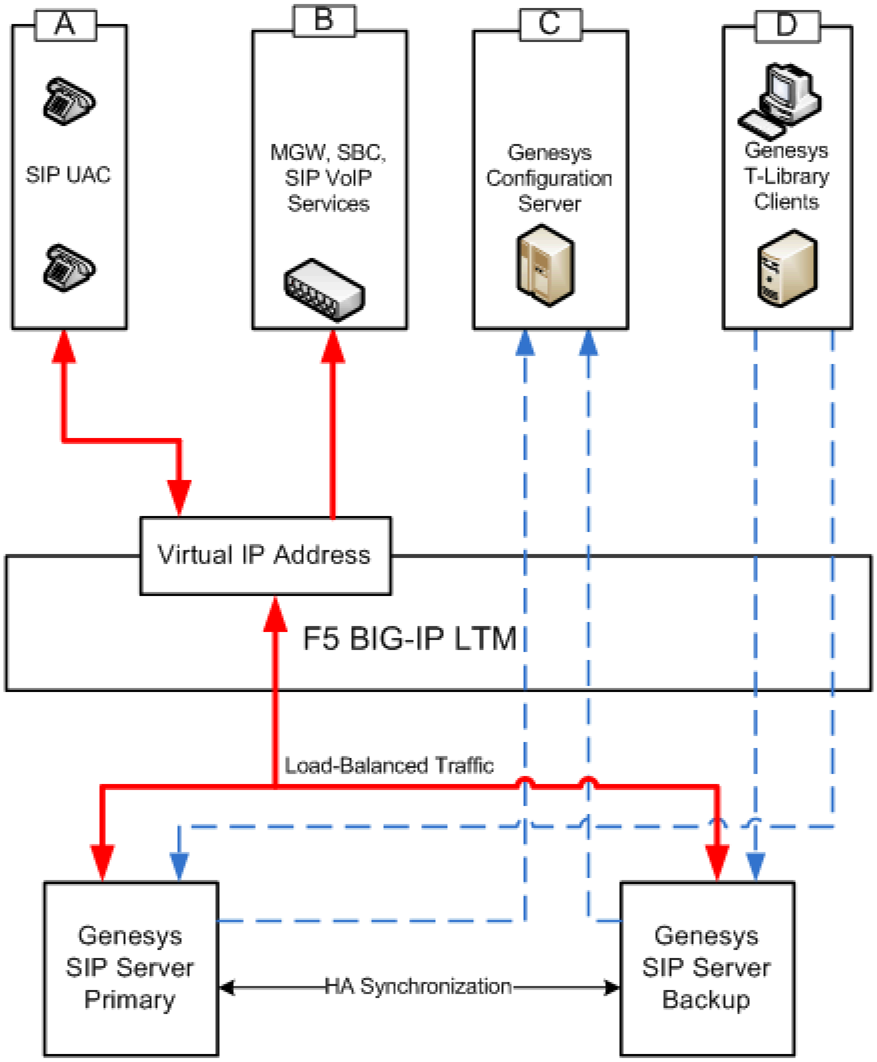
Benefits of using a network hardware device include the following:

- Less complex configuration: Alarm Reactions and Alarm Conditions are not required.
- There is no switch flooding, as there might be with a Windows NLB Unicast configuration.
- A single network device can support multiple SIP Server HA pairs.

Disadvantages might include the cost of a network device and the configuration that is required for Secure Network Address Translation (SNAT).

A network device works by presenting a shared Virtual IP address. SIP endpoints and gateways are configured to communicate with this single Virtual IP address. When the network device receives a request at the Virtual IP address, it routes the request to the SIP Server that is running in primary mode.

The SIP Server and the F5 Networks BIG-IP Local Traffic Manager (LTM) integration solution supports this type of HA configuration as shown in the **HA Configuration Using F5 Networks BIG-IP LTM** figure. F5's BIG-IP LTM monitors the primary SIP Server by sending an OPTIONS request to the SIP Server at configured intervals and listening for a response.


A
SIP UAC
B
MGW, SBC, SIP VoIP Services
C
Genesys Configuration Server
D
Genesys T-Library Clients
Virtual IP Address
F5 BIG-IP LTM
Load-Balanced Traffic
Genesys SIP Server Primary
HA Synchronization
Genesys SIP Server Backup

HA Configuration Using F5 Networks BIG-IP LTM

For more information about a SIP Server HA configuration that uses the F5 Networks BIG-IP LTM, refer to the Framework 8.1 SIP Server Integration Reference Manual. This guide describes configuration steps that are required to implement a hot-standby SIP Server HA configuration that runs behind an F5 Networks BIG-IP LTM.

Other SIP Server HA Enhancements

SIP Server supports several additional capabilities related to high-availability deployments.

- Single Host HA Deployment
- Synchronization of Contact Between SIP Server HA Pair
- SIP Traffic Monitoring
- Monitoring Critical Conditions

Single Host HA Deployment

Starting with version 8.0, SIP Server supports deploying both primary and backup SIP Server applications, as well as the Stream Manager or Media Server application, on the same physical host. Benefits of using the single host HA configuration include the following:

- Efficient use of the hardware equipment.
- Less complex configuration: Virtual IP address control scripts, Alarm Reactions, and Alarm Conditions are not required.

However, this type of HA configuration is supported only for small-size deployments--100 seats or less.

Synchronization of Contact Between SIP Server HA Pair

SIP Server 8.x synchronizes the SIP registration `Contact` header for a particular device across both primary and backup instances of SIP Server. The primary SIP Server sends the contact information to the backup SIP Server using the HA link, as well as through the Configuration Server.

SIP Traffic Monitoring

SIP Server 8.x supports SIP traffic monitoring for enhanced reliability. When configured, SIP Server monitors incoming SIP traffic and can initiate a switchover after a configurable length of time during which no SIP messages are received.

In deployments where two NICs are used, one NIC is dedicated to SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC.

The SIP traffic monitoring feature allows the primary SIP Server to monitor the network connectivity through the NIC that is responsible for SIP communication, to recognize connectivity issues that impact the SIP service, and to initiate reactions that result in recovery of the service.

An Application-level configuration option, sip-pass-check, must be configured to enable this functionality. In addition, at least one service device must be configured for Active Out-Of-Service Detection by using oos-check and oos-force configuration options. See the *Framework 8.1 SIP Server Deployment Guide* for information about the Active Out-Of-Service Detection feature description.

When it is set to true, the sip-pass-check option enables tracking of SIP messages that reach the primary SIP Server, including responses from SIP devices (DNs) that are monitored by SIP Server by using the oos-check and oos-force options.

The primary SIP Server summarizes results of the checks on DNs for out-of-service status and monitors the time that has passed since the last received SIP message. If the primary SIP Server does not receive SIP messages for a certain period of time, SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS. The period of time is chosen as the maximum of sums (among the sums of the oos-check and oos-force option values, configured for service DNs). When SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS, SCS switches the primary SIP Server to the backup mode and this SIP Server reports the SERVICE_RUNNING status to LCA/SCS. The former backup SIP Server becomes the primary server and starts to monitor SIP traffic.

If both the primary and backup servers receive no SIP traffic, a switchover would occur each time that the effective out-of-service timeout expires. To prevent frequent switchovers in this case, SIP Server detects the "double switchover" condition and doubles the effective out-of-service timeout each time that the double switchover happens"up to four times greater than the initially calculated timeout, or until one of the two servers detects SIP traffic. As soon as SIP traffic is detected, the server that detected the traffic remains the primary SIP Server and continues normal operation.

Monitoring Critical Conditions

You can use Genesys Administrator to check the current running status of SIP Server. Starting in release 8.1.0, SIP Server displays its state as Running in Genesys Administrator in cases where it is unable to open a listening port, and it is configured as one instance in a High Availability (HA) pair. Prior to release 8.1.0, (release 8.0.4 and earlier), in this same scenario SIP Server displayed its status as UNAVAILABLE.

To monitor problems with binding a listener (SIP Server is running but unable to open a listening port), Genesys recommends that, for each SIP Server instance, you configure an Alarm Condition for the log event 00-04200. For more information, consult the Solution Control Interface (SCI) help topic, "Using Log Events for Alarm Detection".

To ensure that administrators do not miss the alarm, Genesys recommends that you configure automatic clearing of the activated alarm in accordance with business processes and the schedule of the customer administrator.

The recommended configuration of an Alarm Condition for 00-04200 enables monitoring of a wide range of events that are critical for both SIP Server functionality and for service availability. This includes problems that might occur when binding a listener, unexpected terminations, or unauthorized terminations of the SIP Server process.

In Genesys Administrator, alarms that are detected and activated can be observed through a dedicated view, providing a central location for observing all alarms that occurred in the entire environment.

If required, an alarm reaction can be configured to notify administrators automatically when a critical condition occurs.

After the administrator investigates and resolves the problem, they must manually clear the alarm condition.

If the problem occurred due to a temporary outage (for example, a network switch reboot), SIP Server remains in the `Running` state, ensuring availability of the HA pair once the network switch is recovered; in release 8.0.4, SIP Serer required a manual restart to return to the Running state.

In release 8.0.4, if both SIP Server instances encountered a problem when binding a listener, both instances in the HA pair remained in `UNAVAILABLE` status, requiring a manual operation to resume the service. In release 8.1.0, SIP Server instead switches the primary role between the two HA instances and resumes the service as soon as one of the instances is able to open a listening port.

SIP Server HA Workflows

These topics describes workflows for SIP Server HA Architectures:

- IP Address Takeover HA Workflows
- Windows NLB Cluster HA Workflows

The workflows provide a step-by-step account of events that occur during a manual switchover, during a primary SIP Server failure, and during a primary SIP Server disconnection.

For configuration and deployment information about the log events, Alarm Conditions, Alarm Reaction scripts, and Application objects that are referred to in the SIP Server HA workflows, see SIP Server HA Deployment.

IP Address Takeover HA Workflows

The **HA Configuration with One NIC** figure shows an IP Address Takeover configuration prior to a switchover:

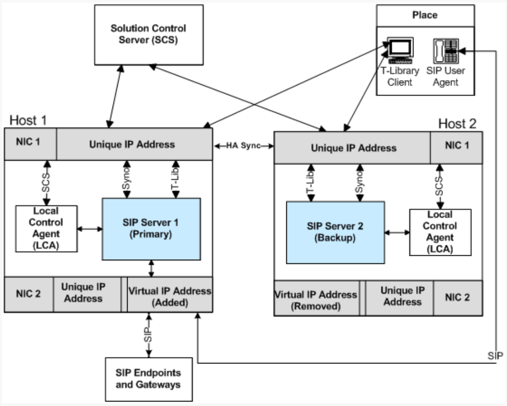
State Prior to Switchover

- SIP Server 1 is in primary mode.
- SIP Server 2 is in backup mode.
- The Virtual IP address at the primary SIP Server (SIP Server 1) is enabled.
- The Virtual IP address at the backup SIP Server (SIP Server 2) is disabled.

State After a Switchover

To see what happens in different scenarios, see the following:

- Manual-Switchover Workflow
- Primary Server-Failure Workflow
- Primary Server-Disconnected Workflow

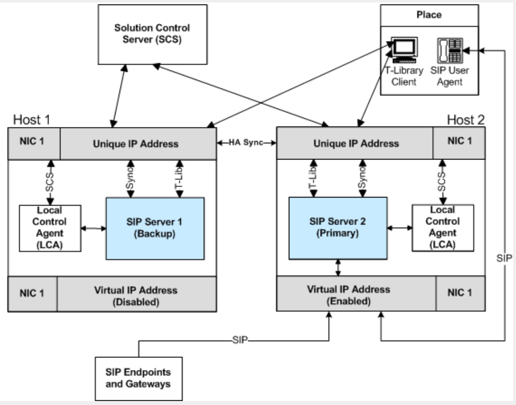


HA Configuration with One NIC

Manual-Switchover Workflow

The following steps describe a primary to backup-switchover workflow for a IP Address Takeover configuration (the **HA Configuration After a Switchover** figure represents the end state of the workflow):

1. The switchover is initiated manually from the Solution Control Interface (SCI).
2. Through LCA, the SCS instructs the primary SIP Server (SIP Server 1) to go into backup mode.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. The SCS generates a log message with Event ID 00-5150 to indicate that SIP Server 2 has changed to primary mode and a log messages with Event ID 00-5151 to indicate that SIP Server 1 has changed to backup mode.
5. The SCS activates the Alarm Conditions, which execute the associated Alarm Reaction scripts.
6. The Alarm Reaction scripts trigger the Virtual IP address control scripts that are configured as applications.
7. The SCS instructs LCA to launch the Virtual IP address control scripts on the SIP Server hosts.
8. The Virtual IP address control scripts disable the Virtual IP address on the SIP Server 1 host (Host 1) and enable the Virtual IP address on the SIP Server 2 host (Host 2).

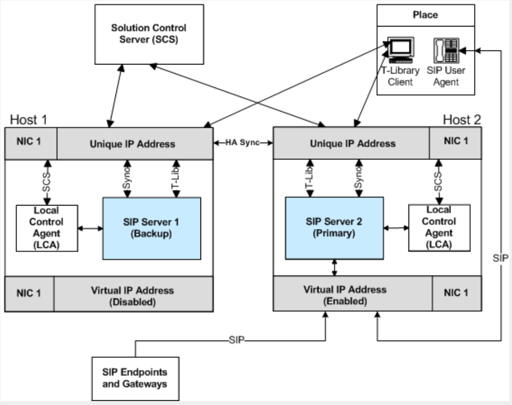


HA Configuration After a Switchover

Primary Server-Failure Workflow

The following steps describe a primary server-failure workflow for an IP Address Takeover configuration (the **HA Configuration After Primary Server Failure** figure represents the end state of the workflow):

1. The primary SIP Server (SIP Server 1) fails.
2. LCA detects the primary SIP Server failure and reports it to the SCS.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. The SCS generates a log message with Event ID 00-5150, to indicate that SIP Server 2 has changed to primary mode.
5. The SCS activates the Alarm Condition, which executes the associated Alarm Reaction scripts.
6. The Alarm Reaction scripts trigger the Virtual IP address control scripts that are configured as applications.
7. The SCS instructs LCA to launch the Virtual IP address control scripts on the SIP Server hosts.
8. The Virtual IP address control scripts disable the Virtual IP address on the SIP Server 1 host (Host 1) and enable the Virtual IP address on the SIP Server 2 host (Host 2).

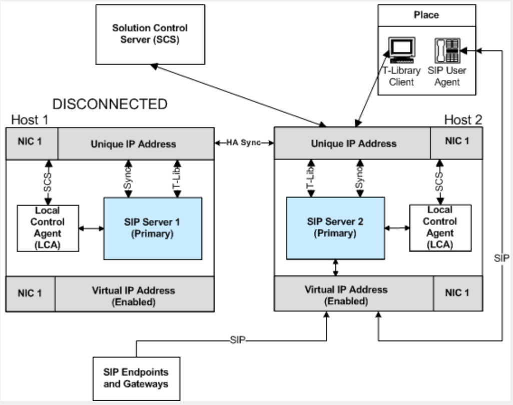


HA Configuration After Primary Server Failure

Primary Server-Disconnected Workflow

The following steps describe a primary server-disconnected workflow for an IP Address Takeover configuration (the **HA Configuration After a Primary Server is Disconnected** figure represents the end state of the workflow):

1. The SCS detects that the connection to the primary SIP Server host (Host 1) has been lost.
2. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
3. The SCS generates a log message with Event ID 00-5150, to indicate that SIP Server 2 has changed to primary mode.
4. The SCS activates the Alarm Condition, which executes the associated Alarm Reaction scripts.
5. The Alarm Reaction scripts trigger the Virtual IP address control scripts that are configured as applications.
6. The SCS instructs LCA to launch the Virtual IP address control scripts on the SIP Server hosts.



HA Configuration After a Primary Server is Disconnected

Because SIP Server 1 is disconnected, the script that disables the Virtual IP address on Host 1 cannot be run. When the connection to SIP Server 1 has been restored, the following workflow will occur (not represented in the **HA Configuration After a Primary Server is Disconnected** figure above):

1. The SCS detects that the connection to the SIP Server 1 host has been restored.
2. The SCS discovers that both SIP Servers are running in primary mode.
3. Through LCA, the SCS instructs SIP Server 1, whose connection was just restored, to go into backup mode.
4. The SCS generates a log message with Event ID 00-5151, to indicate that SIP Server 1 has changed to backup mode.
5. The SCS activates an Alarm Condition, which executes the associated Alarm Reaction script.
6. The Alarm Reaction script triggers a Virtual IP address control script that is configured as an application.
7. The SCS instructs LCA to launch the Virtual IP address control script on the SIP Server 1 host.
8. The Virtual IP address control script runs on the SIP Server 1 host and disables the Virtual IP address.

Windows NLB Cluster HA Workflows

The **HA Windows NLB Cluster Configuration** figure shows a Windows NLB Cluster configuration prior to a switchover.

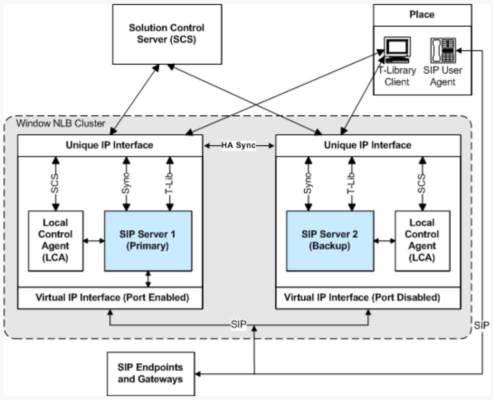
State Prior to Switchover

- SIP Server 1 is in primary mode.
- SIP Server 2 is in backup mode.
- The SIP port is enabled at the primary SIP Server (SIP Server 1).
- The SIP port is disabled at the backup SIP Server (SIP Server 2).

State After a Switchover

To see what happens in different scenarios, see the following:

- Manual-Switchover Workflow
- Primary Server-Failure Workflow
- Primary Server-Disconnected Workflow 1
- Primary Server-Disconnected Workflow 2

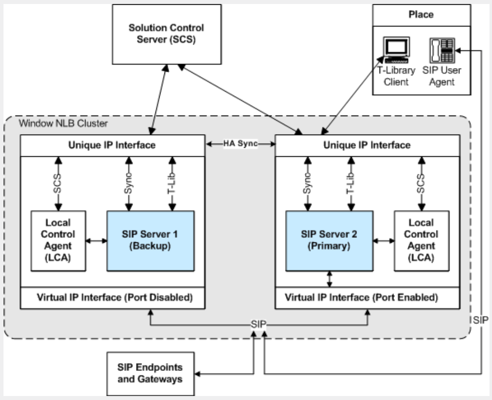

Solution Control Server (SCS)
Place
T-Library Client
SIP User Agent
Window NLB Cluster
Unique IP Interface
HA Sync
Unique IP Interface
SCS
Sync
T-Lib
Sync
T-Lib
SCS
Local Control Agent (LCA)
SIP Server 1 (Primary)
SIP Server 2 (Backup)
Local Control Agent (LCA)
Virtual IP Interface (Port Enabled)
Virtual IP Interface (Port Disabled)
SIP
SIP
SIP Endpoints and Gateways

HA Windows NLB Cluster Configuration

Manual-Switchover Workflow

The following steps describe a switchover workflow for a Windows NLB Cluster configuration (the **HA Windows NLB Cluster Configuration After a Switchover** figure represents the end state of the workflow):

1. The switchover is initiated manually from the Solution Control Interface (SCI).
2. Through Local Control Agent (LCA), the Solution Control Server (SCS) instructs the primary SIP Server (SIP Server 1) to go into backup mode.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. The SCS generates a log message with Event ID 00-5150 to indicate that SIP Server 2 has changed to primary mode and a log messages with Event ID 00-5151 to indicate that SIP Server 1 has changed to backup mode.
5. The SCS activates the Alarm Conditions, which execute the associated Alarm Reaction scripts.
6. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
7. The SCS instructs LCA to launch the Cluster control scripts on the SIP Server hosts.
8. The Cluster control scripts run NLB utilities that disable the Virtual IP port on SIP Server 1 and enable the Virtual IP port on SIP Server 2.

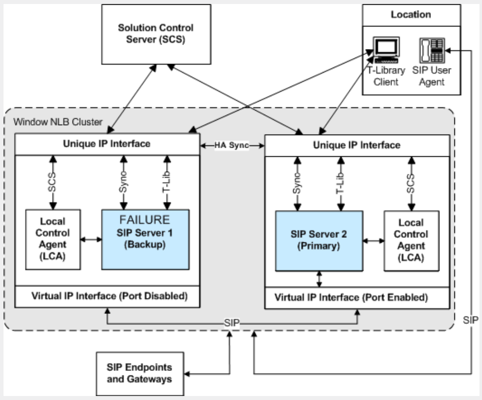

Solution Control Server (SCS)
Place
T-Library Client
SIP User Agent
Window NLB Cluster
Unique IP Interface
HA Sync
Unique IP Interface
SCS
Sync
T-Lib
Sync
T-Lib
SCS
Local Control Agent (LCA)
SIP Server 1 (Backup)
SIP Server 2 (Primary)
Local Control Agent (LCA)
Virtual IP Interface (Port Disabled)
Virtual IP Interface (Port Enabled)
SIP
SIP
SIP Endpoints and Gateways

HA Windows NLB Cluster Configuration After a Switchover

Primary Server-Failure Workflow

The following steps describe a primary server-failure workflow for a Windows NLB Cluster configuration (the **HA Windows NLB Cluster Configuration After Primary Server Failure** figure represents the end state of the workflow):

1. The primary SIP Server (SIP Server 1) fails.
2. LCA detects the primary SIP Server application failure and reports it to the SCS.
3. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. The SCS generates a log message with Event ID 00-5150, to indicate that SIP Server 2 has changed to primary mode.
5. The SCS activates the Alarm Condition, which executes the associated Alarm Reaction scripts.
6. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
7. The SCS instructs LCA to launch the Cluster control scripts on the SIP Server hosts.
8. The Cluster control scripts run Windows NLB utilities that disable the Virtual IP port on SIP Server 1 and enable the Virtual IP port on SIP Server 2.

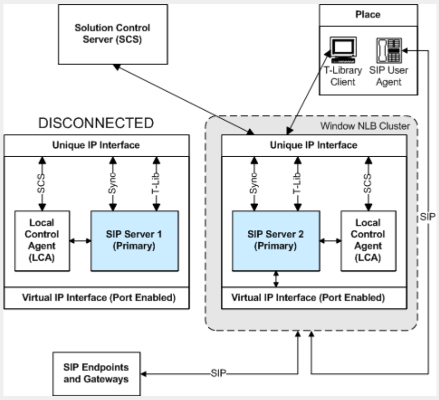


HA Windows NLB Cluster Configuration After Primary Server Failure

Primary Server-Disconnected Workflow 1

The following steps describe a primary server-disconnected workflow for a Windows NLB Cluster configuration (the **HA Windows NLB Cluster Configuration After a Primary Server is Disconnected** figure represents the end state of the workflow):

1. The SCS detects that the connection to the primary SIP Server host (SIP Server 1) has been lost.
2. Through LCA, the SCS instructs the backup SIP Server (SIP Server 2) to go into primary mode.
3. The SCS generates a log message with Event ID 00-5150, to indicate that SIP Server 2 has changed to primary mode.
4. The SCS activates the Alarm Condition, which executes the associated Alarm Reaction scripts.
5. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
6. The SCS instructs LCA to launch the Cluster control scripts on the SIP Server hosts.
7. Because SIP Server 1 is disconnected, the Cluster control script that is used to disable the Virtual IP port on SIP Server 1 cannot be executed, and the port remains enabled. The Cluster control script is able to run on SIP Server 2 and the Virtual IP port is enabled.



