



Framework 8.0

SIP Server

**High-Availability Deployment
Guide**

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

Copyright © 2010 Genesys Telecommunications Laboratories, Inc. All rights reserved.

About Genesys

Alcatel-Lucent's Genesys solutions feature leading software that manages customer interactions over phone, Web, and mobile devices. The Genesys software suite handles customer conversations across multiple channels and resources—self-service, assisted-service, and proactive outreach—fulfilling customer requests and optimizing customer care goals while efficiently using resources. Genesys software directs more than 100 million customer interactions every day for 4,000 companies and government agencies in 80 countries. These companies and agencies leverage their entire organization, from the contact center to the back office, while dynamically engaging their customers. Go to www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Genesys, the Genesys logo, and T-Server are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other trademarks and trade names referred to in this document are the property of other companies. The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support at the regional numbers provided on [page 8](#). For complete contact information and procedures, refer to the [Genesys Technical Support Guide](#).

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the [Genesys Licensing Guide](#).

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 80fr_dep-sip_ha_12-2010_v8.0.401.00



Table of Contents

List of Procedures	5
Preface	7
About SIP Server.....	7
Intended Audience.....	7
Reading Prerequisites	8
Making Comments on This Document	8
Contacting Genesys Technical Support.....	8
Document Change History	9
Chapter 1	SIP Server High-Availability Architecture 11
Overview.....	11
High-Availability Redundancy Types	13
IP Address Takeover HA Configuration	14
Windows and UNIX Platforms	14
IP Address Takeover HA Notes	17
Windows NLB Cluster HA Configuration	17
Network Device-Based HA Configuration.....	19
Other SIP Server HA Enhancements	21
Single Host HA Deployment	21
Synchronization of Contact Between SIP Server HA Pair	21
SIP Traffic Monitoring	21
Chapter 2	SIP Server High-Availability Workflows 23
IP Address Takeover HA Workflows.....	23
Manual-Switchover Workflow	24
Primary Server–Failure Workflow	26
Primary Server-Disconnected Workflow	27
Windows NLB Cluster HA Workflows	29
Manual-Switchover Workflow	30
Primary Server–Failure Workflow	31
Primary Server-Disconnected Workflow 1	32
Primary Server-Disconnected Workflow 2	34

Chapter 3	SIP Server High-Availability Deployment.....	37
	IP Address Takeover HA Deployment on Windows.....	37
	Task Summary: IP Address Takeover HA Deployment on Windows ..	37
	Prerequisites	39
	Deployment Procedures	40
	IP Address Takeover HA Deployment on AIX	59
	Task Summary: IP Address Takeover HA Deployment on AIX.....	59
	Prerequisites	60
	Deployment Procedures	61
	IP Address Takeover HA Deployment on Solaris	76
	Task Summary: IP Address Takeover HA Deployment on Solaris.....	76
	Prerequisites	77
	Deployment Procedures	78
	IP Address Takeover HA Deployment on Linux.....	93
	Task Summary: IP Address Takeover HA Deployment on Linux	93
	Prerequisites	94
	Deployment Procedures	95
	Windows NLB Cluster HA Deployment	111
	Task Summary: Windows NLB Cluster HA Deployment.....	111
	Prerequisites	112
	Deployment Procedures	113
	SIP Server HA Configuration Testing	130
Appendix	SIP Server HA Log Events	133
Supplements	Related Documentation Resources	135
	Document Conventions	137
Index	139



List of Procedures

Configuring the primary SIP Server (IP Address Takeover on Windows)	40
Configuring the backup SIP Server (IP Address Takeover on Windows)	43
Creating Virtual IP address control scripts (IP Address Takeover on Windows)	45
Testing Virtual IP address control scripts (IP Address Takeover on Windows)	49
Creating Application objects for Virtual IP address control scripts (IP Address Takeover on Windows)	51
Creating Alarm Reaction scripts (IP Address Takeover on Windows)	53
Creating Alarm Conditions (IP Address Takeover on Windows)	55
Testing Alarm Conditions (IP Address Takeover on Windows)	58
Configuring the primary SIP Server (IP Address Takeover on AIX)	61
Configuring the backup SIP Server (IP Address Takeover on AIX)	64
Updating the /etc/hosts file (IP Address Takeover on AIX)	67
Creating Virtual IP address control scripts (IP Address Takeover on AIX)	67
Creating Application objects for Virtual IP address control scripts (IP Address Takeover on AIX)	68
Creating Alarm Reaction scripts (IP Address Takeover on AIX)	70
Creating Alarm Conditions (IP Address Takeover on AIX)	72
Testing Alarm Conditions (IP Address Takeover on AIX)	75
Configuring the primary SIP Server (IP Address Takeover on Solaris)	78
Configuring the backup SIP Server (IP Address Takeover on Solaris)	81
Updating the /etc/hosts file (IP Address Takeover on Solaris)	84
Creating Virtual IP address control scripts (IP Address Takeover on Solaris)	84
Creating Application objects for the Virtual IP address control scripts (IP Address Takeover on Solaris)	85
Creating Alarm Reaction scripts (IP Address Takeover on Solaris)	87
Creating Alarm Conditions (IP Address Takeover on Solaris)	89

Testing Alarm Conditions (IP Address Takeover on Solaris)	92
Configuring the primary SIP Server (IP Address Takeover on Linux) . .	95
Configuring the backup SIP Server (IP Address Takeover on Linux). . .	98
Updating the /etc/hosts file (IP Address Takeover on Linux)	101
Creating a configuration file for the Virtual IP interface (IP Address Takeover on Linux).	101
Creating Virtual IP address control scripts (IP Address Takeover on Linux).	102
Creating Application objects for Virtual IP address control scripts (IP Address Takeover on Linux).	103
Creating Alarm Reaction scripts (IP Address Takeover on Linux)	105
Creating Alarm Conditions (IP Address Takeover on Linux)	107
Testing Alarm Conditions (IP Address Takeover on Linux)	110
Configuring Windows NLB cluster parameters.	113
Configuring the primary SIP Server (Windows NLB Cluster)	114
Configuring the backup SIP Server (Windows NLB Cluster)	117
Creating Cluster control scripts (Windows NLB Cluster)	120
Creating Application objects for Cluster control scripts (Windows NLB Cluster)	122
Creating Alarm Reaction scripts (Windows NLB Cluster).	124
Creating Alarm Conditions (Windows NLB Cluster)	126
Testing Alarm Conditions (Windows NLB Cluster).	129
Testing your HA configuration	130



Preface

Welcome to the *Framework 8.0 SIP Server High-Availability Deployment Guide*. This document introduces 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 8.0 SIP Server Deployment Guide* during the deployment planning.

This preface contains the following sections:

- [About SIP Server, page 7](#)
- [Intended Audience, page 7](#)
- [Making Comments on This Document, page 8](#)
- [Contacting Genesys Technical Support, page 8](#)
- [Document Change History, page 9](#)

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on [page 135](#).

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

This document is 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 8.0 SIP Server Deployment Guide* before you use this document. That book contains information about the SIP Server deployment in general.

Making Comments on This Document

If you especially like or dislike anything about this document, feel free to e-mail your comments to Techpubs.webadmin@genesyslab.com.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or Genesys Technical Support, if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way that it believes appropriate, without incurring any obligation to you.

Contacting Genesys Technical Support

If you have purchased support directly from Genesys, contact Genesys Technical Support at the following regional numbers:

Region	Telephone	E-Mail
North America and Latin America	+888-369-5555 (toll-free) +506-674-6767	support@genesyslab.com
Europe, Middle East, and Africa	+44-(0)-1276-45-7002	support@genesyslab.co.uk
Before contacting technical support, refer to the <i>Genesys Technical Support Guide</i> for complete contact information and procedures.		

Region	Telephone	E-Mail
Asia Pacific	+61-7-3368-6868	support@genesyslab.com.au
Malaysia	1-800-814-472 (toll-free) +61-7-3368-6868	support@genesyslab.com.au
India	000-800-100-7136 (toll-free) +91-(022)-3918-0537	support@genesyslab.com.au
Japan	+81-3-6361-8950	support@genesyslab.co.jp
Before contacting technical support, refer to the <i>Genesys Technical Support Guide</i> for complete contact information and procedures.		

Document Change History

This is the first release of the *Framework 8.0 SIP Server High-Availability Deployment Guide*. In the future, this section will list topics that are new or have changed significantly since the first release of this document.



Chapter

1

SIP Server High-Availability 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.

This chapter provides an overview SIP Server high-availability architecture configurations and contains the following sections:

- [Overview, page 11](#)
- [IP Address Takeover HA Configuration, page 14](#)
- [Windows NLB Cluster HA Configuration, page 17](#)
- [Network Device-Based HA Configuration, page 19](#)
- [Other SIP Server HA Enhancements, page 21](#)

Overview

SIP Server supports several high-availability deployment options:

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

[Table 1](#) summarizes SIP Server HA options, their benefits and limitations, and supported operating systems (Windows, Linux, Solaris, or AIX).

Table 1: Comparing High-Availability Options

High Availability Option	Benefits	Limitations
IP Address Takeover	<ul style="list-style-type: none"> Supported on all operating systems Supports multiple NICs 100% Genesys components HA option of choice for reliability ratings and tests 	<ul style="list-style-type: none"> Supports a single subnet Operations on both servers, backup and primary, must succeed Subnet equipment to accept gratuitous ARP
Windows NLB Cluster	<ul style="list-style-type: none"> Widely deployed Thoroughly documented Supports multiple NICs 	<ul style="list-style-type: none"> Supports a single subnet Complexity/Prerequisites Dedicated switch/VLAN
F5 Networks BIG-IP LTM	<ul style="list-style-type: none"> Reliability Flexibility (HA and Load balancing) Supports multiple NICs 	<ul style="list-style-type: none"> 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.

High-Availability 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 Genesys Configuration Manager 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 Chapter 3, “SIP Server High-Availability Deployment,” on [page 37](#).

Hot- and warm-standby redundancy types are described in more detail in the following sections.

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 HA Configuration

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.

[Figure 1](#) shows an IP Address Takeover configuration on the Linux or Solaris platform using 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.

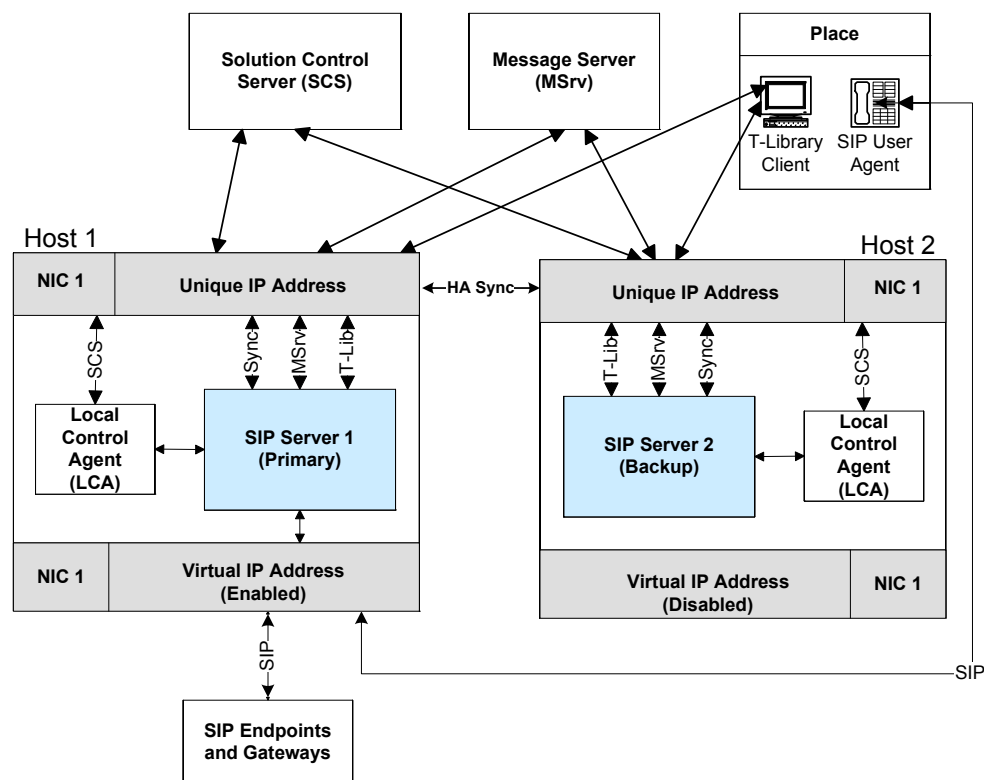


Figure 1: SIP Server HA IP Address Takeover Configuration with One NIC

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

[Figure 2](#) shows an IP Address Takeover configuration using two NICs on the Windows platform.

In a deployment with two NICs, one NIC (NIC 2 in [Figure 2](#)) is used for the SIP communication, while the second NIC (NIC 1 in [Figure 2](#)) 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” on [page 21](#).)

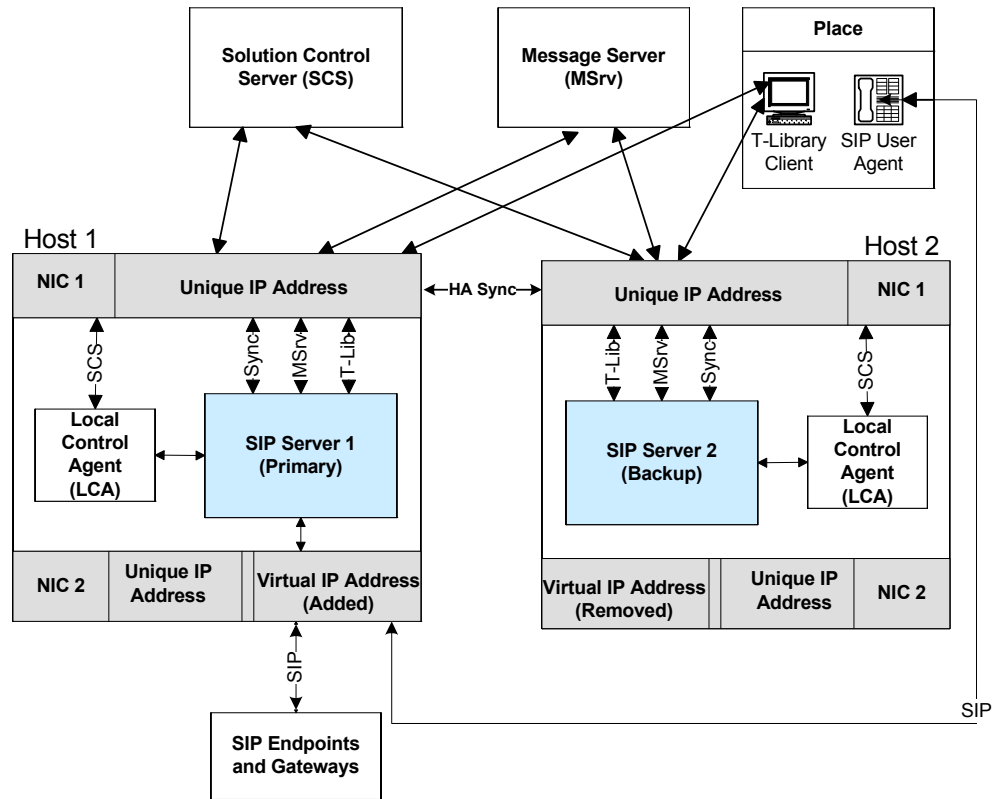


Figure 2: SIP Server HA IP Address Takeover Configuration with Two NICs

See the “IP Address Takeover HA Workflows” on [page 23](#) for step-by-step descriptions of manual switchover, primary SIP Server failure, and primary SIP Server disconnect workflows. For deployment procedures, see:

- “IP Address Takeover HA Deployment on Windows” on [page 37](#)
- “IP Address Takeover HA Deployment on AIX” on [page 59](#).
- “IP Address Takeover HA Deployment on Solaris” on [page 76](#).
- “IP Address Takeover HA Deployment on Linux” on [page 93](#).

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 in Chapter 3, “SIP Server High-Availability Deployment,” on [page 37](#) for information about basic requirements and recommendations for deploying an IP Address Takeover HA configuration in a particular operating system.

Windows NLB Cluster HA Configuration

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.

[Figure 3](#) 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.

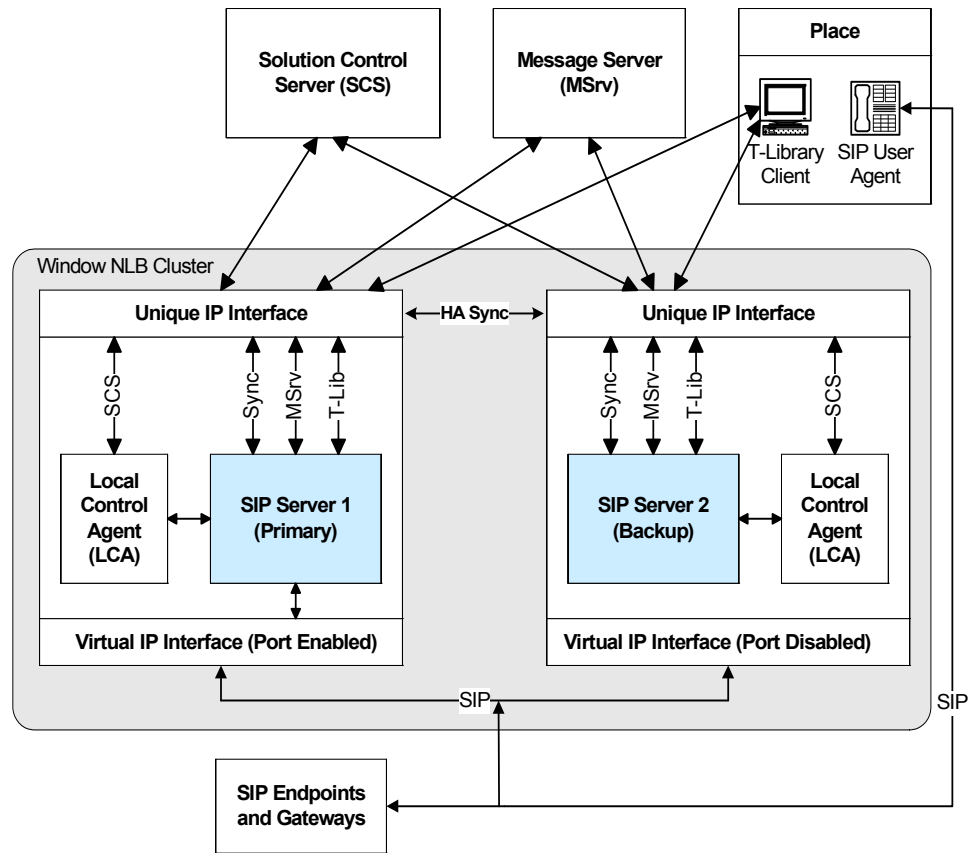


Figure 3: SIP Server HA Windows NLB Cluster Configuration

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” on [page 29](#) 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” on [page 111](#).

Windows NLB 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:
<http://support.microsoft.com/kb/898867>.

- 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.

Windows NLB 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 Configuration

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 [Figure 4](#). 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.

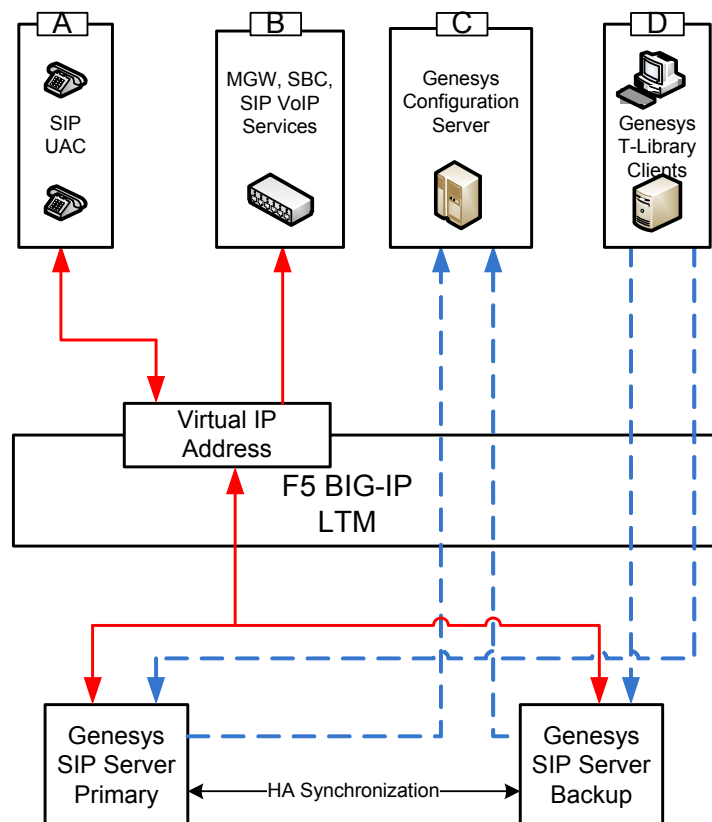


Figure 4: SIP Server HA Configuration Using F5 Networks BIG-IP LTM

For more information about a SIP Server HA configuration that uses the F5 Networks BIG-IP LTM, refer to the *Framework 8.0 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

SIP Server 8.0 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 8.0 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 8.0 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 8.0 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 DN's 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 DN's). 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.



