SIP Server HA Deployment Guide

Windows Server 2003

12/20/2025

Windows Server 2003

Complete these steps to set up SIP Server HA on Windows Server 2003, using the IP Address Takeover method.

IP Address Takeover HA Deployment on Windows

1. Check prerequisites.

Prerequisites

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

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

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

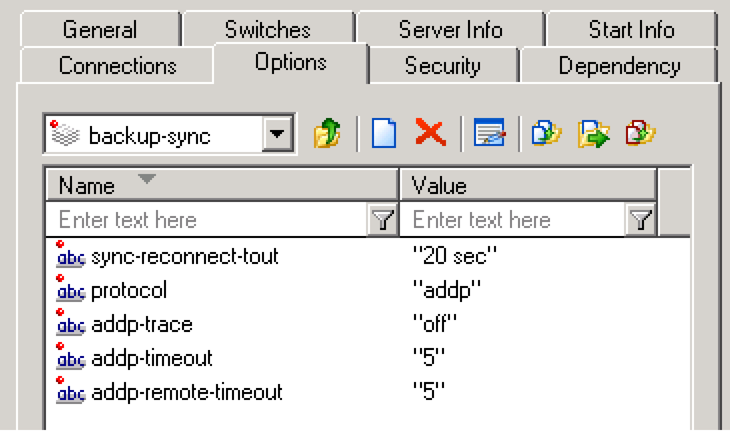
2. Configure the primary SIP Server.

Configuring the primary SIP Server

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

Start

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



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

Configuring the backup-sync Options: Sample Configuration

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

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

- Click the `Switches` tab.

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

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

- Click the `Server Info` tab.

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

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

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

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

iii. Click `OK`.

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

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

a. Select `Auto-Restart`.

