Manuals+ — User Manuals Simplified.

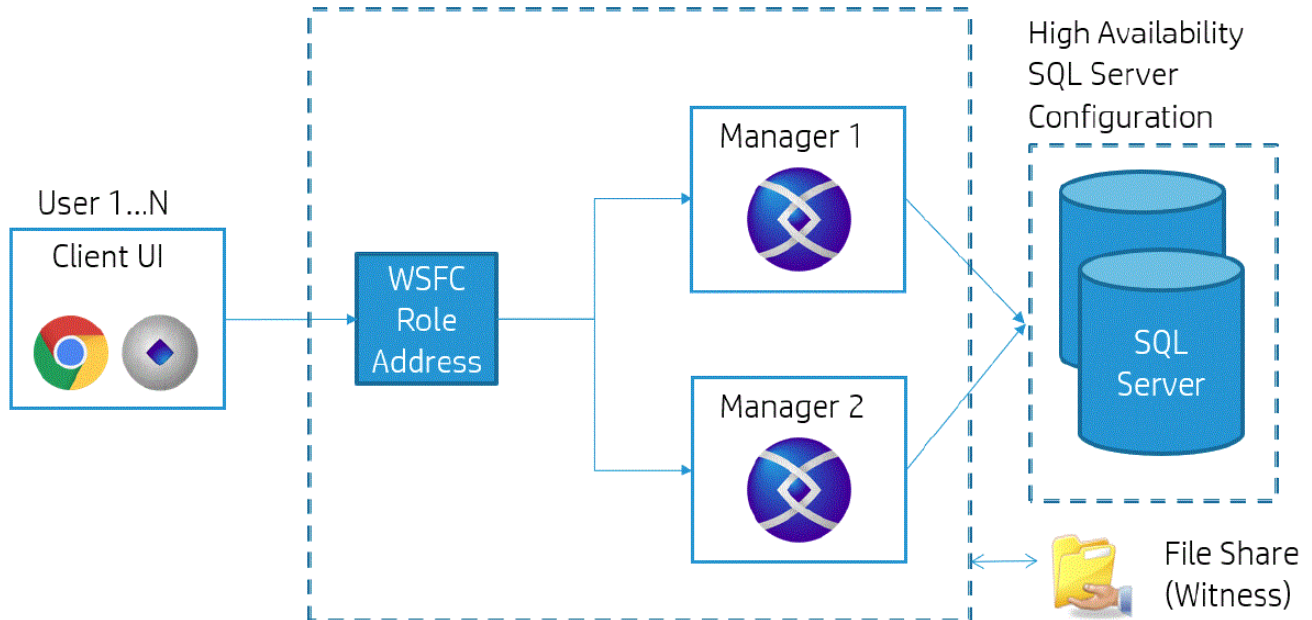# hp ZCentral Connect Failover Software User Guide

Contents

hp ZCentral Connect Failover Software

Overview

Failover can be configured for the HP ZCentral Connect Manager, allowing redundancy and higher uptime. It works by keeping an instance of the Manager in an active state, and another instance of the Manager in an inactive state. Both Manager instances share the same network address and the same database, thus containing the same data. When one instance fails, an automatic failover occurs and the inactive instance takes over and becomes active. In this case, the end user experience is similar to that of a Manager restarting. Agents will disconnect briefly, but will automatically reconnect within a few minutes. This guide provides steps and requirements on how to configure a Failover environment for the Manager using an external Microsoft SQL Server Database Management System.
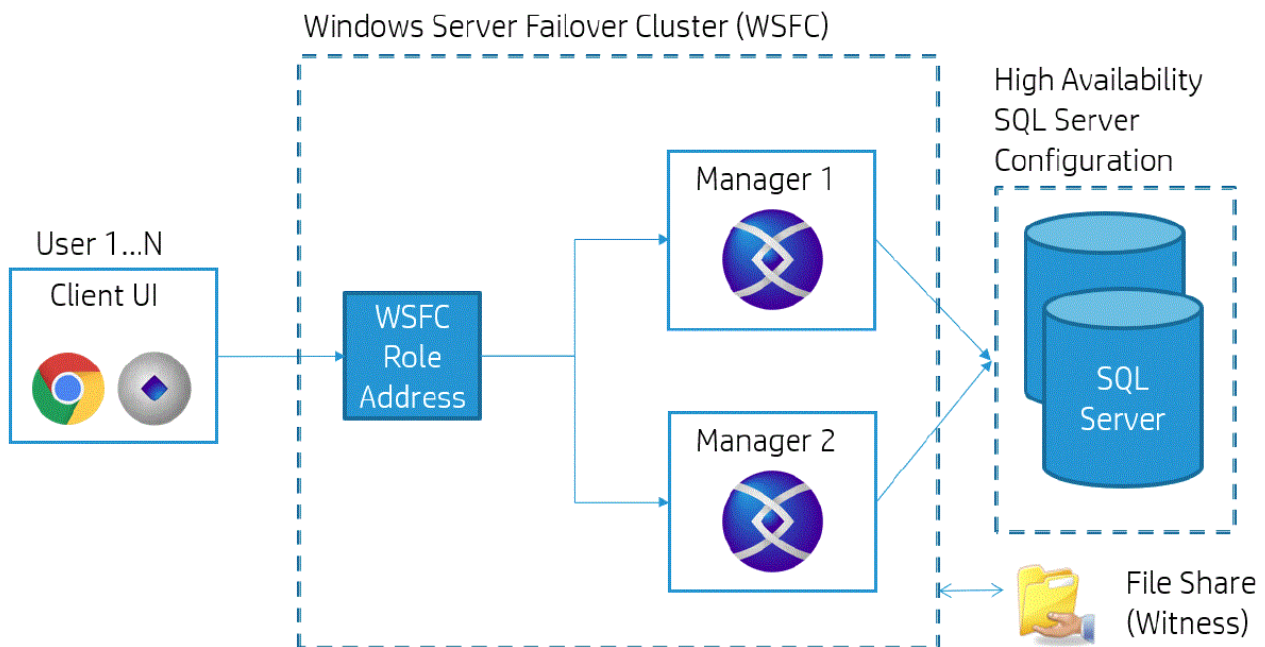
Prerequisites

The following items are required for database Failover for ZCentral Connect 2022 Manager
NOTE ZCentral Connect Manager version 20.3 or greater is required to support Failover.

