

# StarWind Virtual SAN: Configuration Guide for Microsoft Azure Stack HCI [Hyper-V], VSAN Deployed as a Controller VM using PowerShell CLI

2024

TECHNICAL PAPERS



## Trademarks

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

## Changes

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

## Technical Support and Services

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

## About StarWind

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

## Copyright ©2009-2018 StarWind Software Inc.

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

## Annotation

### Relevant products

This guide applies to StarWind Virtual SAN and StarWind Virtual SAN Free (Version V8 (Build 15260, OVF Version 20230901) and earlier).

For newer versions of StarWind Virtual SAN (Version V8 (Build 15260, CVM Version 20231016) and later), please refer to this configuration guide: [StarWind Virtual SAN: Configuration Guide for Microsoft Azure Stack HCI \[Hyper-V\], VSAN Deployed as a Controller Virtual Machine using PowerShell CLI](#)

### Purpose

This guide is to assist users in the deployment and configuration of StarWind VSAN CVM on Microsoft Azure Stack HCI platforms, emphasizing best practices and system requirements.

### Audience

This document is designed for IT professionals, system administrators, and technical users who are looking to deploy and configure StarWind VSAN CVM on Microsoft Azure Stack HCI platforms using PowerShell CLI.

### Expected Results

Following this guide, users will get a fully configured Failover Cluster on Microsoft Azure Stack HCI with shared storage provided by StarWind VSAN.

## Introduction To Starwind Virtual San Cvm

StarWind Virtual SAN Controller Virtual Machine (CVM) comes as a prepackaged Linux Virtual Machine (VM) to be deployed on any industry-standard hypervisor. It creates a VM-centric and high-performing storage pool for a VM cluster.

This guide describes the deployment and configuration process of the StarWind Virtual SAN CVM.

## Starwind Vsan 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:

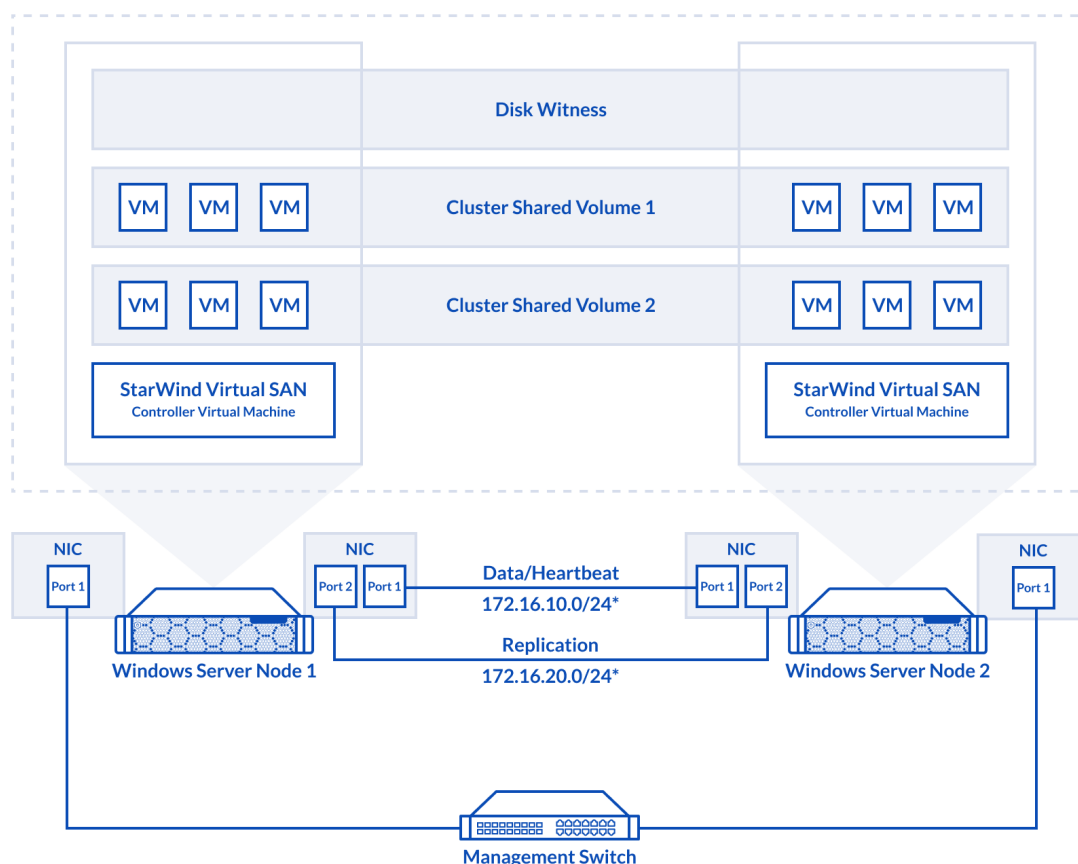
<https://knowledgebase.starwindsoftware.com/guidance/recommended-raid-settings-for-hdd-and-ssd-disks/>

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

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

## Pre-Configuring The Windows Server Hosts

The diagram below illustrates the network and storage configuration of the solution:





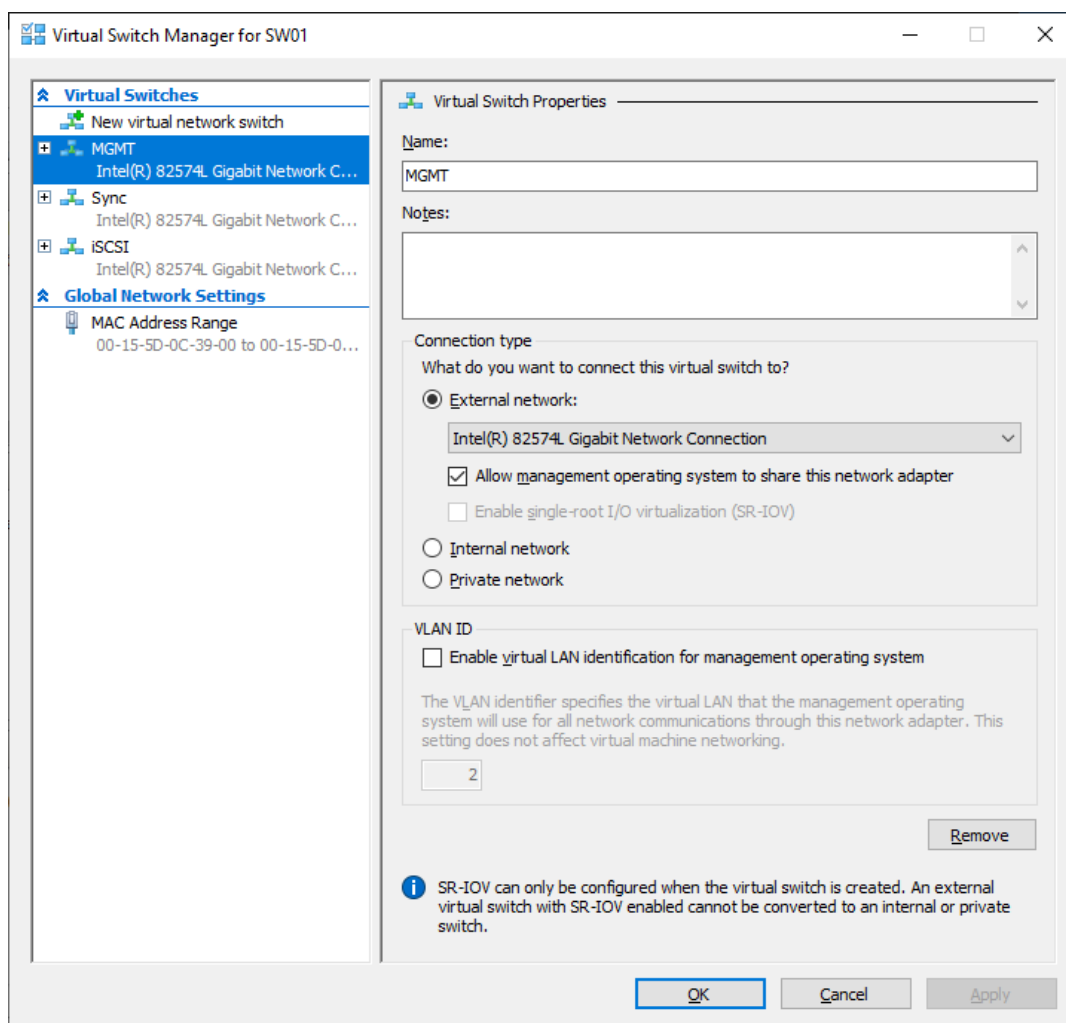
1. Make sure that a domain controller is configured and the servers are added to the domain.

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

4. Separate external Virtual Switches should be created for iSCSI and Synchronization traffic based on the selected before iSCSI and Synchronization interfaces. Using Hyper-V Manager open Virtual Switch Manager and create two external Virtual Switches: one for the iSCSI/StarWind Heartbeat channel (iSCSI) and another one for the Synchronization channel (Sync).



5. Configure and set the IP address on each virtual switch interface. In this document, the 172.16.10.x subnet is used for iSCSI/StarWind heartbeat traffic, while 172.16.20.x subnet is used for the Synchronization traffic.

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

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

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

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

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

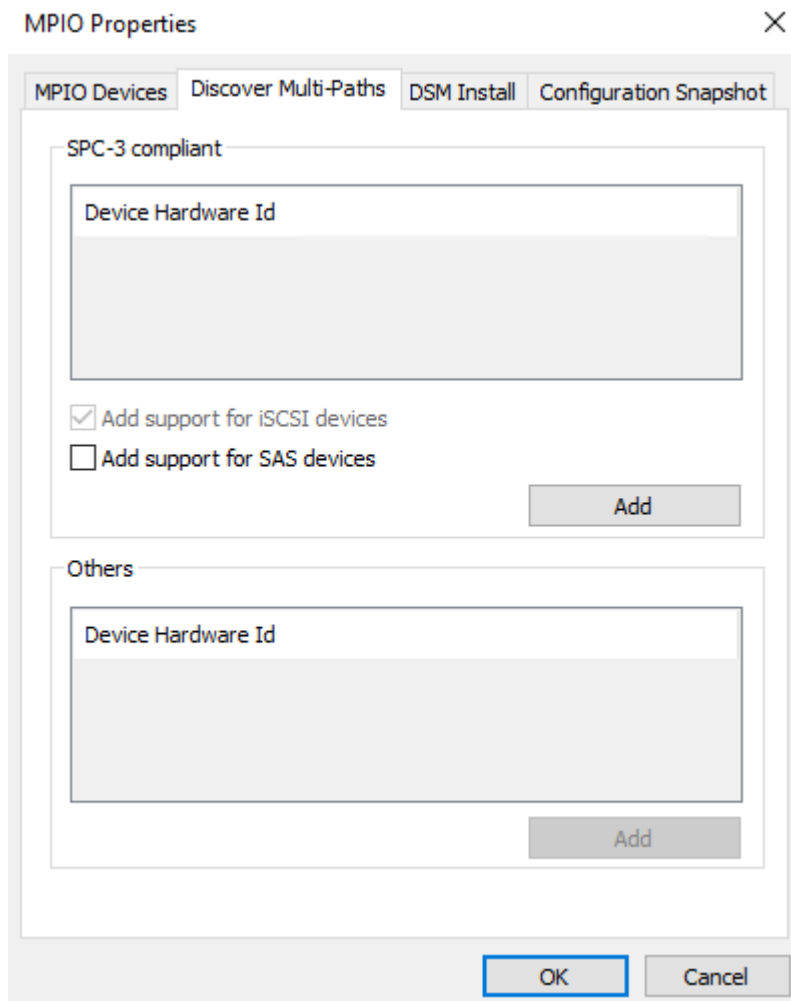
NOTE: MTU setting should be applied on the adapters only if there is no live production running through the NICs.

