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

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.

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

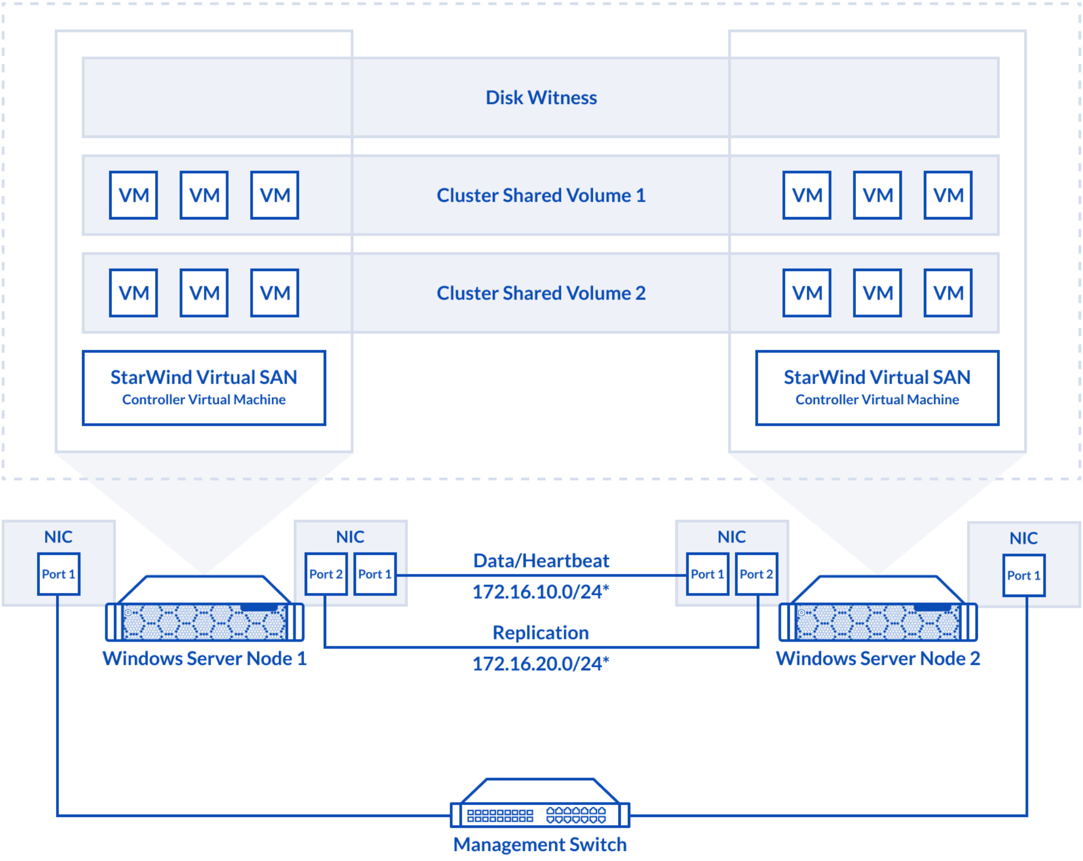
Prior to installing StarWind Virtual SAN, please make sure that the system meets the requirements, which are available via the following link:
https://www.starwindsoftware.com/system-requirements

Recommended RAID settings for HDD and SSD disks:
https://knowledgebase.starwindsoftware.com/guidance/recommended-raid-settings-for-hdd-and-ssd-disks/

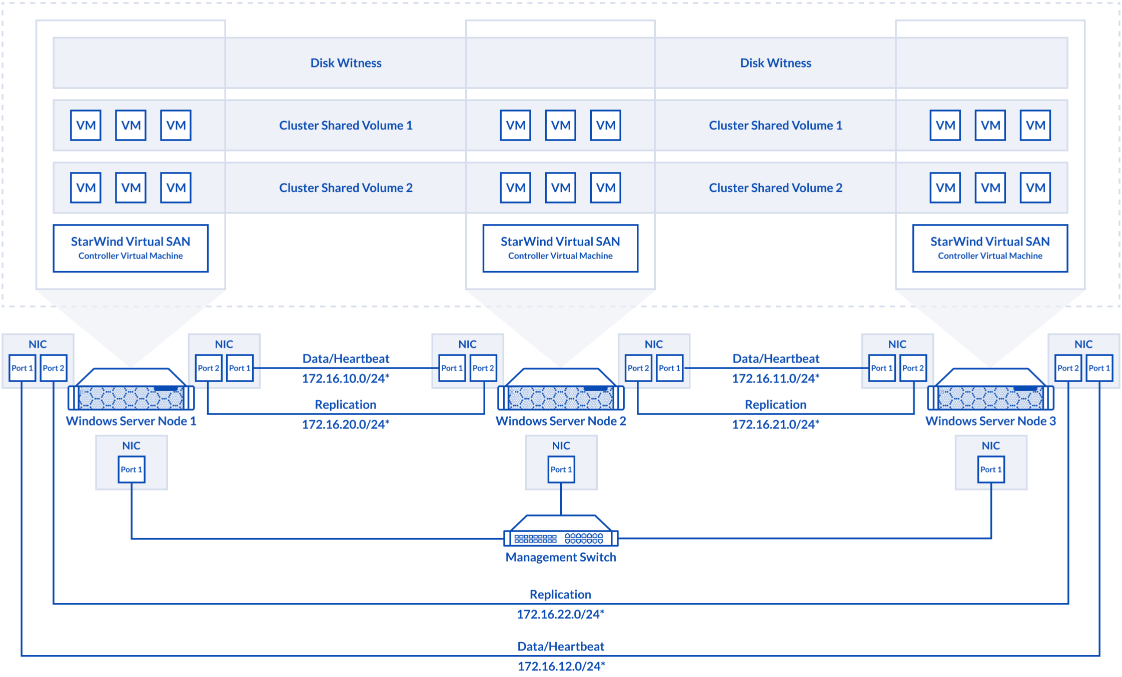
Please read StarWind Virtual SAN Best Practices document for additional information:
https://www.starwindsoftware.com/resource-library/starwind-virtual-san-best-practices

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.

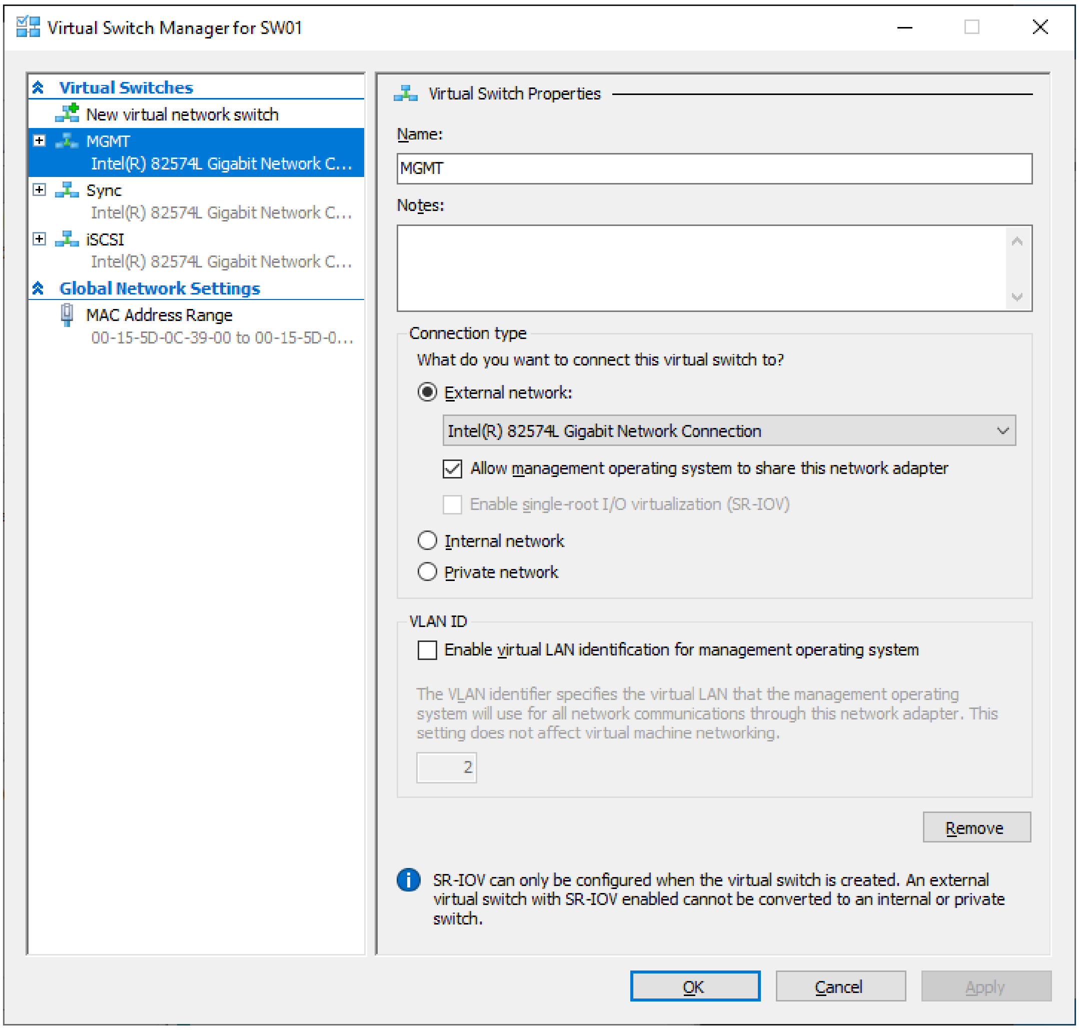
NOTE: Please follow the recommendation in KB article on how to place a DC in case of StarWind Virtual SAN usage.

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).



Virtual Switch Manager for SW01

Virtual Switches
- New virtual network switch
- MGMT – Intel(R) 82574L Gigabit Network C...
- Sync – Intel(R) 82574L Gigabit Network C...
- iSCSI – Intel(R) 82574L Gigabit Network C...

Global Network Settings
- MAC Address Range – 00-15-5D-0C-39-00 to 00-15-5D-0...

Virtual Switch Properties

Name: MGMT

Notes:

Connection type

What do you want to connect this virtual switch to?

● External network: Intel(R) 82574L Gigabit Network Connection

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

○ Internal network

○ Private network

VLAN ID

□ Enable virtual LAN identification for management operating system

The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.

2

SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

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”
}
```

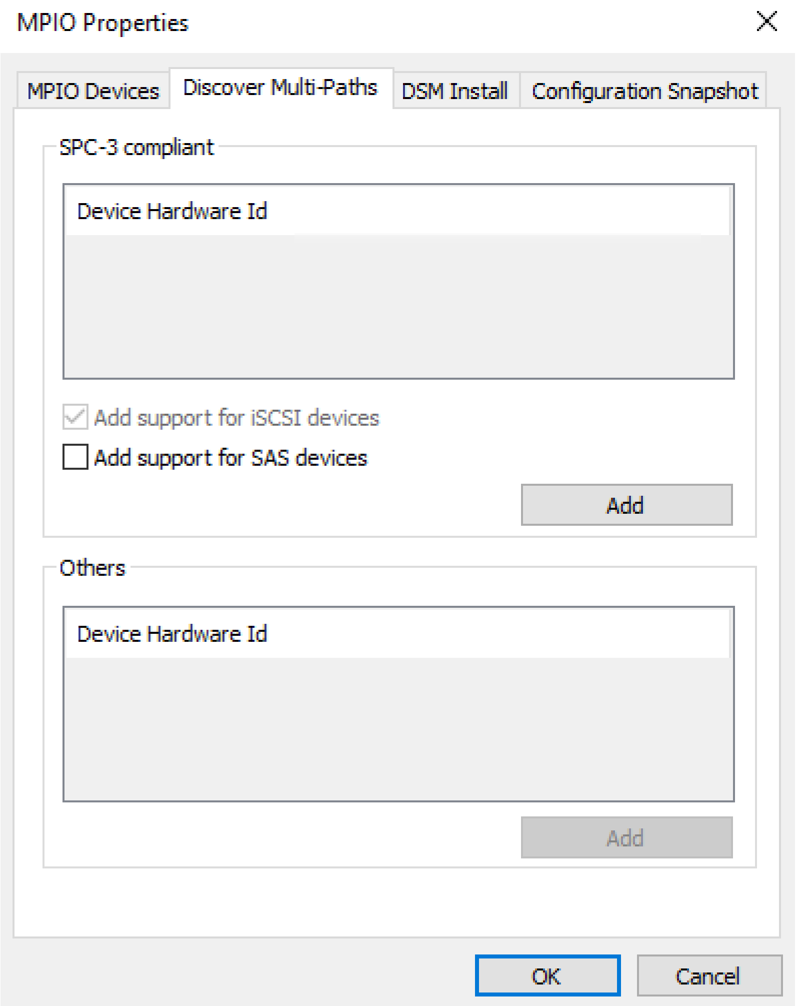
It will apply MTU 9000 to all iSCSI and Sync interfaces if they have iSCSI or Sync as part of their name.

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

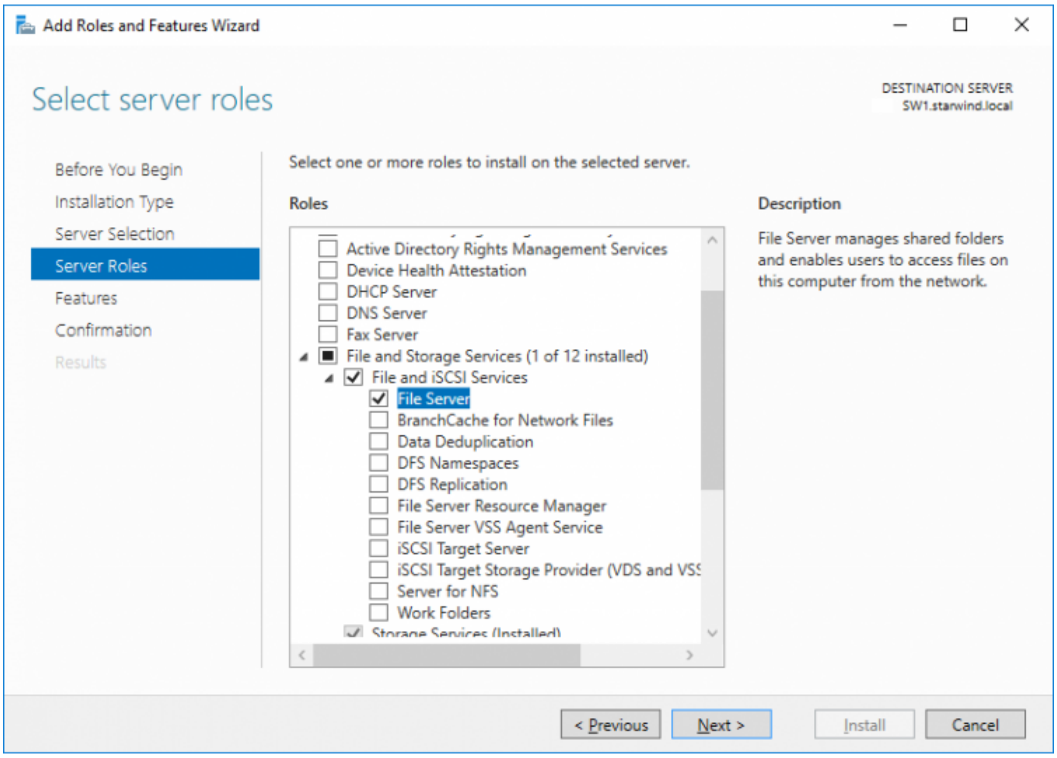
Scale-Out File Server (Sofs) For Application Data

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:



Select server roles

DESTINATION SERVER
SW1.starwind.local

Select one or more roles to install on the selected server.

Roles

☐ Active Directory Rights Management Services
☐ Device Health Attestation
☐ DHCP Server
☐ DNS Server
☐ Fax Server
■ File and Storage Services (1 of 12 installed)
  ☑ File and iSCSI Services
    ☑ File Server
    ☐ BranchCache for Network Files
    ☐ Data Deduplication
    ☐ DFS Namespaces
    ☐ DFS Replication
    ☐ File Server Resource Manager
    ☐ File Server VSS Agent Service
    ☐ iSCSI Target Server
    ☐ iSCSI Target Storage Provider (VDS and VSS
    ☐ Server for NFS
    ☐ Work Folders
  ☑ Storage Services (Installed)

Description

File Server manages shared folders and enables users to access files on this computer from the network.

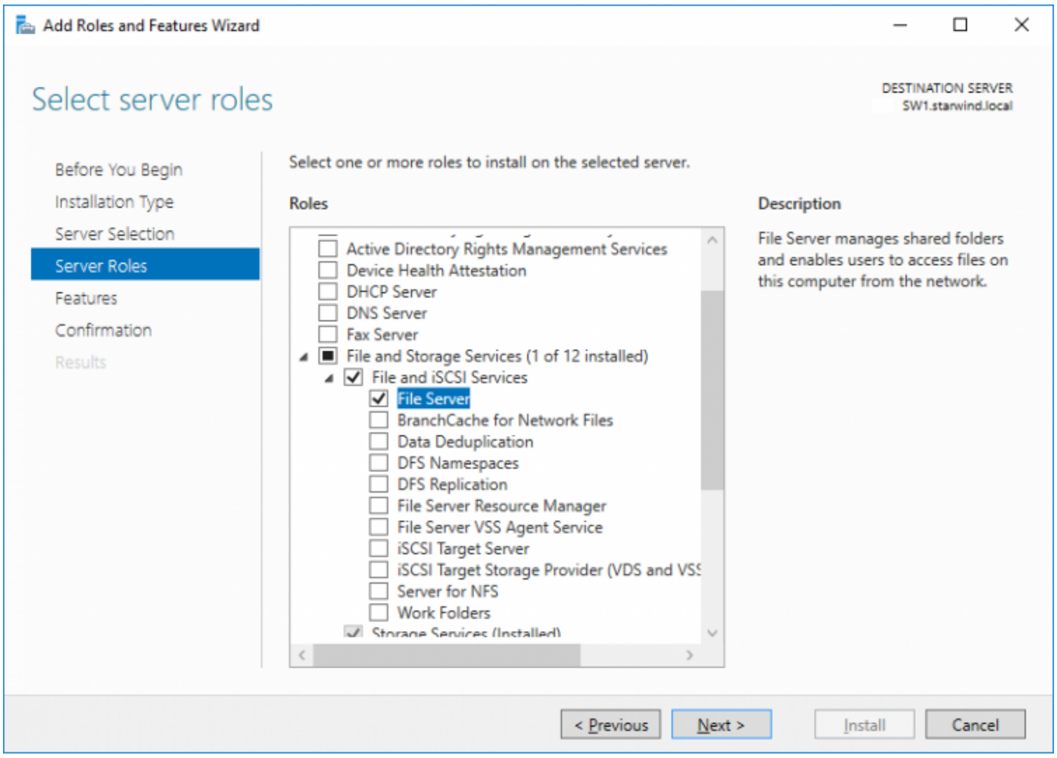
4. Restart the server after installation is completed and perform steps above on the each server.

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:


Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
SW1.starwind.local

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
  - ☑ File and iSCSI Services
    - ☑ File Server
    - □ BranchCache for Network Files
    - □ Data Deduplication
    - □ DFS Namespaces
    - □ DFS Replication
    - □ File Server Resource Manager
    - □ File Server VSS Agent Service
    - □ iSCSI Target Server
    - □ iSCSI Target Storage Provider (VDS and VSS
    - □ Server for NFS
    - □ Work Folders
  - ☑ Storage Services (Installed)

Description

File Server manages shared folders and enables users to access files on this computer from the network.

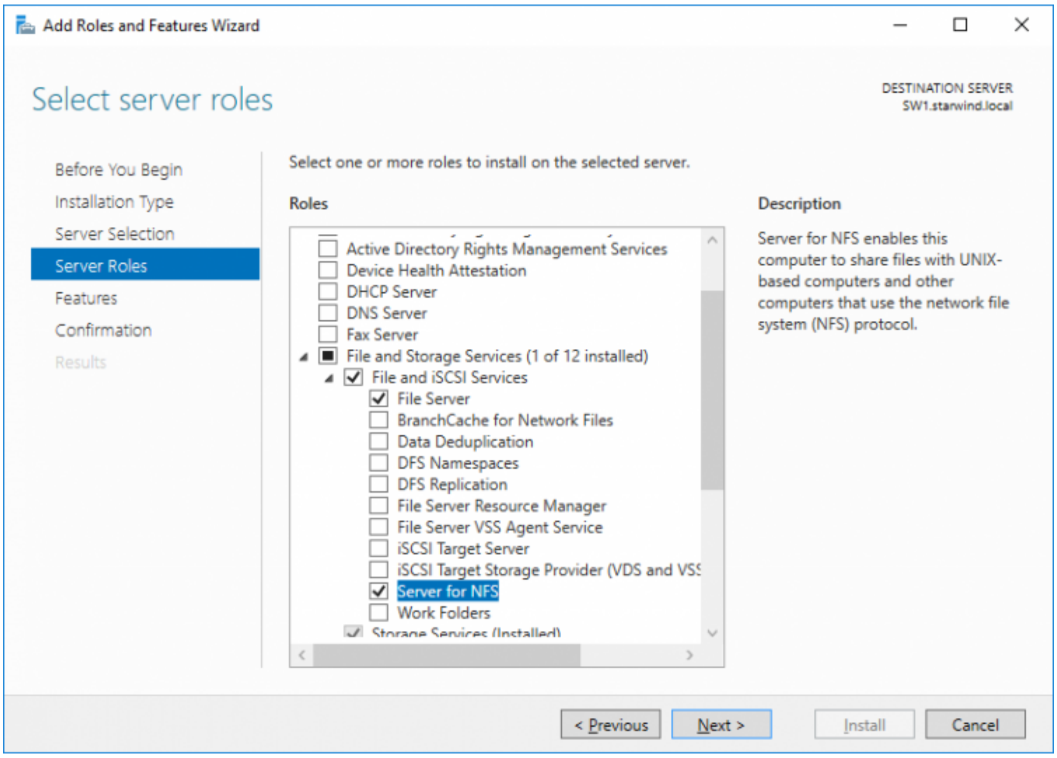
4. Restart the server after installation is completed and perform steps above on each server.

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:



Select server roles

DESTINATION SERVER
SW1.starwind.local

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
  - ☑ File and iSCSI Services
    - ☑ File Server
    - ☐ BranchCache for Network Files
    - ☐ Data Deduplication
    - ☐ DFS Namespaces
    - ☐ DFS Replication
    - ☐ File Server Resource Manager
    - ☐ File Server VSS Agent Service
    - ☐ iSCSI Target Server
    - ☐ iSCSI Target Storage Provider (VDS and VSS
    - ☑ Server for NFS
    - ☐ Work Folders
  - ☑ Storage Services (Installed)

Description

Server for NFS enables this computer to share files with UNIX-based computers and other computers that use the network file system (NFS) protocol.

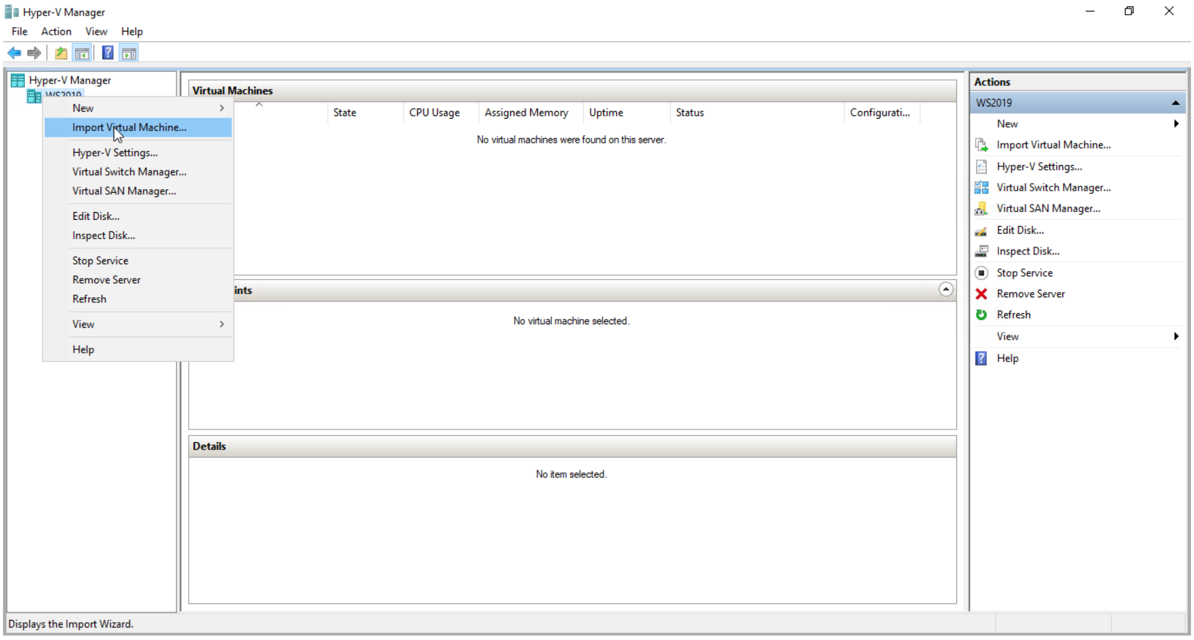
4. Restart the server after installation is completed and perform steps above on each server.

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.



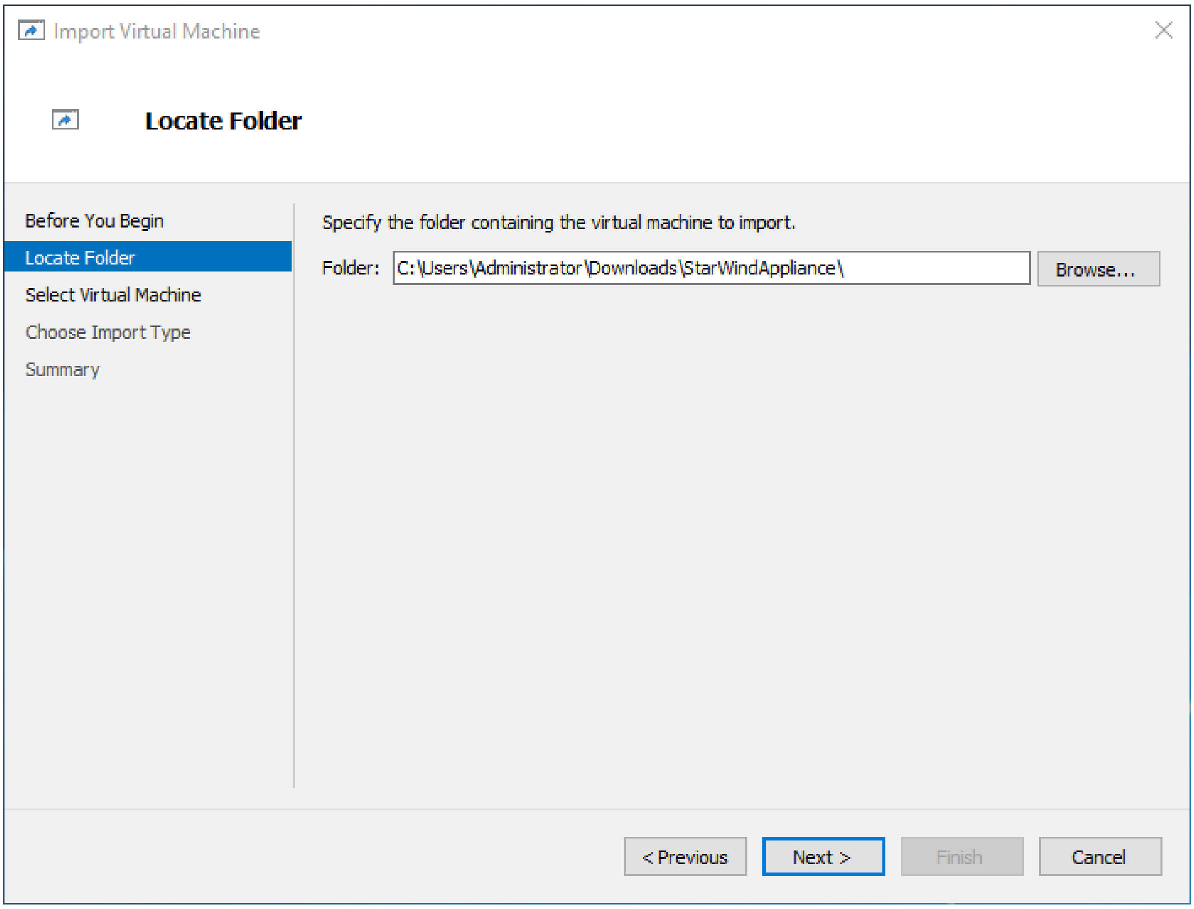
No virtual machines were found on this server.

No virtual machine selected.

No item selected.

Displays the Import Wizard.

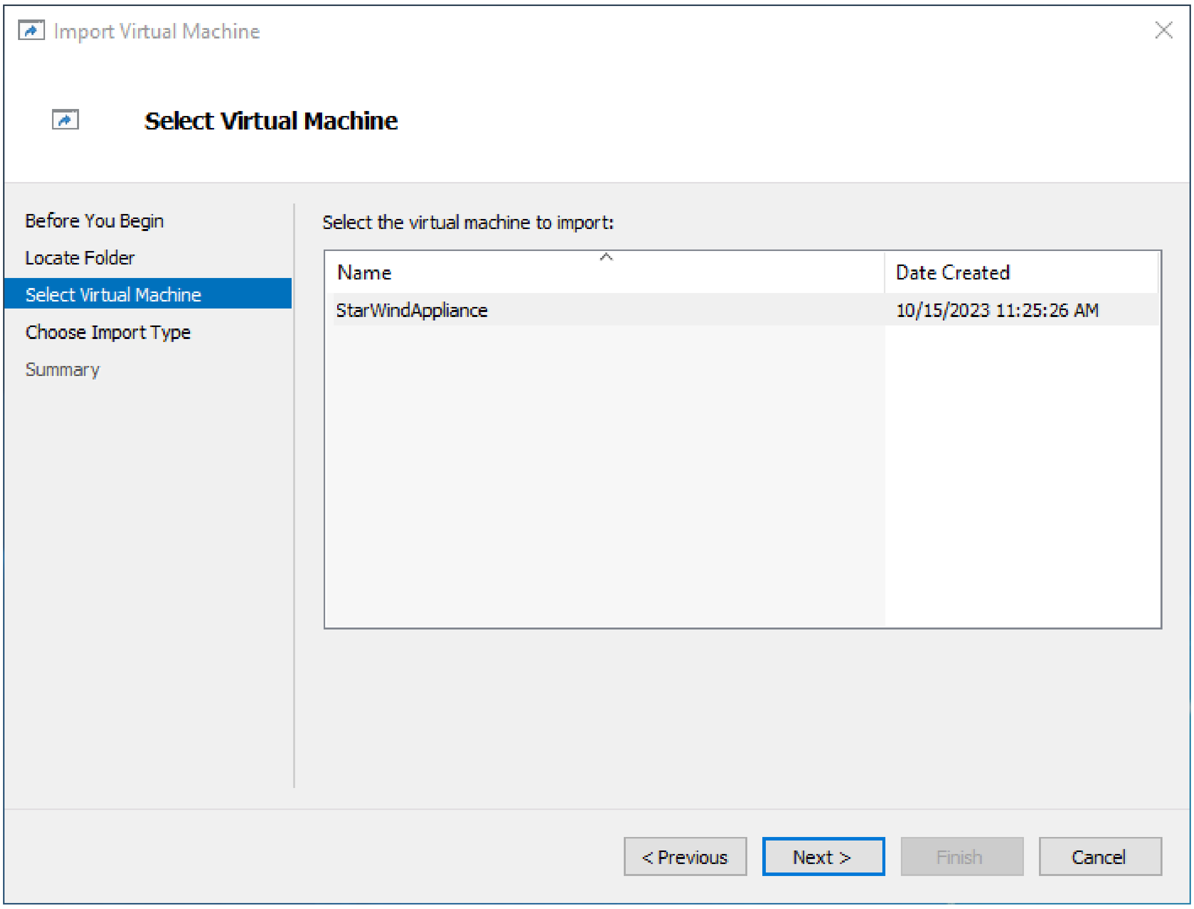
4. On the second page of the wizard, point to the location of the VM template. Select the VM folder and click Next.



Specify the folder containing the virtual machine to import.

Folder: C:\Users\Administrator\Downloads\StarWindAppliance\

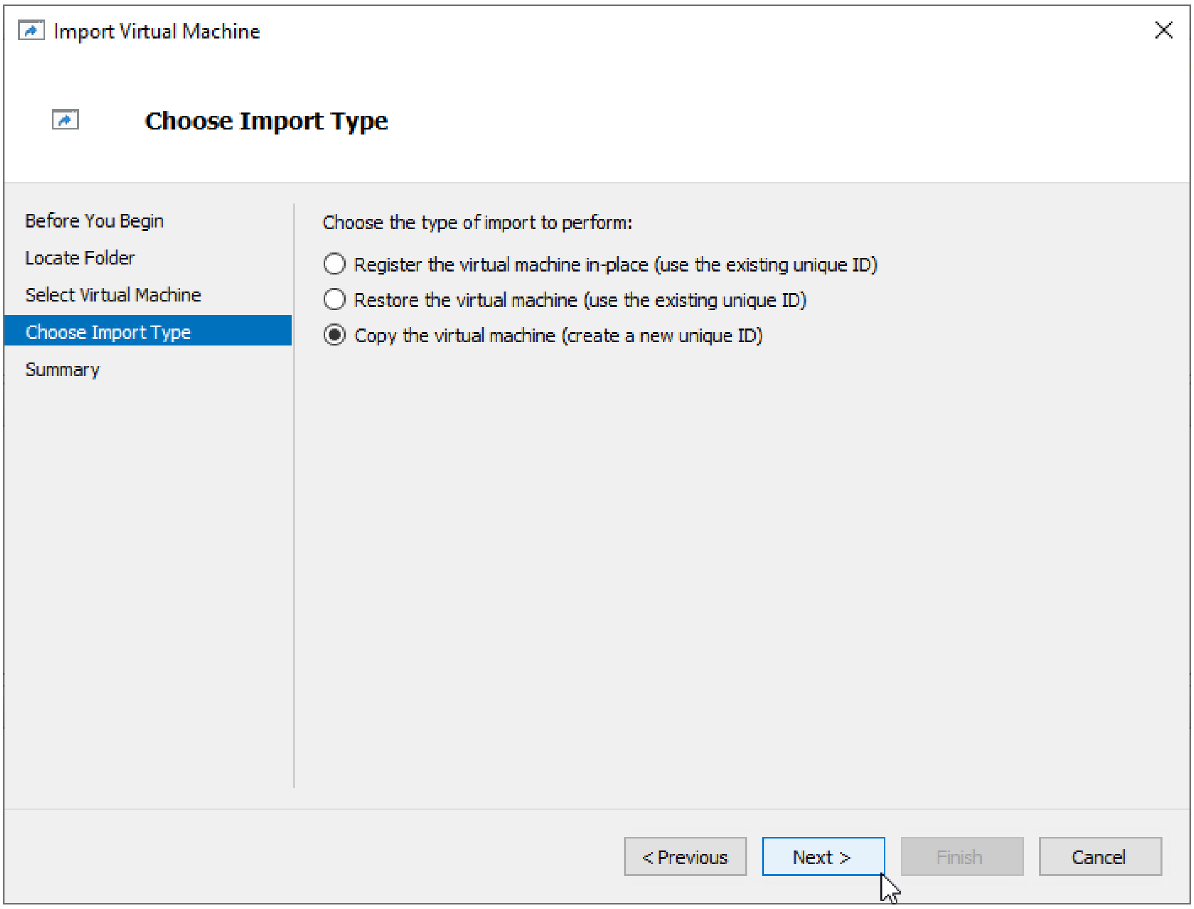
5. Click Next on the “Select Virtual Machine” step.



Select the virtual machine to import:

Name	Date Created
StarWindAppliance	10/15/2023 11:25:26 AM

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



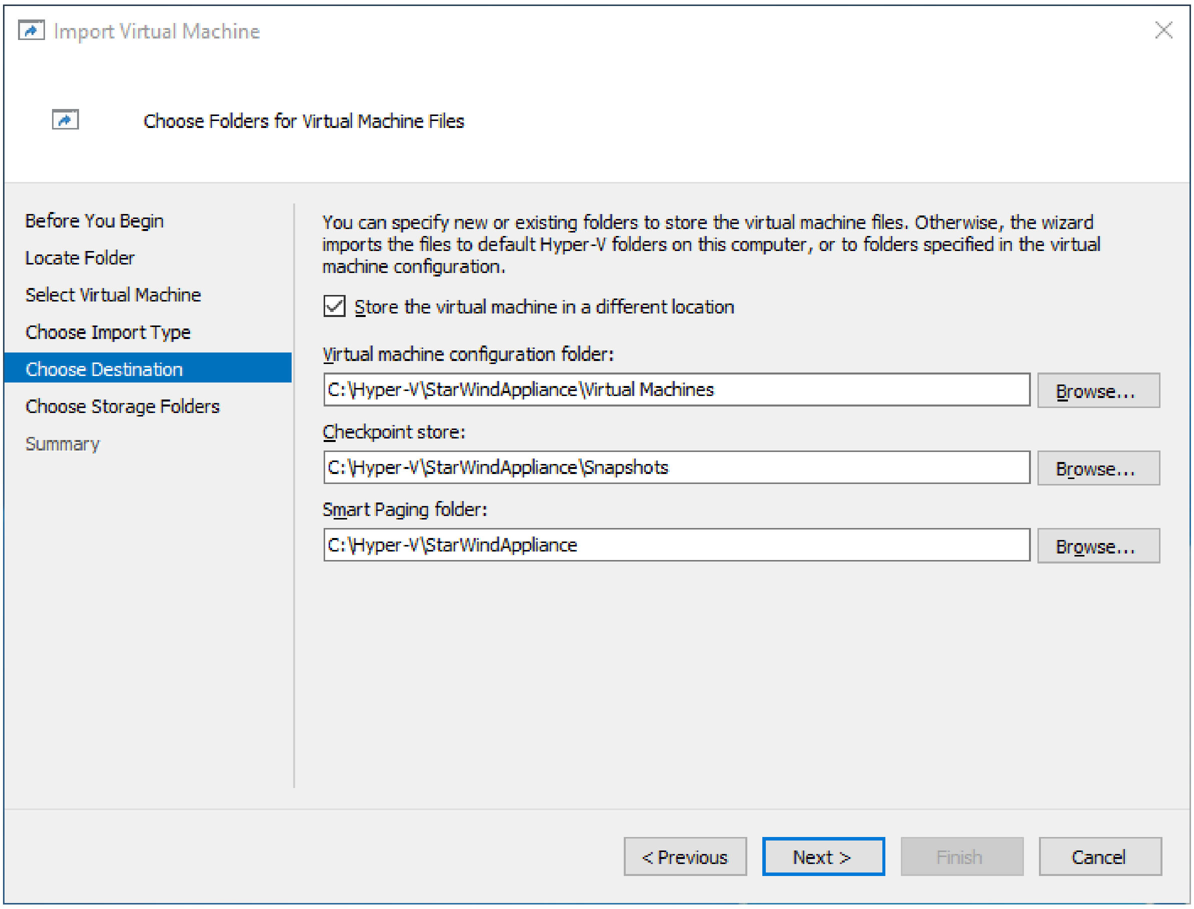
Import Virtual Machine

Choose Import Type

Choose the type of import to perform:

○ Register the virtual machine in-place (use the existing unique ID)
○ Restore the virtual machine (use the existing unique ID)
● Copy the virtual machine (create a new unique ID)

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



Import Virtual Machine

Choose Folders for Virtual Machine Files

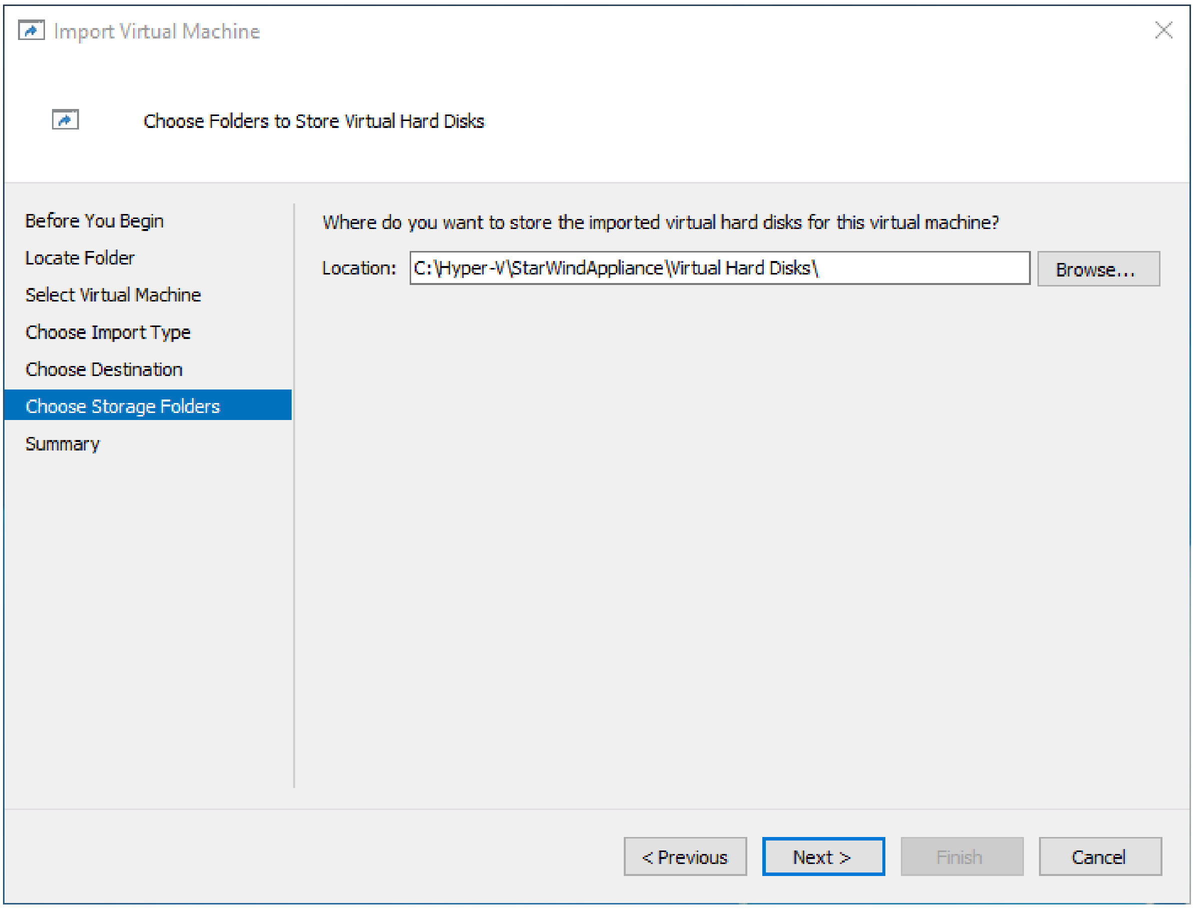
You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

☑ Store the virtual machine in a different location

Virtual machine configuration folder: C:\Hyper-V\StarWindAppliance\Virtual Machines

Checkpoint store: C:\Hyper-V\StarWindAppliance\Snapshots

Smart Paging folder: C:\Hyper-V\StarWindAppliance

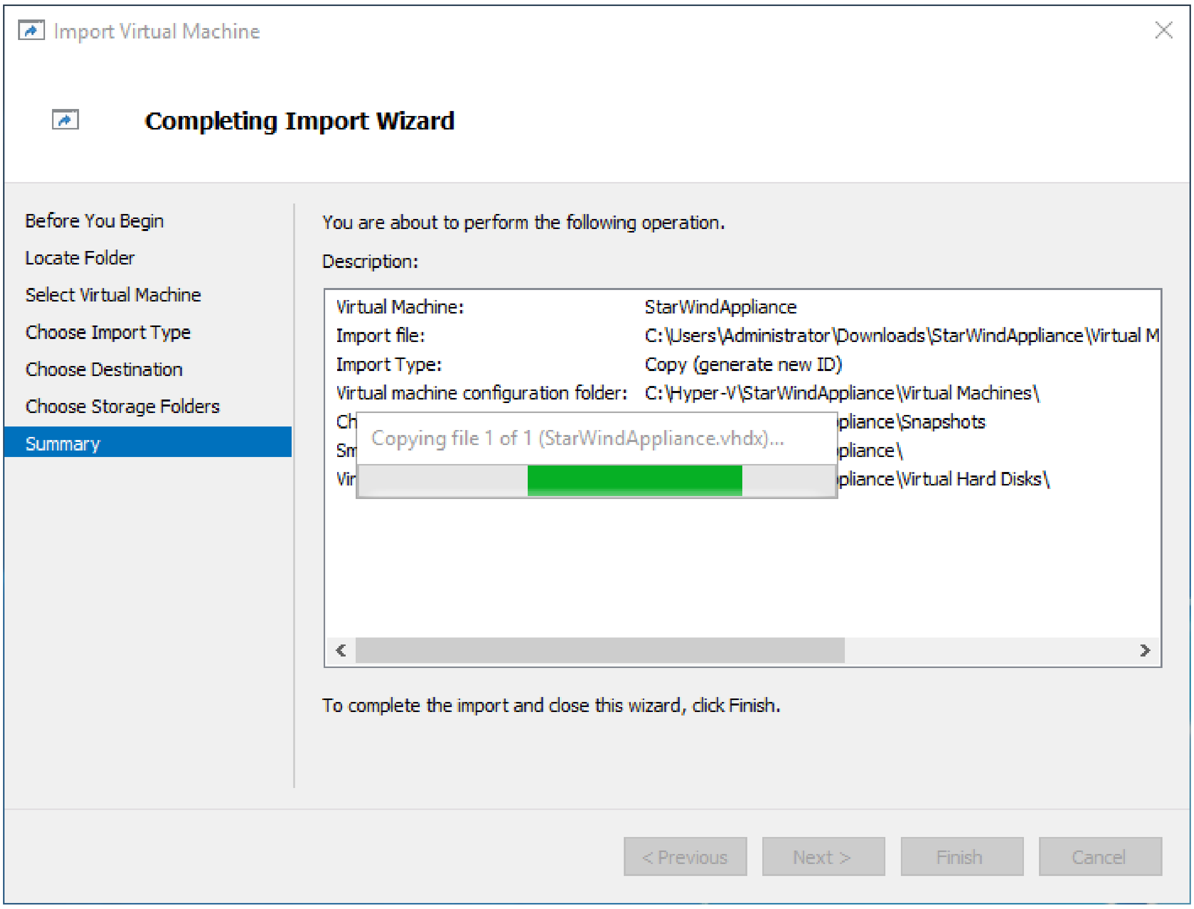


Import Virtual Machine

Choose Folders to Store Virtual Hard Disks

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

Location: C:\Hyper-V\StarWindAppliance\Virtual Hard Disks\



You are about to perform the following operation.

Description:

```
Virtual Machine:                        StarWindAppliance
Import file:                            C:\Users\Administrator\Downloads\StarWindAppliance\Virtual M
Import Type:                            Copy (generate new ID)
Virtual machine configuration folder:   C:\Hyper-V\StarWindAppliance\Virtual Machines\
Ch                                      pliance\Snapshots
Sm                                      pliance\
Vir                                     pliance\Virtual Hard Disks\
```

Copying file 1 of 1 (StarWindAppliance.vhdx)...

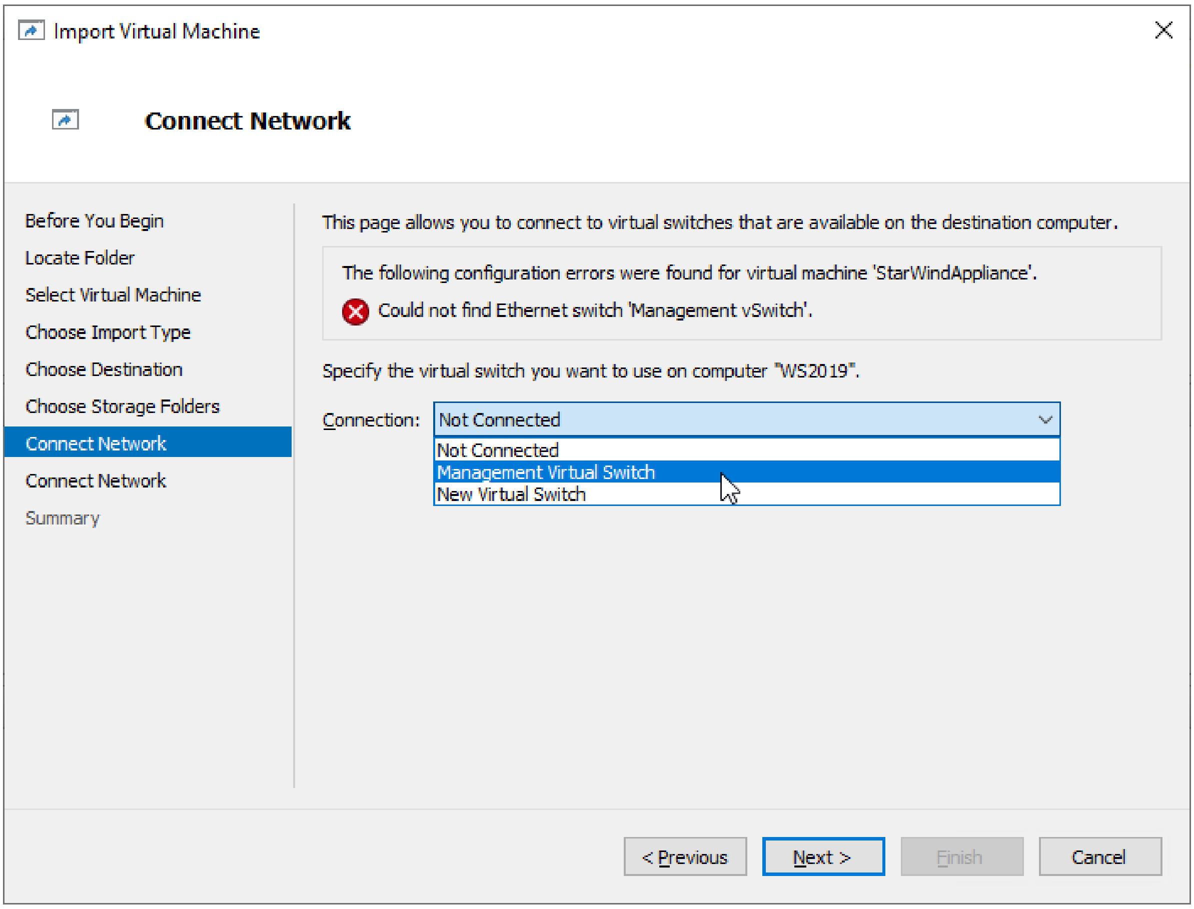
To complete the import and close this wizard, click Finish.

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.



Import Virtual Machine

Connect Network

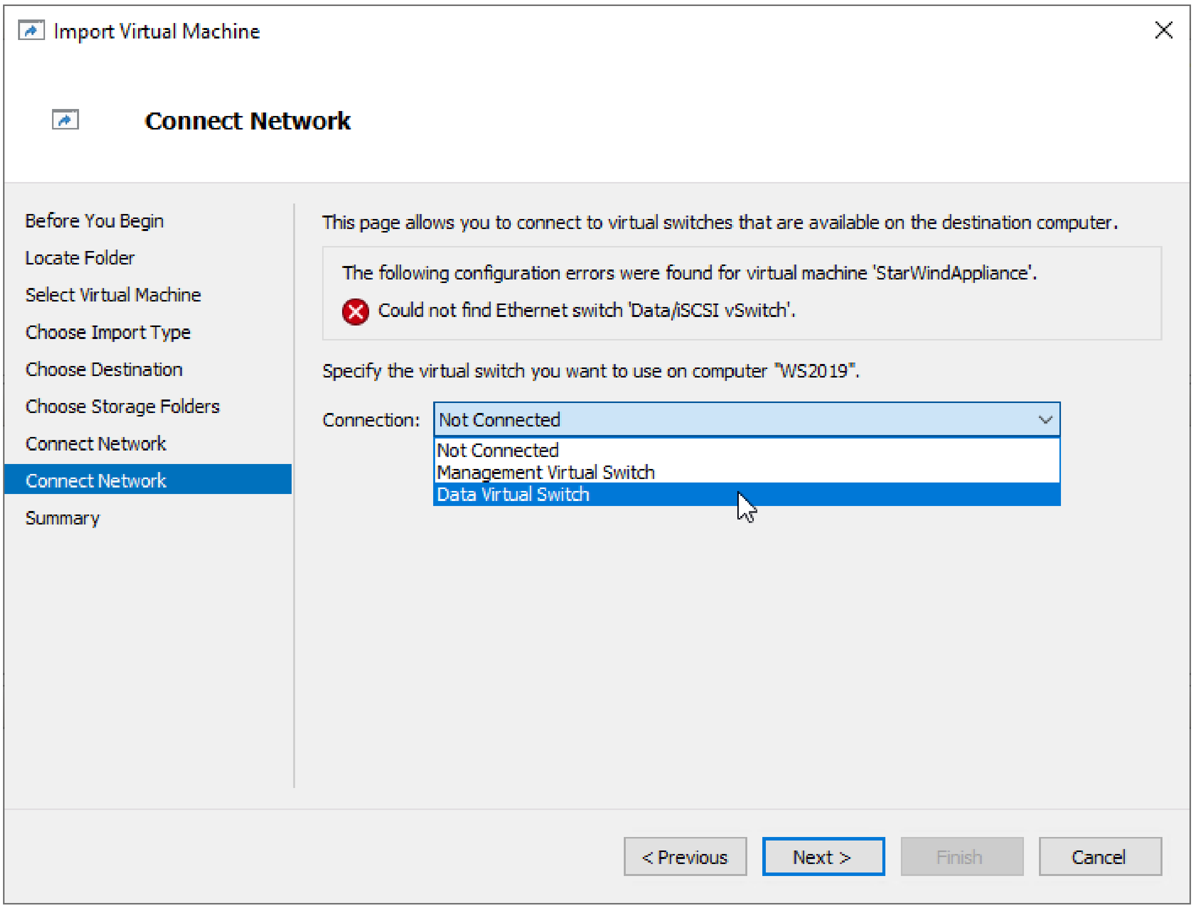
This page allows you to connect to virtual switches that are available on the destination computer.

The following configuration errors were found for virtual machine 'StarWindAppliance'.

Could not find Ethernet switch 'Management vSwitch'.

Specify the virtual switch you want to use on computer "WS2019".

Connection: Not Connected



Import Virtual Machine

Connect Network

This page allows you to connect to virtual switches that are available on the destination computer.

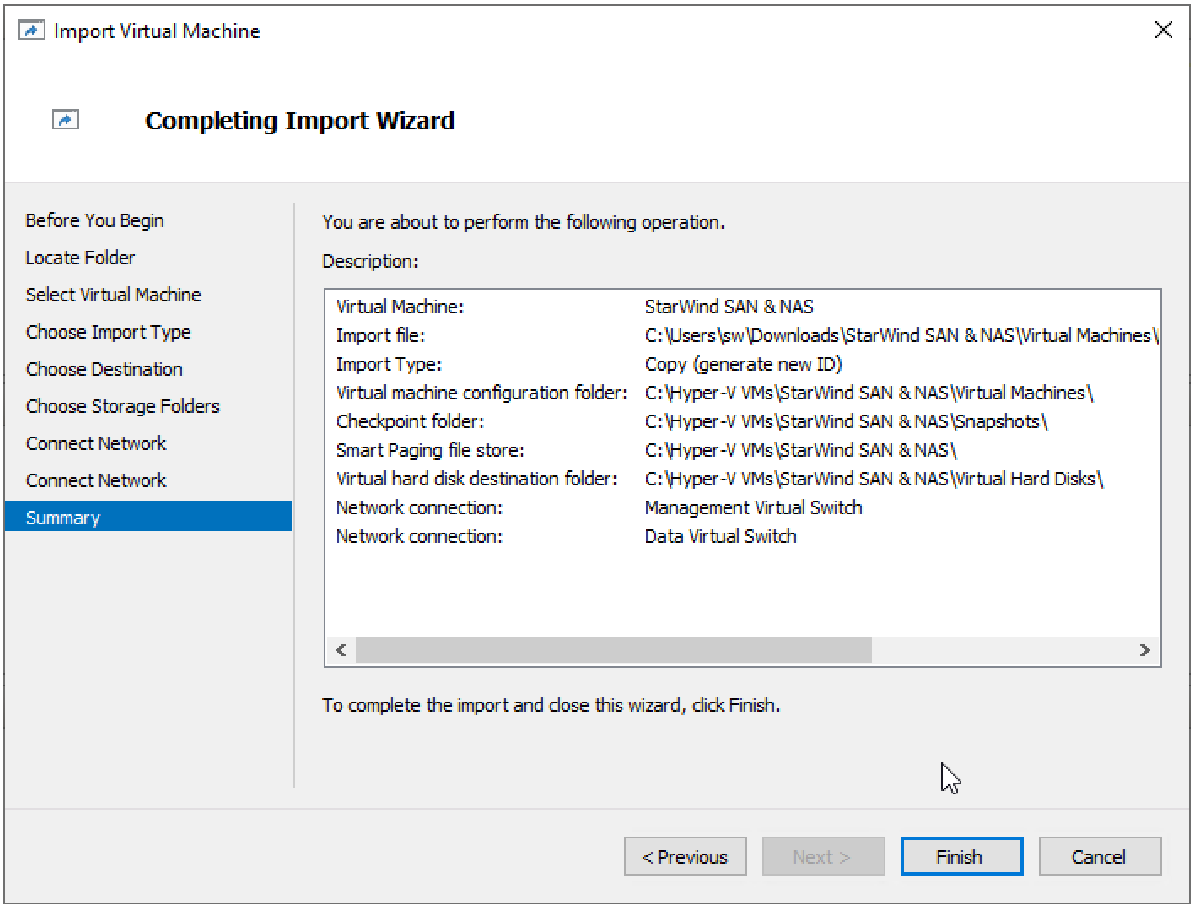
The following configuration errors were found for virtual machine 'StarWindAppliance'.

Could not find Ethernet switch 'Data/iSCSI vSwitch'.

Specify the virtual switch you want to use on computer "WS2019".

Connection: Not Connected

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



You are about to perform the following operation.

Description:

Virtual Machine:	StarWind SAN & NAS
Import file:	C:\Users\sw\Downloads\StarWind SAN & NAS\Virtual Machines\
Import Type:	Copy (generate new ID)
Virtual machine configuration folder:	C:\Hyper-V VMs\StarWind SAN & NAS\Virtual Machines\
Checkpoint folder:	C:\Hyper-V VMs\StarWind SAN & NAS\Snapshots\
Smart Paging file store:	C:\Hyper-V VMs\StarWind SAN & NAS\
Virtual hard disk destination folder:	C:\Hyper-V VMs\StarWind SAN & NAS\Virtual Hard Disks\
Network connection:	Management Virtual Switch
Network connection:	Data Virtual Switch

To complete the import and close this wizard, click Finish.

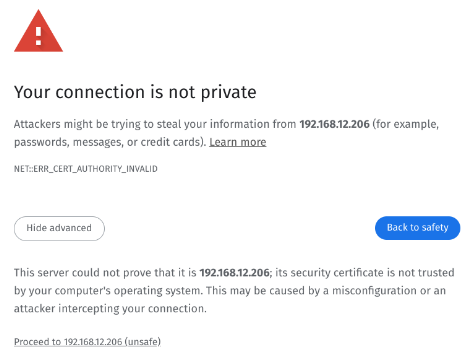
10. Repeat the VM deployment on each partner server which is used for configuring 2-node or 3-node highly available storage according to your licensing.

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

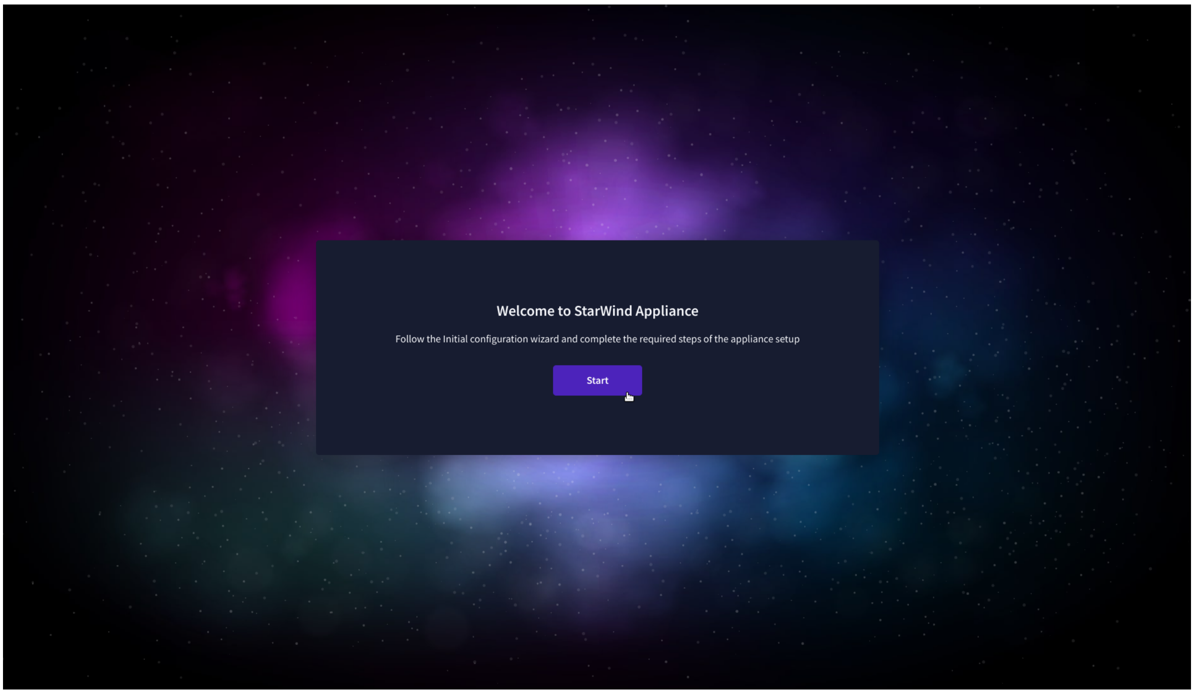
Attackers might be trying to steal your information from **192.168.12.206** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

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)

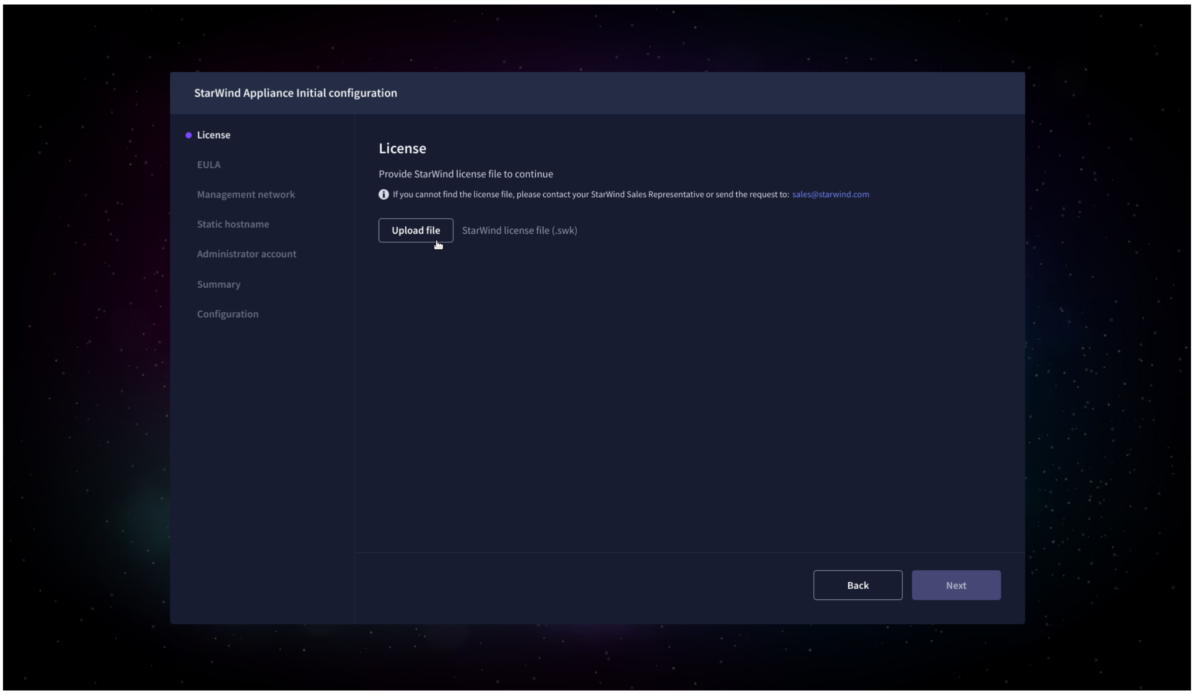
4. StarWind VSAN web UI welcomes you, and the “Initial Configuration” wizard will guide you through the deployment process.



Welcome to StarWind Appliance

Follow the Initial configuration wizard and complete the required steps of the appliance setup

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



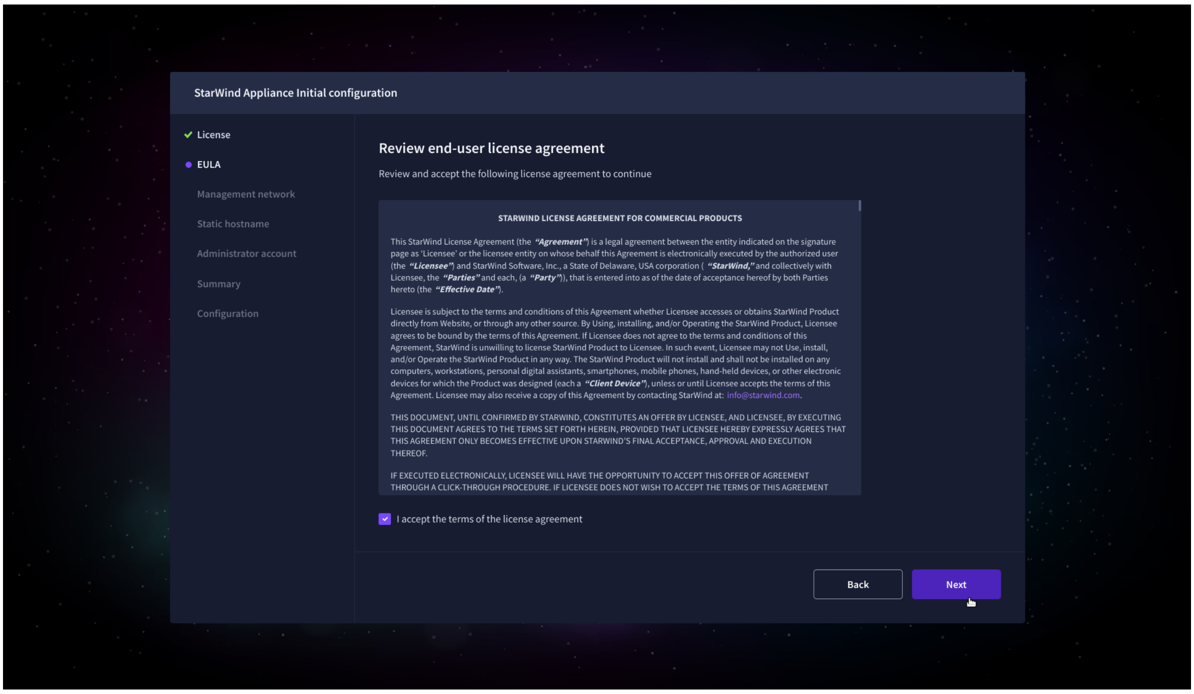
StarWind Appliance Initial configuration

License

Provide StarWind license file to continue

If you cannot find the license file, please contact your StarWind Sales Representative or send the request to: sales@starwind.com

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



StarWind Appliance Initial configuration

Review end-user license agreement

Review and accept the following license agreement to continue

STARWIND LICENSE AGREEMENT FOR COMMERCIAL PRODUCTS

This StarWind License Agreement (the ***"Agreement"***) is a legal agreement between the entity indicated on the signature page as 'Licensee' or the licensee entity on whose behalf this Agreement is electronically executed by the authorized user (the ***"Licensee"***) and StarWind Software, Inc., a State of Delaware, USA corporation (***"StarWind,"*** and collectively with Licensee, the ***"Parties"*** and each, (a ***"Party"***)), that is entered into as of the date of acceptance hereof by both Parties hereto (the ***"Effective Date"***).

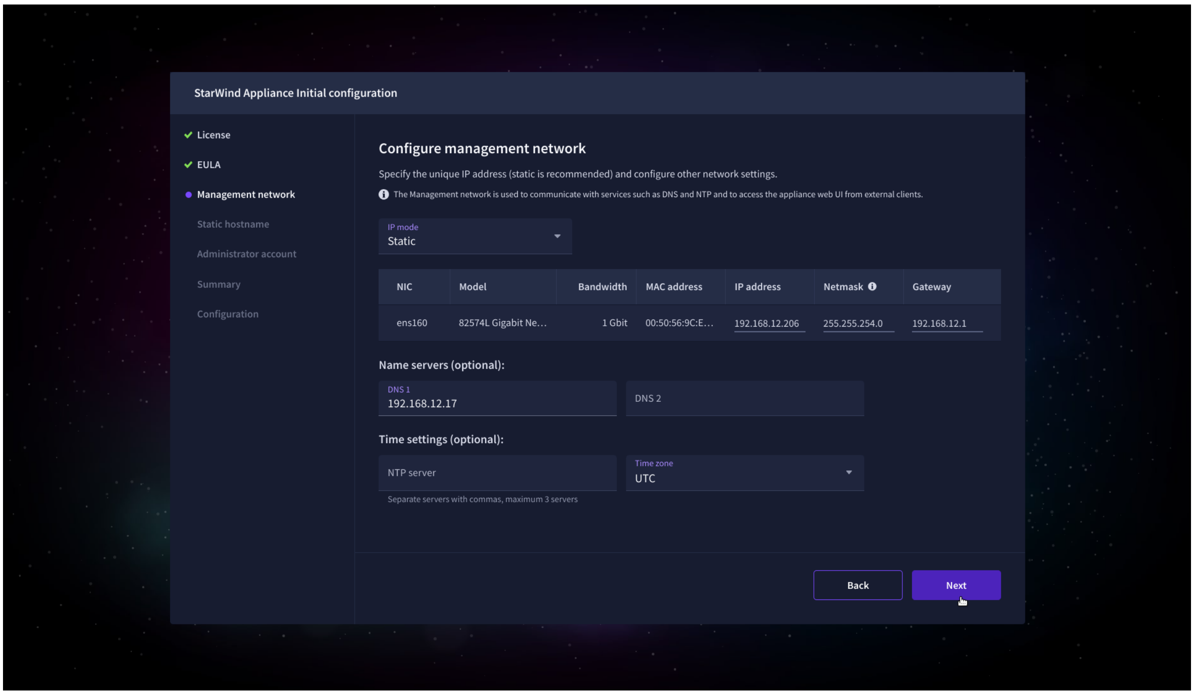
Licensee is subject to the terms and conditions of this Agreement whether Licensee accesses or obtains StarWind Product directly from Website, or through any other source. By Using, installing, and/or Operating the StarWind Product, Licensee agrees to be bound by the terms of this Agreement. If Licensee does not agree to the terms and conditions of this Agreement, StarWind is unwilling to license StarWind Product to Licensee. In such event, Licensee may not Use, install, and/or Operate the StarWind Product in any way. The StarWind Product will not install and shall not be installed on any computers, workstations, personal digital assistants, smartphones, mobile phones, hand-held devices, or other electronic devices for which the Product was designed (each a ***"Client Device"***), unless or until Licensee accepts the terms of this Agreement. Licensee may also receive a copy of this Agreement by contacting StarWind at: info@starwind.com.

THIS DOCUMENT, UNTIL CONFIRMED BY STARWIND, CONSTITUTES AN OFFER BY LICENSEE, AND LICENSEE, BY EXECUTING THIS DOCUMENT AGREES TO THE TERMS SET FORTH HEREIN, PROVIDED THAT LICENSEE HEREBY EXPRESSLY AGREES THAT THIS AGREEMENT ONLY BECOMES EFFECTIVE UPON STARWIND'S FINAL ACCEPTANCE, APPROVAL AND EXECUTION THEREOF.

IF EXECUTED ELECTRONICALLY, LICENSEE WILL HAVE THE OPPORTUNITY TO ACCEPT THIS OFFER OF AGREEMENT THROUGH A CLICK-THROUGH PROCEDURE. IF LICENSEE DOES NOT WISH TO ACCEPT THE TERMS OF THIS AGREEMENT

☑ I accept the terms of the license agreement

7. Review or edit the Network settings and click Next.
NOTE: Static network settings are recommended for the configuration.



Configure management network

Specify the unique IP address (static is recommended) and configure other network settings.

ℹ The Management network is used to communicate with services such as DNS and NTP and to access the appliance web UI from external clients.

IP mode: Static

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

Name servers (optional):

DNS 1: 192.168.12.17

DNS 2

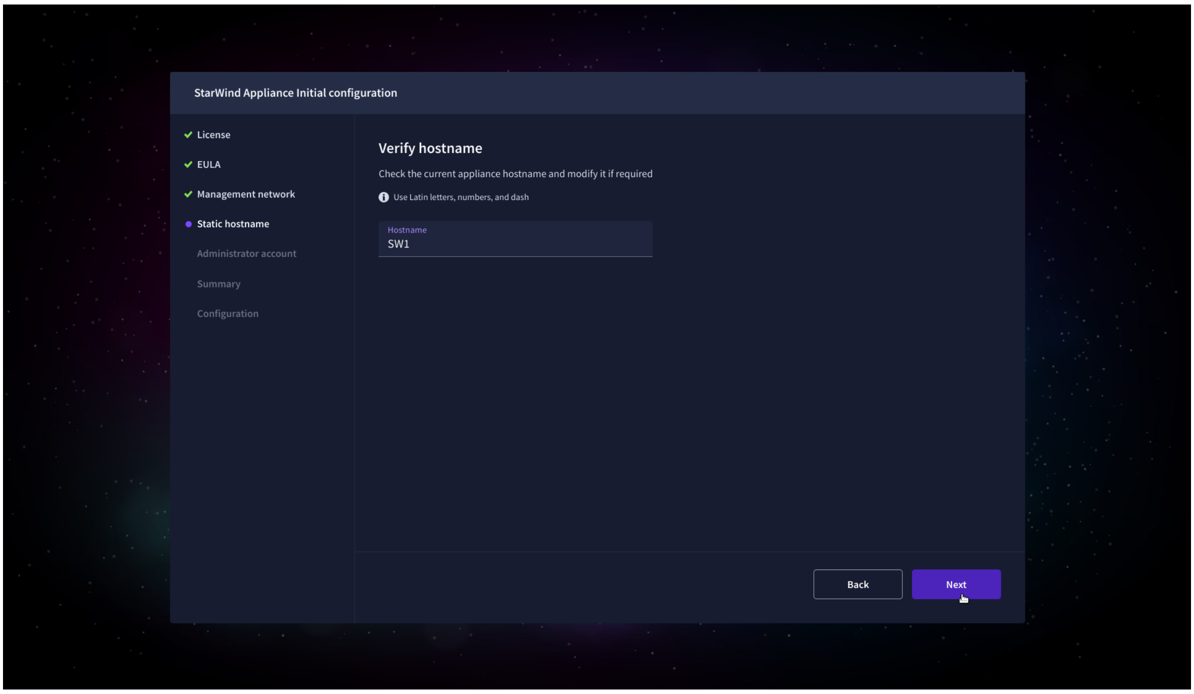
Time settings (optional):

NTP server

Separate servers with commas, maximum 3 servers

Time zone: UTC

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



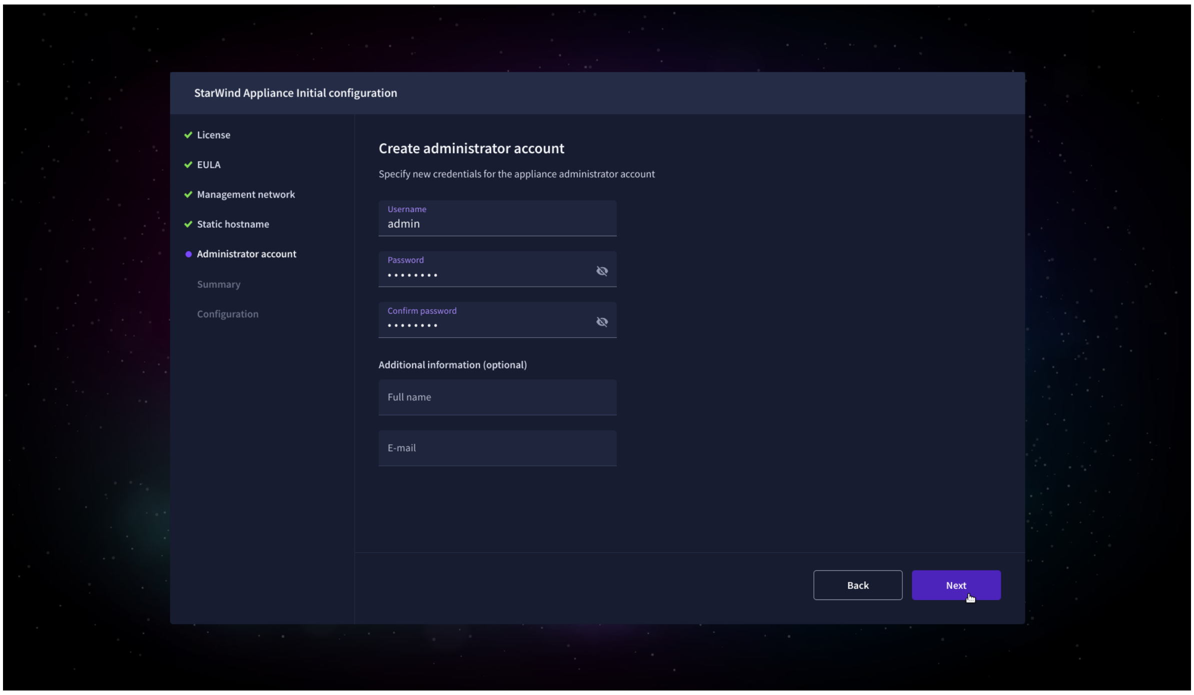
Verify hostname

Check the current appliance hostname and modify it if required

ℹ Use Latin letters, numbers, and dash

Hostname: SW1

9. Create an administrator account. Click Next.



StarWind Appliance Initial configuration

Create administrator account

Specify new credentials for the appliance administrator account

Username: admin

Password: ••••••••

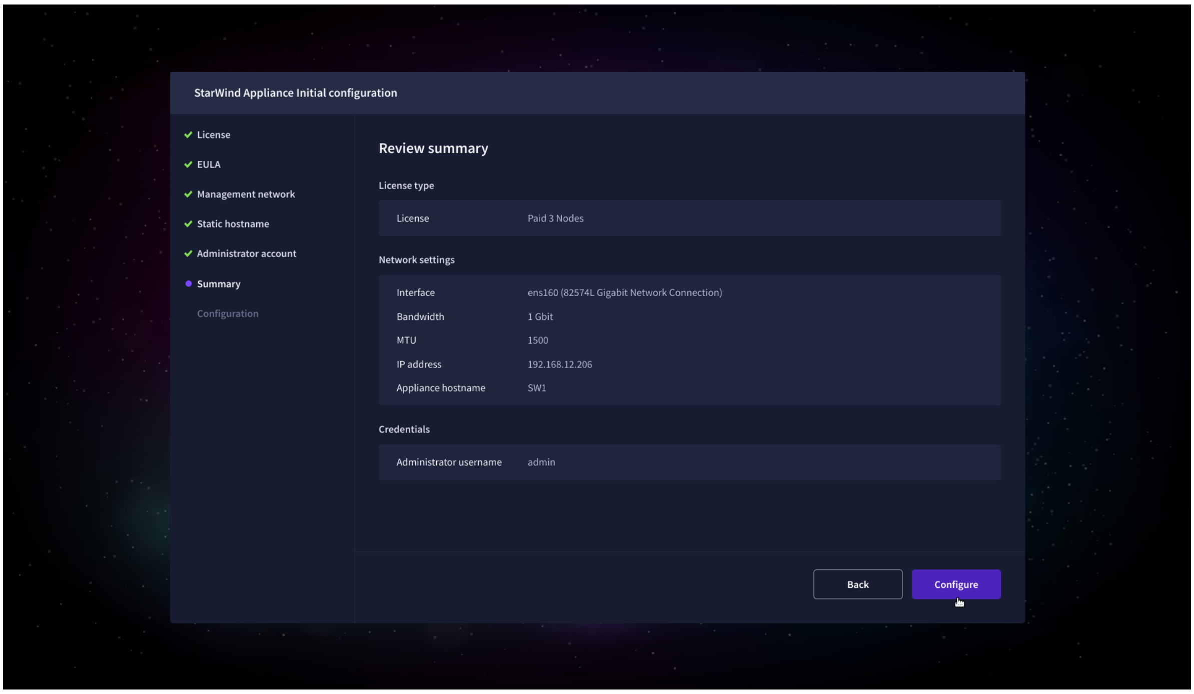
Confirm password: ••••••••

Additional information (optional)

Full name

E-mail

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



StarWind Appliance Initial configuration

Review summary

License type

License	Paid 3 Nodes

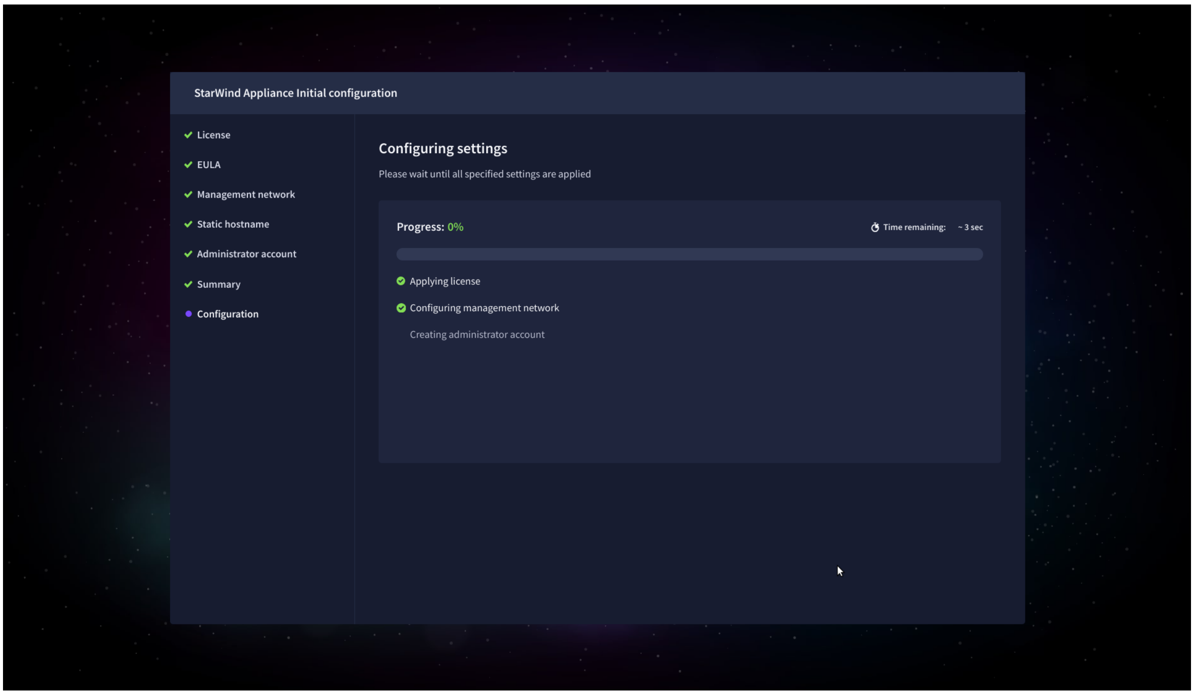
Network settings

Interface	ens160 (82574L Gigabit Network Connection)
Bandwidth	1 Gbit
MTU	1500
IP address	192.168.12.206
Appliance hostname	SW1

Credentials

Administrator username	admin

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



StarWind Appliance Initial configuration

- ✓ License
- ✓ EULA
- ✓ Management network
- ✓ Static hostname
- ✓ Administrator account
- ✓ Summary
- ● Configuration

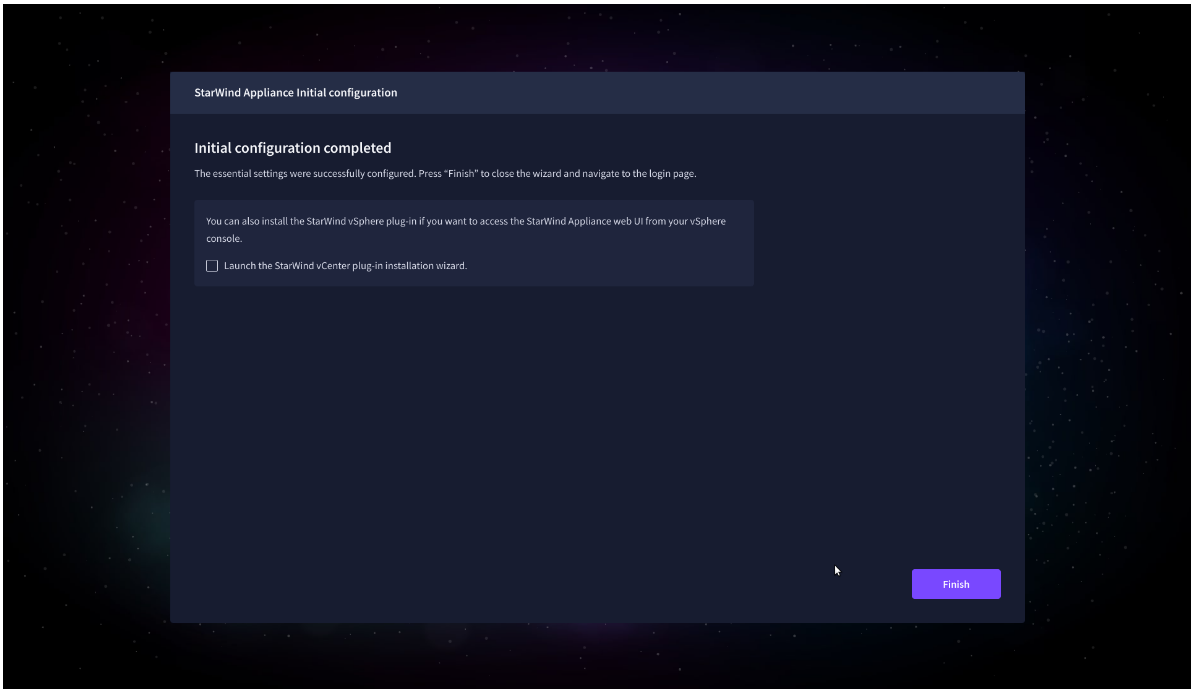
Configuring settings

Please wait until all specified settings are applied

Progress: 0% Time remaining: ~ 3 sec

- ✓ Applying license
- ✓ Configuring management network
- Creating administrator account

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.



StarWind Appliance Initial configuration

Initial configuration completed

The essential settings were successfully configured. Press "Finish" to close the wizard and navigate to the login page.

You can also install the StarWind vSphere plug-in if you want to access the StarWind Appliance web UI from your vSphere console.

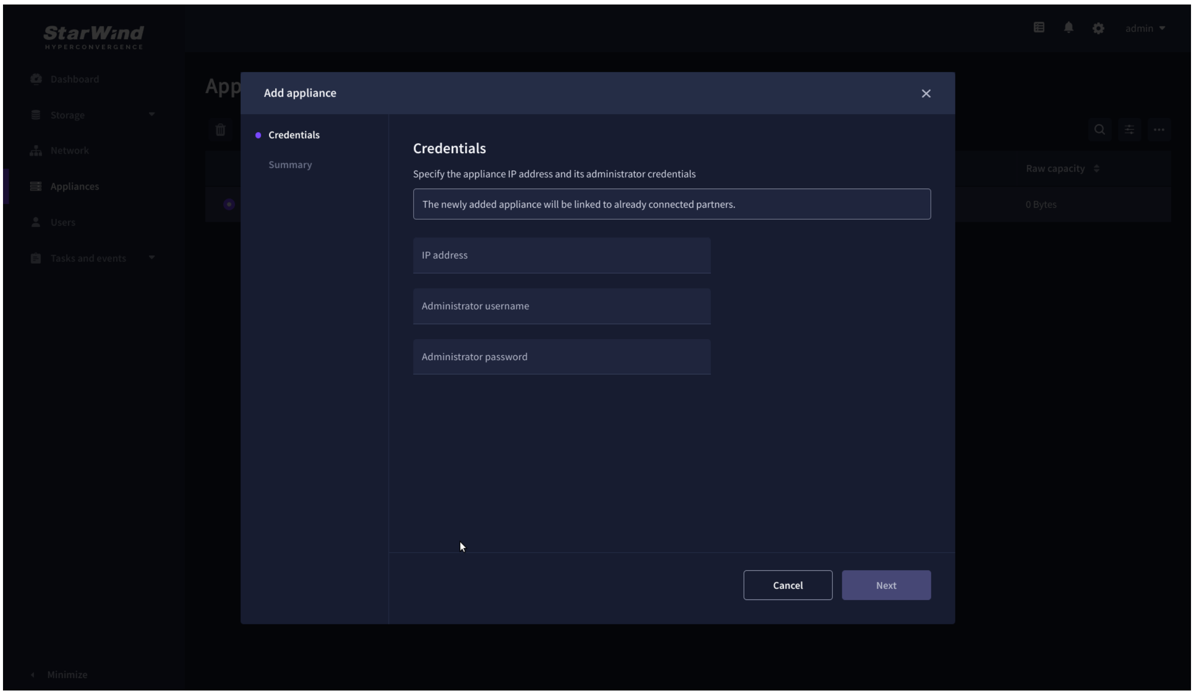
□ Launch the StarWind vCenter plug-in installation wizard.

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.

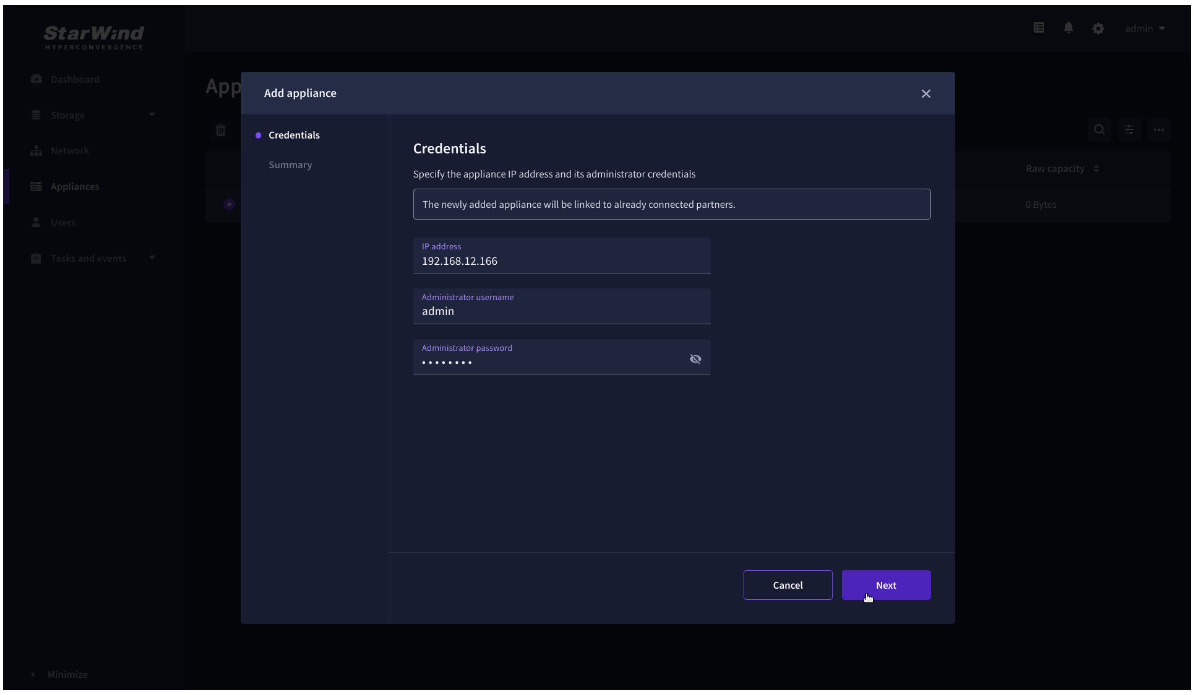

Add appliance

Credentials

Specify the appliance IP address and its administrator credentials

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

2. Provide credentials of partner appliance.



Add appliance

Credentials

Specify the appliance IP address and its administrator credentials

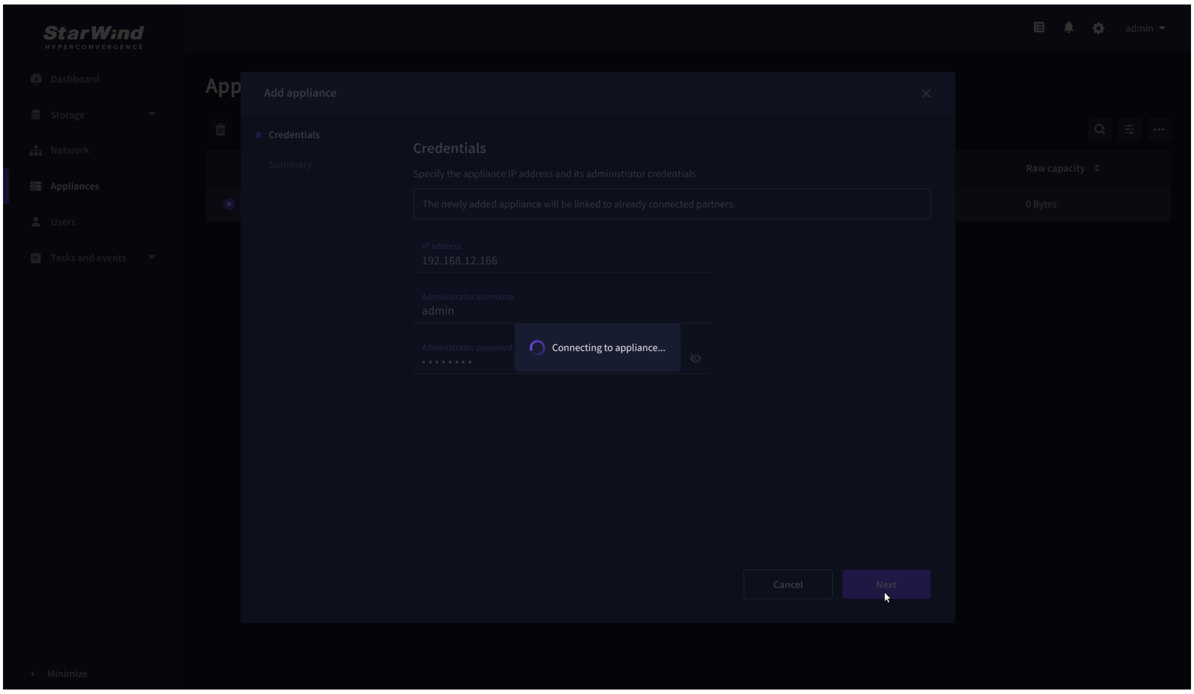
The newly added appliance will be linked to already connected partners.

IP address: 192.168.12.166

Administrator username: admin

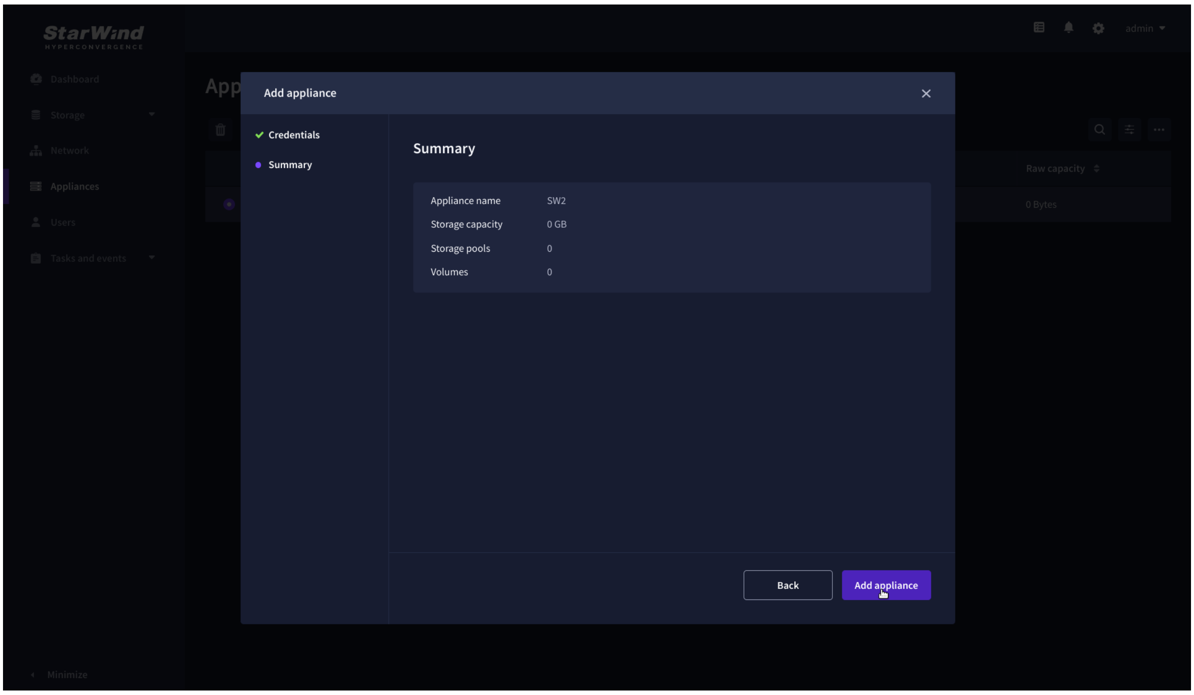
Administrator password: ••••••••

3. Wait for connection and validation of settings.



Connecting to appliance...

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

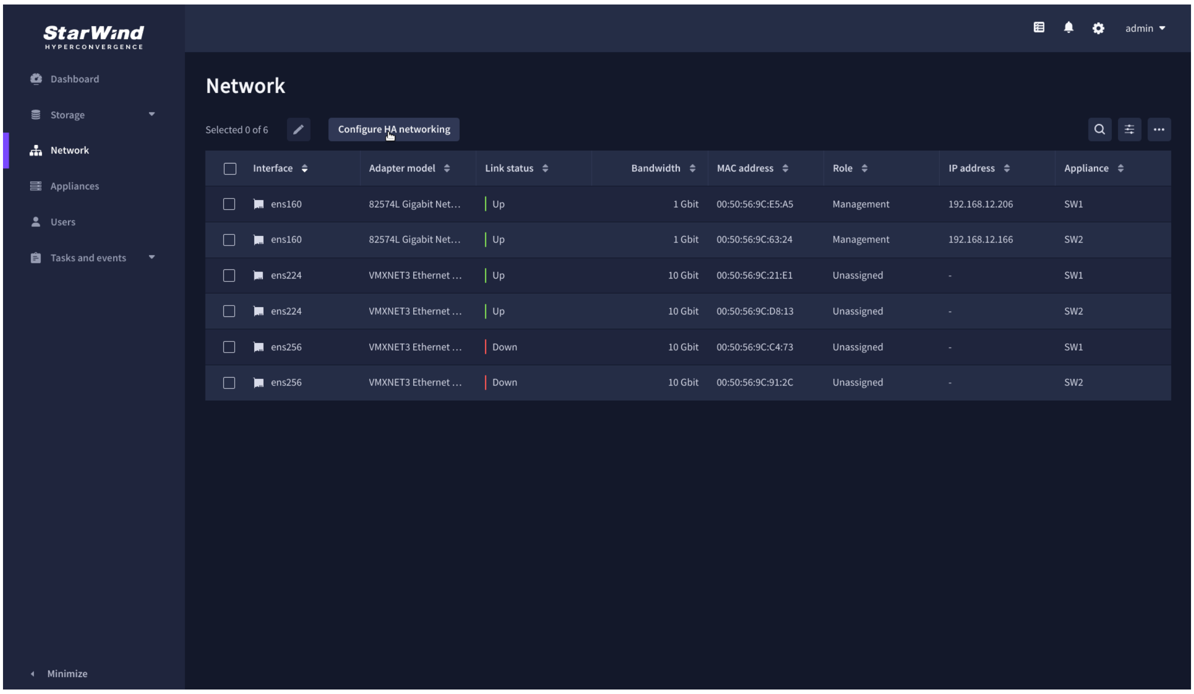


Summary

Appliance name	SW2
Storage capacity	0 GB
Storage pools	0
Volumes	0

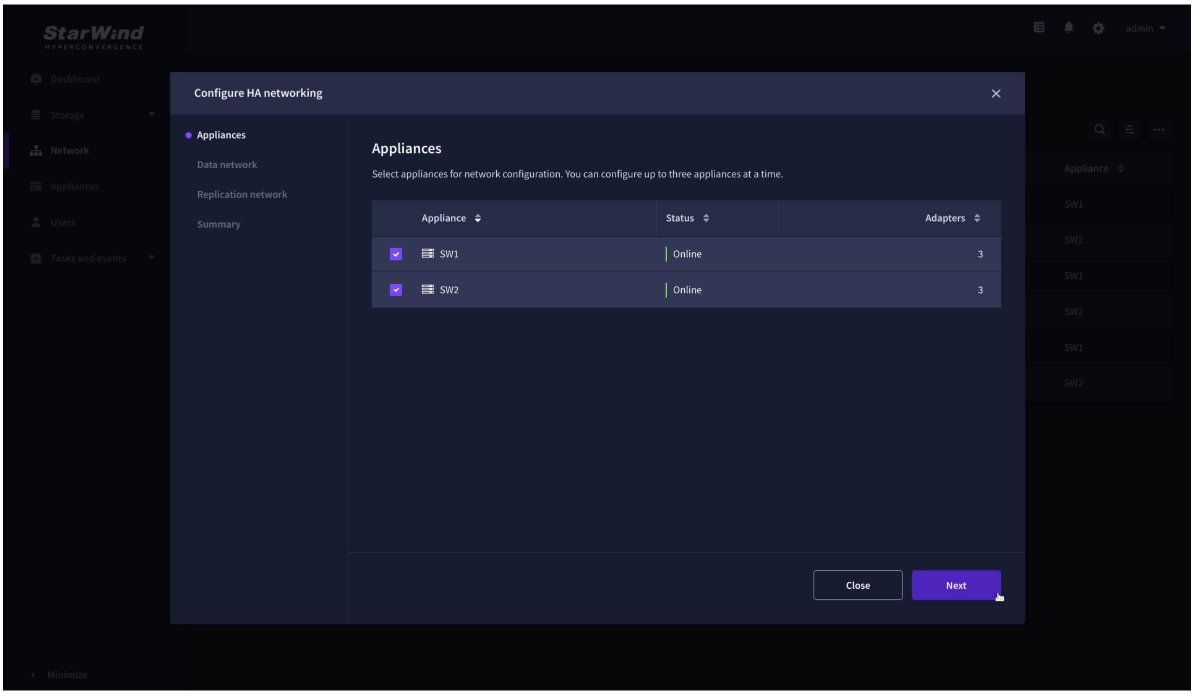
Configure Ha Networking

1. Launch the “Configure HA Networking” wizard.



Interface	Adapter model	Link status	Bandwidth	MAC address	Role	IP address	Appliance
ens160	82574L Gigabit Net...	Up	1 Gbit	00:50:56:9C:E5:A5	Management	192.168.12.206	SW1
ens160	82574L Gigabit Net...	Up	1 Gbit	00:50:56:9C:63:24	Management	192.168.12.166	SW2
ens224	VMXNET3 Ethernet ...	Up	10 Gbit	00:50:56:9C:21:E1	Unassigned	-	SW1
ens224	VMXNET3 Ethernet ...	Up	10 Gbit	00:50:56:9C:D8:13	Unassigned	-	SW2
ens256	VMXNET3 Ethernet ...	Down	10 Gbit	00:50:56:9C:C4:73	Unassigned	-	SW1
ens256	VMXNET3 Ethernet ...	Down	10 Gbit	00:50:56:9C:91:2C	Unassigned	-	SW2

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.



Appliances

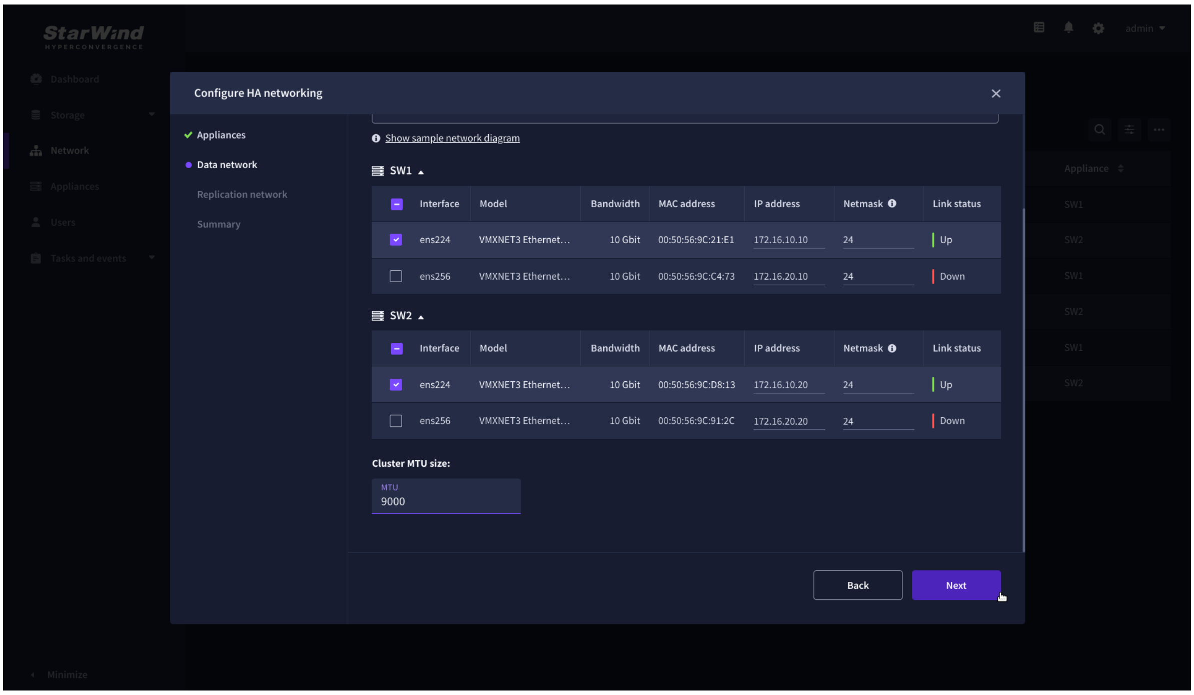
Select appliances for network configuration. You can configure up to three appliances at a time.

	Appliance	Status	Adapters
☑	SW1	Online	3
☑	SW2	Online	3

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.



Configure HA networking

SW1

☐	Interface	Model	Bandwidth	MAC address	IP address	Netmask	Link status
☑	ens224	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:21:E1	172.16.10.10	24	Up
☐	ens256	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:C4:73	172.16.20.10	24	Down

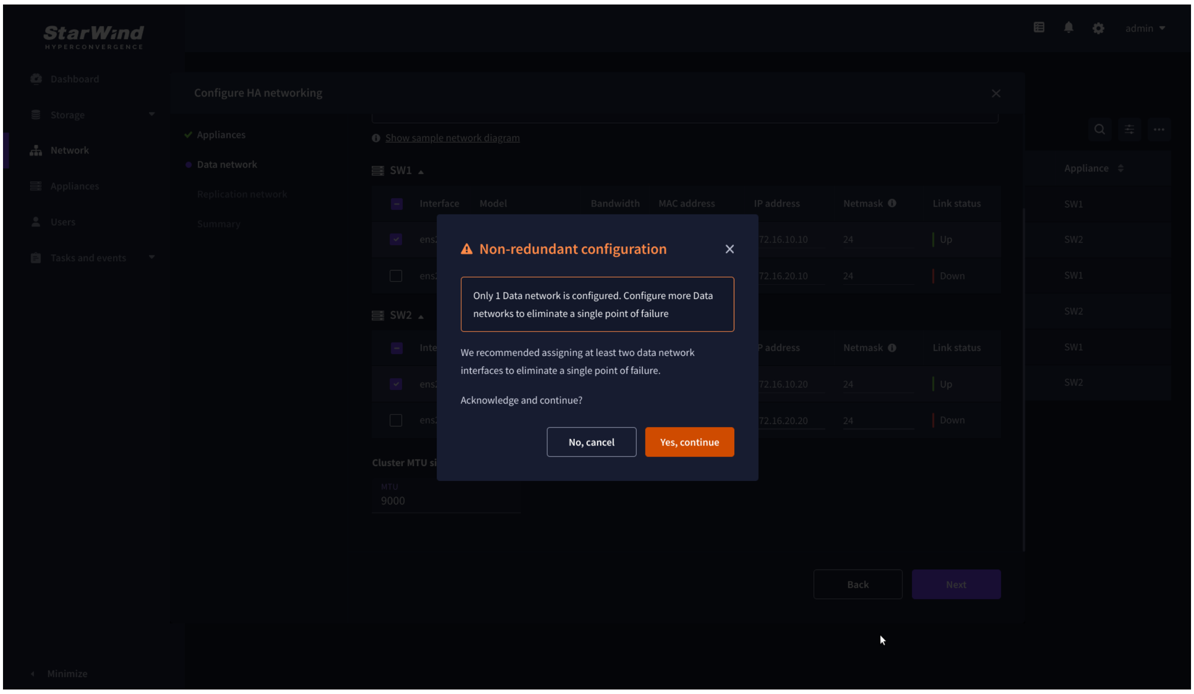
SW2

☐	Interface	Model	Bandwidth	MAC address	IP address	Netmask	Link status
☑	ens224	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:D8:13	172.16.10.20	24	Up
☐	ens256	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:91:2C	172.16.20.20	24	Down

Cluster MTU size:

MTU 9000

5. Click Next to validate Data network settings.



Non-redundant configuration

Only 1 Data network is configured. Configure more Data networks to eliminate a single point of failure

We recommended assigning at least two data network interfaces to eliminate a single point of failure.

Acknowledge and continue?

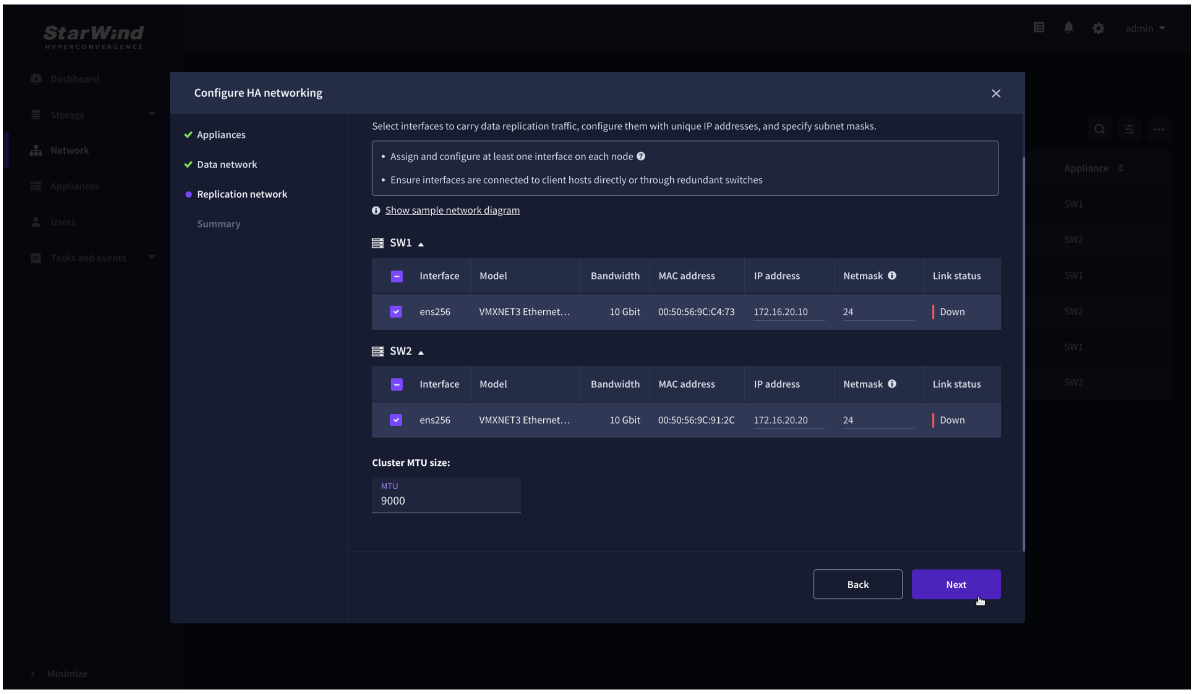
No, cancel | Yes, continue

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.



Configure HA networking

Select interfaces to carry data replication traffic, configure them with unique IP addresses, and specify subnet masks.

- Assign and configure at least one interface on each node
- Ensure interfaces are connected to client hosts directly or through redundant switches

Show sample network diagram

SW1

☐	Interface	Model	Bandwidth	MAC address	IP address	Netmask	Link status
☑	ens256	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:C4:73	172.16.20.10	24	Down

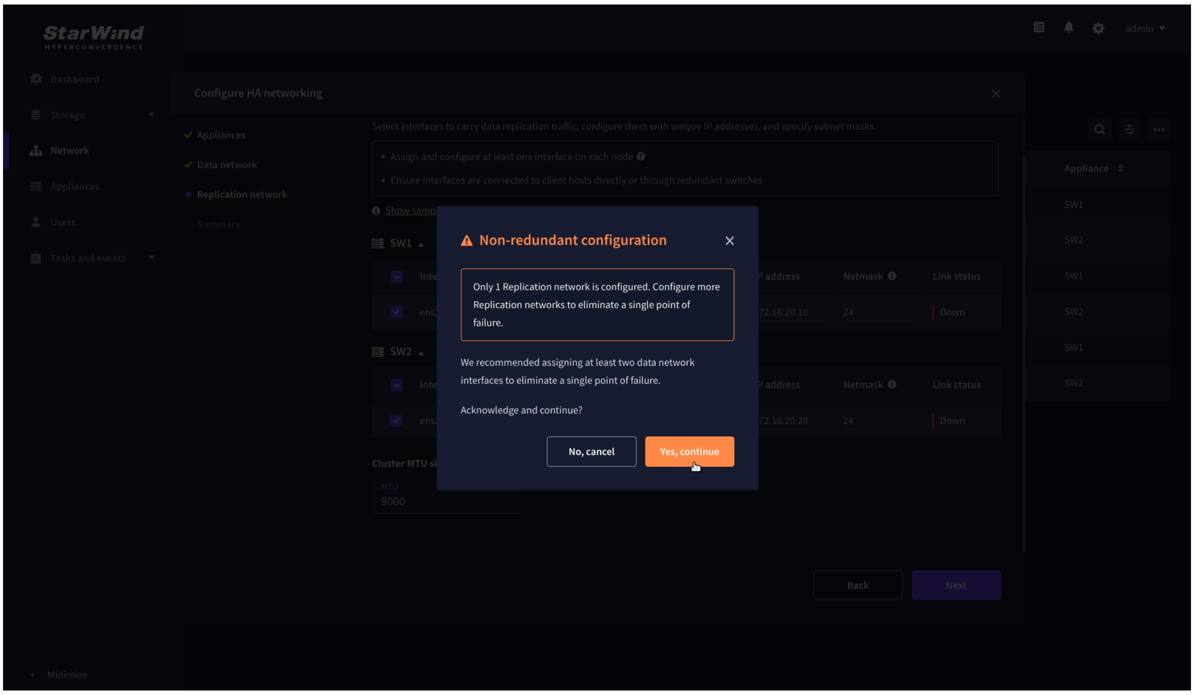
SW2

☐	Interface	Model	Bandwidth	MAC address	IP address	Netmask	Link status
☑	ens256	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:91:2C	172.16.20.20	24	Down

Cluster MTU size:

MTU: 9000

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

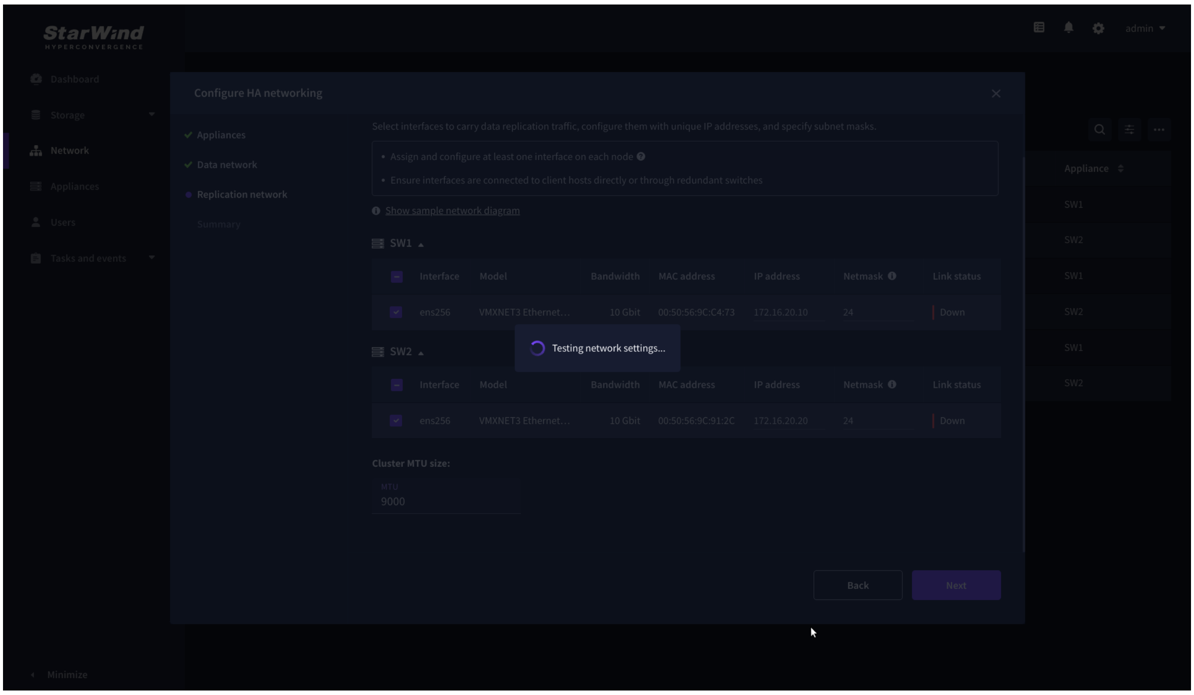


Non-redundant configuration

Only 1 Replication network is configured. Configure more Replication networks to eliminate a single point of failure.

We recommended assigning at least two data network interfaces to eliminate a single point of failure.

Acknowledge and continue?



Configure HA networking

Select interfaces to carry data replication traffic, configure them with unique IP addresses, and specify subnet masks.

- Assign and configure at least one interface on each node
- Ensure interfaces are connected to client hosts directly or through redundant switches

Show sample network diagram

SW1

Interface	Model	Bandwidth	MAC address	IP address	Netmask	Link status
☑ ens256	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:C4:73	172.16.20.10	24	Down

SW2

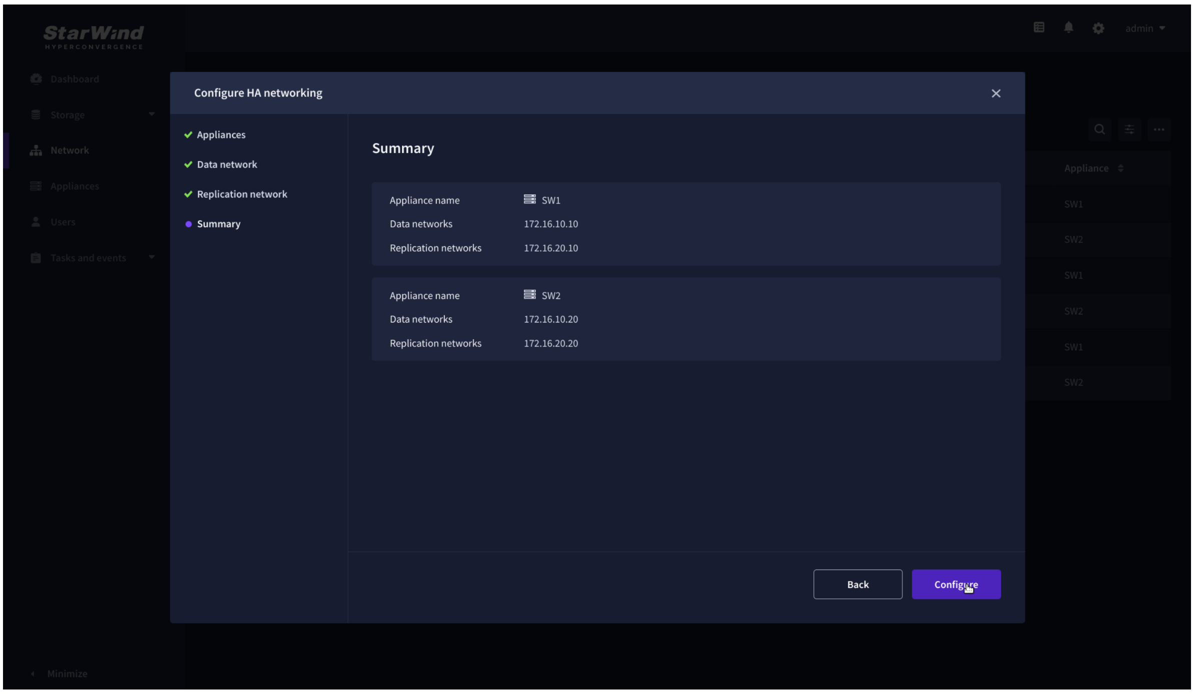
Interface	Model	Bandwidth	MAC address	IP address	Netmask	Link status
☑ ens256	VMXNET3 Ethernet…	10 Gbit	00:50:56:9C:91:2C	172.16.20.20	24	Down

Testing network settings...

Cluster MTU size:

MTU: 9000

9. Review the summary and click Configure.



Configure HA networking

Summary

Appliance name	SW1
Data networks	172.16.10.10
Replication networks	172.16.20.10

Appliance name	SW2
Data networks	172.16.10.20
Replication networks	172.16.20.20

Add Physical Disks

Attach storage to StarWind Virtual SAN Controller VM:

- the physical hosts have all the drives connected through an HBA or RAID controller
- HBA or RAID controller will be added via a DirectPath I/O passthrough device to a StarWind CVM. Follow the instructions from the VMware on how to add a RAID controller as a PCI device to StarWind VM: https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-esxi-host-client/GUID-2B6D43A6-9598-47C4-A2E7-5924E3367BB6.html
- StarWind CVM is installed on each server that is used to configure highly available storage.
- it is recommended to install StarWind CVM on a separate storage device available to the hypervisor host (e.g. SSD, HDD, etc.).
- for VMware vSphere environments, the disks can be added to StarWind VM as RDM. The link to VMware documentation is below: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4236E44E-E11F-4EDD-8CC0-12BA664BB811.html

NOTE: In order to make RDM and VMDK disks available for StarWind devices in StarWind CVM Version 20231016 (build 15260), please follow the steps below.

- stop service