HA Windows NLB Cluster Configuration After a Primary Server is Disconnected

When the connection to SIP Server 1 has been restored, the following workflow occurs (not depicted in the **HA Windows NLB Cluster Configuration After a Primary Server is Disconnected** figure, above):

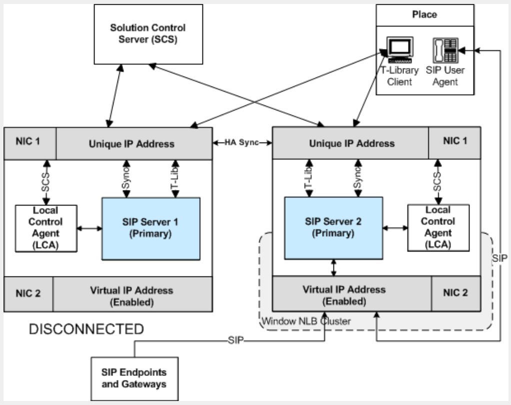
1. The SCS detects that the connection to SIP Server 1 host has been restored.
2. The SCS discovers that both SIP Servers are running in primary mode.
3. Through LCA, the SCS instructs SIP Server 1, whose connection was just restored, to go into backup mode.
4. The SCS generates a log message with Event ID 00-5151, to indicate that SIP Server 1 has changed to backup mode.
5. The SCS activates an Alarm Condition, which executes an associated Alarm Reaction script.
6. The Alarm Reaction script triggers the Cluster control script that is configured as application.
7. The SCS instructs LCA to launch the Cluster control script on SIP Server 1.

8. The Cluster control script runs on SIP Server 1, and the Virtual IP port is disabled.

Primary Server-Disconnected Workflow 2

The following steps describe a primary server-disconnected workflow for a Windows NLB Cluster configuration in the scenario where both SIP Servers use two NICs—one NIC is used for SIP communication (NIC 2), while the second NIC (NIC 1) is used for other kinds of communication with other components on the network. The SIP traffic monitoring feature is enabled (the **HA Windows NLB Cluster Configuration with Two NICs After a Primary Server is Disconnected** figure represents the end state of the workflow):

1. The Ethernet cord is unplugged from NIC 2 on the SIP Server 1 host.
2. The primary SIP Server (SIP Server 1) detects that it does not receive SIP messages for a certain period of time. SIP Server 1 reports the `SERVICE_UNAVAILABLE` status to LCA/SCS.
3. Through LCA, the SCS instructs the primary SIP Server (SIP Server 1) to go into backup mode and it instructs the backup SIP Server (SIP Server 2) to go into primary mode.
4. The SCS generates a log message with Event ID 00-5150 to indicate that SIP Server 2 has changed to primary mode and a log messages with Event ID 00-5151 to indicate that SIP Server 1 has changed to backup mode.
5. The SCS activates the Alarm Conditions, which execute the associated Alarm Reaction scripts.
6. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
7. The SCS instructs LCA to launch the Cluster control scripts on the SIP Server hosts.



HA Windows NLB Cluster Configuration with Two NICs After a Primary Server is Disconnected

8. Because NIC 2 on SIP Server 1 is disconnected, the NLB does not react to reconfiguration commands from the Cluster control script that is used to disable the Virtual IP port on SIP Server 1, and so the port remains enabled. The Cluster control script is successfully executed on SIP Server 2 and the Virtual IP port is enabled.	

When the connection to SIP Server 1 has been restored, the following workflow occurs (not depicted in the **HA Windows NLB Cluster Configuration with Two NICs After a Primary Server is Disconnected** figure):

1. Because the NLB port on SIP Server 1 remained enabled, after network connectivity is restored at NIC 2 on the SIP Server 1 host, the NLB cluster on both hosts is now incorrectly configured"SIP messages are delivered to the NLB cluster node where SIP Server is running in backup mode (SIP Server 1).
2. The primary SIP Server (SIP Server 2) detects that it had not received any SIP messages for a certain period of time. SIP Server 2 reports the `SERVICE_UNAVAILABLE` status to LCA/SCS.
3. Through LCA, the SCS instructs the primary SIP Server (SIP Server 2) to go into backup mode and instructs the backup SIP Server (SIP Server 1) to go into primary mode.
4. The SCS generates a log message with Event ID 00-5150 to indicate that SIP Server 2 has changed to primary mode and a log messages with Event ID 00-5151 to indicate that SIP Server 1 has changed to backup mode.
5. The SCS activates the Alarm Conditions, which execute associated Alarm Reaction scripts.
6. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
7. The SCS instructs LCA to launch the Cluster control scripts on SIP Server hosts.
8. The Cluster control scripts run NLB utilities that disable the Virtual IP port on SIP Server 2 and enable the Virtual IP port on SIP Server 1.

SIP Server HA Deployment

These topics describe how to deploy the SIP Server high-availability (HA) configurations that are described in SIP Server High-Availability Architecture:

- IP Address Takeover HA Deployment on Windows
- IP Address Takeover HA Deployment on AIX
- IP Address Takeover HA Deployment on Solaris
- IP Address Takeover HA Deployment on Linux
- Windows NLB Cluster HA Deployment
- SIP Server HA Configuration Testing

IP Address Takeover

This section describe how to deploy IP Address Takeover configurations on the following operating systems:

- IP Address Takeover HA Deployment on Windows
- IP Address Takeover HA Deployment on AIX
- IP Address Takeover HA Deployment on Solaris
- IP Address Takeover HA Deployment on Linux

Deploying HA on Windows Server 2008 R2

Complete these steps to set up SIP Server HA on Windows Server 2008 R2, using the IP Address Takeover method.

IP Address Takeover HA Deployment on Windows

1. Check prerequisites.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.
  Note: Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.
- Software requirements:
  - For the Windows OS to send a gratuitous ARP packet when a new IP address is assigned on the computer, you must install the Microsoft Hotfix 2811463 for Windows 2008 R2. See http://support.microsoft.com/kb/2811463/en-us.
  - SIP Server must be installed and configured on both host computers.
  - LCA must be installed and configured on both host computers.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).
- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet. A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with SIP Server might fail to update the ARP table during Virtual IP Address Takeover.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The

second NIC on both hosts should be connected to a separate network.

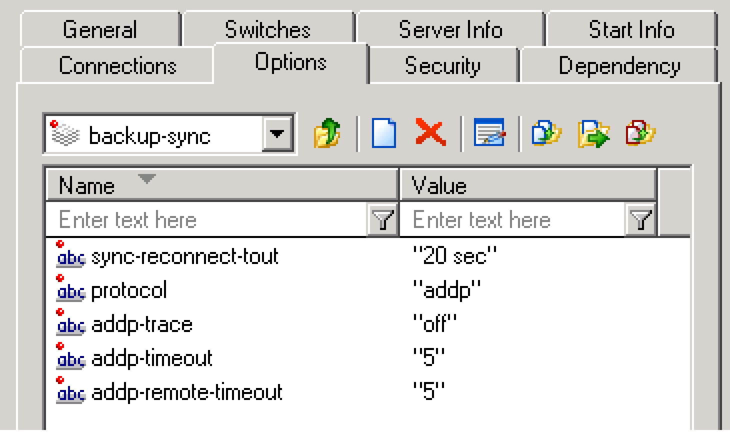
2. Configure the primary SIP Server.

Configuring the primary SIP Server

Purpose
To configure the primary SIP Server Application object for high availability.

Start

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
    a. Select the `TServer` section.
        i. Set the `sip-port` option to the port number that will be used by both the primary and backup SIP Server applications.
        ii. Set the `sip-address` option to the Virtual IP address. (For Windows NLB cluster configurations, set the value to the Windows NLB cluster IP address).
        iii. Click `Apply` to save the configuration changes.
    b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP:
        i. Select the `backup-sync` section, and configure the following options:
            - `sync-reconnect-tout`
            - `protocol`
            - `addp-timeout`
            - `addp-remote-timeout`



Name	Value
Enter text here	Enter text here
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the addp-timeout and addp-remote-timeout options to at least two times the established network-latency time, and to set the sync-reconnect-tout option to at least two times the timeout value plus the established network latency.
Note: For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

5. Click Apply to save the configuration changes.

- Click the Switches tab.

  a. Ensure that the correct Switch object is specified. If necessary, select the correct Switch object by using the Add button.

  b. Click Apply to save the configuration changes.

- Click the Server Info tab.

  a. Select the Redundancy Type. You can select either Hot Standby or Warm Standby.

  b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.

     i. In the Ports section, select the port to which the backup SIP Server will connect for HA data synchronization, and click Edit Port.

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

     iii. Click OK.

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

- For the Backup Server option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.

- Click Apply to save the configuration changes.

- Click the Start Info tab.

  a. Select Auto-Restart.

  b. Click Apply to save the configuration changes.

- Click Apply and then OK to save the configuration changes.

End

3. Configure the backup SIP Server.

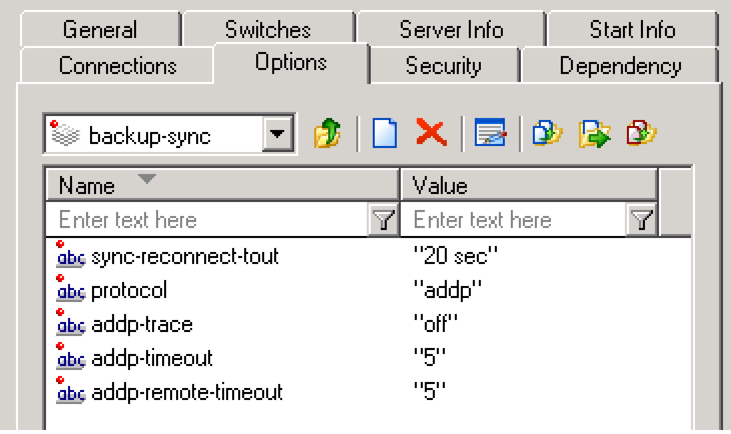
Configuring the backup SIP Server

Purpose

To configure the backup SIP Server Application object for high availability.

Start

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. `Select Properties`.
4. Click the `Switches` tab.
    a. Click `Add`, and select the `Switch` object that you associated with the primary SIP Server Application object.
    b. Click `Apply` to save the configuration changes.
5. Click the `Start Info` tab.
    a. Select `Auto-Restart.`
    b. Click `Apply` to save the configuration changes.
6. Click the `Options` tab.
    a. Select the `TServer` section.
        i. Set the `sip-port` option to the same port number that you specified for the primary SIP Server.
        ii. Set the `sip-address` option to the Virtual IP address. (For Windows NLB cluster configurations, set the value to the Windows NLB cluster IP address)
    b. Click `Apply` to save the configuration changes.
7. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP:
    i. Select the `backup-sync` section, and configure the following options:
        - `sync-reconnect-tout`
        - `protocol`
        - `addp-timeout`
        - `addp-remote-timeout`



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.

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

- Click `Apply` and then `OK` to save the configuration changes.

End

4. Create Virtual IP address control scripts.

Creating Virtual IP address control scripts for Windows 2008 R2 and later

Purpose

To create scripts for the primary and backup SIP Servers that the Management Layer runs to route traffic to the SIP Server that is running in primary mode.

- `HA_IP_ON.bat`—To enable the Virtual IP address
- `HA_IP_OFF.bat`—To disable the Virtual IP address

Start

1. On the primary SIP Server host computer, create a batch file that is named `HA_IP_ON.bat`, and enter the following commands into the file:
   [+] Commands for '''HA_IP_ON.bat'''

```
@set VirtualIP=10.10.11.103
@set vipMask=255.255.255.0
@set VirtualInterface="Local Area Connection"
@echo ********************* HA_IP_ON ********************** >> Takeover.log
@echo %time% >> Takeover.log
@rem check if Virtual IP released on Backup host
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@if not errorlevel 1 goto ready
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@if not errorlevel 1 goto ready
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
:ready
@rem Add VirtualIP
@netsh interface ip delete arpcache
netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
store=active >> Takeover.log
@rem check if VirtualIP added succesefully if not do it again
@cscript.exe check_ip.vbs localhost %VirtualIP% //Nologo >> Takeover.log
@if errorlevel 1 goto done
netsh interface ip delete address name=%VirtualInterface% addr=%VirtualIP% >>
Takeover.log
netsh interface ip add address name=%VirtualInterface% addr=%VirtualIP% mask=%vipMask%
store=active >> Takeover.log
@if errorlevel 1 (
@echo %VirtualIP% not added to %VirtualInterface% >> Takeover.log
@goto done
)
:done
@echo %time% >> Takeover.log
```

Note: The `store=active` parameter of `netsh interface ip add address` is only available when you deploy the IP Address Takeover method on Windows Server 2008 R2.

2. In the first line of the `HA_IP_ON.bat` script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.
3. In the second line of the `HA_IP_ON.bat` script, replace the `vipMask` value of `255.255.255.0` with your Virtual IP mask.
4. In the third line of the `HA_IP_ON.bat` script, ensure that the `VirtualInterface` value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
5. On the primary SIP Server host computer, create a batch file that is named `HA_IP_OFF.bat`, and enter the following commands into the file:
   [+] Commands for '''HA_IP_OFF.bat'''

```
@set VirtualIP=10.10.11.103
@set VirtualInterface="Local Area Connection"
@echo ********************* HA_IP_OFF ********************** >>
Takeover.log
@echo %time% >> Takeover.log
netsh interface ip delete address name=%VirtualInterface%
addr=%VirtualIP% >> Takeover.log
@netsh interface ip delete arpcache
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@echo %time% >> Takeover.log
```

6. In the first line of the `HA_IP_OFF.bat` script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.
7. In the second line of the `HA_IP_OFF.bat` script, ensure that the `VirtualInterface` value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
8. Follow the steps in this procedure to create the same two scripts on the backup SIP Server host.

9. On the primary SIP Server host computer, create an accessory script that is named Ping.vbs, and enter the following commands into the script:
   [+] Commands for Ping.vbs

```
rem ping host and return 1 if ping successful 0 if not
On Error Resume Next
if WScript.Arguments.Count > 0 then
strTarget = WScript.Arguments(0)
Set objShell = CreateObject("WScript.Shell")
Set objExec = objShell.Exec("ping -n 2 -w 1000 " & strTarget)
strPingResults = LCase(objExec.StdOut.ReadAll)
If InStr(strPingResults, "reply from") And Not InStr(strPingResults, "unreachable") Then
WScript.Echo strTarget & " responded to ping."
wscript.Quit 1
Else
WScript.Echo strTarget & " did not respond to ping."
wscript.Quit 0
End If
Else
WScript.Echo "target is not specified."
wscript.Quit -1
End If
```

10. On the primary SIP Server host computer, create an accessory script that is named Check_ip.vbs, and enter the following commands into the script:
    [+] Commands for Check_ip.vbs

```
rem check if IP address (arg0 ) can be found on host (arg1 )
On Error Resume Next
if WScript.Arguments.Count > 0 then
strComputer = WScript.Arguments(0)
targetIPAddress = WScript.Arguments(1)
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate}!\\" & strComputer &
"\root\cimv2")
Set colNicConfigs = objWMIService.ExecQuery _
("SELECT * FROM Win32_NetworkAdapterConfiguration WHERE
IPEnabled = True")
WScript.Echo "Computer Name: " & strComputer & " ip " &
targetIPAddress
For Each objNicConfig In colNicConfigs
For Each strIPAddress In objNicConfig.IPAddress
If InStr(strIPAddress, targetIPAddress) Then
WScript.Echo targetIPAddress & " is found on " &
objNicConfig.Description
wscript.Quit 1
End If
Next
Next
WScript.Echo targetIPAddress & " not found."
wscript.Quit 0
Else
WScript.Echo "target not specified."
wscript.Quit -1
End If
```

11. Place accessory scripts Ping.vbs and Check_ip.vbs in the same directory as the HA_IP_ON.bat and HA_IP_OFF.bat files on both the primary and backup SIP Server hosts.

End

5. Configure primary and backup hosts.

Configuring primary and backup hosts

Purpose

To prepare the primary and backup hosts for a Virtual IP Address Takeover.

Start

- Install the Microsoft Hotfix 2582281 (http://support.microsoft.com/kb/2582281).

End

6. Test Virtual IP address control scripts.

Testing Virtual IP address control scripts

Purpose

To verify that the Virtual IP address control scripts that you created in Step 4 work as expected.

Start

1. Run the `HA_IP_OFF.bat` script on the backup SIP Server host.
2. Run the `HA_IP_ON.bat` script on the primary SIP Server host.
3. Verify that the Virtual IP interface is running on the primary host by using the `ipconfig` command—for example:
   [+] Example ipconfig command

```
C:\GCTI\SWITCHOVER\1NIC>ipconfig
 Windows IP Configuration

 Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  . :
    IP Address. . . . . . . . . . . . : 10.10.11.103
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    IP Address. . . . . . . . . . . . : 10.10.11.101
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 10.10.11.104
```

4. Verify that the Virtual IP interface is not running on the backup SIP Server host—for example:
   [+] Example ipconfig command

```
C:\GCTI\SWITCHOVER\1NIC>ipconfig
 Windows IP Configuration

 Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  . :
    IP Address. . . . . . . . . . . . : 10.10.11.102
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 10.10.11.104
```

5. Run the `HA_IP_OFF.bat` script on the primary SIP Server host.
6. Run the `HA_IP_ON.bat` script on the backup SIP Server host.
7. Verify that the Virtual IP interface is running on the backup SIP Server host by using the `ipconfig` command. Output should appear similar to the following:
   [+] Example ipconfig command

```
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.11.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IP Address. . . . . . . . . . . . : 10.10.11.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.11.104
```

8. Verify that the Virtual IP interface is not running on the primary SIP Server host by using the `ipconfig` command. Output should appear similar to the following:
   [+] Example ipconfig command

```
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.10.11.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.11.104
```

End

7. Create Application objects for Virtual IP address control scripts.

Creating Application objects for Virtual IP address control scripts

Purpose

To create four Application objects of type `Third Party Server`: one for each of the scripts that you created in Step 4. For example:

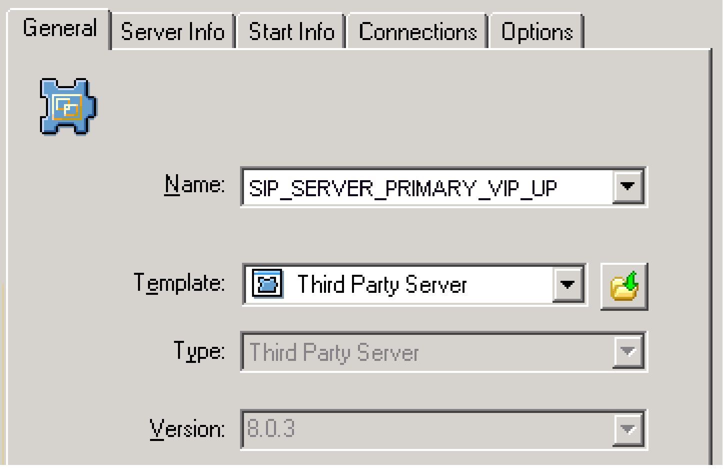
- `SIP_SERVER_PRIMARY_VIP_UP`—For a script that enables the Virtual IP address (to be run on the primary SIP Server host)

- SIP_SERVER_PRIMARY_VIP_DOWN—For a script that disables the Virtual IP address (to be run on the primary SIP Server host)
- SIP_SERVER_BACKUP_VIP_UP—For a script that enables the Virtual IP address (to be run on the backup SIP Server host)
- SIP_SERVER_BACKUP_VIP_DOWN—For a script that disables the Virtual IP address (to be run on the backup SIP Server host)

Creating Application objects for the Virtual IP address control scripts allows the scripts to be run as applications within the Genesys Framework.

Start

1. In the Configuration Manager, select Environment > Applications.
2. Right-click and select New > Application.
3. Select the Third Party Server template from the Application Templates folder, and click OK.
4. On the General tab, enter a name for the Application object—for example, SIP_SERVER_PRIMARY_VIP_UP.

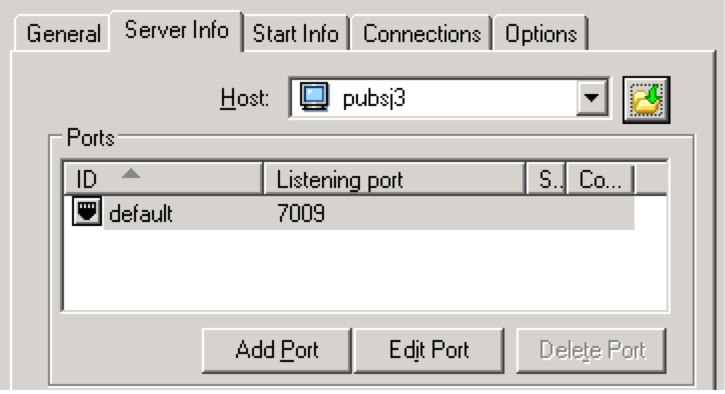


Name: SIP_SERVER_PRIMARY_VIP_UP
Template: Third Party Server
Type: Third Party Server
Version: 8.0.3

Configuring the Application Object for the Script, General Tab: Sample Configuration

Note: You can use the suggested Application object names, or you can specify your own.

5. Select the Server Info tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is located.
   b. If necessary, specify a valid communication-port number by using the Edit Port option.



Host: pubsj3

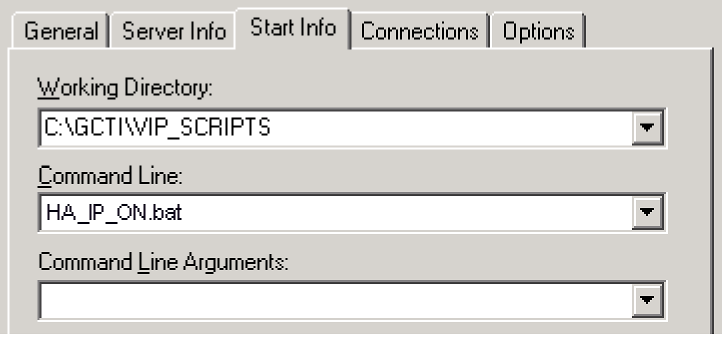
Ports

ID	Listening port	S...	Co...
default	7009		

Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.

   a. Set the `Working Directory` to the location of the Virtual IP address control script, and enter the name of the script in the `Command Line` field. For example, for the `SIP_SERVER_PRIMARY_VIP_UP` Application object, enter the script name that enables the Virtual IP address (`HA_IP_ON.bat`). For the `SIP_SERVER_PRIMARY_VIP_DOWN` Application object, enter the script name that disables the Virtual IP address (`HA_IP_OFF.bat`).



Working Directory: C:\GCTI\VIP_SCRIPTS

Command Line: HA_IP_ON.bat

Command Line Arguments:

Configuring the Application Object for the Script, Start Info Tab: Sample Configuration

   b. If you are configuring an Application object that disables the Virtual IP address (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the `Timeout Startup` value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four Virtual IP address control scripts.

End

8. Create Alarm Reaction scripts

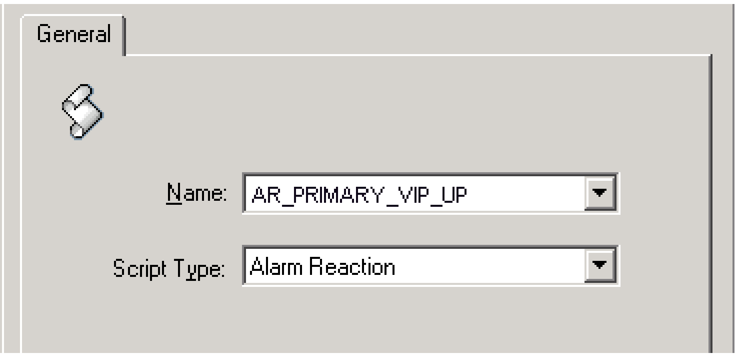
Creating Alarm Reaction scripts

Purpose

To create Alarm Reaction scripts for HA-related Alarm Conditions. When an HA-related Alarm Condition occurs, the associated Alarm Reaction script is run. Alarm Reaction scripts are configured to call the Application objects that you created in Step 6.

