StarWind Virtual SAN: Configuration Guide for Microsoft Windows Server [Hyper-V], VSAN Deployed as a Windows Application

2024

TECHNICAL PAPERS

Trademarks

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

Changes

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

Technical Support and Services

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

About StarWind

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

Copyright ©2009-2018 StarWind Software Inc.

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

Applies To: Windows Server 2016, Windows Server 2019, Windows Server 2022

Annotation

Relevant products

This guide applies to StarWind Virtual SAN and StarWind Virtual SAN Free (Version V8 (build 15260) and earlier).

Purpose

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

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.

Prerequisites

StarWind Virtual SAN system requirements

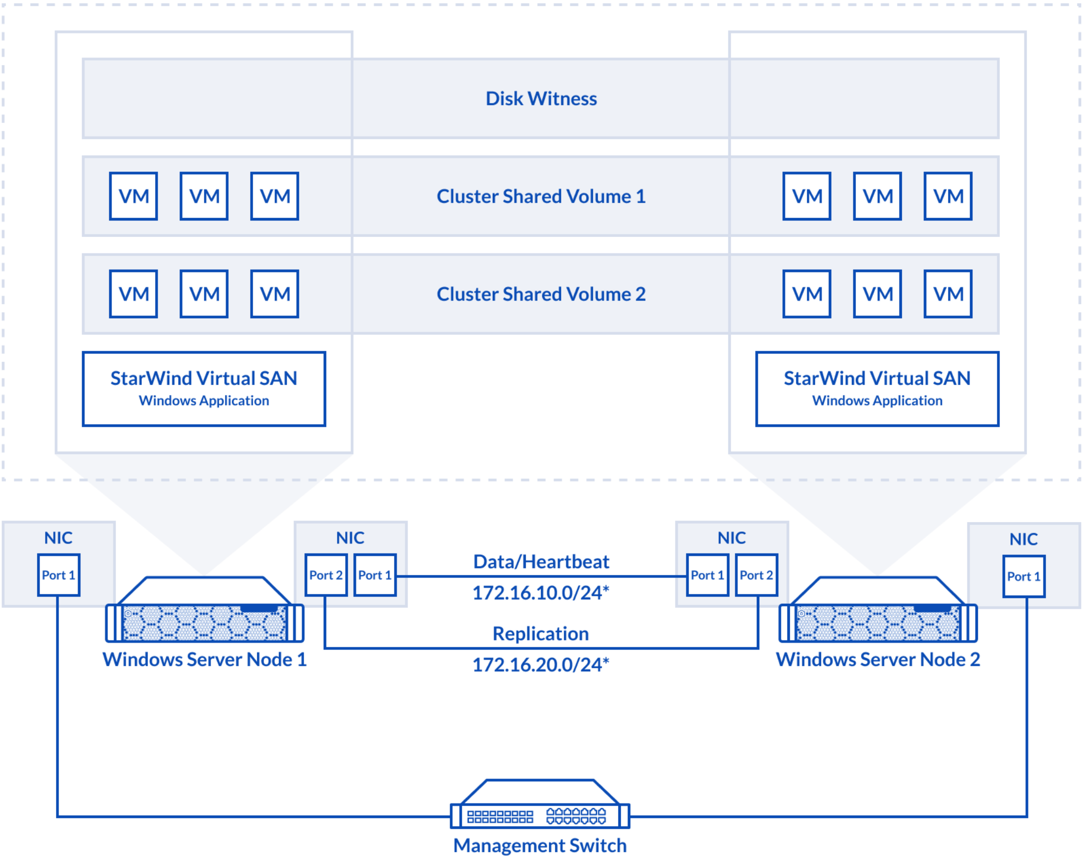
Prior to installing StarWind Virtual SAN, please make sure that the system meets the requirements, which are available via the following link:
https://www.starwindsoftware.com/system-requirements

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

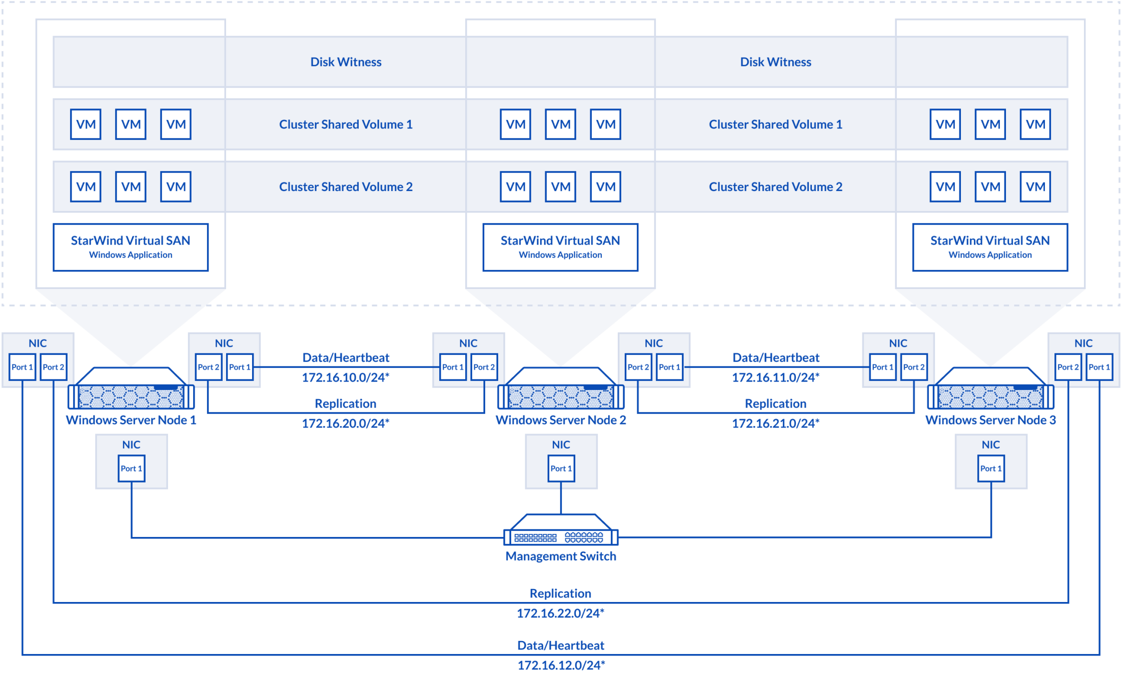
Please read StarWind Virtual SAN Best Practices document for additional information:
https://www.starwindsoftware.com/resource-library/starwind-virtual-san-best-practices

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).

For 2-node scenario, 172.16.10.x subnet is used for iSCSI/StarWind heartbeat traffic, while 172.16.20.x subnet is used for the Synchronization traffic.

For 3-node scenario, 172.16.10.x, 172.16.11.x,172.16.12.x subnets are used for the iSCSI/StarWind heartbeat traffic, while 172.16.20.x,172.16.21.x, 172.16.22.x subnets are used for the Synchronization traffic.

4. Set MTU size to 9014 or 9000 depending on network cards vendor recommendations on iSCSI and Sync interfaces using the following Powershell script.

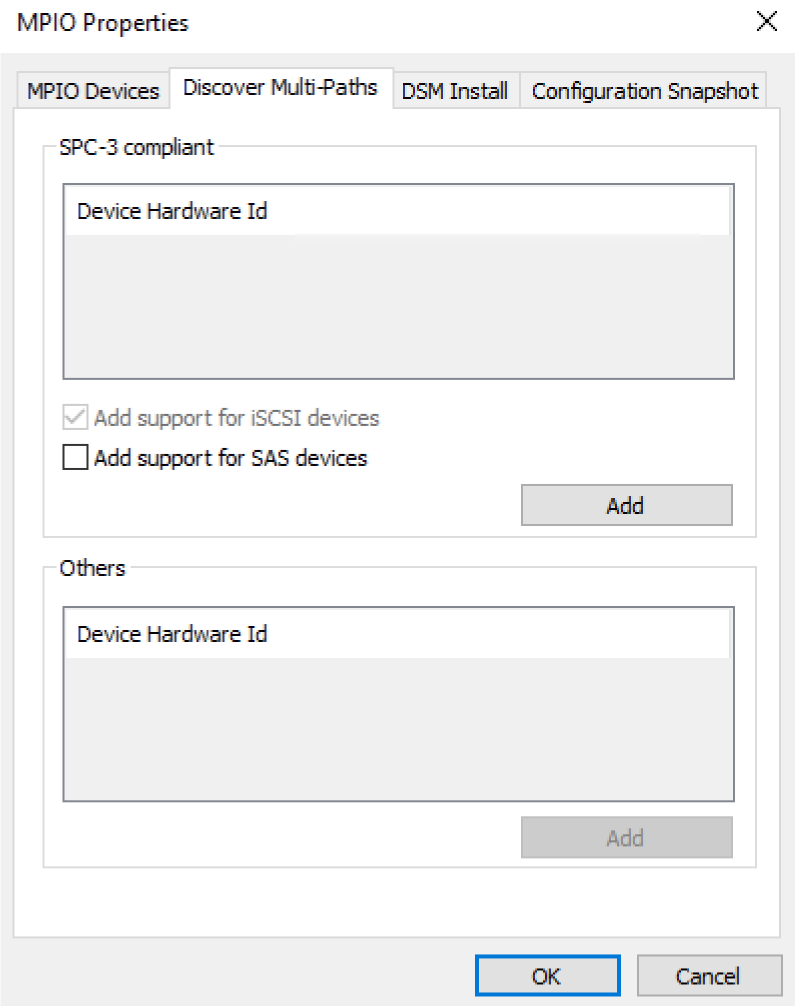
```
$iSCSIs = (Get-NetAdapter -Name "*iSCSI*").Name
$Syncs = (Get-NetAdapter -Name "*Sync*").Name
foreach ($iSCSI in $iSCSIs) {
Set-NetAdapterAdvancedProperty -Name “$iSCSI” -RegistryKeyword
“*JumboPacket” -Registryvalue 9014
Get-NetAdapterAdvancedProperty -Name "$iSCSI" -RegistryKeyword
“*JumboPacket”
}
foreach ($Sync in $Syncs) {
Set-NetAdapterAdvancedProperty -Name “$Sync” -RegistryKeyword
“*JumboPacket” -Registryvalue 9014
Get-NetAdapterAdvancedProperty -Name "$Sync" -RegistryKeyword
“*JumboPacket”
}
```

It will apply MTU 9014 (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.

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

```
mpiocpl
```

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



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

8. Repeat the same procedure on the other server.

Automated Storage Tiering Configuration

In case of using Automated Storage Tiering, the individual spinning disks and flash drives can be either connected into OS directly in Pass-Through mode or preconfigured into separate virtual "SSD" and "HDD" LUNs, and then attached into the host OS.
NOTE: Please make sure that the final configuration which is expected to be put into production is fully supported by either the software vendor (i.e., StarWind, Microsoft, VMware, etc.) or particular MSP/ISV who is in charge of the whole project. Please ensure that specific workload expectations can be met with both existing and future deployments. Depending on the configuration it can be either self-supported, partially supported, or fully supported.
NOTE: Simple Tier has no redundancy built-in, so in case of either individual spinning disk and/or flash drive failure there is a risk of losing the data. It is recommended to

configure resilient storage to be used as the underlying storage for the Tier. Please make sure that such a configuration is supported by either the software vendor (i.e., StarWind, Microsoft, VMware, etc.) or/and MSP/ISV.

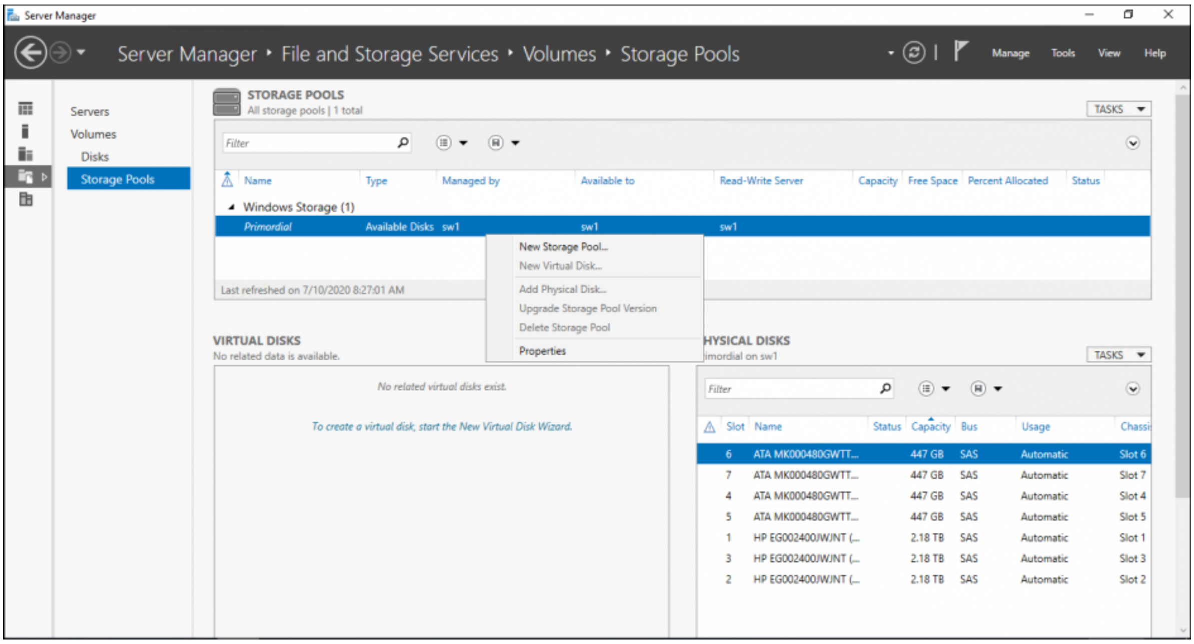
Automated Storage Tier creation

There are two ways to configure Automated Storage Tiering. It can be done via Server Manager and via the PowerShell console.

The first level of Storage Tier is Storage pools. At this level, separate physical disks are united into a single pool, providing the ability to flexibly expand the capacity and delegate administration.

The upper level is Storage Spaces. At this level, virtual disks are created using the available capacity of a storage pool. Storage Spaces feature the following characteristics: resiliency level, storage tiers, fixed provisioning, and precise administrative control.

1. Launch Server Manager->File and Storage Services->Volumes->Storage Pools. All disks available for Storage Pool are listed in Physical Disks. Click New Storage Pool.


Server Manager
Server Manager ‣ File and Storage Services ‣ Volumes ‣ Storage Pools
Manage
Tools
View
Help
Servers
Volumes
Disks
Storage Pools
STORAGE POOLS
All storage pools | 1 total
TASKS
Filter
New Storage Pool...
New Virtual Disk...
Add Physical Disk...
Upgrade Storage Pool Version
Delete Storage Pool
Properties
VIRTUAL DISKS
No related data is available.
No related virtual disks exist.
To create a virtual disk, start the New Virtual Disk Wizard.
HYSICAL DISKS
imordial on sw1
TASKS
Filter

Name	Type	Managed by	Available to	Read-Write Server	Capacity	Free Space	Percent Allocated	Status
Windows Storage (1)								
Primordial	Available Disks	sw1	sw1	sw1				

Last refreshed on 7/10/2020 8:27:01 AM

⚠	Slot	Name	Status	Capacity	Bus	Usage	Chassi
	6	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 6
	7	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 7
	4	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 4
	5	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 5
	1	HP EG002400JWJNT (...		2.18 TB	SAS	Automatic	Slot 1
	3	HP EG002400JWJNT (...		2.18 TB	SAS	Automatic	Slot 3
	2	HP EG002400JWJNT (...		2.18 TB	SAS	Automatic	Slot 2

NOTE:

```
Get-PhysicalDisk
```

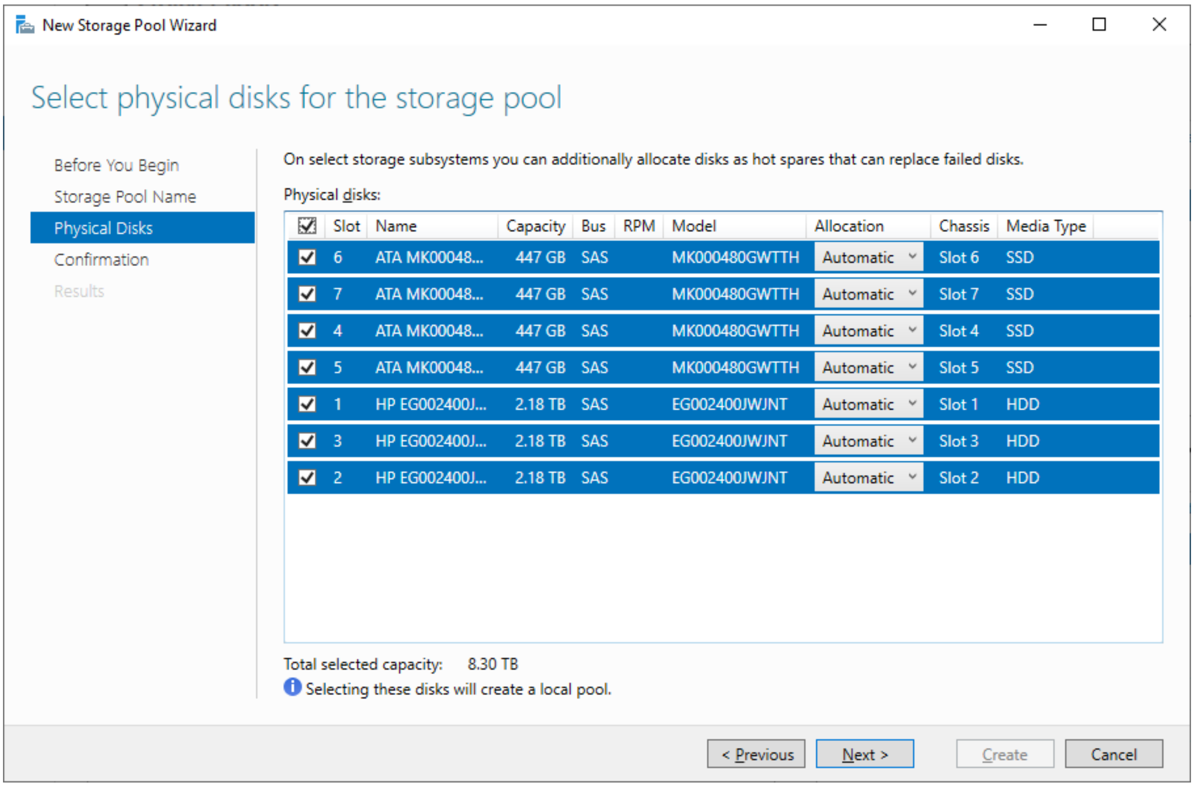
is a PowerShell command that allows checking the disks available for Storage Pool.

```
Get-PhysicalDisk | sort-object SlotNumber | select SlotNumber,
FriendlyName, Manufacturer, Model, PhysicalSectorSize,
LogicalSectorSize | ft
```

is a PowerShell command that allows checking the parameters of physical disks.

2. Specify a Storage Pool name:

3. Select the disks for Storage Pool and then press Next. In case of using Storage Tiers with both SSDs and HDDs, all these disks need to be added into the Storage Pool.



New Storage Pool Wizard

Select physical disks for the storage pool

On select storage subsystems you can additionally allocate disks as hot spares that can replace failed disks.

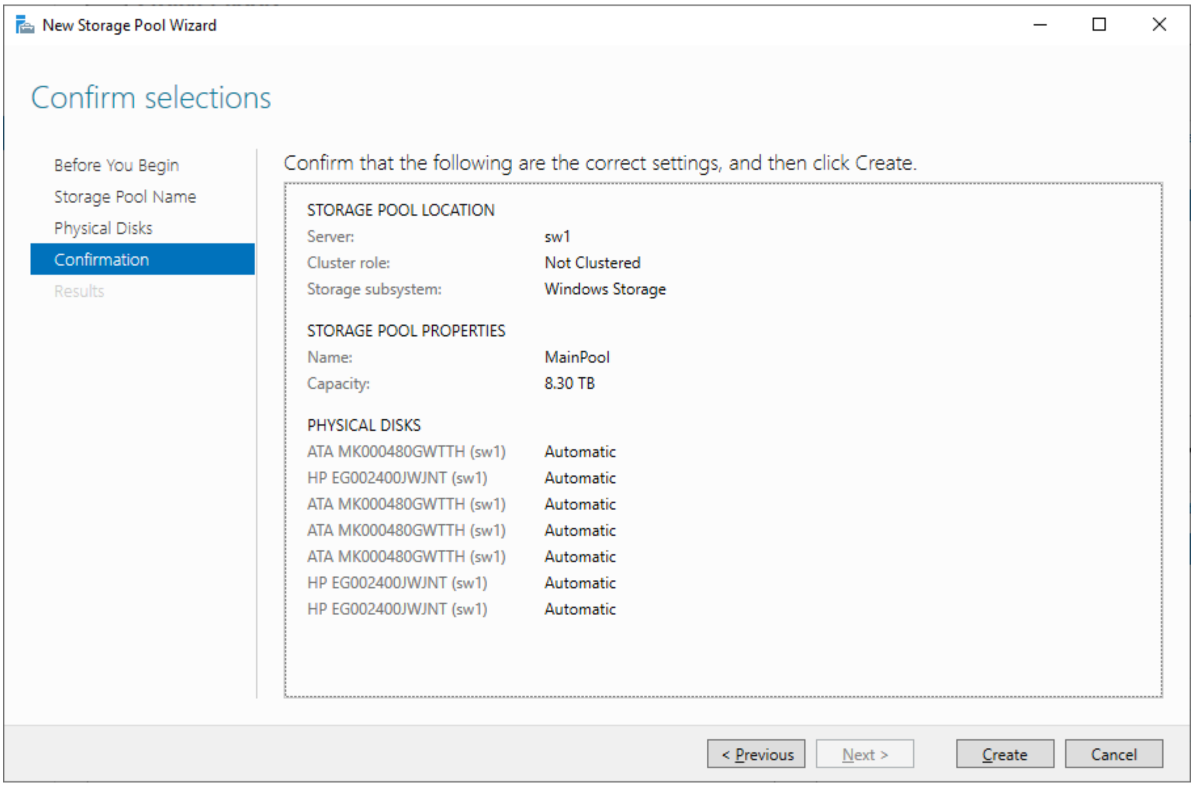
Physical disks:

☑	Slot	Name	Capacity	Bus	RPM	Model	Allocation	Chassis	Media Type
☑	6	ATA MK00048...	447 GB	SAS		MK000480GWTTH	Automatic	Slot 6	SSD
☑	7	ATA MK00048...	447 GB	SAS		MK000480GWTTH	Automatic	Slot 7	SSD
☑	4	ATA MK00048...	447 GB	SAS		MK000480GWTTH	Automatic	Slot 4	SSD
☑	5	ATA MK00048...	447 GB	SAS		MK000480GWTTH	Automatic	Slot 5	SSD
☑	1	HP EG002400J...	2.18 TB	SAS		EG002400JWJNT	Automatic	Slot 1	HDD
☑	3	HP EG002400J...	2.18 TB	SAS		EG002400JWJNT	Automatic	Slot 3	HDD
☑	2	HP EG002400J...	2.18 TB	SAS		EG002400JWJNT	Automatic	Slot 2	HDD

Total selected capacity: 8.30 TB

Selecting these disks will create a local pool.

4. Confirm the correct settings and click Create to create Storage Pool.



Confirm selections

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

STORAGE POOL LOCATION

Server:	sw1
Cluster role:	Not Clustered
Storage subsystem:	Windows Storage

STORAGE POOL PROPERTIES

Name:	MainPool
Capacity:	8.30 TB

PHYSICAL DISKS

ATA MK000480GWTTH (sw1)	Automatic
HP EG002400JWJNT (sw1)	Automatic
ATA MK000480GWTTH (sw1)	Automatic
ATA MK000480GWTTH (sw1)	Automatic
ATA MK000480GWTTH (sw1)	Automatic
HP EG002400JWJNT (sw1)	Automatic
HP EG002400JWJNT (sw1)	Automatic

NOTE: There might be cases when the MediaType parameter should be changed manually. It can be done with the following PowerShell commands:

Assign SSD MediaType for the disk with size less than [ ]GB:

```
Get-PhysicalDisk | where Size -lt [ ]GB | Set-PhysicalDisk -
MediaType SSD
```

Assign HDD MediaType for the disk with size more than [ ]GB:

```
Get-PhysicalDisk | where Size -gt [ ]GB | Set-PhysicalDisk -
MediaType HDD
```

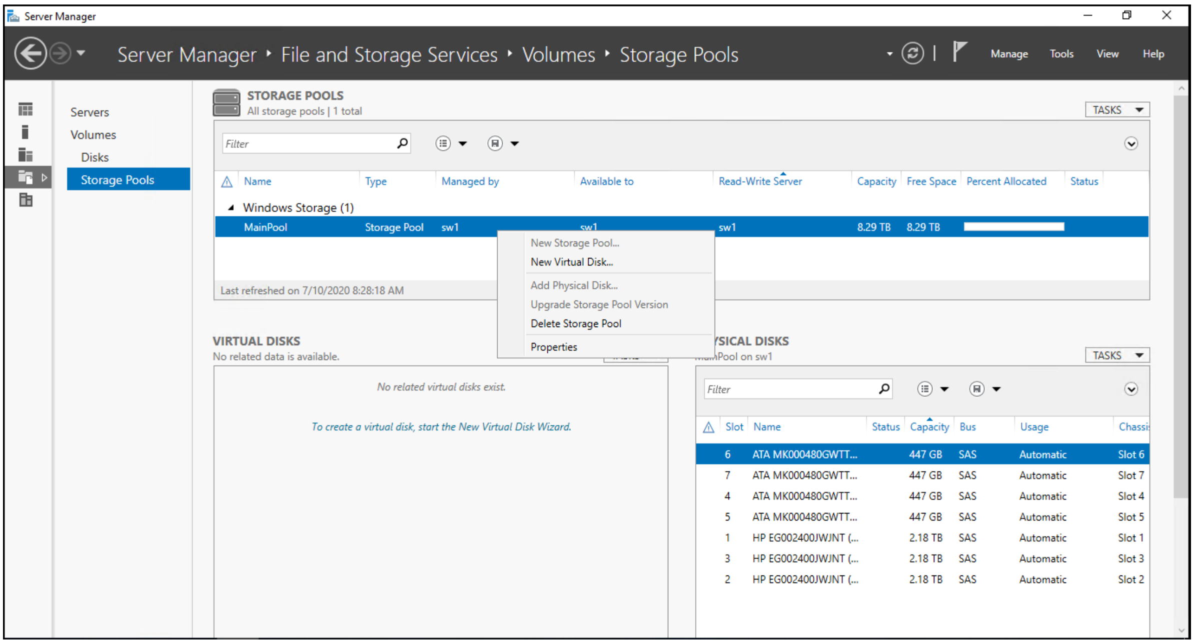
Additionally, the following commands can be used:

```
Get-PhysicalDisk | ft FriendlyName,CanPool,Size,MediaType
Set-PhysicalDisk -FriendlyName [disk name] -MediaType [SSD or
HDD]
```

or

```
Get-PhysicalDisk | ft FriendlyName,CanPool,Size,MediaType
Get-PhysicalDisk | Where Size -EQ [disk size] | Set-
PhysicalDisk -MediaType [SSD or HDD]
```

5. The next step is to create a virtual disk on the storage pool. It is possible to create multiple virtual disks that exist in the storage pool and then create multiple volumes that exist in each virtual disk. Create new virtual disk by right-clicking on the storage pool and selecting New Virtual Disk.



STORAGE POOLS
All storage pools | 1 total

Name	Type	Managed by	Available to	Read-Write Server	Capacity	Free Space	Percent Allocated	Status
Windows Storage (1)								
MainPool	Storage Pool	sw1	sw1	sw1	8.29 TB	8.29 TB		

Last refreshed on 7/10/2020 8:28:18 AM

VIRTUAL DISKS
No related data is available.

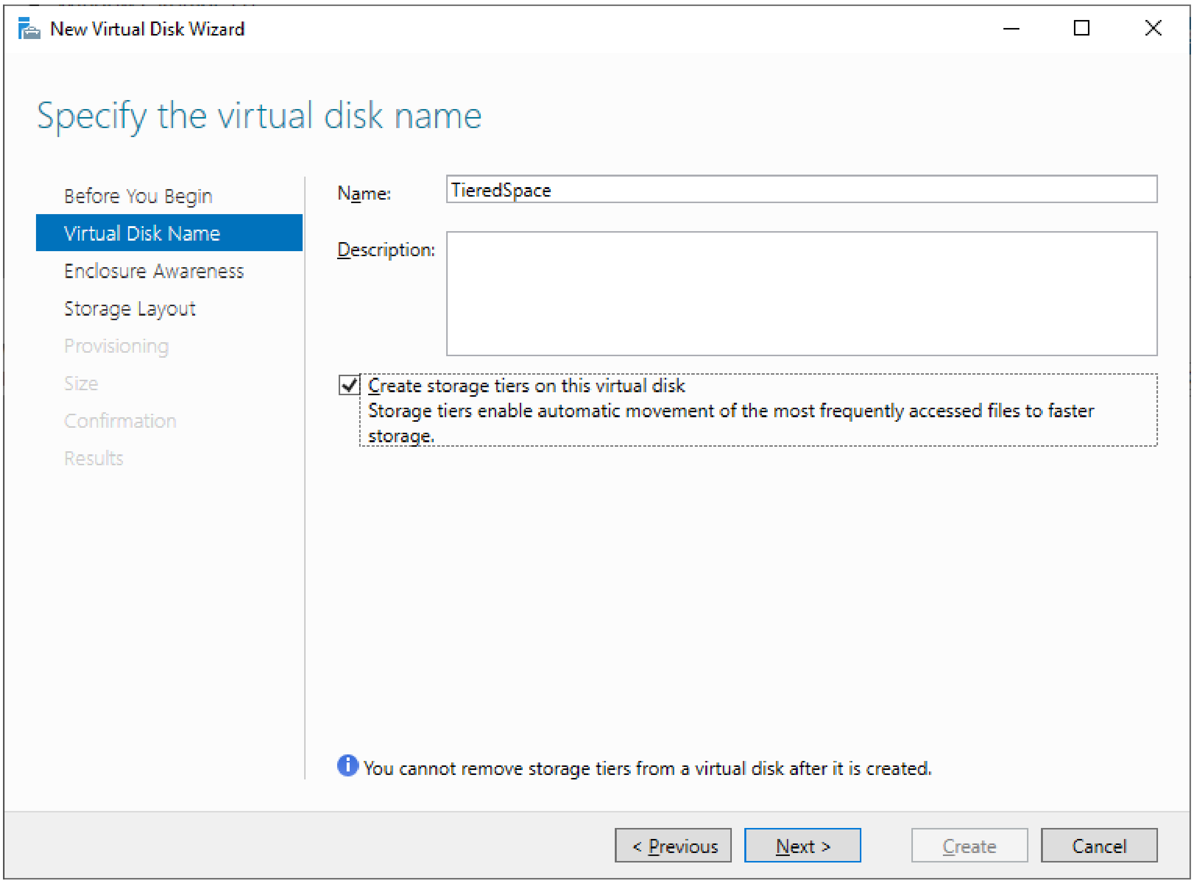
No related virtual disks exist.

To create a virtual disk, start the New Virtual Disk Wizard.

YSICAL DISKS
MainPool on sw1

Slot	Name	Status	Capacity	Bus	Usage	Chassi
6	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 6
7	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 7
4	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 4
5	ATA MK000480GWTT...		447 GB	SAS	Automatic	Slot 5
1	HP EG002400JWJNT (...		2.18 TB	SAS	Automatic	Slot 1
3	HP EG002400JWJNT (...		2.18 TB	SAS	Automatic	Slot 3
2	HP EG002400JWJNT (...		2.18 TB	SAS	Automatic	Slot 2

6. For Automated Storage Tiering, both HDD- and SSD-based disks or storage arrays should be in the storage pool to make use of Storage Tiers. In case of using Storage Tiers, Storage Layout can be only Simple and Mirror. Specify Virtual Disk Name and select Create storage tiers on this virtual disk.



New Virtual Disk Wizard

Specify the virtual disk name

Name: TieredSpace

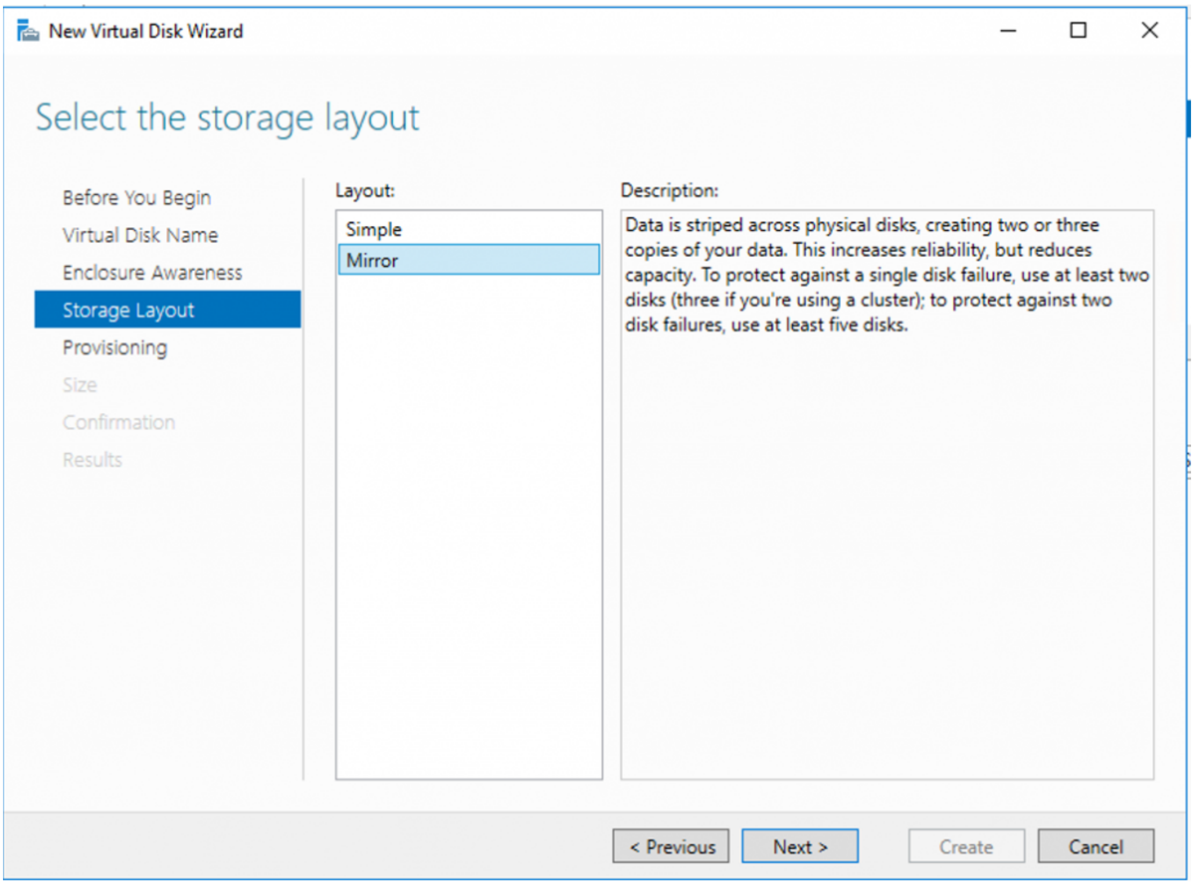
Description:

☑ Create storage tiers on this virtual disk
Storage tiers enable automatic movement of the most frequently accessed files to faster storage.

You cannot remove storage tiers from a virtual disk after it is created.

NOTE: Simple Tier has no redundancy built-in, so in case of either individual spinning disk and/or flash drive failure there is a risk of losing the data. It is recommended to configure resilient storage to be used as the underlying storage for the Tier. Please make sure that such a configuration is supported by either the software vendor (i.e., StarWind, Microsoft, VMware, etc.) or/and MSP/ISV.

7. Select the storage layout type. Under the Simple layout, the data is striped across physical disks. This would be equivalent to a RAID-0 configuration. In case of using at least two disks, the Mirror configuration can be configured. The Mirror is equivalent to RAID-1. Once done, click next.



Layout:

Simple

Mirror

Description:

Data is striped across physical disks, creating two or three copies of your data. This increases reliability, but reduces capacity. To protect against a single disk failure, use at least two disks (three if you're using a cluster); to protect against two disk failures, use at least five disks.

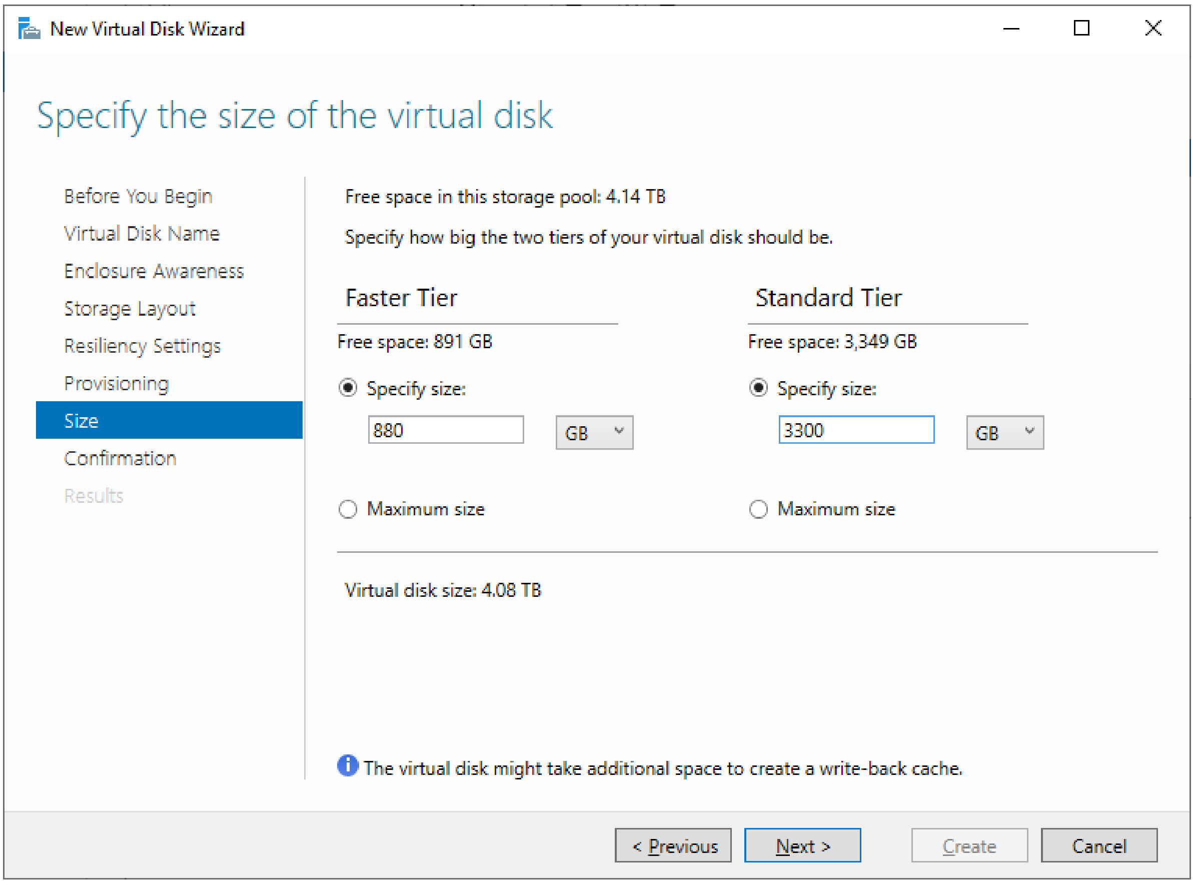
8. Specify the provisioning type.

Fixed. This provision type means that virtual disk cannot exceed the actual storage pool capacity.

Thin. This provision type means that there is a possibility to create a volume with a size exceeding the storage pool capacity and then add physical disks later.

Choose fixed disk provisioning since this type is required by Storage Tiers. Click Next.

9. Specify the size of the Virtual Disk.



New Virtual Disk Wizard

Specify the size of the virtual disk

Free space in this storage pool: 4.14 TB

Specify how big the two tiers of your virtual disk should be.

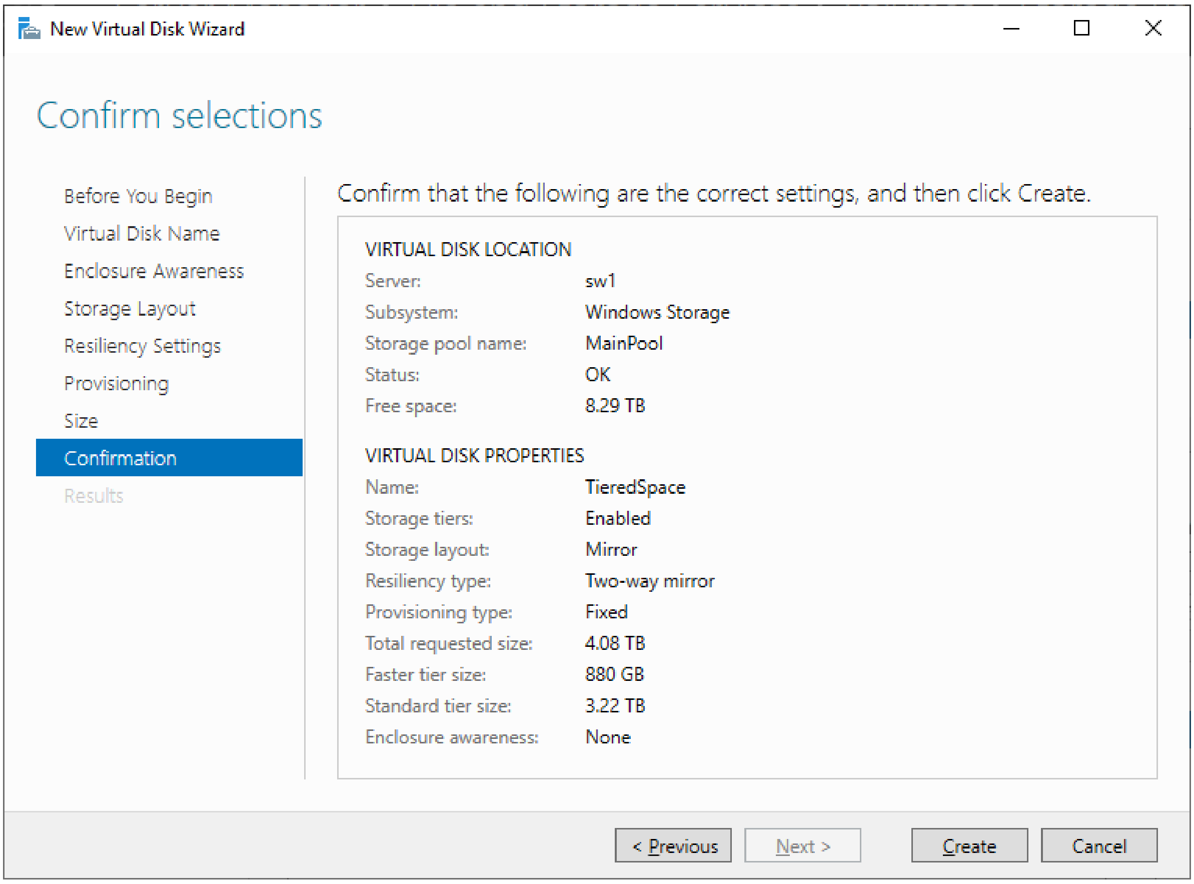
Faster Tier	Standard Tier
Free space: 891 GB	Free space: 3,349 GB
● Specify size: 880 GB	● Specify size: 3300 GB
○ Maximum size	○ Maximum size

Virtual disk size: 4.08 TB

The virtual disk might take additional space to create a write-back cache.

NOTE: At least 8 GB of free space on each Tier should be provisioned to allow Automated Storage rebuilding in case of the disk loss.

10. Confirm the settings and click Create to create Virtual Disk.



Confirm selections

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

VIRTUAL DISK LOCATION

Server:	sw1
Subsystem:	Windows Storage
Storage pool name:	MainPool
Status:	OK
Free space:	8.29 TB

VIRTUAL DISK PROPERTIES

Name:	TieredSpace
Storage tiers:	Enabled
Storage layout:	Mirror
Resiliency type:	Two-way mirror
Provisioning type:	Fixed
Total requested size:	4.08 TB
Faster tier size:	880 GB
Standard tier size:	3.22 TB
Enclosure awareness:	None

NOTE: In case of using both SSD and HDD disks or virtual LUNs, automated Storage Tier consists of the so-called “hot” and “cold” Tiers. Automated Storage Tier elaborates a data map taking into account how often the certain data is used, thus defining how hot separate data blocks are. During the process of optimization that is launched automatically every day, the hot data, i.e. data that is used on the most frequent basis, is transferred to the fast SSD tier, with the data used less frequently, the so-called cold data, being transferred to the slower HDD tier.

As the SSD tier-based data gets updated only once a day, it is possible to manually optimize it with the help of the following CMD one-liner:

```
defrag.exe /C /H /K /G
```

This command should be run on all cluster nodes, as it optimizes only those virtual disks the owner node for which is the one where the command is running.

For certain files, it can be optimal to permanently stay on the SSD tier. An example is a VHDX file that is accessed frequently and requires minimum latency and high performance. Such a result can be achieved by pinning the file to the SSD tier.

The following recommendations should be taken into account before running the command:

- the command should be run from the node owning the storage (Cluster Shared Volume) with the file stored on it.
- local path to the storage (Cluster Shared Volume) on the node should be used.

After a file is pinned, it will stay in the tier until the next optimization process triggered either automatically or manually.

