



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

UC Connector Deployment Guide

UC Connector HA Deployment Procedures

12/18/2025

UC Connector HA Deployment Procedures

Note: The information below presents an NLB cluster approach rather than the recommended **IP Address Takeover Approach**.

Windows NLB Cluster HA Deployment Prerequisite

Windows NLB Cluster HA Deployment Prerequisites

- Two separate physical host computers, one for the primary UC Connector and one for the backup UC Connector.
- Software requirements:
 - UC Connector must be installed and configured on both host computers.
 - A Local Control Agent (LCA) must be installed and configured on both host computers.
 - A Message Server must be installed.
- 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.  Server clustering does not support IP addresses assigned through DHCP.
 - A dedicated network switch or separate VLAN for cluster adapters is recommended to reduce switch flooding that may be caused by Windows Network Load Balancing.
 - Access to a domain controller is required. If the cluster service is unable to authenticate the user account used to start the service, the cluster may 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 the other for the node-to-node private cluster network.
 - A dedicated private network adapter is required for HCL certification.
 - All nodes must have two physically independent LANs or Virtual LANs 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.

Configuring Windows NLB cluster parameters

Configuring Windows NLB cluster parameters

Purpose: To configure Windows Network Load Balancing (NLB) parameters required for a UC Connector HA deployment.

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 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.
 - Specify a Port range that includes the port that you will assign as the web port.
 - In the Protocols section, select Both (for both UDP and TCP).
 - In the Filtering mode section, select Multiple host and set Affinity to None or Single.
 - 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.

Configuring the primary UC Connector (Windows NLB cluster)

Configuring the primary UC Connector (Windows NLB cluster)

Purpose: To configure the primary UC Connector Application object for high availability.

1. Stop the UC Connector service on the primary and backup hosts. Genesys UC Connector services can be stopped using the Windows Services dialog box.
2. Change the HTTP host to the virtual IP address for the Windows NLB cluster. In the UC Connector

Application object, go to the Start Info tab and modify the Command Line Arguments as follows:
`-ucc_host <Virtual_IP_address_of_NLB_cluster>`

3. Make sure that the HTTP port is one that can be shared on both primary and backup UC Connector hosts. To check the primary HTTP port, go to the Command Line Arguments and take note of the port number specified by the following parameter:
`-http_port <shared_port_number>`

Important

Modifying the Command Line Arguments is suggested for enabling

HA on existing UC Connector instances only. If you are deploying new instances of UC Connector for HA, you can specify these Host and Port parameters in the User Parameters page of the Installation wizard. The same rules apply:

- Set `ucc_host` for both primary and backup to the same virtual IP address of the Windows NLB cluster.
- Set `http_port` for both primary and backup to the same value.

4. Open Configuration Manager.

5. Select the Applications folder and right click the UC Connector Application object that you want to configure as the primary UC Connector. Select Properties.

6. Click the Options tab, Log section.

- Set the standard option to network.
- Set the verbose option to `all`.

Important

Setting logging options is required for this UC Connector HA

configuration. HA-related log events pass through the Message Server to activate alarm conditions and reaction scripts necessary for managing failover between the primary and backup instances of

UC Connector.

- Click Apply to save the configuration changes.

7. Click the Server Info tab.

- Set the Redundancy Type to Warm Standby.
- For the Backup Server option, select the UC Connector Application object you want to use as the backup UC Connector. If necessary, browse to locate the backup UC Connector Application object.
- Click Apply to save the configuration changes.

8. Click the Start Info tab.

- Select Auto-Restart.
- Click Apply to save the configuration changes.

9. Click the Connections tab, and then click Add to create a connection to the Message Server.

10. Click Apply and OK to save the configuration changes.

Configuring the Backup UC Connector (Windows NLB cluster)

Configuring the Backup UC Connector (Windows NLB cluster)

Purpose: To configure the backup UC Connector Application object for high availability.

1. Stop both primary and backup UC Connectors if they are running. You can stop the UC Connector service using the Windows Services dialog.

2. Change the HTTP host to the virtual IP address for the Windows NLB cluster. In the UC Connector Application object, go to the Start Info tab and modify the Command Line Arguments as follows:
`-ucc_host to ucc_host <Virtual_IP_address_of_NLB_cluster>`

3. Assign the same HTTP port as used in the primary UC Connector host. Go to the Command Line Arguments and enter the shared port number in the following parameter:
`-ucc_port <shared_port_number>`

Important

Modifying the Command Line Arguments is suggested for enabling HA on existing UC Connector instances only. If you are deploying new UC Connectors for HA, you can specify these Host and Port parameters in the User Parameters page of the Installation wizard. The same rules apply:

- Set `ucc_host` for both primary and backup to the same virtual IP address of the NLB cluster.
- Set `http_port` for both primary and backup to the same value.

4. Open Configuration Manager.

5. Select the Applications folder and right click on the UC Connector application object that you want to configure as the backup UC Connector.