Start

1. Open the Configuration Manager.
2. Select `Resources > Scripts`.
3. Right-click and select `New > Script`.
4. Create four scripts: one for each of the Application objects that you created previously. For example:
    - `AR_SCRIPT_PRIMARY_VIP_UP`—To trigger a script that enables the Virtual IP address (to be run on the primary SIP Server host)
    - `AR_SCRIPT_PRIMARY_VIP_DOWN`—To trigger a script that disables the Virtual IP address (to be run on the primary SIP Server host)
    - `AR_SCRIPT_BACKUP_VIP_UP`—To trigger a script that enables the Virtual IP address (to be run on the backup SIP Server host)
    - `AR_SCRIPT_BACKUP_VIP_DOWN`—To trigger a script that disables the Virtual IP address (to be run on the backup SIP Server host)

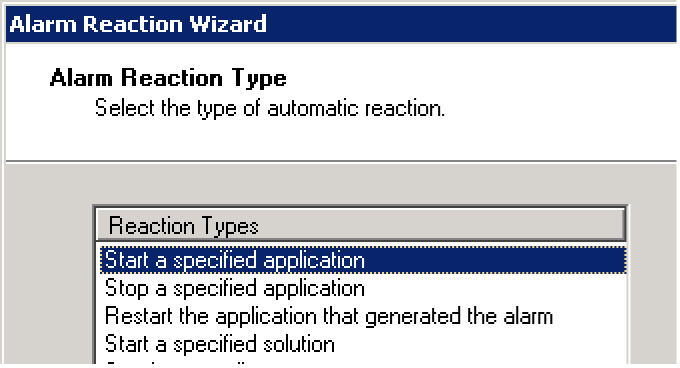


Name: AR_PRIMARY_VIP_UP

Script Type: Alarm Reaction

Configuring the Alarm Reaction Script: Sample Configuration

5. For each of the Alarm Reaction scripts, select `Alarm Reaction` as the `Script Type`.
6. For each of the Alarm Reaction scripts, use the Alarm Reaction Wizard to configure the `Alarm Reaction` Type.
    a. Select an Alarm Reaction script, and right-click to open the Alarm Reaction Wizard (select `Wizard > Configure`).
    b. In the Alarm Reaction Wizard, click `Next`.
    c. In the `Alarm Reaction Type` dialog box, select `Start a specified application`, and click `Next`.



Alarm Reaction Wizard

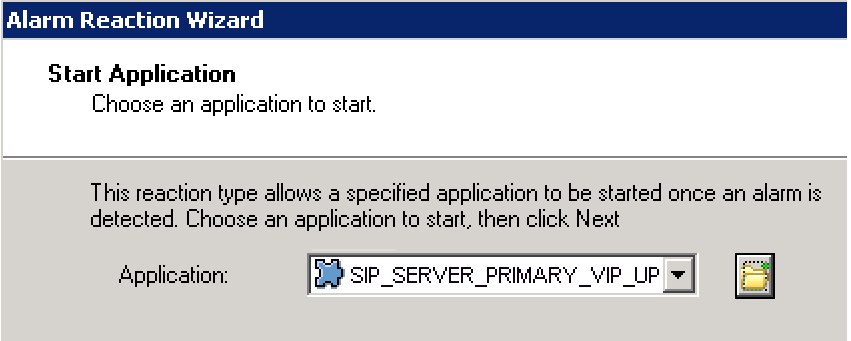
Alarm Reaction Type

Select the type of automatic reaction.

Reaction Types
Start a specified application
Stop a specified application
Restart the application that generated the alarm
Start a specified solution

Alarm Reaction: Selecting the Alarm Reaction Type

d. Browse to select the corresponding Application object. For example, for the `AR_SCRIPT_PRIMARY_VIP_UP` Alarm Reaction script, select the `SIP_SERVER_PRIMARY_VIP_UP` Application object of type `Third Party Server`.



Alarm Reaction Wizard

Start Application

Choose an application to start.

This reaction type allows a specified application to be started once an alarm is detected. Choose an application to start, then click Next

Application: SIP_SERVER_PRIMARY_VIP_UP

Alarm Reaction: Selecting the Application to Start

e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in Step 4.

End

9. Create Alarm Conditions.

Creating Alarm Conditions

Purpose

Alarm Conditions are required to handle log events that occur when a SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you will configure them to trigger the Alarm Reaction scripts that you created in Step 7.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. The following table outlines the Alarm Conditions for both hot-standby and warm-standby configurations.

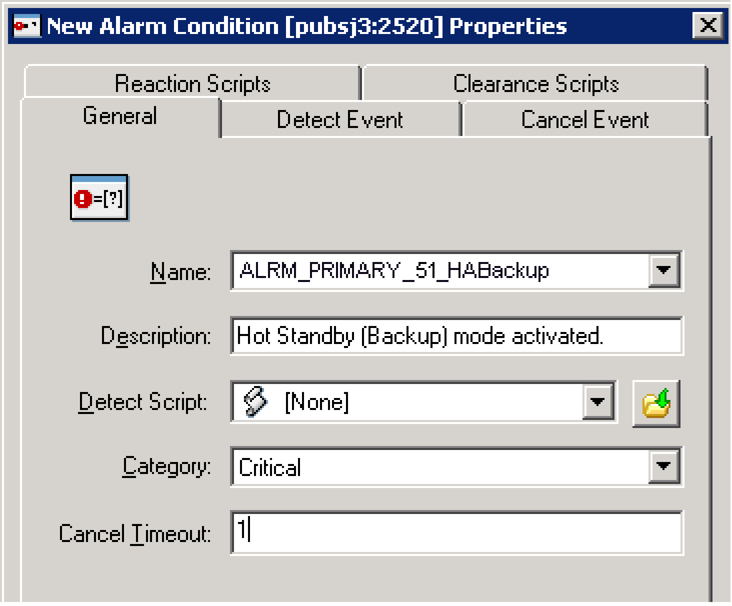
Alarm Conditions: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
00-05151	SIP_SERVER_PRIMARY	ALRM_PRIMARY_51_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
00-05150	SIP_SERVER_PRIMARY	ALRM_PRIMARY_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN AR_SCRIPT_PRIMARY_VIP_UP
00-05151	SIP_SERVER_BACKUP	ALRM_BACKUP_51_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
00-05150	SIP_SERVER_BACKUP	ALRM_BACKUP_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP AR_SCRIPT_PRIMARY_VIP_DOWN

For information about the log events for which you are creating Alarm Conditions, refer to Log events generated by SCS.

Start

1. Open the Configuration Manager.
2. Navigate to the `Environment > Alarm Conditions folder`.
3. Right-click and select `New > Alarm Condition` to open the `New Alarm Condition Properties` dialog box.
4. On the `General` tab:
   - Enter the `Name` for the Alarm Condition—for example, `ALRM_PRIMARY_51_HABackup`.
   - Optionally, enter a description.
   - For the `Category` value, select `Critical`.
   - Set `Cancel Timeout` to `1`.



Name: ALRM_PRIMARY_51_HABackup

Description: Hot Standby (Backup) mode activated.

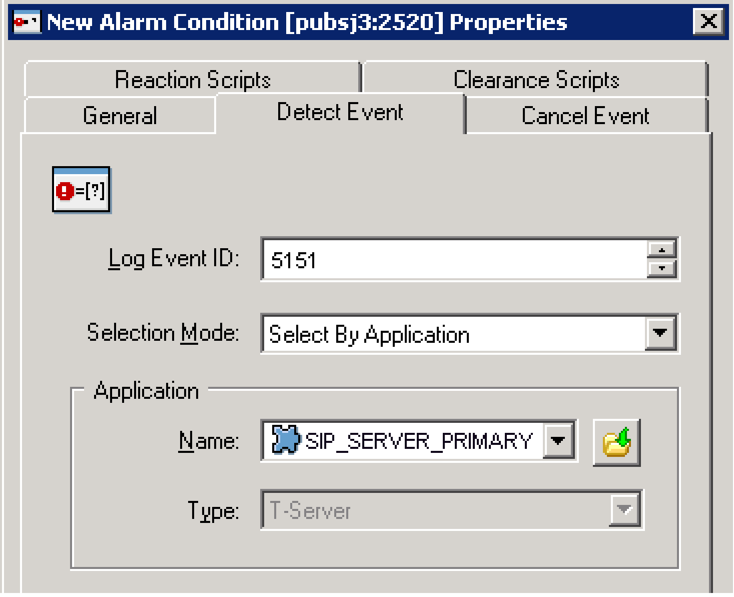
Detect Script: [None]

Category: Critical

Cancel Timeout: 1

Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the Detect Event tab:
   - Set the Log Event ID as defined in the table above.
   - Set the Selection Mode to Select By Application.
   - For the Application Name field, click the folder icon to browse for the SIP Server Application object. If you are creating an Alarm Condition for the primary SIP Server, select the primary SIP Server Application object. If you are creating an Alarm Condition for the backup SIP Server, select the backup SIP Server Application object.



Log Event ID: 5151

Selection Mode: Select By Application

Name: SIP_SERVER_PRIMARY

Type: T-Server

Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.

7. On the Reaction Scripts tab, add the Alarm Reaction script as defined in the previous table.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your configuration.

End

10. Test Alarm Conditions.

Testing Alarm Conditions

Purpose

To verify that the Alarm Conditions work as expected.

Start

1. Use Telnet to access the SIP Server Virtual IP interface.
2. Open the Solution Control Interface (SCI).
3. Under Alarm Conditions, select the Alarm Condition that you created in the previous procedure—for example, ALRM_PRIMARY_51_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_51_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP address at the primary SIP Server and disable the Virtual IP address at the backup SIP Server.
4. Use the ipconfig command to verify that the Virtual IP interface is active on the backup SIP Server and that the Virtual IP interface is inactive on the primary SIP Server.

End

11. Verify the HA configuration.

Testing your SIP Server HA configuration

Purpose

To validate your HA configuration, you can perform the following tests.

Prerequisites

- Ensure that the Management Layer is up and running.
- Start the primary SIP Server, and ensure that it is in primary mode.
- Start the backup SIP Server, and ensure that it is in backup mode.

Start

1. Test 1: Manual switchover
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 2: Manual switchback
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 3: Stop primary SIP Server
    a. Establish a call between two SIP endpoints.
    b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

End

Deploying HA on AIX

Complete these steps to set up SIP Server HA on AIX, using the IP Address Takeover method.

IP Address Takeover HA Deployment on AIX

1. Check prerequisites.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.
  Note: Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.
- Software requirements:
  - For the Windows OS to send a gratuitous ARP packet when a new IP address is assigned on the computer, you must install the Microsoft Hotfix 2811463 for Windows 2008 R2. See http://support.microsoft.com/kb/2811463/en-us.
  - SIP Server must be installed and configured on both host computers.
  - LCA must be installed and configured on both host computers.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).
- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet. A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with SIP Server might fail to update the ARP table during Virtual IP Address Takeover.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

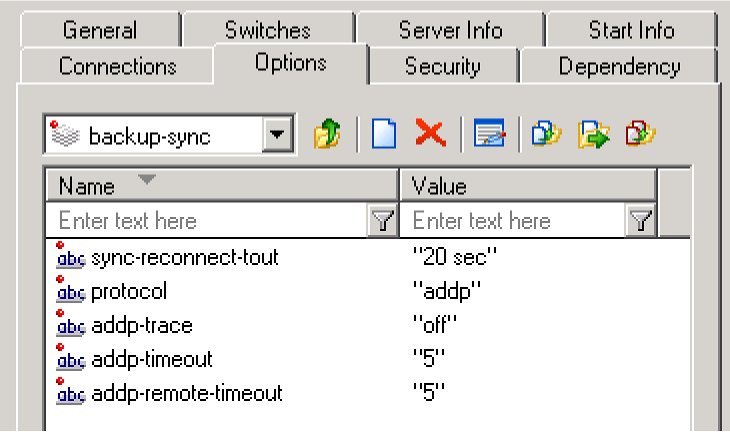
2. Configure the primary SIP Server.

Configuring the primary SIP Server

Purpose
To configure the primary SIP Server Application object for high availability.

Start

1. Stop the SIP Server service on the primary and backup hosts. Genesys SIP Server services can be stopped by using the Windows Services dialog box.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
    a. Select the `TServer` section.
        i. Set the `sip-port` option to the port number that will be used by both the primary and backup SIP Server applications.
        ii. Set the `sip-address` option to the Virtual IP address.
        iii. Click `Apply` to save the configuration changes.
    b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP:
        i. Select the `backup-sync` section, and configure the following options:
            - `sync-reconnect-tout`
            - `protocol`
            - `addp-timeout`
            - `addp-remote-timeout`



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.
Note: For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

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

- Click the `Switches` tab.

  a. Ensure that the correct `Switch` object is specified. If necessary, select the correct `Switch` object by using the `Add` button.

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

- Click the `Server Info` tab.

  a. Select the `Redundancy Type`. You can select either `Hot Standby` or `Warm Standby`.

  b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.

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

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

     iii. Click `OK.`

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

- For the `Backup Server` option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.

- Click `Apply` to save the configuration changes.

- Click the `Start Info` tab.

  a. Select `Auto-Restart.`

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

- Click `Apply` and then `OK` to save the configuration changes.

End

3. Configure the backup SIP Server.

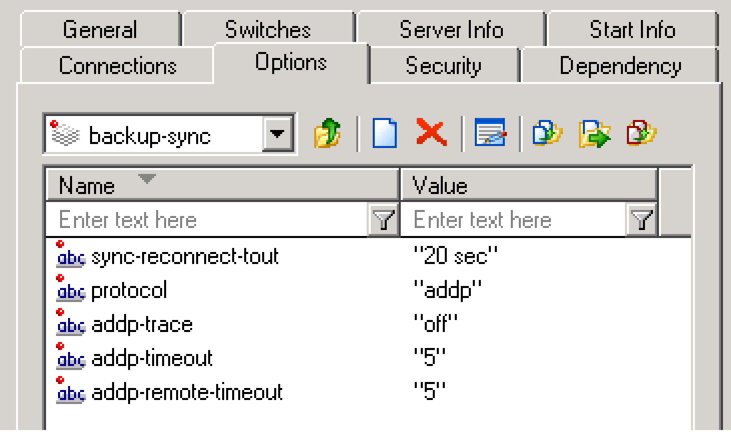
Configuring the backup SIP Server

Purpose

To configure the backup SIP Server Application object for high availability.

Start

1. Stop both primary and backup SIP Servers, if they are running. You can stop the SIP Server service by using the Windows Services dialog box.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. `Select Properties`.
4. Click the `Switches` tab.
    a. Click `Add`, and select the `Switch` object that you associated with the primary SIP Server Application object.
    b. Click `Apply` to save the configuration changes.
5. Click the `Start Info` tab.
    a. Select `Auto-Restart`.
    b. Click `Apply` to save the configuration changes.
6. Click the `Options` tab.
    a. Select the `TServer` section.
        i. Set the `sip-port` option to the same port number that you specified for the primary SIP Server.
        ii. Set the `sip-address` option to the Virtual IP address.
    b. Click `Apply` to save the configuration changes.
7. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP:
    i. Select the `backup-sync` section, and configure the following options:
        - `sync-reconnect-tout`
        - `protocol`
        - `addp-timeout`
        - `addp-remote-timeout`



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.

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

- Click `Apply` and then `OK` to save the configuration changes.

End

4. Update the /etc/hosts file.

Updating the /etc/hosts file

Purpose

To update the `/etc/hosts` file on the primary and backup SIP Server host computers to make the address and host name of the Virtual IP interface known to the DNS server.

Start

1. On the primary SIP Server host computer, open the `/etc/hosts` file in a text editor.
2. Add an entry for the Virtual IP interface by using the following format:
   `<IP_address> <host_name>`
   For example:
   ```
   IPAddress Hostname
   127.0.0.1 sip_host_1
   ```
3. Perform the same steps on the backup SIP Server host computer.

End

5. Create Virtual IP address control scripts.

Creating Virtual IP address control scripts

Purpose

To create Virtual IP address control scripts and wrap them in shell files. The Virtual IP address is enabled and disabled by using the `ifconfig` administrative command.

Start

1. On both SIP Server host computers, create two shell files: one to enable the Virtual IP address and another to disable it—for example:
   - `set_ip_up.sh`—To enable the Virtual IP address
   - `set_ip_down.sh`—To disable the Virtual IP address
2. In the `set_ip_up.sh` file, enter the following command line:
   `ifconfig <name_of_ethernet_interface> <vip_address> netmask <vip_netmask> alias`
   where:
   - `<name_of_ethernet_interface>` is the name of the Virtual IP interface
   - `<vip_address>` is the Virtual IP–interface IP address
   - `<vip_netmask>` is the Virtual IP netmask
3. In the `set_ip_down.sh` file, enter the following command line:
   `ifconfig <name_of_ethernet_interface> <vip_address> delete`
   where:
   - `<name_of_ethernet_interface>` is the name of the Virtual IP interface
   - `<vip_address>` is the Virtual IP–interface IP address

End

6. Create Application objects for Virtual IP address control script.

Creating Application objects for the Virtual IP address control scripts

Purpose

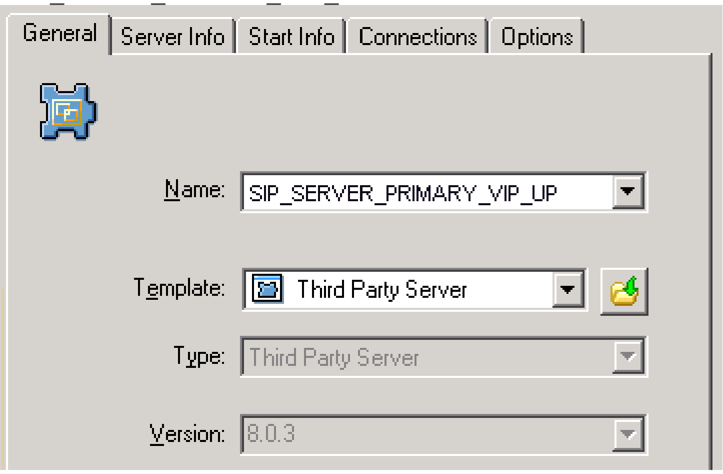
To create four Application objects of type `Third Party Server`: one for each of the shell files that you created previously. For example:

- `SIP_SERVER_PRIMARY_VIP_UP`—For a script that enables the Virtual IP address (to be run on the primary SIP Server host)
- `SIP_SERVER_PRIMARY_VIP_DOWN`—For a script that disables the Virtual IP address (to be run on the primary SIP Server host)
- `SIP_SERVER_BACKUP_VIP_UP`—For a script that enables the Virtual IP address (to be run on the backup SIP Server host)
- `SIP_SERVER_BACKUP_VIP_DOWN`—For a script that disables the Virtual IP address (to be run on the backup SIP Server host)

Creating Application objects for the shell files allows the shell files to be run as applications within the Genesys Framework.

Start

1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the `Third Party Server` template from the Application Templates folder, and click `OK`.
4. On the `General` tab, enter a name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.



Name: SIP_SERVER_PRIMARY_VIP_UP

Template: Third Party Server

Type: Third Party Server

Version: 8.0.3

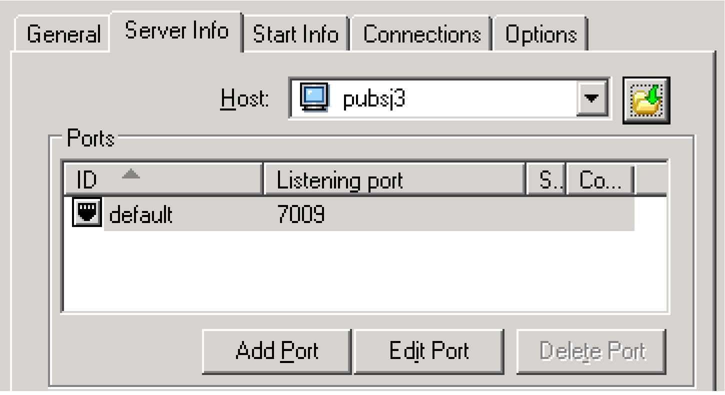
Configuring the Application Object for the Script, General Tab: Sample Configuration

Note: You can use the previously listed Application object names, or you can specify your own.

5. Select the `Server Info` tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is

located.

b. If necessary, specify a valid communication-port number by using the `Edit Port` option.



Host: pubsj3

ID	Listening port	S..	Co...
default	7009		

Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the script, and enter the name of the script in the `Command Line` field. For example, for the SIP_SERVER_PRIMARY_VIP_UP Application object, enter the script name that enables the Virtual IP address (`set_ip_up.sh`). For the SIP_SERVER_PRIMARY_VIP_DOWN Application object, enter the script name that disables the Virtual IP address (`set_ip_down.sh`).
   b. If you are configuring an Application object that disables the Virtual IP interface (SIP_SERVER_PRIMARY_VIP_DOWN and SIP_SERVER_BACKUP_VIP_DOWN), set the `Timeout Startup` value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four scripts.

End

7. Create Alarm Reaction scripts.

Creating Alarm Reaction scripts

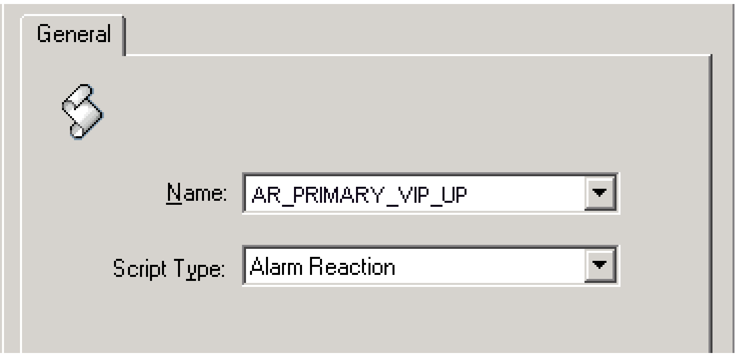
Purpose

To create Alarm Reaction scripts for HA-related Alarm Conditions. When an HA-related Alarm Condition occurs, the associated Alarm Reaction script is run. Alarm Reaction scripts are configured to call the Application objects that you created in Step 6.

Start

1. Open the Configuration Manager.

2. Select `Resources > Scripts`.
3. Right-click and select `New > Script`.
4. Create four scripts: one for each of the Application objects that you created previously. For example:
   - AR_SCRIPT_PRIMARY_VIP_UP—To trigger a script that enables the Virtual IP address (to be run on the primary SIP Server host)
   - AR_SCRIPT_PRIMARY_VIP_DOWN—To trigger a script that disables the Virtual IP address (to be run on the primary SIP Server host)
   - AR_SCRIPT_BACKUP_VIP_UP—To trigger a script that enables the Virtual IP address (to be run on the backup SIP Server host)
   - AR_SCRIPT_BACKUP_VIP_DOWN—To trigger a script that disables the Virtual IP address (to be run on the backup SIP Server host)

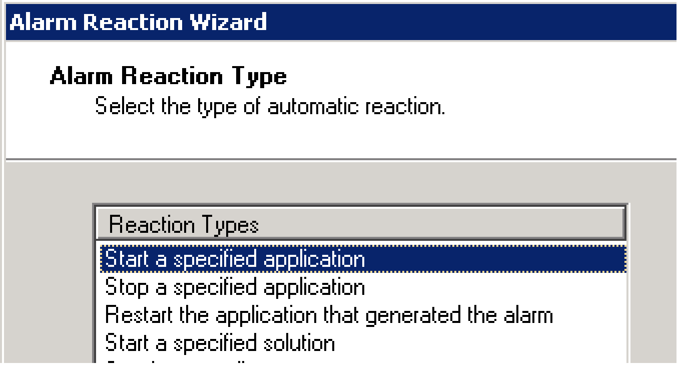


Name: AR_PRIMARY_VIP_UP

Script Type: Alarm Reaction

Configuring the Alarm Reaction Script: Sample Configuration

5. For each of the Alarm Reaction scripts, select `Alarm Reaction` as the `Script Type`.
6. For each of the Alarm Reaction scripts, use the Alarm Reaction Wizard to configure the `Alarm Reaction Type`.
   a. Select an Alarm Reaction script, and right-click to open the Alarm Reaction Wizard (select `Wizard > Configure`).
   b. In the Alarm Reaction Wizard, click `Next`.
   c. In the `Alarm Reaction Type` dialog box, select `Start a specified application`, and click `Next`.



Alarm Reaction Type

Select the type of automatic reaction.