```
sudo systemctl stop starwind-san-and-nas-console
```

- get VMDK/RDM/ device letter using lsblk command

```
lsblk |grep -v sda # sda - is excluded system drive.
```

- edit config file

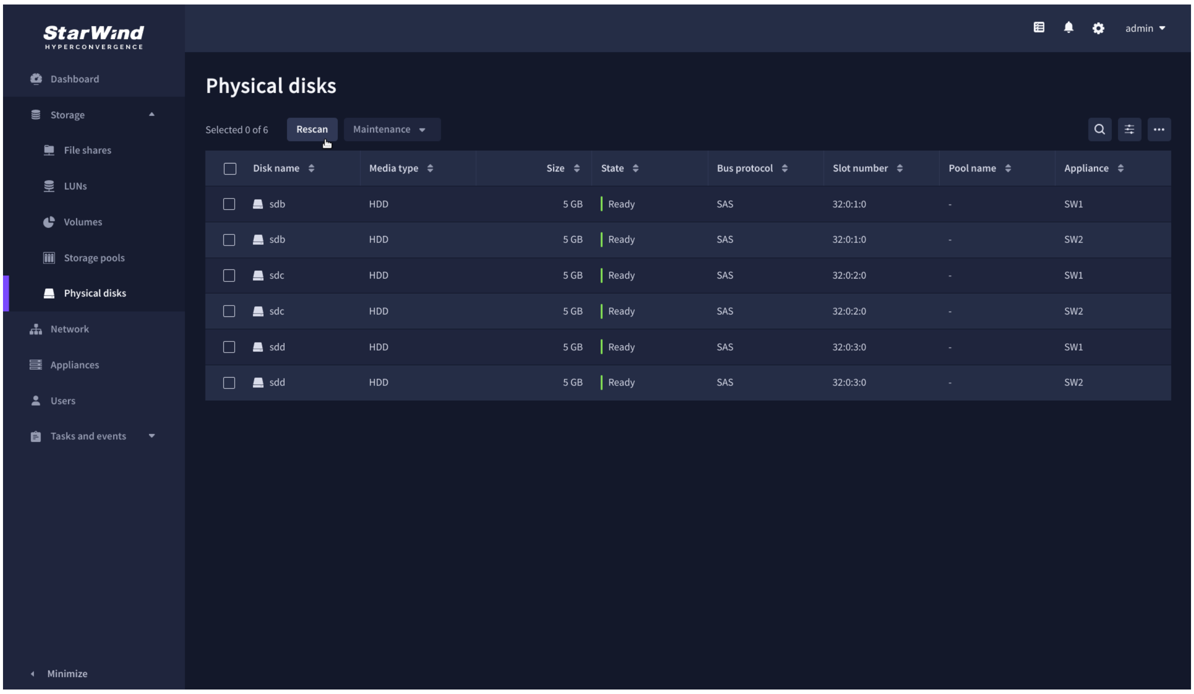
```
 sudo nano /opt/starwind/starwind-san-and-nas-console/appsettings.json
```

- add lines to the file, previously setting the disk letters to config (e.g. sdb, sdc)

```
"HardwareRaidImulation": {"PhysicalDisks": [ "sdb", "sdc" ] },
```

- start service

```
sudo systemctl start starwind-san-and-nas-console
```

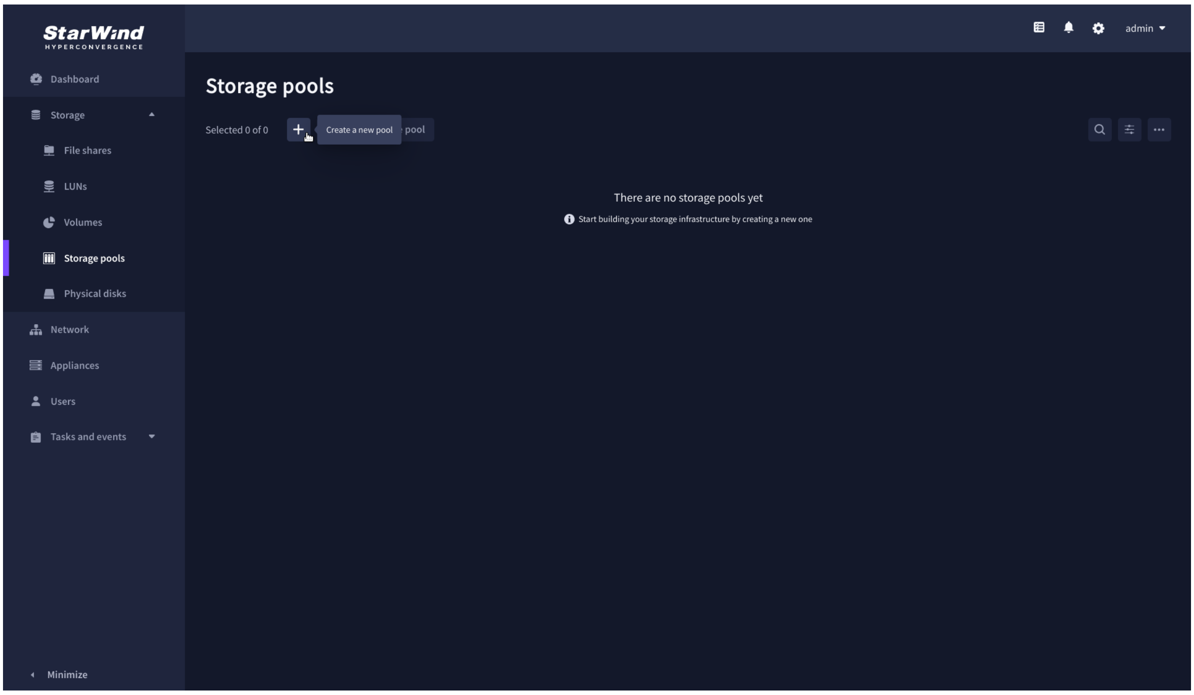


Disk name	Media type	Size	State	Bus protocol	Slot number	Pool name	Appliance
sdb	HDD	5 GB	Ready	SAS	32:0:1:0	-	SW1
sdb	HDD	5 GB	Ready	SAS	32:0:1:0	-	SW2
sdc	HDD	5 GB	Ready	SAS	32:0:2:0	-	SW1
sdc	HDD	5 GB	Ready	SAS	32:0:2:0	-	SW2
sdd	HDD	5 GB	Ready	SAS	32:0:3:0	-	SW1
sdd	HDD	5 GB	Ready	SAS	32:0:3:0	-	SW2

Create Storage Pool

1. Click the “Add” button to create a storage pool.

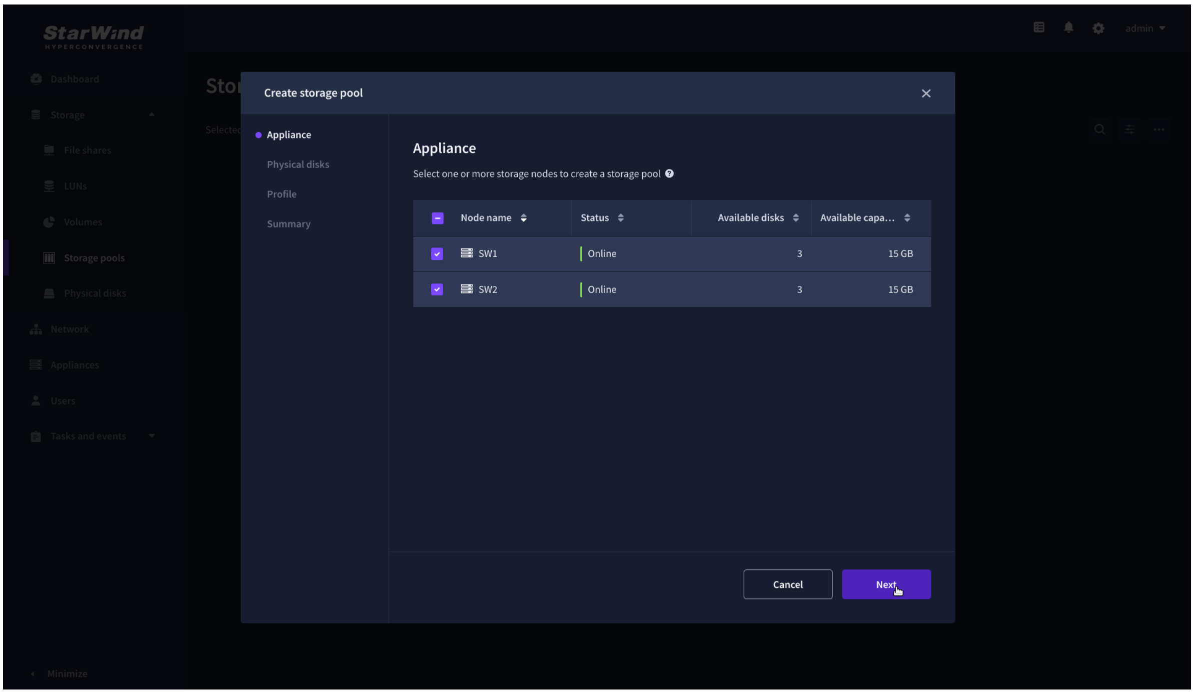
2. Select two storage nodes to create a storage pool on them simultaneously.



Storage pools

There are no storage pools yet

Start building your storage infrastructure by creating a new one



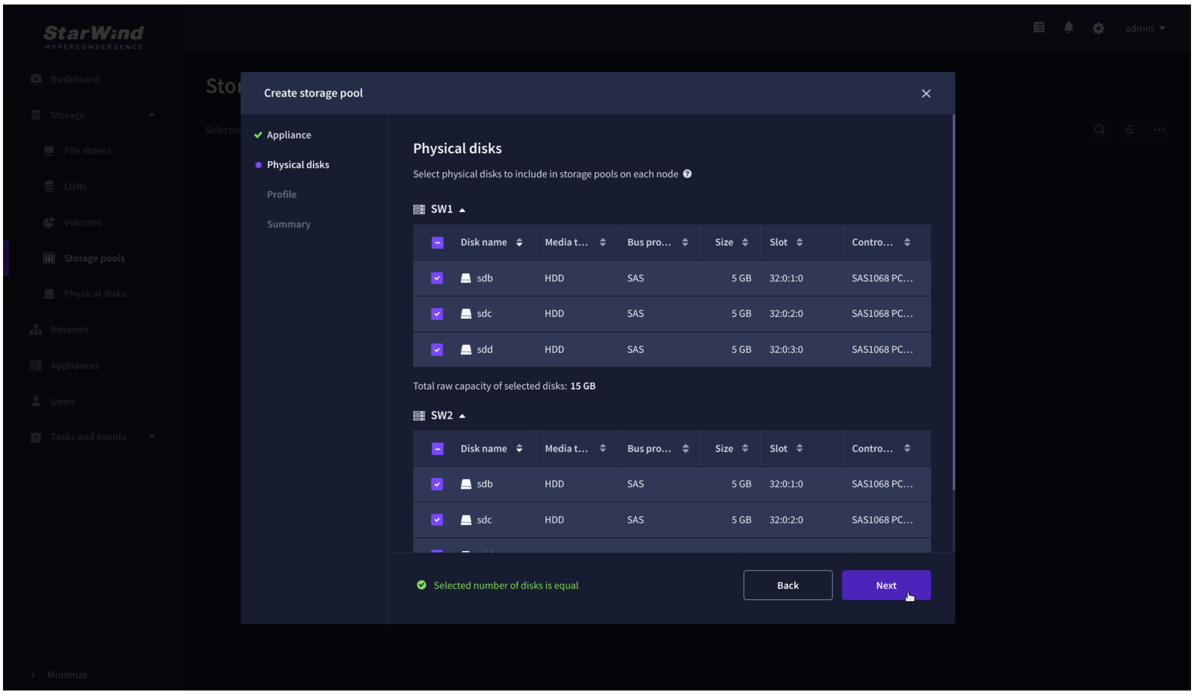
Create storage pool

Appliance

Select one or more storage nodes to create a storage pool

	Node name	Status	Available disks	Available capa...
☑	SW1	Online	3	15 GB
☑	SW2	Online	3	15 GB

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.



Physical disks

Select physical disks to include in storage pools on each node

SW1

☐	Disk name	Media t…	Bus pro…	Size	Slot	Contro…
☑	sdb	HDD	SAS	5 GB	32:0:1:0	SAS1068 PC…
☑	sdc	HDD	SAS	5 GB	32:0:2:0	SAS1068 PC…
☑	sdd	HDD	SAS	5 GB	32:0:3:0	SAS1068 PC…

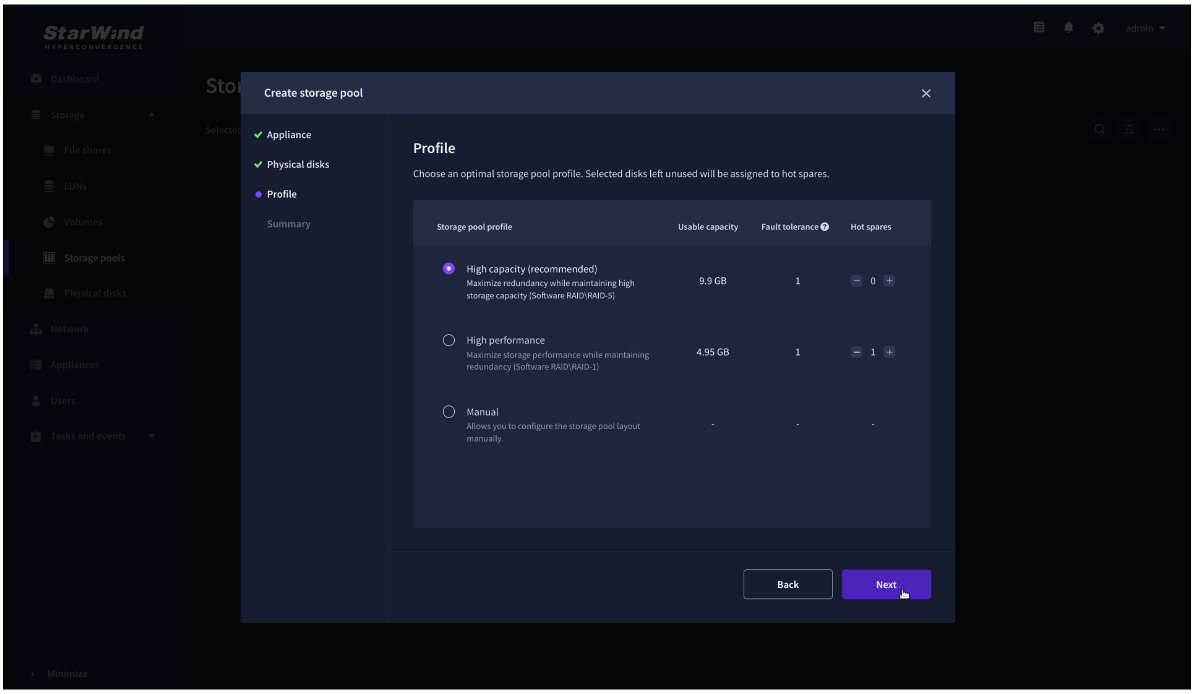
Total raw capacity of selected disks: **15 GB**

SW2

☐	Disk name	Media t…	Bus pro…	Size	Slot	Contro…
☑	sdb	HDD	SAS	5 GB	32:0:1:0	SAS1068 PC…
☑	sdc	HDD	SAS	5 GB	32:0:2:0	SAS1068 PC…

✓ Selected number of disks is equal

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.



Profile

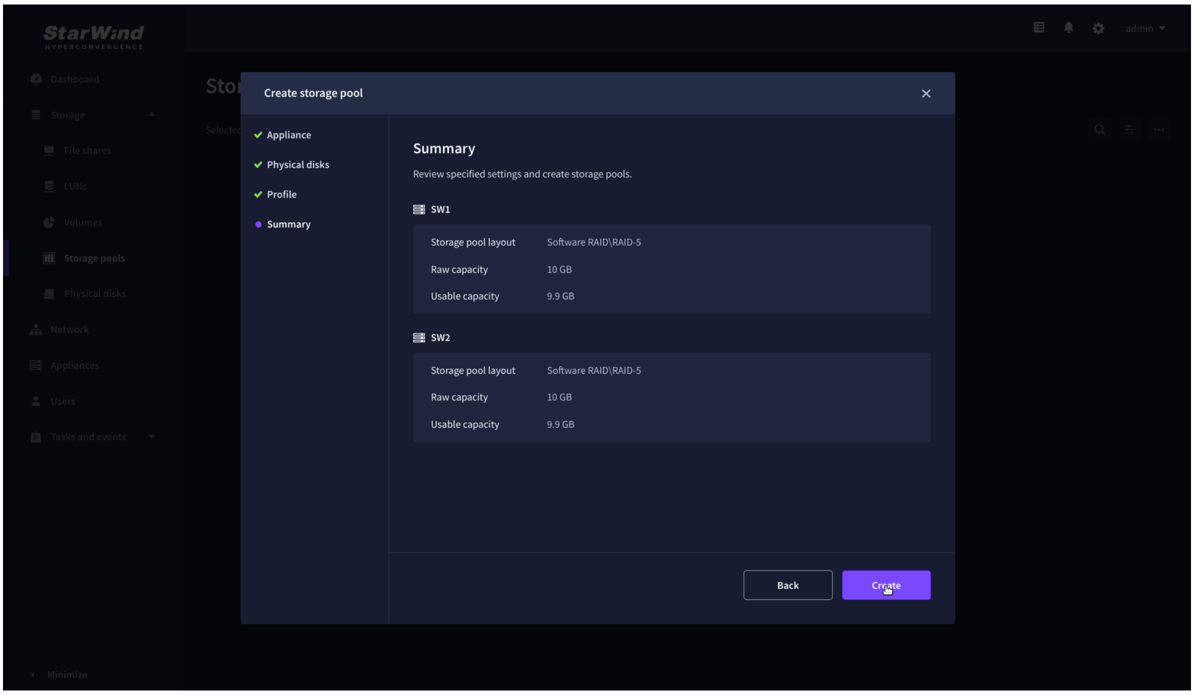
Choose an optimal storage pool profile. Selected disks left unused will be assigned to hot spares.

Storage pool profile	Usable capacity	Fault tolerance	Hot spares
● High capacity (recommended) Maximize redundancy while maintaining high storage capacity (Software RAID\RAID-5)	9.9 GB	1	− 0 +
○ High performance Maximize storage performance while maintaining redundancy (Software RAID\RAID-1)	4.95 GB	1	− 1 +
○ Manual Allows you to configure the storage pool layout manually.	-	-	-

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.



Summary

Review specified settings and create storage pools.

SW1

Storage pool layout	Software RAID\RAID-5
Raw capacity	10 GB
Usable capacity	9.9 GB

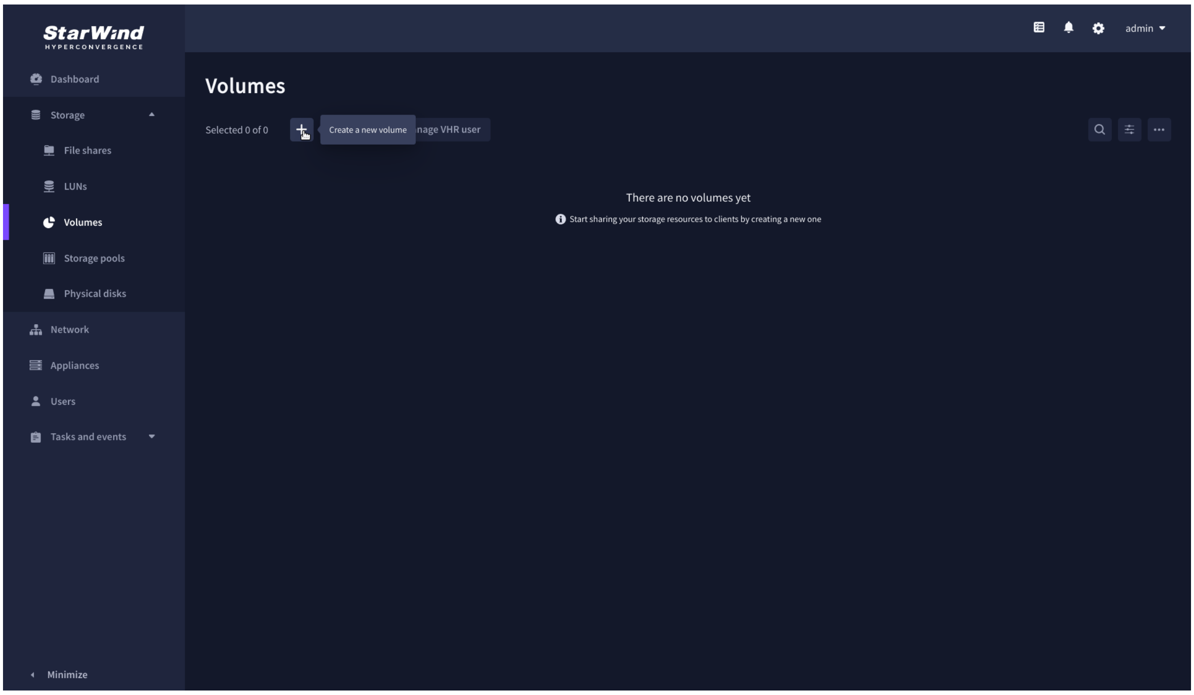
SW2

Storage pool layout	Software RAID\RAID-5
Raw capacity	10 GB
Usable capacity	9.9 GB

Create Volume

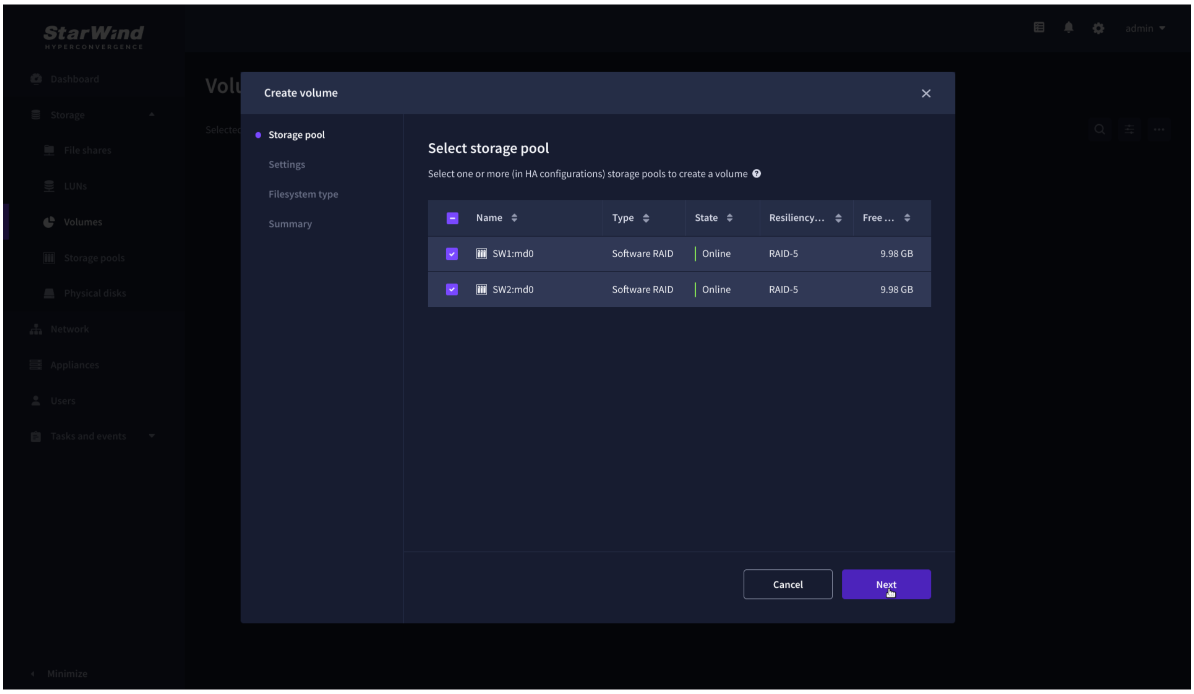
1. To create volumes, click the “Add” button.

2. Select two identical storage pools to create a volume simultaneously.



There are no volumes yet

Start sharing your storage resources to clients by creating a new one

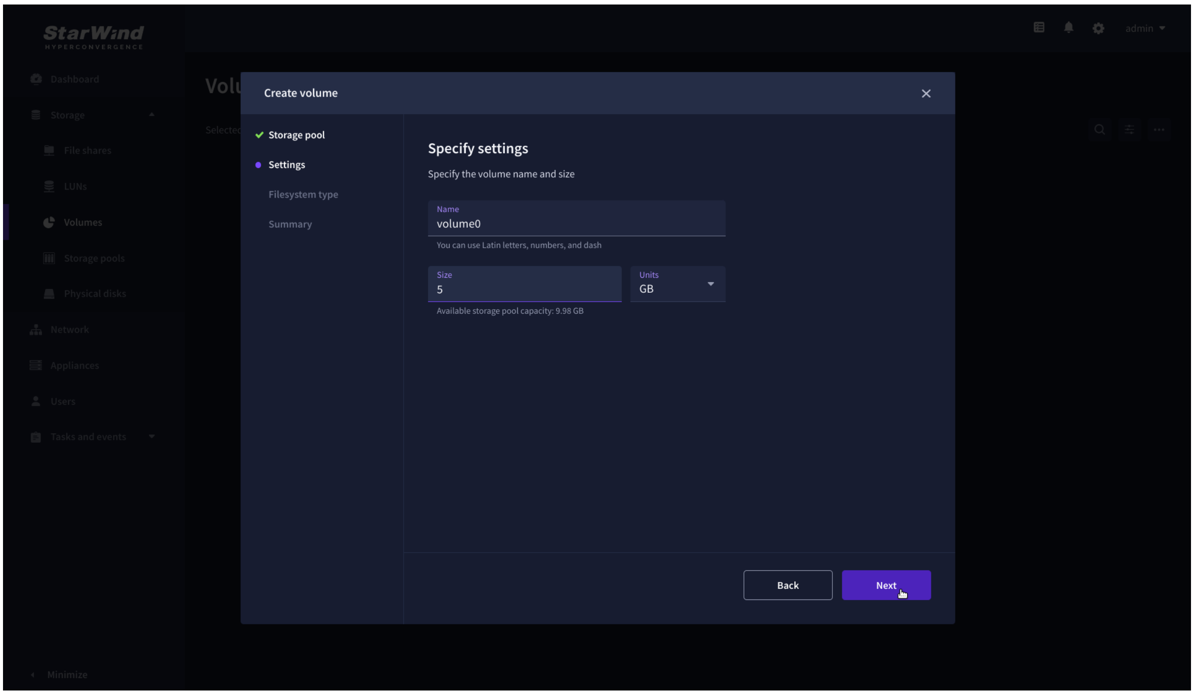


Select storage pool

Select one or more (in HA configurations) storage pools to create a volume

☑	Name	Type	State	Resiliency...	Free ...
☑	SW1:md0	Software RAID	Online	RAID-5	9.98 GB
☑	SW2:md0	Software RAID	Online	RAID-5	9.98 GB

3. Specify volume name and capacity.



Specify settings

Specify the volume name and size

Name: volume0

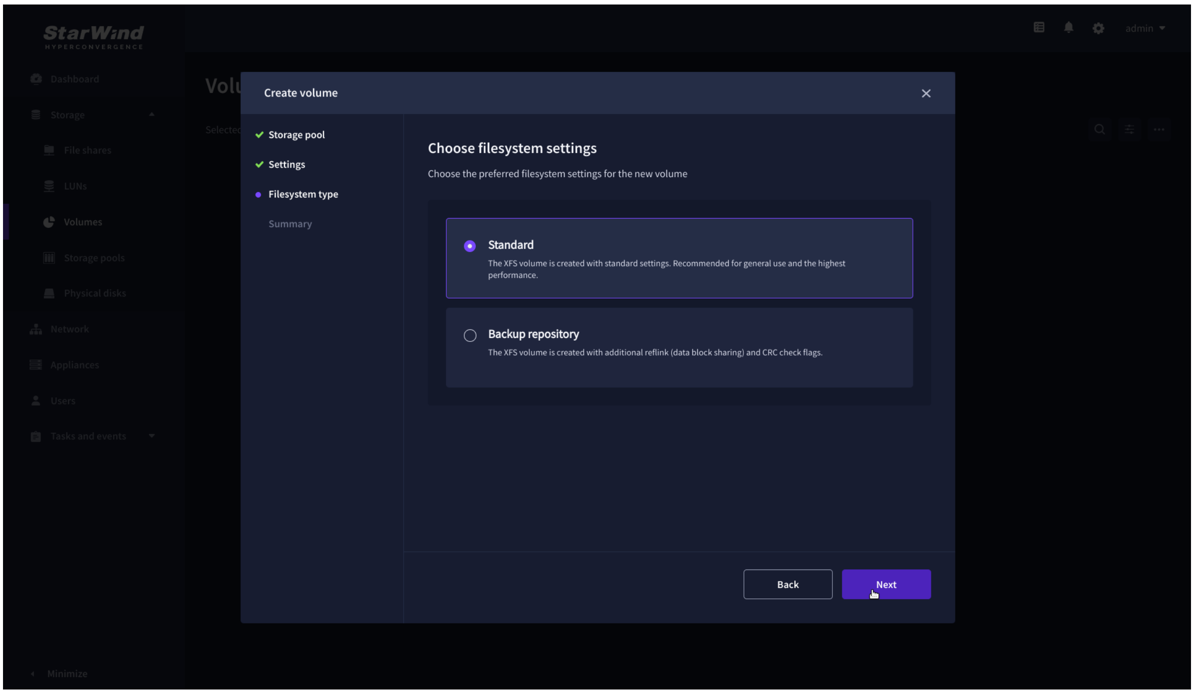
You can use Latin letters, numbers, and dash

Size: 5

Units: GB

Available storage pool capacity: 9.98 GB

4. Select the Standard volume type.



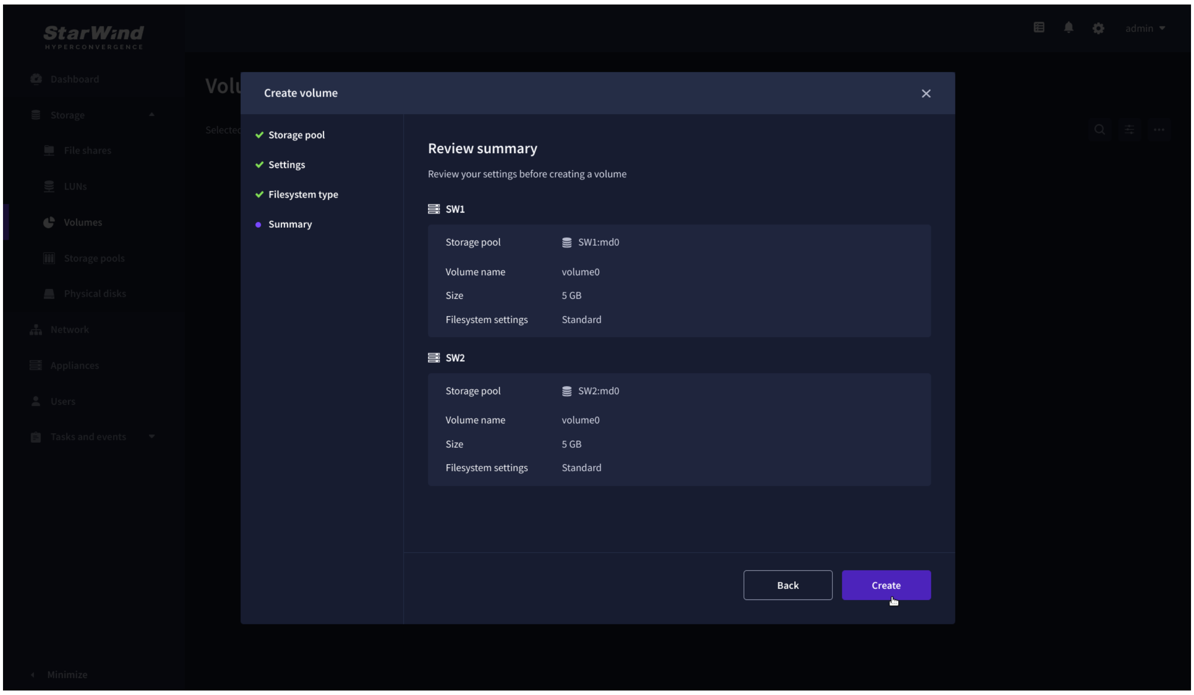
Choose filesystem settings

Choose the preferred filesystem settings for the new volume

● Standard
The XFS volume is created with standard settings. Recommended for general use and the highest performance.

○ Backup repository
The XFS volume is created with additional reflink (data block sharing) and CRC check flags.

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



Review summary

Review your settings before creating a volume

SW1

Storage pool	SW1:md0
Volume name	volume0
Size	5 GB
Filesystem settings	Standard

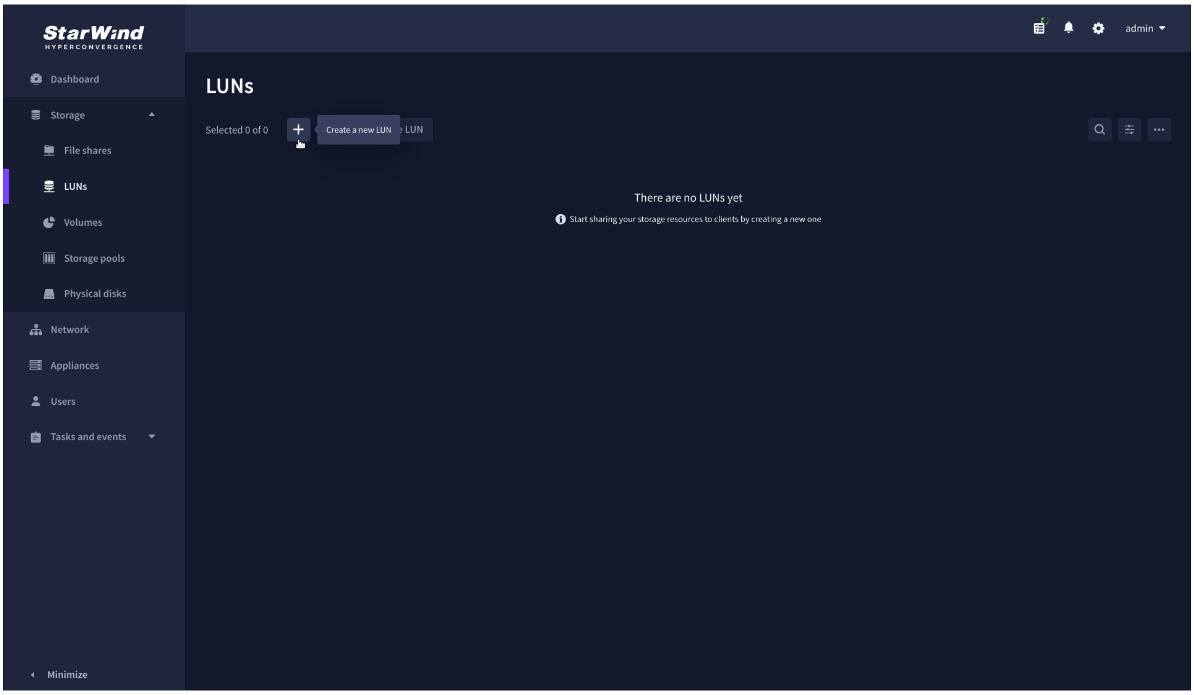
SW2

Storage pool	SW2:md0
Volume name	volume0
Size	5 GB
Filesystem settings	Standard

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.

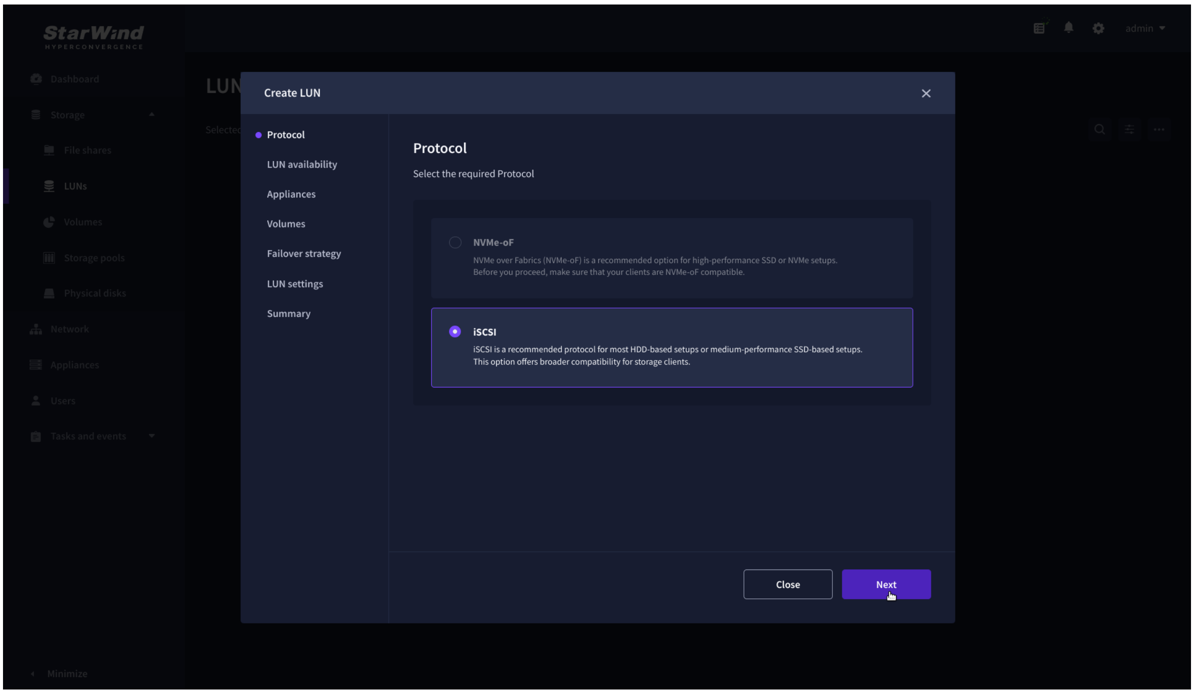
1. To create a virtual disk, click the Add button.



There are no LUNs yet

Start sharing your storage resources to clients by creating a new one

2. Select the protocol.



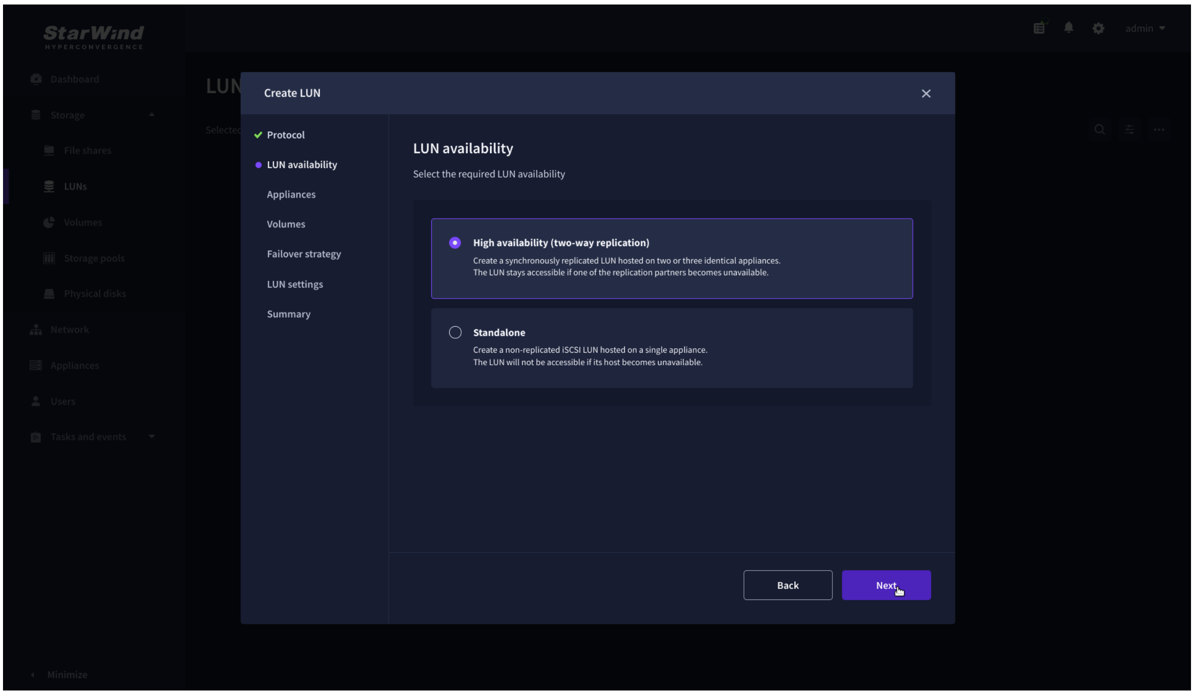
Protocol

Select the required Protocol

○ NVMe-oF
NVMe over Fabrics (NVMe-oF) is a recommended option for high-performance SSD or NVMe setups. Before you proceed, make sure that your clients are NVMe-oF compatible.

● iSCSI
iSCSI is a recommended protocol for most HDD-based setups or medium-performance SSD-based setups. This option offers broader compatibility for storage clients.

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



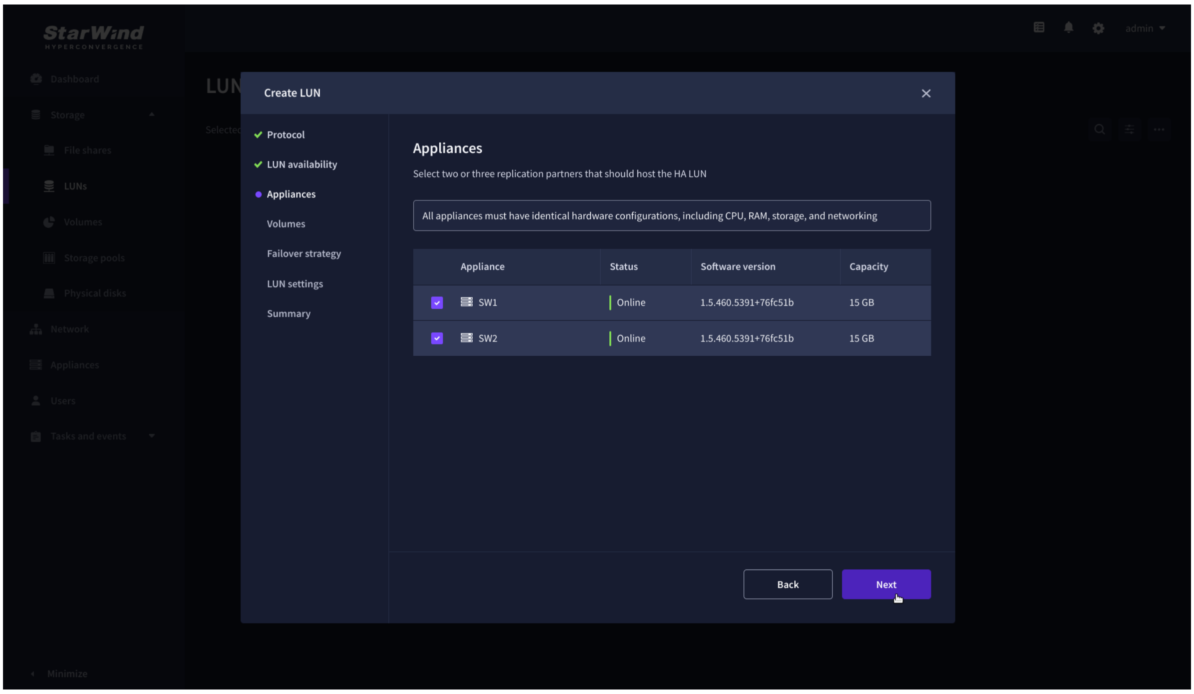
LUN availability

Select the required LUN availability

● **High availability (two-way replication)**
Create a synchronously replicated LUN hosted on two or three identical appliances.
The LUN stays accessible if one of the replication partners becomes unavailable.

○ **Standalone**
Create a non-replicated iSCSI LUN hosted on a single appliance.
The LUN will not be accessible if its host becomes unavailable.

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



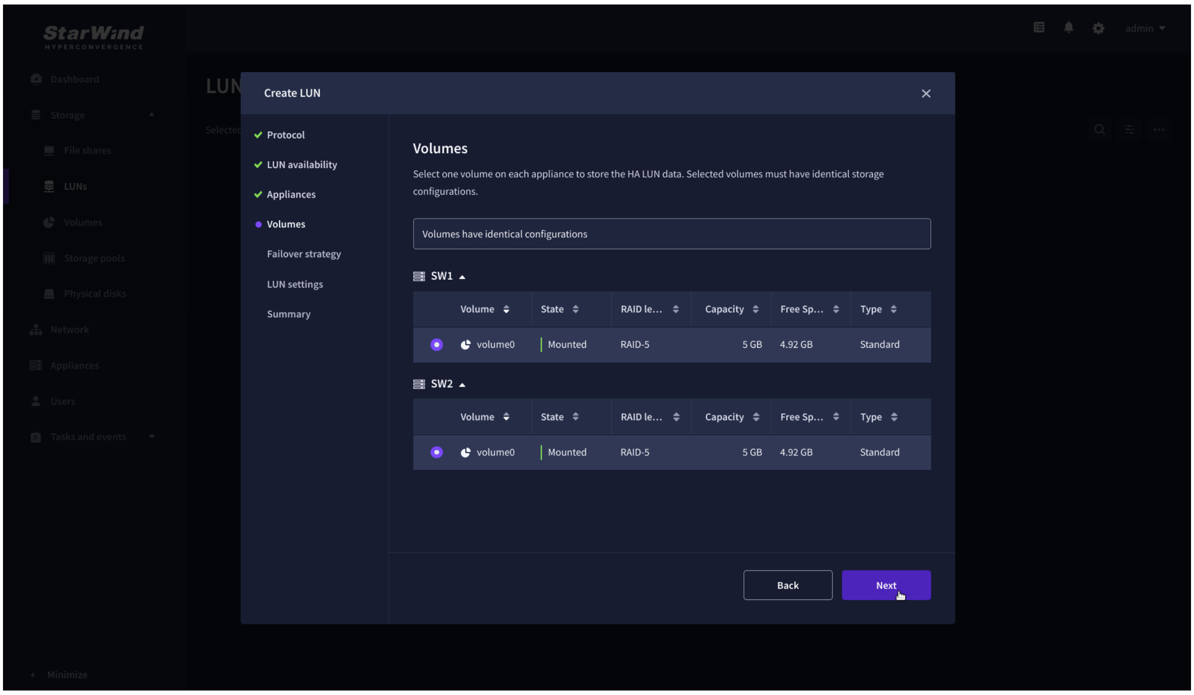
Appliances

Select two or three replication partners that should host the HA LUN

All appliances must have identical hardware configurations, including CPU, RAM, storage, and networking

	Appliance	Status	Software version	Capacity
☑	SW1	Online	1.5.460.5391+76fc51b	15 GB
☑	SW2	Online	1.5.460.5391+76fc51b	15 GB

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



Create LUN

✓ Protocol
✓ LUN availability
✓ Appliances
● Volumes
Failover strategy
LUN settings
Summary

Volumes

Select one volume on each appliance to store the HA LUN data. Selected volumes must have identical storage configurations.

Volumes have identical configurations

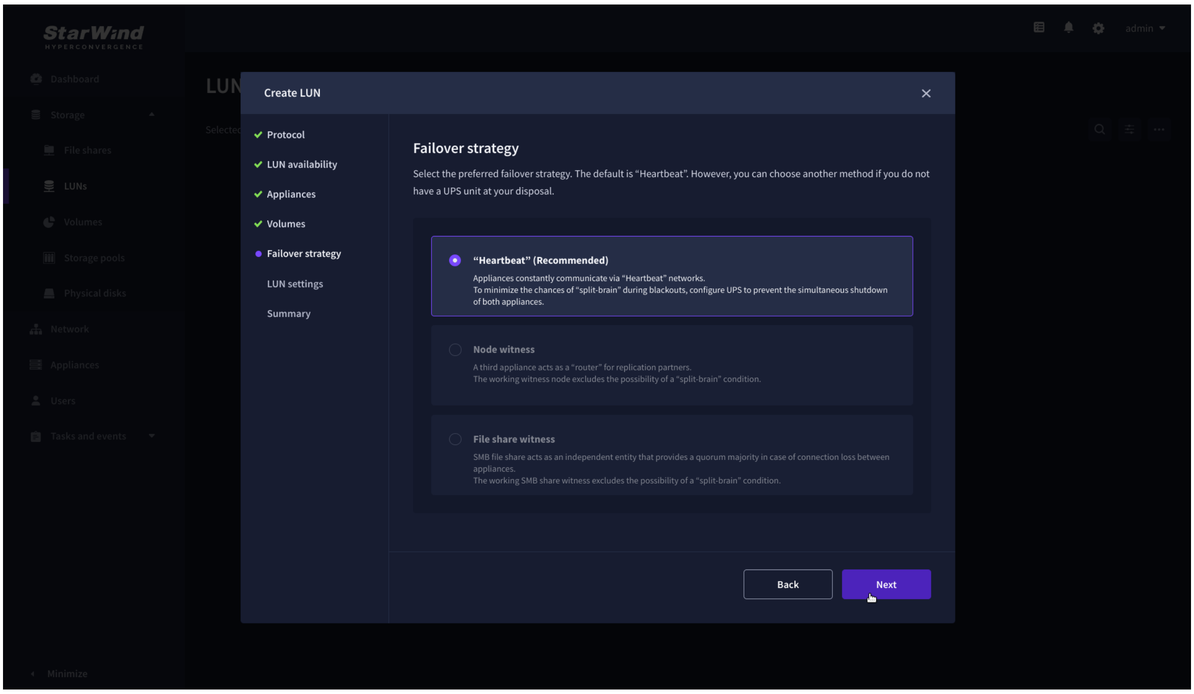
SW1

	Volume	State	RAID le...	Capacity	Free Sp...	Type
●	volume0	Mounted	RAID-5	5 GB	4.92 GB	Standard

SW2

	Volume	State	RAID le...	Capacity	Free Sp...	Type
●	volume0	Mounted	RAID-5	5 GB	4.92 GB	Standard

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.



Create LUN

✓ Protocol
✓ LUN availability
✓ Appliances
✓ Volumes
● Failover strategy
LUN settings
Summary

Failover strategy

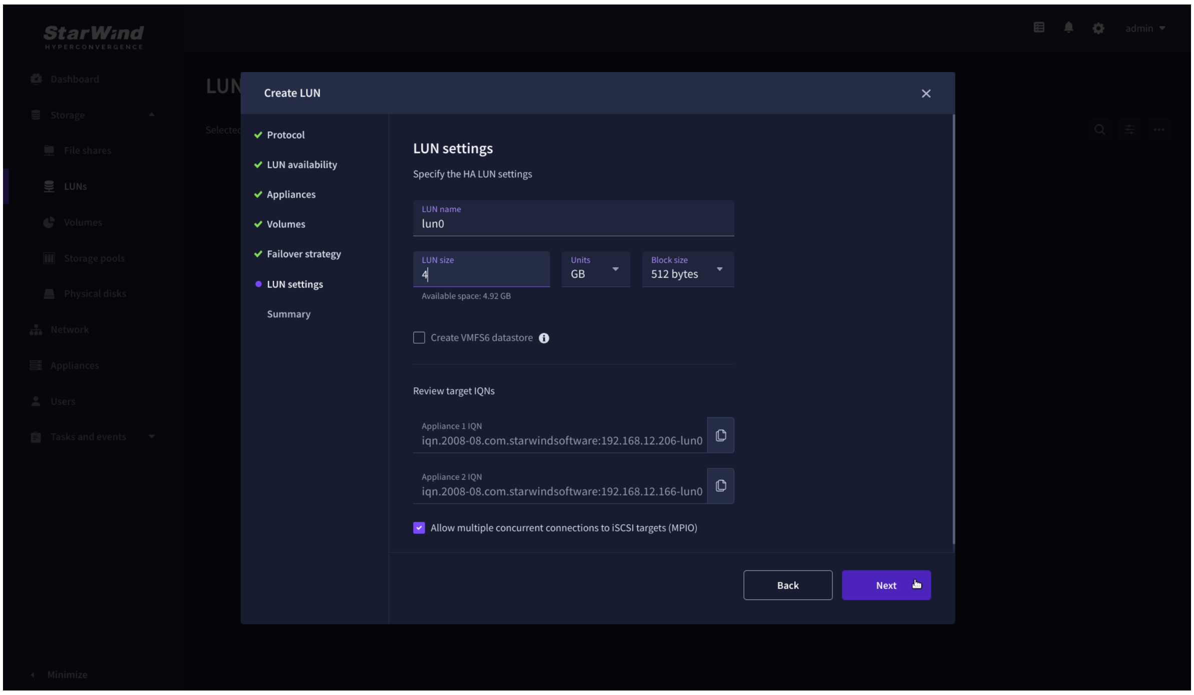
Select the preferred failover strategy. The default is “Heartbeat”. However, you can choose another method if you do not have a UPS unit at your disposal.

● **“Heartbeat” (Recommended)**
Appliances constantly communicate via “Heartbeat” networks.
To minimize the chances of “split-brain” during blackouts, configure UPS to prevent the simultaneous shutdown of both appliances.

○ **Node witness**
A third appliance acts as a “router” for replication partners.
The working witness node excludes the possibility of a “split-brain” condition.

○ **File share witness**
SMB file share acts as an independent entity that provides a quorum majority in case of connection loss between appliances.
The working SMB share witness excludes the possibility of a “split-brain” condition.

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



LUN settings

Specify the HA LUN settings

LUN name: lun0

LUN size: 4

Units: GB

Block size: 512 bytes

Available space: 4.92 GB

□ Create VMFS6 datastore

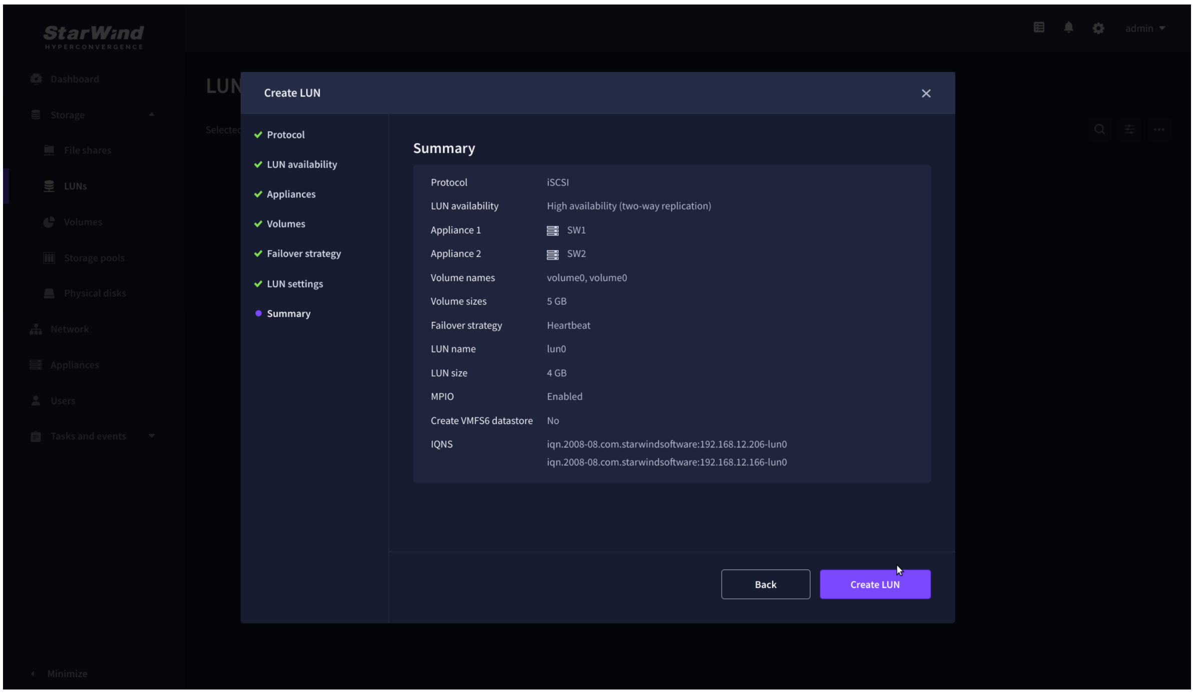
Review target IQNs

Appliance 1 IQN: iqn.2008-08.com.starwindsoftware:192.168.12.206-lun0

Appliance 2 IQN: iqn.2008-08.com.starwindsoftware:192.168.12.166-lun0

☑ Allow multiple concurrent connections to iSCSI targets (MPIO)

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



Summary

Protocol	iSCSI
LUN availability	High availability (two-way replication)
Appliance 1	SW1
Appliance 2	SW2
Volume names	volume0, volume0
Volume sizes	5 GB
Failover strategy	Heartbeat
LUN name	lun0
LUN size	4 GB
MPIO	Enabled
Create VMFS6 datastore	No
IQNS	iqn.2008-08.com.starwindsoftware:192.168.12.206-lun0 iqn.2008-08.com.starwindsoftware:192.168.12.166-lun0

Connecting Starwind Virtual Disk To Hyper-V Servers

Enabling Multipath Support on Hyper-V Servers

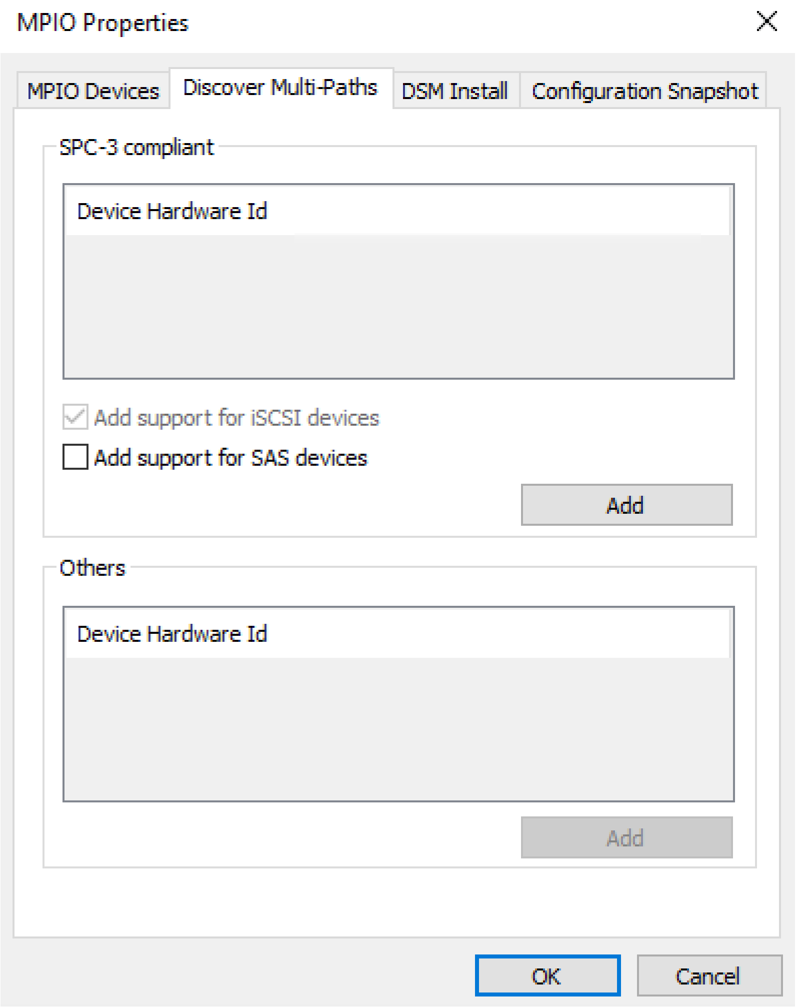
1. Install the Multipath I/O feature by executing the following command in the PowerShell window:

```
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.



☑ Add support for iSCSI devices

□ Add support for SAS devices

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.

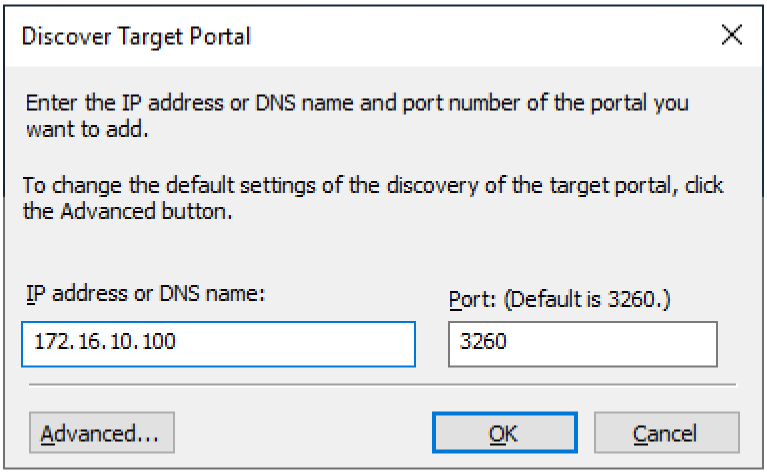
Provisioning StarWind SAN & NAS Storage to Hyper-V Server Hosts

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.



Discover Target Portal

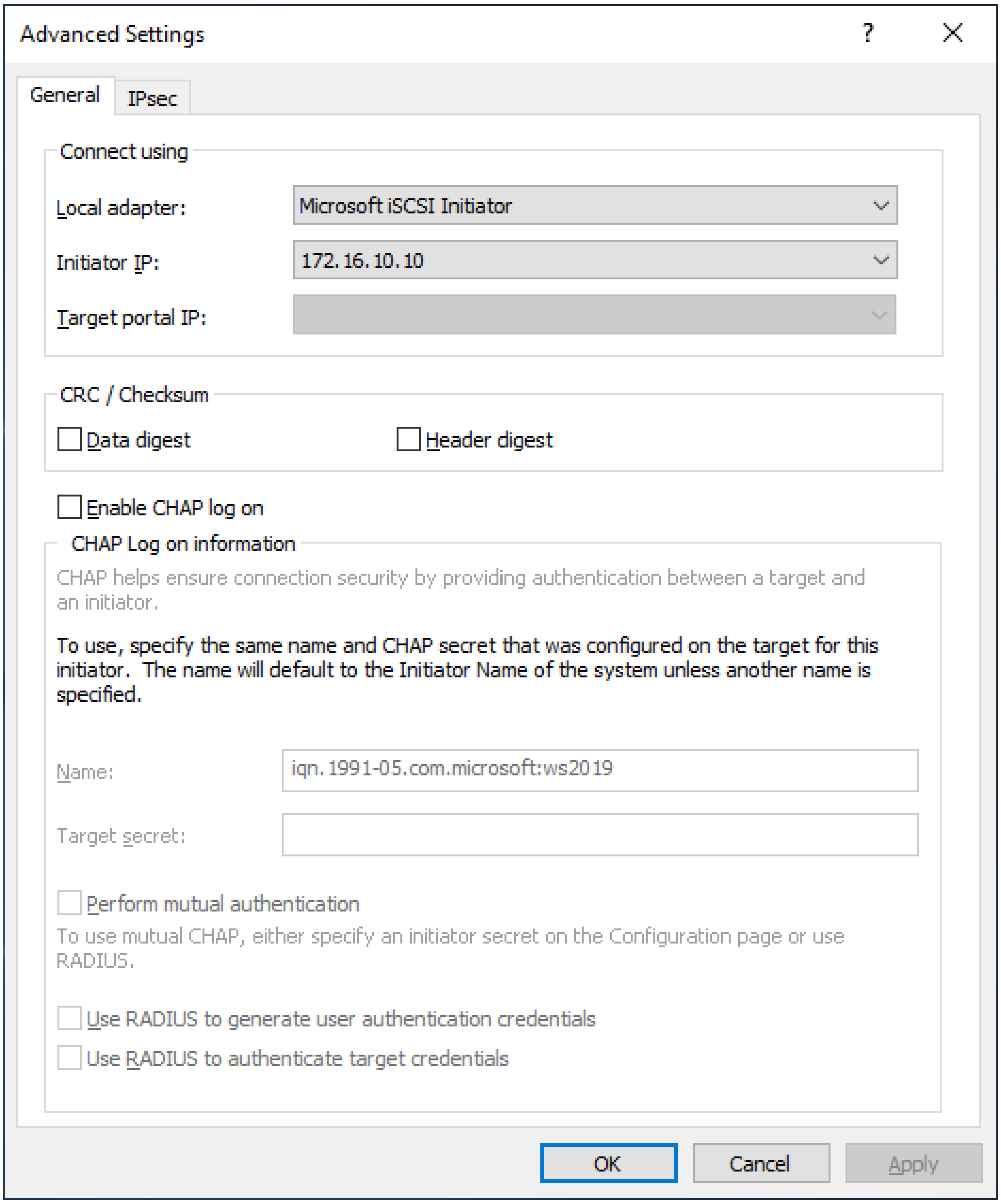
Enter the IP address or DNS name and port number of the portal you want to add.

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

IP address or DNS name: 172.16.10.100

Port: (Default is 3260.) 3260

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.



Advanced Settings

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.16.10.10

Target portal IP:

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:ws2019

Target secret:

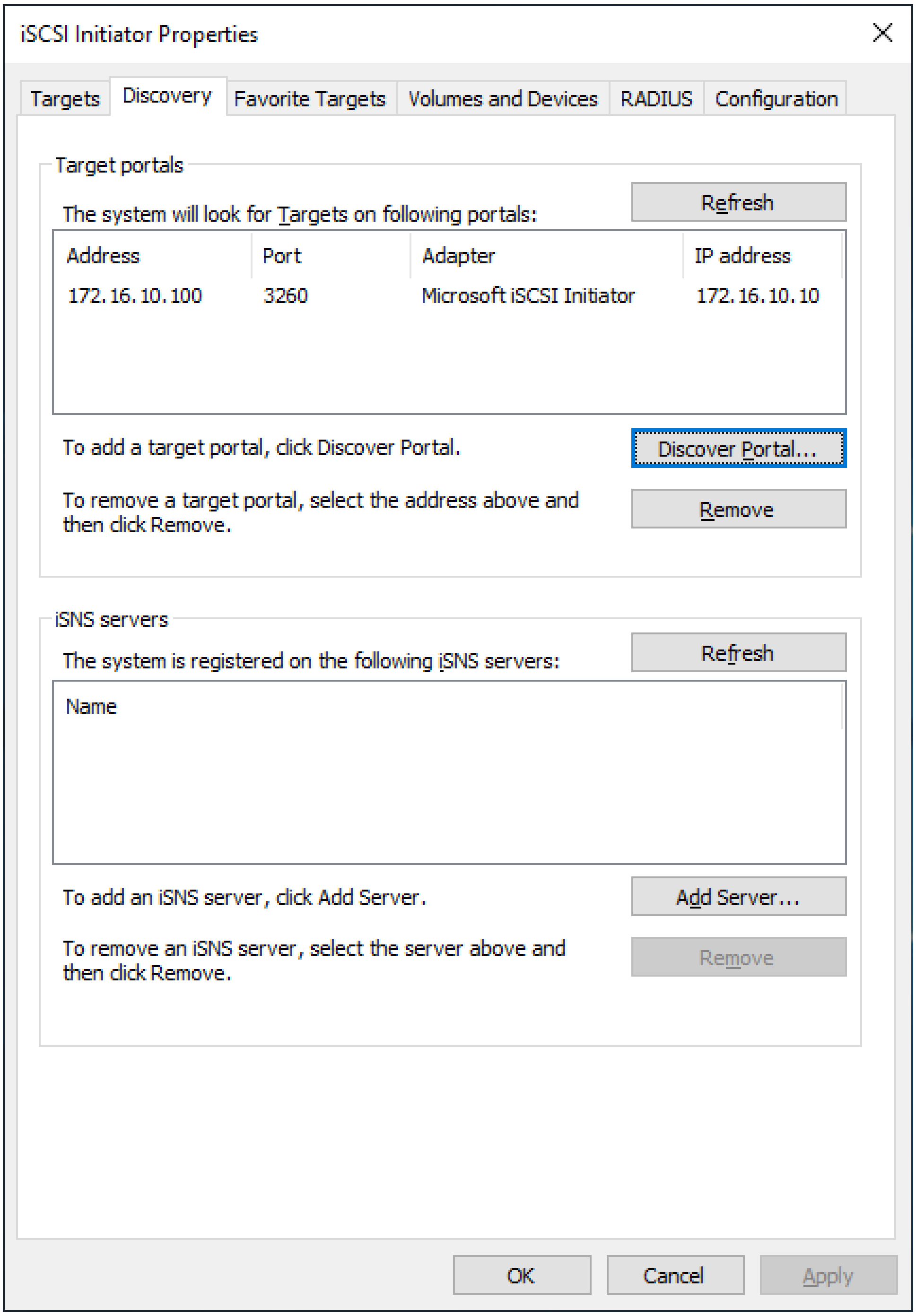
□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

5. The target portals are added on this server.



iSCSI Initiator Properties

Target portals

The system will look for Targets on following portals:

Address	Port	Adapter	IP address
172.16.10.100	3260	Microsoft iSCSI Initiator	172.16.10.10

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

iSNS servers

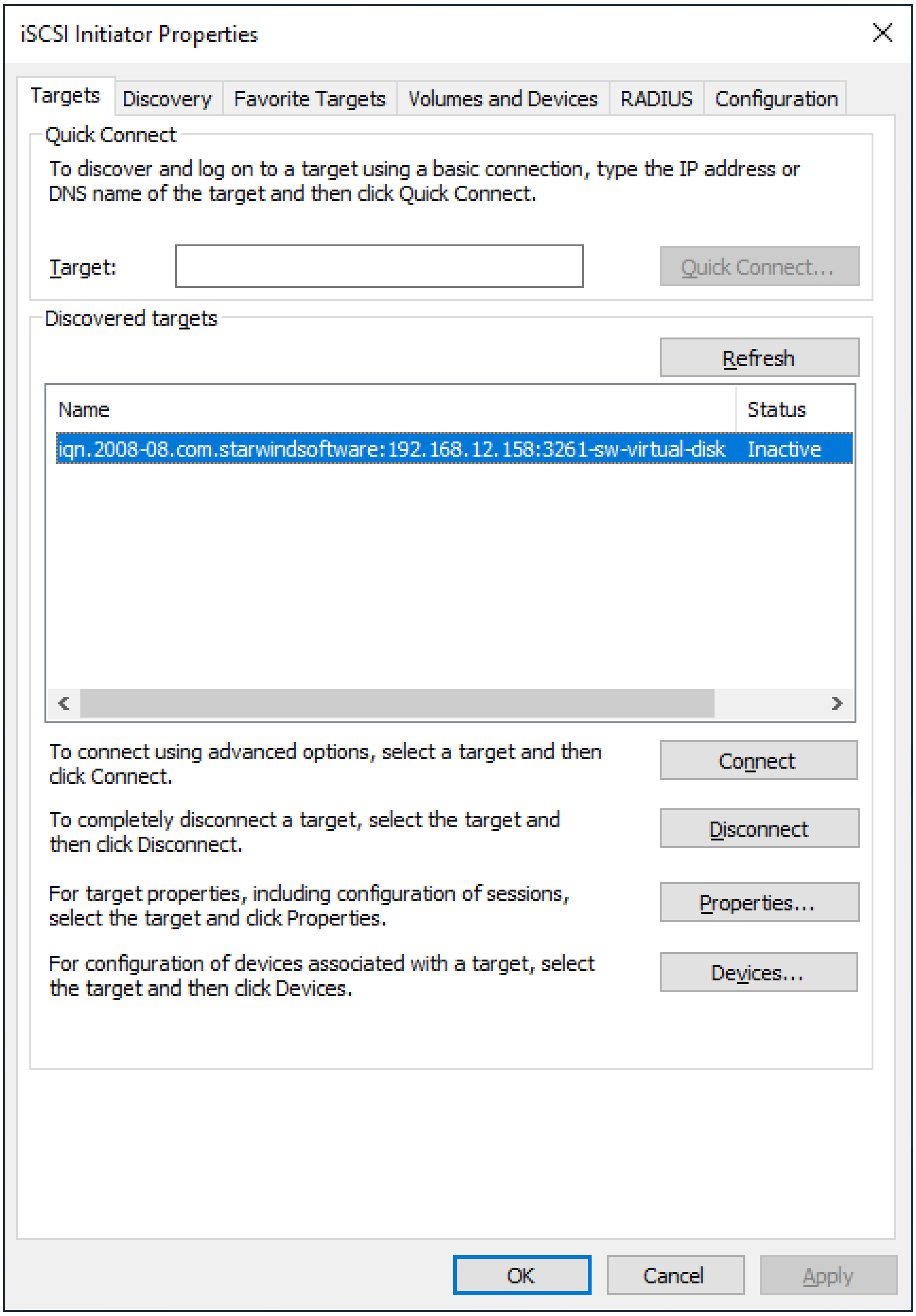
The system is registered on the following iSNS servers:

Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

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



iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2008-08.com.starwindsoftware:192.168.12.158:3261-sw-virtual-disk	Inactive

To connect using advanced options, select a target and then click Connect.

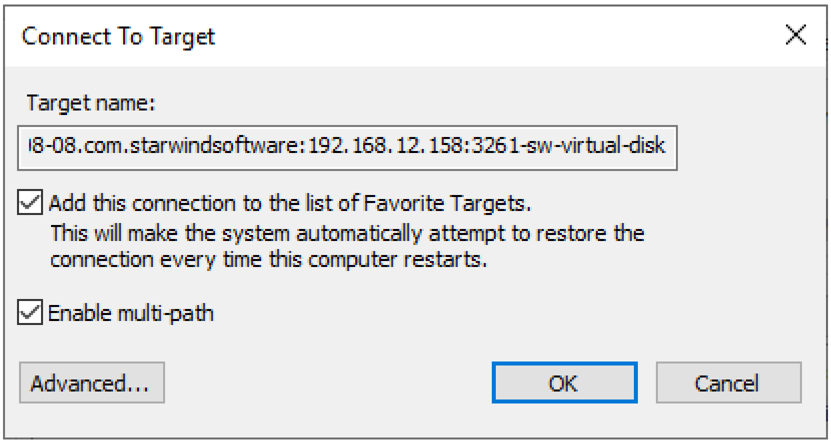
To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

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.



Connect To Target

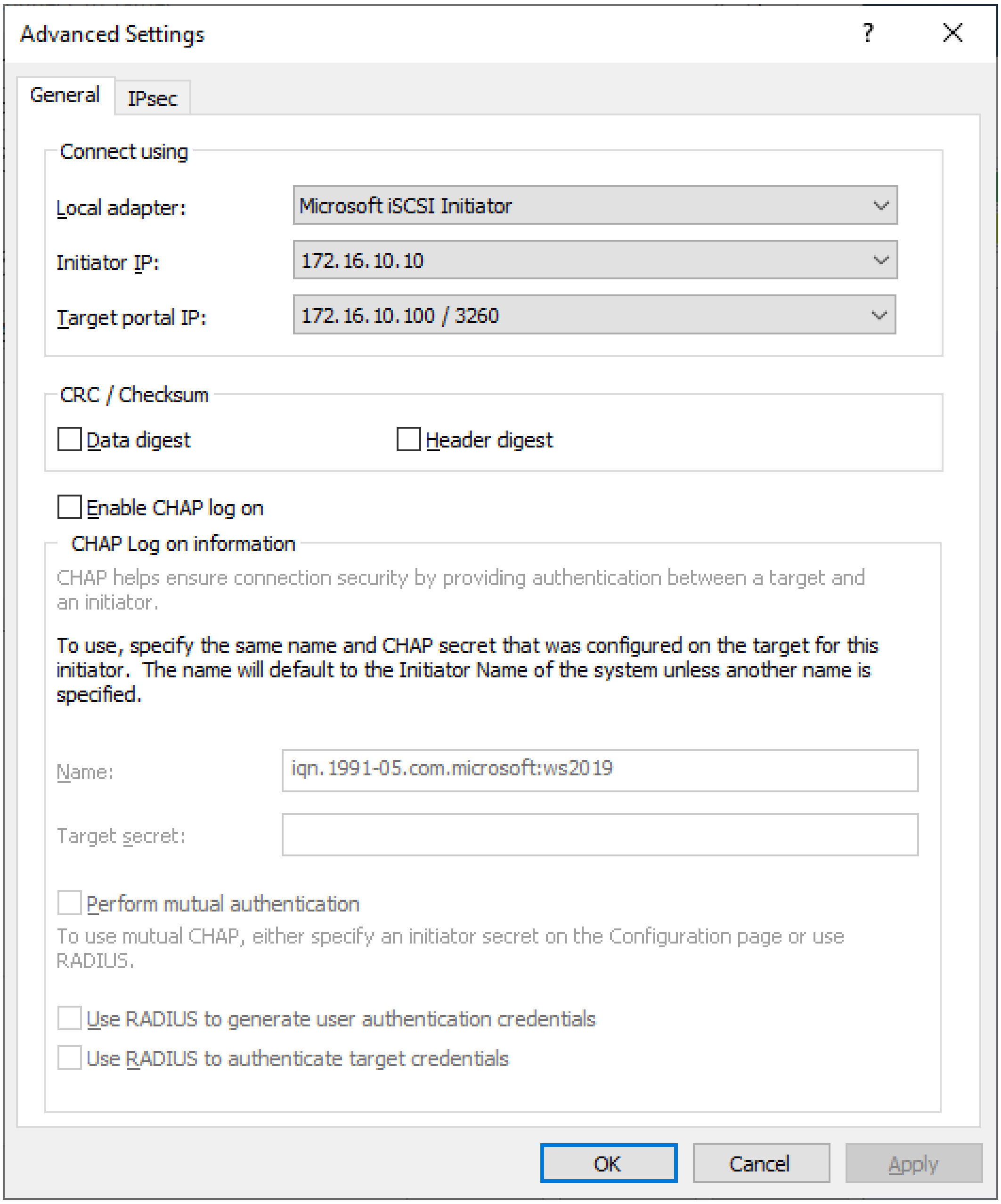
Target name:

i8-08.com.starwindsoftware:192.168.12.158:3261-sw-virtual-disk

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

☑ Enable multi-path

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.



Advanced Settings

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.16.10.10

Target portal IP: 172.16.10.100 / 3260

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:ws2019

Target secret:

□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

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.

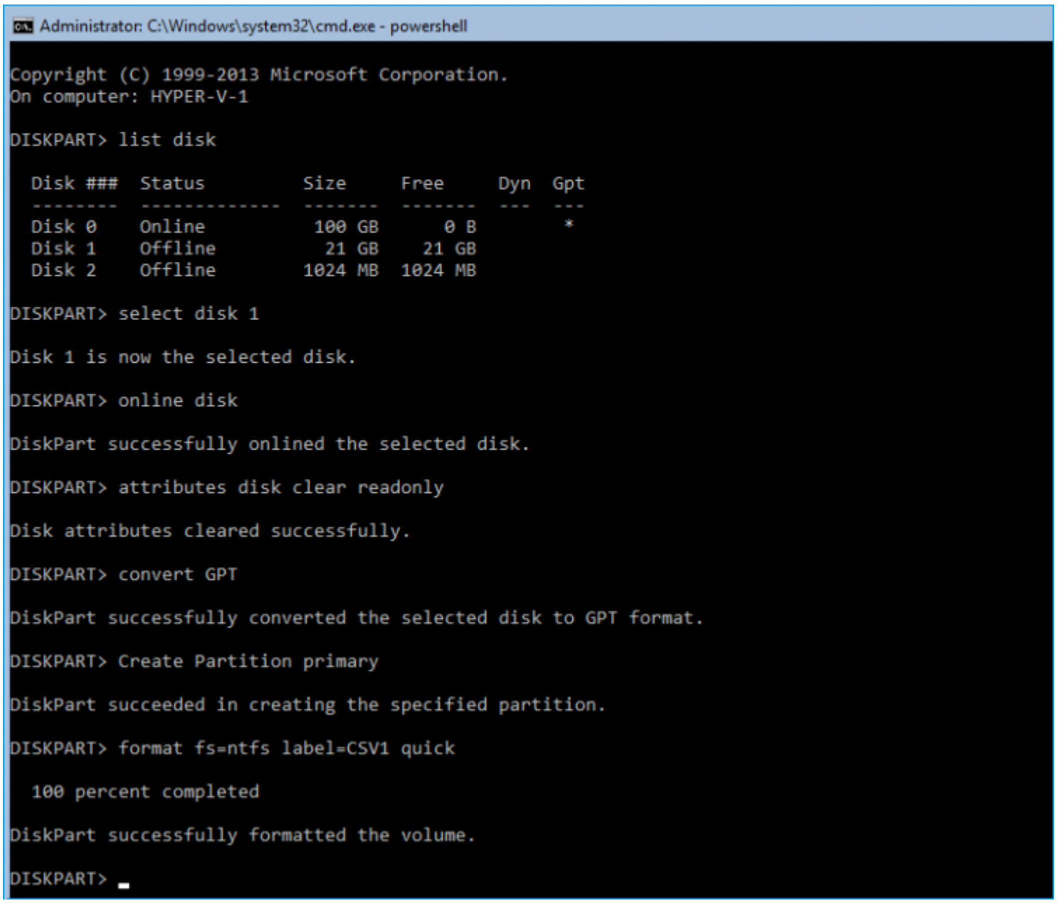
Connecting Disks to Servers

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.



```
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> _
```

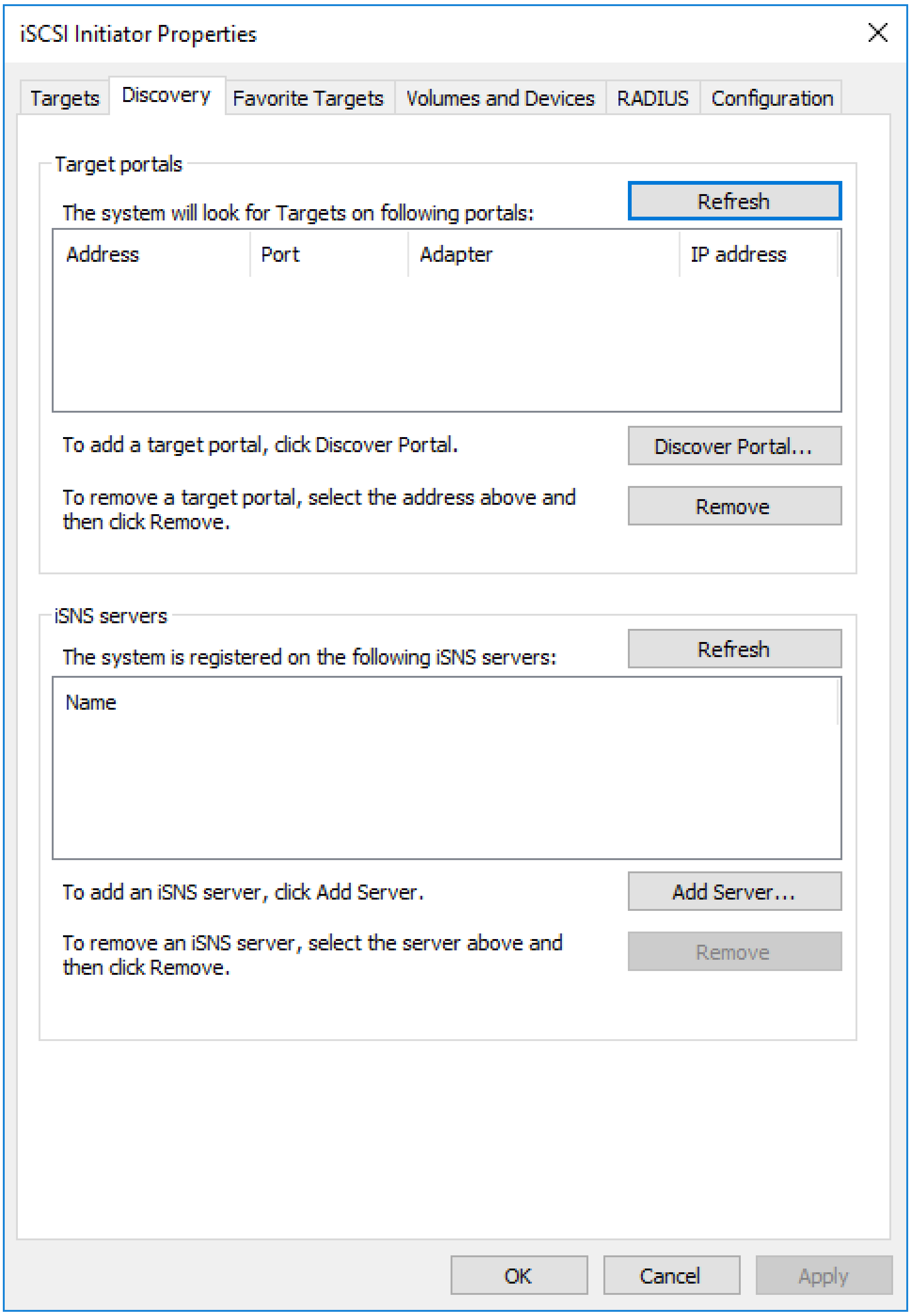
2. Perform the steps above on other compute servers.

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.



iSCSI Initiator Properties

Target portals

The system will look for Targets on following portals:

Address	Port	Adapter	IP address

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

iSNS servers

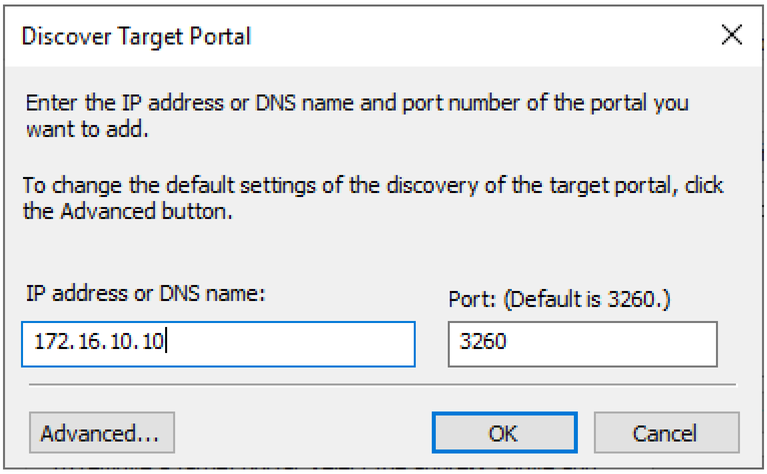
The system is registered on the following iSNS servers:

Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

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


Discover Target Portal

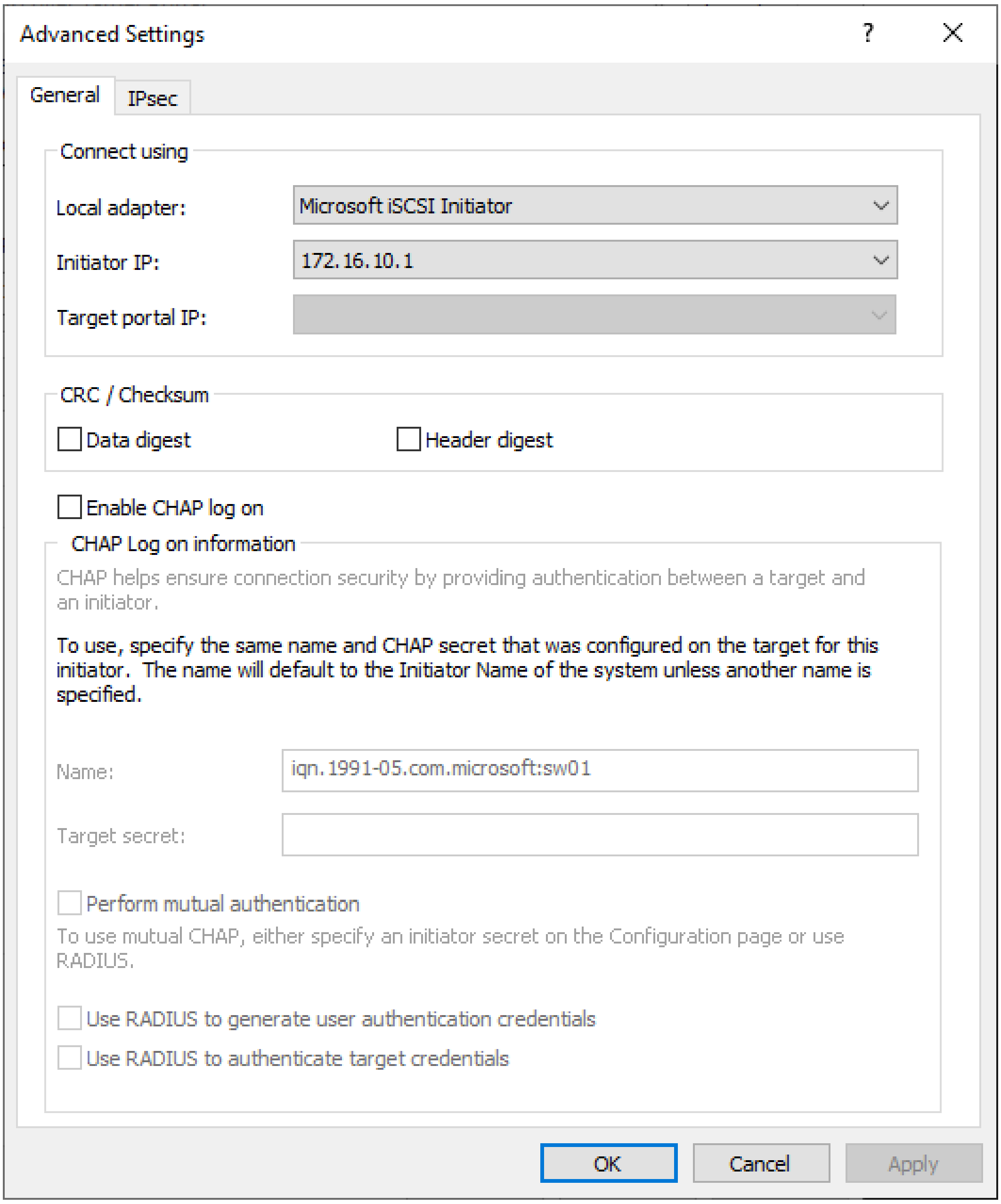
Enter the IP address or DNS name and port number of the portal you want to add.

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

IP address or DNS name: 172.16.10.10

Port: (Default is 3260.) 3260

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.



Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.16.10.1

Target portal IP:

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:sw01

Target secret:

□ Perform mutual authentication

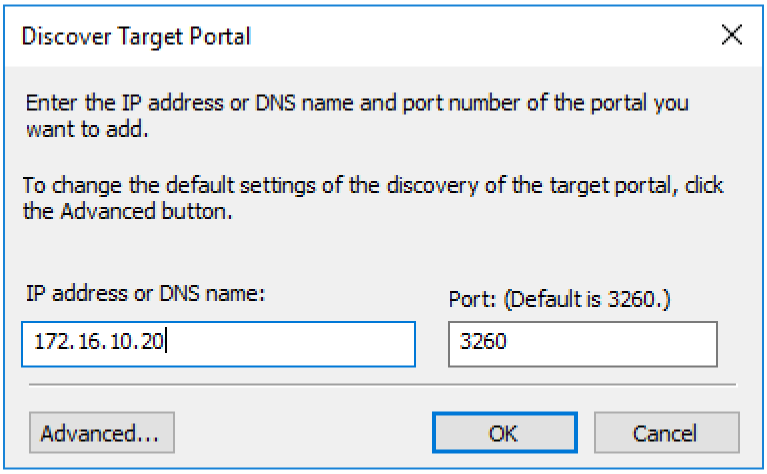
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

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

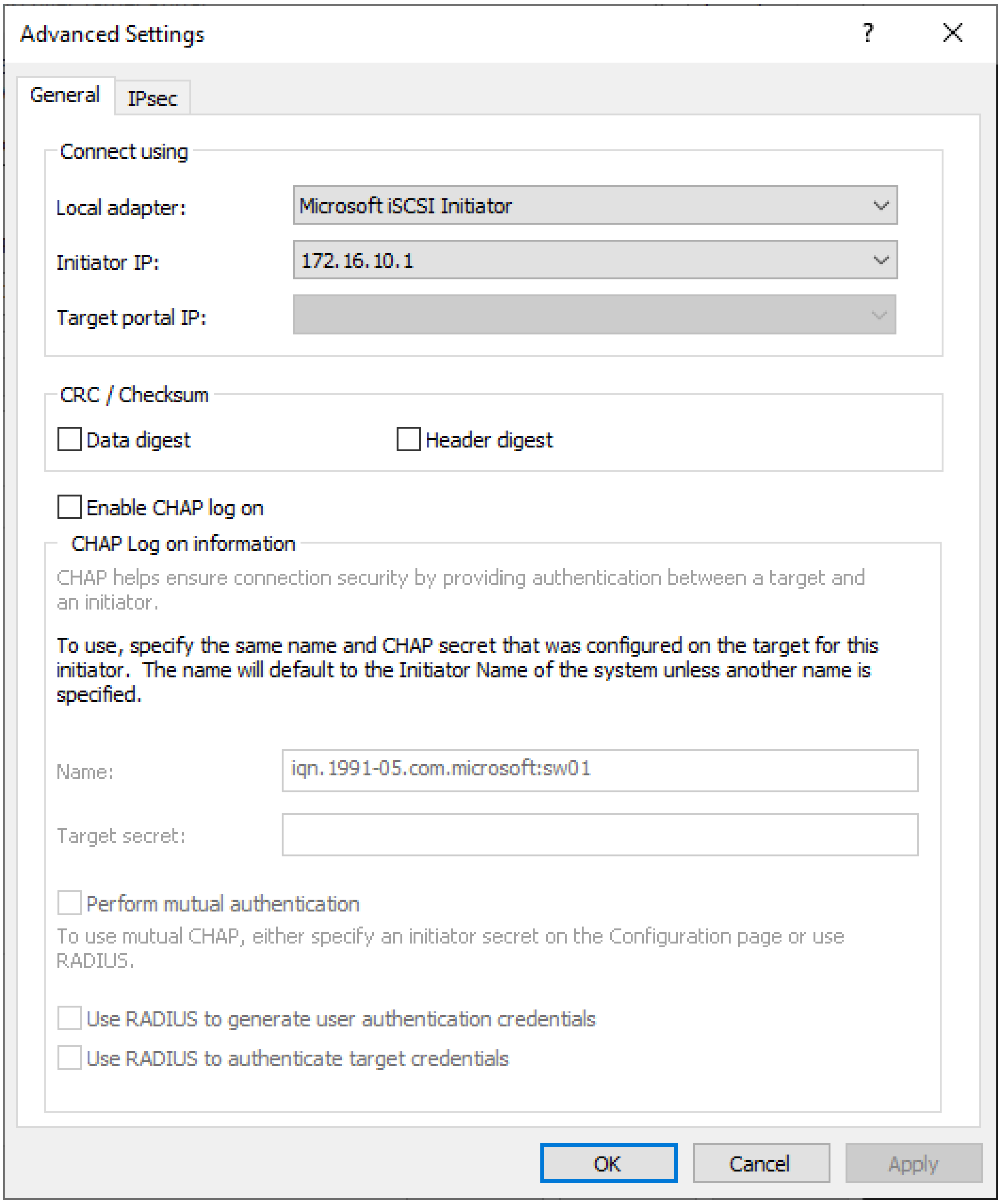
Enter the IP address or DNS name and port number of the portal you want to add.

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

IP address or DNS name: 172.16.10.20

Port: (Default is 3260.) 3260

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.



Advanced Settings

General | IPsec

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.16.10.1

Target portal IP:

CRC / Checksum

☐ Data digest ☐ Header digest

☐ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:sw01

Target secret:

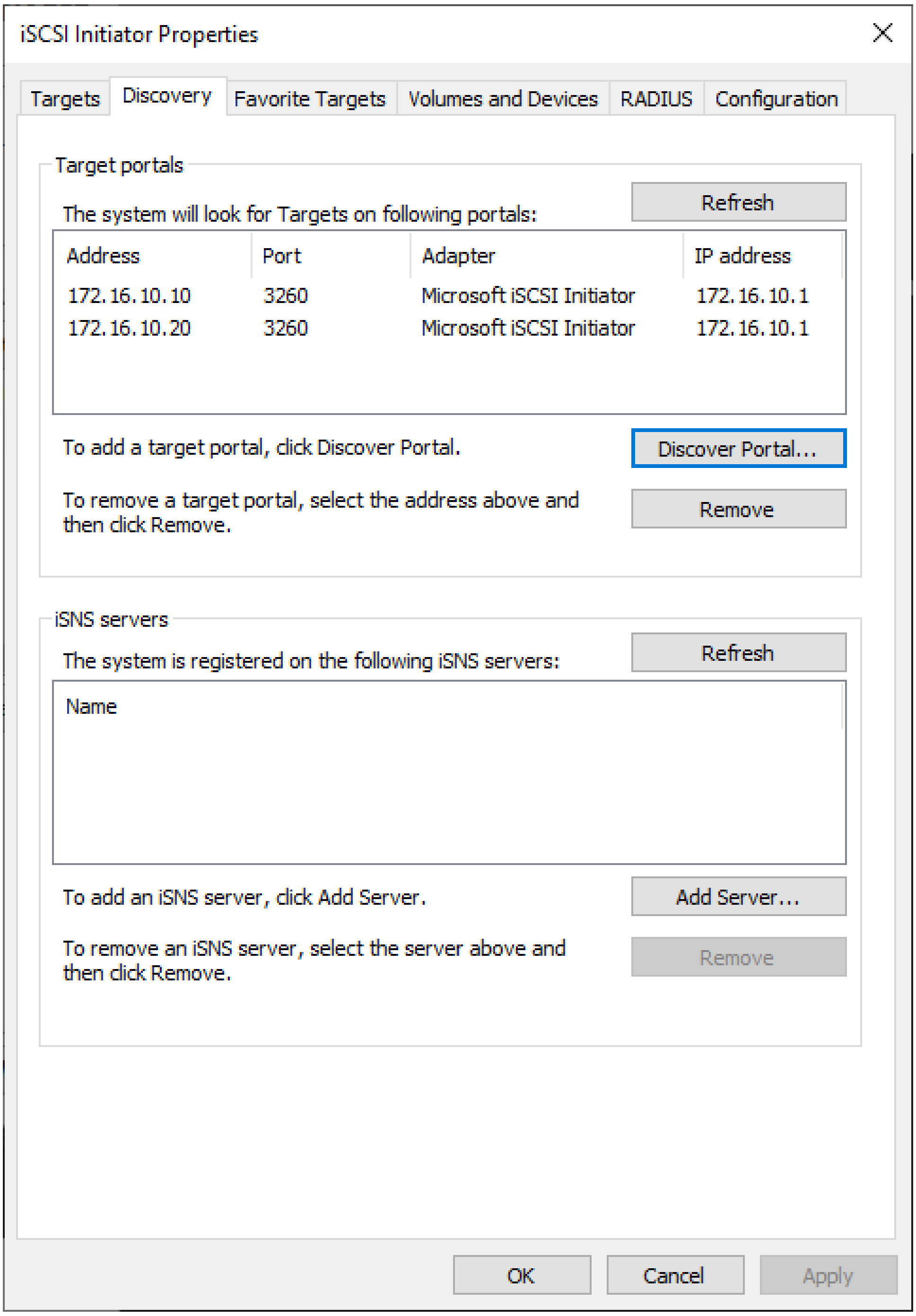
☐ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

☐ Use RADIUS to generate user authentication credentials

☐ Use RADIUS to authenticate target credentials

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



iSCSI Initiator Properties

Target portals

The system will look for Targets on following portals:

Address	Port	Adapter	IP address
172.16.10.10	3260	Microsoft iSCSI Initiator	172.16.10.1
172.16.10.20	3260	Microsoft iSCSI Initiator	172.16.10.1

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

iSNS servers

The system is registered on the following iSNS servers:

Name

To add an iSNS server, click Add Server.

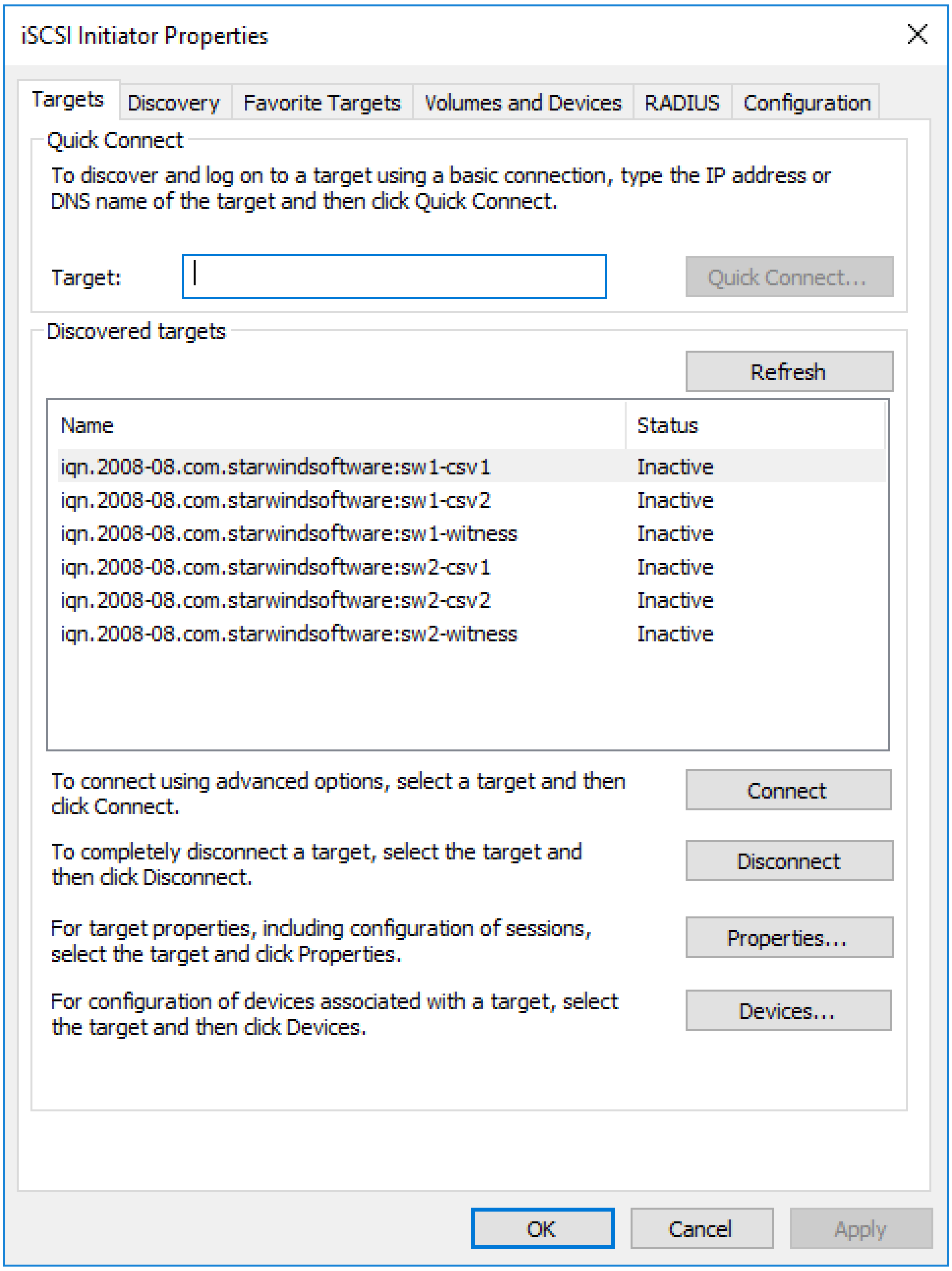
To remove an iSNS server, select the server above and then click Remove.