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

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

End

3. Configure the backup SIP Server.

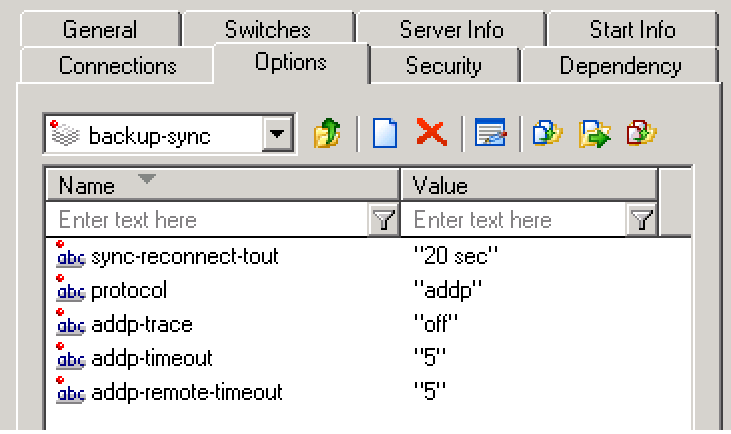
Configuring the backup SIP Server

Purpose

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

Start

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



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

Configuring the backup-sync Options: Sample Configuration

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

8. Click Apply to save the configuration changes.

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

End

4. Create Virtual IP address control scripts.

Creating Virtual IP address control scripts

Purpose

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

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

Start

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

```
@set VirtualIP=10.10.11.103
 @set vipMask=255.255.255.0
```

```
@set VirtualInterface="Local Area Connection"
@echo ********************* HA_IP_ON ********************** >>
Takeover.log
@echo %time% >> Takeover.log
@rem check if Virtual IP released on Backup host
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@if not errorlevel 1 goto ready
@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
@if not errorlevel 1 goto ready

@cscript.exe ping.vbs %VirtualIP% //Nologo >> Takeover.log
:ready
@rem Add VirtualIP
@netsh interface ip delete arpcache
netsh interface ip add address name=%VirtualInterface%
addr=%VirtualIP% mask=%vipMask% >> Takeover.log
@rem check if VirtualIP added succesefully if not do it again
@cscript.exe check_ip.vbs localhost %VirtualIP% //Nologo >>
Takeover.log
@if errorlevel 1 goto done
netsh interface ip delete address name=%VirtualInterface%
addr=%VirtualIP% >> Takeover.log
netsh interface ip add address name=%VirtualInterface%
addr=%VirtualIP% mask=%vipMask% >> 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 `HA_IP_ON.bat` script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.
3. In the second line of the `HA_IP_ON.bat` script, replace the `vipMask` value of `255.255.255.0` with your Virtual IP mask.
4. In the third line of the `HA_IP_ON.bat` script, ensure that the `VirtualInterface` value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
5. On the primary SIP Server host computer, create a batch file that is named `HA_IP_OFF.bat`, and enter the following commands into the file:
   [+] Commands for HA_IP_OFF.bat

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

6. In the first line of the `HA_IP_OFF.bat` script, replace the `VirtualIP` value of `10.10.11.103` with your Virtual IP address.
7. In the second line of the `HA_IP_OFF.bat` script, ensure that the `VirtualInterface` value is set to the NIC connection name that is defined in the Windows Network Connections dialog box.