To pin files to the SSD tier, run the following PowerShell command:

```
Set-FileStorageTier –FilePath <localFilePath> -
DesiredStorageTierFriendlyName<ssdTierName>
```

To unpin files from the SSD tier, run the following PowerShell command:

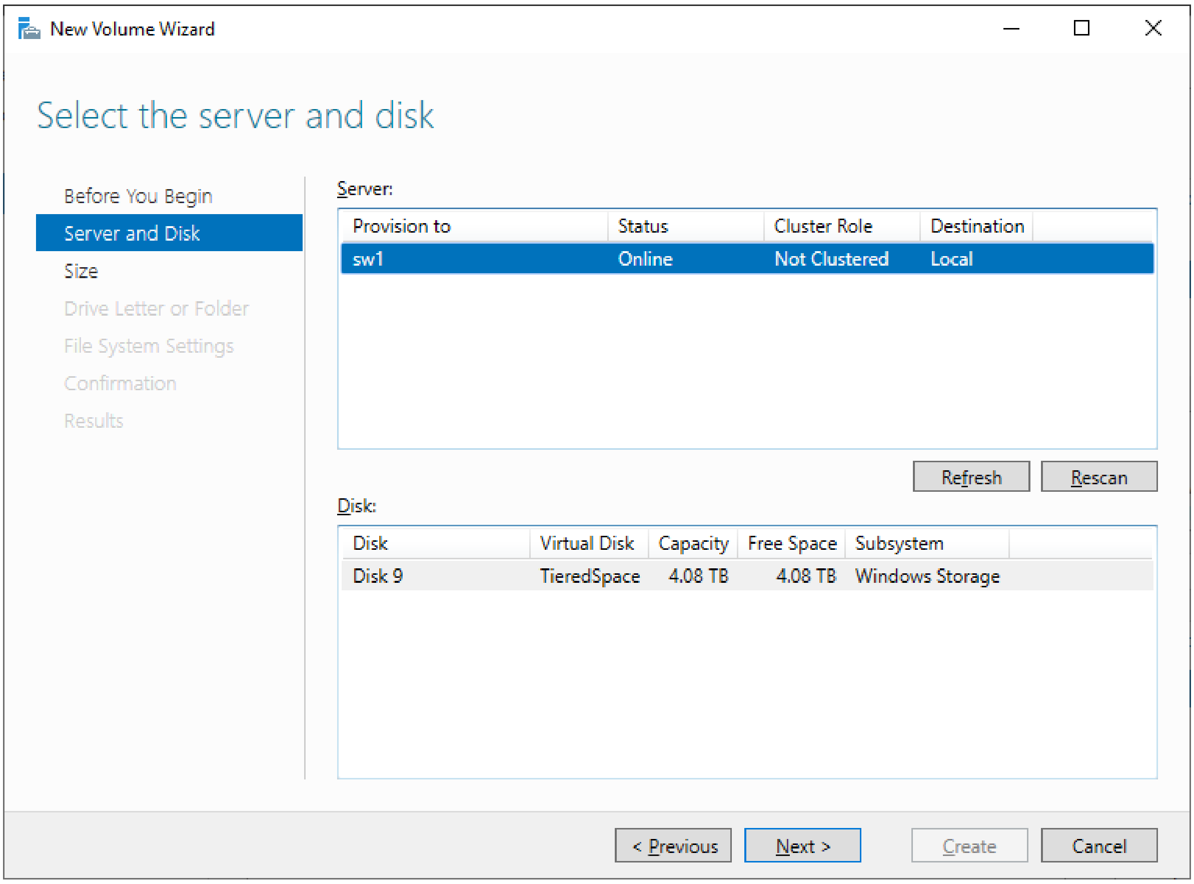
```
Set-FileStorageTier –FilePath <localFilePath>
```

The below PowerShell command lists all files that are currently pinned:

```
Get-FileStorageTier –VolumePath <csvVolumePath>
```

11. Create a New Volume using New Volume Wizard:

12. Select the server and disk and click Next.



Select the server and disk

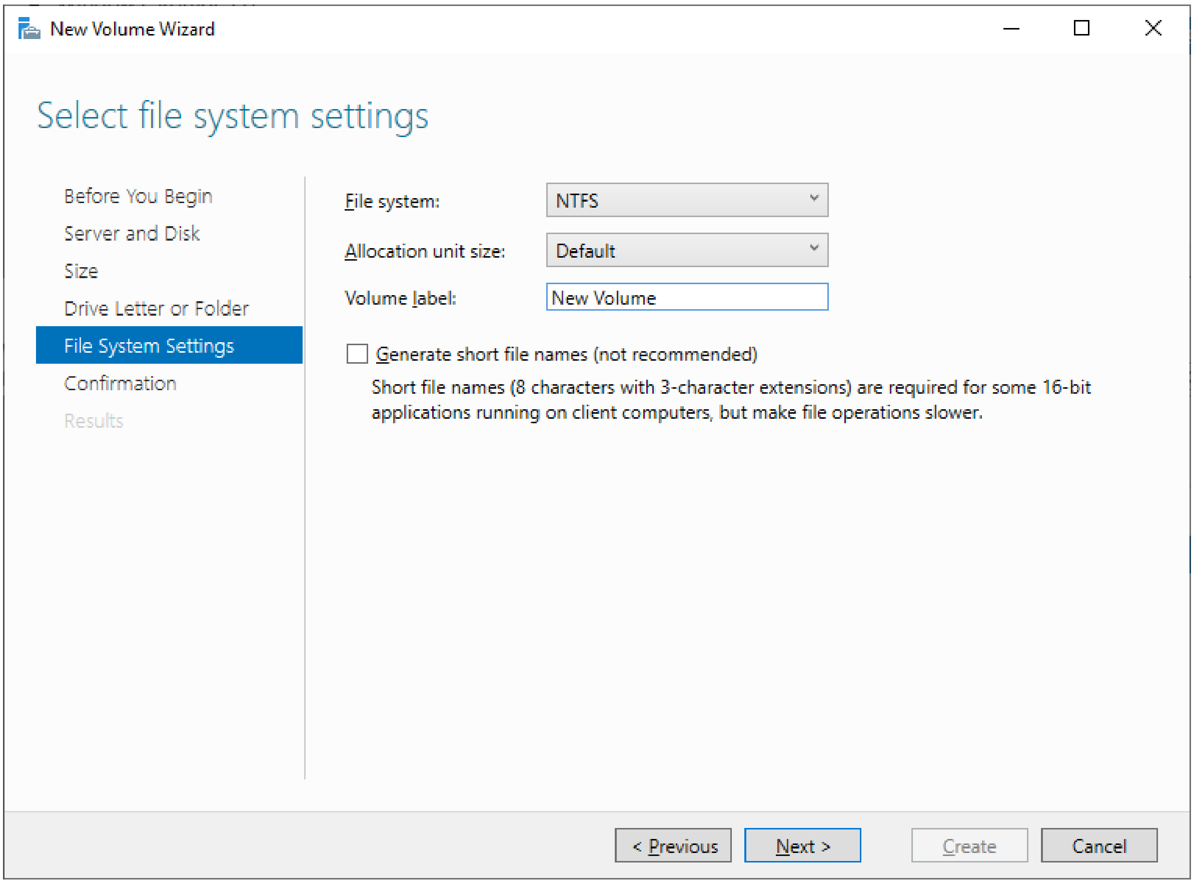
Server:

Provision to	Status	Cluster Role	Destination
sw1	Online	Not Clustered	Local

Disk:

Disk	Virtual Disk	Capacity	Free Space	Subsystem
Disk 9	TieredSpace	4.08 TB	4.08 TB	Windows Storage

13. Select the file system settings and click Next to proceed.



Select file system settings

File system: NTFS

Allocation unit size: Default

Volume label: New Volume

☐ Generate short file names (not recommended)

Short file names (8 characters with 3-character extensions) are required for some 16-bit applications running on client computers, but make file operations slower.

NOTE: The steps described above can be performed with help of PowerShell commands. Also, with help of PowerShell, additional parameters can be configured for better performance:

Set 64K size of interleave: *–Interleave 65536*.

Set *LogicalSectorSizeDefault 4096* instead of default *512*.

The cache size can be changed with the help of *–WriteCacheSize [ ]GB* parameter. It is possible to set cache size only via PowerShell commands for creating Automated Storage Tier.

Set SSD tier in two-way mirror: *ResiliencySettingName Mirror -NumberOfDataCopies 2*

The number of threads can be set with *-NumberOfColumns parameter*. The recommended number is the number of SSDs divided by 2.

The example of the PowerShell commands for Storage Pool and Virtual Disk with Tiered Storage creation is provided below:

```
Get-StorageSubsystem – check the storage subsystem name before
running the commands below.

Get-PhysicalDisk

$disks = Get-PhysicalDisk |? {$_.CanPool -eq $true}

New-StoragePool -StorageSubSystemFriendlyName "[ ]*" -
FriendlyName [ ] -PhysicalDisks $disks -
LogicalSectorSizeDefault 4096

Get-PhysicalDisk | where Size -lt [ ]GB | Set-PhysicalDisk -
MediaType SSD

Get-PhysicalDisk | where Size -gt [ ]GB | Set-PhysicalDisk -
MediaType HDD

Get-StoragePool -FriendlyName [ ]

New-StorageTier -MediaType SSD -StoragePoolFriendlyName [ ] -
FriendlyName SSDTier -ResiliencySettingName [Simple, Mirror or
Parity] -NumberOfDataCopies 2 -NumberOfColumns [ ] -Interleave
65536

New-StorageTier -MediaType HDD -StoragePoolFriendlyName [ ] -
FriendlyName HDDTier -ResiliencySettingName [Simple, Mirror or
Parity] -Interleave 65536

$SSD = Get-StorageTier -FriendlyName SSDTier

$HDD = Get-StorageTier -FriendlyName HDDTier

New-VirtualDisk -FriendlyName "[ ]" -StoragePoolFriendlyName [
] –StorageTiers $SSD, $HDD -StorageTierSizes [ ]GB, [ ]Gb -
ResiliencySettingName [Simple, Mirror or Parity] -
ProvisioningType fixed -WriteCacheSize [ ]GB
```

IMPORTANT NOTE: The virtual storage configuration created with PowerShell script must be reviewed by the software vendor (i.e., StarWind, Microsoft, VMware, etc.) for compliance and is fully supported and validated by either software vendor or MSP / ISV to satisfy and match the existing and future workload requirements and expectations of the specific production environment.

The operations specified in this section should be performed on each server.

Installing File Server Roles

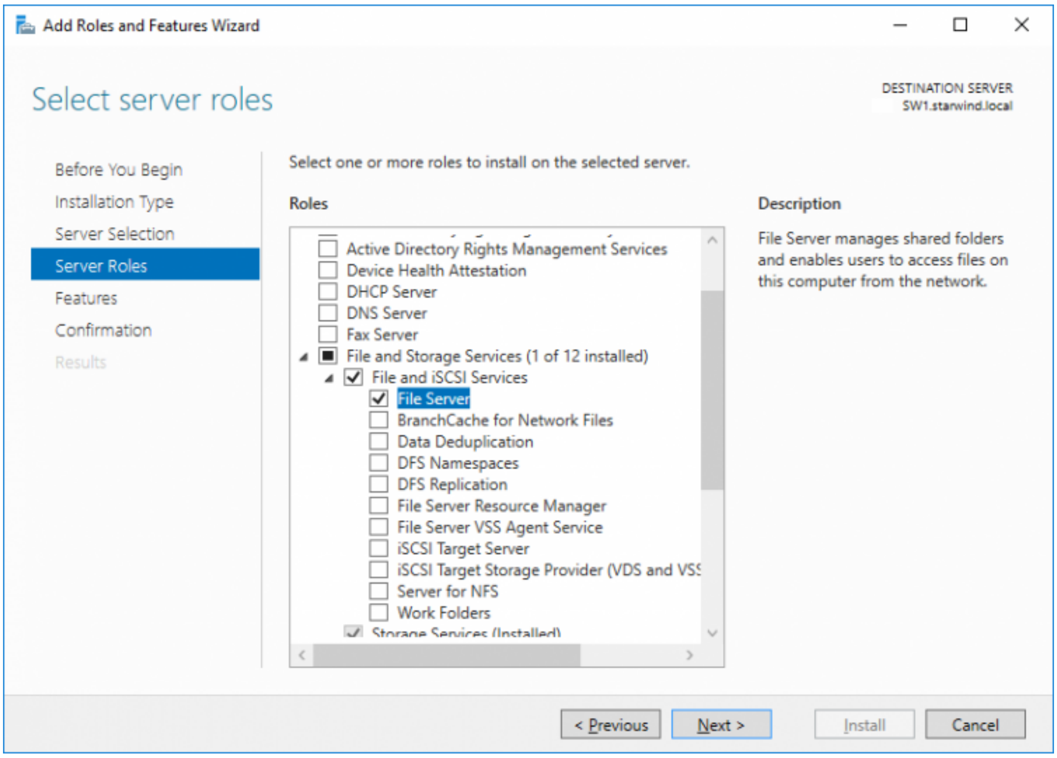
Please follow the steps below if file shares configuration is required

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 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.

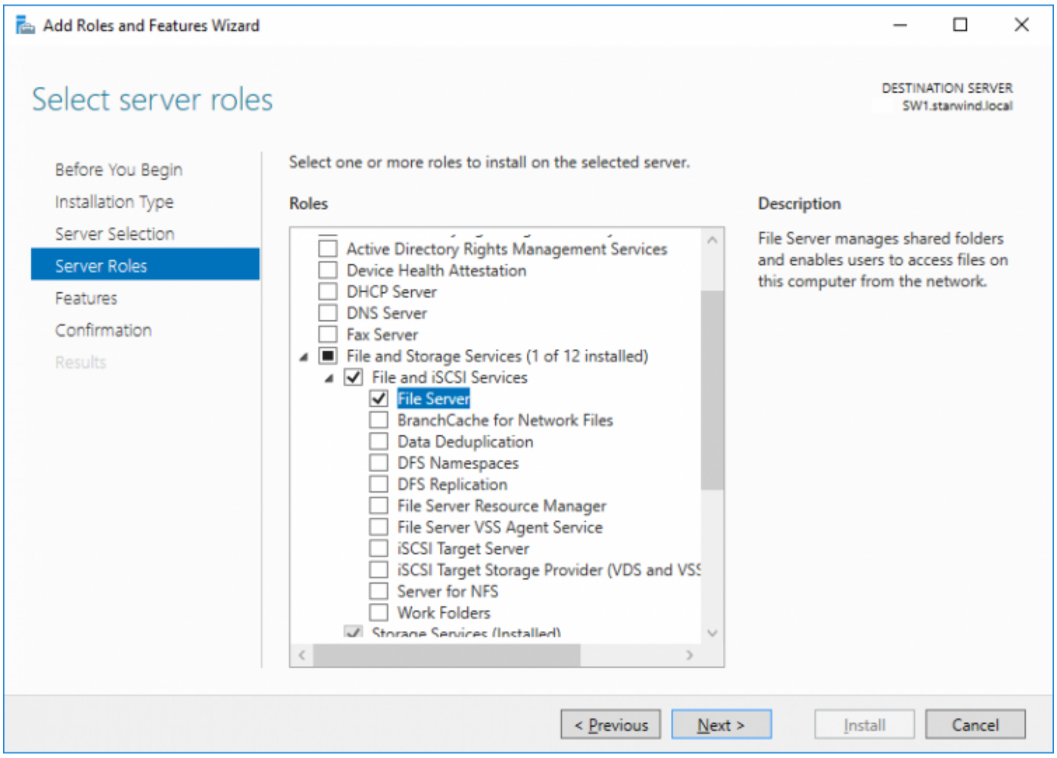
4. Restart the server after installation is completed and perform steps above on the each server.

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.

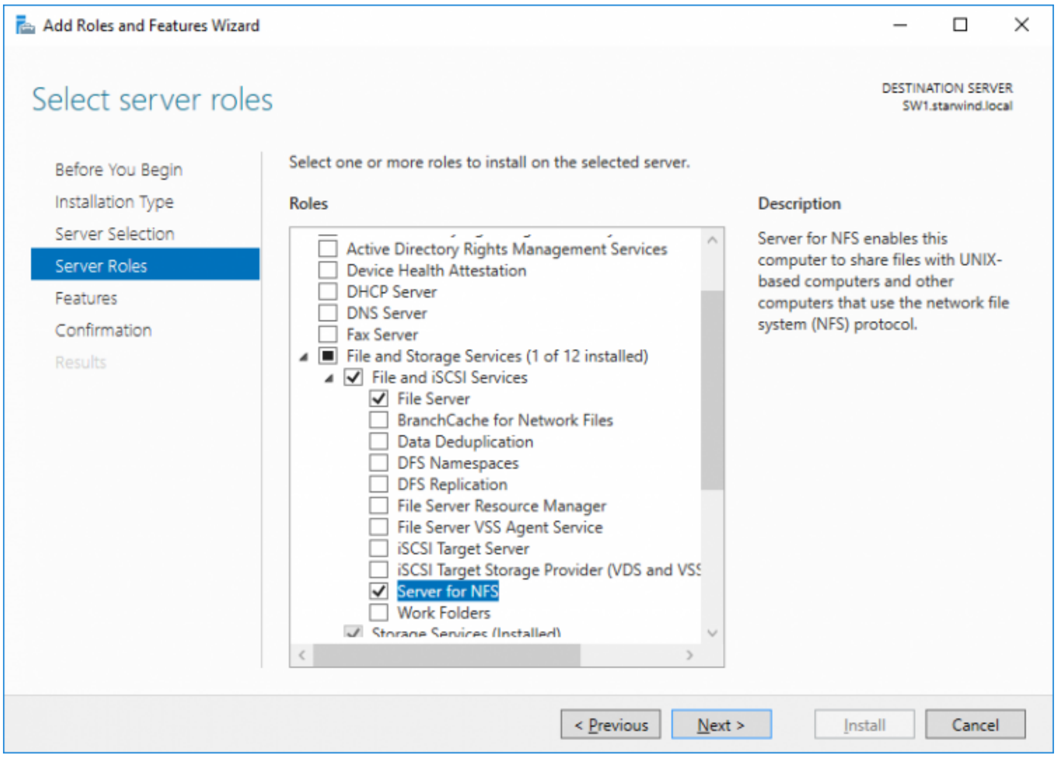
4. Restart the server after installation is completed and perform steps above on each server.

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:



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

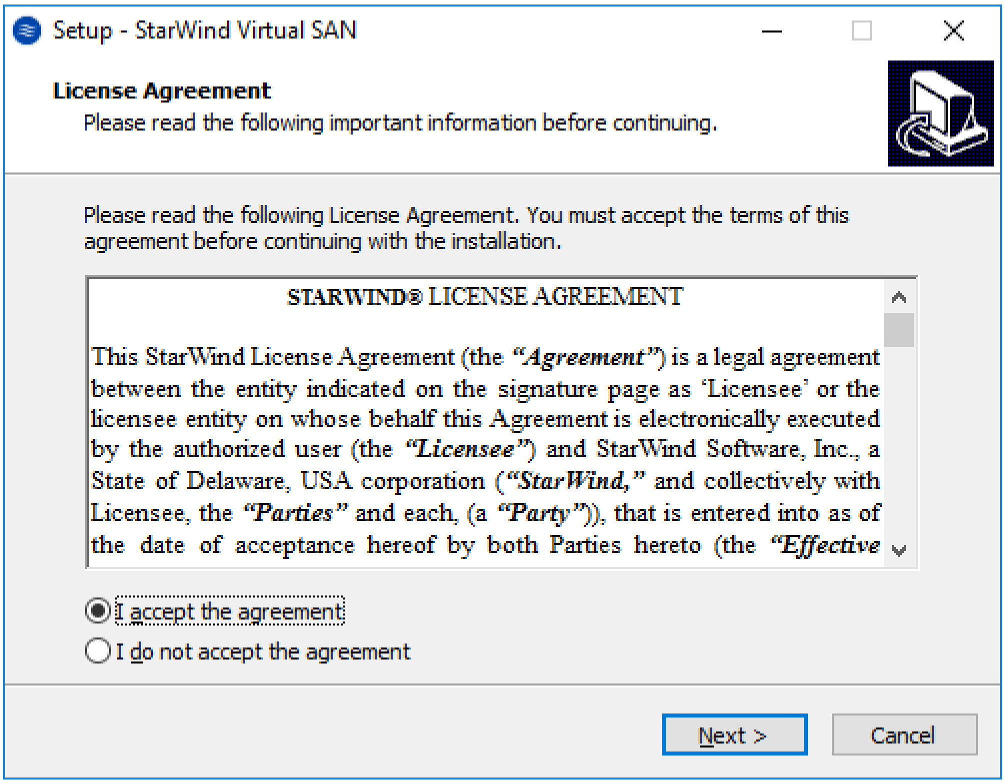
Server for NFS enables this computer to share files with UNIX-based computers and other computers that use the network file system (NFS) protocol.

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

Installing Starwind Vsan For Hyper-V

1. Download the StarWind setup executable file from the StarWind website: https://www.starwind.com/registration-starwind-virtual-san

2. Launch the downloaded setup file on the server to install StarWind Virtual SAN or one of its components. The Setup wizard will appear. Read and accept the License Agreement.



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

STARWIND® LICENSE AGREEMENT

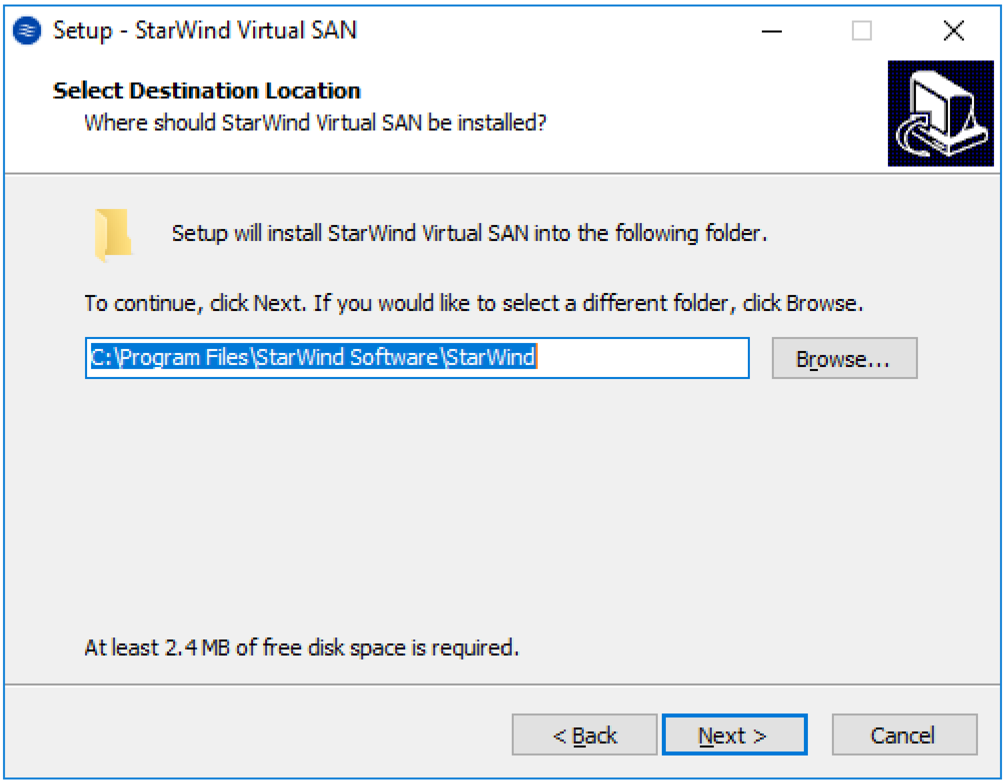
This StarWind License Agreement (the *"Agreement"*) is a legal agreement between the entity indicated on the signature page as 'Licensee' or the licensee entity on whose behalf this Agreement is electronically executed by the authorized user (the *"Licensee"*) and StarWind Software, Inc., a State of 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*

● I accept the agreement

○ I do not accept the agreement

3. Carefully read the information about the new features and improvements. Red text indicates warnings for users that are updating the existing software installations.

4. Select Browse to modify the installation path if necessary. Click on Next to continue.



Select Destination Location

Where should StarWind Virtual SAN be installed?

Setup will install StarWind Virtual SAN into the following folder.

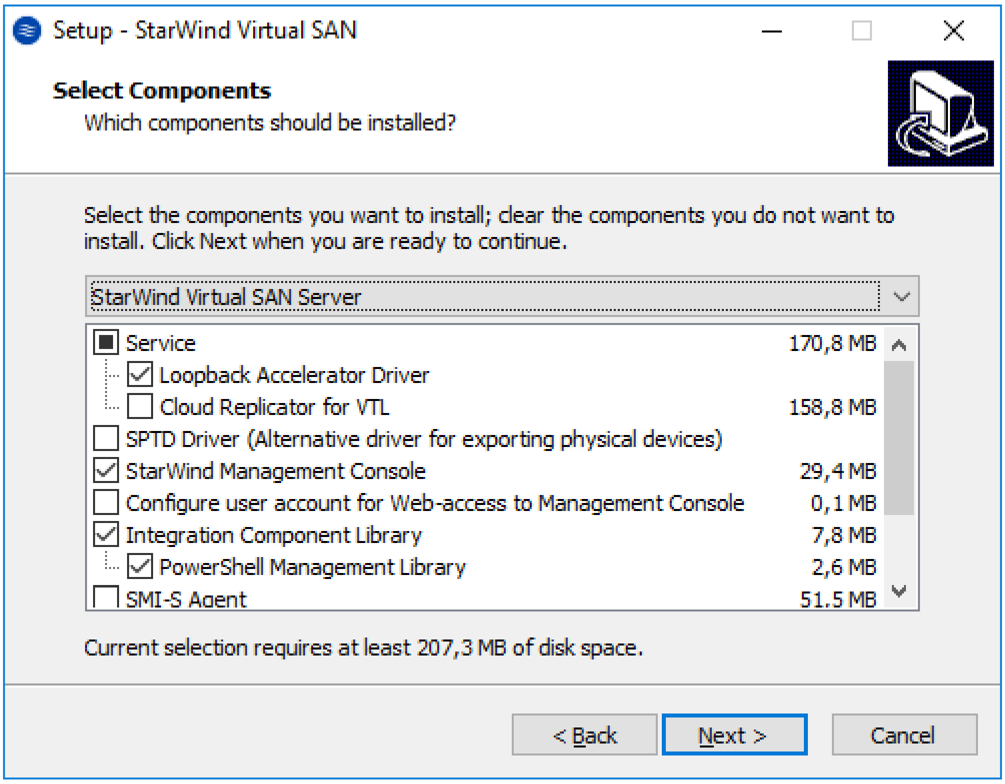
To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\StarWind Software\StarWind

At least 2.4 MB of free disk space is required.

5. Select the following components for the minimum setup:

- StarWind Virtual SAN Service. The StarWind Virtual SAN service is the “core” of the software. It can create iSCSI targets as well as share virtual and physical devices. The service can be managed from StarWind Management Console on any Windows computer that is on the same network. Alternatively, the service can be managed from StarWind Web Console deployed separately.
- StarWind Management Console. Management Console is the Graphic User Interface (GUI) part of the software that controls and monitors all storage-related operations (e.g., allows users to create targets and devices on StarWind Virtual SAN servers connected to the network).
  NOTE: To manage StarWind Virtual SAN installed on a Windows Server Core edition with no GUI, StarWind Management Console should be installed on a different computer running the GUI-enabled Windows edition.



Setup - StarWind Virtual SAN

Select Components

Which components should be installed?

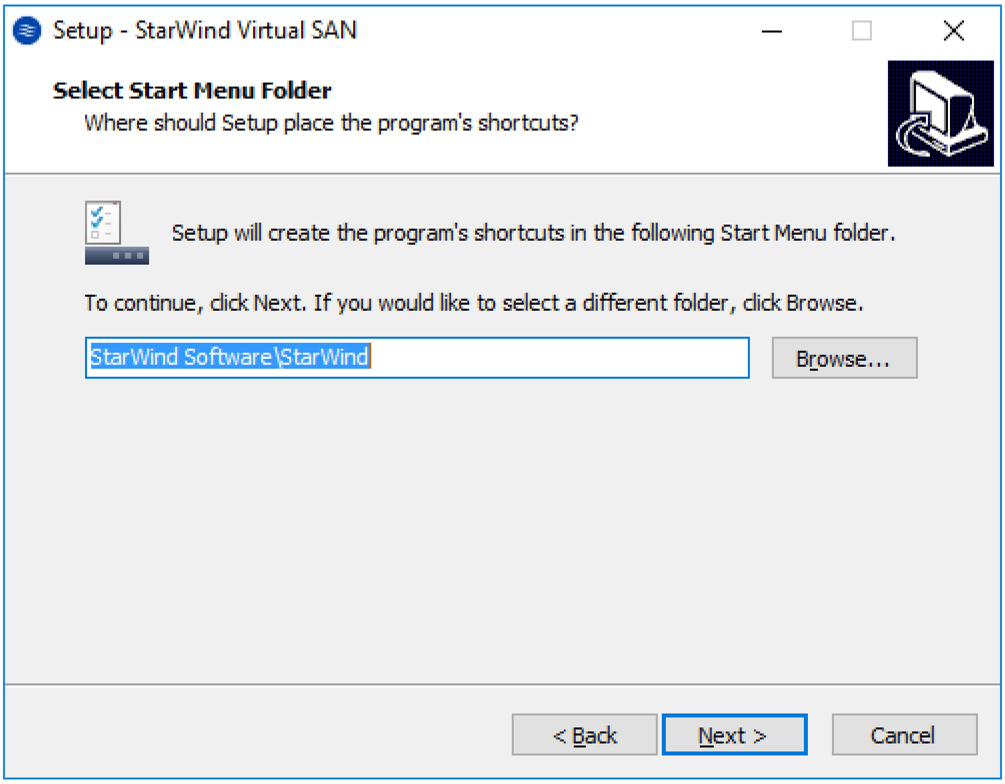
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

StarWind Virtual SAN Server

■ Service	170,8 MB
☑ Loopback Accelerator Driver	
□ Cloud Replicator for VTL	158,8 MB
□ SPTD Driver (Alternative driver for exporting physical devices)	
☑ StarWind Management Console	29,4 MB
□ Configure user account for Web-access to Management Console	0,1 MB
☑ Integration Component Library	7,8 MB
☑ PowerShell Management Library	2,6 MB
□ SMI-S Agent	51,5 MB

Current selection requires at least 207,3 MB of disk space.

6. Specify Start Menu Folder.



Setup - StarWind Virtual SAN

Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

StarWind Software\StarWind

7. Enable the checkbox if a desktop icon needs to be created. Click on Next to continue.

8. When the license key prompt appears, choose the appropriate option:

- request time-limited fully functional evaluation key.
- request FREE version key.
- relect the previously purchased commercial license key.

9. Click on the Browse button to locate the license file.

10. Review the licensing information.

11. Verify the installation settings. Click on Back to make any changes or Install to proceed with installation.

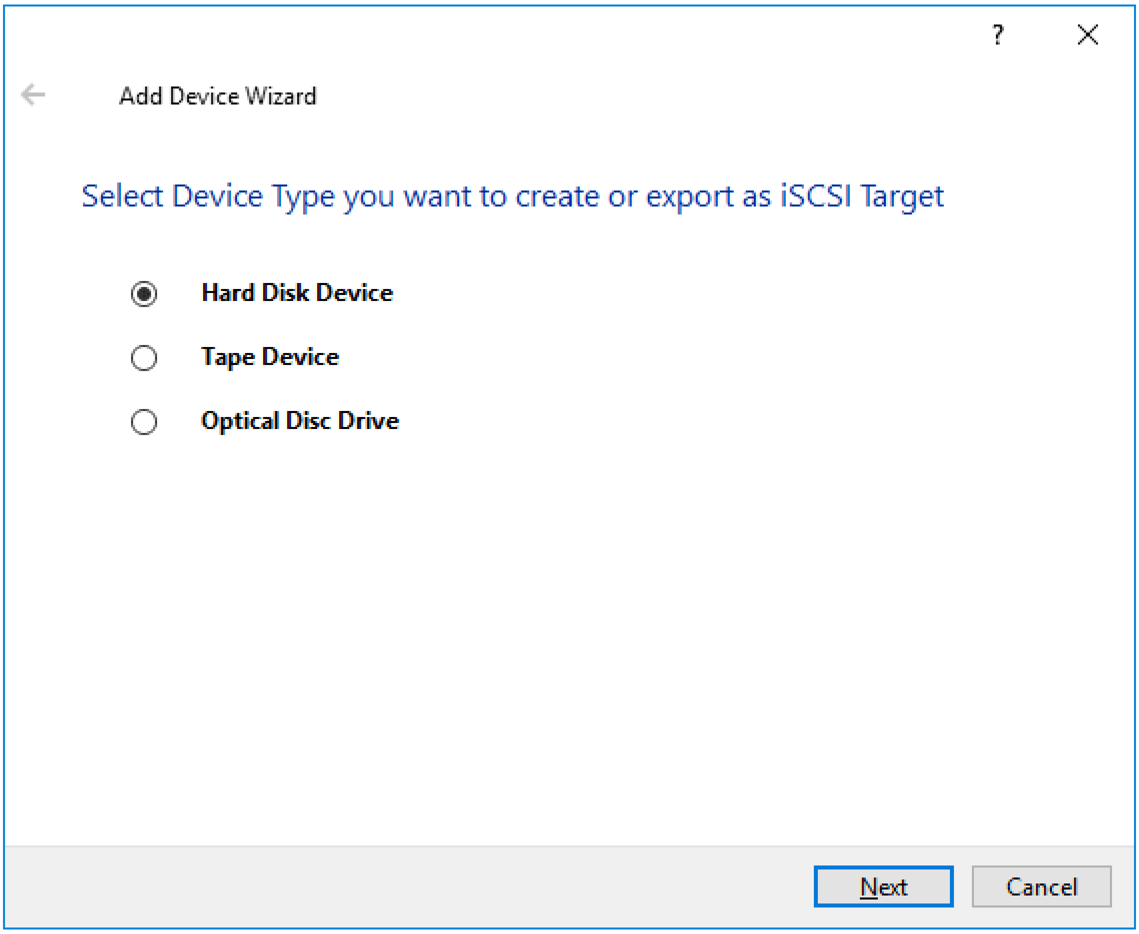
12. Enable the appropriate checkbox to launch StarWind Management Console right after the setup wizard is closed and click on Finish.

13. Repeat the installation steps on the partner node.

Creating Starwind Devices

1. In the StarWind Management Console click to Add Device (advanced) button and open Add Device (advanced) Wizard.

2. Select Hard Disk Device as the type of device to be created.



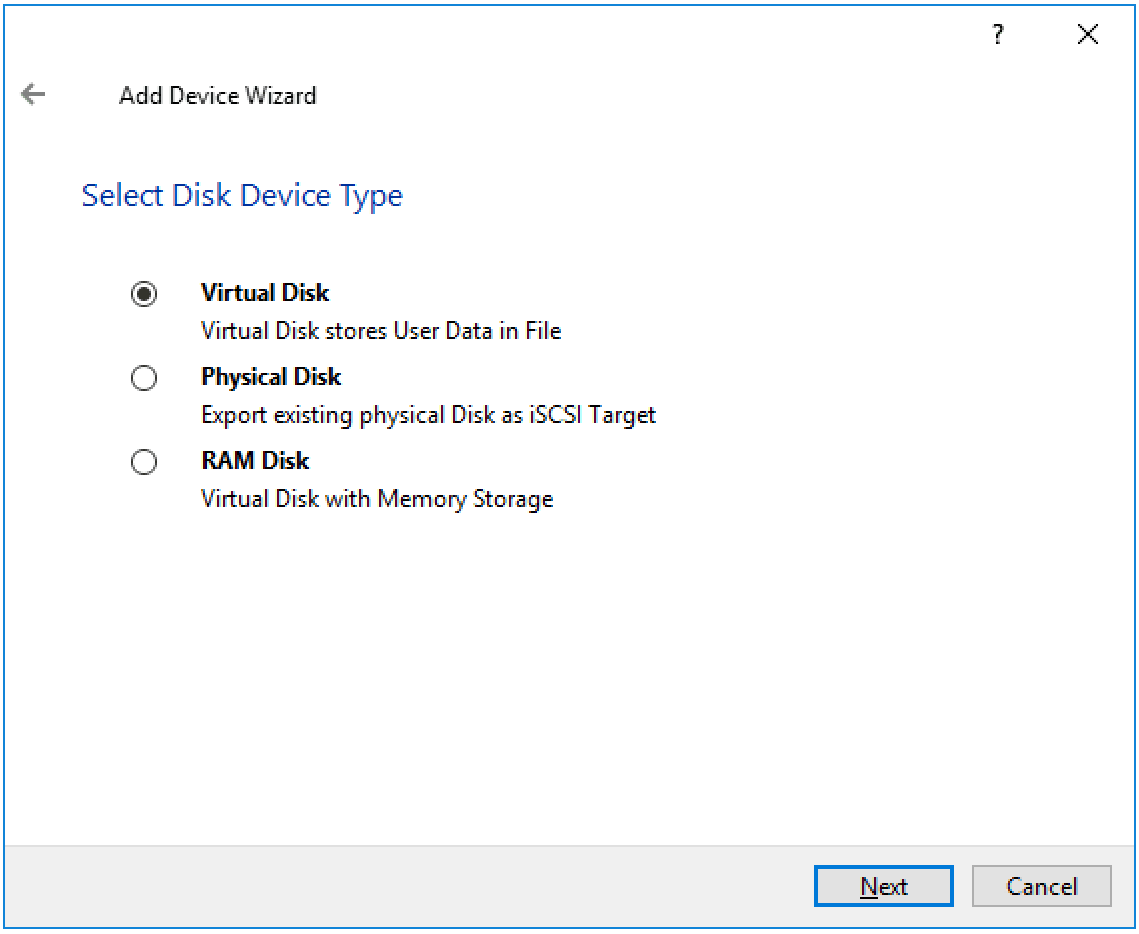
Select Device Type you want to create or export as iSCSI Target

● Hard Disk Device

○ Tape Device

○ Optical Disc Drive

3. Select Virtual Disk.



Add Device Wizard

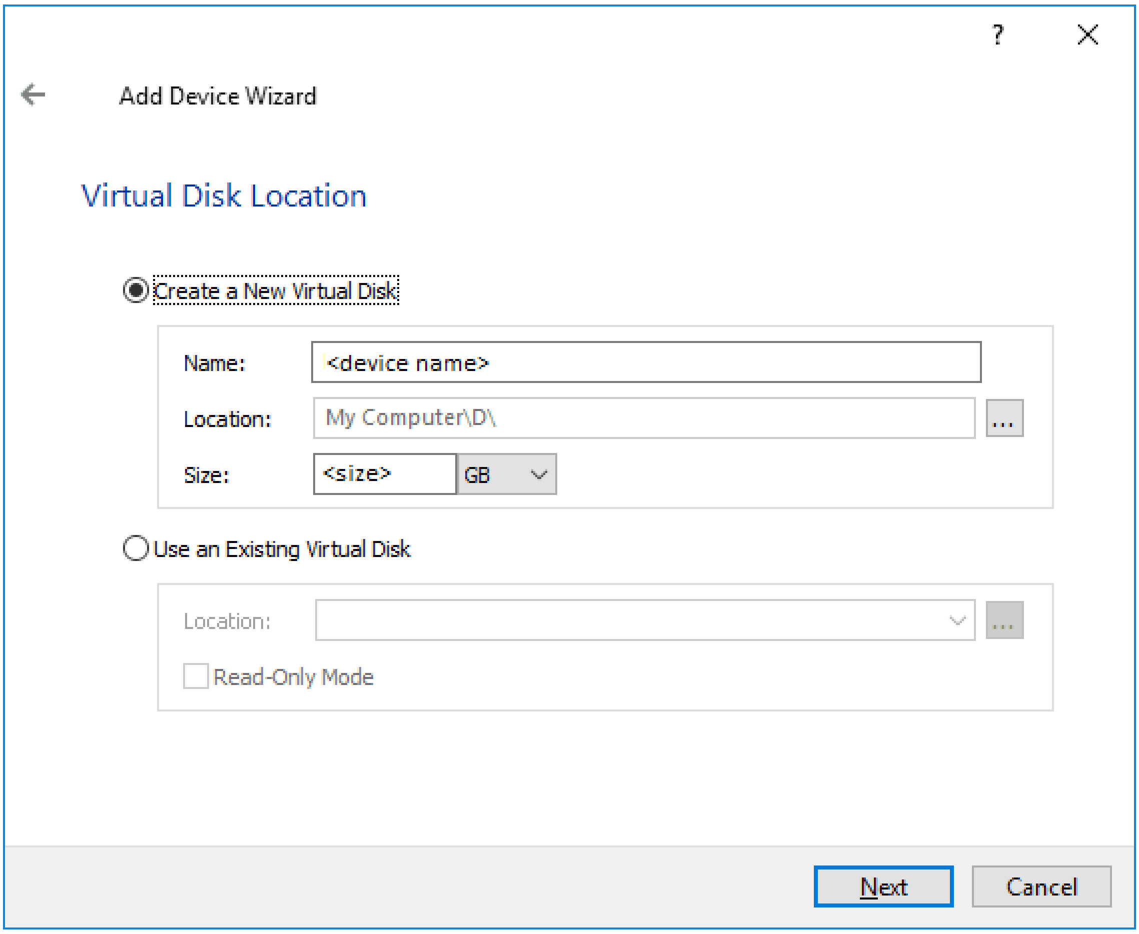
Select Disk Device Type

● **Virtual Disk**
Virtual Disk stores User Data in File

○ **Physical Disk**
Export existing physical Disk as iSCSI Target

○ **RAM Disk**
Virtual Disk with Memory Storage

4. Specify a virtual disk Name, Location, and Size.



● Create a New Virtual Disk

Name: <device name>

Location: My Computer\D\

Size: <size> GB

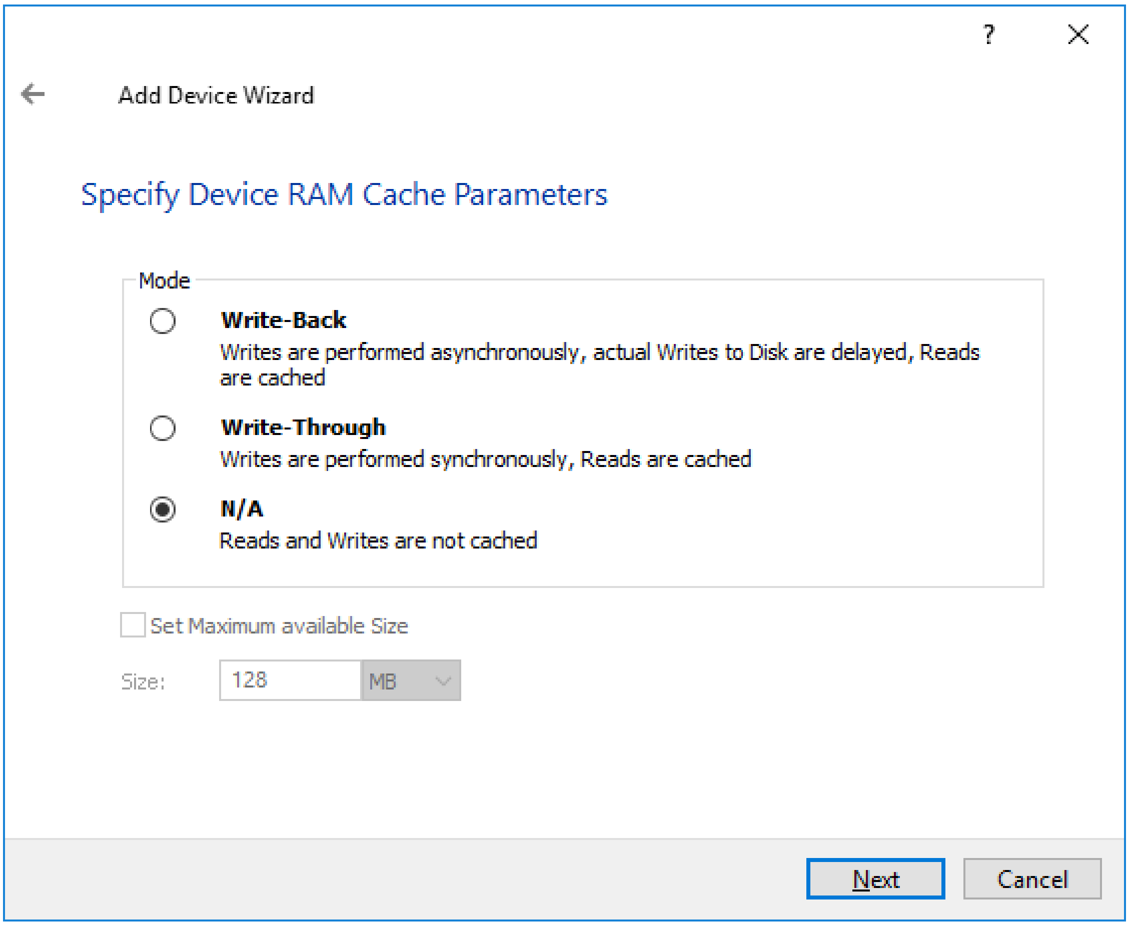
○ Use an Existing Virtual Disk

Location:

□ Read-Only Mode

5. Select the Thick provisioned disk type and block size.
NOTE: Use 4096 sector size for targets, connected on Windows-based systems and 512 bytes sector size for targets, connected on Linux-based systems (ESXi/Xen/KVM).

6. Define a caching policy and specify a cache size (in MB). Also, the maximum available cache size can be specified by selecting the appropriate checkbox. Optionally, define the L2 caching policy and cache size.



Add Device Wizard

Specify Device RAM Cache Parameters

Mode

○ **Write-Back**
Writes are performed asynchronously, actual Writes to Disk are delayed, Reads are cached

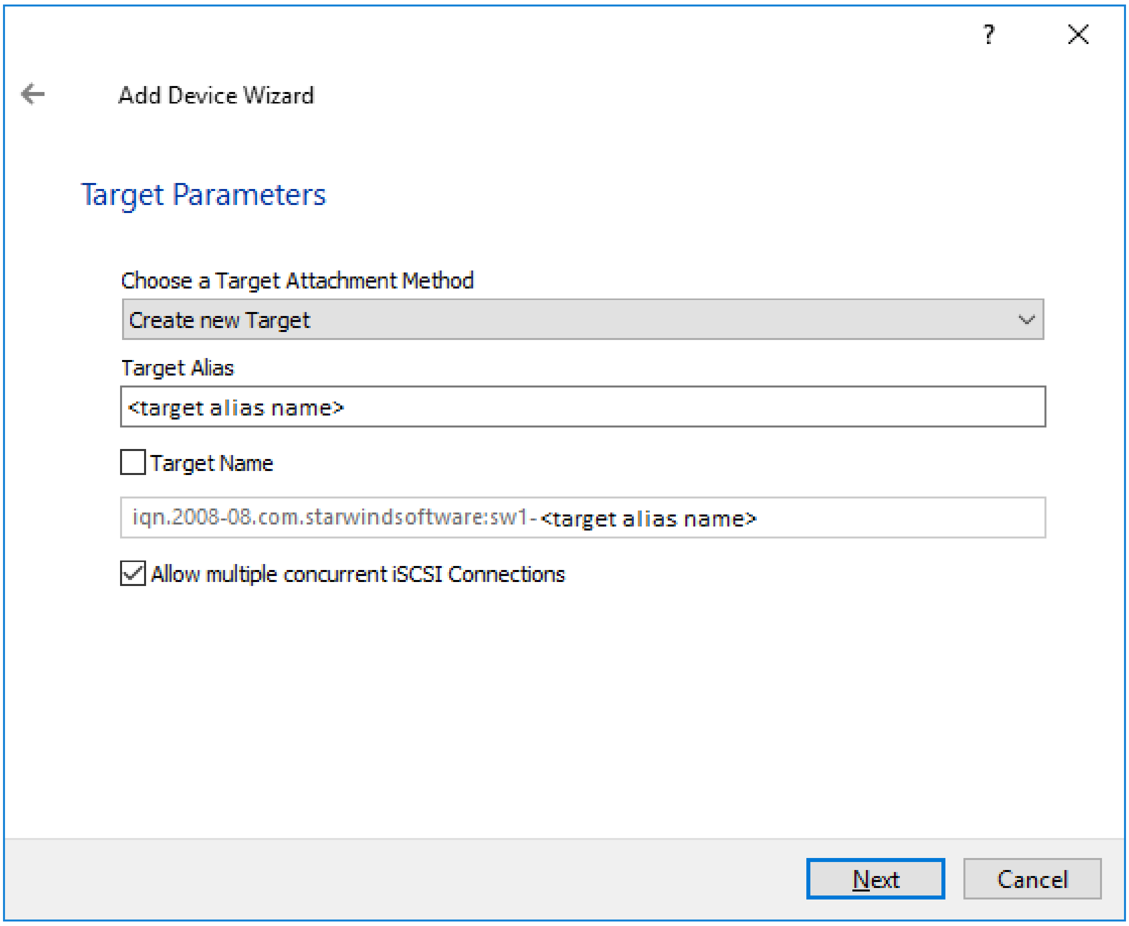
○ **Write-Through**
Writes are performed synchronously, Reads are cached

● **N/A**
Reads and Writes are not cached

□ Set Maximum available Size

Size: 128 MB

7. Specify Target Parameters. Select the Target Name checkbox to enter a custom target name. Otherwise, the name is generated automatically in accordance with the specified target alias.