Reaction Types

Start a specified application

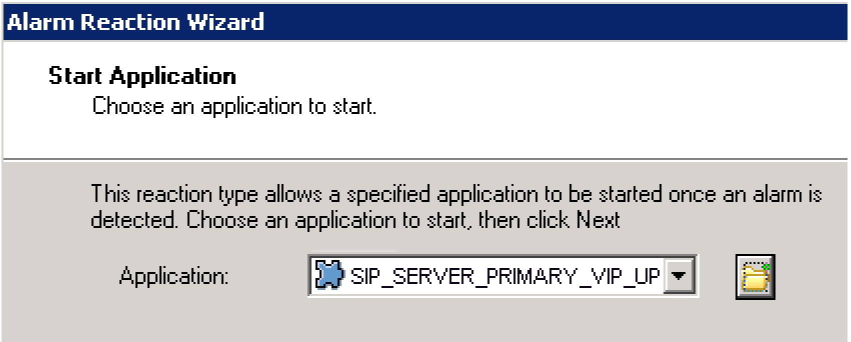
Stop a specified application

Restart the application that generated the alarm

Start a specified solution

Alarm Reaction: Selecting the Alarm Reaction Type

   d. Browse to select the corresponding Application object. For example, for the AR_SCRIPT_PRIMARY_VIP_UP Alarm Reaction script, select the SIP_SERVER_PRIMARY_VIP_UP Application object of type `Third Party Server`.


Alarm Reaction Wizard

Start Application

Choose an application to start.

This reaction type allows a specified application to be started once an alarm is detected. Choose an application to start, then click Next

Application: SIP_SERVER_PRIMARY_VIP_UP

Alarm Reaction: Selecting the Application to Start

e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in Step 4.

End

8. Create Alarm Conditions.

Creating Alarm Conditions

Purpose

Alarm Conditions are required to handle log events that occur when a SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you will configure them to trigger the Alarm Reaction scripts that you created in Step 7.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. The following table outlines the Alarm Conditions for both hot-standby and warm-standby configurations.

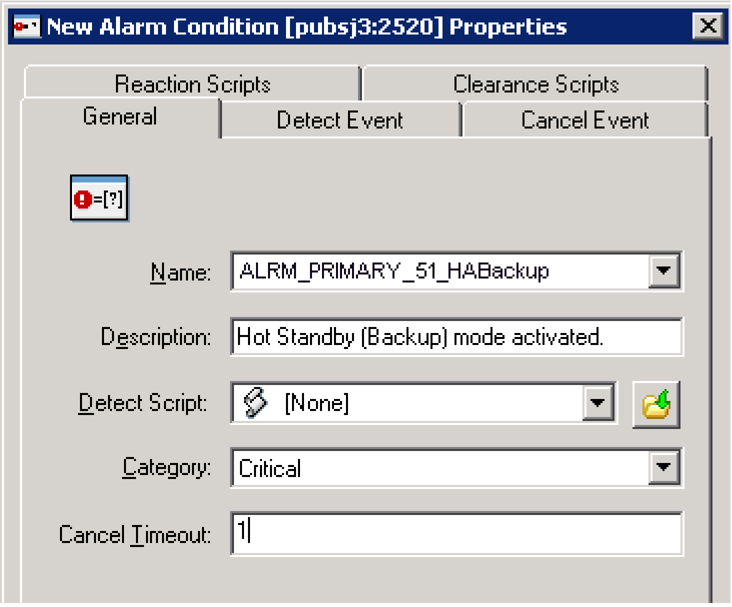
Alarm Conditions: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
00-05151	SIP_SERVER_PRIMARY	ALRM_PRIMARY_51_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
00-05150	SIP_SERVER_PRIMARY	ALRM_PRIMARY_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN AR_SCRIPT_PRIMARY_VIP_UP
00-05151	SIP_SERVER_BACKUP	ALRM_BACKUP_51_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
00-05150	SIP_SERVER_BACKUP	ALRM_BACKUP_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP AR_SCRIPT_PRIMARY_VIP_DOWN

For information about the log events for which you are creating Alarm Conditions, refer to Log events generated by SCS.

Start

1. Open the Configuration Manager.
2. Navigate to the `Environment > Alarm Conditions folder`.
3. Right-click and select `New > Alarm Condition` to open the `New Alarm Condition Properties` dialog box.
4. On the `General` tab:
   - Enter the Name for the Alarm Condition—for example, `ALRM_PRIMARY_51_HABackup`.
   - Optionally, enter a description.
   - For the `Category` value, select `Critical`.
   - Set `Cancel Timeout` to 1.



New Alarm Condition [pubsj3:2520] Properties

Name: ALRM_PRIMARY_51_HABackup

Description: Hot Standby (Backup) mode activated.

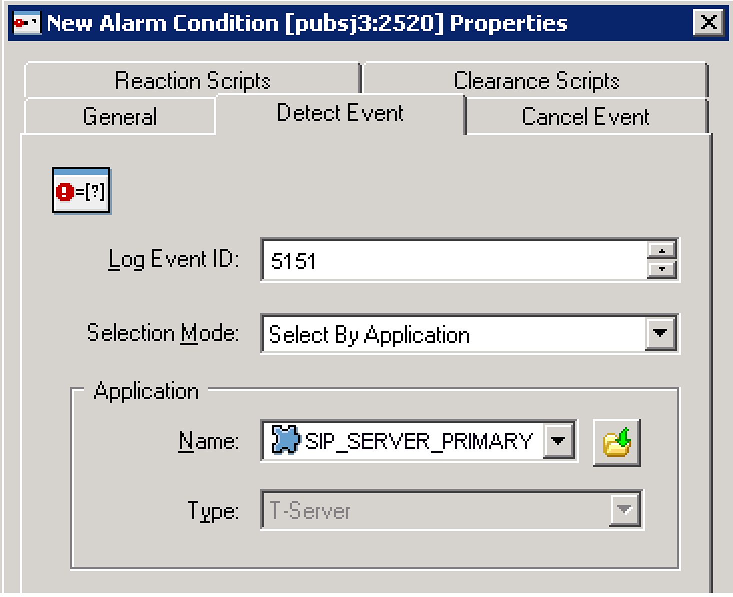
Detect Script: [None]

Category: Critical

Cancel Timeout: 1

Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the `Detect Event` tab:
   - Set the `Log Event ID` as defined in the table above.
   - Set the `Selection Mode` to `Select By Application`.
   - For the `Application Name` field, click the folder icon to browse for the SIP Server Application object. If you are creating an Alarm Condition for the primary SIP Server, select the primary SIP Server Application object. If you are creating an Alarm Condition for the backup SIP Server, select the backup SIP Server Application object.



Log Event ID: 5151

Selection Mode: Select By Application

Application

Name: SIP_SERVER_PRIMARY

Type: T-Server

Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the `Reaction Scripts` tab, add the Alarm Reaction script as defined in the previous table.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your configuration.

End

9. Test Alarm Conditions.

Testing Alarm Conditions

Purpose

To verify that the Alarm Conditions work as expected.

Start

1. Use Telnet to access the SIP Server Virtual IP interface.
2. Open the Solution Control Interface (SCI).
3. Under `Alarm Conditions`, select the Alarm Condition that you created in the previous procedure—for example, ALRM_PRIMARY_51_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_51_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP address at the primary SIP Server and disable the Virtual IP address at the backup SIP Server.

4. Use the `ipconfig` command to verify that the Virtual IP interface is active on the backup SIP Server and that the Virtual IP interface is inactive on the primary SIP Server.

End

10. Verify the HA configuration.

Testing your SIP Server HA configuration

Purpose

To validate your HA configuration, you can perform the following tests.

Prerequisites

- Ensure that the Management Layer is up and running.
- Start the primary SIP Server, and ensure that it is in primary mode.
- Start the backup SIP Server, and ensure that it is in backup mode.

Start

1. Test 1: Manual switchover
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 2: Manual switchback
   a. Establish a call between two SIP endpoints.
   b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
   c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
   d. Release the call.

5. Test 3: Stop primary SIP Server
   a. Establish a call between two SIP endpoints.

b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.

c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

End

Deploying HA on Solaris

Complete these steps to set up SIP Server HA on Solaris, using the IP Address Takeover method.

IP Address Takeover HA Deployment on Solaris

1. Check prerequisites.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.
  Note: Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.
- Software requirements:
  - For the Windows OS to send a gratuitous ARP packet when a new IP address is assigned on the computer, you must install the Microsoft Hotfix 2811463 for Windows 2008 R2. See http://support.microsoft.com/kb/2811463/en-us.
  - SIP Server must be installed and configured on both host computers.
  - LCA must be installed and configured on both host computers.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).
- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet. A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with SIP Server might fail to update the ARP table during Virtual IP Address Takeover.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

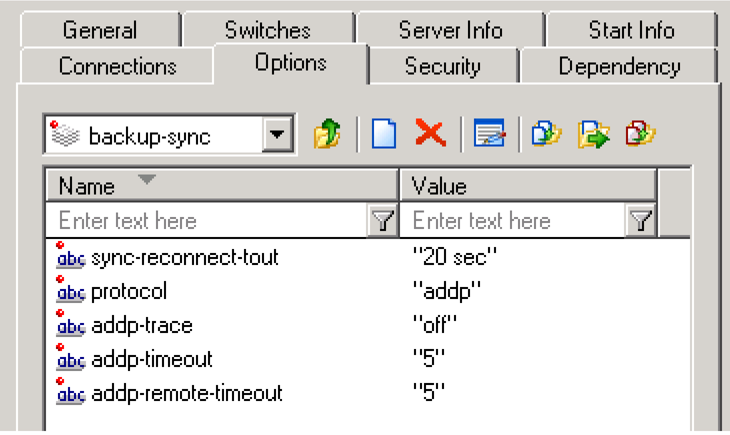
2. Configure the primary SIP Server.

Configuring the primary SIP Server

Purpose
To configure the primary SIP Server Application object for high availability.

Start

1. Stop the SIP Server service on the primary and backup hosts. Genesys SIP Server services can be stopped by using the Windows Services dialog box.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the `TServer` section.
      i. Set the `sip-port` option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the `sip-address` option to the Virtual IP address.
      iii. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP:
      i. Select the `backup-sync` section, and configure the following options:
         - `sync-reconnect-tout`
         - `protocol`
         - `addp-timeout`
         - `addp-remote-timeout`



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.
Note: For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

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

- Click the `Switches` tab.

a. Ensure that the correct `Switch` object is specified. If necessary, select the correct `Switch` object by using the `Add` button.

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

- Click the `Server Info` tab.

a. Select the `Redundancy Type`. You can select either `Hot Standby` or `Warm Standby`.

b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.

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

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

iii. Click `OK`.

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

- For the `Backup Server` option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.
- Click `Apply` to save the configuration changes.
- Click the `Start Info` tab.

a. Select `Auto-Restart`.

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

- Click `Apply` and then `OK` to save the configuration changes.

End

3. Configure the backup SIP Server.

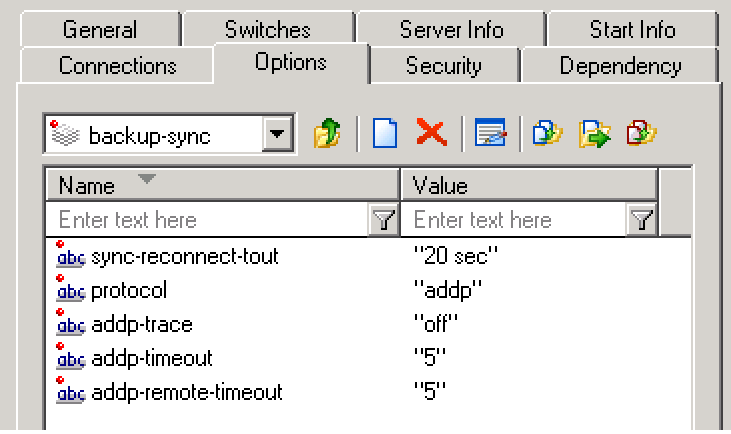
Configuring the backup SIP Server

Purpose

To configure the backup SIP Server Application object for high availability.

Start

1. Stop both primary and backup SIP Servers, if they are running. You can stop the SIP Server service by using the Windows Services dialog box.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. `Select Properties`.
4. Click the `Switches` tab.
    a. Click `Add`, and select the `Switch` object that you associated with the primary SIP Server Application object.
    b. Click `Apply` to save the configuration changes.
5. Click the `Start Info` tab.
    a. Select `Auto-Restart`.
    b. Click `Apply` to save the configuration changes.
6. Click the `Options` tab.
    a. Select the `TServer` section.
        i. Set the `sip-port` option to the same port number that you specified for the primary SIP Server.
        ii. Set the `sip-address` option to the Virtual IP address.
    b. Click `Apply` to save the configuration changes.
7. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP:
    i. Select the `backup-sync` section, and configure the following options:
        - `sync-reconnect-tout`
        - `protocol`
        - `addp-timeout`
        - `addp-remote-timeout`



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.

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

- Click `Apply` and then `OK` to save the configuration changes.

End

4. Update the /etc/hosts file.

Updating the /etc/hosts file

Purpose

To update the /etc/hosts file on the primary and backup SIP Server host computers to make the address and host name of the Virtual IP interface known to the DNS server.

Start

1. On the primary SIP Server host computer, inside the `/etc` directory, create the file:
   `/etc/hostname.<interface_name>:<n>`
   where `interface_name` is the actual name of the Virtual IP interface on that computer—for example:
   `/etc/hostname.dmfe0:1`
   This file must contain the hostname of the Virtual IP interface as it is known to the DNS server and is recorded inside the `/etc/hosts` file.
2. Perform the same steps on the backup SIP Server host computer.

End

5. Create Virtual IP address control scripts.

Creating Virtual IP address control scripts

Purpose

To create Virtual IP interface/address control scripts and wrap them in shell files. The Virtual IP interface is enabled and disabled by using the `ifconfig` administrative command.

Start

1. On both SIP Server host computers, create two shell files: one to enable the Virtual IP interface and another to disable it--for example:
   - `set_ip_up.sh`—To enable the Virtual IP interface
   - `set_ip_down.sh`—To disable the Virtual IP interface
2. In the `set_ip_up.sh` file, enter the following command line:
   `ifconfig hostname.<interface_name>:<n> up`
   where `interface_name` is the name of the Virtual IP interface—for example:
   `ifconfig /etc/hostname.dmfe0:1 up`
3. In the `set_ip_down.sh` file, enter the following command line:
   `ifconfig hostname.<interface_name>:<n> down`
   where `interface_name` is the name of the Virtual IP interface—for example:
   `ifconfig /etc/hostname.dmfe0:1 down`

End

6. Create Application objects for Virtual IP address control scripts.

Creating Application objects for the Virtual IP address control scripts

Purpose

To create four Application objects of type `Third Party Server`: one for each of the shell files that you created previously. For example:

- `SIP_SERVER_PRIMARY_VIP_UP`—For a script that enables the Virtual IP address (to be run on the primary

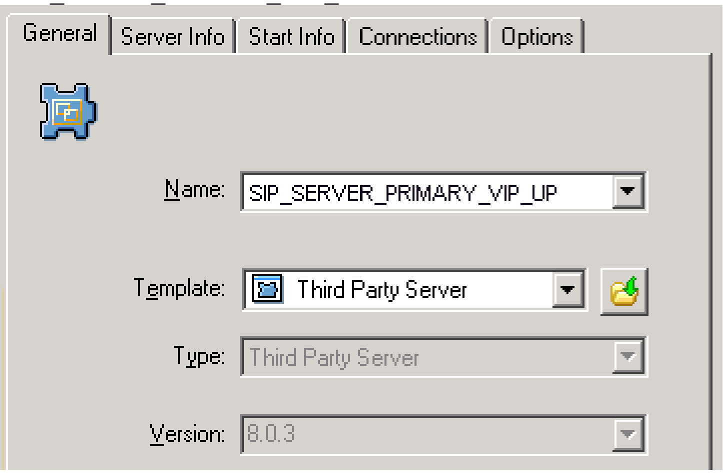
SIP Server host)

- SIP_SERVER_PRIMARY_VIP_DOWN—For a script that disables the Virtual IP address (to be run on the primary SIP Server host)
- SIP_SERVER_BACKUP_VIP_UP—For a script that enables the Virtual IP address (to be run on the backup SIP Server host)
- SIP_SERVER_BACKUP_VIP_DOWN—For a script that disables the Virtual IP address (to be run on the backup SIP Server host)

Creating Application objects for the shell files allows the shell files to be run as applications within the Genesys Framework.

Start

1. In the Configuration Manager, select Environment > Applications.
2. Right-click and select New > Application.
3. Select the Third Party Server template from the Application Templates folder, and click OK.
4. On the General tab, enter a name for the Application object—for example, SIP_SERVER_PRIMARY_VIP_UP.



Name: SIP_SERVER_PRIMARY_VIP_UP

Template: Third Party Server

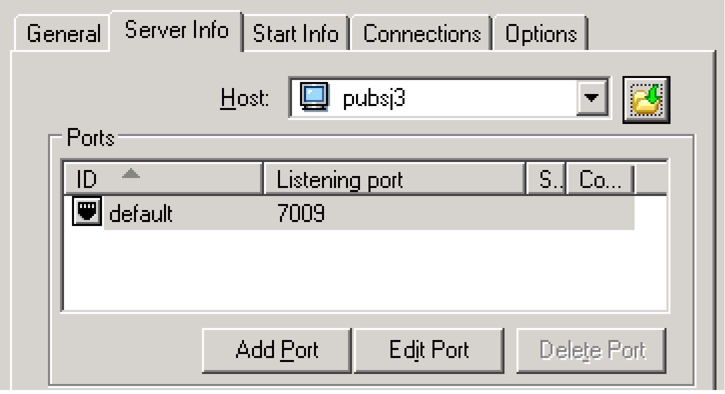
Type: Third Party Server

Version: 8.0.3

Configuring the Application Object for the Script, General Tab: Sample Configuration

Note: You can use the previously listed Application object names, or you can specify your own.

5. Select the Server Info tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is located.
   b. If necessary, specify a valid communication-port number by using the Edit Port option.



Host: pubsj3

Ports

ID	Listening port	S..	Co...
default	7009		

Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the script, and enter the name of the script in the `Command Line` field. For example, for the SIP_SERVER_PRIMARY_VIP_UP Application object, enter the script name that enables the Virtual IP address (`set_ip_up.sh`). For the SIP_SERVER_PRIMARY_VIP_DOWN Application object, enter the script name that disables the Virtual IP address (`set_ip_down.sh`).
   b. If you are configuring an Application object that disables the Virtual IP interface (SIP_SERVER_PRIMARY_VIP_DOWN and SIP_SERVER_BACKUP_VIP_DOWN), set the `Timeout Startup` value to 8.
3. Repeat the steps in this procedure to create an Application object for each of the four scripts.

End

7. Create Alarm Reaction scripts.

Creating Alarm Reaction scripts

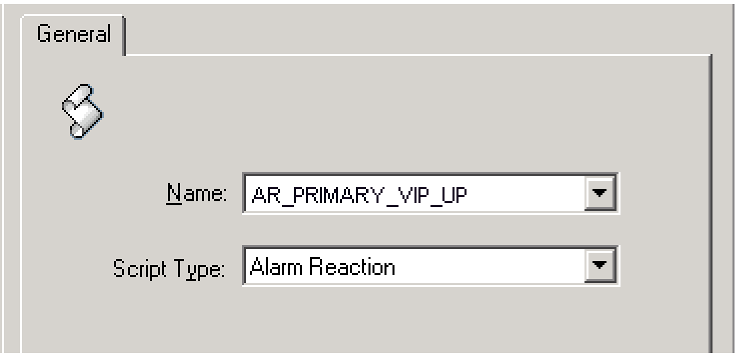
Purpose

To create Alarm Reaction scripts for HA-related Alarm Conditions. When an HA-related Alarm Condition occurs, the associated Alarm Reaction script is run. Alarm Reaction scripts are configured to call the Application objects that you created in Step 6.

Start

1. Open the Configuration Manager.
2. Select `Resources > Scripts`.
3. Right-click and select `New > Script`.

4. Create four scripts: one for each of the Application objects that you created previously. For example:
   - AR_SCRIPT_PRIMARY_VIP_UP—To trigger a script that enables the Virtual IP address (to be run on the primary SIP Server host)
   - AR_SCRIPT_PRIMARY_VIP_DOWN—To trigger a script that disables the Virtual IP address (to be run on the primary SIP Server host)
   - AR_SCRIPT_BACKUP_VIP_UP—To trigger a script that enables the Virtual IP address (to be run on the backup SIP Server host)
   - AR_SCRIPT_BACKUP_VIP_DOWN—To trigger a script that disables the Virtual IP address (to be run on the backup SIP Server host)

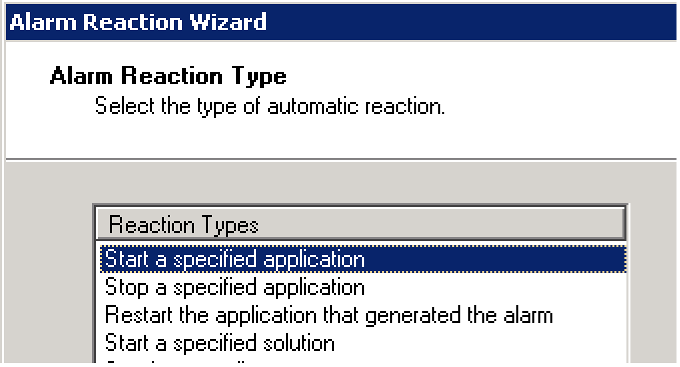


Name: AR_PRIMARY_VIP_UP

Script Type: Alarm Reaction

Configuring the Alarm Reaction Script: Sample Configuration

5. For each of the Alarm Reaction scripts, select `Alarm Reaction` as the `Script Type`.
6. For each of the Alarm Reaction scripts, use the Alarm Reaction Wizard to configure the `Alarm Reaction Type`.
   a. Select an Alarm Reaction script, and right-click to open the Alarm Reaction Wizard (select `Wizard > Configure`).
   b. In the Alarm Reaction Wizard, click `Next`.
   c. In the `Alarm Reaction Type` dialog box, select `Start a specified application`, and click `Next`.



Alarm Reaction Wizard

Alarm Reaction Type

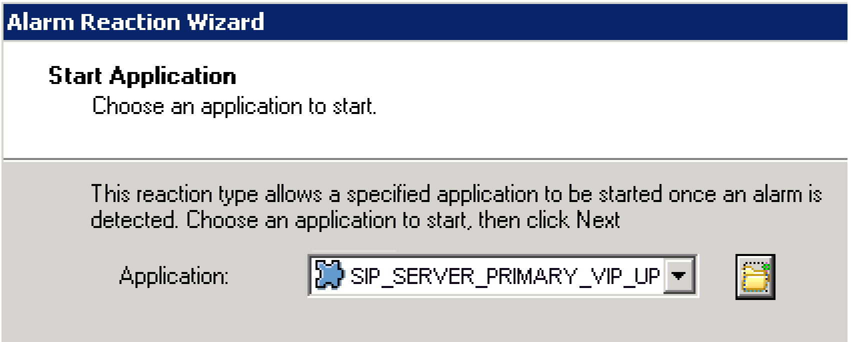
Select the type of automatic reaction.

Reaction Types

Start a specified application
Stop a specified application
Restart the application that generated the alarm
Start a specified solution

Alarm Reaction: Selecting the Alarm Reaction Type

   d. Browse to select the corresponding Application object. For example, for the AR_SCRIPT_PRIMARY_VIP_UP Alarm Reaction script, select the SIP_SERVER_PRIMARY_VIP_UP Application object of type `Third Party Server`.



Alarm Reaction Wizard

Start Application

Choose an application to start.

This reaction type allows a specified application to be started once an alarm is detected. Choose an application to start, then click Next

Application: SIP_SERVER_PRIMARY_VIP_UP

Alarm Reaction: Selecting the Application to Start

e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in Step 4.

End

8. Create Alarm Conditions.

Creating Alarm Conditions

Purpose

Alarm Conditions are required to handle log events that occur when a SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you will configure them to trigger the Alarm Reaction scripts that you created in Step 7.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. The following table outlines the Alarm Conditions for both hot-standby and warm-standby configurations.