#### Enabling Multipath Support

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

```
mpiocpl
```

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



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

10. Repeat the same procedure on the other server.

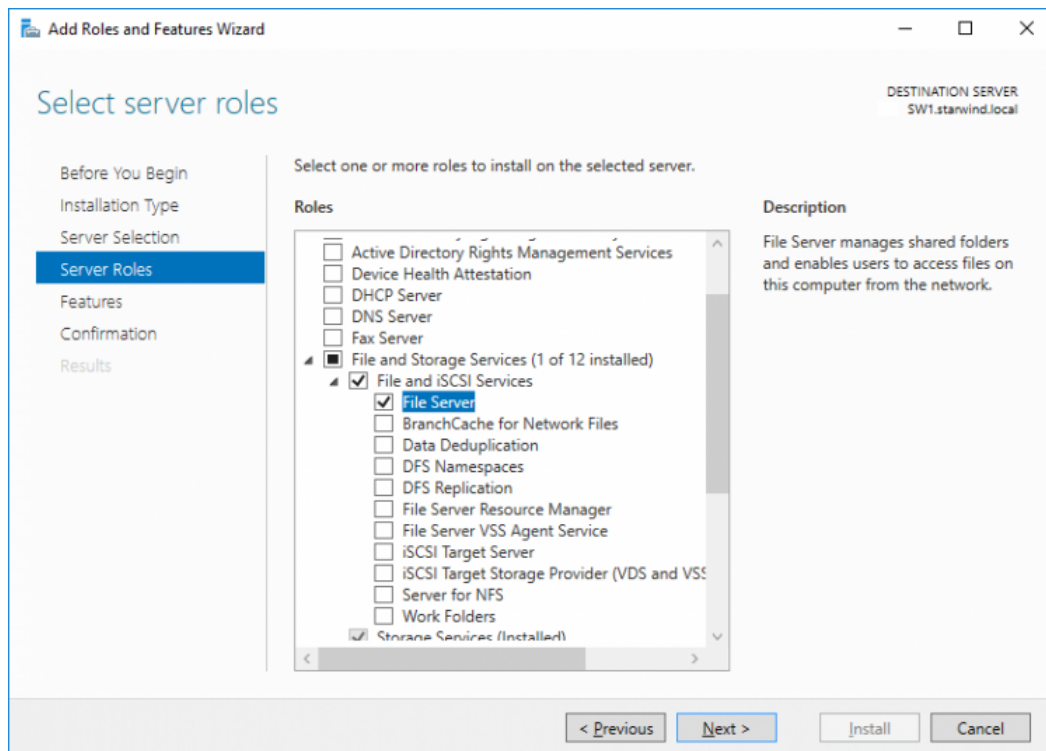
## Installing File Server Roles

Please follow the steps below if file shares configuration is required

## Scale-Out File Server (Sofs) For Application Data

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

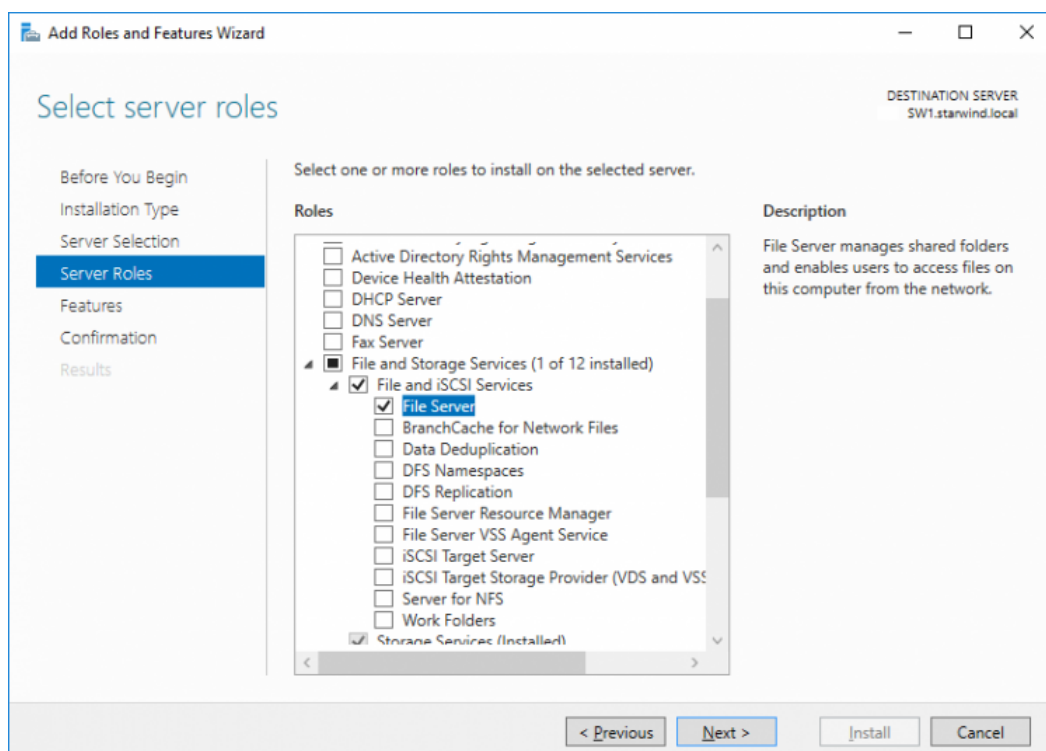
below:



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

## File Server For General Use With Smb Share

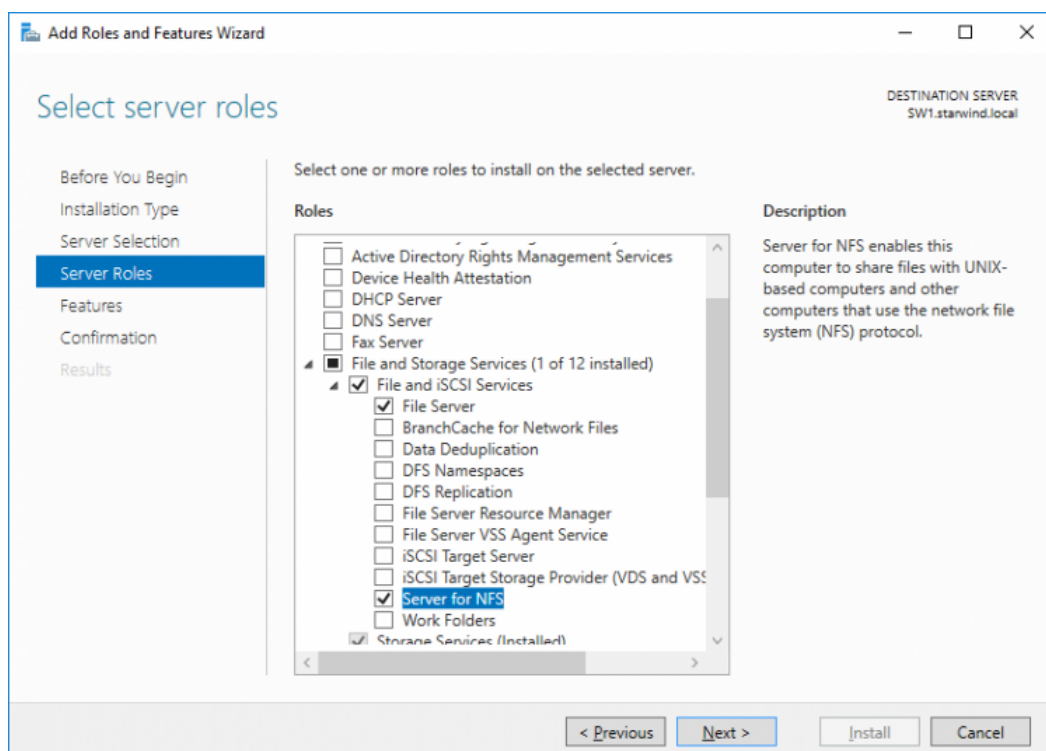
1. Open Server Manager: Start -> Server Manager.
2. Select: Manage -> Add Roles and Features.
3. Follow the installation wizard steps to install the roles selected in the screenshot below:



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

## File Server For General Use With Nfs Share

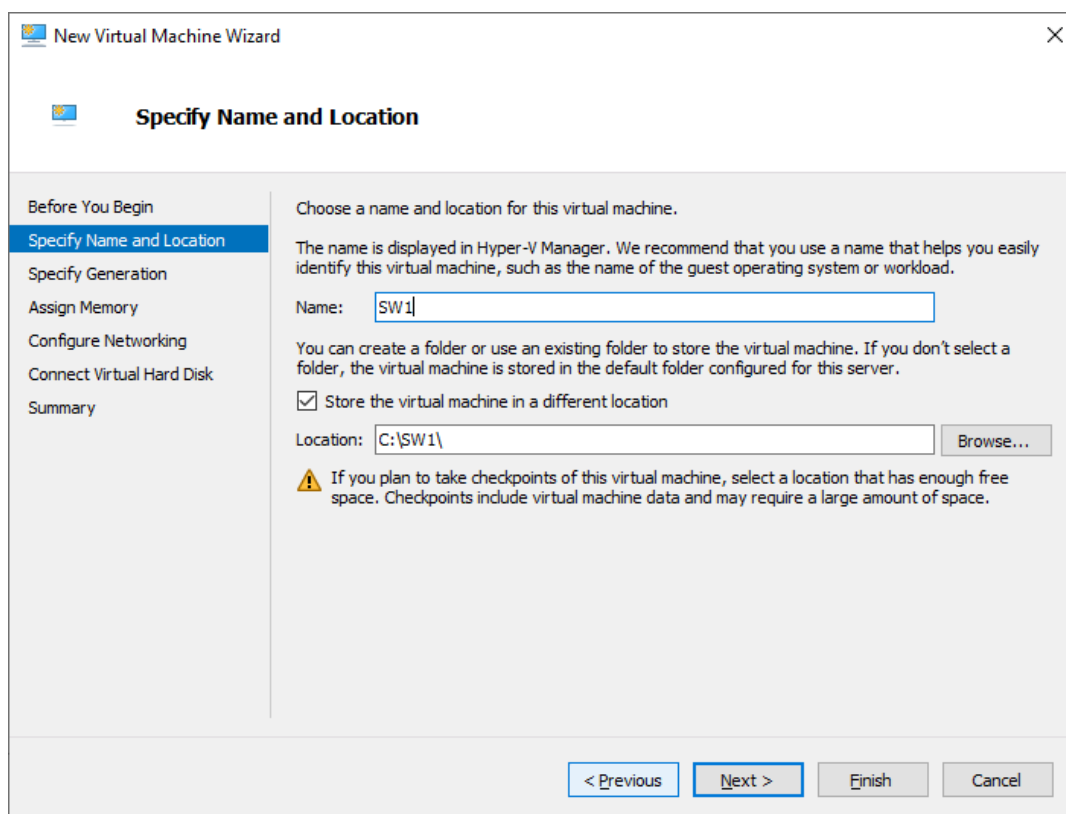
1. Open Server Manager: Start -> Server Manager.
2. Select: Manage -> Add Roles and Features.
3. Follow the installation wizard steps to install the roles selected in the screenshot below:



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

## Deploying Starwind Virtual San Cvm

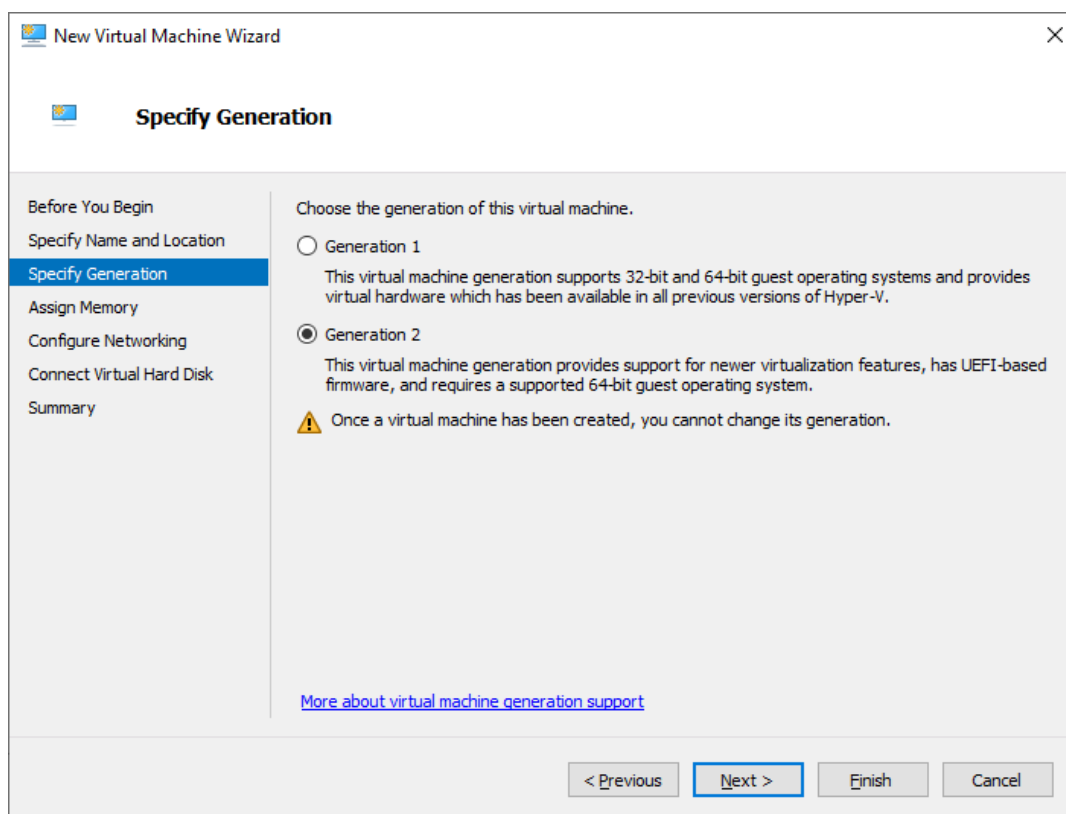
1. Download StarWind VSAN CVM to the Hyper-V server:  
[VSAN by StarWind: Overview](#)
2. Extract the VM .vhdx file from the downloaded archive.
3. Open Hyper-V Manager and create a new Hyper-V VM.
4. Specify the name of the virtual machine with StarWind VSAN, and choose the location for the VM. For example: C:\SW1\