Chapter

2

SIP Server High-Availability Workflows

This chapter describes workflows for SIP Server HA architectures that are described in Chapter 1, “SIP Server High-Availability Architecture,” on [page 11](#). 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.

This chapter contains the following sections:

- [IP Address Takeover HA Workflows, page 23](#)
- [Windows NLB Cluster HA Workflows, page 29](#)

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 Chapter 3, “SIP Server High-Availability Deployment,” on [page 37](#).

IP Address Takeover HA Workflows

[Figure 5](#) shows an IP Address Takeover configuration prior to a switchover from the primary SIP Server to the backup SIP Server:

- 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.

This section describes the following workflows:

- [Manual-Switchover Workflow, page 24](#)
- [Primary Server–Failure Workflow, page 26](#)
- [Primary Server-Disconnected Workflow, page 27](#)

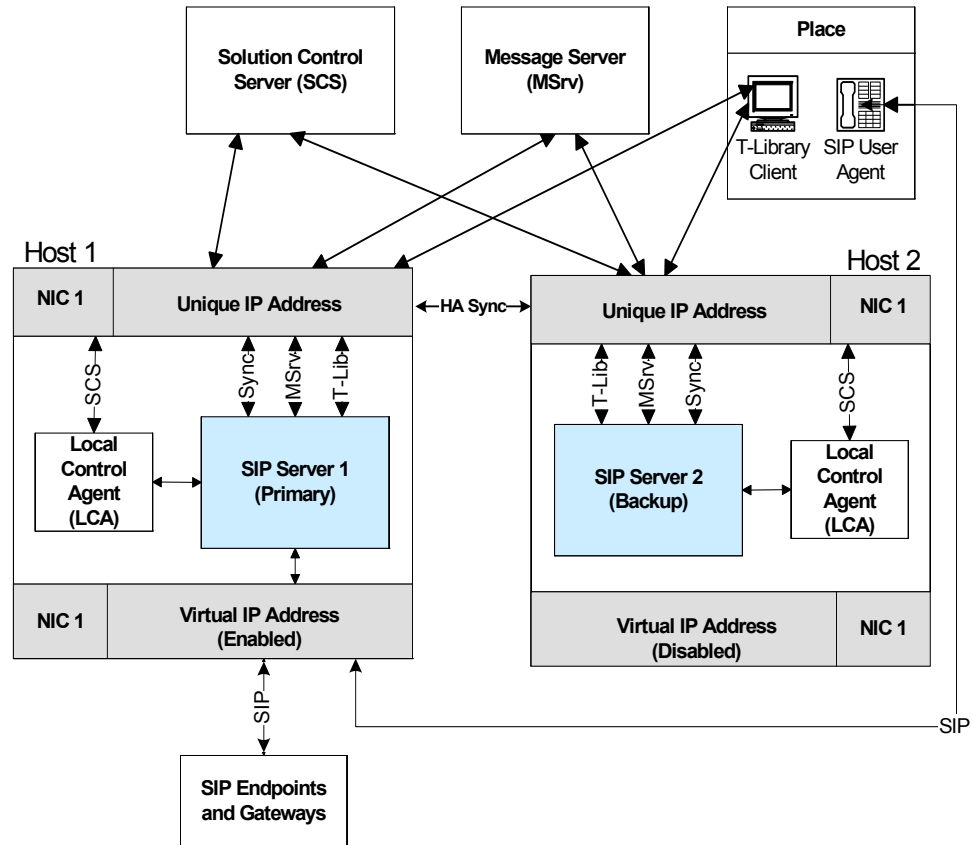


Figure 5: SIP Server HA IP Address Takeover Configuration with One NIC

Manual-Switchover Workflow

The following steps describe a primary to backup–switchover workflow for a IP Address Takeover configuration (Figure 6 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. SIP Server 1 sends a log message with Event ID 00-04561 if it is a hot standby redundancy type (or 00-04560 if it is a warm standby redundancy type) to the Message Server, to indicate that SIP Server 1 has changed to backup mode.

5. SIP Server 2 sends a log message with Event ID 00-04563 if it is a hot-standby redundancy type (or 00-04562 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to primary mode.
6. The Message Server detects the Alarm Conditions that are associated with the Event IDs and notifies the SCS.
7. The SCS activates the Alarm Conditions, which execute the associated Alarm Reaction scripts.
8. The Alarm Reaction scripts trigger the Virtual IP address control scripts that are configured as applications.
9. The SCS instructs LCA to launch the Virtual IP address control scripts on the SIP Server hosts.
10. 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).

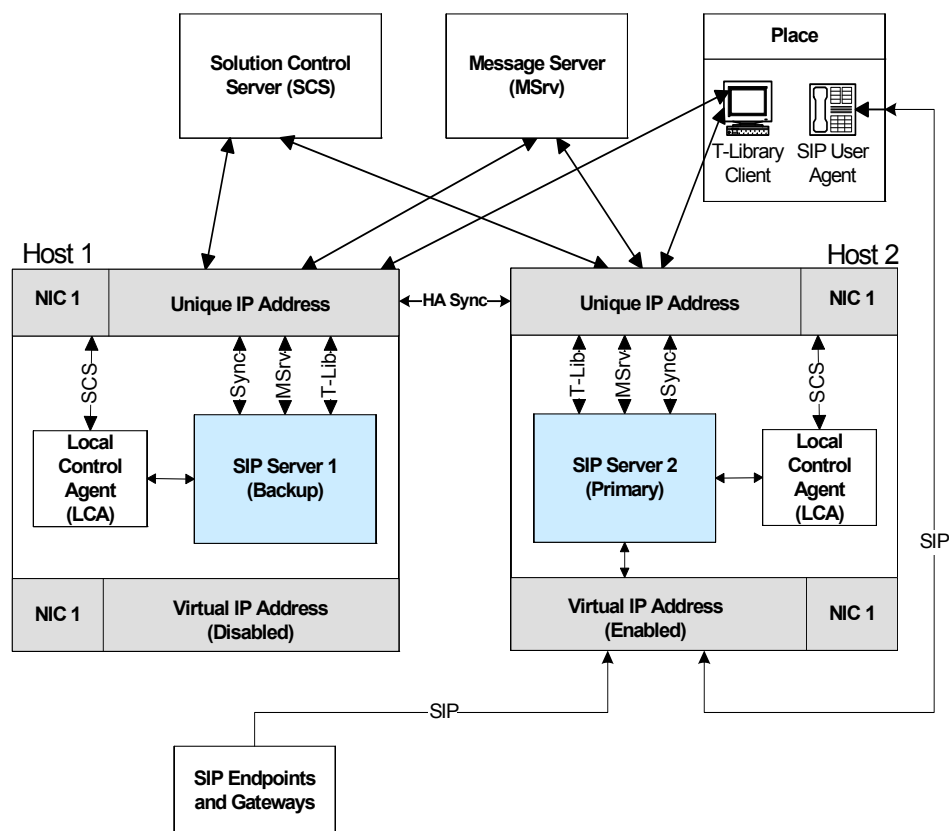


Figure 6: SIP Server HA IP Address Takeover Configuration After a Switchover

Primary Server–Failure Workflow

The following steps describe a primary server–failure workflow for an IP Address Takeover configuration (Figure 7 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. SIP Server 2 sends a log message with Event ID 00-04563 if it is a hot standby redundancy type (or 00-04562 if it is a warm standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to primary mode.
5. The Message Server detects the Alarm Condition that is associated with the Event ID and notifies the SCS.
6. The SCS activates the Alarm Condition, which executes the associated Alarm Reaction scripts.
7. The Alarm Reaction scripts trigger the Virtual IP address control scripts that are configured as applications.

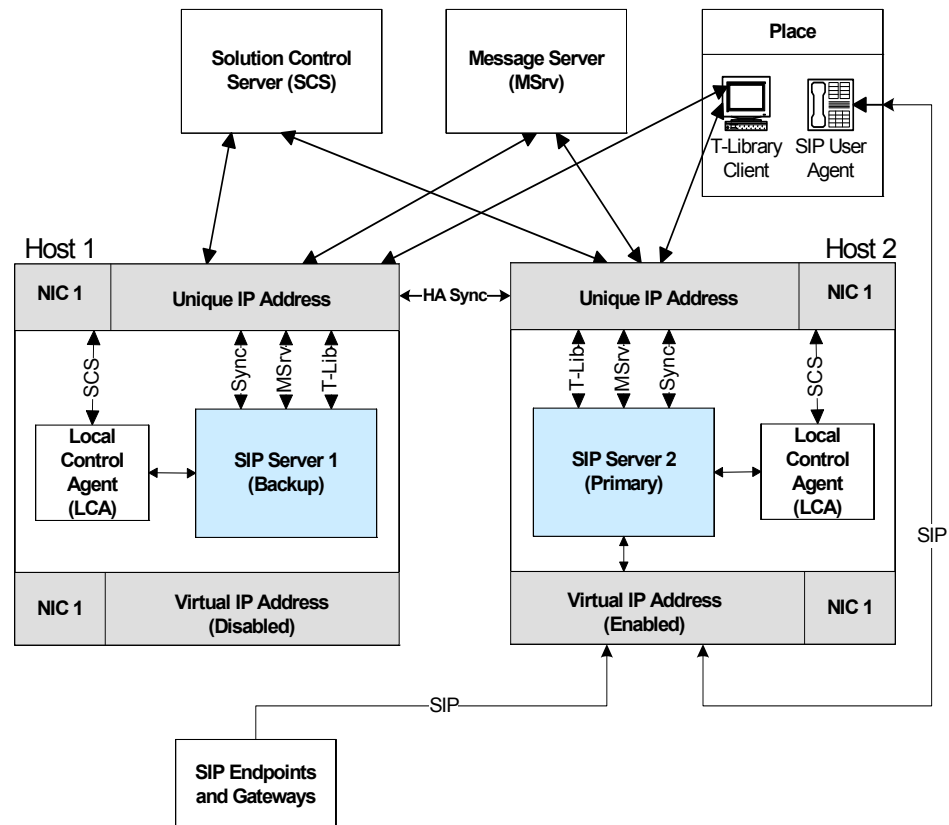


Figure 7: SIP Server HA IP Address Takeover Configuration After Primary Server Failure

8. The SCS instructs LCA to launch the Virtual IP address control scripts on the SIP Server hosts.
9. 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).

Primary Server-Disconnected Workflow

The following steps describe a primary server-disconnected workflow for an IP Address Takeover configuration ([Figure 8](#) 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. SIP Server 2 sends a log message with Event ID 00-04563 if it is a hot standby redundancy type (or 00-04562 if it is a warm standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to primary mode.
4. The Message Server detects the Alarm Condition that is associated with the Event ID and notifies the SCS.
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.

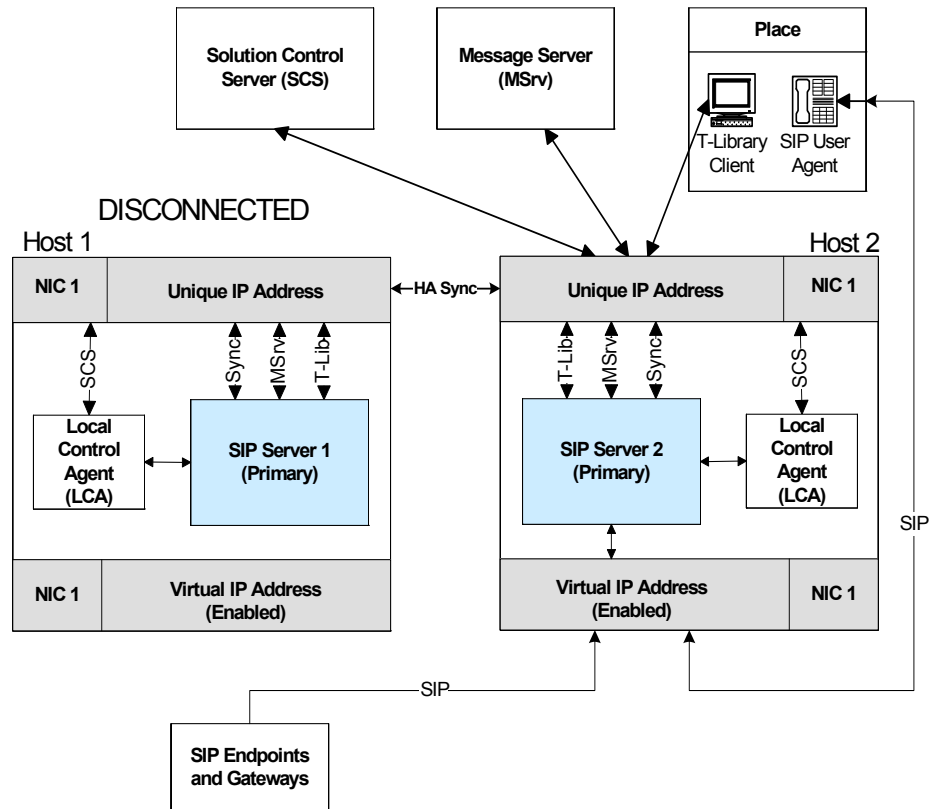


Figure 8: SIP Server HA IP Address Takeover Configuration After a Primary Server is Disconnected

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 [Figure 8](#)):

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. SIP Server 1 sends a log message with Event ID 00-04561 if it is a hot-standby redundancy type (or 00-04560 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 1 has changed to backup mode.
5. The Message Server detects the Alarm Condition that is associated with the Event ID, and notifies the SCS.
6. The SCS activates an Alarm Condition, which executes the associated Alarm Reaction script.
7. The Alarm Reaction script triggers a Virtual IP address control script that is configured as an application.

8. The SCS instructs LCA to launch the Virtual IP address control script on the SIP Server 1 host.
9. The Virtual IP address control script runs on the SIP Server 1 host and disables the Virtual IP address.

Windows NLB Cluster HA Workflows

Figure 9 shows a Windows NLB Cluster configuration prior to a 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).

This section describes the following workflows:

- [Manual-Switchover Workflow, page 30](#)
- [Primary Server–Failure Workflow, page 31](#)
- [Primary Server-Disconnected Workflow 1, page 32](#)
- [Primary Server-Disconnected Workflow 2, page 34](#)

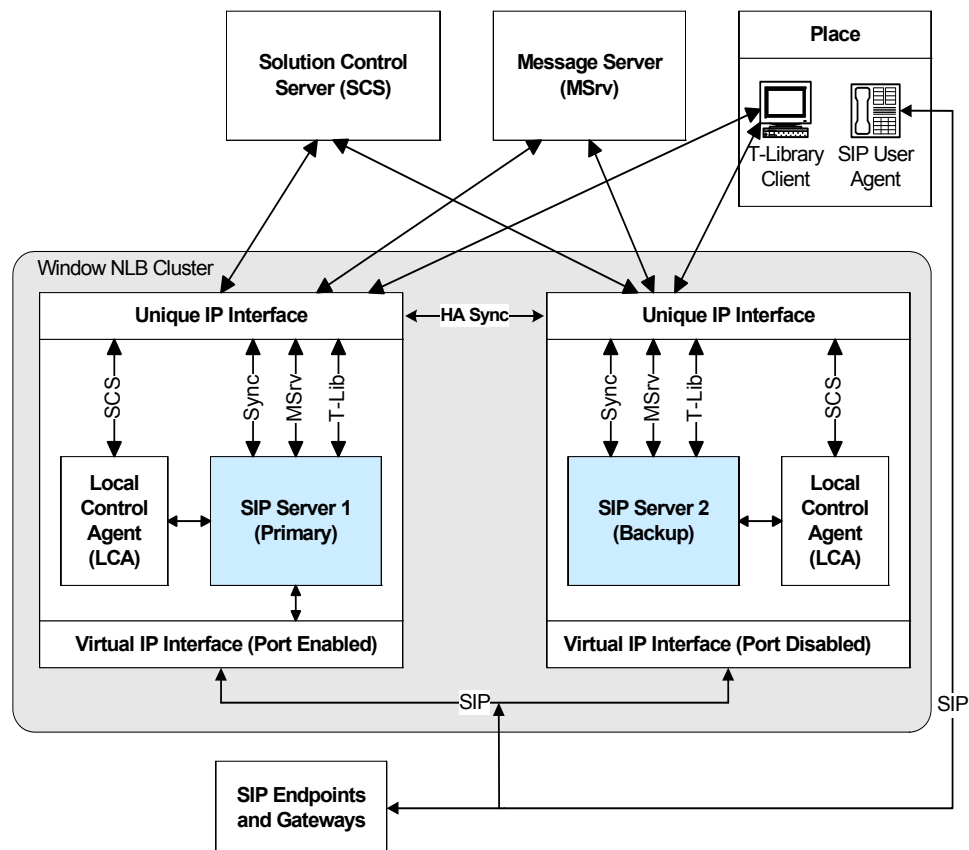


Figure 9: SIP Server HA Windows NLB Cluster Configuration

Manual-Switchover Workflow

The following steps describe a switchover workflow for a Windows NLB Cluster configuration ([Figure 10](#) 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. SIP Server 1 sends a log message with Event ID 00-04561 if it is a hot standby redundancy type (or 00-04560 if it is a warm standby redundancy type) to the Message Server, to indicate that SIP Server 1 has changed to backup mode.
5. SIP Server 2 sends a log message with Event ID 00-04563 if it is a hot-standby redundancy type (or 00-04562 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to primary mode.
6. The Message Server detects the Alarm Conditions that are associated with the Event IDs and notifies the SCS.
7. The SCS activates the Alarm Conditions, which execute the associated Alarm Reaction scripts.
8. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
9. The SCS instructs LCA to launch the Cluster control scripts on the SIP Server hosts.
10. 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.

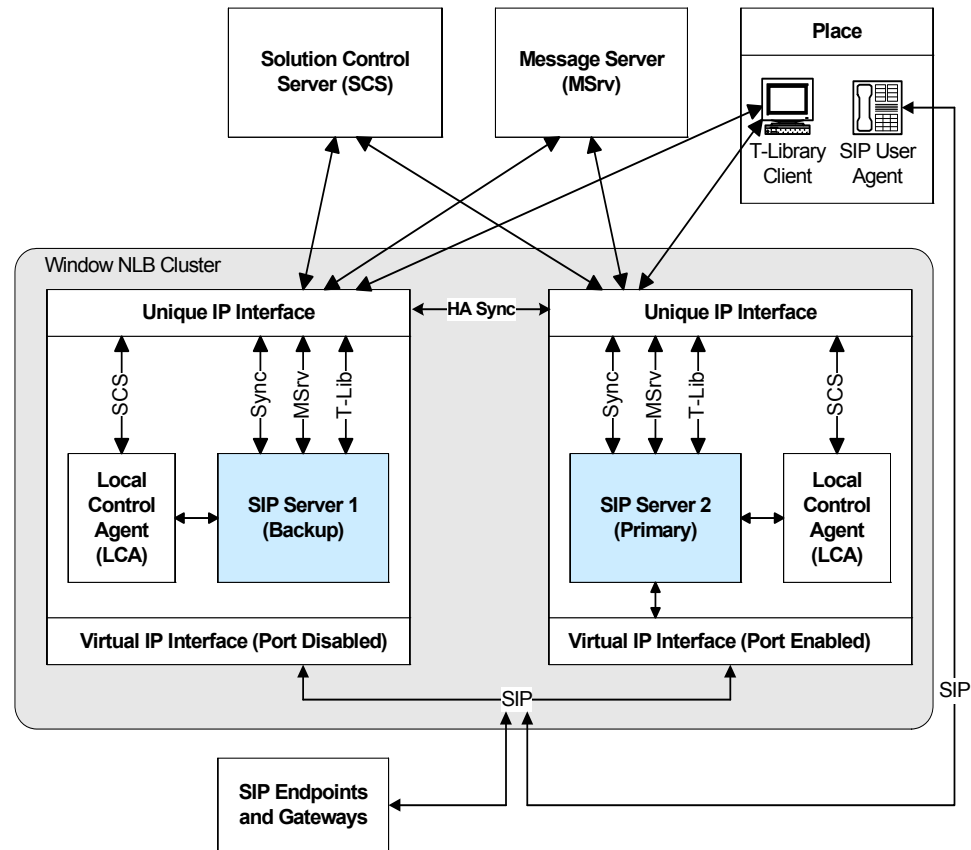


Figure 10: SIP Server HA Windows NLB Cluster Configuration After a Switchover

Primary Server–Failure Workflow

The following steps describe a primary server–failure workflow for a Windows NLB Cluster configuration (Figure 11 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. SIP Server 2 sends a log message with Event ID 00-04563 if it is a hot-standby redundancy type (or 00-04562 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to primary mode.
5. The Message Server detects the Alarm Condition that is associated with the Event ID and notifies the SCS.