1. A computer with Windows Server 2019 to act as Manager (1) and cluster node.

2. A computer with Windows Server 2019 to act as Manager (2) and cluster node.
3. A high-available SQL Server Database. HP recommends using Always On Availability Group
4. Domain accounts to run ZCentral Connect Managers. HP recommends using Managed Service Accounts (MSA)
5. A Certificate Authority (CA) that all nodes will trust.
   The Manager Config will create a CA or an existing CA can be used.
6. A license key file tied to the cluster address name.

Licensing

Each instance of the Manager will require a license key file that is tied to its Windows Server Failover Cluster (WSFC) role address name. There are three options for licensing to support failover:

1. If you have not already purchased a license for ZCentral Connect, see the Licensing Guide section of the User Guide for more information on purchasing and installing a ZCentral Connect license. When redeeming this license file, you must provide the WSFC role address name.
2. The hostname listed in your .lic file can be recycled as your WSFC role address name. In this case, you do not need to request a new license. This file can be copied and used for all instances running in your cluster.
3. A request for a replacement license file tied to your WSFC role address name to support failover can be made via the HP Licensing Support Center.

You will need to provide the following with your request:

1. Proof of purchase of your existing license. This can be provided in one of three ways.
   1. A copy of your entitlement certificate
   2. A copy of your EDR, Electronic Delivery Receipt
   3. Your EON, Entitlement Order Number
2. The quantity you wish to support. Typically this is the full quantity purchased from the original license, but may be less than this if you partially redeemed your original license.
3. The WSFC role address name of your cluster. For example, if your WSFC role address is zcentral.local, the name to provide is central.

The WSFC role address name will be entered into the Hostname field of the request.

For convenience, click on the following hyperlink and fill in the necessary fields. **Request for failover license**

Proof of Purchase

Please attach to this email one of the following from your original license purchase to provide proof of purchase:

Entitlement Certificate (attach to email)

Copy of your EDR, Electronic Delivery Receipt (attach to email)

EON (Entitlement order number (append here if applicable) : [enter your EON number here]

Number of Connections

Please specify the number of connections you wish to support for failover. This is typically the total number of connections of your original license, but may be less if you've partially redeemed your original license.

Number of Connections: [enter the number of connections needed to support failover here]

Hostname

Please enter the Windows Server Failover Cluster (WSFC) Role Address name that requires support. For example, if your WSFC role address is zcentral.local, enter zcentral below.

Hostname: [enter the WSFC role address name needed to support failover here]

HP support will generally fulfill this request within 1-2 business days.

The HP Licensing Support Center will generally fulfill this request within 1-2 business days. Follow the Licensing Guide section in the User Guide for instructions on installing a license file.

Installing Windows Server Failover Clustering

For each computer that will be part of the Cluster (Manager 1 and 2):

1. Install Windows Server 2019 (Desktop experience recommended).
2. Configure the computer hostname to be unique and assure the computer has a unique IP address.
3. Join the computer to the domain.
4. Open Server Manager and add the following Roles and Features:
   - Failover Clustering
   - NET Framework 3.5
     Active Directory module for Windows PowerShell
5. If using a Managed Service Account (MSA), before creating the MSA, the Key Distribution Service (KDS) must

be configured with a root key in the Domain Controller. After creating a KDS root key, you must wait 10 hours for the key to become active before creating an MSA.

6. Create a Managed Service Account (MSA) for the computer using the provided MSASetup.ps1 script (located at scripts directory within the ZCentral Connect installation package).

   - Run the following command as the Domain Administrator to create the account:
   - **PowerShell.exe -ExecutionPolicy Bypass -File .\msasetup.ps1 add <account_name>**

NOTE If you face an issue in the previous step, open the script file with a text editor and inspect its instructions.

Configuring Windows Server Failover Clustering

Do the following steps on the primary Manager node (Manager 1):