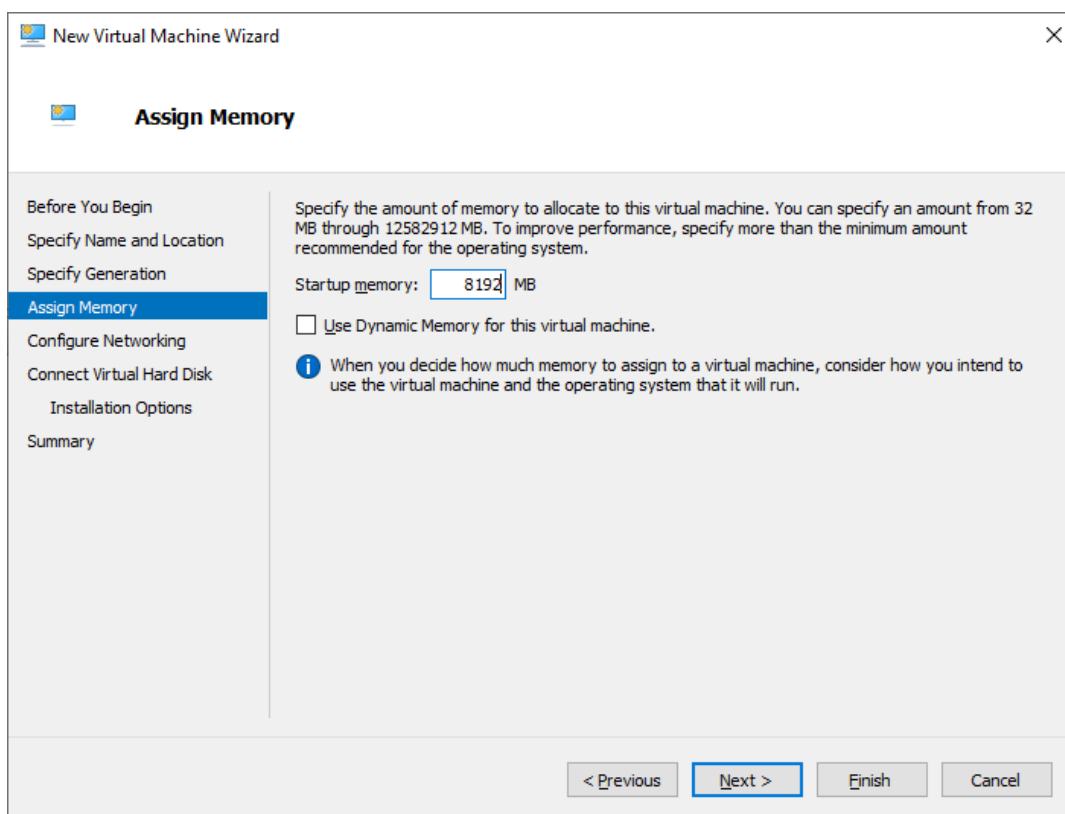
5. Copy .vhdx to the folder where the VM was created. In this case, its C:\ SW1\Virtual Hard Disks\

6. Choose Generation 2 VM.





7. Assign memory to the VM. We recommend allocating at least 8GB of RAM for StarWind CVM. If StarWind L1 cache is used, an appropriate amount of RAM should be assigned.



**New Virtual Machine Wizard**

**Assign Memory**

Before You Begin  
Specify Name and Location  
Specify Generation  
**Assign Memory**  
Configure Networking  
Connect Virtual Hard Disk  
Installation Options  
Summary

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

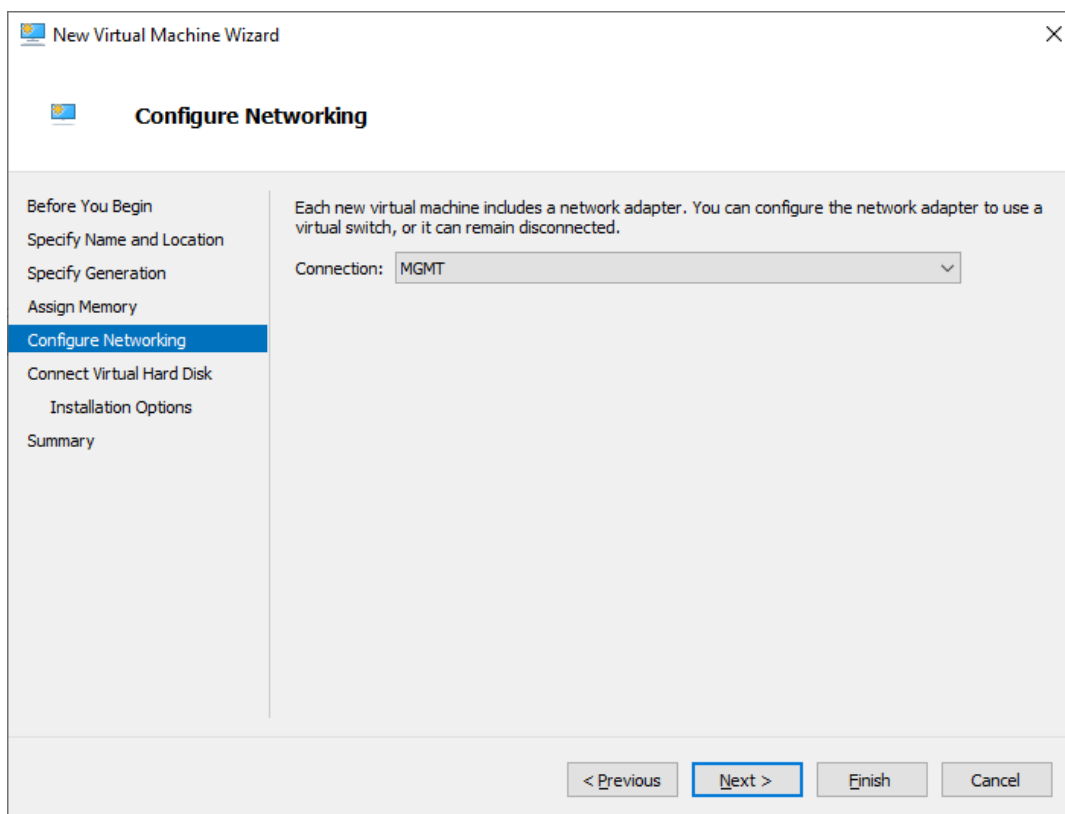
Startup memory:  MB

☐ Use Dynamic Memory for this virtual machine.

**i** When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

< Previous   **Next >**   Finish   Cancel

8. Choose the management network for the VM.



**New Virtual Machine Wizard**

**Configure Networking**

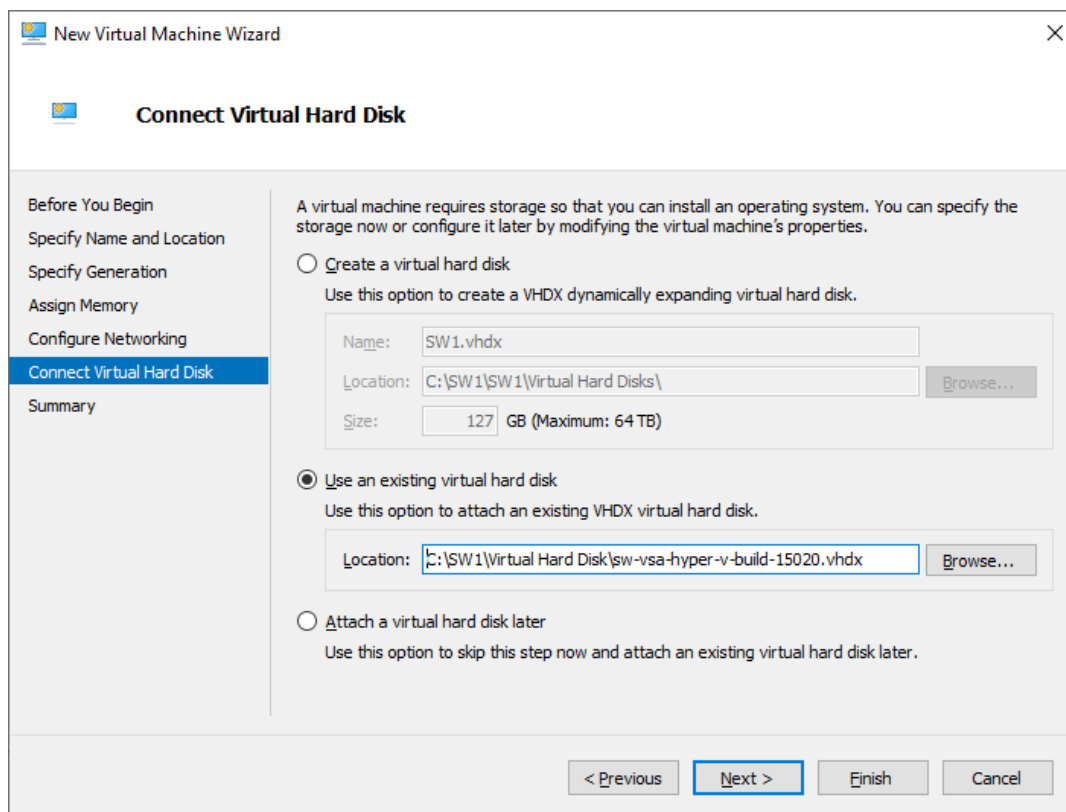
Before You Begin  
Specify Name and Location  
Specify Generation  
Assign Memory  
**Configure Networking**  
Connect Virtual Hard Disk  
Installation Options  
Summary

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection:

< Previous   **Next >**   Finish   Cancel

9. Connect .vhdx to the VM.



**New Virtual Machine Wizard**

**Connect Virtual Hard Disk**

Before You Begin  
Specify Name and Location  
Specify Generation  
Assign Memory  
Configure Networking  
**Connect Virtual Hard Disk**  
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☐ Create a virtual hard disk  
Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:   
Location:    
Size:  GB (Maximum: 64 TB)

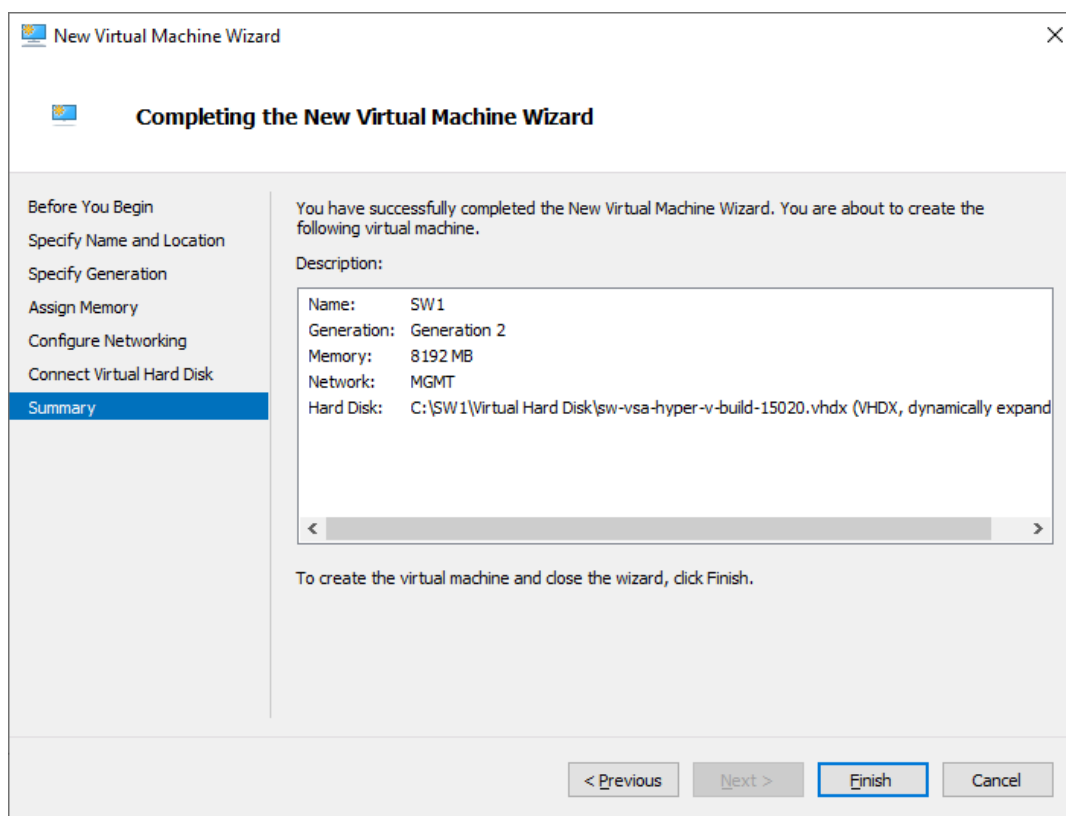
☒ Use an existing virtual hard disk  
Use this option to attach an existing VHDX virtual hard disk.