6. The SCS activates the Alarm Condition, which executes the associated Alarm Reaction scripts.
7. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
8. The SCS instructs LCA to launch the Cluster control scripts on the SIP Server hosts.
9. 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.

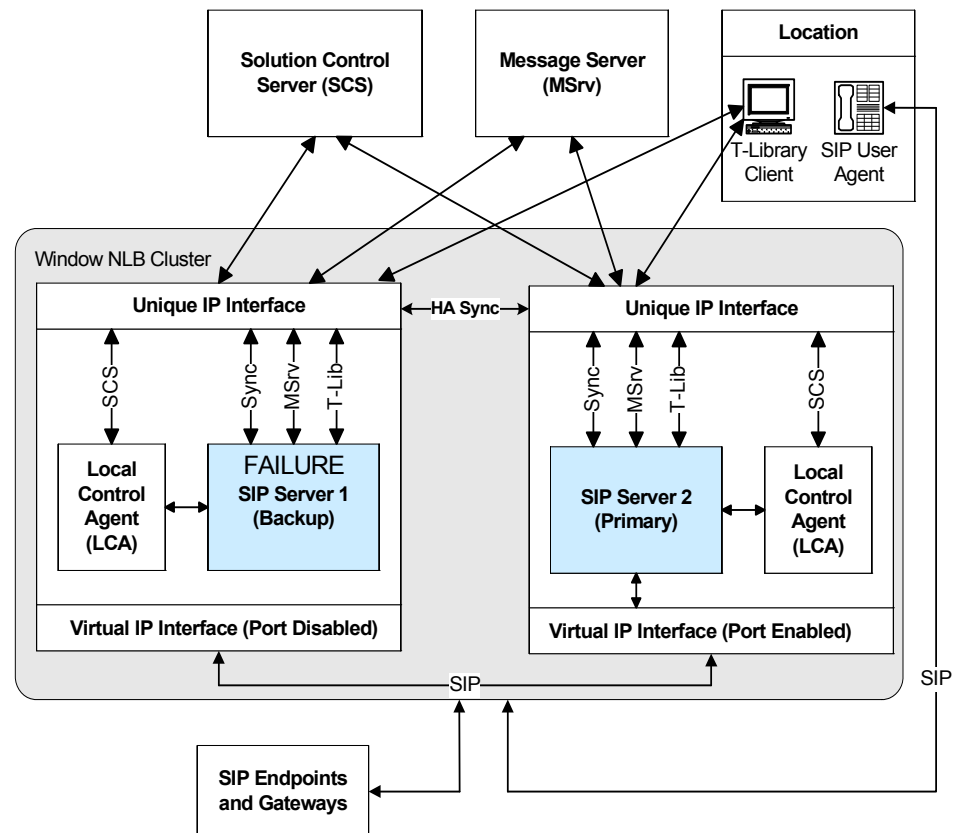


Figure 11: SIP Server HA Windows NLB Cluster Configuration After Primary Server Failure

Primary Server-Disconnected Workflow 1

The following steps describe a primary server-disconnected workflow for a Windows NLB Cluster configuration (Figure 12 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. SIP Server 2 sends a log message with Event ID 00-04563 if it is a hot-standby redundancy type (or 00-04562 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to primary mode.
4. The Message Server detects the Alarm Condition that is associated with the Event ID and notifies the SCS.
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. 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.

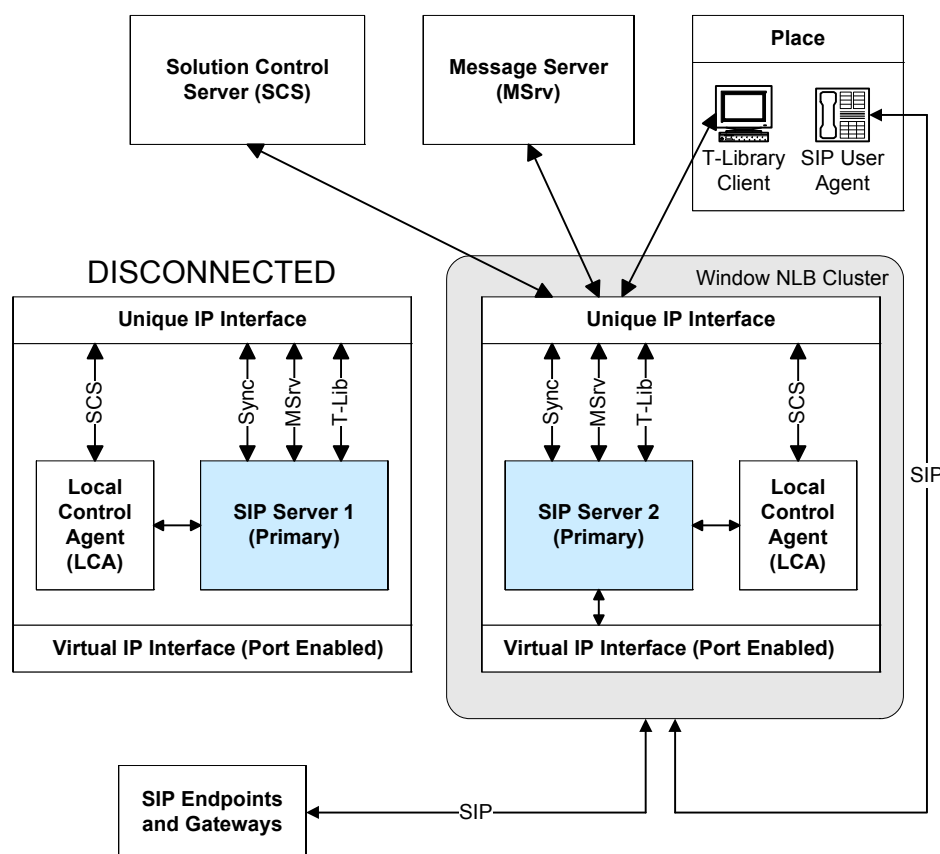


Figure 12: SIP Server HA Windows NLB Cluster Configuration After a Primary Server is Disconnected

When the connection to SIP Server 1 has been restored, the following workflow occurs (not depicted in [Figure 12](#)):

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. SIP Server 1 sends a log message with Event ID 00-04561 if it is a hot standby redundancy type (or 00-04560 if it is a warm standby redundancy type) to the Message Server, 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 ([Figure 13](#) 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. SIP Server 1 sends a log message with Event ID 00-04561 if it is a hot-standby redundancy type (or 00-04560 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 1 has changed to backup mode.
5. SIP Server 2 sends a log message with Event ID 00-04563 if it is a hot-standby redundancy type (or 00-04562 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to primary mode.

6. The Message Server detects the Alarm Conditions that are associated with the Event IDs and notifies the SCS.
7. The SCS activates the Alarm Conditions, which execute the associated Alarm Reaction scripts.
8. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
9. The SCS instructs LCA to launch the Cluster control scripts on the SIP Server hosts.
10. 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.

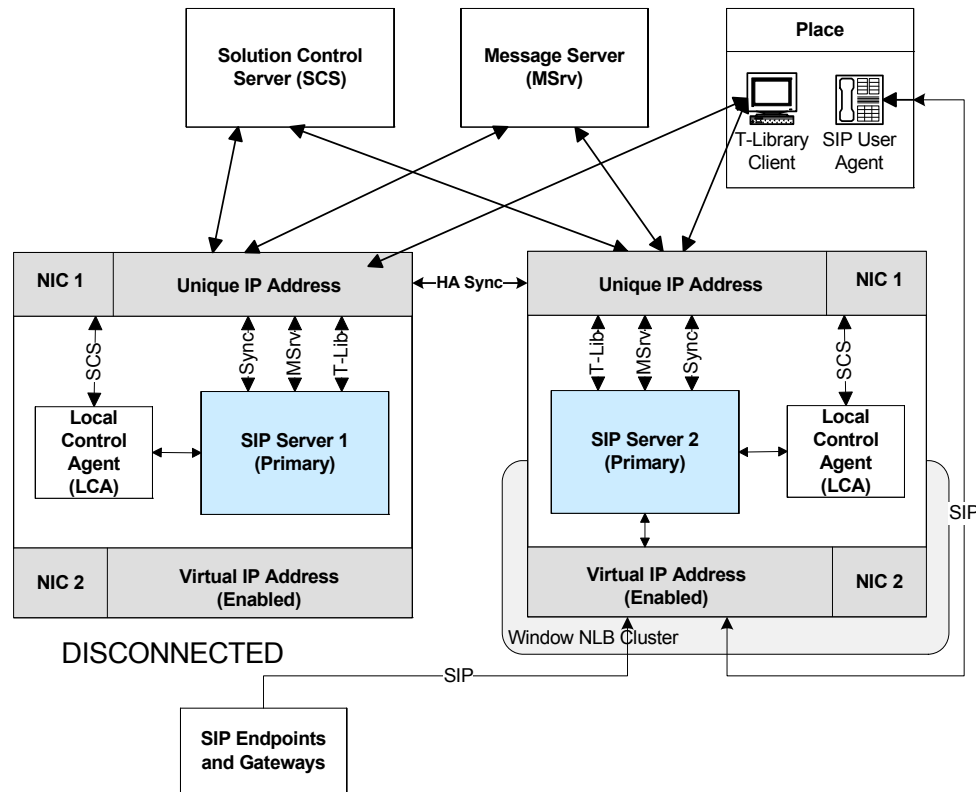


Figure 13: SIP Server HA Windows NLB Cluster Configuration with Two NICs After a Primary Server is Disconnected

When the connection to SIP Server 1 has been restored, the following workflow occurs (not depicted in [Figure 13](#)):

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. SIP Server 2 sends a log message with Event ID 00-04561 if it is a hot-standby redundancy type (or 00-04560 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 2 has changed to backup mode.
5. SIP Server 1 sends a log message with Event ID 00-04563 if it is a hot-standby redundancy type (or 00-04562 if it is a warm-standby redundancy type) to the Message Server, to indicate that SIP Server 1 has changed to primary mode.
6. The Message Server detects the Alarm Conditions that are associated with the Event IDs and notifies the SCS.
7. The SCS activates the Alarm Conditions, which execute associated Alarm Reaction scripts.
8. The Alarm Reaction scripts trigger the Cluster control scripts that are configured as applications.
9. The SCS instructs LCA to launch the Cluster control scripts on SIP Server hosts.
10. 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.



Chapter

3

SIP Server High-Availability Deployment

This chapter describes how to deploy the SIP Server high-availability (HA) configurations that are described in Chapter 1, “SIP Server High-Availability Architecture,” on [page 11](#).

This chapter contains the following sections:

- [IP Address Takeover HA Deployment on Windows, page 37](#)
- [IP Address Takeover HA Deployment on AIX, page 59](#)
- [IP Address Takeover HA Deployment on Solaris, page 76](#)
- [IP Address Takeover HA Deployment on Linux, page 93](#)
- [Windows NLB Cluster HA Deployment, page 111](#)
- [SIP Server HA Configuration Testing, page 130](#)

IP Address Takeover HA Deployment on Windows

Task Summary: IP Address Takeover HA Deployment on Windows

The following table provides an overview of the tasks that you must complete to deploy an IP Address Takeover HA configuration of SIP Server in a Windows environment.

Task Summary: IP Address Takeover HA Deployment on Windows

Objectives	Related procedures and actions
Ensure that your system meets the deployment prerequisites.	“Prerequisites” on page 39 .
Deploy the SIP Server HA configuration.	<p>SIP Server IP Address Takeover HA deployment in a Windows environment includes the following tasks:</p> <ol style="list-style-type: none"> 1. Procedure: Configuring the primary SIP Server (IP Address Takeover on Windows), on page 40. 2. Procedure: Configuring the backup SIP Server (IP Address Takeover on Windows), on page 43. 3. Procedure: Creating Virtual IP address control scripts (IP Address Takeover on Windows), on page 45. Scripts are used to enable and disable the Virtual IP address when SIP Servers change modes. 4. Procedure: Testing Virtual IP address control scripts (IP Address Takeover on Windows), on page 49. 5. Procedure: Creating Application objects for Virtual IP address control scripts (IP Address Takeover on Windows), on page 51. Application objects allow the Virtual IP address control scripts to be run as applications. 6. Procedure: Creating Alarm Reaction scripts (IP Address Takeover on Windows), on page 53. Alarm Reaction scripts are called when HA-related Alarm Conditions are activated. 7. Procedure: Creating Alarm Conditions (IP Address Takeover on Windows), on page 55. When an HA-related log event occurs, such as a log event that records when a SIP Server changes from primary to backup mode, Alarm Conditions are activated. 8. Procedure: Testing Alarm Conditions (IP Address Takeover on Windows), on page 58.
Verify the SIP Server HA configuration deployment.	Procedure: Testing your HA configuration , on page 130 . In this procedure, you perform tests to ensure that your HA configuration works as expected.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in a Windows 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:
 - SIP Server must be installed and configured on both host computers.
 - LCA must be installed and configured on both host computers.
 - Message Server must be installed and configured.
 - 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.

Deployment Procedures

Procedure:

Configuring the primary SIP Server (IP Address Takeover on Windows)

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

Start of procedure

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.

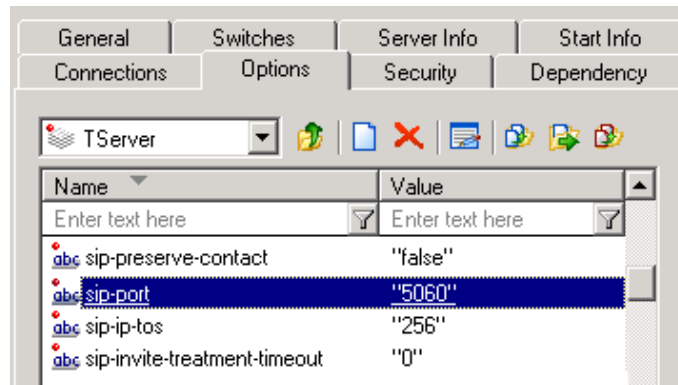


Figure 14: Configuring the sip-port Option: Sample Configuration

- ii. Set the sip-address option to the Virtual IP address.
 - iii. Click Apply to save the configuration changes.
- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.

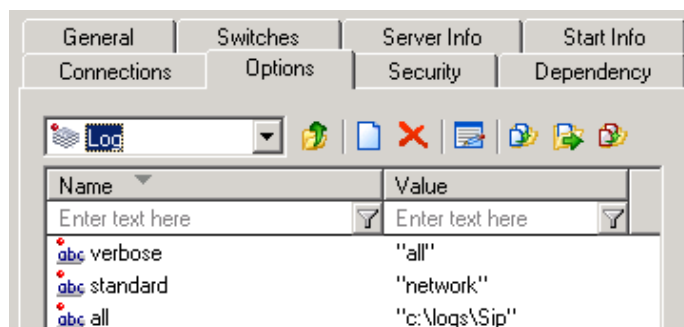


Figure 15: Configuring the Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

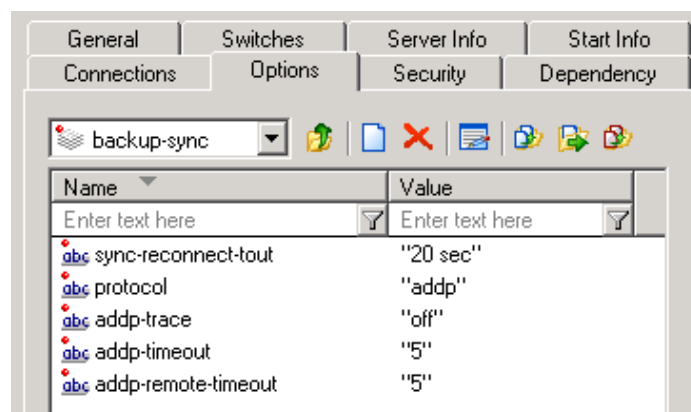


Figure 16: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click Apply to save the configuration changes.
5. 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.
6. 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.

- c. 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.
- d. Click Apply to save the configuration changes.
7. Click the Start Info tab.
 - a. Select Auto-Restart.
 - b. Click Apply to save the configuration changes.
8. Click the Connections tab, and then click Add to create a connection to the Message Server.
9. Click Apply and then OK to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Configuring the backup SIP Server \(IP Address Takeover on Windows\)](#)

Procedure:
Configuring the backup SIP Server (IP Address Takeover on Windows)

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

Start of procedure

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.
 - iii. Click Apply to save the configuration changes.

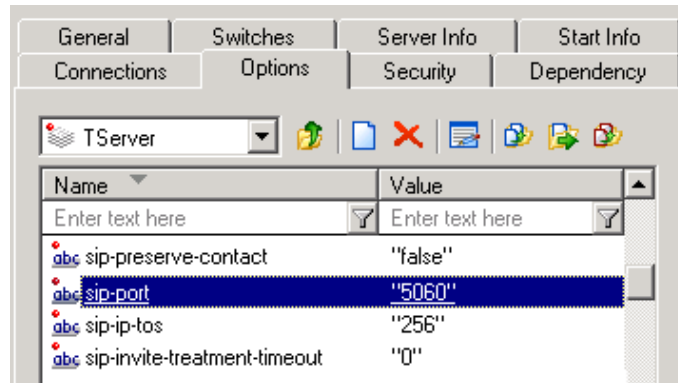


Figure 17: Configuring the sip-port Option: Sample Configuration

- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.