1. Open Failover Cluster Manager app
2. Click on Validate Configuration:
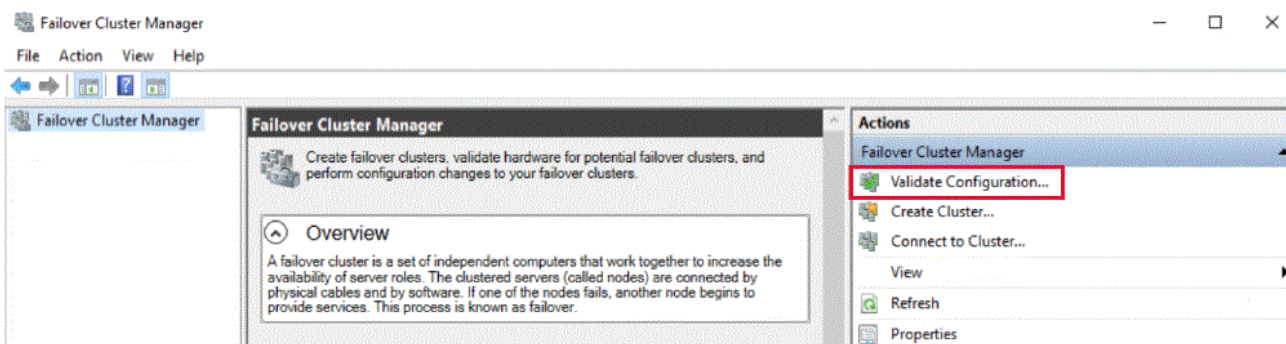
3. Add Manager 1 and 2 computers to the Configuration Wizard:
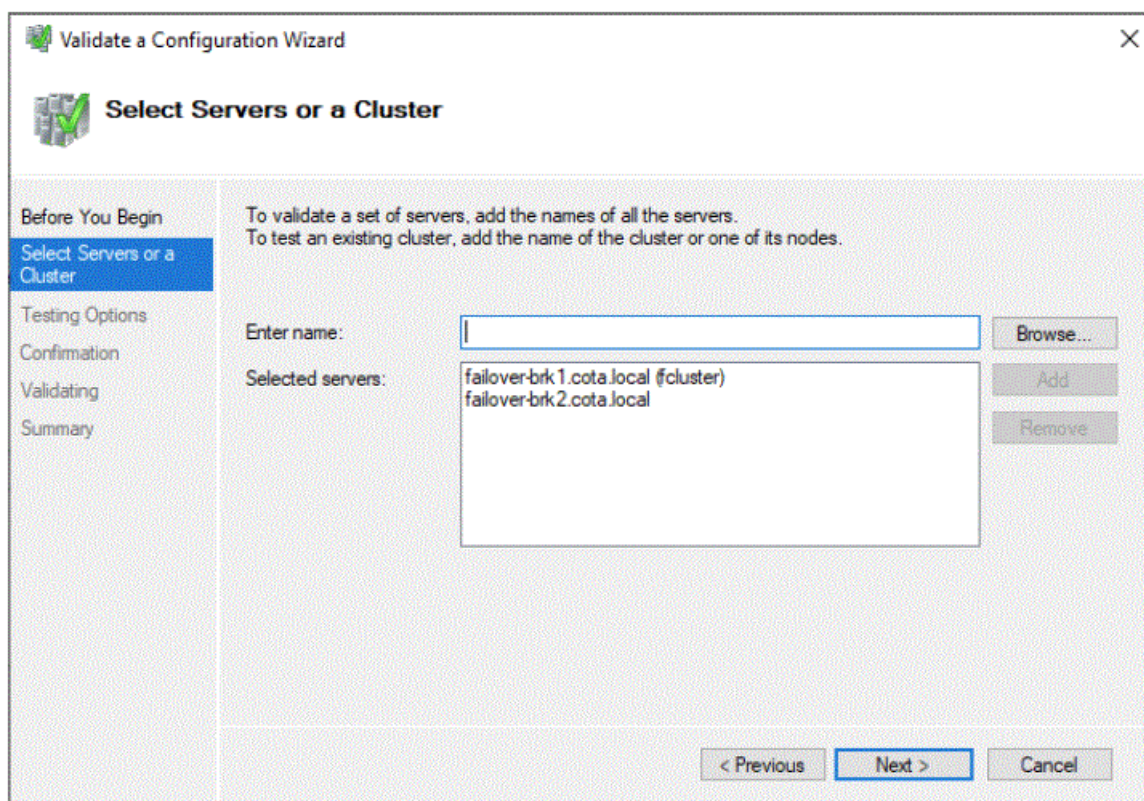
4. Click next and select 'Run all tests':

5. Click next and follow the wizard.

6. After the report is complete, review the warnings and check if there are any issues that need to be fixed before the next step. Warnings are normal and may be raised if the computer OS requires updates; the IP address is not static; or only a single network card is found.

