

StarWind Virtual SAN: Configuration Guide for Microsoft Windows Server [Hyper-V], VSAN Deployed as a Controller Virtual Machine (CVM) using Web UI

2024

TECHNICAL PAPERS



Trademarks

“StarWind”, “StarWind Software” and the StarWind and the StarWind Software logos are registered trademarks of StarWind Software. “StarWind LSFS” is a trademark of StarWind Software which may be registered in some jurisdictions. All other trademarks are owned by their respective owners.

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, StarWind Software assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein. StarWind Software reserves the right to make changes in the product design without reservation and without notification to its users.

Technical Support and Services

If you have questions about installing or using this software, check this and other documents first - you will find answers to most of your questions on the [Technical Papers](#) webpage or in [StarWind Forum](#). If you need further assistance, please [contact us](#) .

About StarWind

StarWind is a pioneer in virtualization and a company that participated in the development of this technology from its earliest days. Now the company is among the leading vendors of software and hardware hyper-converged solutions. The company's core product is the years-proven StarWind Virtual SAN, which allows SMB and ROBO to benefit from cost-efficient hyperconverged IT infrastructure. Having earned a reputation of reliability, StarWind created a hardware product line and is actively tapping into hyperconverged and storage appliances market. In 2016, Gartner named StarWind “Cool Vendor for Compute Platforms” following the success and popularity of StarWind HyperConverged Appliance. StarWind partners with world-known companies: Microsoft, VMware, Veeam, Intel, Dell, Mellanox, Citrix, Western Digital, etc.

Copyright ©2009-2018 StarWind Software Inc.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of StarWind Software.

Annotation

Relevant Products

This guide is applicable to StarWind Virtual SAN and StarWind Virtual SAN Free (CVM Version 20231016 and later).

For older versions of StarWind Virtual SAN (OVF Version 20230901 and earlier), please refer to this configuration guide:

[StarWind Virtual SAN \(VSAN\): Configuration Guide for Microsoft Windows Server \[Hyper-V\], VSAN Deployed as a Windows Application using Legacy GUI.](#)

Purpose

This document outlines how to configure a Microsoft Hyper-V Failover Cluster using StarWind Virtual SAN (VSAN), with VSAN running as a Controller Virtual Machine (CVM). The guide includes steps to prepare Hyper-V hosts for clustering, configure physical and virtual networking, and set up the Virtual SAN Controller Virtual Machine.

For more information about StarWind VSAN architecture and available installation options, please refer to the:

[StarWind Virtual \(VSAN\) Getting Started Guide.](#)

Audience

This technical guide is intended for storage and virtualization architects, system administrators, and partners designing virtualized environments using StarWind Virtual SAN (VSAN).

Expected Result

The end result of following this guide will be a fully configured high-availability Windows Failover Cluster that includes virtual machine shared storage provided by StarWind VSAN.

NOTE: This guide universally applies to both 2-node and 3-node clusters. Please follow the quick notes within the configuration steps to carry out the necessary actions required for each cluster size.

Prerequisites

Starwind Virtual San System Requirements

Prior to installing StarWind Virtual SAN, please make sure that the system meets the requirements, which are available via the following link:

<https://www.starwindsoftware.com/system-requirements>

Recommended RAID settings for HDD and SSD disks:

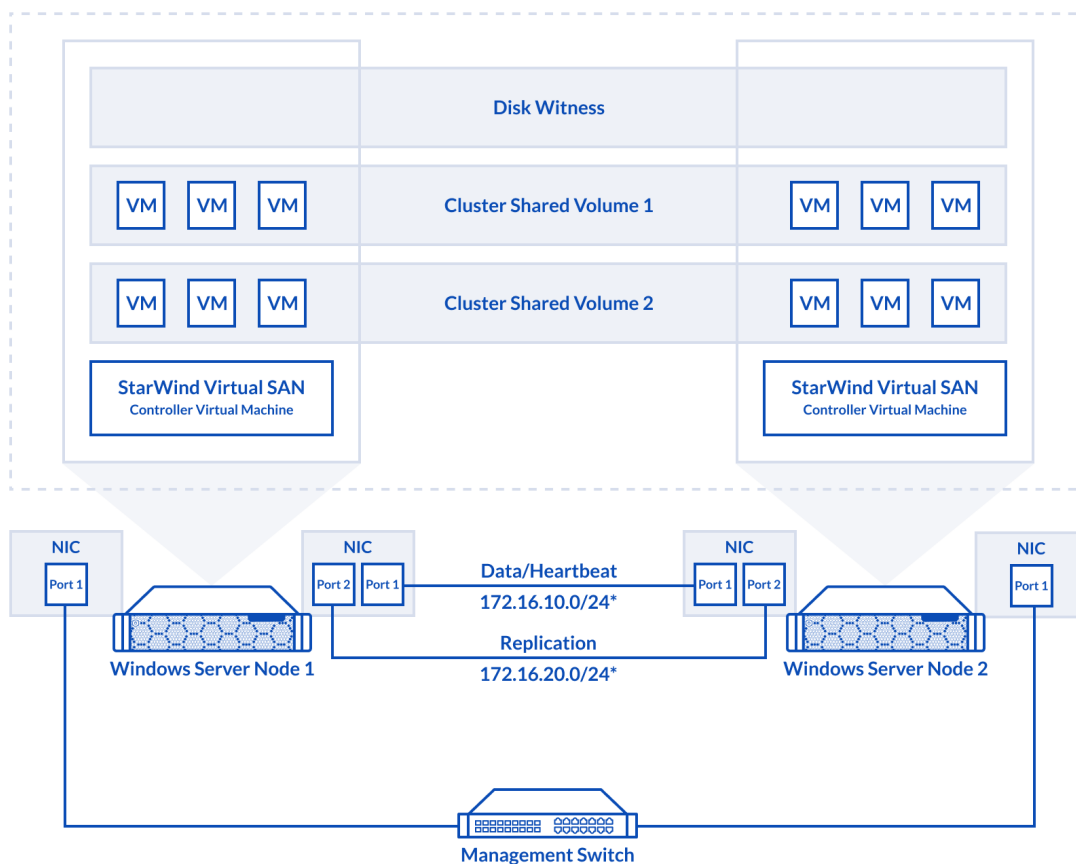
<https://knowledgebase.starwindsoftware.com/guidance/recommended-raid-settings-for-hdd-and-ssd-disks/>

Please read StarWind Virtual SAN Best Practices document for additional information:

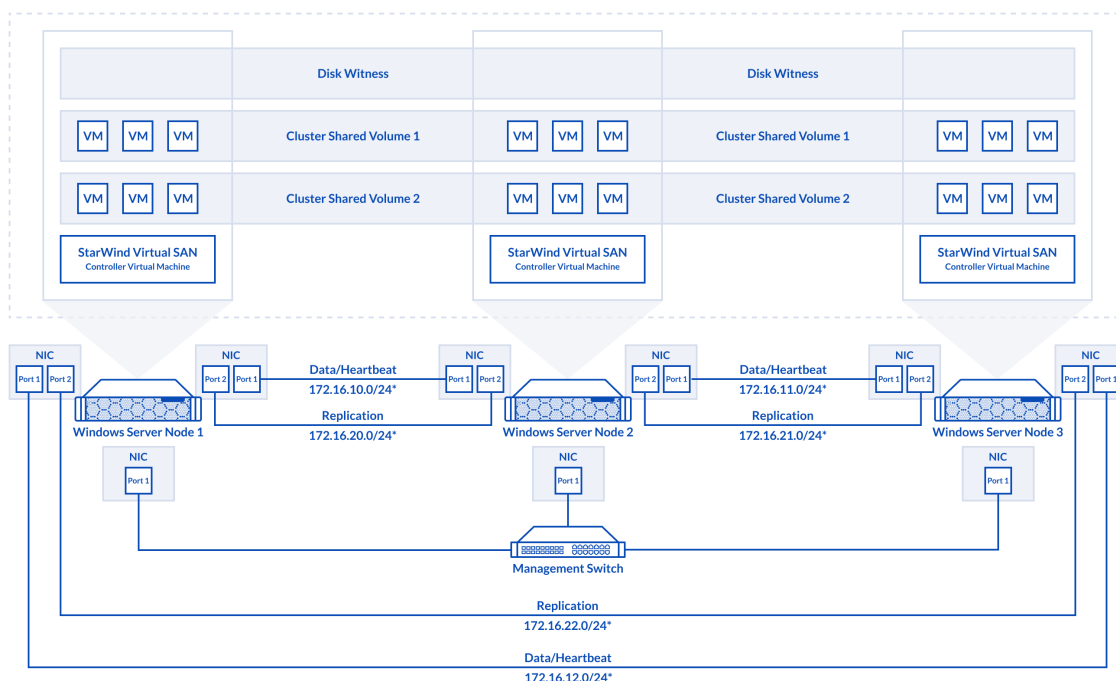
<https://www.starwindsoftware.com/resource-library/starwind-virtual-san-best-practices>

Solution Diagram

The diagrams below illustrate the network and storage configuration of the solution:



2-node cluster



3-node cluster

Preconfiguring cluster nodes

1. Make sure that a domain controller is configured and the servers are added to the domain.

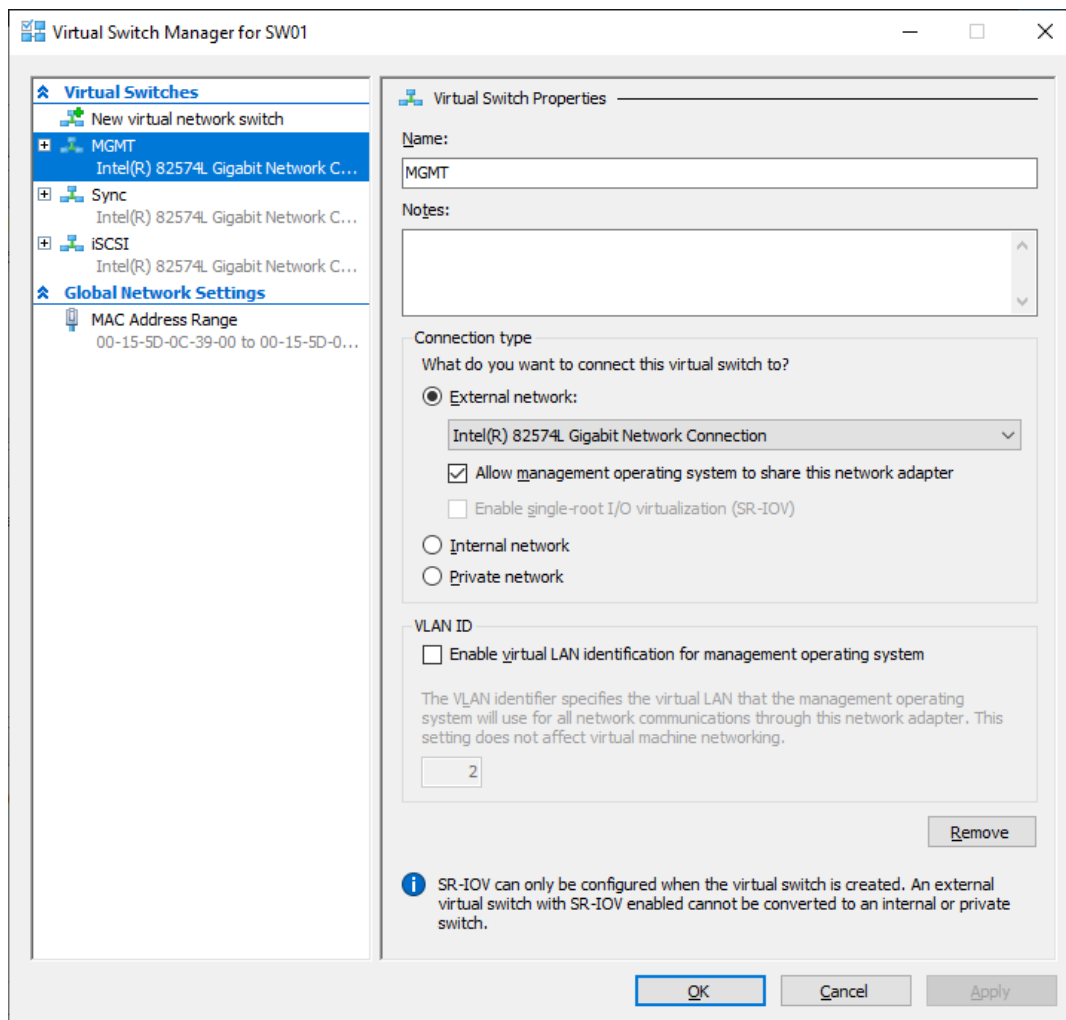
NOTE: Please follow the recommendation in [KB article](#) on how to place a DC in case of StarWind Virtual SAN usage.

2. Deploy Windows Server on each server and install Failover Clustering and Multipath I/O features, as well as the Hyper-V role on both servers. This can be done through Server Manager (Add Roles and Features menu item).

3. Define at least 2x network interfaces (2 node scenario) or 4x network interfaces (3 node scenario) on each node that will be used for the Synchronization and iSCSI/StarWind heartbeat traffic. Do not use iSCSI/Heartbeat and Synchronization channels over the same physical link. Synchronization and iSCSI/Heartbeat links can be connected either via redundant switches or directly between the nodes (see diagram above).

4. Separate external Virtual Switches should be created for iSCSI and Synchronization traffic based on the selected before iSCSI and Synchronization interfaces. Using Hyper-V

Manager open Virtual Switch Manager and create two external Virtual Switches: one for the iSCSI/StarWind Heartbeat channel (iSCSI) and another one for the Synchronization channel (Sync).



5. Configure and set the IP address on each virtual switch interface. In this document, 172.16.1x.x subnets are used for iSCSI/StarWind heartbeat traffic, while 172.16.2x.x subnets are used for the Synchronization traffic.

NOTE: In case NIC supports SR-IOV, enable it for the best performance. An additional internal switch is required for iSCSI Connection. Contact support for additional details.

6. Set MTU size to 9000 on iSCSI and Sync interfaces using the following Powershell script.

```
$iSCSIs = (Get-NetAdapter -Name "*iSCSI*").Name
$Syncs = (Get-NetAdapter -Name "*Sync*").Name
foreach ($iSCSI in $iSCSIs) {
```

```
Set-NetAdapterAdvancedProperty -Name "$iSCSI" -RegistryKeyword
"*JumboPacket" -Registryvalue 9014
Get-NetAdapterAdvancedProperty -Name "$iSCSI" -RegistryKeyword
"*JumboPacket"
}
foreach ($Sync in $Syncs) {
Set-NetAdapterAdvancedProperty -Name "$Sync" -RegistryKeyword
"*JumboPacket" -Registryvalue 9014
Get-NetAdapterAdvancedProperty -Name "$Sync" -RegistryKeyword
"*JumboPacket"
}
```

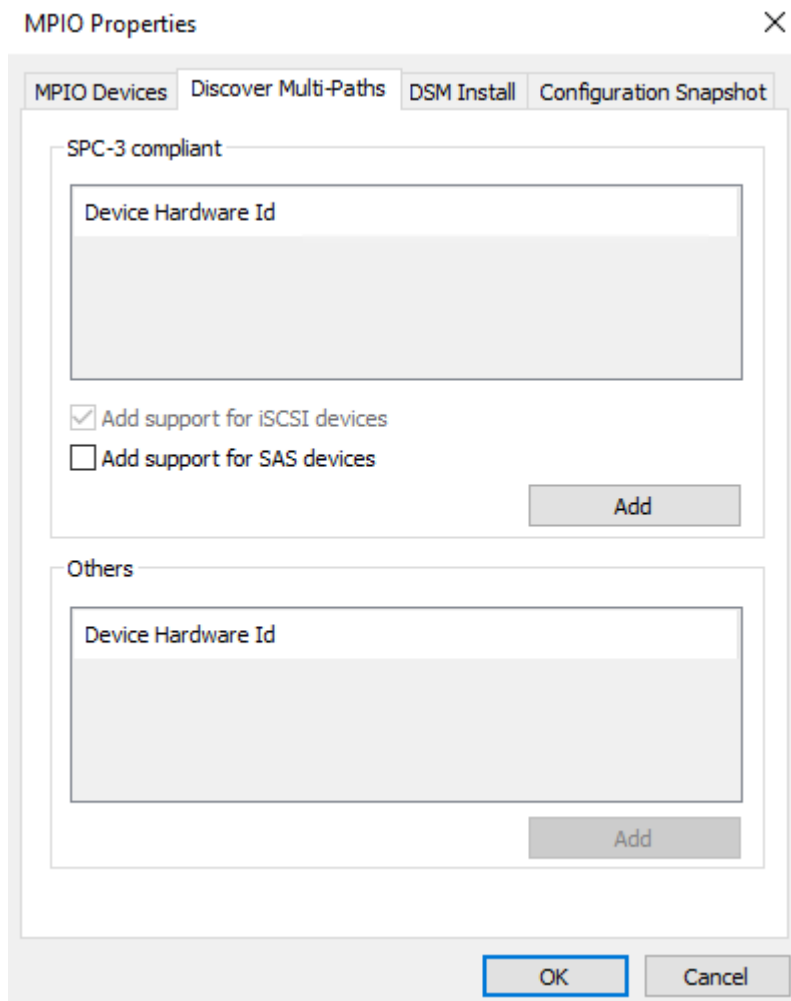
It will apply MTU 9000 to all iSCSI and Sync interfaces if they have iSCSI or Sync as part of their name.

NOTE: MTU setting should be applied on the adapters only if there is no live production running through the NICs.

7. Open the MPIO Properties manager: Start -> Windows Administrative Tools -> MPIO. Alternatively, run the following PowerShell command :

```
mpiocpl
```

8. In the Discover Multi-Paths tab, select the Add support for iSCSI devices checkbox and click Add.



9. When prompted to restart the server, click Yes to proceed.

10. Repeat the same procedure on the other server.

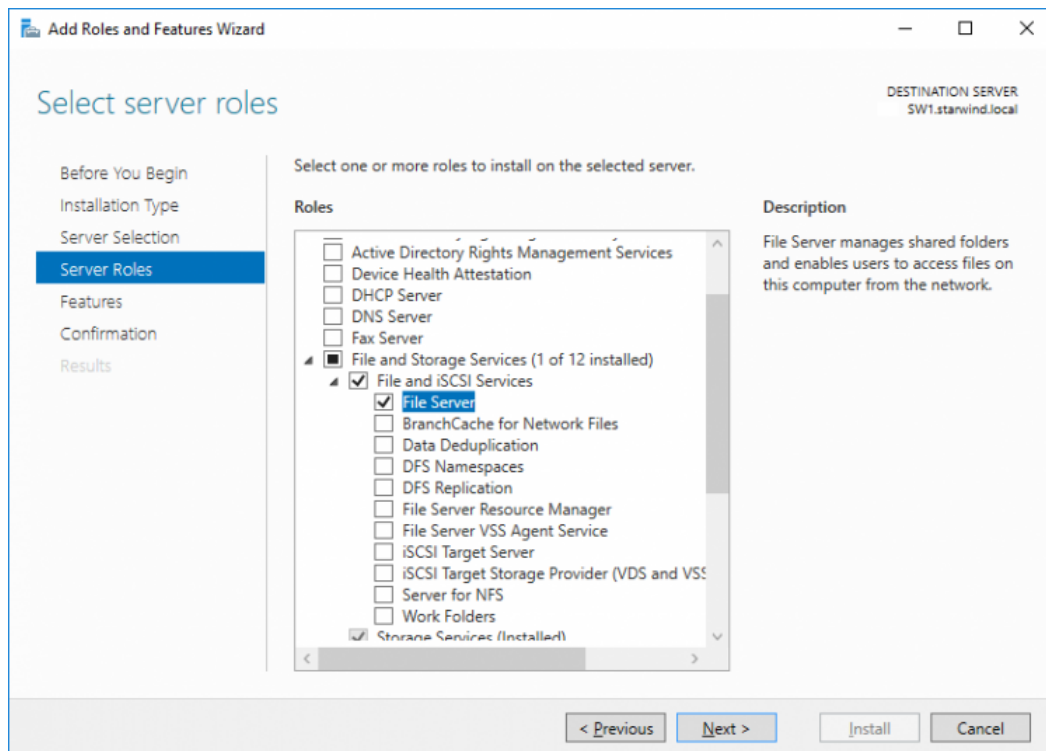
Installing File Server Roles

Please follow the steps below if file shares configuration is required

Scale-Out File Server (Sofs) For Application Data

1. Open Server Manager: Start -> Server Manager.
2. Select: Manage -> Add Roles and Features.
3. Follow the installation wizard steps to install the roles selected in the screenshot

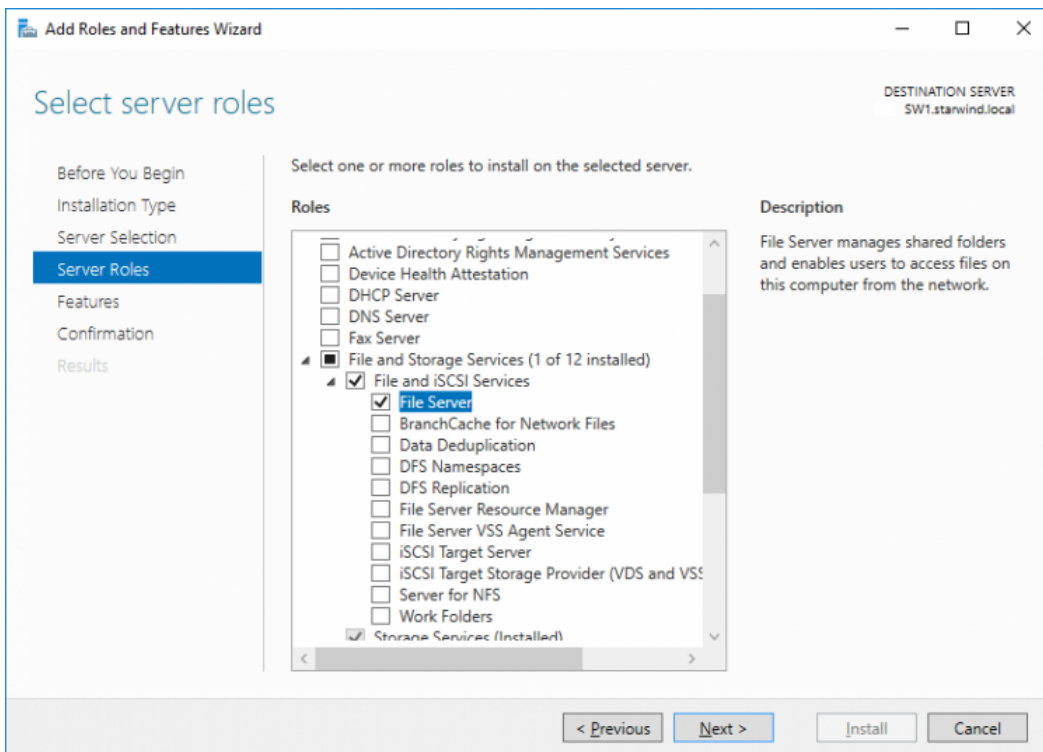
below:



4. Restart the server after installation is completed and perform steps above on the each server.

File Server For General Use With Smb Share

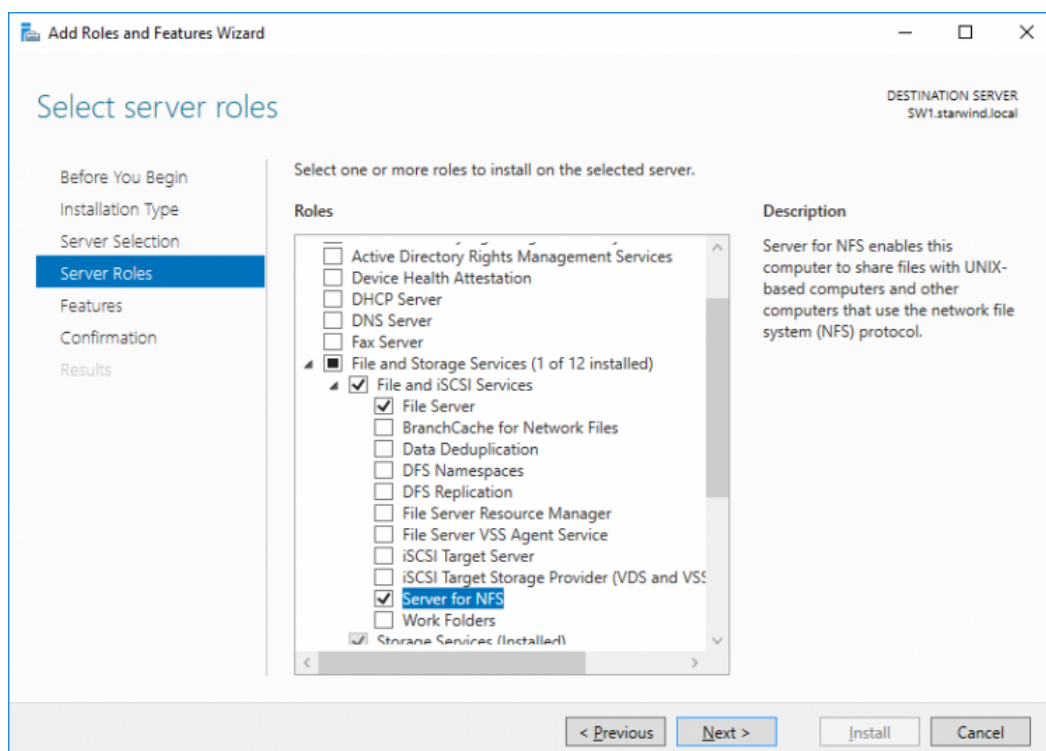
1. Open Server Manager: Start -> Server Manager.
2. Select: Manage -> Add Roles and Features.
3. Follow the installation wizard steps to install the roles selected in the screenshot below:



4. Restart the server after installation is completed and perform steps above on each server.

File Server For General Use With Nfs Share

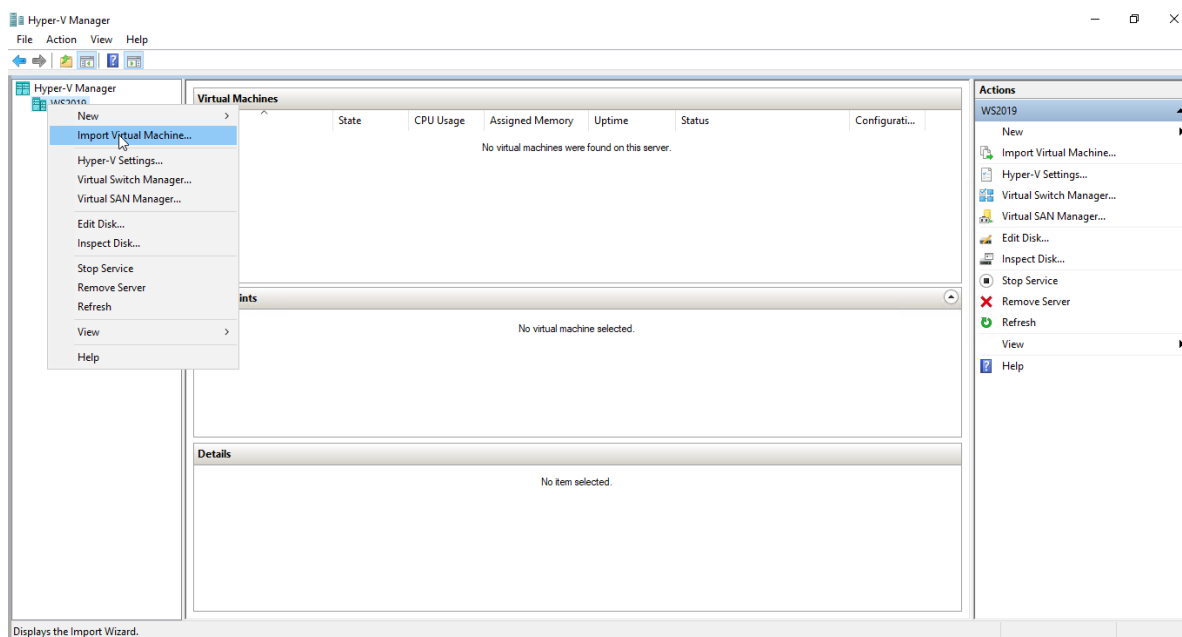
1. Open Server Manager: Start -> Server Manager.
2. Select: Manage -> Add Roles and Features.
3. Follow the installation wizard steps to install the roles selected in the screenshot below:



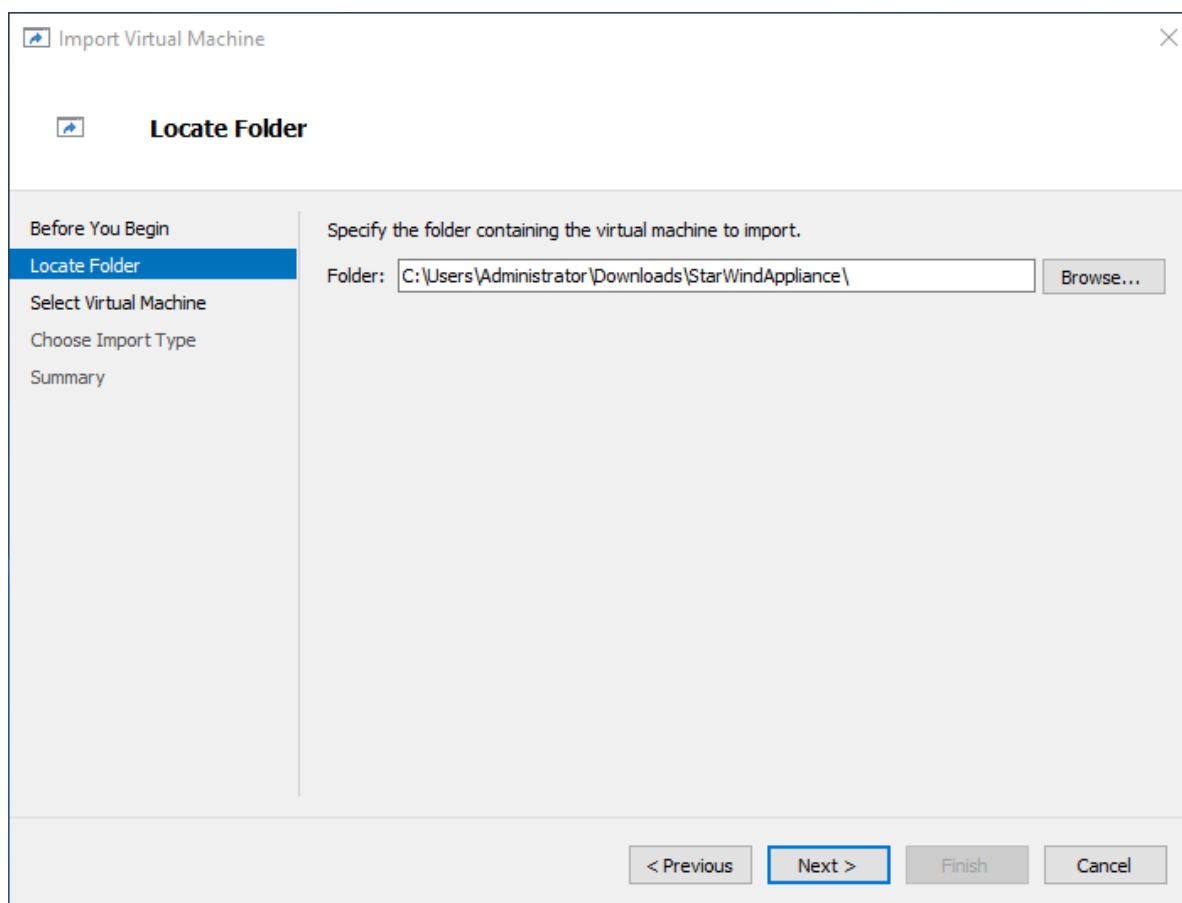
4. Restart the server after installation is completed and perform steps above on each server.

Deploying Starwind Virtual San Cvm

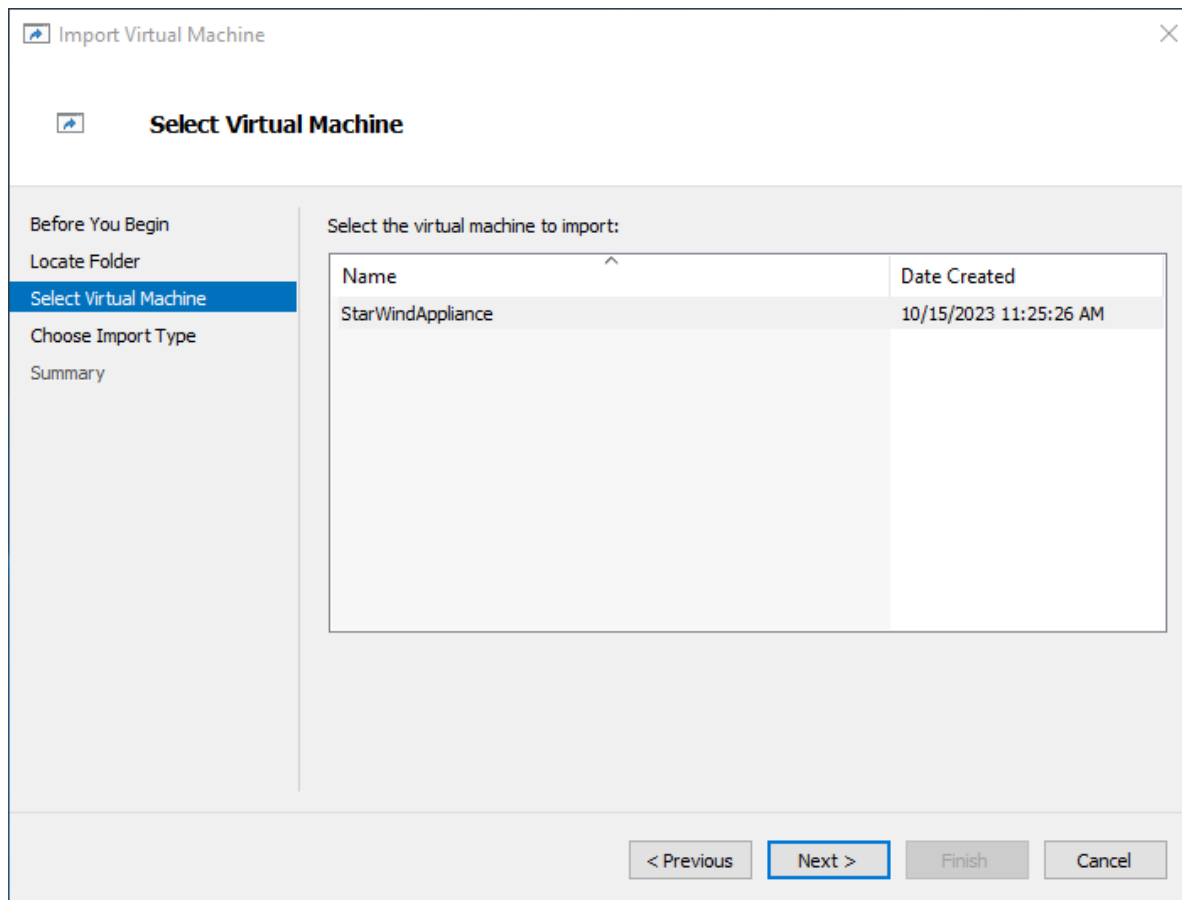
1. Download the zip archive that contains StarWind Virtual SAN CVM
<https://www.starwindsoftware.com/vsan#download>
2. Extract the virtual machine files.
3. Deploy the control virtual machine to the Microsoft Hyper-V Server using the "Import Virtual Machine" wizard in Hyper-V Manager.



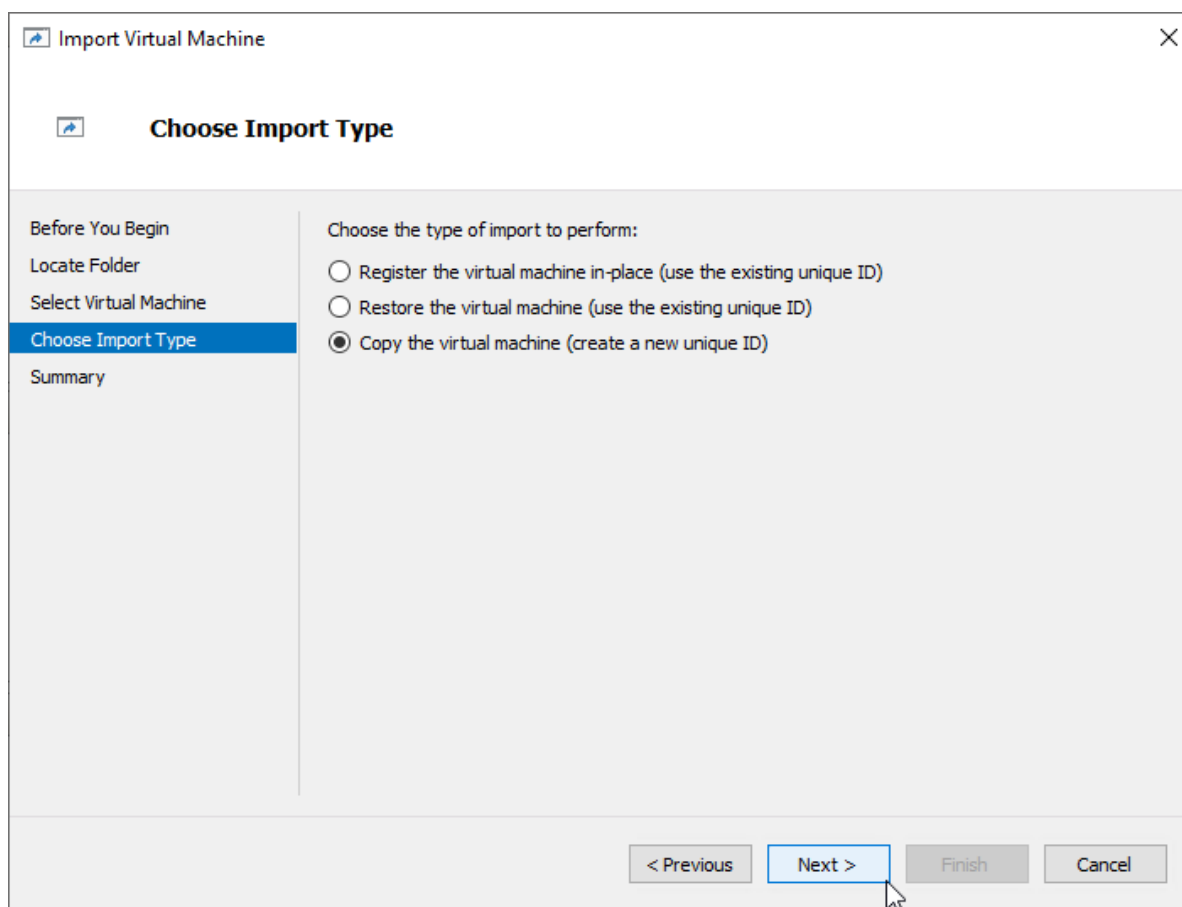
4. On the second page of the wizard, point to the location of the VM template. Select the VM folder and click Next.



5. Click Next on the “Select Virtual Machine” step.



6. Select the “Copy the virtual machine” import type and click Next.



7. Specify new or existing folders to store virtual machine files, such as configuration, snapshots, smart paging, and virtual disk. Click Next.

StarWind Virtual SAN: Configuration Guide for Microsoft Windows Server [Hyper-V], VSAN
Deployed as a Controller Virtual Machine (CVM) using Web UI

16

Import Virtual Machine

Choose Folders to Store Virtual Hard Disks

Before You Begin

Locate Folder

Select Virtual Machine

Choose Import Type

Choose Destination

Choose Storage Folders

Summary

Where do you want to store the imported virtual hard disks for this virtual machine?

Location:

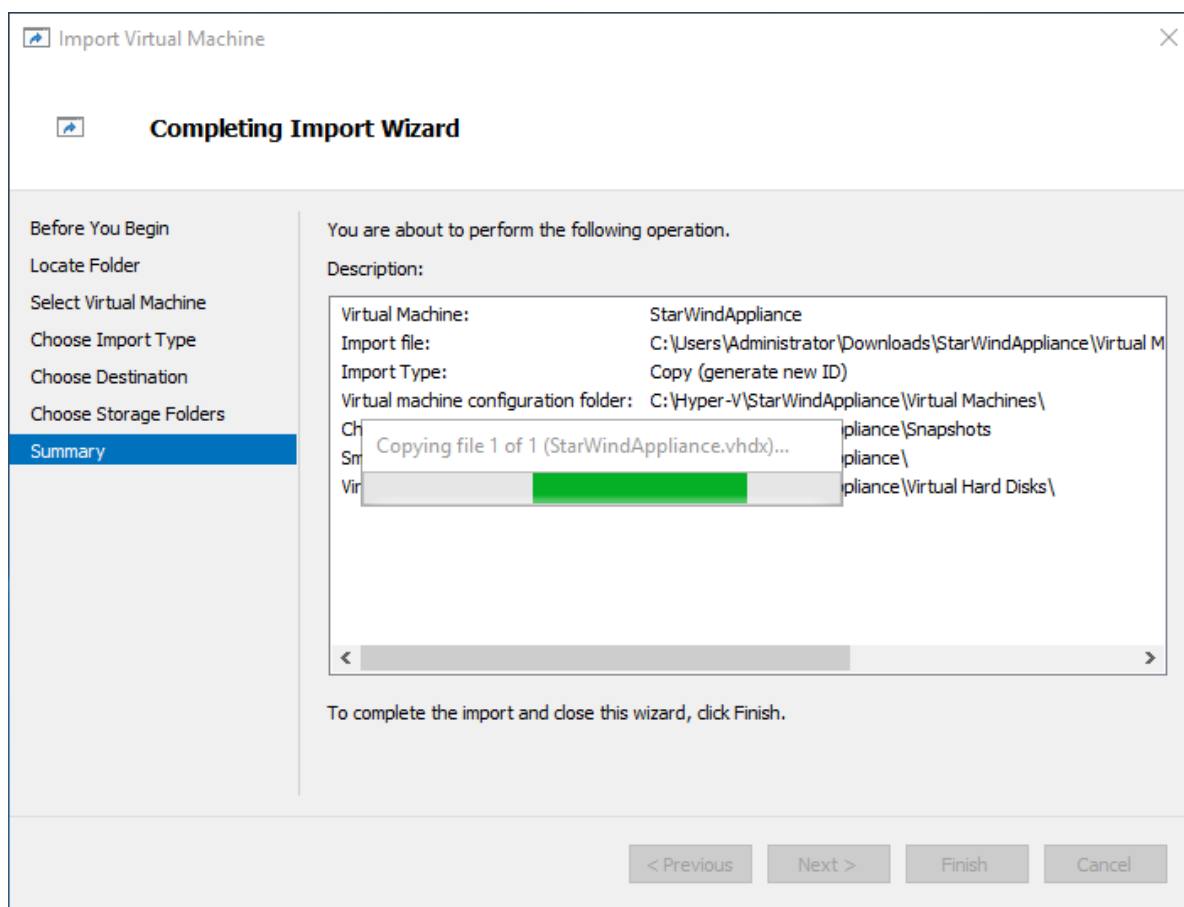
Browse...

< Previous

Next >

Finish

Cancel

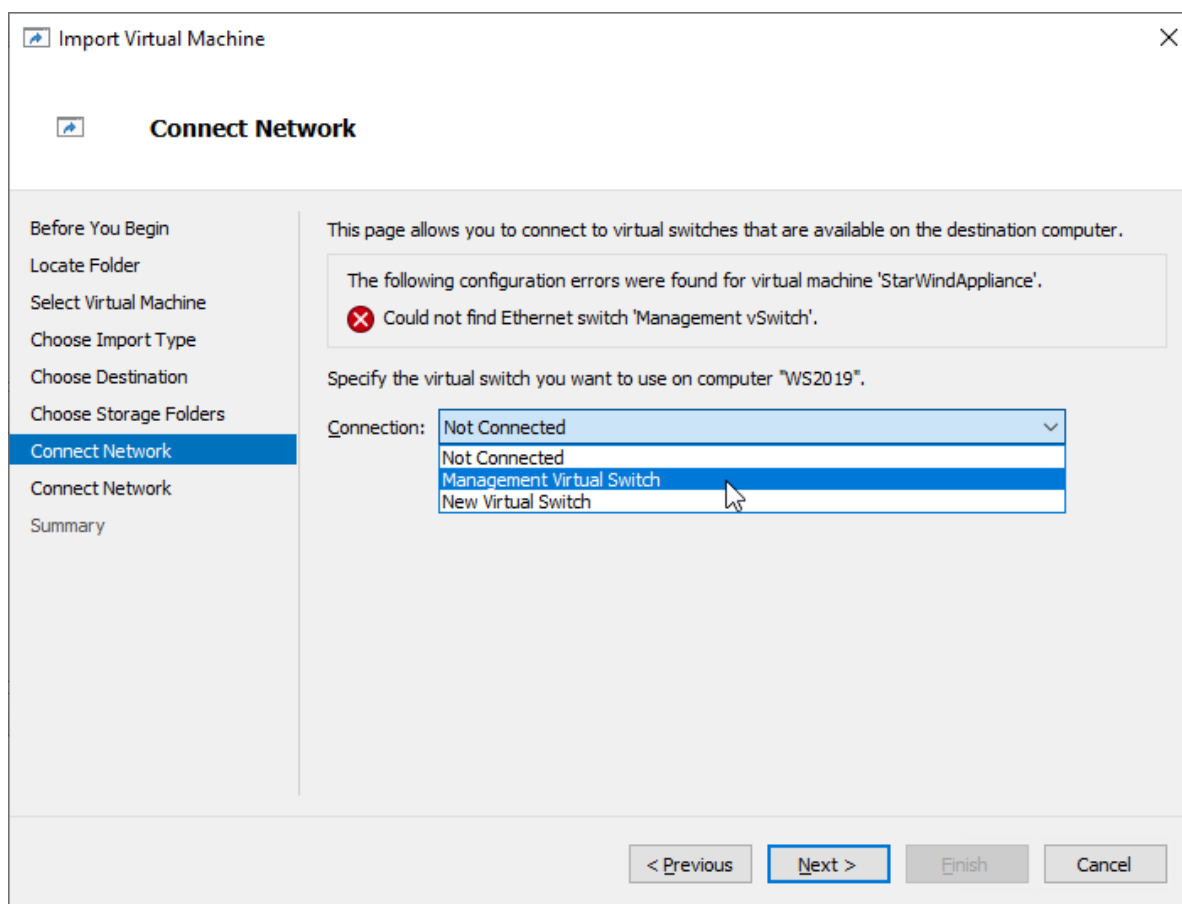


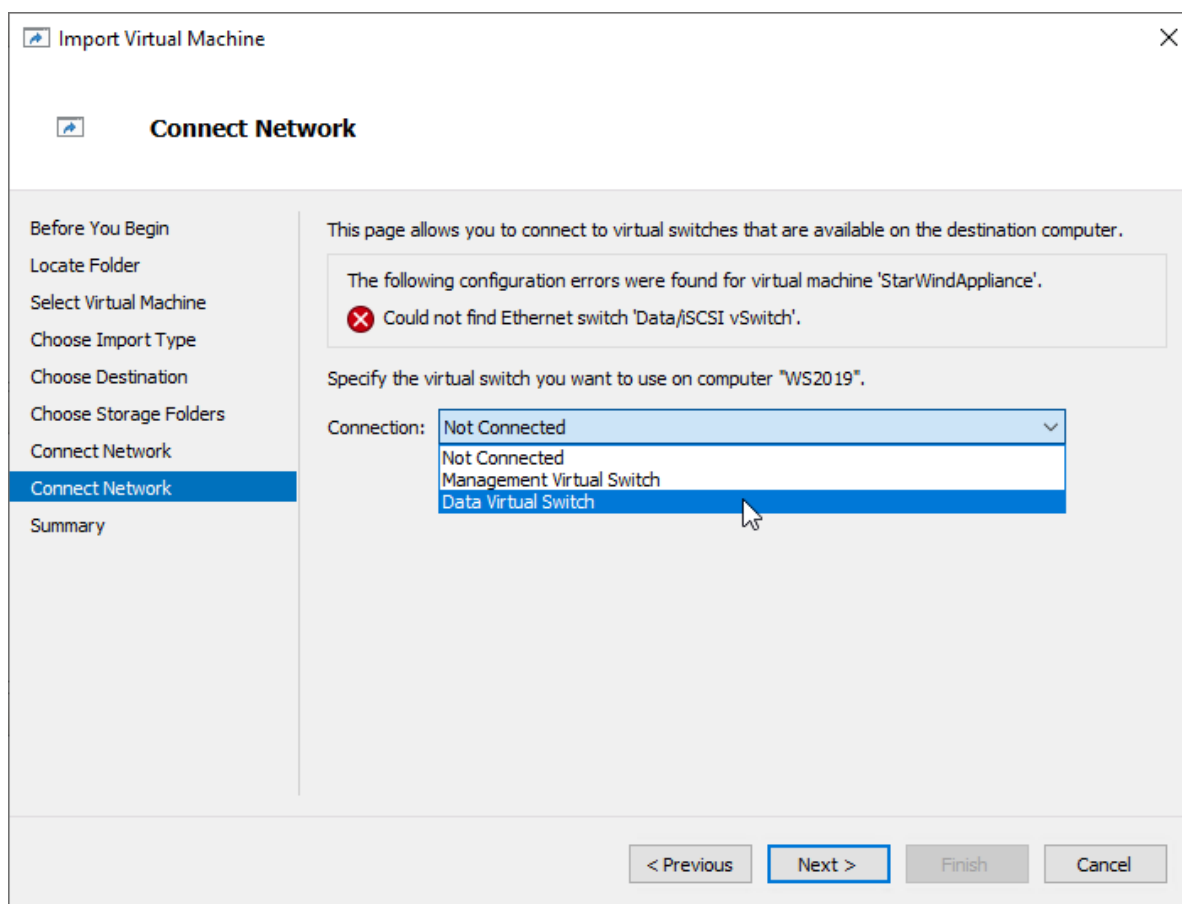
8. In the second step of the wizard, the “VM import” wizard will validate the network.