6. Click the Start Info tab.

- Select Auto-Restart.
- Click Apply to save the configuration changes.

7. Click the Options tab, Log section.

- Set the standard option to network.
- Set the verbose option to all.

Important

Setting Log options is required for this UC Connector HA configuration. HA related log events pass through the Message Server to activate alarm conditions and reaction scripts necessary for managing failover between the primary and backup UC Connectors.

- Click Apply to save the configuration changes.

8. Click Apply and OK to save the configuration changes.

Configuring HA for Custom Server

Configuring HA for Custom Server

Purpose: To complete the configuration steps required to support integration of Custom Server with the Windows NLB virtual IP address.

Custom Server does not need to be deployed in an HA pair. However, the Custom Server application must be configured on a host created for the virtual IP address.

1. In Configuration Manager, create a new Host object, specifying the IP address that you configured as the virtual IP for the NLB cluster.
2. Create a new Custom Server Application object, specifying this virtual IP-based Genesys host. For details about creating this object, see [Creating the Custom Server Application object](#).

Creating Virtual IP Interface control scripts (Windows NLB cluster)

Creating Virtual IP Interface control scripts (Windows NLB cluster)

Purpose: To create Virtual IP (VIP) control scripts for each of the UC Connectors. Each UC Connector host requires VIP control scripts to enable or disable the Virtual IP (VIP) interface on the host computer when the role of the UC Connector changes. The scripts are used to enable the VIP interface on the host where the UC Connector is in primary mode and disabled the VIP interface on the host where the UC Connector is in backup mode.

In this procedure, you will create the following four VIP Control Scripts:

- `uc_connector_prime_up.bat`: Enables the VIP interface on the primary host.
- `uc_connector_prime_down.bat`: Disables the VIP interface on the primary host
- `uc_connector_backup_up.bat`: Enables the VIP interface on the backup host
- `uc_connector_backup_down.bat`: Disables the VIP interface on the backup host

Important

You can use the script names listed above or you can specify your own script names. If you get security-related error messages for these scripts, you may need to add a password parameter to the `wlbs.exe` commands. For example, add `/PASSW <your_password>` to the command: `wlbs.exe enable 5060 123.45.68.90:2 /PASSW yourpass123`

1. On the primary UC Connector host, create a batch file named `uc_connector_prime_up.bat` and

input the following commands:

```
@title Enable Virtual IP Control Script
@echo ***** Primary VIP Enabled ***** >> vip1.log
@echo %time% >> vip1.log
wlbs.exe start uccluster:1 >> vip1.log
wlbs.exe enable <your_web_port> uccluster:1 >> vip1.log
wlbs.exe enable <your_Custom_Server_port> uccluster:1 >> vip1.log
wlbs.exe disable <your_web_port> uccluster:2 >> vip1.log
wlbs.exe enable <your_Custom_Server_port> uccluster:2 >> vip1.log
exit
```

2. On the primary UC Connector host, create a batch file named `uc_connector_prime_down.bat` and input the following commands:

```
@title Disable Virtual IP Control Script
@echo ***** Primary VIP Disabled ***** >> vip1.log
@echo %time% >> vip1.log
wlbs.exe disable <your_web_port> uccluster:1 >> vip1.log
wlbs.exe disable <your_Custom_Server_port> uccluster:1 >> vip1.log
ping -n 2 127.0.0.1
exit
```

3. On the backup UC Connector host, create a batch file named `uc_connector_backup_up.bat` and input the following commands:

```
@title Enable Virtual IP Control Script
@echo ***** Backup VIP Enabled ***** >> vip2.log
@echo %time% >> vip2.log
wlbs.exe start uccluster:2 >> vip2.log
wlbs.exe enable <your_web_port> uccluster:2 >> vip2.log
wlbs.exe enable <your_Custom_Server_port> uccluster:2 >> vip2.log
wlbs.exe disable <your_web_port> uccluster:1 >> vip2.log
wlbs.exe disable <your_Customer_Server_port> uccluster:1 >> vip2.log
exit
```

4. On the backup UC Connector host, create a batch file named `uc_connector_backup_down.bat` and input the following commands:

```
@title Disable Virtual IP Control Script
@echo ***** Backup VIP Disabled ***** >> vip2.log
@echo %time% >> vip2.log
wlbs.exe disable <your_web_port> uccluster:2 >> vip2.log
wlbs.exe disable <your_Custom_Server_port> uccluster:2 >> vip2.log
ping -n 2 127.0.0.1
exit
```

Important

The scripts above include commands to log script execution. The logs are created in the directory where the script is located.

Creating application objects for VIP control scripts (Windows NLB)

cluster)

Creating application objects for VIP control scripts (Windows NLB cluster)

Purpose: To create the four “Third Party Server” application objects listed below; one for each of the VIP control scripts created in [Creating Virtual IP Interface control scripts \(Windows NLB cluster\)](#).

