SIP Server HA Deployment Guide

Windows NLB Cluster

4/4/2026

Contents

- 1 Windows NLB Cluster
  - 1.1 Check prerequisites
  - 1.2 Configure Windows NLB parameters
  - 1.3 Configure the primary SIP Server
  - 1.4 Configure the backup SIP Server
  - 1.5 Create Cluster control scripts
  - 1.6 Creating Application objects for Cluster control scripts
  - 1.7 Verify the HA configuration

Windows NLB Cluster

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

1. Check prerequisites
2. Configure Windows NLB parameters
3. Configure the primary SIP Server
4. Configure the backup SIP Server
5. Create Cluster control scripts
6. Create Application objects for Cluster control scripts
7. Verify the HA configuration

Check prerequisites

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

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

> **Important**
>
> 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 2008 or later with Microsoft Windows Network Load Balancing (NLB).
- Software requirements:
  - SIP Server must be installed and configured on both host computers.
  - Local Control Agent (LCA) release 8.1.2 or higher must be installed and configured on both host computers.
- Networking requirements:
  - A name-resolution method such as Domain Name System (DNS), DNS dynamic-update protocol, or Windows Internet Name Service (WINS) is required.
  - Both host computers must be members of the same domain.

- A domain-level account that is a member of the local Administrators group is required on each host computer. A dedicated account is recommended.
- Each host computer must have a unique NetBIOS name.
- A static IP address is required for each of the network interfaces on both host computers.

> **Important**
>
> 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.

Configure Windows NLB parameters

1. Open the Microsoft Network Load Balancing Manager tool.
2. Select a cluster host, and open the `Cluster Properties` window.
3. On the `Cluster Parameters` tab, select the `Cluster operation mode`. You can choose either Unicast (default) or Multicast mode. For information about Windows NLB Unicast and Multicast modes, refer to your Microsoft Windows Server documentation.
4. Click the `Port Rules` tab.
   a. Specify a `Port range` that includes the port that you will assign as the `sip-port`. See "Configuring the primary SIP Server".
   b. In the `Protocols` section, select `Both` (both UDP and TCP).
   c. In the `Filtering mode` section, select `Multiple host`, and set `Affinity` to either `None` or `Single`.

   d. Set `Load weight` to `Equal`.

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

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

Configure the primary SIP Server

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 Windows NLB cluster IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the primary SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (`SIP_SERVER_PRIMARY_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the primary SIP Server host.
      vi. Disable Virtual IP address monitoring by setting the **sip-iptakeover-monitoring** option to `false`.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the `sip-nic-address` option and set the **sip-nic-monitoring** option to `true`.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.
      x. 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, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**

- **addp-timeout**
- **addp-remote-timeout**

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 5 sec or 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.

> **Important**
>
> For more information about ADDP configuration parameters, see the "Backup-Synchronization Section" section in the Framework 8.1 SIP Server Deployment Guide.

c. 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.
   d. 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.
   e. 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 Apply and then OK to save the configuration changes.

Configure the backup SIP Server

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 Windows NLB cluster IP address.
      iii. Set the **control-vip-scripts** option to `true`.
      iv. Set the **sip-vip-script-up** option to the name of the Application object (`SIP_SERVER_BACKUP_VIP_UP`) that will be created later for a script that enables the Virtual IP address on the backup SIP Server host.
      v. Set the **sip-vip-script-down** option to the name of the Application object (`SIP_SERVER_BACKUP_VIP_DOWN`) that will be created later for a script that disables the Virtual IP address on the backup SIP Server host.
      vi. Disable Virtual IP address monitoring by setting the **sip-iptakeover-monitoring** option to `false`.
      vii. To enable NIC status monitoring, set the **tlib-nic-monitoring** option to `true`.
      viii. To enable SIP NIC status monitoring, in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), configure the **sip-nic-address** option and set the **sip-nic-monitoring** option to `true`.
      ix. To enable SIP traffic monitoring, set the **sip-pass-check** option to `true`.
      x. Click `Apply` to save the configuration changes.
   b. 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, select the **[backup-sync]** section, and configure the following options:
      - **sync-reconnect-tout**
      - **protocol**
      - **addp-timeout**
      - **addp-remote-timeout**

      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 5 sec or 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.
   c. Click `Apply` to save the configuration changes.
7. Click `Apply` and then `OK` to save the configuration changes.