Location:

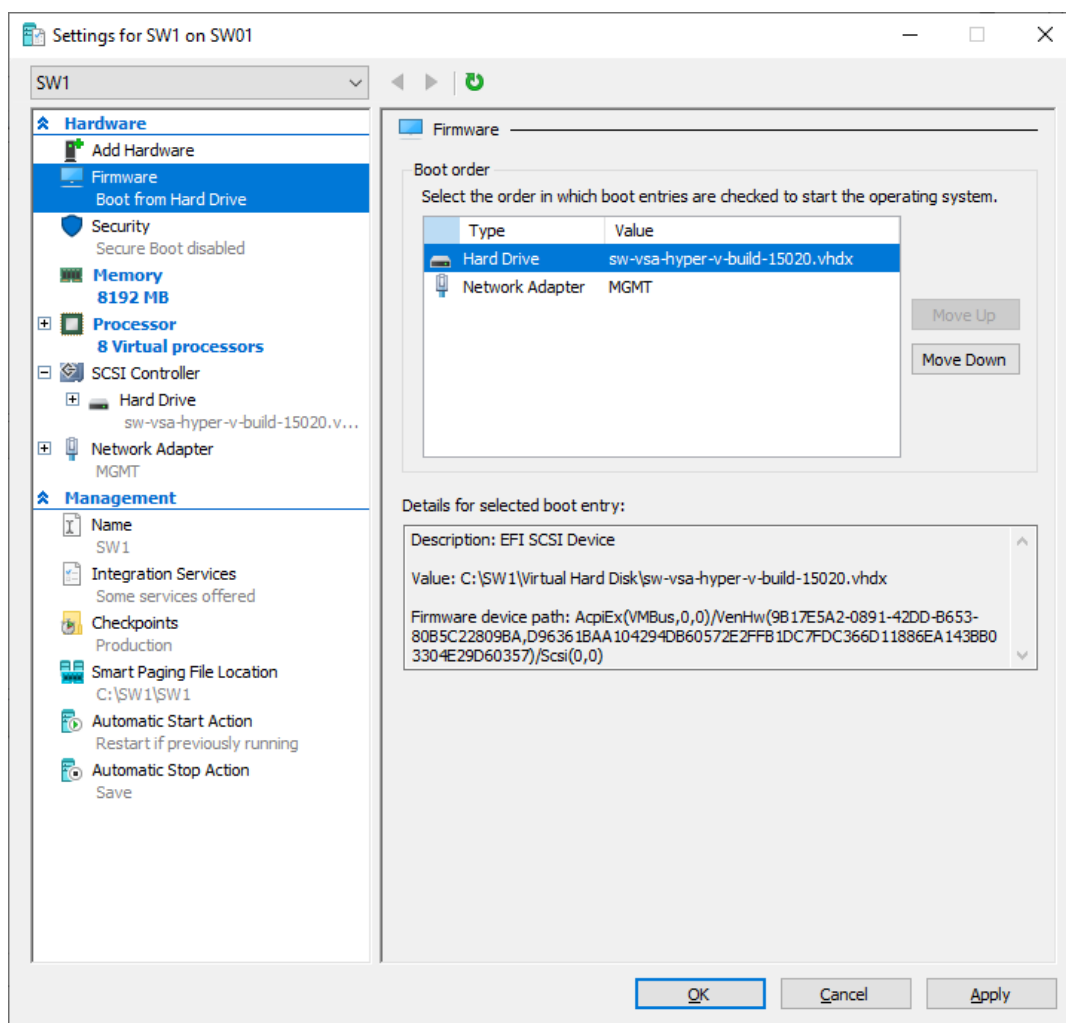
☐ Attach a virtual hard disk later  
Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous   **Next >**   Finish   Cancel

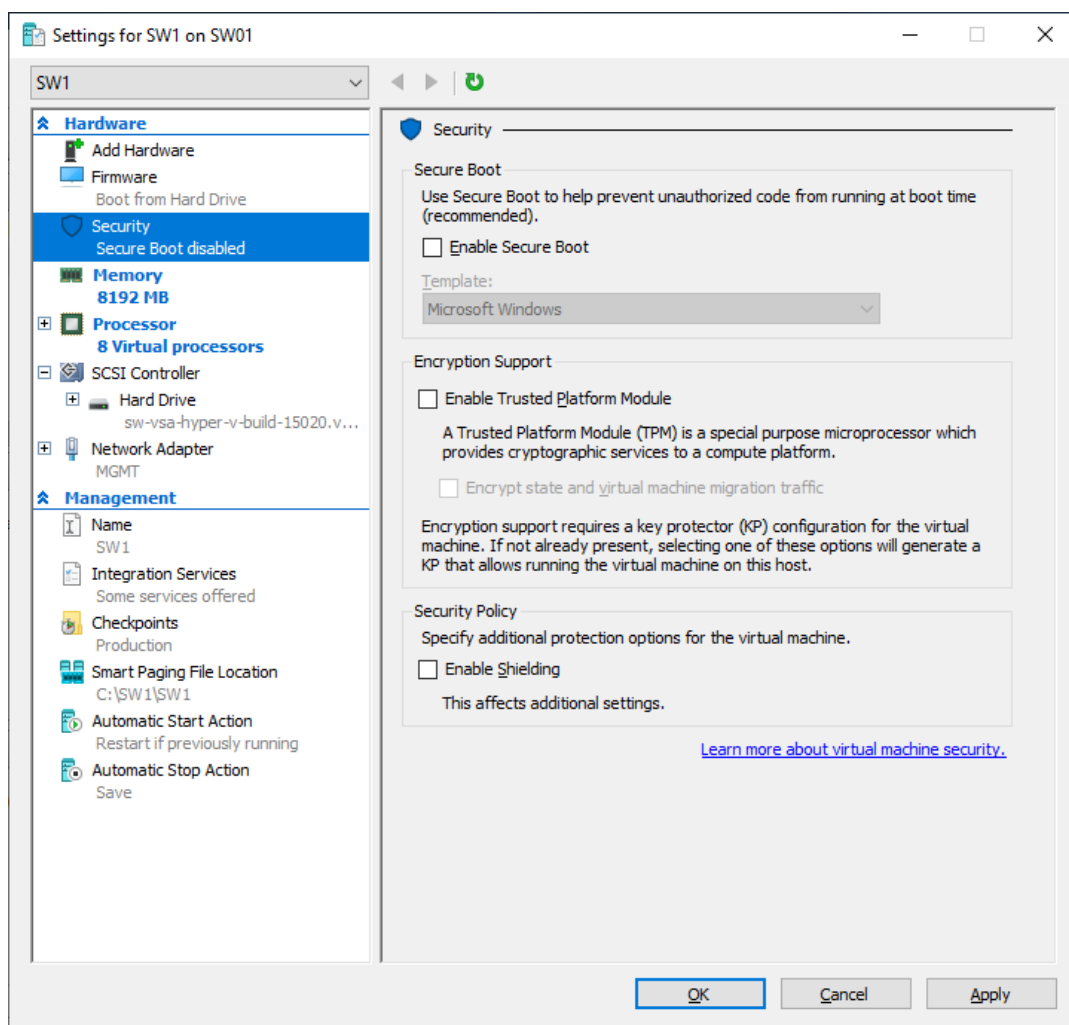
10. Review the Summary and click Finish to create the VM.



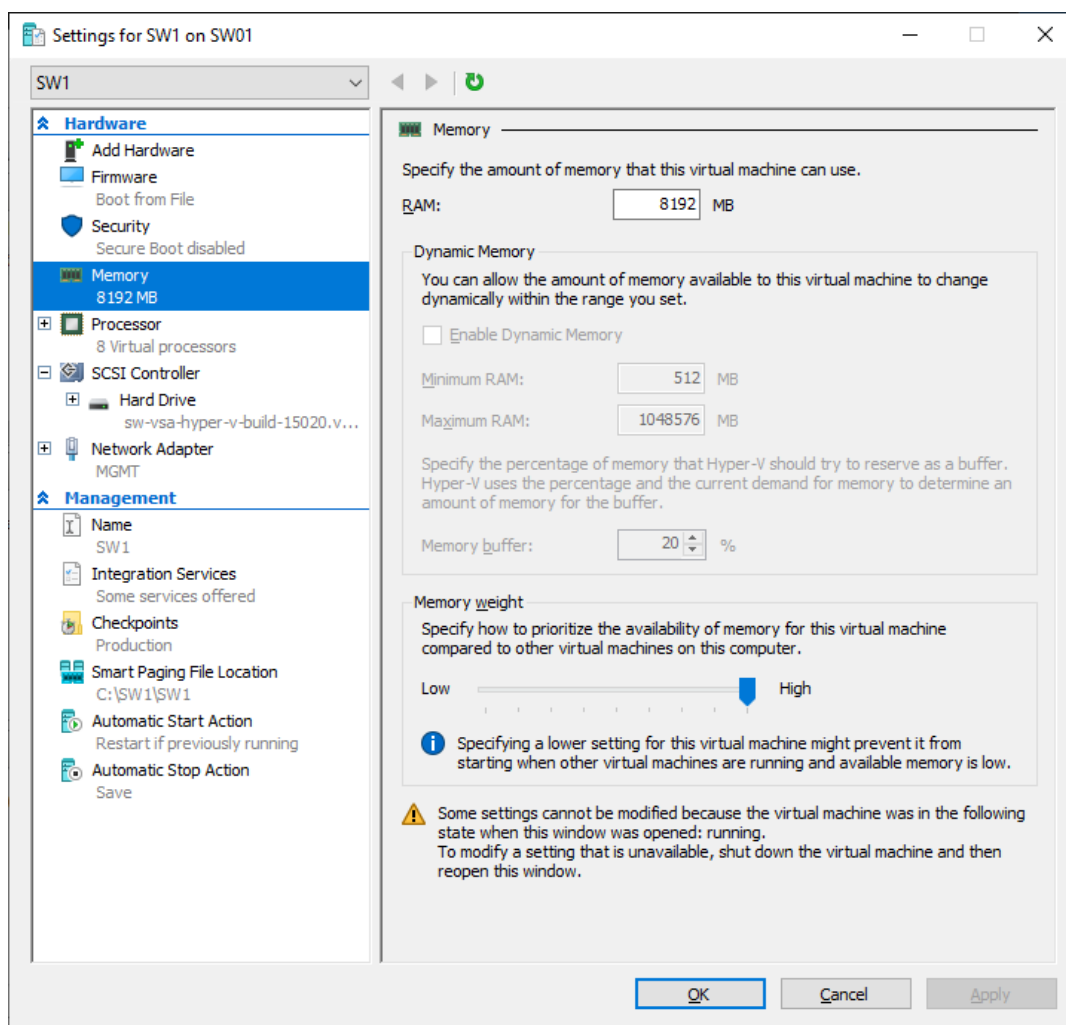
11. Right-click on the VM and choose Settings. Open Firmware and move the option Hard Drive to the first place in the list.



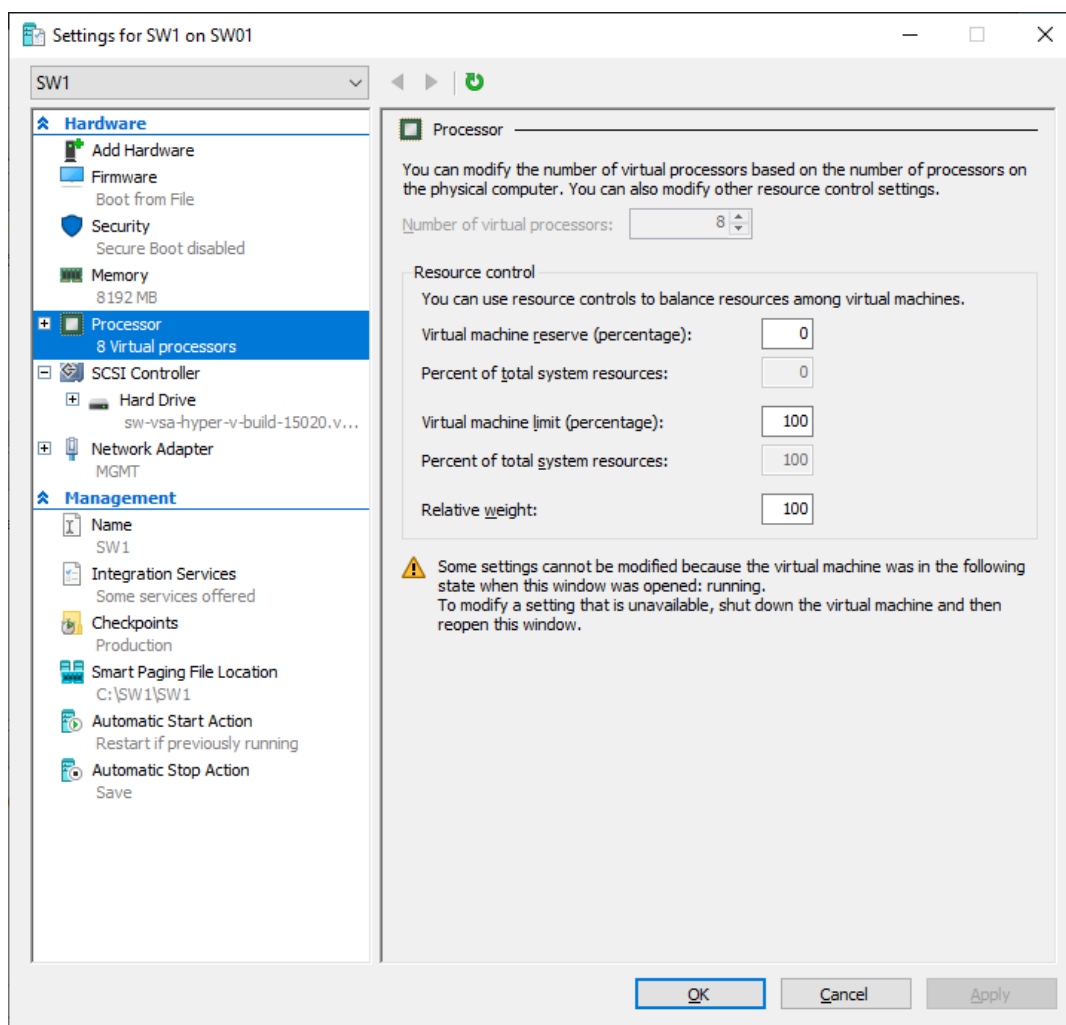
12. Go to the Security page and uncheck the Enable Secure Boot box.