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.



iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2008-08.com.starwindsoftware:sw1-csv1	Inactive
iqn.2008-08.com.starwindsoftware:sw1-csv2	Inactive
iqn.2008-08.com.starwindsoftware:sw1-witness	Inactive
iqn.2008-08.com.starwindsoftware:sw2-csv1	Inactive
iqn.2008-08.com.starwindsoftware:sw2-csv2	Inactive
iqn.2008-08.com.starwindsoftware:sw2-witness	Inactive

To connect using advanced options, select a target and then click Connect.

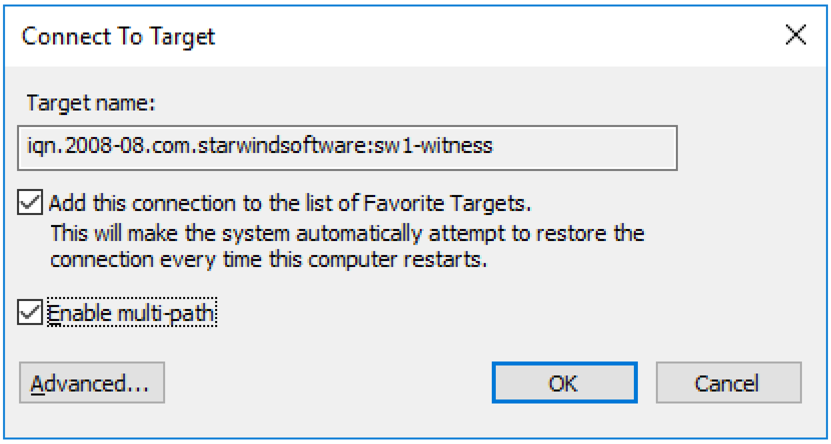
To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

2. Select the Witness target from the local server and click Connect.

3. Enable checkboxes as shown in the image below. Click Advanced.



Connect To Target

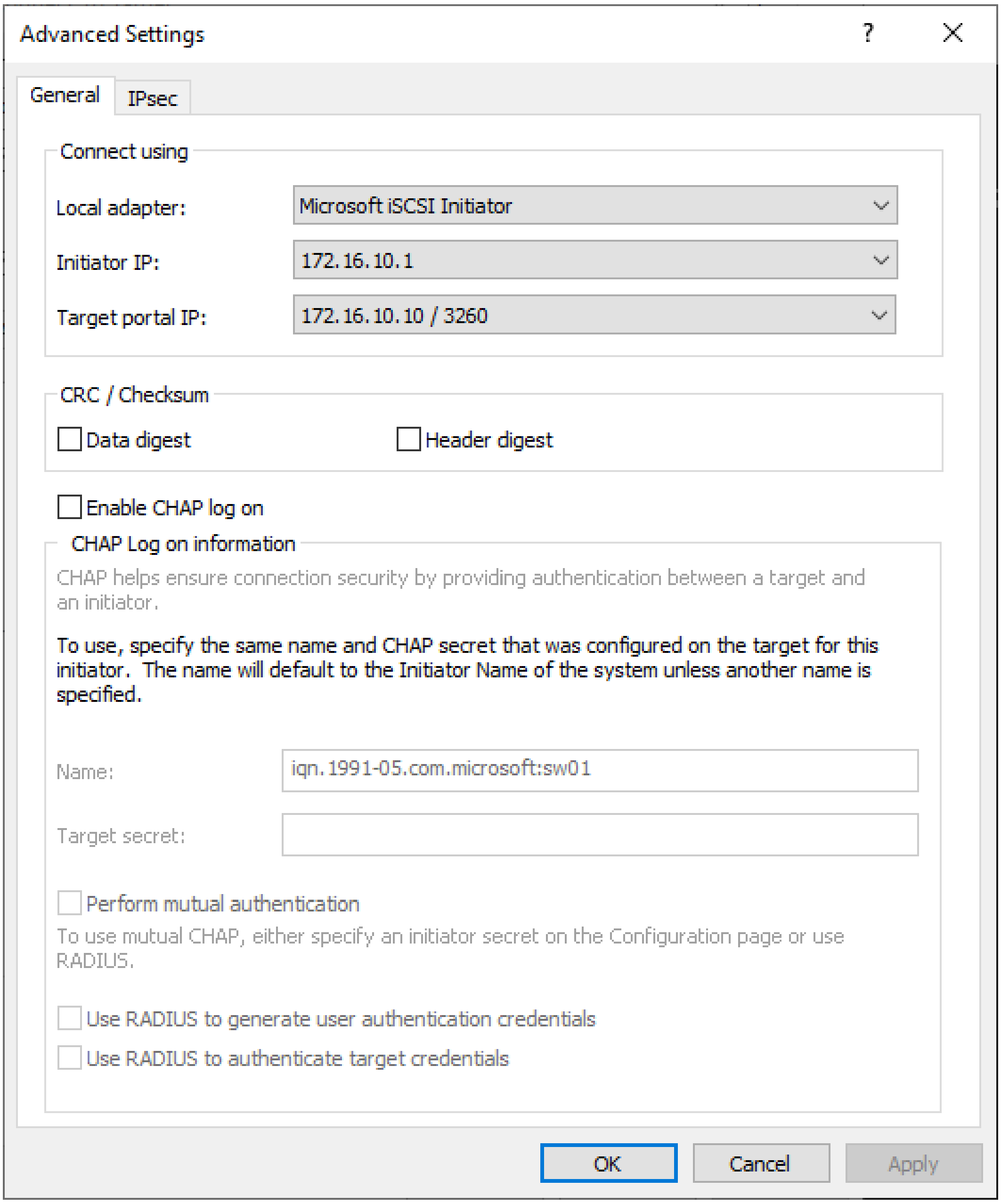
Target name:

iqn.2008-08.com.starwindsoftware:sw1-witness

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

☑ Enable multi-path

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.



Advanced Settings

General | IPsec

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.16.10.1

Target portal IP: 172.16.10.10 / 3260

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:sw01

Target secret:

□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

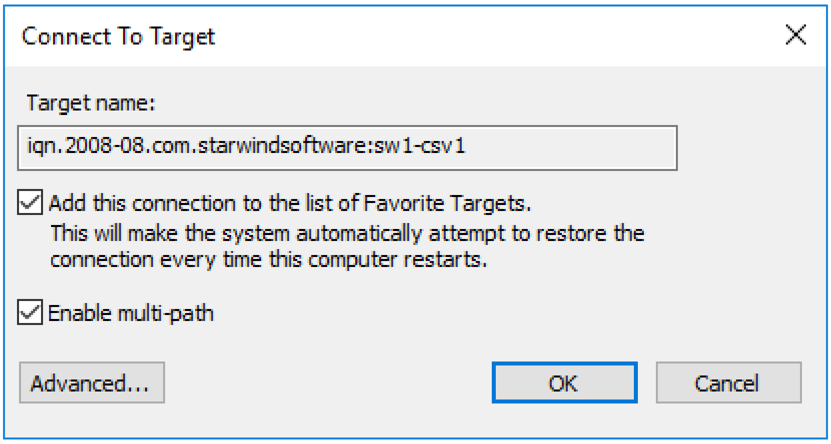
□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

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.


Connect To Target

Target name:

iqn.2008-08.com.starwindsoftware:sw1-csv1

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

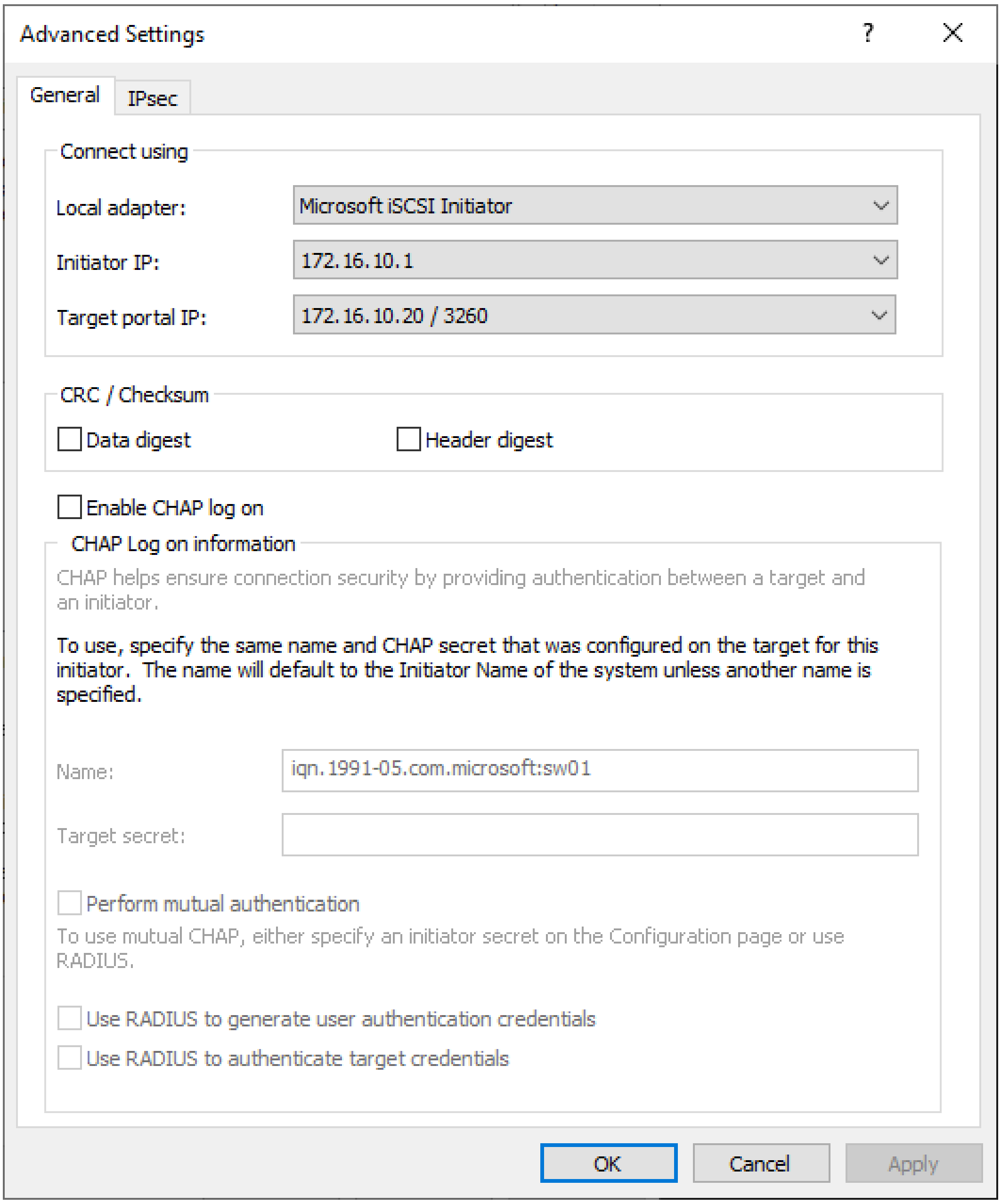
☑ Enable multi-path

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.



Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: 172.16.10.1

Target portal IP: 172.16.10.20 / 3260

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:sw01

Target secret:

□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

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

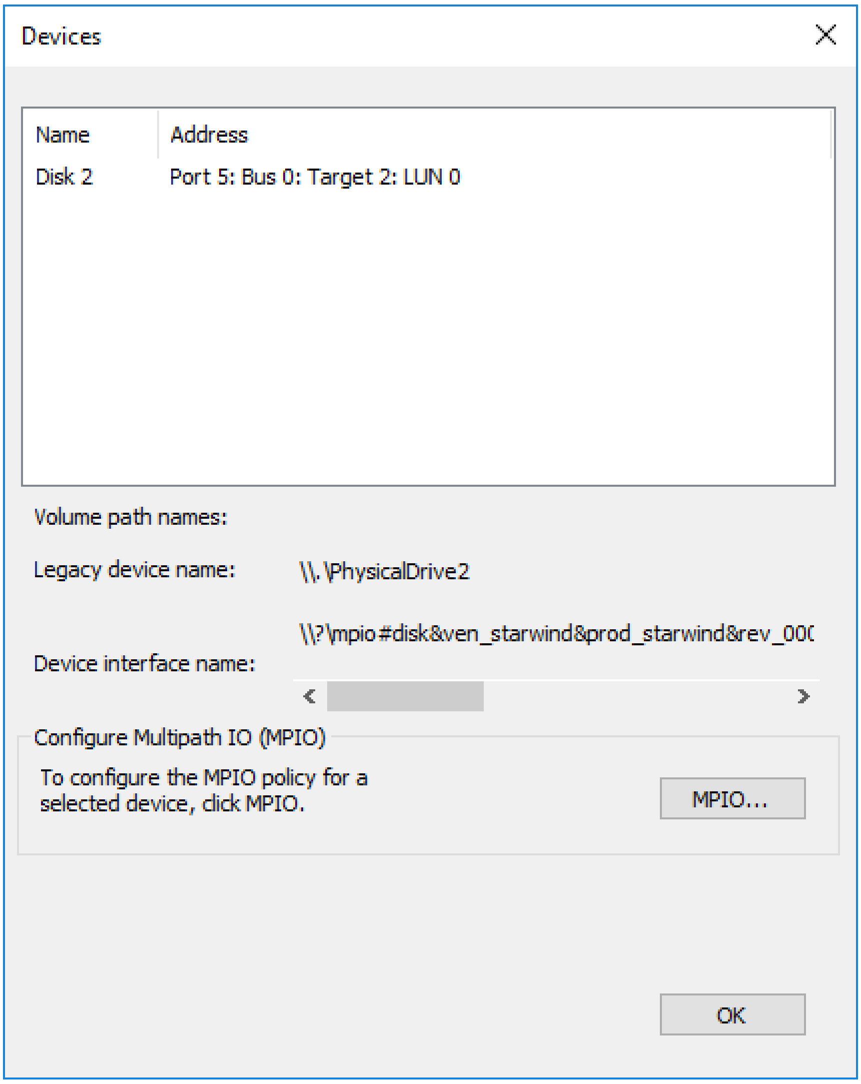
12. Repeat the steps 1-11 on the other StarWind node, specifying corresponding data channel IP addresses.

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.



Devices

Name	Address
Disk 2	Port 5: Bus 0: Target 2: LUN 0

Volume path names:

Legacy device name: \\.\PhysicalDrive2

Device interface name: \\?\mpio#disk&ven_starwind&prod_starwind&rev_00(

Configure Multipath IO (MPIO)

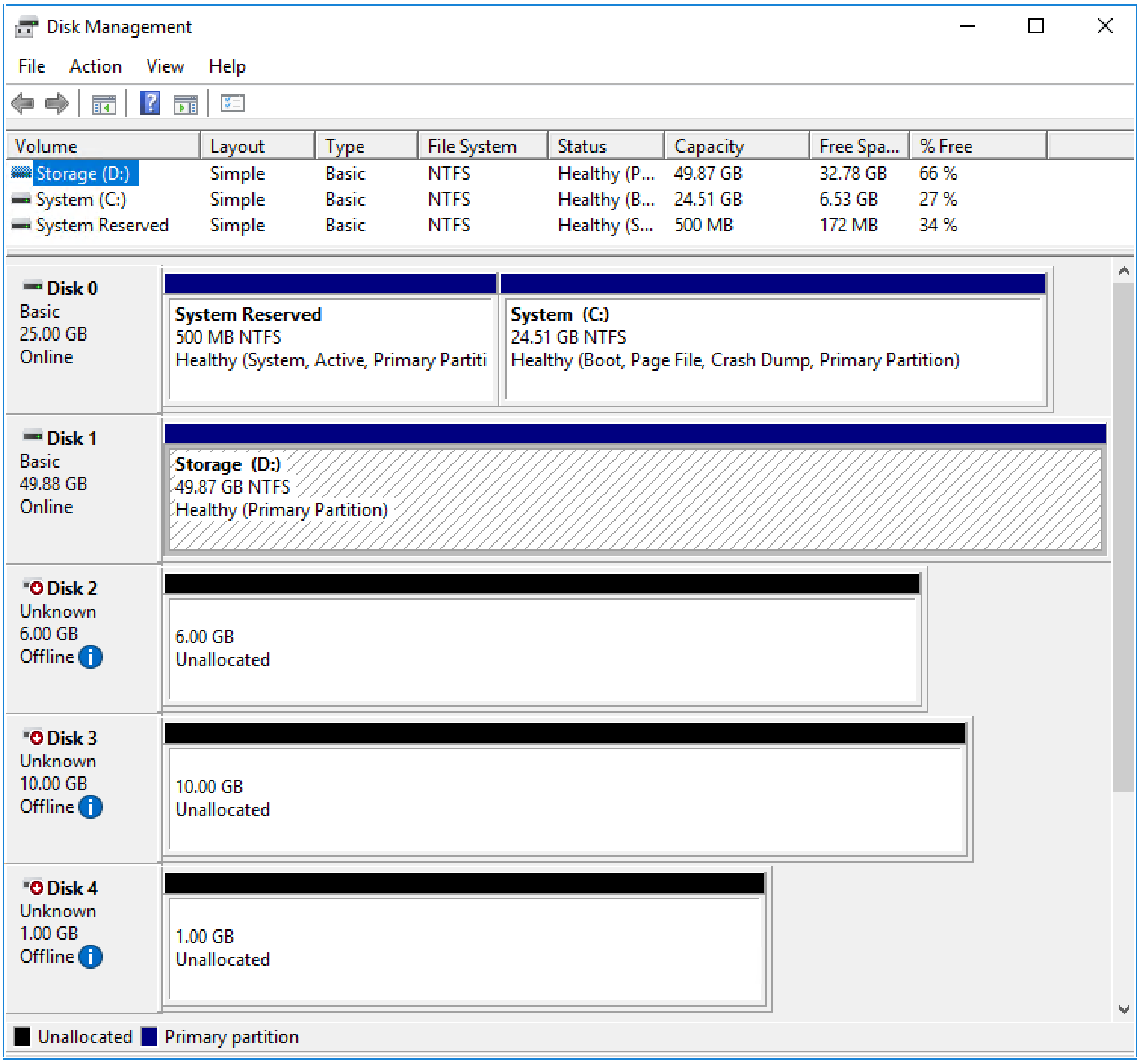
To configure the MPIO policy for a selected device, click MPIO.

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.



Disk Management

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
Storage (D:)	Simple	Basic	NTFS	Healthy (P...	49.87 GB	32.78 GB	66 %
System (C:)	Simple	Basic	NTFS	Healthy (B...	24.51 GB	6.53 GB	27 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	500 MB	172 MB	34 %

Disk 0
Basic
25.00 GB
Online

System Reserved
500 MB NTFS
Healthy (System, Active, Primary Partiti

System (C:)
24.51 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
49.88 GB
Online

Storage (D:)
49.87 GB NTFS
Healthy (Primary Partition)

Disk 2
Unknown
6.00 GB
Offline

6.00 GB
Unallocated

Disk 3
Unknown
10.00 GB
Offline

10.00 GB
Unallocated

Disk 4
Unknown
1.00 GB
Offline

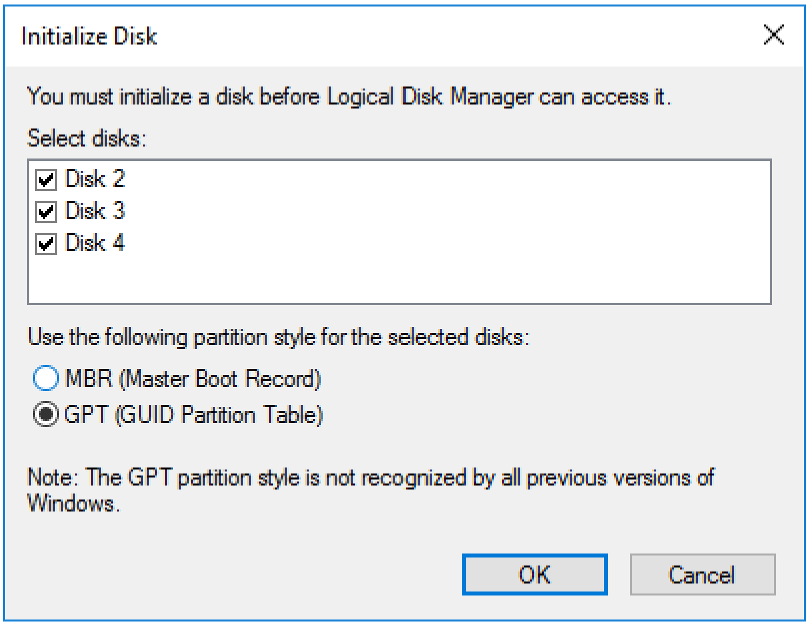
1.00 GB
Unallocated

■ Unallocated ■ Primary partition

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.



Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 2
☑ Disk 3
☑ Disk 4

Use the following partition style for the selected disks:

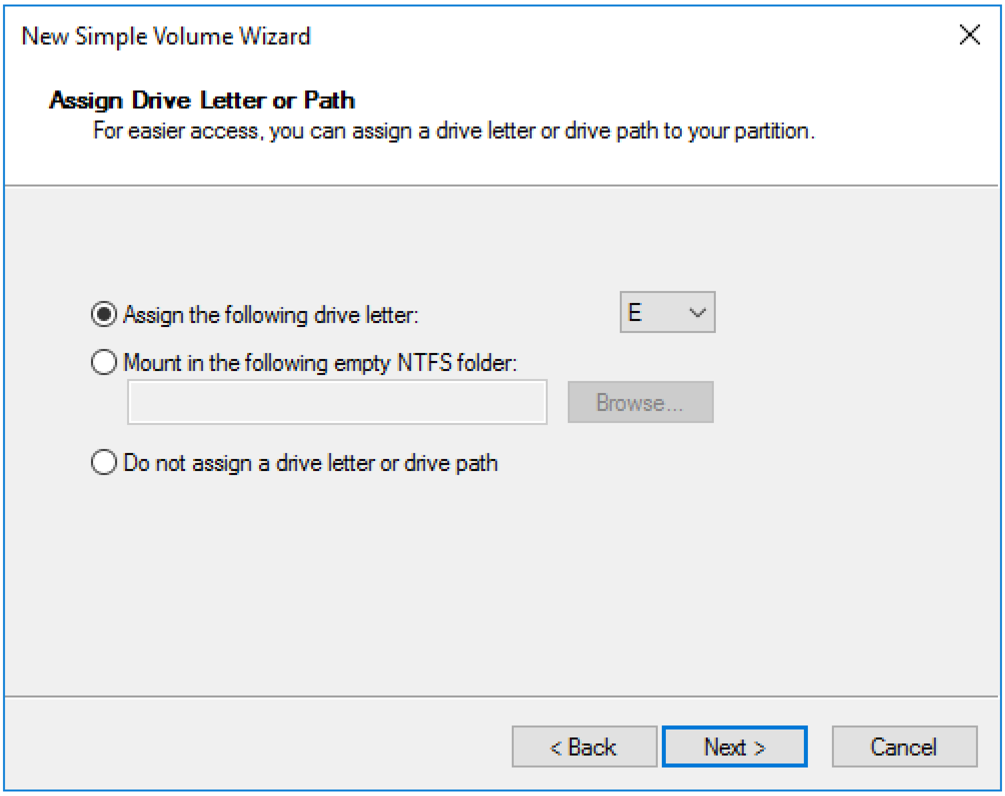
○ MBR (Master Boot Record)
● GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

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.



New Simple Volume Wizard

Assign Drive Letter or Path

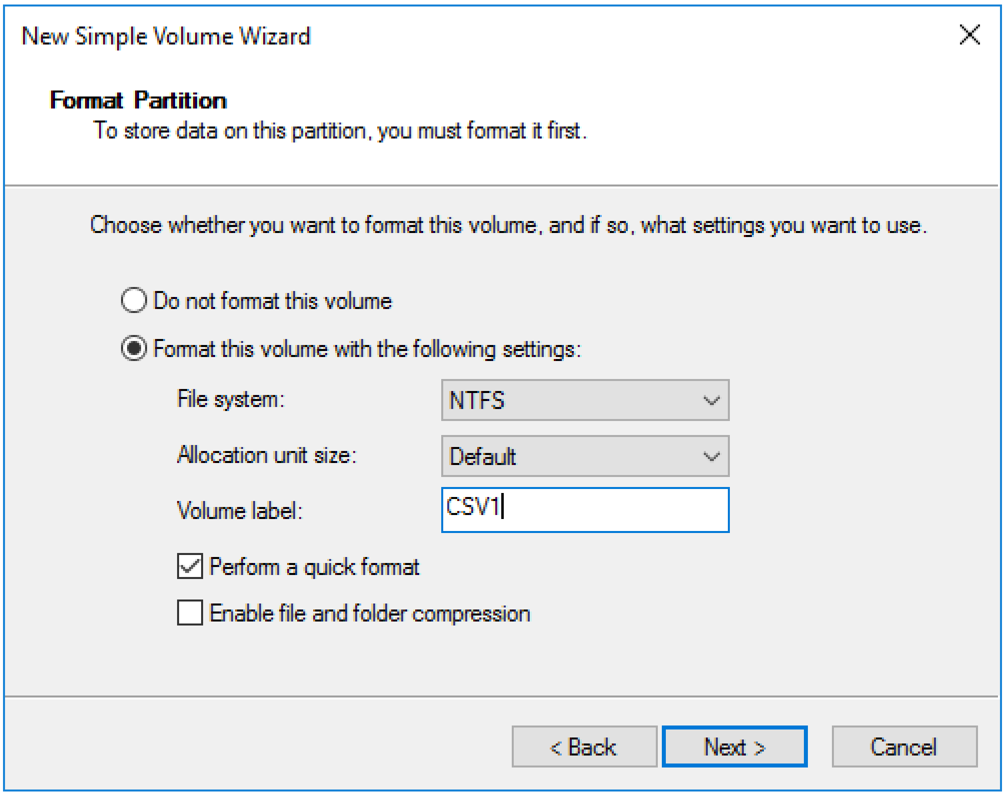
For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: E

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

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

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

Allocation unit size: Default

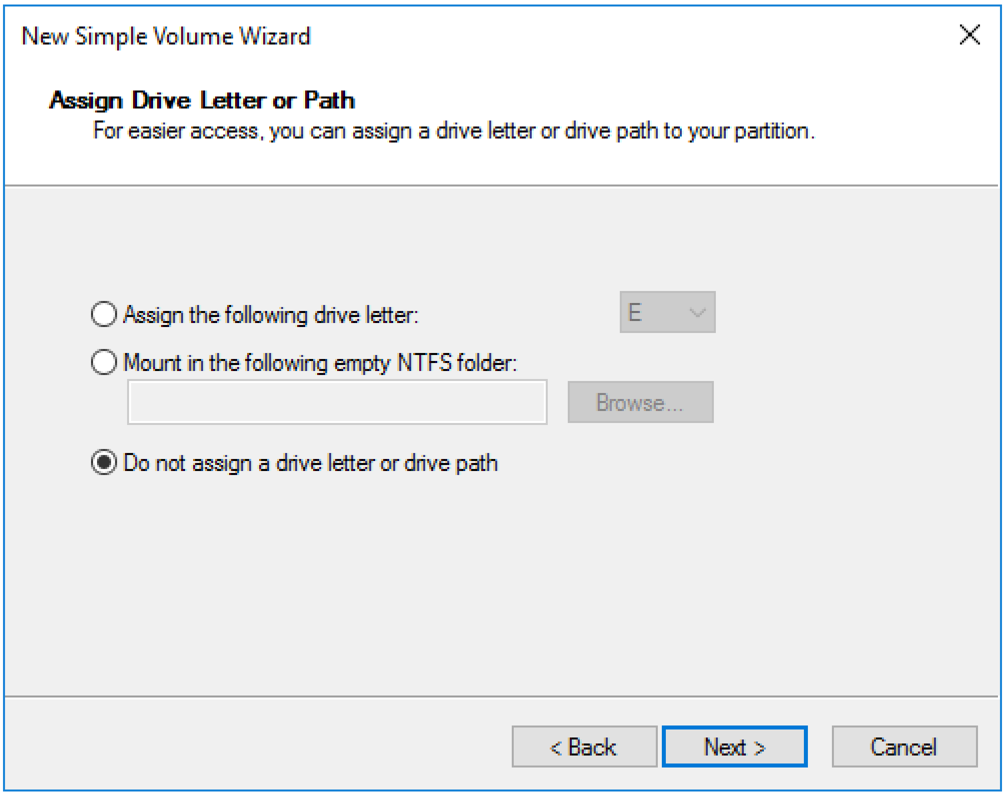
Volume label: CSV1

☑ Perform a quick format

□ Enable file and folder compression

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.



New Simple Volume Wizard

Assign Drive Letter or Path

For easier access, you can assign a drive letter or drive path to your partition.

○ Assign the following drive letter: E

○ Mount in the following empty NTFS folder:

● Do not assign a drive letter or drive path

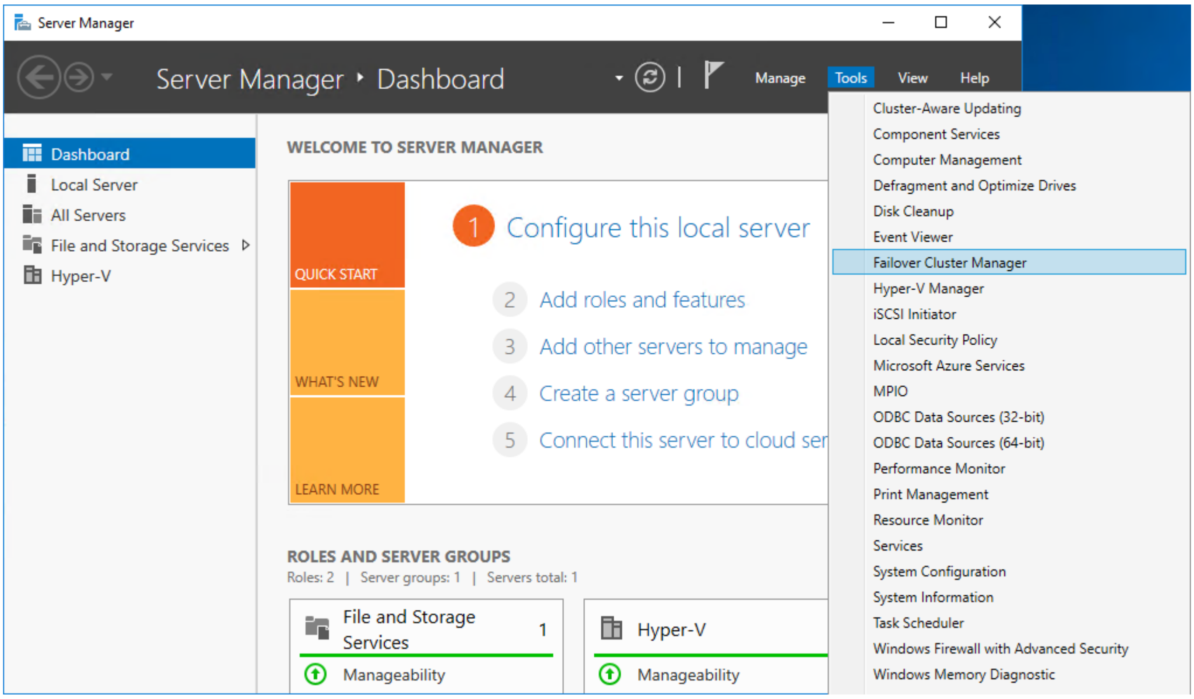
11. On the partner node, open the Disk Management snap-in. All StarWind disks will appear offline. If the status is different from the one shown below,
click Action->Refresh in the top menu to update the information about the disks.

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

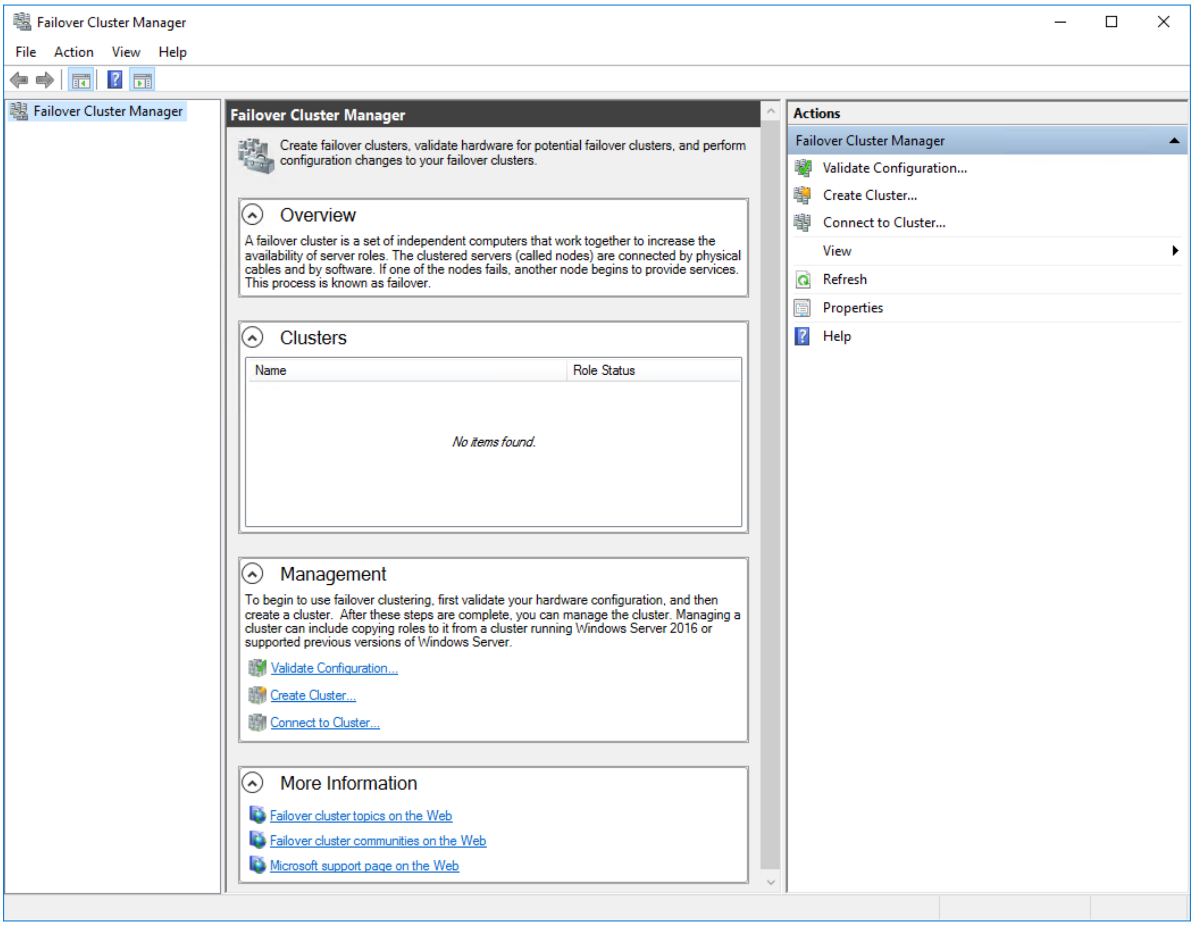
Creating A Failover Cluster In Windows Server

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.



Failover Cluster Manager

Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

Overview

A failover cluster is a set of independent computers that work together to increase the availability of server roles. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services. This process is known as failover.

Clusters

Name	Role Status

No items found.

Management

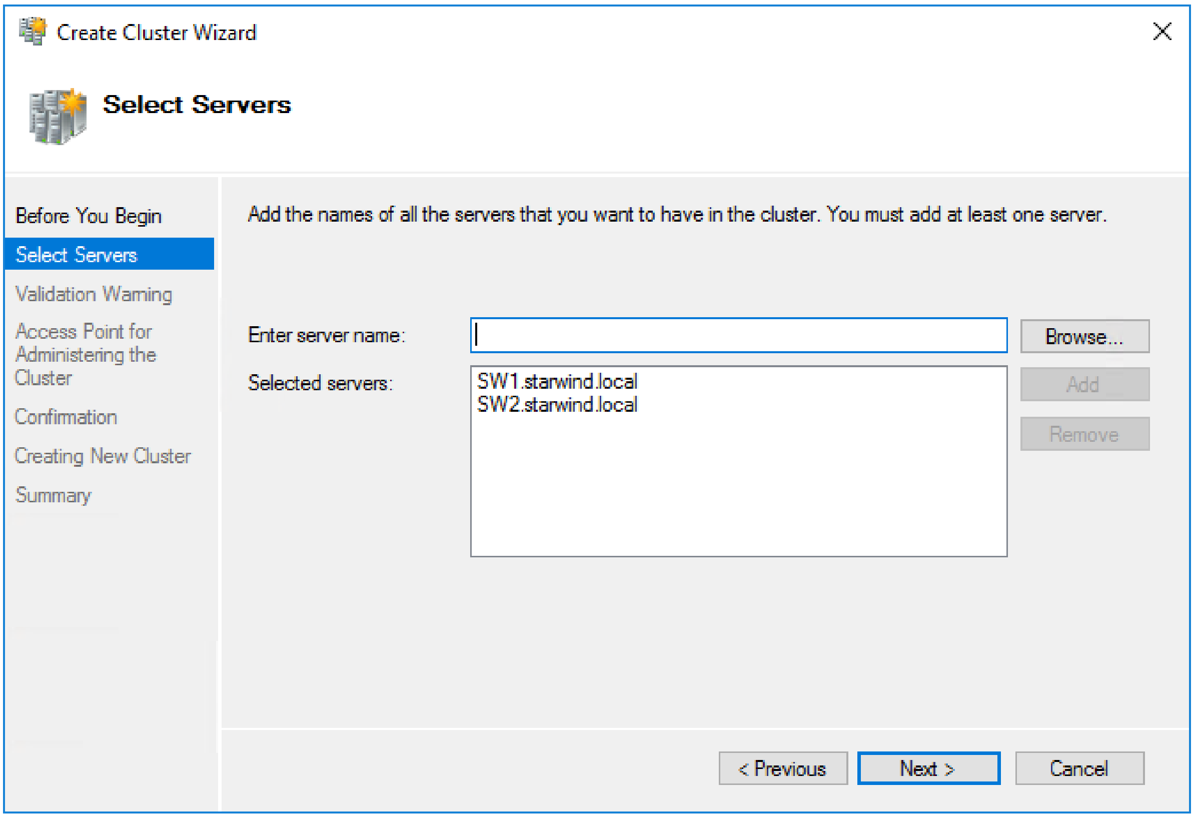
To begin to use failover clustering, first validate your hardware configuration, and then create a cluster. After these steps are complete, you can manage the cluster. Managing a cluster can include copying roles to it from a cluster running Windows Server 2016 or supported previous versions of Windows Server.

- Validate Configuration...
- Create Cluster...
- Connect to Cluster...

More Information

- Failover cluster topics on the Web
- Failover cluster communities on the Web
- Microsoft support page on the Web

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

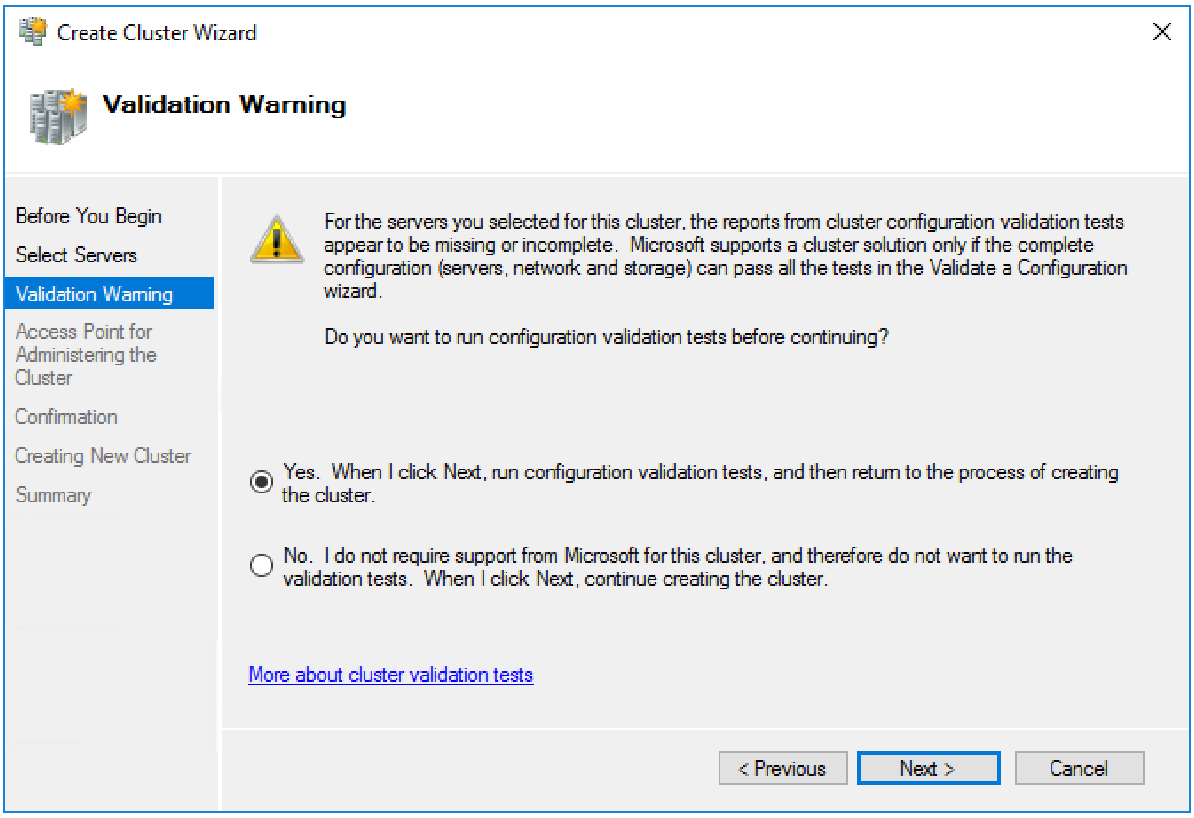


Add the names of all the servers that you want to have in the cluster. You must add at least one server.

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.



Create Cluster Wizard

Validation Warning

For the servers you selected for this cluster, the reports from cluster configuration validation tests appear to be missing or incomplete. Microsoft supports a cluster solution only if the complete configuration (servers, network and storage) can pass all the tests in the Validate a Configuration wizard.

Do you want to run configuration validation tests before continuing?

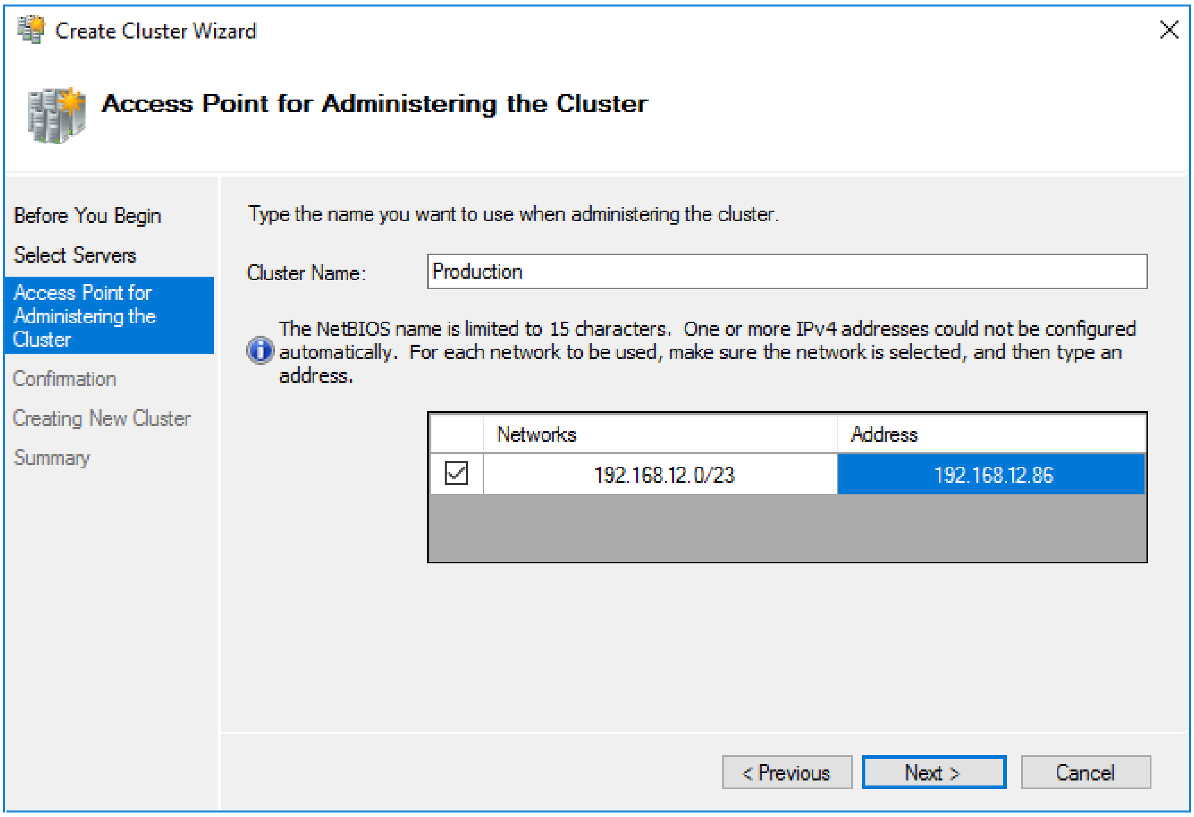
● Yes. When I click Next, run configuration validation tests, and then return to the process of creating the cluster.

○ No. I do not require support from Microsoft for this cluster, and therefore do not want to run the validation tests. When I click Next, continue creating the cluster.

More about cluster validation tests

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.



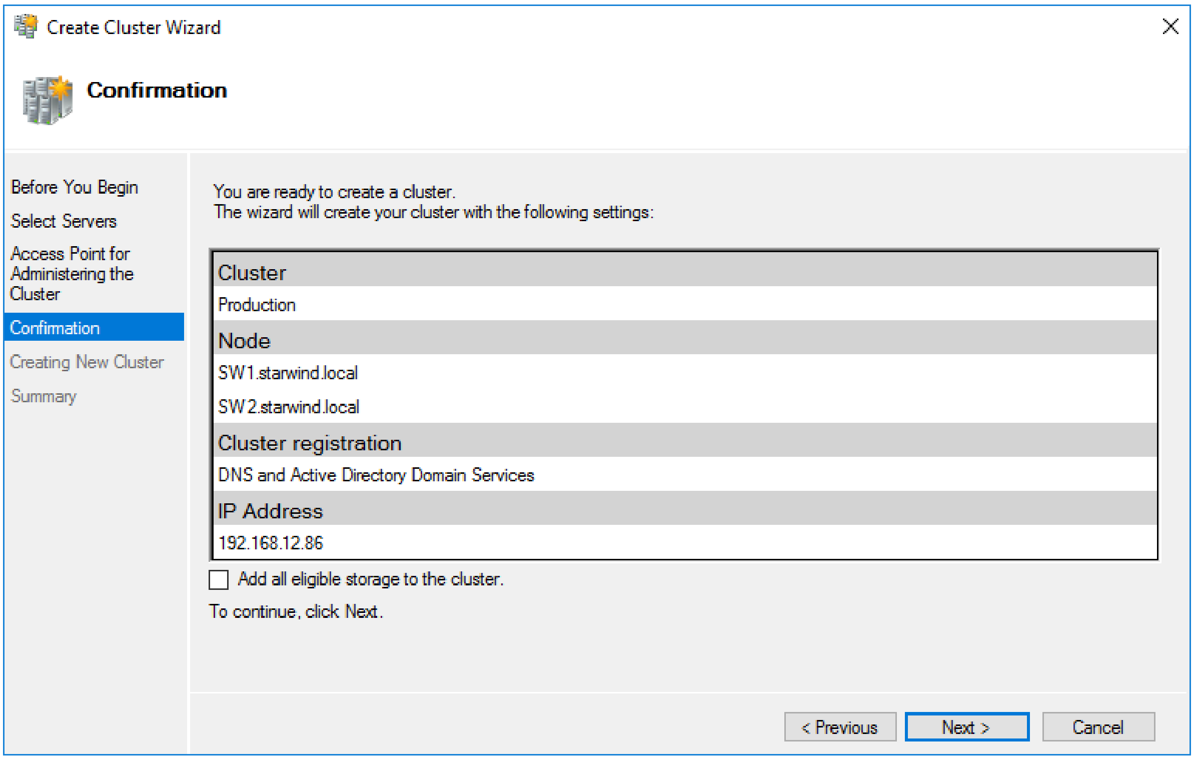
Type the name you want to use when administering the cluster.

Cluster Name: Production

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
☑	192.168.12.0/23	192.168.12.86

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



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

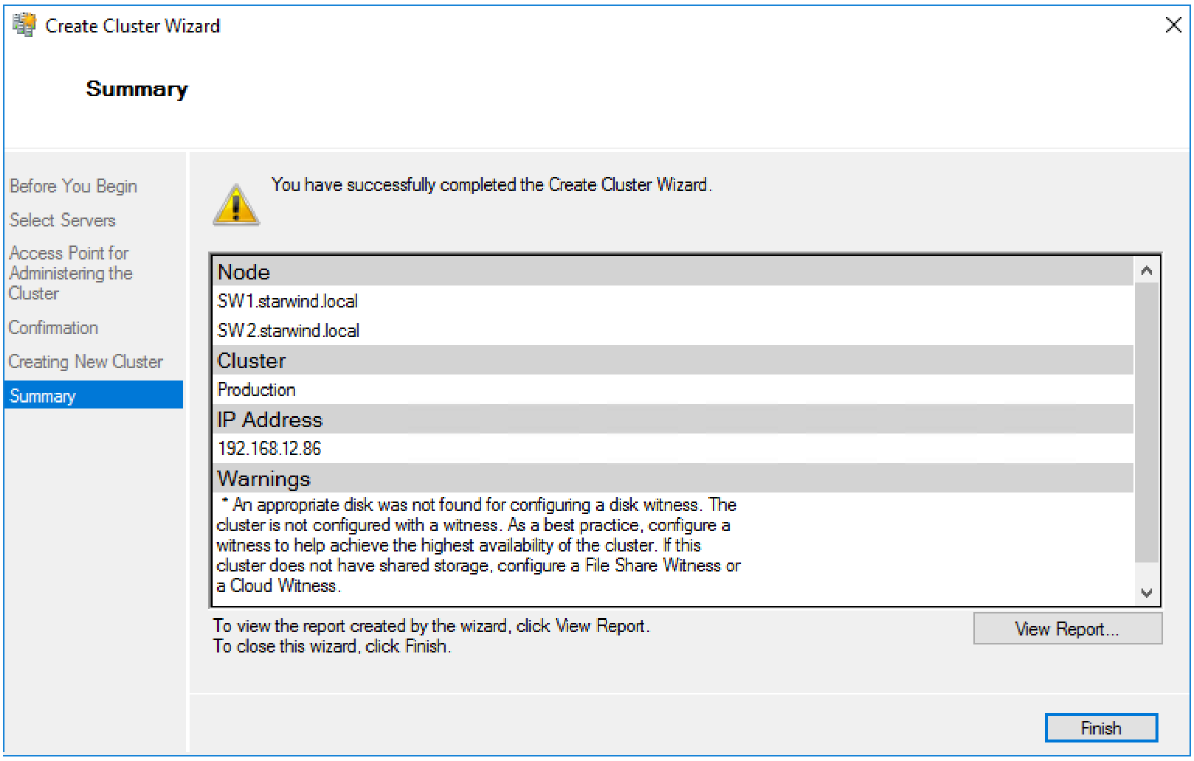
IP Address
192.168.12.86

□ Add all eligible storage to the cluster.

To continue, click Next.

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.



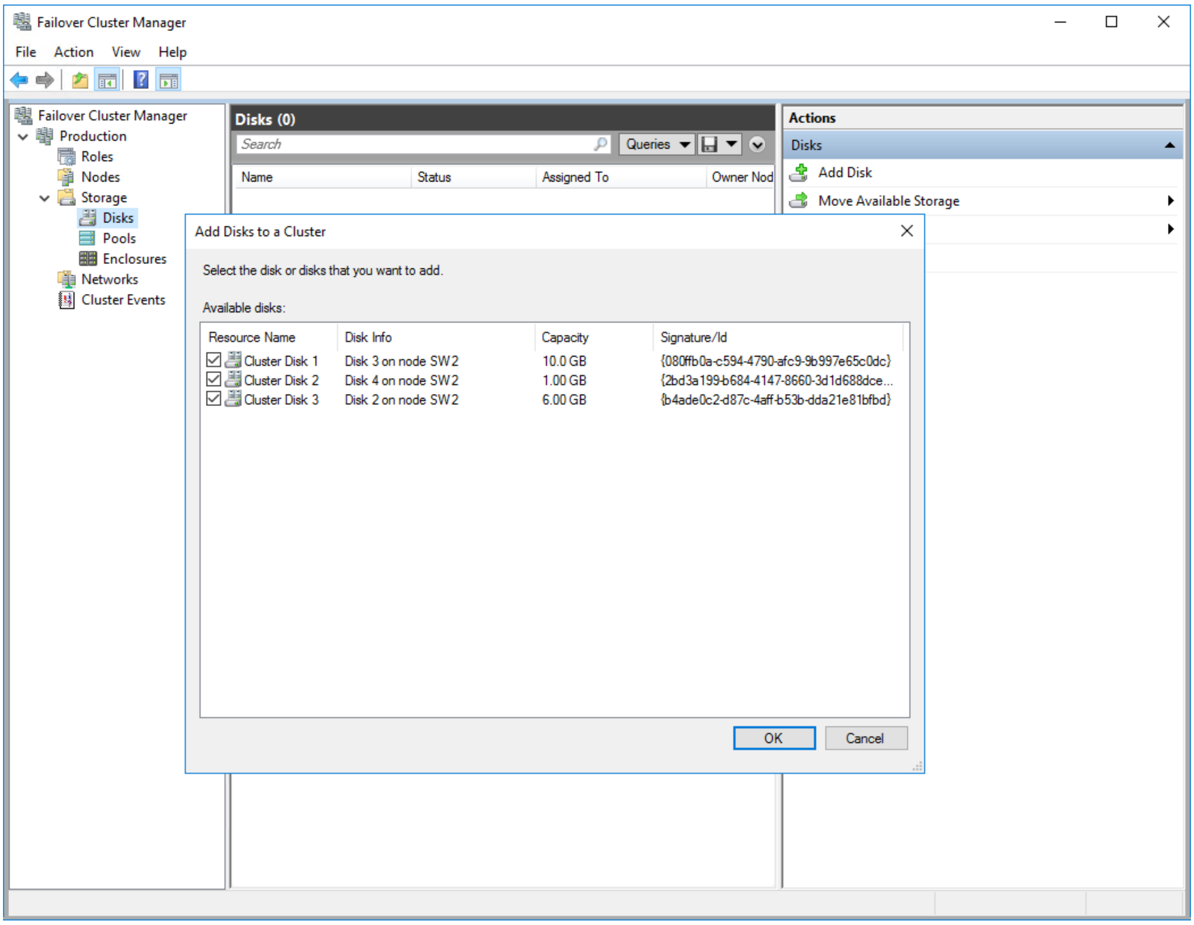
You have successfully completed the Create Cluster Wizard.