Add Device Wizard

Target Parameters

Choose a Target Attachment Method

Create new Target

Target Alias

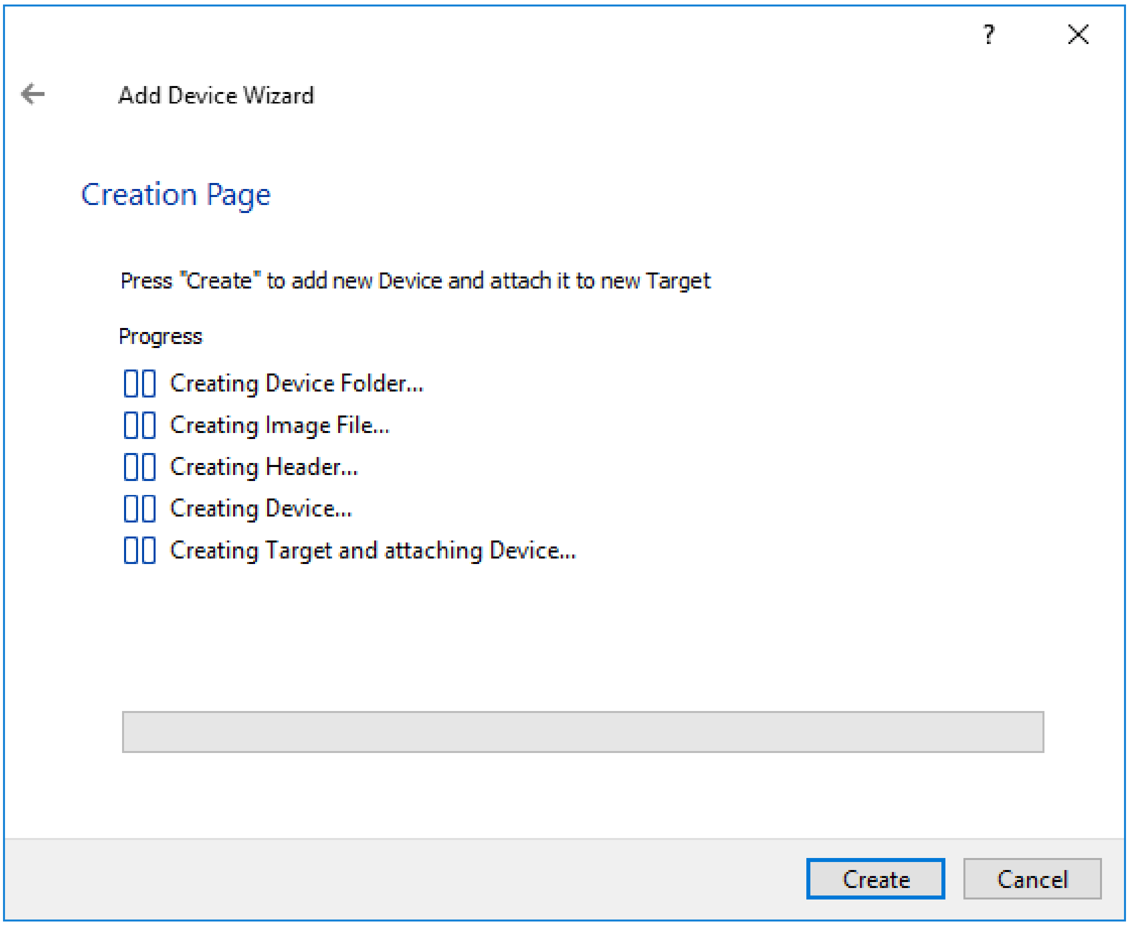
<target alias name>

□ Target Name

iqn.2008-08.com.starwindsoftware:sw1-<target alias name>

☑ Allow multiple concurrent iSCSI Connections

8. Click Create to add a new device and attach it to the target.



Add Device Wizard

Creation Page

Press "Create" to add new Device and attach it to new Target

Progress

Creating Device Folder...
Creating Image File...
Creating Header...
Creating Device...
Creating Target and attaching Device...

9. Click Close to finish the device creation.

10. The successfully added devices appear in the StarWind Management Console.

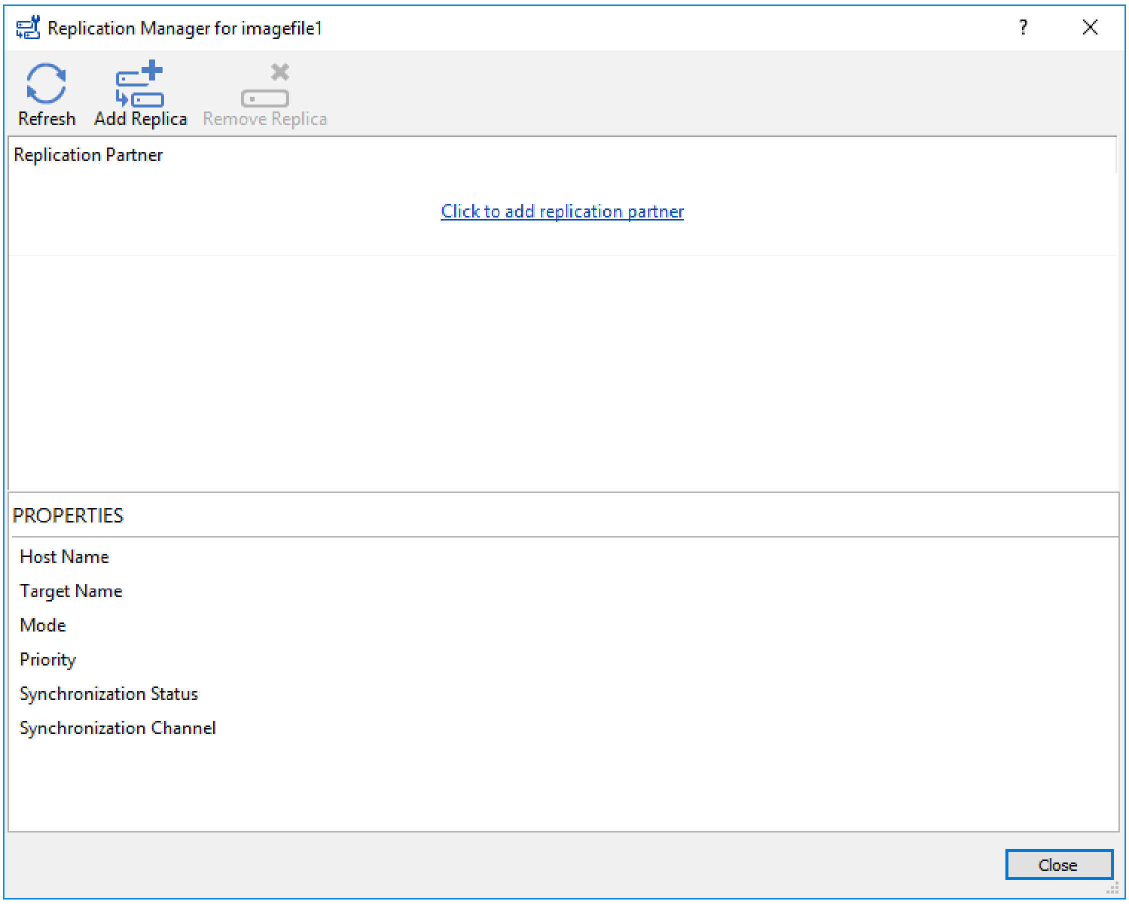
Select The Required Replication Mode

The replication can be configured using Synchronous “Two-Way” Replication mode: Synchronous or active-active replication ensures real-time synchronization and load balancing of data between two or three cluster nodes. Such a configuration tolerates the failure of two out of three storage nodes and enables the creation of an effective business continuity plan. With synchronous mirroring, each write operation requires control confirmation from both storage nodes. It guarantees the reliability of data transfers but is demanding in bandwidth since mirroring will not work on high-latency networks.

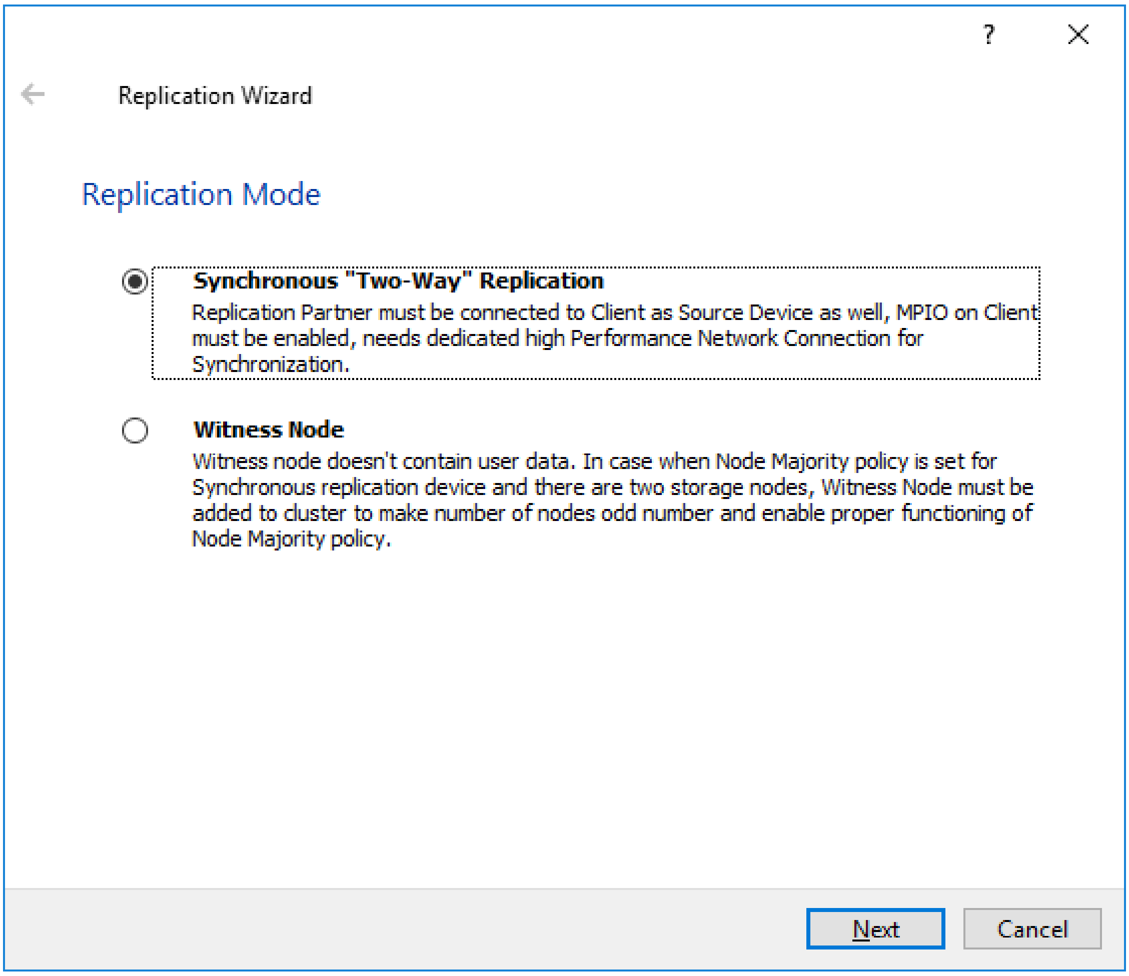
Synchronous “Two-Way” Replication

1. Right-click the recently created device and select Replication Manager from the shortcut menu.

2. Select the Add Replica button in the top menu.



3. Select Synchronous “Two-Way” replication as a replication mode.



Replication Mode

● **Synchronous "Two-Way" Replication**
Replication Partner must be connected to Client as Source Device as well, MPIO on Client must be enabled, needs dedicated high Performance Network Connection for Synchronization.

○ **Witness Node**
Witness node doesn't contain user data. In case when Node Majority policy is set for Synchronous replication device and there are two storage nodes, Witness Node must be added to cluster to make number of nodes odd number and enable proper functioning of Node Majority policy.

4. Specify a partner Host name or IP address and Port Number.

Selecting The Failover Strategy

StarWind provides 2 options for configuring a failover strategy:

Heartbeat

The Heartbeat failover strategy allows avoiding the “split-brain” scenario when the HA cluster nodes are unable to synchronize but continue to accept write commands from the initiators independently. It can occur when all synchronization and heartbeat channels disconnect simultaneously, and the partner nodes do not respond to the node’s requests. As a result, StarWind service assumes the partner nodes to be offline and continues operations on a single-node mode using data written to it.
If at least one heartbeat link is online, StarWind services can communicate with each other via this link. The device with the lowest priority will be marked as not synchronized and get subsequently blocked for the further read and write operations until the synchronization channel resumption. At the same time, the partner device on the

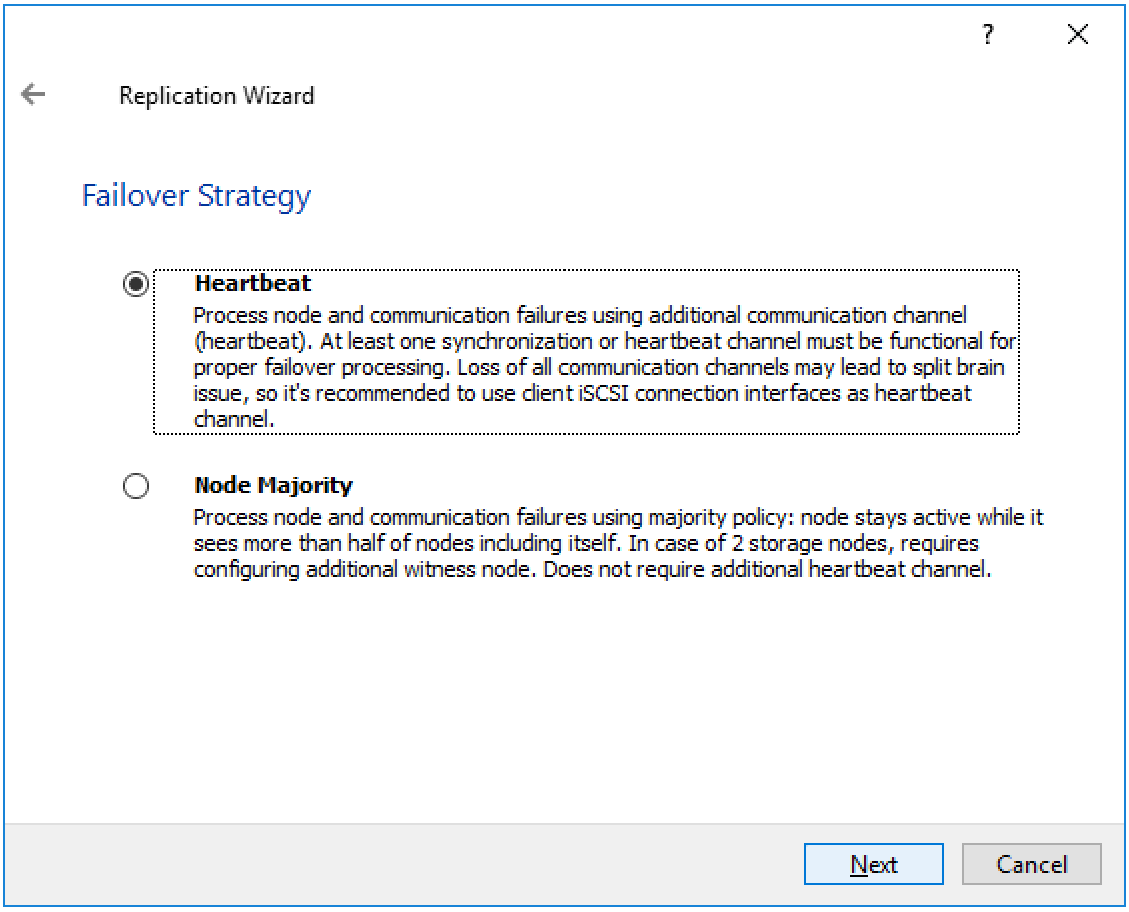
synchronized node flushes data from the cache to the disk to preserve data integrity in case the node goes down unexpectedly. It is recommended to assign more independent heartbeat channels during the replica creation to improve system stability and avoid the “split-brain” issue.
With the heartbeat failover strategy, the storage cluster will continue working with only one StarWind node available.

Node Majority

The Node Majority failover strategy ensures the synchronization connection without any additional heartbeat links. The failure-handling process occurs when the node has detected the absence of the connection with the partner.
The main requirement for keeping the node operational is an active connection with more than half of the HA device’s nodes. Calculation of the available partners is based on their “votes”.
In case of a two-node HA storage, all nodes will be disconnected if there is a problem on the node itself, or in communication between them. Therefore, the Node Majority failover strategy requires the addition of the third Witness node or file share (SMB) which participates in the nodes count for the majority, but neither contains data on it nor is involved in processing clients’ requests. In case an HA device is replicated between 3 nodes, no Witness node is required.
With Node Majority failover strategy, failure of only one node can be tolerated. If two nodes fail, the third node will also become unavailable to clients’ requests.
Please select the required option:

Heartbeat

1. Select Failover Strategy.



Failover Strategy

● **Heartbeat**
Process node and communication failures using additional communication channel (heartbeat). At least one synchronization or heartbeat channel must be functional for proper failover processing. Loss of all communication channels may lead to split brain issue, so it's recommended to use client iSCSI connection interfaces as heartbeat channel.

○ **Node Majority**
Process node and communication failures using majority policy: node stays active while it sees more than half of nodes including itself. In case of 2 storage nodes, requires configuring additional witness node. Does not require additional heartbeat channel.

2. Select Create new Partner Device and click Next.

3. Select a partner device Location and click Next.

4. Select Synchronization Journal Strategy and click Next.
NOTE: There are several options – RAM-based journal (default) and Disk-based journal with failure and continuous strategy, that allow to avoid full synchronization cases.

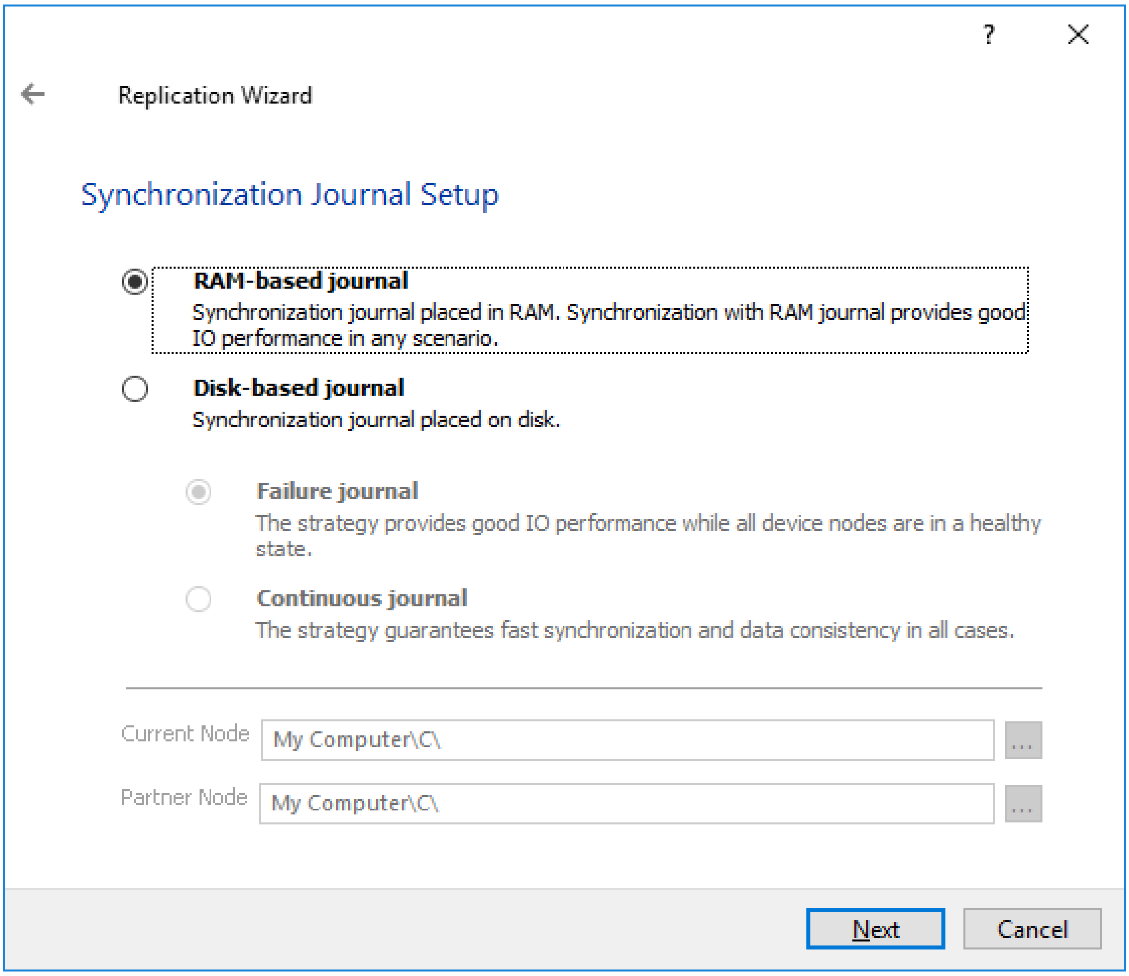
RAM-based (default) synchronization journal is placed in RAM. Synchronization with RAM journal provides good I/O performance in any scenario. Full synchronization could occur in the cases described in this KB: https://knowledgebase.starwindsoftware.com/explanation/reasons-why-full-synchronization-may-start/

Disk-based journal placed on a separate disk from StarWind devices. It allows to avoid full synchronization for the devices where it’s configured even when StarWind service is being stopped on all nodes.
Disk-based synchronization journal should be placed on a separate, preferably faster disk from StarWind devices. SSDs and NVMe disks are recommended as the device performance is defined by the disk speed, where the journal is located. For example, it

can be placed on the OS boot volume.
It is required to allocate 2 MB of disk space for the synchronization journal per 1 TB of HA device size with a disk-based journal configured and 2-way replication and 4MB per 1 TB of HA device size for 3-way replication.

Failure journal – provides good I/O performance, as a RAM-based journal, while all device nodes are in a healthy synchronized state. If a device on one node went into a not synchronized state, the disk-based journal activates and a performance drop could occur as the device performance is defined by the disk speed, where the journal is located. Fast synchronization is not guaranteed in all cases. For example, if a simultaneous hard reset of all nodes occurs, full synchronization will occur.

Continuous journal – guarantees fast synchronization and data consistency in all cases. Although, this strategy has the worst I/O performance, because of frequent write operations to the journal, located on the disk, where the journal is located.



Synchronization Journal Setup

● **RAM-based journal**
Synchronization journal placed in RAM. Synchronization with RAM journal provides good IO performance in any scenario.

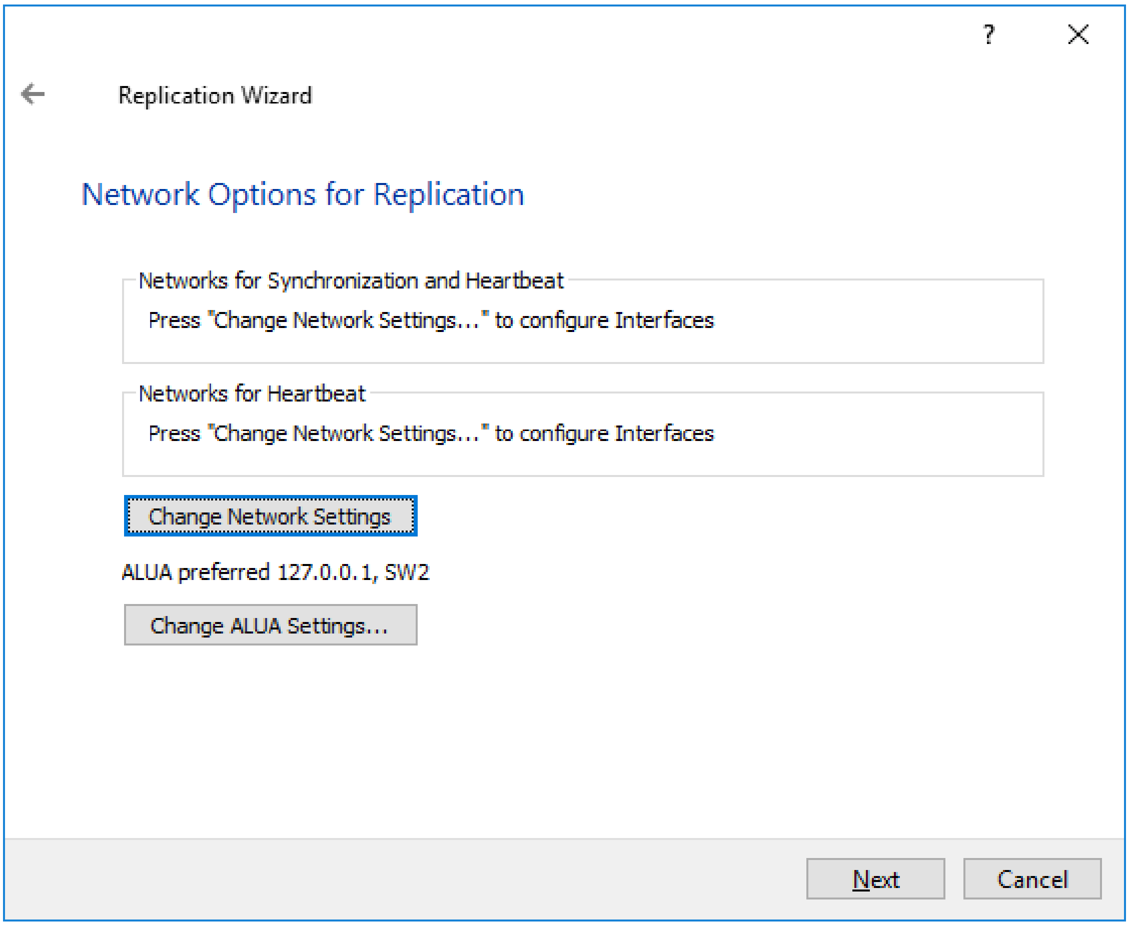
○ **Disk-based journal**
Synchronization journal placed on disk.

● **Failure journal**
The strategy provides good IO performance while all device nodes are in a healthy state.

○ **Continuous journal**
The strategy guarantees fast synchronization and data consistency in all cases.

Current Node: My Computer\C\
Partner Node: My Computer\C\

5. Click Change Network Settings.



Replication Wizard

Network Options for Replication

Networks for Synchronization and Heartbeat

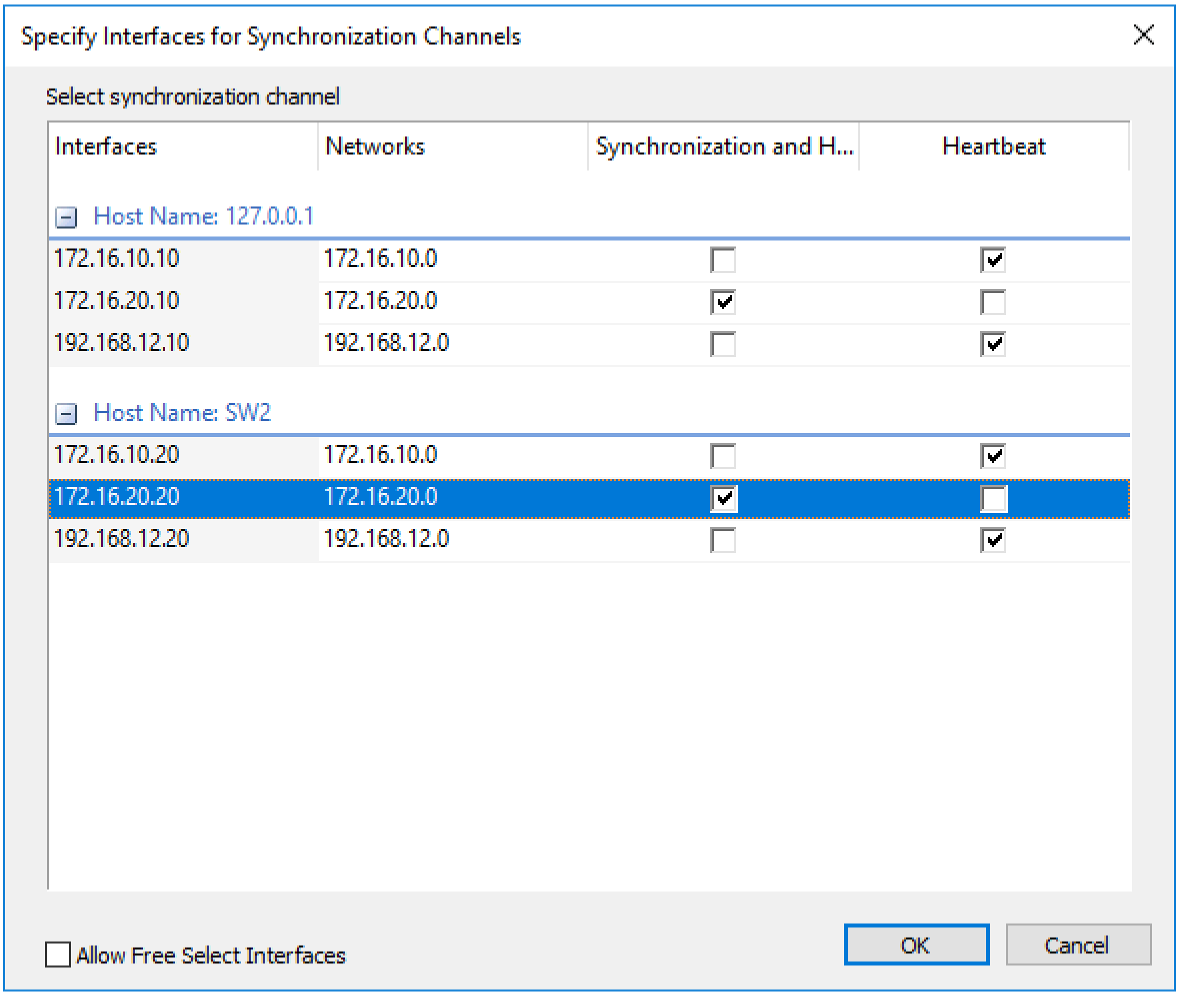
Press "Change Network Settings..." to configure Interfaces

Networks for Heartbeat

Press "Change Network Settings..." to configure Interfaces

ALUA preferred 127.0.0.1, SW2

6. Specify the interfaces for Synchronization and Heartbeat Channels. Click OK and then click Next.



Specify Interfaces for Synchronization Channels

Select synchronization channel

Interfaces	Networks	Synchronization and H...	Heartbeat
⊟ Host Name: 127.0.0.1			
172.16.10.10	172.16.10.0	□	☑
172.16.20.10	172.16.20.0	☑	□
192.168.12.10	192.168.12.0	□	☑
⊟ Host Name: SW2			
172.16.10.20	172.16.10.0	□	☑
172.16.20.20	172.16.20.0	☑	□
192.168.12.20	192.168.12.0	□	☑

□ Allow Free Select Interfaces

7. In Select Partner Device Initialization Mode, select Synchronize from existing Device and click Next.

8. Click Create Replica. Click Finish to close the wizard.
The successfully added device appears in StarWind Management Console.

9. Follow the similar procedure for the creation of other virtual disks that will be used as storage repositories.
NOTE: To extend an Image File or a StarWind HA device to the required size, please check the article below:

https://knowledgebase.starwindsoftware.com/maintenance/how-to-extend-image-file-or-high-availability-device/

Node Majority

There are two ways to configure Witness for 2-nodes StarWind HA device, created with

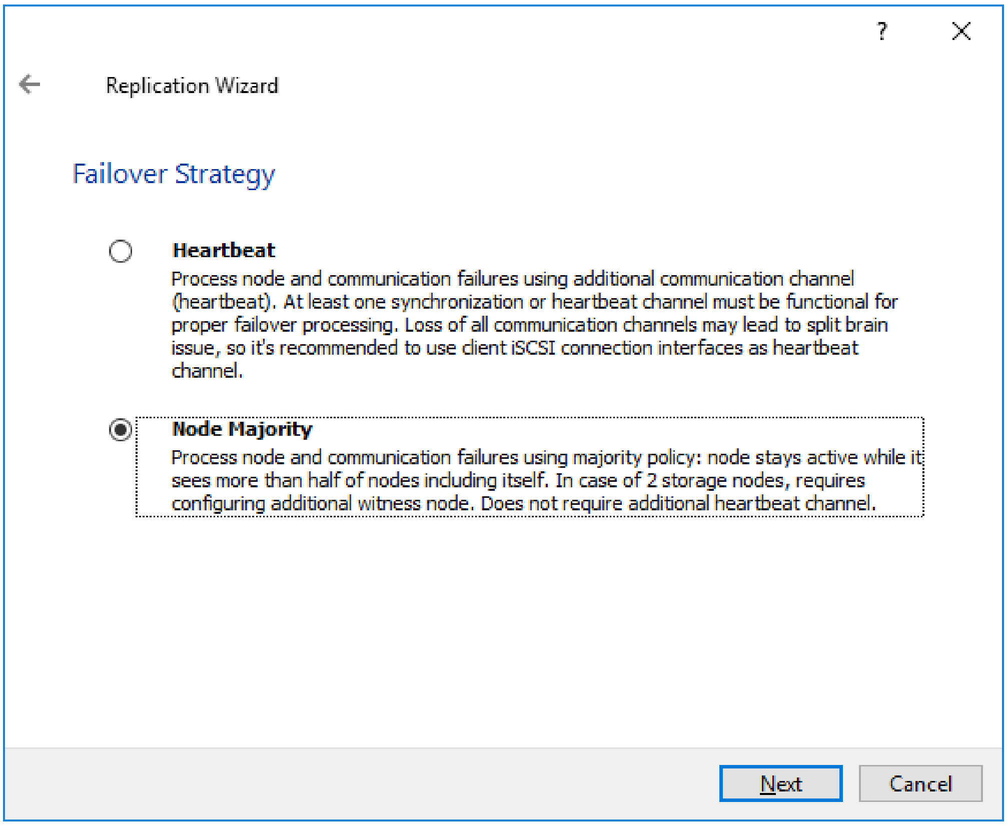
Node Majority Failover Strategy: File Share (SMB) as Witness and additional server as Witness Node.

– Creating HA device with File SHare(SMB) as Witness:

SMB Witness is a file, located on SMB share, which can be accessed by both nodes and help them to eliminate the split-brain issue in case of synchronization connection interruption between the nodes. To set up the SMB file share as a Witness for 2-nodes HA device with Node Majority Failover Strategy, perform the actions, described on this page:
https://www.starwindsoftware.com/help/ConfiguringFileShareSMBasWitness.html

– Creating HA device with Witness Node:

1. Select the Node Majority failover strategy and click Next.



Failover Strategy

○ **Heartbeat**
Process node and communication failures using additional communication channel (heartbeat). At least one synchronization or heartbeat channel must be functional for proper failover processing. Loss of all communication channels may lead to split brain issue, so it's recommended to use client iSCSI connection interfaces as heartbeat channel.

● **Node Majority**
Process node and communication failures using majority policy: node stays active while it sees more than half of nodes including itself. In case of 2 storage nodes, requires configuring additional witness node. Does not require additional heartbeat channel.

2. Choose Create new Partner Device and click Next.

3. Specify the partner device Location and modify the target name if necessary. Click Next. Select Synchronization Journal strategy and location and click Next.

4. In Network Options for Replication, press the Change network settings button and

select the synchronization channel for the HA device.

5. In Specify Interfaces for Synchronization Channels, select the checkboxes with the appropriate networks and click OK. Then click Next.

6. Select Synchronize from existing Device as the partner device initialization mode.

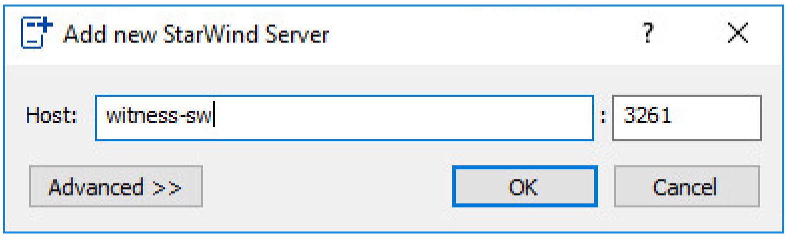
7. Press the Create Replica button and close the wizard.

8. The added devices will appear in StarWind Management Console.
Repeat the steps above to create other virtual disks if necessary.

Adding Witness Node

Witness node can be configured on a separate host or as a virtual machine in a cloud. It requires StarWind Virtual SAN service installed on it.
NOTE: Since the device created in this guide is replicated between 2 active nodes with the Node Majority failover strategy, a Witness node must be added to it.

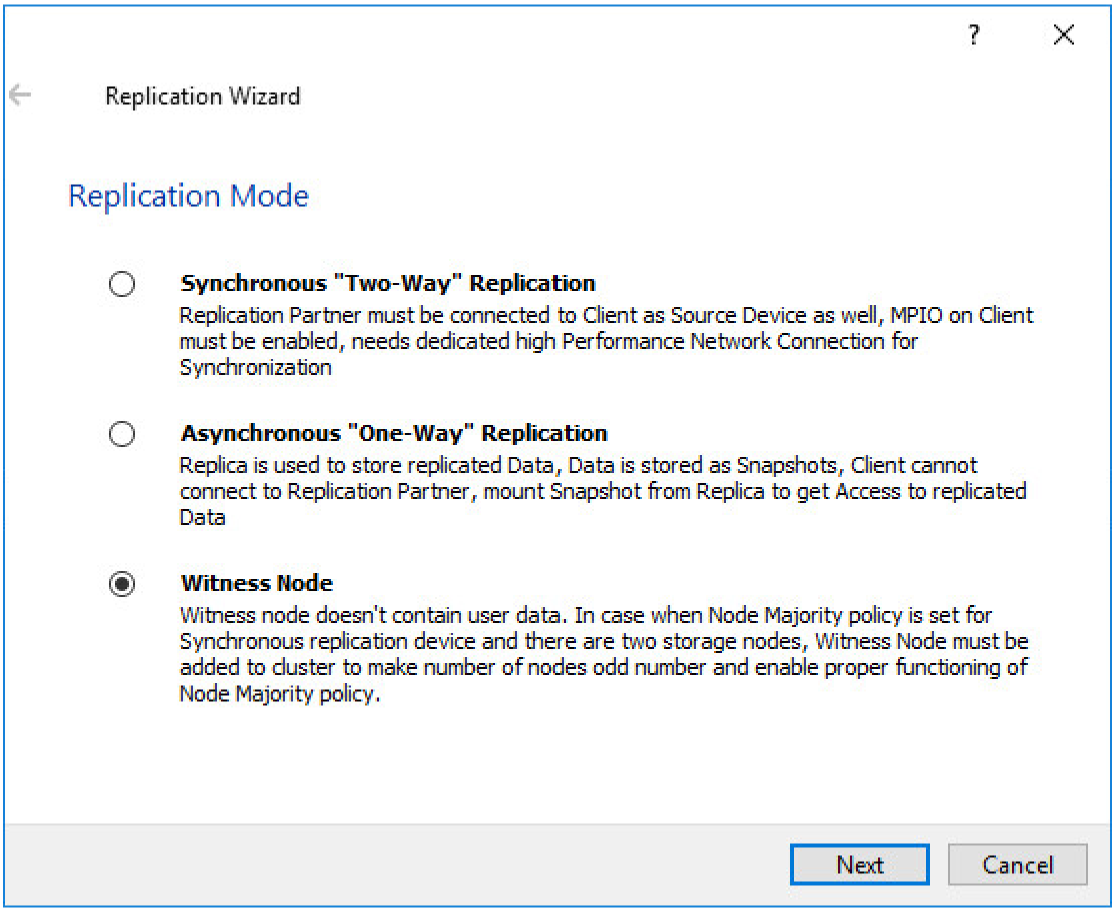
1. Open StarWind Management Console, right-click on the Servers field and press the Add Server button. Add a new StarWind Server which will be used as the Witness node and click OK.


Add new StarWind Server

Host: witness-sw : 3261

2. Right-click on the HA device with the configured Node Majority failover policy and select Replication Manager and press the Add Replica button.

3. Select Witness Node.



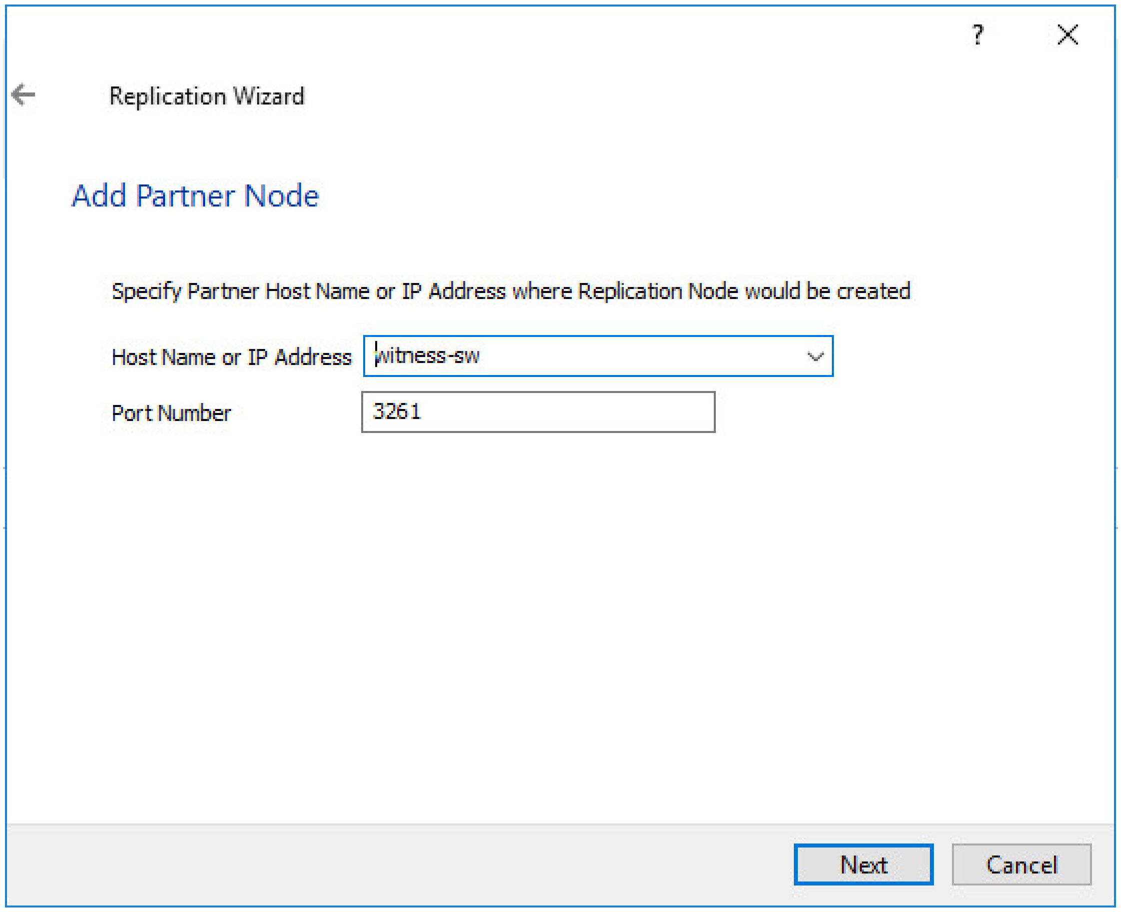
Replication Mode

○ **Synchronous "Two-Way" Replication**
Replication Partner must be connected to Client as Source Device as well, MPIO on Client must be enabled, needs dedicated high Performance Network Connection for Synchronization

○ **Asynchronous "One-Way" Replication**
Replica is used to store replicated Data, Data is stored as Snapshots, Client cannot connect to Replication Partner, mount Snapshot from Replica to get Access to replicated Data

● **Witness Node**
Witness node doesn't contain user data. In case when Node Majority policy is set for Synchronous replication device and there are two storage nodes, Witness Node must be added to cluster to make number of nodes odd number and enable proper functioning of Node Majority policy.

4. Specify the Witness node Host Name or IP address. The default Port Number is 3261.



Add Partner Node

Specify Partner Host Name or IP Address where Replication Node would be created

Host Name or IP Address: witness-sw

Port Number: 3261

5. In Partner Device Setup, specify the Witness device Location. Optionally, modify the target name by clicking the appropriate button.

6. In Network Options for Replication, select the synchronization channel with the Witness node by clicking the Change Network Settings button.