13. Go to Memory and move the slider for Memory weight to High.

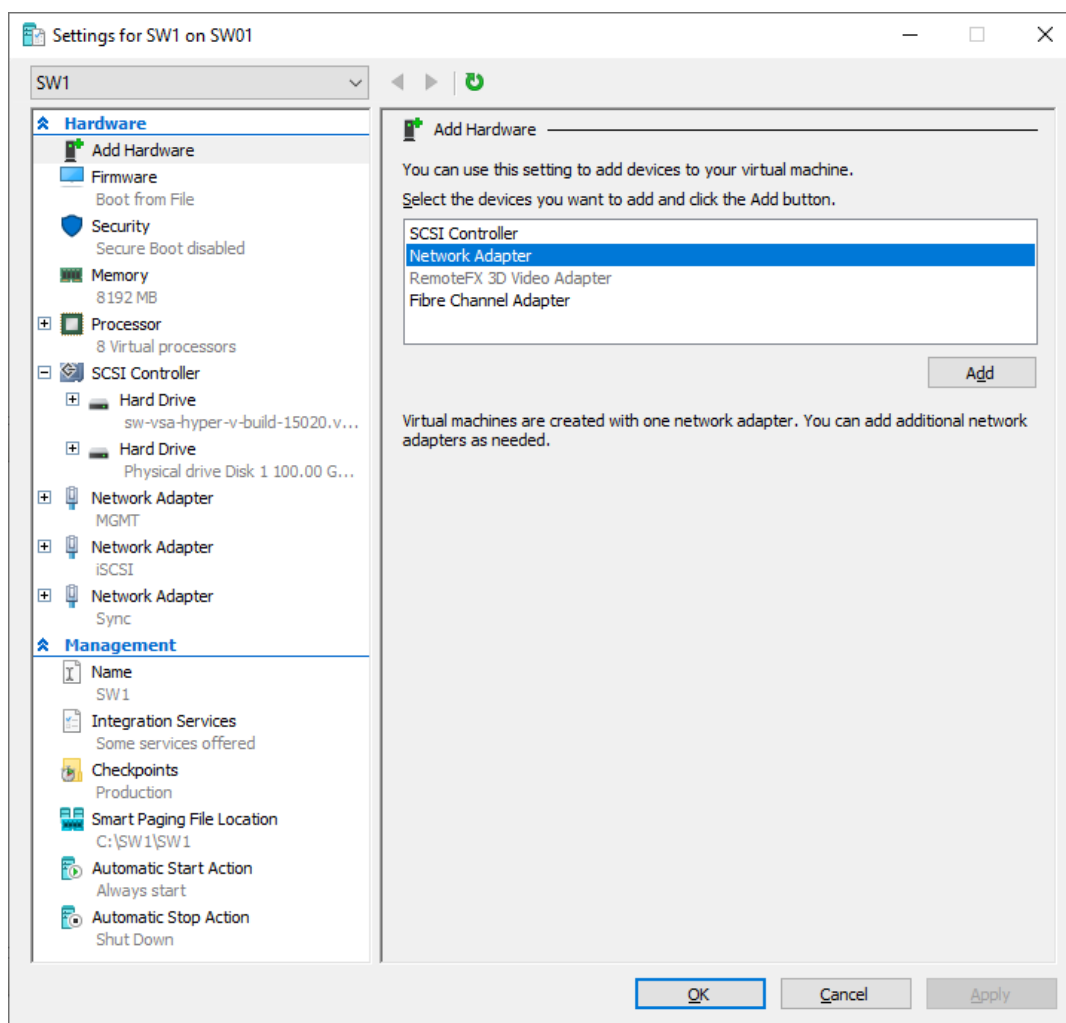


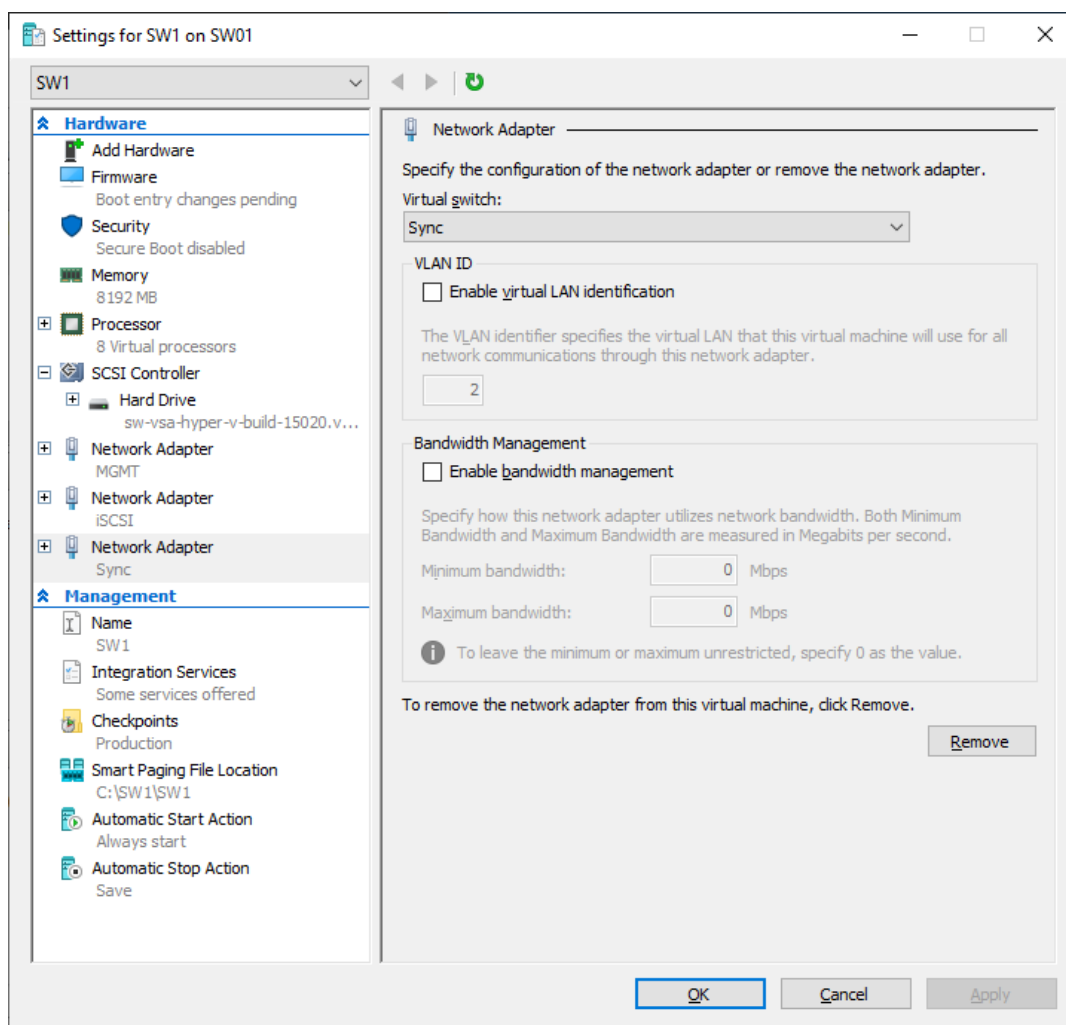
14. Go to Processor and assign 8 vCPUs to the VM.



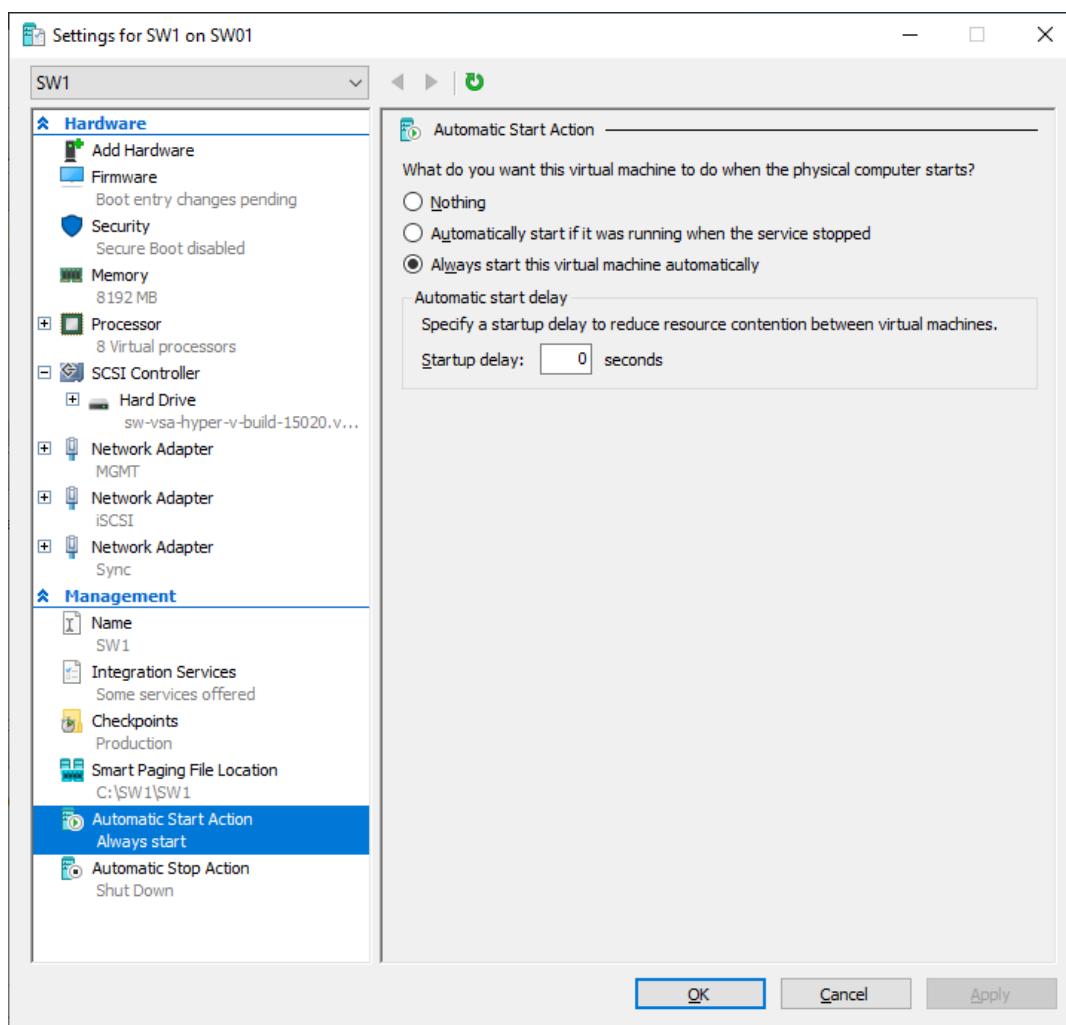
15. Click Add Hardware and add NICs for iSCSI and Synchronization traffic to the VM.