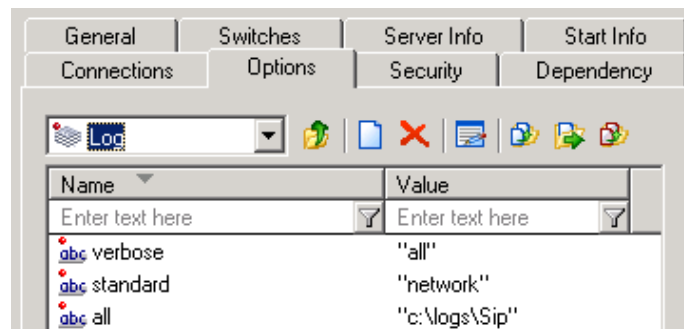


Figure 18: Configuring the Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

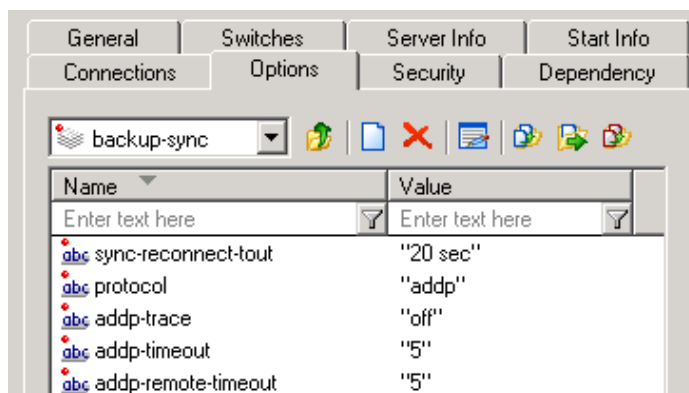


Figure 19: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click **Apply** to save the configuration changes.
7. Click the **Connections** tab, and then click **Add** to create a connection to the same Message Server to which you created a connection for the primary SIP Server.
8. Click **Apply** and then **OK** to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on Windows\)](#)

Procedure: Creating Virtual IP address control scripts (IP Address Takeover on Windows)

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 of procedure

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:

```
@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% >> Takeover.log
@rem check if VirtualIP added succeseefully 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% >> Takeover.log
@if errorlevel 1 echo %VirtualIP% not added to %VirtualInterface% >>
Takeover.log

:done
@echo %time% >> Takeover.log
```

2. In the first line of the script, replace the VirtualIP value of 10.10.11.103 with your Virtual IP address.

3. In the second line of the script, replace the `vipMask` value of `255.255.255.0` with your Virtual IP mask.
4. In the third line of the 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:

```
@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 script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.
7. In the second line of the 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:

```
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") 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:

```

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 of procedure

Next Steps

- [Procedure: Testing Virtual IP address control scripts \(IP Address Takeover on Windows\)](#)

Procedure: Testing Virtual IP address control scripts (IP Address Takeover on Windows)

Purpose: To verify that the Virtual IP address control scripts that you created in [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on Windows\)](#) work as expected.

Start of procedure

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:

```
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:

```
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:

```
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:

```
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 of procedure

Next Steps

- [Procedure: Creating Application objects for Virtual IP address control scripts \(IP Address Takeover on Windows\)](#)

Procedure:**Creating Application objects for Virtual IP address control scripts (IP Address Takeover on Windows)**

Purpose: To create four Application objects of type Third Party Server: one for each of the scripts that you created in [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on Windows\)](#), on page 45. 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 of procedure

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.

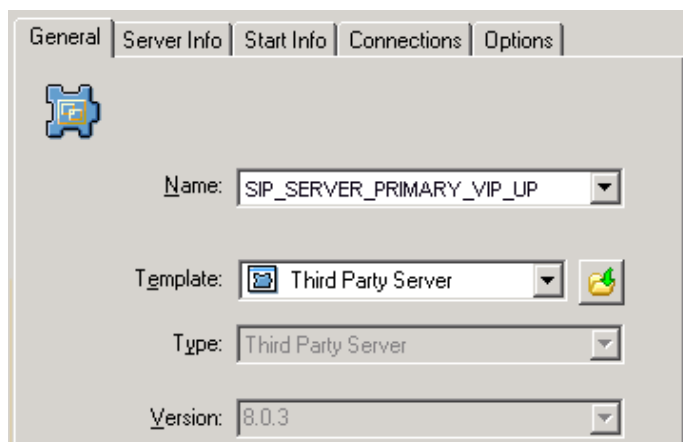


Figure 20: Configuring the Application Object for the Script, General Tab: Sample Configuration

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.

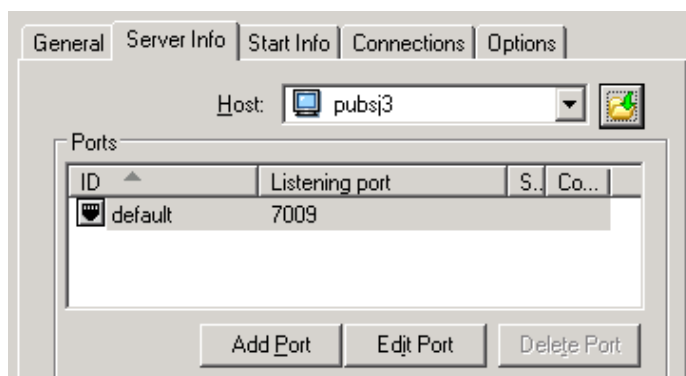


Figure 21: Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

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).

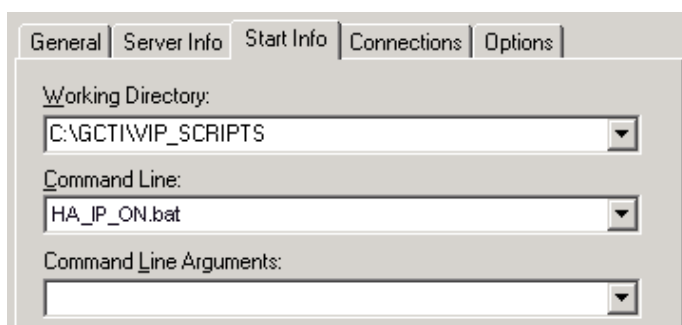


Figure 22: Configuring the Application Object for the Script, Start Info Tab: Sample Configuration

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

End of procedure

Next Steps

- [Procedure: Creating Alarm Reaction scripts \(IP Address Takeover on Windows\)](#)

Procedure: Creating Alarm Reaction scripts (IP Address Takeover on Windows)

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 [Procedure: Creating Application objects for Virtual IP address control scripts \(IP Address Takeover on Windows\)](#), on page 51.

Start of procedure

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)

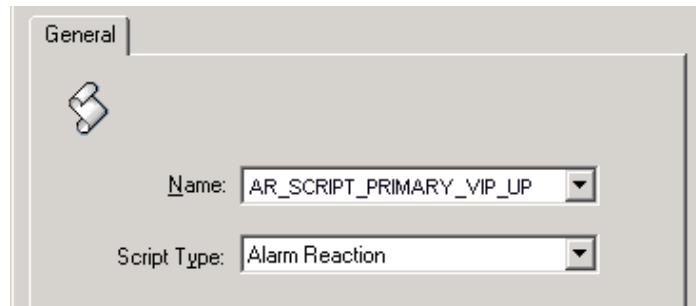


Figure 23: Configuring the Alarm Reaction Script: Sample Configuration

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.

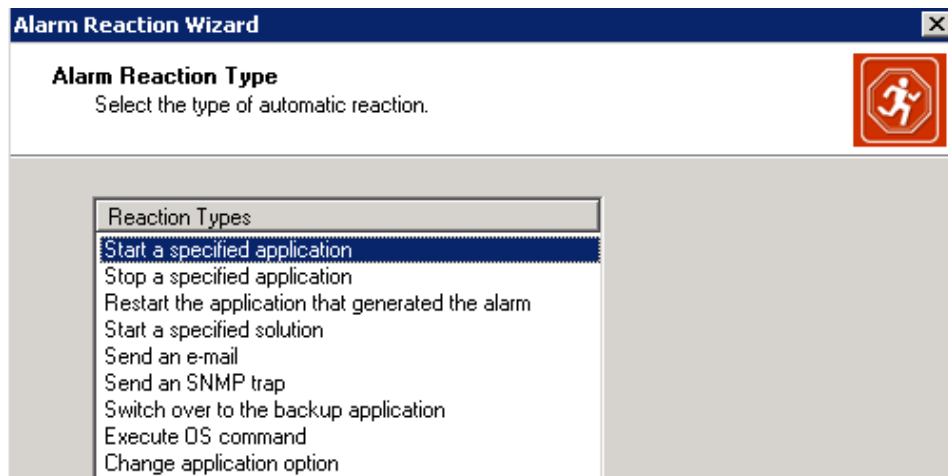


Figure 24: Alarm Reaction: Selecting the Alarm Reaction Type

- 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.

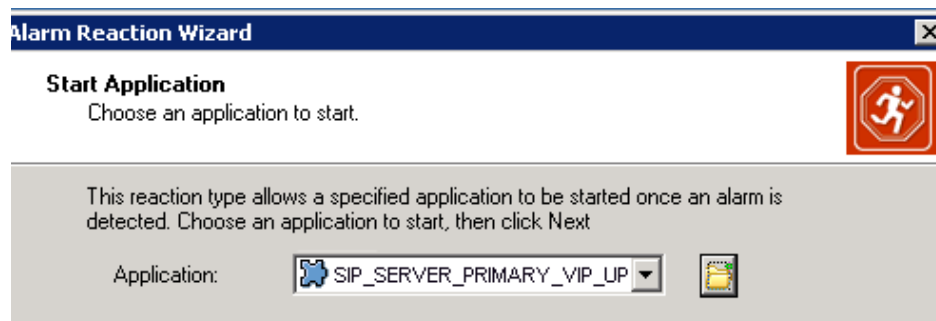


Figure 25: Alarm Reaction: Selecting the Application to Start

- e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in [Step 4](#).

End of procedure

Next Steps

- [Procedure: Creating Alarm Conditions \(IP Address Takeover on Windows\)](#)

Procedure: Creating Alarm Conditions (IP Address Takeover on Windows)

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 [Procedure: Creating Alarm Reaction scripts \(IP Address Takeover on Windows\)](#), on [page 53](#).

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. [Tables 2](#) and [3](#) outline the Alarm Conditions for hot-standby and warm-standby configurations, respectively. Refer to the procedure that follows to create the Alarm Conditions that are required for your configuration.

For information about the log events for which you are creating Alarm Conditions, refer to “SIP Server HA Log Events” on [page 133](#).

Table 2: Alarm Conditions for Hot Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4561	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4561_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4563	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN, AR_SCRIPT_PRIMARY_VIP_UP
4561	SIP_SERVER_BACKUP	ALRM_BACKUP_4561_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4563	SIP_SERVER_BACKUP	ALRM_BACKUP_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Table 3: Alarm Conditions for Warm Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4560	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4560_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4562	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4562_HAPrimary	AR_SCRIPT_PRIMARY_VIP_UP, AR_SCRIPT_BACKUP_VIP_DOWN
4560	SIP_SERVER_BACKUP	ALRM_BACKUP_4560_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4562	SIP_SERVER_BACKUP	ALRM_BACKUP_4562_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Start of procedure

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_4561_HABackup.
 - Optionally, enter a description.
 - For the Category value, select Critical.
 - Set Cancel Timeout to 1.

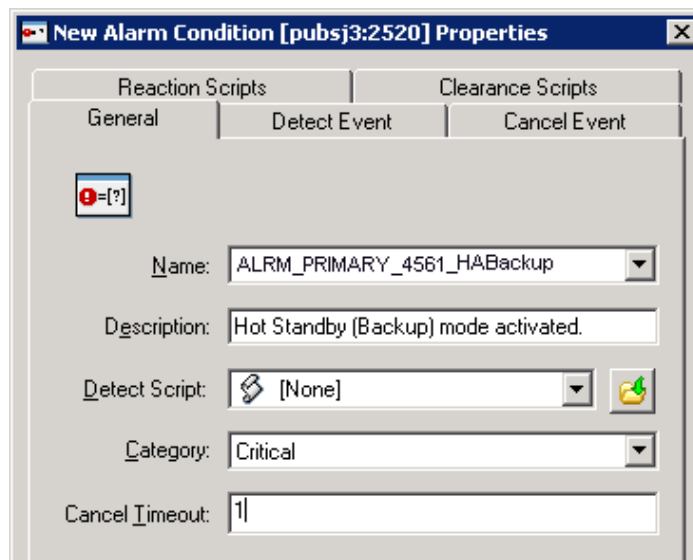


Figure 26: Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the Detect Event tab:

- Set the Log Event ID as defined in Table 2 on [page 56](#) if you configure Hot Standby mode or as defined in Table 3 on [page 56](#) if you configure Warm Standby mode.
- 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.

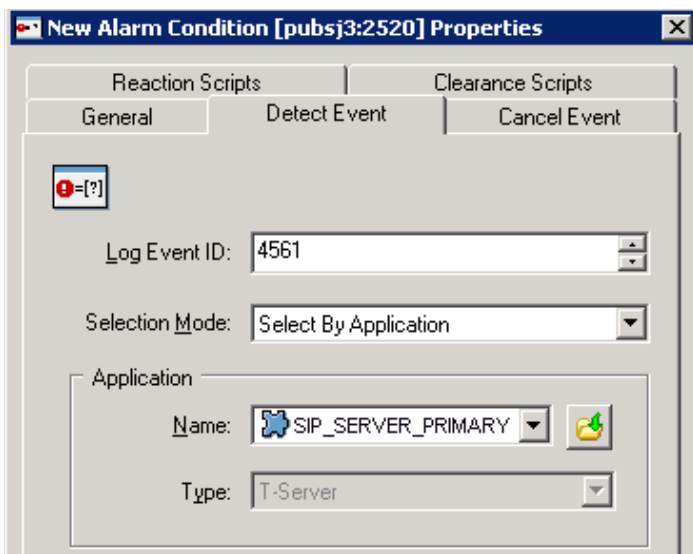


Figure 27: Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the Reaction Scripts tab, add the Alarm Reaction script as defined in Table 2 on [page 56](#) if you configure Hot Standby mode or as defined in Table 3 on [page 56](#) if you configure Warm Standby mode.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your hot-standby or warm-standby configuration.

End of procedure

Next Steps

- [Procedure: Testing Alarm Conditions \(IP Address Takeover on Windows\)](#)

Procedure: Testing Alarm Conditions (IP Address Takeover on Windows)

Purpose: To verify that the Alarm Conditions work as expected.

Start of procedure

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_4561_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_4561_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 of procedure

Next Steps

- [Procedure: Testing your HA configuration, on page 130](#)

IP Address Takeover HA Deployment on AIX

Task Summary: IP Address Takeover HA Deployment on AIX

The following table provides an overview of the main steps that you must complete in order to deploy a SIP Server HA configuration in an IBM AIX environment.

Task Summary: IP Address Takeover HA Deployment on AIX

Objectives	Related procedures and actions
Ensure that your system meets the deployment prerequisites.	“Prerequisites” on page 60 .
Deploy the SIP Server HA configuration.	<p>SIP Server HA deployment in an IBM AIX environment includes the following tasks:</p> <ol style="list-style-type: none"> 1. Procedure: Configuring the primary SIP Server (IP Address Takeover on AIX), on page 61. 2. Procedure: Configuring the backup SIP Server (IP Address Takeover on AIX), on page 64. 3. Procedure: Updating the /etc/hosts file (IP Address Takeover on AIX), on page 67. The update to the /etc/hosts file makes the address and host name of the Virtual IP interface known to the DNS server. 4. Procedure: Creating Virtual IP address control scripts (IP Address Takeover on AIX), on page 67. The command-shell files are used to enable and disable the Virtual IP address when SIP Servers change modes. 5. Procedure: Creating Application objects for Virtual IP address control scripts (IP Address Takeover on AIX), on page 68. Application objects allow the Virtual IP address control scripts to be run as applications. 6. Procedure: Creating Alarm Reaction scripts (IP Address Takeover on AIX), on page 70. Alarm Reaction scripts are called when HA-related Alarm Conditions are activated.

Task Summary: IP Address Takeover HA Deployment on AIX (Continued)

Objectives	Related procedures and actions
Deploy the SIP Server HA configuration (continued).	<p>7. Procedure: Creating Alarm Conditions (IP Address Takeover on AIX), on page 72. When an HA-related log event occurs, such as a log event that records when SIP Servers change modes, Alarm Conditions are activated.</p> <p>8. Procedure: Testing Alarm Conditions (IP Address Takeover on AIX), on page 75.</p>
Verify the SIP Server HA configuration deployment.	Procedure: Testing your HA configuration , on page 130 . In this procedure, you perform tests to ensure that your HA configuration works as expected.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in an IBM AIX 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:
 - SIP Server must be installed and configured on both host computers.
 - LCA must be installed and configured on both host computers.
 - Message Server must be installed and configured.
 - 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.

Deployment Procedures

Procedure:

Configuring the primary SIP Server (IP Address Takeover on AIX)

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

Start of procedure

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.

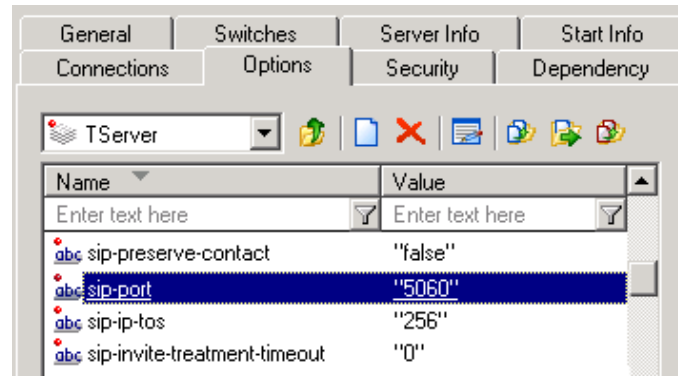


Figure 28: Configuring the sip-port Option: Sample Configuration

- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.

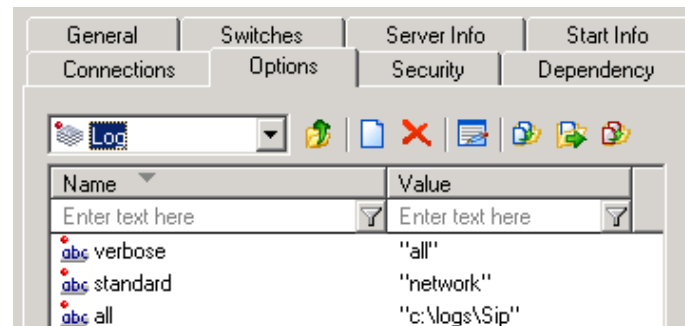


Figure 29: Configuring Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

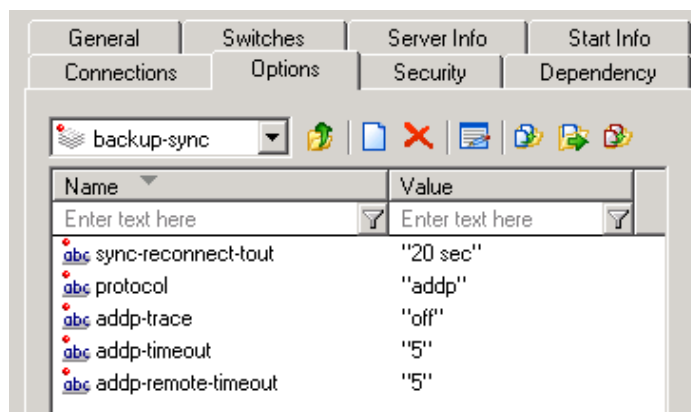


Figure 30: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click **Apply** to save the configuration changes.
5. 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.
6. 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.

- c. 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.
 - d. Click Apply to save the configuration changes.
7. Click the Start Info tab.
 - a. Select Auto-Restart.
 - b. Click Apply to save the configuration changes.
8. Click the Connections tab, and then click Add to create a connection to the Message Server.
9. Click Apply and then OK to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Configuring the backup SIP Server \(IP Address Takeover on AIX\)](#)

Procedure: Configuring the backup SIP Server (IP Address Takeover on AIX)

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

Start of procedure

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.

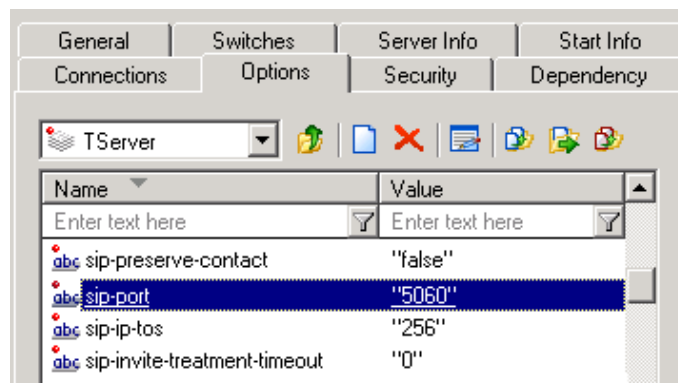


Figure 31: Configuring the sip-port Option: Sample Configuration

- ii. Set the sip-address option to the Virtual IP address.
 - iii. Click Apply to save the configuration changes.
- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.

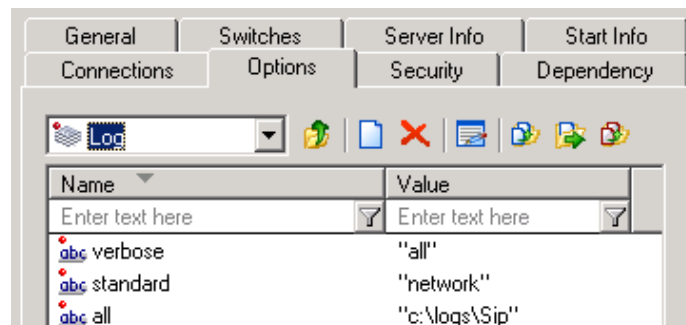


Figure 32: Configuring Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

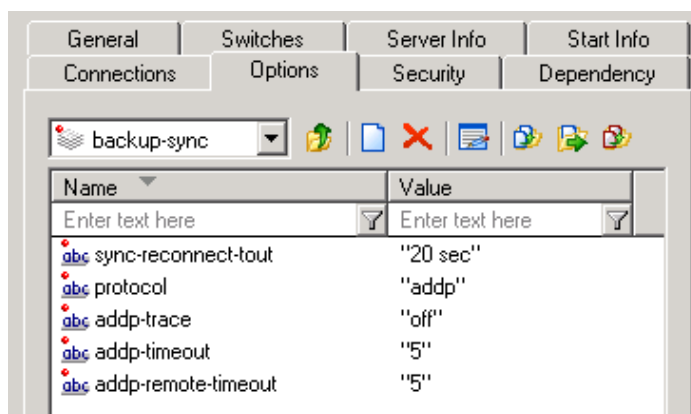


Figure 33: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click Apply to save the configuration changes.
7. Click the Connections tab, and then click Add to create a connection to the same Message Server to which you created a connection for the primary SIP Server.
8. Click Apply and then OK to save the configuration changes.

End of procedure

Next Steps

[Procedure: Updating the /etc/hosts file \(IP Address Takeover on AIX\)](#)

Procedure: Updating the /etc/hosts file (IP Address Takeover on AIX)

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 of procedure

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 of procedure

Next Steps

- [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on AIX\)](#)

Procedure: Creating Virtual IP address control scripts (IP Address Takeover on AIX)

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 of procedure

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 of procedure

Next Steps

- [Procedure: Creating Application objects for Virtual IP address control scripts \(IP Address Takeover on AIX\)](#)

Procedure: Creating Application objects for Virtual IP address control scripts (IP Address Takeover on AIX)

Purpose: To create four Application objects of type `Third Party Server`: one for each of the shell files that you created in [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on AIX\)](#). 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 of procedure

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.

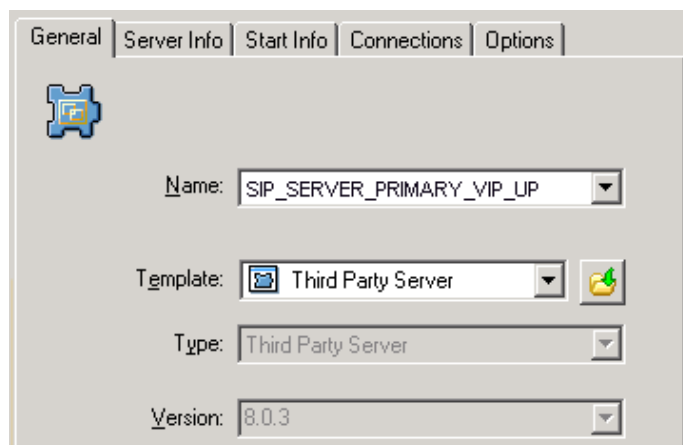


Figure 34: Configuring the Application Object for the Script, General Tab: Sample Configuration

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.

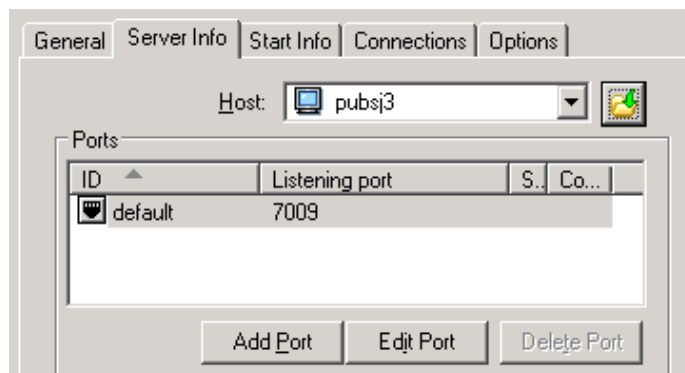


Figure 35: Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

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 address (`SIP_SERVER_PRIMARY_VIP_DOWN` and `SIP_SERVER_BACKUP_VIP_DOWN`), set the **Timeout Startup** value to 8.
7. Repeat the steps in this procedure to create an Application object for each of the four scripts.

End of procedure

Next Steps

- [Procedure: Creating Alarm Reaction scripts \(IP Address Takeover on AIX\)](#)

Procedure: Creating Alarm Reaction scripts (IP Address Takeover on AIX)

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 [Procedure: Creating Application objects for Virtual IP address control scripts \(IP Address Takeover on AIX\)](#), on page 68.

Start of procedure

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)

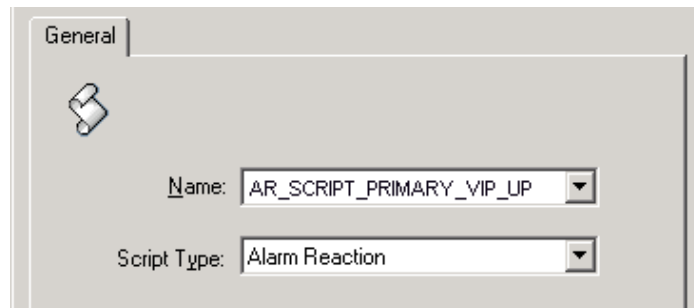


Figure 36: Configuring the Alarm Reaction Script: Sample Configuration

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.

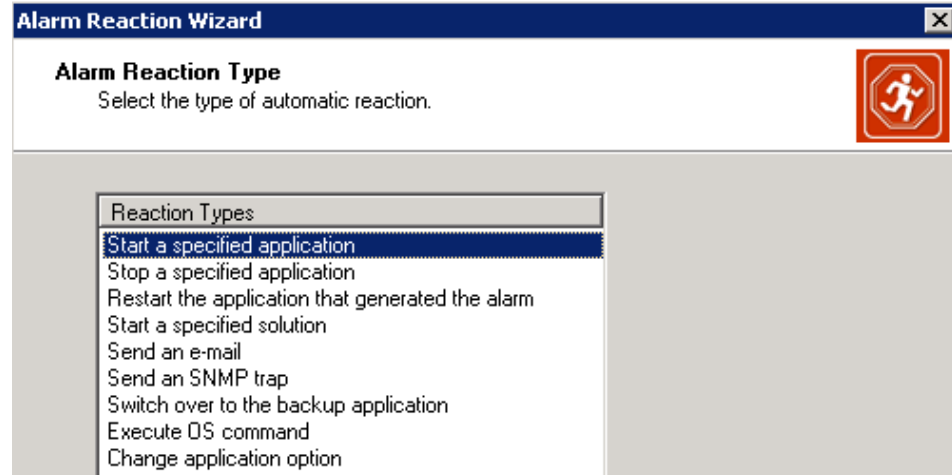


Figure 37: Alarm Reaction: Selecting the Alarm Reaction Type

- 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.

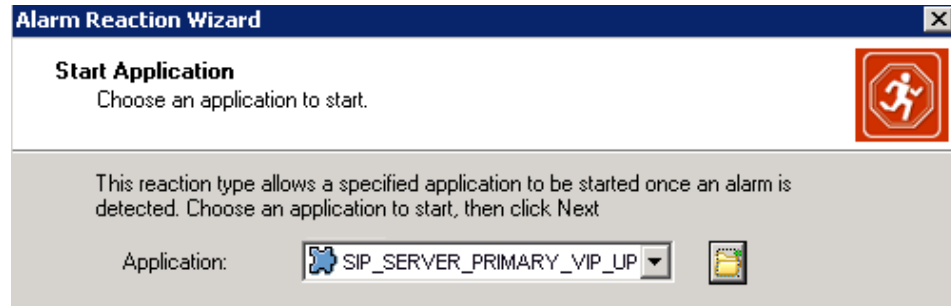


Figure 38: Alarm Reaction: Selecting the Application to Start

- e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in [Step 4](#).

End of procedure

Next Steps

- [Procedure: Creating Alarm Conditions \(IP Address Takeover on AIX\)](#)

Procedure: Creating Alarm Conditions (IP Address Takeover on AIX)

Purpose: Alarm Conditions are required to handle log events that occur when the primary or backup SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you also configure them to trigger the Alarm Reaction scripts that you created previously.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. [Tables 4](#) and [5](#) outline the Alarm Conditions for hot-standby and warm-standby configurations, respectively. Refer to the procedure that follows to create the Alarm Conditions that are required for your configuration.

For information about the log events for which you are creating Alarm Conditions, refer to “SIP Server HA Log Events” on [page 133](#).

Table 4: Alarm Conditions for Hot Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4561	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4561_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4563	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN, AR_SCRIPT_PRIMARY_VIP_UP
4561	SIP_SERVER_BACKUP	ALRM_BACKUP_4561_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4563	SIP_SERVER_BACKUP	ALRM_BACKUP_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Table 5: Alarm Conditions for Warm Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4560	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4560_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4562	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4562_HAPrimary	AR_SCRIPT_PRIMARY_VIP_UP, AR_SCRIPT_BACKUP_VIP_DOWN
4560	SIP_SERVER_BACKUP	ALRM_BACKUP_4560_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4562	SIP_SERVER_BACKUP	ALRM_BACKUP_4562_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Start of procedure

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_4561_HABackup.
 - Optionally, enter a description.
 - For the Category value, select Critical.
 - Set Cancel Timeout to 1.

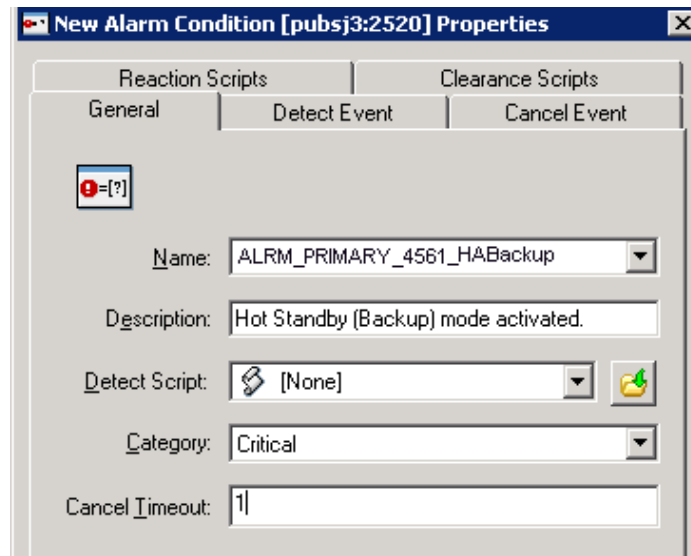


Figure 39: Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the Detect Event tab:

- Set the Log Event ID as defined in Table 4 on [page 73](#) if you configure Hot Standby mode or as defined in Table 5 on [page 73](#) if you configure Warm Standby mode.
- 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.

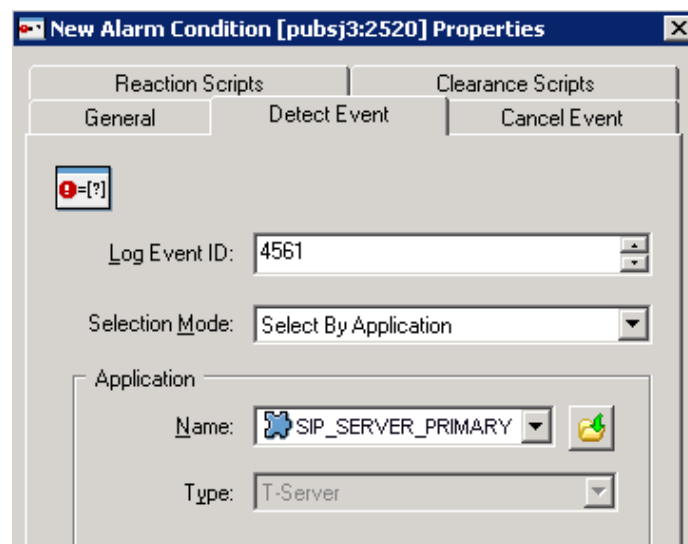


Figure 40: Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the Reaction Scripts tab, add the Alarm Reaction script as defined in Table 4 on [page 73](#) if you configure Hot Standby mode or as defined in Table 5 on [page 73](#) if you configure Warm Standby mode.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your hot-standby or warm-standby configuration.

End of procedure

Next Steps

- [Procedure: Testing Alarm Conditions \(IP Address Takeover on AIX\)](#)

Procedure: Testing Alarm Conditions (IP Address Takeover on AIX)

Purpose: To verify that the Alarm Conditions work as expected.

Start of procedure

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_4561_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_4561_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP interface at the primary SIP Server and disable the Virtual IP interface at the backup SIP Server.
3. Use an `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 of procedure

Next Steps

- [Procedure: Testing your HA configuration, on page 130](#)

IP Address Takeover HA Deployment on Solaris

Task Summary: IP Address Takeover HA Deployment on Solaris

The following table provides an overview of the tasks that you must complete to deploy a SIP Server HA configuration in a Sun Solaris environment.

Task Summary: IP Address Takeover HA Deployment on Solaris

Objectives	Related procedures and actions
Ensure that your system meets the deployment prerequisites.	“Prerequisites” on page 77 .
Deploy the SIP Server HA configuration.	<p>SIP Server HA deployment in a Sun Solaris environment includes the following tasks:</p> <ol style="list-style-type: none"> 1. Procedure: Configuring the primary SIP Server (IP Address Takeover on Solaris), on page 78. 2. Procedure: Configuring the backup SIP Server (IP Address Takeover on Solaris), on page 81. 3. Procedure: Updating the /etc/hosts file (IP Address Takeover on Solaris), on page 84. 4. Procedure: Creating Virtual IP address control scripts (IP Address Takeover on Solaris), on page 84. Virtual IP address control scripts are used to enable and disable the Virtual IP address when SIP Servers change modes. 5. Procedure: Creating Application objects for the Virtual IP address control scripts (IP Address Takeover on Solaris), on page 85. The Application objects allow the Virtual IP address control scripts to be run as applications. 6. Procedure: Creating Alarm Reaction scripts (IP Address Takeover on Solaris), on page 87. Alarm Reaction scripts are called when HA-related Alarm Conditions are activated.

Task Summary: IP Address Takeover HA Deployment on Solaris (Continued)

Objectives	Related procedures and actions
Deploy the SIP Server HA configuration (continued).	<p>7. Procedure: Creating Alarm Conditions (IP Address Takeover on Solaris), on page 89. When an HA-related log event occurs, such as a log event that records when a primary SIP Server changes from primary to backup mode, the Alarm Conditions that you configured in the previous procedure are activated.</p> <p>8. Procedure: Testing Alarm Conditions (IP Address Takeover on Solaris), on page 92.</p>
Verify the SIP Server HA configuration deployment.	Procedure: Testing your HA configuration , on page 130 . In this procedure, you perform tests to ensure that your HA configuration works as expected.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in a Sun Solaris 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:
 - SIP Server must be installed and configured on both host computers.
 - LCA must be installed and configured on both host computers.
 - Message Server must be installed and configured.
 - 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.

Deployment Procedures

Procedure:

Configuring the primary SIP Server (IP Address Takeover on Solaris)

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

Start of procedure

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.

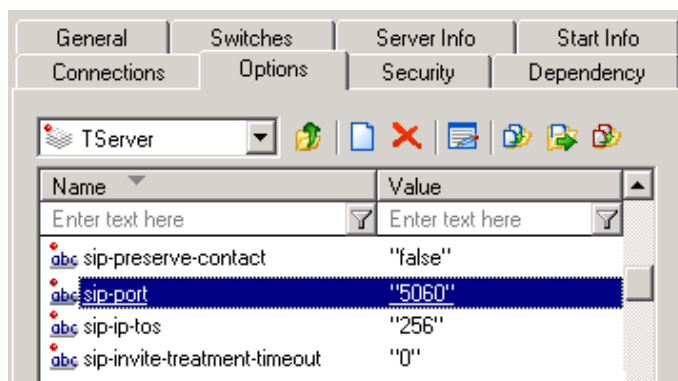


Figure 41: Configuring the sip-port Option: Sample Configuration

- ii. Set the sip-address option to the Virtual IP address.
- iii. Click Apply to save the configuration changes.
- b. Select the Log section.
 - i. Set the standard option to network .
 - ii. Set the verbose option to all .

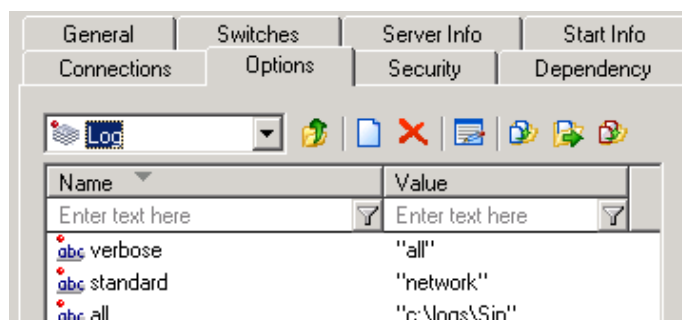


Figure 42: Configuring Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

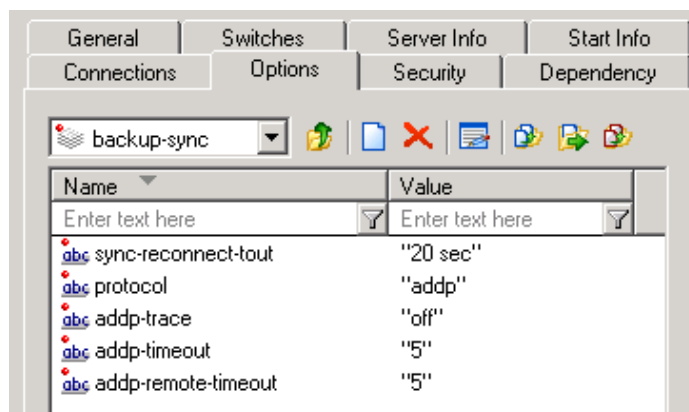


Figure 43: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click **Apply** to save the configuration changes.
5. 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.
6. 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.

- c. 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.
 - d. Click Apply to save the configuration changes.
7. Click the Start Info tab.
 - a. Select Auto-Restart.
 - b. Click Apply to save the configuration changes.
8. Click the Connections tab, and then click Add to create a connection to the Message Server.
9. Click Apply and then OK to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Configuring the backup SIP Server \(IP Address Takeover on Solaris\)](#)

Procedure: Configuring the backup SIP Server (IP Address Takeover on Solaris)

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

Start of procedure

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.

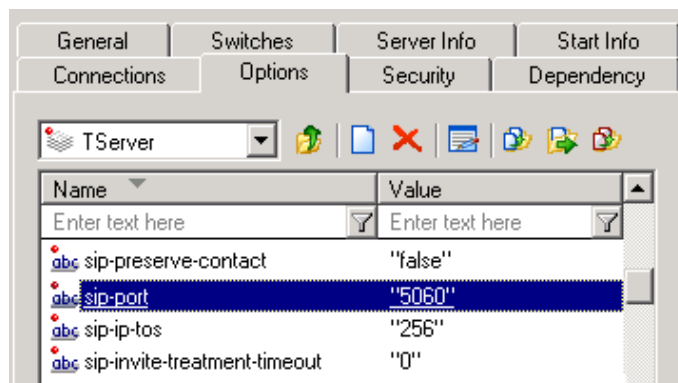


Figure 44: Configuring the sip-port Option: Sample Configuration

- ii. Set the sip-address option to the Virtual IP address.
 - iii. Click Apply to save the configuration changes.
- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.

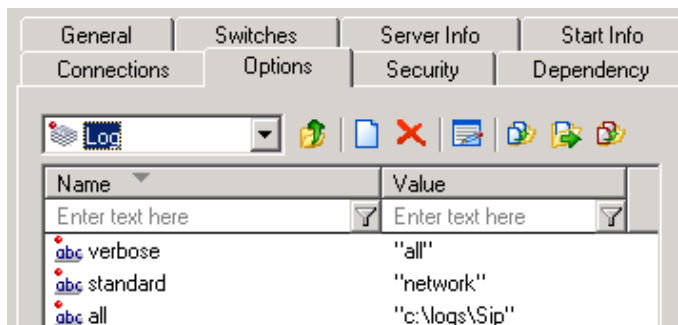


Figure 45: Configuring the Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

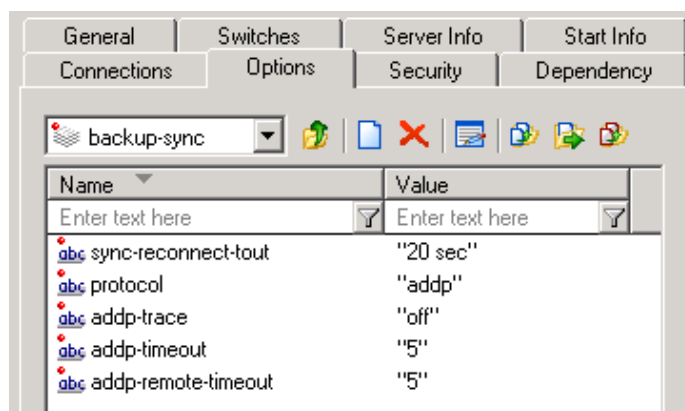


Figure 46: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click **Apply** to save the configuration changes.
7. Click the **Connections** tab, and then click **Add** to create a connection to the same Message Server to which you created a connection for the primary SIP Server.
8. Click **Apply** and then **OK** to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Updating the /etc/hosts file \(IP Address Takeover on Solaris\)](#)

Procedure:
Updating the /etc/hosts file (IP Address Takeover on Solaris)

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 of procedure

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 of procedure**Next Steps**

- [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on Solaris\)](#)

Procedure:
Creating Virtual IP address control scripts (IP Address Takeover on Solaris)

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 of procedure

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 of procedure**Next Steps**

- [Procedure: Creating Application objects for the Virtual IP address control scripts \(IP Address Takeover on Solaris\)](#)

Procedure:**Creating Application objects for the Virtual IP address control scripts (IP Address Takeover on Solaris)**

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 of procedure

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.

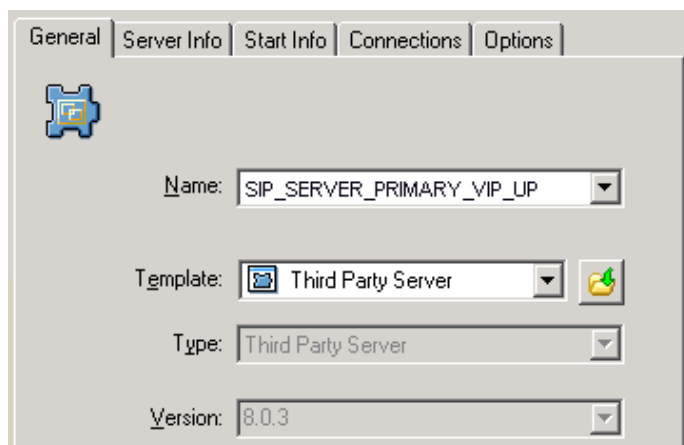


Figure 47: Configuring the Application Object for the Script, General Tab: Sample Configuration

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.

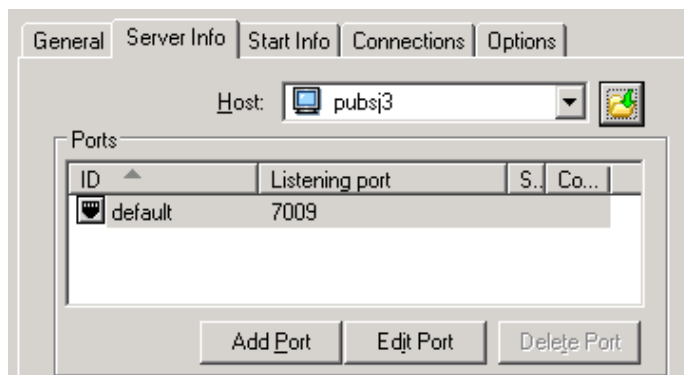


Figure 48: Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

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

End of procedure

Next Steps

- [Procedure: Creating Alarm Reaction scripts \(IP Address Takeover on Solaris\)](#)

Procedure: Creating Alarm Reaction scripts (IP Address Takeover on Solaris)