The default naming for virtual switches:

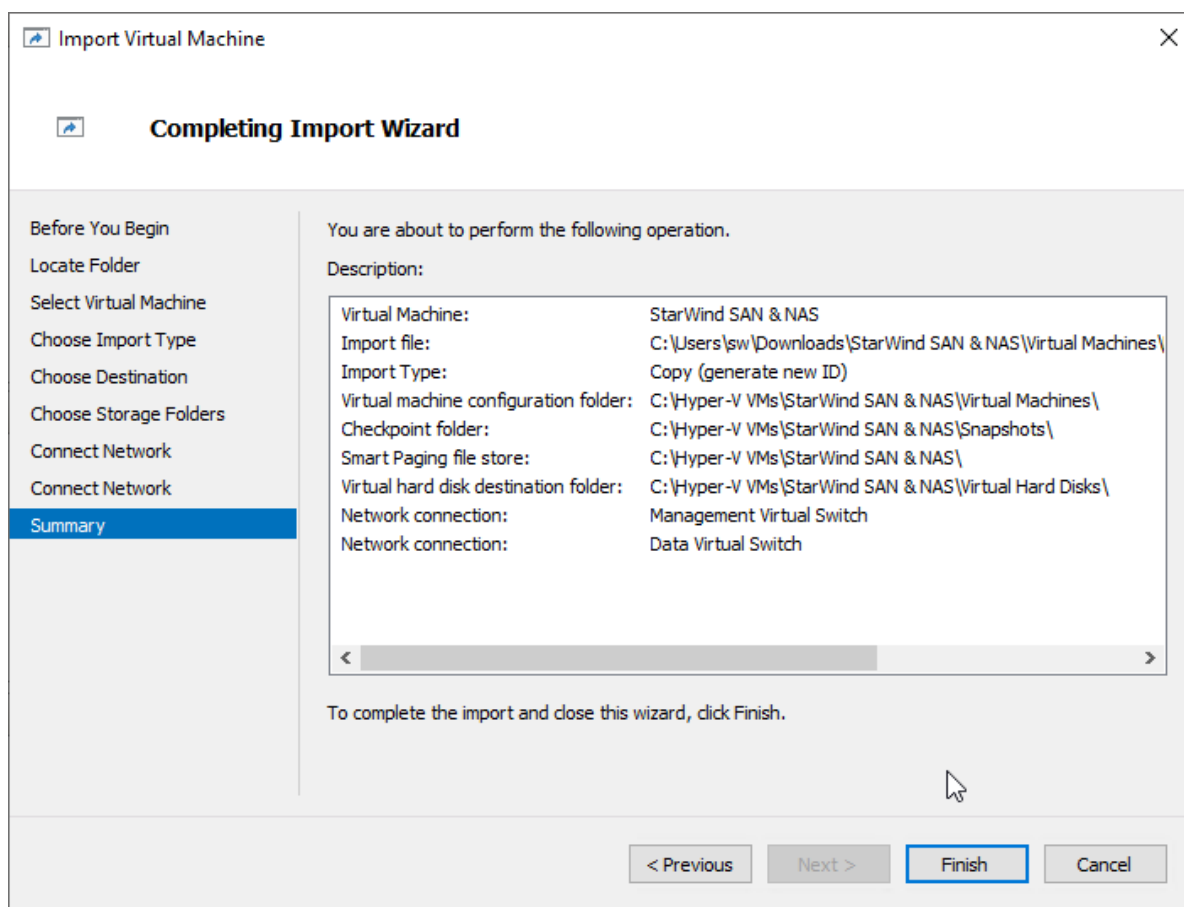
- the Management virtual switch is “Management vSwitch”
- the iSCSI virtual switch is “Data/iSCSI vSwitch”
- the Synchronization virtual switch is “Replication/Sync vSwitch”

If existing virtual switches have different names, specify corresponding network connections. Click Next.





9. Review the import configuration and click Finish to complete the import.



10. Repeat the VM deployment on each partner server which is used for configuring 2-node or 3-node highly available storage according to your licensing.

Initial Configuration Wizard

1. Start StarWind Virtual SAN CVM.

2. Launch VM console to see the VM boot process and get the IPv4 address of the Management network interface.

NOTE: in case VM has no IPv4 address obtained from a DHCP server, use the Text-based User Interface (TUI) to set up a Management network.

3. Using the web browser, open a new tab and enter the VM IPv4 address to open StarWind VSAN Web Interface. Click “Advanced” and then “Continue to...”



Your connection is not private

Attackers might be trying to steal your information from **192.168.12.206** (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR_CERT_AUTHORITY_INVALID

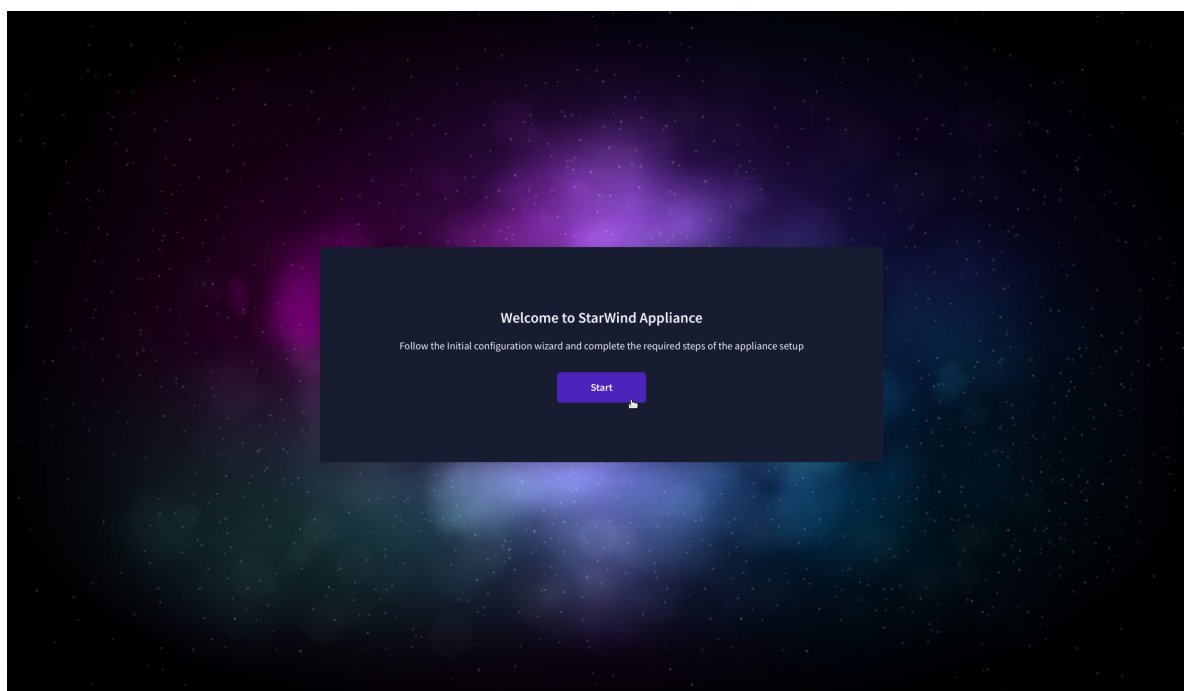
Hide advanced

Back to safety

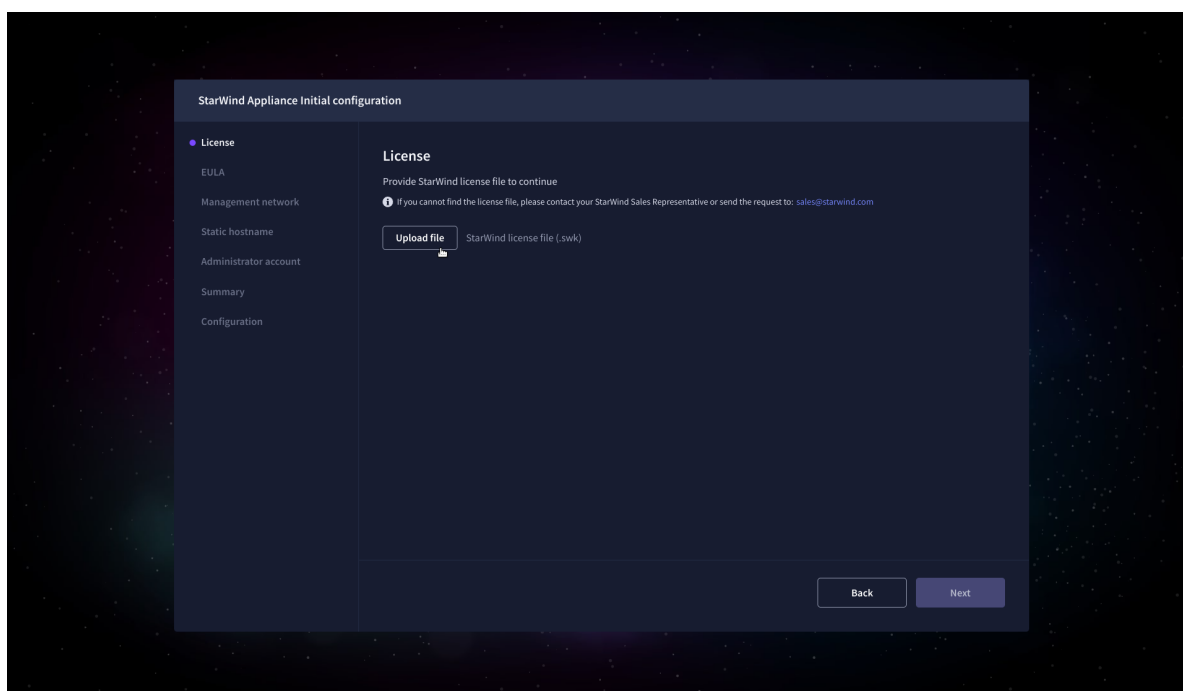
This server could not prove that it is **192.168.12.206**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.12.206 \(unsafe\)](#)

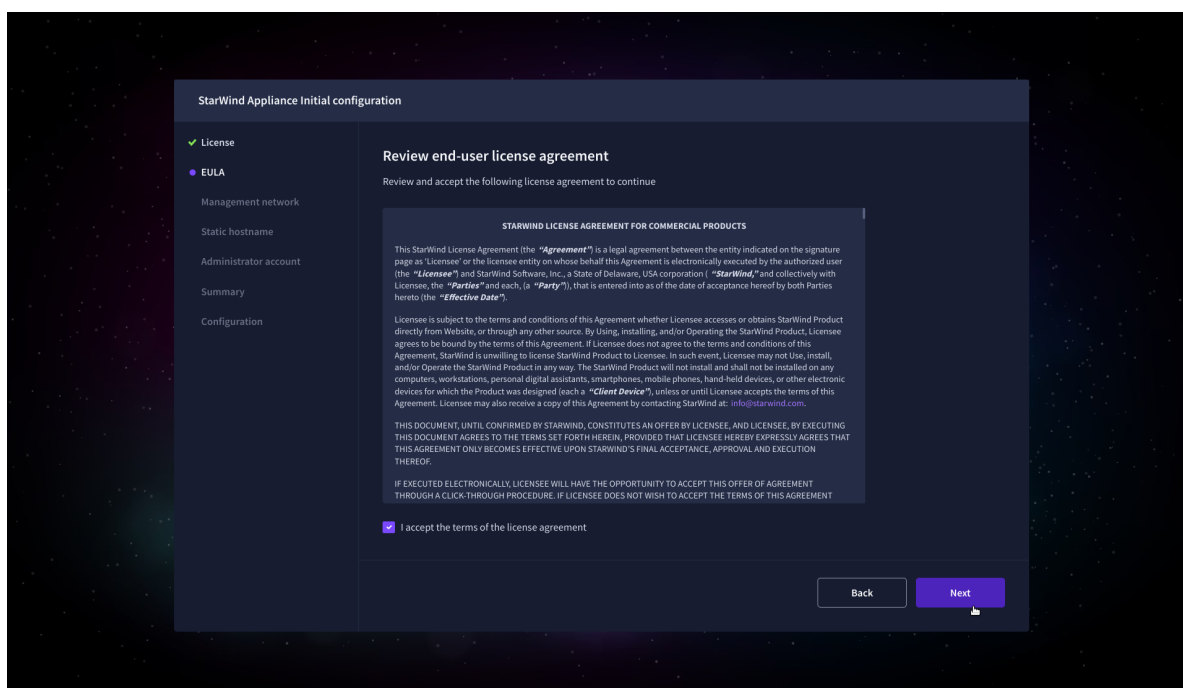
4. StarWind VSAN web UI welcomes you, and the “Initial Configuration” wizard will guide you through the deployment process.



5. In the following step, upload the license file.

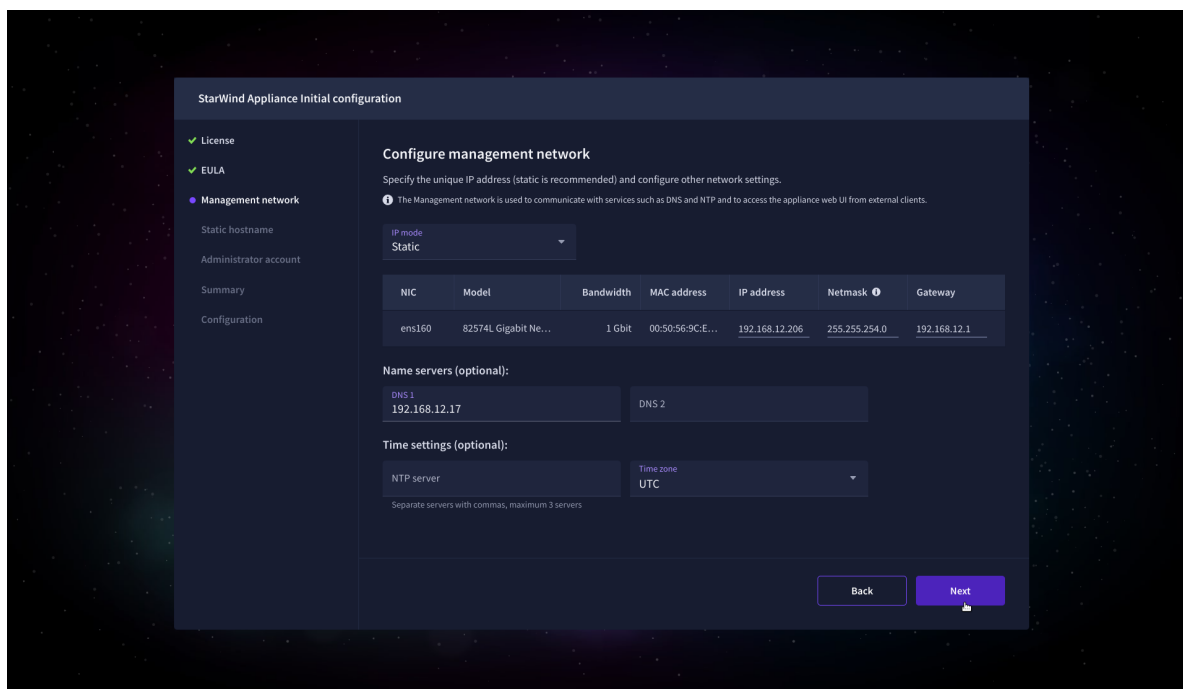


6. Read and accept the End User License Agreement to proceed.



7. Review or edit the Network settings and click Next.

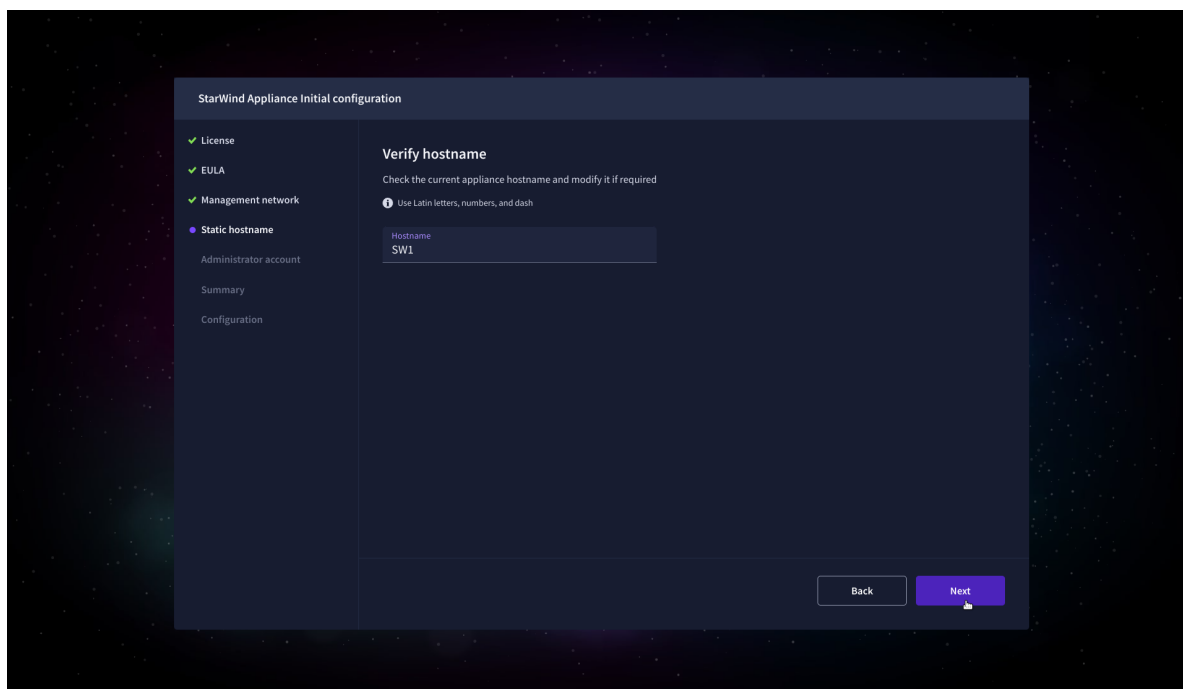
NOTE: Static network settings are recommended for the configuration.



The screenshot shows the 'StarWind Appliance Initial configuration' window. On the left sidebar, the 'Management network' step is selected. The main area is titled 'Configure management network' and includes instructions to specify a unique IP address. A table lists network details for the 'ens160' interface. Below the table, there are optional fields for DNS servers and NTP settings. 'Back' and 'Next' buttons are at the bottom right.

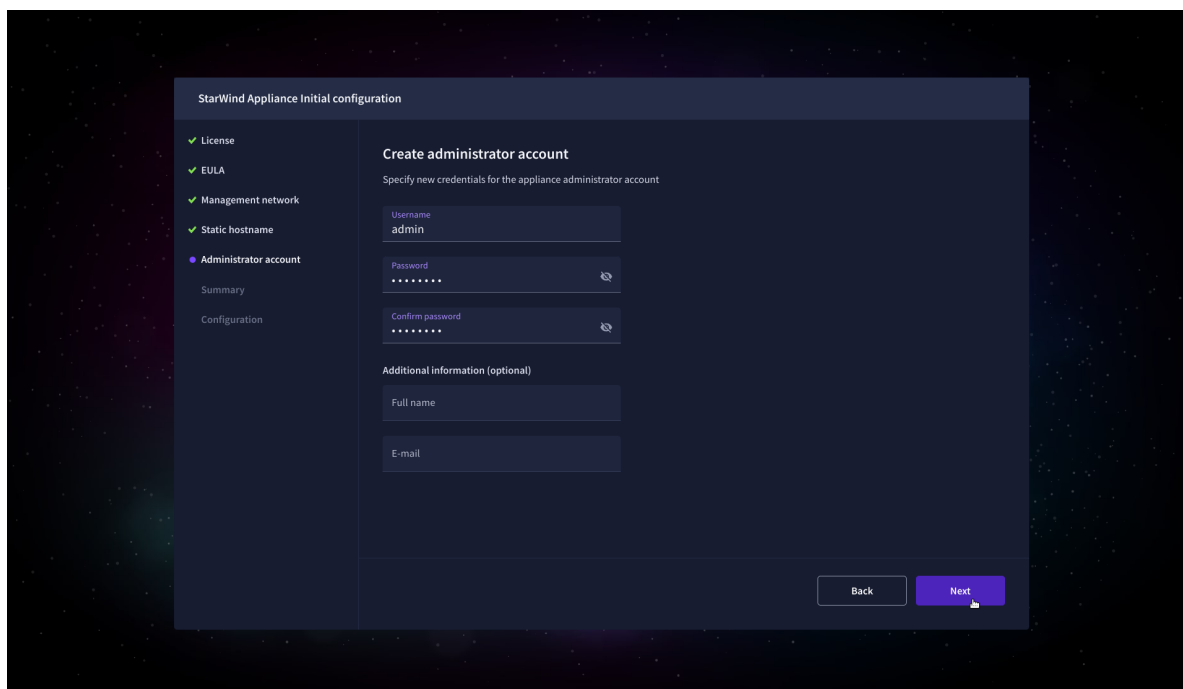
NIC	Model	Bandwidth	MAC address	IP address	Netmask	Gateway
ens160	82574L Gigabit Ne...	1 Gbit	00:50:56:9C:E...	192.168.12.206	255.255.254.0	192.168.12.1

8. Specify the hostname for the virtual machine and click Next.



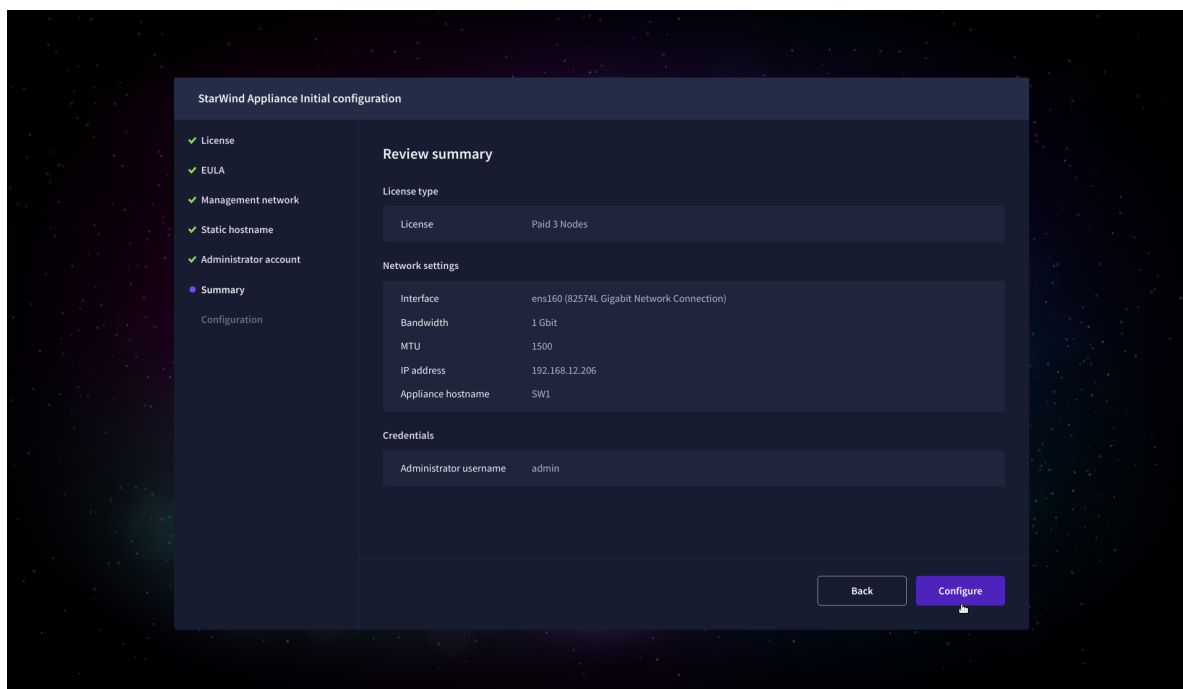
The screenshot shows the 'StarWind Appliance Initial configuration' window. On the left sidebar, the 'Static hostname' step is selected. The main area is titled 'Verify hostname' and includes instructions to check the current appliance hostname. A text field shows the hostname 'SW1'. 'Back' and 'Next' buttons are at the bottom right.

9. Create an administrator account. Click Next.



The screenshot shows the 'StarWind Appliance Initial configuration' window. On the left sidebar, the steps are: License (checked), EULA (checked), Management network (checked), Static hostname (checked), Administrator account (selected), Summary, and Configuration. The main area is titled 'Create administrator account' with the instruction 'Specify new credentials for the appliance administrator account'. It contains three input fields: 'Username' with the value 'admin', 'Password' (masked with dots), and 'Confirm password' (masked with dots). Below these are optional fields for 'Full name' and 'E-mail'. At the bottom right are 'Back' and 'Next' buttons.

10. Review your settings selection before setting up StarWind VSAN.

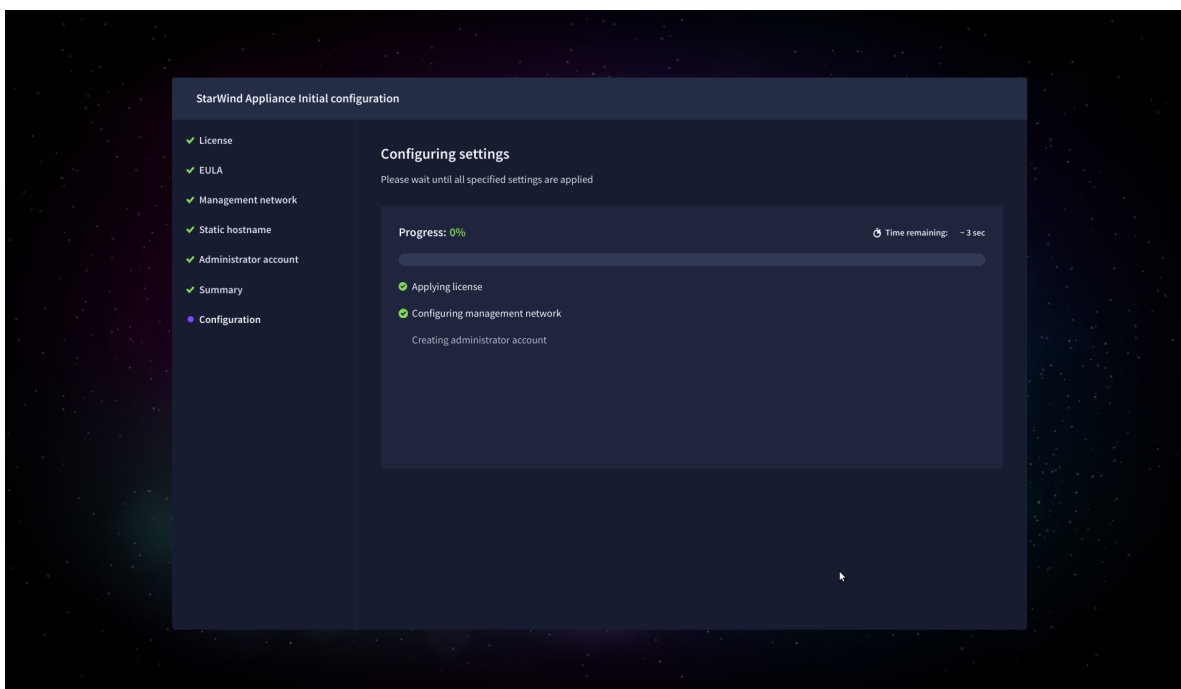


The screenshot shows the 'StarWind Appliance Initial configuration' window at the 'Review summary' step. The left sidebar now has 'Summary' selected. The main area is titled 'Review summary' and displays the following configuration details:

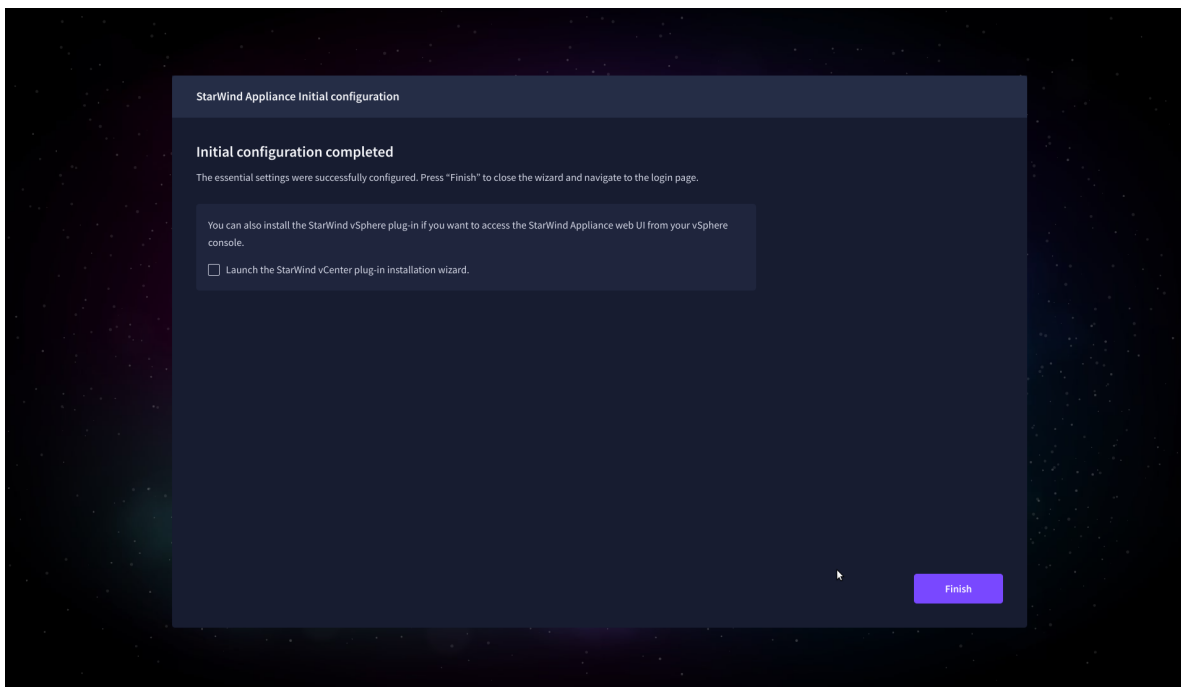
- License type:** License Paid 3 Nodes
- Network settings:**
 - Interface: ens160 (82574L Gigabit Network Connection)
 - Bandwidth: 1 Gbit
 - MTU: 1500
 - IP address: 192.168.12.206
 - Appliance hostname: SW1
- Credentials:**
 - Administrator username: admin

At the bottom right are 'Back' and 'Configure' buttons.

11. Please standby until the Initial Configuration Wizard configures StarWind VSAN for you.



12. The appliance is set and ready. Click on the Done button to install the StarWind vCenter Plugin right now or uncheck the checkbox to skip this step and proceed to the [Login page](#).



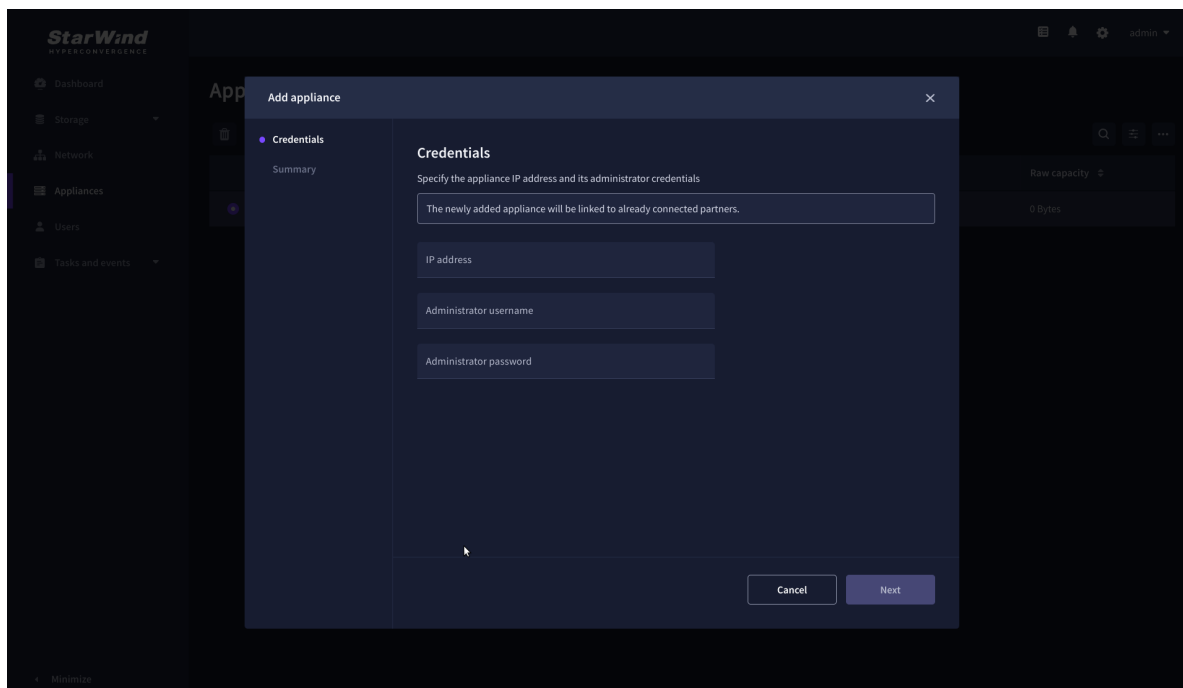
13. Repeat the initial configuration on other StarWind CVMs that will be used to create 2-node or 3-node HA shared storage.

Add Appliance

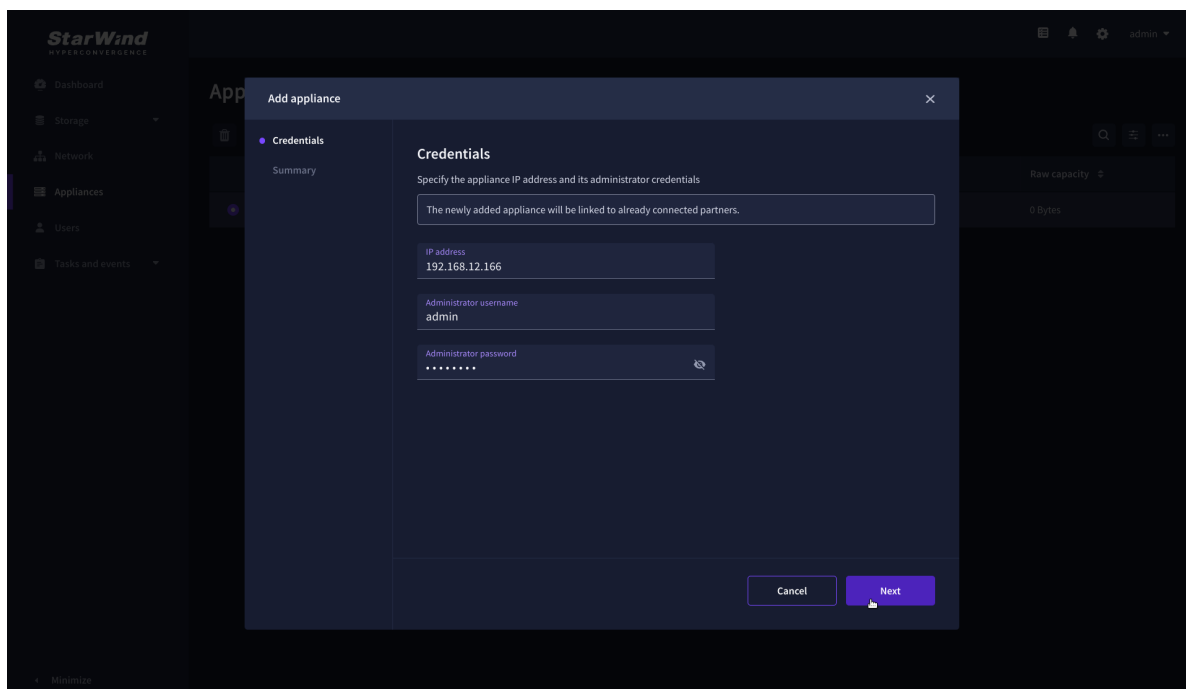
To create 2-way or 3-way synchronously replicated highly available storage, add partner appliances that use the same license key.

1. Add StarWind appliance(s) in the web console, on the Appliances page.

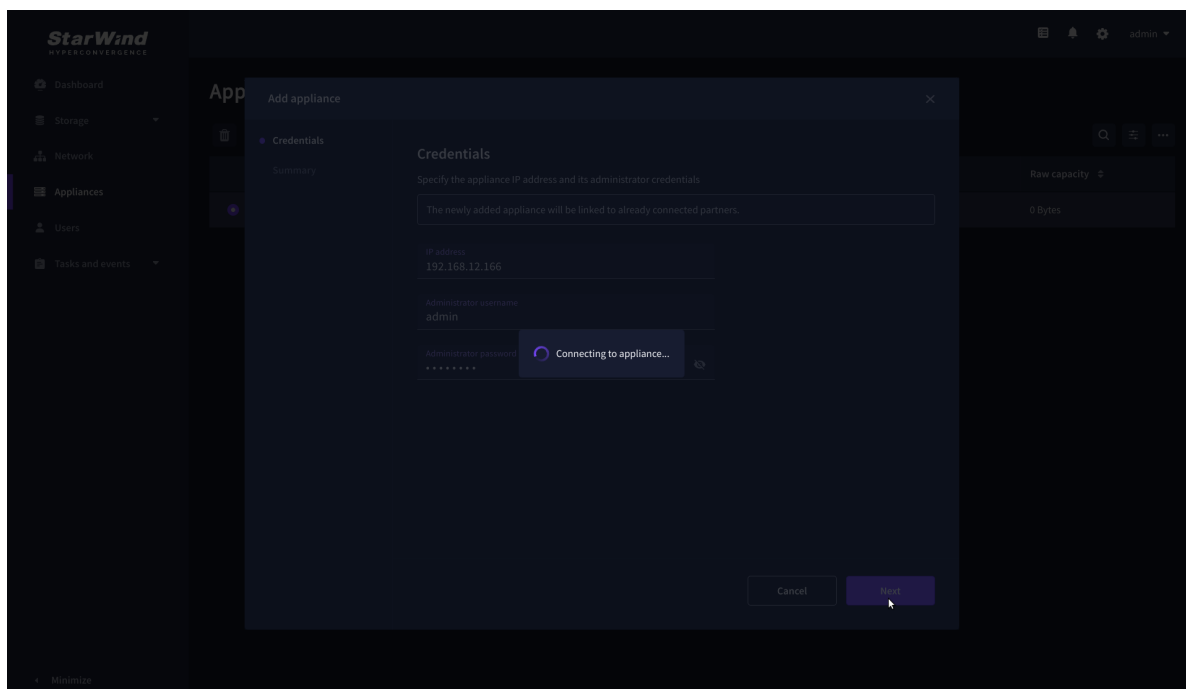
NOTE: The newly added appliance will be linked to already connected partners.



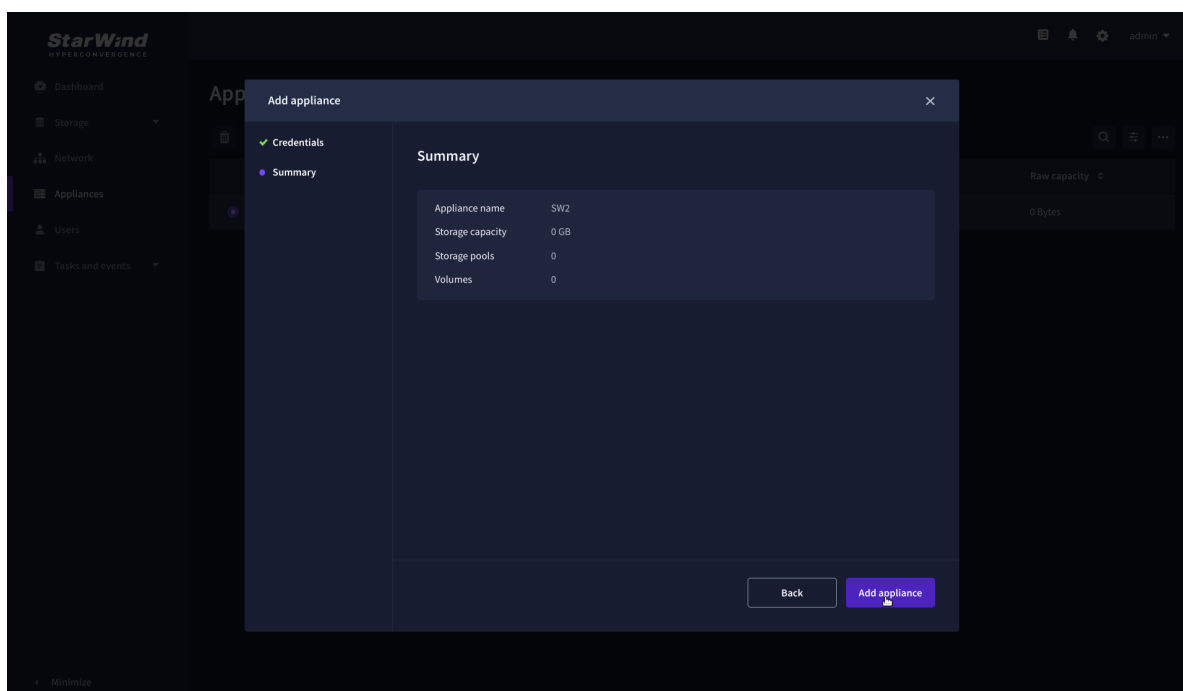
2. Provide credentials of partner appliance.



3. Wait for connection and validation of settings.

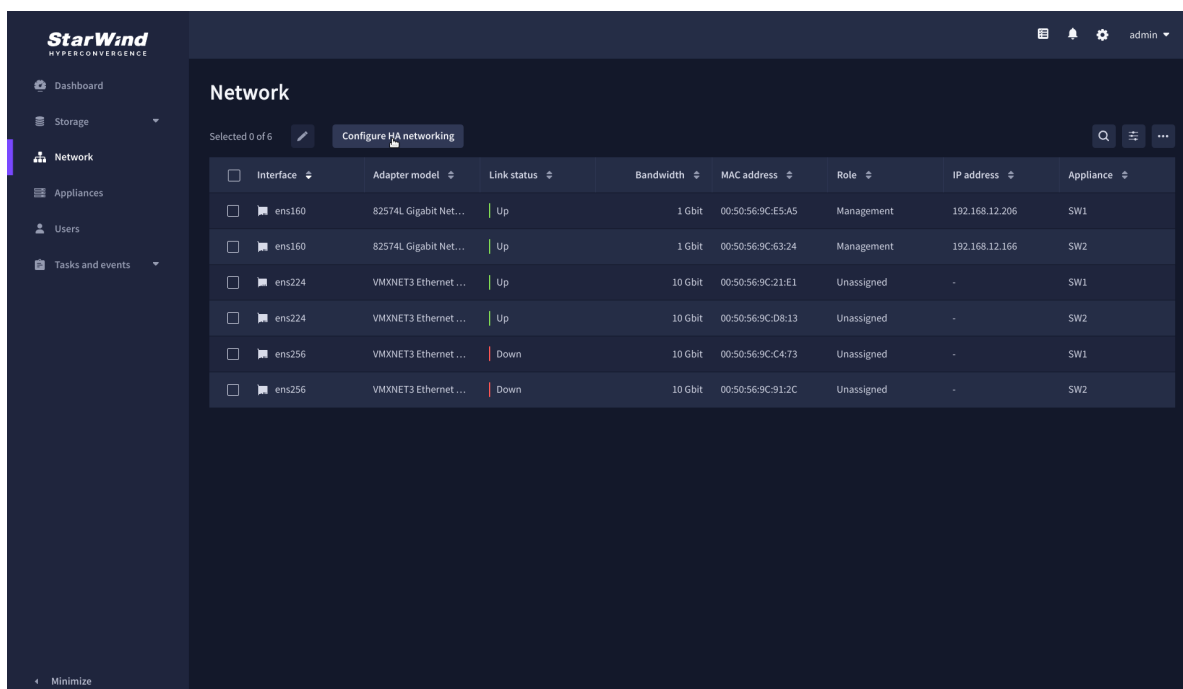


4. Review the summary and click “Add appliance”.



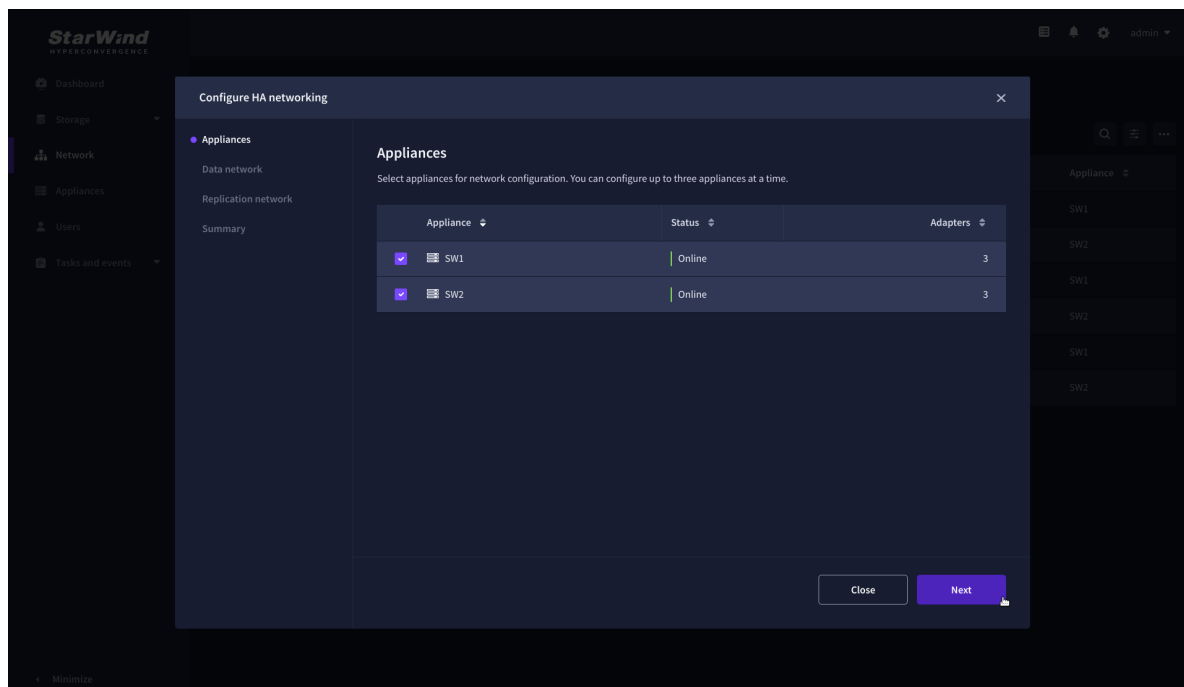
Configure Ha Networking

1. Launch the “Configure HA Networking” wizard.



2. Select appliances for network configuration.

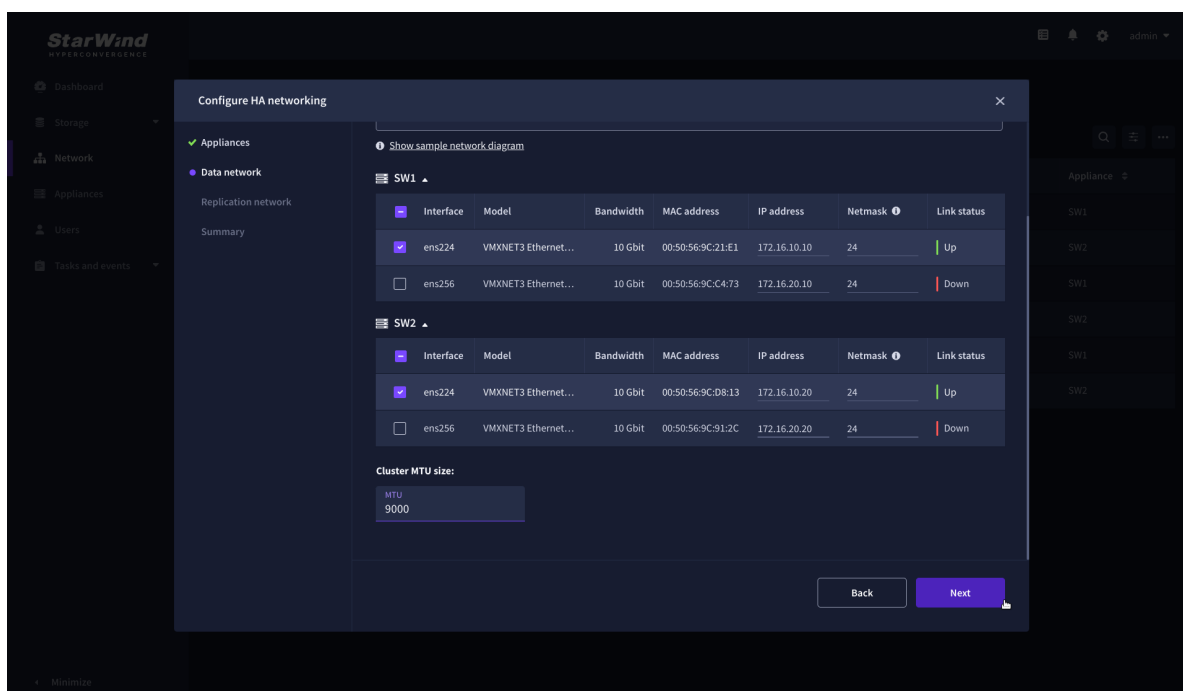
NOTE: the number of appliances to select is limited by your license, so can be either two or three appliances at a time.