8. Follow the steps in this procedure to create the same two scripts on the backup SIP Server host.
9. On the primary SIP Server host computer, create an accessory script that is named `Ping.vbs`, and enter the following commands into the script:

[+] Commands for Ping.vbs

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

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

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

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

End

5. Test Virtual IP address control scripts.

Testing Virtual IP address control scripts

Purpose

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

Start

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

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

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

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

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

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

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

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

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

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

End

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

Creating Application objects for Virtual IP address control scripts

Purpose

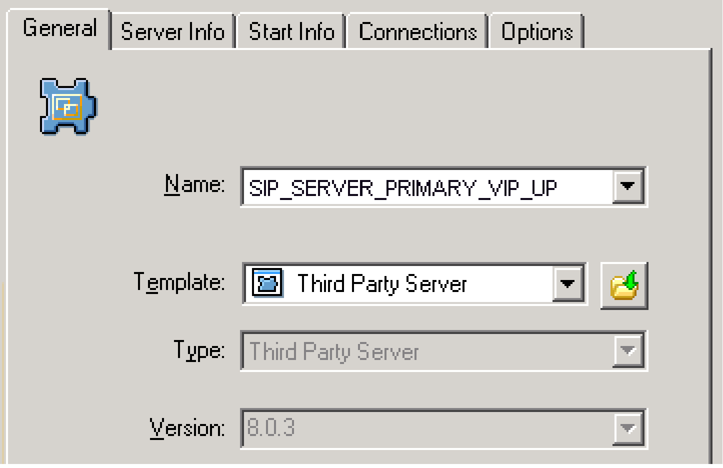
To create four Application objects of type `Third Party Server`: one for each of the scripts that you created in Step 4. For example:

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

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

Start

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



Name: SIP_SERVER_PRIMARY_VIP_UP

Template: Third Party Server

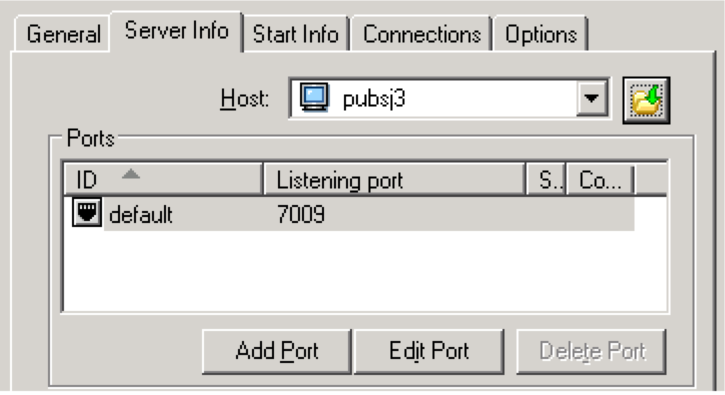
Type: Third Party Server

Version: 8.0.3

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

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

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



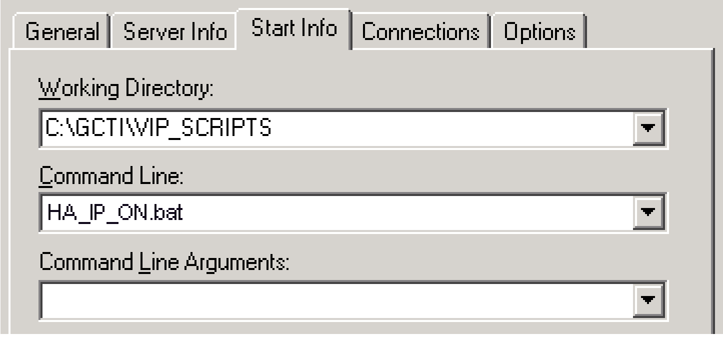
Host: pubsj3

Ports

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

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

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



Working Directory: C:\GCTI\VIP_SCRIPTS

Command Line: HA_IP_ON.bat

Command Line Arguments:

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

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

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

End

7. Create Alarm Reaction scripts

Creating Alarm Reaction scripts

Purpose

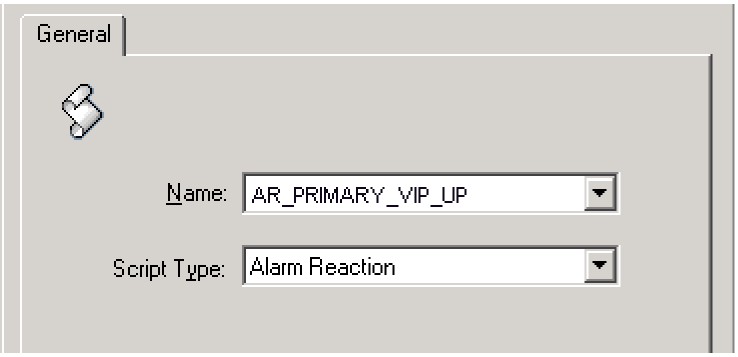
To create Alarm Reaction scripts for HA-related Alarm Conditions. When an HA-related Alarm Condition occurs, the associated Alarm Reaction script is run. Alarm Reaction scripts are configured to call the Application objects that you created in Step 6.

Start

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

backup SIP Server host)