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 [Procedure: Creating Application objects for the Virtual IP address control scripts \(IP Address Takeover on Solaris\)](#), on [page 85](#).

Start of procedure

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)

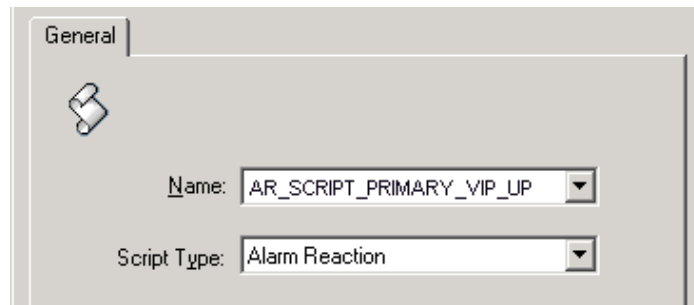


Figure 49: Configuring the Alarm Reaction Script: Sample Configuration

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.

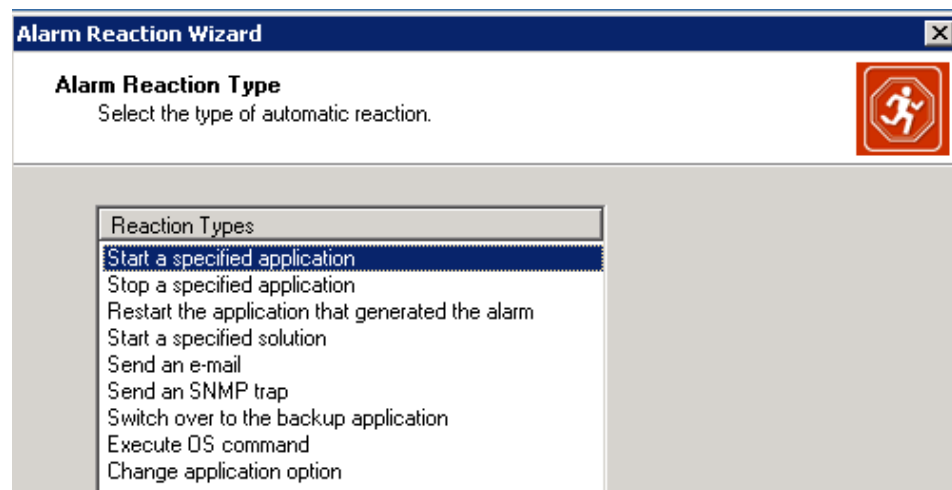


Figure 50: Alarm Reaction: Selecting the Alarm Reaction Type

- 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.

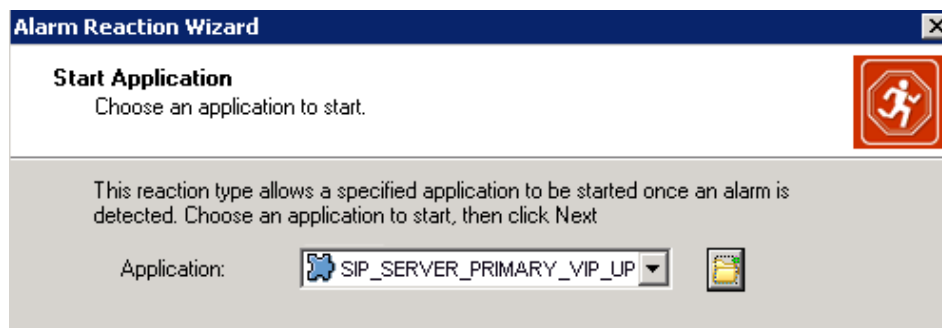


Figure 51: Alarm Reaction: Selecting the Application to Start

- e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in [Step 4](#).

End of procedure

Next Steps

- [Procedure: Creating Alarm Conditions \(IP Address Takeover on Solaris\)](#)

Procedure: Creating Alarm Conditions (IP Address Takeover on Solaris)

Purpose: Alarm Conditions are required to handle log events that occur when the primary or backup SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you also configure them to trigger the Alarm Reaction scripts that you created previously.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. [Tables 6](#) and [7](#) outline the Alarm Conditions for hot-standby and warm-standby configurations, respectively. Refer to the procedure that follows to create the Alarm Conditions that are required for your configuration.

For information about the log events for which you are creating Alarm Conditions, refer to “SIP Server HA Log Events” on [page 133](#).

Table 6: Alarm Conditions for Hot Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4561	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4561_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4563	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN, AR_SCRIPT_PRIMARY_VIP_UP
4561	SIP_SERVER_BACKUP	ALRM_BACKUP_4561_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4563	SIP_SERVER_BACKUP	ALRM_BACKUP_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Table 7: Alarm Conditions for Warm Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4560	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4560_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4562	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4562_HAPrimary	AR_SCRIPT_PRIMARY_VIP_UP, AR_SCRIPT_BACKUP_VIP_DOWN
4560	SIP_SERVER_BACKUP	ALRM_BACKUP_4560_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4562	SIP_SERVER_BACKUP	ALRM_BACKUP_4562_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Start of procedure

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 a Name for the Alarm Condition—for example, ALRM_PRIMARY_4561_HABackup.
 - Optionally, enter a description.
 - For the Category value, select Critical.
 - Set Cancel Timeout to 1.

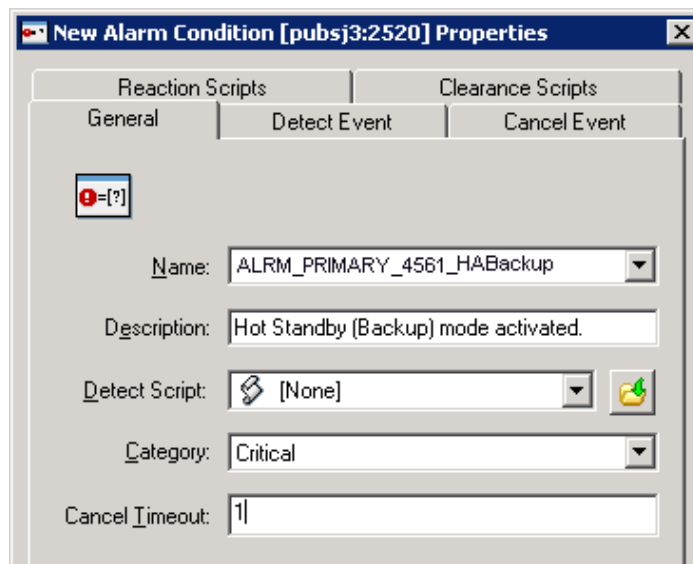


Figure 52: Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the Detect Event tab:

- Set the Log Event ID as defined in Table 6 on [page 90](#) if you configure Hot Standby mode or as defined in Table 7 on [page 90](#) if you configure Warm Standby mode.
- 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.

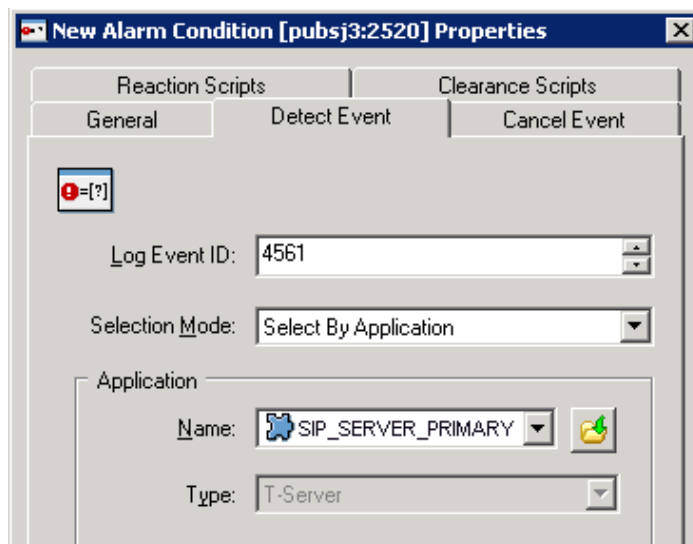


Figure 53: Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the Reaction Scripts tab, add the Alarm Reaction script as defined in Table 6 on [page 90](#) if you configure Hot Standby mode or as defined in Table 7 on [page 90](#) if you configure Warm Standby mode.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your hot-standby or warm-standby configuration.

End of procedure

Next Steps

- [Procedure: Testing Alarm Conditions \(IP Address Takeover on Solaris\)](#)

Procedure: Testing Alarm Conditions (IP Address Takeover on Solaris)

Purpose: To verify that the Alarm Conditions work as expected.

Start of procedure

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_4561_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_4561_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP interface at the primary SIP Server and disable the Virtual IP interface at the backup SIP Server.
4. Use an `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 of procedure

Next Steps

- [Procedure: Testing your HA configuration, on page 130](#)

IP Address Takeover HA Deployment on Linux

Task Summary: IP Address Takeover HA Deployment on Linux

The following table provides an overview of the main steps that you must complete in order to deploy a SIP Server HA deployment in a Red Hat Linux environment.

Task Summary: IP Address Takeover HA Deployment on Linux

Objectives	Related procedures and actions
Ensure that your system meets the deployment prerequisites.	“Prerequisites” on page 94 .
Deploy the SIP Server HA configuration.	<p>SIP Server HA deployment in a Linux environment includes the following tasks:</p> <ol style="list-style-type: none"> 1. Procedure: Configuring the primary SIP Server (IP Address Takeover on Linux), on page 95. 2. Procedure: Configuring the backup SIP Server (IP Address Takeover on Linux), on page 98. 3. Procedure: Updating the /etc/hosts file (IP Address Takeover on Linux), on page 101. 4. Procedure: Creating a configuration file for the Virtual IP interface (IP Address Takeover on Linux), on page 101. 5. Procedure: Creating Virtual IP address control scripts (IP Address Takeover on Linux), on page 102. Virtual IP address control scripts are used to enable and disable the Virtual IP address when SIP Servers change modes. 6. Procedure: Creating Application objects for Virtual IP address control scripts (IP Address Takeover on Linux), on page 103. The Application objects allow the Virtual IP address control scripts to be run as applications. 7. Procedure: Creating Alarm Reaction scripts (IP Address Takeover on Linux), on page 105. Alarm Reaction scripts are called when HA-related Alarm Conditions are activated.

Task Summary: IP Address Takeover HA Deployment on Linux (Continued)

Objectives	Related procedures and actions
Deploy the SIP Server HA configuration (continued).	<p>8. Procedure: Creating Alarm Conditions (IP Address Takeover on Linux), on page 107. When an HA-related log event occurs, such as a log event that records when a primary SIP Server changes from primary to backup mode, the Alarm Conditions that you configured in the previous procedure are activated.</p> <p>9. Procedure: Testing Alarm Conditions (IP Address Takeover on Linux), on page 110.</p>
Verify the SIP Server HA configuration deployment.	Procedure: Testing your HA configuration , on page 130. In this procedure, you perform tests to ensure that your HA configuration works as expected.

Prerequisites

There are basic requirements and recommendations for deploying an IP Address Takeover HA configuration of SIP Server in a Red Hat Linux 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:
 - SIP Server must be installed and configured on both host computers.
 - LCA must be installed and configured on both host computers.
 - Message Server must be installed and configured.
 - 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.

Deployment Procedures

Procedure:

Configuring the primary SIP Server (IP Address Takeover on Linux)

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

Start of procedure

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.

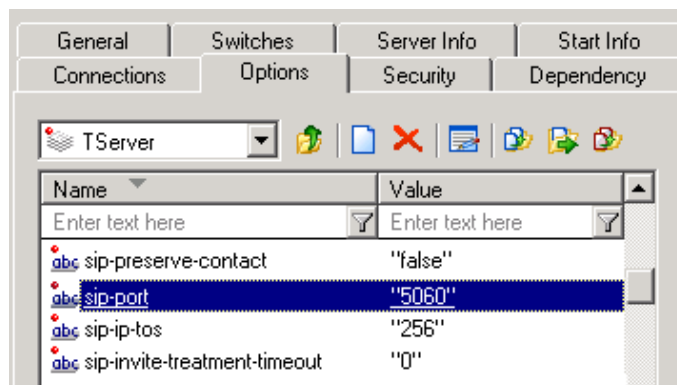


Figure 54: Configuring the sip-port Option: Sample Configuration

- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.



Figure 55: Configuring the Log Options: Sample Configuration

Note: Setting logging options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

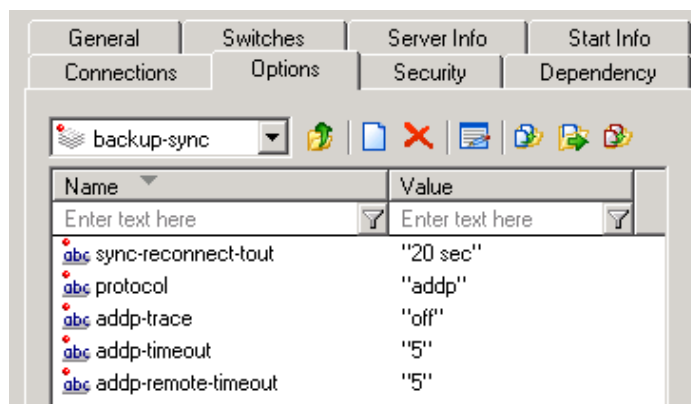


Figure 56: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click **Apply** to save the configuration changes.
5. 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.
6. 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.

- c. 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.
 - d. Click Apply to save the configuration changes.
7. Click the Start Info tab.
 - a. Select Auto-Restart.
 - b. Click Apply to save the configuration changes.
8. Click the Connections tab, and then click Add to create a connection to the Message Server.
9. Click Apply and then OK to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Configuring the backup SIP Server \(IP Address Takeover on Linux\)](#)

Procedure: Configuring the backup SIP Server (IP Address Takeover on Linux)

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

Start of procedure

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.



Figure 57: Configuring the sip-port Option: Sample Configuration

- ii. Set the sip-address option to the Virtual IP address.
 - iii. Click Apply to save the configuration changes.
- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.



Figure 58: Configuring the Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.

ii. Configure the following backup-sync options:

- sync-reconnect-tout
- protocol
- addp-timeout
- addp-remote-timeout

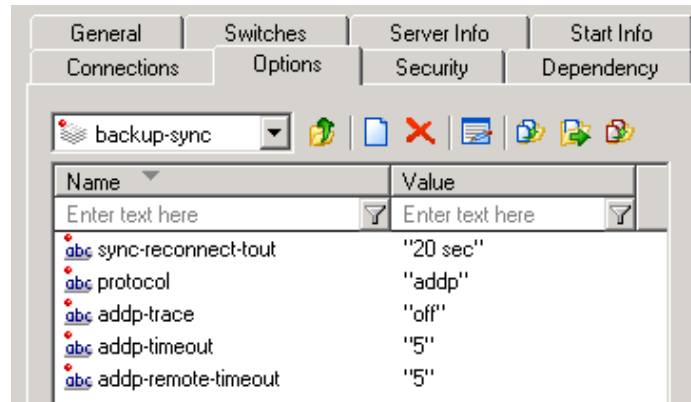


Figure 59: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click Apply to save the configuration changes.
7. Click the Connections tab, and then click Add to create a connection to the same Message Server to which you created a connection for the primary SIP Server.
8. Click Apply and then OK to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Updating the /etc/hosts file \(IP Address Takeover on Linux\)](#)

Procedure: **Updating the /etc/hosts file (IP Address Takeover on Linux)**

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

Start of procedure

- 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 of procedure

Next Steps

- [Procedure: Creating a configuration file for the Virtual IP interface \(IP Address Takeover on Linux\)](#)

Procedure: **Creating a configuration file for the Virtual IP interface (IP Address Takeover on Linux)**

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

Start of procedure

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 of procedure

Next Steps

- [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on Linux\)](#)

Procedure:

Creating Virtual IP address control scripts (IP Address Takeover on Linux)

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 of procedure

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 of procedure

Next Steps

- [Procedure: Creating Application objects for Virtual IP address control scripts \(IP Address Takeover on Linux\)](#)

Procedure:

Creating Application objects for Virtual IP address control scripts (IP Address Takeover on Linux)

Purpose: To create four Application objects of type Third Party Server: one for each of the shell files that you created in [Procedure: Creating Virtual IP address control scripts \(IP Address Takeover on Linux\)](#), on page 102. 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 of procedure

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.

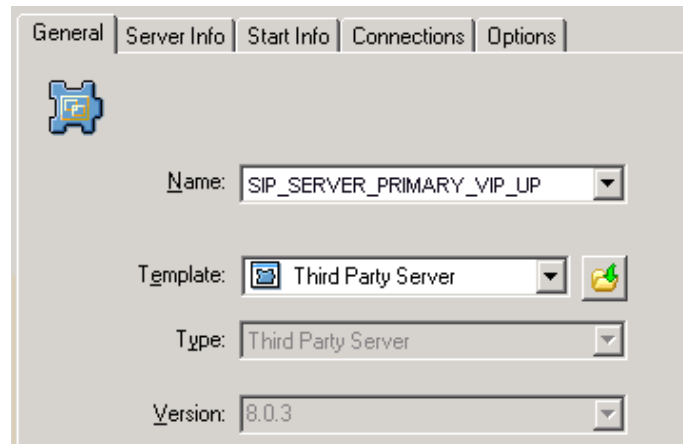


Figure 60: Configuring the Application Object for the Script, General Tab: Sample Configuration

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 shell script is located.
 - b. If necessary, specify a valid communication-port number by using the **Edit Port** option.

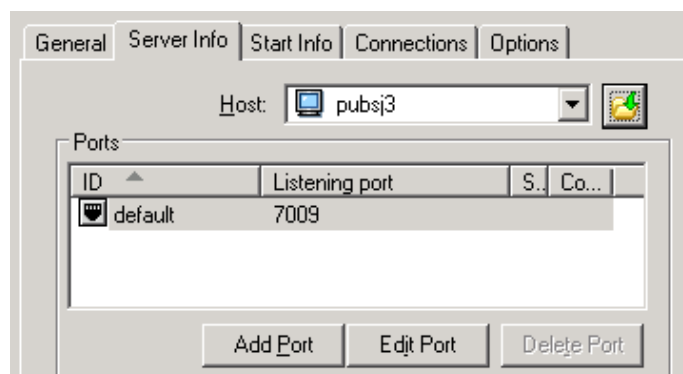


Figure 61: Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

6. Select the **Start Info** tab.
 - a. Set the **Working Directory** to the location of the shell 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 address (SIP_SERVER_PRIMARY_VIP_DOWN and SIP_SERVER_BACKUP_VIP_DOWN), set the Timeout Startup value to 8.
7. Repeat the steps in this procedure to create an Application object for each of the four scripts.

End of procedure

Next Steps

- [Procedure: Creating Alarm Reaction scripts \(IP Address Takeover on Linux\)](#)

Procedure: Creating Alarm Reaction scripts (IP Address Takeover on Linux)

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 [Procedure: Creating Application objects for Virtual IP address control scripts \(IP Address Takeover on Linux\)](#), on page 103.

Start of procedure

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)

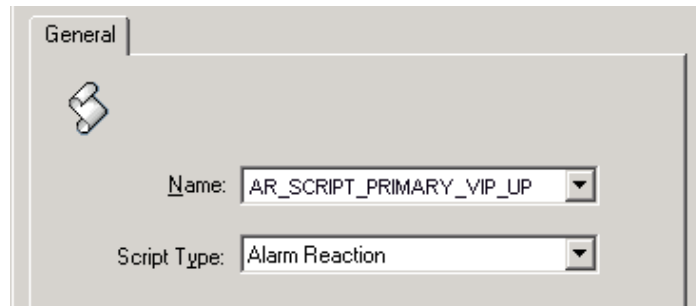


Figure 62: Configuring the Alarm Reaction Script: Sample Configuration

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.

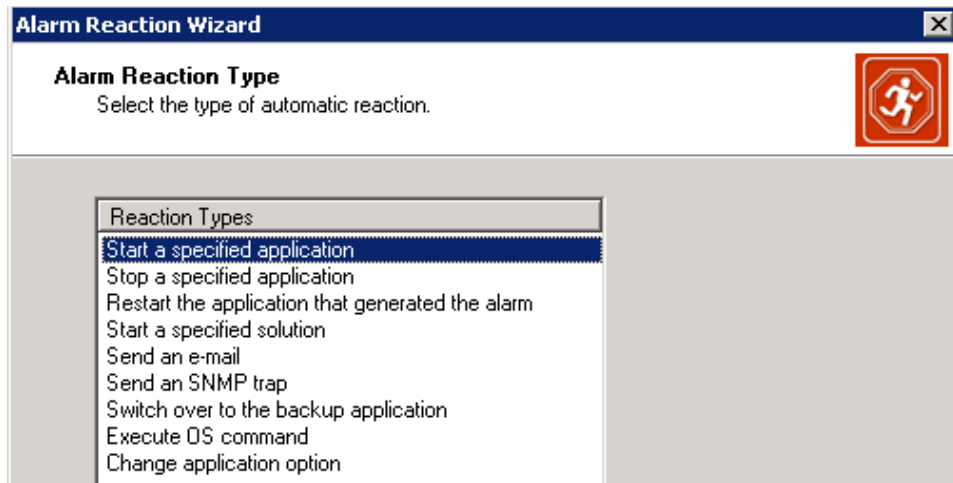


Figure 63: Alarm Reaction: Selecting the Alarm Reaction Type

- 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.

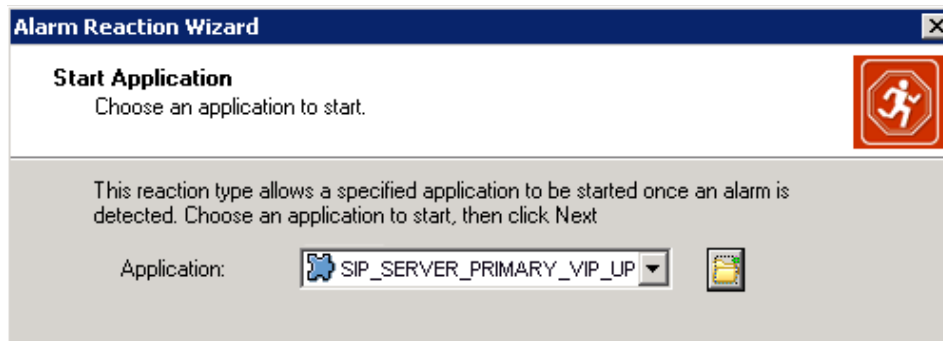


Figure 64: Alarm Reaction: Selecting the Application to Start

- e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in [Step 4](#).

End of procedure

Next Steps

- [Procedure: Creating Alarm Conditions \(IP Address Takeover on Linux\)](#)

Procedure: Creating Alarm Conditions (IP Address Takeover on Linux)

Purpose: Alarm Conditions are required to handle log events that occur when the primary or backup SIP Server changes its mode from primary to backup or from backup to primary. When you create the Alarm Conditions, you also configure them to trigger the Alarm Reaction scripts that you created previously.

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. [Tables 8](#) and [9](#) outline the Alarm Conditions for hot-standby and warm-standby configurations, respectively. Refer to the procedure that follows to create the Alarm Conditions that are required for your configuration.

For information about the log events for which you are creating Alarm Conditions, refer to “SIP Server HA Log Events” on [page 133](#).

Table 8: Alarm Conditions for Hot Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4561	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4561_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4563	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN, AR_SCRIPT_PRIMARY_VIP_UP
4561	SIP_SERVER_BACKUP	ALRM_BACKUP_4561_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4563	SIP_SERVER_BACKUP	ALRM_BACKUP_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Table 9: Alarm Conditions for Warm Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
4560	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4560_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4562	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4562_HAPrimary	AR_SCRIPT_PRIMARY_VIP_UP, AR_SCRIPT_BACKUP_VIP_DOWN
4560	SIP_SERVER_BACKUP	ALRM_BACKUP_4560_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4562	SIP_SERVER_BACKUP	ALRM_BACKUP_4562_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP, AR_SCRIPT_PRIMARY_VIP_DOWN

Start of procedure

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 a Name for the Alarm Condition—for example, ALRM_PRIMARY_4561_HABackup.
 - Optionally, enter a description.
 - For the Category value, select Critical.
 - Set Cancel Timeout to 1.

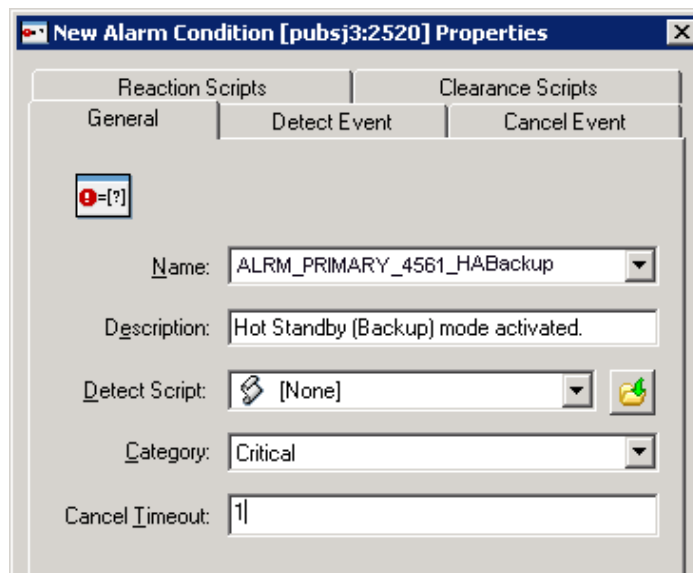


Figure 65: Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the Detect Event tab:
 - Set the Log Event ID as defined in Table 8 on [page 108](#) if you configure Hot Standby mode or as defined in Table 9 on [page 108](#) if you configure Warm Standby mode.
 - 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.

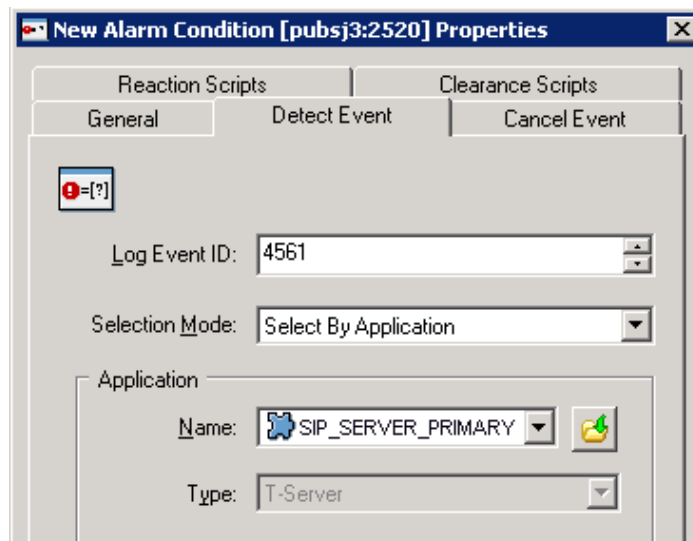


Figure 66: Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the Reaction Scripts tab, add the Alarm Reaction script as defined in Table 8 on [page 108](#) if you configure Hot Standby mode or as defined in Table 9 on [page 108](#) if you configure Warm Standby mode.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your hot-standby or warm-standby configuration.

End of procedure

Next Steps

- [Procedure: Testing Alarm Conditions \(IP Address Takeover on Linux\)](#)

Procedure: Testing Alarm Conditions (IP Address Takeover on Linux)

Purpose: To verify that the Alarm Conditions work as expected.

Start of procedure

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_4561_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_4561_HABackup Alarm Condition indicates that the primary SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP interface at the primary SIP Server and disable the Virtual IP interface at the backup SIP Server.
4. Use an `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 of procedure

Next Steps

- [Procedure: Testing your HA configuration, on page 130](#)

Windows NLB Cluster HA Deployment

Task Summary: Windows NLB Cluster HA Deployment

The following table provides an overview of the tasks that you must complete to deploy a highly available configuration of SIP Server in a Windows NLB Cluster environment.

Task Summary: Windows NLB Cluster HA Deployment

Objectives	Related procedures and information
Ensure that your system meets the deployment prerequisites.	“Prerequisites” on page 112 .
Configure Windows Network Load Balancing (NLB) parameters.	Use the Microsoft NLB Manager to configure load-balancing parameters, as described in Procedure: Configuring Windows NLB cluster parameters , on page 113 .
Deploy the SIP Server HA configuration.	<p>Complete the following procedures to deploy your SIP Server HA configuration:</p> <ol style="list-style-type: none"> 1. Procedure: Configuring the primary SIP Server (Windows NLB Cluster), on page 114. 2. Procedure: Configuring the backup SIP Server (Windows NLB Cluster), on page 117. 3. Procedure: Creating Cluster control scripts (Windows NLB Cluster), on page 120. Cluster control scripts are used to enable and disable SIP Server ports when SIP Servers change modes. 4. Procedure: Creating Application objects for Cluster control scripts (Windows NLB Cluster), on page 122. Application objects allow the Cluster control scripts to be run as applications. 5. Procedure: Creating Alarm Reaction scripts (Windows NLB Cluster), on page 124. Alarm Reaction scripts are called when HA-related Alarm Conditions are activated.

Task Summary: Windows NLB Cluster HA Deployment (Continued)

Objectives	Related procedures and information
Deploy the SIP Server HA configuration (continued).	6. Procedure: Creating Alarm Conditions (Windows NLB Cluster) , on page 126. When an HA-related log event occurs, such as a log event that records when a SIP Server changes from primary to backup mode, Alarm Conditions are activated. 7. Procedure: Testing Alarm Conditions (Windows NLB Cluster) , on page 129.
Verify the SIP Server HA configuration deployment.	Procedure: Testing your HA configuration , on page 130. In this procedure, you perform tests to ensure that your HA configuration works as expected.

Prerequisites

There are basic requirements and recommendations for deploying 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.
 - Message Server must be installed and configured.
- 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.

Deployment Procedures

Procedure:

Configuring Windows NLB cluster parameters

Purpose: To configure Windows NLB cluster parameters that are required for this type of SIP Server HA deployment.

Start of procedure

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 [Procedure: Configuring the primary SIP Server \(Windows NLB Cluster\)](#) for steps on configuring the sip-port.
 - 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 of procedure**Next Steps**

- [Procedure: Configuring the primary SIP Server \(Windows NLB Cluster\)](#)

Procedure:
Configuring the primary SIP Server (Windows NLB Cluster)

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

Start of procedure

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.

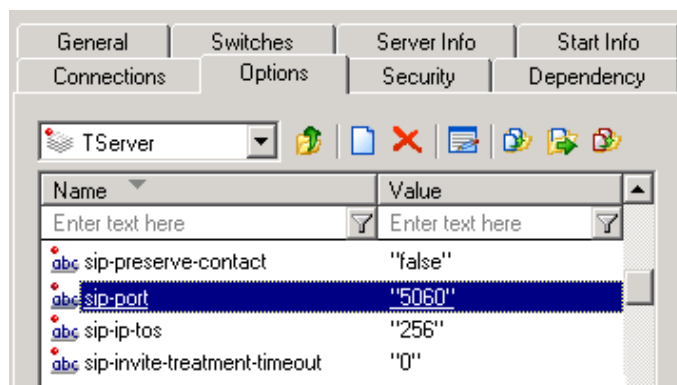


Figure 67: Configuring the sip-port Option: Sample Configuration

- ii. Set the sip-address option to the Windows NLB cluster IP address (the Virtual IP address).
 - iii. Click Apply to save the configuration changes.
- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.

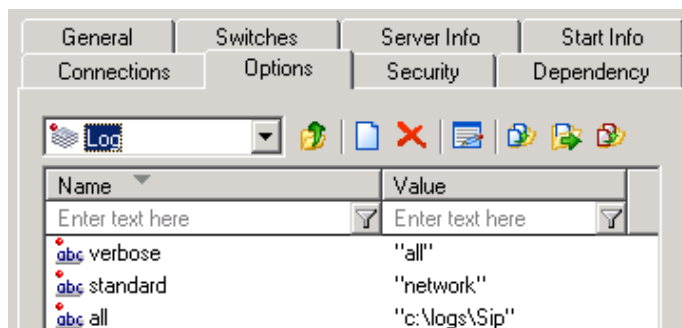


Figure 68: Configuring Log Options: Sample Configuration

Note: Setting logging options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. If you are deploying a hot-standby configuration, it is recommended that you enable the Advanced Disconnect Detection Protocol (ADDP) for communication between the primary and backup SIP Servers. To enable ADDP, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

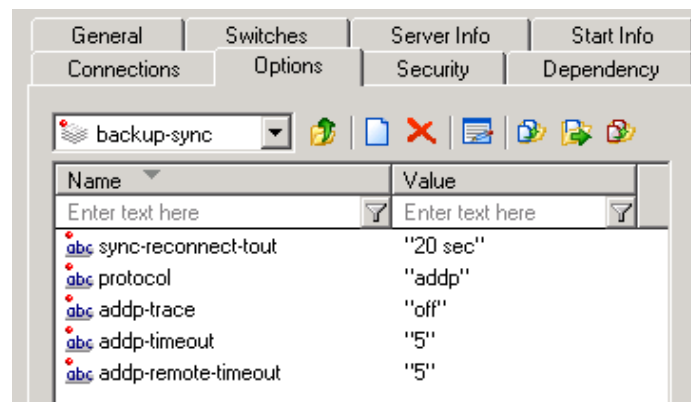


Figure 69: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click Apply to save the configuration changes.
5. 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.
6. 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.

- c. 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.
 - d. Click **Apply** to save the configuration changes.
7. Click the **Start Info** tab.
 - a. Select **Auto-Restart**.
 - b. Click **Apply** to save the configuration changes.
 8. Click the **Connections** tab, and then click **Add** to create a connection to the Message Server.
 9. Click **Apply** and then **OK** to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Configuring the backup SIP Server \(Windows NLB Cluster\)](#)

Procedure: Configuring the backup SIP Server (Windows NLB Cluster)

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

Start of procedure

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.

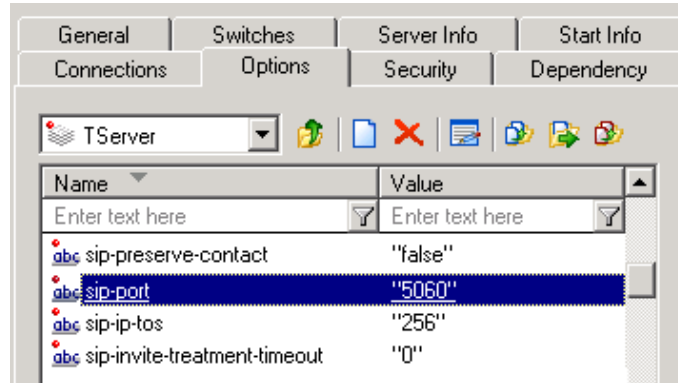


Figure 70: Configuring the sip-port Option: Sample Configuration

- ii. Set the sip-address option to the Windows NLB cluster IP address (the Virtual IP address).
- iii. Click Apply to save the configuration changes.
- b. Select the Log section.
 - i. Set the standard option to network.
 - ii. Set the verbose option to all.

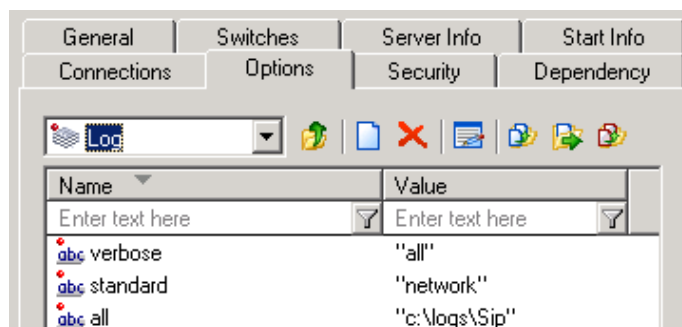


Figure 71: Configuring the Log Options: Sample Configuration

Note: Setting Log options is required for this SIP Server HA configuration. HA-related log events pass through the Message Server to activate Alarm Conditions and Alarm Reaction scripts that are necessary for managing switchover between the primary and backup SIP Servers.

- c. 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, perform the following steps:
 - i. Open the backup-sync section.
 - ii. Configure the following backup-sync options:
 - sync-reconnect-tout
 - protocol
 - addp-timeout
 - addp-remote-timeout

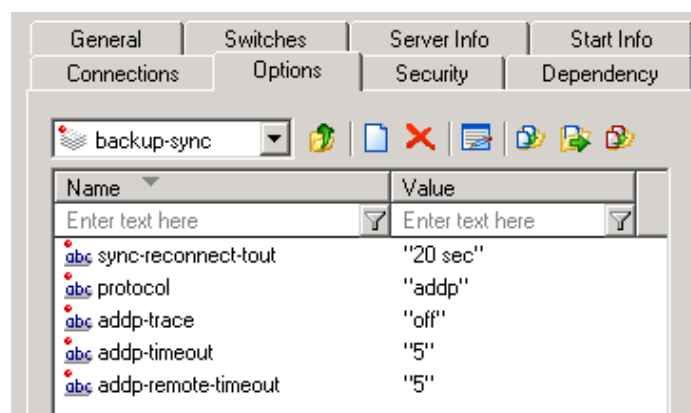


Figure 72: Configuring the backup-sync Options: Sample Configuration

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 “T-Server Common Functions and Procedures” chapter of the *Framework 8.0 SIP Server Deployment Guide*.

- d. Click **Apply** to save the configuration changes.
7. Click the **Connections** tab, and then click **Add** to create a connection to the same Message Server to which you created a connection for the primary SIP Server.
8. Click **Apply** and then **OK** to save the configuration changes.

End of procedure

Next Steps

- [Procedure: Creating Cluster control scripts \(Windows NLB Cluster\)](#)

Procedure: Creating Cluster control scripts (Windows NLB Cluster)

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 of procedure

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:

```
@title Enable Cluster Control Script
@echo ***** Primary Virtual IP Enabled ***** >>
vip1.log
@echo %time% >> vip1.log
wlbs.exe start sipcluster:1 >> vip1.log
wlbs.exe enable 5060 sipcluster:1 >> vip1.log
wlbs.exe disable 5060 sipcluster:2 >> vip1.log
exit
```

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:

```
@title Disable Cluster Control Script
@echo ***** Primary Virtual IP Disabled ***** >>
vip1.log
@echo %time% >> vip1.log
wlbs.exe disable 5060 sipcluster:1 >> 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:

```
@title Enable Cluster Control Script
@echo ***** Backup Virtual IP Enabled ***** >>
vip2.log
@echo %time% >> vip2.log
wlbs.exe start sipcluster:2 >> vip2.log
wlbs.exe enable 5060 sipcluster:2 >> vip2.log
wlbs.exe disable 5060 sipcluster:1 >> 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:

```
@title Disable Cluster Control Script
@echo ***** Backup Virtual IP Disabled ***** >>
vip2.log
@echo %time% >> vip2.log
wlbs.exe disable 5060 sipcluster:2 >> 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 of procedure

Next Steps

- [Procedure: Creating Application objects for Cluster control scripts \(Windows NLB Cluster\)](#)

Procedure: Creating Application objects for Cluster control scripts (Windows NLB Cluster)

Purpose: To create four Application objects of type Third Party Server: one for each of the Cluster control scripts that you created in [Procedure: Creating Cluster control scripts \(Windows NLB Cluster\)](#). 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 of procedure

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.