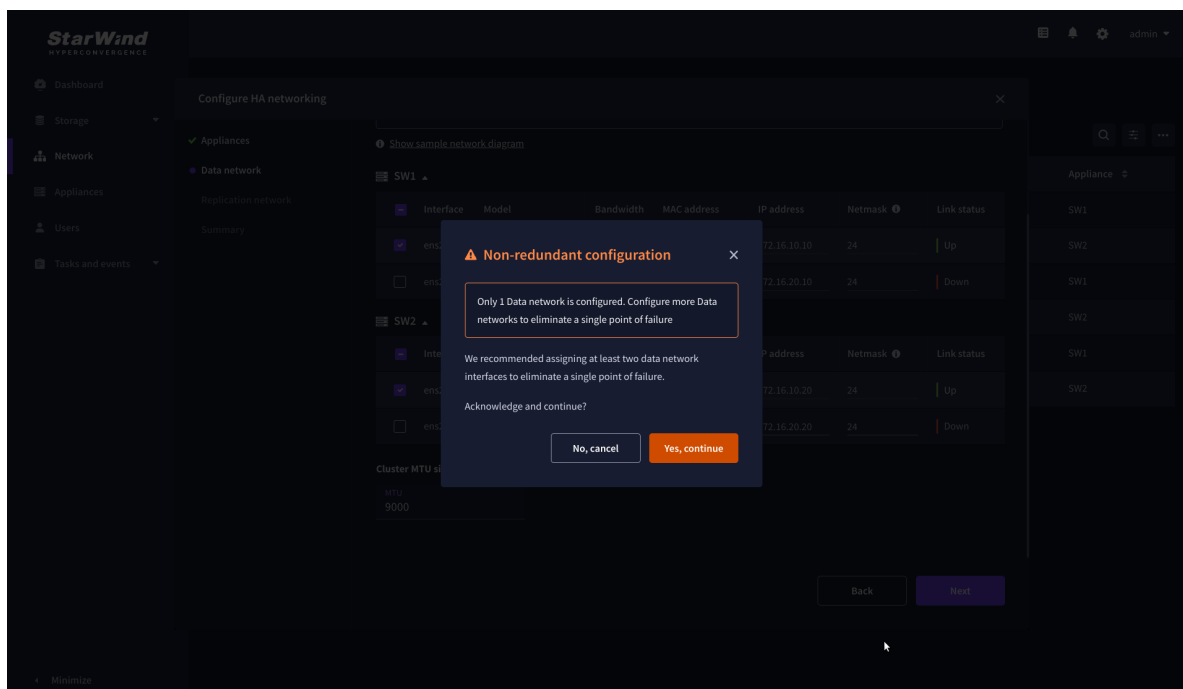
3. Configure the “Data” network. Select interfaces to carry storage traffic, configure them with static IP addresses in unique networks, and specify subnet masks:

- assign and configure at least one interface on each node
- for redundant configuration, select two interfaces on each node
- ensure interfaces are connected to client hosts directly or through redundant switches

4. Assign MTU value to all selected network adapters, e.g. 1500 or 9000. Ensure the switches have the same MTU value set.



5. Click Next to validate Data network settings.

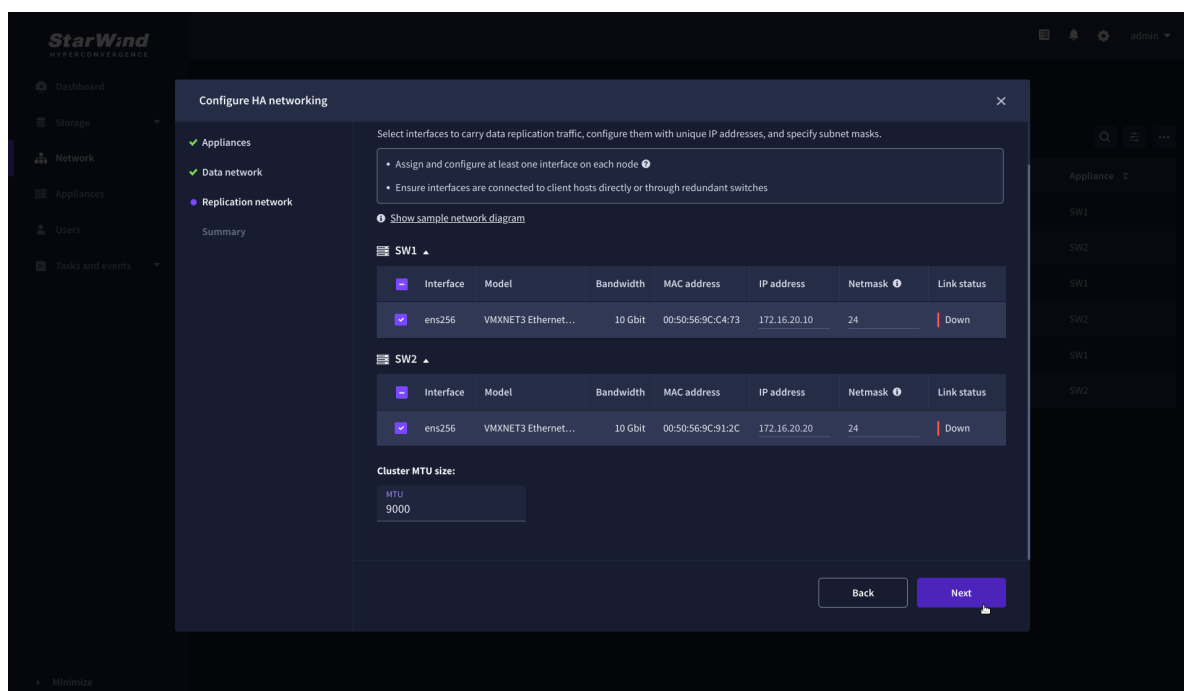


6. Configure the “Replication” network. Select interfaces to carry storage traffic, configure them with static IP addresses in unique networks, and specify subnet masks:

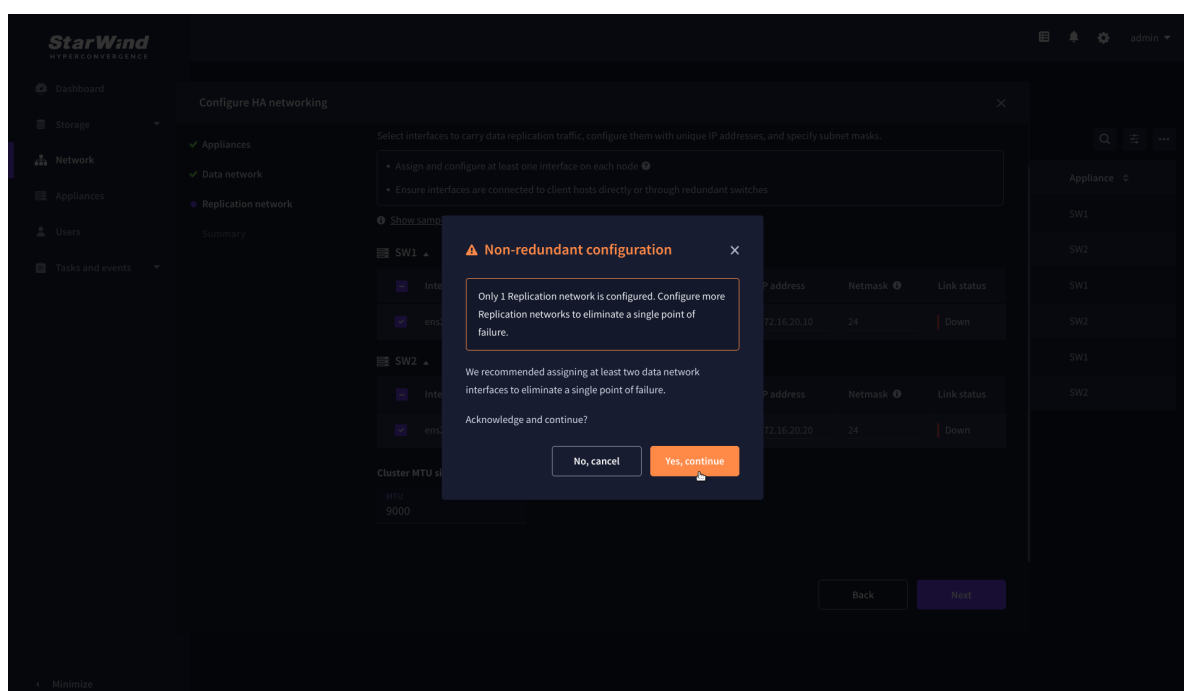
- assign and configure at least one interface on each node
- for redundant configuration, select two interfaces on each node

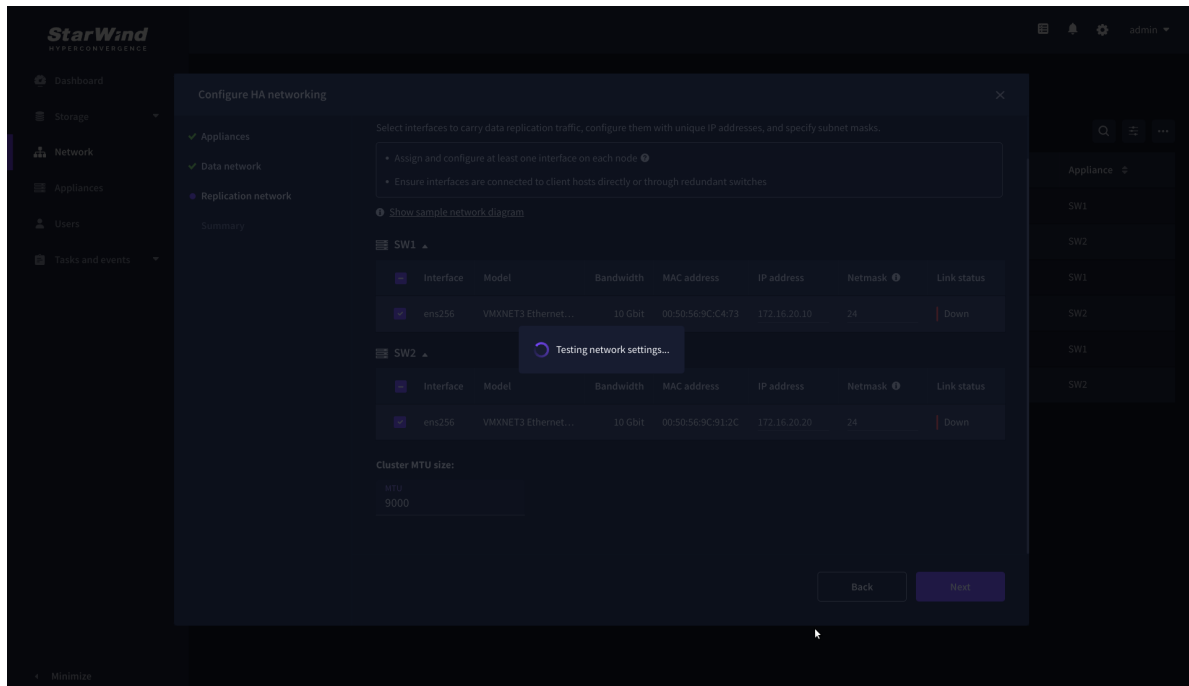
- ensure interfaces are connected to client hosts directly or through redundant switches

7. Assign MTU value to all selected network adapters, e.g. 1500 or 9000. Ensure the switches have the same MTU value set.

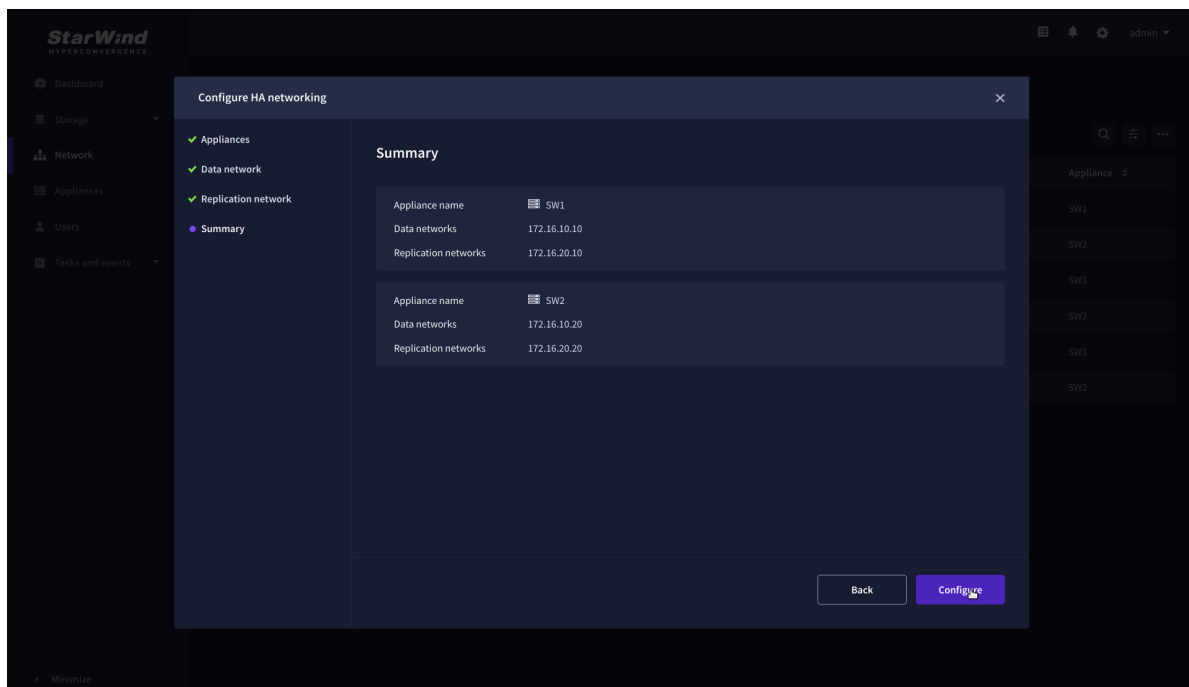


8. Click Next to validate the Replication network settings completion.





9. Review the summary and click Configure.



Add Physical Disks

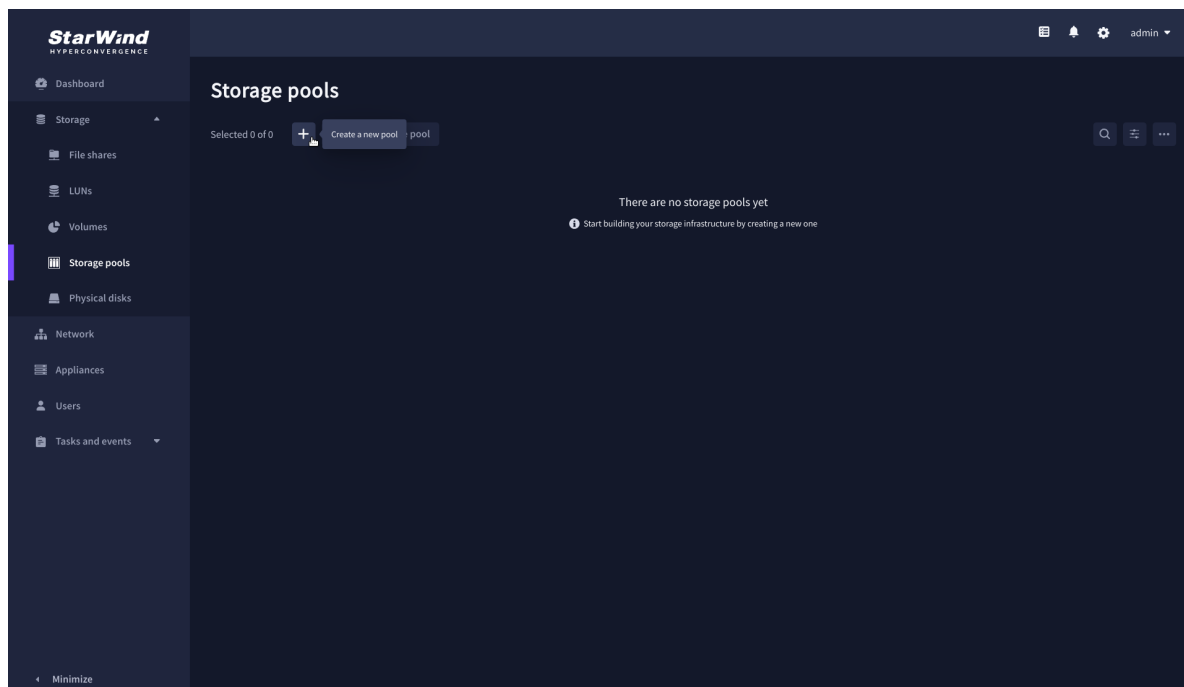
Attach physical storage to StarWind Virtual SAN Controller VM:

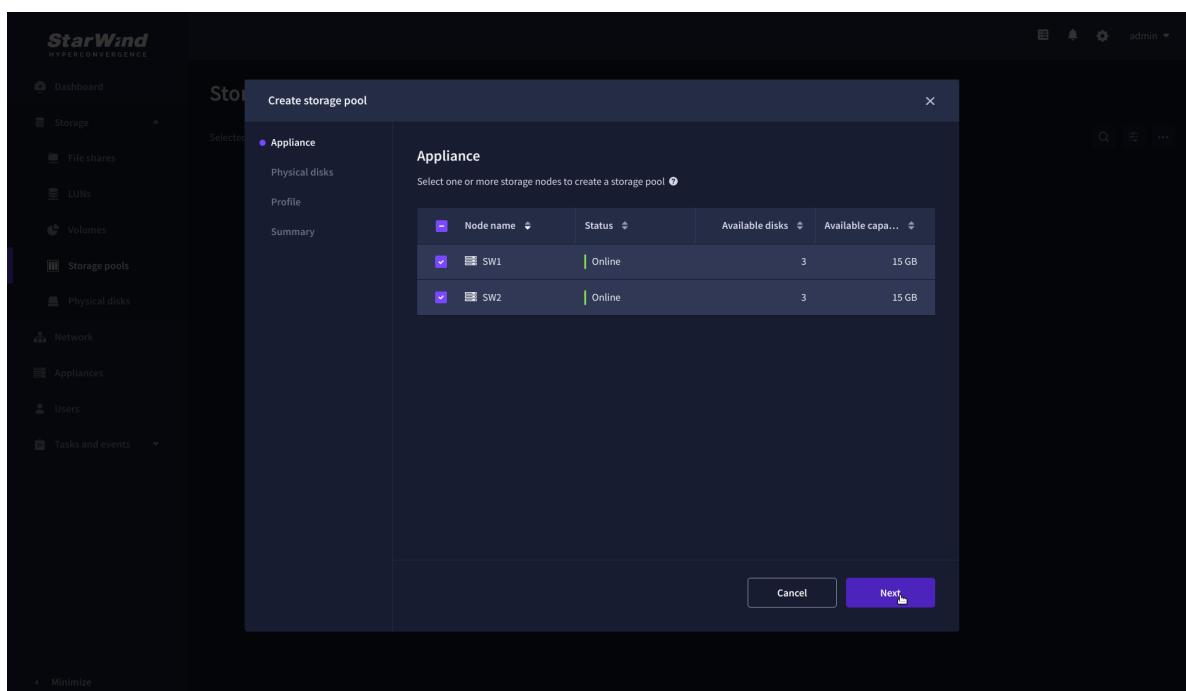
- Ensure that all physical drives are connected through an HBA or RAID controller.
- Deploy StarWind VSAN CVM on each server that will be used to configure fault-tolerant standalone or highly available storage.
- Store StarWind VSAN CVM on a separate storage device accessible to the hypervisor host (e.g., SSD, HDD).
- Add HBA, RAID controllers, or NVMe SSD drives to StarWind CVM via a passthrough device.

Learn more about storage provisioning guidelines in the [KB article](#).

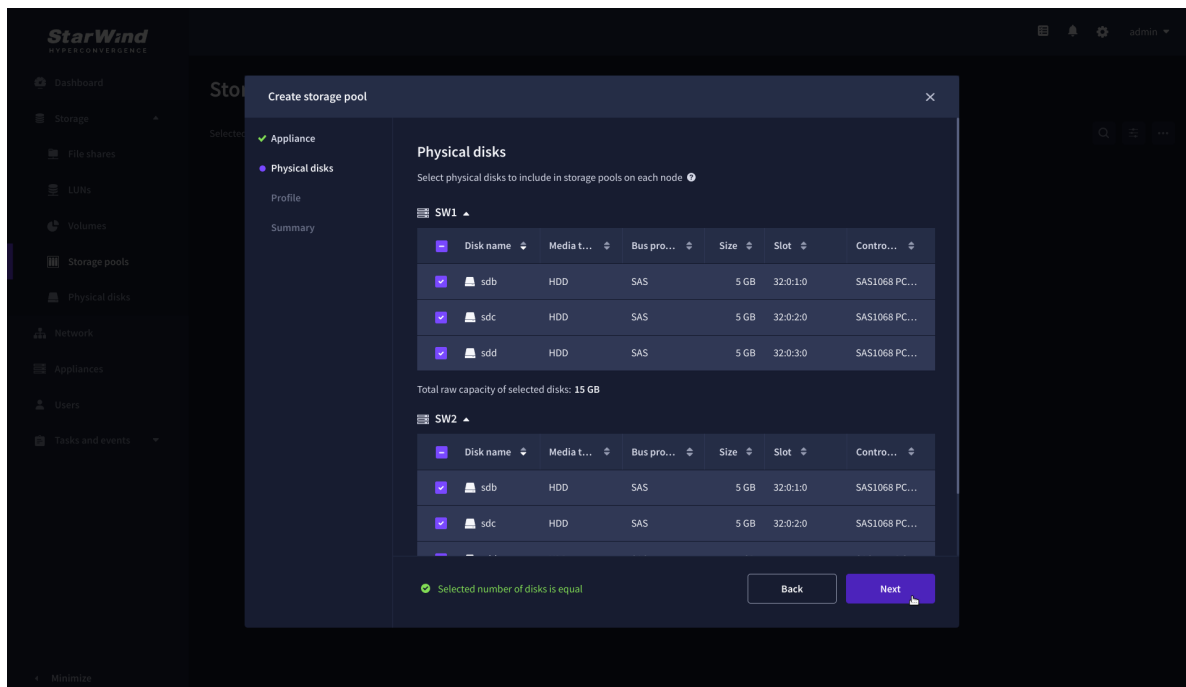
Create Storage Pool

1. Click the “Add” button to create a storage pool.
2. Select two storage nodes to create a storage pool on them simultaneously.

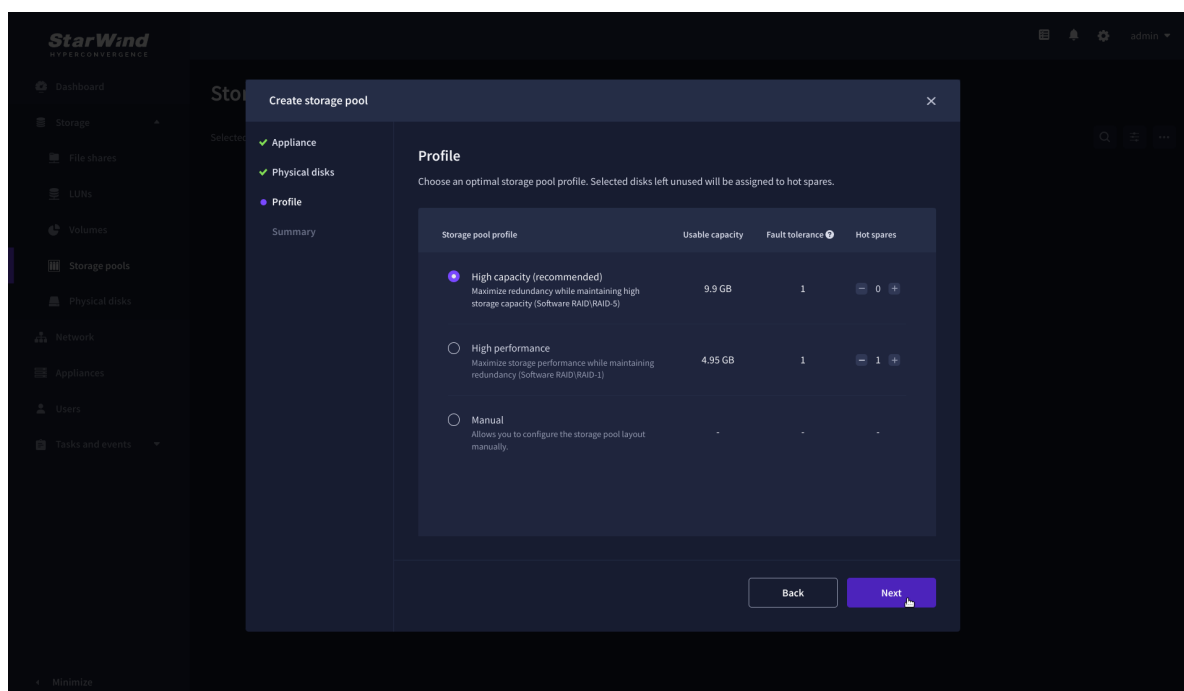




3. Select physical disks to include in the storage pool name and click the “Next” button.
NOTE: Select identical type and number of disks on each storage node to create identical storage pools.



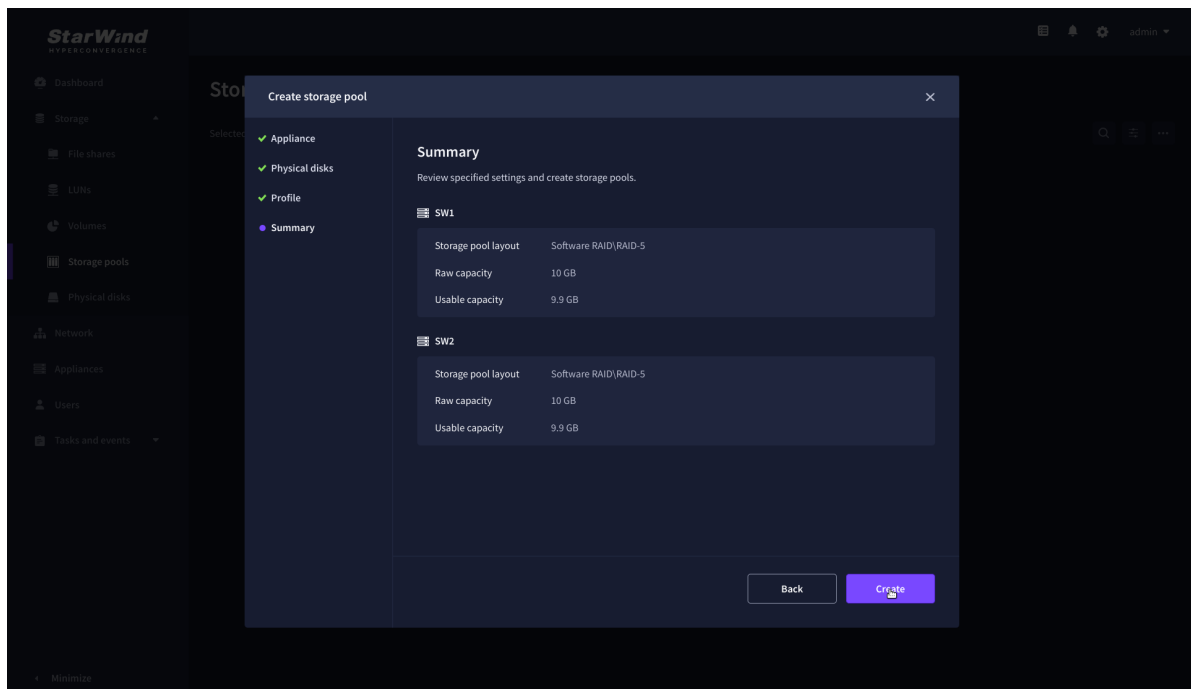
4. Select one of the preconfigured storage profiles or create a redundancy layout for the new storage pool manually according to your redundancy, capacity, and performance requirements.



Hardware RAID, Linux Software RAID, and ZFS storage pools are supported and integrated into the StarWind CVM web interface. To make easier the storage pool configuration, the preconfigured storage profiles are provided to configure the recommended pool type and layout according to the direct-attached storage:

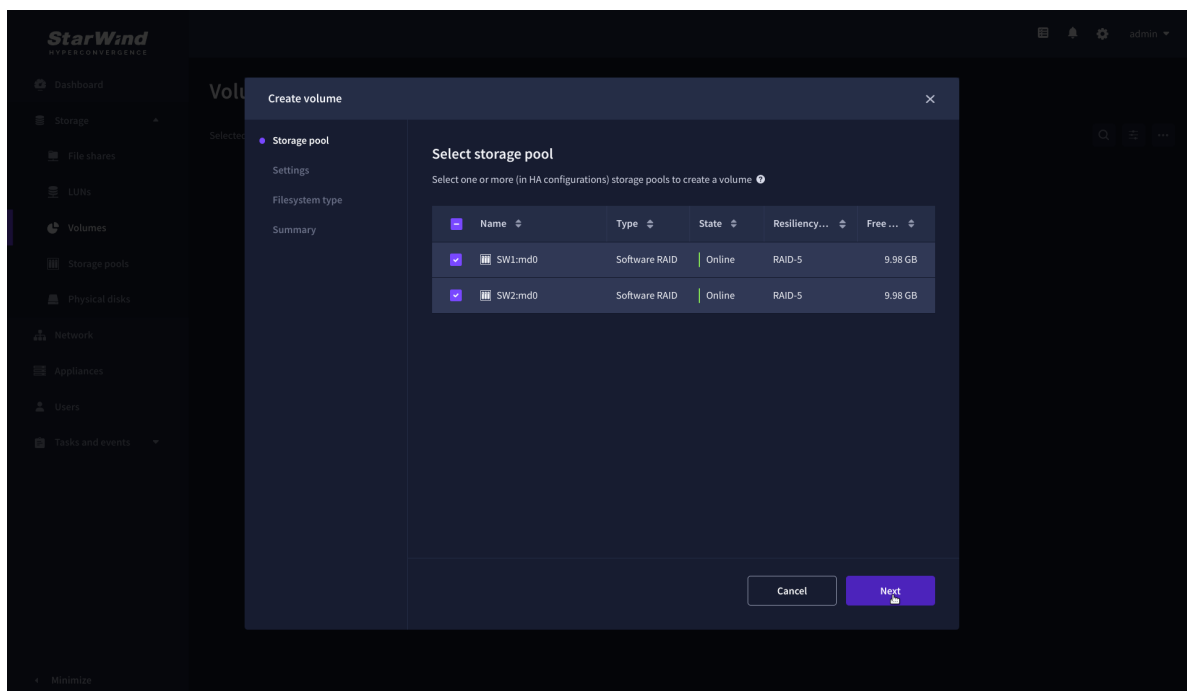
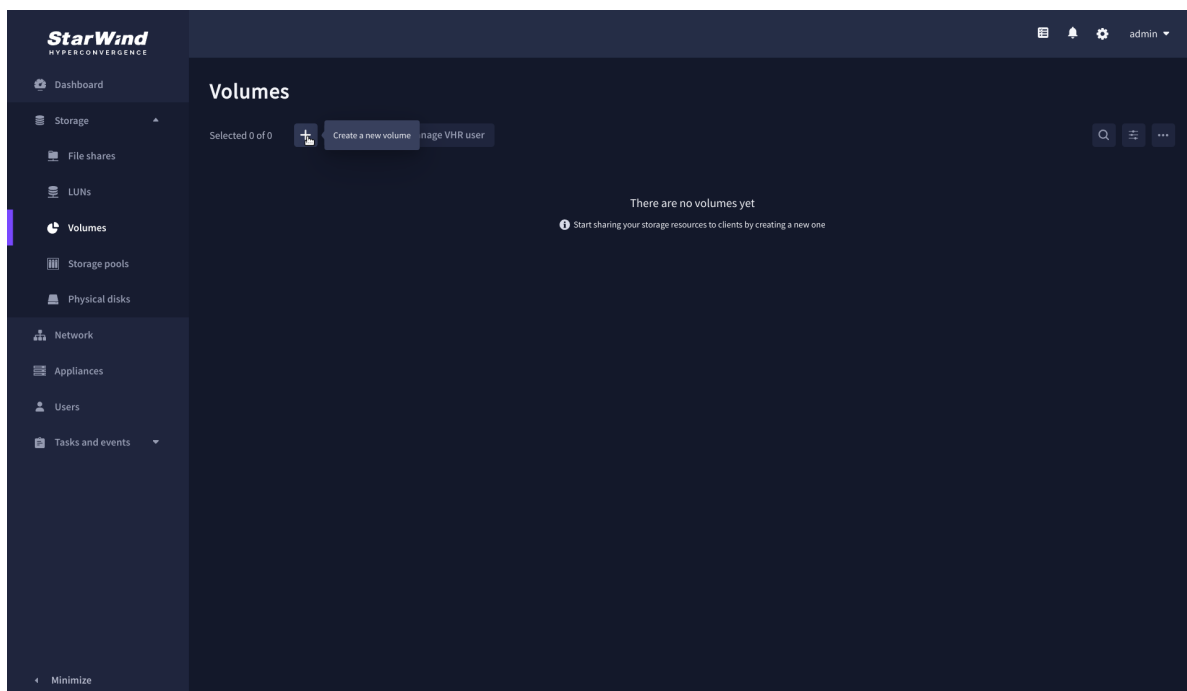
- hardware RAID – configures Hardware RAID’s virtual disk as a storage pool. It is available only if a hardware RAID controller is passed through to the CVM
- high performance – creates Linux Software RAID-10 to maximize storage performance while maintaining redundancy
- high capacity – creates Linux Software RAID-5 to maximize storage capacity while maintaining redundancy
- better redundancy – creates ZFS Stripped RAID-Z2 (RAID 60)) to maximize redundancy while maintaining high storage capacity
- manual – allows users to configure any storage pool type and layout with attached storage

5. Review “Summary” and click the “Create” button to create the pools on storage servers simultaneously.

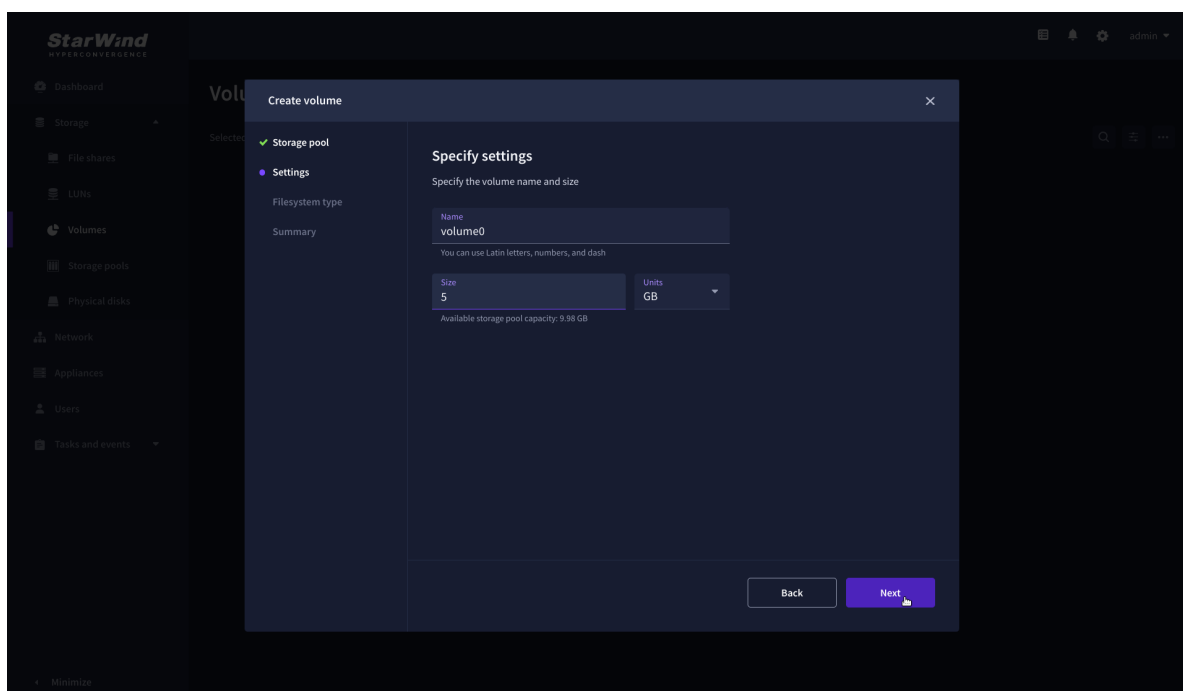


Create Volume

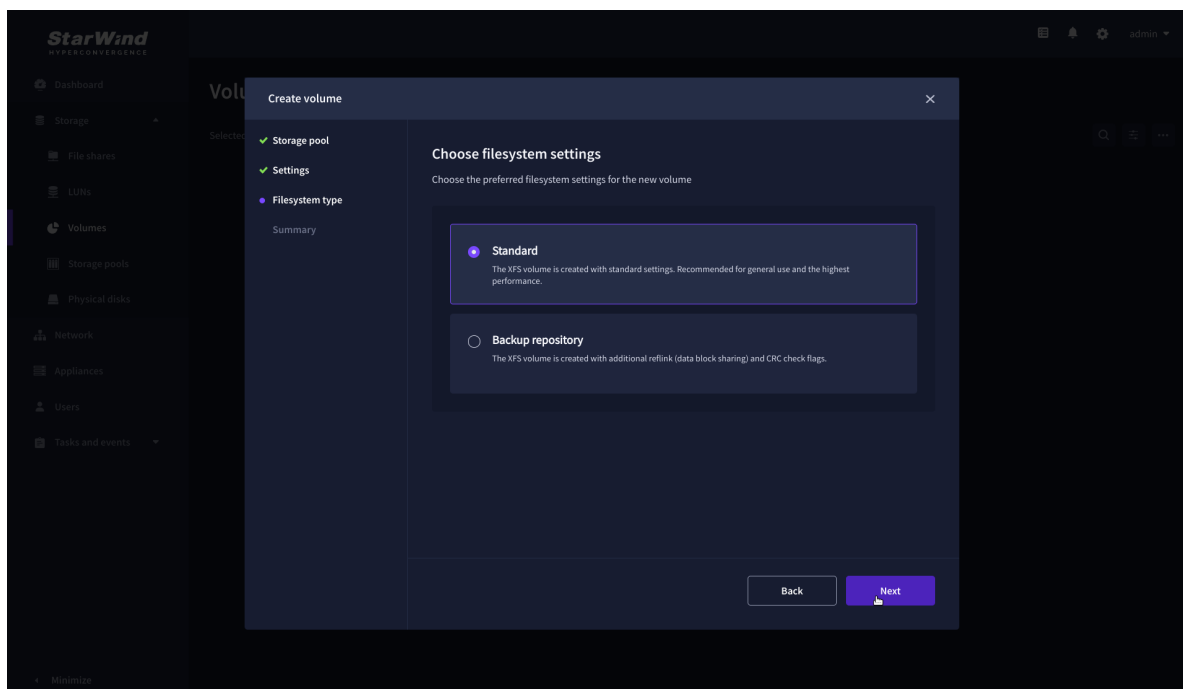
1. To create volumes, click the “Add” button.
2. Select two identical storage pools to create a volume simultaneously.



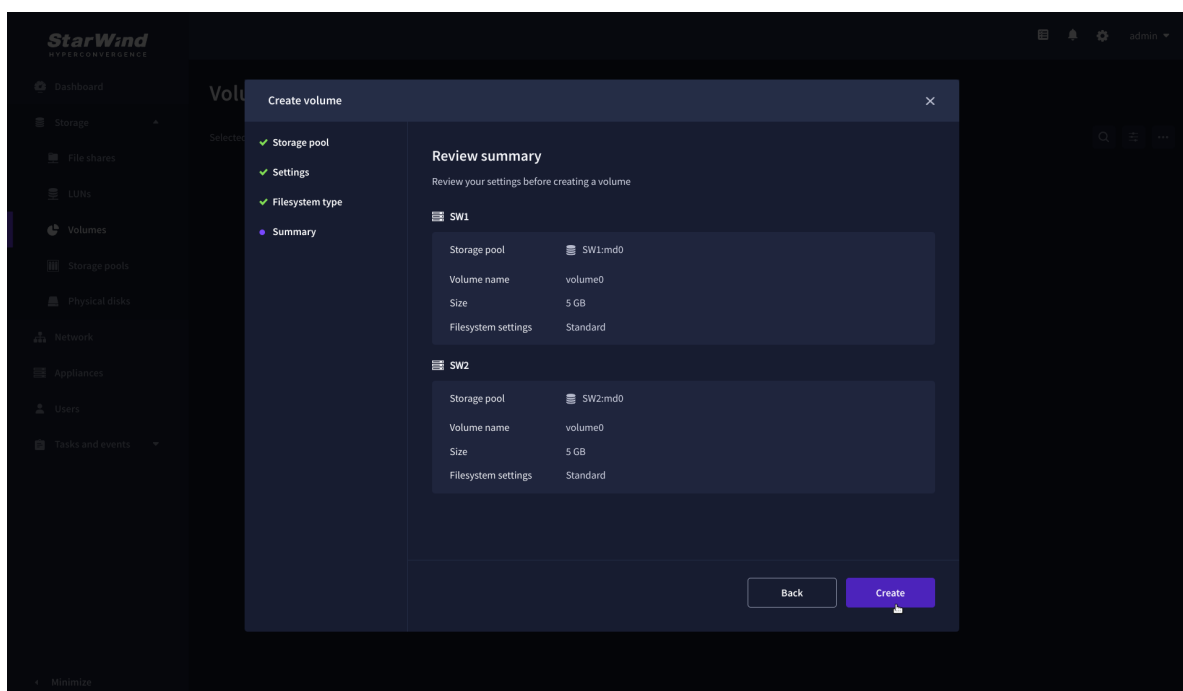
3. Specify volume name and capacity.



4. Select the Standard volume type.



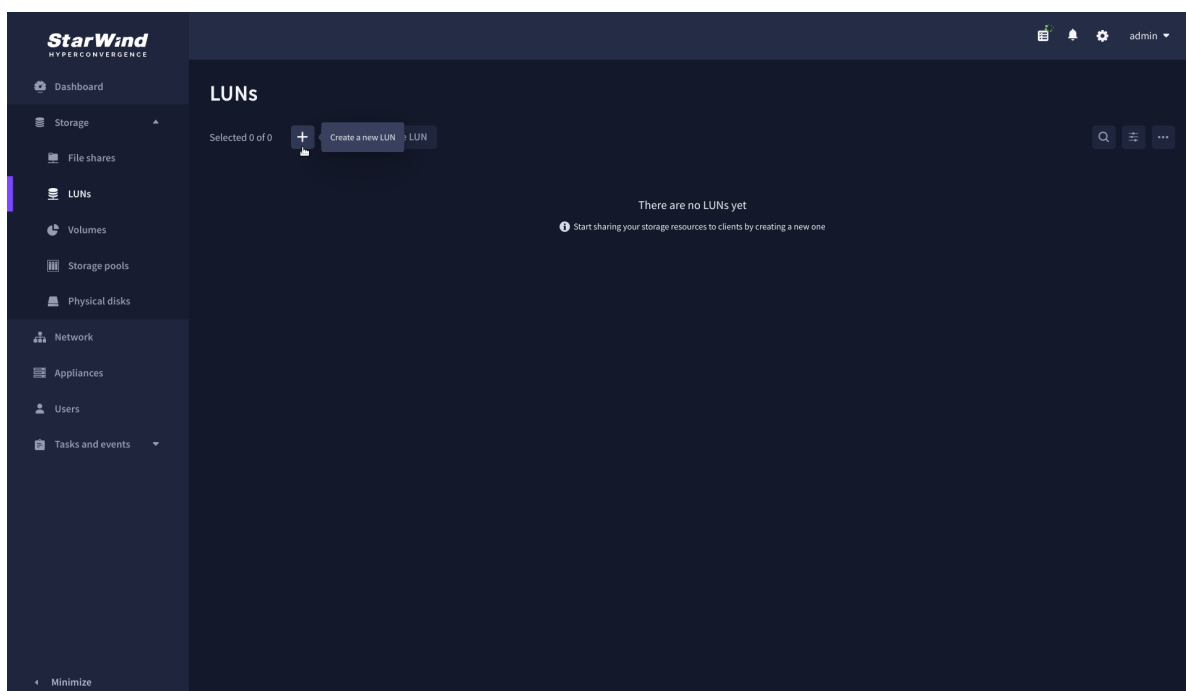
5. Review “Summary” and click the “Create” button to create the pool.