7. Specify the interface for Synchronization and Heartbeat and click OK.

8. Click Create Replica and then close the wizard.

9. Repeat the steps above to create other virtual disks if necessary.
NOTE: To extend an Image File or a StarWind HA device to the required size, please check the article below:

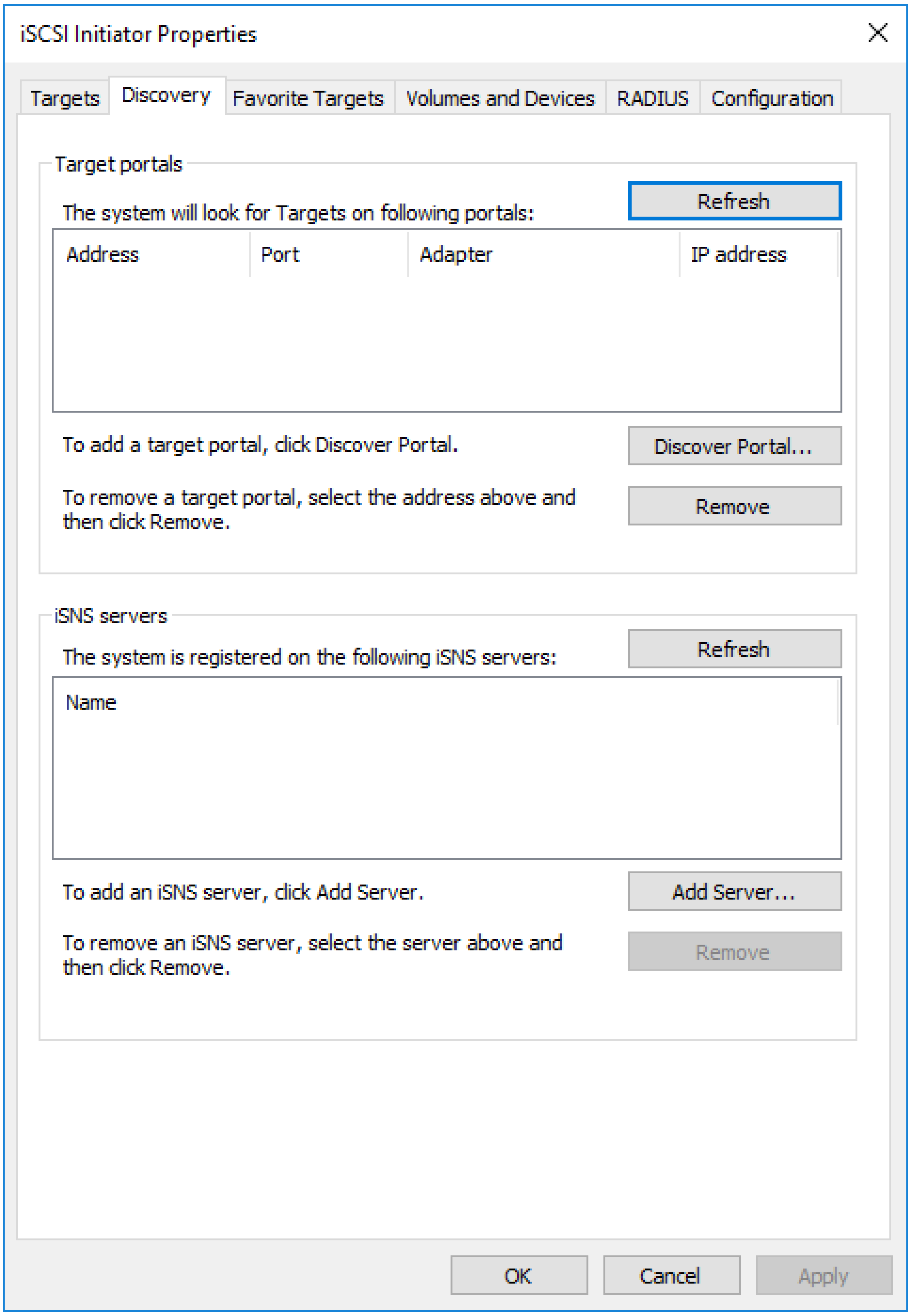
https://knowledgebase.starwindsoftware.com/maintenance/how-to-extend-image-file-or-high-availability-device/

Provisioning Starwind Ha Storage To Windows Server Host

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.



The system will look for Targets on following portals:

To add a target portal, click Discover Portal.

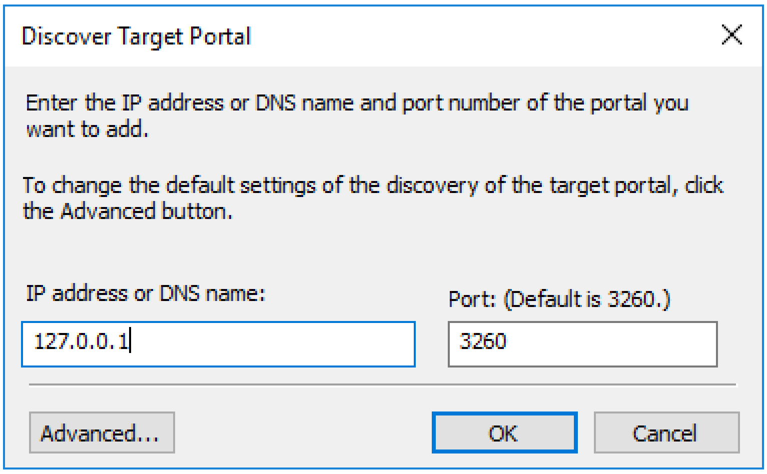
To remove a target portal, select the address above and then click Remove.

The system is registered on the following iSNS servers:

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 127.0.0.1.



Discover Target Portal

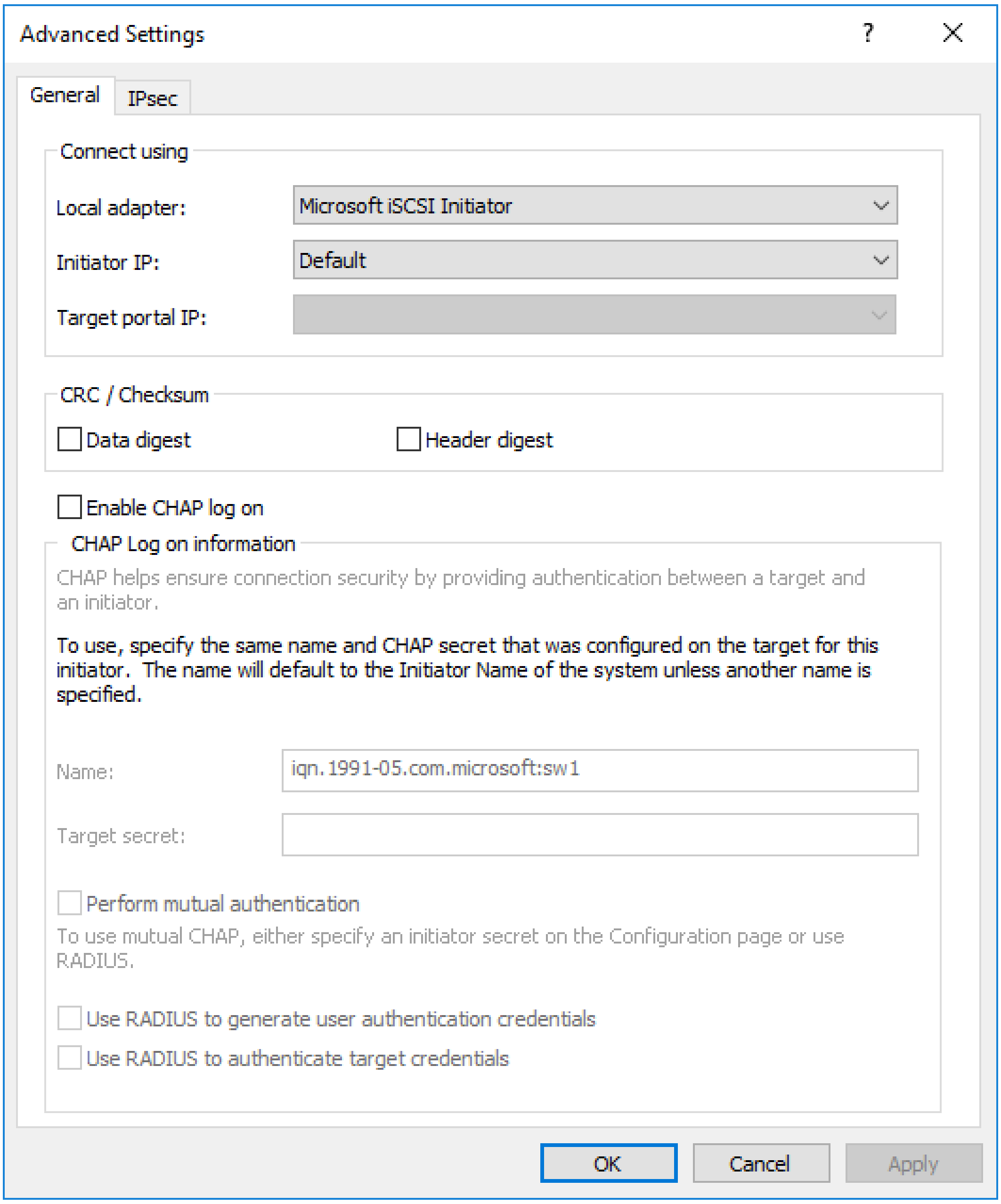
Enter the IP address or DNS name and port number of the portal you want to add.

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

IP address or DNS name: 127.0.0.1

Port: (Default is 3260.) 3260

4. Click the Advanced button. Select Microsoft iSCSI Initiator as a Local adapter and select Initiator IP (leave default for 127.0.0.1). Confirm the actions to complete the Target Portal discovery.



Advanced Settings

General | IPsec

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: Default

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:sw1

Target secret:

□ Perform mutual authentication

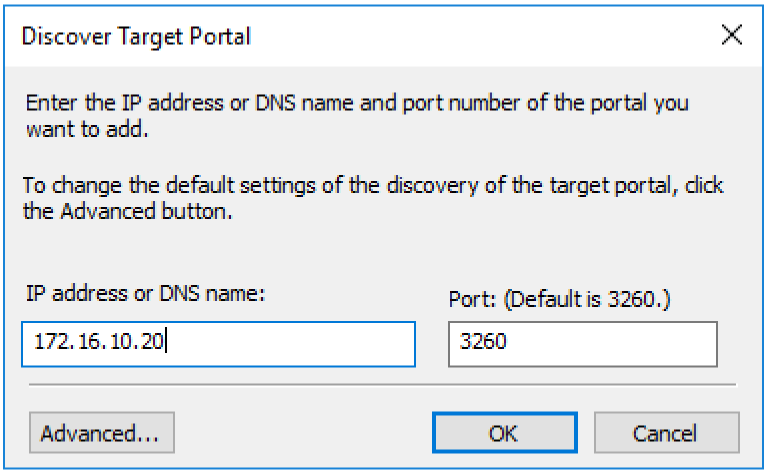
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ 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

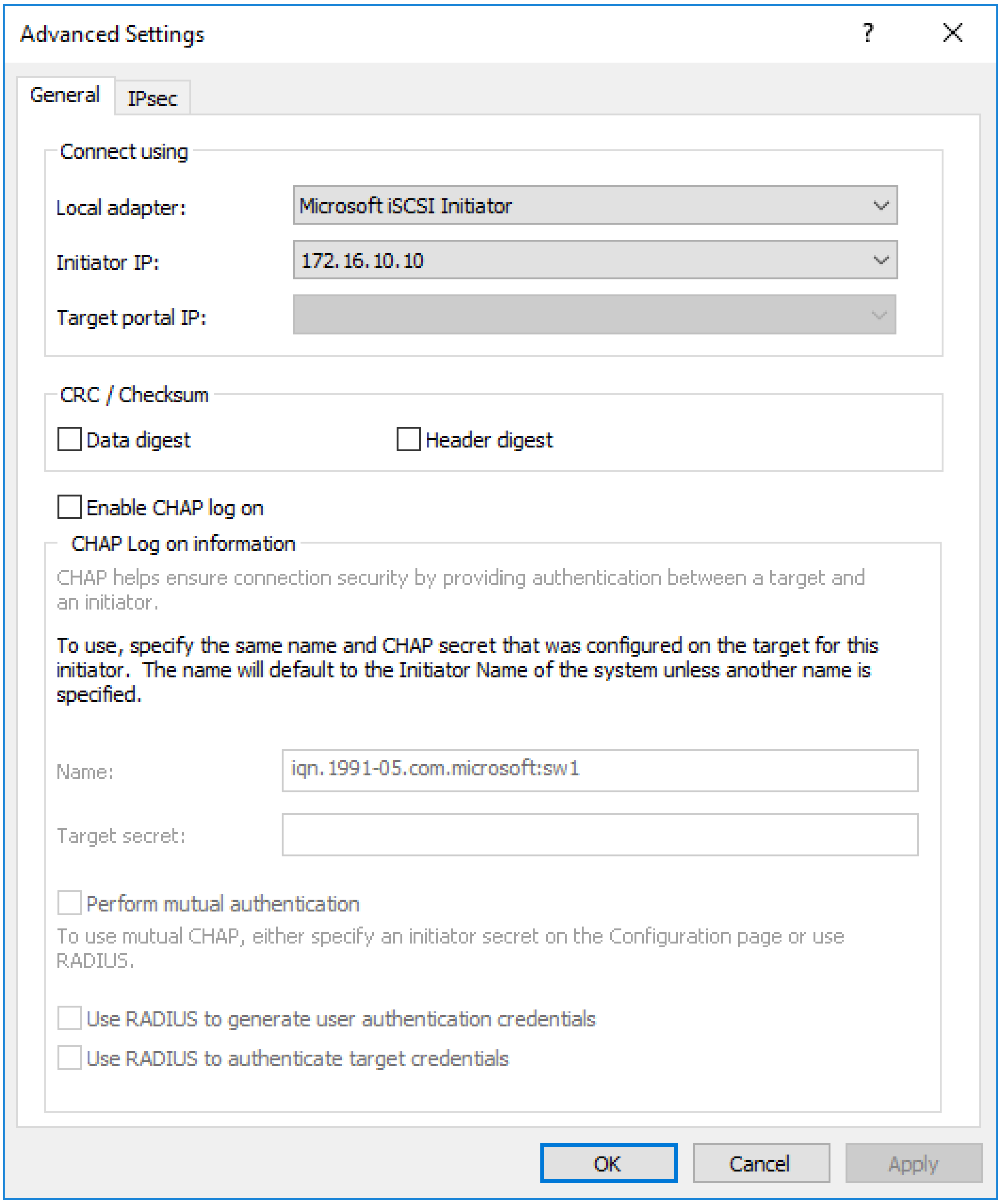
Enter the IP address or DNS name and port number of the portal you want to add.

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.



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:sw1

Target secret:

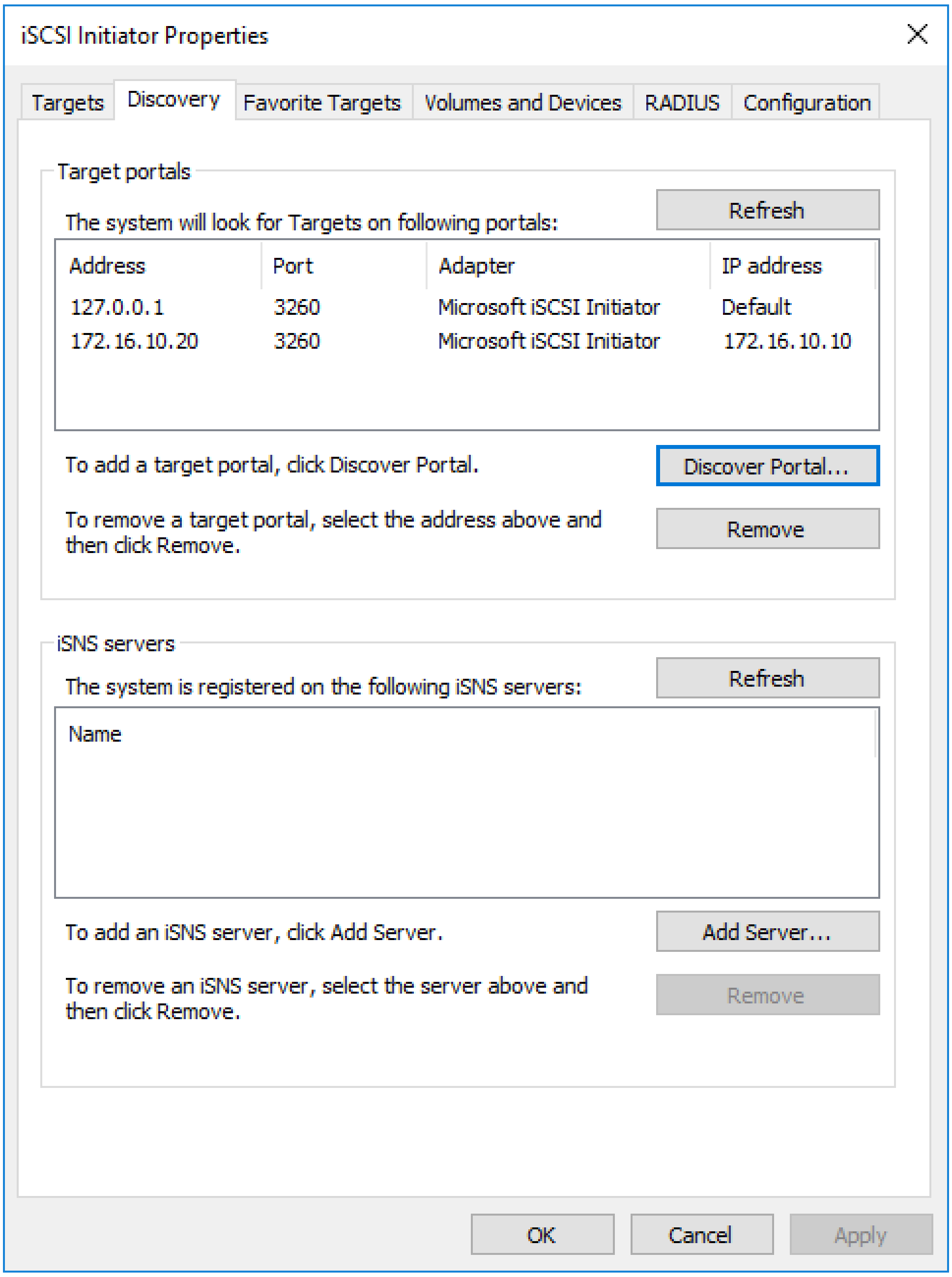
□ Perform mutual authentication

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
127.0.0.1	3260	Microsoft iSCSI Initiator	Default
172.16.10.20	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.

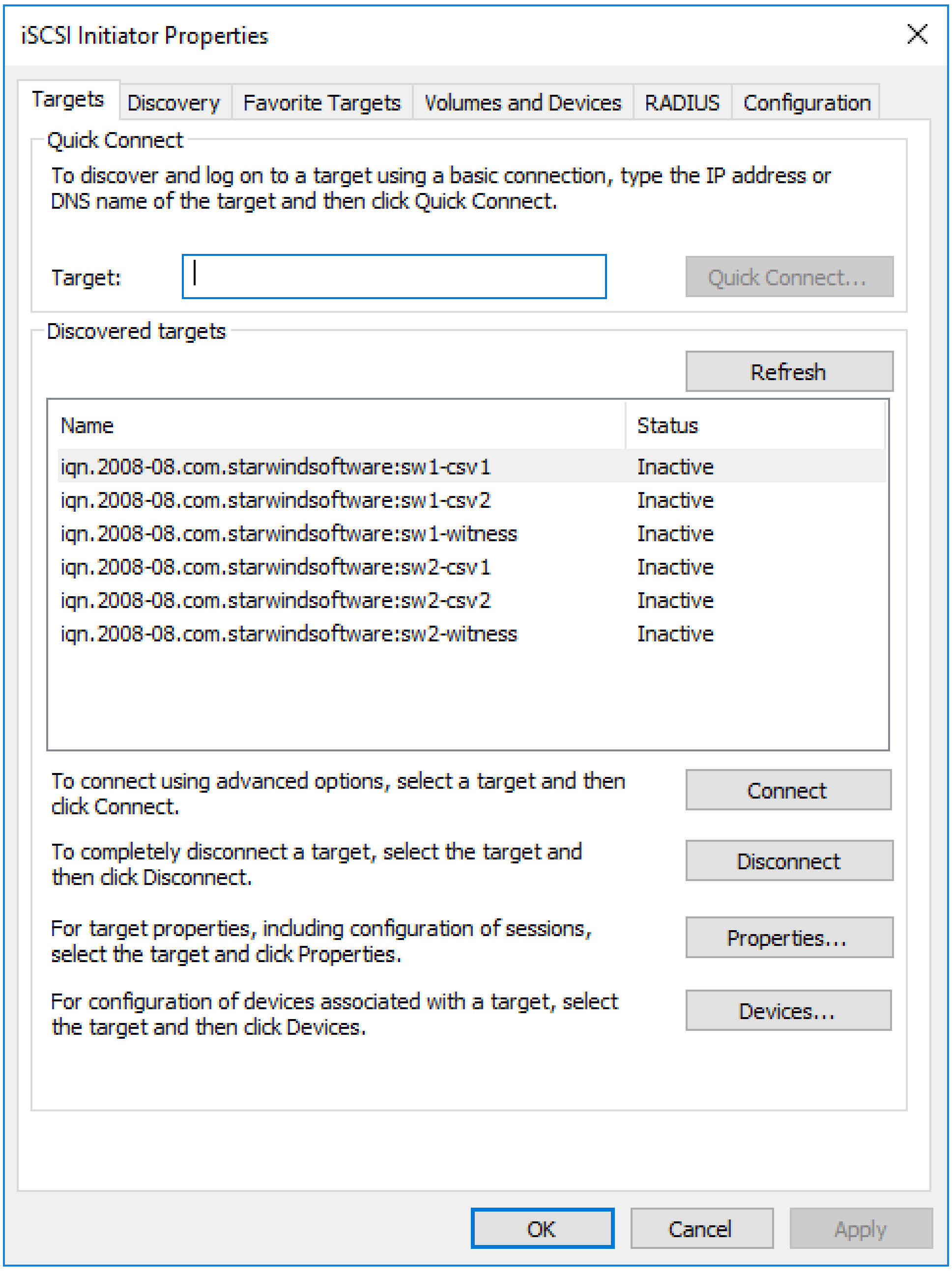
To remove an iSNS server, select the server above and then click Remove.

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.



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.

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.

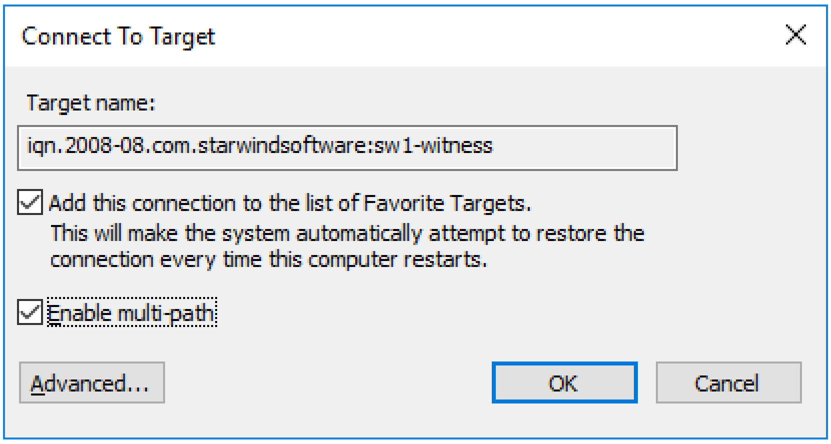
To completely disconnect a target, select the target and then click Disconnect.

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.

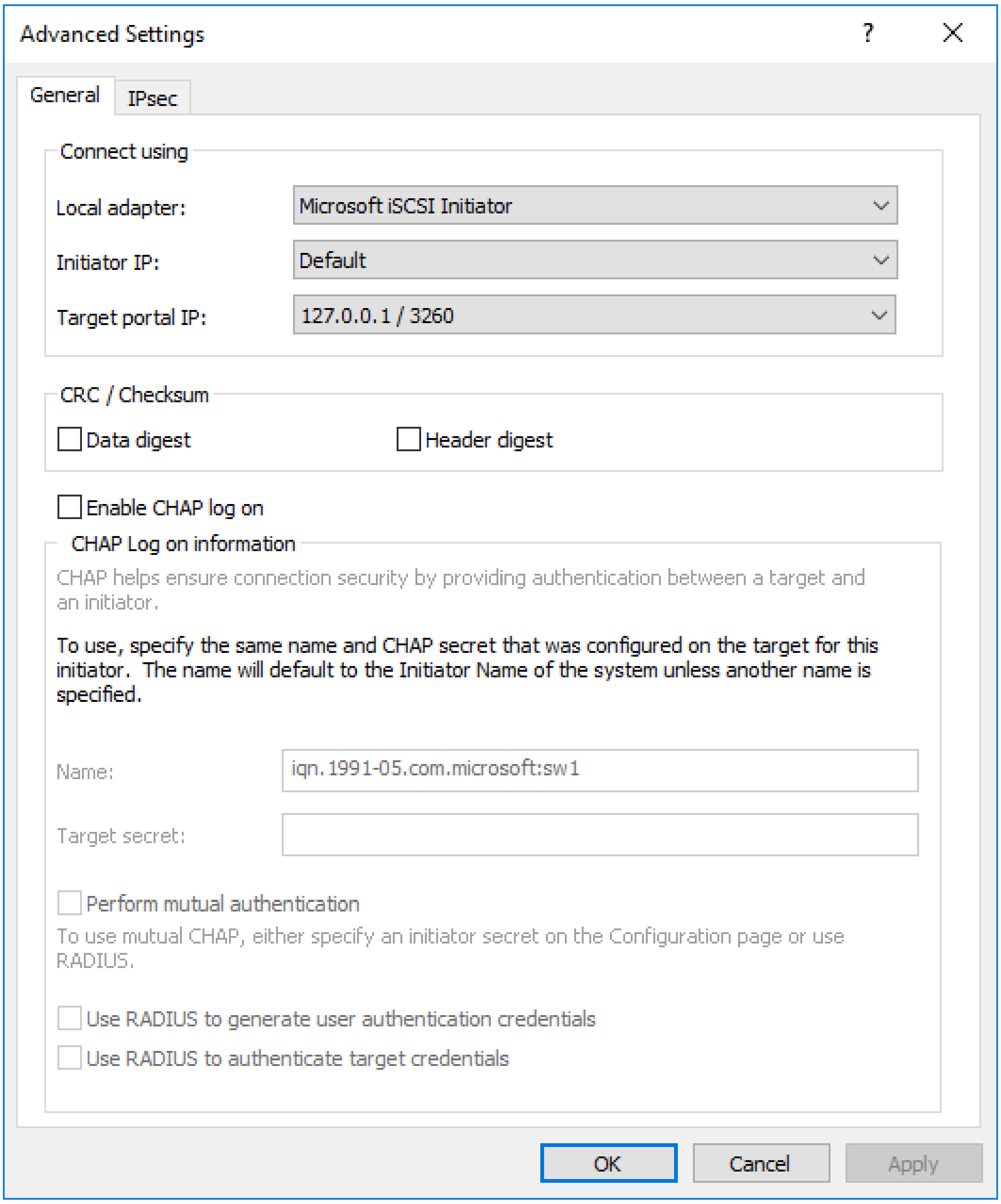


Target name:
iqn.2008-08.com.starwindsoftware:sw1-witness

☑ 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 Target portal IP, select 127.0.0.1. Confirm the actions.



Advanced Settings

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: Default

Target portal IP: 127.0.0.1 / 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:sw1

Target secret:

□ Perform mutual authentication

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

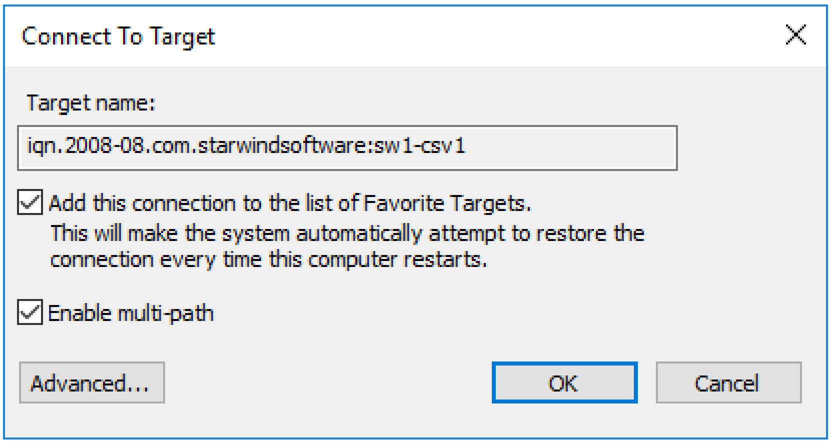
□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

NOTE: It is recommended to connect the Witness device only by loopback (127.0.0.1) address. Do not connect the target to the Witness device from the partner StarWind node.

5. Select the CSV1 target discovered from the local server and click Connect.

6. 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.

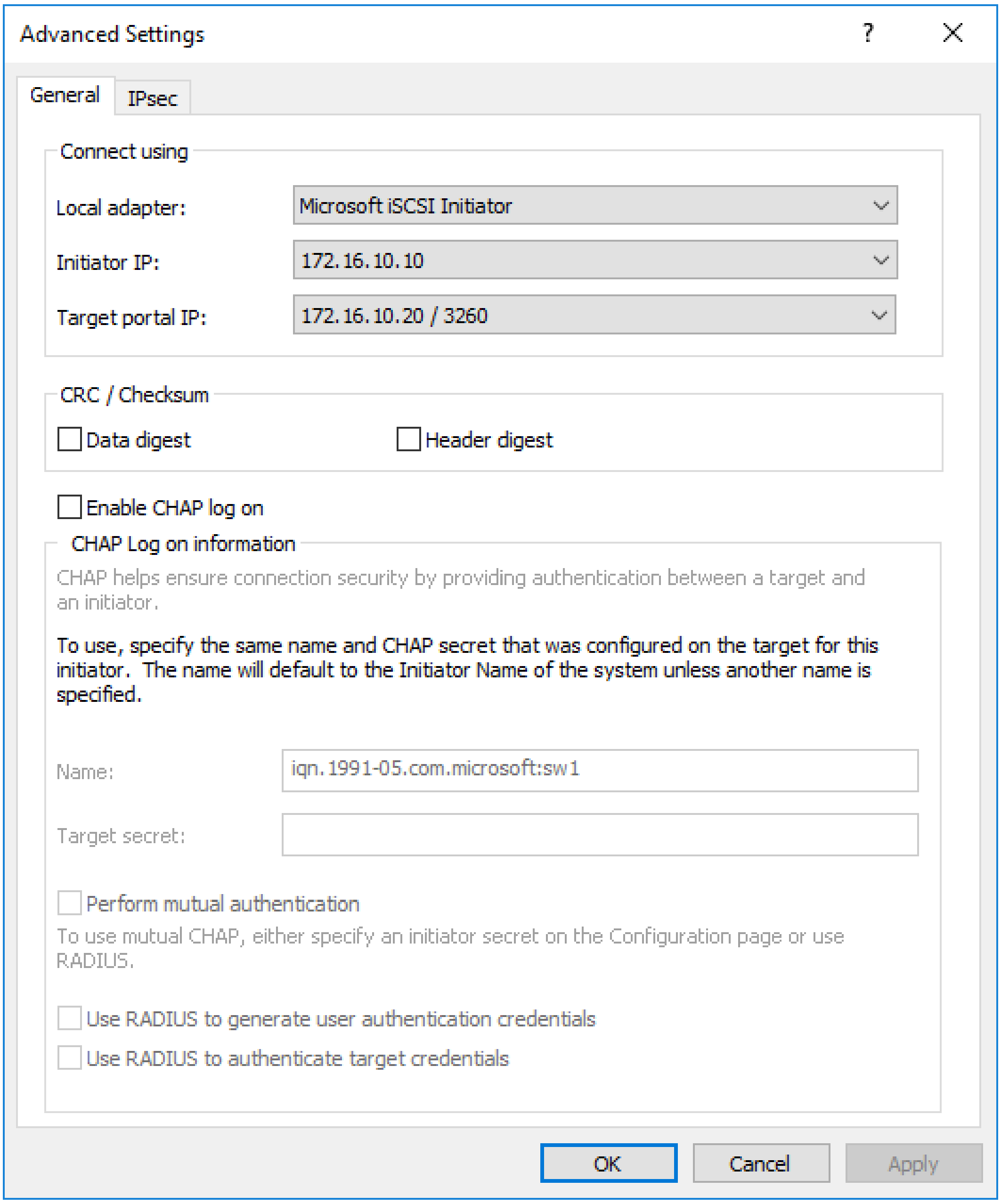
☑ Enable multi-path

7. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Target portal IP, select 127.0.0.1. Confirm the actions.

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

9. Repeat the step 6.

10. 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: 172.16.10.10

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:sw1

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.

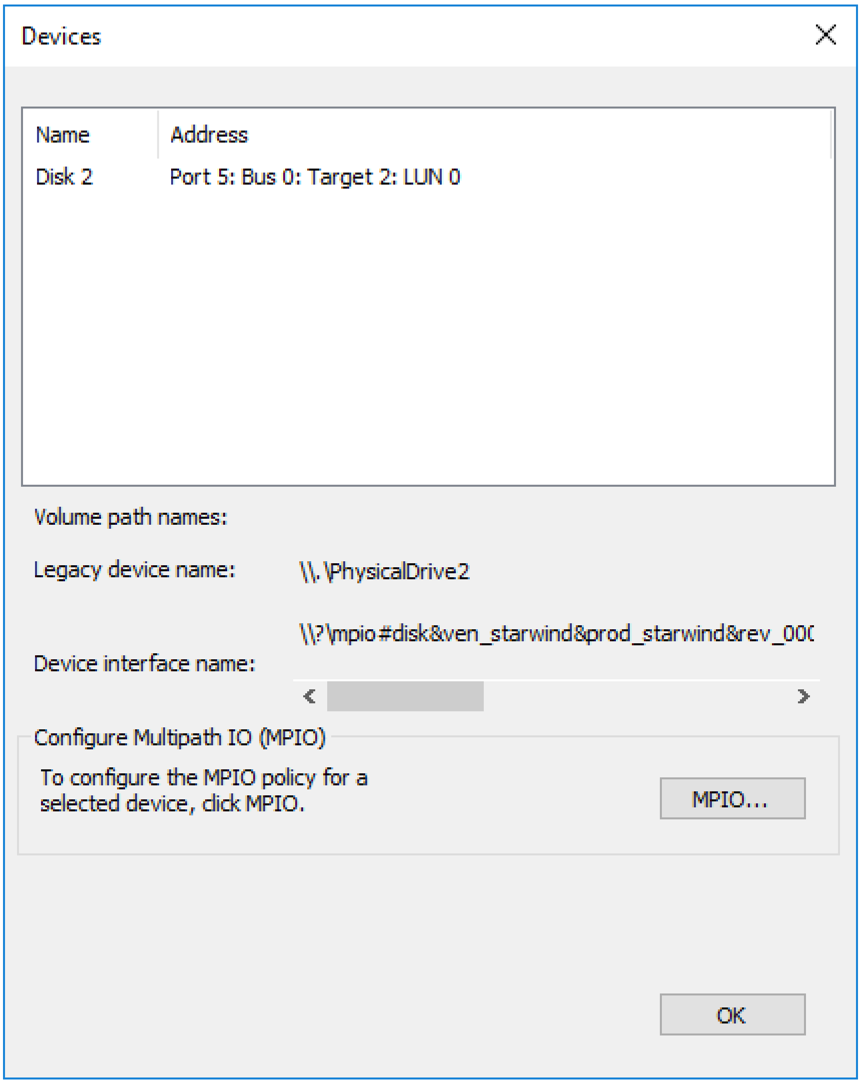
12. Repeat the steps 1-11 on the other StarWind node, specifying corresponding local and data channel IP addresses.

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 except for Witness 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.



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

Volume path names:

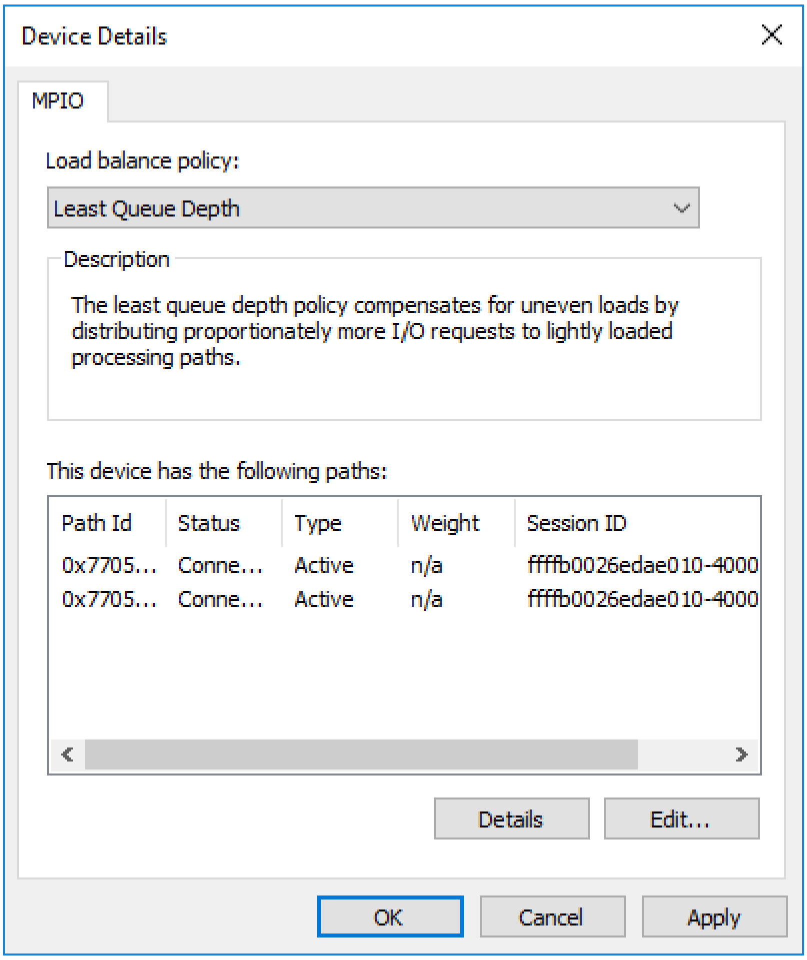
Legacy device name: \\.\PhysicalDrive2

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.



Device Details

MPIO

Load balance policy:

Least Queue Depth

Description

The least queue depth policy compensates for uneven loads by distributing proportionately more I/O requests to lightly loaded processing paths.

This device has the following paths:

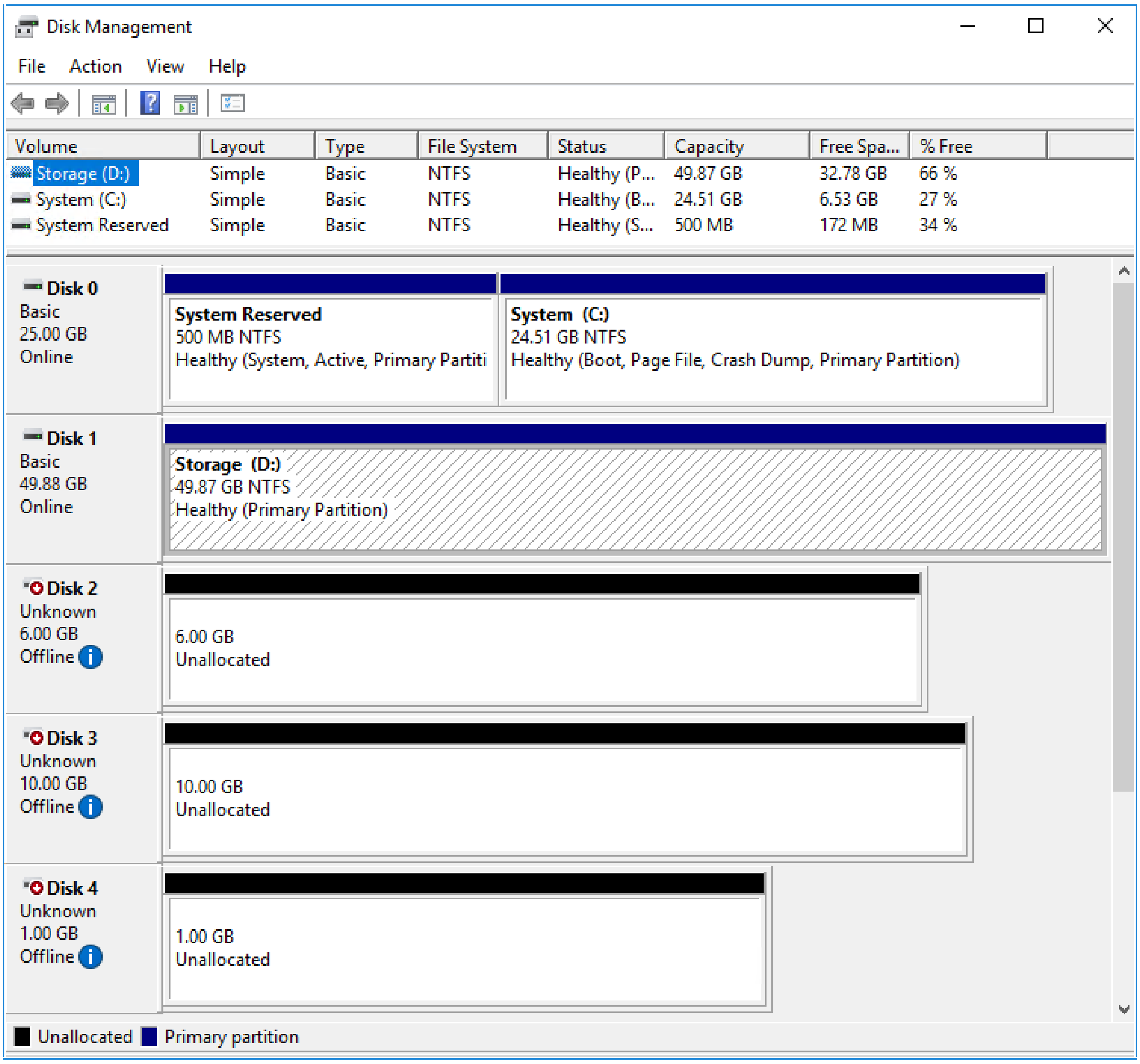
Path Id	Status	Type	Weight	Session ID
0x7705...	Conne...	Active	n/a	ffffb0026edae010-4000
0x7705...	Conne...	Active	n/a	ffffb0026edae010-4000

4. For the Witness target, set the load balance policy to Failover Only.

5. Repeat the steps 1-4 for configuring the MPIO policy for each remaining device on the current node and on the partner node.
NOTE: In case the Failover Only MPIO policy is used, make sure to check that the local path (127.0.0.1) is set to Active, while the partner connection is set to Standby.

Connecting Disks to Servers

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



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

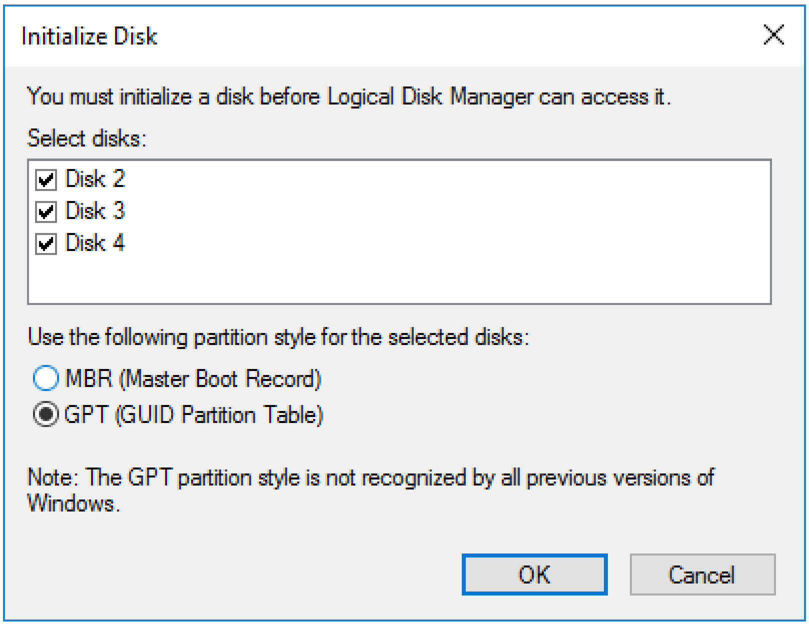
1.00 GB
Unallocated

■ 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:

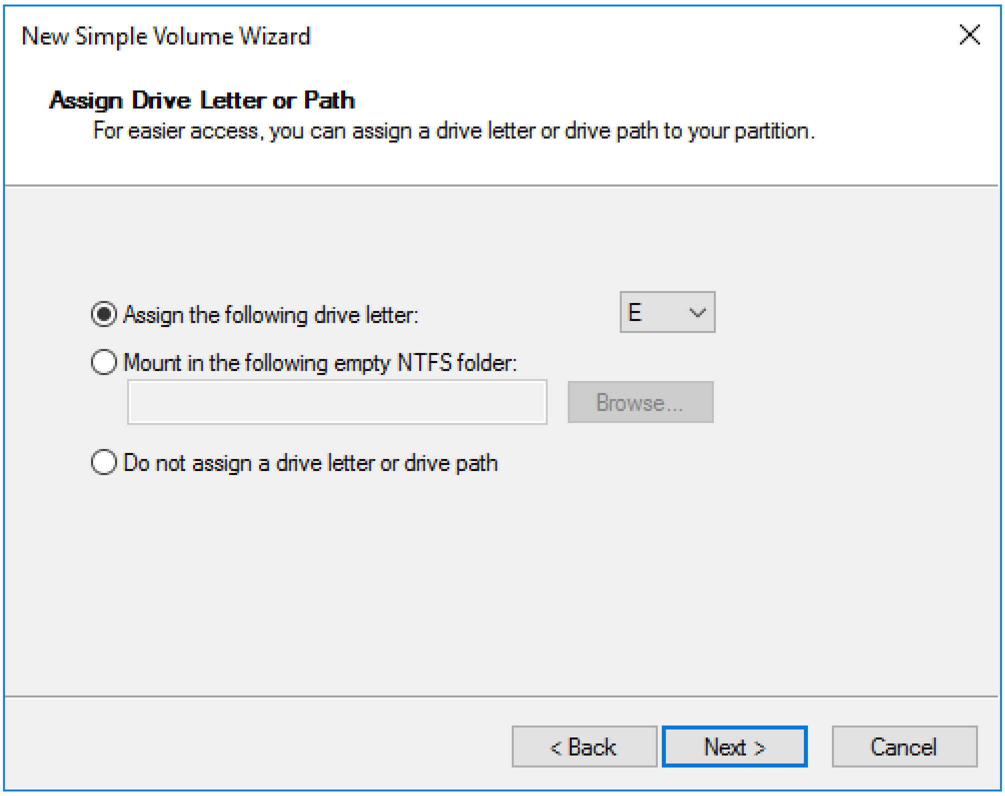
○ MBR (Master Boot Record)
● GPT (GUID Partition Table)

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.