Node
SW1.starwind.local
SW2.starwind.local
Cluster
Production
IP Address
192.168.12.86
Warnings
* An appropriate disk was not found for configuring a disk witness. The cluster is not configured with a witness. As a best practice, configure a witness to help achieve the highest availability of the cluster. If this cluster does not have shared storage, configure a File Share Witness or a Cloud Witness.

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

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.



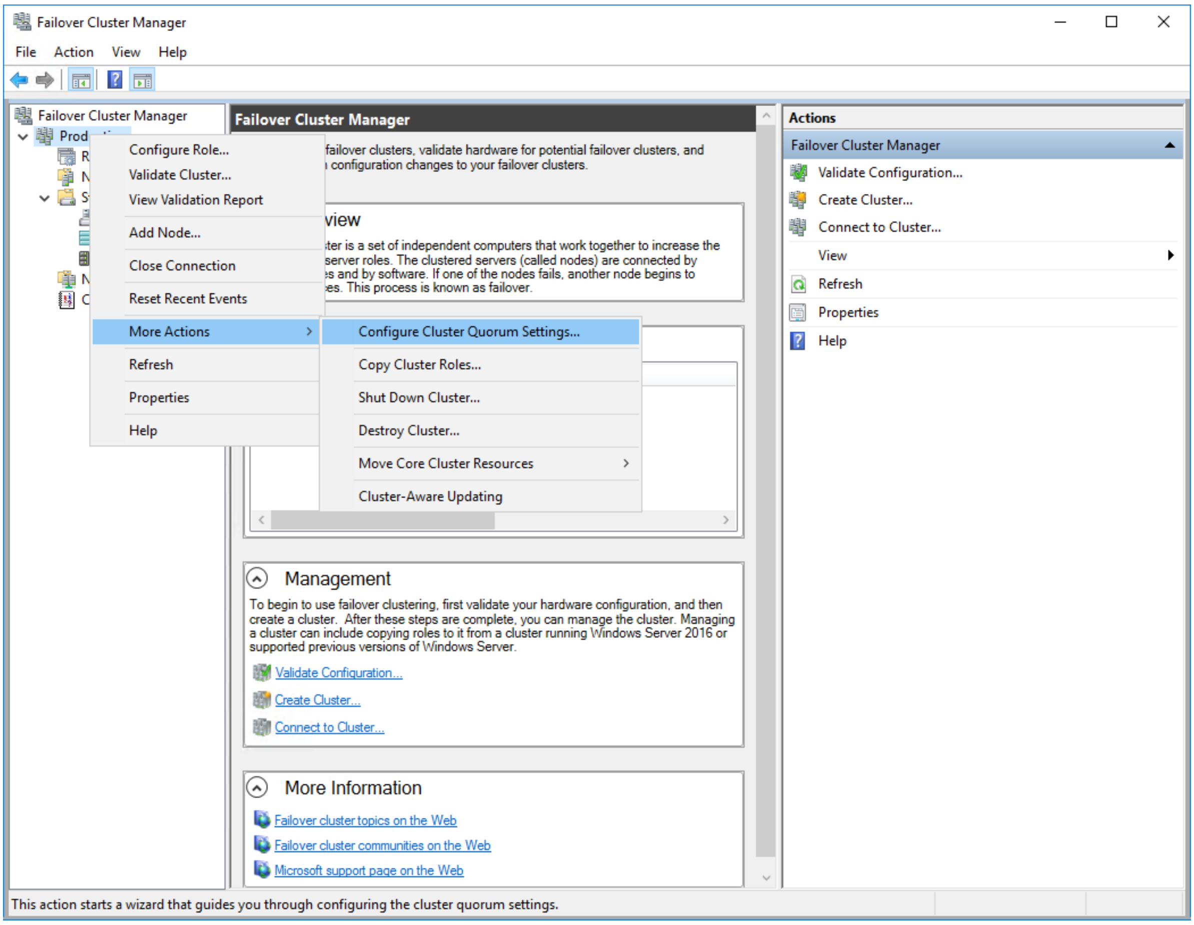
Add Disks to a Cluster

Select the disk or disks that you want to add.

Available disks:

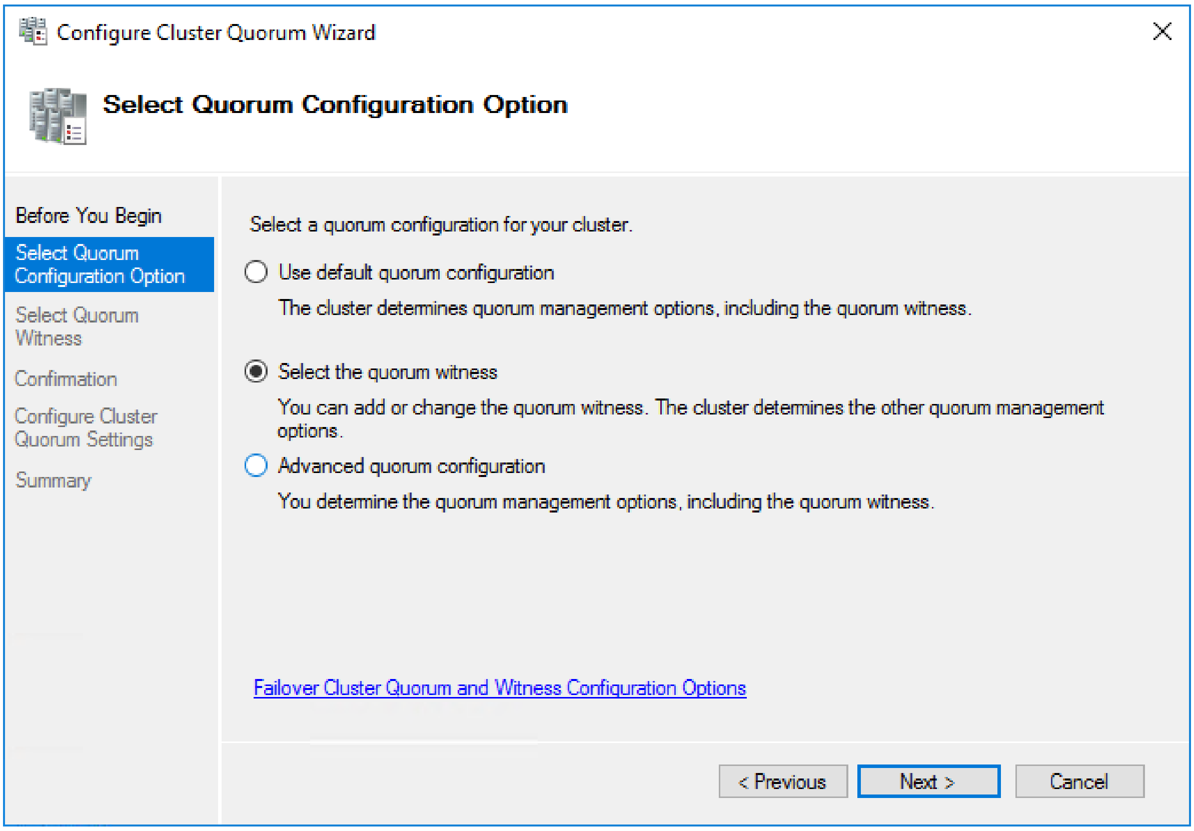
Resource Name	Disk Info	Capacity	Signature/Id
☑ Cluster Disk 1	Disk 3 on node SW2	10.0 GB	{080ffb0a-c594-4790-afc9-9b997e65c0dc}
☑ Cluster Disk 2	Disk 4 on node SW2	1.00 GB	{2bd3a199-b684-4147-8660-3d1d688dce...
☑ Cluster Disk 3	Disk 2 on node SW2	6.00 GB	{b4ade0c2-d87c-4aff-b53b-dda21e81bfbd}

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



This action starts a wizard that guides you through configuring the cluster quorum settings.

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



Configure Cluster Quorum Wizard

Select Quorum Configuration Option

Before You Begin
Select Quorum Configuration Option
Select Quorum Witness
Confirmation
Configure Cluster Quorum Settings
Summary

Select a quorum configuration for your cluster.

○ Use default quorum configuration

The cluster determines quorum management options, including the quorum witness.

● Select the quorum witness

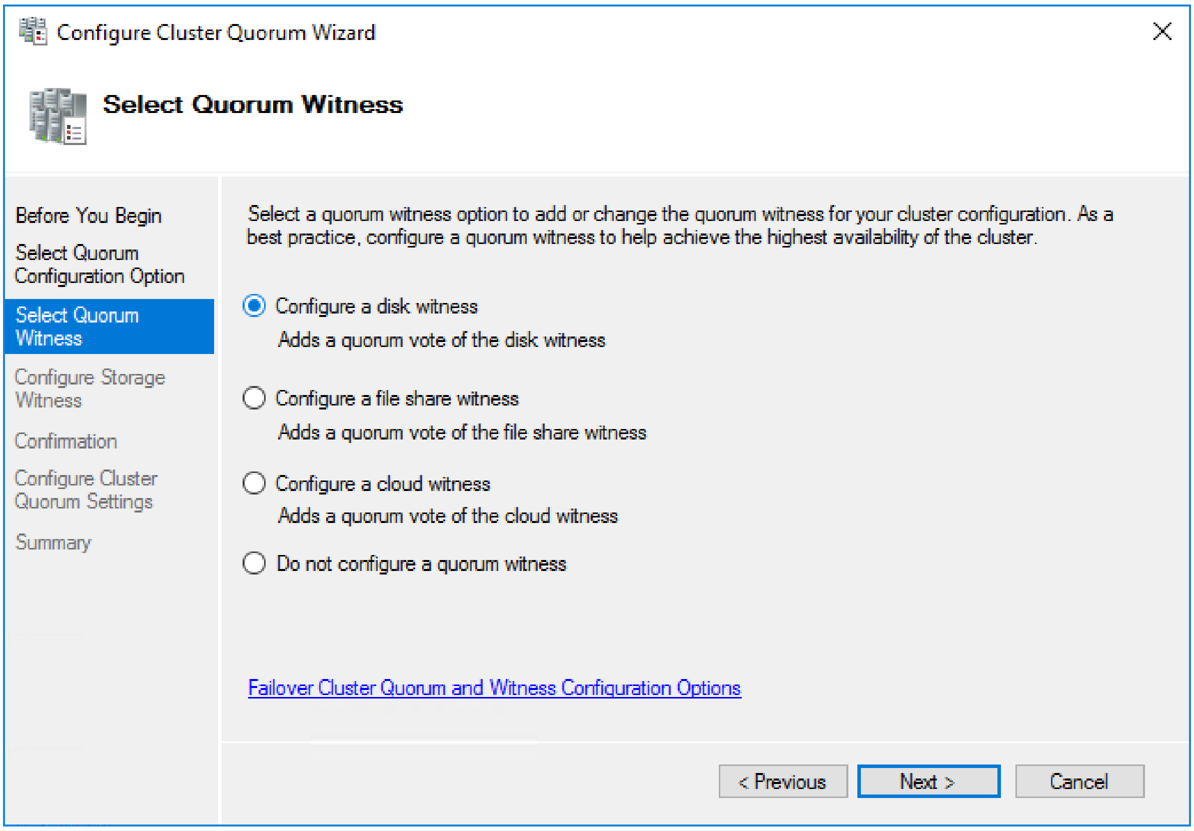
You can add or change the quorum witness. The cluster determines the other quorum management options.

○ Advanced quorum configuration

You determine the quorum management options, including the quorum witness.

Failover Cluster Quorum and Witness Configuration Options

4. Select Configure a disk witness. Click Next.



Configure Cluster Quorum Wizard

Select Quorum Witness

Before You Begin
Select Quorum Configuration Option
Select Quorum Witness
Configure Storage Witness
Confirmation
Configure Cluster Quorum Settings
Summary

Select a quorum witness option to add or change the quorum witness for your cluster configuration. As a best practice, configure a quorum witness to help achieve the highest availability of the cluster.

● Configure a disk witness
Adds a quorum vote of the disk witness

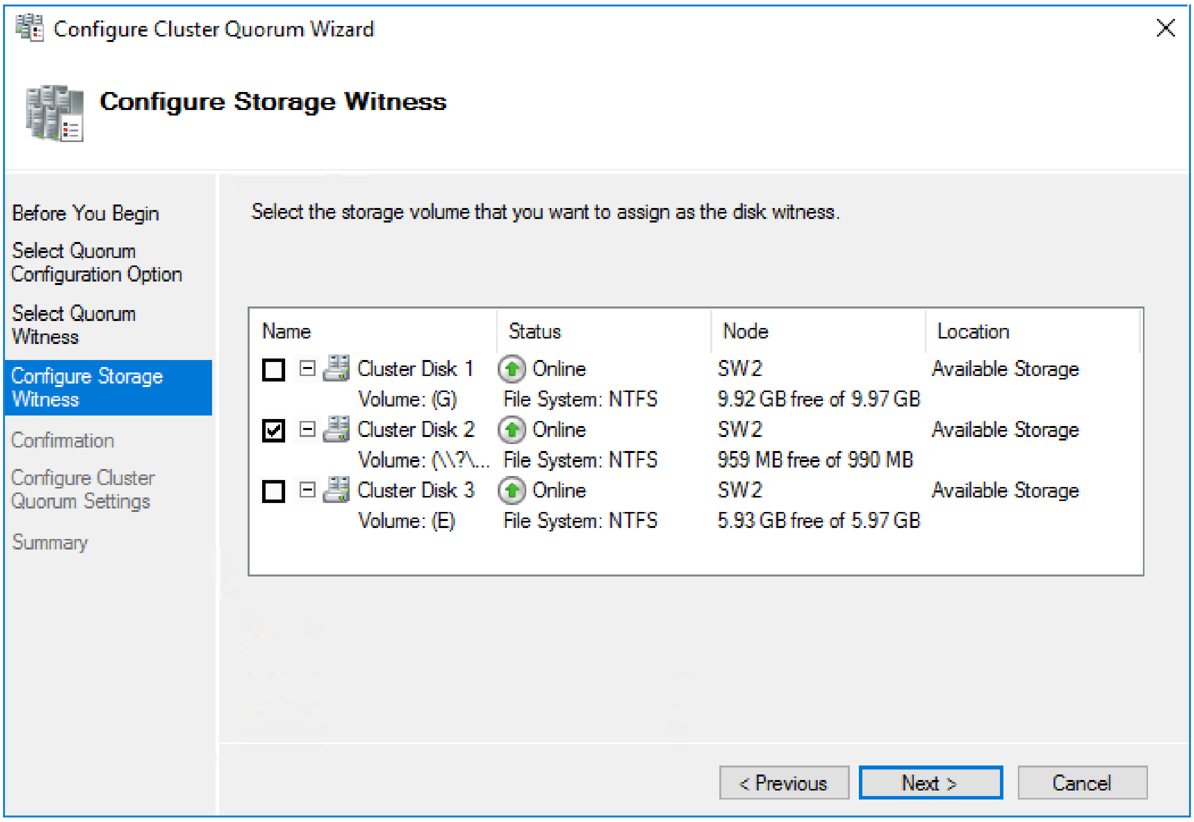
○ Configure a file share witness
Adds a quorum vote of the file share witness

○ Configure a cloud witness
Adds a quorum vote of the cloud witness

○ Do not configure a quorum witness

Failover Cluster Quorum and Witness Configuration Options

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



Configure Cluster Quorum Wizard

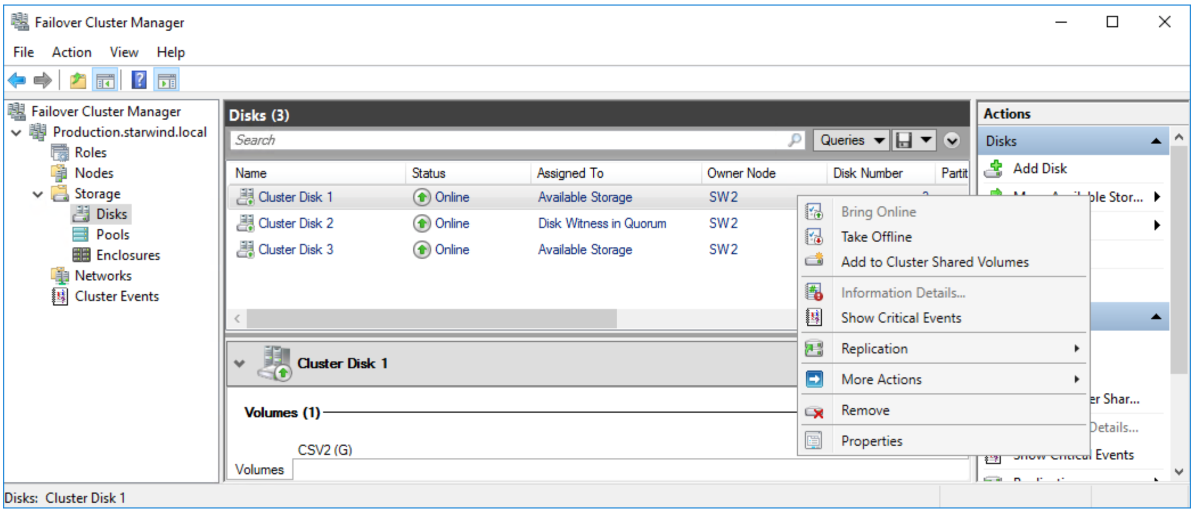
Configure Storage Witness

Before You Begin
Select Quorum Configuration Option
Select Quorum Witness
Configure Storage Witness
Confirmation
Configure Cluster Quorum Settings
Summary

Select the storage volume that you want to assign as the disk witness.

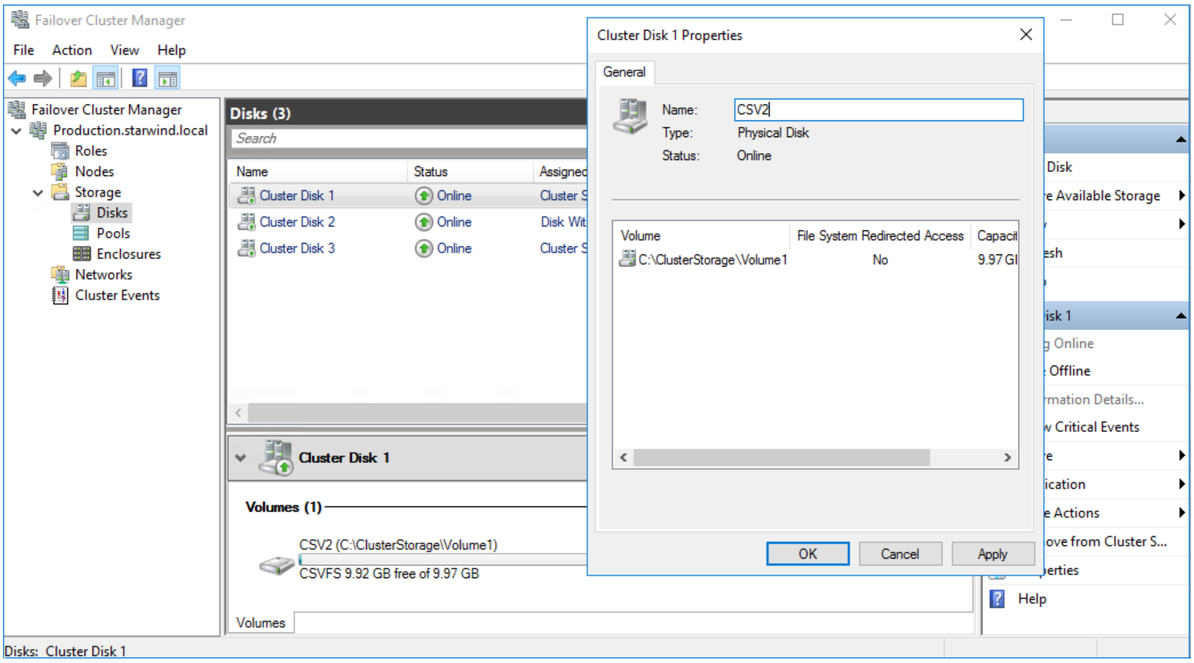
	Name	Status	Node	Location
□	Cluster Disk 1 Volume: (G)	Online File System: NTFS	SW2 9.92 GB free of 9.97 GB	Available Storage
☑	Cluster Disk 2 Volume: (\\?\...	Online File System: NTFS	SW2 959 MB free of 990 MB	Available Storage
□	Cluster Disk 3 Volume: (E)	Online File System: NTFS	SW2 5.93 GB free of 5.97 GB	Available Storage

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



Name	Status	Assigned To	Owner Node	Disk Number
Cluster Disk 1	Online	Available Storage	SW2	
Cluster Disk 2	Online	Disk Witness in Quorum	SW2	
Cluster Disk 3	Online	Available Storage	SW2	

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.



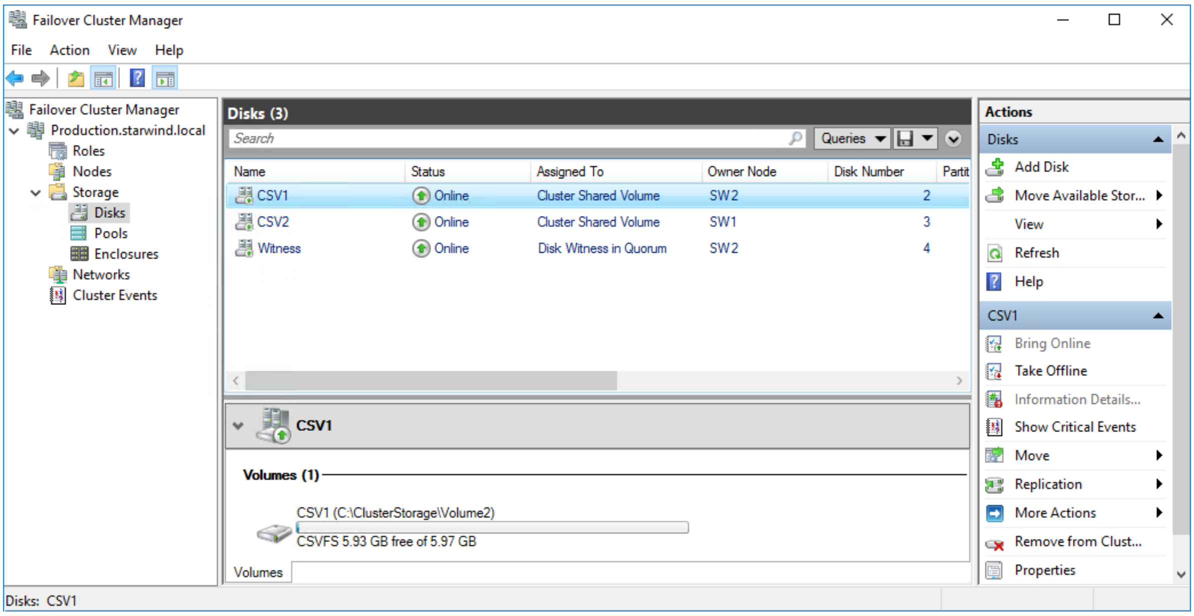
Name	Status	Assigned
Cluster Disk 1	Online	Cluster S
Cluster Disk 2	Online	Disk Wit
Cluster Disk 3	Online	Cluster S

CSV2 (C:\ClusterStorage\Volume1)
CSVFS 9.92 GB free of 9.97 GB

Name: CSV2
Type: Physical Disk
Status: Online

Volume	File System Redirected Access	Capaci
C:\ClusterStorage\Volume1	No	9.97 GI

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.



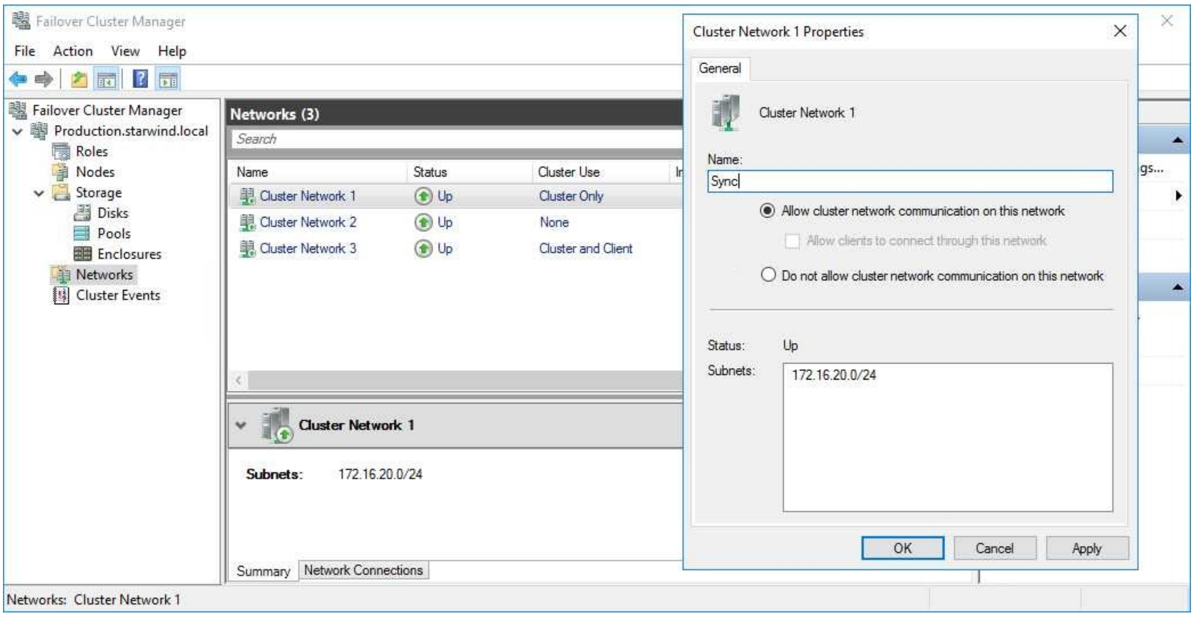
Name	Status	Assigned To	Owner Node	Disk Number	Partit
CSV1	Online	Cluster Shared Volume	SW2	2	
CSV2	Online	Cluster Shared Volume	SW1	3	
Witness	Online	Disk Witness in Quorum	SW2	4	

CSV1 (C:\ClusterStorage\Volume2)
CSVFS 5.93 GB free of 5.97 GB

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



Networks (3)

Name	Status	Cluster Use
Cluster Network 1	Up	Cluster Only
Cluster Network 2	Up	None
Cluster Network 3	Up	Cluster and Client

Cluster Network 1

Subnets: 172.16.20.0/24

Cluster Network 1 Properties

General

Cluster Network 1

Name: Sync

● Allow cluster network communication on this network

□ Allow clients to connect through this network

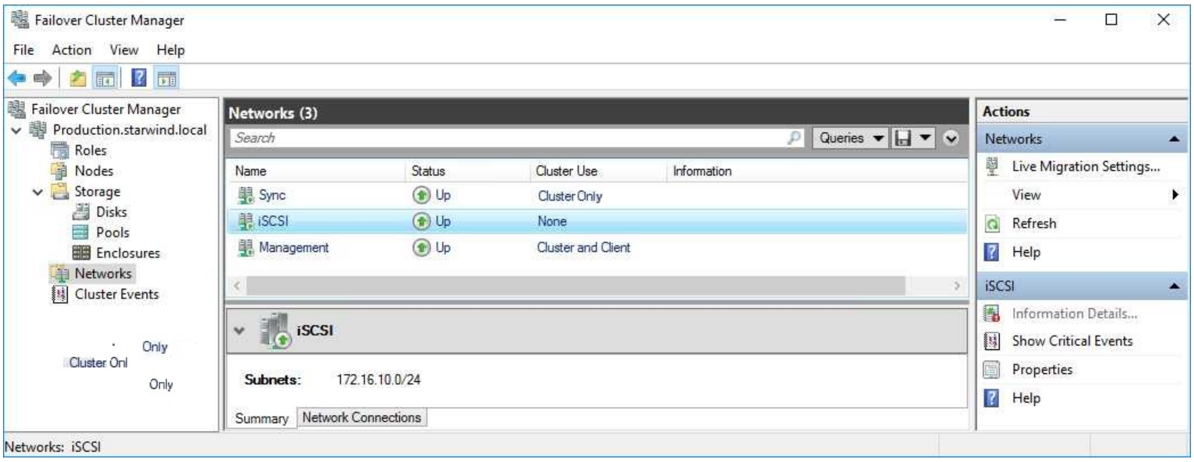
○ Do not allow cluster network communication on this network

Status: Up

Subnets: 172.16.20.0/24

Networks: Cluster Network 1

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



Networks (3)

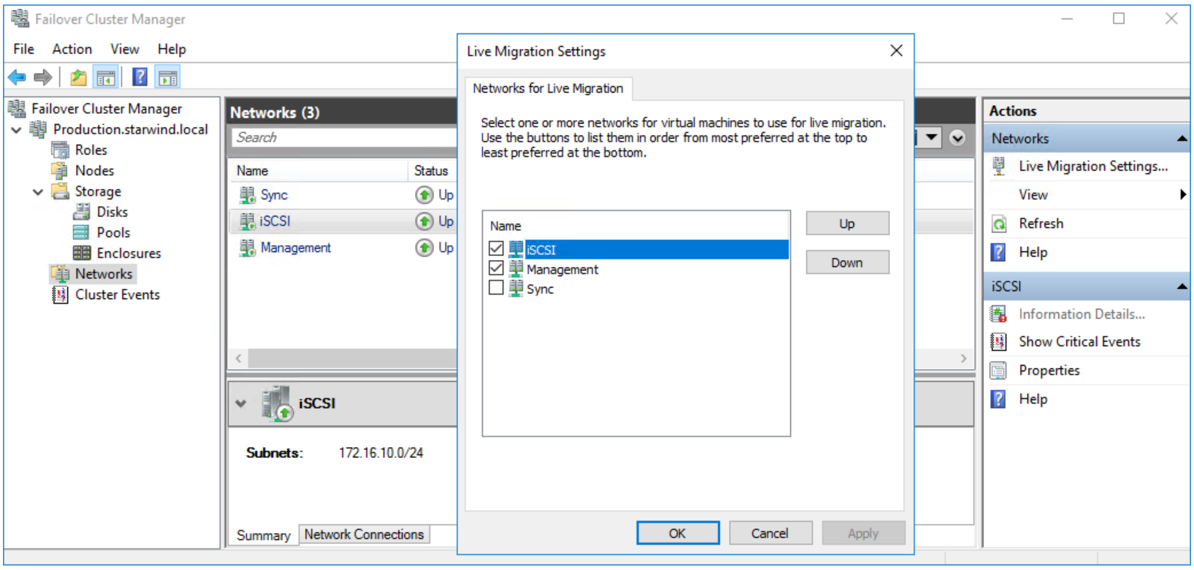
Name	Status	Cluster Use	Information
Sync	Up	Cluster Only	
iSCSI	Up	None	
Management	Up	Cluster and Client	

iSCSI

Subnets: 172.16.10.0/24

Networks: iSCSI

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.



Subnets: 172.16.10.0/24

Select one or more networks for virtual machines to use for live migration. Use the buttons to list them in order from most preferred at the top to least preferred at the bottom.

☑ iSCSI
☑ Management
□ Sync

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.

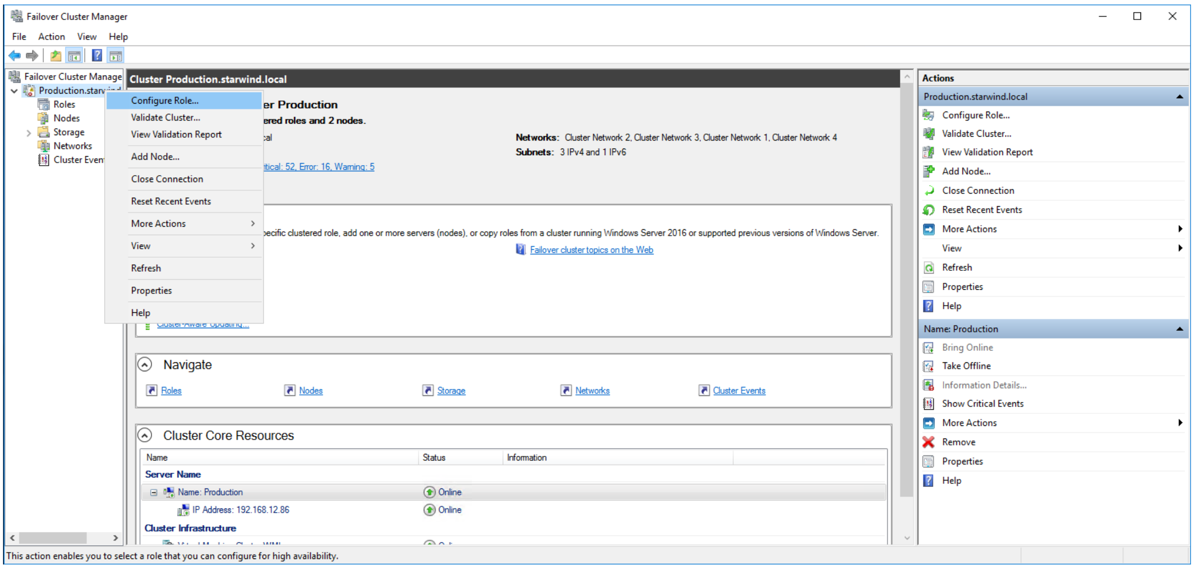
Configuring File Shares

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.



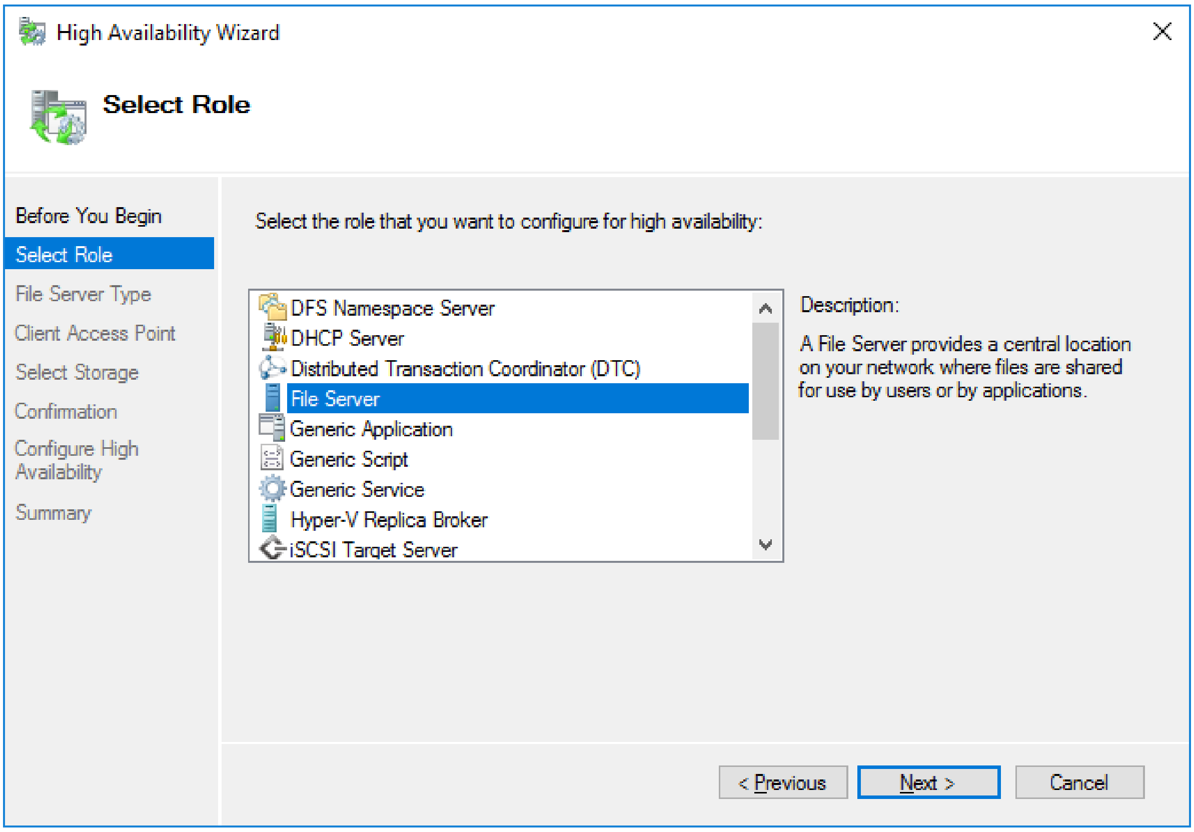
Networks: Cluster Network 2, Cluster Network 3, Cluster Network 1, Cluster Network 4
Subnets: 3 IPv4 and 1 IPv6

...ecific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2016 or supported previous versions of Windows Server.

Failover cluster topics on the Web

This action enables you to select a role that you can configure for high availability.

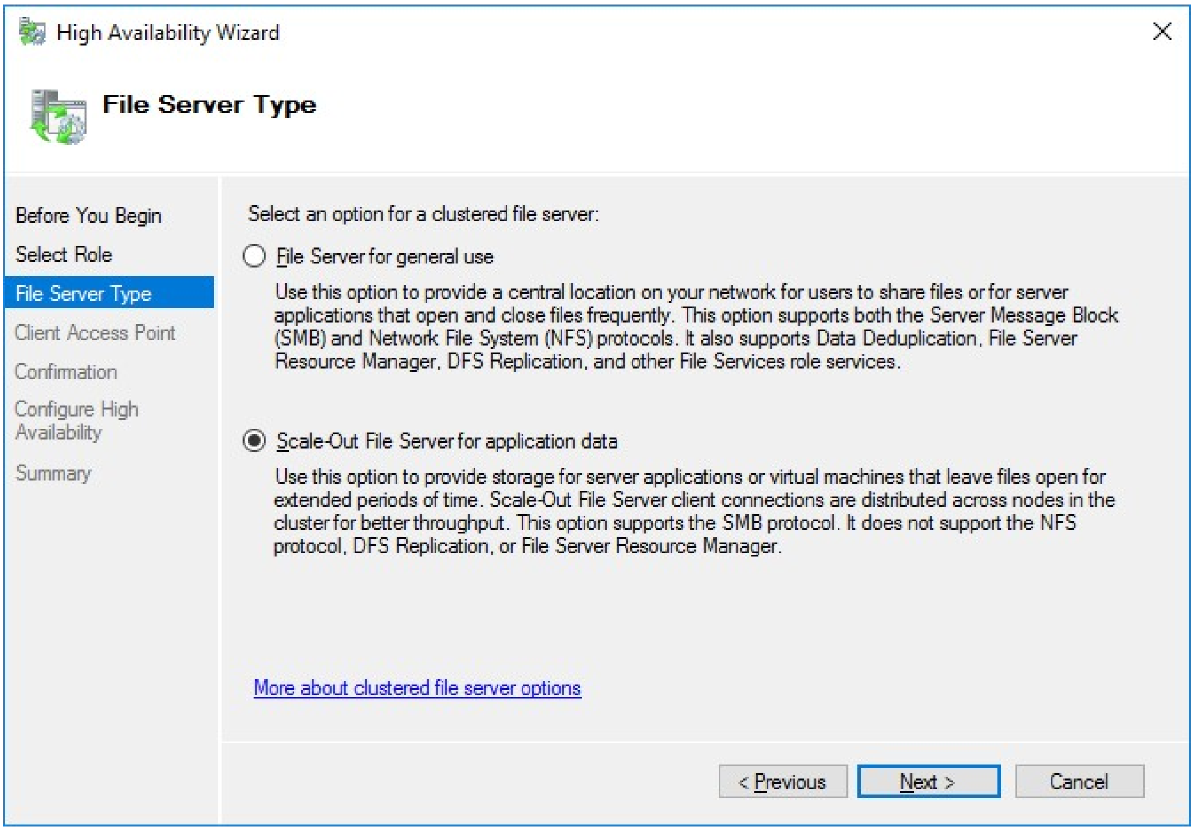
3. Select the File Server item from the list in High Availability Wizard and click Next to continue.



Select the role that you want to configure for high availability:

A File Server provides a central location on your network where files are shared for use by users or by applications.

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



High Availability Wizard

File Server Type

Select an option for a clustered file server:

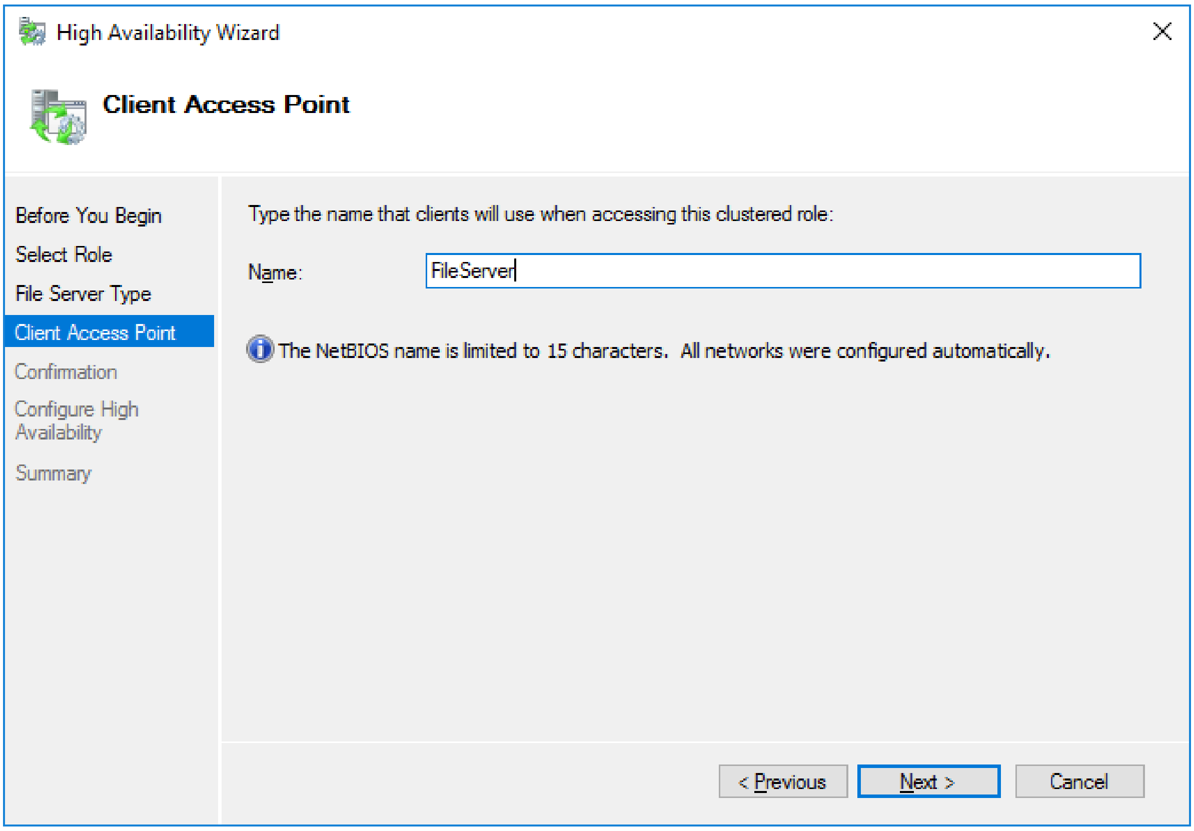
○ File Server for general use

Use this option to provide a central location on your network for users to share files or for server applications that open and close files frequently. This option supports both the Server Message Block (SMB) and Network File System (NFS) protocols. It also supports Data Deduplication, File Server Resource Manager, DFS Replication, and other File Services role services.

● Scale-Out File Server for application data

Use this option to provide storage for server applications or virtual machines that leave files open for extended periods of time. Scale-Out File Server client connections are distributed across nodes in the cluster for better throughput. This option supports the SMB protocol. It does not support the NFS protocol, DFS Replication, or File Server Resource Manager.

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.



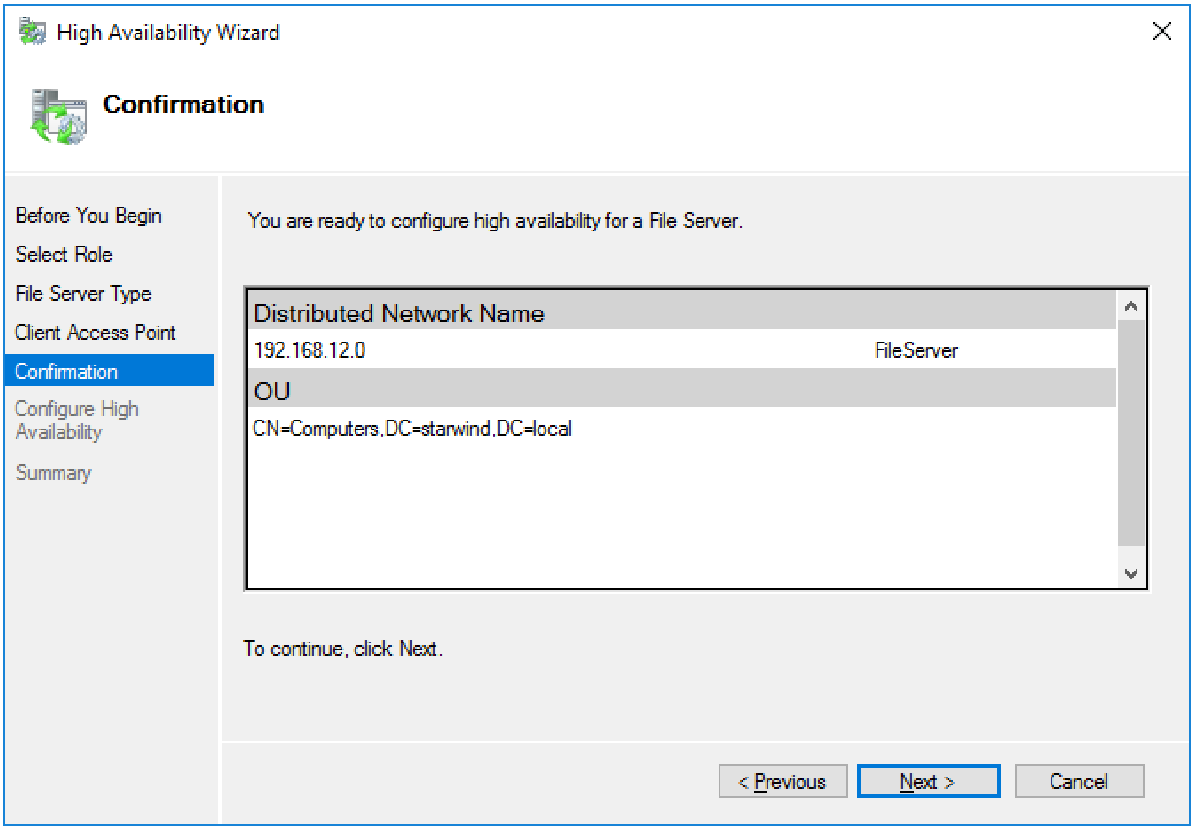
Type the name that clients will use when accessing this clustered role:

Name: FileServer

The NetBIOS name is limited to 15 characters. All networks were configured automatically.

Click Next to continue.

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

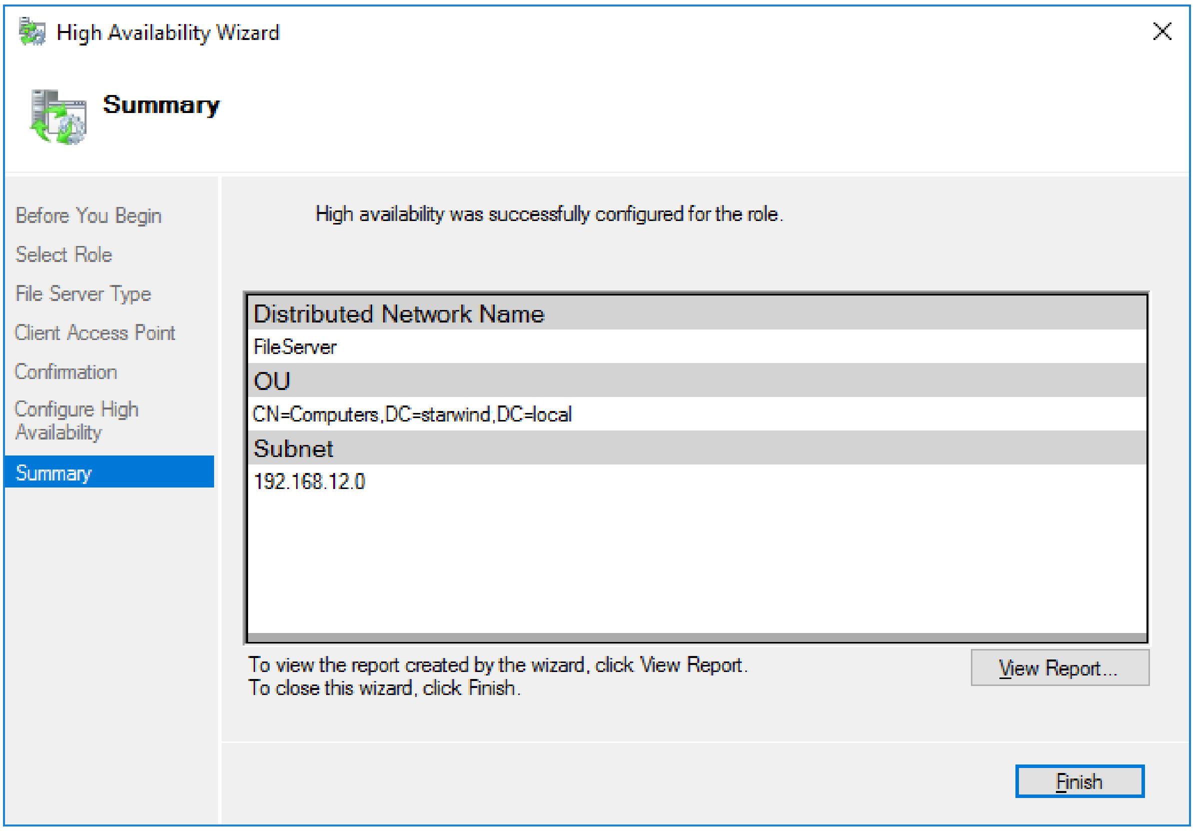


You are ready to configure high availability for a File Server.

Distributed Network Name	
192.168.12.0	FileServer
OU	
CN=Computers,DC=starwind,DC=local	

To continue, click Next.

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

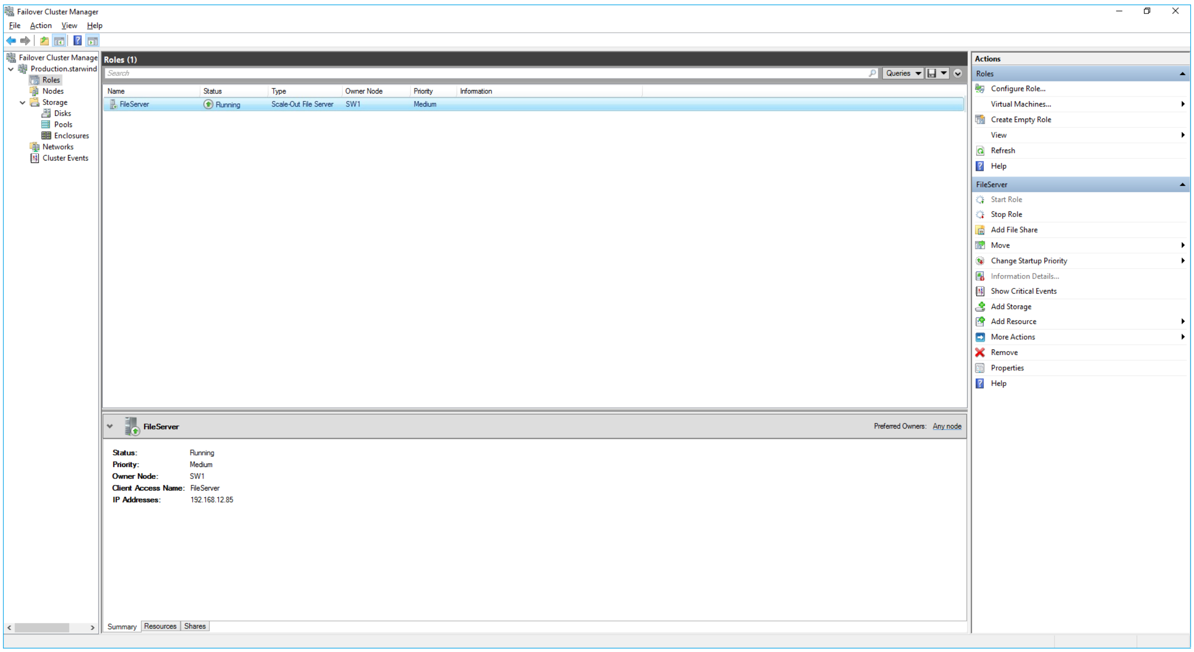


High availability was successfully configured for the role.