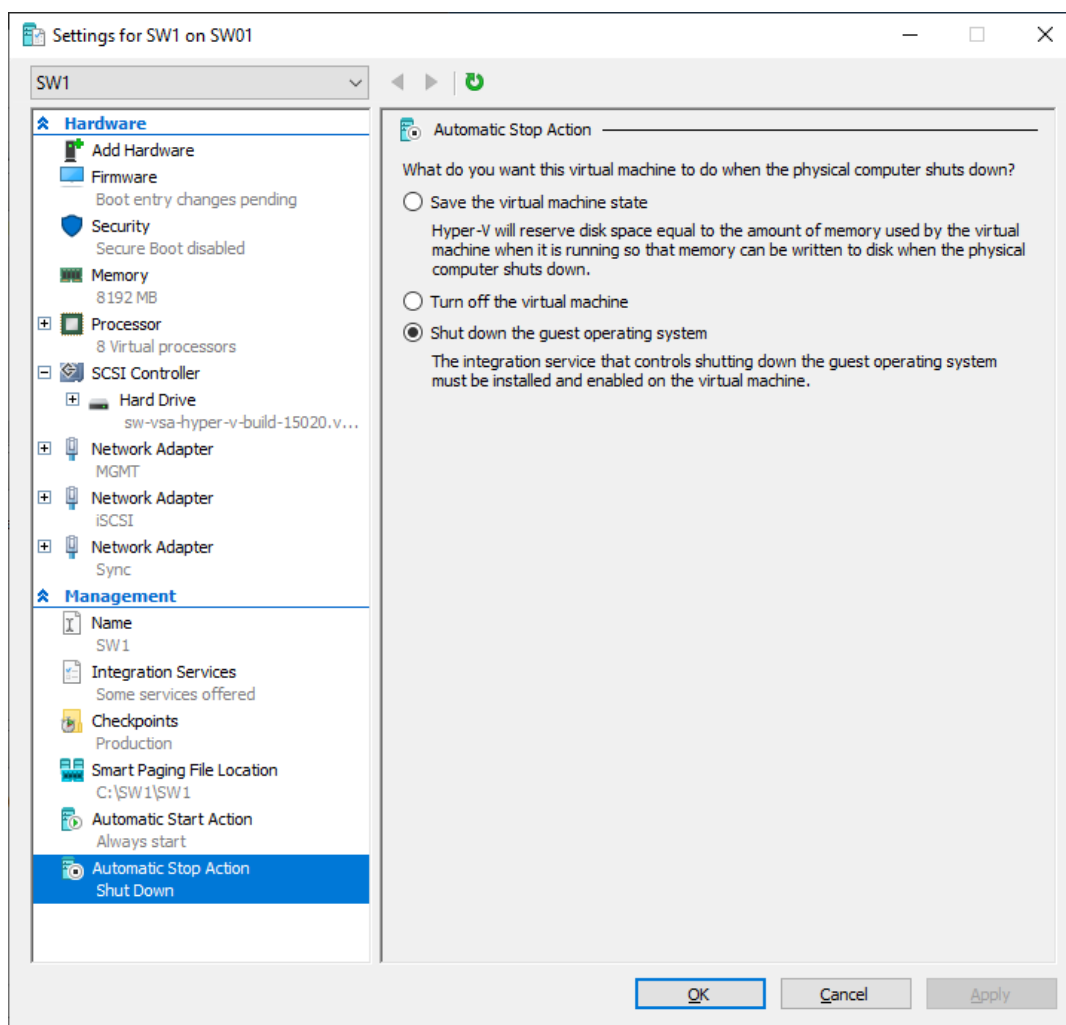




16. Configure Automatic Start and Stop actions, so the VM will always start automatically.



17. Choose Shut down the guest operating system as an Automatic Stop Action.

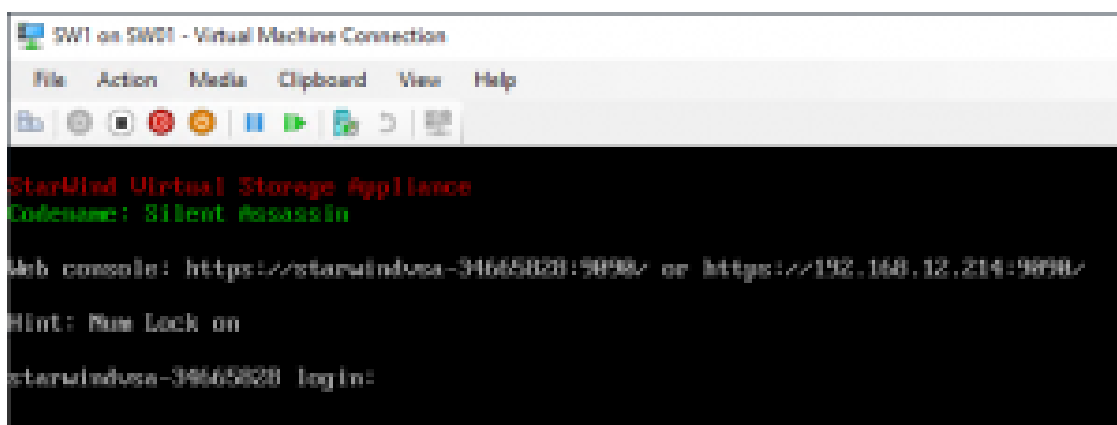


18. Repeat all the steps from this section on other Windows Server hosts.

19. Start virtual machines on all Windows Server hosts.

## Configuring Starwind Virtual San Vm Settings

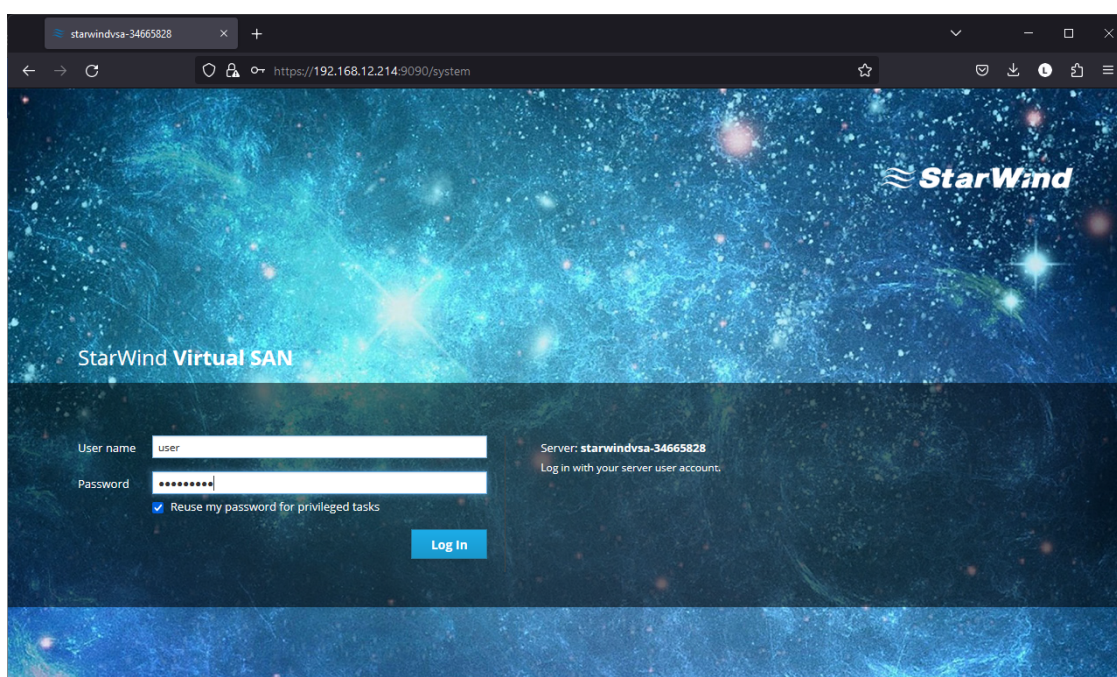
1. Open the VM console and check the IP address received via DHCP (or which was assigned manually).



Another alternative is to log into the VM via console and assign static IP using nmcli if there is no DHCP,

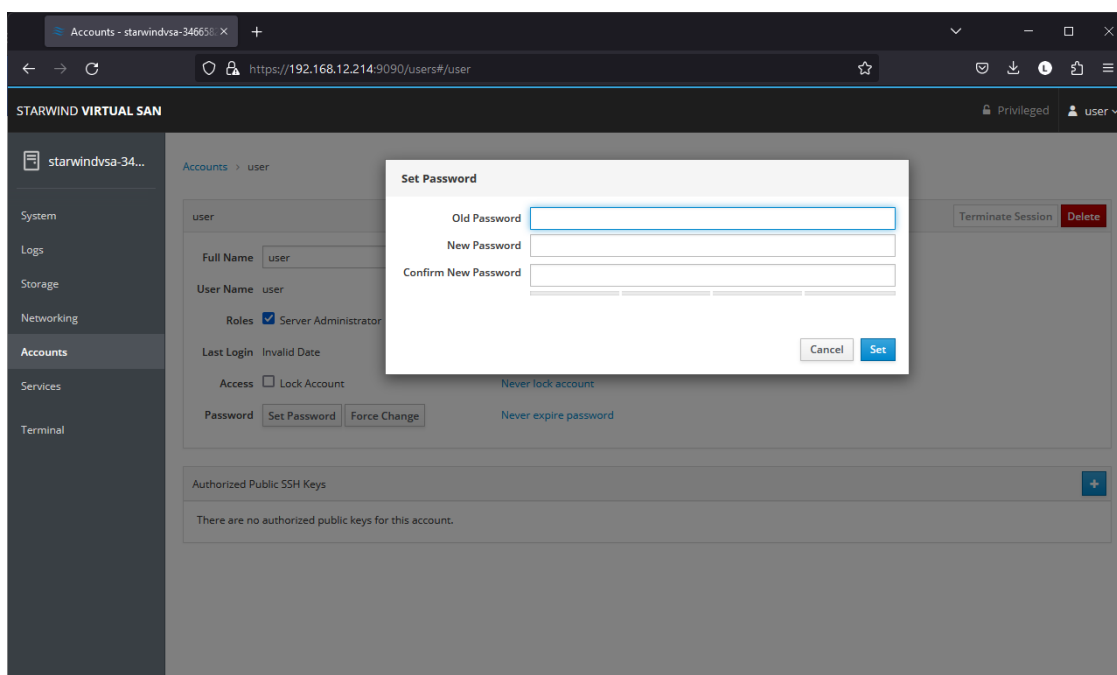
2. Now, open the web browser and enter the IP address of the VM. Log into the VM using the following default credentials:

- username: user
- password: rds123RDS
- NOTE: Make sure to check the “Reuse my password for privileged tasks” box