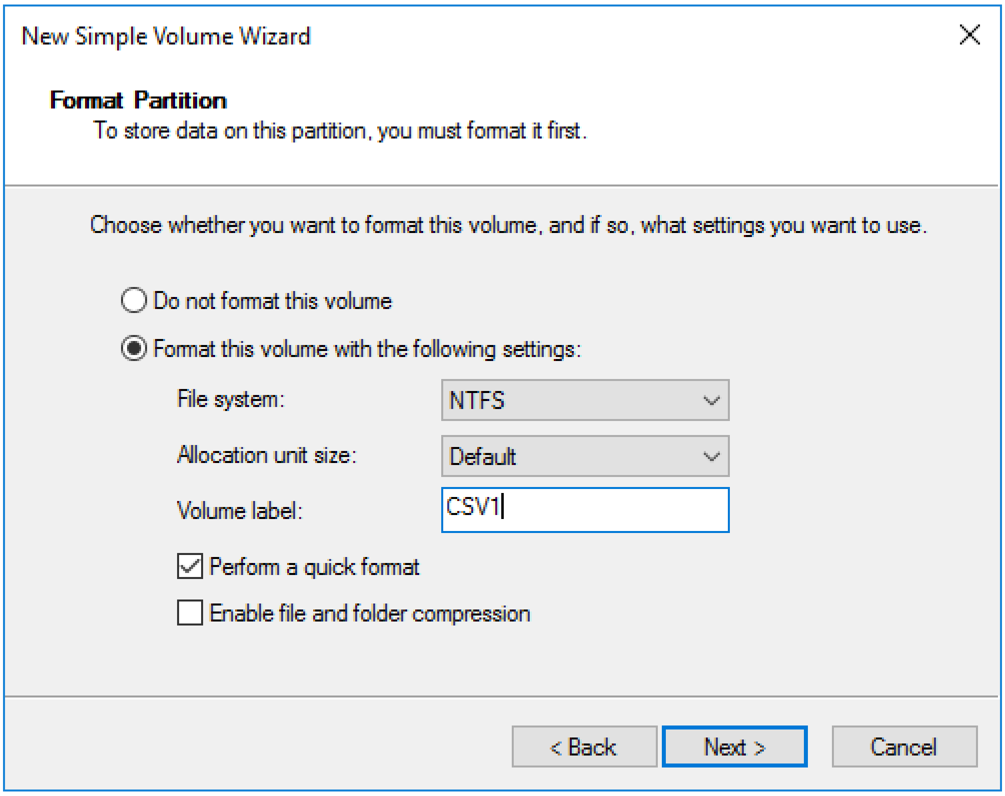


New Simple Volume Wizard

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

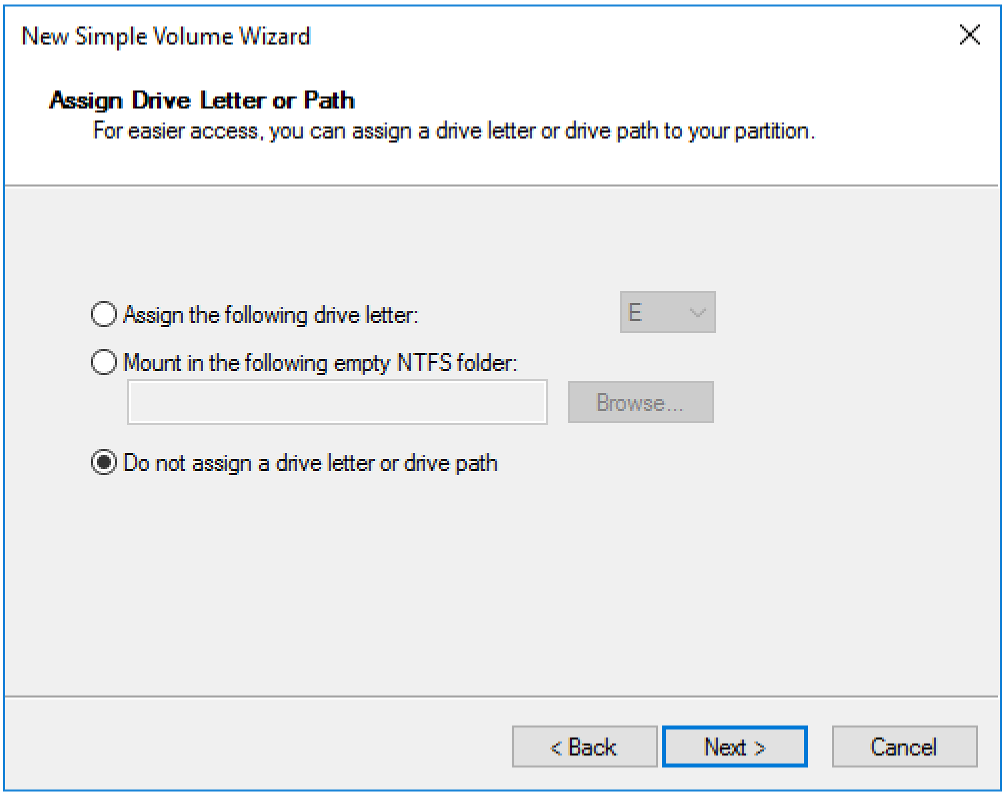
Volume label: CSV1

☑ 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

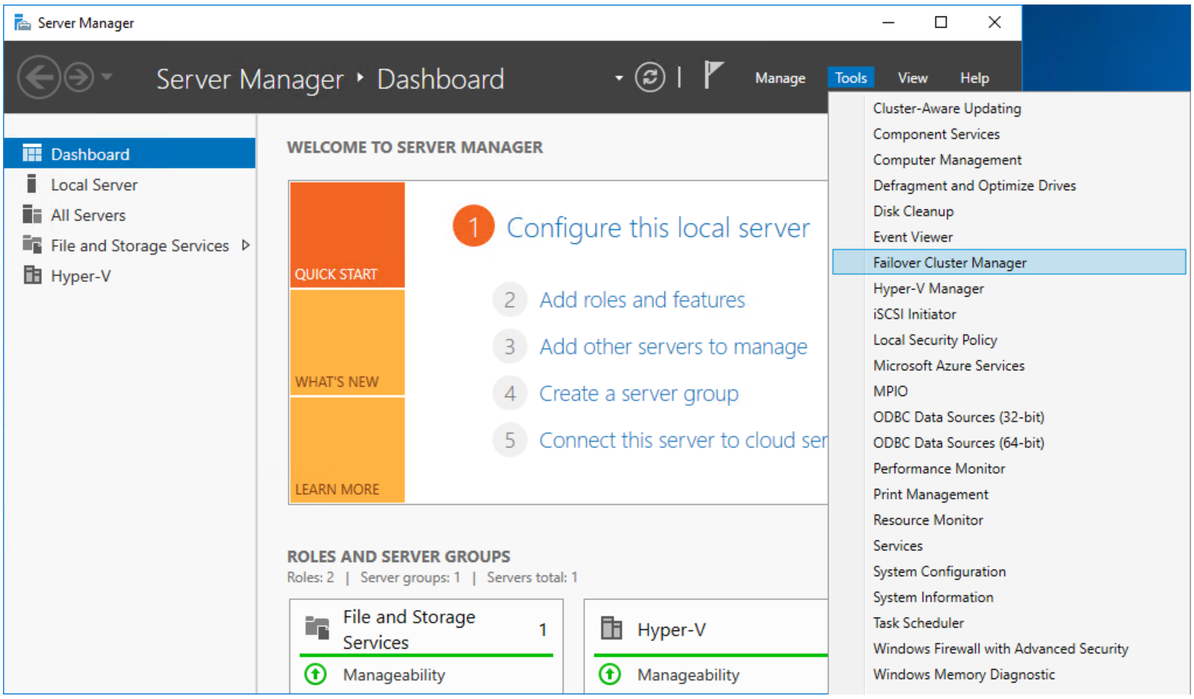
11. On the partner node, open the Disk Management snap-in. All StarWind disks will appear offline. If the status is different from the one shown below,
click Action->Refresh in the top menu to update the information about the disks.

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

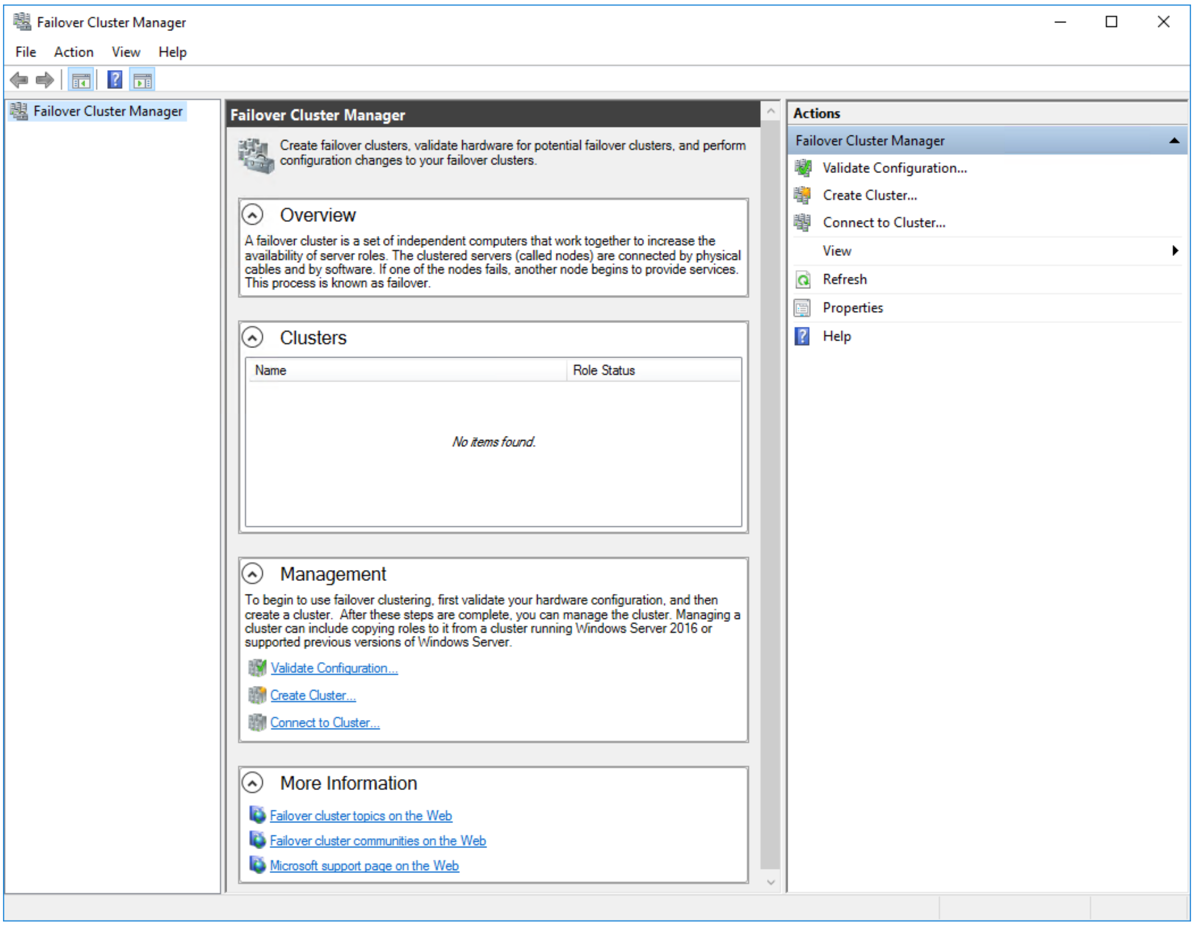
Creating A Failover Cluster In Windows Server

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.

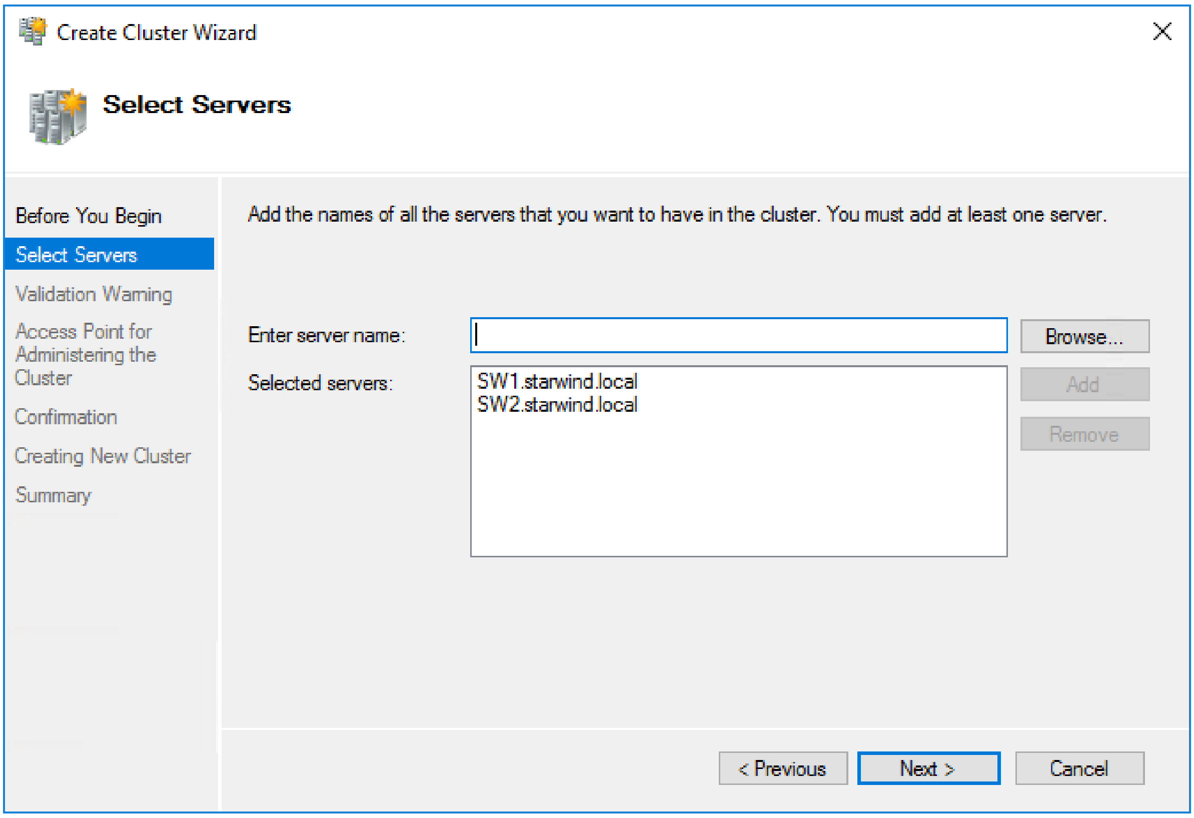


Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

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.

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.

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

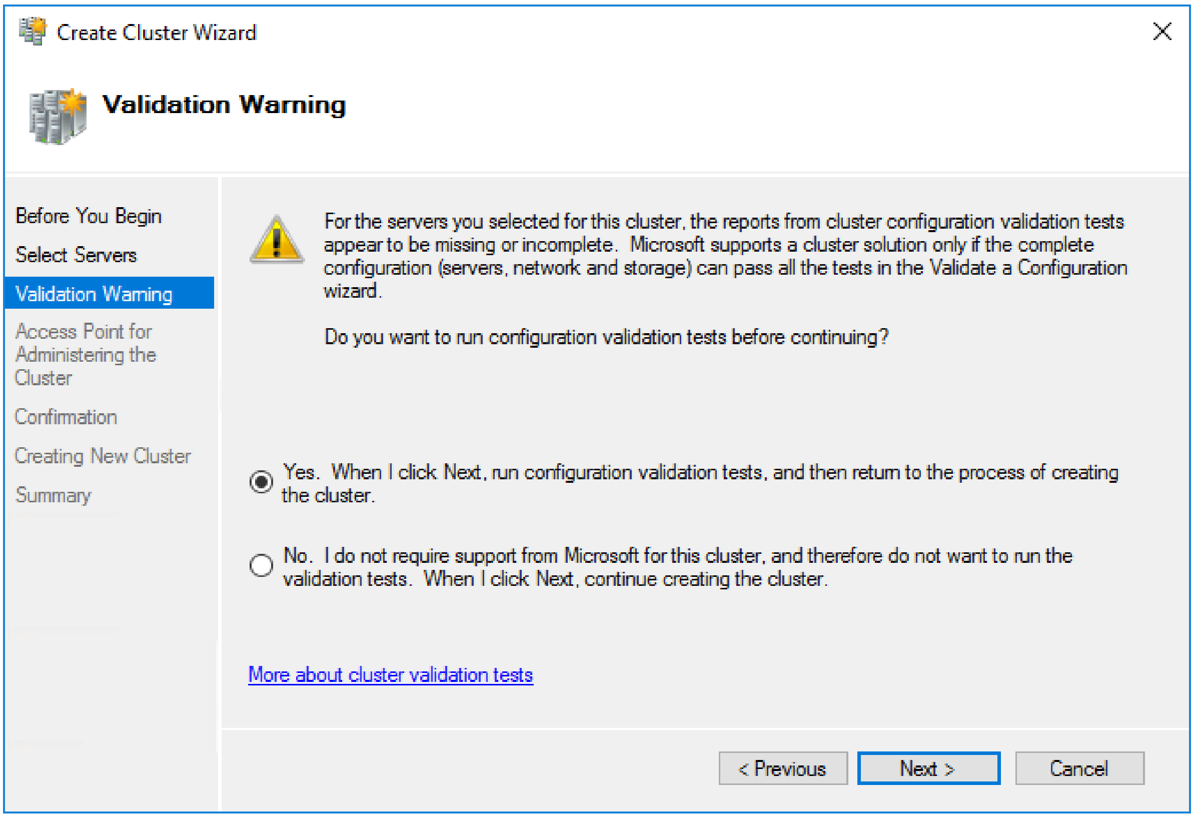


Add the names of all the servers that you want to have in the cluster. You must add at least one server.

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?

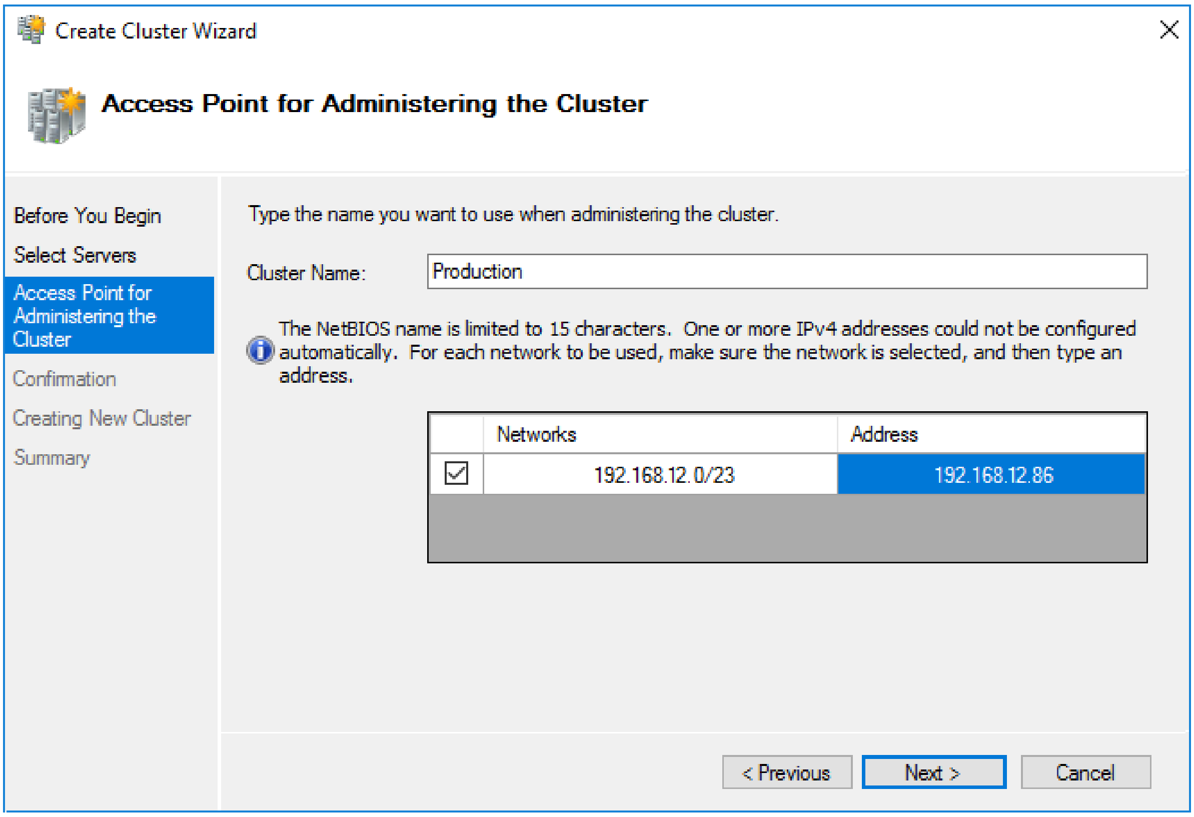
● Yes. When I click Next, run configuration validation tests, and then return to the process of creating the cluster.

○ 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.



Create Cluster Wizard

Access Point for Administering the Cluster

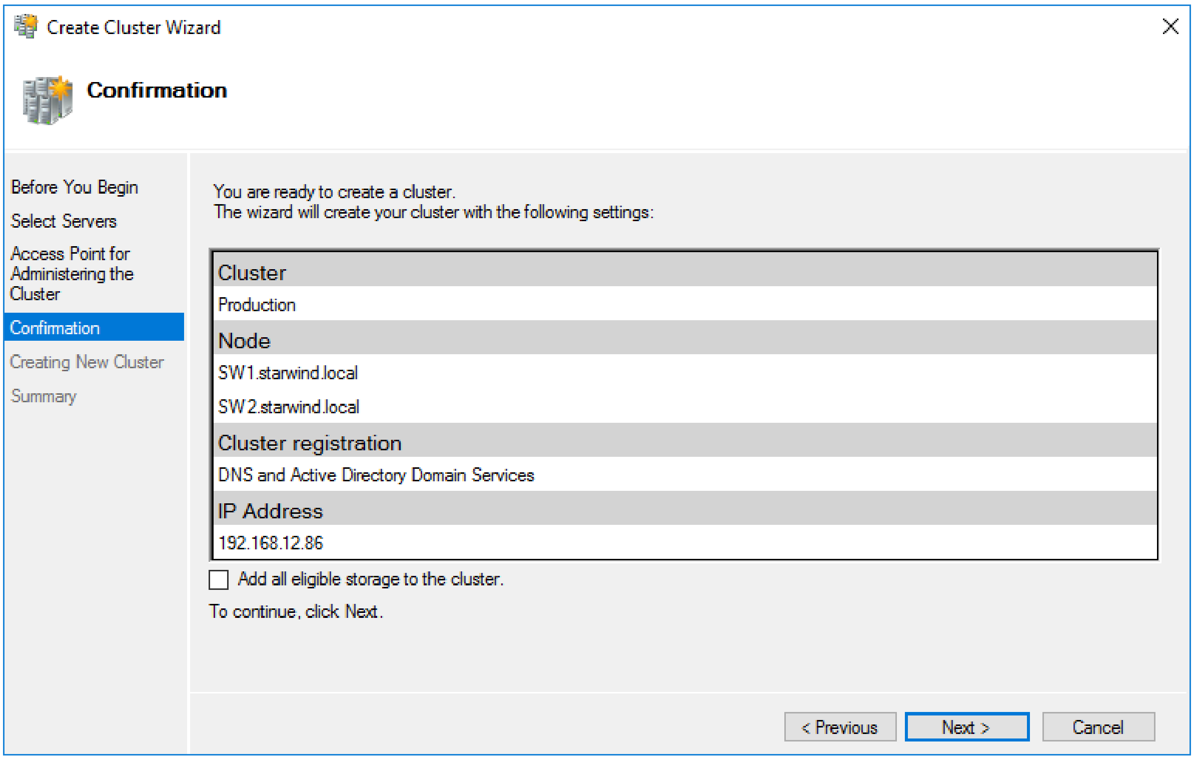
Type the name you want to use when administering the cluster.

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.



Create Cluster Wizard

Confirmation

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

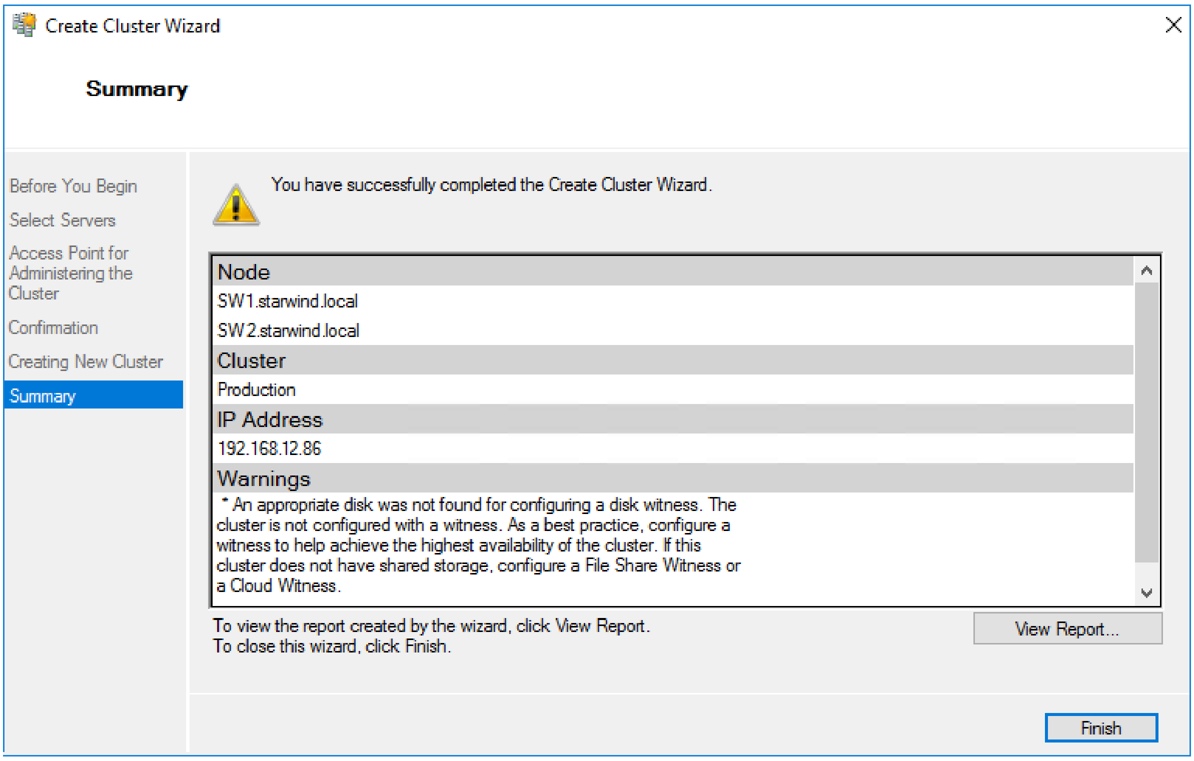
IP Address
192.168.12.86

□ 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.



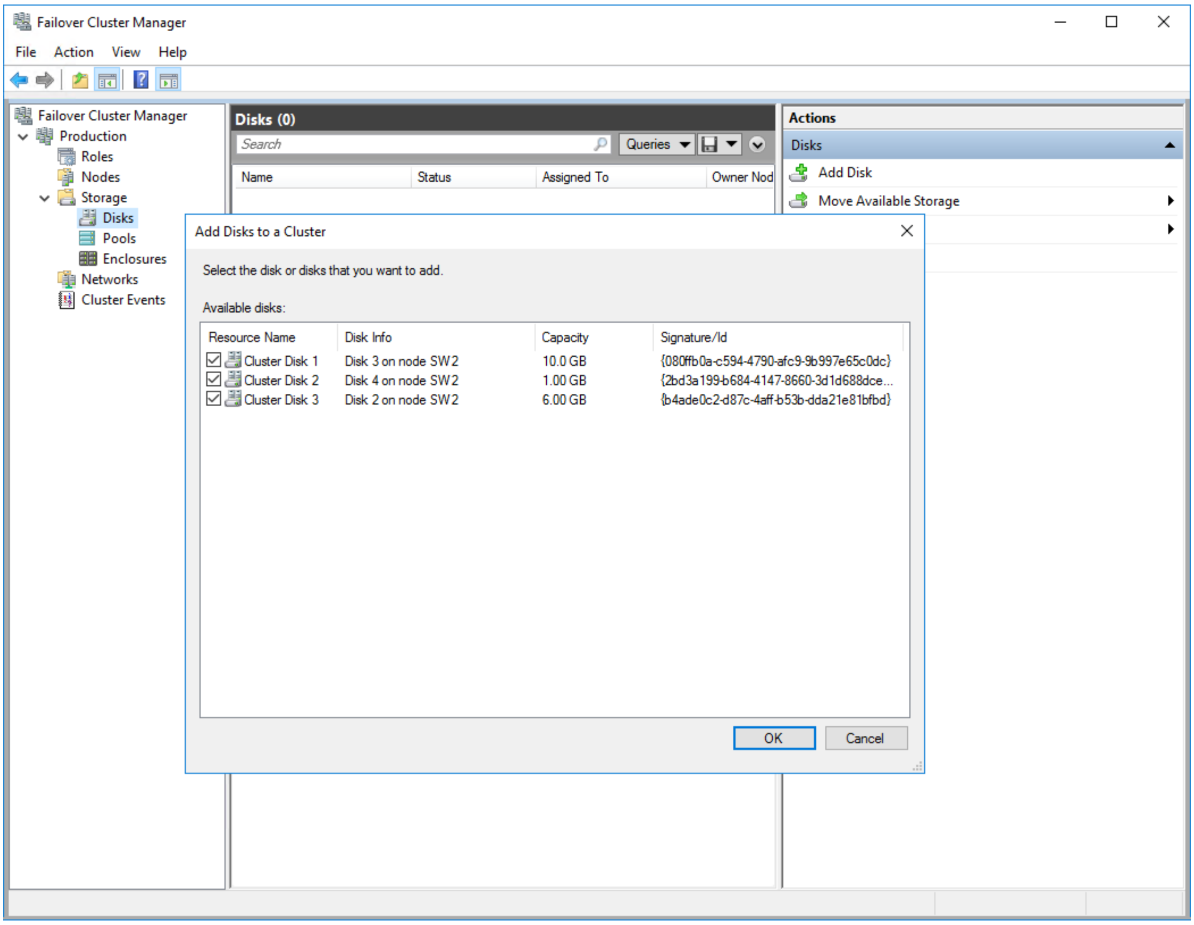
You have successfully completed the Create Cluster Wizard.

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.



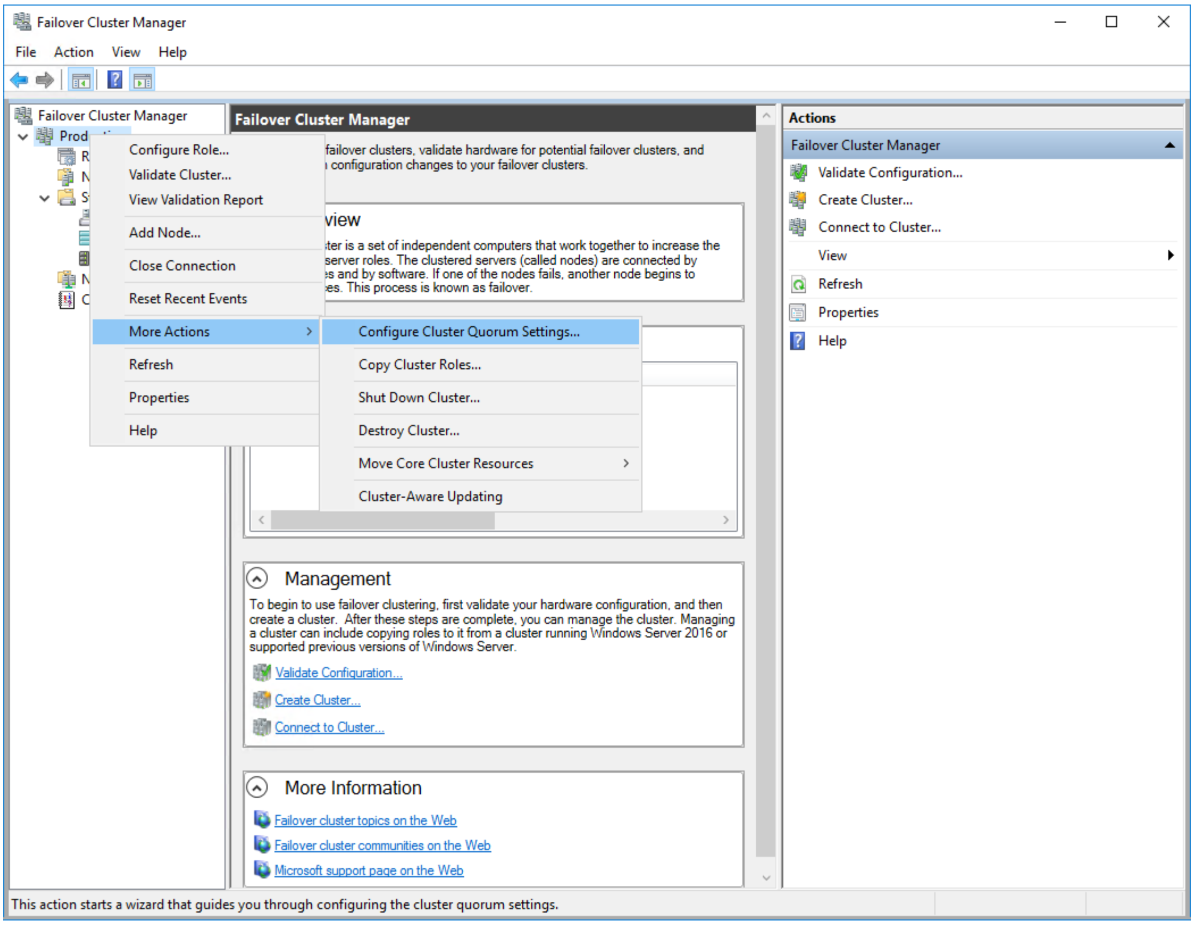
Add Disks to a Cluster

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}

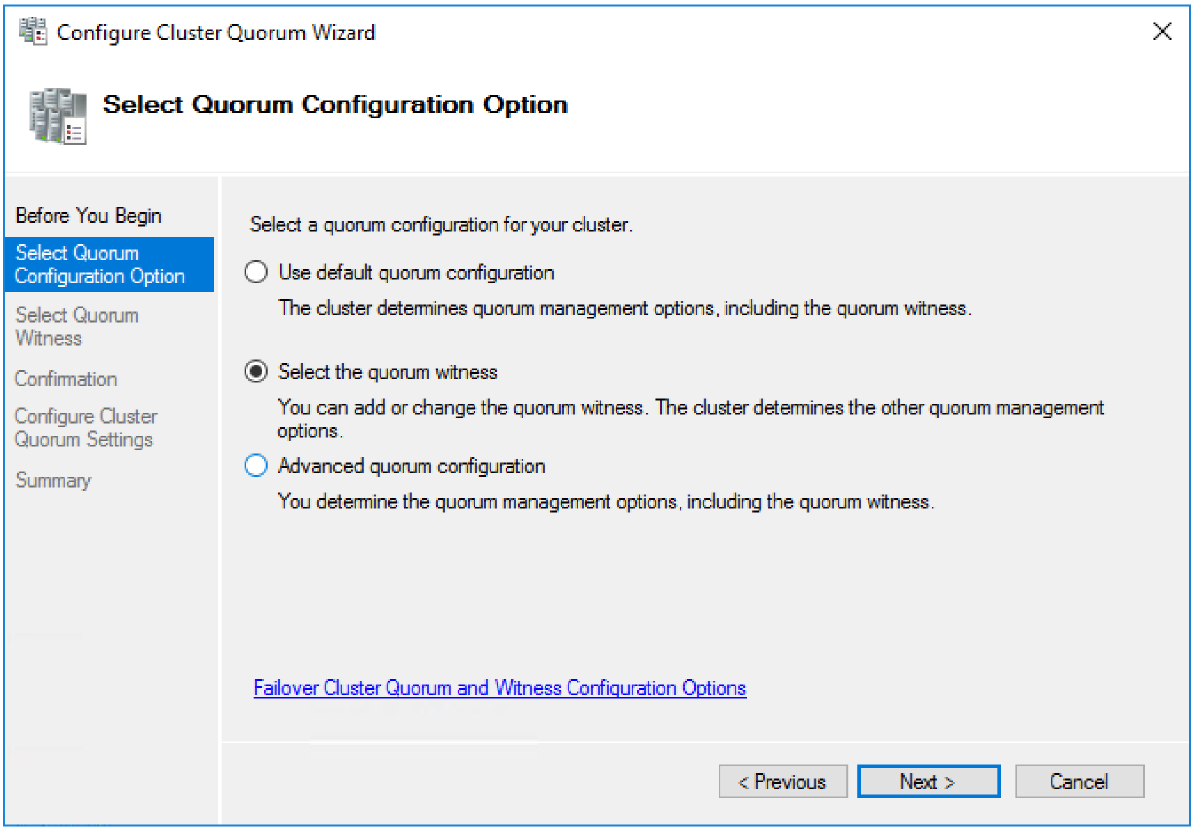
2. To configure the cluster witness disk, right-click on Cluster and proceed to More Actions -> Configure Cluster Quorum Settings.



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.

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.

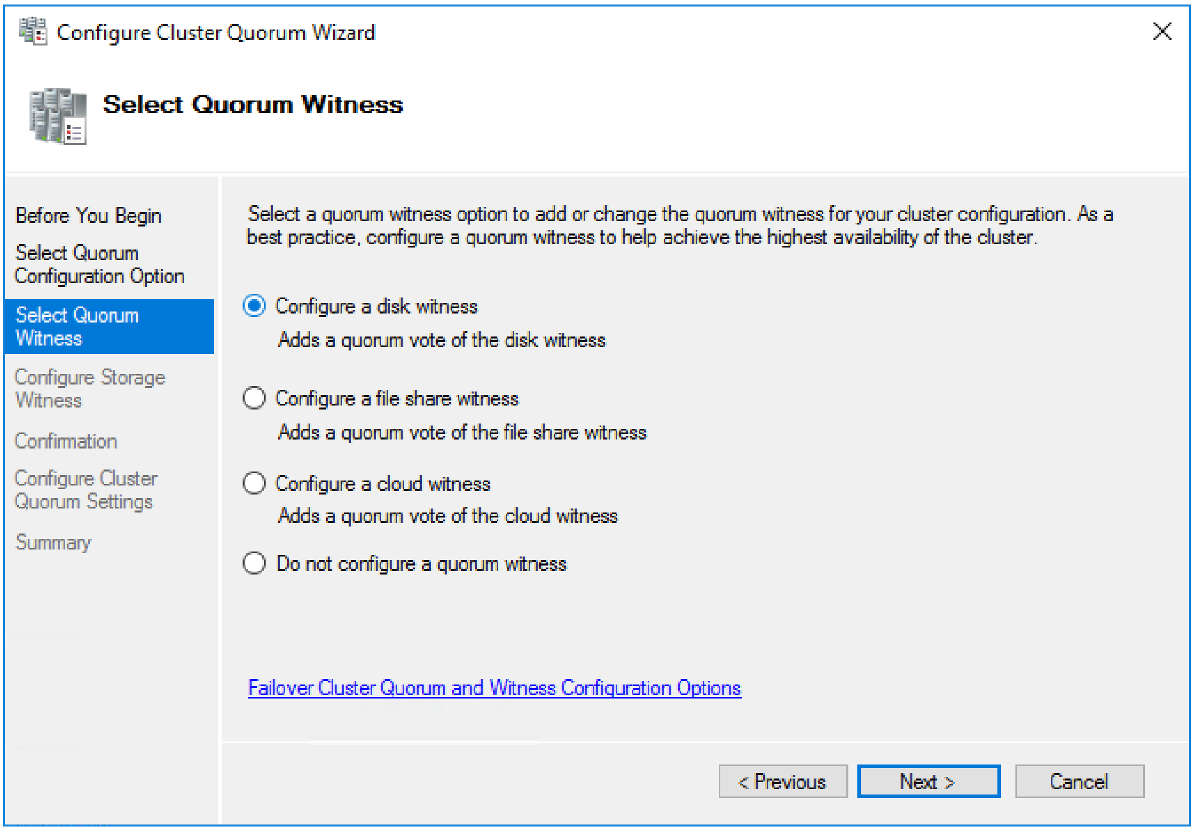
● Select the quorum witness

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.

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

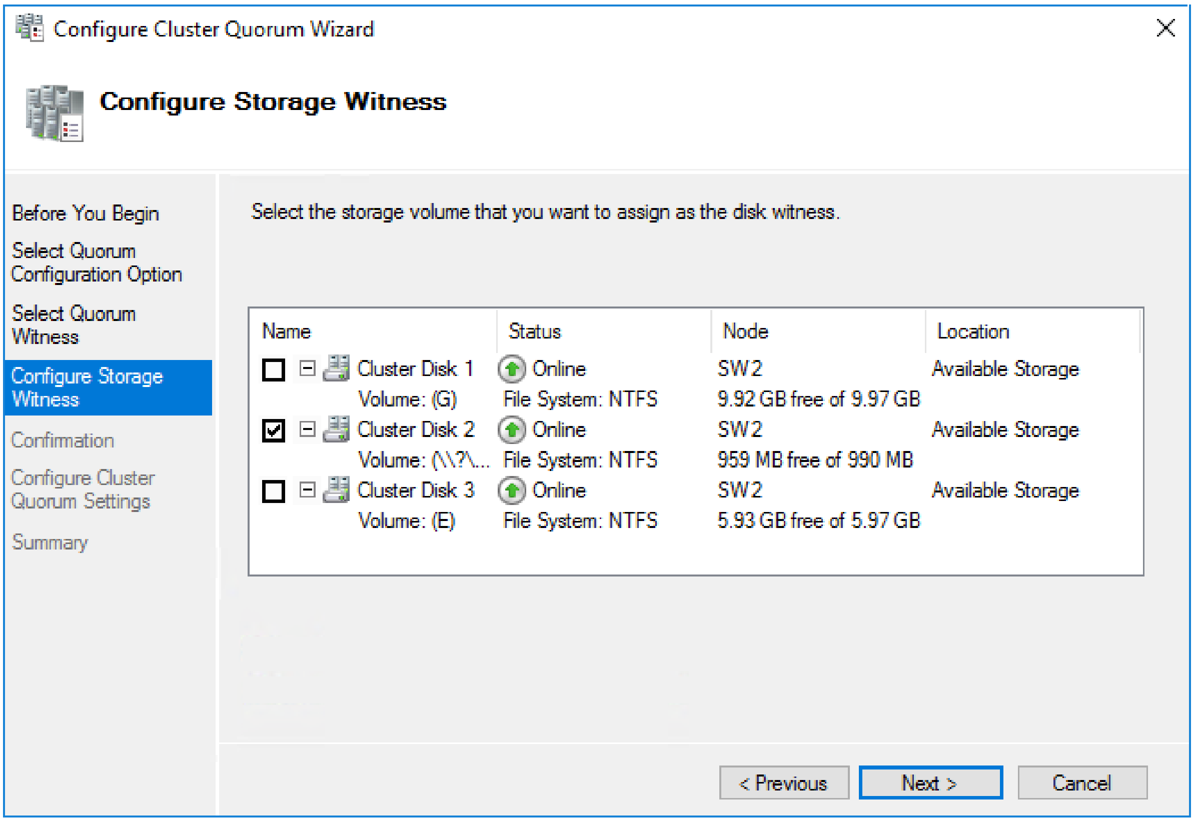
○ Configure a file share witness
Adds a quorum vote of the file share witness

○ 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.