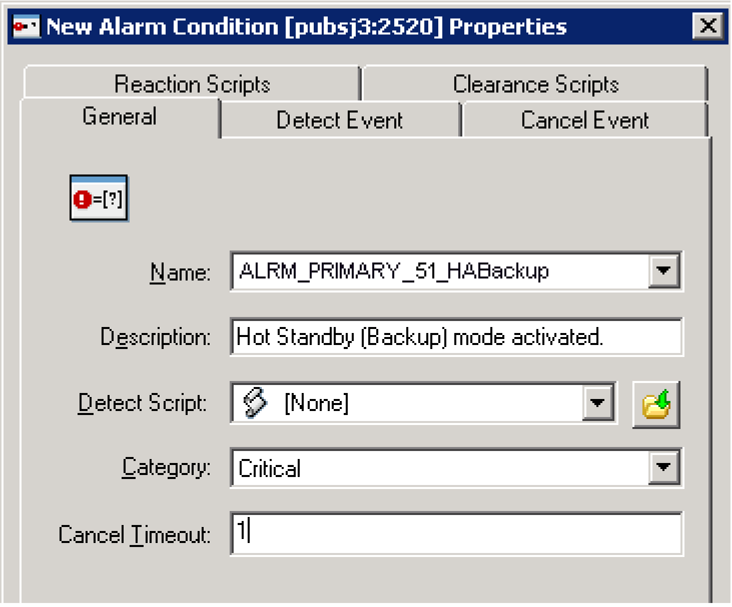
Alarm Conditions: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
00-05151	SIP_SERVER_PRIMARY	ALRM_PRIMARY_51_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
00-05150	SIP_SERVER_PRIMARY	ALRM_PRIMARY_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN AR_SCRIPT_PRIMARY_VIP_UP
00-05151	SIP_SERVER_BACKUP	ALRM_BACKUP_51_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
00-05150	SIP_SERVER_BACKUP	ALRM_BACKUP_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP AR_SCRIPT_PRIMARY_VIP_DOWN

For information about the log events for which you are creating Alarm Conditions, refer to Log events generated by SCS.

Start

1. Open the Configuration Manager.
2. Navigate to the `Environment > Alarm Conditions folder`.
3. Right-click and select `New > Alarm Condition` to open the `New Alarm Condition Properties` dialog box.
4. On the `General` tab:
   - Enter the Name for the Alarm Condition—for example, `ALRM_PRIMARY_51_HABackup`.
   - Optionally, enter a description.
   - For the `Category` value, select `Critical`.
   - Set `Cancel Timeout` to 1.



Name: ALRM_PRIMARY_51_HABackup

Description: Hot Standby (Backup) mode activated.

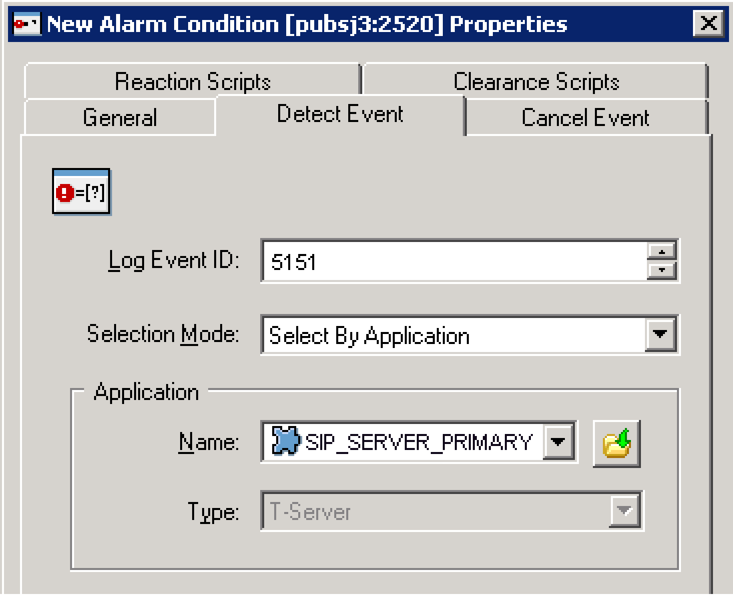
Detect Script: [None]

Category: Critical

Cancel Timeout: 1

Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the `Detect Event` tab:
   - Set the `Log Event ID` as defined in the table above.
   - Set the `Selection Mode` to `Select By Application`.
   - For the `Application Name` field, click the folder icon to browse for the SIP Server Application object. If you are creating an Alarm Condition for the primary SIP Server, select the primary SIP Server Application object. If you are creating an Alarm Condition for the backup SIP Server, select the backup SIP Server Application object.



Log Event ID: 5151

Selection Mode: Select By Application

Name: SIP_SERVER_PRIMARY

Type: T-Server

Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the `Reaction Scripts` tab, add the Alarm Reaction script as defined in the previous table.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your configuration.

End

9. Test Alarm Conditions.

Testing Alarm Conditions

Purpose

To verify that the Alarm Conditions work as expected.

Start

1. Use Telnet to access the SIP Server Virtual IP interface.
2. Open the Solution Control Interface (SCI).
3. Under `Alarm Conditions`, select the Alarm Condition that you created in the previous procedure—for example, ALRM_PRIMARY_51_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_51_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP address at the primary SIP Server and disable the Virtual IP address at the backup SIP Server.

4. Use the `ipconfig` command to verify that the Virtual IP interface is active on the backup SIP Server and that the Virtual IP interface is inactive on the primary SIP Server.

End

10. Verify the HA configuration.

Testing your SIP Server HA configuration

Purpose

To validate your HA configuration, you can perform the following tests.

Prerequisites

- Ensure that the Management Layer is up and running.
- Start the primary SIP Server, and ensure that it is in primary mode.
- Start the backup SIP Server, and ensure that it is in backup mode.

Start

1. Test 1: Manual switchover
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 2: Manual switchback
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 3: Stop primary SIP Server
    a. Establish a call between two SIP endpoints.

b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.

c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

End

Deploying HA on Linux

Complete these steps to set up SIP Server HA on Linux, using the IP Address Takeover method.

IP Address Takeover HA Deployment on Linux

1. Ensure that your system meets the deployment prerequisites.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in your environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.
  Note: Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.
- Software requirements:
  - For the Windows OS to send a gratuitous ARP packet when a new IP address is assigned on the computer, you must install the Microsoft Hotfix 2811463 for Windows 2008 R2. See http://support.microsoft.com/kb/2811463/en-us.
  - SIP Server must be installed and configured on both host computers.
  - LCA must be installed and configured on both host computers.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC. When you create a Host object, make sure you specify the hostname or IP address of the second NIC (dedicated to other non-SIP communication).
- Networking requirements:
  - Static IP addresses are required for all network interfaces on both host computers.
  - It is highly recommended that you have primary and backup SIP Server hosts on a dedicated subnet. A dedicated subnet ensures that Virtual IP Address Takeover affects only the Address Resolution Protocol (ARP) table on the subnet router. Without a dedicated subnet, hosts that communicate with SIP Server might fail to update the ARP table during Virtual IP Address Takeover.
  - In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

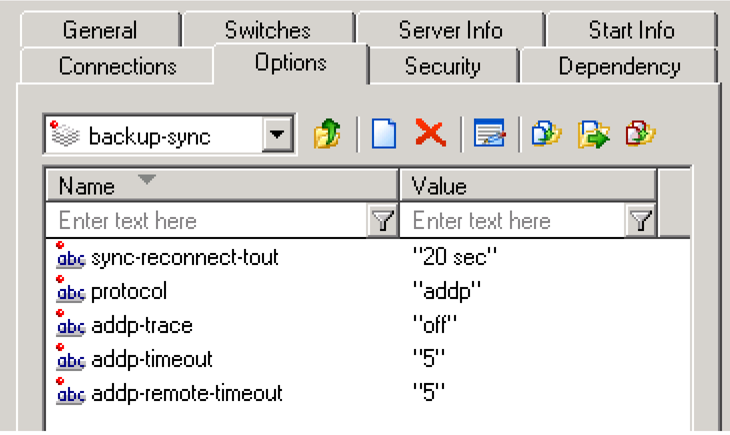
2. Configure the primary SIP Server.

Configuring the primary SIP Server

Purpose
To configure the primary SIP Server Application object for high availability.

Start

1. Stop the SIP Server service on the primary and backup hosts. Genesys SIP Server services can be stopped by using the Windows Services dialog box.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the `TServer` section.
      i. Set the `sip-port` option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the `sip-address` option to the Virtual IP address.
      iii. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP:
      i. Select the `backup-sync` section, and configure the following options:
         - `sync-reconnect-tout`
         - `protocol`
         - `addp-timeout`
         - `addp-remote-timeout`



backup-sync

Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.
Note: For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

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

- Click the `Switches` tab.

a. Ensure that the correct `Switch` object is specified. If necessary, select the correct `Switch` object by using the `Add` button.

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

- Click the `Server Info` tab.

a. Select the `Redundancy Type`. You can select either `Hot Standby` or `Warm Standby`.

b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.

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

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

iii. Click `OK.`

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

- For the `Backup Server` option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.
- Click `Apply` to save the configuration changes.
- Click the `Start Info` tab.

a. Select `Auto-Restart.`

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

- Click `Apply` and then `OK` to save the configuration changes.

End

3. Configure the backup SIP Server.

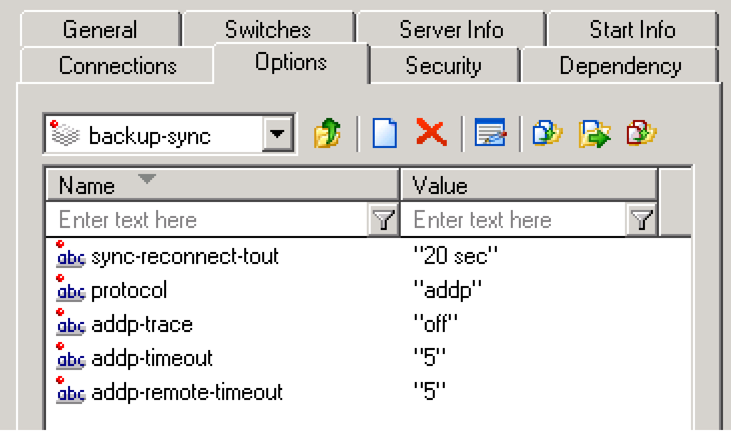
Configuring the backup SIP Server

Purpose

To configure the backup SIP Server Application object for high availability.

Start

1. Stop both primary and backup SIP Servers, if they are running. You can stop the SIP Server service by using the Windows Services dialog box.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. `Select Properties`.
4. Click the `Switches` tab.
    a. Click `Add`, and select the `Switch` object that you associated with the primary SIP Server Application object.
    b. Click `Apply` to save the configuration changes.
5. Click the `Start Info` tab.
    a. Select `Auto-Restart`.
    b. Click `Apply` to save the configuration changes.
6. Click the `Options` tab.
    a. Select the `TServer` section.
        i. Set the `sip-port` option to the same port number that you specified for the primary SIP Server.
        ii. Set the `sip-address` option to the Virtual IP address.
    b. Click `Apply` to save the configuration changes.
7. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP:
    i. Select the `backup-sync` section, and configure the following options:
        - `sync-reconnect-tout`
        - `protocol`
        - `addp-timeout`
        - `addp-remote-timeout`



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.

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

- Click `Apply` and then `OK` to save the configuration changes.

End

4. Update the /etc/hosts file.

Updating the /etc/hosts file

Purpose

To make the address and host name of the Virtual IP interface known to the DNS server.

Start

On both the primary and backup SIP Server host computers, add an entry for the Virtual IP interface by using the following format:

```
<IP_address> <host_name>
```

For example:

```
IPAddress Hostname
```

```
127.0.0.1 sipdev1
```

End

5. Create a configuration file for the Virtual IP interface.

Creating a configuration file for the Virtual IP interface

Purpose

To create a configuration file for the Virtual IP interface. This procedure must be performed on both SIP Server host computers.

Start

1. On each of the SIP Server host computers, locate the `/etc/sysconfig/network-scripts/ifcfg-eth0` file.
2. Create a copy that is named `/etc/sysconfig/network-scripts/ifcfg-eth0:1`.
3. Define `IPADDR`, `NETMASK`, and `NETWORK` parameters values for the Virtual IP interface. When you are finished, the content of the file should appear similar to the following example:
   ```
   DEVICE=eth0:1
   BOOTPROTO=static
   USERCTL=yes
   TYPE=Ethernet
   IPADDR=192.51.14.208
   NETMASK=255.255.255.0
   NETWORK=192.51.14.0
   BROADCAST=192.51.14.255
   ONPARENT=no
   ```

End

6. Create Virtual IP address control scripts.

Creating Virtual IP address control scripts

Purpose

The Virtual IP interface/address is enabled and disabled by using the `ifconfig` administrative command. To facilitate the enabling and disabling of the Virtual IP interface, you can wrap `ifconfig` commands in shell files.

Start

1. On both SIP Server host computers, create two shell files: one to enable the Virtual IP interface and another to disable it—for example:
   - `set_ip_up.sh`—To enable the Virtual IP interface
   - `set_ip_down.sh`—To disable the Virtual IP interface
2. In the `set_ip_up.sh` file, enter the following command line:
   `ifconfig <name_of_ethernet_interface>:1 xxx.xxx.xxx.xxx up`
   where `name_of_ethernet_interface` is the name of the Virtual IP interface and `xxx.xxx.xxx.xxx` is the Virtual IP--interface IP address.
3. In the `set_ip_down.sh` file, enter the following command line:
   `ifconfig <name_of_ethernet_interface>:1 down`
   where name_of_ethernet_interface is the name of the Virtual IP interface.

End

7. Create Application objects for Virtual IP address control scripts.

Creating Application objects for the Virtual IP address control scripts

Purpose

To create four Application objects of type `Third Party Server`: one for each of the shell files that you created previously. For example:

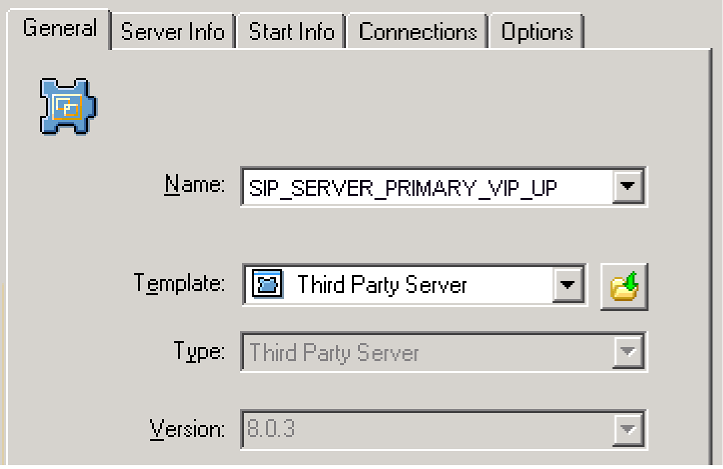
- `SIP_SERVER_PRIMARY_VIP_UP`—For a script that enables the Virtual IP address (to be run on the primary SIP Server host)
- `SIP_SERVER_PRIMARY_VIP_DOWN`—For a script that disables the Virtual IP address (to be run on the primary SIP Server host)
- `SIP_SERVER_BACKUP_VIP_UP`—For a script that enables the Virtual IP address (to be run on the backup SIP Server host)
- `SIP_SERVER_BACKUP_VIP_DOWN`—For a script that disables the Virtual IP address (to be run on the backup SIP Server host)

Creating Application objects for the shell files allows the shell files to be run as applications within the

Genesys Framework.

Start

1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the `Third Party Server` template from the Application Templates folder, and click OK.
4. On the `General` tab, enter a name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.



Name: SIP_SERVER_PRIMARY_VIP_UP

Template: Third Party Server

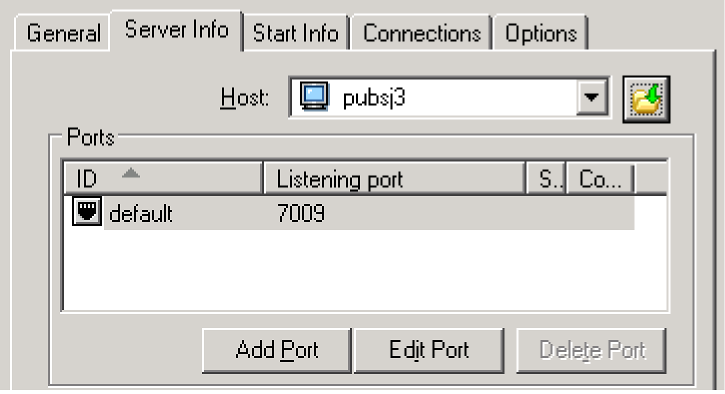
Type: Third Party Server

Version: 8.0.3

Configuring the Application Object for the Script, General Tab: Sample Configuration

Note: You can use the previously listed Application object names, or you can specify your own.

5. Select the `Server Info` tab.
   a. Select the host name of the SIP Server on which the corresponding Virtual IP address control script is located.
   b. If necessary, specify a valid communication-port number by using the `Edit Port` option.



Host: pubsj3

ID	Listening port	S...	Co...
default	7009		

Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the script, and enter the name of the script in the `Command Line` field. For example, for the `SIP_SERVER_PRIMARY_VIP_UP` Application object, enter

the script name that enables the Virtual IP address (`set_ip_up.sh`). For the `SIP_SERVER_PRIMARY_VIP_DOWN` Application object, enter the script name that disables the Virtual IP address (`set_ip_down.sh`).

b. If you are configuring an Application object that disables the Virtual IP interface (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the `Timeout Startup` value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four scripts.

End

8. Create Alarm Reaction scripts.

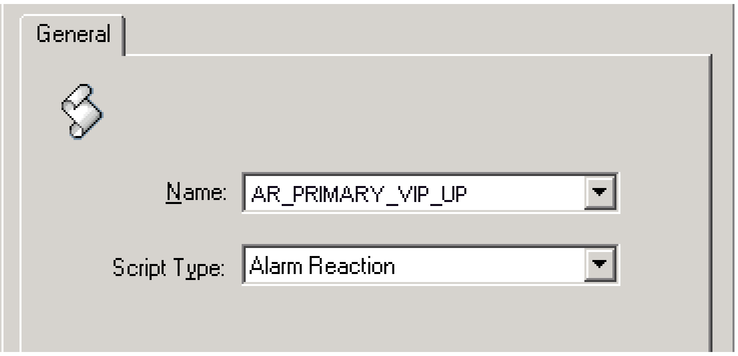
Creating Alarm Reaction scripts

Purpose

To create Alarm Reaction scripts for HA-related Alarm Conditions. When an HA-related Alarm Condition occurs, the associated Alarm Reaction script is run. Alarm Reaction scripts are configured to call the Application objects that you created in Step 7.

Start

1. Open the Configuration Manager.
2. Select `Resources > Scripts`.
3. Right-click and select `New > Script`.
4. Create four scripts: one for each of the Application objects that you created previously. For example:
   - `AR_SCRIPT_PRIMARY_VIP_UP`—To trigger a script that enables the Virtual IP address (to be run on the primary SIP Server host)
   - `AR_SCRIPT_PRIMARY_VIP_DOWN`—To trigger a script that disables the Virtual IP address (to be run on the primary SIP Server host)
   - `AR_SCRIPT_BACKUP_VIP_UP`—To trigger a script that enables the Virtual IP address (to be run on the backup SIP Server host)
   - `AR_SCRIPT_BACKUP_VIP_DOWN`—To trigger a script that disables the Virtual IP address (to be run on the backup SIP Server host)

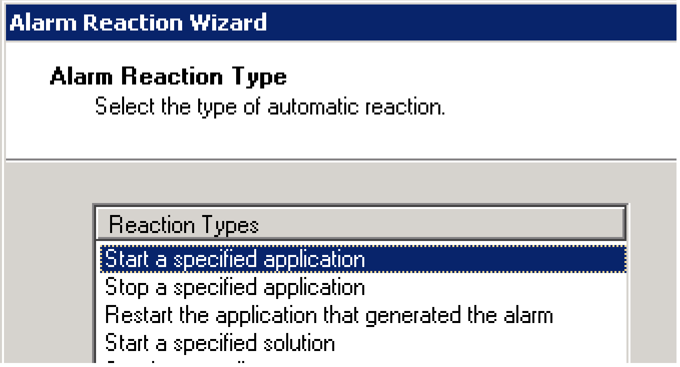


Name: AR_PRIMARY_VIP_UP

Script Type: Alarm Reaction

Configuring the Alarm Reaction Script: Sample Configuration

5. For each of the Alarm Reaction scripts, select `Alarm Reaction` as the `Script Type`.
6. For each of the Alarm Reaction scripts, use the Alarm Reaction Wizard to configure the `Alarm Reaction Type`.
   a. Select an Alarm Reaction script, and right-click to open the Alarm Reaction Wizard (select `Wizard > Configure`).
   b. In the Alarm Reaction Wizard, click `Next`.
   c. In the `Alarm Reaction Type` dialog box, select `Start a specified application`, and click `Next`.



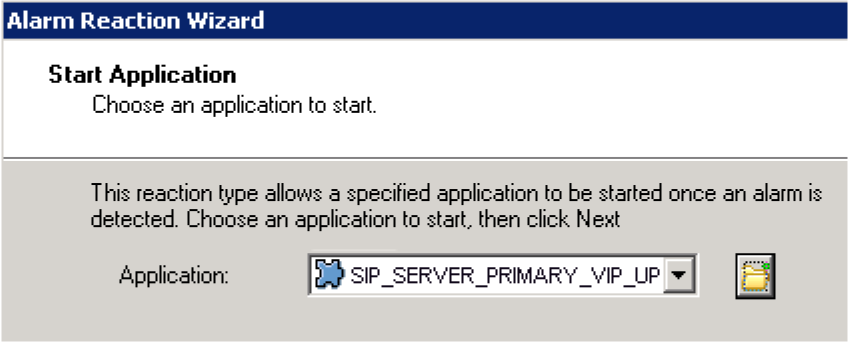
Alarm Reaction Type

Select the type of automatic reaction.

Reaction Types
- Start a specified application
- Stop a specified application
- Restart the application that generated the alarm
- Start a specified solution

Alarm Reaction: Selecting the Alarm Reaction Type

   d. Browse to select the corresponding Application object. For example, for the AR_SCRIPT_PRIMARY_VIP_UP Alarm Reaction script, select the SIP_SERVER_PRIMARY_VIP_UP Application object of type `Third Party Server`.



Start Application

Choose an application to start.

This reaction type allows a specified application to be started once an alarm is detected. Choose an application to start, then click Next

Application: SIP_SERVER_PRIMARY_VIP_UP

Alarm Reaction: Selecting the Application to Start

   e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in Step 4.

End

9. Create Alarm Conditions.

Creating Alarm Conditions

Purpose

Alarm Conditions are required to handle log events that occur when a SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you will configure them to trigger the Alarm Reaction scripts that you created in Step 8.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. The following table outlines the Alarm Conditions for both hot-standby and warm-standby configurations.

Alarm Conditions: Sample Configuration

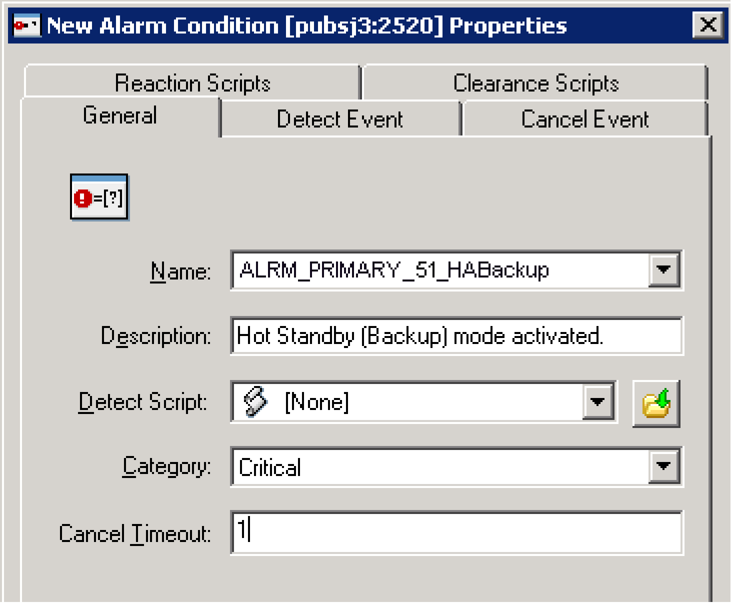
Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
00-05151	SIP_SERVER_PRIMARY	ALRM_PRIMARY_51_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
00-05150	SIP_SERVER_PRIMARY	ALRM_PRIMARY_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN AR_SCRIPT_PRIMARY_VIP_UP
00-05151	SIP_SERVER_BACKUP	ALRM_BACKUP_51_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
00-05150	SIP_SERVER_BACKUP	ALRM_BACKUP_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP AR_SCRIPT_PRIMARY_VIP_DOWN

For information about the log events for which you are creating Alarm Conditions, refer to Log events generated by SCS.