Create Cluster control scripts

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

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

   where:

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

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

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

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

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

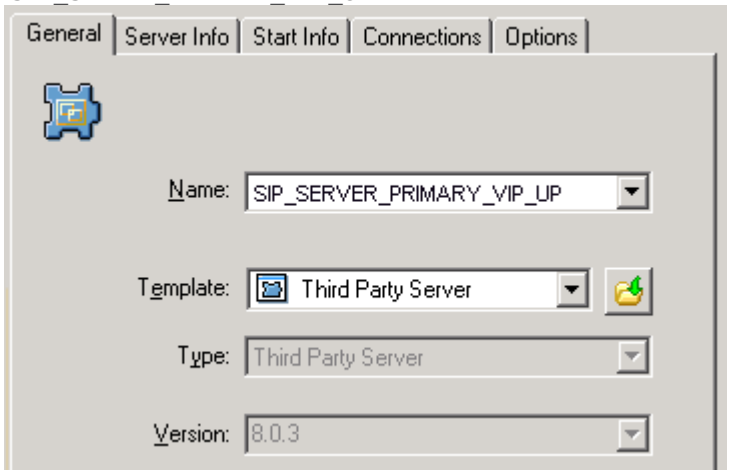
4. On the backup SIP Server host computer, create a batch file that is named `sip_server_backup_vip_down.bat` and enter the following commands:
   [+] Commands for sip_server_backup_vip_down.bat

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

> **Important**
> The preceding scripts include commands for logging script execution. The logs are created in the directory in which the script is located.

Creating Application objects for Cluster control scripts

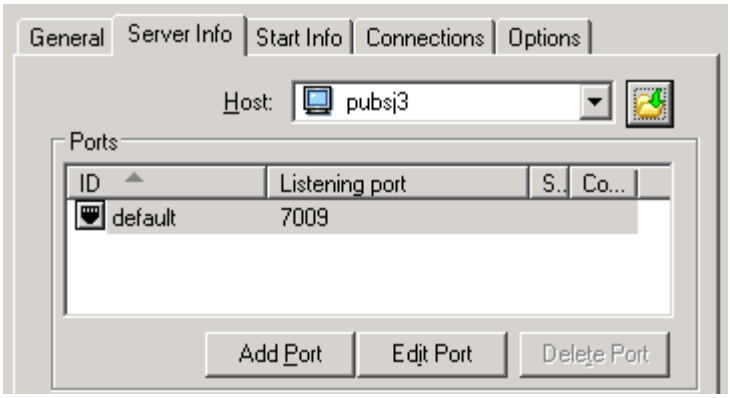
1. In the Configuration Manager, select `Environment > Applications`.
2. Right-click and select `New > Application`.
3. Select the Third Party Server template from the Application Templates folder, and click OK.
4. On the `General` tab, enter the name for the Application object—for example, `SIP_SERVER_PRIMARY_VIP_UP`.



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

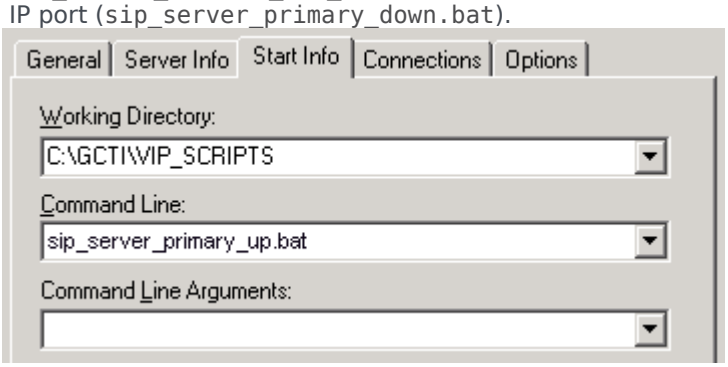
> **Important**
> You can use the suggested Application object names, or you can specify your own.

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.



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`).



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

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

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

Verify the HA configuration

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.