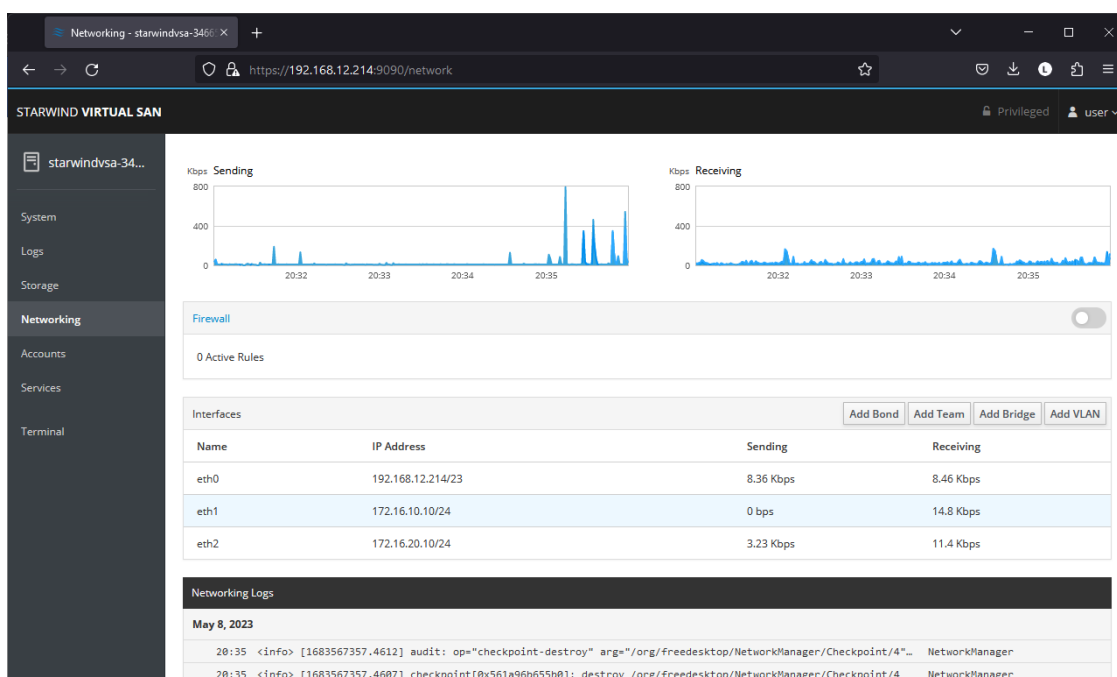


3. After a successful login, click Accounts on the left sidebar.

4. Select a user and click Set Password.

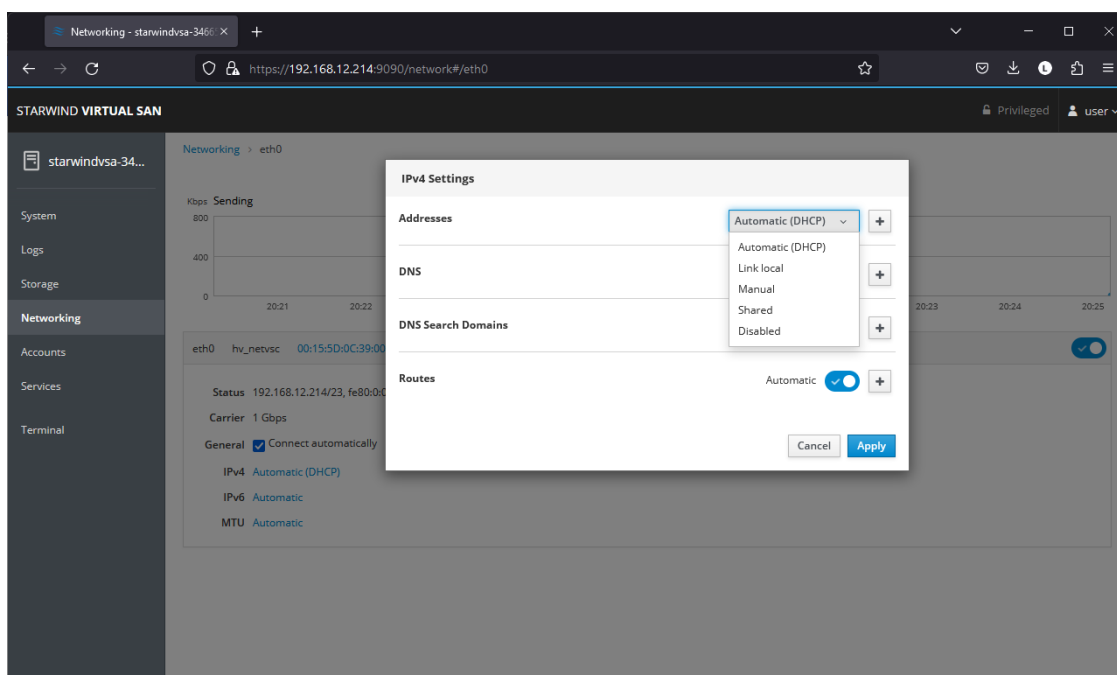


5. On the left sidebar, click Networking.

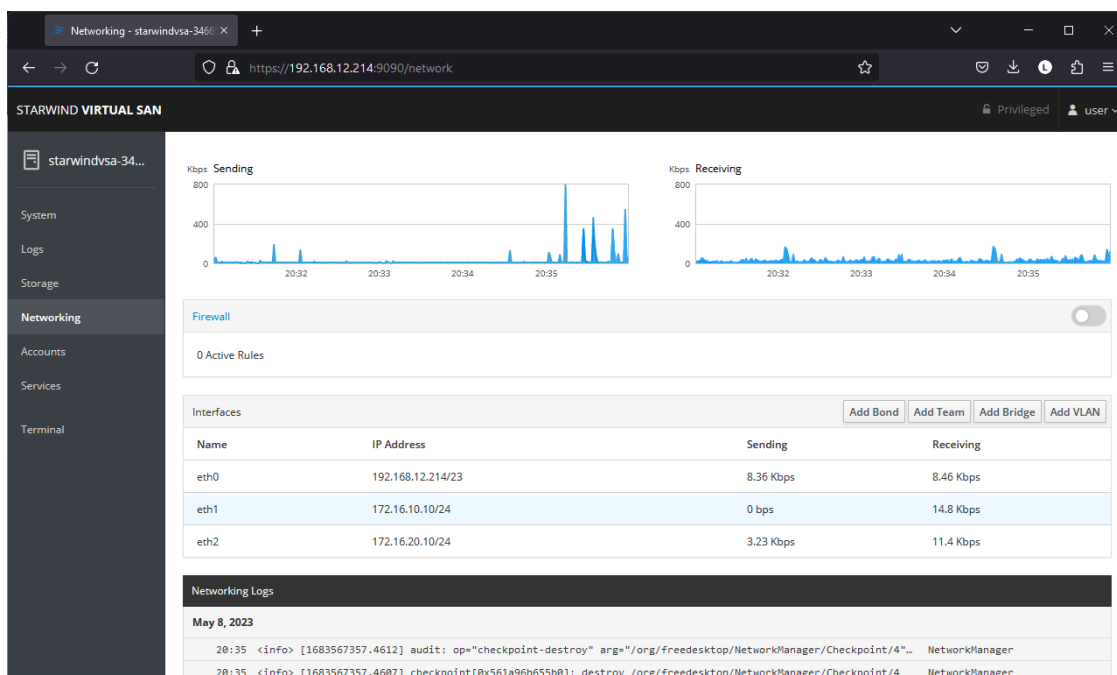


Here, the Management IP address of the StarWind Virtual SAN Virtual Machine can be configured, as well as IP addresses for iSCSI and Synchronization networks. In case the Network interface is inactive, click on the interface, turn it on, and set it to Connect automatically.

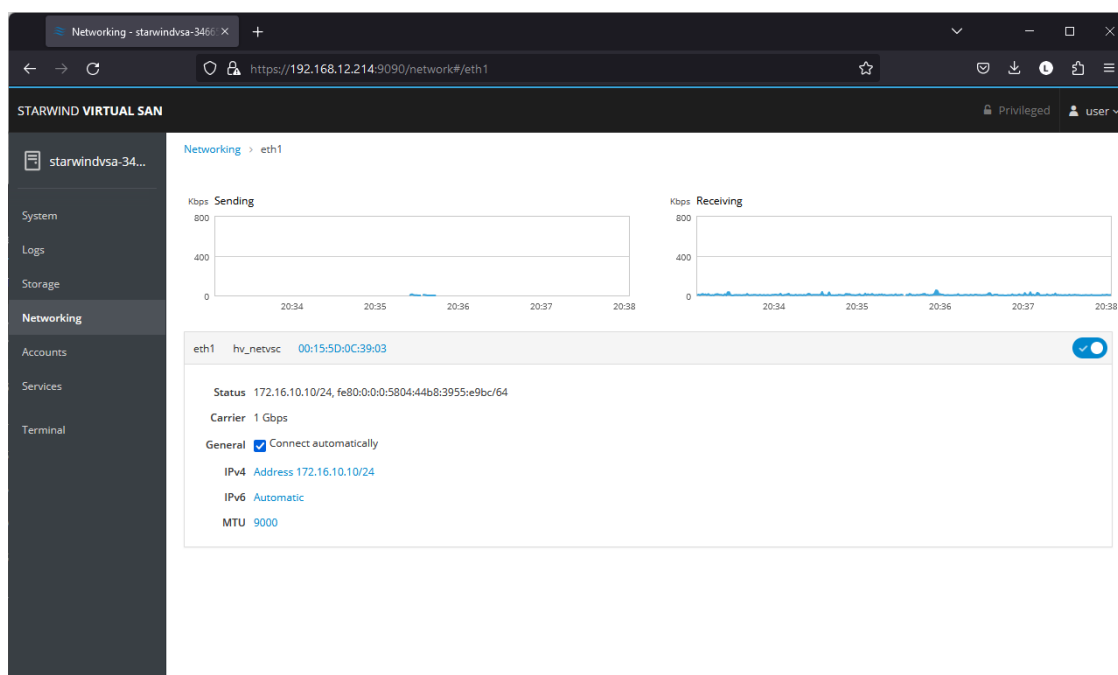
6. Click on Automatic (DHCP) to set the IP address (DNS and gateway – for Management).



7. The result should look like in the picture below:



NOTE: It is recommended to set MTU to 9000 on interfaces dedicated for iSCSI and Synchronization traffic. Change Automatic to 9000, if required.



8. Alternatively, log into the VM via the VMware console and assign a static IP address by editing the configuration file of the interface located by the following path:  
`/etc/sysconfig/network-scripts`

9. Open the file corresponding to the Management interface using a text editor, for example: `sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0`

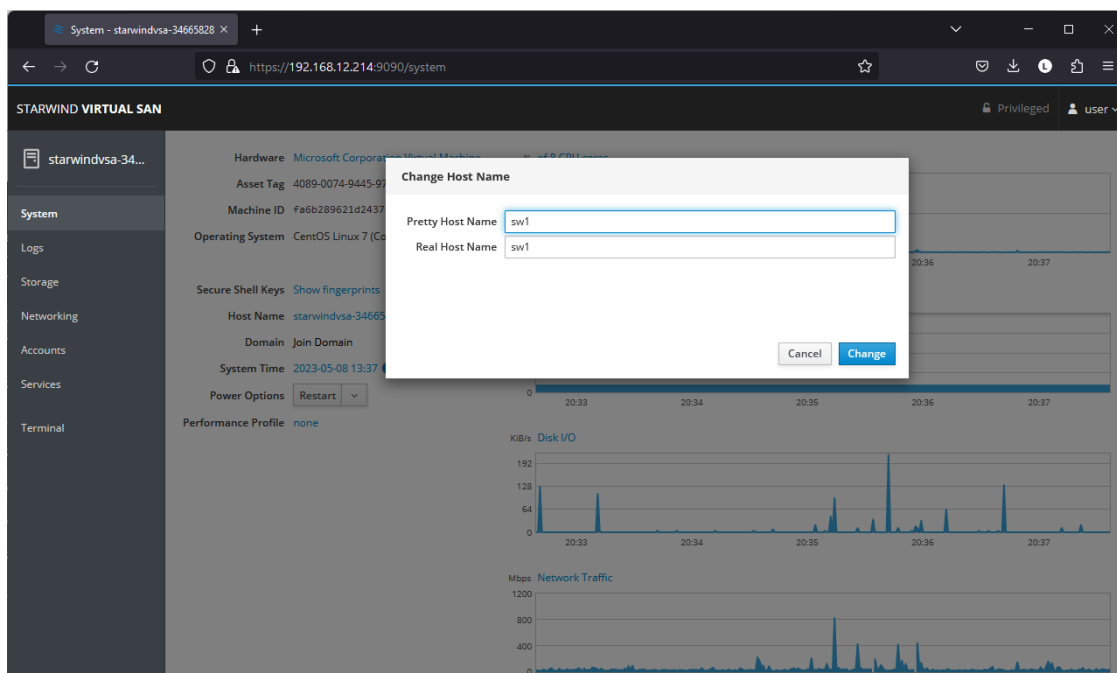
10. Edit the file:

- change the line `BOOTPROTO=dhcp` to: `BOOTPROTO=static`
- add the IP settings needed to the file:
- `IPADDR=192.168.12.10`
- `NETMASK=255.255.255.0`
- `GATEWAY=192.168.12.1`
- `DNS1=192.168.1.1`

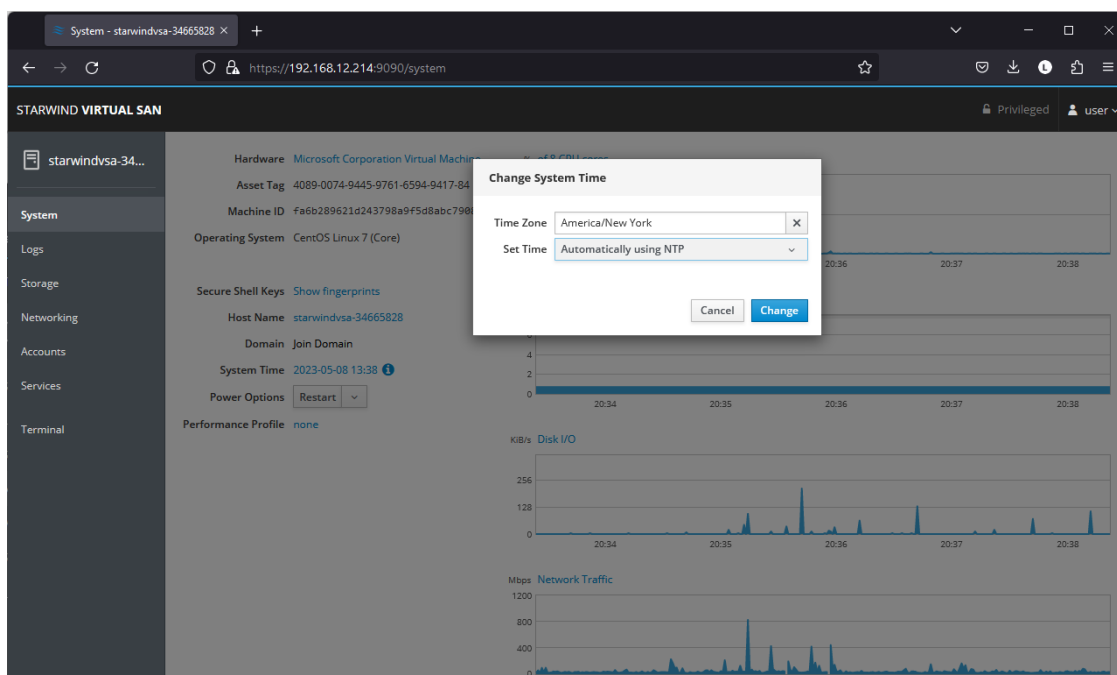
11. Restart the interface using the following cmdlet: `sudo ifdown eth0`, `sudo ifup eth0`, or restart the VM.