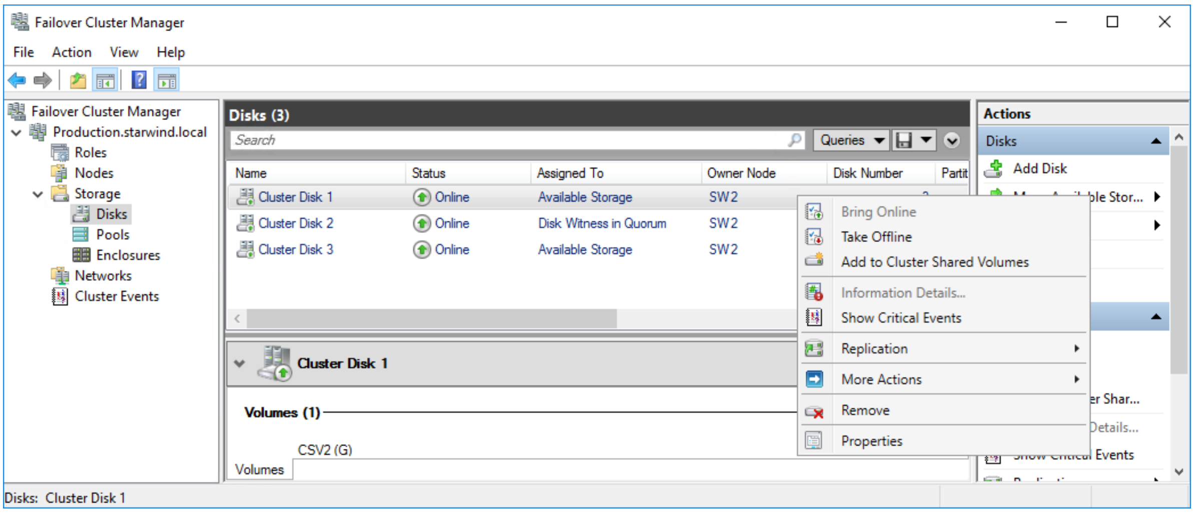

Configure Cluster Quorum Wizard
Before You Begin
Select Quorum Configuration Option
Select Quorum Witness
Configure Storage Witness
Confirmation
Configure Cluster Quorum Settings
Summary
< Previous
Next >
Cancel

Configure Storage Witness

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

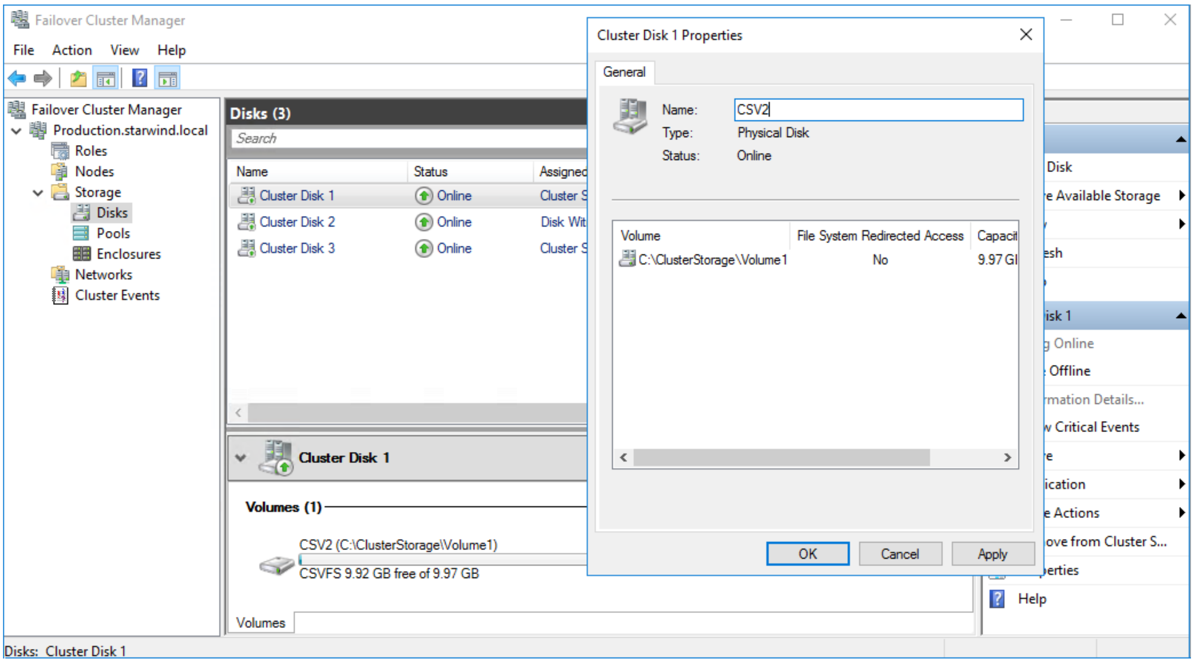
Name	Status	Node	Location
□ ⊟ Cluster Disk 1	Online	SW2	Available Storage
Volume: (G)	File System: NTFS	9.92 GB free of 9.97 GB	
☑ ⊟ Cluster Disk 2	Online	SW2	Available Storage
Volume: (\\?\...	File System: NTFS	959 MB free of 990 MB	
□ ⊟ Cluster Disk 3	Online	SW2	Available Storage
Volume: (E)	File System: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

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

Name: CSV2
Type: Physical Disk
Status: Online

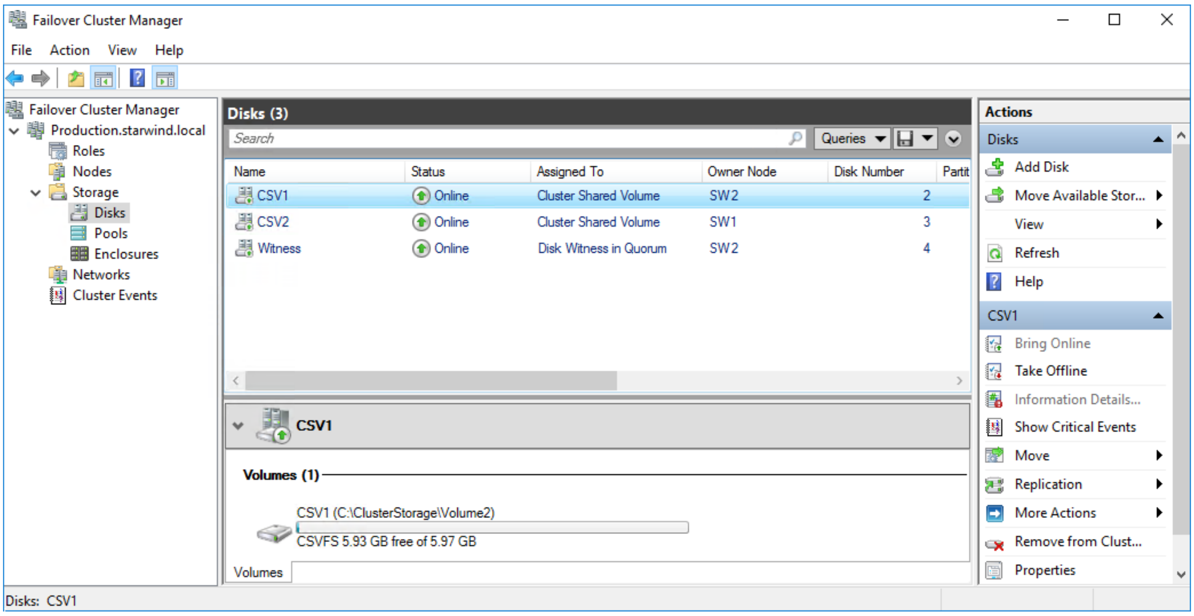
Volume	File System Redirected Access	Capaci
C:\ClusterStorage\Volume1	No	9.97 GI

Cluster Disk 1

Volumes (1)

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

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

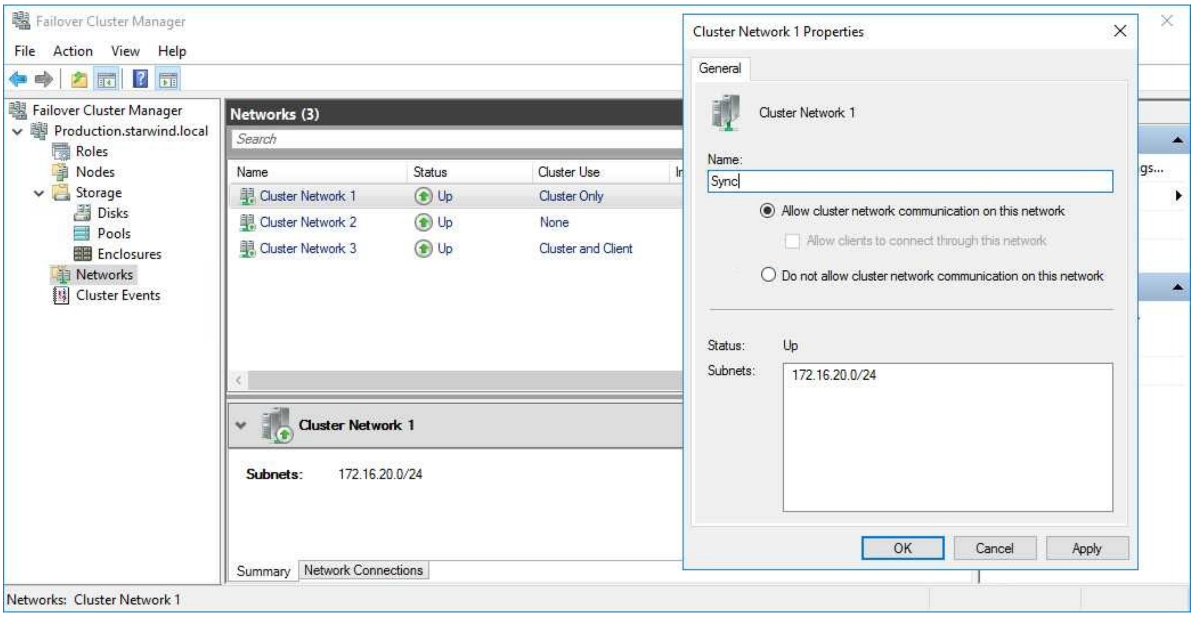
Volumes (1)

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

Networks: Cluster Network 1

Cluster Network 1 Properties

General

Cluster Network 1

Name: Sync

● Allow cluster network communication on this network

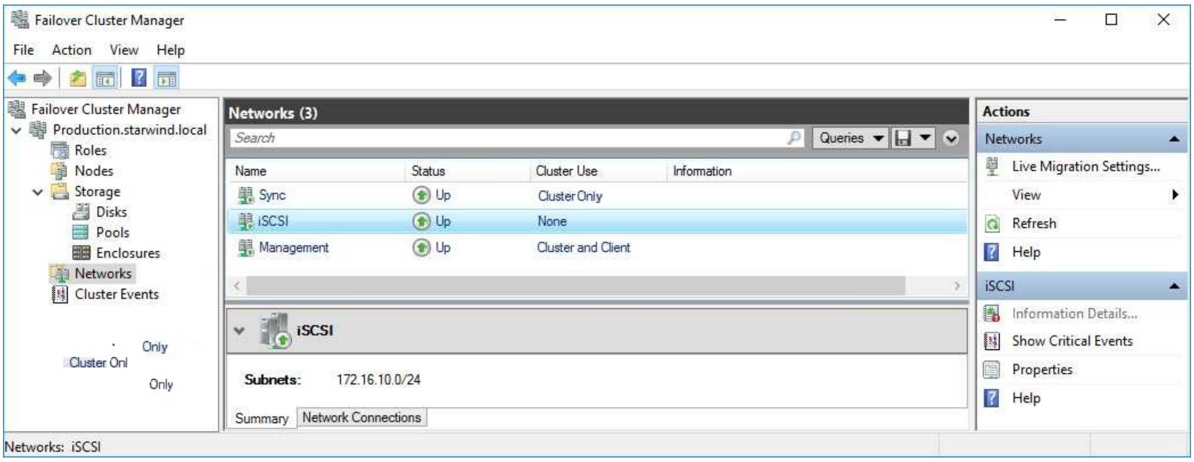
□ Allow clients to connect through this network

○ Do not allow cluster network communication on this network

Status: Up

Subnets: 172.16.20.0/24

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



Networks (3)

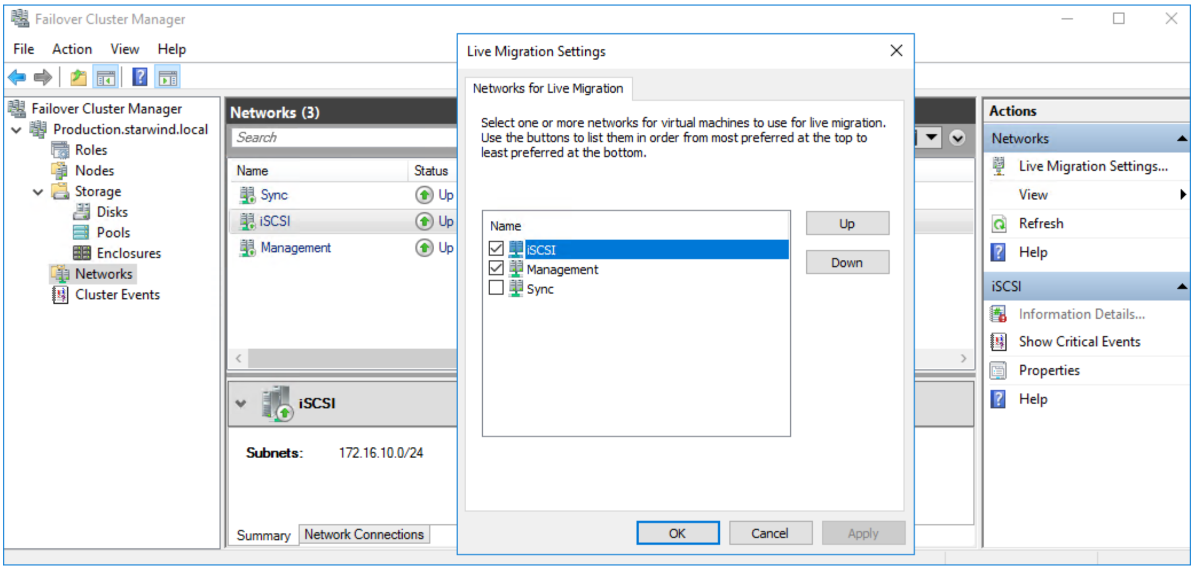
Name	Status	Cluster Use	Information
Sync	Up	Cluster Only	
iSCSI	Up	None	
Management	Up	Cluster and Client	

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.



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.

Name
☑ 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.

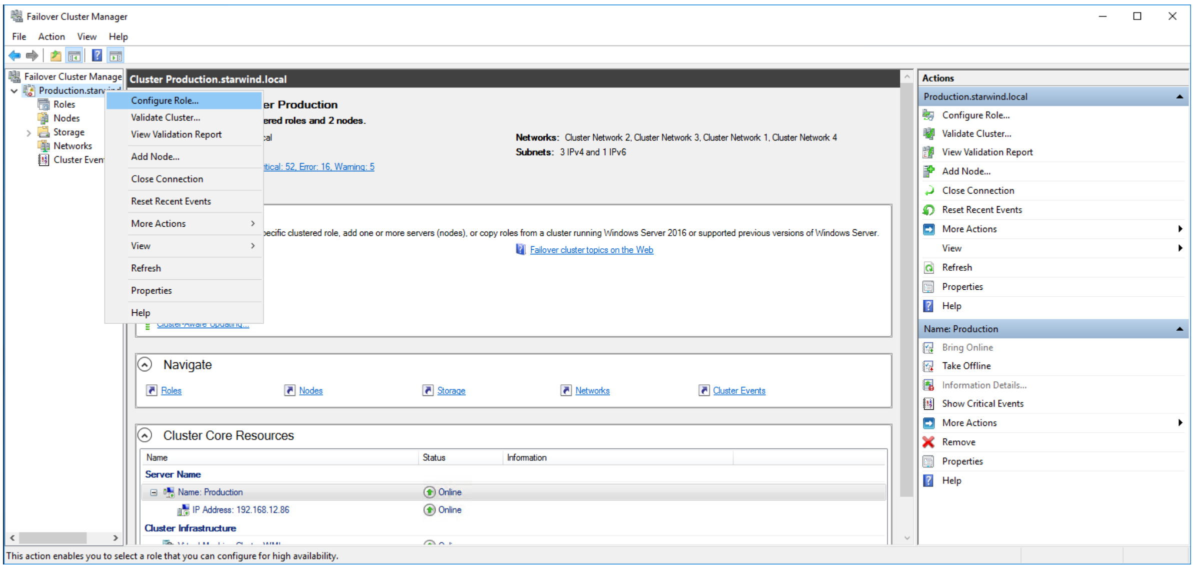
Configuring File Shares

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.

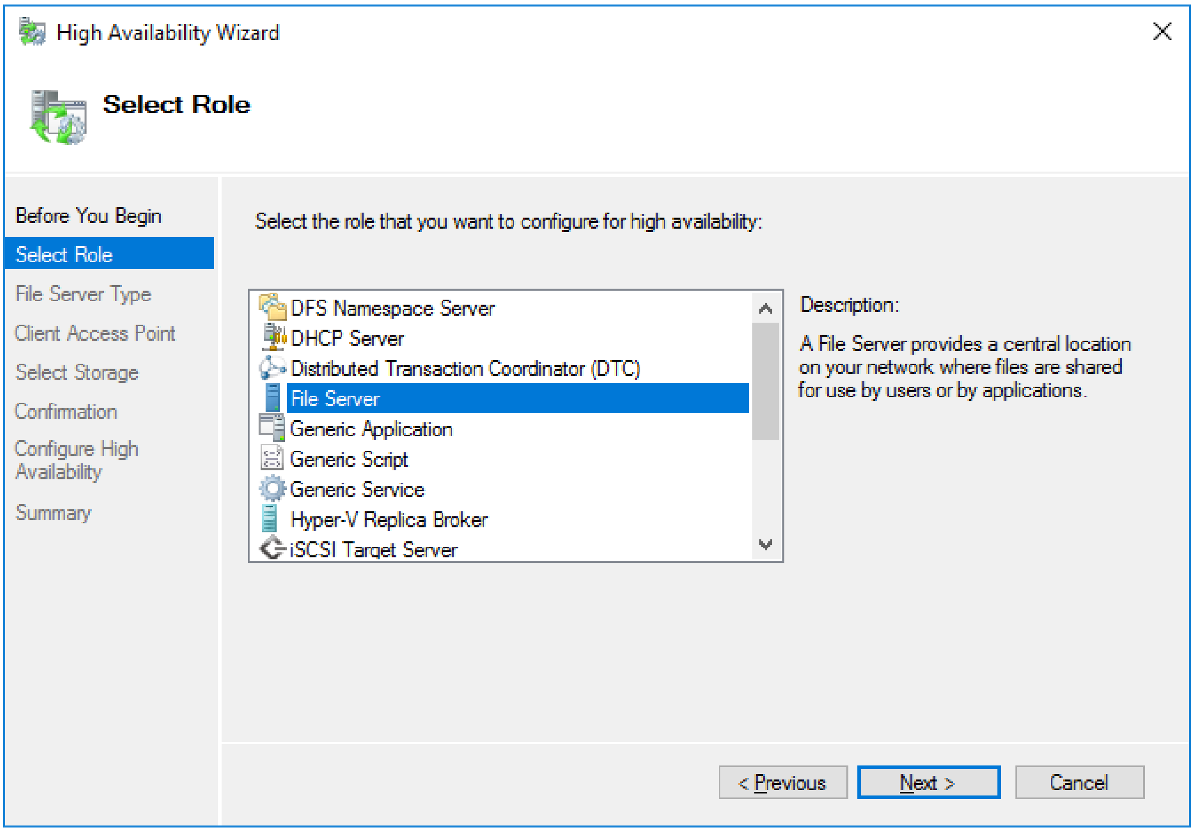


Networks: Cluster Network 2, Cluster Network 3, Cluster Network 1, Cluster Network 4
Subnets: 3 IPv4 and 1 IPv6

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.

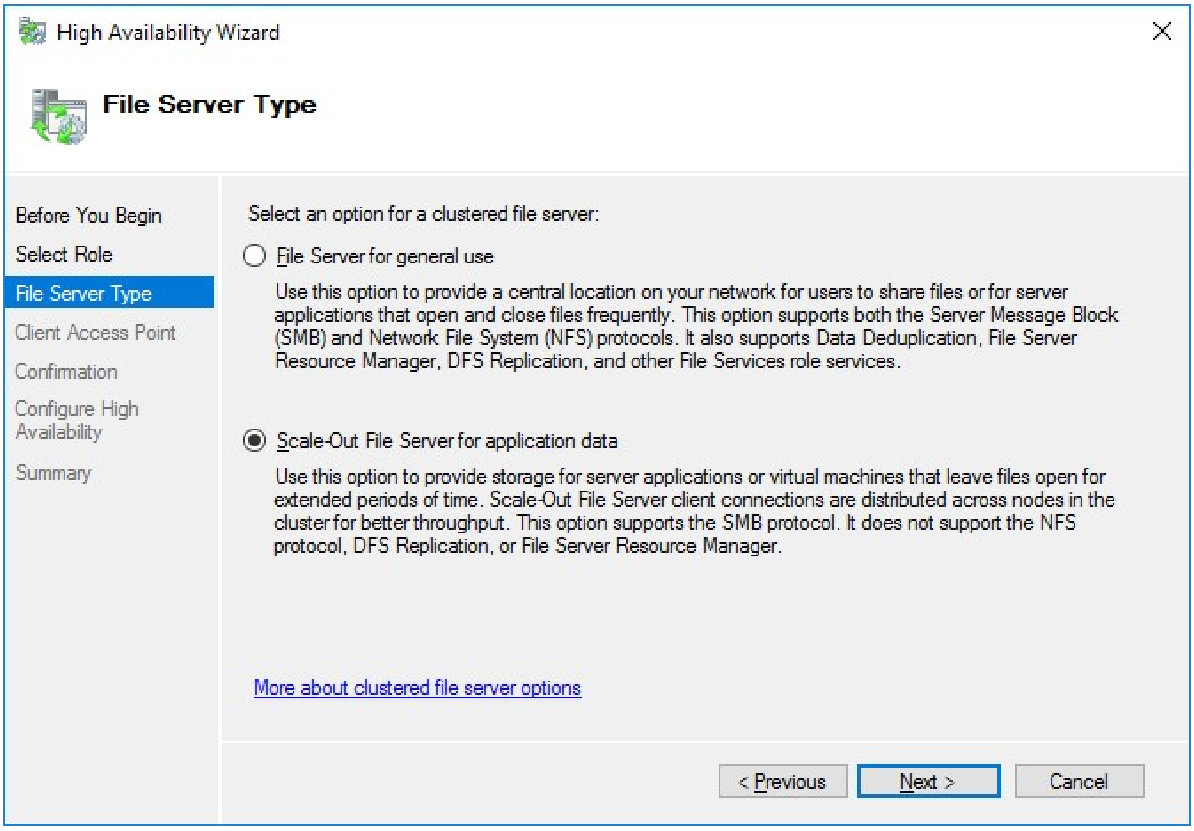


Select the role that you want to configure for high availability:

Description:

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.



Select an option for a clustered file server:

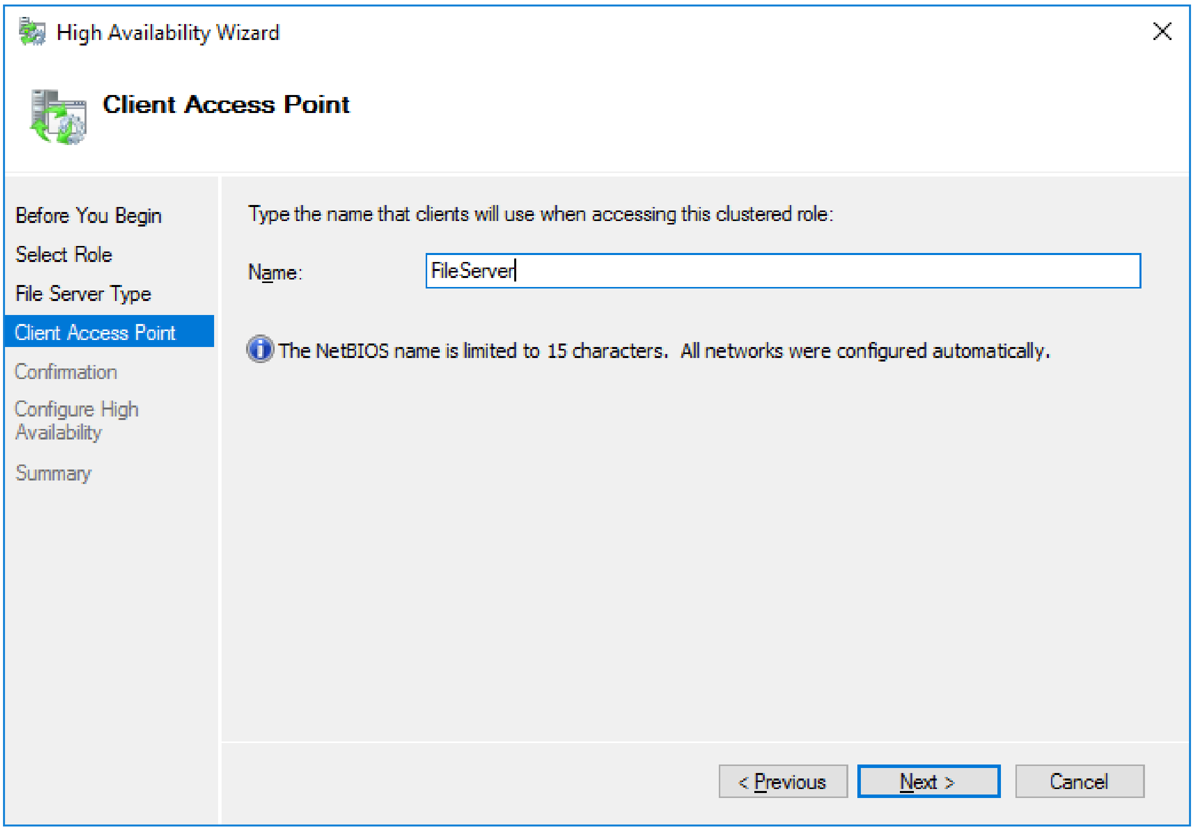
○ File Server for general use

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.



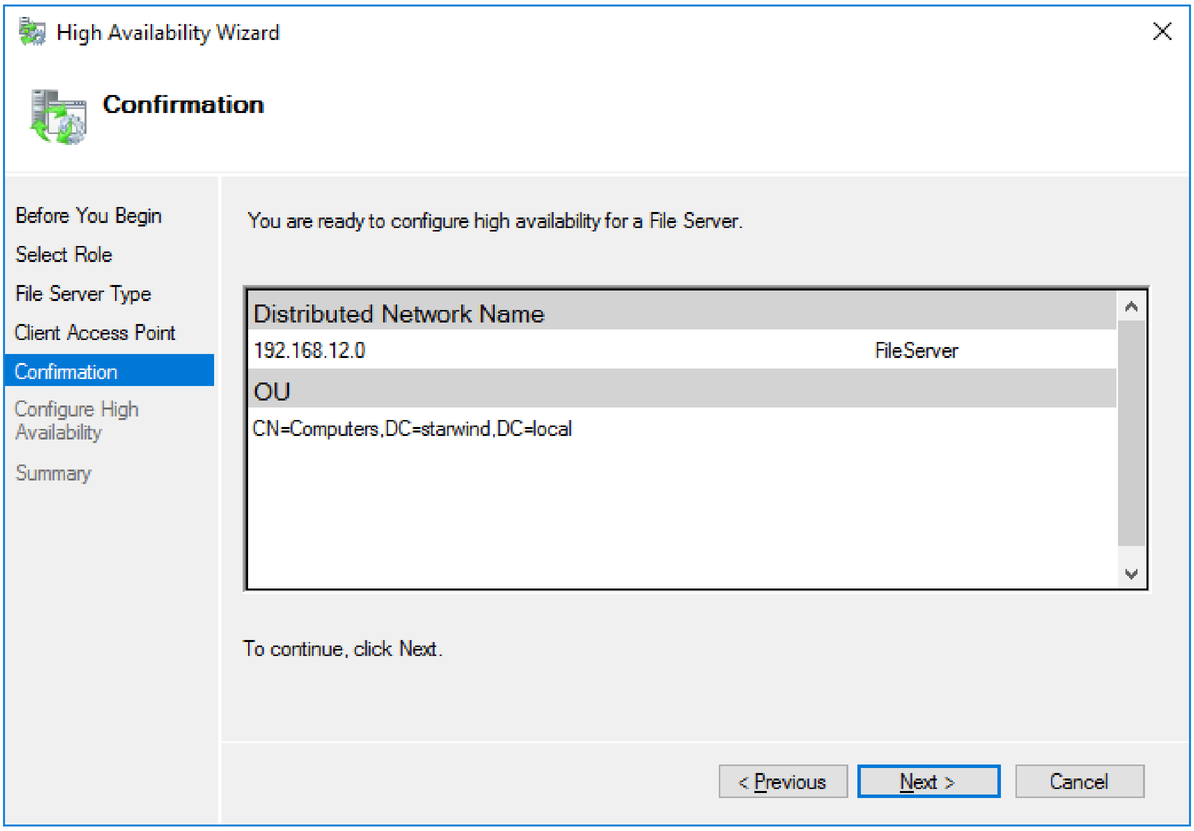
Type the name that clients will use when accessing this clustered role:

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.

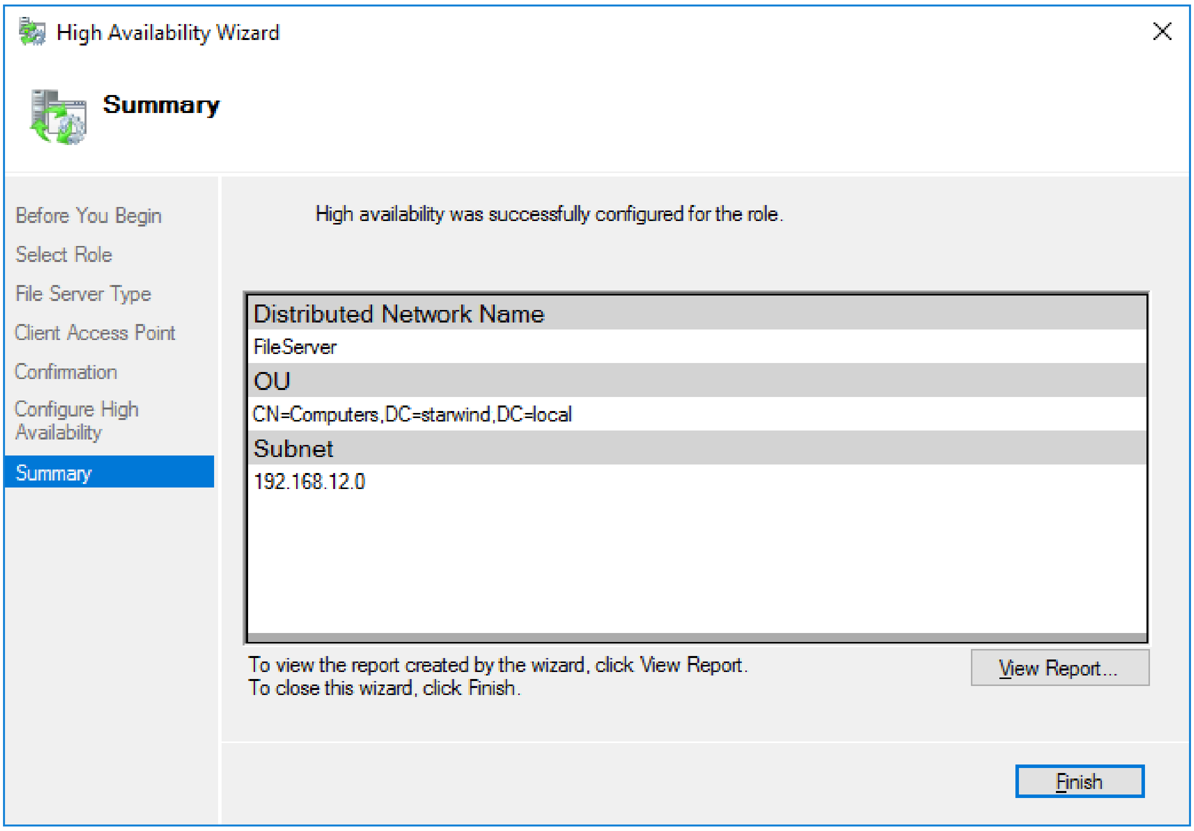


You are ready to configure high availability for a File Server.

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.

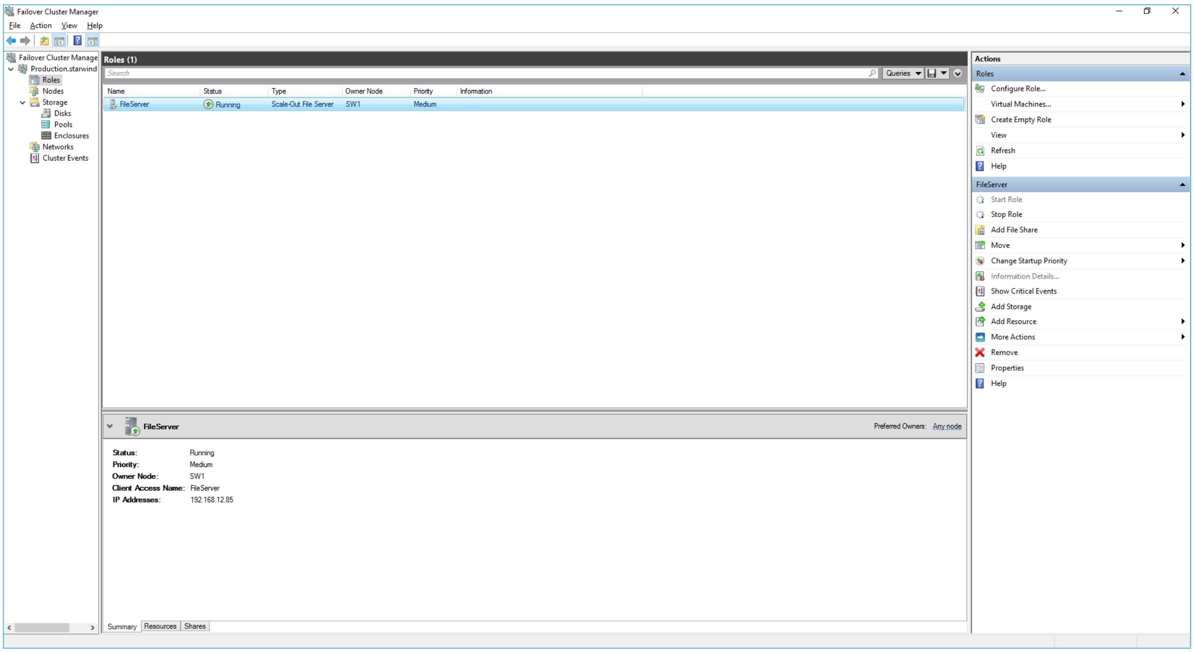


High availability was successfully configured for the role.

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.

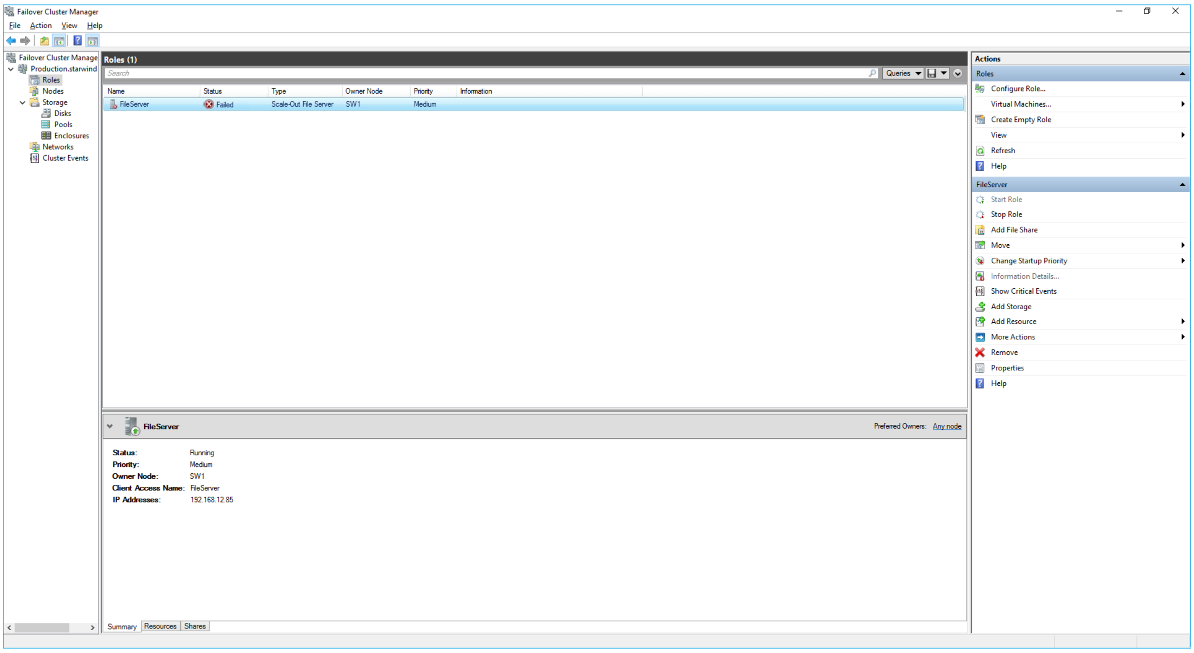


Name	Status	Type	Owner Node	Priority	Information
FileServer	Running	Scale-Out File Server	SW1	Medium	

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:



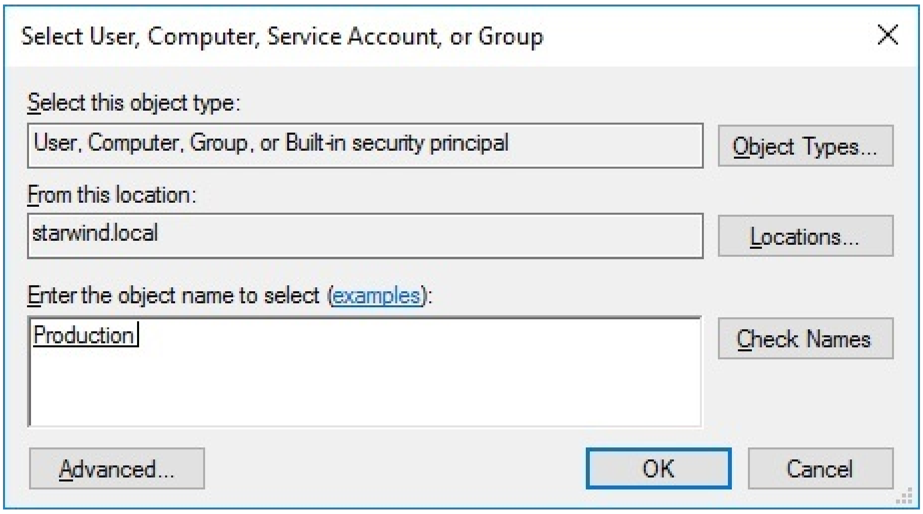
Roles (1)

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)

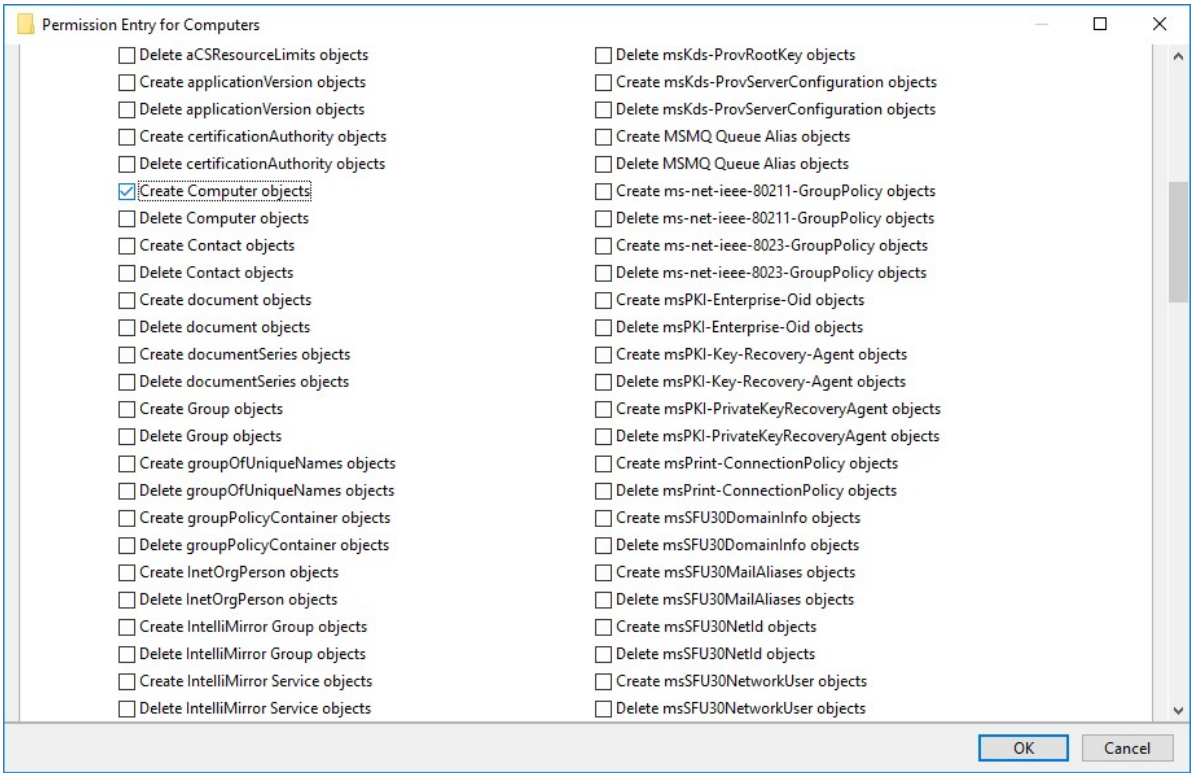


Select this object type:
User, Computer, Group, or Built-in security principal

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

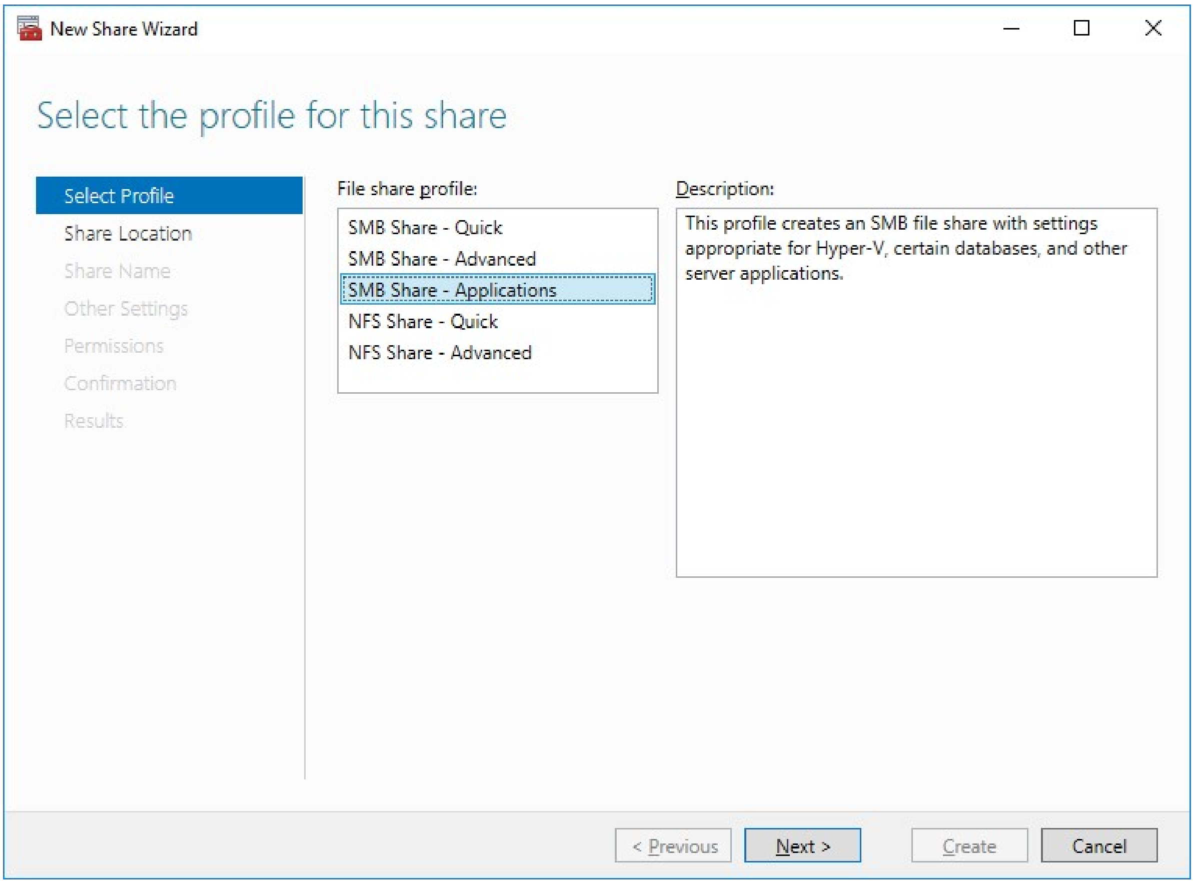
□ Delete msKds-ProvRootKey objects
□ Create msKds-ProvServerConfiguration objects
□ Delete msKds-ProvServerConfiguration objects
□ Create MSMQ Queue Alias objects
□ Delete MSMQ Queue Alias objects
□ Create ms-net-ieee-80211-GroupPolicy objects
□ Delete ms-net-ieee-80211-GroupPolicy objects
□ Create ms-net-ieee-8023-GroupPolicy 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



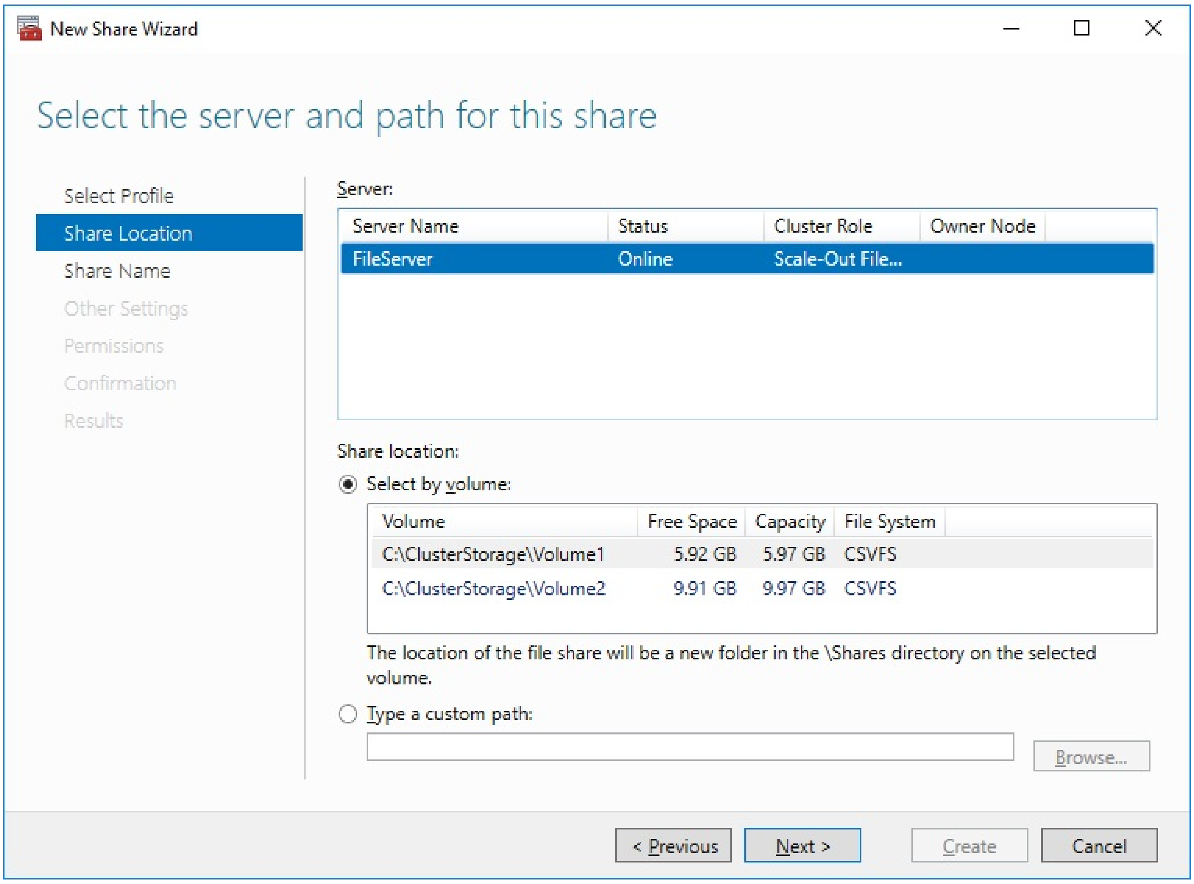
File share profile:

- SMB Share - Quick
- SMB Share - Advanced
- SMB Share - Applications
- NFS Share - Quick
- NFS Share - Advanced

Description:

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.