7. Select 'Create the cluster now using the validated nodes':

8. Enter the cluster name and make note of it for future use:

9. Review and finish the wizard.

10. After the cluster is created, the following structure will be created:
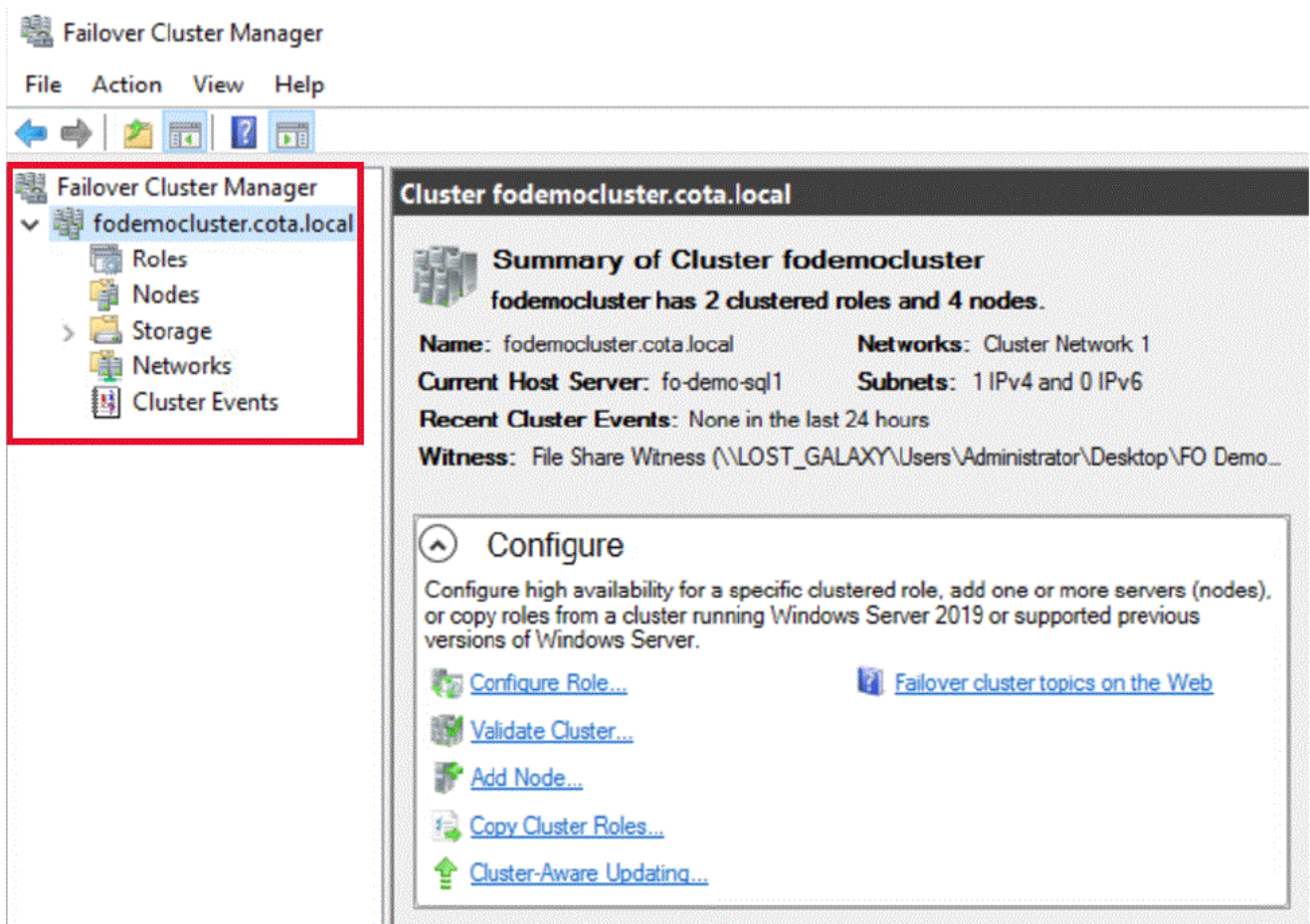
11. If required, configure the Cluster IP address to be static.

12. **IMPORTANT:** The Quarantine Threshold feature on the cluster can disrupt node functionality. A node becomes "quarantined" after a determined number of failures, interfering with ZCentral failover behavior. Disable the Quarantine Threshold settings to protect against failover.

- To configure the cluster to disable Quarantine Threshold, run the following command using PowerShell:
  - (Get-Cluster).QuarantineThreshold=0
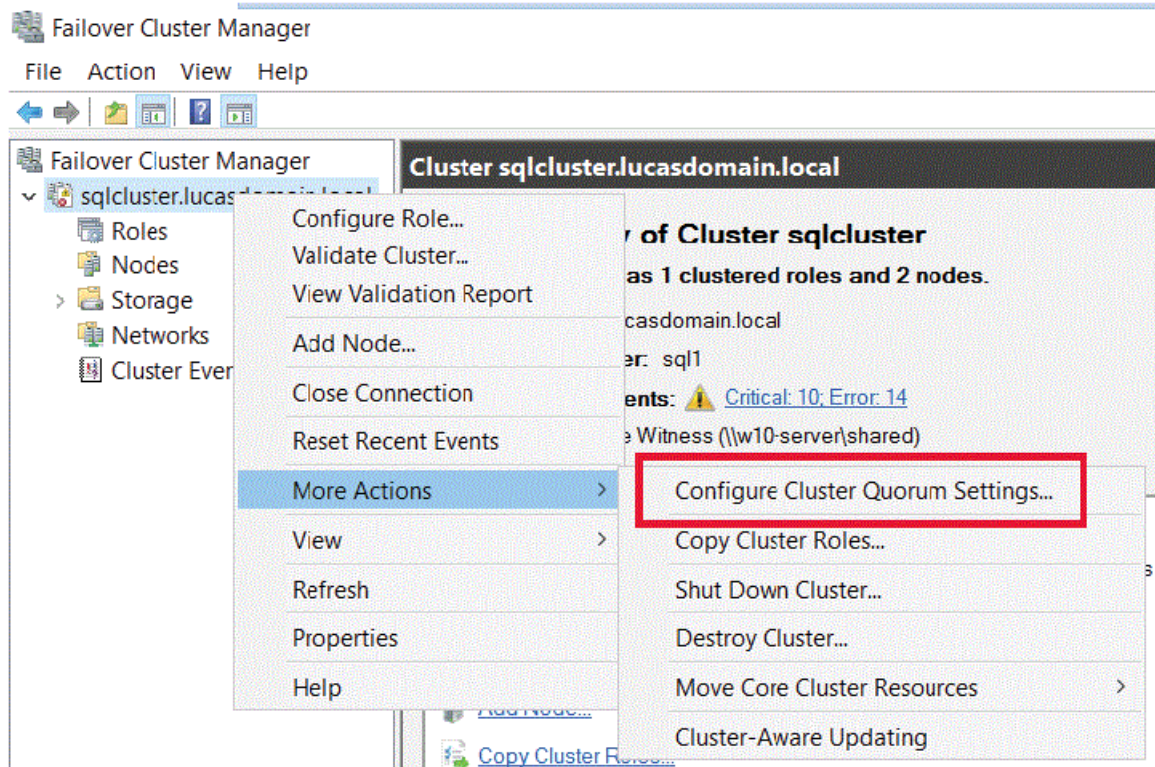 - (Get-Cluster).QuarantineDuration=0

Configuring the Witness

A witness must be added to the cluster to ensure that automatic failover is a success in the event that one node goes down. The following Microsoft Documentation provides more information on cluster and pool quorums. To add a File Share to be the witness of the cluster follow the steps below:

1. Create a File Share on a computer that is accessible by all nodes, for example, on the Domain Controller of your environment.
2. Connect to the File Share from one of the nodes and edit the permissions to allow the cluster and its nodes to read/write on it. Example:
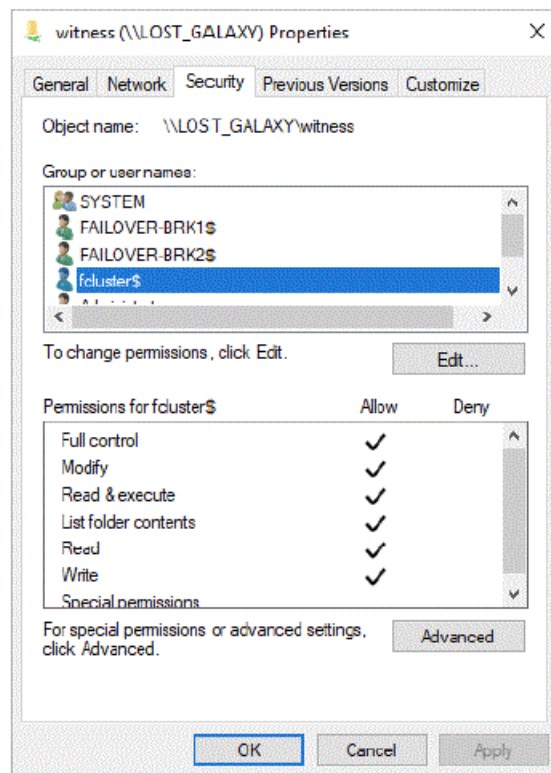
3. Open Failover Cluster Manager app
4. Right click on the Cluster, then click on Configure Cluster Quorum Settings:

5. Click on "Select the quorum witness"

6. Click on "Configure a file share witness":

7. Select the File Share Path and authenticate with domain credentials:

8. Finish the wizard.
9. You can see the File Share Witness in the Cluster dashboard:

Install and Configure ZCentral Connect Manager Nodes

The following steps describe the process to install the ZCentral Connect Manager instances and configure each instance to listen at the WSFC role address and point to your high availability SQL Server database. Additionally, the Manager Config failover command will reissue a self signed Certificate Authority and new certificates configured for failover. NOTE A fresh install of ZCentral Connect Manager, version 20.3 or greater is required to support failover. Any existing information from a 20.2 or previous installs will need to be reimported and reconfigured. It is recommended to archive any existing database to another location. You can backup the Manager database file located at path:
%PROGRAMDATA%\HP\ZCentralConnectManager\Manager.db.

NOTE Depending on your SQL Server configuration it may be required for you to give permissions to the domain accounts to enable the Manager to access the database. Installation steps for the primary HP ZCentral Manager:

1. If the ZCentral Connect Manager is not already installed on this machine, install it.
   - **IMPORTANT:** Install ZCentral Connect Manager specifying the Manager hostname as the hostname of this computer.
2. Create the WSFC Role to host the ZCentral Connect instance.
   1. Go to the Failover Cluster Manager, right click on Roles and Click on Configure Role.
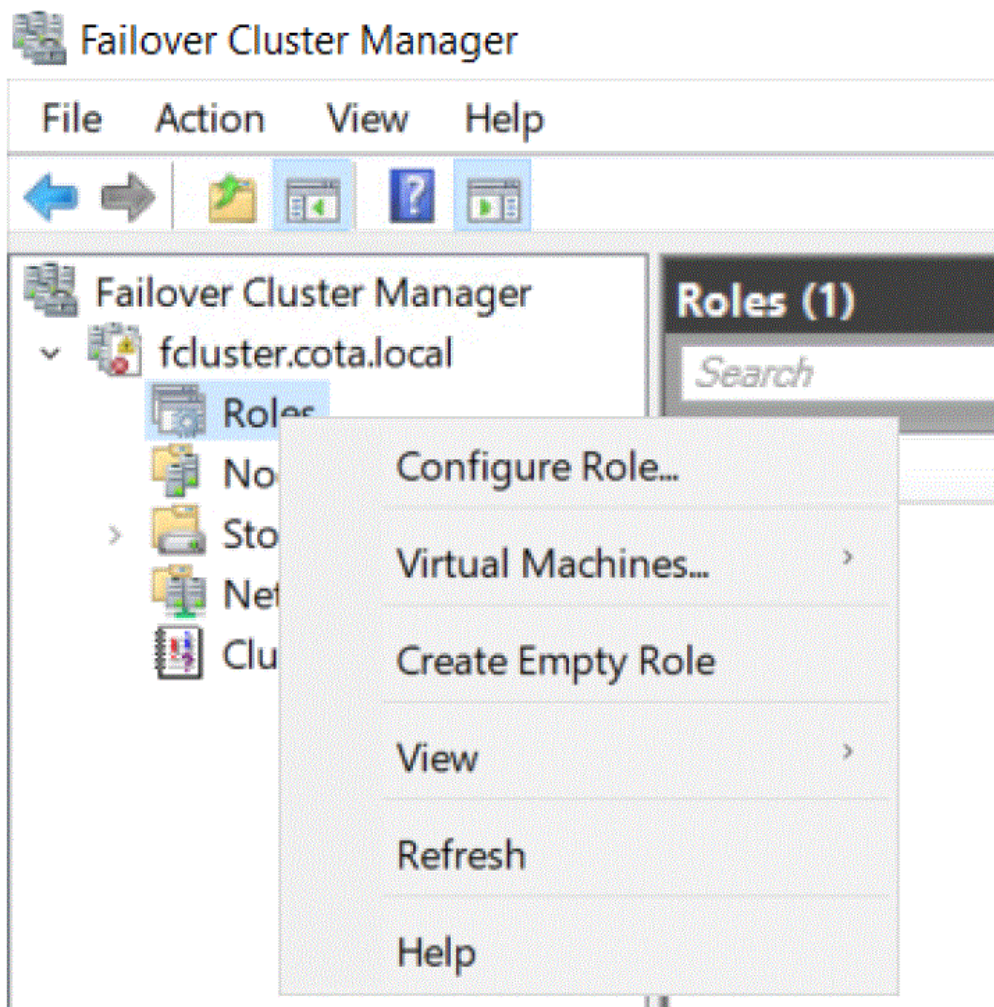