Start

1. Open the Configuration Manager.
2. Navigate to the `Environment > Alarm Conditions folder`.
3. Right-click and select `New > Alarm Condition` to open the `New Alarm Condition Properties` dialog box.
4. On the `General` tab:
   - Enter the `Name` for the Alarm Condition—for example, `ALRM_PRIMARY_51_HABackup`.
   - Optionally, enter a description.

- For the Category value, select Critical.
- Set Cancel Timeout to 1.



New Alarm Condition [pubsj3:2520] Properties

Name: ALRM_PRIMARY_51_HABackup

Description: Hot Standby (Backup) mode activated.

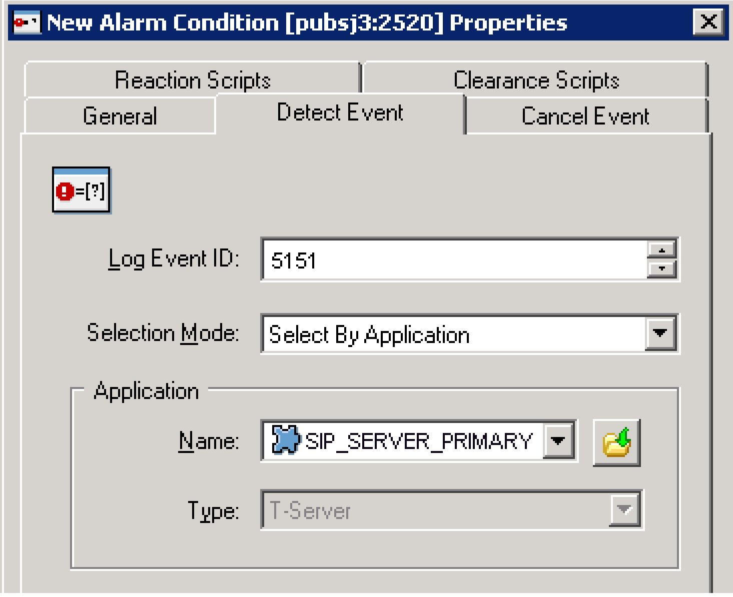
Detect Script: [None]

Category: Critical

Cancel Timeout: 1

Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the Detect Event tab:
   - Set the Log Event ID as defined in the table above.
   - Set the Selection Mode to Select By Application.
   - For the Application Name field, click the folder icon to browse for the SIP Server Application object. If you are creating an Alarm Condition for the primary SIP Server, select the primary SIP Server Application object. If you are creating an Alarm Condition for the backup SIP Server, select the backup SIP Server Application object.



New Alarm Condition [pubsj3:2520] Properties

Log Event ID: 5151

Selection Mode: Select By Application

Application

Name: SIP_SERVER_PRIMARY

Type: T-Server

Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the `Reaction Scripts` tab, add the Alarm Reaction script as defined in the previous table.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your configuration.

End

10. Test Alarm Conditions.

Testing Alarm Conditions

Purpose

To verify that the Alarm Conditions work as expected.

Start

1. Use Telnet to access the SIP Server Virtual IP interface.
2. Open the Solution Control Interface (SCI).
3. Under `Alarm Conditions`, select the Alarm Condition that you created in the previous procedure—for example, ALRM_PRIMARY_51_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_51_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP address at the primary SIP Server and disable the Virtual IP address at the backup SIP Server.
4. Use the `ipconfig` command to verify that the Virtual IP interface is active on the backup SIP Server and that the Virtual IP interface is inactive on the primary SIP Server.

End

11. Verify the HA configuration.

Testing your SIP Server HA configuration

Purpose

To validate your HA configuration, you can perform the following tests.

Prerequisites

- Ensure that the Management Layer is up and running.
- Start the primary SIP Server, and ensure that it is in primary mode.
- Start the backup SIP Server, and ensure that it is in backup mode.

Start

1. Test 1: Manual switchover
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 2: Manual switchback
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 3: Stop primary SIP Server
    a. Establish a call between two SIP endpoints.
    b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary mode.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

End

Deploying HA in Windows NLB Cluster

Complete these steps to set up SIP Server HA on Windows, using Windows Network Load Balancing (NLB) Cluster functionality.

Windows NLB Cluster HA Deployment

1. Check prerequisites.

Prerequisites

The following are the basic requirements and recommendations that must be complete before you can deploy a SIP Server HA configuration in a Windows NLB Cluster environment.

- Two separate physical host computers: one for the primary SIP Server and one for the backup SIP Server.

Note: Genesys recommends that you install primary and backup instances of SIP Server on different host computers. However, SIP Server does support HA configurations in which both primary and backup SIP Server instances reside on a single host server.

- Operating-system requirement:
  - Windows Server 2003 or Windows Server 2008 with Microsoft Windows Network Load Balancing (NLB).
- Software requirements:
  - SIP Server must be installed and configured on both host computers.
  - Local Control Agent (LCA) must be installed and configured on both host computers.
- Networking requirements:
  - A name-resolution method such as Domain Name System (DNS), DNS dynamic-update protocol, or Windows Internet Name Service (WINS) is required.
  - Both host computers must be members of the same domain.
  - A domain-level account that is a member of the local Administrators group is required on each host computer. A dedicated account is recommended.
  - Each host computer must have a unique NetBIOS name.
  - A static IP address is required for each of the network interfaces on both host computers. **Note:** Server clustering does not support IP addresses that are assigned through Dynamic Host Configuration Protocol (DHCP) servers.

- A dedicated network switch or separate virtual local-area network (VLAN) for cluster adapters is recommended to reduce switch flooding that might be caused by Windows NLB.
- Access to a domain controller is required. If the cluster service is unable to authenticate the user account that is used to start the service, the cluster might fail. It is recommended that the domain controller be on the same local-area network (LAN) as the cluster, to ensure availability.
- Each node must have at least two network adapters: one for the connection to the public network and another for the connection to the private node-to-node cluster network.
- A dedicated private-network adapter is required for HCL certification.
- All nodes must have two physically independent LANs or VLANs for public and private communication.
- If you are using fault-tolerant network cards or network-adapter teaming, verify that firmware and drivers are up to date, and check with your network-adapter manufacturer for Windows NLB cluster compatibility.
- In deployments where SIP Server uses two NICs, one NIC is used for SIP communication, while the second NIC is used for other kinds of communication with various components. Each host has one NIC connected to a subnet dedicated to SIP communication. The Virtual IP address should be within the range of the network to which the NIC dedicated to SIP communication is connected. The second NIC on both hosts should be connected to a separate network.

2. Configure Windows NLB parameters.

Configuring Windows NLB cluster parameters

Purpose

To configure Windows NLB cluster parameters that are required for this type of SIP Server HA deployment. Use the Microsoft Network Load Balancing (NLB) Manager to configure load-balancing parameters, as described in the following procedure.

Start

1. Open the Microsoft Network Load Balancing Manager tool.
2. Select a cluster host, and open the `Cluster Properties` window.
3. On the `Cluster Parameters` tab, select the `Cluster operation mode`. You can choose either Unicast (default) or Multicast mode. For information about Windows NLB Unicast and Multicast modes, refer to your Microsoft Windows Server documentation.
4. Click the `Port Rules` tab.
    a. Specify a `Port` range that includes the port that you will assign as the `sip-port`. See "Configuring the primary SIP Server".
    b. In the `Protocols` section, select `Both` (both UDP and TCP).

   c. In the `Filtering mode` section, select `Multiple host`, and set `Affinity` to either None or `Single`.
   d. Set `Load weight` to `Equal`.

5. Click the `Host Parameters` tab. In the `Initial host state` section, set the `Default state` to `Stopped`.

For more information about Windows NLB cluster parameters, refer to your Microsoft Windows Server documentation.

End

3. Configure the primary SIP Server.

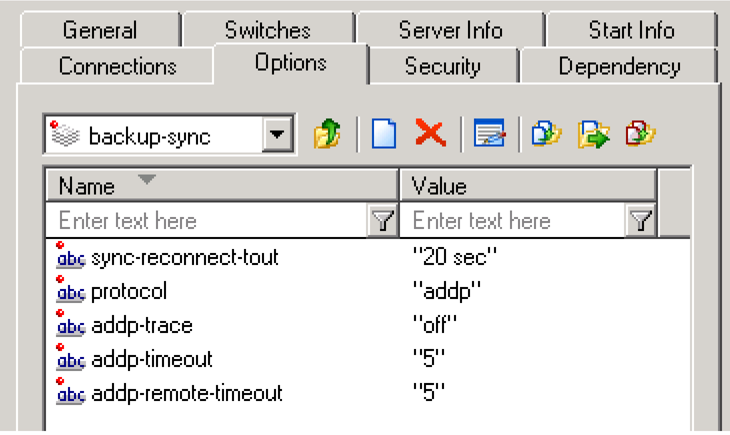
Configuring the primary SIP Server

Purpose
To configure the primary SIP Server Application object for high availability.

Start

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the `Applications` folder, and right-click the SIP Server Application object that you want to configure as the primary SIP Server. Select `Properties`.
4. Click the `Options` tab.
   a. Select the `TServer` section.
      i. Set the `sip-port` option to the port number that will be used by both the primary and backup SIP Server applications.
      ii. Set the `sip-address` option to the Virtual IP address. (For Windows NLB cluster configurations, set the value to the Windows NLB cluster IP address).
      iii. Click `Apply` to save the configuration changes.
   b. If you are deploying a hot-standby configuration, it is recommended that you enable ADDP for communication between the primary and backup SIP Servers. To enable ADDP:
      i. Select the `backup-sync` section, and configure the following options:
         - `sync-reconnect-tout`
         - `protocol`
         - `addp-timeout`

- `addp-remote-timeout`



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the `addp-timeout` and `addp-remote-timeout` options to at least two times the established network-latency time, and to set the `sync-reconnect-tout` option to at least two times the timeout value plus the established network latency.
Note: For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

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

- Click the `Switches` tab.

  a. Ensure that the correct `Switch` object is specified. If necessary, select the correct `Switch` object by using the `Add` button.

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

- Click the `Server Info` tab.

  a. Select the `Redundancy Type`. You can select either `Hot Standby` or `Warm Standby`.

  b. Complete this step if you are deploying a hot-standby configuration. If you are deploying a warm-standby configuration, proceed to Step c.

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

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

     iii. Click `OK`.

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

- For the `Backup Server` option, select the SIP Server Application object that you want to use as the backup SIP Server. If necessary, browse to locate the backup SIP Server Application object.

- Click `Apply` to save the configuration changes.

- Click the `Start Info` tab.

  a. Select `Auto-Restart`.

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

- Click `Apply` and then `OK` to save the configuration changes.

End

4. Configure the backup SIP Server.

Configuring the backup SIP Server

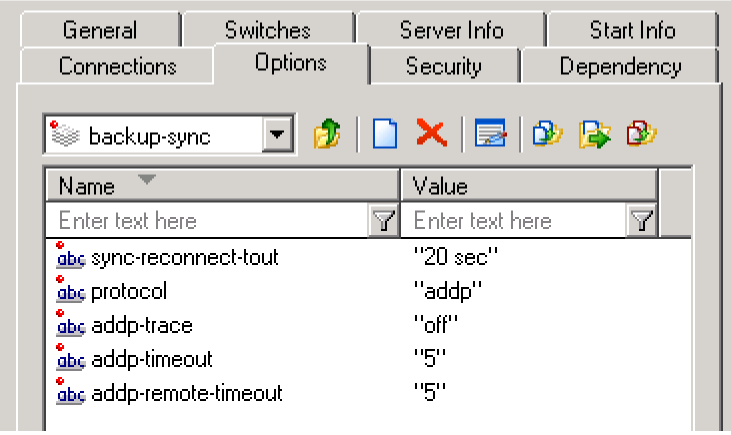
Purpose

To configure the backup SIP Server Application object for high availability.

Start

1. Stop the SIP Server applications on the primary and backup hosts. Genesys SIP Server applications can be stopped by using the Genesys Solution Control Interface.
2. Open the Configuration Manager.
3. Select the Applications folder, and right-click the SIP Server Application object that you want to configure as the backup SIP Server. `Select Properties`.
4. Click the `Switches` tab.
    a. Click `Add`, and select the `Switch` object that you associated with the primary SIP Server Application object.
    b. Click `Apply` to save the configuration changes.
5. Click the `Start Info` tab.
    a. Select `Auto-Restart.`
    b. Click `Apply` to save the configuration changes.
6. Click the `Options` tab.
    a. Select the `TServer` section.
        i. Set the `sip-port` option to the same port number that you specified for the primary SIP Server.
        ii. Set the `sip-address` option to the Virtual IP address. (For Windows NLB cluster configurations, set the value to the Windows NLB cluster IP address)
    b. Click `Apply` to save the configuration changes.
7. If you are deploying a hot-standby configuration and have configured ADDP communication on the primary SIP Server, you must configure ADDP also on the backup SIP Server. To enable ADDP:
    i. Select the `backup-sync` section, and configure the following options:
        - `sync-reconnect-tout`
        - `protocol`

- addp-timeout
- addp-remote-timeout



Name	Value
sync-reconnect-tout	"20 sec"
protocol	"addp"
addp-trace	"off"
addp-timeout	"5"
addp-remote-timeout	"5"

Configuring the backup-sync Options: Sample Configuration

In the preceding example, the guideline that is used to configure ADDP settings is to set the addp-timeout and addp-remote-timeout options to at least two times the established network-latency time, and to set the sync-reconnect-tout option to at least two times the timeout value plus the established network latency.

8. Click Apply to save the configuration changes.

- Click Apply and then OK to save the configuration changes.

End

5. Create Cluster control scripts.

Creating Cluster control scripts

Purpose

To create Cluster control scripts for each of the SIP Servers. The scripts are used to enable the Virtual IP port on the host on which the SIP Server is in primary mode and disable the Virtual IP port on the host on which the SIP Server is in backup mode.

In this procedure, you will create the following four Cluster control scripts:

- sip_server_primary_vip_up.bat—Enables the Virtual IP port on the primary SIP Server host
- sip_server_primary_vip_down.bat—Disables the Virtual IP port on the primary SIP Server host
- sip_server_backup_vip_up.bat—Enables the Virtual IP port on the backup SIP Server host
- sip_server_backup_vip_down.bat—Disables the Virtual IP port on the backup SIP Server host

Note: You can use the previously listed script names, or you can specify your own.

Start

1. On the primary SIP Server host computer, create a batch file that is named `sip_server_primary_vip_up.bat` and enter the following commands:
   [+] Commands for sip_server_primary_vip_up.bat

   ```
   @title Enable Cluster Control Script
   @echo ************** Primary Virtual IP Enabled ************** >>
   vip1.log
   @echo %time% >> vip1.log
   wlbs.exe start sipcluster:host1_ip >> vip1.log
   wlbs.exe enable 5060 sipcluster:host1_ip >> vip1.log
   wlbs.exe drainstop sipcluster:host2_ip >> vip1.log
   exit
   ```

   where:

   - `host1_ip` is the dedicated cluster IP address of the primary host
   - `host2_ip` is the dedicated cluster IP address of the backup host

2. On the primary SIP Server host computer, create a batch file that is named `sip_server_primary_vip_down.bat` and enter the following commands:
   [+] Commands for sip_server_primary_vip_down.bat

   ```
   @title Disable Cluster Control Script
   @echo *************** Primary Virtual IP Disabled ************ >>
   vip1.log
   @echo %time% >> vip1.log
   wlbs.exe drainstop sipcluster:host1_ip >> vip1.log
   ping -n 2 127.0.0.1
   exit
   ```

3. On the backup SIP Server host computer, create a batch file that is named `sip_server_backup_vip_up.bat` and enter the following commands:
   [+] Commands for sip_server_backup_vip_up.bat

   ```
   @title Enable Cluster Control Script
   @echo ************** Backup Virtual IP Enabled *************** >>
   vip2.log
   @echo %time% >> vip2.log
   wlbs.exe start sipcluster:host2_ip >> vip2.log
   wlbs.exe enable 5060 sipcluster:host2_ip >> vip2.log
   wlbs.exe drainstop sipcluster:host1_ip >> vip2.log
   exit
   ```

4. On the backup SIP Server host computer, create a batch file that is named `sip_server_backup_vip_down.bat` and enter the following commands:
   [+] Commands for sip_server_backup_vip_down.bat

   ```
   @title Disable Cluster Control Script
   @echo ***************** Backup Virtual IP Disabled *********** >>
   vip2.log
   @echo %time% >> vip2.log
   wlbs.exe drainstop sipcluster:host2_ip >> vip2.log
   ping -n 2 127.0.0.1
   exit
   ```

   Note: The preceding scripts include commands for logging script execution. The logs are created in the directory in which the script is located.

End

6. Creating Application objects for Cluster control scripts.

Creating Application objects for Cluster control scripts

Purpose

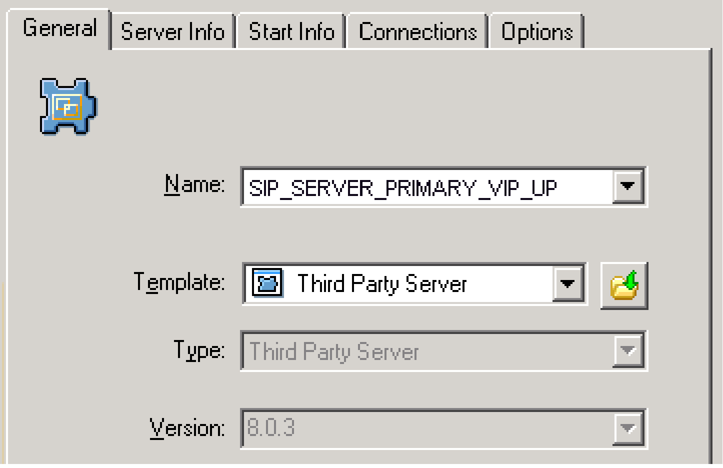
To create four Application objects of type `Third Party Server`: one for each of the Cluster control scripts that you created in Step 5. For example:

- `SIP_SERVER_PRIMARY_VIP_UP`—For a script that enables the Virtual IP port on the primary SIP Server host
- `SIP_SERVER_PRIMARY_VIP_DOWN`—For a script that disables the Virtual IP port on the primary SIP Server host
- `SIP_SERVER_BACKUP_VIP_UP`—For a script that enables the Virtual IP port on the backup SIP Server host
- `SIP_SERVER_BACKUP_VIP_DOWN`—For a script that disables the Virtual IP port on the backup SIP Server host

Creating Application objects for the Cluster control scripts allows the scripts to be run as applications within the Genesys Framework.

Start

1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the Third Party Server template from the Application Templates folder, and click `OK`.
4. On the `General` tab, enter the name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.



Name: SIP_SERVER_PRIMARY_VIP_UP

Template: Third Party Server

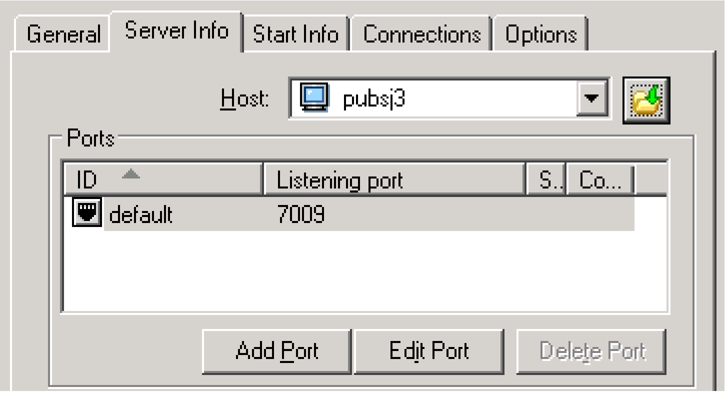
Type: Third Party Server

Version: 8.0.3

Configuring the Application Object for the Script, General Tab: Sample Configuration

Note: You can use the suggested Application object names, or you can specify your own.

5. Select the `Server Info` tab.
   a. Select the host name of the SIP Server on which the corresponding Cluster control script is located.
   b. If necessary, specify a valid communication-port number by using the `Edit Port` option.

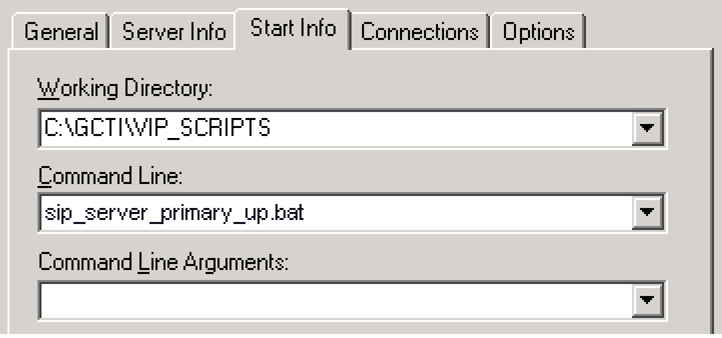


Host: pubsj3

ID	Listening port	S..	Co...
default	7009		

Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the `Start Info` tab.
   a. Set the `Working Directory` to the location of the control script, and enter the name of the script in the `Command Line` field. For example, for the SIP_SERVER_PRIMARY_VIP_UP Application object, enter the script name that enables the Virtual IP port (`sip_server_primary_up.bat`). For the SIP_SERVER_PRIMARY_VIP_DOWN Application object, enter the script name that disables the Virtual IP port (`sip_server_primary_down.bat`).



Working Directory: C:\GCTI\VIP_SCRIPTS

Command Line: sip_server_primary_up.bat

Command Line Arguments:

Configuring the Application Object for the Script, Start Info Tab: Sample Configuration

b. If you are configuring an Application object that disables a Virtual IP port (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the `Timeout Startup` value to 8.

3. Repeat the steps in this procedure to create an Application object for each of the four Cluster control scripts.

End

7. Create Alarm Reaction scripts.

Creating Alarm Reaction scripts

Purpose

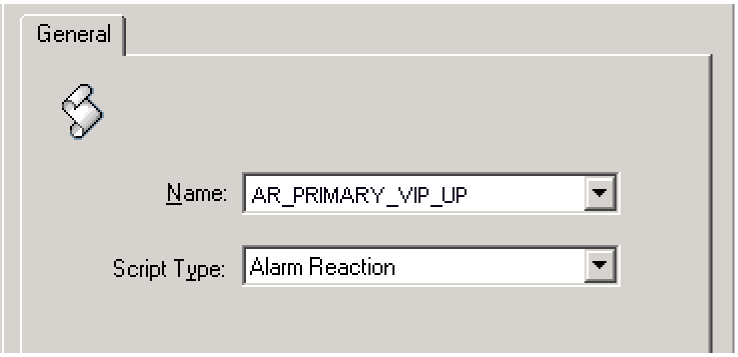
To create Alarm Reaction scripts for HA-related Alarm Conditions. When an HA-related Alarm Condition occurs, the associated Alarm Reaction script is run. Alarm Reaction scripts are configured to call the Application objects that you created in Step 6.

Start

1. Open the Configuration Manager.
2. Select `Resources > Scripts`.
3. Right-click and select `New > Script`.
4. Create four scripts: one for each of the Application objects that you created previously. For example:
   - `AR_SCRIPT_PRIMARY_VIP_UP`—To trigger a script that enables the Virtual IP address (to be run on the primary SIP Server host)
   - `AR_SCRIPT_PRIMARY_VIP_DOWN`—To trigger a script that disables the Virtual IP address (to be run on the primary SIP Server host)
   - `AR_SCRIPT_BACKUP_VIP_UP`—To trigger a script that enables the Virtual IP address (to be run on the

backup SIP Server host)

- AR_SCRIPT_BACKUP_VIP_DOWN—To trigger a script that disables the Virtual IP address (to be run on the backup SIP Server host)

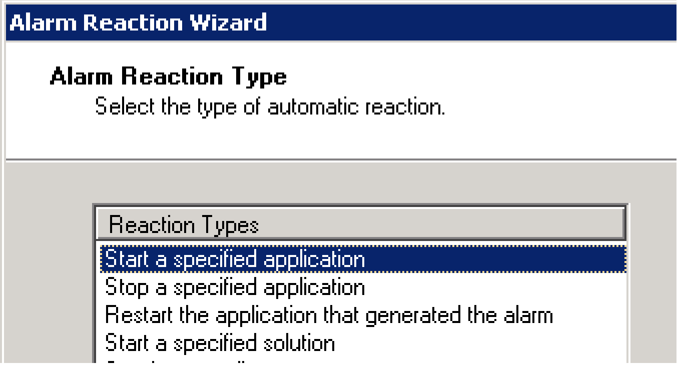


Name: AR_PRIMARY_VIP_UP

Script Type: Alarm Reaction

Configuring the Alarm Reaction Script: Sample Configuration

5. For each of the Alarm Reaction scripts, select Alarm Reaction as the Script Type.
6. For each of the Alarm Reaction scripts, use the Alarm Reaction Wizard to configure the Alarm Reaction Type.
   a. Select an Alarm Reaction script, and right-click to open the Alarm Reaction Wizard (select Wizard > Configure).
   b. In the Alarm Reaction Wizard, click Next.
   c. In the Alarm Reaction Type dialog box, select Start a specified application, and click Next.