Server:

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

Share location:

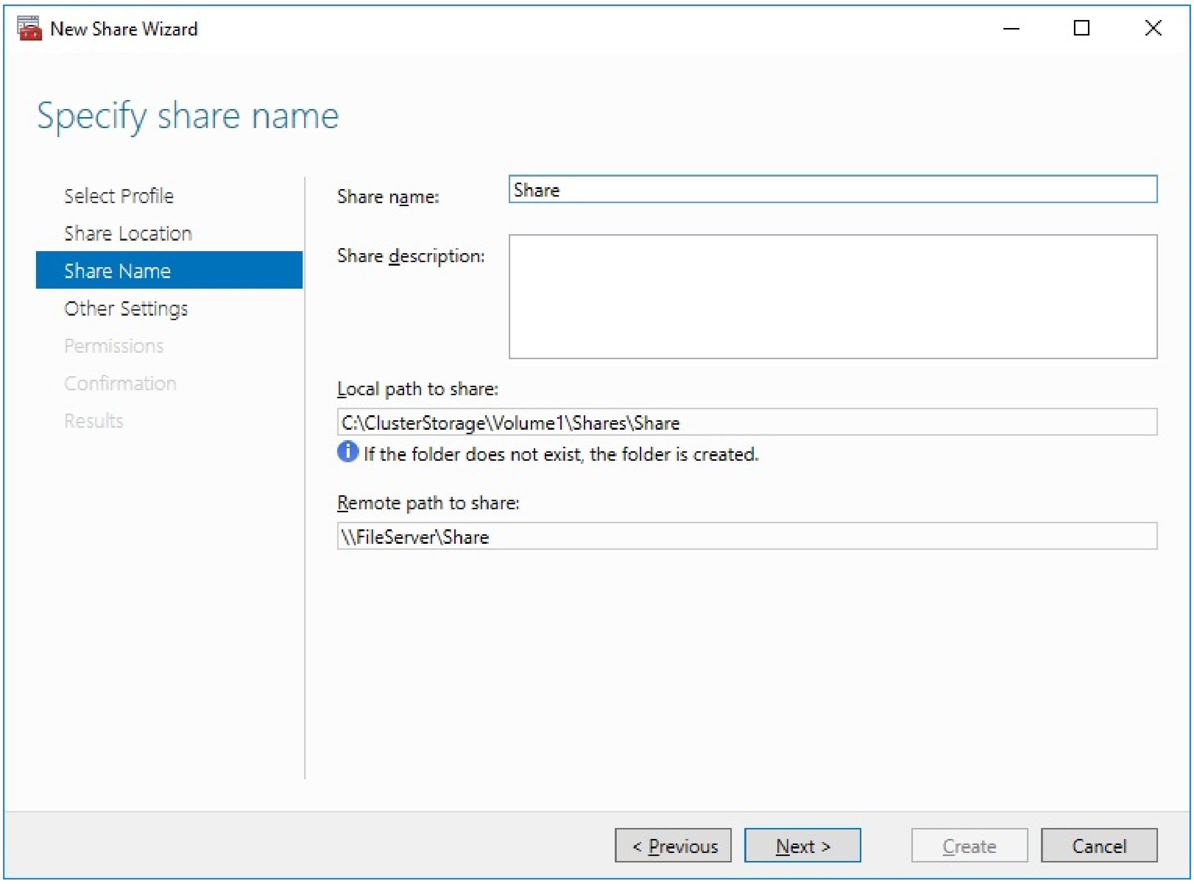
● Select by volume:

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

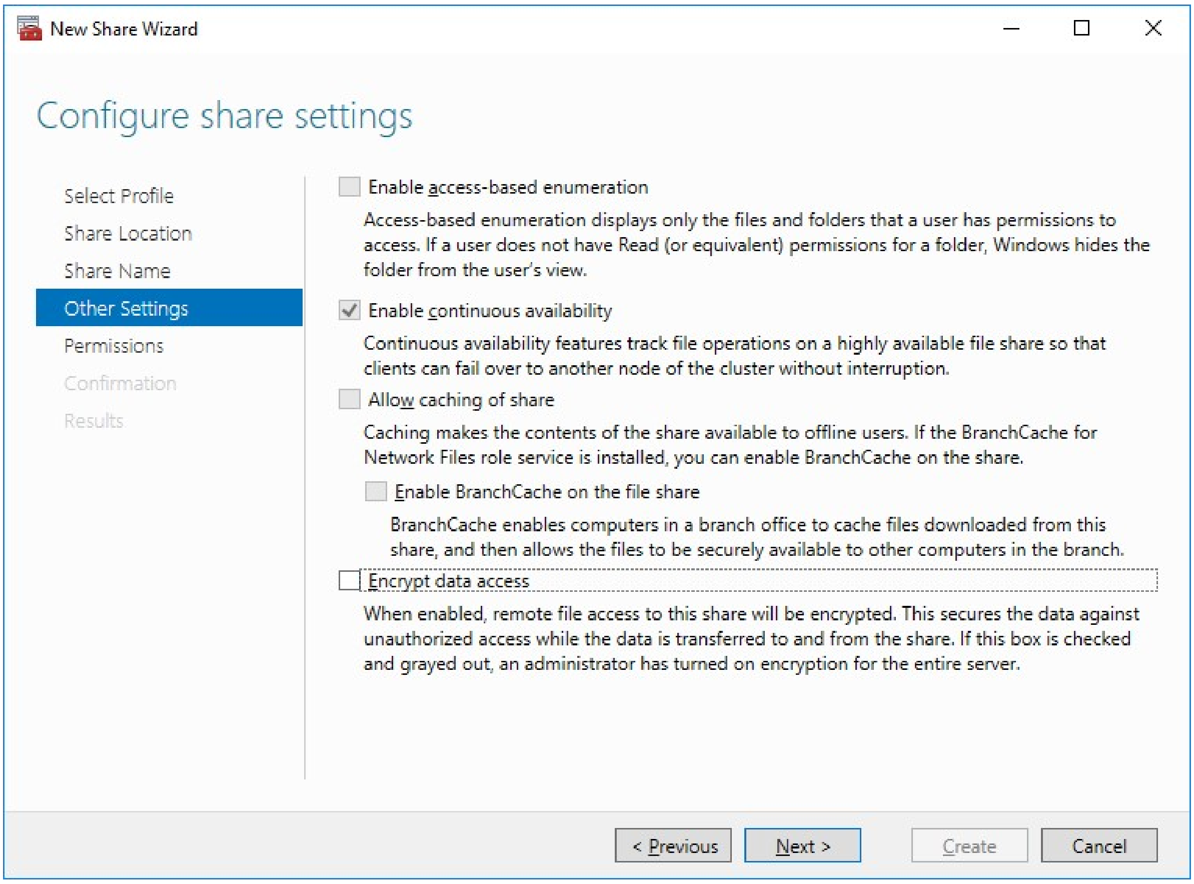
Share description:

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.



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.

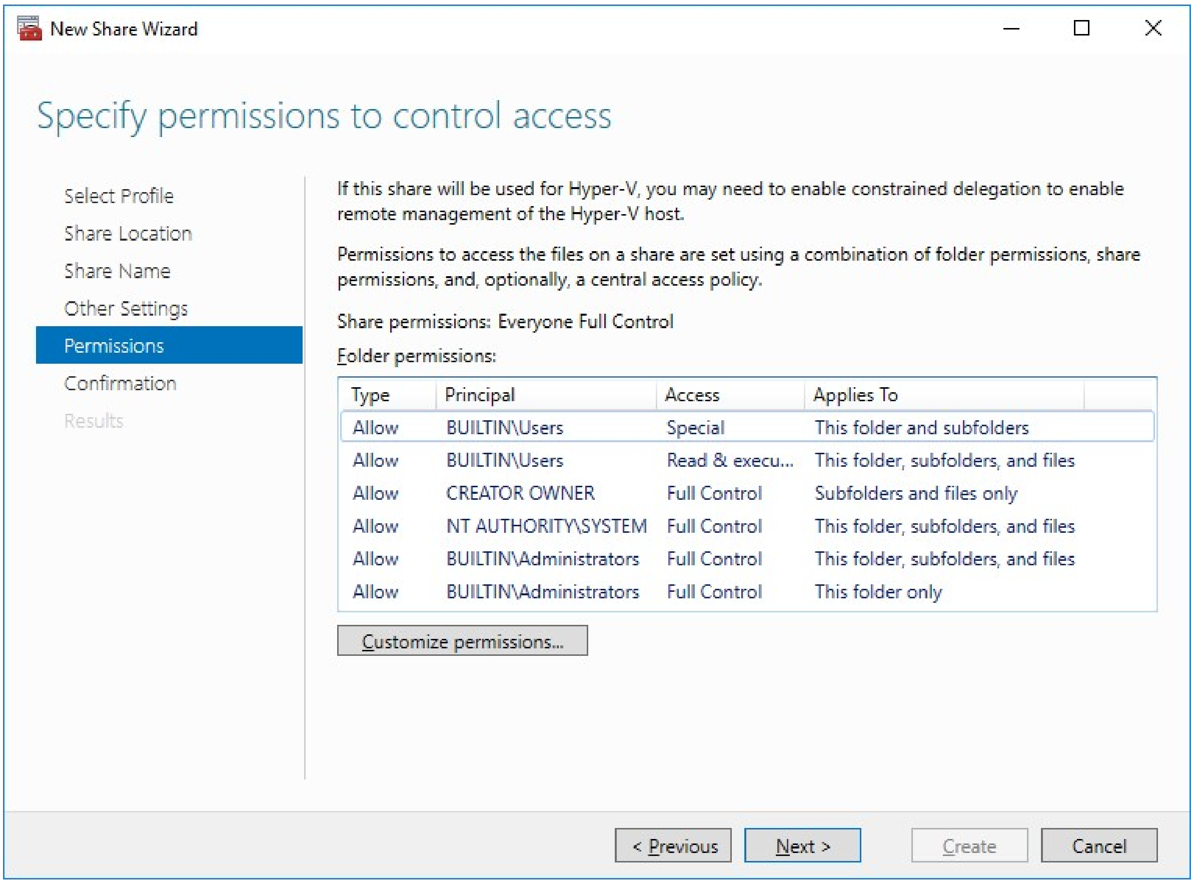
□ Enable BranchCache on the file share

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

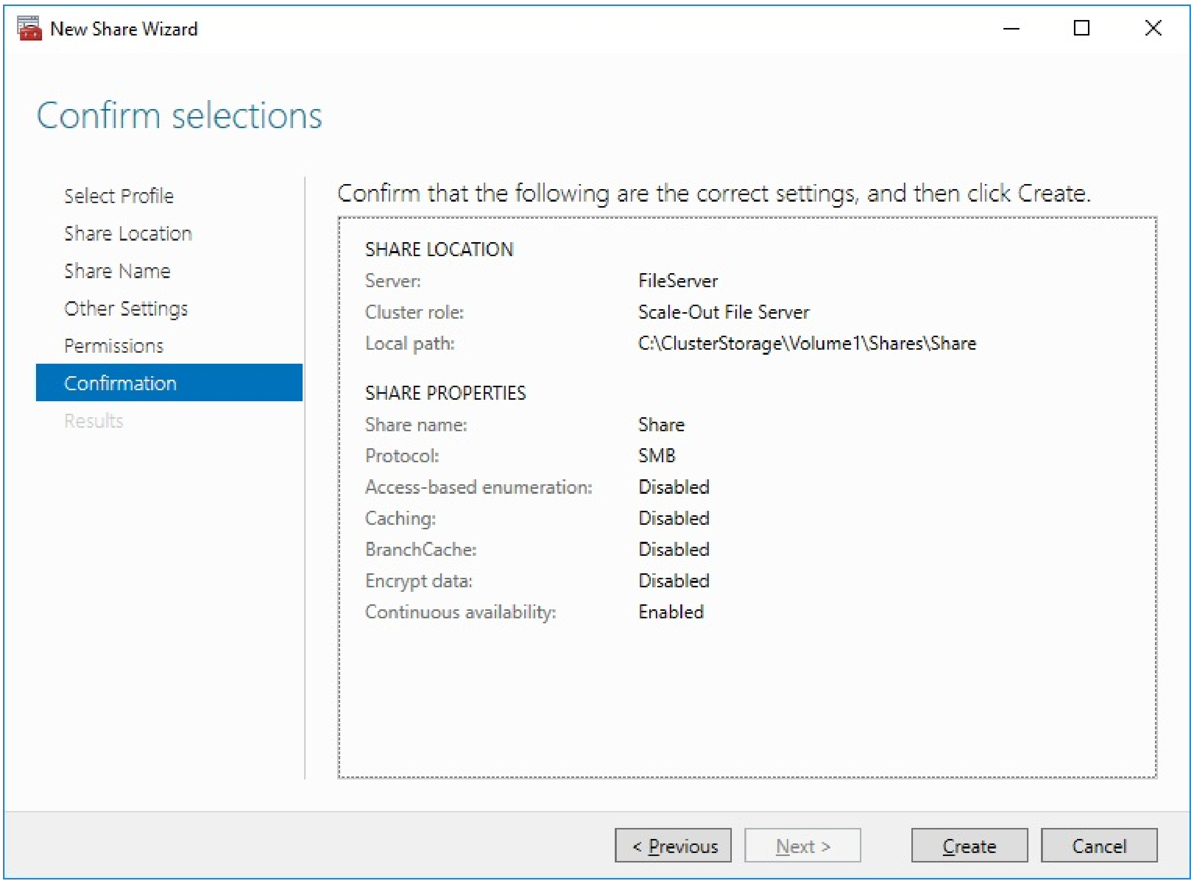
Folder permissions:

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.

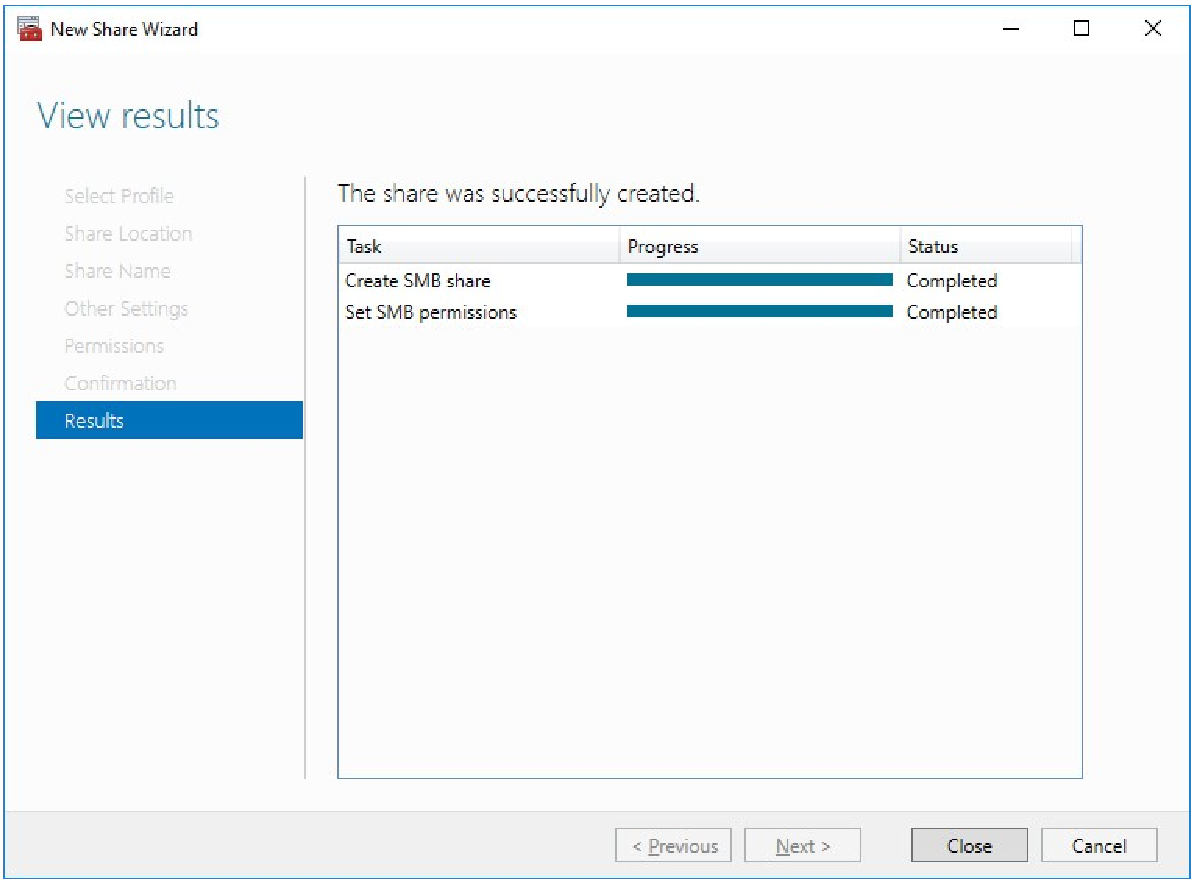
SHARE LOCATION

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.

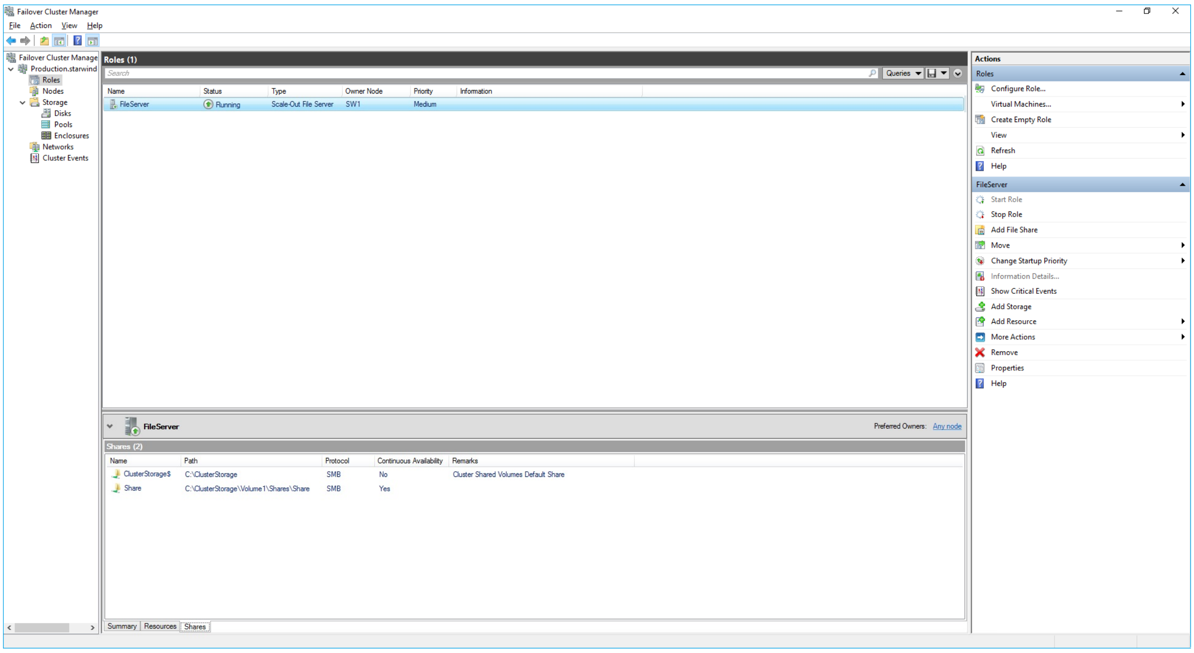


The share was successfully created.

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:



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

Shares (2)

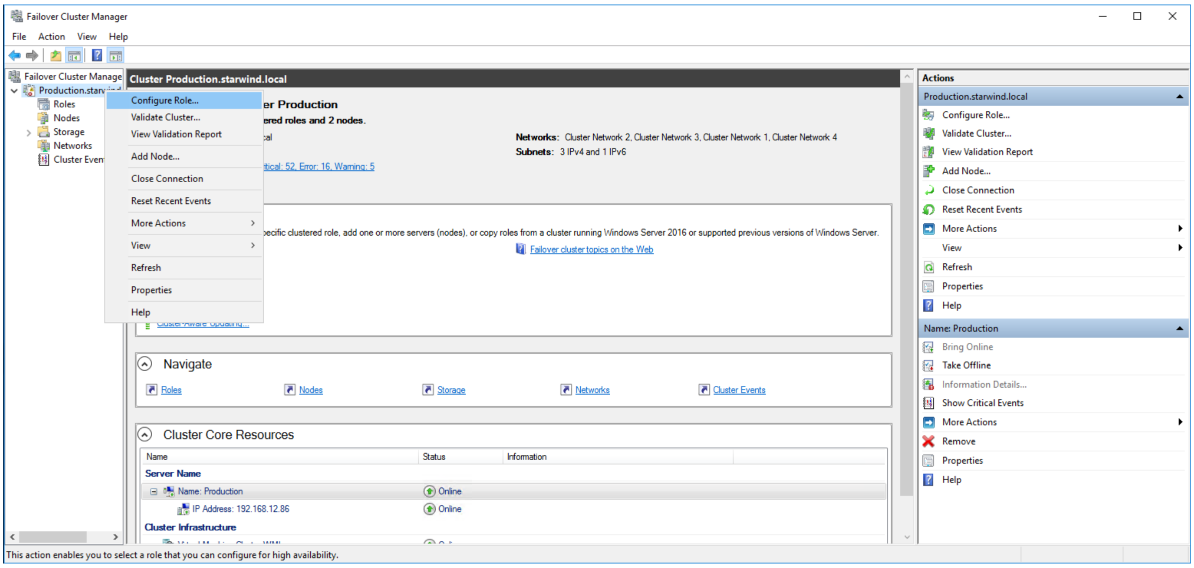
Name	Path	Protocol	Continuous Availability	Remarks
ClusterStorage$	C:\ClusterStorage	SMB	No	Cluster Shared Volumes Default Share
Share	C:\ClusterStorage\Volume1\Shares\Share	SMB	Yes	

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.



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

tical: 52, Error: 16, Warning: 5

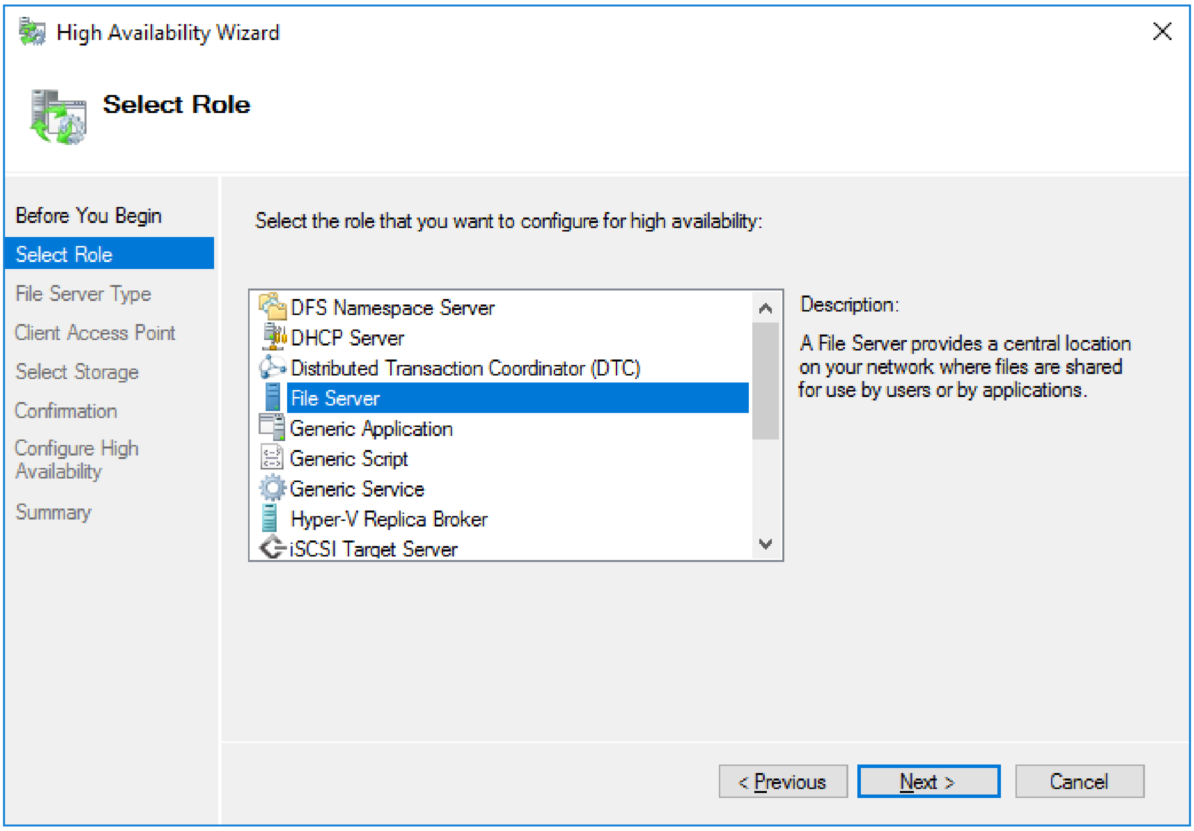
pecific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2016 or supported previous versions of Windows Server.

Failover cluster topics on the Web

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.



High Availability Wizard

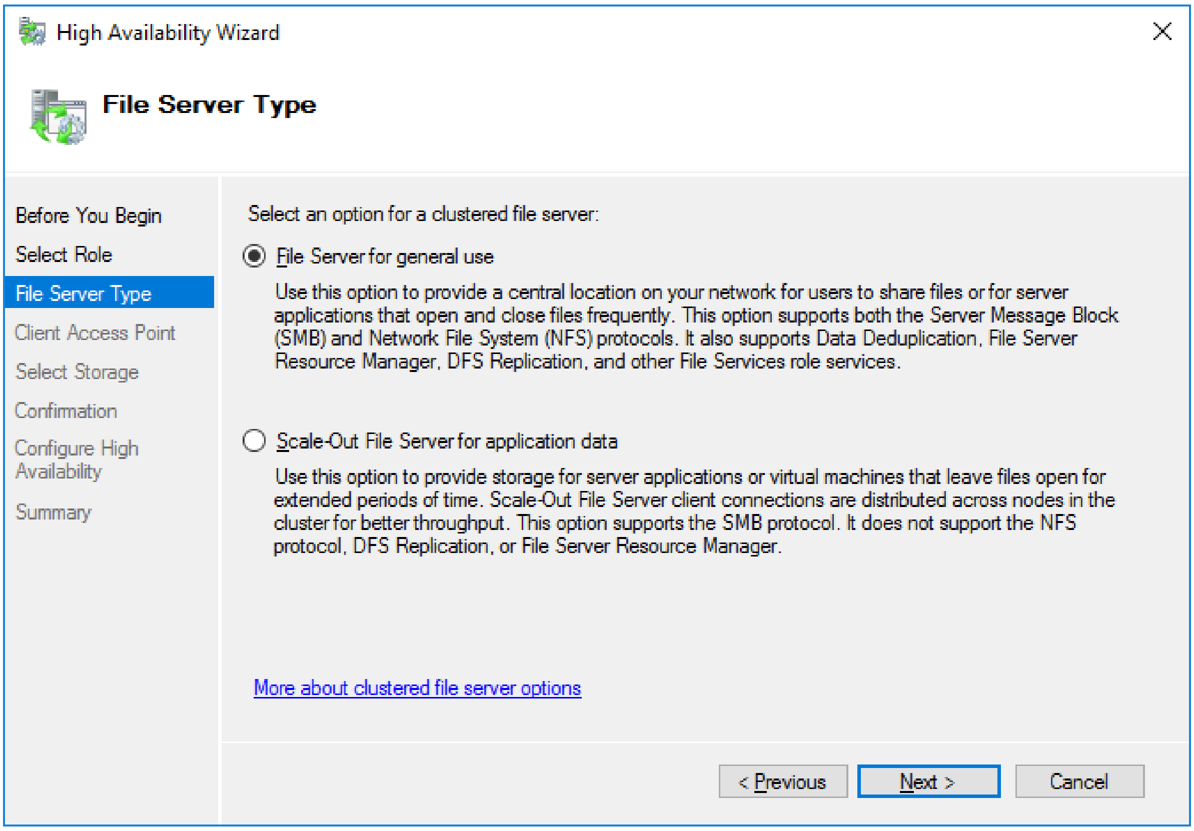
Select Role

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

Description:

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

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



Select an option for a clustered file server:

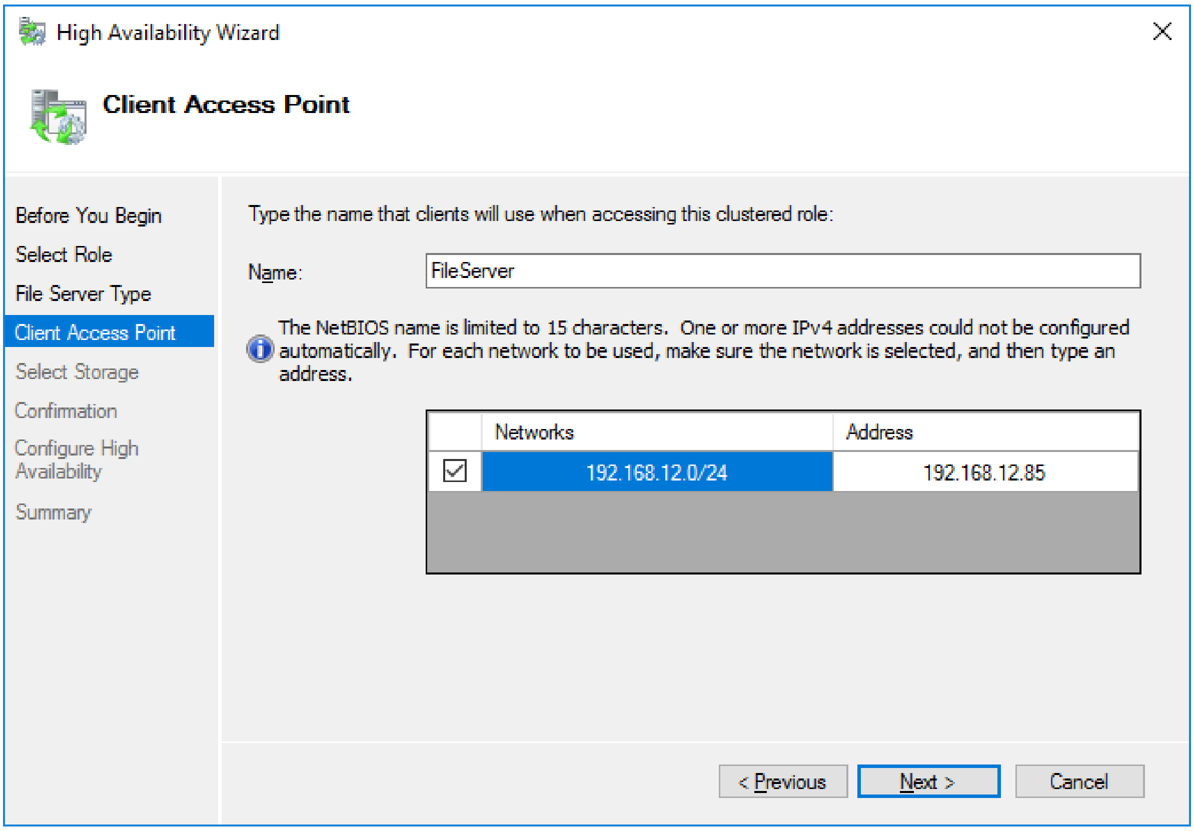
● File Server for general use

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.



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

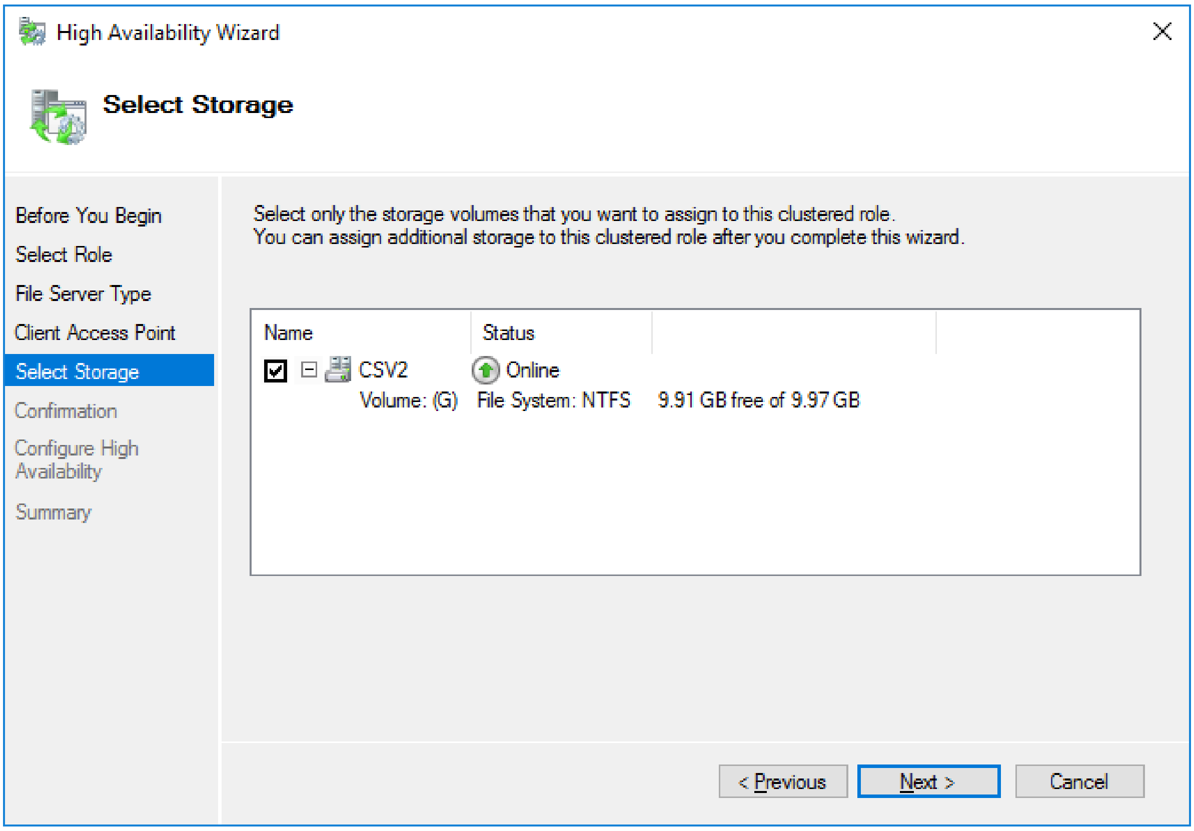
Name: FileServer

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.

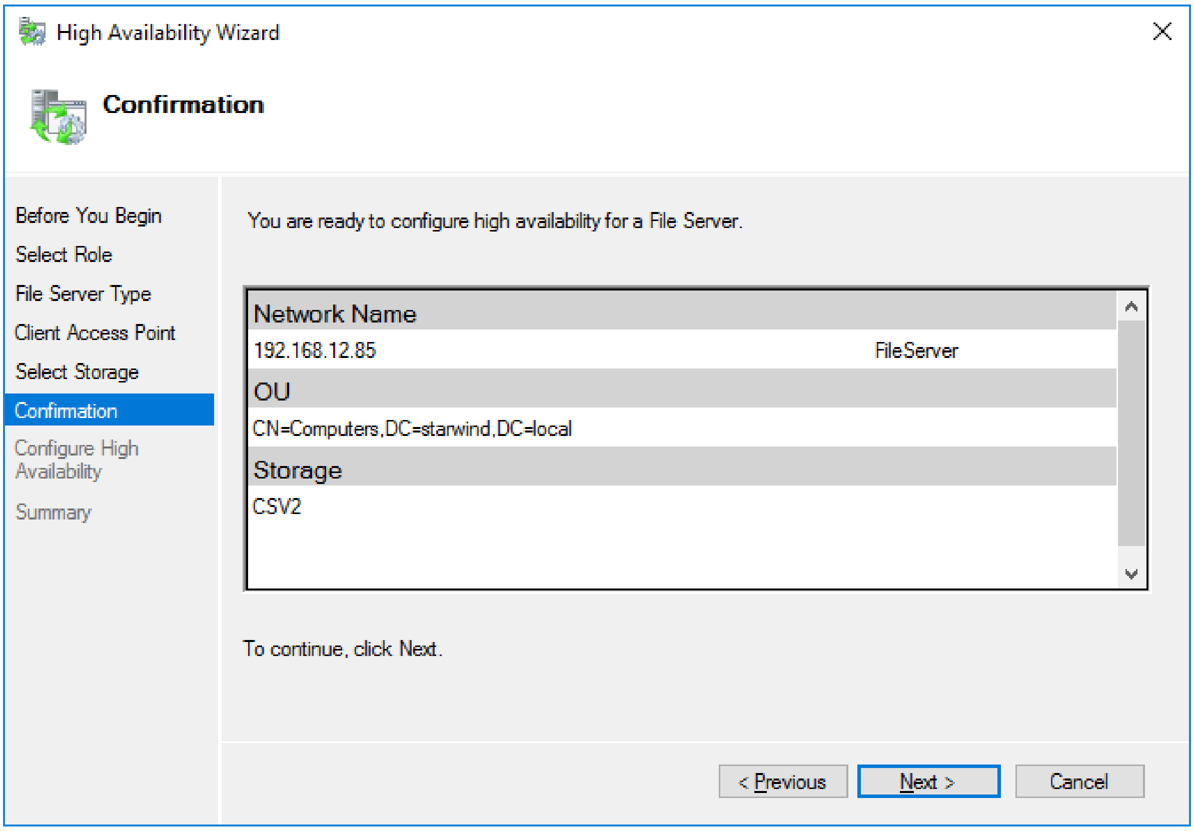
6. Select the Cluster disk and click Next.



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.



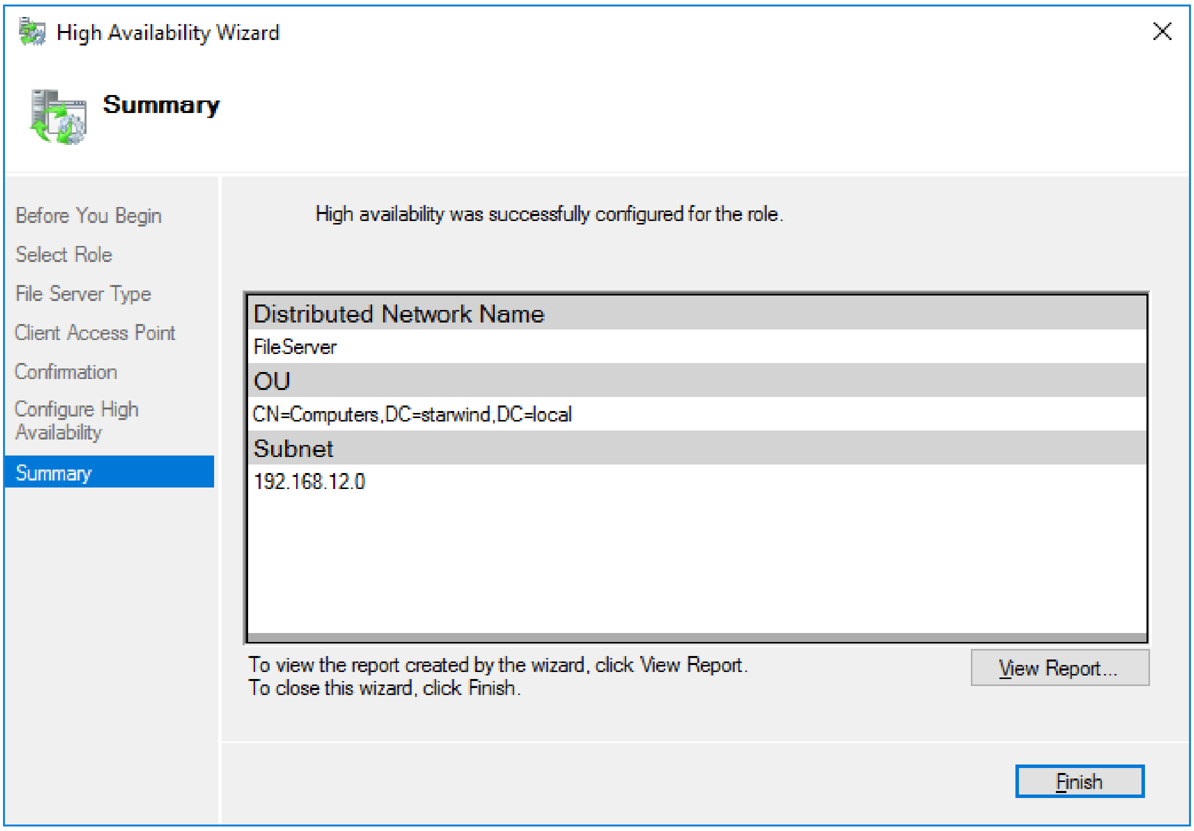
You are ready to configure high availability for a File Server.

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.

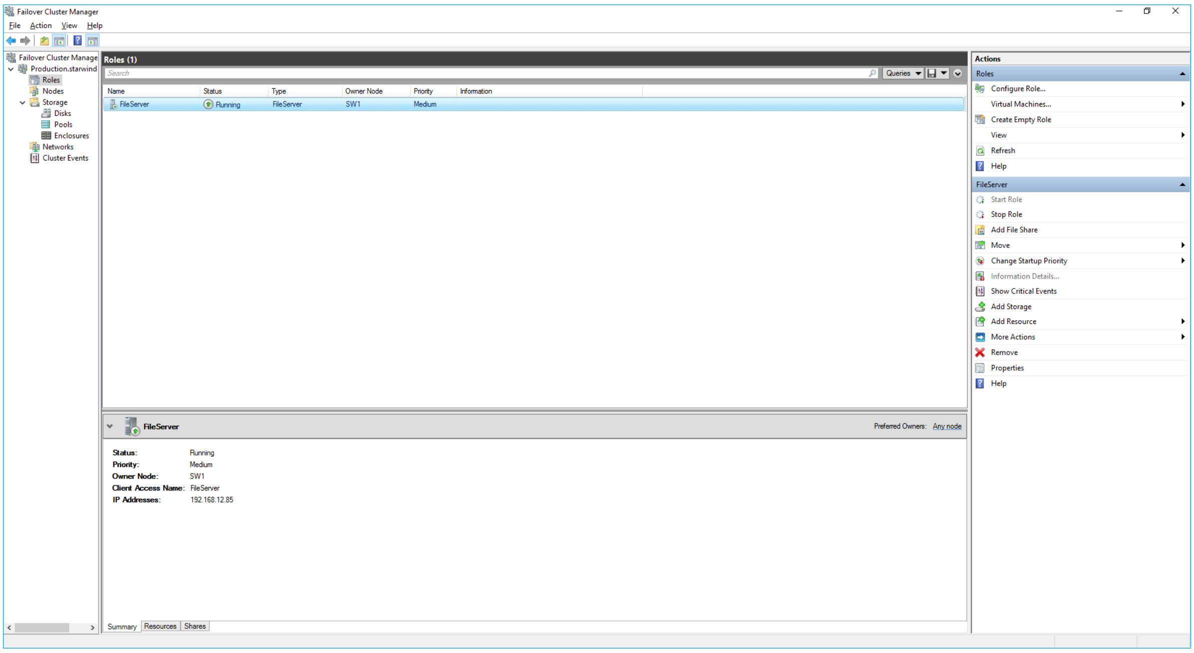


High availability was successfully configured for the role.