2. On the High Availability Wizard, select Generic Service and click on Next.
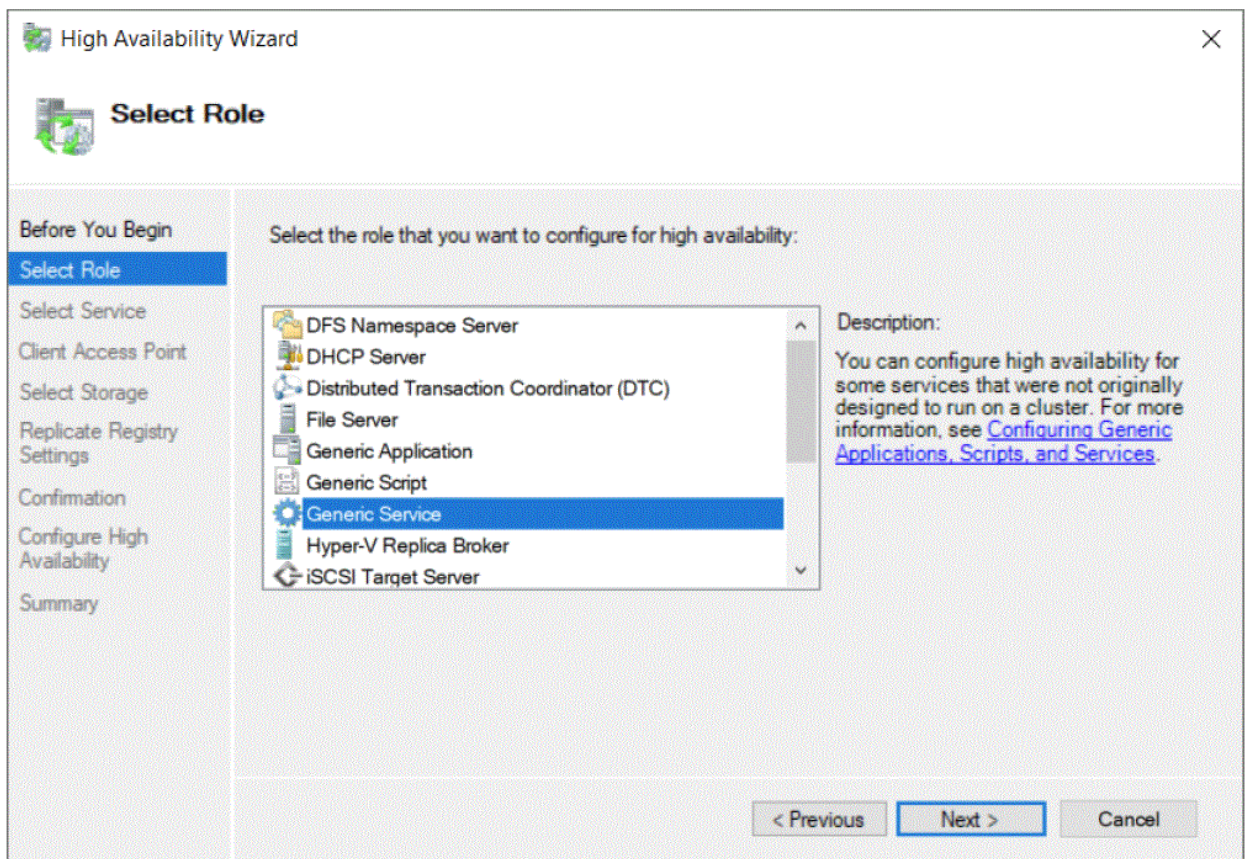
3. Select HP ZCentral Connect Manager service.
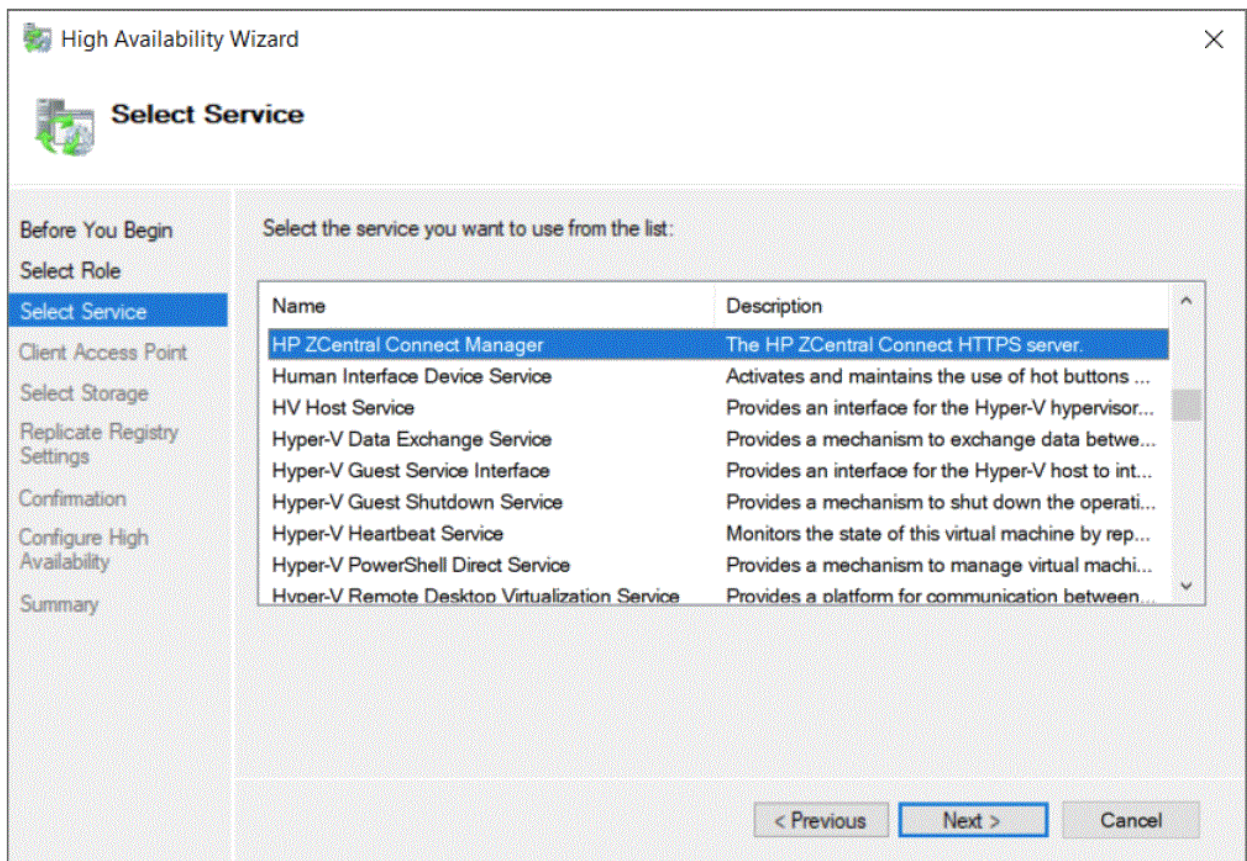
4. Define the WSFC Role Address. This will be the address which your Manager will be accessible by all clients,
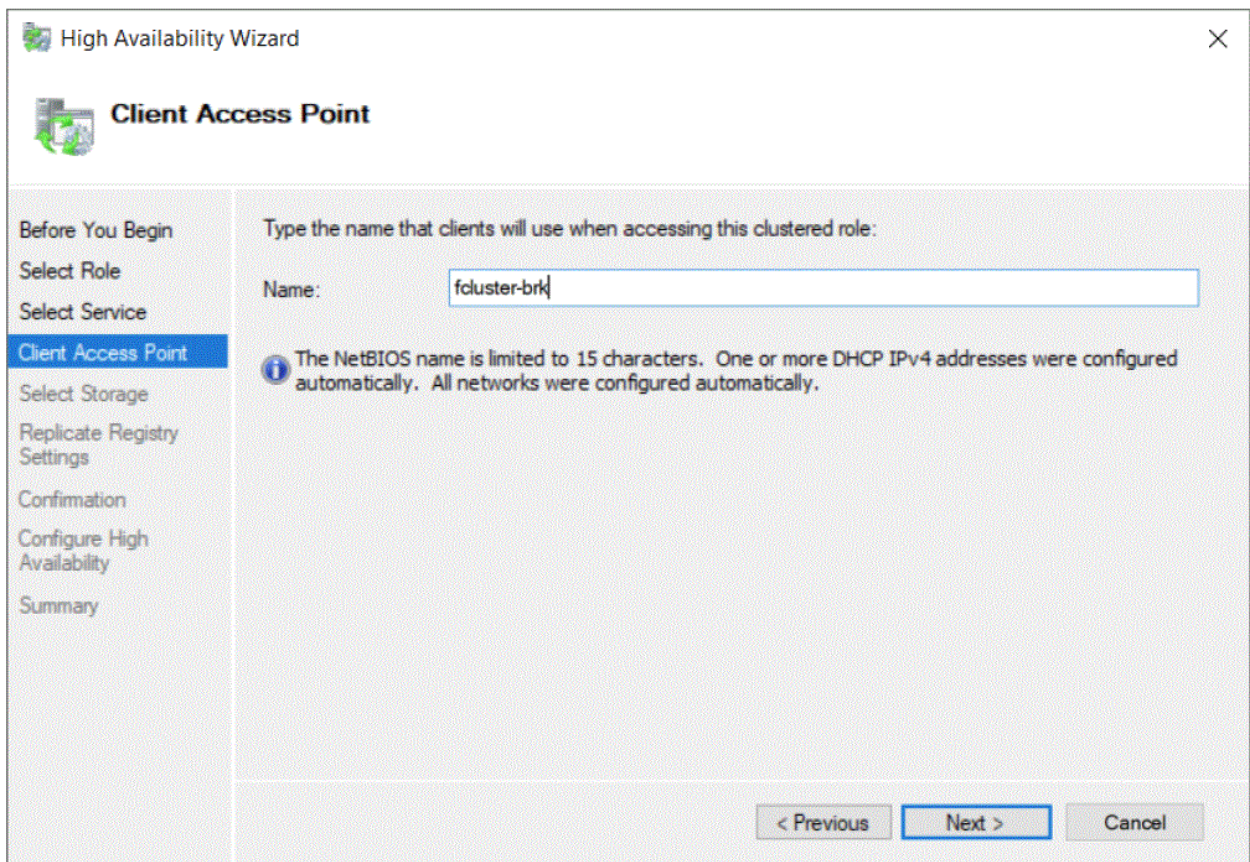
5. Press Next until finishing the Wizard.