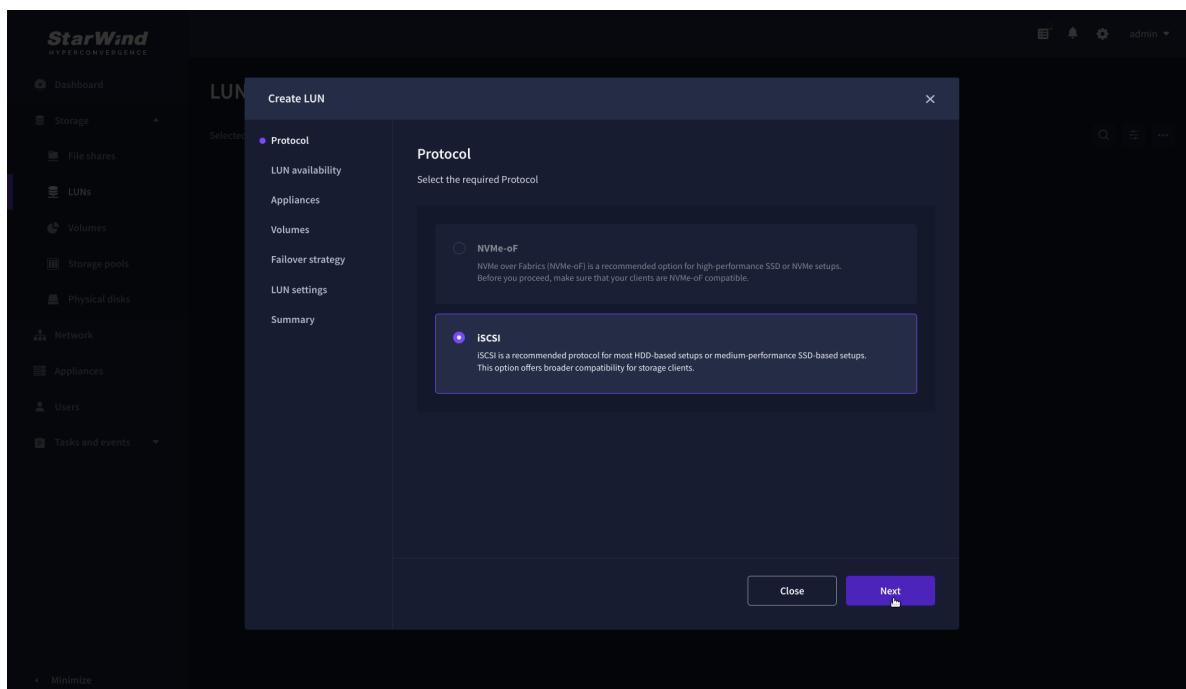
Create Ha Lun

The LUN availability for StarWind LUN can be Standalone and High availability (2-way or 3-way replication) and is narrowed by your license.

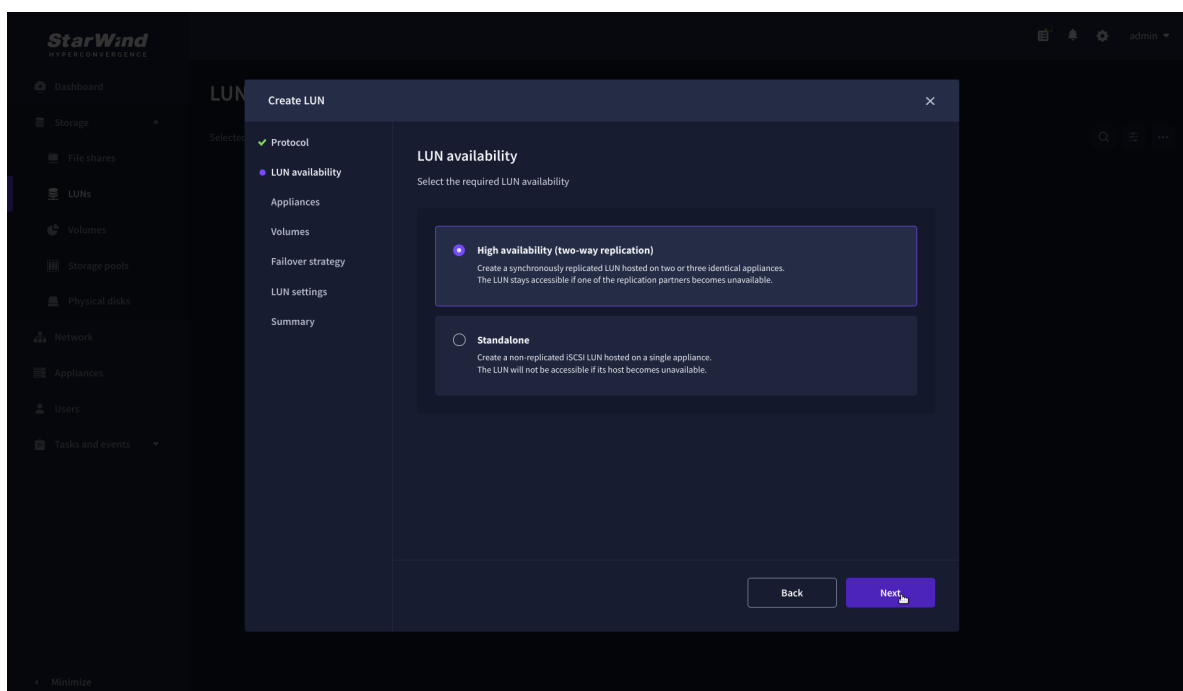
1. To create a virtual disk, click the Add button.



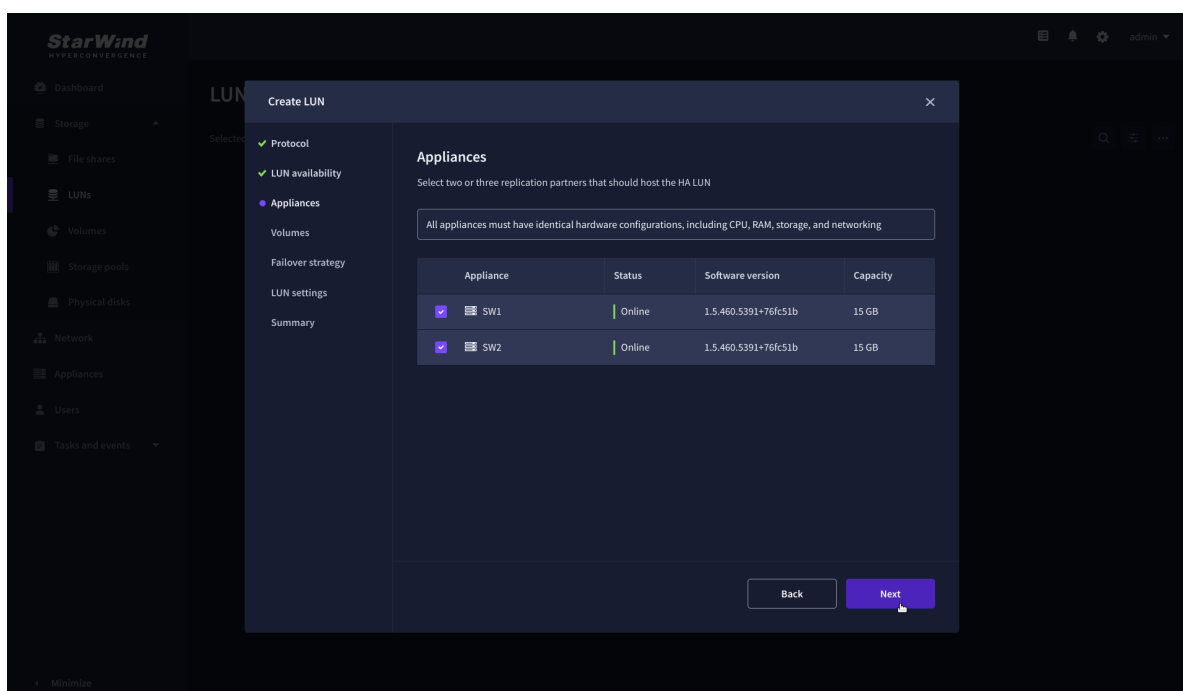
2. Select the protocol.



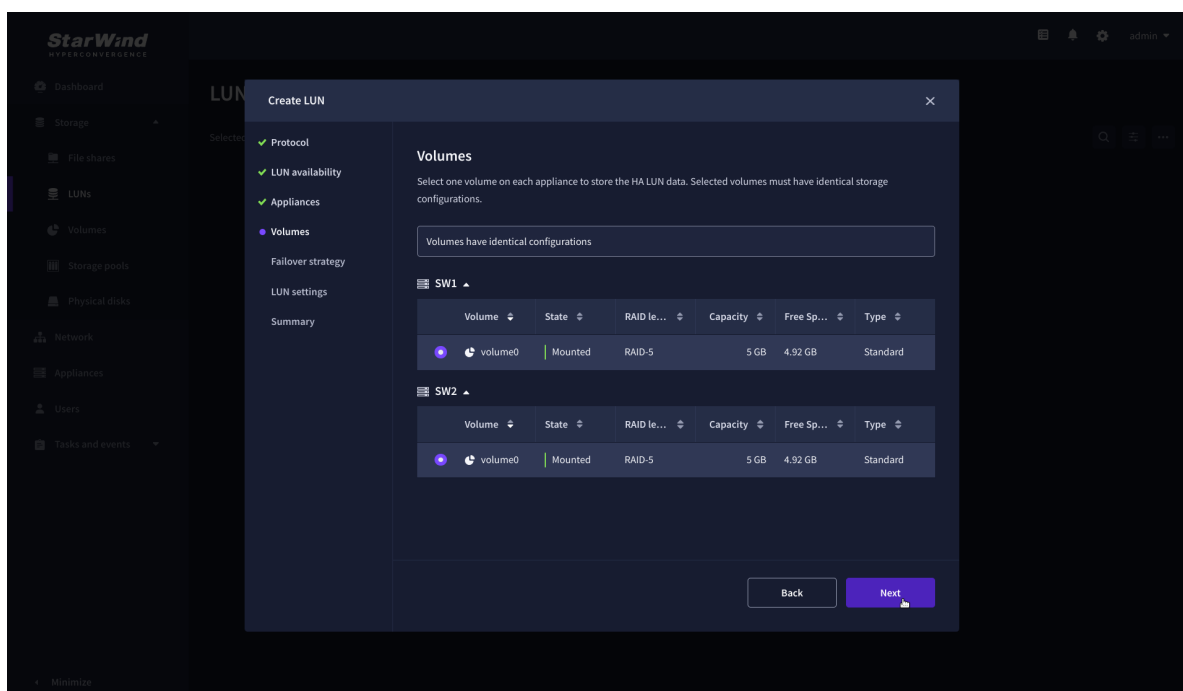
3. Choose the “High availability” LUN availability type.



4. Select the appliances that will host the LUN. Partner appliances must have identical hardware configurations, including CPU, RAM, storage, and networking.

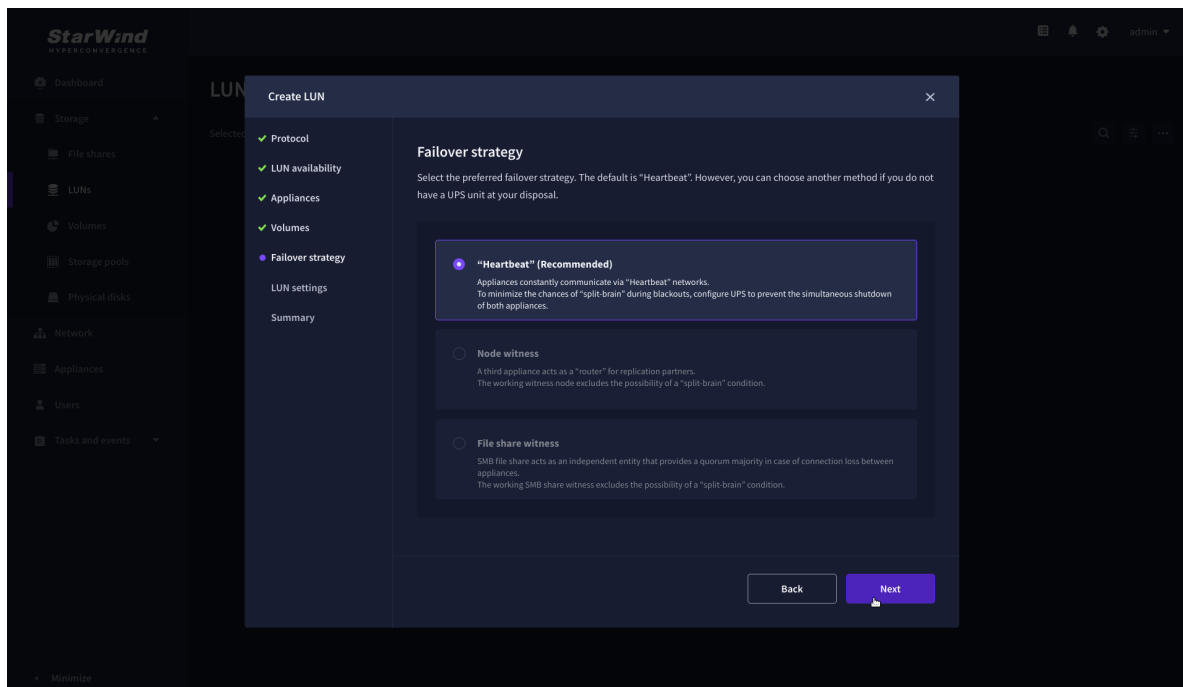


5. Select a volume to store the LUN data. Selected volumes must have identical storage configurations.

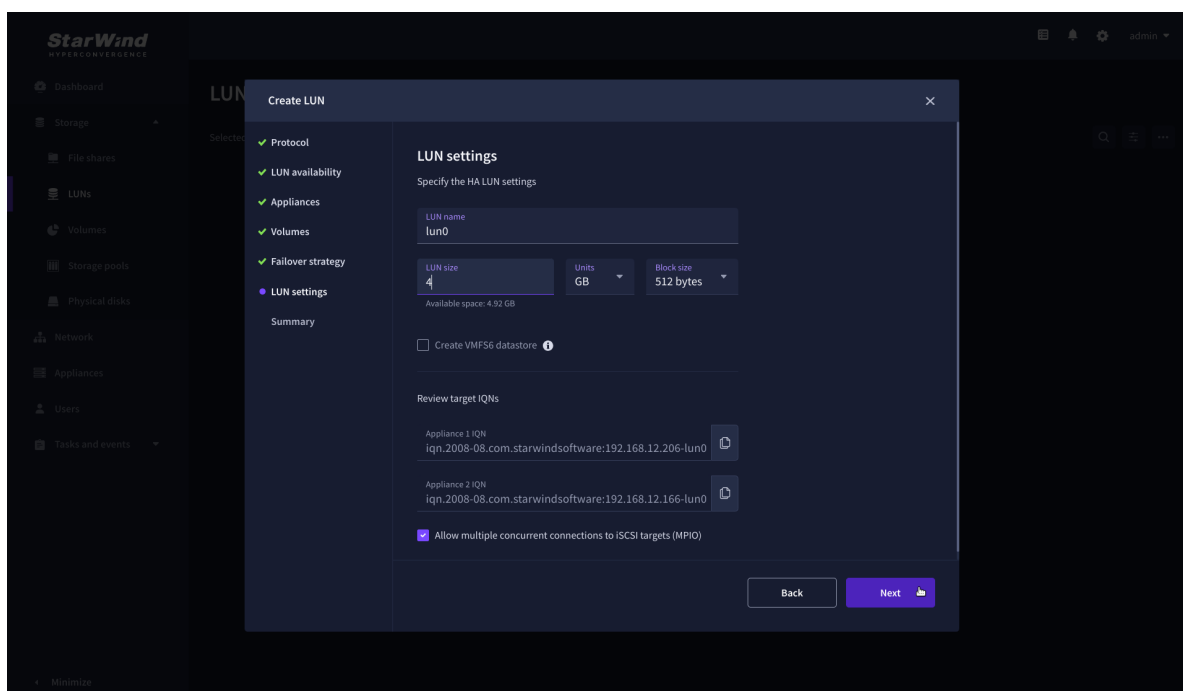


6. Select the “Heartbeat” failover strategy.

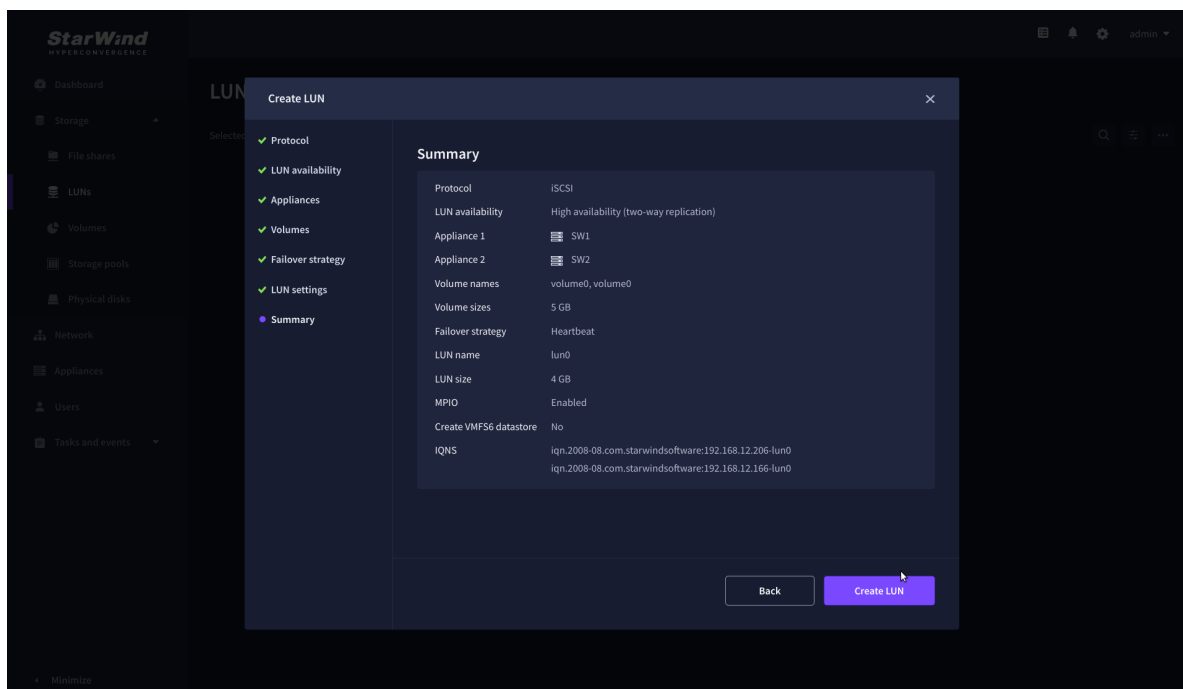
NOTE: To use the Node witness or the File share witness failover strategies, the appliances should have these features licensed.



7. Specify the HA LUN settings, e.g. name, size, and block size. Click Next.



8. Review “Summary” and click the “Create” button to create the LUN.



Connecting Starwind Virtual Disk To Hyper-V Servers

Enabling Multipath Support on Hyper-V Servers

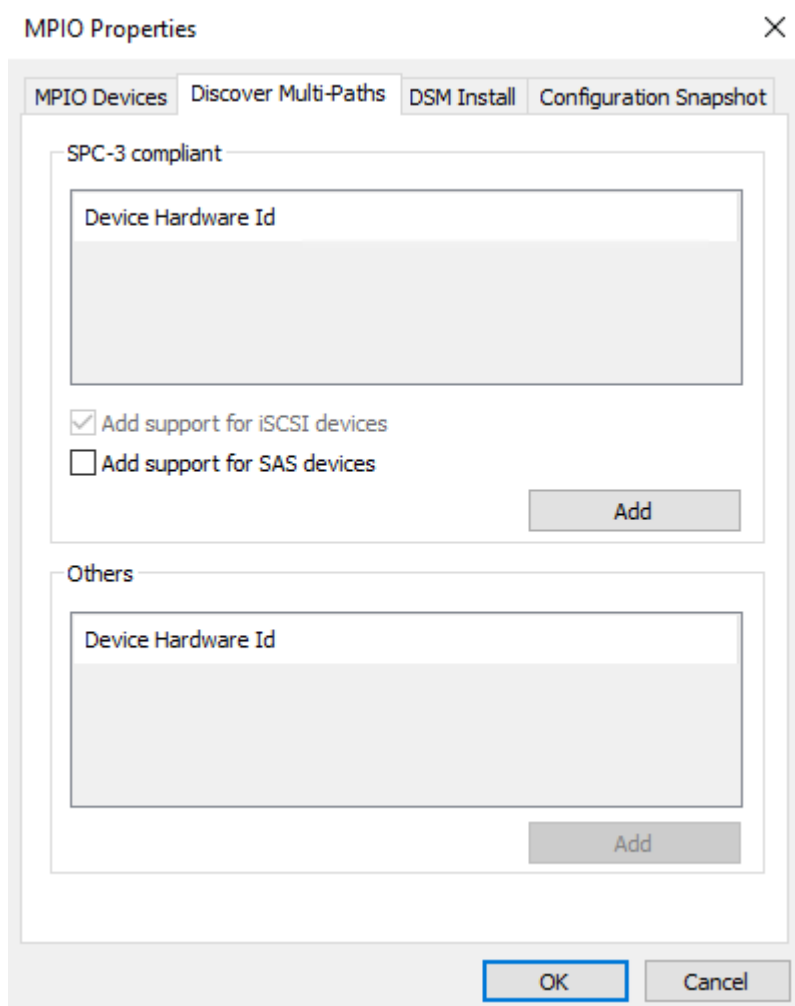
1. Install the Multipath I/O feature by executing the following command in the PowerShell window:

```
dism /online /enable-feature:MultipathIo
```

2. Open MPIO Properties by executing the following command in the CMD window:

```
mpioctl
```

3. In the Discover Multi-Paths tab, select the Add support for iSCSI devices checkbox and click Add.



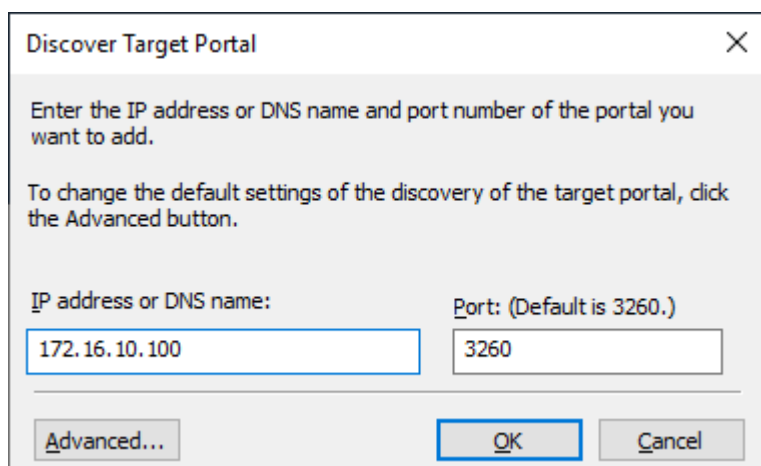
4. When prompted to restart the server, click Yes to proceed.
5. Repeat the same procedure on the other compute server that will be connected to SAN & NAS appliance.

Provisioning StarWind SAN & NAS Storage to Hyper-V Server Hosts

1. Launch Microsoft iSCSI Initiator by executing the following command in the CMD window:

```
iscsicpl
```

2. Navigate to the Discovery tab.
3. Click the Discover Portal button. The Discover Target Portal dialog appears. Type the IP address assigned to iSCSI/Data interface, i.e. 172.16.10.100.

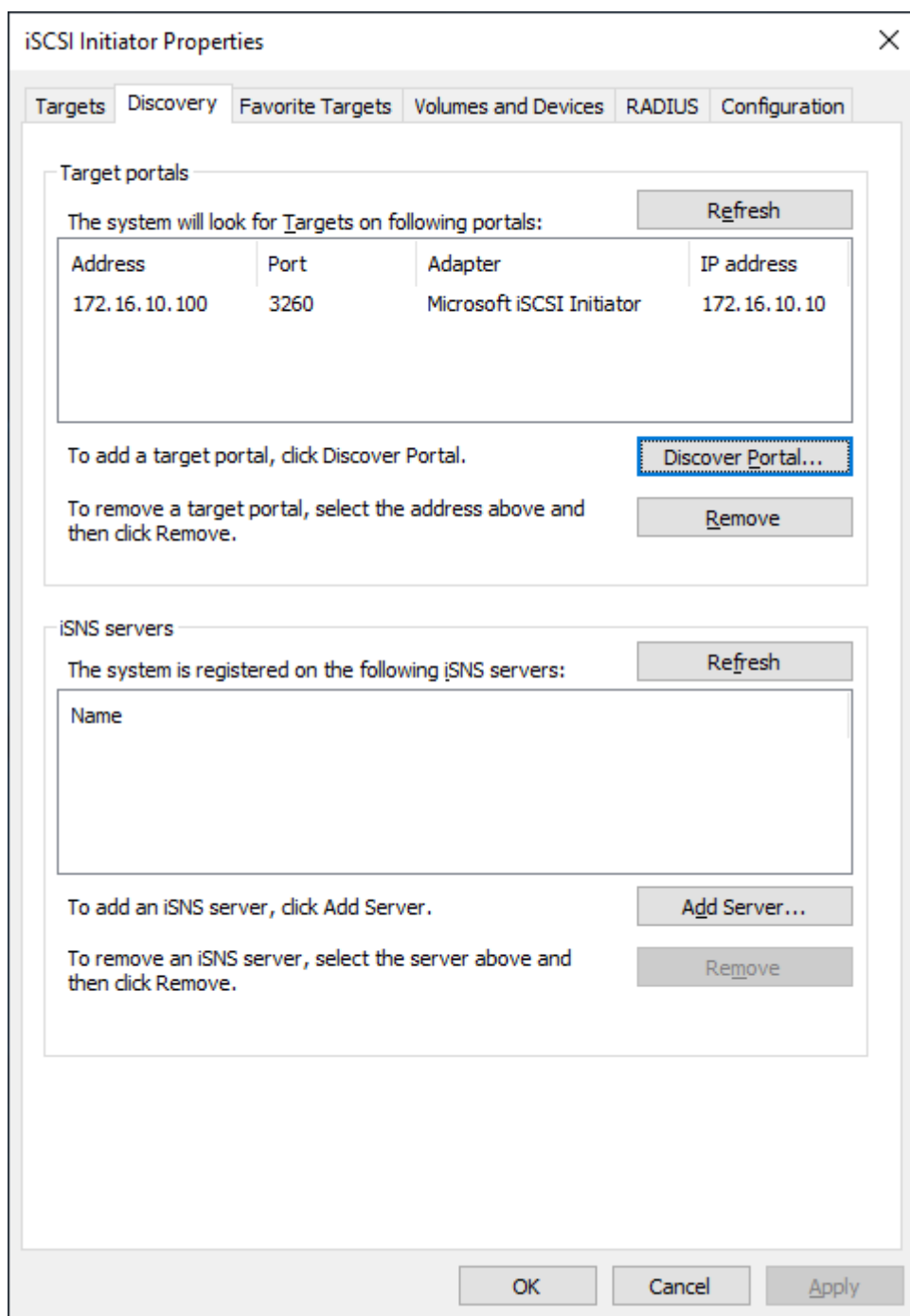


The image shows a 'Discover Target Portal' dialog box. It has a title bar with a close button (X). The main text area contains instructions: 'Enter the IP address or DNS name and port number of the portal you want to add.' and 'To change the default settings of the discovery of the target portal, click the Advanced button.' Below this, there are two input fields: 'IP address or DNS name:' with the value '172.16.10.100' and 'Port: (Default is 3260.)' with the value '3260'. At the bottom, there are three buttons: 'Advanced...', 'OK', and 'Cancel'.

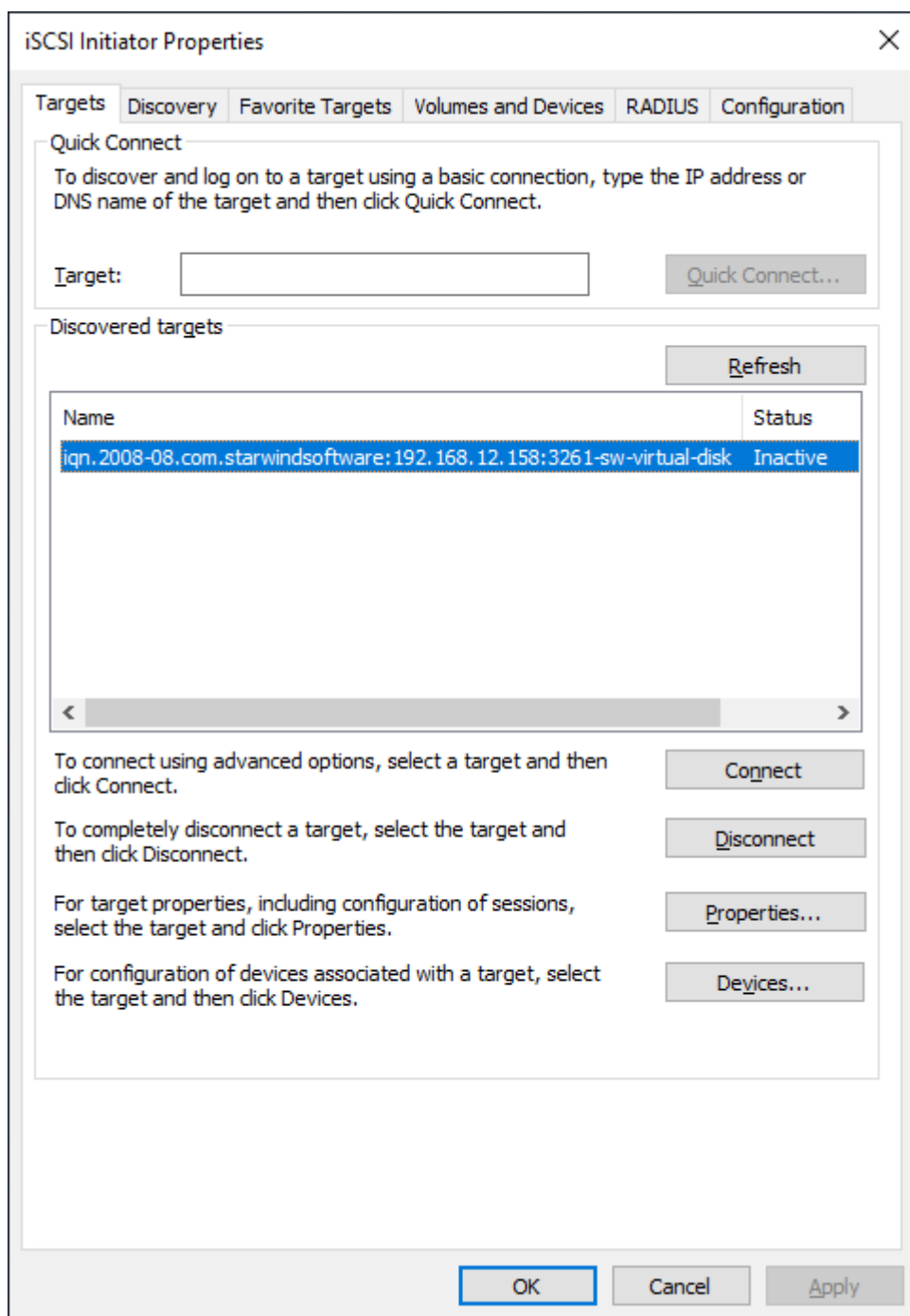
4. Click the Advanced button. Select Microsoft iSCSI Initiator as a Local adapter and as Initiator IP select the IP address of a network adapter connected to the Data\iSCSI virtual switch. Confirm the actions to complete the Target Portal discovery.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to '172.16.10.10', and 'Target portal IP' which is empty. The 'CRC / Checksum' section has two unchecked checkboxes: 'Data digest' and 'Header digest'. The 'Enable CHAP log on' checkbox is also unchecked. The 'CHAP Log on information' section contains a text box for 'Name' with the value 'iqn.1991-05.com.microsoft:ws2019' and an empty 'Target secret' text box. Below this, there are three more unchecked checkboxes: 'Perform mutual authentication', 'Use RADIUS to generate user authentication credentials', and 'Use RADIUS to authenticate target credentials'. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

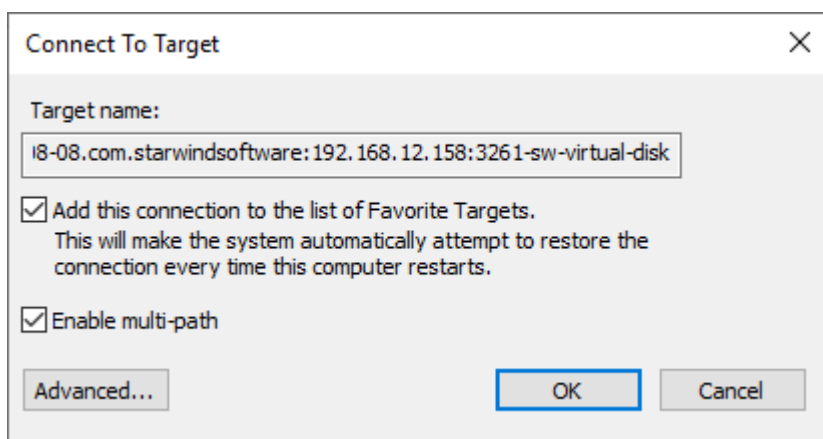
5. The target portals are added on this server.



6. Click the Targets tab. The previously created targets (virtual disks) are listed in the Discovered Targets section.



7. Select the target created in StarWind SAN & NAS web console and click Connect.
8. Enable checkboxes as shown in the image below. Click Advanced.



9. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In the Initiator IP field, select the IP address for the Data/iSCSI channel. In the Target portal IP, select the corresponding portal IP from the same subnet. Confirm the actions.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to '172.16.10.10', and 'Target portal IP' set to '172.16.10.100 / 3260'. The 'CRC / Checksum' section has two unchecked checkboxes: 'Data digest' and 'Header digest'. The 'Enable CHAP log on' checkbox is also unchecked. The 'CHAP Log on information' section contains a text box for 'Name' with the value 'iqn.1991-05.com.microsoft:ws2019' and an empty 'Target secret' text box. Below this, there are three more unchecked checkboxes: 'Perform mutual authentication', 'Use RADIUS to generate user authentication credentials', and 'Use RADIUS to authenticate target credentials'. The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

10. Repeat steps 1-9 for all remaining device targets.

11. Repeat steps 1-9 on the other compute servers, specifying corresponding Data/iSCSI channel IP addresses.

Connecting Disks to Servers

To initialize the connected iSCSI target disks and create the partitions on them use DISKPART.

1. Run diskpart in the CMD window:

List disk

Select disk X //where X is the number of the disk to be processed

Online disk

Clean

Attributes disk clear readonly

Convert GPT

Create Partition Primary

Format fs=ntfs label=X quick //where X is the name of the Volume

NOTE: It is recommended to initialize the disks as GPT.

```

Administrator: C:\Windows\system32\cmd.exe - powershell

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: HYPER-V-1

DISKPART> list disk

   Disk ###    Status         Size      Free      Dyn  Gpt
   -----    -
   Disk 0      Online            100 GB         0 B
   Disk 1      Offline           21 GB        21 GB
   Disk 2      Offline          1024 MB       1024 MB

DISKPART> select disk 1
Disk 1 is now the selected disk.

DISKPART> online disk
DiskPart successfully onlined the selected disk.

DISKPART> attributes disk clear readonly
Disk attributes cleared successfully.

DISKPART> convert GPT
DiskPart successfully converted the selected disk to GPT format.

DISKPART> Create Partition primary
DiskPart succeeded in creating the specified partition.

DISKPART> format fs=ntfs label=CSV1 quick
100 percent completed
DiskPart successfully formatted the volume.

DISKPART> _
  
```

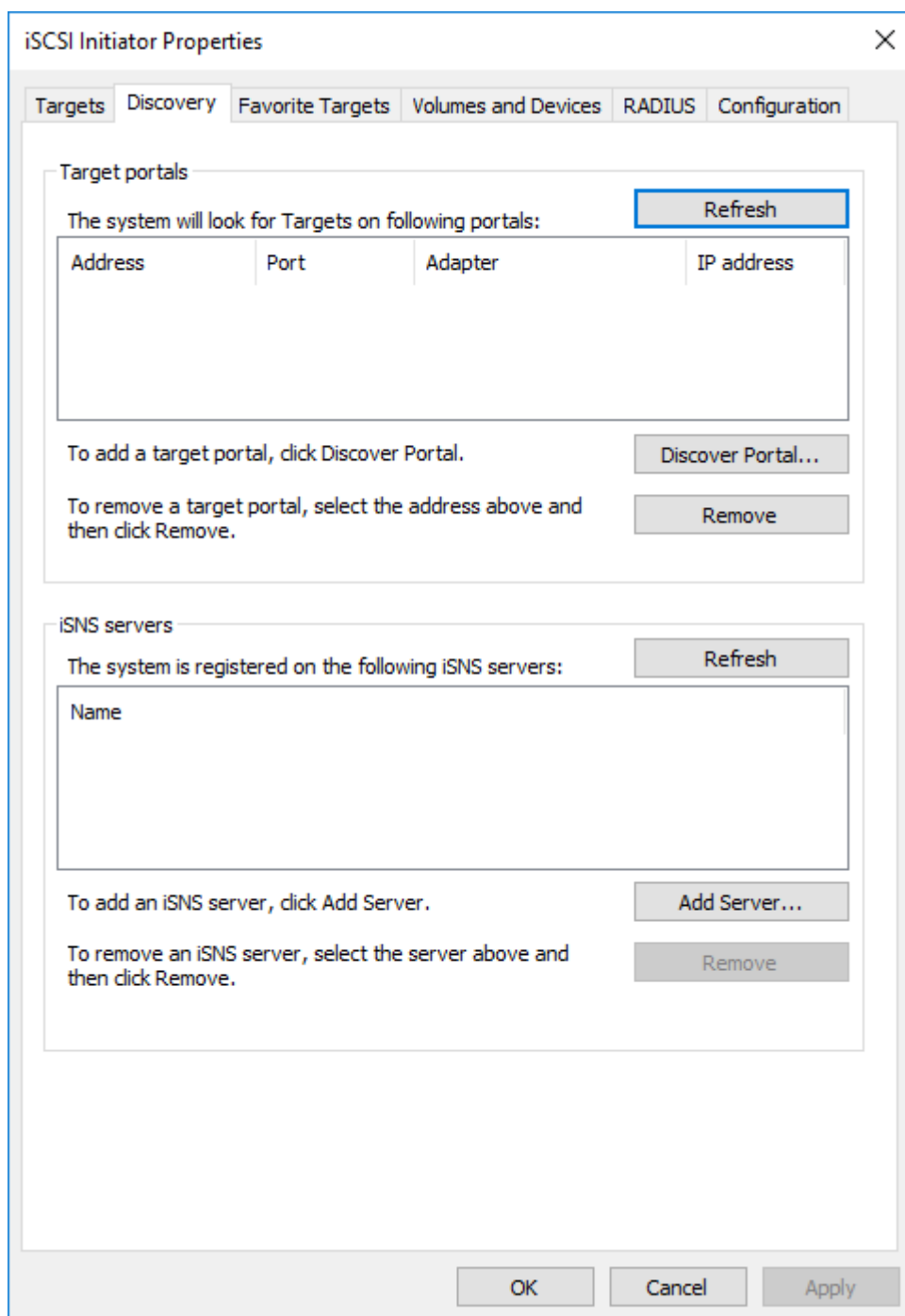
2. Perform the steps above on other compute servers.

Provisioning Starwind Ha Storage To Windows Server Hosts

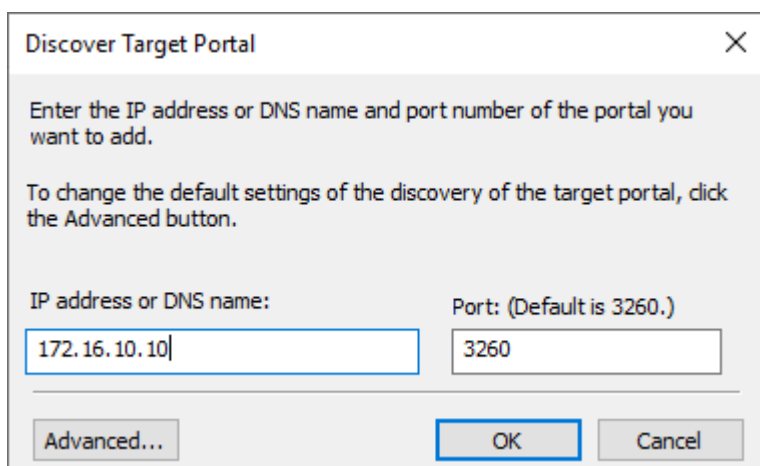
1. Launch Microsoft iSCSI Initiator: Start -> Windows Administrative Tools -> iSCSI Initiator. Alternatively, launch it using the command below in the command line interface:

```
iscsicpl
```

2. Navigate to the Discovery tab.



3. Click the Discover Portal button. The Discover Target Portal dialog appears. Type 172.16.10.10.



The image shows a 'Discover Target Portal' dialog box. It has a title bar with a close button (X). The main text area contains instructions: 'Enter the IP address or DNS name and port number of the portal you want to add.' and 'To change the default settings of the discovery of the target portal, click the Advanced button.' Below this, there are two input fields: 'IP address or DNS name:' with the value '172.16.10.10' and 'Port: (Default is 3260.)' with the value '3260'. At the bottom, there are three buttons: 'Advanced...', 'OK', and 'Cancel'.

4. Click the Advanced button. Select Microsoft iSCSI Initiator as a Local adapter and select Initiator IP. Confirm the actions to complete the Target Portal discovery.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to '172.16.10.1', and 'Target portal IP' which is empty. The 'CRC / Checksum' section has two unchecked checkboxes: 'Data digest' and 'Header digest'. Below this is an unchecked checkbox for 'Enable CHAP log on'. The 'CHAP Log on information' section contains a text box for 'Name' with the value 'iqn.1991-05.com.microsoft:sw01' and an empty text box for 'Target secret'. At the bottom of this section are three unchecked checkboxes: 'Perform mutual authentication', 'Use RADIUS to generate user authentication credentials', and 'Use RADIUS to authenticate target credentials'. The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

5. Click the Discover Portal... button once again.

6. In Discover Target Portal dialog, type in the iSCSI interface IP address of the partner node that will be used to connect the StarWind provisioned targets. Click Advanced.

Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name:

Port: (Default is 3260.)

172.16.10.20

3260

Advanced...

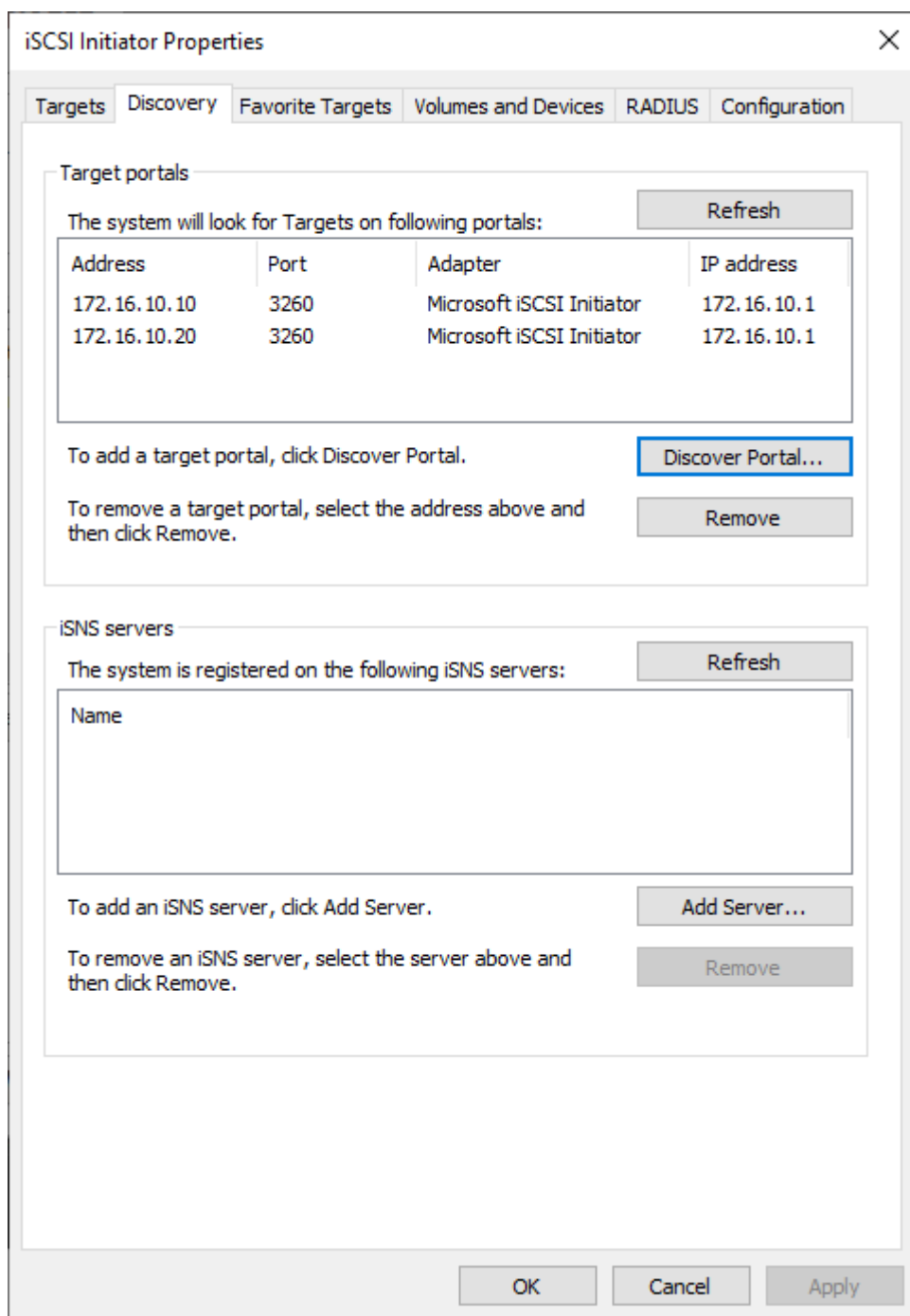
OK

Cancel

7. Select Microsoft iSCSI Initiator as the Local adapter, select the Initiator IP in the same subnet as the IP address of the partner server from the previous step. Confirm the actions to complete the Target Portal discovery.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'General' tab is also visible. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to '172.16.10.1', and 'Target portal IP' is empty. The 'CRC / Checksum' section has two checkboxes: 'Data digest' and 'Header digest', both unchecked. The 'Enable CHAP log on' checkbox is also unchecked. The 'CHAP Log on information' section contains a text box for 'Name' with the value 'iqn.1991-05.com.microsoft:sw01' and an empty 'Target secret' text box. Below this, there are three more checkboxes: 'Perform mutual authentication' (unchecked), 'Use RADIUS to generate user authentication credentials' (unchecked), and 'Use RADIUS to authenticate target credentials' (unchecked). At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

8. Now, all the target portals are added on the first node.



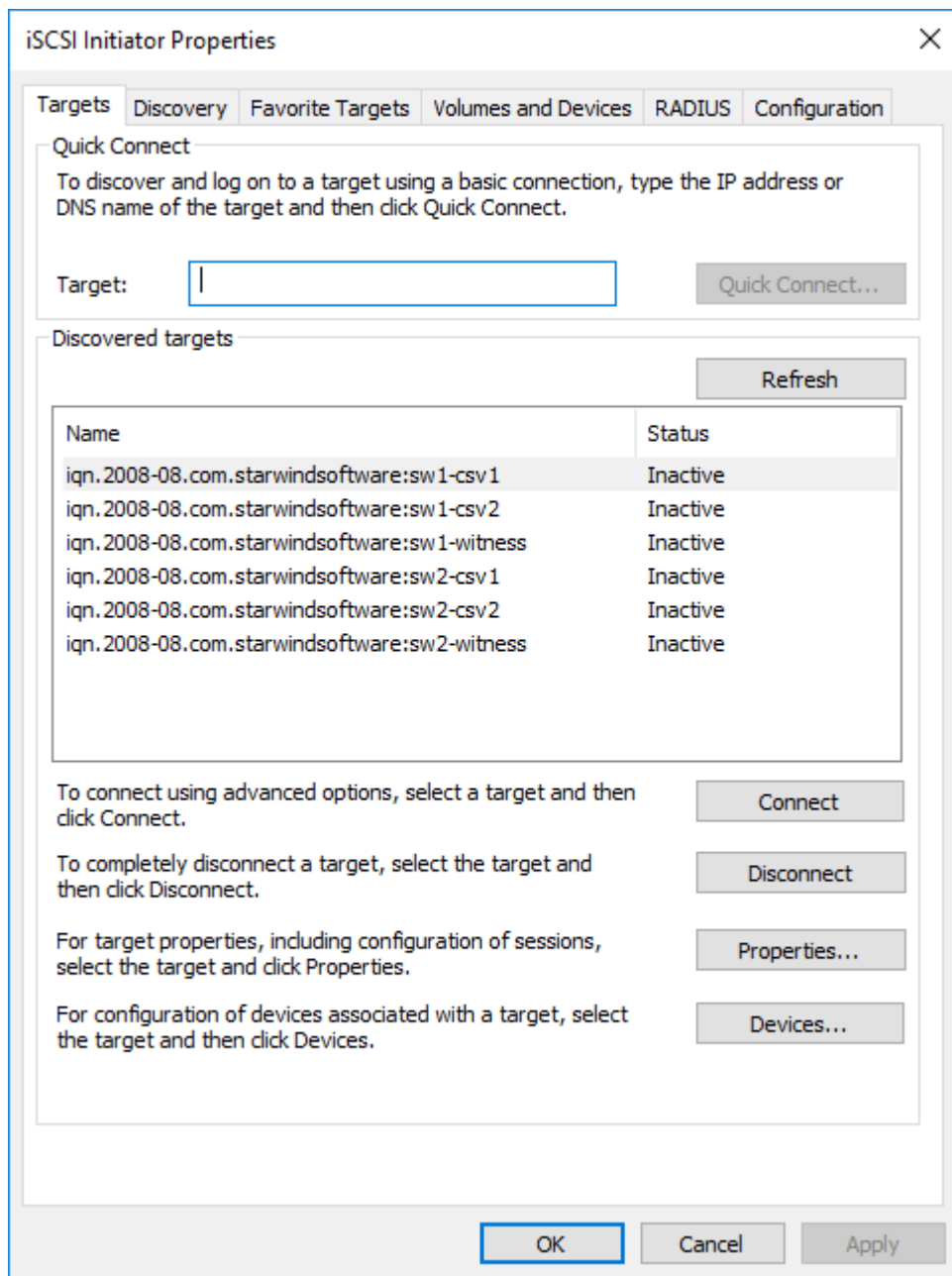
9. Repeat the steps 1-8 on the partner node.