Distributed Network Name
FileServer
OU
CN=Computers,DC=starwind,DC=local
Subnet
192.168.12.0

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

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



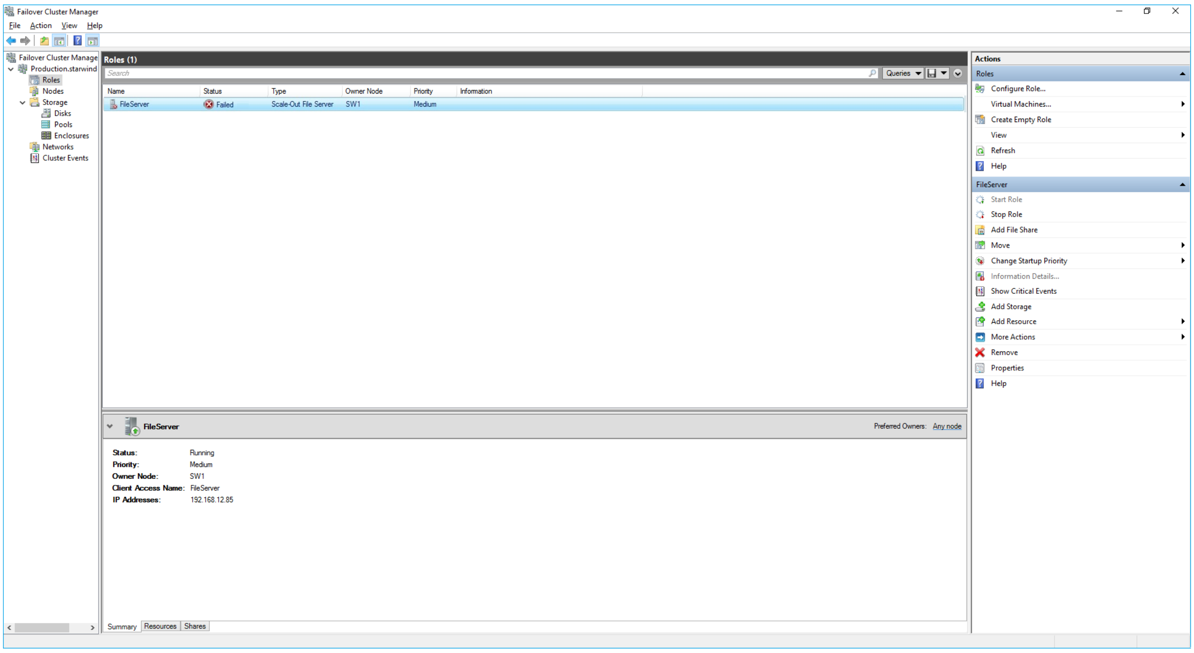
Roles (1)

Name	Status	Type	Owner Node	Priority	Information
FileServer	Running	Scale-Out File Server	SW1	Medium	

FileServer

Status: Running
Priority: Medium
Owner Node: SW1
Client Access Name: FileServer
IP Addresses: 192.168.12.85

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

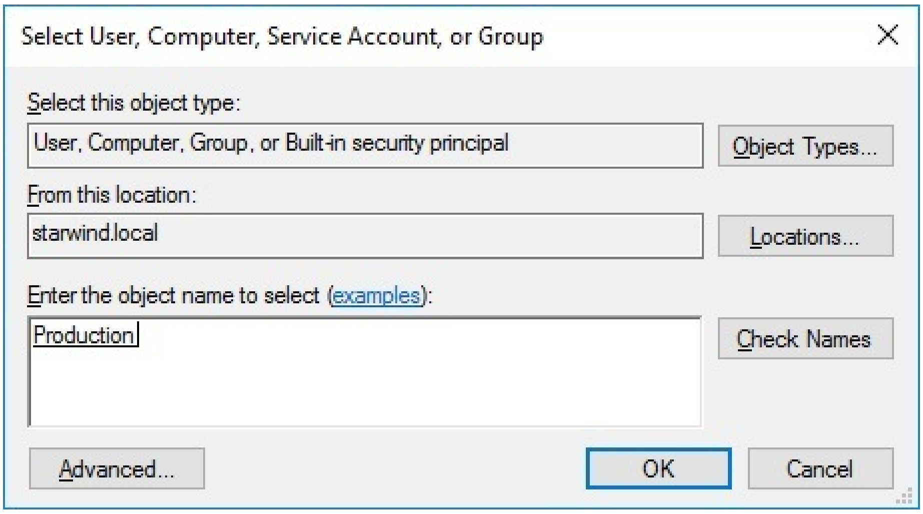


Name	Status	Type	Owner Node	Priority	Information
FileServer	Failed	Scale-Out File Server	SW1	Medium	

FileServer

Status: Running
Priority: Medium
Owner Node: SW1
Client Access Name: FileServer
IP Addresses: 192.168.12.85

- 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)

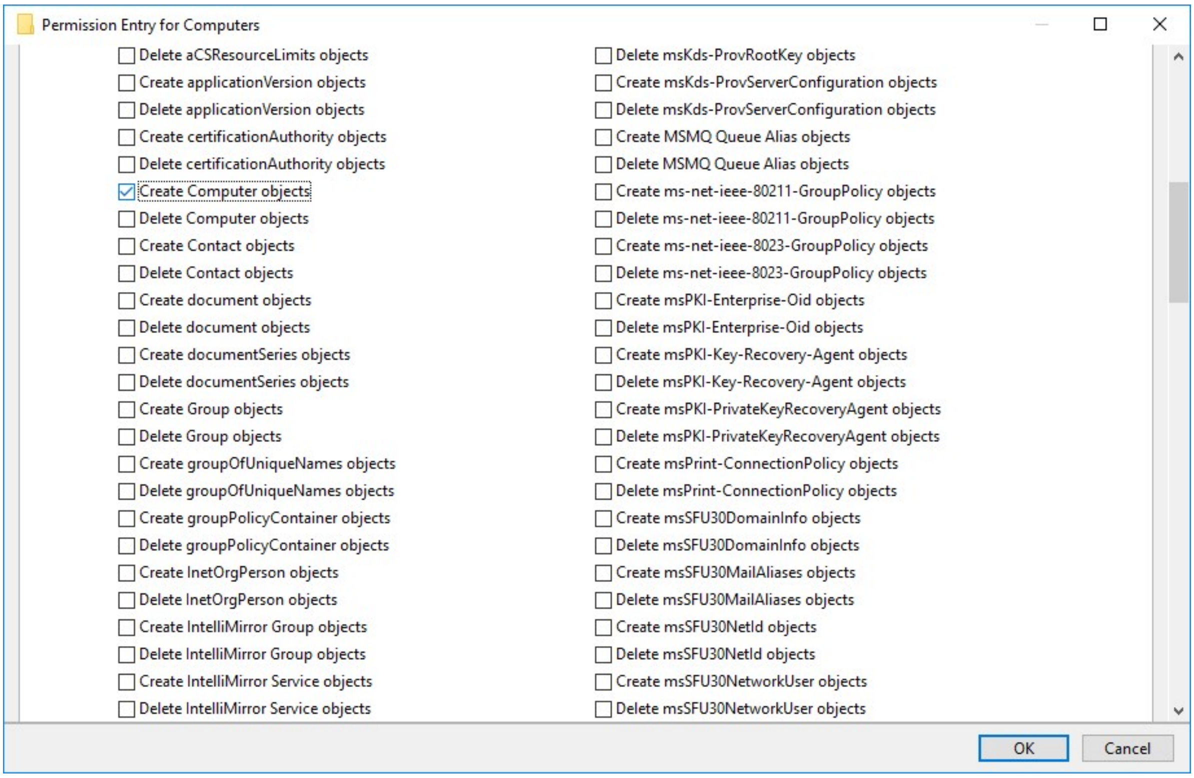


Select this object type:
User, Computer, Group, or Built-in security principal

From this location:
starwind.local

Enter the object name to select (examples):
Production

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



Permission Entry for Computers

□ Delete aCSResourceLimits objects
□ Create applicationVersion objects
□ Delete applicationVersion objects
□ Create certificationAuthority objects
□ Delete certificationAuthority objects
☑ Create Computer objects
□ Delete Computer objects
□ Create Contact objects
□ Delete Contact objects
□ Create document objects
□ Delete document objects
□ Create documentSeries objects
□ Delete documentSeries objects
□ Create Group objects
□ Delete Group objects
□ Create groupOfUniqueNames objects
□ Delete groupOfUniqueNames objects
□ Create groupPolicyContainer objects
□ Delete groupPolicyContainer objects
□ Create InetOrgPerson objects
□ Delete InetOrgPerson objects
□ Create IntelliMirror Group objects
□ Delete IntelliMirror Group objects
□ Create IntelliMirror Service objects
□ Delete IntelliMirror Service objects

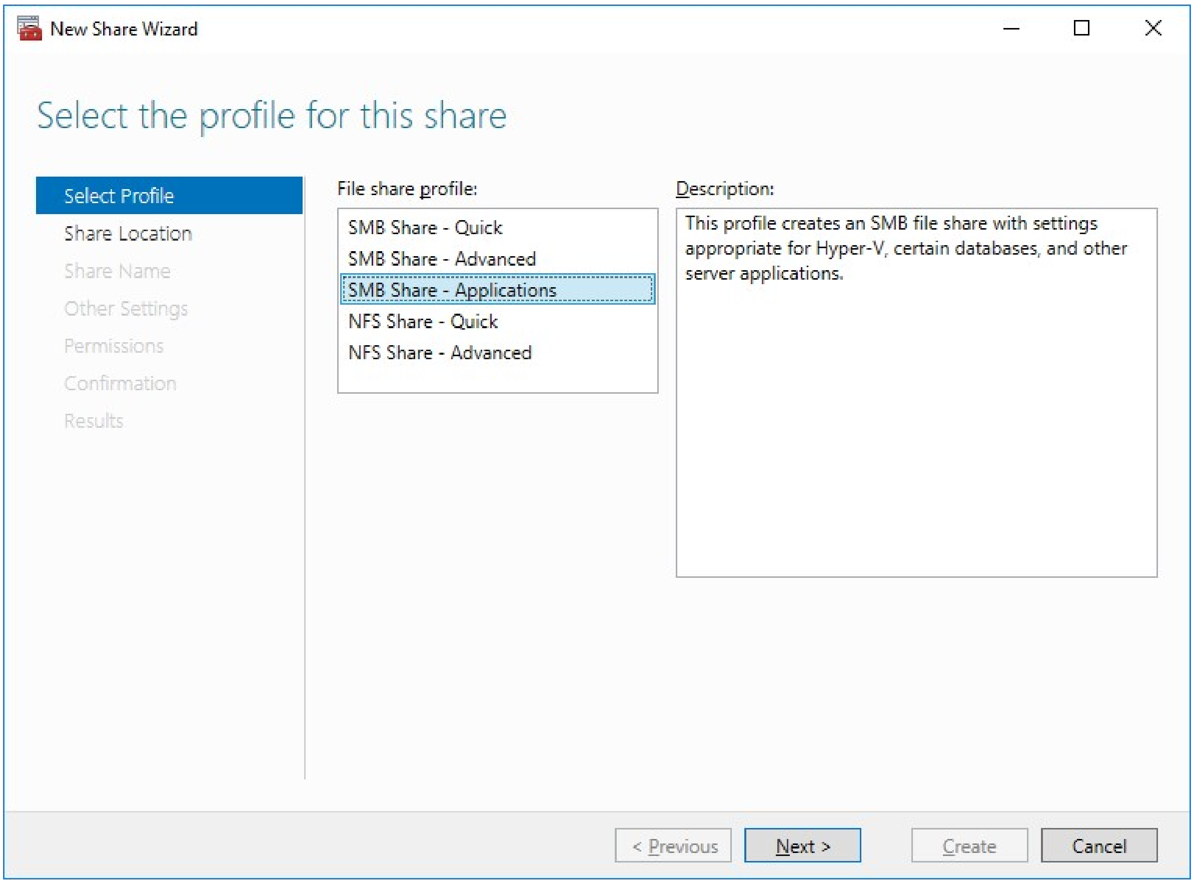
□ Delete msKds-ProvRootKey objects
□ Create msKds-ProvServerConfiguration objects
□ Delete msKds-ProvServerConfiguration objects
□ Create MSMQ Queue Alias objects
□ Delete MSMQ Queue Alias objects
□ Create ms-net-ieee-80211-GroupPolicy objects
□ Delete ms-net-ieee-80211-GroupPolicy objects
□ Create ms-net-ieee-8023-GroupPolicy objects
□ Delete ms-net-ieee-8023-GroupPolicy objects
□ Create msPKI-Enterprise-Oid objects
□ Delete msPKI-Enterprise-Oid objects
□ Create msPKI-Key-Recovery-Agent objects
□ Delete msPKI-Key-Recovery-Agent objects
□ Create msPKI-PrivateKeyRecoveryAgent objects
□ Delete msPKI-PrivateKeyRecoveryAgent objects
□ Create msPrint-ConnectionPolicy objects
□ Delete msPrint-ConnectionPolicy objects
□ Create msSFU30DomainInfo objects
□ Delete msSFU30DomainInfo objects
□ Create msSFU30MailAliases objects
□ Delete msSFU30MailAliases objects
□ Create msSFU30NetId objects
□ Delete msSFU30NetId objects
□ Create msSFU30NetworkUser objects
□ Delete msSFU30NetworkUser 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

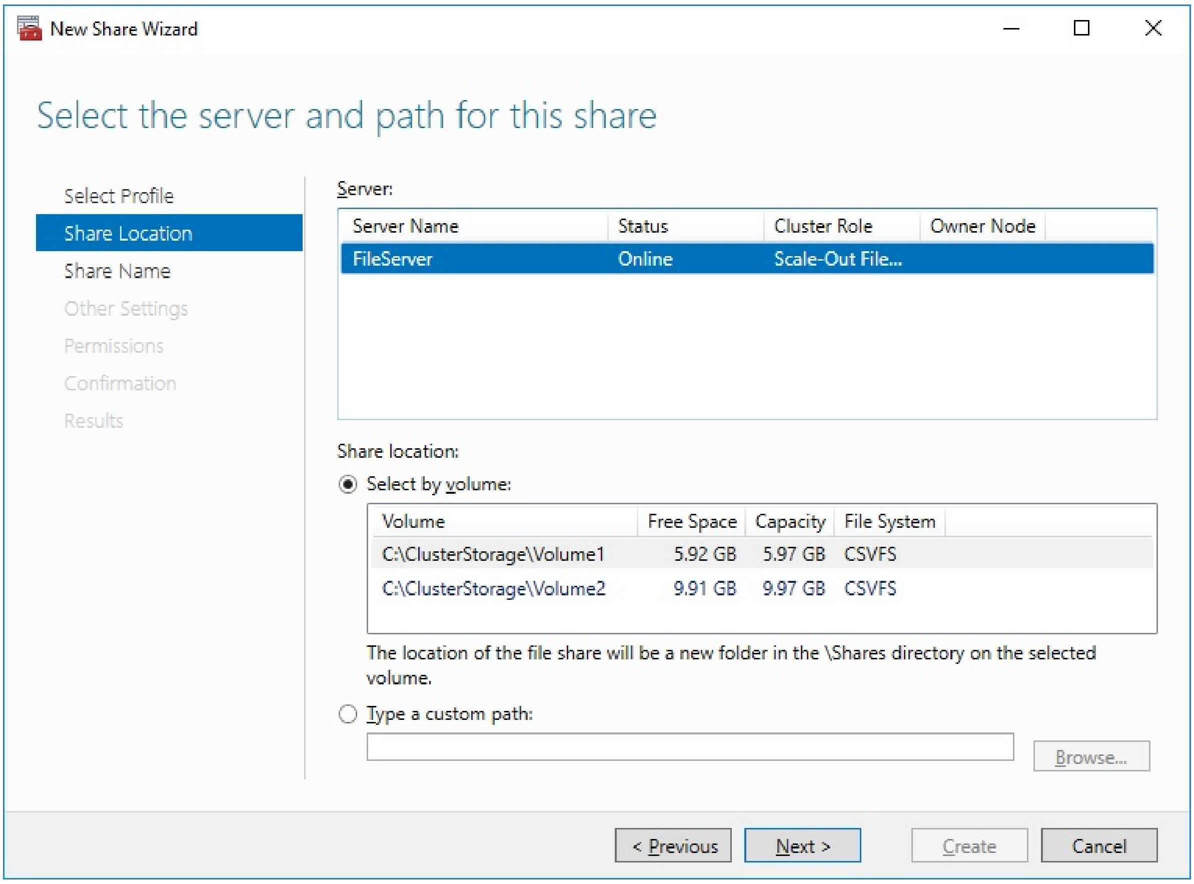
To Add File Share:

- 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



This profile creates an SMB file share with settings appropriate for Hyper-V, certain databases, and other server applications.

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



New Share Wizard

Select the server and path for this share

Server:

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

Share location:

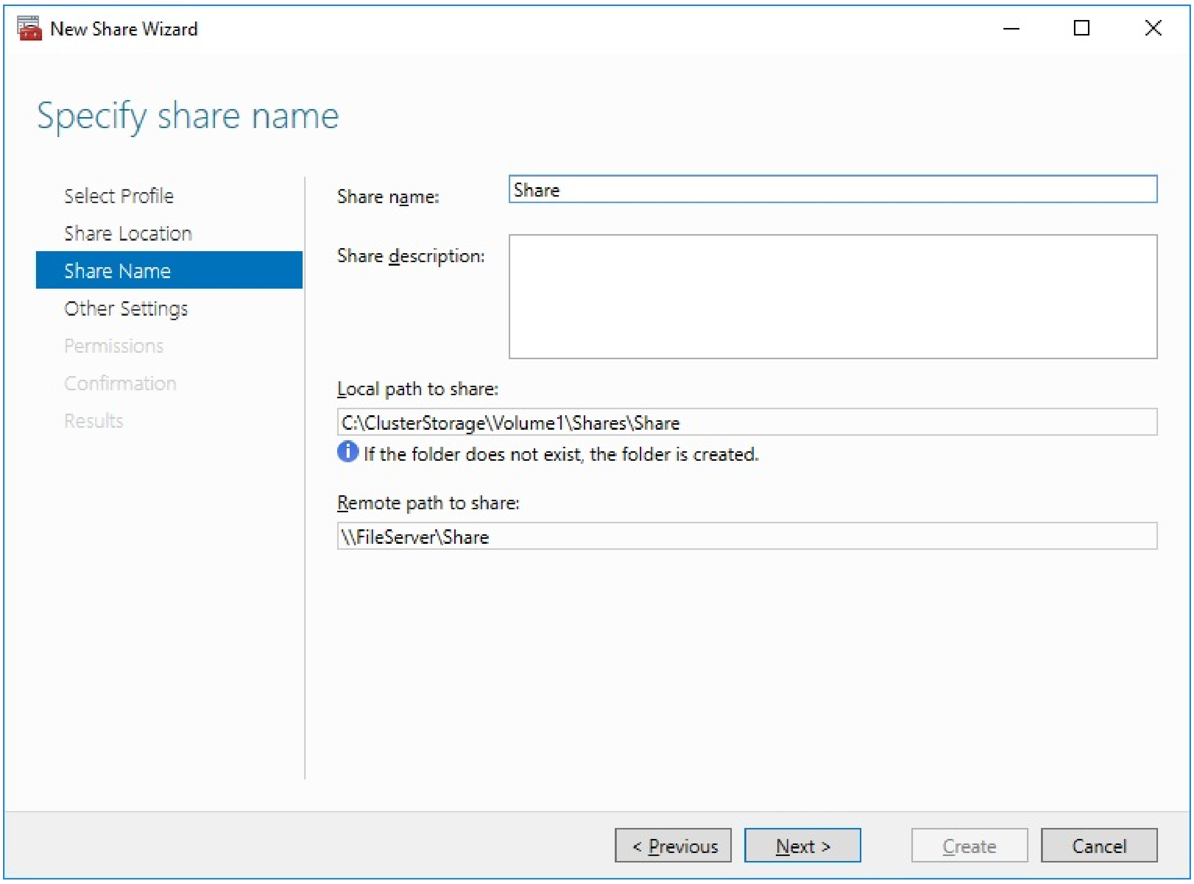
● Select by volume:

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:

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



Share name: Share

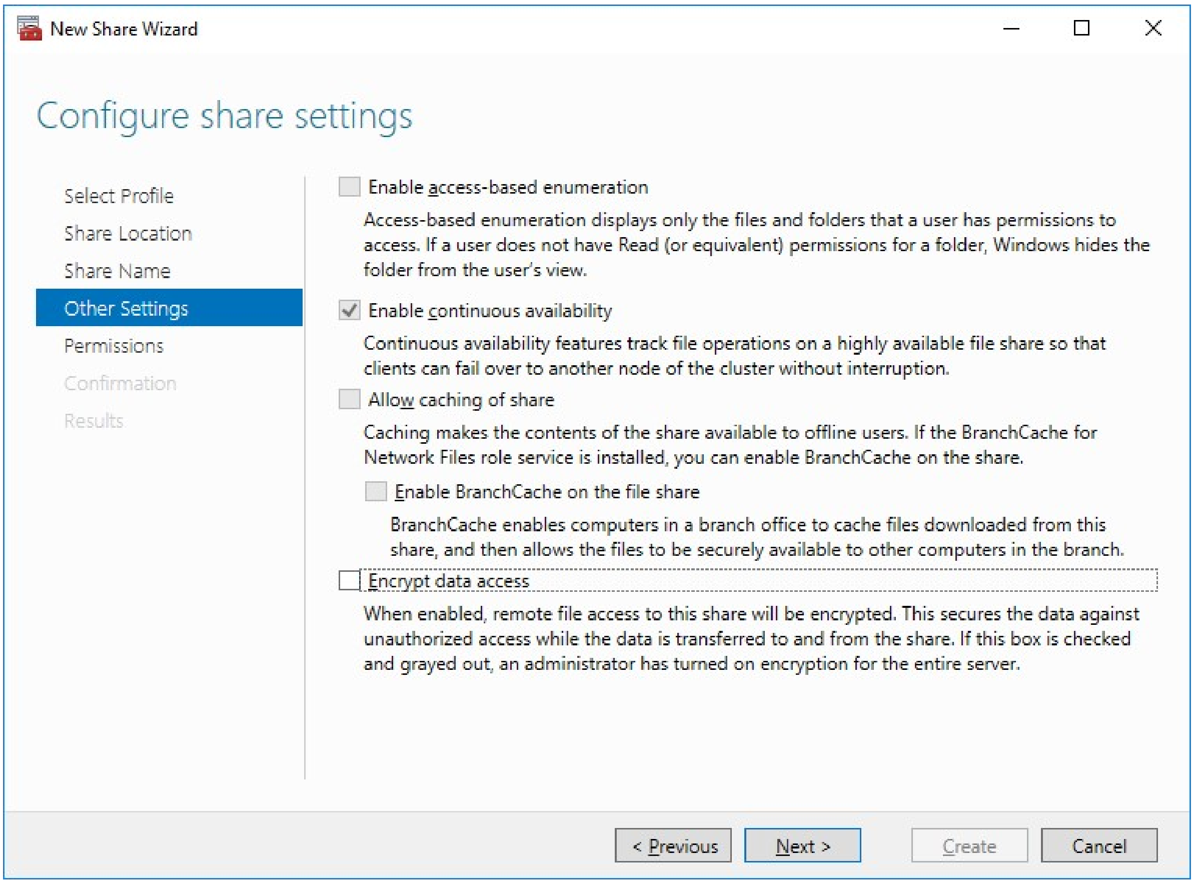
Share description:

Local path to share:
C:\ClusterStorage\Volume1\Shares\Share

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

Remote path to share:
\\FileServer\Share

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



New Share Wizard

Configure share settings

□ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☑ Enable continuous availability

Continuous availability features track file operations on a highly available file share so that clients can fail over to another node of the cluster without interruption.

□ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

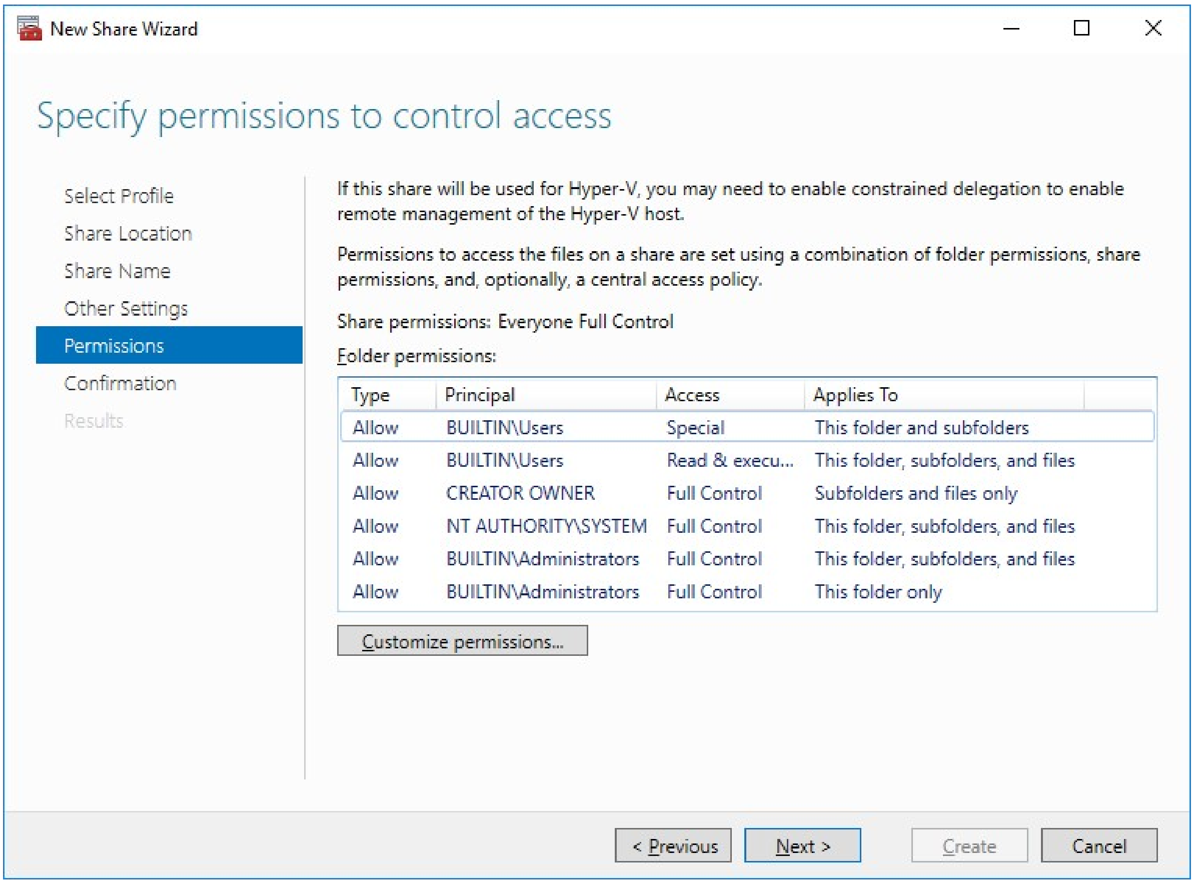
□ Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

□ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

8. Specify the access permissions for the file share.



Specify permissions to control access

If this share will be used for Hyper-V, you may need to enable constrained delegation to enable remote management of the Hyper-V host.

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

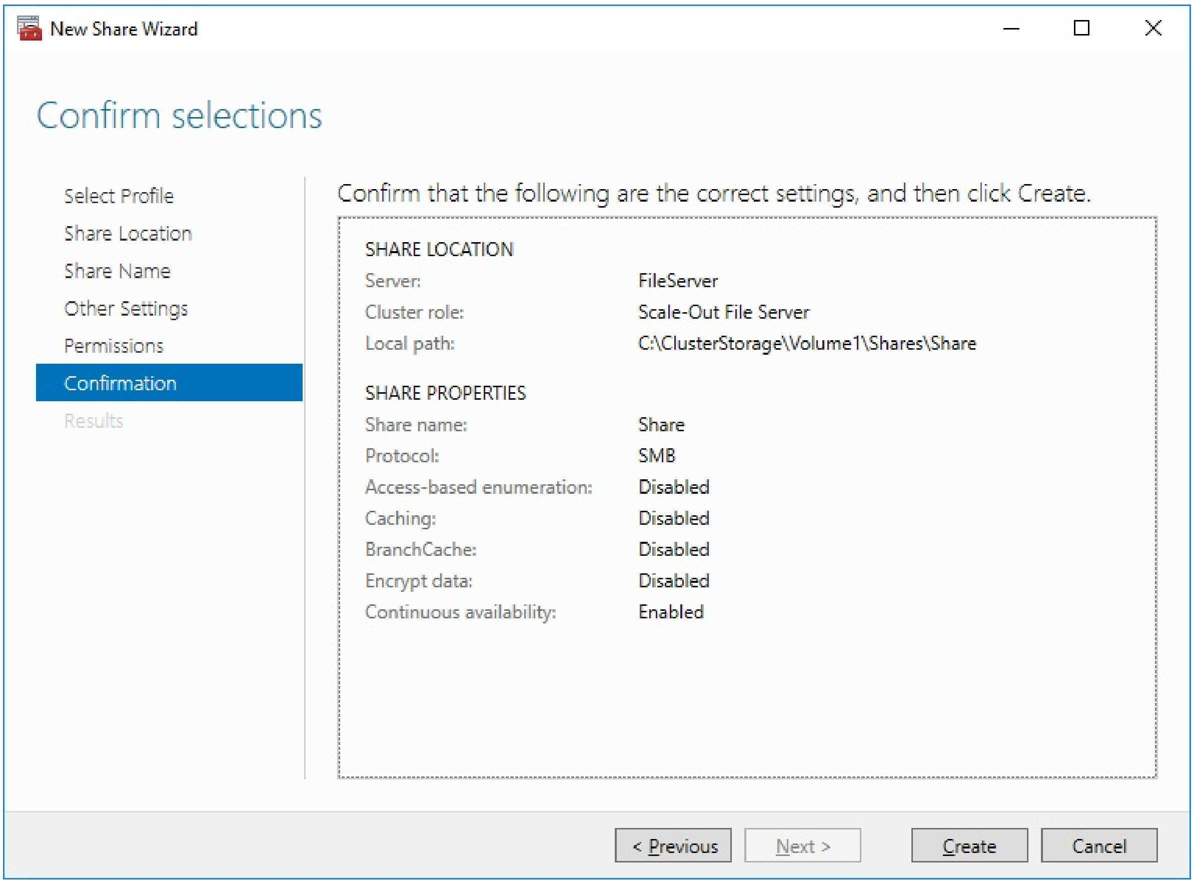
Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

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.



Confirm selections

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

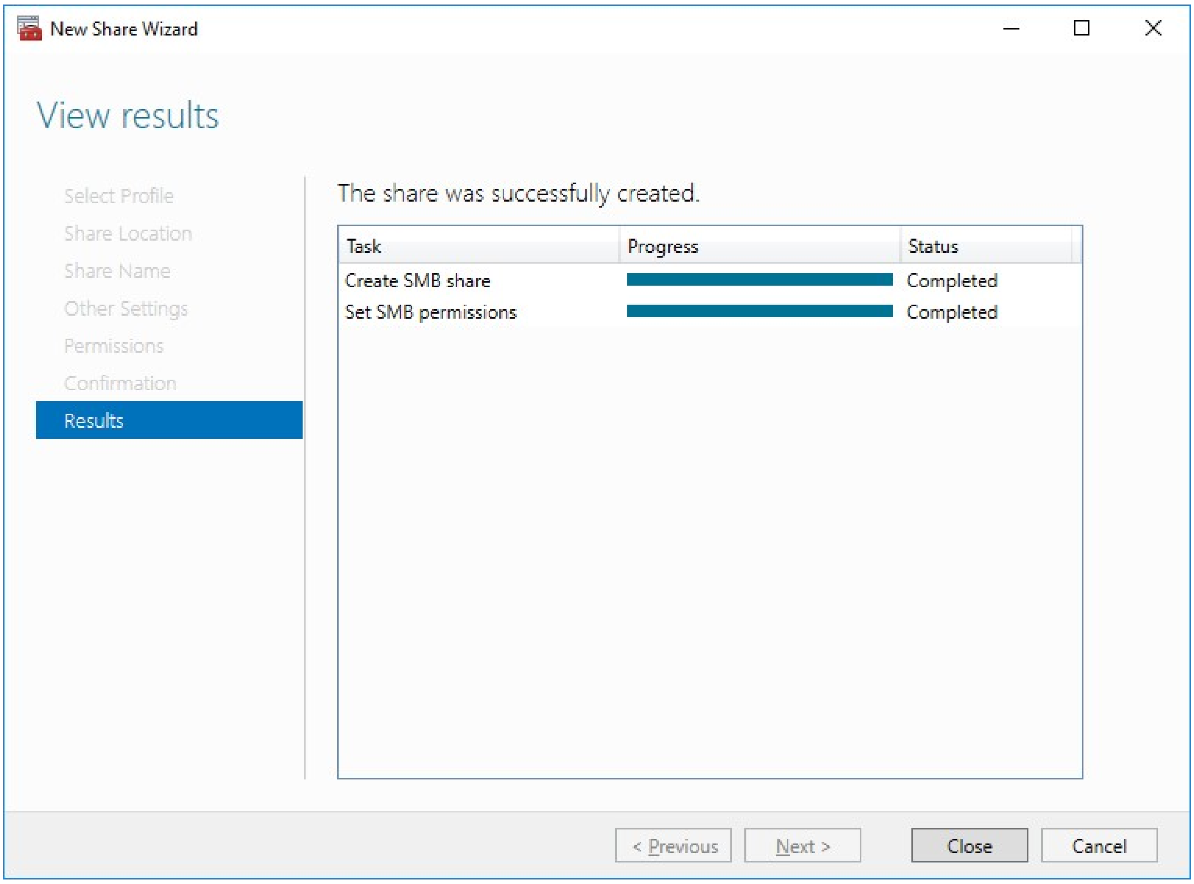
SHARE LOCATION

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

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

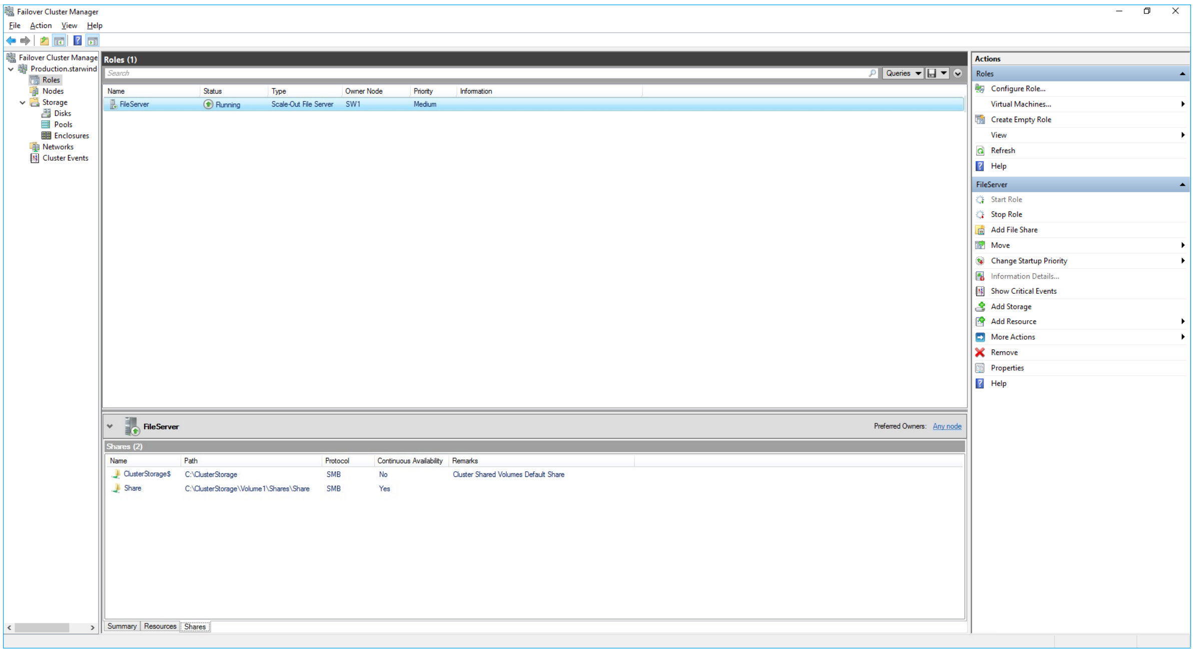


The share was successfully created.

Task	Progress	Status
Create SMB share		Completed
Set SMB permissions		Completed

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:



Roles (1)

Name	Status	Type	Owner Node	Priority	Information
FileServer	Running	Scale-Out File Server	SW1	Medium	

FileServer Preferred Owners: Any node

Shares (2)

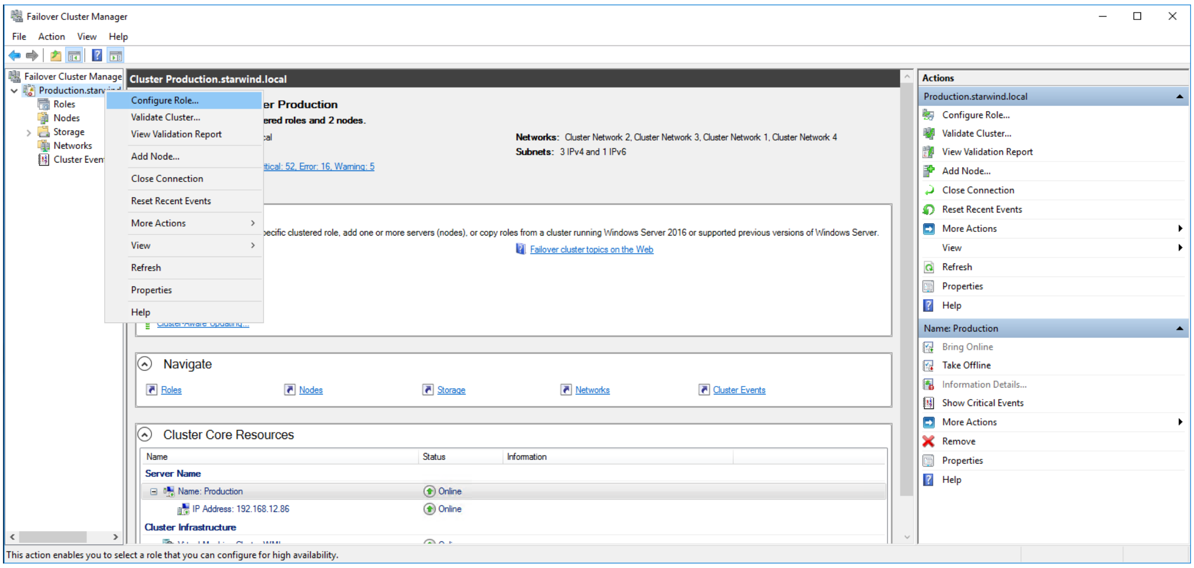
Name	Path	Protocol	Continuous Availability	Remarks
ClusterStorage$	C:\ClusterStorage	SMB	No	Cluster Shared Volumes Default Share
Share	C:\ClusterStorage\Volume1\Shares\Share	SMB	Yes	

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.



Cluster Production.starwind.local

er Production

ered roles and 2 nodes.

Networks: Cluster Network 2, Cluster Network 3, Cluster Network 1, Cluster Network 4
Subnets: 3 IPv4 and 1 IPv6

itical: 52, Error: 16, Warning: 5

ecific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2016 or supported previous versions of Windows Server.

Failover cluster topics on the Web

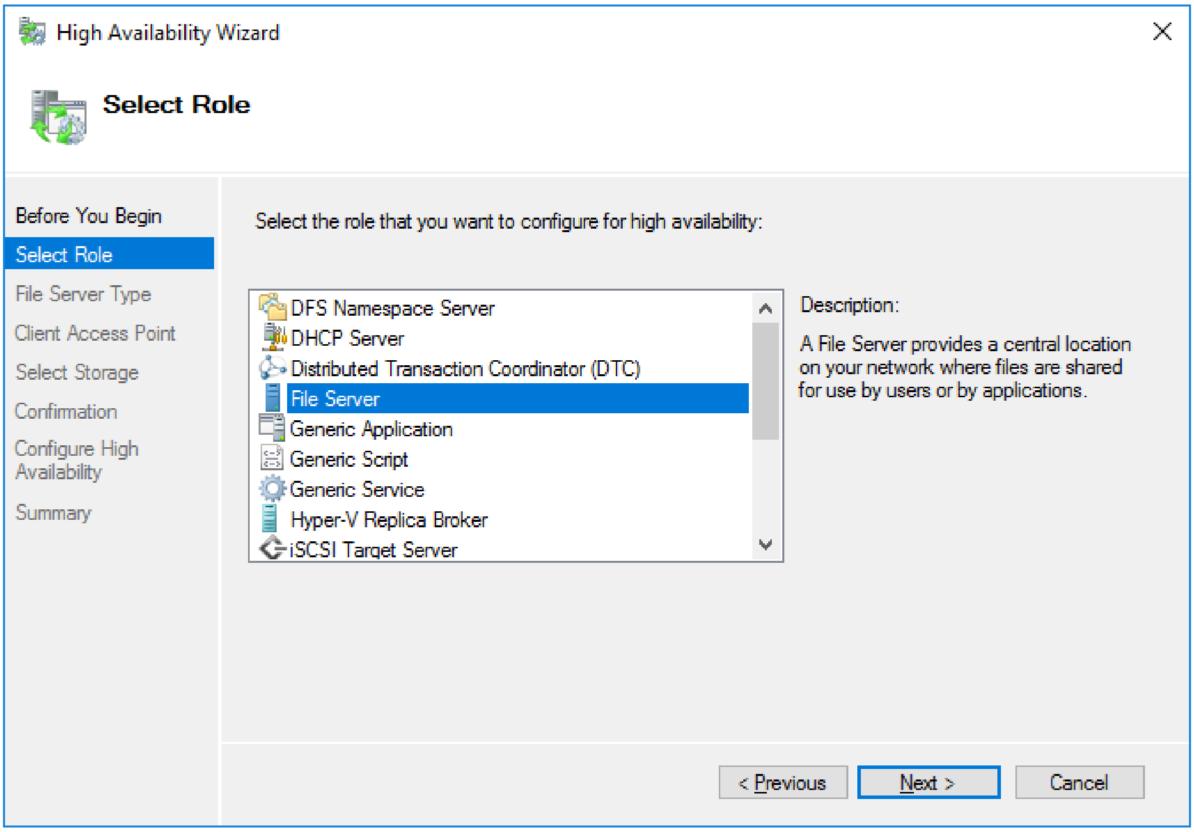
Cluster Core Resources

Name	Status	Information
Server Name		
Name: Production	Online	
IP Address: 192.168.12.86	Online	
Cluster Infrastructure		

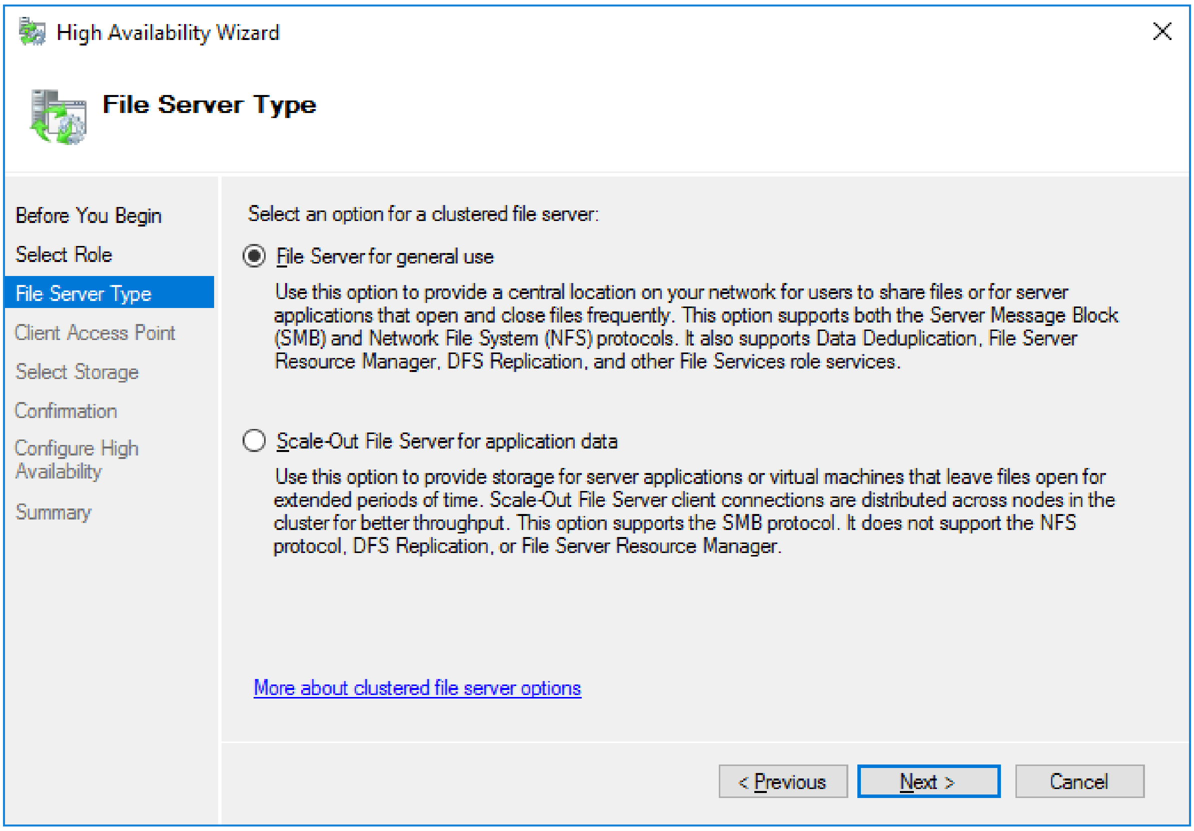
This action enables you to select a role that you can configure for high availability.

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.



High Availability Wizard

File Server Type

Select an option for a clustered file server:

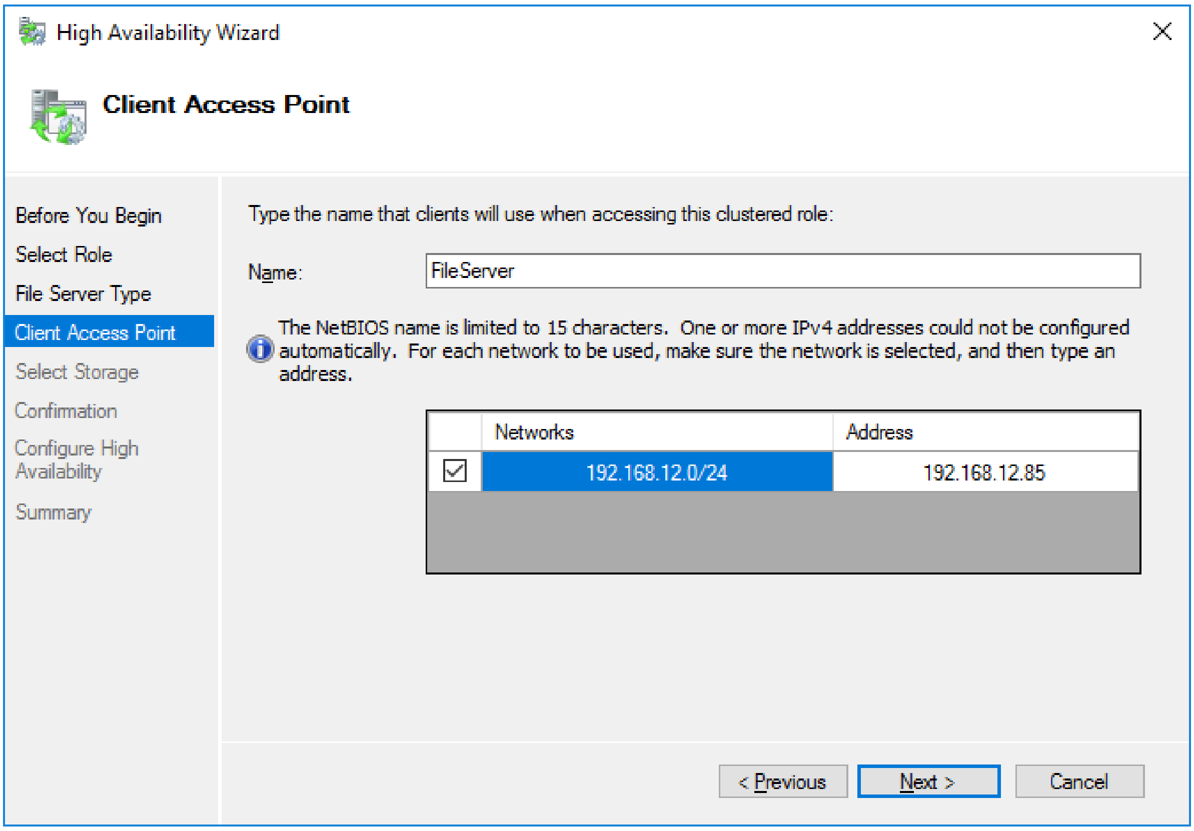
● File Server for general use

Use this option to provide a central location on your network for users to share files or for server applications that open and close files frequently. This option supports both the Server Message Block (SMB) and Network File System (NFS) protocols. It also supports Data Deduplication, File Server Resource Manager, DFS Replication, and other File Services role services.

○ Scale-Out File Server for application data

Use this option to provide storage for server applications or virtual machines that leave files open for extended periods of time. Scale-Out File Server client connections are distributed across nodes in the cluster for better throughput. This option supports the SMB protocol. It does not support the NFS protocol, DFS Replication, or File Server Resource Manager.

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.



High Availability Wizard

Client Access Point

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

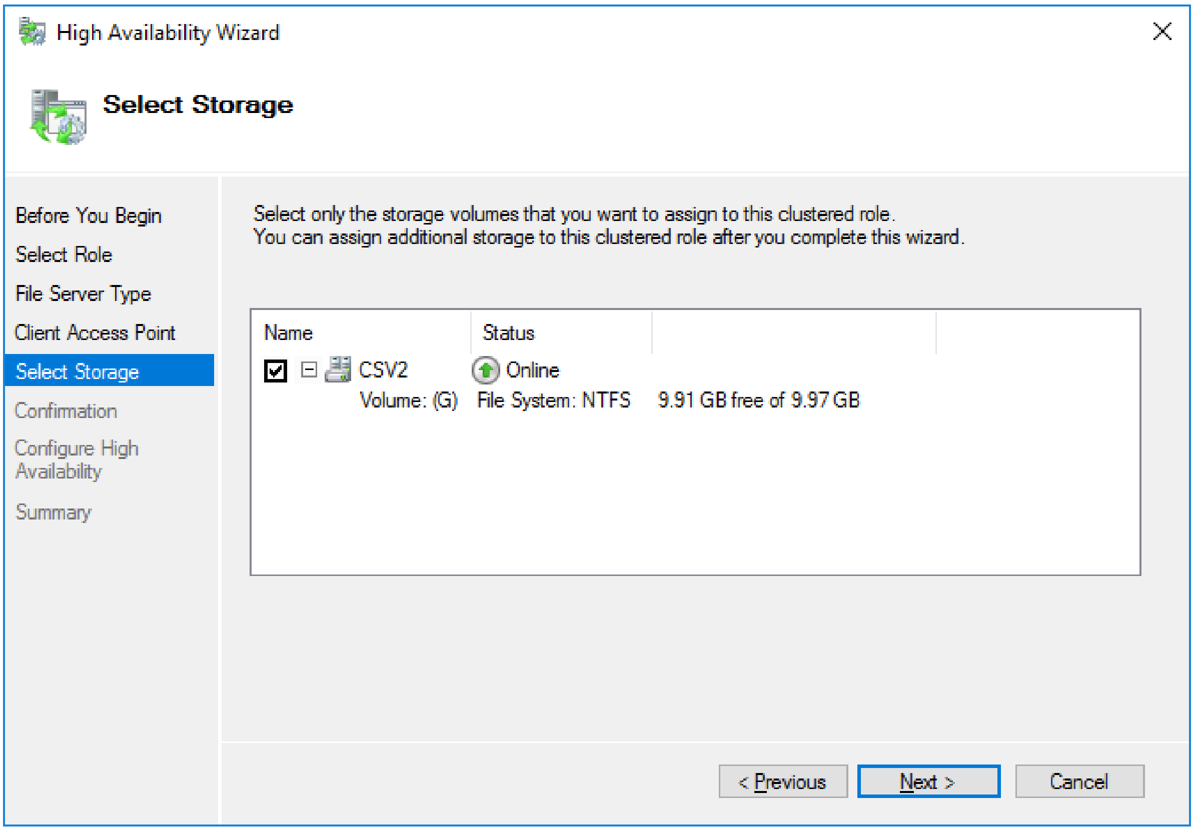
Name: FileServer

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
☑	192.168.12.0/24	192.168.12.85

Click Next to continue.

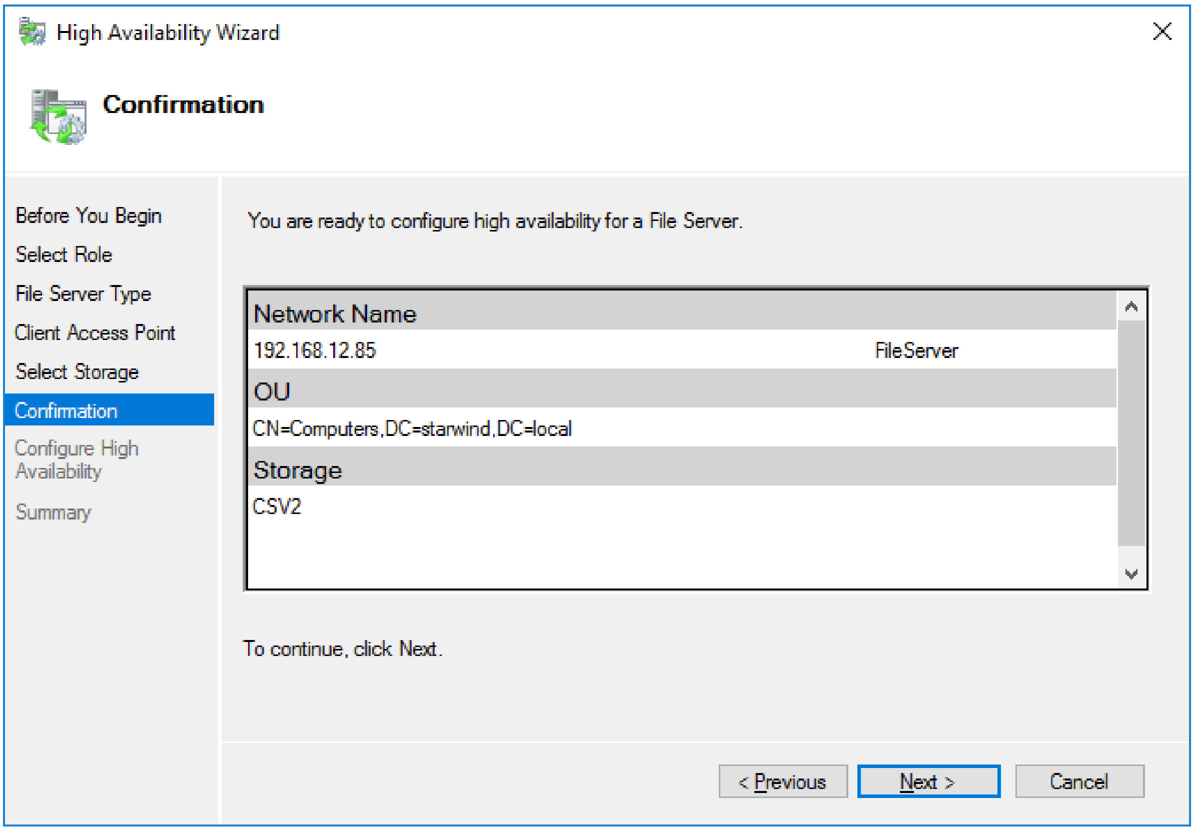
6. Select the Cluster disk and click Next.



Select only the storage volumes that you want to assign to this clustered role.
You can assign additional storage to this clustered role after you complete this wizard.

Name	Status		
☑ ⊟ CSV2	Online		
Volume: (G)	File System: NTFS	9.91 GB free of 9.97 GB	

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



You are ready to configure high availability for a File Server.

Network Name
192.168.12.85 FileServer

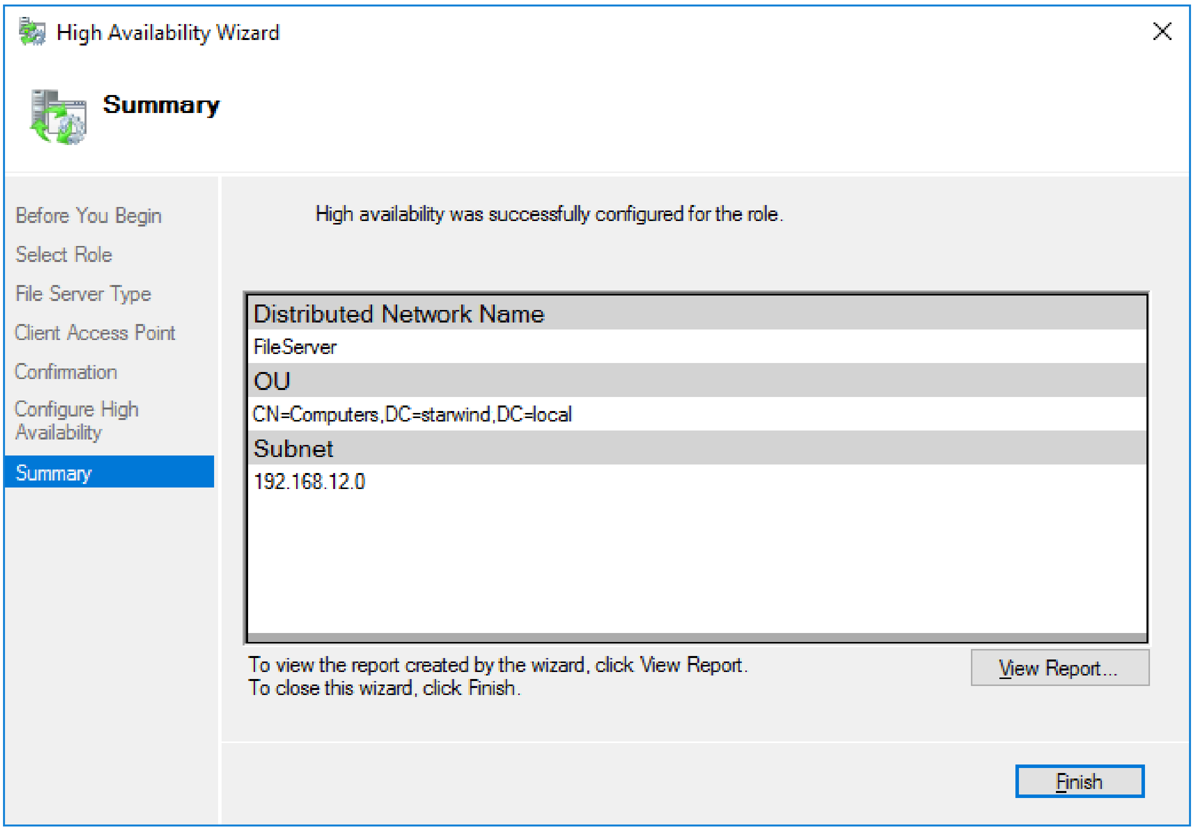
OU
CN=Computers,DC=starwind,DC=local

Storage
CSV2

To continue, click Next.

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

Click Finish to close the Wizard.



High availability was successfully configured for the role.