3. Copy the license file issued for the WSFC Role Address name to the %PROGRAMDATA%\HP\ZCentralConnectManager folder.

4. Configure the primary Manager using the provided HP ZCentral Connect Manager Config app. This tool is called ManagerConfig.exe and is located in the same folder where HP ZCentral Connect Manager is installed,

typically %PROGRAMFILES%\HP\ZCentralConnectManager\bin.

1. Open a command prompt as Administrator and run the following command:
   - ManagerConfig.exe failover –export –cluster hostname <WSFC Role Address name> – secondaryHostname
     <manager hostname> –serviceAccount <domain\manager msa account$> – sqlServerConnectionString <full SQL Server connection string>
   - An example of a full SQL Server connection string may look similar to **Server=<you server address>,<port>;Database=<db name>;Integrated Security=SSPI;Encrypt=yes;**
2. Follow the on-screen instructions, you will be prompted for a password to export a newly created certi██cate for the secondary Manager. You will need this password again when you configure the secondary Manager.
3. When the command completes successfully the primary Manager should be setup and ready.
4. A new file, manager_failover.zip, will be created in %PROGRAMDATA%\HP\ZCentralConnectManager folder. This file will contain the certificate for the secondary Manager and other needed settings for the secondary Manager.

Installation steps for the secondary HP ZCentral Manager:

1. If the ZCentral Connect Manager is not already installed on this machine, install it.
   - **IMPORTANT:** Install ZCentral Connect Manager specifying the Manager hostname as the hostname of this computer.
2. Copy the license file issued for the WSFC Role Address name to the %PROGRAMDATA%\HP\ZCentralConnectManager folder.
3. Copy the manager_failover.zip file created with the primary configuration steps to the same path, %PROGRAMDATA%\HP\ZCentralConnectManager on the secondary machine.
4. Open a command prompt as Administrator from %PROGRAMFILES%\HP\ZCentralConnectManager\bin, and run the following command:
   - ManagerConfig.exe failover –import –serviceAccount <domain\manager msa account$>
5. You will be prompted to enter the password for the certificate you created in the primary configuration.
6. When the command completes successfully the secondary Manager should be configured and ready.

NOTE The Manager Config failover export and import command will attempt to start the Manager service to verify configurations are valid. It will then stop the service to ensure that Manager services are only started via the cluster manager. If the attempt to start the Manager service at the end of each command fails, refer to the Troubleshooting Failover Guide for help.
NOTE Once these steps are complete, if you choose to use your own trusted CA, refer to the Renewing or Configuring new HP ZCentral Connect Manager Certificate section in the User Guide for instructions on using the Manager Config to change the certificate that the Manager uses. This must be completed on both Manager instances.

Configuring Agents

To enable Agents to connect to any of the Manager nodes, the Agents computer must trust the Certificate Authority (CA).

1. To export the CA, look for instructions in the Accepting the Self-Signed Certificate Authority in Your

Environment section in the User Guide.

2. Refer to the Trusting a Certificate Authority section in the User Guide for instructions on how to trust the CA.
3. Install the Agent using the WSFC Role Address as the Manager hostname.
    - If the Agent is already installed, it will be required to register the Agent again.
        1. Refer to the ZCentral Connect Agent Config section in the User Guide for instructions on registering the Agent.
        2. Open the Agent settings file with a Text Editor, it can be found in the following path: %PROGRAMDATA%\HP\ZCentral ConnectAgent\settings.json in Windows and /etc/hpzcentralconnectagent/settings.json in Linux®.
        3. Leave the setting "ManagerCertificateThumbprint" empty: "ManagerCertificateThumbprint": "",
        4. Save the file and restart the HP ZCentral Connect Agent service to apply the changes.

Configuring AMT Hosts

To ensure that AMT Hosts send Hardware Alerts and are able to perform Power Operations, the following steps are required:

1. Login as Administrator into the HP ZCentral Connect Manager using the WSFC Role Address.
2. On the side menu, navigate to Hosts tab. The list of Hosts will be shown:

3. For each Host where the AMT column is not Unmanaged, click on the Host hostname on the table then click on the Refresh Monitoring Data button in the Manage Host panel.:

Manage Host

lost_galaxy.cota.local

DETAILS ⌃

Availability: Available

Owner: PR (Pool)

Logged in User(s): None

IP Address: 192.168.0.1

Model: HP ZCentral 4R

Serial Number: HPZC4R2020

AMT: Ready

System ID LED: ⬭

Remote Boost Sender: Running

Remote Boost Sender Version: 20.1.0.0

Agent: Connected

Agent Version: 20.1.0.0

🖉 Generate New Authorization Code ⓘ

⟳ Refresh Monitoring Data

EDIT ⌄

POWER OPERATIONS ⌄

4. Execute a Power Operation on the Host to make sure it's working as intended.

- If the Power Operation failed to execute, remove the Host and add the Host again.
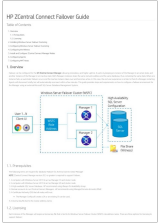
Copyright and License

Trademark Credits

Third-party notice
Third-party source code and licenses are redistributed, if required, with HP ZCentral Connect.

Document Version

Edition: 22.0.0
Part Number: M46647-007

Documents / Resources

	hp ZCentral Connect Failover Software [pdf] User Guide ZCentral Connect Failover Software, ZCentral Connect Failover, Software

References

- ▦ **Understand cluster and pool quorum on Azure Stack HCI and Windows Server clusters - Azure Stack HCI | Microsoft Docs**
- *hp* **Contact US| My HP Licensing**