Connecting Targets

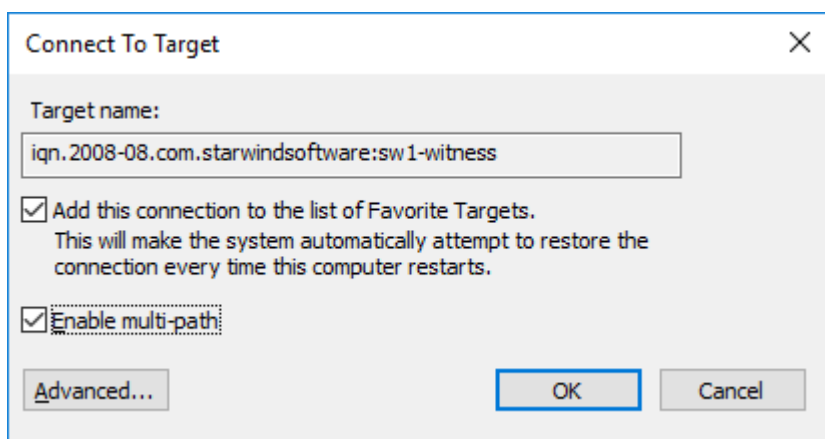
1. Click the Targets tab. The previously created targets are listed in the Discovered Targets section.

NOTE: If the created targets are not listed, check the firewall settings of the StarWind Server as well as the list of networks served by the StarWind Server (go to StarWind

Management Console -> Configuration -> Network). Alternatively, check the Access Rights tab on the corresponding StarWind VSAN server in StarWind Management Console for any restrictions.



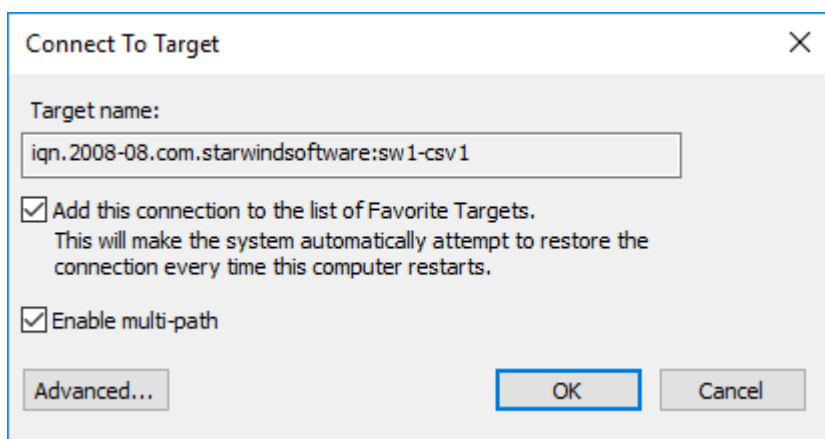
2. Select the Witness target from the local server and click Connect.
3. Enable checkboxes as shown in the image below. Click Advanced.



4. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In the Initiator IP field, select the IP address for the iSCSI channel. In the Target portal IP, select the corresponding portal IP from the same subnet. Confirm the actions.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to '172.16.10.1', and 'Target portal IP' set to '172.16.10.10 / 3260'. The 'CRC / Checksum' section has two unchecked checkboxes: 'Data digest' and 'Header digest'. The 'Enable CHAP log on' checkbox is also unchecked. The 'CHAP Log on information' section contains a text box for 'Name' with the value 'iqn.1991-05.com.microsoft:sw01' and an empty text box for 'Target secret'. Below this, there are three more unchecked checkboxes: 'Perform mutual authentication', 'Use RADIUS to generate user authentication credentials', and 'Use RADIUS to authenticate target credentials'. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

5. Repeat the steps 2-4 to connect to partner node.
6. Select the CSV1 target discovered from the local server and click Connect.
7. Enable checkboxes as shown in the image below. Click Advanced.



8. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Target portal IP, select 172.16.10.10. Confirm the actions.

9. Select the partner target from the other StarWind node and click Connect.

10. Repeat the step 6.

11. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In the Initiator IP field, select the IP address for the iSCSI channel. In the Target portal IP, select the corresponding portal IP from the same subnet. Confirm the actions.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to '172.16.10.1', and 'Target portal IP' set to '172.16.10.20 / 3260'. The 'CRC / Checksum' section has two unchecked checkboxes: 'Data digest' and 'Header digest'. The 'Enable CHAP log on' checkbox is also unchecked. The 'CHAP Log on information' section contains a text box for 'Name' with the value 'iqn.1991-05.com.microsoft:sw01' and an empty 'Target secret' text box. Below this, there are three more unchecked checkboxes: 'Perform mutual authentication', 'Use RADIUS to generate user authentication credentials', and 'Use RADIUS to authenticate target credentials'. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

11. Repeat the steps 1-10 for all remaining HA device targets.

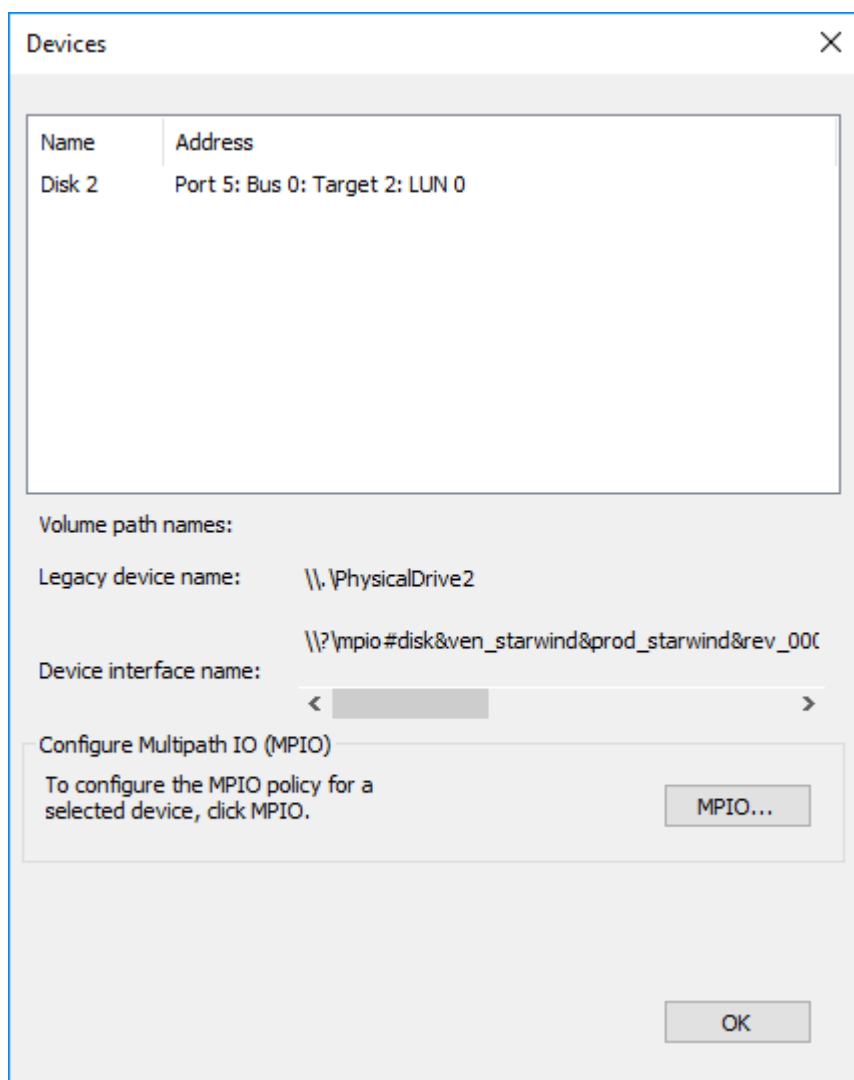
12. Repeat the steps 1-11 on the other StarWind node, specifying corresponding data channel IP addresses.

Configuring Multipath

NOTE: It is recommended to configure the different MPIO policies depending on iSCSI channel throughput. For 1 Gbps iSCSI channel throughput, it is recommended to set Failover Only or Least Queue Depth MPIO load balancing policy. For 10 Gbps iSCSI channel throughput, it is recommended to set Round Robin or Least Queue Depth MPIO

load balancing policy.

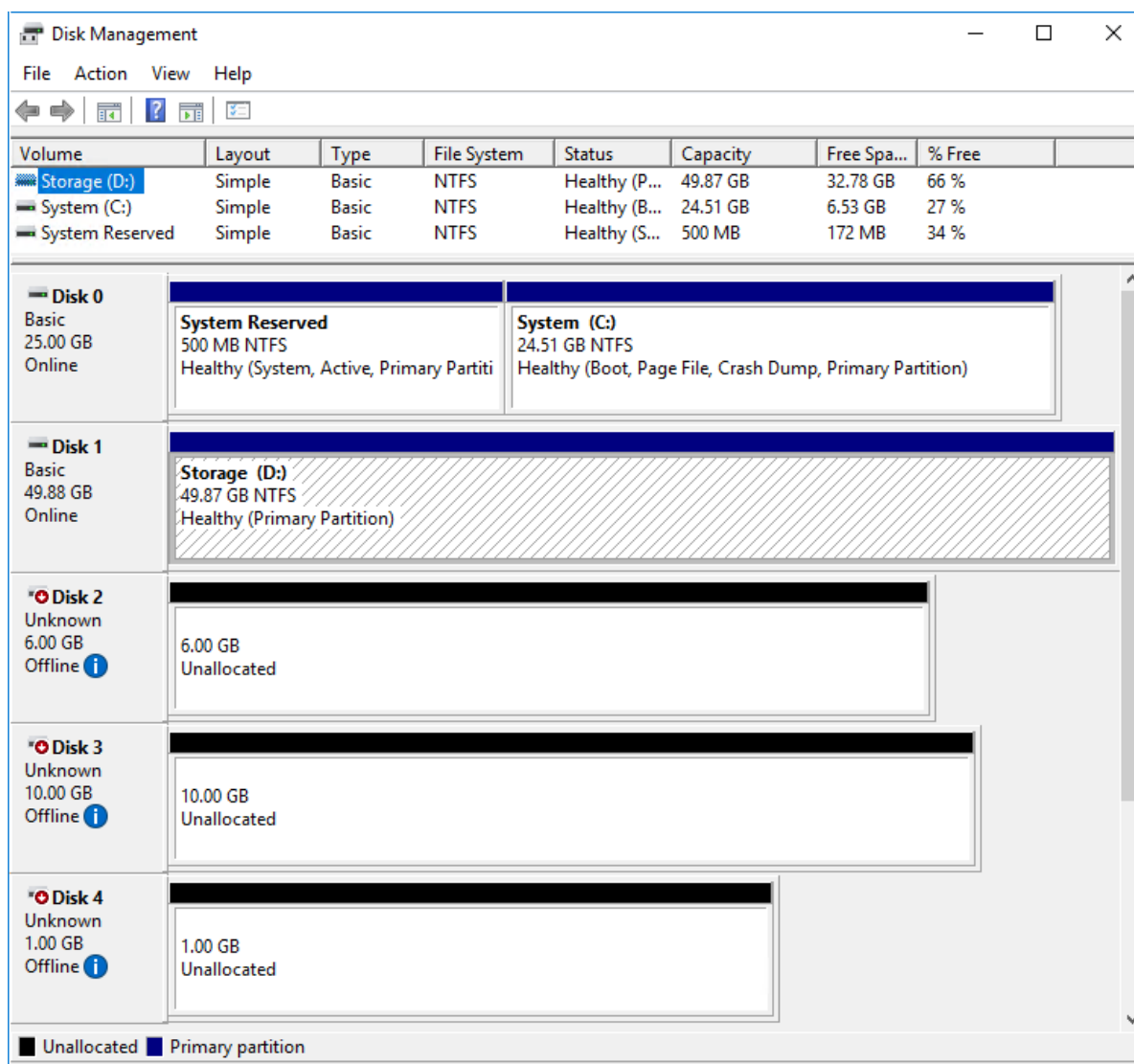
1. Configure the MPIO policy for each target with the load balance policy of choice. Select the Target located on the local server and click Devices.
2. In the Devices dialog, click MPIO.



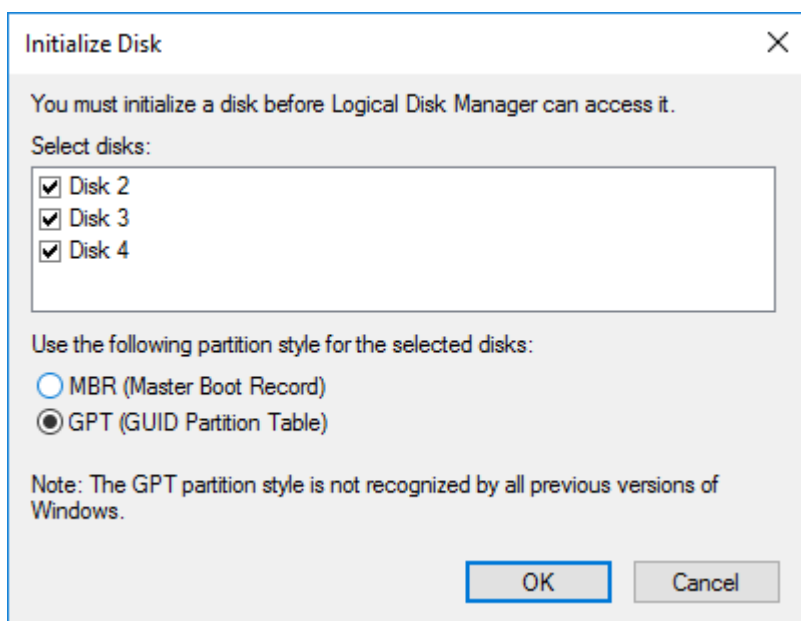
3. Select the appropriate load balancing policy.
4. Repeat the steps 1-3 for configuring the MPIO policy for each remaining device on the current node and on the partner node.

Connecting Disks to Servers

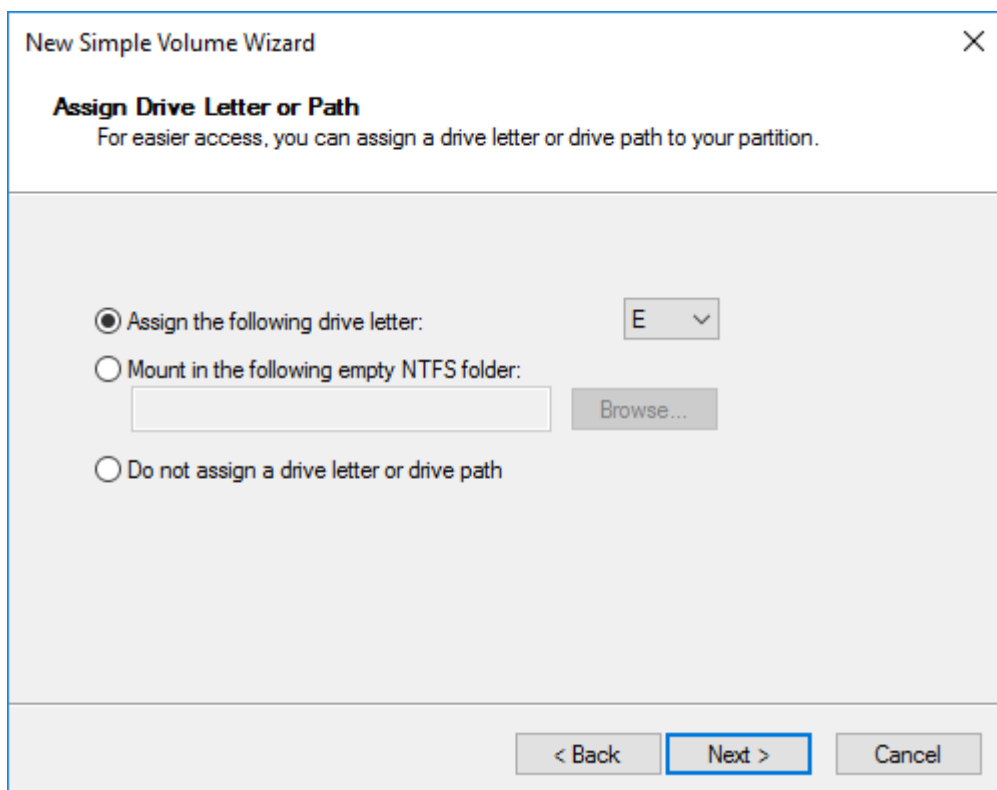
1. Open the Disk Management snap-in. The StarWind disks will appear as unallocated and offline.



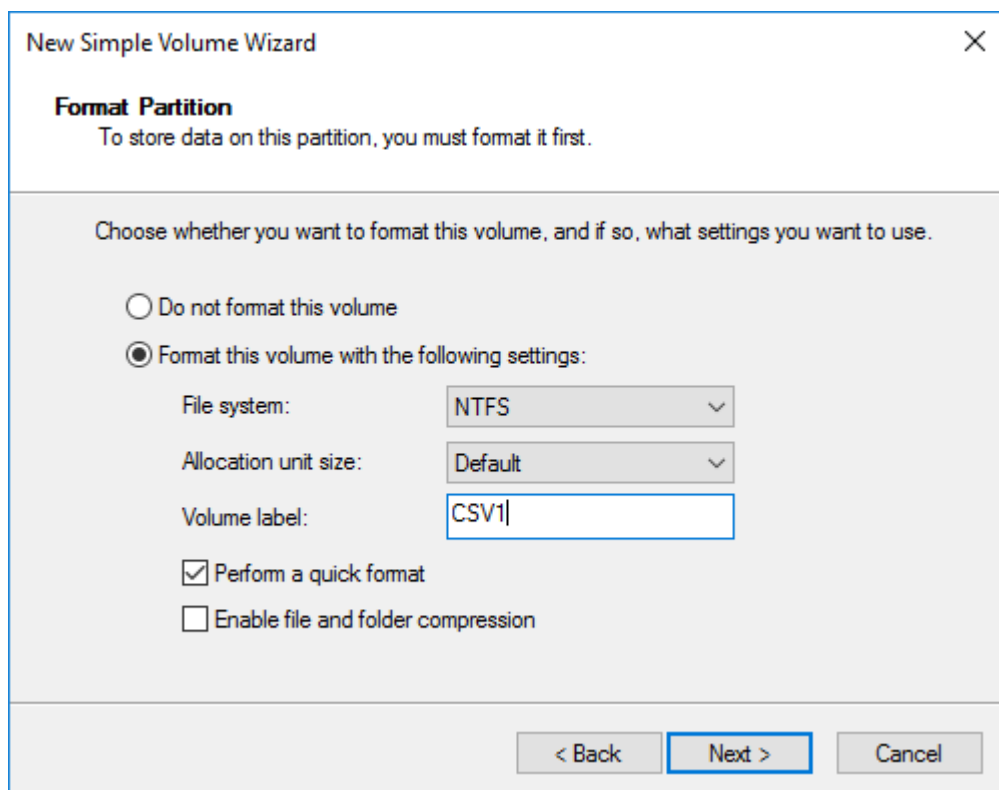
2. Bring the disks online by right-clicking on them and selecting the Online menu option.
3. Select the CSV disk (check the disk size to be sure) and right-click on it to initialize.
4. By default, the system will offer to initialize all non-initialized disks. Use the Select Disks area to choose the disks. Select GPT (GUID Partition Style) for the partition style to be applied to the disks. Press OK to confirm.



5. Right-click on the selected disk and choose New Simple Volume.
6. In New Simple Volume Wizard, indicate the volume size. Click Next.
7. Assign a drive letter to the disk. Click Next.



8. Select NTFS in the File System dropdown menu. Keep Allocation unit size as Default. Set the Volume Label of choice. Click Next.



New Simple Volume Wizard [X]

Format Partition
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS [v]

Allocation unit size: Default [v]

Volume label: CSV1 []

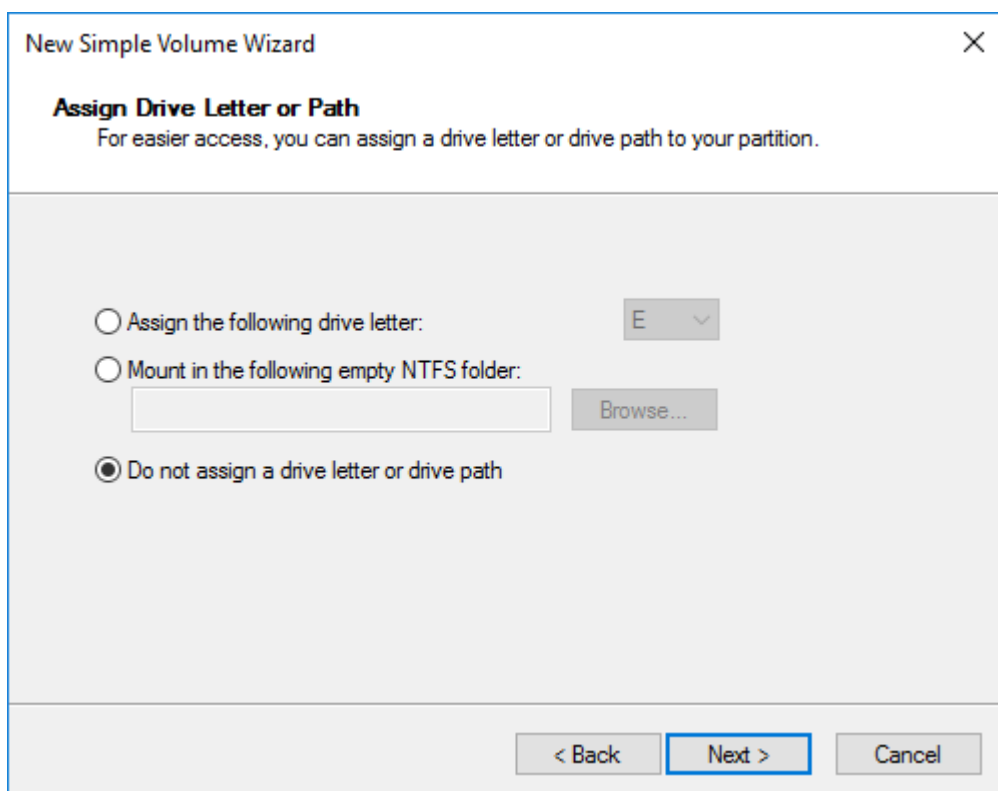
☒ Perform a quick format

☐ Enable file and folder compression

< Back **Next >** Cancel

9. Press Finish to complete.

10. Complete the steps 1-9 for the Witness disk. Do not assign any drive letter or drive path for it.



11. On the partner node, open the Disk Management snap-in. All StarWind disks will appear offline. If the status is different from the one shown below, click Action->Refresh in the top menu to update the information about the disks.

12. Repeat step 2 to bring all the remaining StarWind disks online.

Creating A Failover Cluster In Windows Server

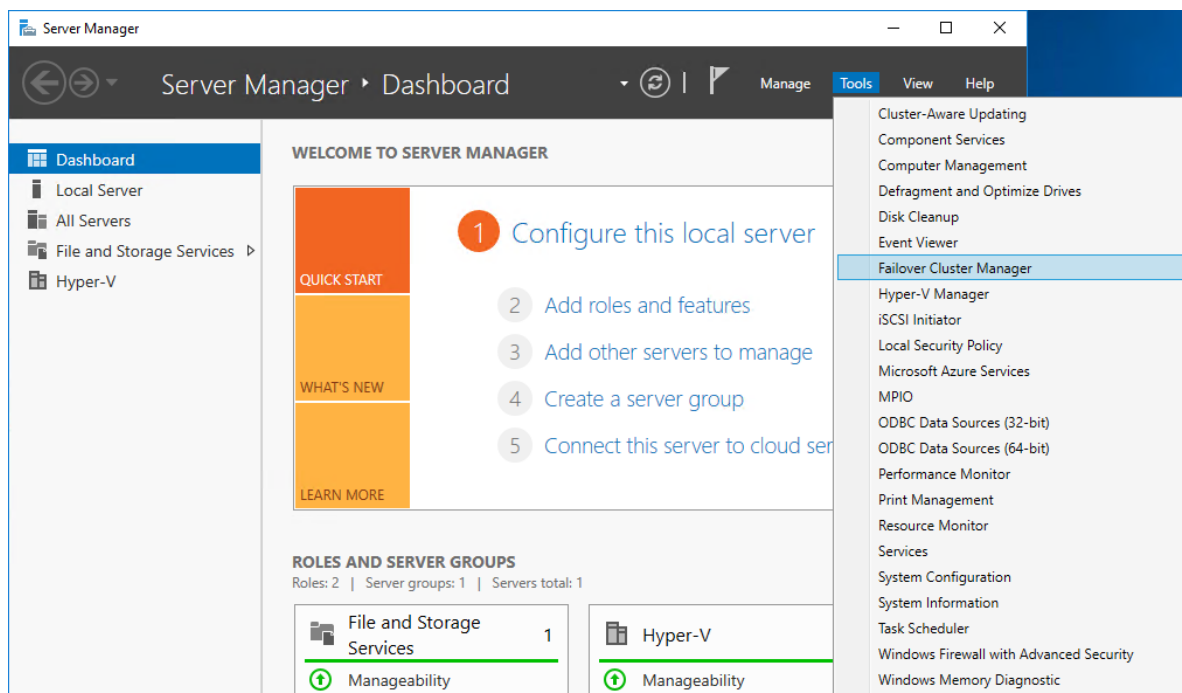
NOTE: To avoid issues during the cluster validation configuration, it is recommended to install the latest Microsoft updates on each node.

NOTE: Server Manager can be opened on the server with desktop experience enabled (necessary features should be installed). Alternatively, the Failover cluster can be managed with Remote Server Administration Tools:

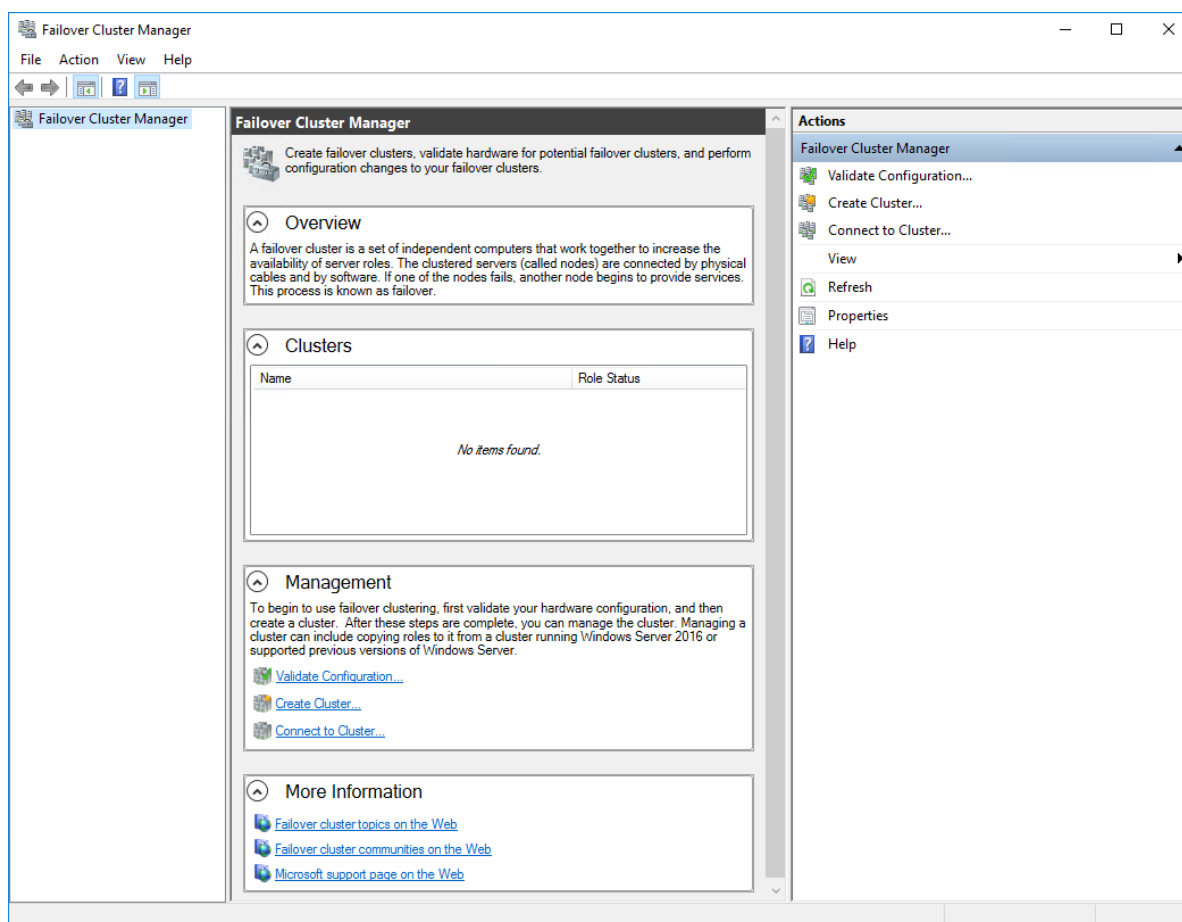
<https://docs.microsoft.com/en-us/windows-server/remote/remote-server-administration-tools>

NOTE: For converged deployment (SAN & NAS running as a dedicated storage cluster) the Microsoft Failover Cluster is deployed on separate computing nodes. Additionally, for the converged deployment scenario, the storage nodes that host StarWind SAN & NAS as CVM or bare metal do not require a domain controller and Failover Cluster to operate.

1. Open Server Manager. Select the Failover Cluster Manager item from the Tools menu.



2. Click the Create Cluster link in the Actions section of Failover Cluster Manager.



3. Specify the servers to be added to the cluster. Click Next to continue.

Create Cluster Wizard

Select Servers

Before You Begin
Select Servers
 Validation Warning
 Access Point for Administering the Cluster
 Confirmation
 Creating New Cluster
 Summary

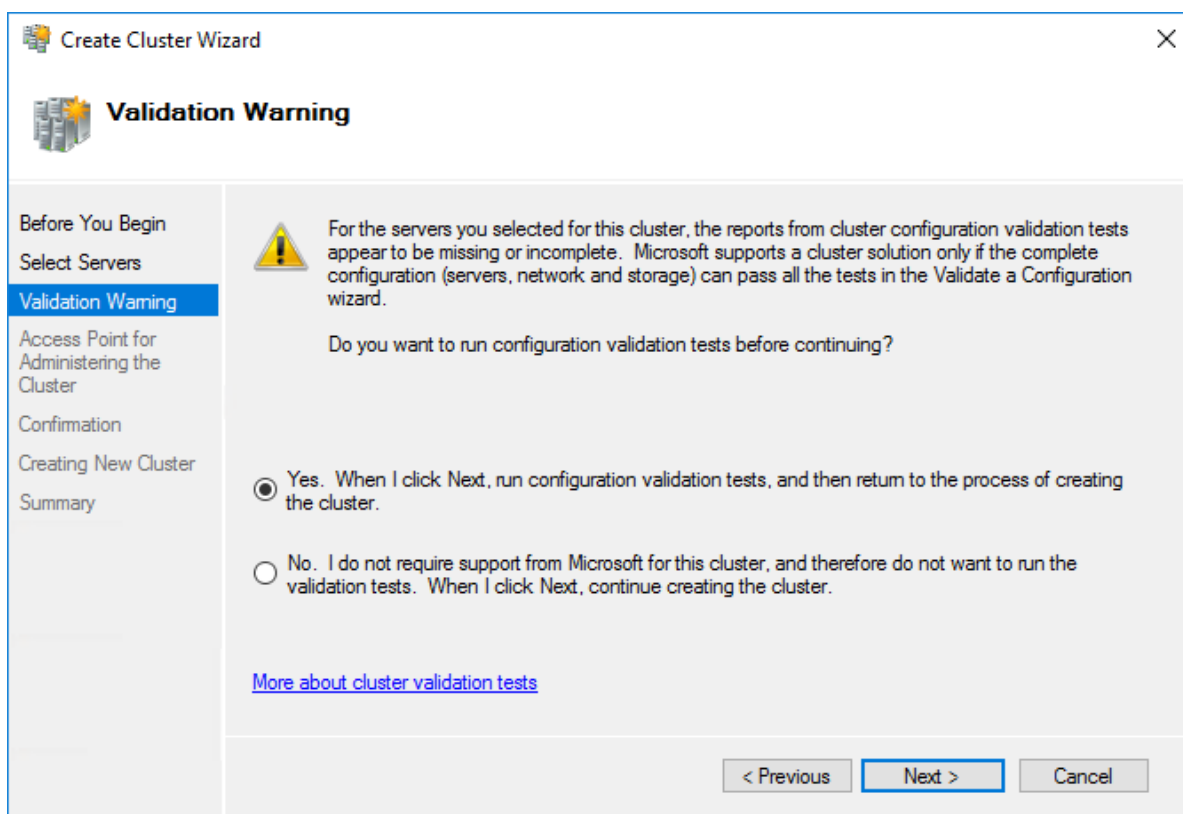
Add the names of all the servers that you want to have in the cluster. You must add at least one server.

Enter server name:

Selected servers:

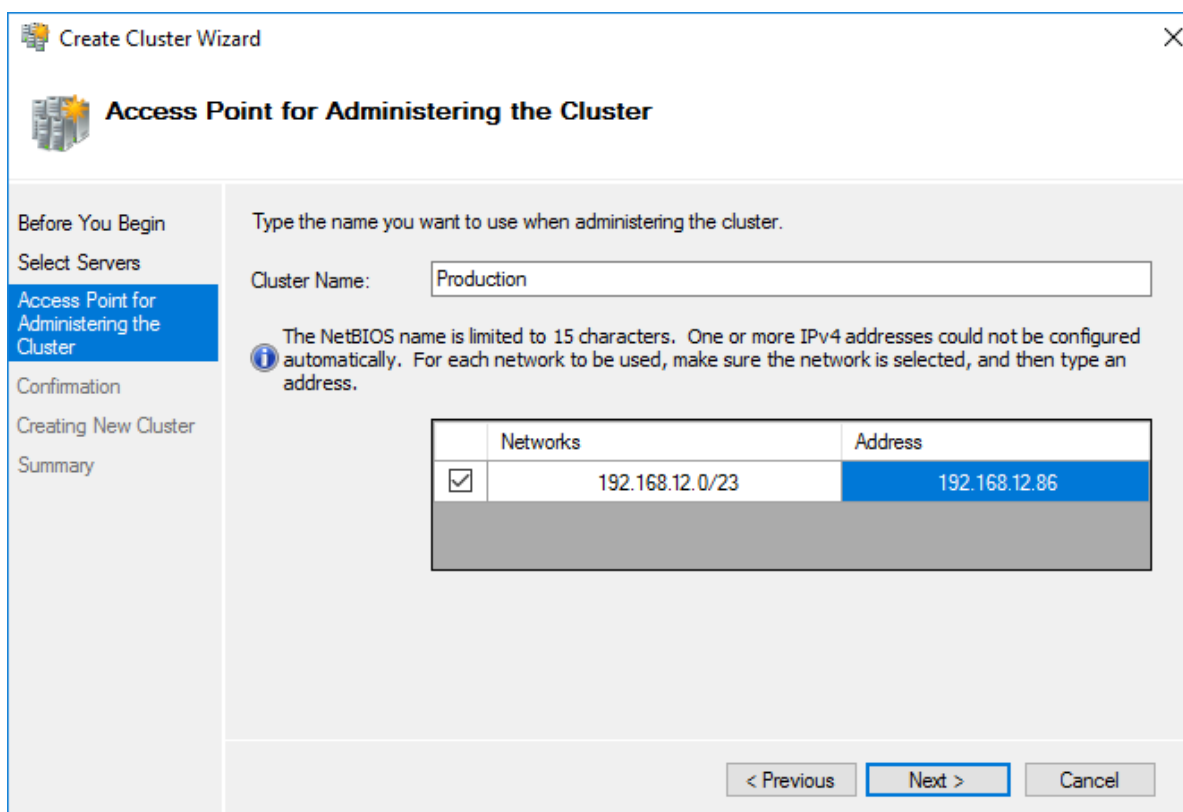
- SW1.starwind.local
- SW2.starwind.local

4. Validate the configuration by running the cluster validation tests: select Yes... and click Next to continue.



5. Specify the cluster name.

NOTE: If the cluster servers get IP addresses over DHCP, the cluster also gets its IP address over DHCP. If the IP addresses are set statically, set the cluster IP address manually.



Create Cluster Wizard

Access Point for Administering the Cluster

Before You Begin
Select Servers
Access Point for Administering the Cluster
Confirmation
Creating New Cluster
Summary

Type the name you want to use when administering the cluster.

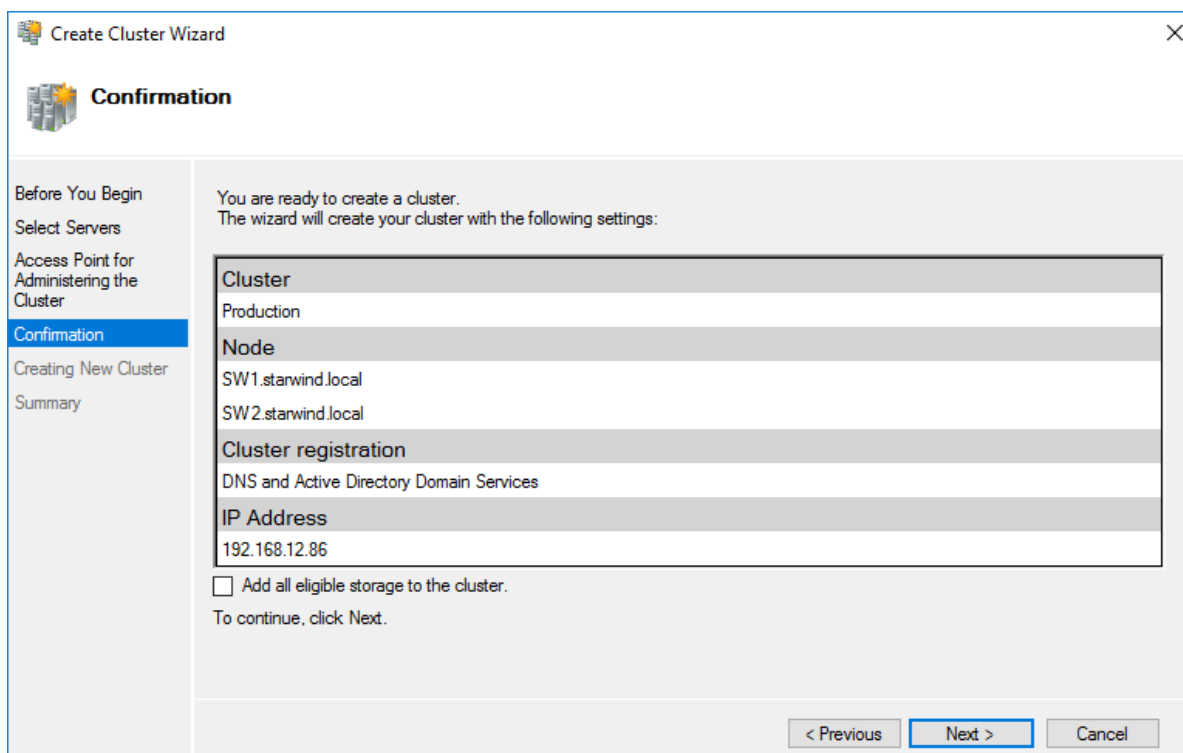
Cluster Name:

i The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

	Networks	Address
<input checked="" type="checkbox"/>	192.168.12.0/23	192.168.12.86

< Previous **Next >** Cancel

6. Make sure that all settings are correct. Click Previous to make any changes or Next to proceed.



Create Cluster Wizard

Confirmation

Before You Begin
Select Servers
Access Point for Administering the Cluster
Confirmation
Creating New Cluster
Summary

You are ready to create a cluster.
The wizard will create your cluster with the following settings:

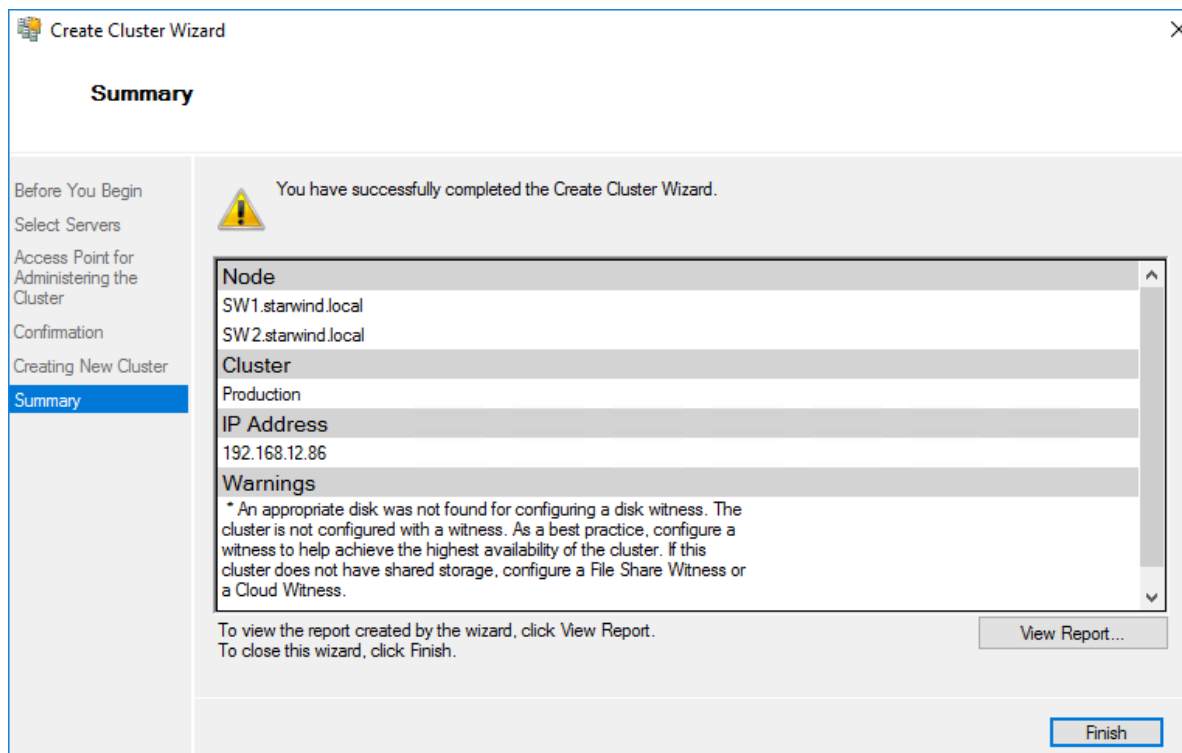
Cluster	Production
Node	SW1.starwind.local SW2.starwind.local
Cluster registration	DNS and Active Directory Domain Services
IP Address	192.168.12.86

☐ Add all eligible storage to the cluster.
To continue, click Next.