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	

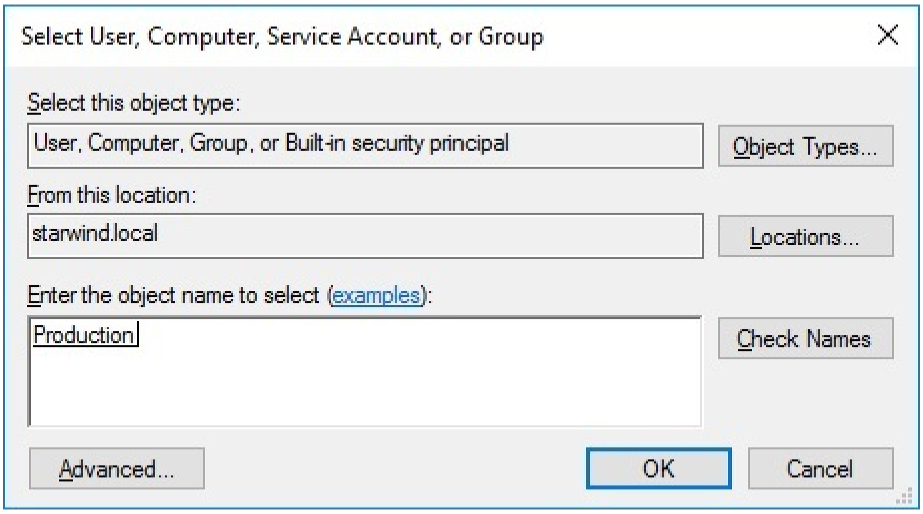
FileServer — Preferred Owners: Any node

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)

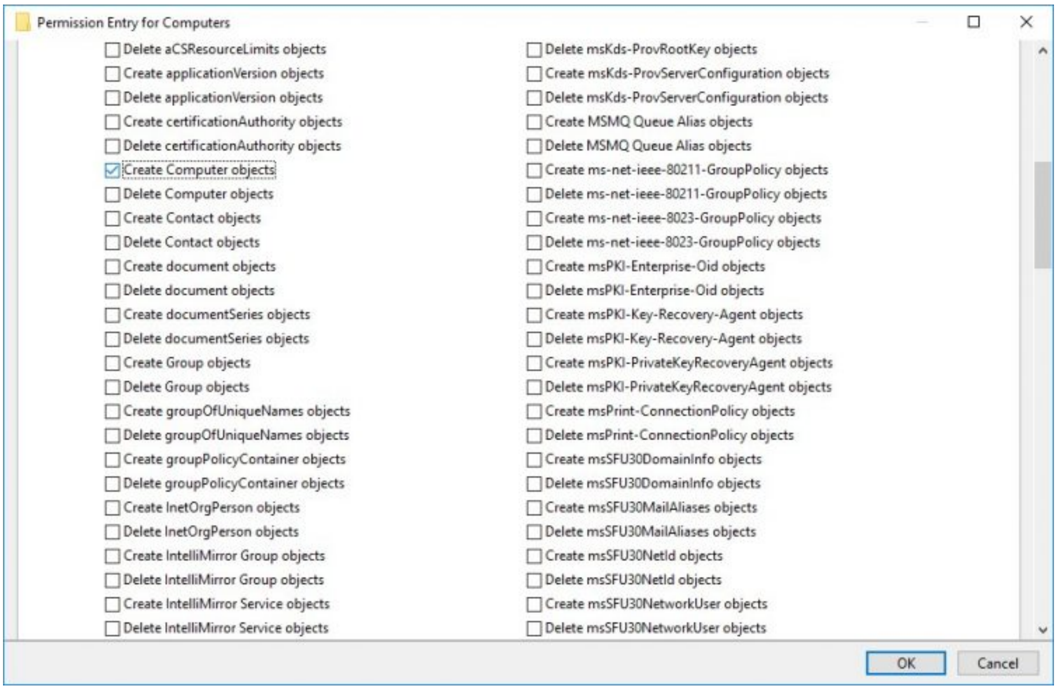


Select this object type:
User, Computer, Group, or Built-in security principal

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



□ 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

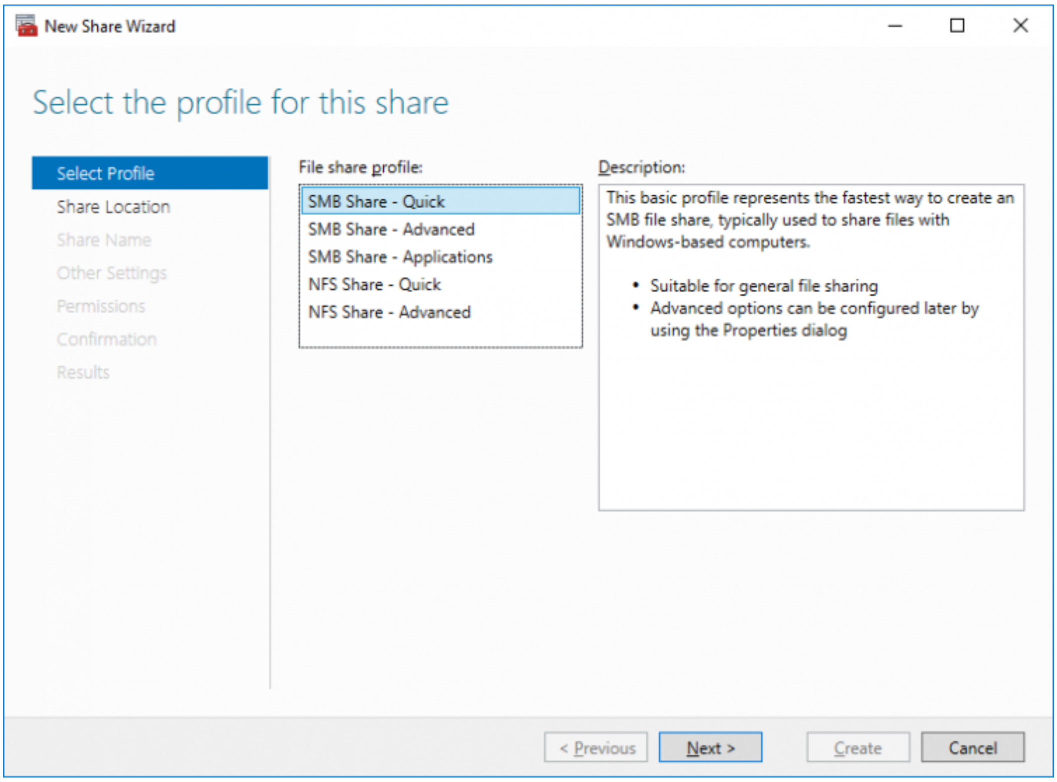
To Add SMB File Share

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:

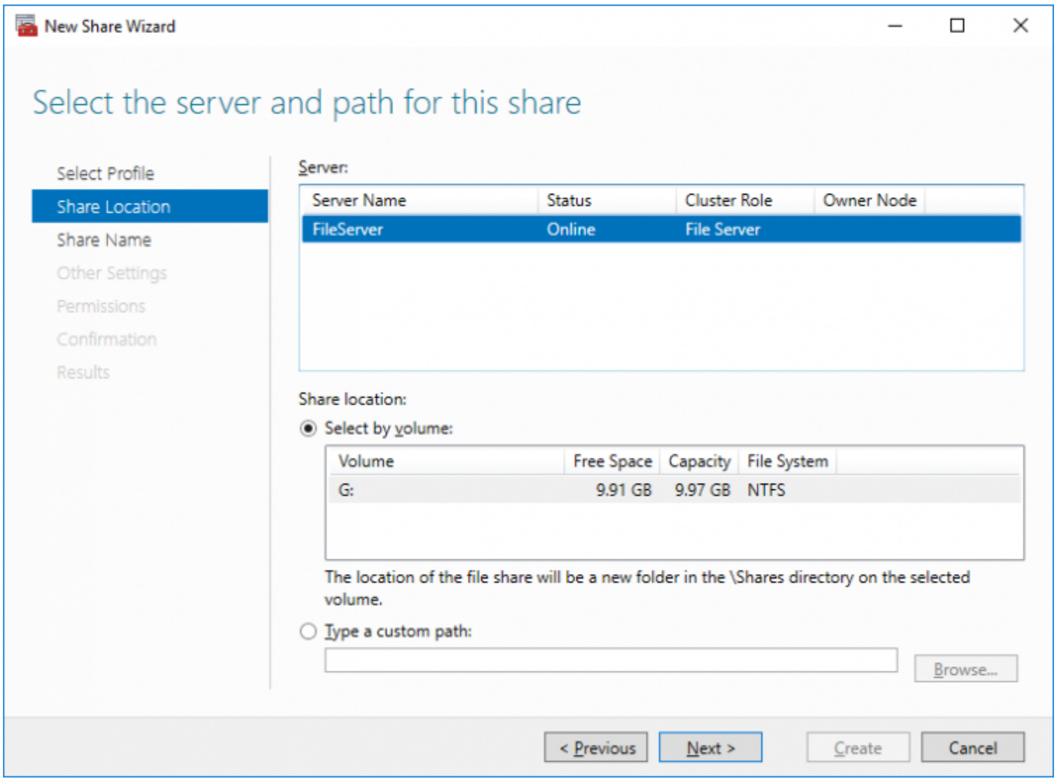
- SMB Share - Quick
- SMB Share - Advanced
- SMB Share - Applications
- NFS Share - Quick
- NFS Share - Advanced

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:

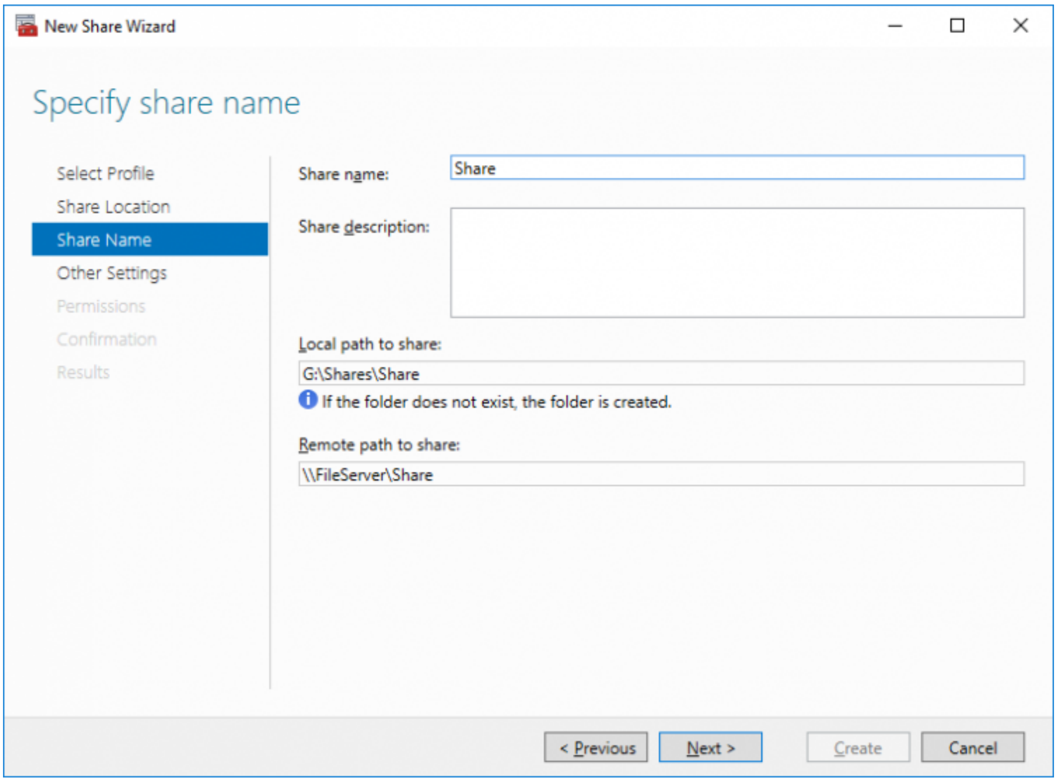
● Select by volume:

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

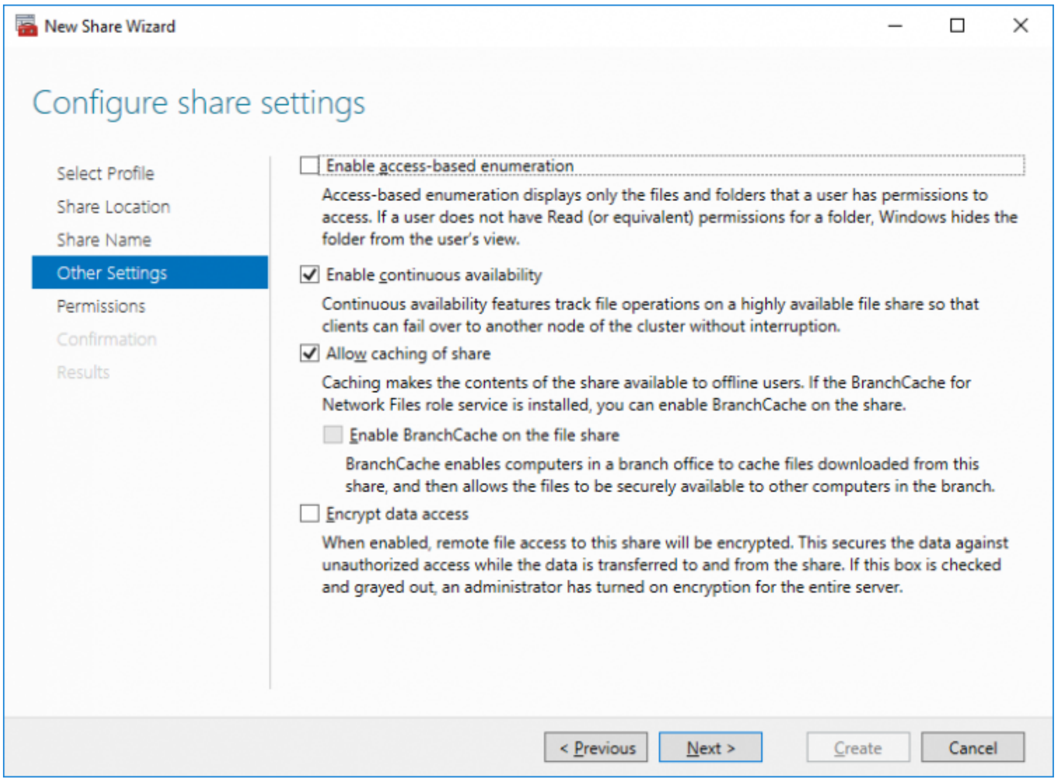
If the folder does not exist, the folder is created.

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.

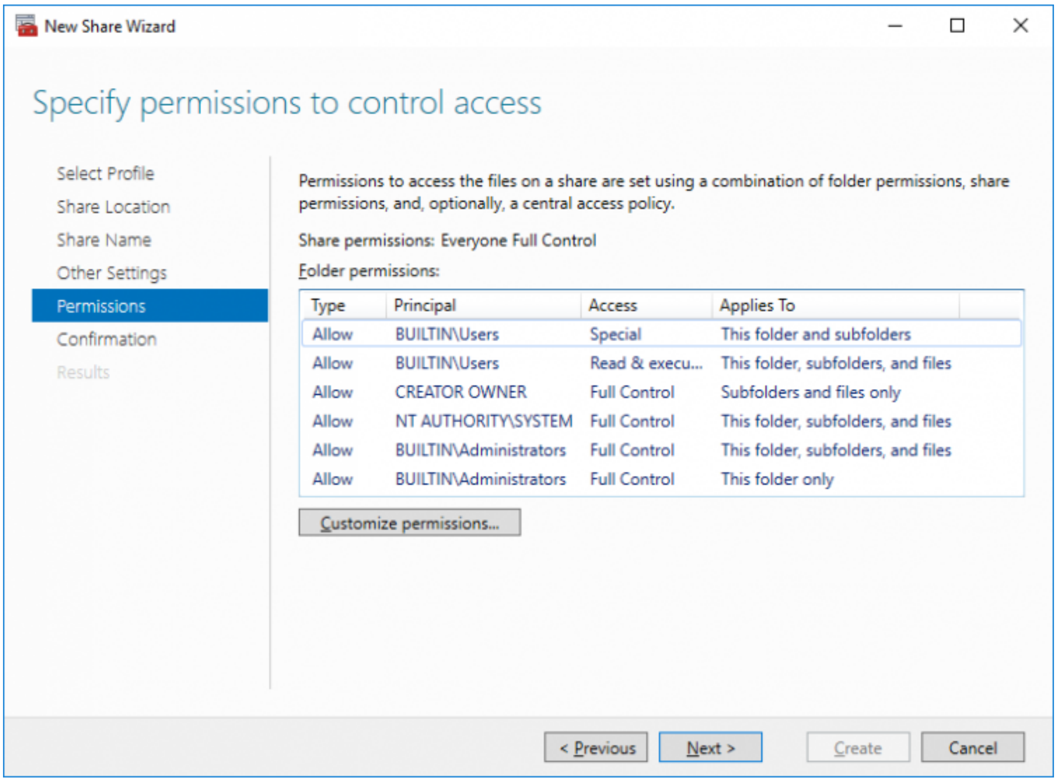
□ Enable BranchCache on the file share

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

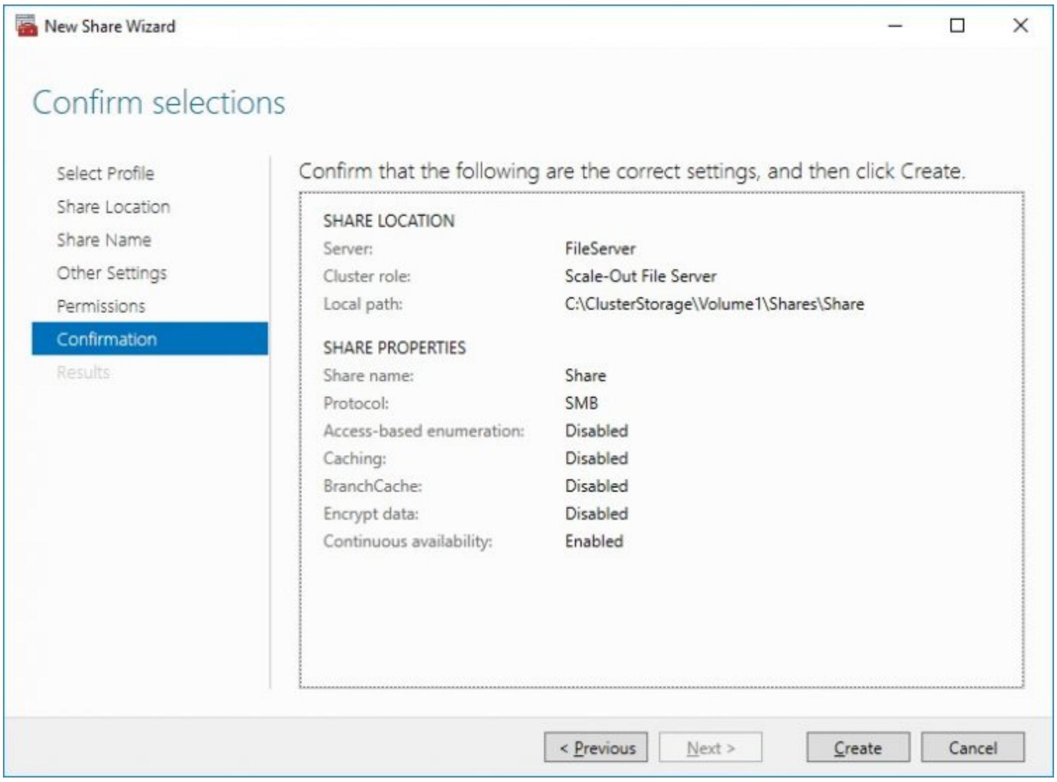
Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

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.

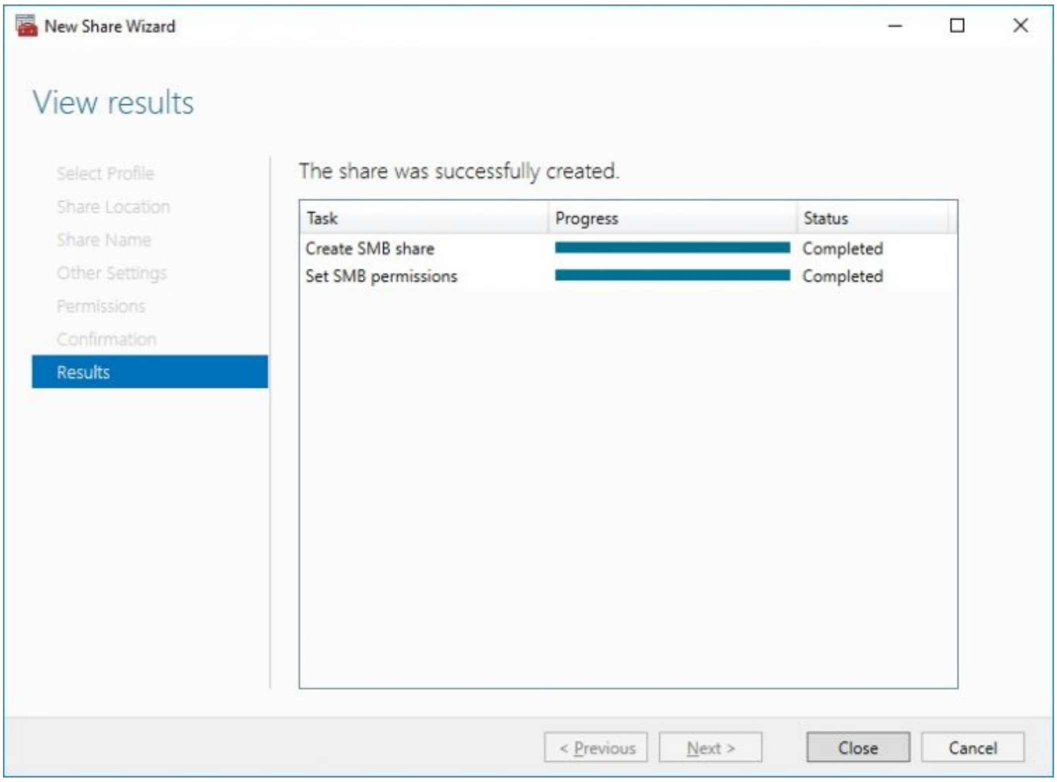
SHARE LOCATION

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.

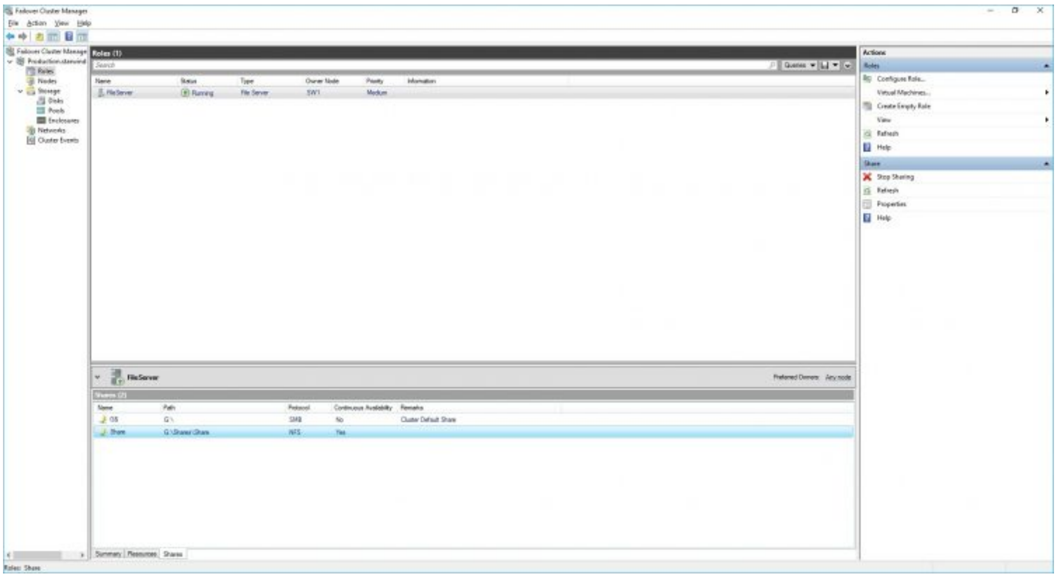
Task	Progress	Status
Create SMB share		Completed
Set SMB permissions		Completed

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
G$	G:\	SMB	No	Cluster Default Share
Share	G:\Shares\Share	NFS	Yes	

Configuring Nfs File Share

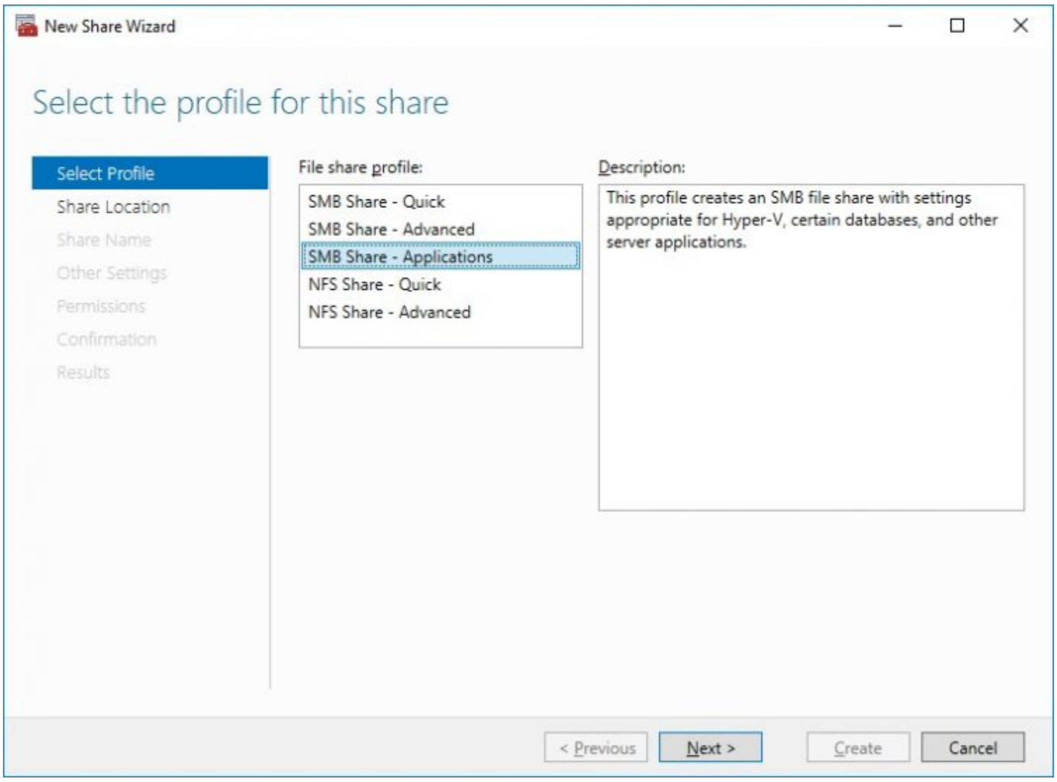
To Add NFS File Share

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.



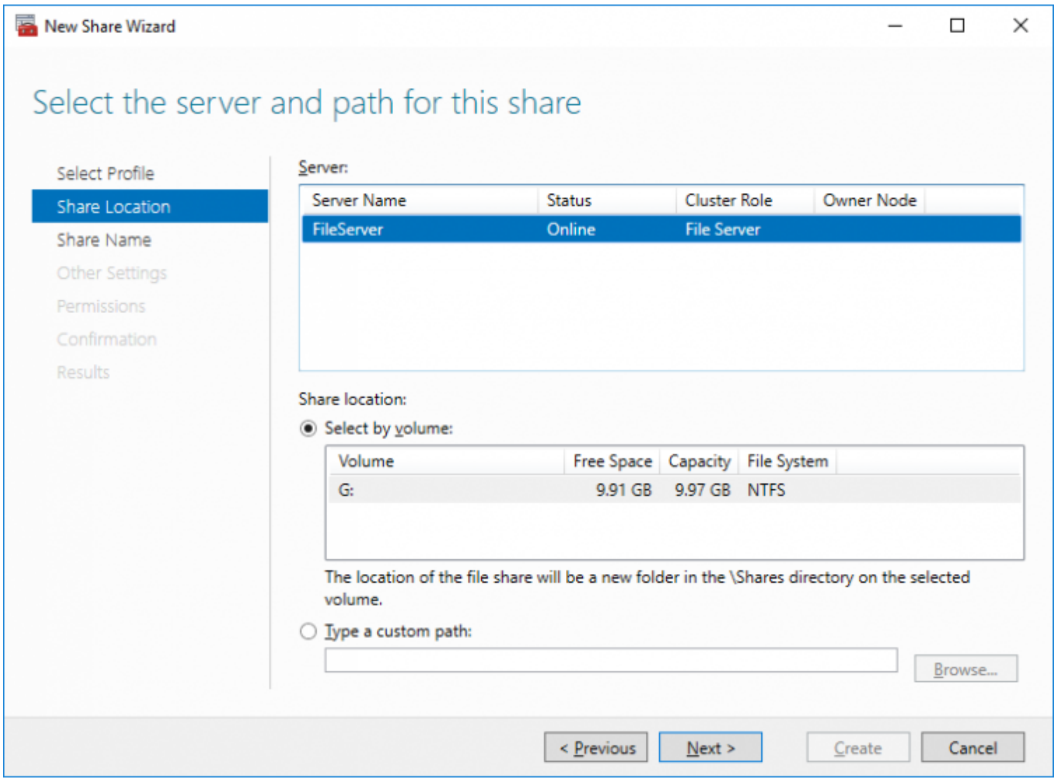
New Share Wizard

Select the profile for this share

File share profile:
- SMB Share - Quick
- SMB Share - Advanced
- SMB Share - Applications
- NFS Share - Quick
- NFS Share - Advanced

Description:
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.



Select the server and path for this share

Server:

Server Name	Status	Cluster Role	Owner Node
FileServer	Online	File Server	

Share location:

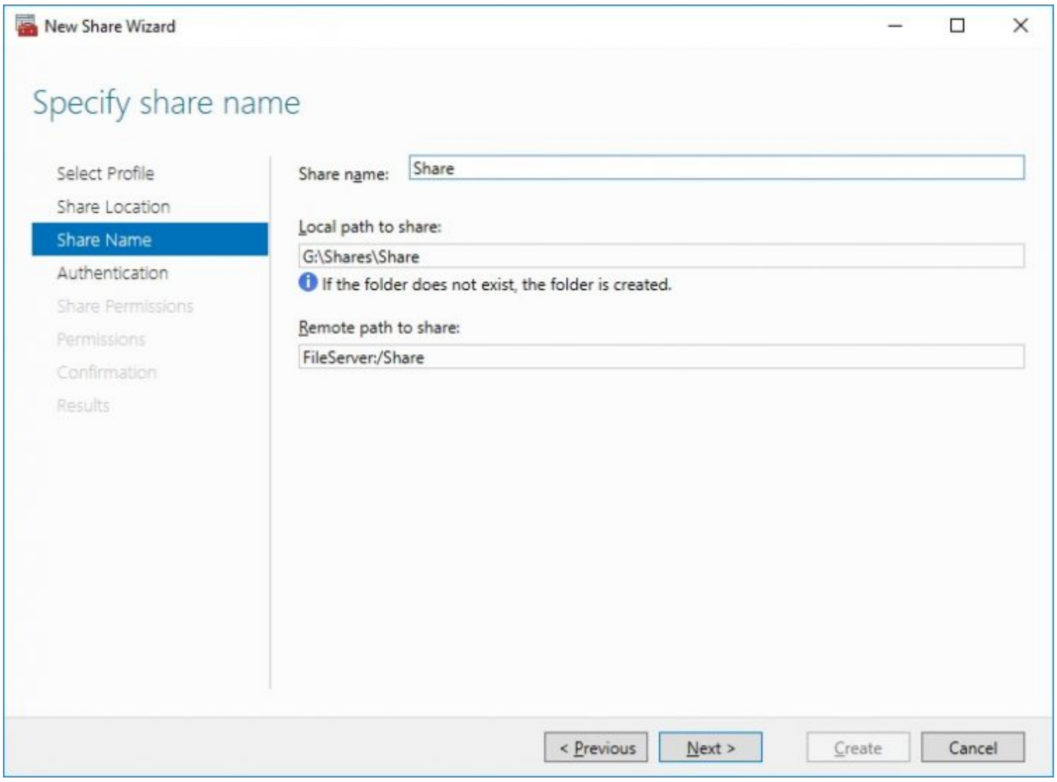
● Select by volume:

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.



Specify share name

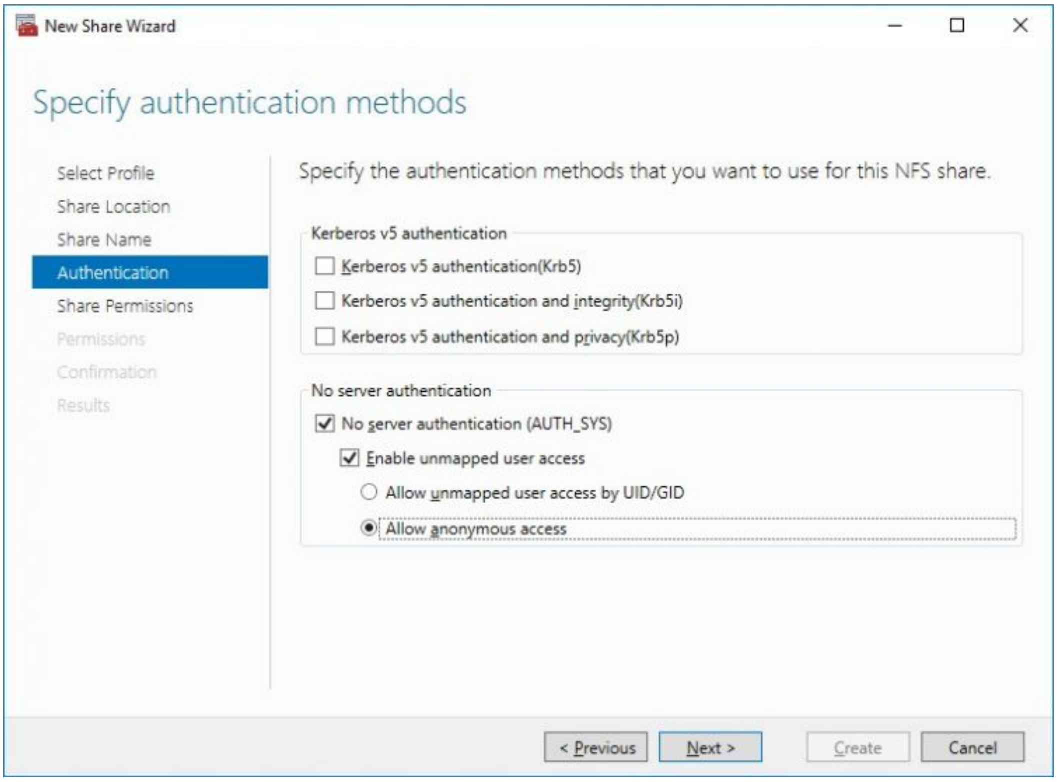
Share name: Share

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.



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

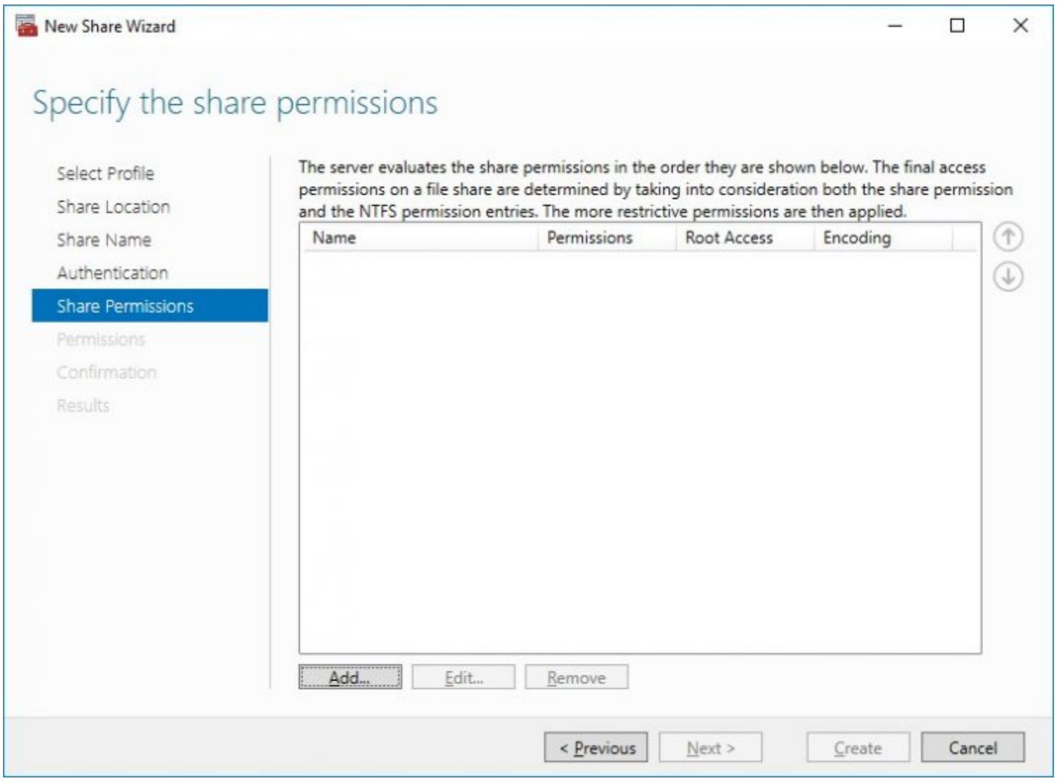
☑ No server authentication (AUTH_SYS)

☑ Enable unmapped user access

○ Allow unmapped user access by UID/GID

● Allow anonymous access

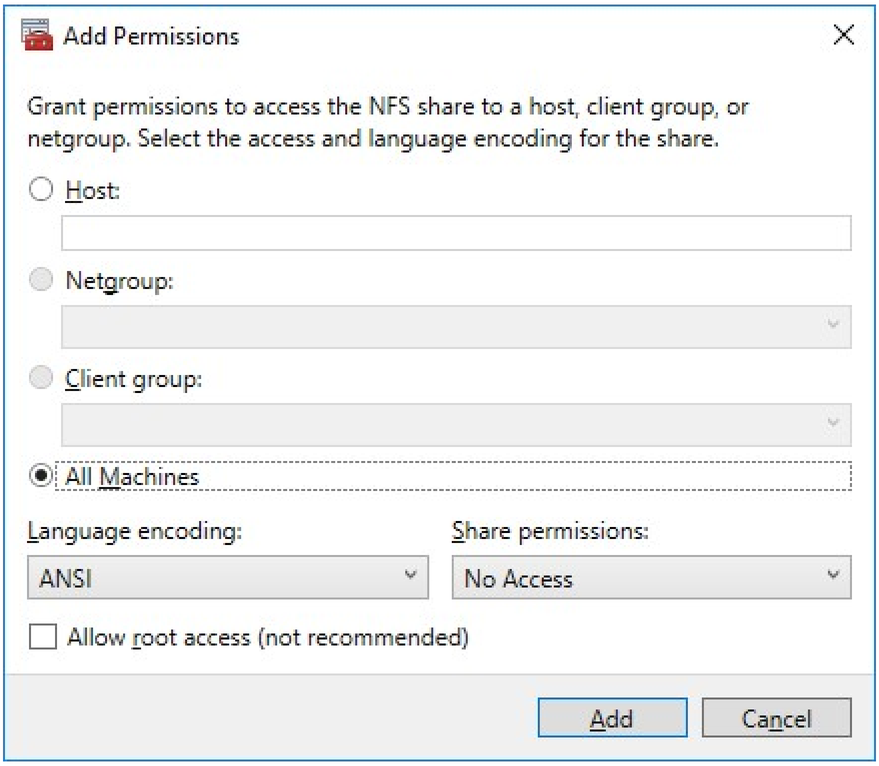
8. Click Add and specify Share Permissions.



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:

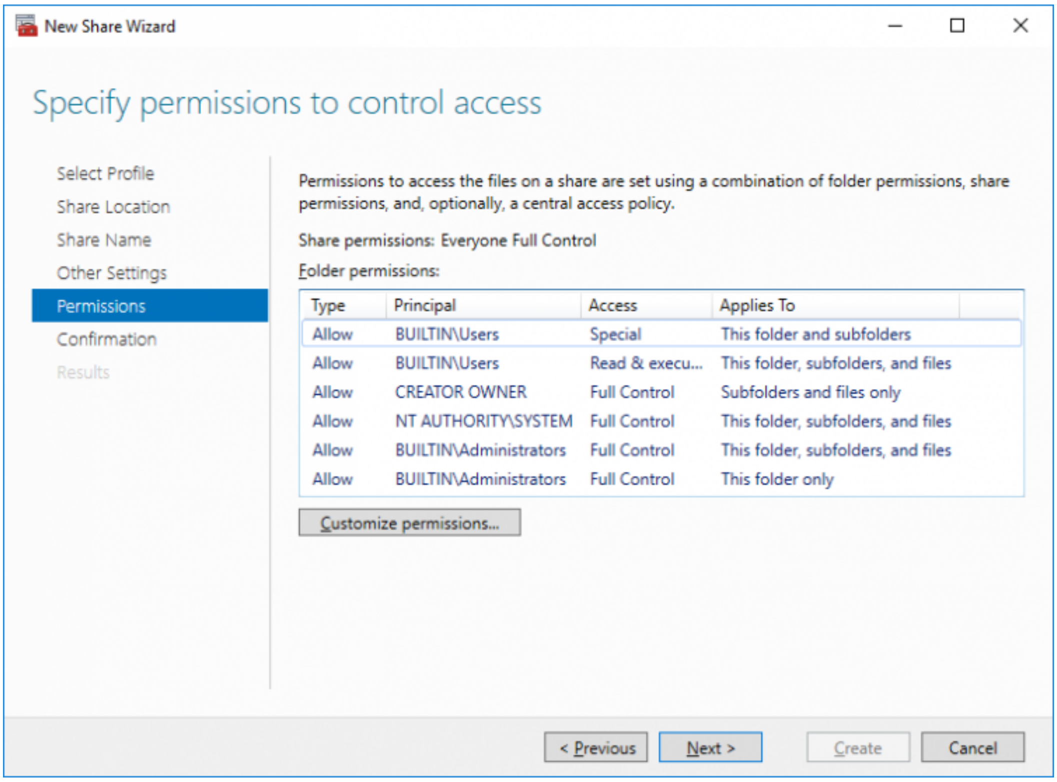
● All Machines

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

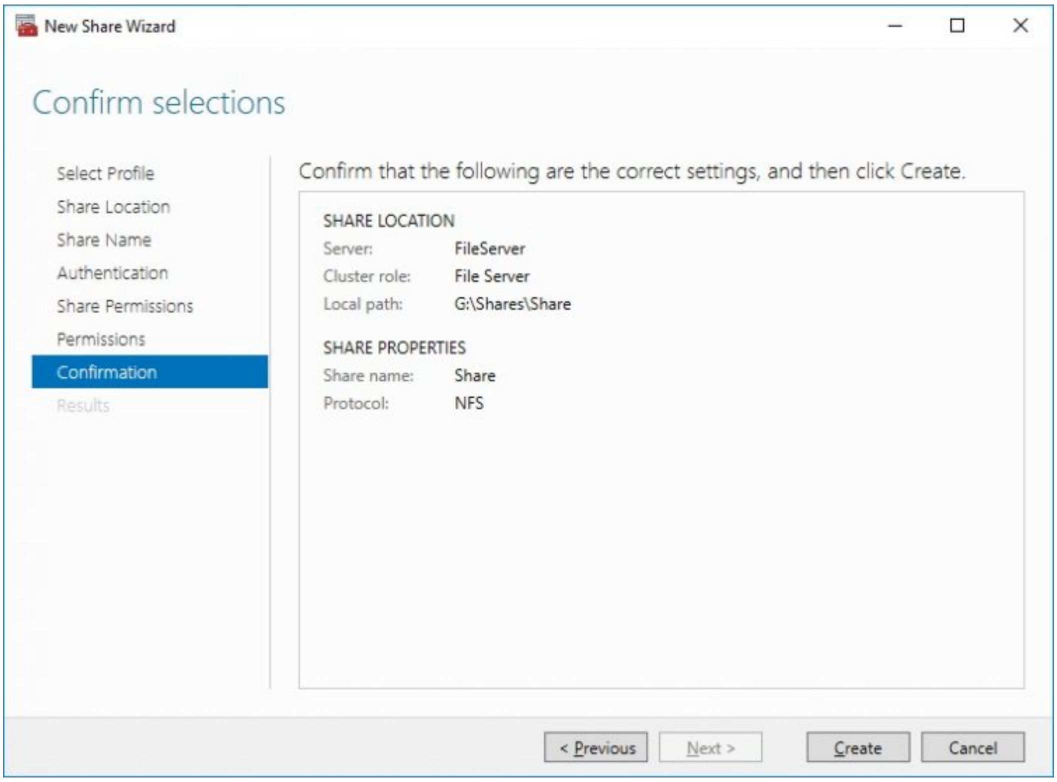
Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

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.

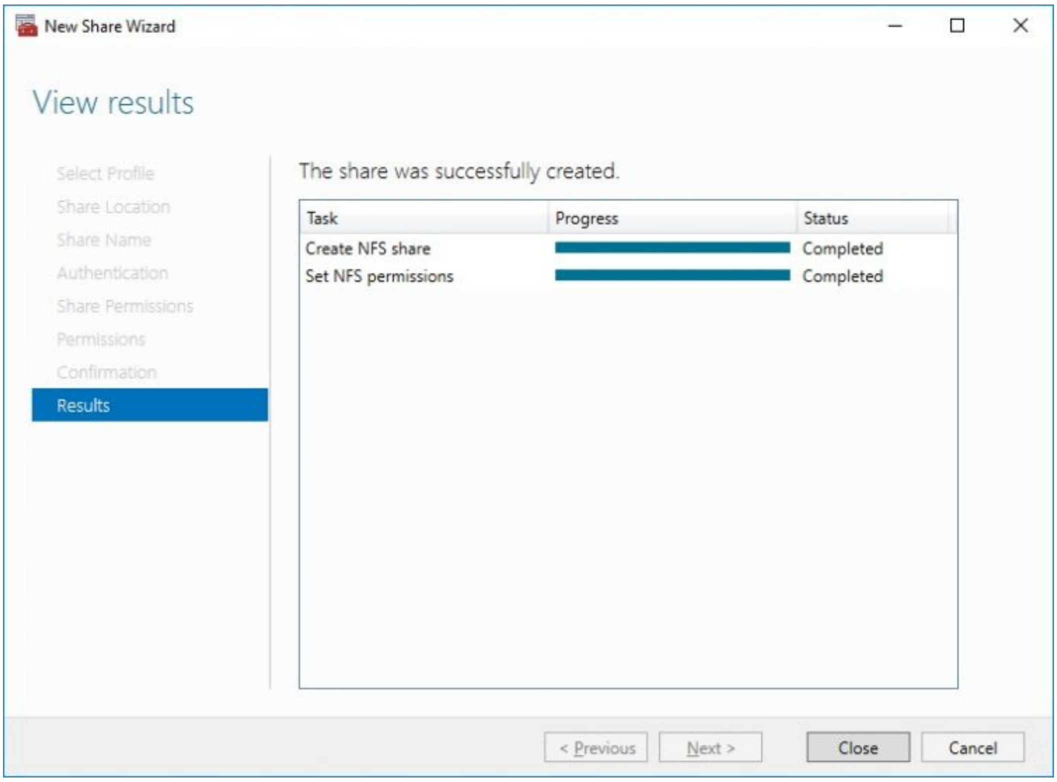


Confirm that the following are the correct settings, and then click Create.

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.



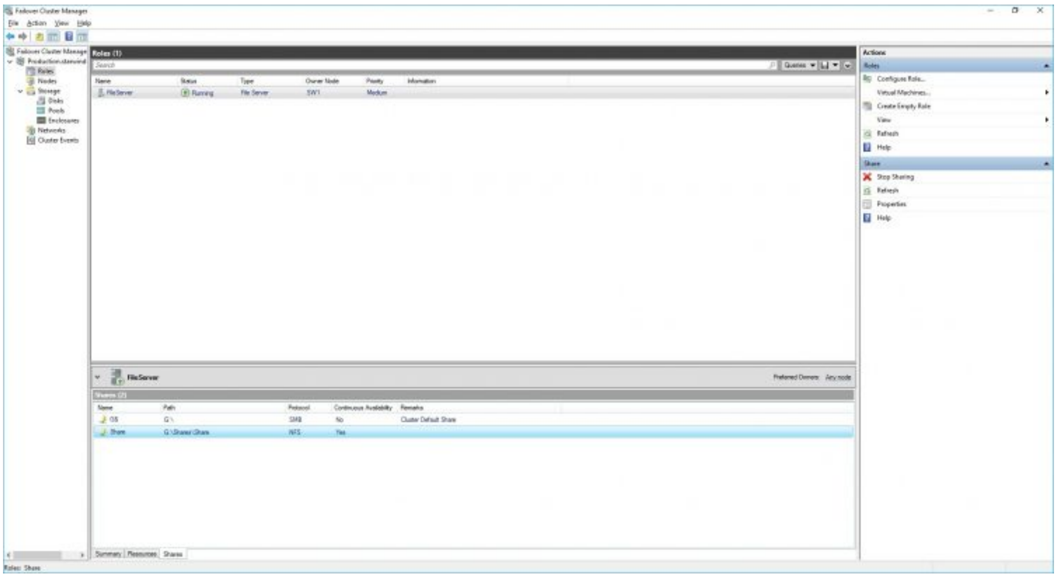
View results

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	

Shares (2)

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

Conclusion

Following this guide, the Failover Cluster was deployed and configured with StarWind Virtual SAN (VSAN) running in Windows application 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

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