Alarm Reaction Wizard

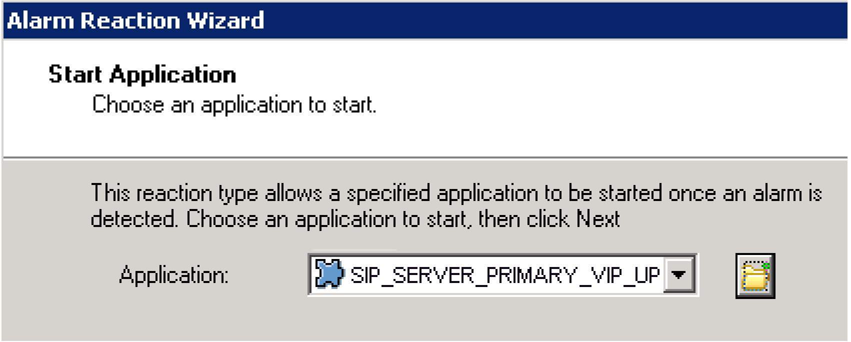
Alarm Reaction Type

Select the type of automatic reaction.

Reaction Types
Start a specified application
Stop a specified application
Restart the application that generated the alarm
Start a specified solution

Alarm Reaction: Selecting the Alarm Reaction Type

   d. Browse to select the corresponding Application object. For example, for the AR_SCRIPT_PRIMARY_VIP_UP Alarm Reaction script, select the SIP_SERVER_PRIMARY_VIP_UP Application object of type Third Party Server.


Alarm Reaction Wizard

Start Application

Choose an application to start.

This reaction type allows a specified application to be started once an alarm is detected. Choose an application to start, then click Next

Application: SIP_SERVER_PRIMARY_VIP_UP

Alarm Reaction: Selecting the Application to Start

e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in Step 4.

End

8. Create Alarm Conditions.

Creating Alarm Conditions

Purpose

Alarm Conditions are required to handle log events that occur when a SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you will configure them to trigger the Alarm Reaction scripts that you created in Step 7.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. The following table outlines the Alarm Conditions for both hot-standby and warm-standby configurations.

Alarm Conditions: Sample Configuration

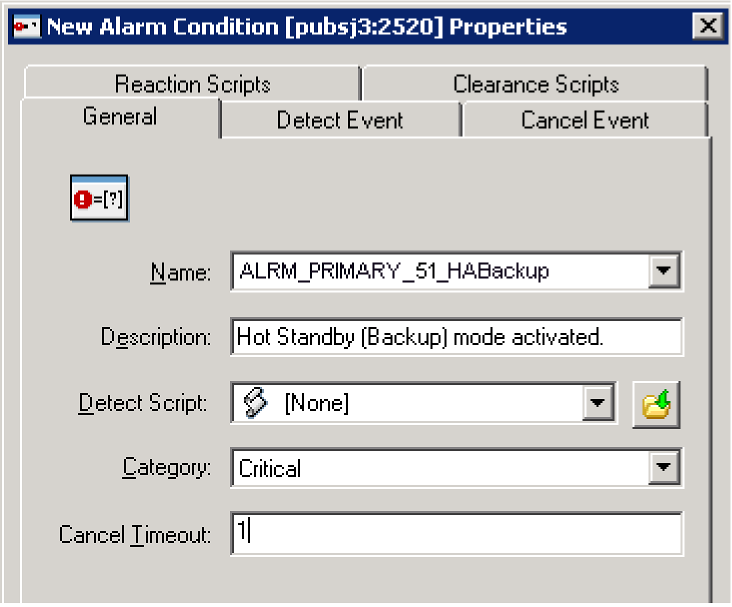
Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
00-05151	SIP_SERVER_PRIMARY	ALRM_PRIMARY_51_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
00-05150	SIP_SERVER_PRIMARY	ALRM_PRIMARY_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN AR_SCRIPT_PRIMARY_VIP_UP
00-05151	SIP_SERVER_BACKUP	ALRM_BACKUP_51_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
00-05150	SIP_SERVER_BACKUP	ALRM_BACKUP_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP AR_SCRIPT_PRIMARY_VIP_DOWN

For information about the log events for which you are creating Alarm Conditions, refer to Log events generated by SCS.

Start

1. Open the Configuration Manager.
2. Navigate to the `Environment > Alarm Conditions folder`.
3. Right-click and select `New > Alarm Condition` to open the `New Alarm Condition Properties` dialog box.

4. On the `General` tab:
   - Enter the Name for the Alarm Condition—for example, `ALRM_PRIMARY_51_HABackup`.
   - Optionally, enter a description.
   - For the `Category` value, select `Critical`.
   - Set `Cancel Timeout` to 1.



New Alarm Condition [pubsj3:2520] Properties

Name: ALRM_PRIMARY_51_HABackup

Description: Hot Standby (Backup) mode activated.

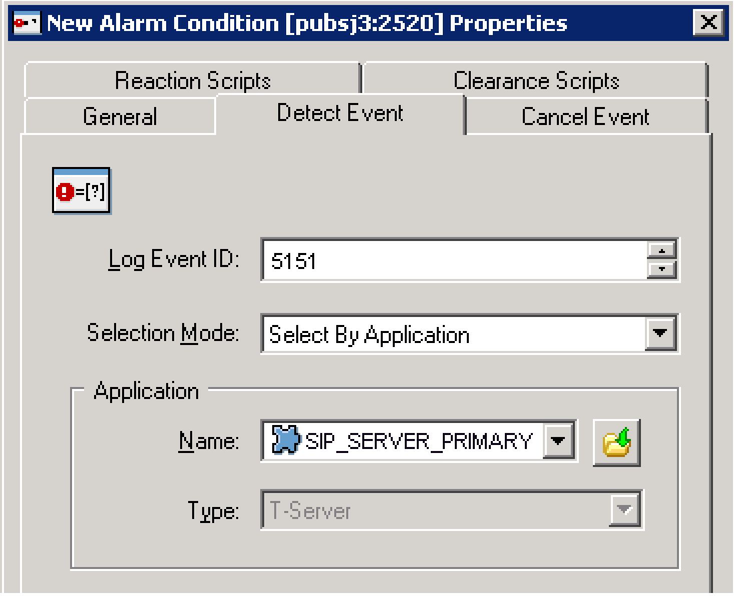
Detect Script: [None]

Category: Critical

Cancel Timeout: 1

Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the `Detect Event` tab:
   - Set the `Log Event ID` as defined in the table above.
   - Set the `Selection Mode` to `Select By Application`.
   - For the `Application Name` field, click the folder icon to browse for the SIP Server Application object. If you are creating an Alarm Condition for the primary SIP Server, select the primary SIP Server Application object. If you are creating an Alarm Condition for the backup SIP Server, select the backup SIP Server Application object.



Log Event ID: 5151

Selection Mode: Select By Application

Application

Name: SIP_SERVER_PRIMARY

Type: T-Server

Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the `Reaction Scripts` tab, add the Alarm Reaction script as defined in the previous table.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your configuration.

End

9. Test Alarm Conditions.

Testing Alarm Conditions

Purpose

To verify that the Alarm Conditions work as expected.

Start

1. Open the Solution Control Interface (SCI).
2. Under `Alarm Conditions`, select the Alarm Condition that you created in the previous procedure—for example, ALRM_PRIMARY_51_HABackup—right-click it, and then click `Test`. The ALRM_PRIMARY_51_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP portat the primary SIP Server and disable the Virtual IP port at the backup SIP Server.
3. Use an `wlbs queryport` command to verify that the Virtual IP port is disabled on the primary SIP Server

and that the Virtual IP port is enabled on the backup SIP Server.

End

10. Verify the HA configuration.

Testing your SIP Server HA configuration

Purpose

To validate your HA configuration, you can perform the following tests.

Prerequisites

- Ensure that the Management Layer is up and running.
- Start the primary SIP Server, and ensure that it is in primary mode.
- Start the backup SIP Server, and ensure that it is in backup mode.

Start

1. Test 1: Manual switchover
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 2: Manual switchback
    a. Establish a call between two SIP endpoints.
    b. Perform a manual switchover again by using the SCI. In the SCI, verify that the SIP Server roles have changed.
    c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.
    d. Release the call.

5. Test 3: Stop primary SIP Server
    a. Establish a call between two SIP endpoints.
    b. Stop the primary SIP Server. Use the SCI to verify that the backup SIP Server goes into primary

mode.

c. Verify that hold, retrieve, and transfer functions can be performed on the call that was established before the switchover.

d. Release the call.

End

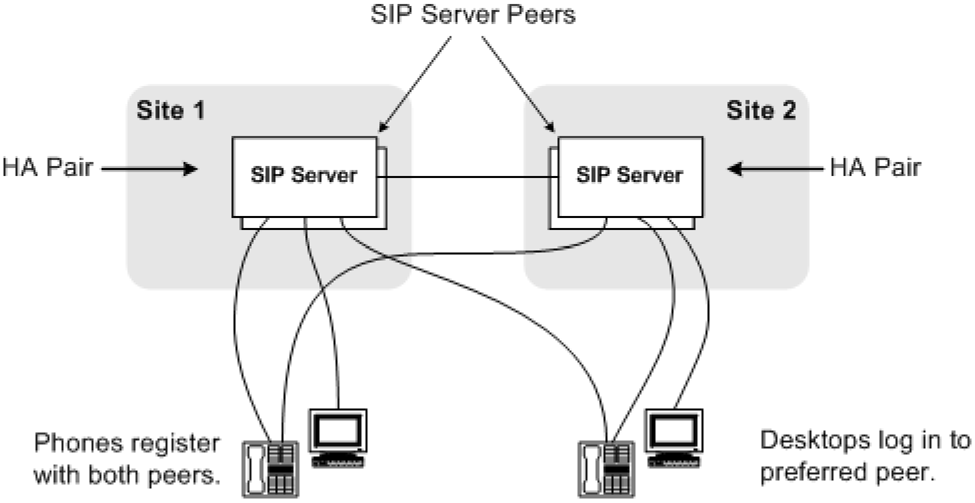
Business Continuity

This section contains information about SIP Business Continuity, which provides the ability for a group of agents to continue offering critical business functions to customers in the event of a loss of all Genesys components running at a particular site.

SIP Business Continuity Architecture

SIP Business Continuity provides the ability for a group of agents to continue offering critical business functions to customers in the event of a loss of all Genesys components running at a particular site. The SIP Business Continuity architecture uses a synchronized, two-site deployment, where Genesys switch and server components are mirrored at each site in an active-active configuration, so that any agent can log in to either switch, at any time.

The **Business Continuity Overview** figure shows the basic connections between SIP Server instances and endpoints across the redundant sites.


SIP Server Peers
Site 1
Site 2
HA Pair
SIP Server
SIP Server
HA Pair
Phones register with both peers.
Desktops log in to preferred peer.

Business Continuity Overview

What Does It Do?

SIP Business Continuity includes (though not limited to) the following functions:

- Work area redundancy
- Disaster Recovery
- Graceful Migration

For regular call processing, agent activity can be load-balanced across the two sites, or you can configure agents to use one preferred site over the other. In the event of a failure at one site (a SIP Server HA pair or all Genesys components go down), agents connected to the failed site are re-logged in automatically to the surviving site. Although any active calls on the failed site are terminated at the moment of failure (including calls on the surviving site that include the failed SIP Server in the signaling path), the surviving site is able to process all new calls, with minimal impact to queue wait times.

Note: Business Continuity does not provide recovery for the local failure of particular agent endpoints or workstations. It is intended to provide redundancy for Genesys components only.

Note: Alcatel-Lucent 4000-series IP Phones do not support dual registration. Instead, an active-backup registration scheme is used to handle disaster recovery scenarios. Special configuration for these phones is required. For more information, see Using IP Phones with SIP Server in Business Continuity Mode.

SIP Server Peers

A pair of primary and backup SIP Server instances are deployed at each site, providing local high availability (HA). For Business Continuity, these dual HA pairs are known as *SIP Server Peers*. The SIP Server Peers rely on synchronized configuration for all agent-related objects: `Extension` DNs, `Places`, `Agent Logins` (and the references to their related `User` or `Person` object). Each agent desktop is configured with a "Preferred Site", indicating to which site it should connect if possible.

Synchronizing Configuration Objects

Using Genesys Administrator, you can synchronize all agent-related configuration object (DNs of certain types, Places, Agent Logins and the reference to their associated User or Person) between the SIP Server Peers.

Synchronization applies to the following configuration objects:

- `ACD Position` DN
- `ACD Queue` DN
- `Call Processing Port` DN
- `Extension` DN
- `Agent Login`

After you run the synchronization once, Genesys Administrator will automatically synchronize any further configuration changes of Places and Users between the SIP Peers--as long as the changes are made using Genesys Administrator.

SIP Phones

Business Continuity only supports SIP endpoints that are able to maintain dual registrations--one registration for each site (Alcatel 4000-series phones are the exception). For outbound 1pcc calls, one of the sites is considered "preferred" based on either 3rd-party configuration on the phone itself, or based on DNS SRV record priority.

For Alcatel 4000-series phones, an active-backup registration scheme is used--where the phone registers to the SIP Server on the backup site only if the primary is unavailable.

For details, see Using IP Phones with SIP Server in Business Continuity Mode.

Agent Desktop

The agent desktop maintains a login to a single site at one time. Typically, the agent desktop logs into the "Preferred Site" specified in the desktop configuration, but it will log in to the other peer if both the preferred site is unavailable and the SIP endpoint switches registration to the backup site. The agent desktop maintains a basic connection (no login) to the backup peer site.

For more information, see the *Interaction Workspace 8.1 Deployment Guide*.

Call Delivery

During regular call processing, external media gateways distribute incoming traffic between the SIP Server Peers. Or optionally, an additional SIP Server or Network SIP Server can be deployed at the network level to provide intelligent pre-routing, or for scaling SIP Server Peers.

Each SIP Server Peer delivers routed calls, internal calls, direct inbound calls, and external calls to a particular agent through the SIP Server instance to which the agent is currently logged on. The agent initiates calls through the SIP Server where they are logged in.

- About the Call Forwarding Procedure
- Call Delivery - SIP Server Peer
- Call Delivery - Network SIP Server
- Call Delivery - Multi-Site

About the Call Forwarding Procedure

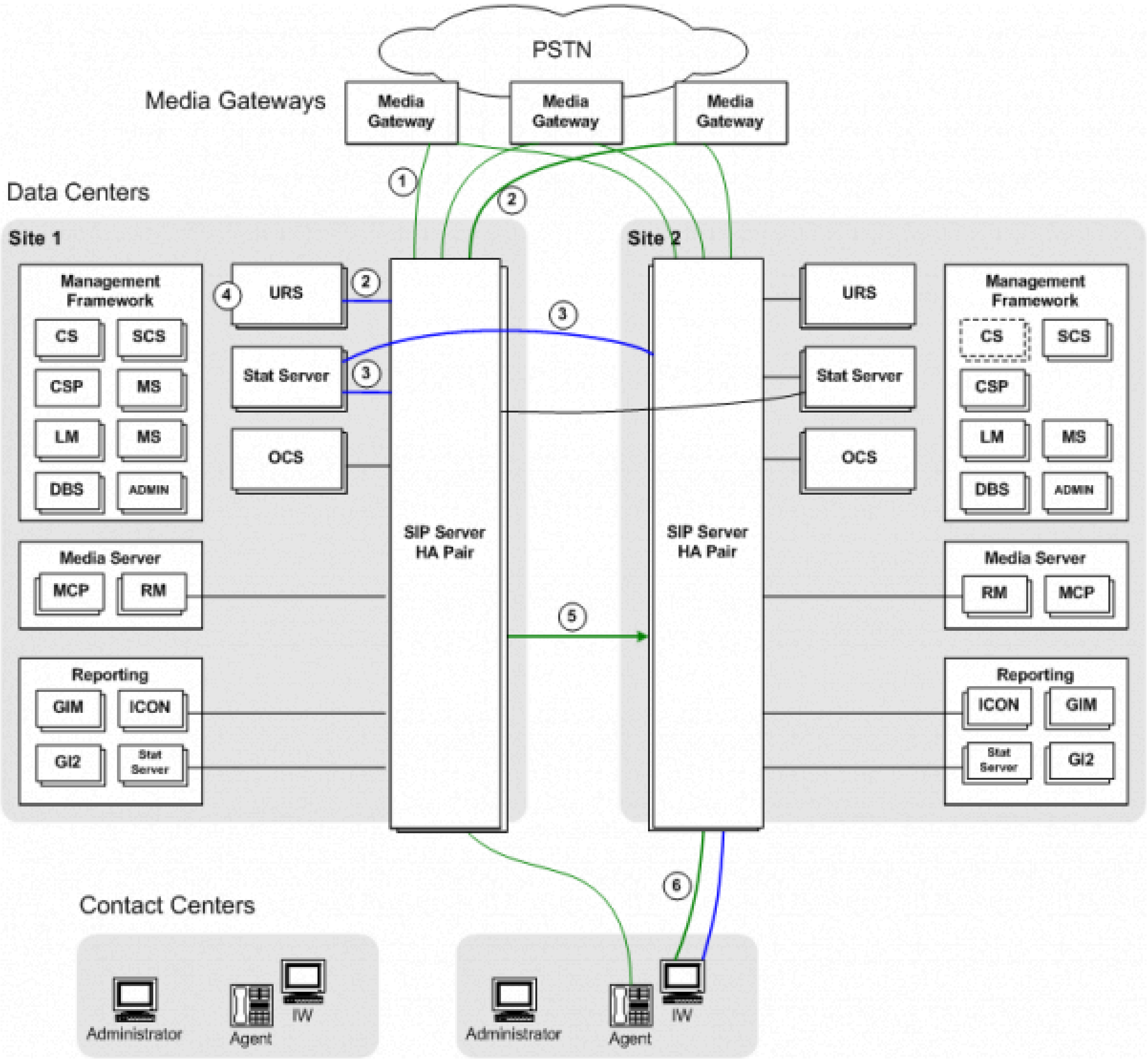
In case of a direct call to an agent phone number, Business Continuity takes special measures to make sure that the call is delivered to the DN where the agent's SIP phone is actually registered. Since agents can be registered on either SIP Server Peer site, the party that makes the call does not know the agent's current location, meaning the call can arrive at either SIP Server in the peer group. This SIP Server instance uses an internal call forwarding procedure to determine the location of the call destination (the agent phone number) and deliver the call there. This procedure ensures that the call is delivered to the site where T-Library messaging is linked to the logged in agent (identified as the `User` or `Person`), so that proper reporting takes place. The option `dr-forward` controls the rules for this call forwarding procedure.

The call forwarding procedure typically takes place as follows:

1. An inbound direct call arrives on SIP Server 1.
2. SIP Server 1 detects that the agent's phone is registered and accessible, but the agent is not logged in.
3. SIP Server 1 initiates an Out-of-Signaling-Path (OOSP) transfer--it sends a `302 Moved Temporarily` response back to the caller with the address of the DN on its SIP Server Peer.
4. The media gateway sends the secondary `INVITE` to SIP Server 2, targeting the same DN number.
5. SIP Server 2 processes the `INVITE` and tries to establish the call with the target. To prevent a forwarding loop, because the call has already been processed on SIP Server 1, SIP Server 2 will not forward the call back to that site, even if it turns out that the agent is not logged in on the SIP Server 2 site either.

Call Delivery - SIP Server Peers

The **Call Delivery, Direct to SIP Server Peer** figure shows a typical call flow for inbound call delivery to an agent, where the call arrives directly at the SIP Server Peer (no network-level SIP Server in the flow).



Call Delivery, Direct to SIP Server Peer

The following steps describe the call flow from media gateway to selected agent:

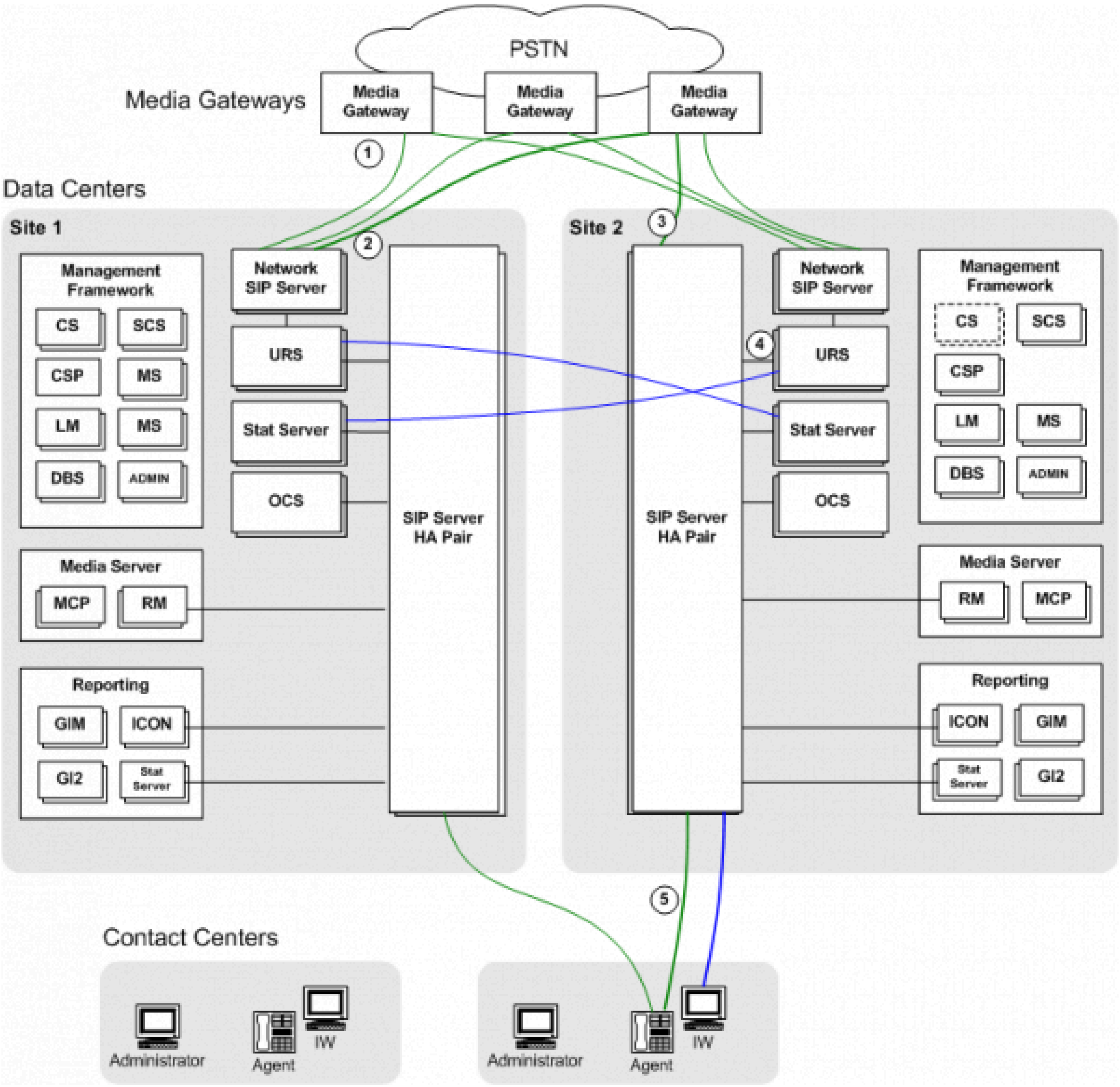
1. Media gateways distribute incoming traffic across both sites.
2. A call arrives at SIP Server on Site 1. SIP Server requests routing instructions from the Universal Routing Server (URS).
3. Each Stat Server monitors both SIP Server Peers. As such, the Stat Server on Site 1 is able to determine agent availability on both SIP Server Peers--agents can be logged in on either SIP Server Peer.
4. URS selects the appropriate agent to handle the call. In this example, the selected agent is logged in on the other SIP Server Peer site. URS sends a `TRouteRequest` to SIP Server, instructing it to route the call to the targeted agent.