< Previous **Next >** Cancel

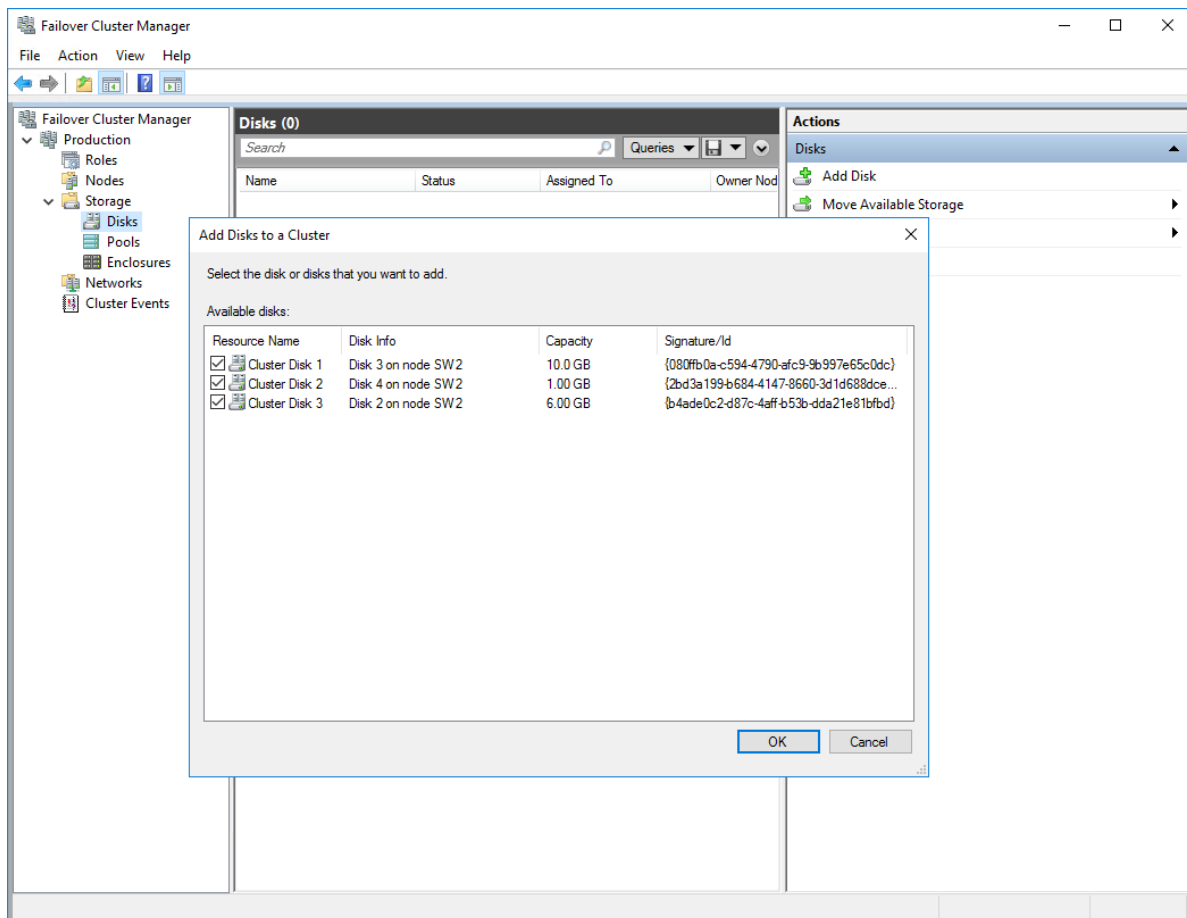
NOTE: If checkbox Add all eligible storage to the cluster is selected, the wizard will add all disks to the cluster automatically. The device with the smallest storage volume will be assigned as a Witness. It is recommended to uncheck this option before clicking Next and add cluster disks and the Witness drive manually.

7. The process of the cluster creation starts. Upon the completion, the system displays the summary with the detailed information. Click Finish to close the wizard.

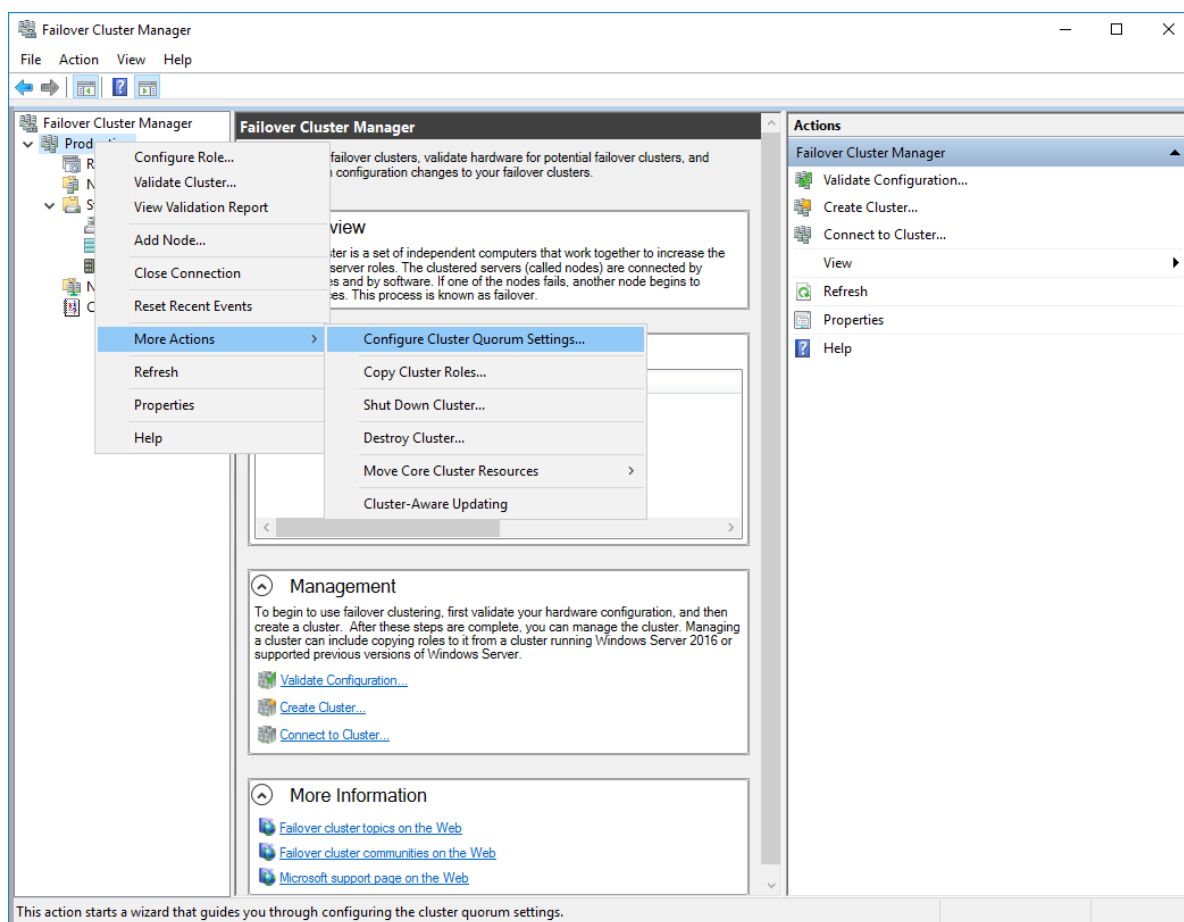


Adding Storage to the Cluster

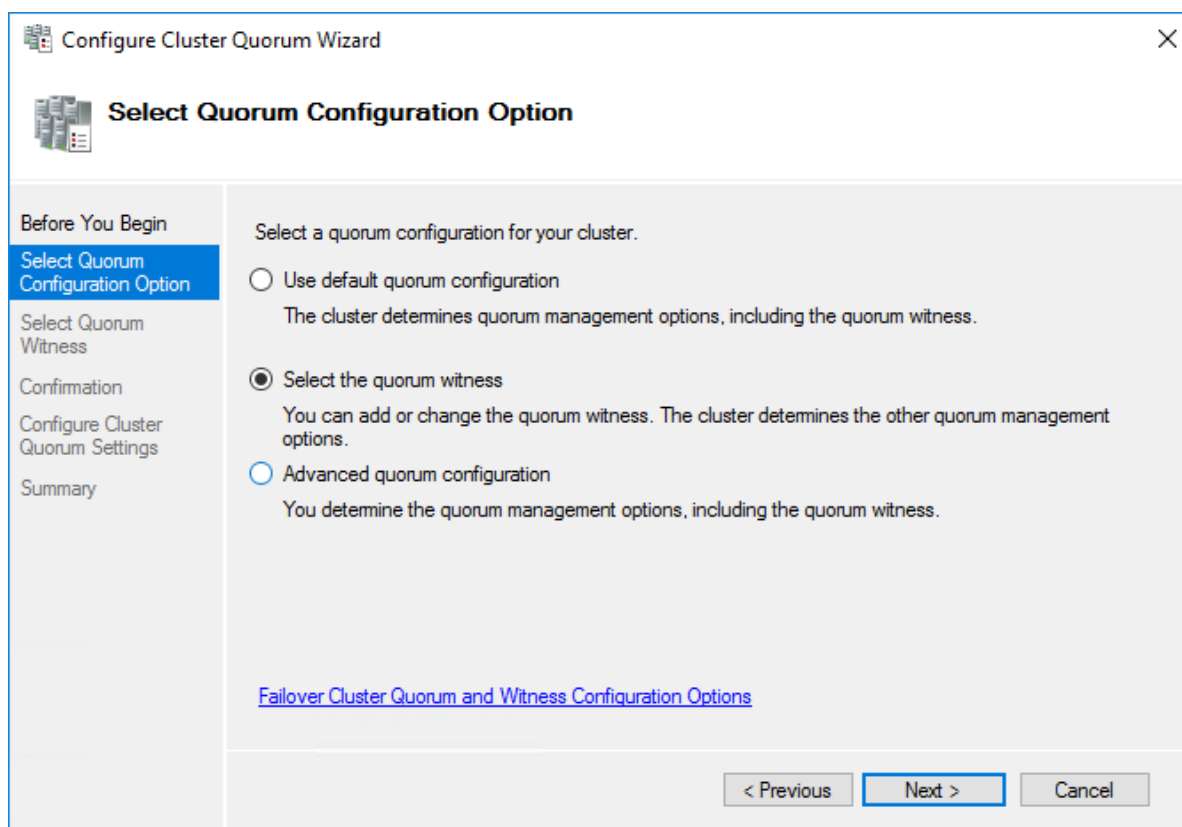
1. In Failover Cluster Manager, navigate to Cluster -> Storage -> Disks. Click Add Disk in the Actions panel, choose StarWind disks from the list and confirm the selection.



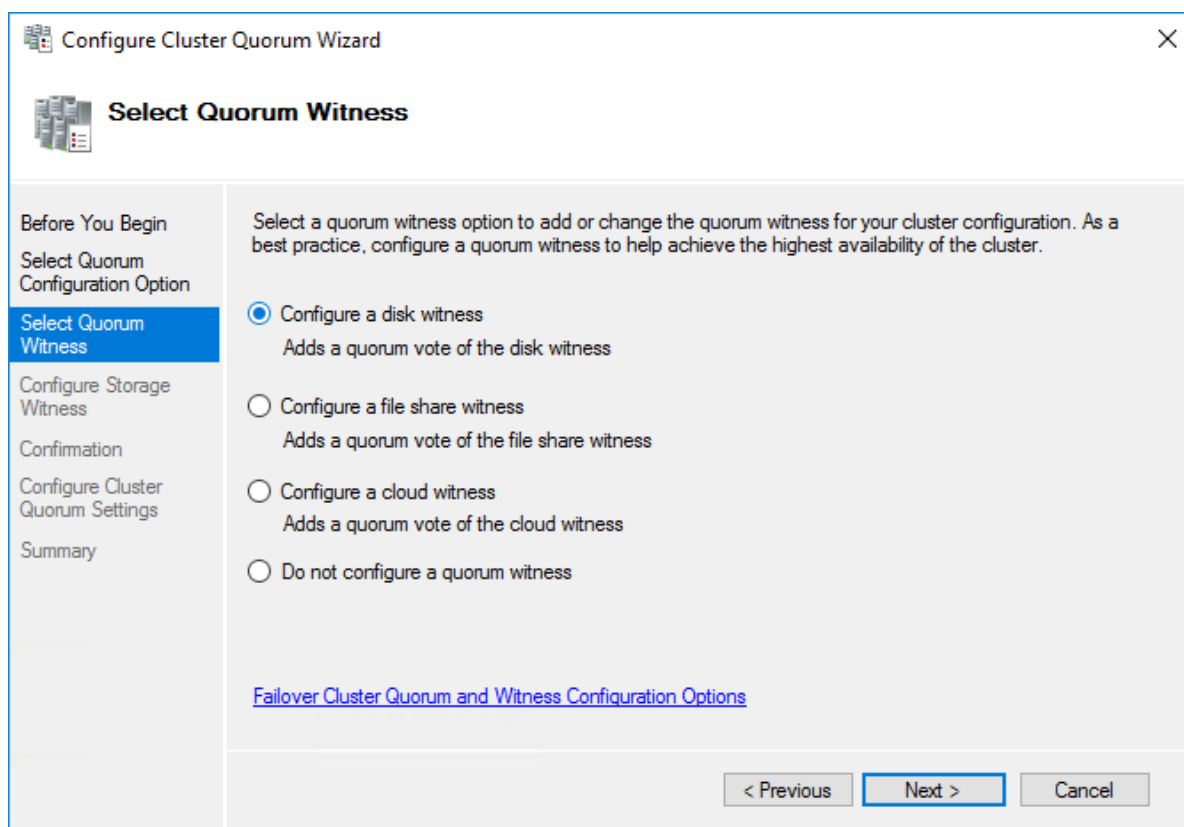
2. To configure the cluster witness disk, right-click on Cluster and proceed to More Actions -> Configure Cluster Quorum Settings.



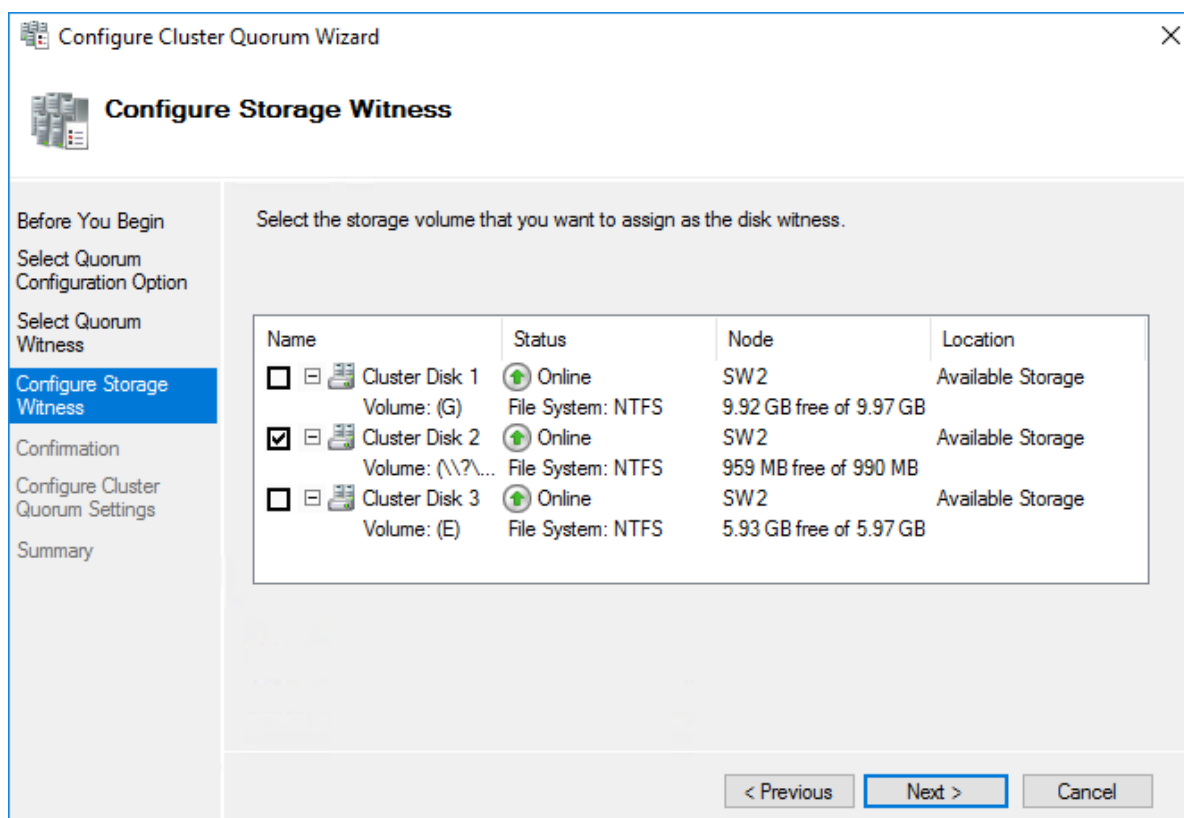
3. Follow the wizard and use the Select the quorum witness option. Click Next.



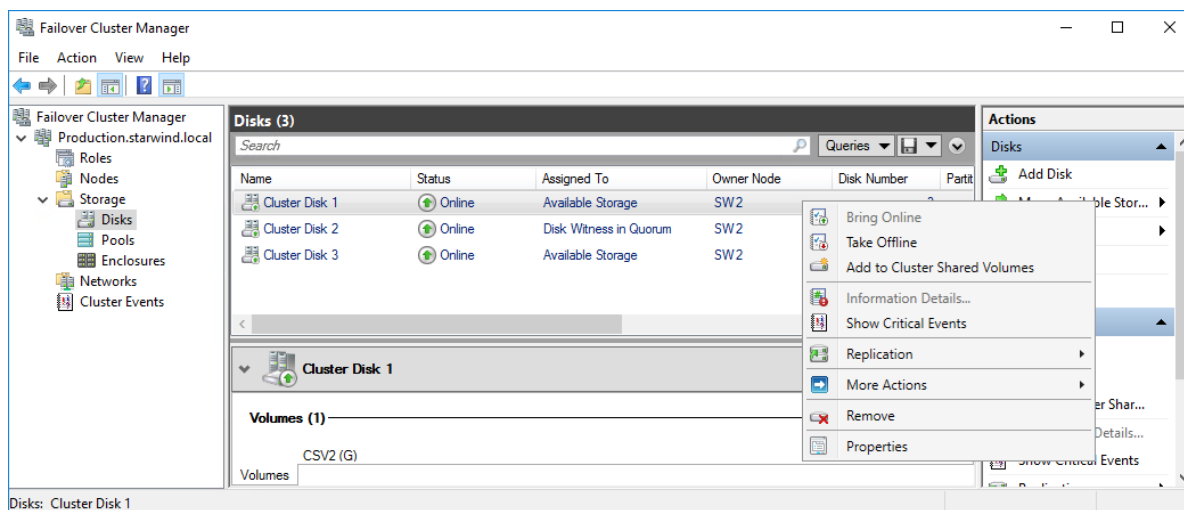
4. Select Configure a disk witness. Click Next.



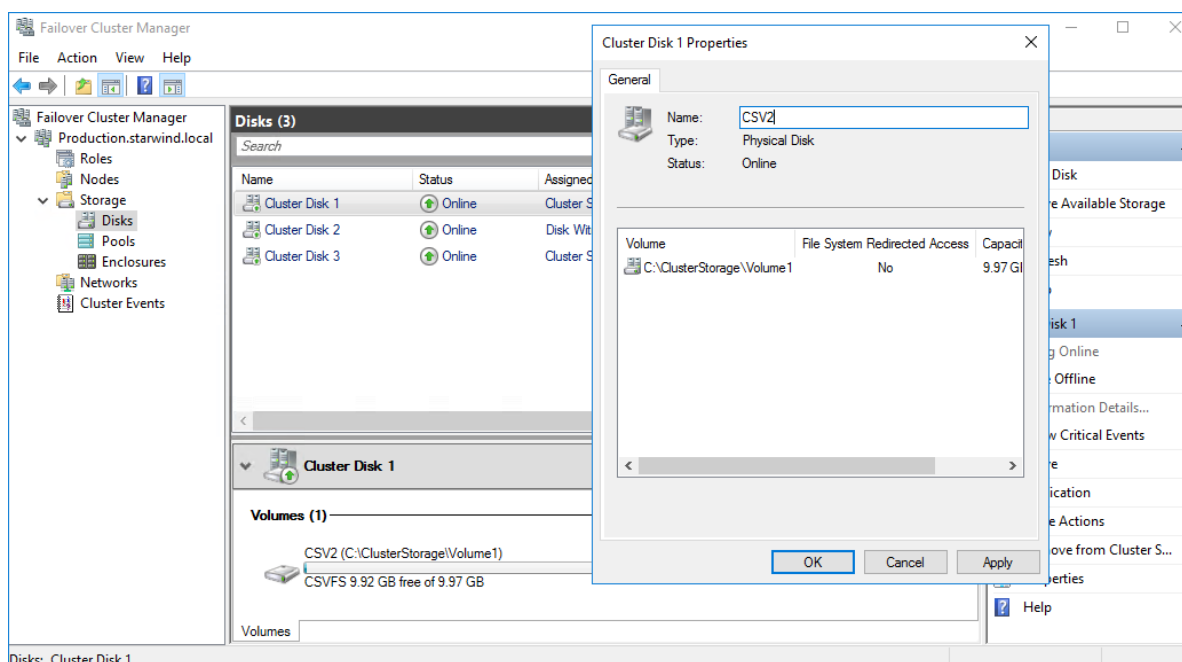
5. Select the Witness disk to be assigned as the cluster witness disk. Click Next and press Finish to complete the operation.



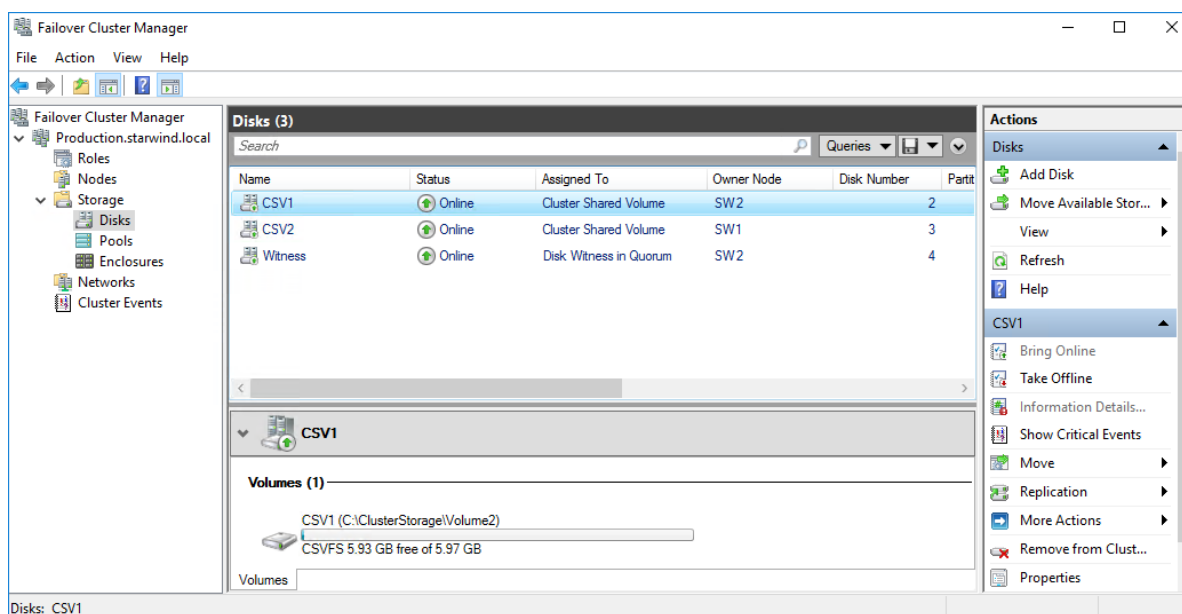
6. In Failover Cluster Manager, Right-click the disk and select Add to Cluster Shared Volumes.



7. If renaming of the cluster shared volume is required, right-click on the disk and select Properties. Type the new name for the disk and click Apply followed by OK.



8. Perform the steps 6-7 for any other disk in Failover Cluster Manager. The resulting list of disks will look similar to the screenshot below.

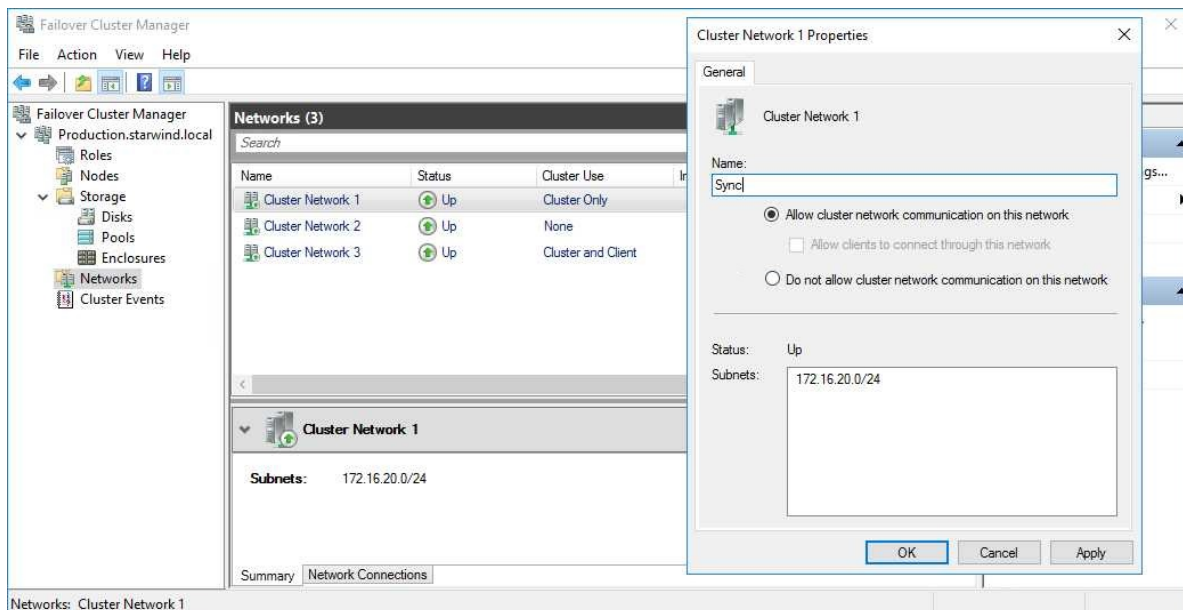


Configuring Cluster Network Preferences

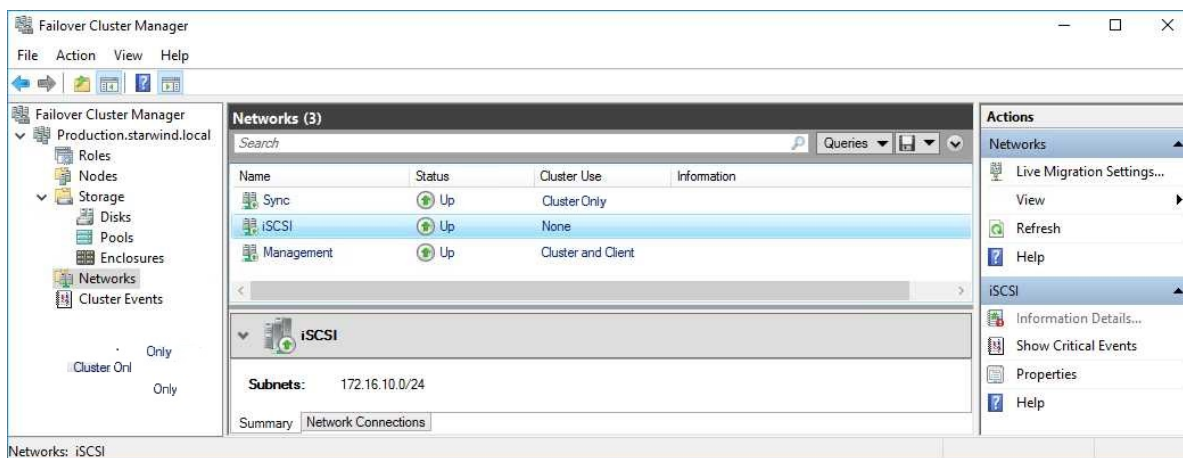
1. In the Networks section of the Failover Cluster Manager, right-click on the network from the list. Set its new name if required to identify the network by its subnet. Apply the change and press OK.

NOTE: Please double-check that cluster communication is configured with redundant networks:

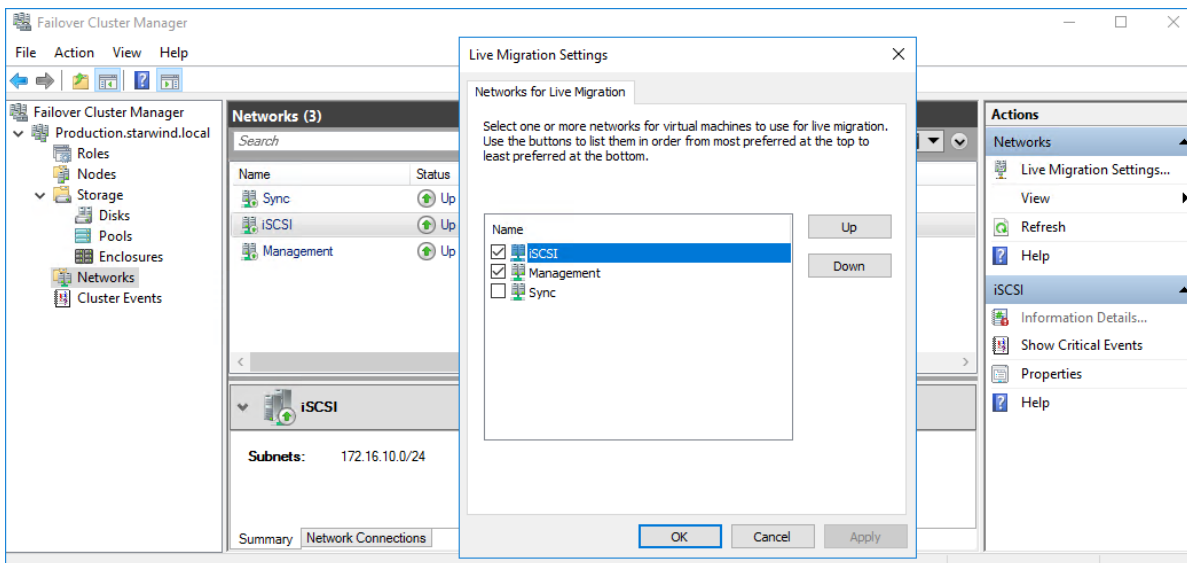
<https://docs.microsoft.com/en-us/windows-server/failover-clustering/smb-multichannel>



2. Rename other networks as described above, if required.



3. In the Actions tab, click Live Migration Settings. Uncheck the synchronization network, while the iSCSI network can be used if it is 10+ Gbps. Apply the changes and click OK.



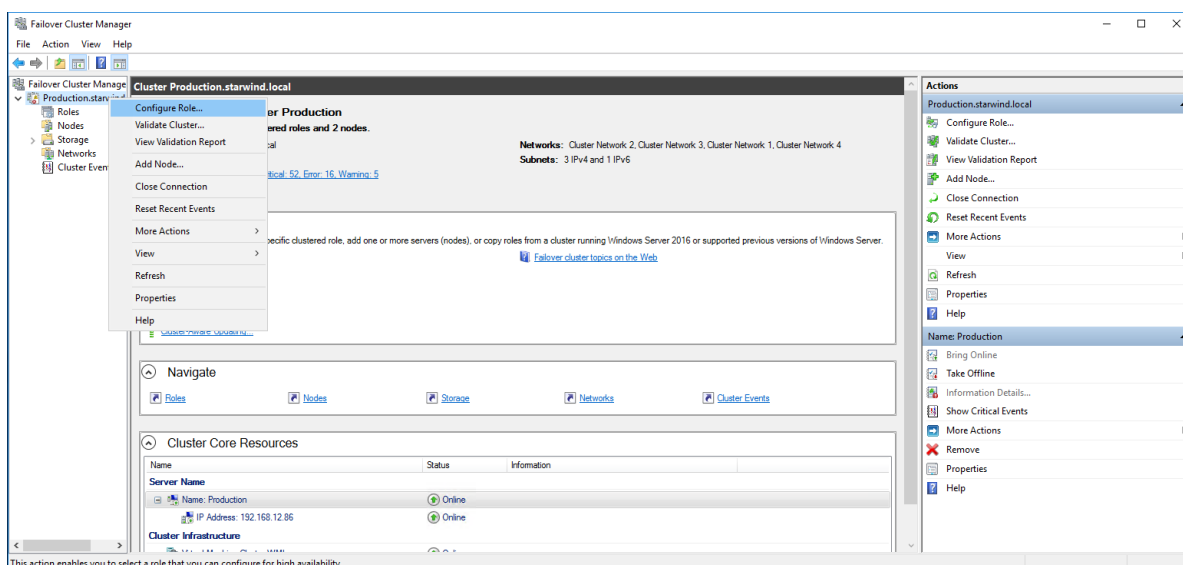
The cluster configuration is completed and it is ready for virtual machines deployment. Select Roles and in the Action tab, click Virtual Machines -> New Virtual Machine. Complete the wizard.

Configuring File Shares

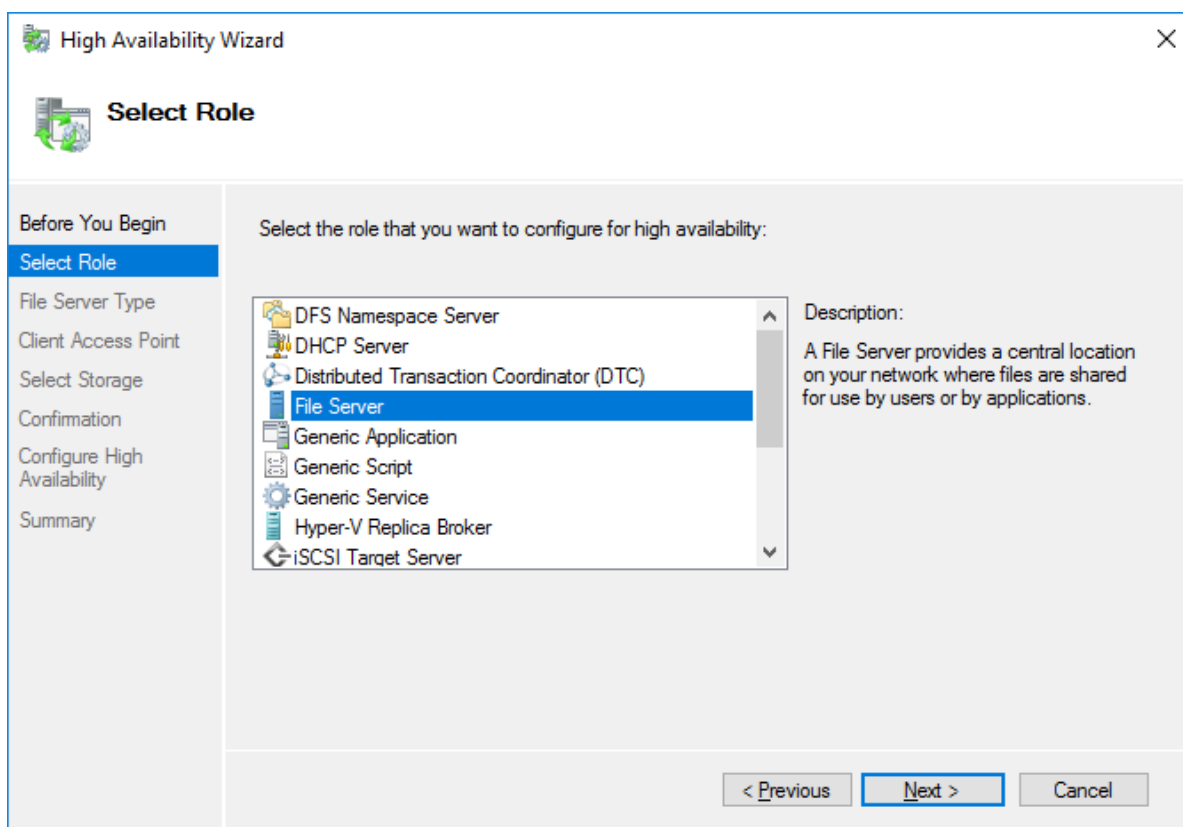
Please follow the steps below if file shares should be configured on cluster nodes.

Configuring The Scale-Out File Server Role

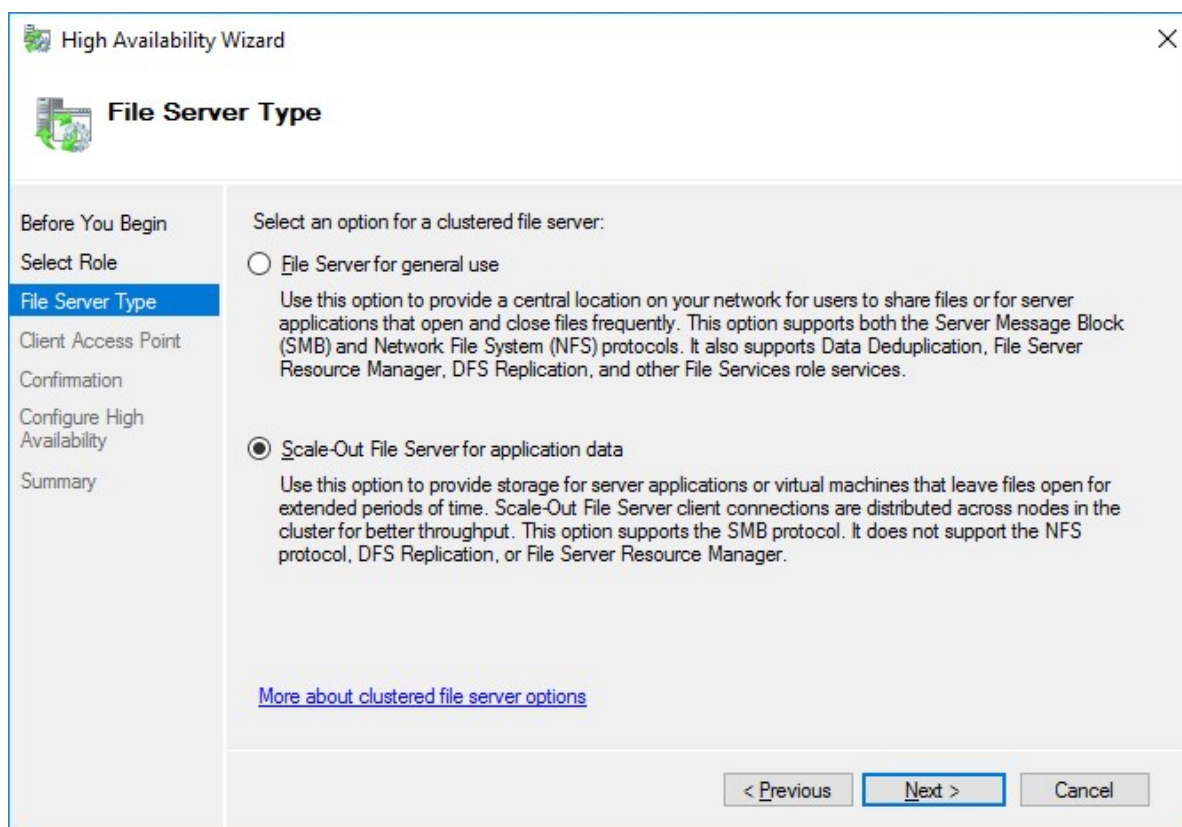
1. To configure the Scale-Out File Server Role, open Failover Cluster Manager.
2. Right-click the cluster name, then click Configure Role and click Next to continue.



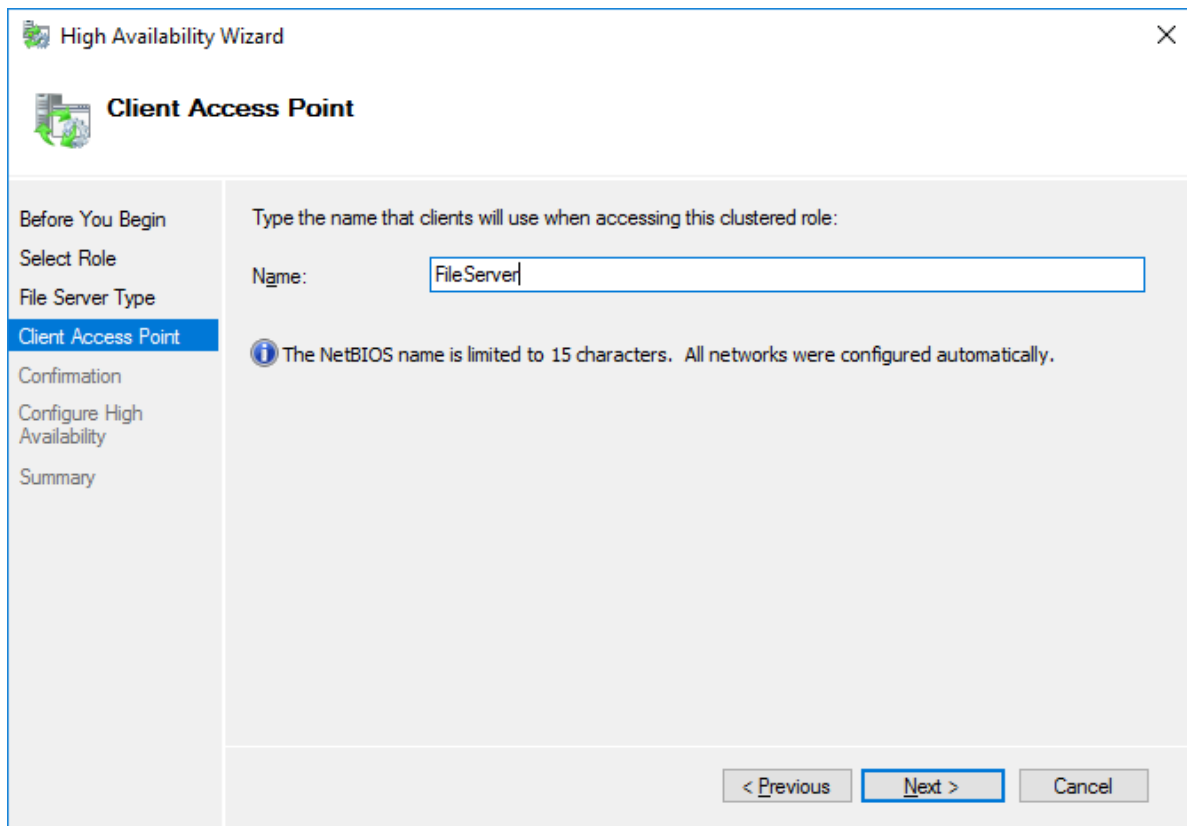
3. Select the File Server item from the list in High Availability Wizard and click Next to continue.



4. Select Scale-Out File Server for application data and click Next.



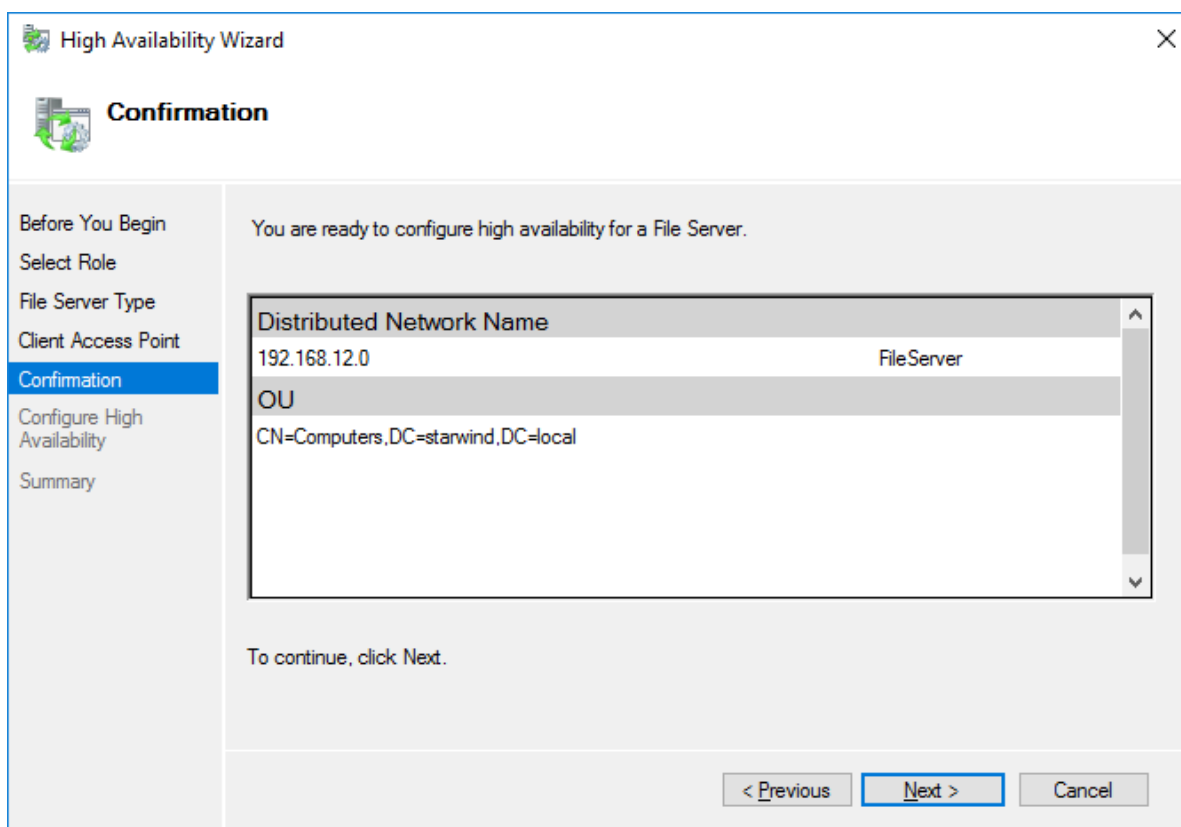
5. On the Client Access Point page, in the Name text field, type the NetBIOS name that will be used to access a Scale-Out File Server.



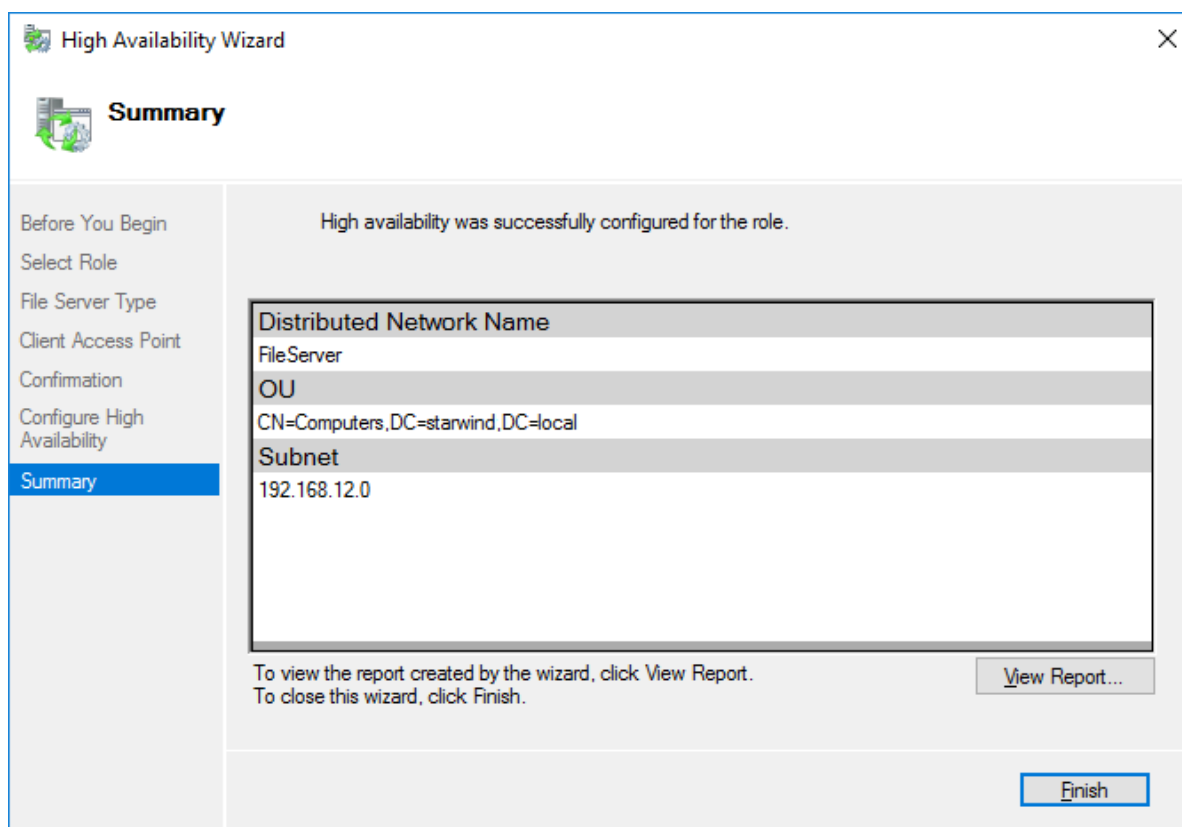
The image shows a screenshot of the 'High Availability Wizard' window, specifically the 'Client Access Point' step. The window has a title bar with the text 'High Availability Wizard' and a close button. On the left side, there is a vertical navigation pane with the following steps: 'Before You Begin', 'Select Role', 'File Server Type', 'Client Access Point' (which is currently selected and highlighted in blue), 'Confirmation', 'Configure High Availability', and 'Summary'. The main area of the wizard is titled 'Client Access Point' and contains the instruction: 'Type the name that clients will use when accessing this clustered role:'. Below this instruction is a text input field with the label 'Name:' and the text 'FileServer' entered. A blue border highlights the input field. Below the input field, there is an information icon (a blue circle with a white 'i') followed by the text: 'The NetBIOS name is limited to 15 characters. All networks were configured automatically.' At the bottom right of the wizard, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Click Next to continue.