Distributed Network Name

FileServer

OU

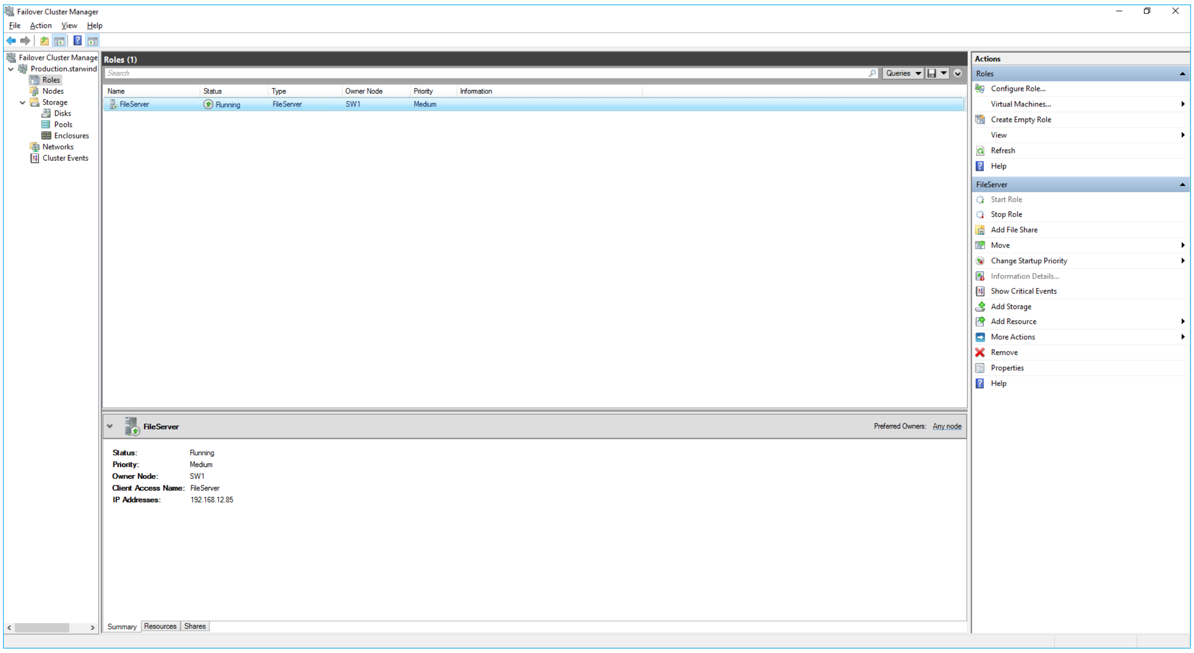
CN=Computers,DC=starwind,DC=local

Subnet

192.168.12.0

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

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



Name	Status	Type	Owner Node	Priority	Information
FileServer	Running	FileServer	SW1	Medium	

FileServer

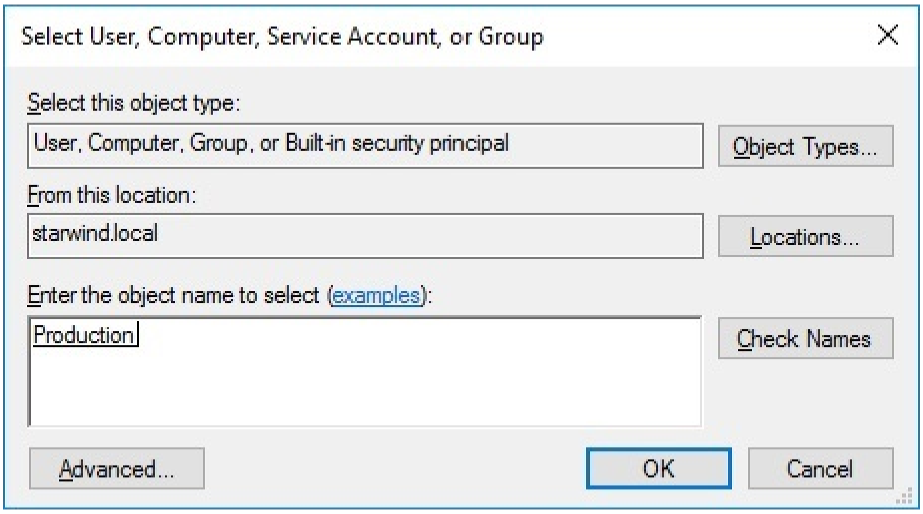
Preferred Owners: Any node

Status: Running
Priority: Medium
Owner Node: SW1
Client Access Name: FileServer
IP Addresses: 192.168.12.85

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)



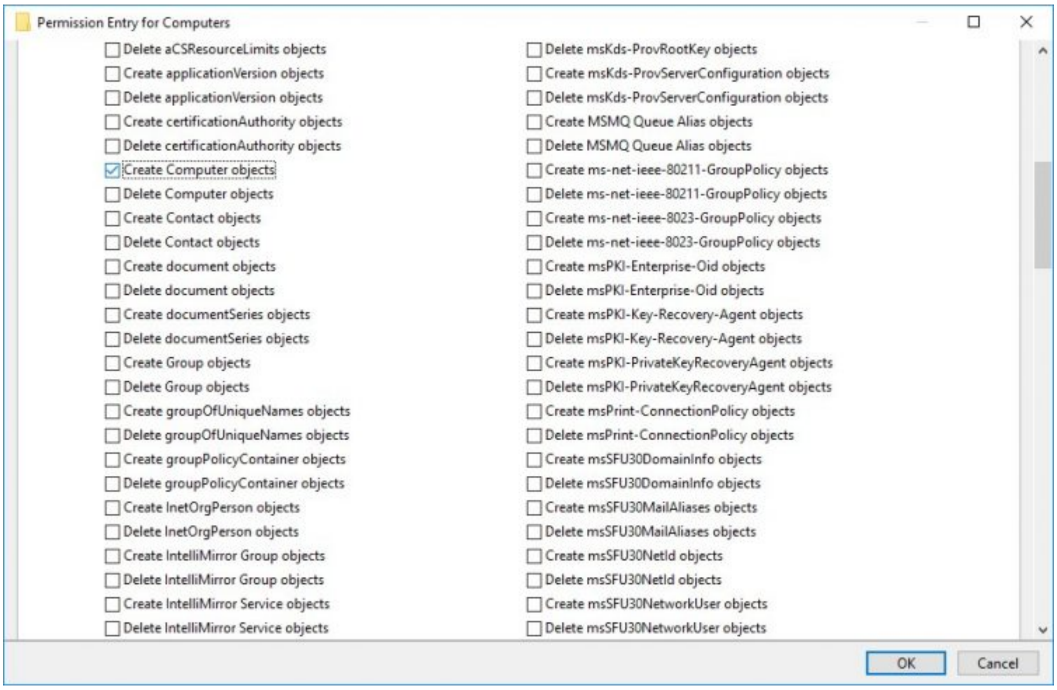
Select User, Computer, Service Account, or Group

Select this object type:
User, Computer, Group, or Built-in security principal

From this location:
starwind.local

Enter the object name to select (examples):
Production

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



Permission Entry for Computers

□ Delete aCSResourceLimits objects
□ Create applicationVersion objects
□ Delete applicationVersion objects
□ Create certificationAuthority objects
□ Delete certificationAuthority objects
☑ Create Computer objects
□ Delete Computer objects
□ Create Contact objects
□ Delete Contact objects
□ Create document objects
□ Delete document objects
□ Create documentSeries objects
□ Delete documentSeries objects
□ Create Group objects
□ Delete Group objects
□ Create groupOfUniqueNames objects
□ Delete groupOfUniqueNames objects
□ Create groupPolicyContainer objects
□ Delete groupPolicyContainer objects
□ Create InetOrgPerson objects
□ Delete InetOrgPerson objects
□ Create IntelliMirror Group objects
□ Delete IntelliMirror Group objects
□ Create IntelliMirror Service objects
□ Delete IntelliMirror Service objects
□ Delete msKds-ProvRootKey objects
□ Create msKds-ProvServerConfiguration objects
□ Delete msKds-ProvServerConfiguration objects
□ Create MSMQ Queue Alias objects
□ Delete MSMQ Queue Alias objects
□ Create ms-net-ieee-80211-GroupPolicy objects
□ Delete ms-net-ieee-80211-GroupPolicy objects
□ Create ms-net-ieee-8023-GroupPolicy objects
□ Delete ms-net-ieee-8023-GroupPolicy objects
□ Create msPKI-Enterprise-Oid objects
□ Delete msPKI-Enterprise-Oid objects
□ Create msPKI-Key-Recovery-Agent objects
□ Delete msPKI-Key-Recovery-Agent objects
□ Create msPKI-PrivateKeyRecoveryAgent objects
□ Delete msPKI-PrivateKeyRecoveryAgent objects
□ Create msPrint-ConnectionPolicy objects
□ Delete msPrint-ConnectionPolicy objects
□ Create msSFU30DomainInfo objects
□ Delete msSFU30DomainInfo objects
□ Create msSFU30MailAliases objects
□ Delete msSFU30MailAliases objects
□ Create msSFU30NetId objects
□ Delete msSFU30NetId objects
□ Create msSFU30NetworkUser objects
□ Delete msSFU30NetworkUser 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

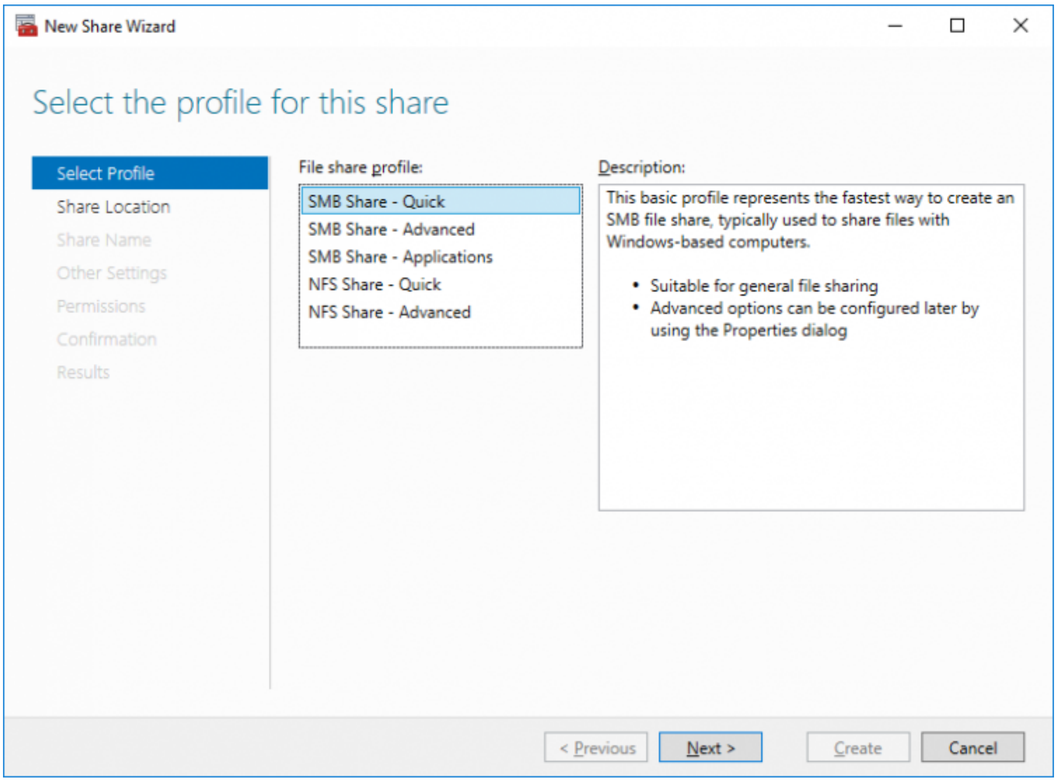
To Add SMB File Share

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.



New Share Wizard

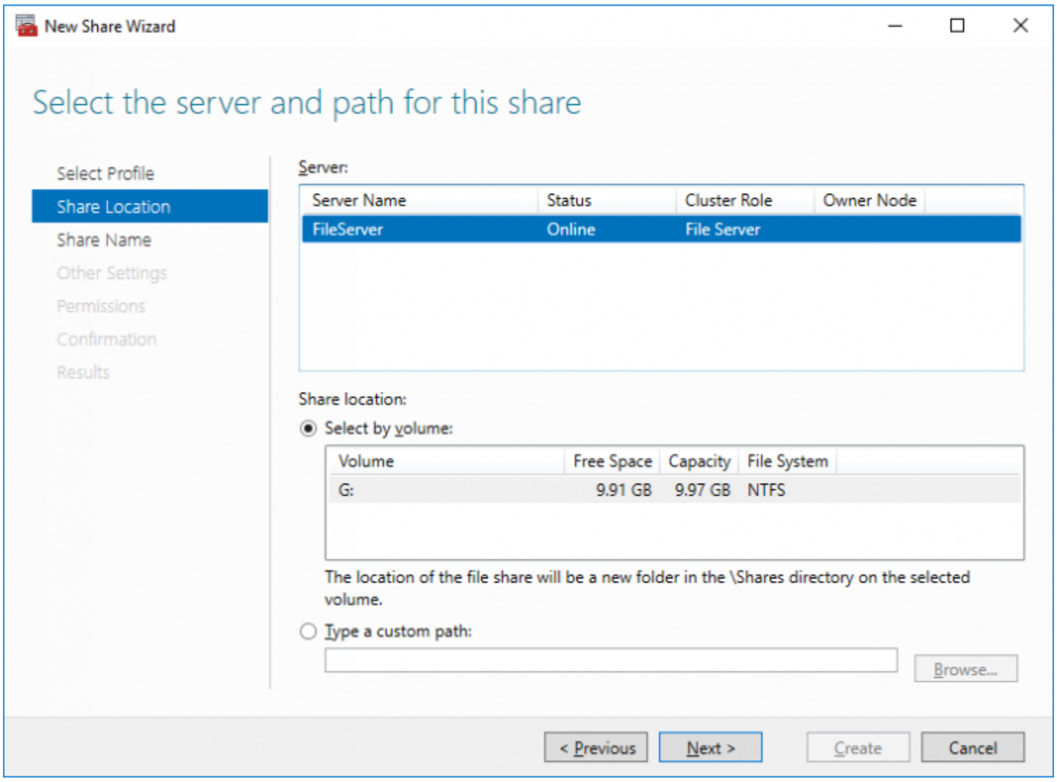
Select the profile for this share

File share profile: SMB Share - Quick

Description:
This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.

- Suitable for general file sharing
- Advanced options can be configured later by using the Properties dialog

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



New Share Wizard

Select the server and path for this share

Server:

Server Name	Status	Cluster Role	Owner Node
FileServer	Online	File Server	

Share location:

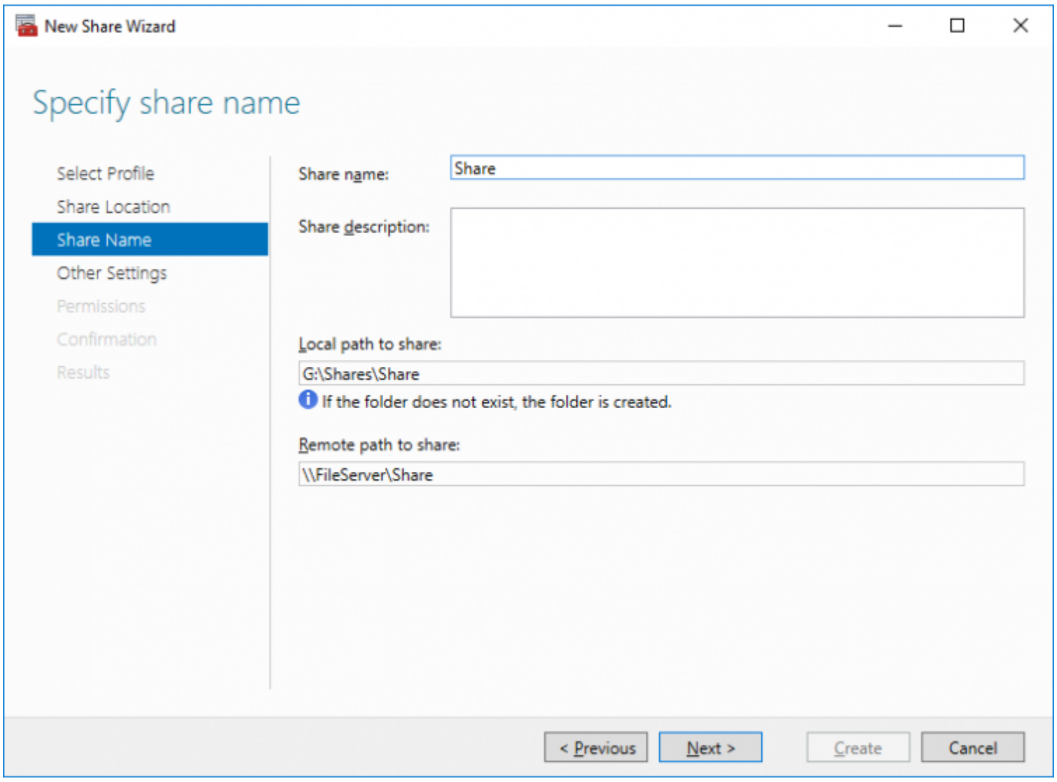
● Select by volume:

Volume	Free Space	Capacity	File System
G:	9.91 GB	9.97 GB	NTFS

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

○ Type a custom path:

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



New Share Wizard

Specify share name

Share name: Share

Share description:

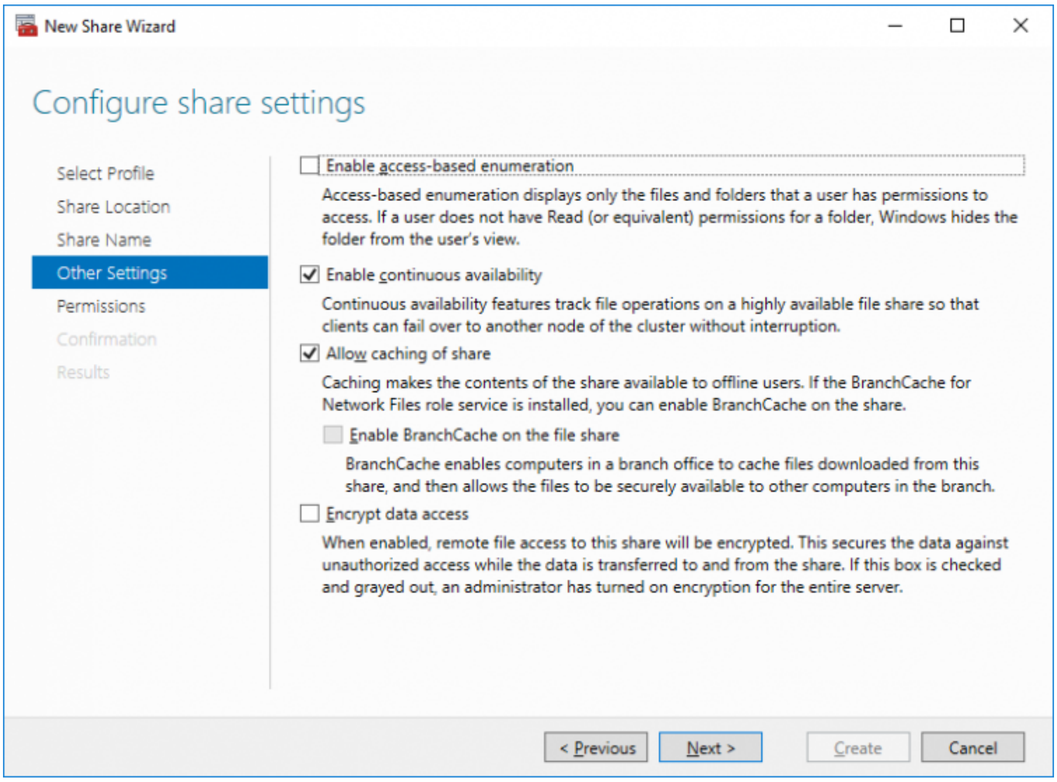
Local path to share:
G:\Shares\Share

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

Remote path to share:
\\FileServer\Share

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

continue.



Configure share settings

□ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☑ Enable continuous availability

Continuous availability features track file operations on a highly available file share so that clients can fail over to another node of the cluster without interruption.

☑ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

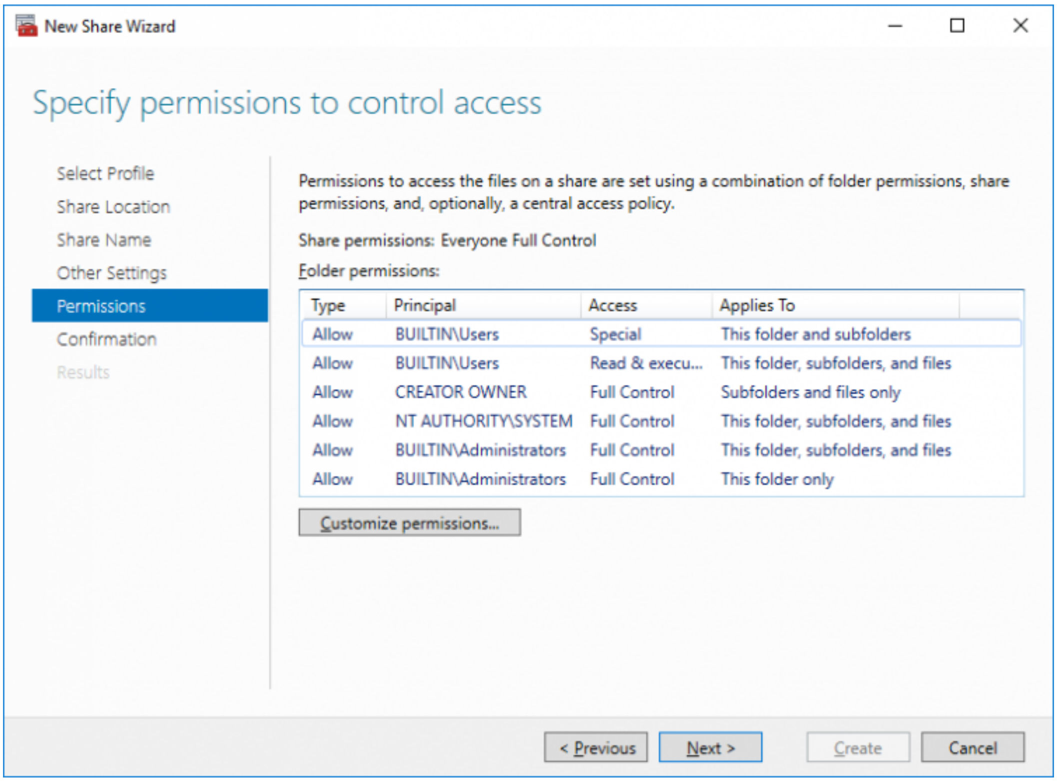
□ Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

□ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

8.Specify the access permissions for the file share.



Specify permissions to control access

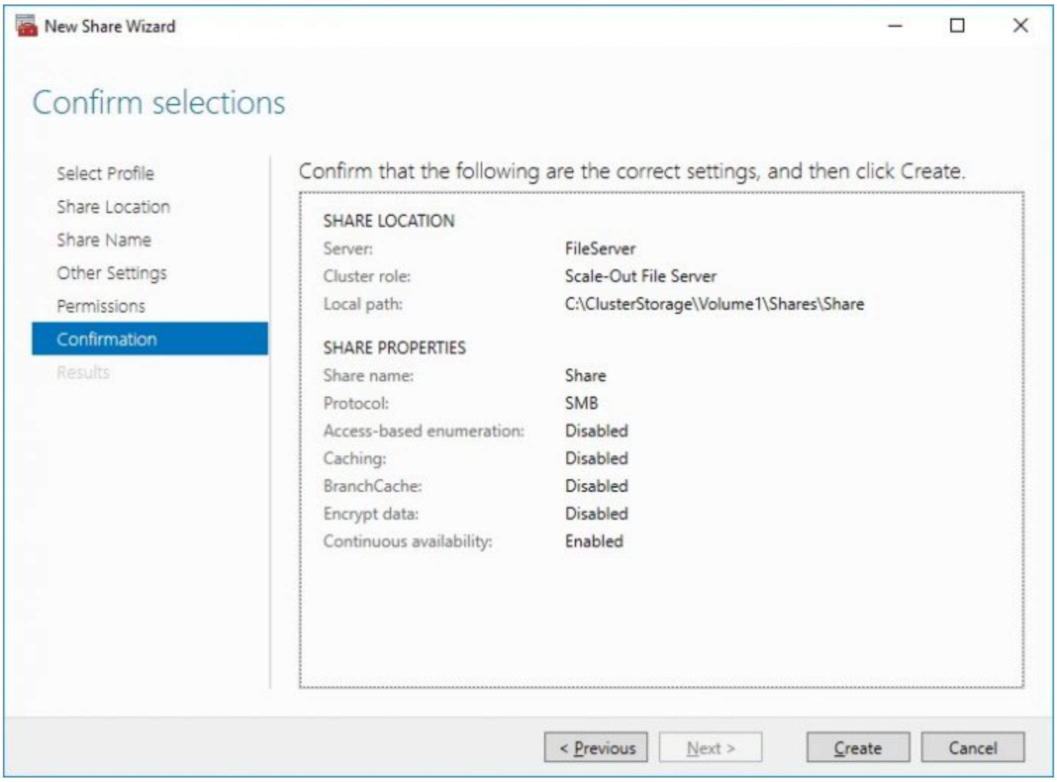
Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

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



Confirm selections

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

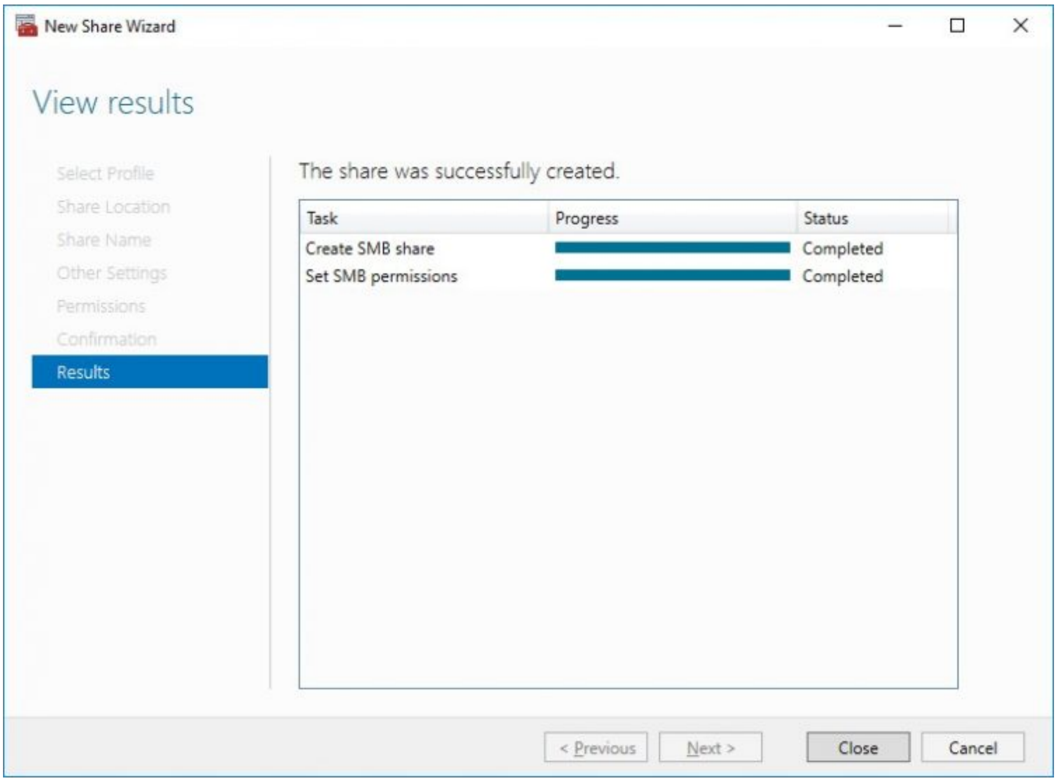
SHARE LOCATION

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

10. Check the summary and click Close.



The share was successfully created.

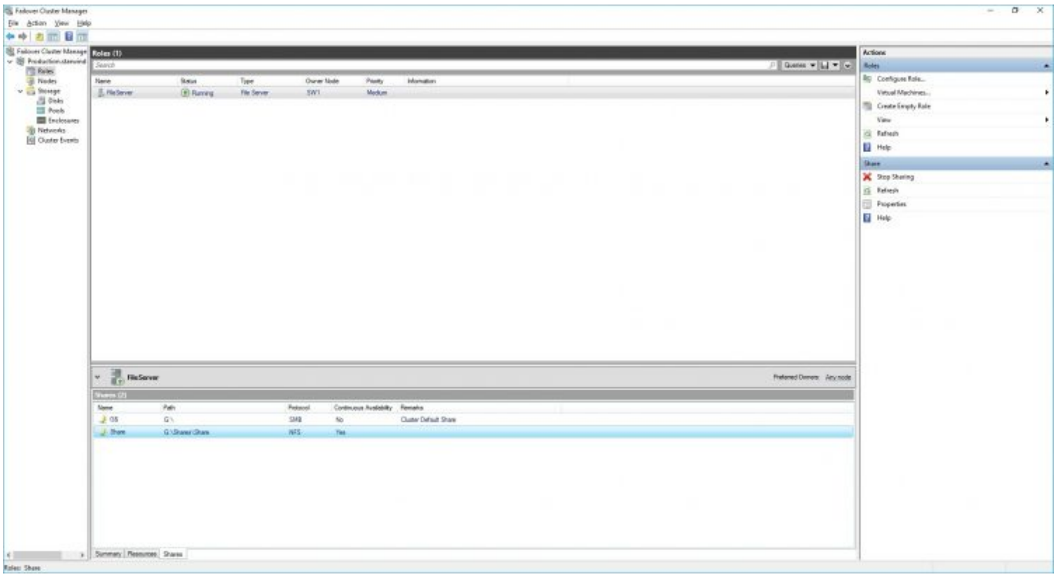
Task	Progress	Status
Create SMB share		Completed
Set SMB permissions		Completed

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.



Name	Status	Type	Owner Node	Priority	Information
FileServer	Running	File Server	SW1	Medium	

Name	Path	Protocol	Continuous Availability	Remarks
OS	G:\	SMB	No	Cluster Default Share
Share	G:\Shares\Share	NFS	Yes	

Configuring Nfs File Share

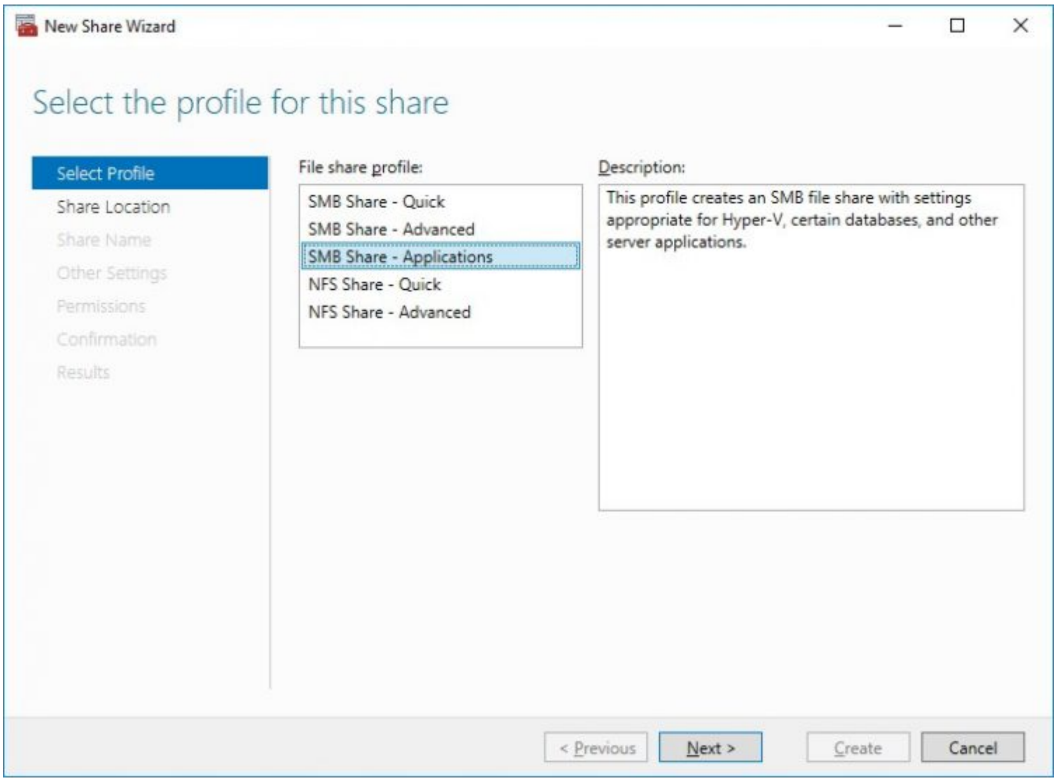
To Add NFS File Share

1. Open Failover Cluster Manager.

2. Expand the cluster and then click Roles.

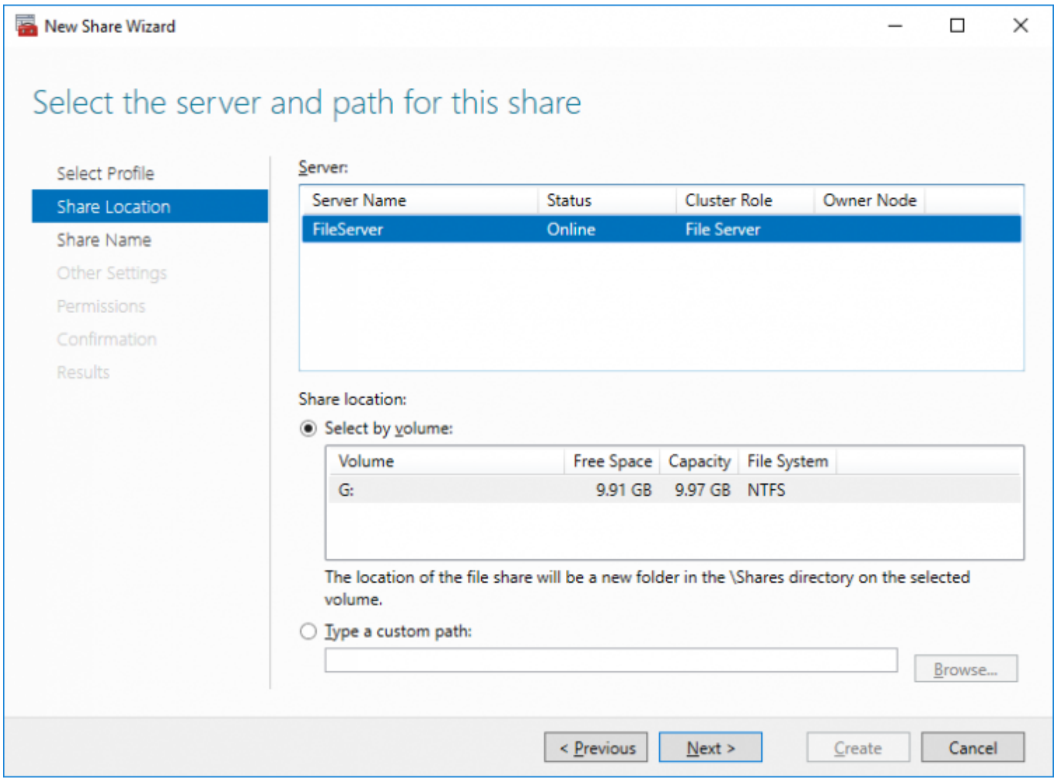
3. Right-click the File Server role and then press Add File Share.

4. On the Select the profile for this share page, click NFS Share – Quick and then click Next.



This profile creates an SMB file share with settings appropriate for Hyper-V, certain databases, and other server applications.

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



Server:

Server Name	Status	Cluster Role	Owner Node
FileServer	Online	File Server	

Share location:

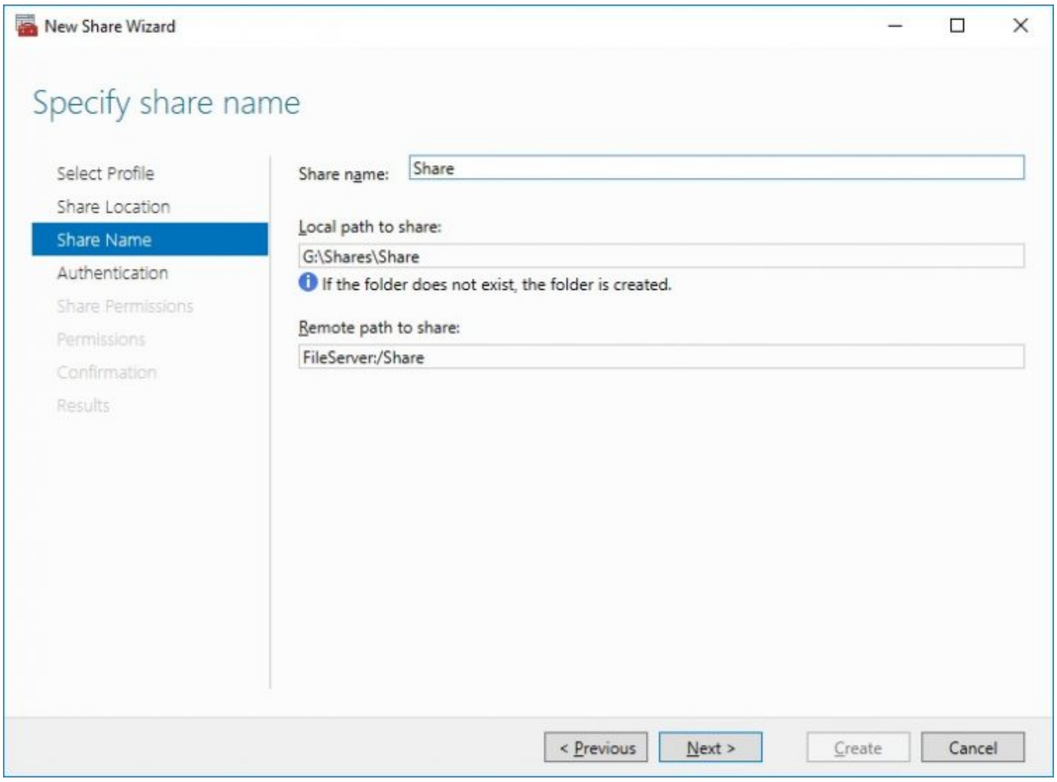
● Select by volume:

Volume	Free Space	Capacity	File System
G:	9.91 GB	9.97 GB	NTFS

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

○ Type a custom path:

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



Share name: Share

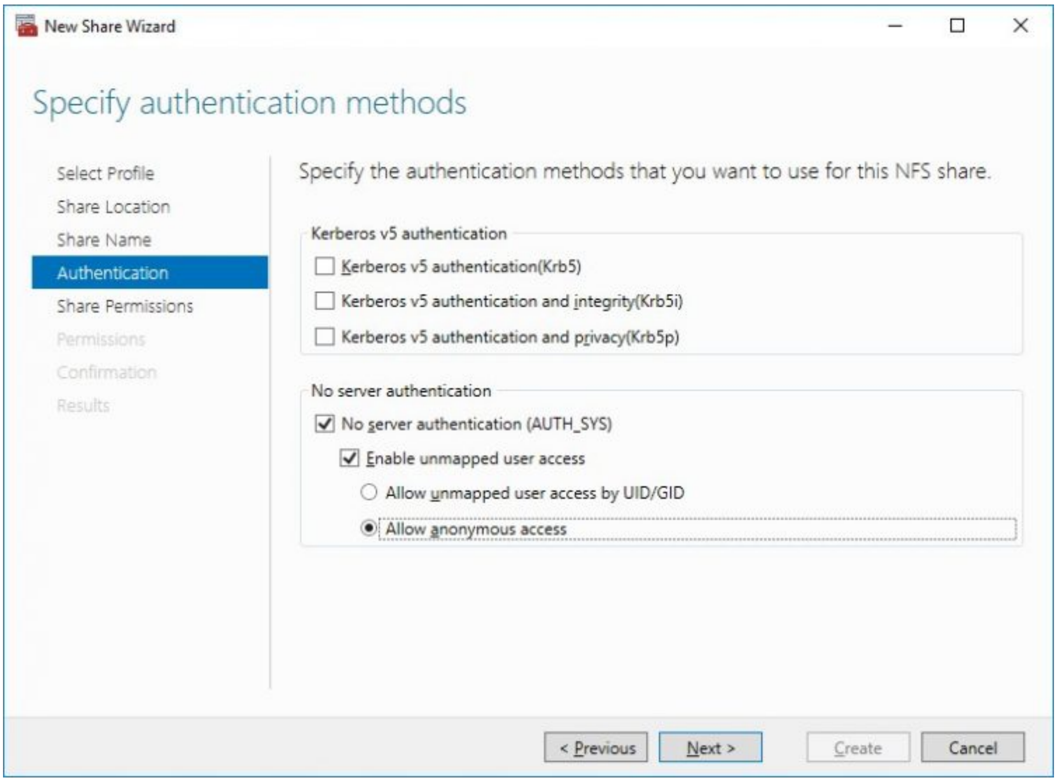
Local path to share:
G:\Shares\Share

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

Remote path to share:
FileServer:/Share

7. Specify the Authentication. Click Next and confirm the message in pop-up window to

continue.



New Share Wizard

Specify authentication methods

Specify the authentication methods that you want to use for this NFS share.

Kerberos v5 authentication

□ Kerberos v5 authentication(Krb5)

□ Kerberos v5 authentication and integrity(Krb5i)

□ Kerberos v5 authentication and privacy(Krb5p)

No server authentication

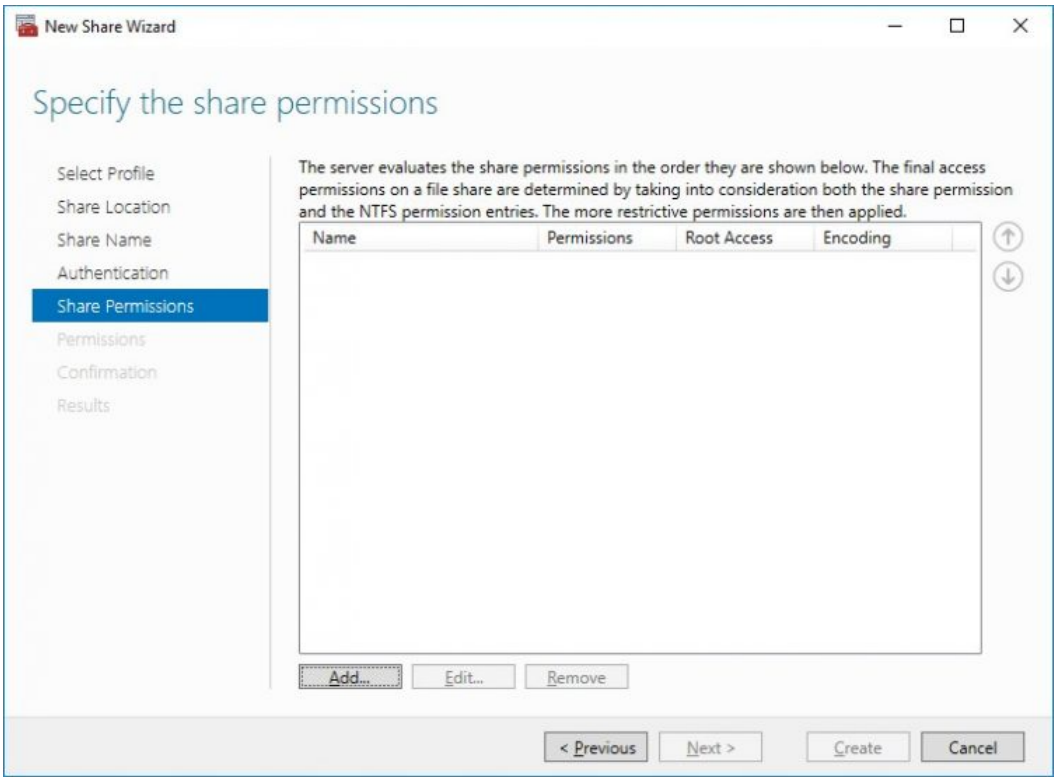
☑ No server authentication (AUTH_SYS)

☑ Enable unmapped user access

○ Allow unmapped user access by UID/GID

● Allow anonymous access

8. Click Add and specify Share Permissions.

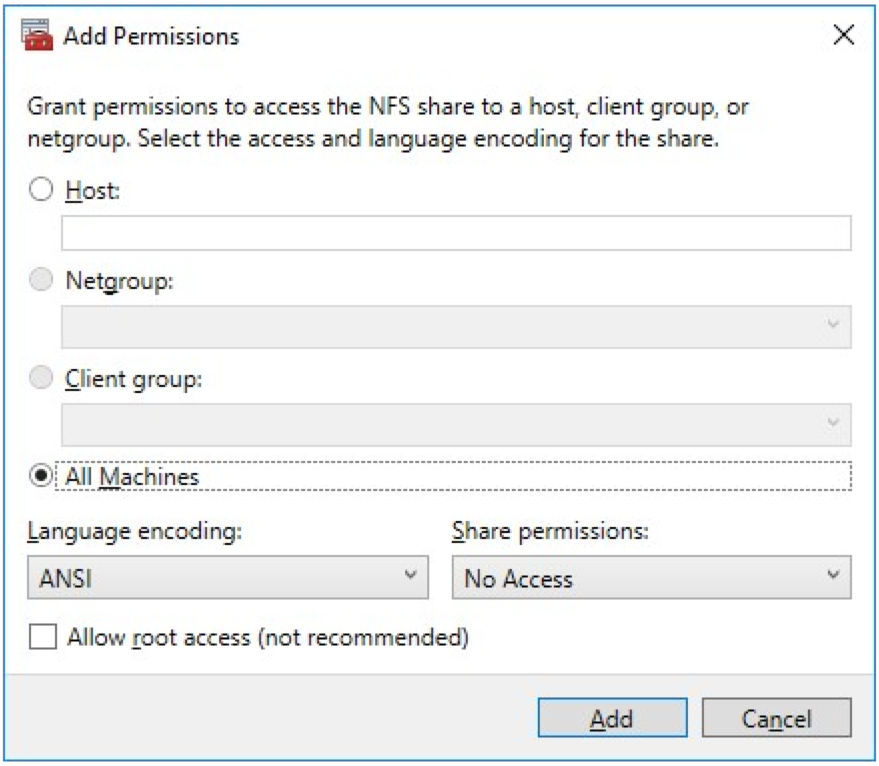


New Share Wizard

Specify the share permissions

The server evaluates the share permissions in the order they are shown below. The final access permissions on a file share are determined by taking into consideration both the share permission and the NTFS permission entries. The more restrictive permissions are then applied.

Name	Permissions	Root Access	Encoding



Add Permissions

Grant permissions to access the NFS share to a host, client group, or netgroup. Select the access and language encoding for the share.

○ Host:

○ Netgroup:

○ Client group:

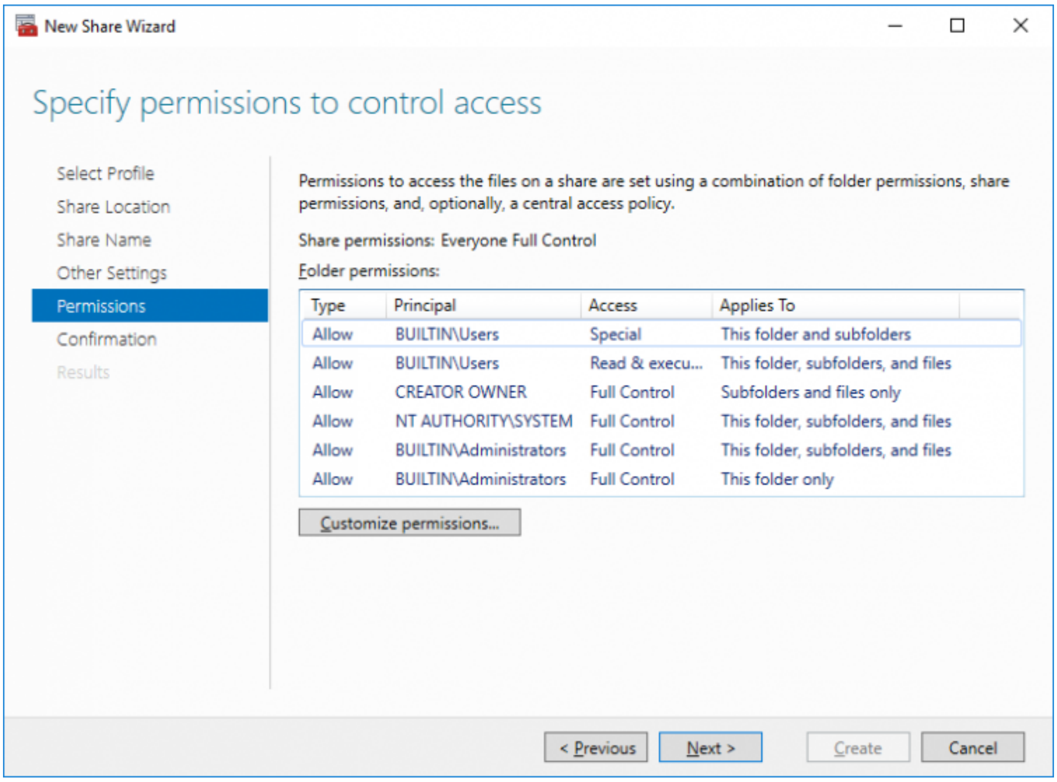
● All Machines

Language encoding: ANSI

Share permissions: No Access

□ Allow root access (not recommended)

9. Specify the access permissions for the file share.



New Share Wizard

Specify permissions to control access

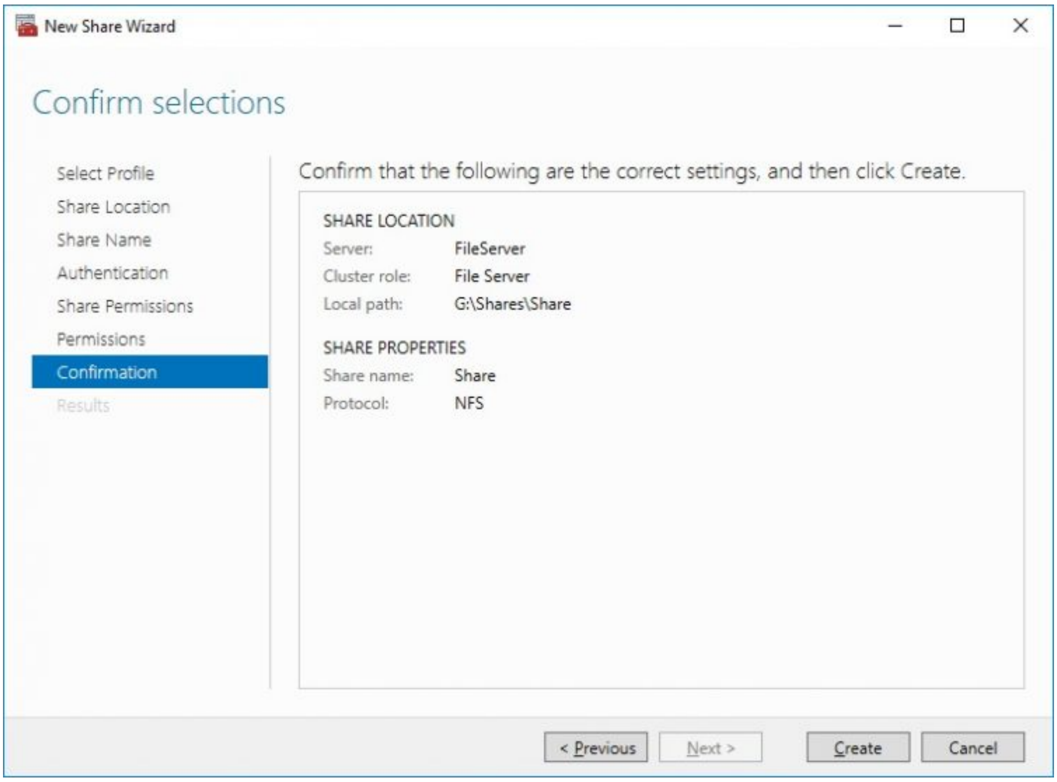
Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

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



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

SHARE LOCATION

Server: FileServer

Cluster role: File Server

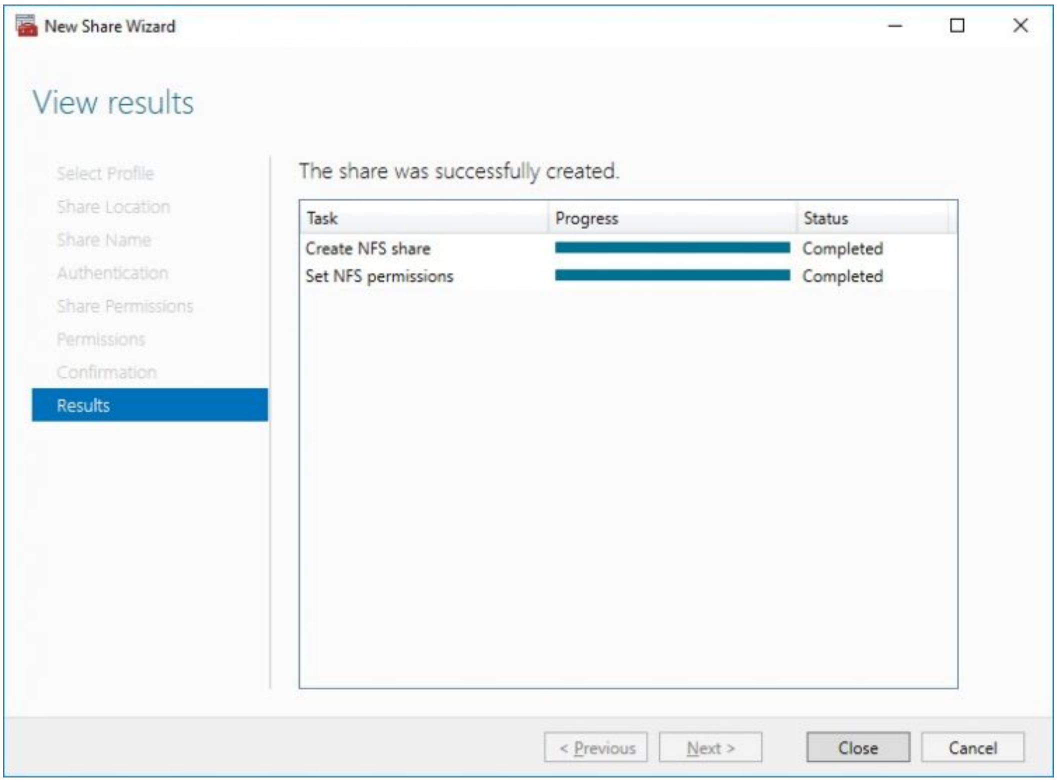
Local path: G:\Shares\Share

SHARE PROPERTIES

Share name: Share

Protocol: NFS

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

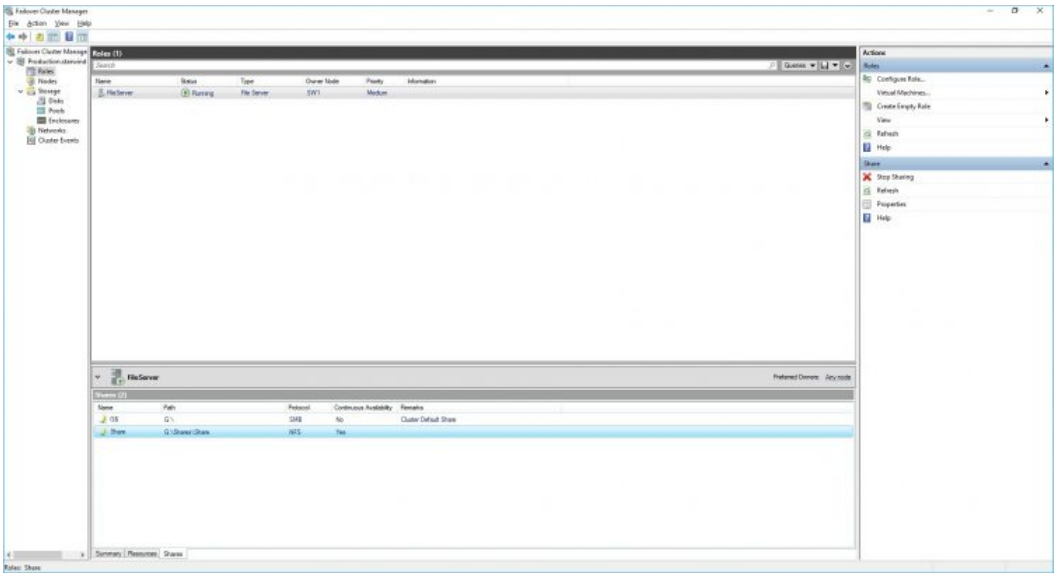


The share was successfully created.

Task	Progress	Status
Create NFS share		Completed
Set NFS permissions		Completed

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



Name	Status	Type	Owner Node	Priority	Information
FileServer	Running	File Server	SW1	Medium	

Name	Path	Protocol	Continuous Availability	Remarks
G$	G:\	SMB	No	Cluster Default Share
Share	G:\Shares\Share	NFS	Yes	

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