Note: To route calls across sites (using Inter Server Call Control (ISCC)), Agent Reservation must be enabled. For more information, see the "Agent Reservation" section in the "T-Server Fundamentals" chapter of the SIP Server Deployment Guide. Also, see the *Universal Routing 8.1 Deployment Guide*.

1. As part of its internal Business Continuity Forwarding procedure, SIP Server first determines that the selected agent is not logged in locally. Based on this logic (and related option values that control the procedure), SIP Server then forwards the call to Site 2 through the specially configured inter-site Trunk DN, using ISCC routing.
2. The SIP Server Peer on Site 2 delivers the call to the agent.

Call Delivery - Network SIP Server

The **Call Delivery, Network SIP Server** figure shows a typical call flow for inbound call delivery to an agent, where the call first passes through a Network SIP Server.



Call Delivery, Network SIP Server

Note: The Network SIP Server in this architecture could be replaced with a Premise SIP Server instance, installed at the network level. In either case, Genesys recommends configuring default routing.

The following steps describe the call flow from media gateway to selected agent:

1. The media gateways distribute incoming traffic between Network SIP Server instances at the two sites. Network SIP Server, in conjunction with URS, can provide additional intelligence when deciding to which site to route the call. For example, routing can be configured to send a greater share of calls to whichever site currently has more logged in agents. Network SIP Server can also distribute calls across multiple SIP Server Peer groups, for scaled deployments.
2. The call arrives at the Network SIP Server on Site 1. URS at Site 1 determines that the call should go to Site 2, which currently has more agents logged in.

3. Network SIP Server sends a `302 Moved Temporarily` message to the media gateway. The media gateway sends a new `INVITE` to the SIP Server at Site 2.
4. URS at Site 2 selects the best agent to handle the call. In this example, the selected agent is logged in to Site 2.
5. URS sends a `TRouteRequest` to SIP Server, instructing it to route the call to the targeted agent. SIP Server establishes the call with the agent.

Call Delivery - Multi-Site

In cases where the deployment includes an external Genesys location in addition to the SIP Server Peers, the call is delivered to one of the SIP Server Peers, based on how the targeted Trunk is resolved. For example, if the `INVITE` through `Trunk1` arrives at SIP Server on Site 1, but the targeted agent DN is not found at this site, Business Continuity Forwarding is applied, and the call is forwarded to the other SIP Server Peer at Site 2.

For configuration details, see Deploying SIP Business Continuity With a Remote Site.

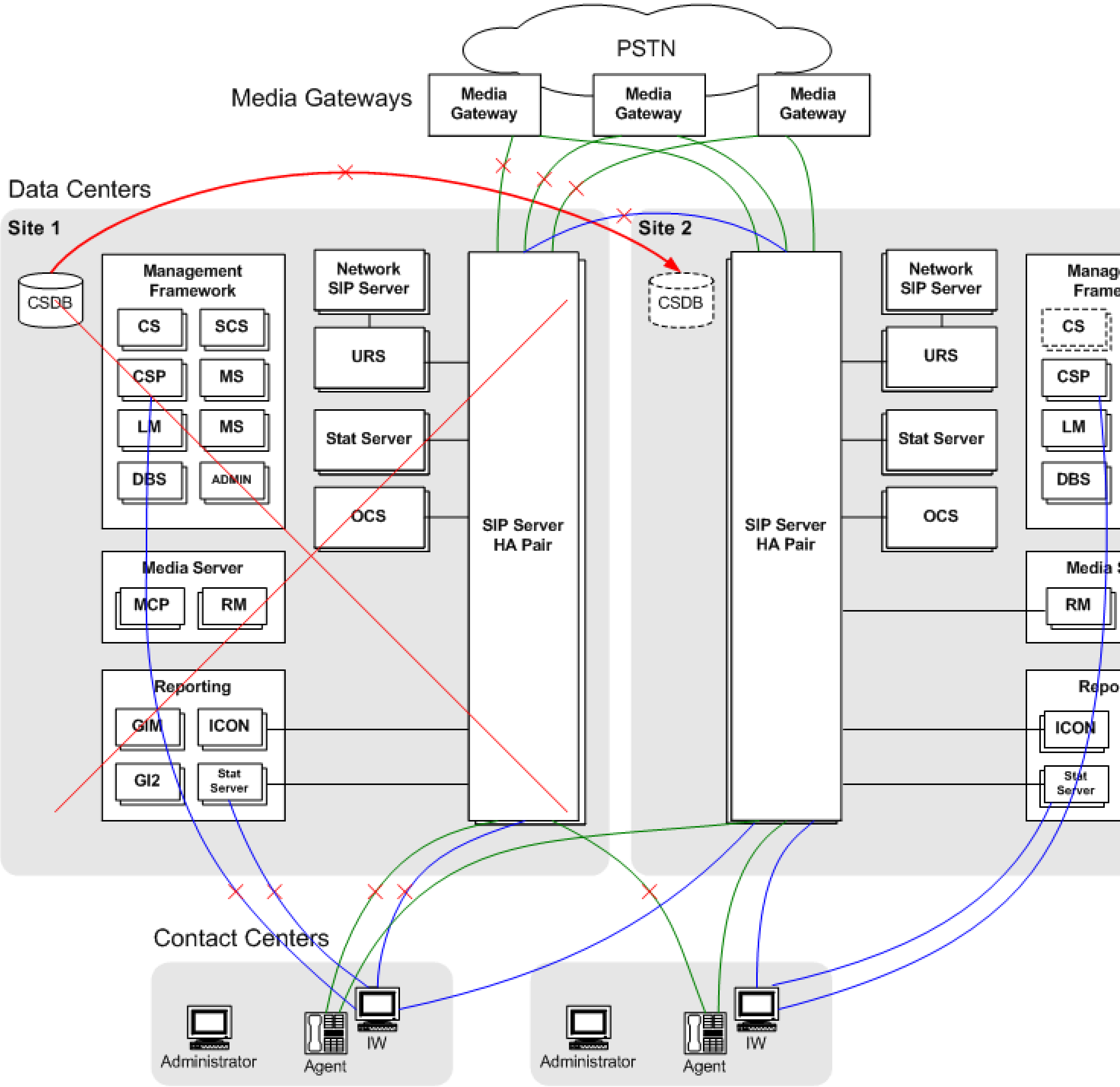
Disaster Recovery

In the event of the catastrophic failure of a particular site--in which all Genesys components become unavailable, including locally paired HA servers--peer site redundancy is used to provide ongoing support for all logged in agents. For those agents logged in to the surviving SIP Server Peer, their login remains unaffected and they can continue handling calls. For those agents that were logged in to the failed site, there is a temporary increase in queue wait times as these agents are logged in to the surviving site. Some loss of calls may occur at the failed site.

- Site Failure
- Networking Failure Between Sites

Site Failure

The **Site Failure** figure illustrates what typically happens when one site in a SIP Server Peer group suffers a catastrophic failure.



Site Failure

The following steps describe how Business Continuity recovers from a catastrophic failure of a particular SIP Server Peer site:

1. Site 1 suffers a catastrophic failure. All Genesys components, including paired HA servers, are

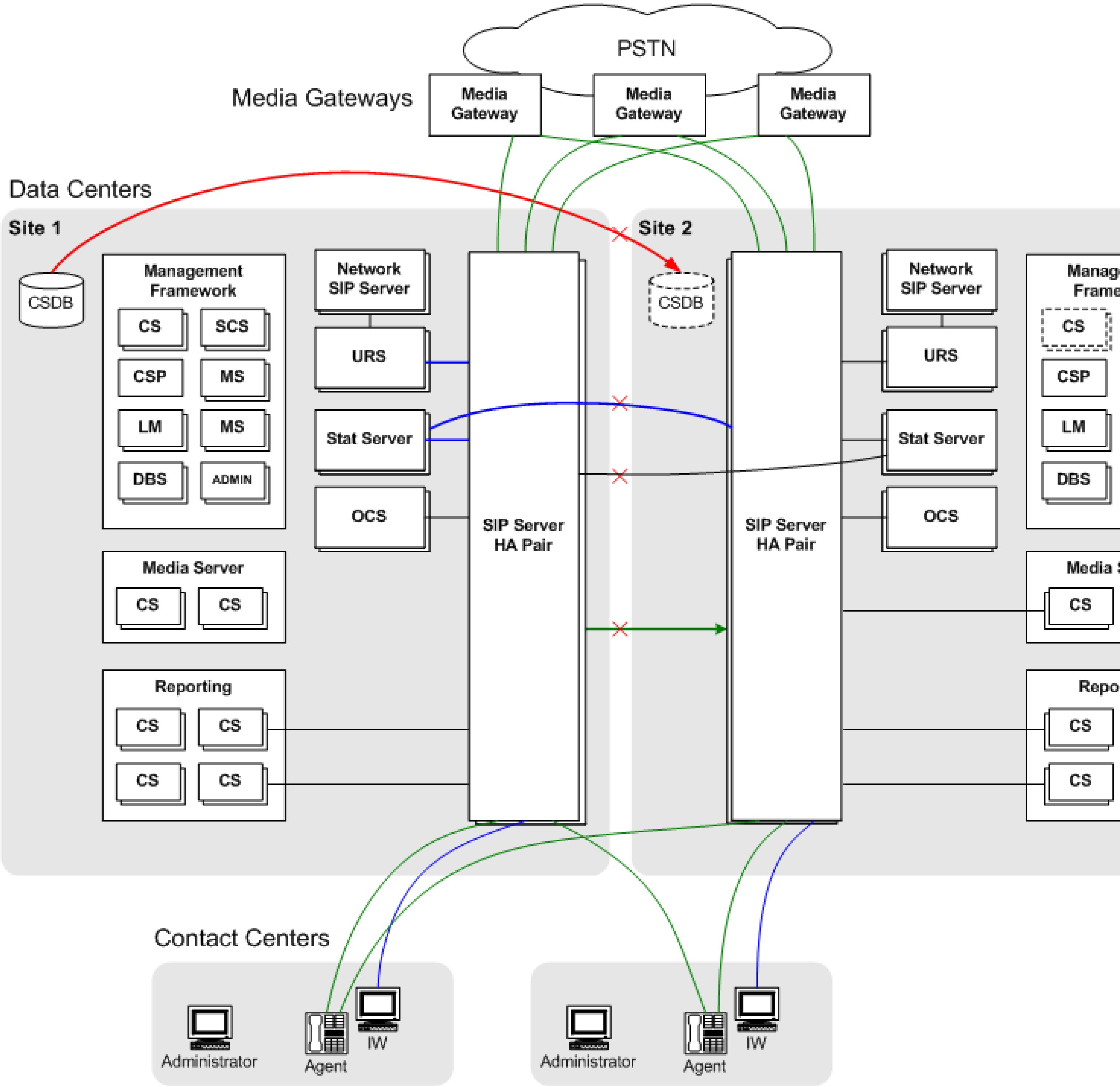
unavailable.

2. The media gateways detect a response timeout from Site 1. In response, the media gateways begin sending all new calls to Site 2.
   If the media gateway itself is affected by the disaster outage, the PSTN should detect this; load-balancing at the gateway level should redirect calls to the surviving media gateways.
3. Agents that are currently logged in to Site 2 continue to handle calls. Queue wait times increase temporarily.
4. The agent's SIP phone responds in either of the following ways:
   - If the phone is configured to register on one site only, it re-registers now on the Site 2 SIP Server.
   - If the phone is configured for dual-registration, the phone automatically switches call handling from the local site to the backup site (Site 2).

   Agent desktops detect Site 1 failure, and re-login automatically to the SIP Server on Site 2. In addition, the desktop establishes connections to the Stat Server and Configuration Server Proxy on Site 2.
5. The standby Configuration Server and Configuration Server Database as Site 2 are brought into service.
6. When the surviving SIP Server detects that its peer is failed, it continues operation in single-site mode, stopping Business Continuity functions as follows:
   - It no longer applies the call forwarding procedure to new calls.
   - It allows agents to log in independently of the status of their endpoint.
   - It does not employ the forced logout procedure

Networking Failure Between Sites

The **Networking Failure** figure illustrates what typically happens when a networking failure occurs between SIP Server Peer sites.



Networking Failure

The following steps describe how Business Continuity recovers from a networking failure between the SIP Server Peer sites:

1. In this example, network connectivity between the two data center sites is lost. SIP Server detects this

failure through Active Out of Service detection (options `oos-check` and `oos-force`) of the inter-site `Trunk` DN. Connectivity between the media gateways and contact centers at each site are still available.

2. The SIP Server instances at each site revert to their normal non-peered operation.
3. Incoming calls at each site are routed only to agents logged in at that site--Business Continuity Forwarding does not apply.
4. In this case, the Business Continuity solution avoids any "split-brain" problems because there are no longer any inter-dependencies between the sites.
5. For short-term outages, the Configuration Server Proxy on Site 2 provides configuration data to local Site 2 applications. For longer outages, Site 2 Configuration Server and Configuration Server Database can be brought into service.
6. When the surviving SIP Server detects that its peer is failed, it continues operation in single-site mode, stopping Business Continuity functions as follows:
    - It no longer applies the call forwarding procedure to new calls.
    - It allows agents to log in independently of the status of their endpoint.
    - It does not employ the forced logout procedure

Graceful Migration

Business Continuity supports the graceful migration of operations from two active SIP Server Peer sites to a single site, in cases where one full site needs to be taken offline or powered off--for example, to perform maintenance on an entire data center. The goal of graceful migration is to gradually move all business activity to the second site with no lost calls. Agents must migrate to the second site.

To start a graceful migration, you first configure your environment to stop sending calls to the SIP Server Peer site that you intend to shutdown. Using Genesys Administrator, you then initiate a graceful shutdown of the SIP Server itself, in which SIP Server stops accepting new calls, while still allowing any ongoing calls to finish, ensuring that no calls are dropped when this SIP Server instance is finally stopped.

Assuming that Site 2 is going to be taken offline, the overall procedure for graceful migration is follows:

1. Configure the media gateways to stop sending new calls to Site 2.
2. Configure the routing strategy to stop sending new calls to Site 2.
3. Initiate the graceful shutdown procedure for SIP Server. You can initiate this in one of two ways:
   - Using Genesys Administrator, initiate the graceful shutdown procedure from the SIP Server `Application` object.
   - Sending a `TPrivateRequest` with `serviceid=3019` from a T-Library client.

   Either of these actions starts the SIP Server graceful shutdown process.
4. All agents are forcedly moved into the `NotReady` state. New calls can no longer be distributed to these agents.
5. All new `INVITE` requests are rejected with a configurable error response (the option `shutdown-sip-reject-code`). All new calls initiated by T-Library requests are rejected.
6. Agents on this SIP Server instance are forcedly logged out as they end their calls with an appropriate reason code. Once there are no more calls on this SIP Server, it shuts down.
7. If the agents use Genesys Interaction Workspace, then they are logged in automatically at Site 1. SIP Server at Site 1 now handles all calls.

Deploying SIP Business Continuity

This pages describes how to deploy SIP Business Continuity in different scenarios, environments, and modes:

Basic Deployment

Use these procedures to set up basic SIP Business Continuity.

Deploying Basic SIP Continuity

Setup a Remote Site

Use these additional procedures to include a remote site in the continuity setup.

Deplying SIP Continuity With a Remote Site

Basic Deployment

The following tasks are required to deploy basic SIP Business Continuity in your environment. Unless otherwise stated, refer to the Framework 8.1 SIP Server Deployment Guide for information about the configuration options.

Deploying Basic SIP Business Continuity

1. Create the peer switch.

For each DR pair required, use the Sync Switch Wizard in Genesys Administrator to create a new peer switch or use an existing switch as the peer. Each switch in the DR pair must be located at a separate site. The Wizard sets up the switches as peers, synchronizes switch-related elements between them, and then keeps them synchronized.

For remote agents, before using the Sync Switch Wizard in Genesys Administrator to create a new peer switch:

1. Configure the `contact` option with the value equal the FQDN of the media gateway for all remote agent DNs or a softswitch.
2. Configure local DNS servers for each peer to resolve this FQDN to respective gateway addresses.

> **Important**
>
> The switches are not synchronized automatically for changes made outside of Genesys Administrator. However, you can re-synchronize these switches at any time by using the Sync Switch Wizard. For more information about the Sync Switch Wizard, refer to *Genesys Administrator 8.1 Help*.

2. Interconnect the DR peers.

On each DR peer:

1. Configure a `Trunk` DN pointing to the other peer.
2. Assign to each DN a unique prefix that does not match a possible dialed number to avoid the DN being mistaken for use by an outbound call. The options `oos-check` and `oos-force` must be configured to enable Active Out Of Service Detection.
   Note: Use the names of these DNs when configuring the Application option `dr-peer-trunk`.

3. Set the dr-peer-location option to the name of the Switch object of the other SIP Server in the DR pair.
4. Do not configure the auto-redirect-enabled option.

3. Configure ISCC COF between the DR peer switches.

Refer to the Framework 8.1 SIP Server Deployment Guide for instructions.Set the following options in the extrouter section on each SIP Server:

- cof-feature=true
- default-network-call-id-matching=sip

4. Set up default routing.

Do one or both of the following, as appropriate:

- If you are using premise SIP Servers at the network level, use the configuration options router-timeout and default-dn.
- If you are using Network SIP Servers, use the configuration option default-route-destination.

5. Configure routing from premise to peer.

On each premise SIP Server, use the configuration option dr-peer-trunk to identify that the SIP Server is a part of a DR pair, and to identify the Trunk DN that points to the other SIP Server in the pair. Genesys also recommends the following:

- Add the addresses of both DR peers to the list of addresses in the option enforce-external-domains, to ensure that the call parties are properly recognized based on the Host element of the contacts.
- Use the option dr-forward at the Application or DN level to define the mode of forwarding inbound and internal calls when SIP Server is operating in Business Continuity mode. Set this option to one of the following values, as appropriate:
  - no-agent—for call center deployments or for an agent's DNs
  - oos—for Alcatel-Lucent and Bria IP phones that do not support simultaneous registrations on two sites
  - off—for office (that is, non-agent) deployments of endpoints

6. (Optional) Configure the preferred site for agents.

Interaction Workspace (IW) supports preferred-site connections for agents. Other agent desktops must use the same mechanism as used by IW for configuring preferred-site connections. For configuration details, see the *Interaction Workspace 8.1 Deployment Guide*.

DR Peer and Remote Site Deployment

The following tasks describe the steps necessary to deploy SIP Business Continuity in the following scenario:

- Two sites, S1 and S2, are configured as a DR peer. You want to call the agents in the DR peer from a third site S3.

Unless otherwise stated, refer to the Framework 8.1 SIP Server Deployment Guide for information about the configuration options.

Deploying SIP Business Continuity With a Remote Site

1. Configure sites S1 and S2 as DR peers.

See Basic Deployment.

2. Configure two trunks on the third switch, one each to the other switches in the DR pair.

1. On the third switch, configure two Trunk DNs, and configure the **contact** option on each DN as follows:
   - First DN: **contact**=<FQDN of DR peer>
   - Second DN: **contact**=<FQDN of DR peer>
2. On both DNs, do no configure the **auto-redirect-enabled** option.

All other options can remain the same. However, if you want, you can use the options **priority** and **capacity** to indicate the preference of one trunk over the other.

3. Configure ISCC COF between DR peer switches.

Configure ISCC COF access between the following sites:

- The remote site and the first DR pair site.
- The remote site and the second DR pair site.

Refer to the Framework 8.1 SIP Server Deployment Guide for instructions. Set the following options in the `extrouter` section on each SIP Server:

- **cof-feature**=`true`
- **default-network-call-id-matching**=`sip`

Configuration Options

This section describes configuration options that are used in the deployment of SIP Business Continuity. All options are in the TServer section, and unless otherwise specified, are set at the Application level.

dr-forward

Default Value: off
Valid Values:

- off -- DR peer forwarding is turned off. SIP Server works in the traditional single mode and always tries to deliver the call to the requested destination on the local switch.
- no-agent -- SIP Server tries to determine if the call should be forwarded to its DR peer when there is no agent logged into the DN.
  Note: Use this setting for only ALU 4000-series IP Phones. Contact Genesys Technical Support if you want to utilize it for other SIP endpoints.
- oos -- SIP Server forwards the call to the second SIP Server peer if an endpoint is in an Out-Of-Service (OOS) state.

Changes Take Effect: Immediately

Defines a system-wide mode of forwarding inbound and internal calls when SIP Server is operating in Business Continuity mode. This option can also be set at the DN level, in which case the setting overrides that set at the Application level.

dr-peer-trunk

Default Value: NULL
Valid Values: A valid name of a Trunk DN that points to the DR peer site.
Changes Take Effect: Immediately

Specifies that this SIP Server is a part of a DR pair, and identifies the Trunk DN that points to the other SIP Server in the DR pair. If set to NULL (the default), SIP Server operates in the traditional single mode.

shutdown-sip-reject-code

Default Value: 603
Valid Values: 300–603
Changes Take Effect: Immediately

Specifies the error response used for rejecting new INVITE messages received by the system that is in shutdown mode. If set to 300, 301, or 302, SIP Server first checks to see if dr-peer-trunk is configured, and if so, sends the contact of that Trunk DN in the 302 response.

Using IP Phones

This section describes how SIP endpoints, such as IP Phones, work with SIP Server in Business Continuity mode.

Supported IP Phones

The following is a list of IP Phones that can be configured to support SIP Business Continuity, with the actual model that was tested in parentheses:

- CounterPath Bria 3.x IP Phones (Bria 3.0)
- Polycom SoundPoint IP Phones using firmware version 3.2 or later (Polycom SoundPoint IP330 with firmware version 3.2)
- Alcatel-Lucent (ALU) 4000-series IP Phones with SIP version 2.10.80 or later (ALU 4008/4018 with SIP version 2.10.80)

Note: Advanced IP Phone features, such as Presence and MWI, are not available in SIP Business Continuity Mode.

Refer to device-specific documentation for detailed information and instructions for configuring the phone.

Registration Requirements

In a stand-alone SIP Server configuration with Business Continuity mode activated, agents' phones must be able to register on two sites in one of the following ways:

- Simultaneously--Register on both peer Sip Servers at the same time.
- Sequentially--Register on the main peer SIP Server first; if that peer SIP Server is down, then register on the secondary peer SIP Server.

There are also specific Configuration Server configuration requirements for SIP endpoints. In the following situations, the `dr-forward` must be set to `oos`:

- When SIP endpoints are configured to register sequentially.
- When Bria or ALU IP Phones are configured.

Using Siemens OSV

SIP Server integrated with Siemens OpenScape Voice version 5 can be configured in Business Continuity mode. You must configure the option `dr-forward`=`no-agent` on the Application or DN (`Voice over IP Service` DN with `service type=softswitch`) when you configure SIP Server.

See the *Framework 8.1 SIP Server Integration Reference Manual* for information and instructions about configuring the Siemens OpenScape Voice PBX.

Log Events

To launch the Virtual IP address control scripts or Cluster control scripts on SIP Server host, configure the Alarm Conditions to execute Alarm Reaction scripts, which instructs the Management Layer by using the Application objects.

This configuration aligns the IP configuration of the host computer with the run mode of the respective SIP Server application, enabling the switchover process to be completed successfully.

The following log events, which are relevant to SIP Server HA hot- and warm-standby configurations, respectively, are fully described in the *Framework 8.1 Combined Log Events Help*.

Log Events Generated by SCS

SCS generates the following log events when an application changes run modes (from backup to primary or from primary to backup):

`00-05150`
Level: Standard
Text: The run mode of the Application is changed to Primary
Attributes: None
Description: Solution Control Server (SCS) generates this log event on behalf of any application when the application starts to run in Primary mode.

`00-05151`
Level: Standard
Text: The run mode of the Application is changed to Backup
Attributes: None
Description: Solution Control Server (SCS) generates this log event on behalf of any application when the application starts to run in Backup mode.