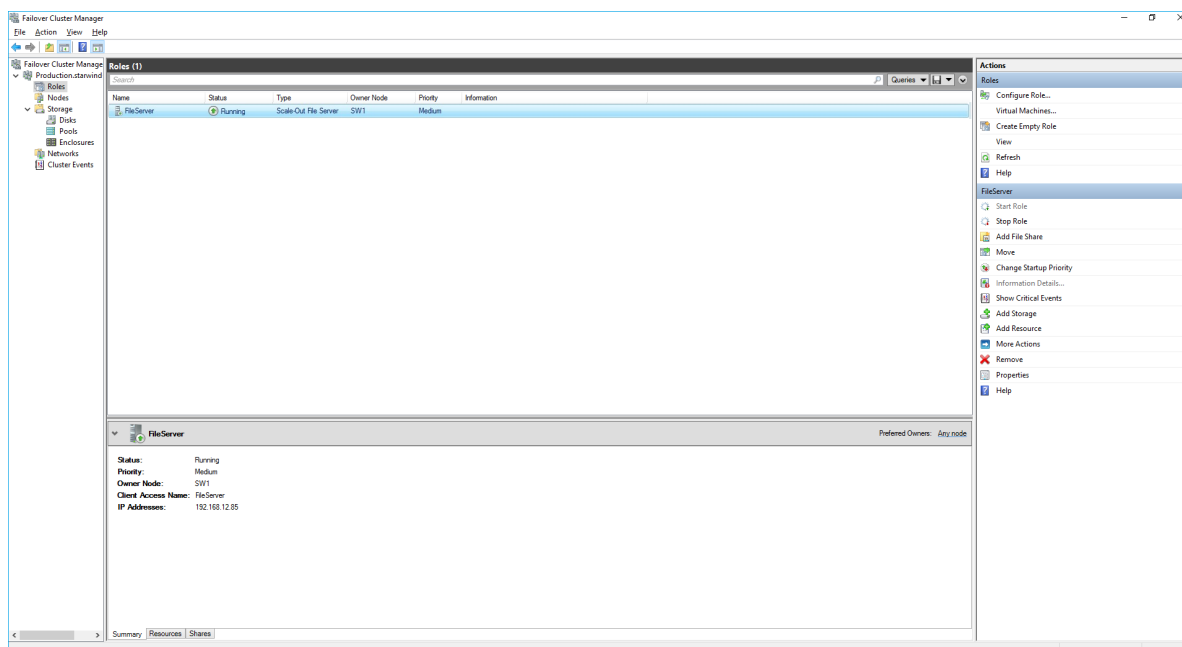
6. Check whether the specified information is correct. Click Next to continue or Previous to change the settings.



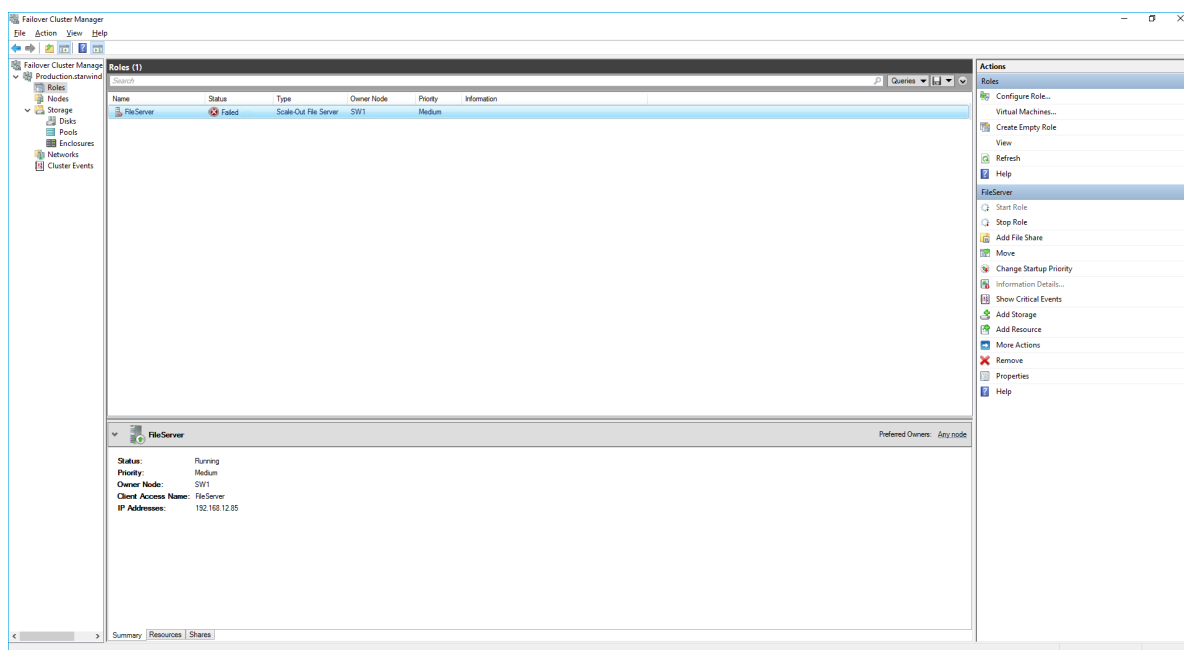
7. Once the installation is finished successfully, the Wizard should now look like the screenshot below.
Click Finish to close the Wizard.



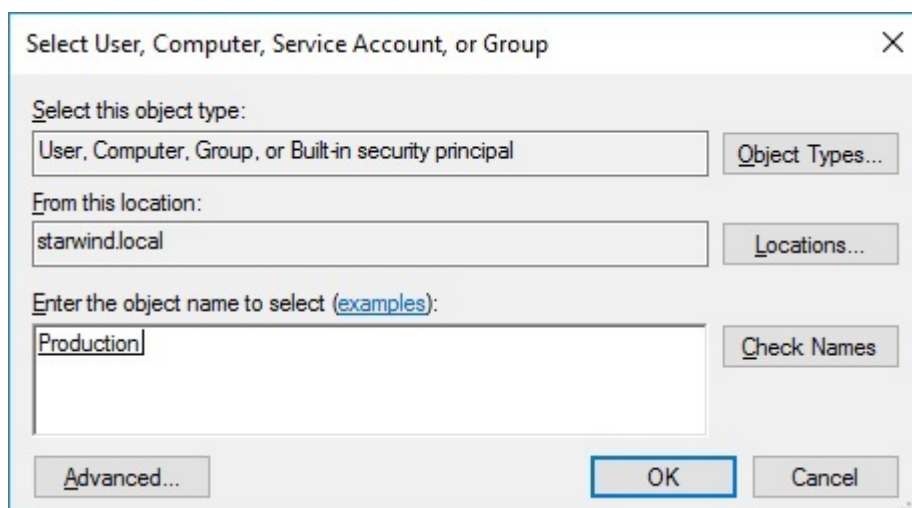
8. The newly created role should now look like the screenshot below.



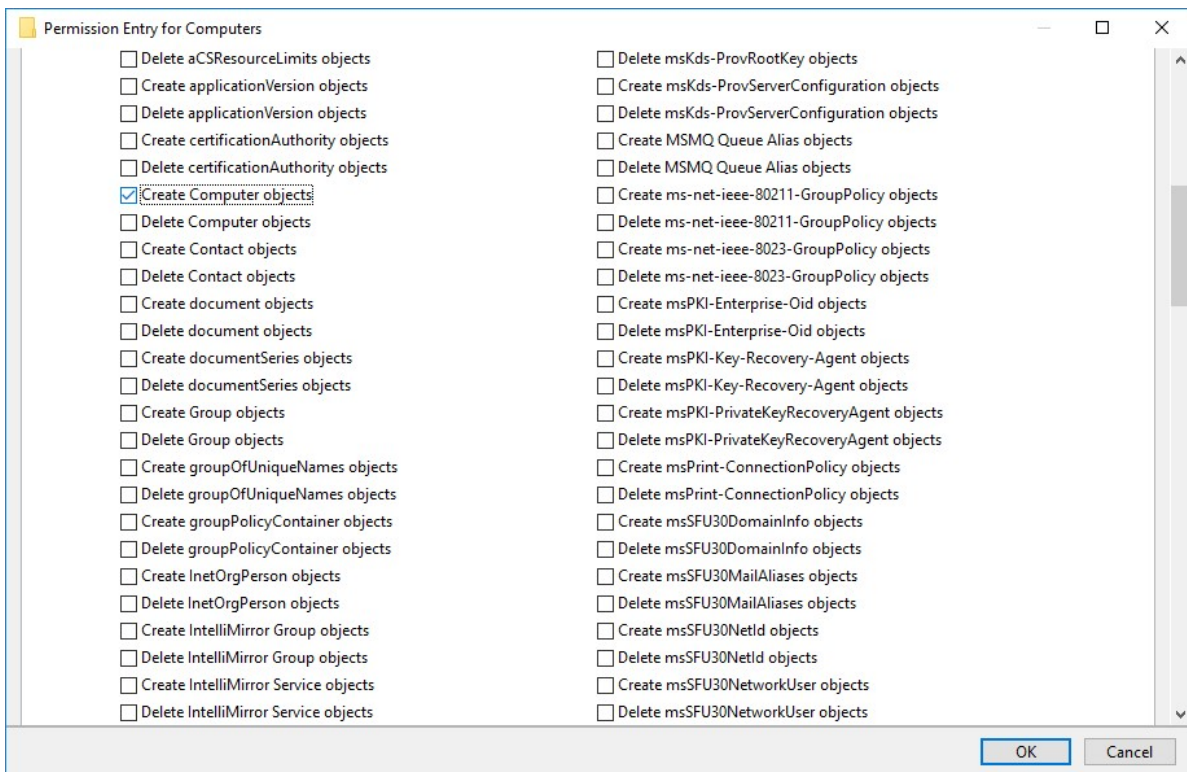
NOTE: If the role status is Failed and it is unable to Start, please, follow the next steps:



- open Active Directory Users and Computers
- enable the Advanced view if it is not enabled
- edit the properties of the OU containing the cluster computer object (in this case – Production)
- open the Security tab and click Advanced
- in the appeared window, press Add (the Permission Entry dialog box opens), click Select a principal
- in the appeared window, click Object Types, select Computers, and click OK
- enter the name of the cluster computer object (in this case – Production)



- go back to Permission Entry dialog, scroll down, and select Create Computer Objects,

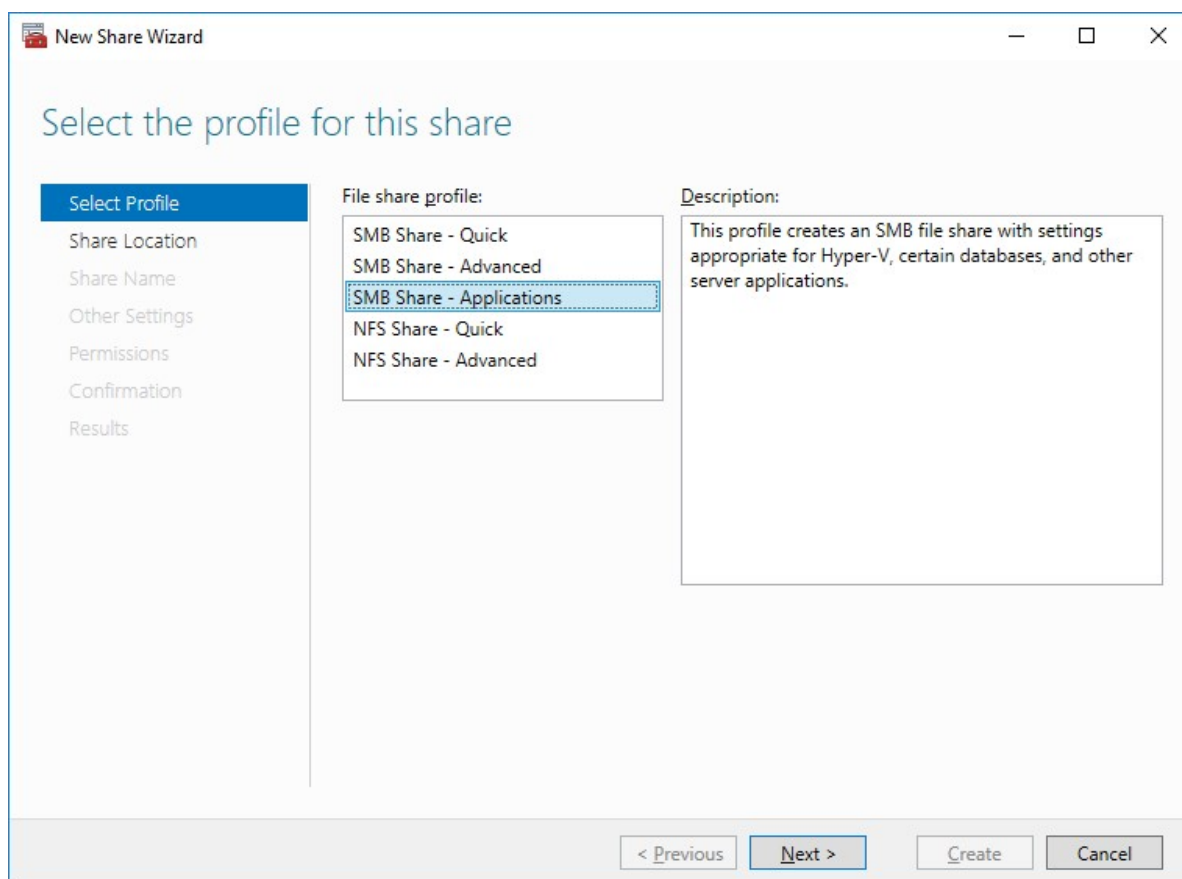


- click OK on all opened windows to confirm the changes
- open Failover Cluster Manager, right-click SOFS role and click Start Role

Configuring File Share

To Add File Share:

- open Failover Cluster Manager
- expand the cluster and then click Roles
- right-click the file server role and then press Add File Share
- on the Select the profile for this share page, click SMB Share – Applications and then click Next



5. Select a CSV to host the share. Click Next to proceed.

Select the server and path for this share

Select Profile
Share Location
 Share Name
 Other Settings
 Permissions
 Confirmation
 Results

Server:

Server Name	Status	Cluster Role	Owner Node
FileServer	Online	Scale-Out File...	

Share location:

☒ Select by volume:

Volume	Free Space	Capacity	File System
C:\ClusterStorage\Volume1	5.92 GB	5.97 GB	CSVFS
C:\ClusterStorage\Volume2	9.91 GB	9.97 GB	CSVFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

☐ Type a custom path:

< Previous Next > Create Cancel

6. Type in the file share name and click Next.

New Share Wizard

Specify share name

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

Share name:

Share description:

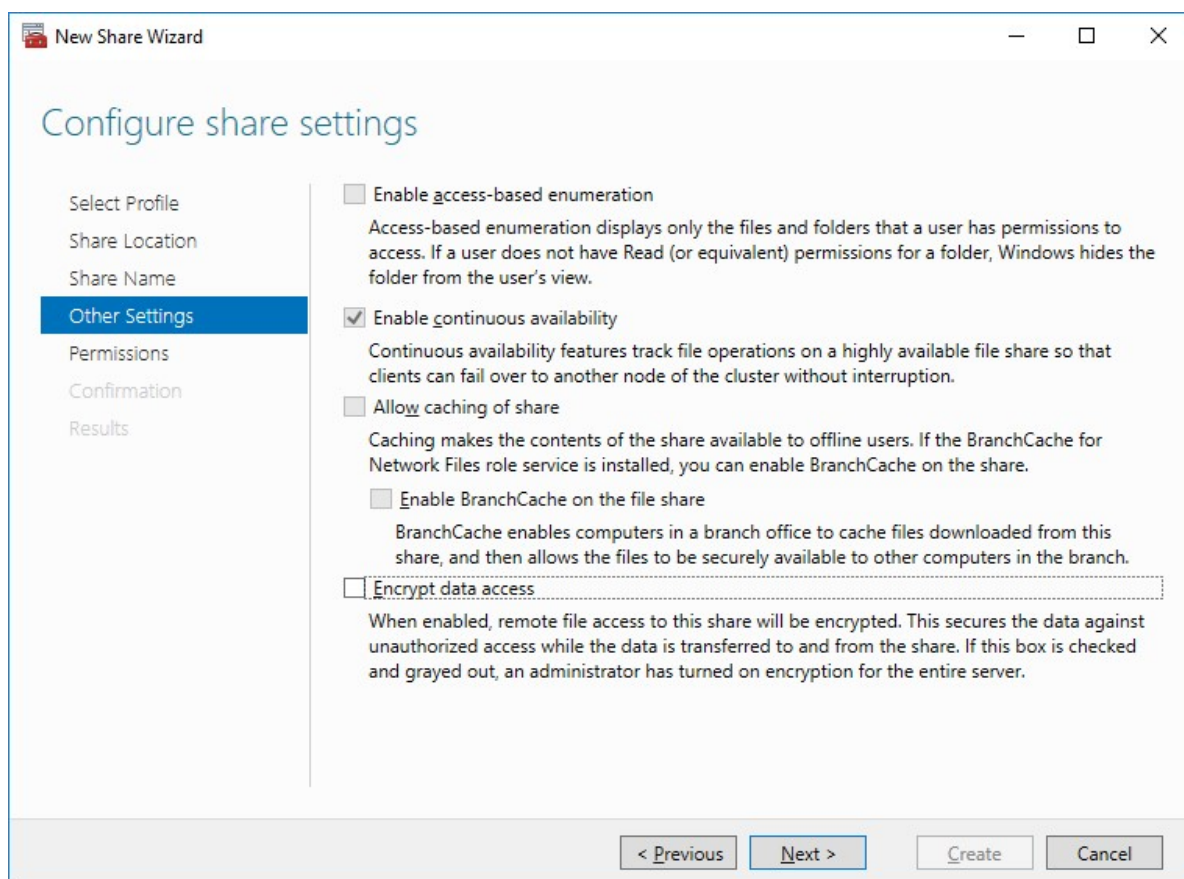
Local path to share:

! If the folder does not exist, the folder is created.

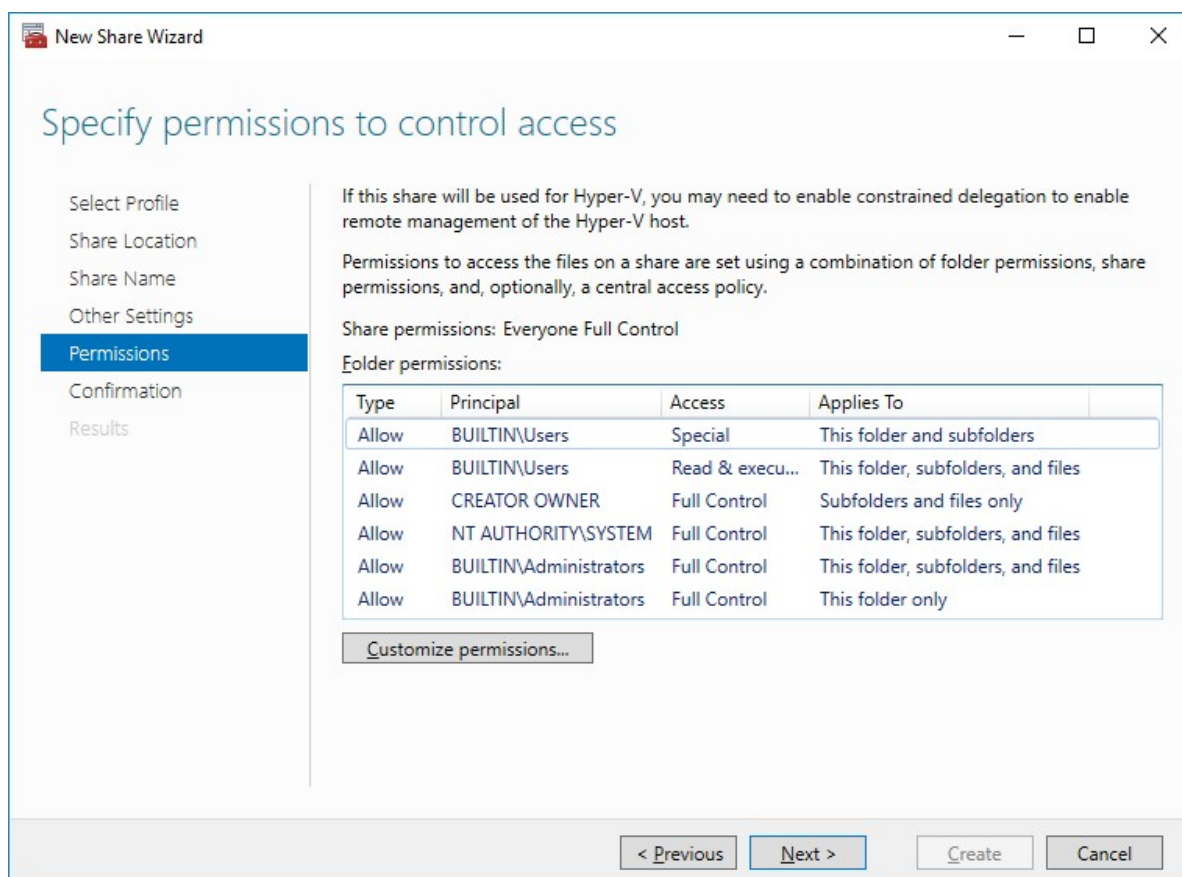
Remote path to share:

< Previous Next > Create Cancel

7. Make sure that the Enable Continuous Availability box is checked. Click Next to proceed.



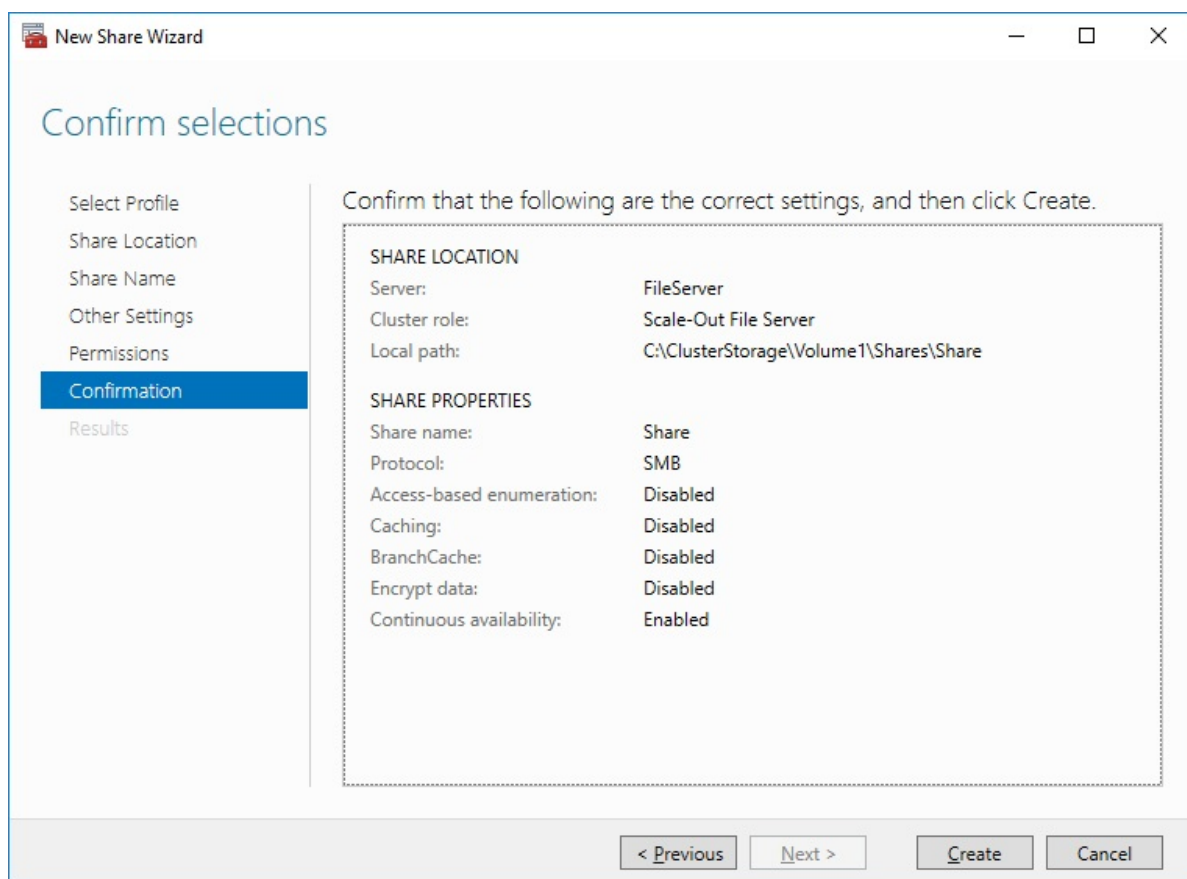
8. Specify the access permissions for the file share.



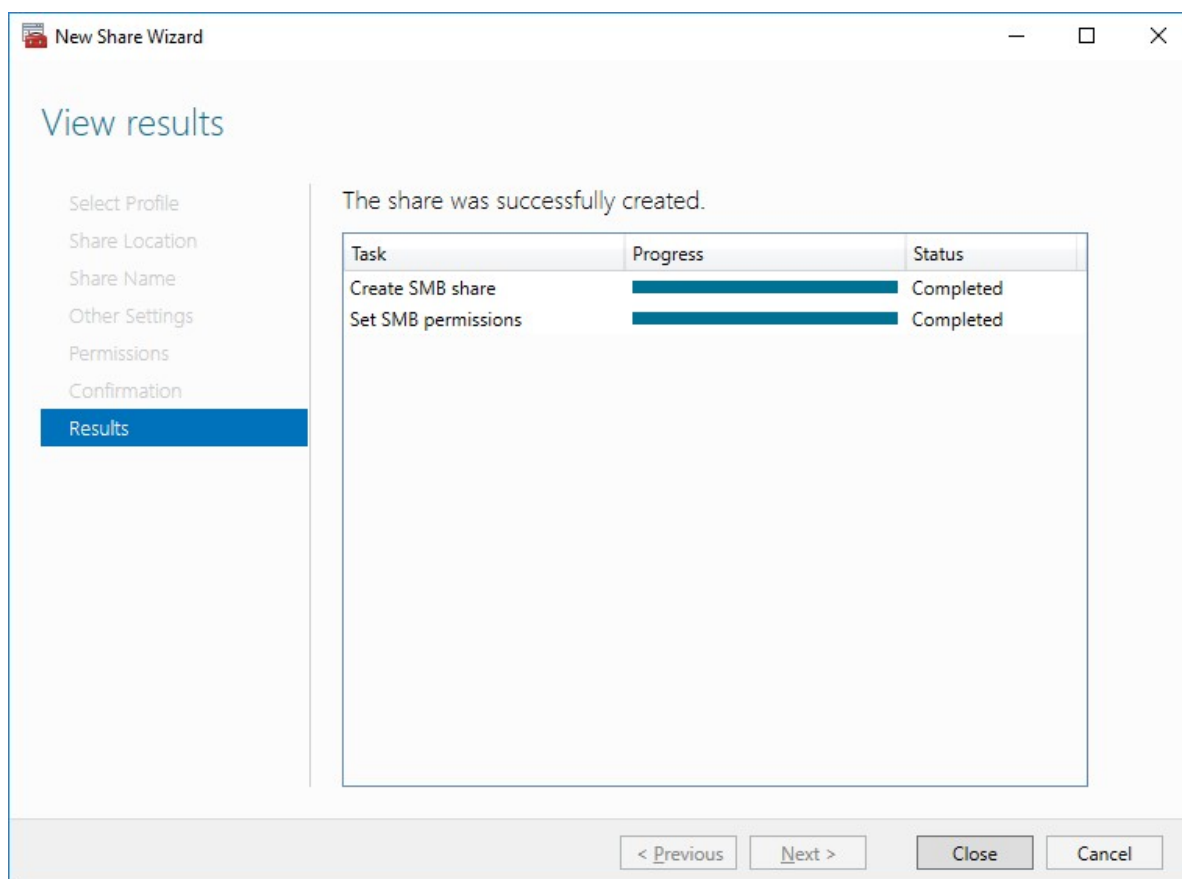
NOTE:

- for the Scale-Out File Server for Hyper-V, all Hyper-V computer accounts, the SYSTEM account, and all Hyper-V administrators must be provided with the full control on the share and file system
- for the Scale-Out File Server on Microsoft SQL Server, the SQL Server service account must be granted full control on the share and the file system

9. Check whether specified settings are correct. Click Previous to make any changes or click Create to proceed.

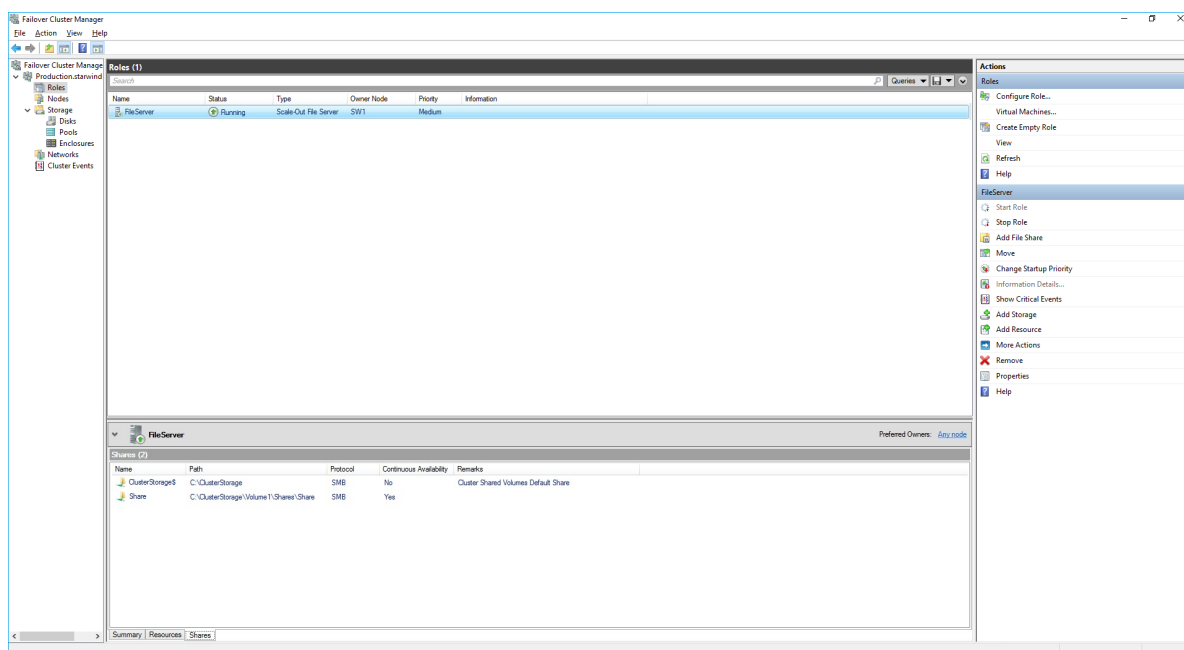


10. Check the summary and click Close to close the Wizard.



To Manage Created File Shares:

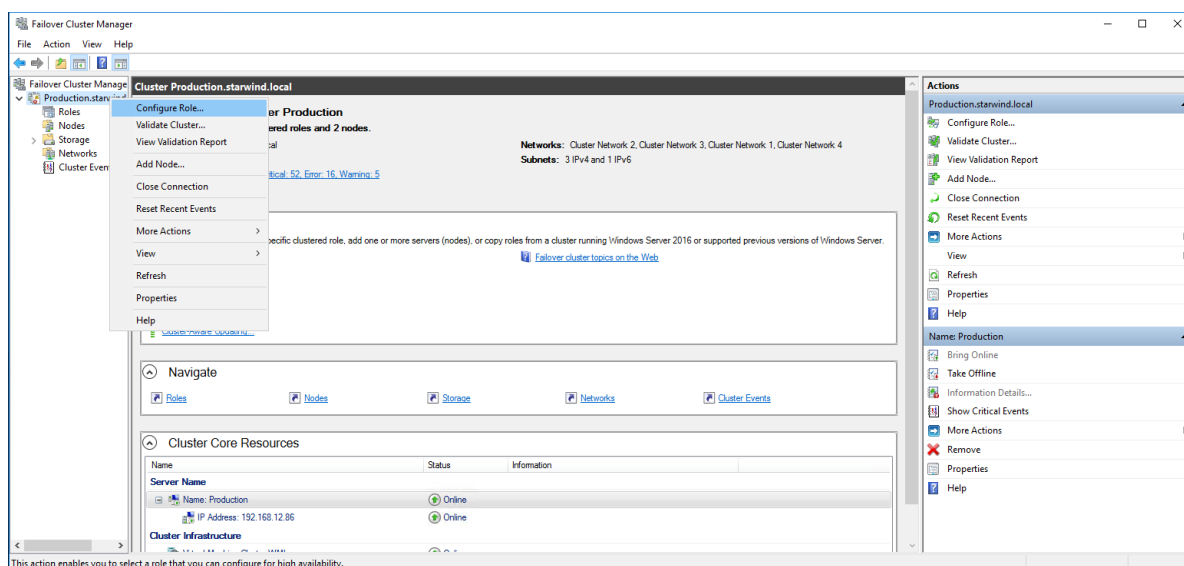
- open Failover Cluster Manager
- expand the cluster and click Roles
- choose the file share role, select the Shares tab, right-click the created file share, and select Properties:



Configuring The File Server For General Use Role

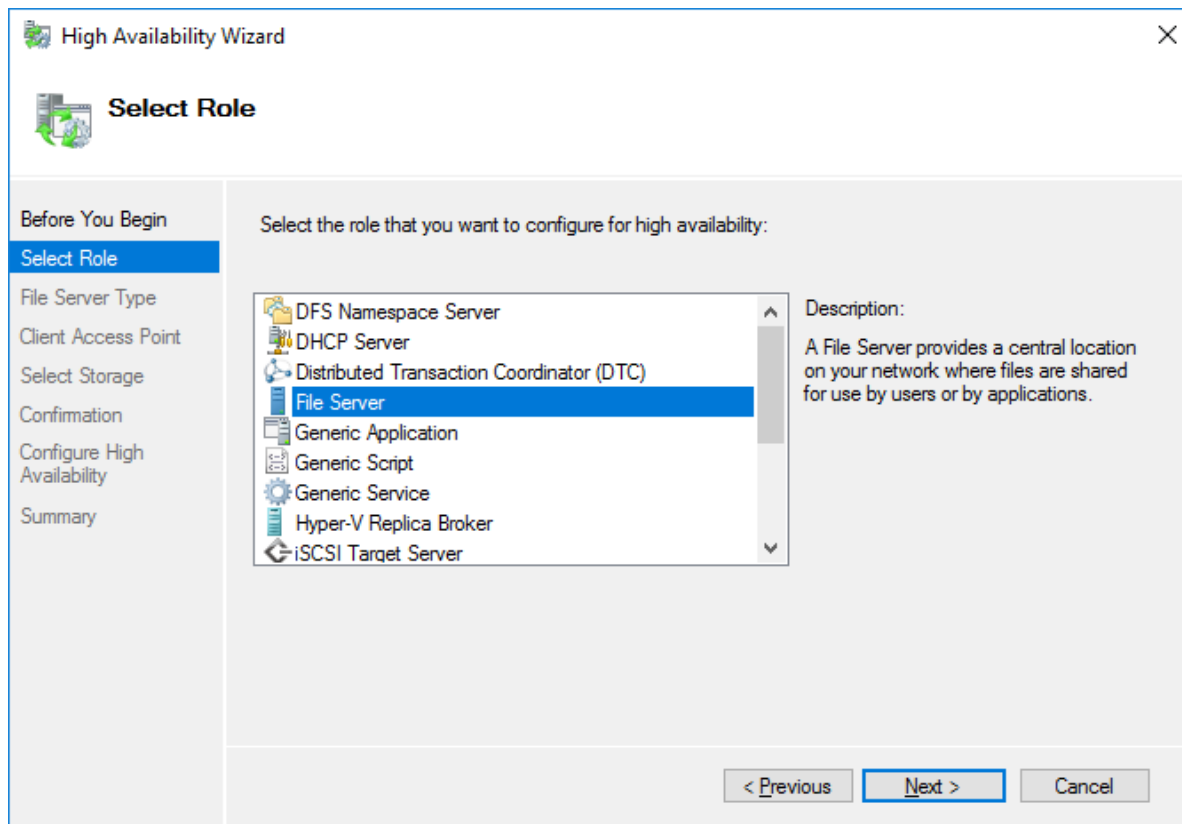
NOTE: To configure File Server for General Use, the cluster should have available storage

1. To configure the File Server for General Use role, open Failover Cluster Manager.
2. Right-click on the cluster name, then click Configure Role and click Next to continue.

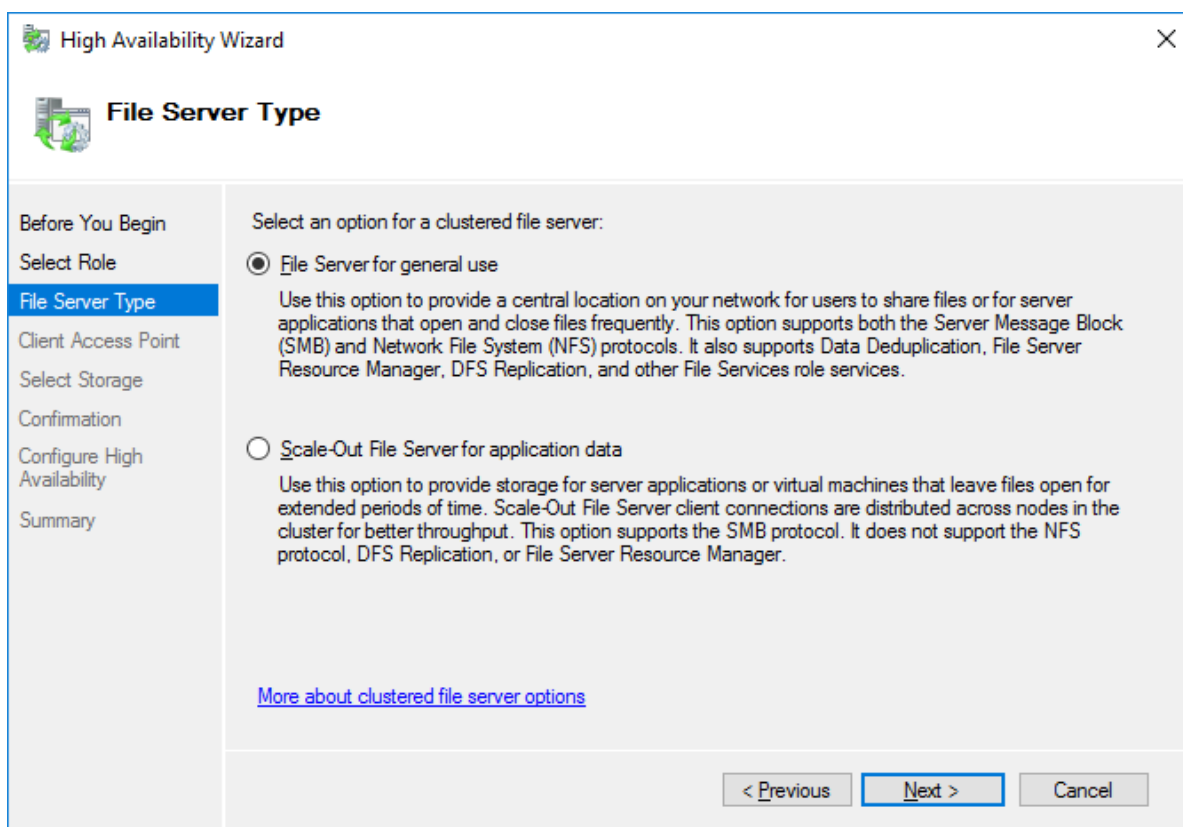


3. Select the File Server item from the list in High Availability Wizard and click Next to

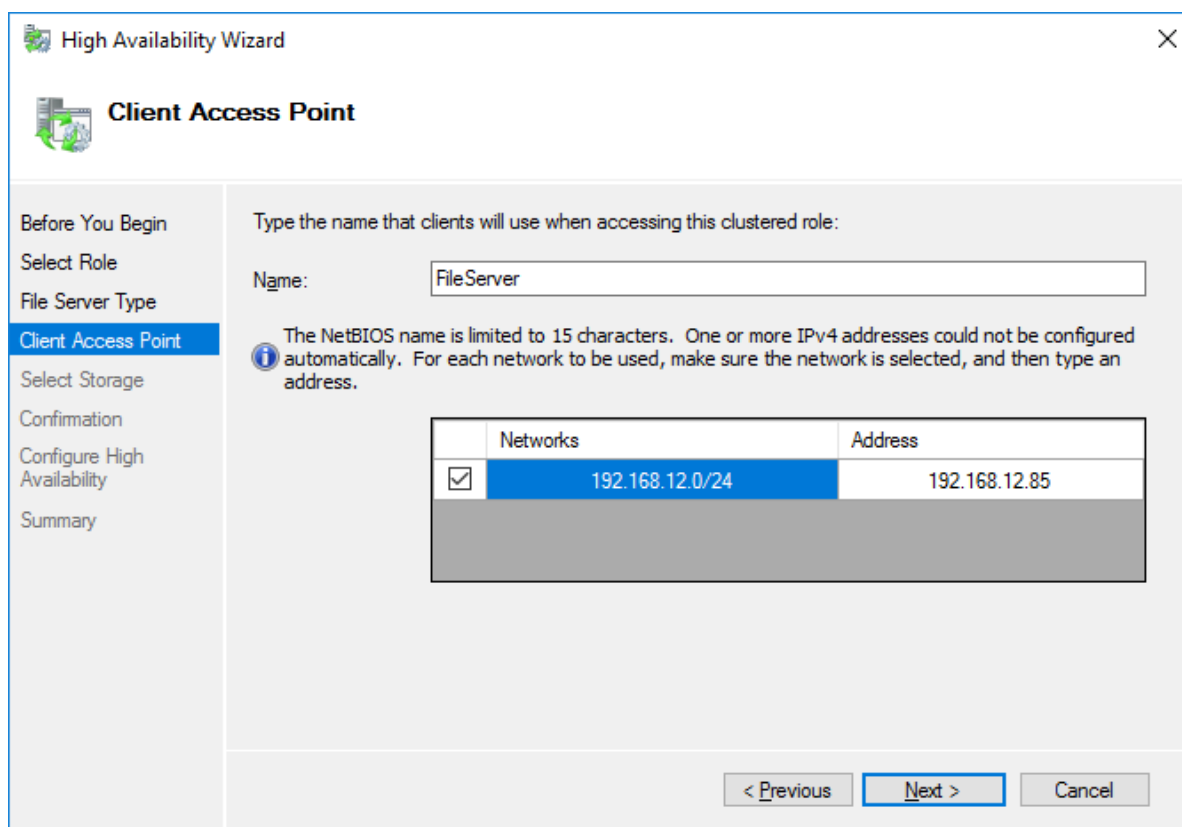
continue.



4. Select File Server for general use and click Next.



5. On the Client Access Point page, in the Name text field, type the NETBIOS name that will be used to access the File Server and IP for it.



The screenshot shows the 'High Availability Wizard' window, specifically the 'Client Access Point' step. On the left is a navigation pane with steps: 'Before You Begin', 'Select Role', 'File Server Type', 'Client Access Point' (highlighted), 'Select Storage', 'Confirmation', 'Configure High Availability', and 'Summary'. The main area is titled 'Client Access Point' and contains the instruction: 'Type the name that clients will use when accessing this clustered role:'. Below this is a text box labeled 'Name:' containing 'FileServer'. An information icon (i) is followed by a note: 'The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.' Below the note is a table with two columns: 'Networks' and 'Address'. The first row shows a checked checkbox, the network '192.168.12.0/24', and the address '192.168.12.85'. At the bottom right are three buttons: '< Previous', 'Next >' (highlighted), and 'Cancel'.

High Availability Wizard

Client Access Point

Before You Begin
Select Role
File Server Type
Client Access Point
Select Storage
Confirmation
Configure High Availability
Summary

Type the name that clients will use when accessing this clustered role:

Name:

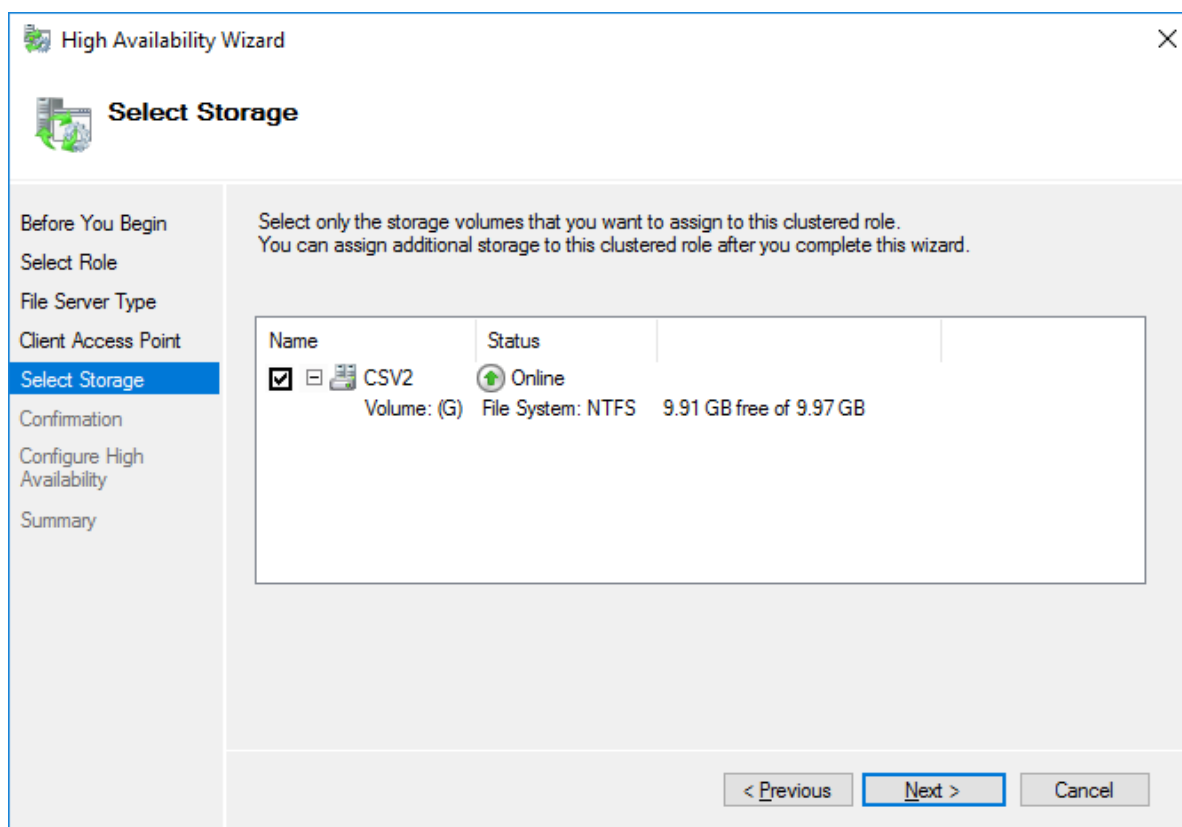
i The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

	Networks	Address
<input checked="" type="checkbox"/>	192.168.12.0/24	192.168.12.85

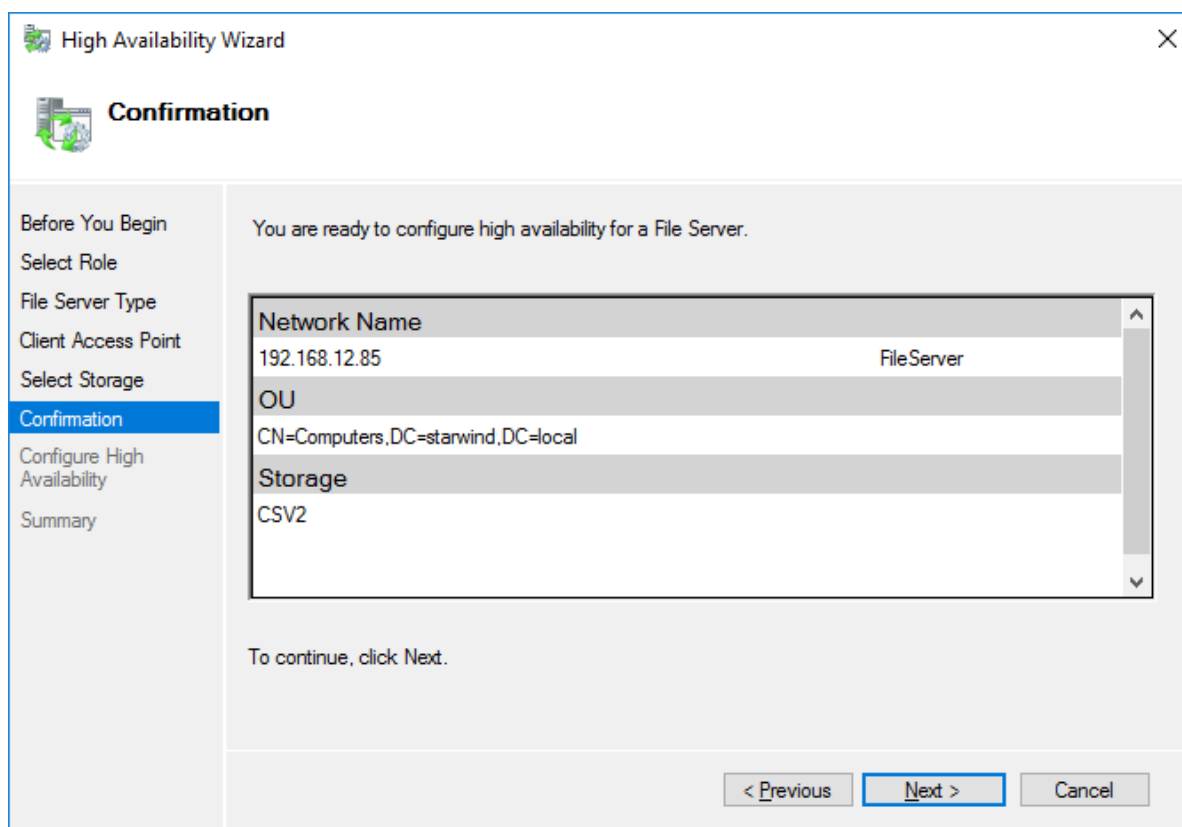
< Previous **Next >** Cancel

Click Next to continue.