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

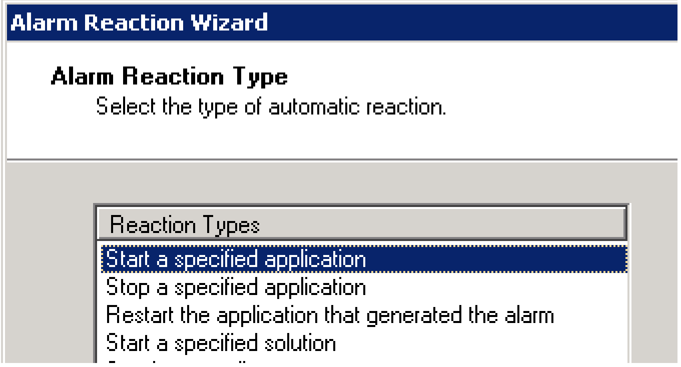


Name: AR_PRIMARY_VIP_UP

Script Type: Alarm Reaction

Configuring the Alarm Reaction Script: Sample Configuration

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



Alarm Reaction Wizard

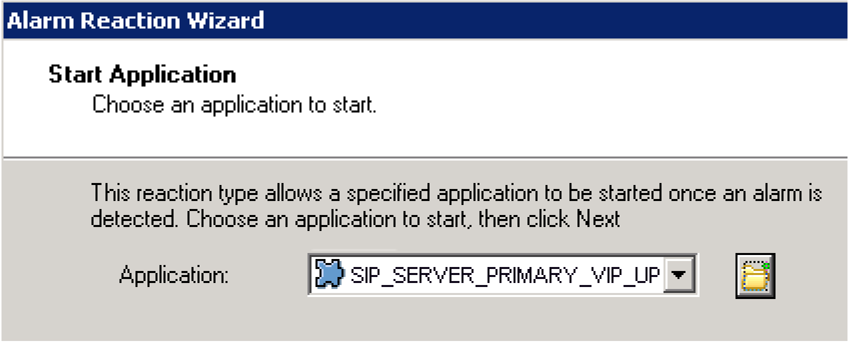
Alarm Reaction Type

Select the type of automatic reaction.

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

Alarm Reaction: Selecting the Alarm Reaction Type

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



Alarm Reaction Wizard

Start Application

Choose an application to start.

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

Application: SIP_SERVER_PRIMARY_VIP_UP

Alarm Reaction: Selecting the Application to Start

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

End

8. Create Alarm Conditions.

Creating Alarm Conditions

Purpose

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

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

Alarm Conditions: Sample Configuration

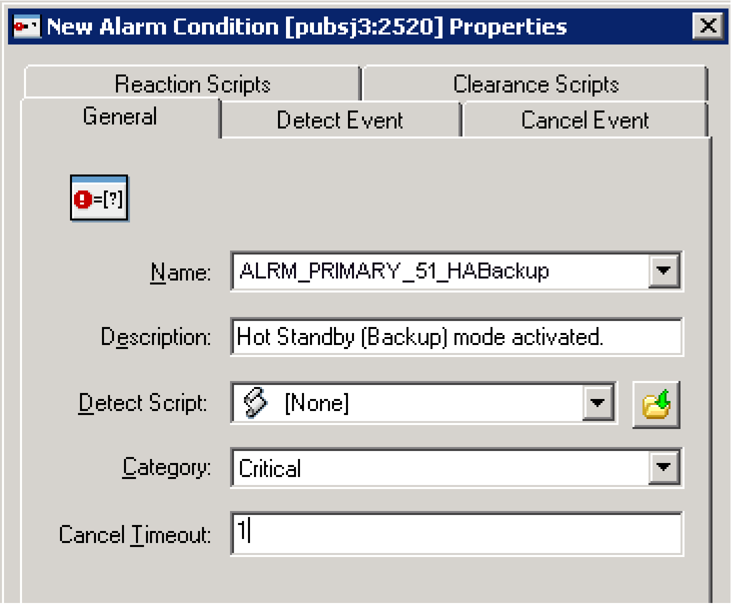
Log Event ID	SIP Server Application	Alarm Condition	Alarm Reaction Scripts
00-05151	SIP_SERVER_PRIMARY	ALRM_PRIMARY_51_HABackup	AR_SCRIPT_PRIMARY_VIP_DOWN
00-05150	SIP_SERVER_PRIMARY	ALRM_PRIMARY_50_HAPrimary	AR_SCRIPT_BACKUP_VIP_DOWN AR_SCRIPT_PRIMARY_VIP_UP
00-05151	SIP_SERVER_BACKUP	ALRM_BACKUP_51_HABackup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

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

Start

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

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



Name: ALRM_PRIMARY_51_HABackup

Description: Hot Standby (Backup) mode activated.

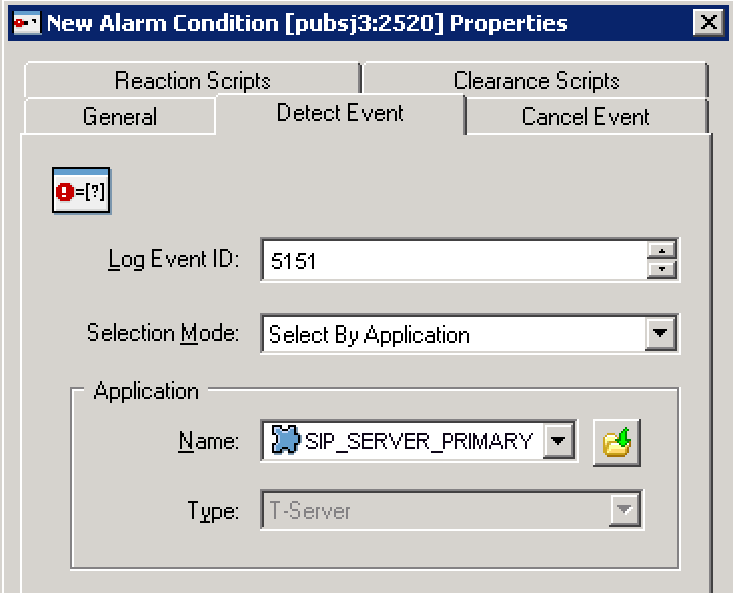
Detect Script: [None]

Category: Critical

Cancel Timeout: 1

Configuring the Alarm Condition, General Tab: Sample Configuration

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



Log Event ID: 5151

Selection Mode: Select By Application

Name: SIP_SERVER_PRIMARY

Type: T-Server

Configuring the Alarm Condition, Detect Event Tab: Sample Configuration

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

End

9. Test Alarm Conditions.

Testing Alarm Conditions

Purpose

To verify that the Alarm Conditions work as expected.

Start

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

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

End

10. Verify the HA configuration.

Testing your SIP Server HA configuration

Purpose

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

Prerequisites

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

Start

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

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

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

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

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

d. Release the call.

End