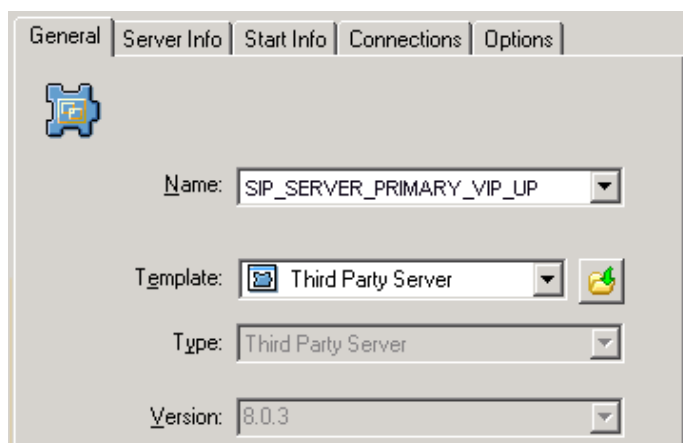


Figure 73: Configuring the Application Object for the Script, General Tab: Sample Configuration

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.

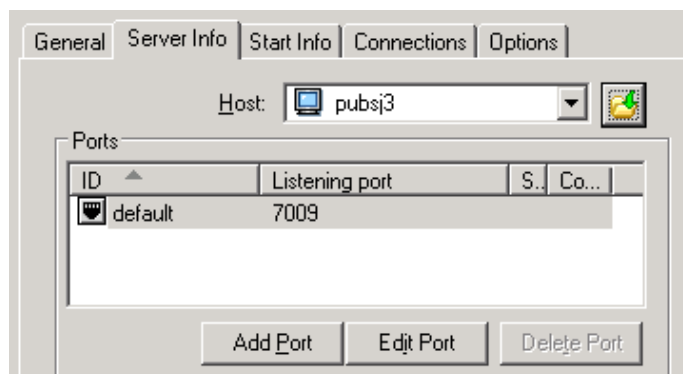


Figure 74: Configuring the Application Object for the Script, Server Info Tab: Sample Configuration

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`).

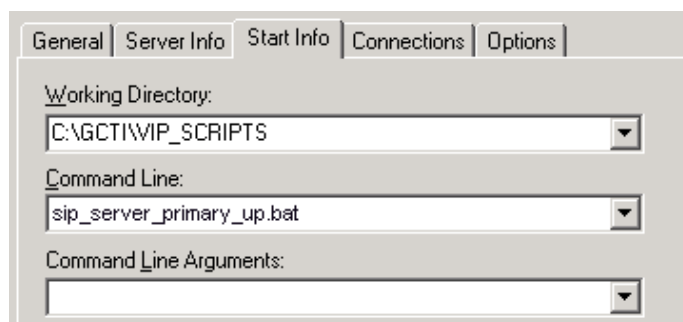


Figure 75: Configuring the Application Object for the Script, Start Info Tab: Sample Configuration

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

End of procedure

Next Steps

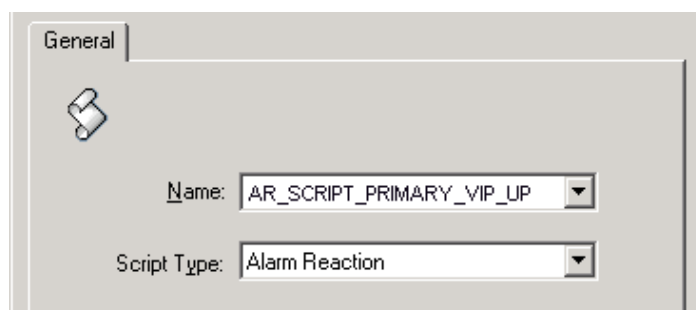
- [Procedure: Creating Alarm Reaction scripts \(Windows NLB Cluster\)](#)

Procedure: Creating Alarm Reaction scripts (Windows NLB Cluster)

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 [Procedure: Creating Application objects for Cluster control scripts \(Windows NLB Cluster\)](#), on page 122.

Start of procedure

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)

**Figure 76: 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.

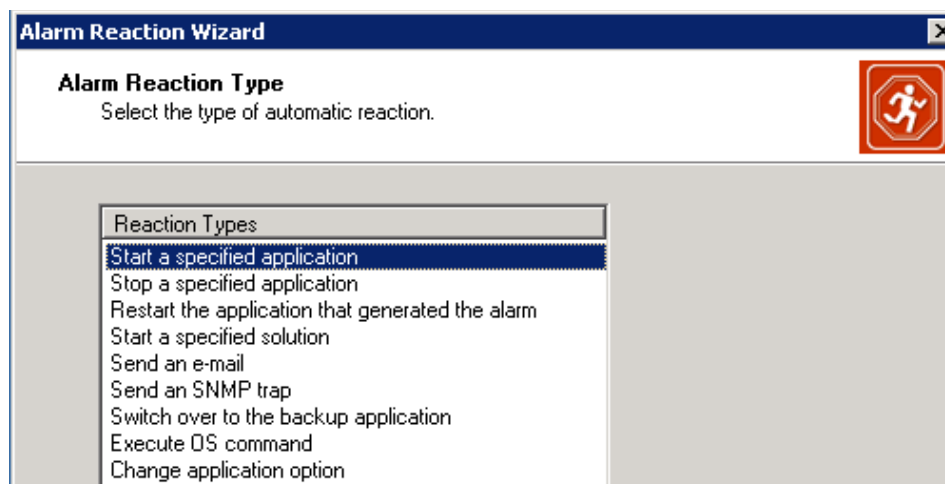


Figure 77: Alarm Reaction: Selecting the Alarm Reaction Type

- 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.

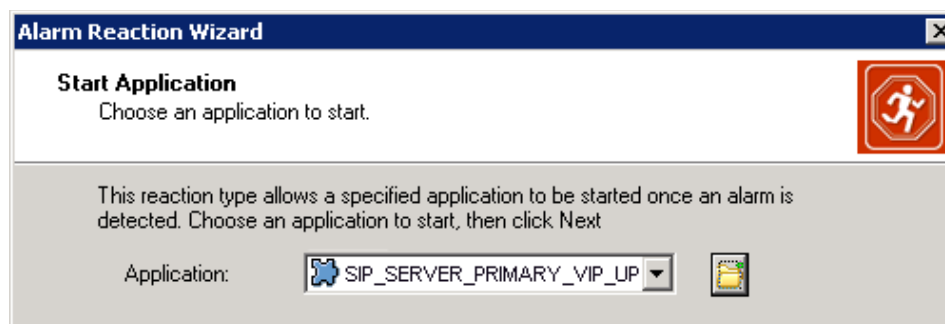


Figure 78: Alarm Reaction: Selecting an Application to Start

- e. Repeat the previous steps to configure each of the Alarm Reaction scripts that you created in [Step 4](#).

End of procedure

Next Steps

- [Procedure: Creating Alarm Conditions \(Windows NLB Cluster\)](#)

Procedure: Creating Alarm Conditions (Windows NLB Cluster)

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 configure them to trigger the Alarm Reaction scripts that you created in [Procedure: Creating Alarm Reaction scripts \(Windows NLB Cluster\)](#).

Four Alarm Conditions are required for your HA configuration: two for the primary SIP Server application and two for the backup. [Tables 10 and 11](#) outline the Alarm Conditions for Hot Standby and Warm Standby configurations, respectively. Refer to the procedure that follows to create the Alarm Conditions that are required for your configuration.

For information about the log events for which you are creating Alarm Conditions, refer to “SIP Server HA Log Events” on [page 133](#).

Table 10: Alarm Conditions for Hot Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Script
4561	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4561_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4563	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4563_HAPrimary	AR_SCRIPT_PRIMARY_VIP_UP
4561	SIP_SERVER_BACKUP	ALRM_BACKUP_4561_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4563	SIP_SERVER_BACKUP	ALRM_BACKUP_4563_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP

Table 11: Alarm Conditions for Warm Standby: Sample Configuration

Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Script
4560	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4560_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
4562	SIP_SERVER_PRIMARY	ALRM_PRIMARY_4562_HAPrimary	AR_SCRIPT_PRIMARY_VIP_UP
4560	SIP_SERVER_BACKUP	ALRM_BACKUP_4560_HABackup	AR_SCRIPT_BACKUP_VIP_DOWN
4562	SIP_SERVER_BACKUP	ALRM_BACKUP_4562_HAPrimary	AR_SCRIPT_BACKUP_VIP_UP

Start of procedure

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_4561_HABackup.
 - Optionally, enter a description.

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

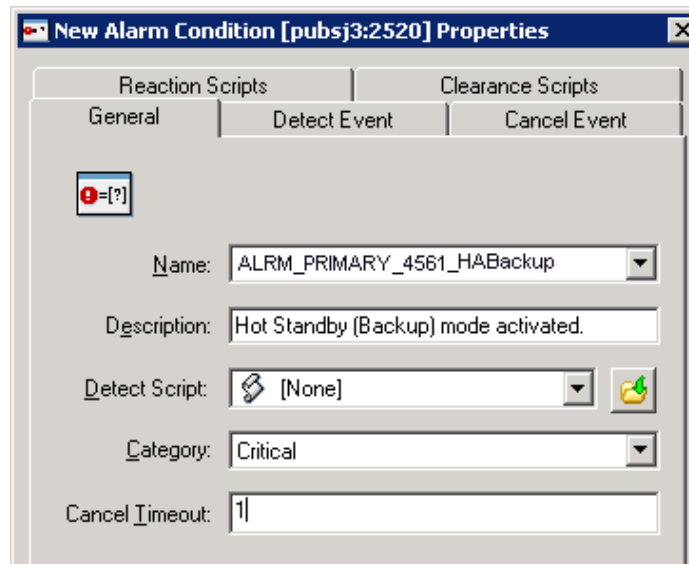


Figure 79: Configuring the Alarm Condition, General Tab: Sample Configuration

5. On the Detect Event tab:
 - Set the Log Event ID as defined in Table 10 on [page 127](#) if you configure Hot Standby mode or as defined in Table 11 on [page 127](#) if you configure Warm Standby mode.
 - 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.

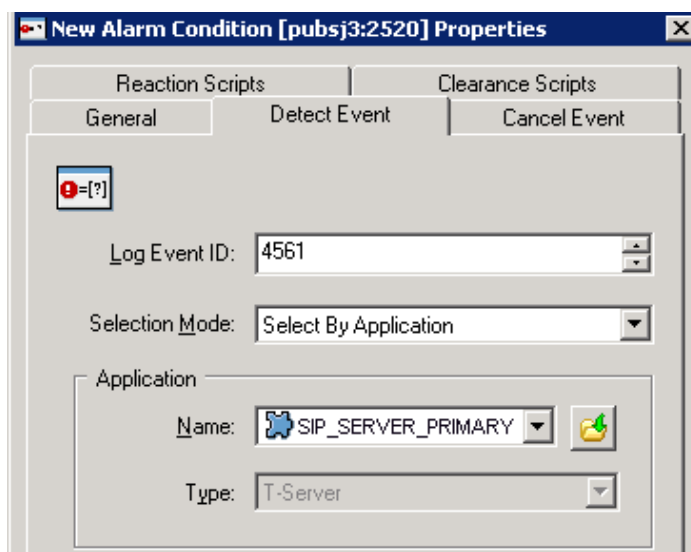


Figure 80: Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

6. Click OK.
7. On the Reaction Scripts tab, add the Alarm Reaction script as defined in Table 10 on [page 127](#) if you configure Hot Standby mode or as defined in Table 11 on [page 127](#) if you configure Warm Standby mode.
8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your Hot Standby or Warm Standby configuration.

End of procedure

Next Steps

- [Procedure: Testing Alarm Conditions \(Windows NLB Cluster\)](#)

Procedure: Testing Alarm Conditions (Windows NLB Cluster)

Purpose: To verify that the Alarm Conditions work as expected.

Start of procedure

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_4561_HABackup—right-click it, and then click Test. The ALRM_PRIMARY_4561_HABackup Alarm Condition indicates that the primary

SIP Server is in backup mode, which triggers the Alarm Reaction scripts that disable the Virtual IP port at the primary SIP Server and enable 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 of procedure

Next Steps

[Procedure: Testing your HA configuration](#), on [page 130](#)

SIP Server HA Configuration Testing

Use the following procedure to test your SIP Server HA deployment.

Procedure: Testing your 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 of procedure

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.
2. 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.
- 3. 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 of procedure



Appendix

SIP Server HA Log Events

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.

The log events for which Alarm Conditions defined are different for hot- and warm-standby configurations.

The following log events, which are relevant to SIP Server HA hot- and warm-standby configurations, respectively, are taken from the *Framework 8.0 Combined Log Events Help*.

Log Events for Hot-Standby Redundancy Type

00-04563

Level: Standard

Text: Hot Standby (Primary) mode activated

Attributes: None

Description: Management Layer command: reports that the primary server is working in Hot Standby mode.

00-04561

Level: Standard

Text: Hot Standby (backup) mode activated

Attributes: None

Description: Management Layer command: reports that the backup server is working in Hot Standby mode.

Log Events for Warm-Standby Redundancy Type

00-04560

Level: Standard

Text: Warm Standby (backup) mode activated

Attributes: None

Description: Management Layer command: reports that the backup server is working in Warm Standby mode.

00-04562

Level: Standard

Text: Warm Standby (Primary) mode activated

Attributes: None

Description: Management Layer command: reports that the primary server is working in Warm Standby mode.

When you set up your SIP Servers for the HA configuration, you create Alarm Conditions to be activated when the Management Layer detects log events that correspond to the redundancy type you have chosen for your configuration.

Two Alarm Conditions are created for the primary SIP Server application and two Alarm Conditions are created for the backup SIP Server application.

You need to configure the Alarm Conditions to execute Alarm Reaction scripts, which will instruct the Management Layer by means of the Application objects to launch the Virtual IP address control scripts or Cluster control scripts on SIP Server hosts.

As a result, the IP configuration of the host computer will be aligned with the run mode of the respective SIP Server application, and the switchover process will be complete successfully.



Supplements

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources, as necessary.

SIP Server

- The *Framework 8.0 Deployment Guide*, which will help you configure, install, start, and stop Framework components
- The *Framework 7.6 Stream Manager Deployment Guide*, which will help you configure, install, start, and stop Stream Manager

Management Framework

- The *Framework 8.0 Configuration Options Reference Manual*, which will provide you with descriptions of configuration options for other Framework components
- The *Framework 8.0 Configuration Manager Help*, which will help you use the Configuration Manager

Genesys

- The *Genesys Technical Publications Glossary*, which ships on the Genesys Documentation Library DVD and provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms that are used in this document.
- The *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD and provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support, for more information.

- Release Notes and Product Advisories for this product, which are available on the Genesys Technical Support website at <http://genesyslab.com/support>.

Information about supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *[Genesys Supported Operating Environment Reference Manual](#)*
- *[Genesys Supported Media Interfaces Reference Manual](#)*

Consult the following additional resources, as necessary:

- The *Genesys Hardware Sizing Guide*, which provides information about Genesys hardware sizing guidelines for the Genesys 8.x releases.
- The *Genesys Interoperability Guide*, which provides information about the compatibility of Genesys products with various Configuration Layer Environments; Interoperability of Reporting Templates and Solutions; and *Gplus* Adapters Interoperability.
- The *Genesys Licensing Guide*, which introduces you to the concepts, terminology, and procedures that are relevant to the Genesys licensing system.
- The *Genesys Database Sizing Estimator Worksheets*, which provides a range of expected database sizes for various Genesys products.

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Technical Support website, accessible from the [system level documents by release](#) tab in the Knowledge Base Browse Documents Section.

Genesys product documentation is available on the:

- Genesys Technical Support website at <http://genesyslab.com/support>.
- Genesys Documentation Library DVD, which you can order by e-mail from Genesys Order Management at orderman@genesyslab.com.

Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. The following is a sample version number:

80fr_ref_06-2008_v8.0.001.00

You will need this number when you are talking with Genesys Technical Support about this product.

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. The text that accompanies and explains the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

Type Styles

[Table 12](#) describes and illustrates the type conventions that are used in this document.

Table 12: Type Styles

Type Style	Used For	Examples
Italic	<ul style="list-style-type: none"> Document titles Emphasis Definitions of (or first references to) unfamiliar terms Mathematical variables <p>Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 138).</p>	<p>Please consult the <i>Genesys Migration Guide</i> for more information.</p> <p>Do <i>not</i> use this value for this option.</p> <p>A <i>customary and usual</i> practice is one that is widely accepted and used within a particular industry or profession.</p> <p>The formula, $x + 1 = 7$ where x stands for . . .</p>

Table 12: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like teletype or typewriter text)	<p>All programming identifiers and GUI elements. This convention includes:</p> <ul style="list-style-type: none"> The <i>names</i> of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages. The values of options. Logical arguments and command syntax. Code samples. <p>Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.</p>	<p>Select the Show variables on screen check box.</p> <p>In the Operand text box, enter your formula.</p> <p>Click OK to exit the Properties dialog box.</p> <p>T-Server distributes the error messages in EventError events.</p> <p>If you select true for the inbound-bsns-calls option, all established inbound calls on a local agent are considered business calls.</p> <p>Enter exit on the command line.</p>
Square brackets ([])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	smcp_server -host [/flags]
Angle brackets (< >)	<p>A placeholder for a value that the user must specify. This might be a DN or a port number that is specific to your enterprise.</p> <p>Note: In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.</p>	smcp_server -host <confighost>



Index

Symbols

[] (square brackets)	138
/etc/hosts	84
< > (angle brackets)	138

A

angle brackets	138
architecture	
Virtual IP-based HA	11
ARP table	17, 19
audience, for document	7

B

brackets	
angle	138
square	138

C

Check_ip.vbs	48
commenting on this document	8
conventions	
in document	137
type styles	137

D

document	
audience	7
change history	9
conventions	137
errors, commenting on	8
version number	137
Domain Name System (DNS)	112

F

F5 Networks BIG-IP LTM	
benefits and limitations	12
overview	20
font styles	
italic	137
monospace	138

H

High Availability	
comparing options	12
deployment testing	130
hot standby	13
IP Address Takeover	14
network device-based	19
overview	11
redundancy types	13
warm standby	14
Windows NLB Cluster	17
hot standby	
overview	13

I

intended audience	7
Internet Group Management Protocol (IGMP)	19
IP Address Takeover	
benefits and limitations	12
deployment notes	17
deployment on AIX	59
deployment on Linux	93
deployment on Solaris	76
deployment on Windows	37
manual-switchover workflow	24
overview	14
primary server–disconnected workflow	27
primary server–failure workflow	26
using one NIC	14

using two NICs	15
workflows	23
italics	137

M

MAC address	18
manual-switchover workflow	
IP Address Takeover	24
Windows NLB Cluster	30
monospace font	138
Multicast method	
Windows NLB Cluster	19

N

NetBIOS	113
Netsh command	17
Network device-based HA	
benefits	20
overview	19
nlb.exe	
Windows NLB Cluster utility	18

O

oos-check	
configuration option	22
oos-force	
configuration option	22

P

Ping.vbs	47
primary server-disconnected workflow	
IP Address Takeover	27
Windows NLB Cluster	32
primary server-failure workflow	
IP Address Takeover	26
Windows NLB Cluster	31

R

redundancy type	
hot standby	13
warm standby	14

S

set_ip_down.sh.	68, 85, 102
set_ip_up.sh	68, 85, 102
Single host HA	
overview	21

SIP traffic monitoring	
overview	21
sip-pass-check	
configuration option	22
square brackets	138

T

type styles	
conventions	137
italic	137
monospace	138
typographical styles	137

U

Unicast method	
Windows NLB Cluster.	18

V

version numbering, document	137
Virtual IP address	
concept	11
Virtual IP-based HA architecture.	11

W

warm standby	
overview	14
Windows Internet Name Service (WINS)	112
Windows NLB Cluster	
benefits and limitations	12
deployment	111
manual-switchover workflow	30
Multicast method	19
overview	17
primary server-disconnected workflow	32
primary server-failure workflow.	31
Unicast method	18
utility	18
workflows	29
Windows Server 2003	
limitation.	19
wlbs.exe	
Windows NLB Cluster utility	18