6. Select the Cluster disk and click Next.

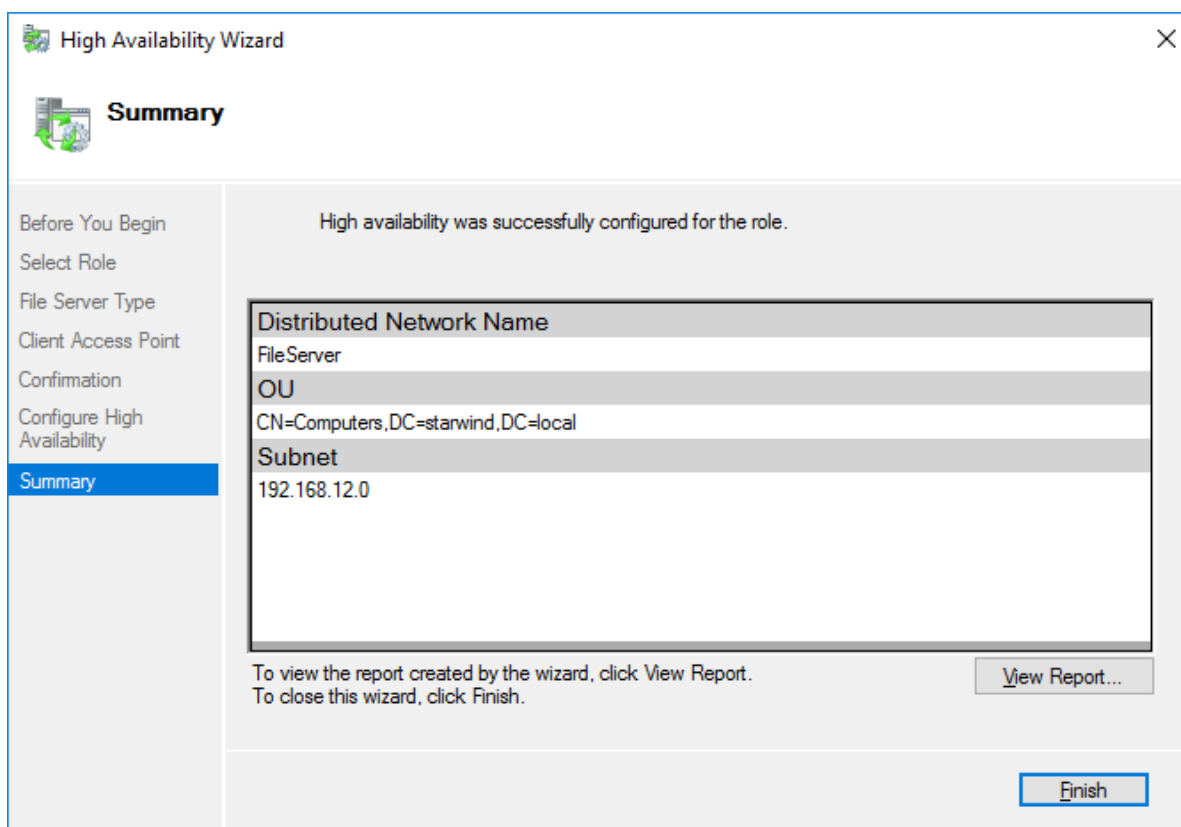


7. Check whether the specified information is correct. Click Next to proceed or Previous to change the settings.

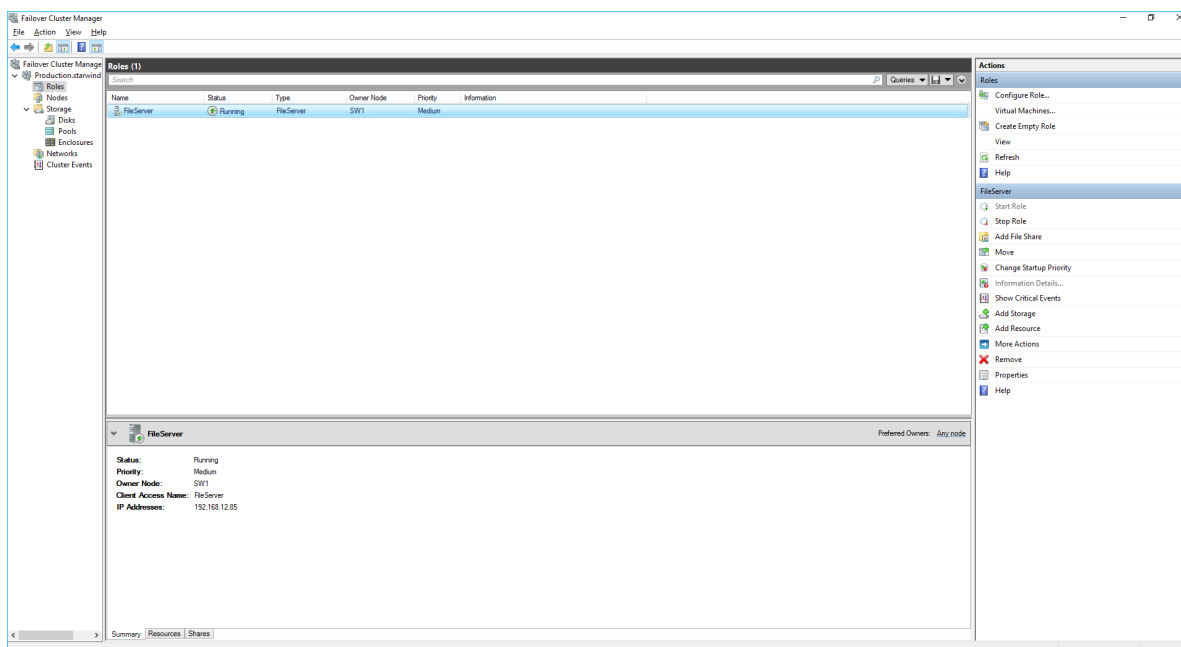


8. Once the installation has been finished successfully, the Wizard should now look like the screenshot below.

Click Finish to close the Wizard.



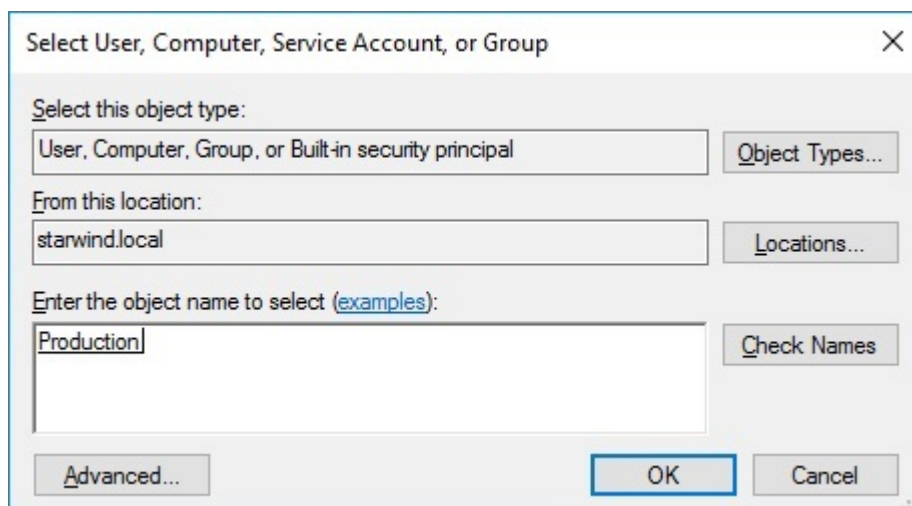
9. The newly created role should now look like the screenshot below.



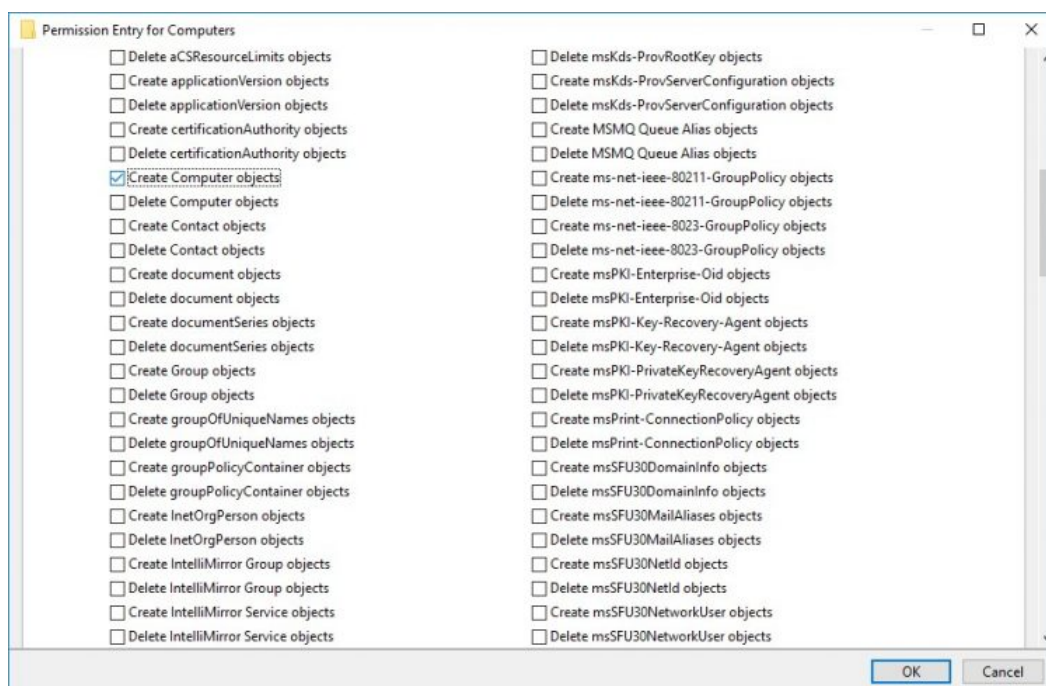
NOTE: If the role status is Failed and it is unable to Start, please, follow the next steps:

- open Active Directory Users and Computers

- enable the Advanced view if it is not enabled
- edit the properties of the OU containing the cluster computer object (in this case – Production)
- open the Security tab and click Advanced
- in the appeared window, press Add (the Permission Entry dialog box opens), click Select a principal
- in the appeared window, click Object Types, select Computers, and click OK
- enter the name of the cluster computer object (in this case – Production)



- go back to Permission Entry dialog, scroll down, and select Create Computer Objects



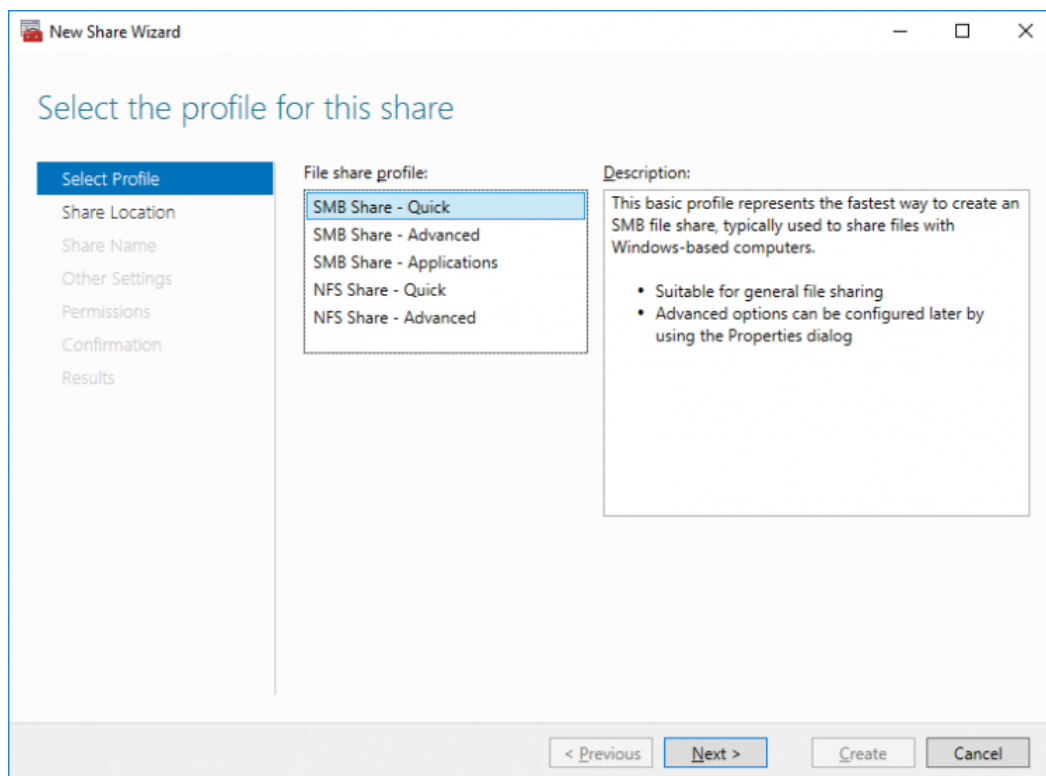
- click OK on all opened windows to confirm the changes

- open Failover Cluster Manager, right-click File Share role and click Start Role

Configuring Smb File Share

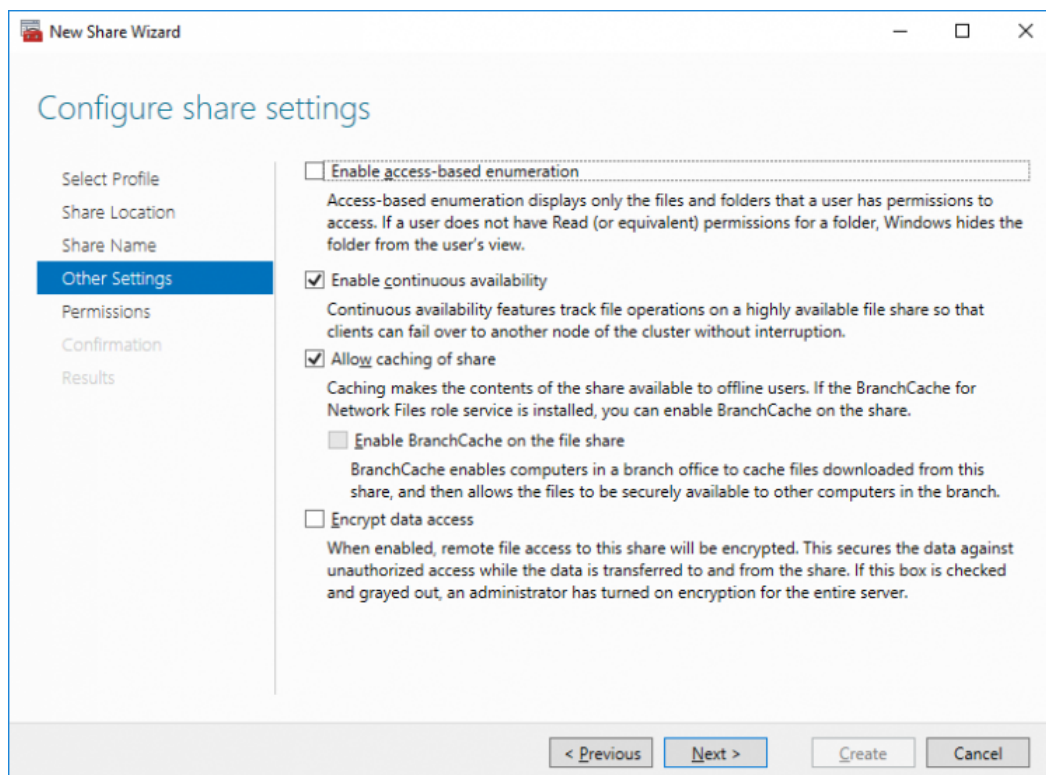
To Add SMB File Share

1. Open Failover Cluster Manager.
2. Expand the cluster and then click Roles.
3. Right-click the File Server role and then press Add File Share.
4. On the Select the profile for this share page, click SMB Share – Quick and then click Next.

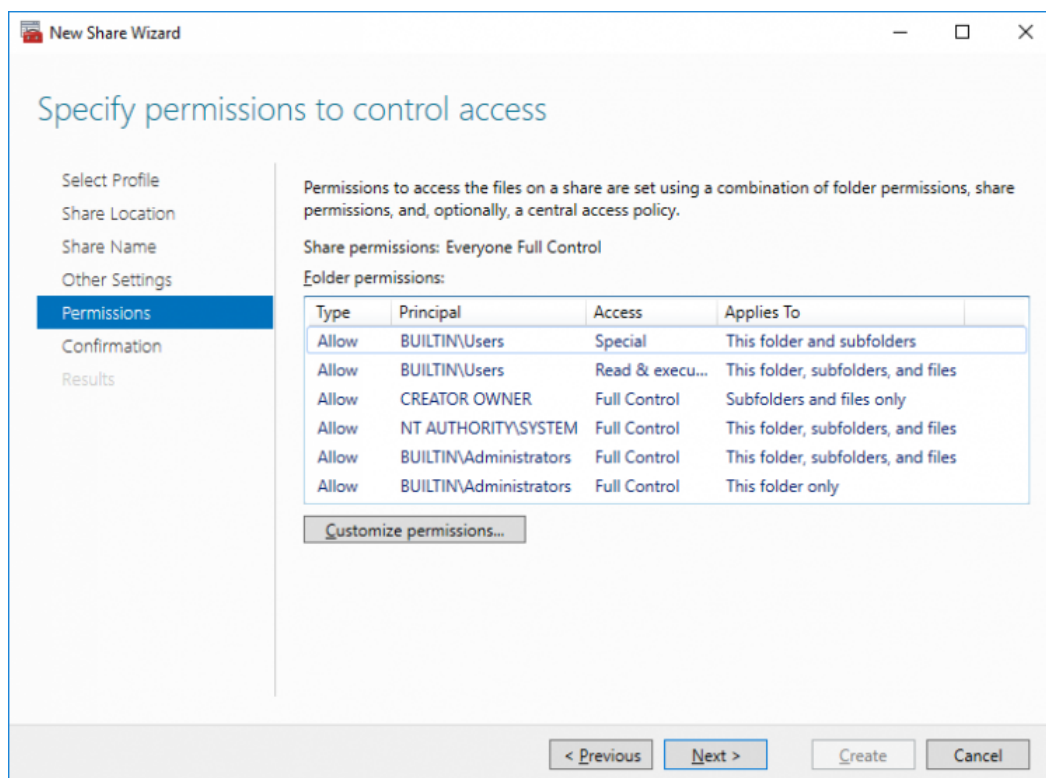


5. Select available storage to host the share. Click Next to continue.

continue.



8.Specify the access permissions for the file share.



9. Check whether specified settings are correct. Click Previous to make any changes or Next/Create to continue.

New Share Wizard

Confirm selections

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

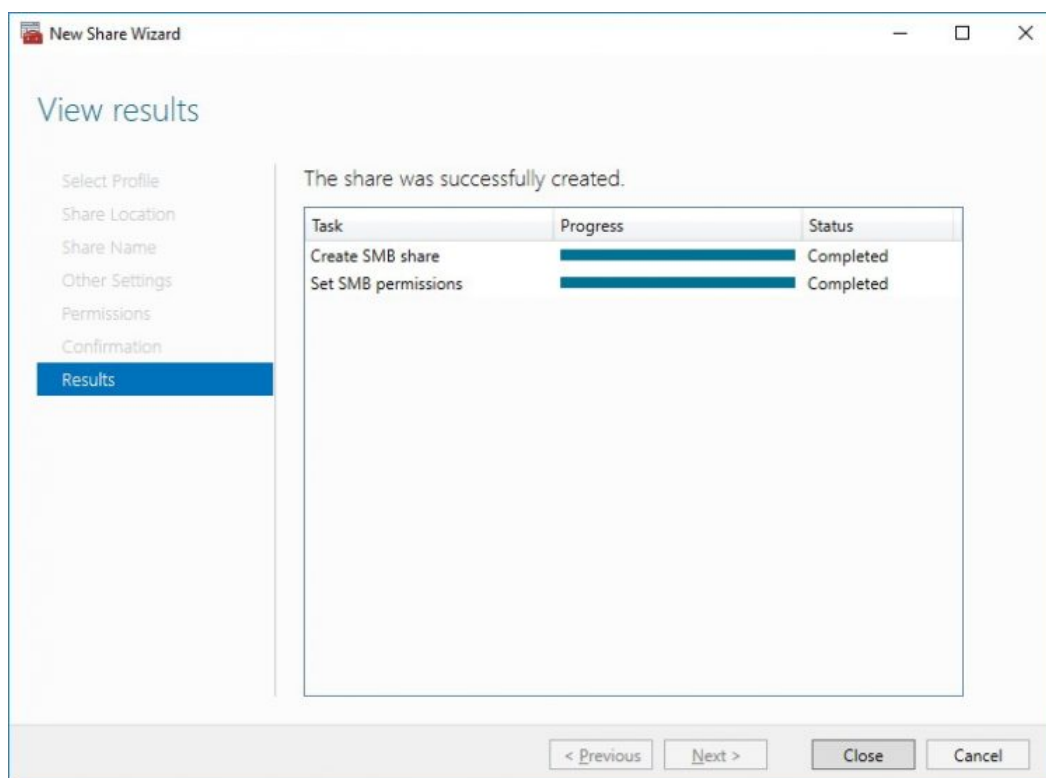
Confirm that the following are the correct settings, and then click Create.

SHARE LOCATION	
Server:	FileServer
Cluster role:	Scale-Out File Server
Local path:	C:\ClusterStorage\Volume1\Shares\Share

SHARE PROPERTIES	
Share name:	Share
Protocol:	SMB
Access-based enumeration:	Disabled
Caching:	Disabled
BranchCache:	Disabled
Encrypt data:	Disabled
Continuous availability:	Enabled

< Previous Next > Create Cancel

10. Check the summary and click Close.

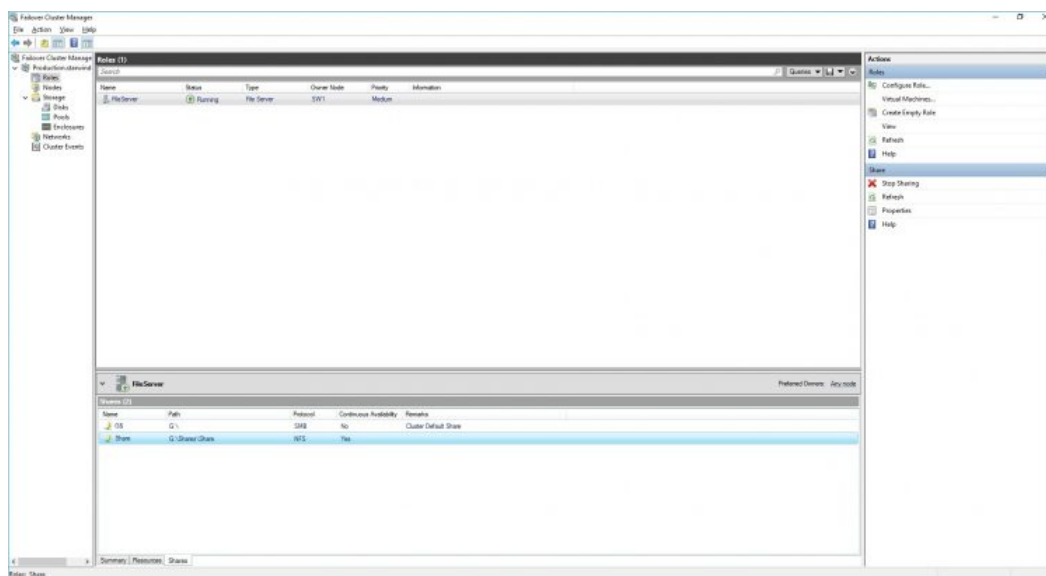


To manage created SMB File Shares

11. Open Failover Cluster Manager.

12. Expand the cluster and click Roles.

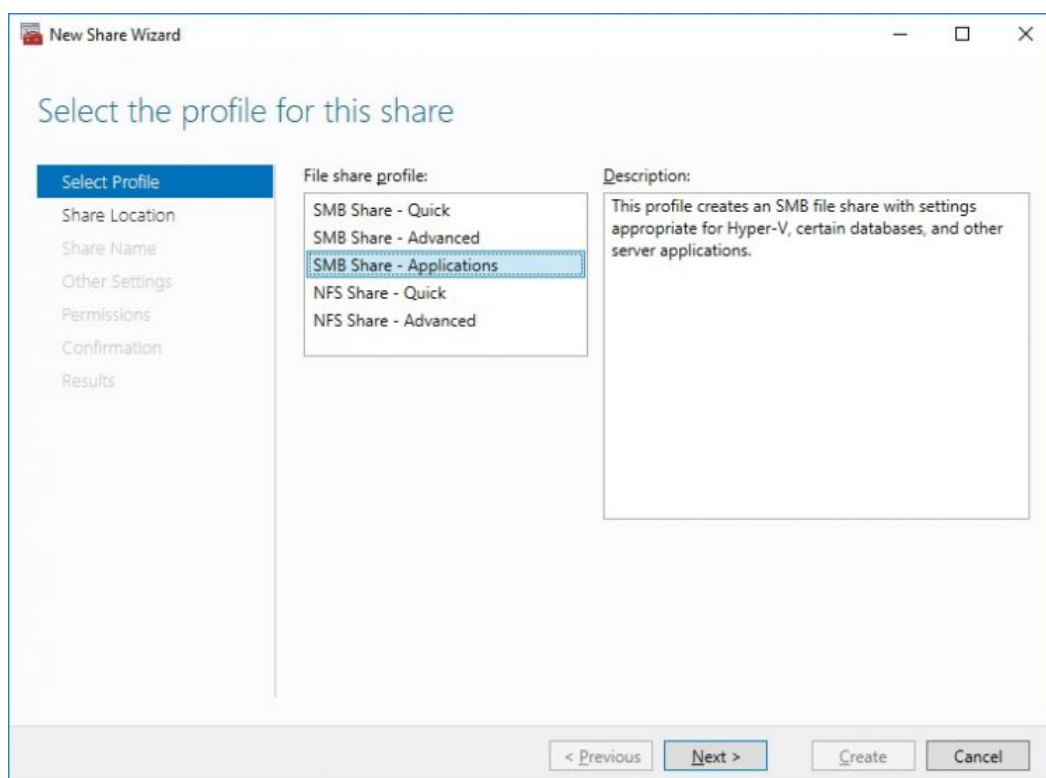
13. Choose the File Share role, select the Shares tab, right-click the created file share, and select Properties.



Configuring Nfs File Share

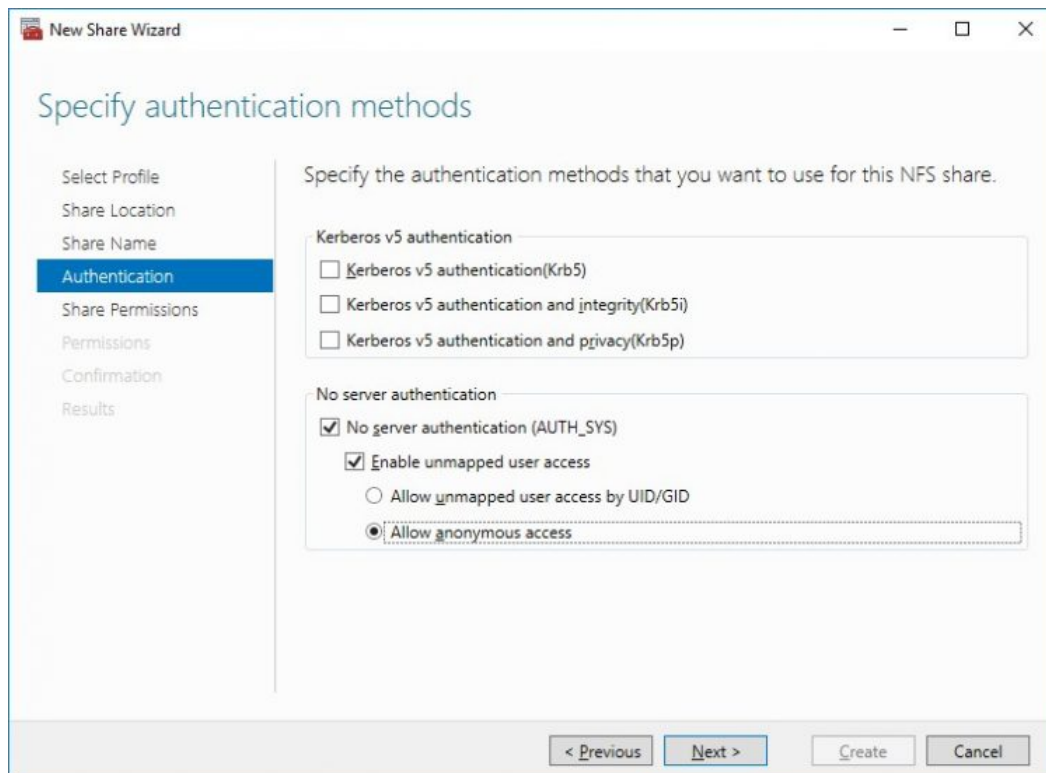
To Add NFS File Share

1. Open Failover Cluster Manager.
2. Expand the cluster and then click Roles.
3. Right-click the File Server role and then press Add File Share.
4. On the Select the profile for this share page, click NFS Share – Quick and then click Next.

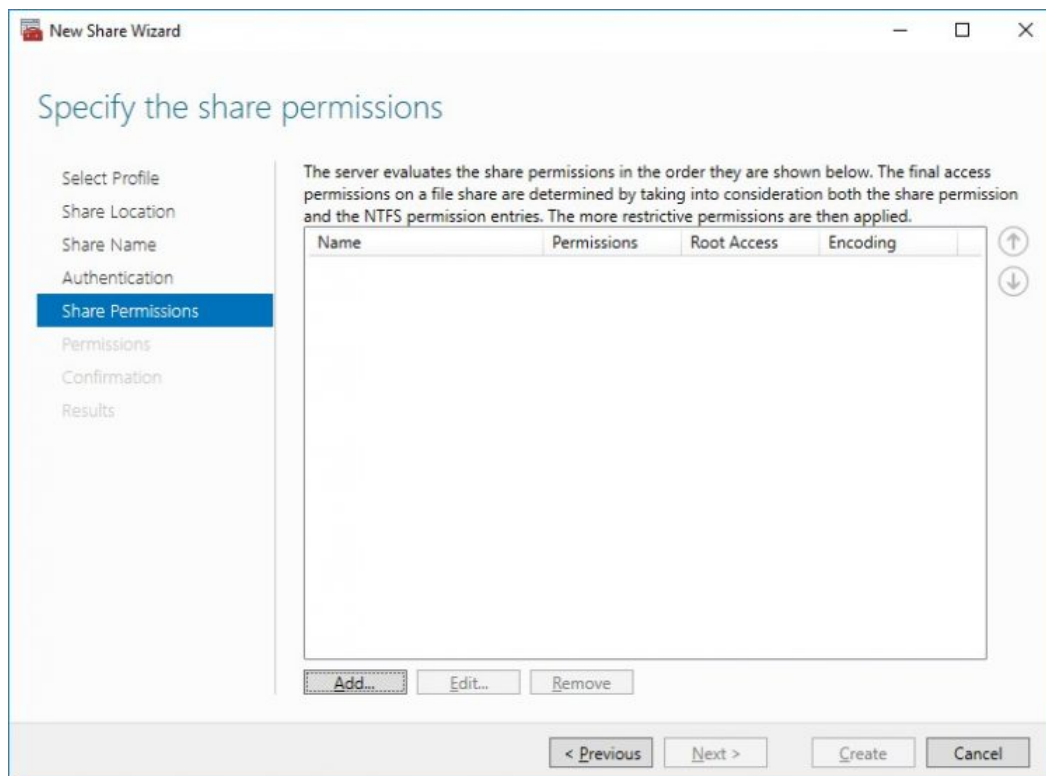


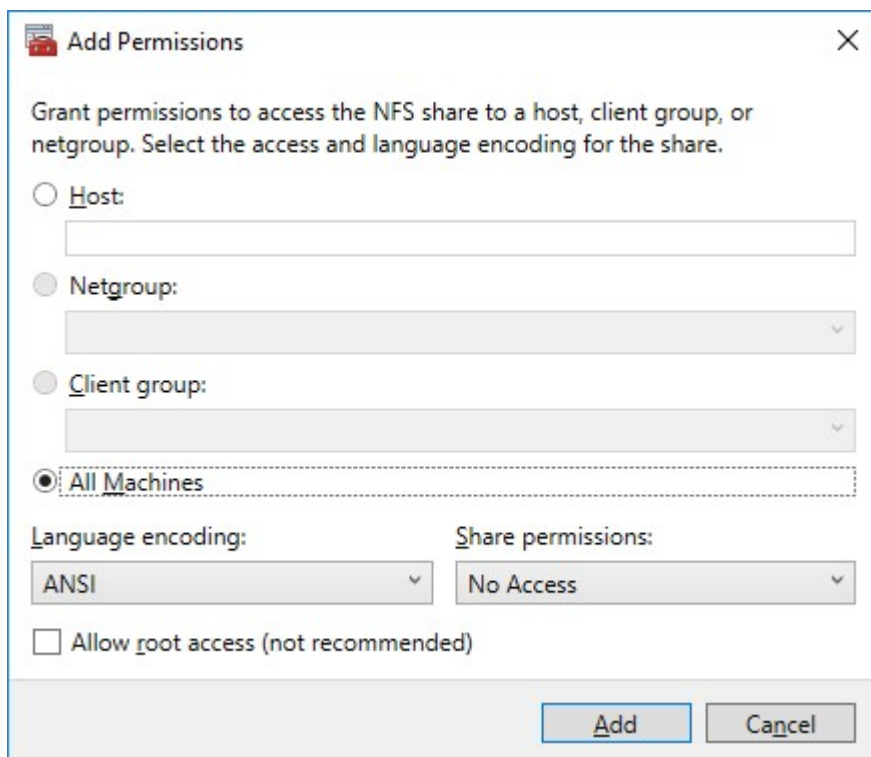
5. Select available storage to host the share. Click Next to continue.

continue.

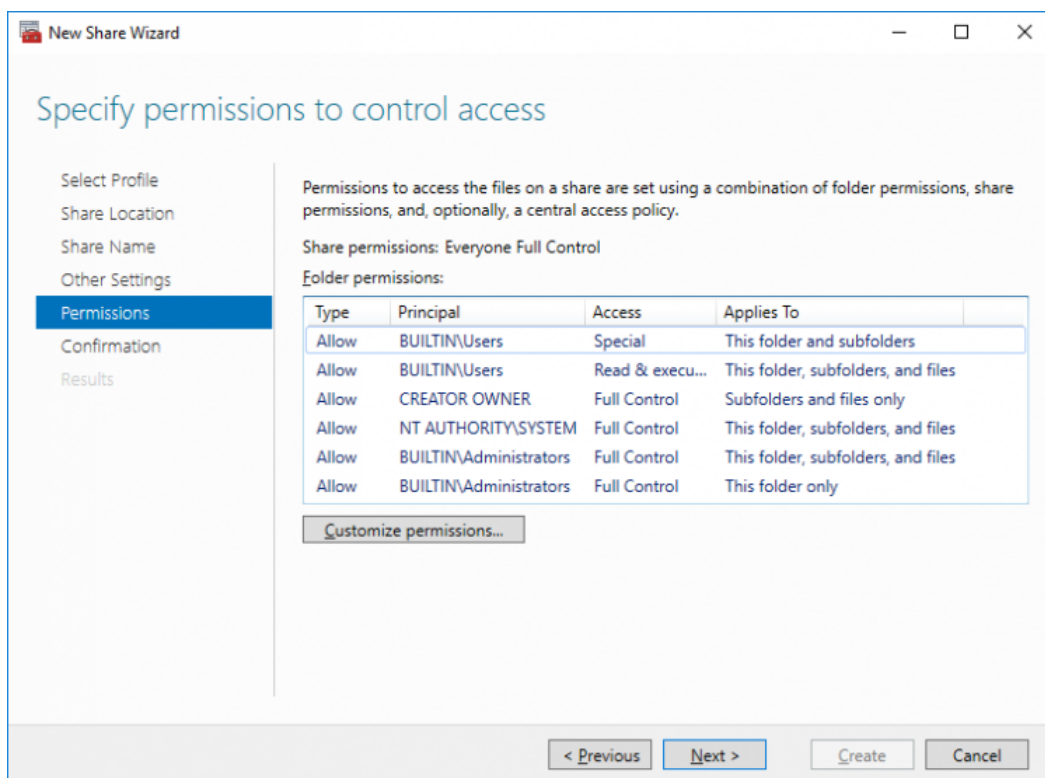


8. Click Add and specify Share Permissions.

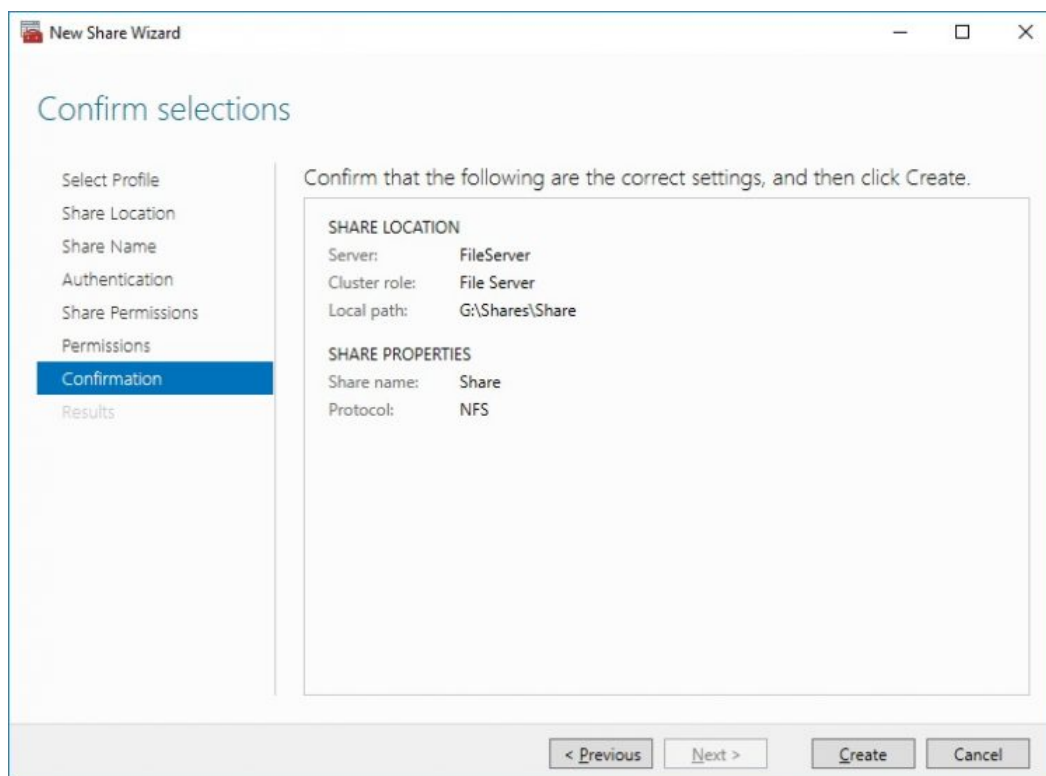




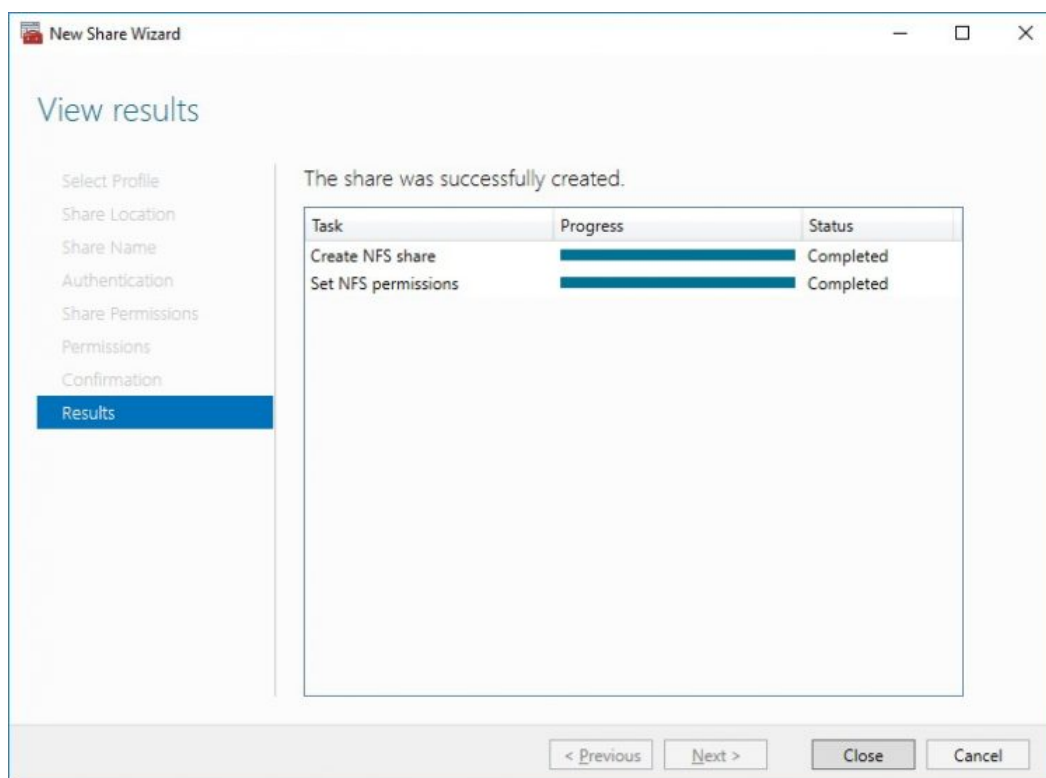
9. Specify the access permissions for the file share.



10. Check whether specified settings are correct. Click Previous to make any changes or click Create to continue.

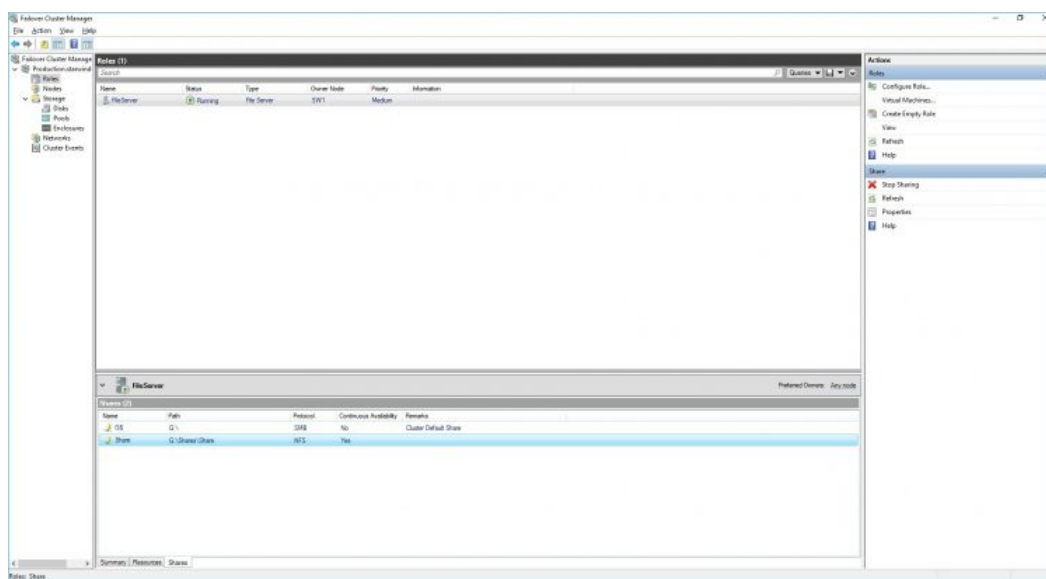


11. Check a summary and click Close to close the Wizard.



To manage created NFS File Shares:








- open Failover Cluster Manager
- expand the cluster and click Roles
- choose the File Share role, select the Shares tab, right-click the created file share, and select Properties



Conclusion

Following this guide, a 2-node Failover Cluster was deployed and configured with StarWind Virtual SAN (VSAN) running in a CVM on each host. As a result, a virtual shared storage “pool” accessible by all cluster nodes was created for storing highly available virtual machines.

Contacts

US Headquarters	EMEA and APAC
 +1 617 829 44 95	 +44 2037 691 857 (United Kingdom)
 +1 617 507 58 45	 +49 800 100 68 26 (Germany)
 +1 866 790 26 46	 +34 629 03 07 17 (Spain and Portugal)
	 +33 788 60 30 06 (France)

Customer Support Portal: <https://www.starwind.com/support>

Support Forum: <https://www.starwind.com/forums>

Sales: sales@starwind.com

General Information: info@starwind.com



StarWind Software, Inc. 100 Cummings Center Suite 224-C Beverly MA 01915, USA
www.starwind.com ©2024, StarWind Software Inc. All rights reserved.