- uc_connector_Prime_Up
- uc_connector_Prime_Down
- uc_connector_Backup_Up
- uc_connector_Backup_Down

Creating application objects for the VIP control scripts allows the scripts to be run as applications within the Genesys framework.

Prerequisites

The Third Party Server template must already exist in the Application Templates folder. If not, right-click this folder, select Import Application Template, and import the Third Party Server template from your Management Framework CD.

1. In 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.

Important

You can use the application object names listed above or you can specify your own.

5. Select the Server Info tab.
 - Select the host name of the UC Connector where the corresponding VIP control script is located.
 - If necessary, specify a valid communication port number using the Edit Port option.

Important

This port will not be used. However, because of the way the application works, the port may have to be specified in order to save the application.

6. Select the **Start Info** tab.

- Set the **Working Directory** to the location of the control script and enter name of the script in the **Command Line** field.
- If you are configuring an application object that disables a VIP interface (uc_connector_Prime_Down and uc_connector_Backup_Down), set the **Timeout Startup** value to 8.

7. Repeat the steps in this procedure to create application objects for each of the four VIP control scripts.

Creating alarm reaction scripts (Windows NLB cluster)

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 you created in [Creating application objects for VIP control scripts \(Windows NLB cluster\)](#).

1. Open Configuration Manager.

2. Select **Resources > Scripts**.

3. Right click and select **New > Script**.

4. Create four scripts, one for each of the applications objects you created earlier. Select **Alarm Reaction** as the **Script Type**. For example, create the following four Alarm Reaction scripts:

- AR_Script_Prime_Up
- AR_Script_Prime_Down
- AR_Script_Backup_Up
- AR_Script_Backup_Down

5. For each of the Alarm Reaction scripts, use the Alarm Reaction Wizard to configure the **Alarm Reaction Type**.

- Select an Alarm Reaction script and right-click to open the Alarm Reaction Wizard (select Wizard > Configure).
- In the Alarm Reaction Wizard, click Next.
- In the Alarm Reaction Type dialog, select Start a specified application and click Next.
- Browse to select the corresponding application object. For example, for the AR_Script_Prime_Up Alarm Reaction script, select the uc_connector_Prime_Up Third Party Server application object.
- Repeat the previous steps to configure each of the Alarm Reaction scripts you created.

Creating alarm conditions (Windows NLB cluster)

Creating alarm conditions (Windows NLB cluster)

Purpose: Alarm Conditions are required to handle log events that occur when a UC Connector changes its mode from primary to backup or backup to primary. When you create the Alarm Conditions, you configure them to trigger the alarm reaction scripts you created in [Creating alarm reaction scripts \(Windows NLB cluster\)](#).

Four alarm conditions are required for your HA configuration, two for the primary UC Connector application and two for the backup. Refer to the procedure that follows to create the alarm conditions required for your configuration.

Alarm Conditions for Warm Standby

Name	Log Event ID	Application	Reaction Script
ALRM_Primary_down_4560	4560	<Primary UC Connector>	AR_Script_Prime_Down
ALRM_Primary_up_4562	4562	<Primary UC Connector>	AR_Script_Prime_Up
ALRM_Backup_down_4560	4560	<Backup UC Connector>	AR_Script_Backup_Down
ALRM_Backup_up_4562	4562	<Backup UC Connector>	AR_Script_Backup_Up

1. Open 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.
4. On the General tab:
 - Enter a Name for the Alarm Condition.
 - Optionally, enter a description.

- For the Category value, select Critical.
- Set Cancel Timeout to 3.

5. On the Detect Event tab:

- Set the Log Event ID.
- Set the Selection Mode to Select By Application.
- For the Application Name field, click the folder icon to browse for the UC Connector Application object. If you are creating an Alarm Condition for the primary UC Connector, select the primary UC Connector application object. If you are creating an Alarm Condition for the backup UC Connector, select the backup UC Connector application object.

6. Click OK.

7. On the Reaction Scripts tab, add the alarm reaction script as defined according to the table at the beginning of this procedure.

8. Repeat the steps in this procedure to create each of the four Alarm Conditions for your hot or warm standby configuration.

Testing alarm conditions (Windows NLB cluster)

Testing alarm conditions (Windows NLB cluster)

Purpose: To verify that the alarm conditions work as expected.

1. Open the Solution Control Interface (SCI).

2. Under Alarm Conditions, select the ALRM_Primary_4561 Alarm Condition, right click, and click Test. The ALRM_Primary_4561 Alarm Condition indicates that the primary UC Connector is in backup mode which triggers the alarm reaction scripts that disable the Virtual IP interface at the primary UC Connector and disable the VIP interface at the backup UC Connector.

3. Use an `wlbs queryport <your_web_port> or <your_Custom_Server_port>` command to verify that the Virtual IP interface is active on the backup UC Connector and that the Virtual IP interface is inactive on the primary UC Connector.