12. Change the Host Name from the System tab by clicking on it:





13. Change System time and NTP settings if required:



14. Repeat the steps above on each StarWind VSAN VM.

## Configuring Storage

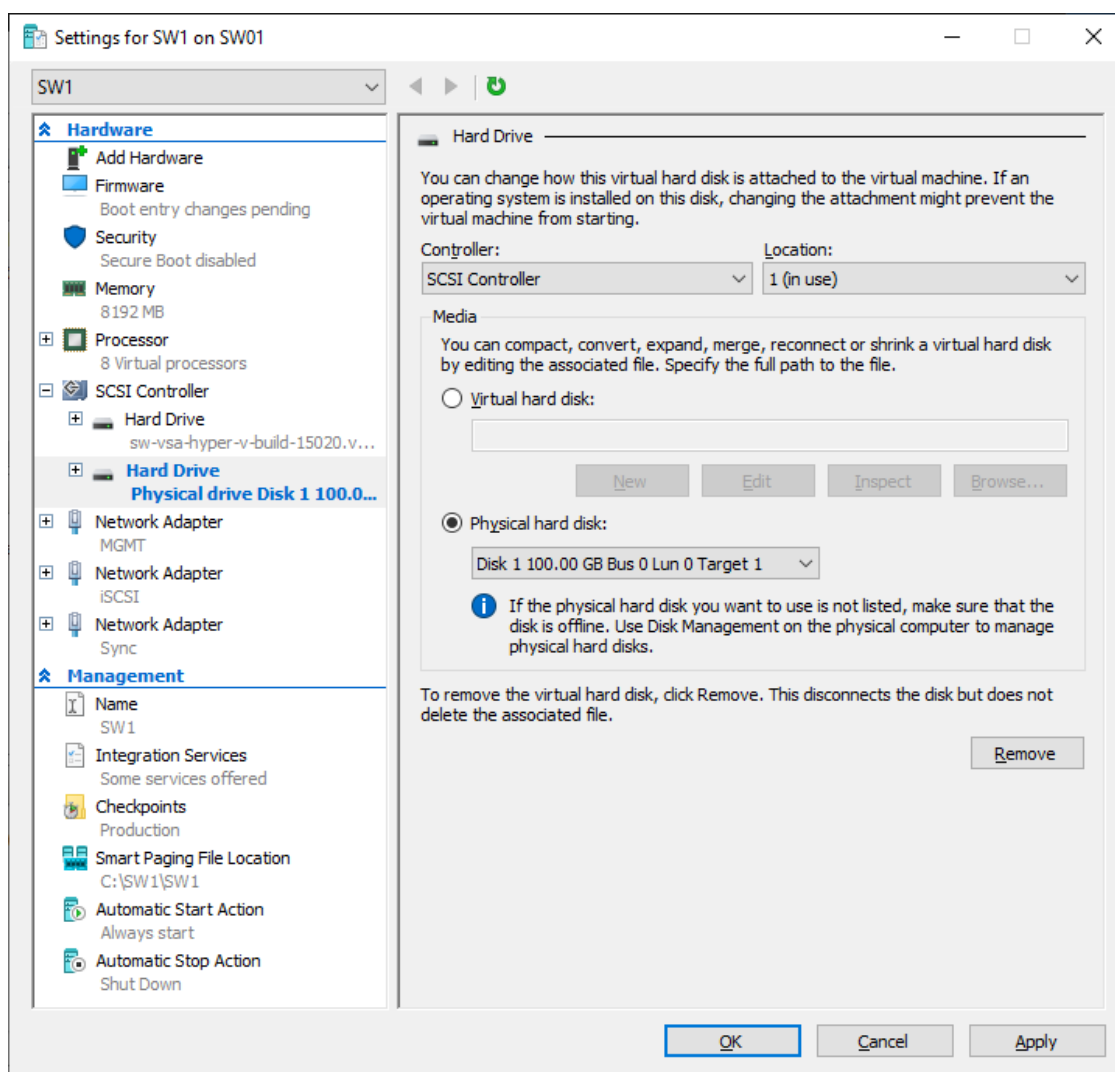
StarWind Virtual SAN for vSphere can work on top of Hardware RAID or Linux Software RAID (MDADM) inside of the Virtual Machine.

Please select the required option:

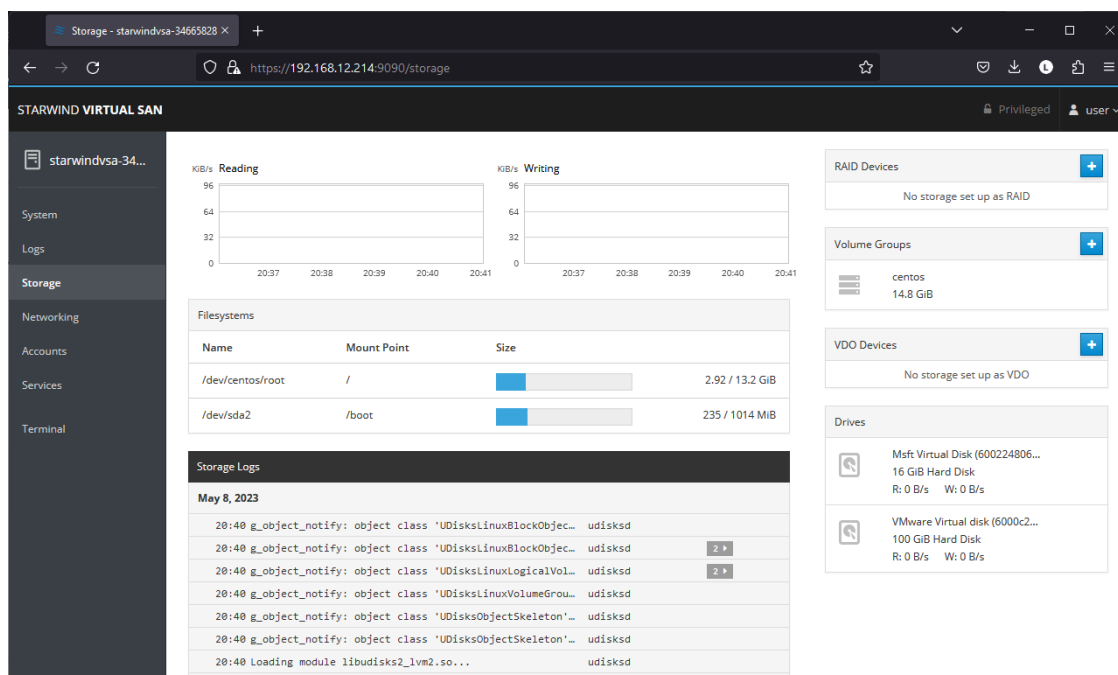
## Configuring Storage With Hardware Raid

1. Open VM Settings in Hyper-V and add drive to the VM, which going to be used by StarWind service. It is recommended to pass the entire RAID array to the VM by selecting a physical hard disk option.

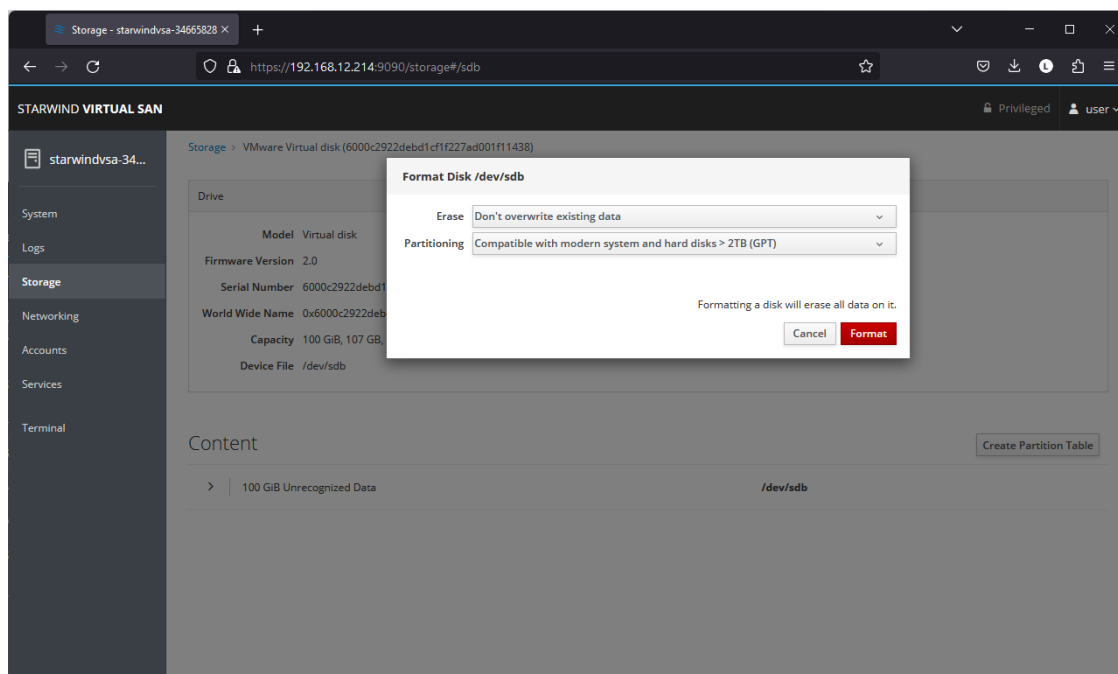
NOTE: Using virtual hard disks is not recommended due to potential performance issues. Thick provisioned virtual disks should be used to improve storage performance.



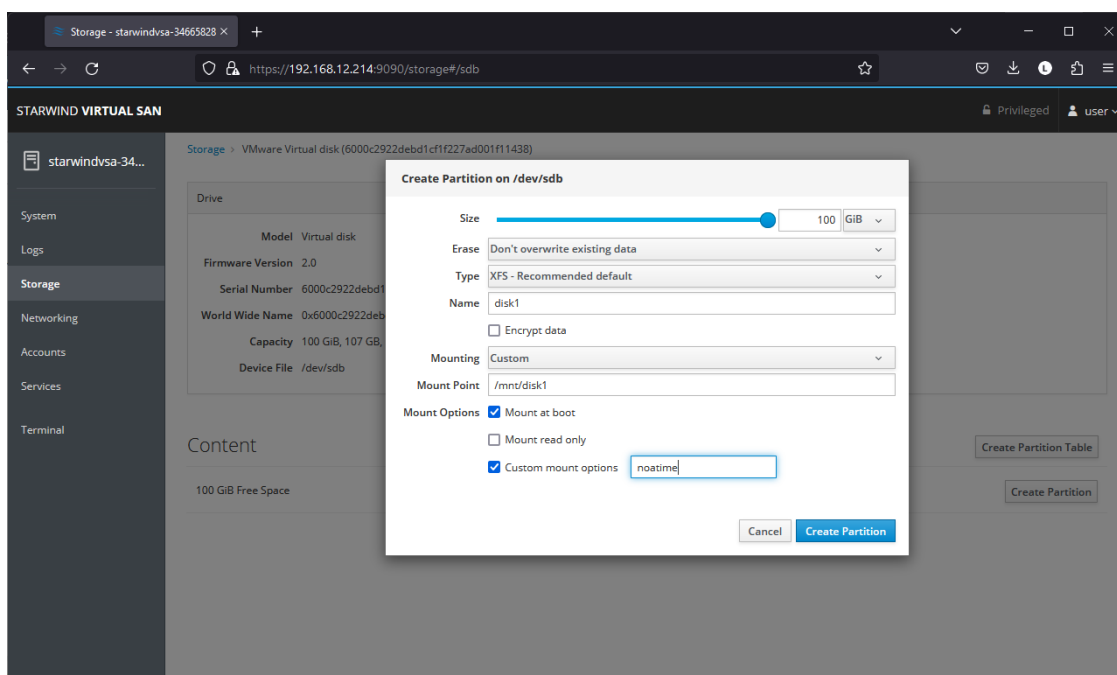
2. Login to StarWind VSAN VM web console and access the Storage section. Locate the recently added disk in the Drives section and choose it.



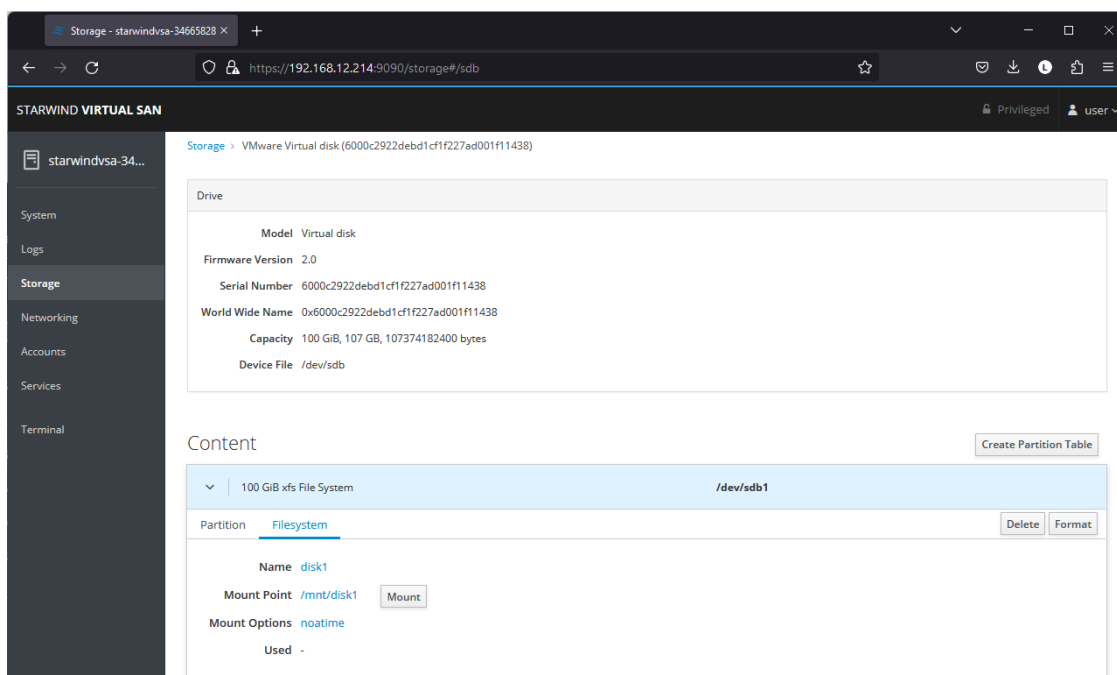
3. The added disk does not have any partitions and filesystem. Press the Create Partition Table button to create the partition.



4. Press Create Partition to format the disk and set the mount point. The mount point should be as follows: /mnt/%yourdiskname%



5. On the Storage section, under Content, navigate to the Filesystem tab. Click Mount.



## Configuring Starwind Management Console

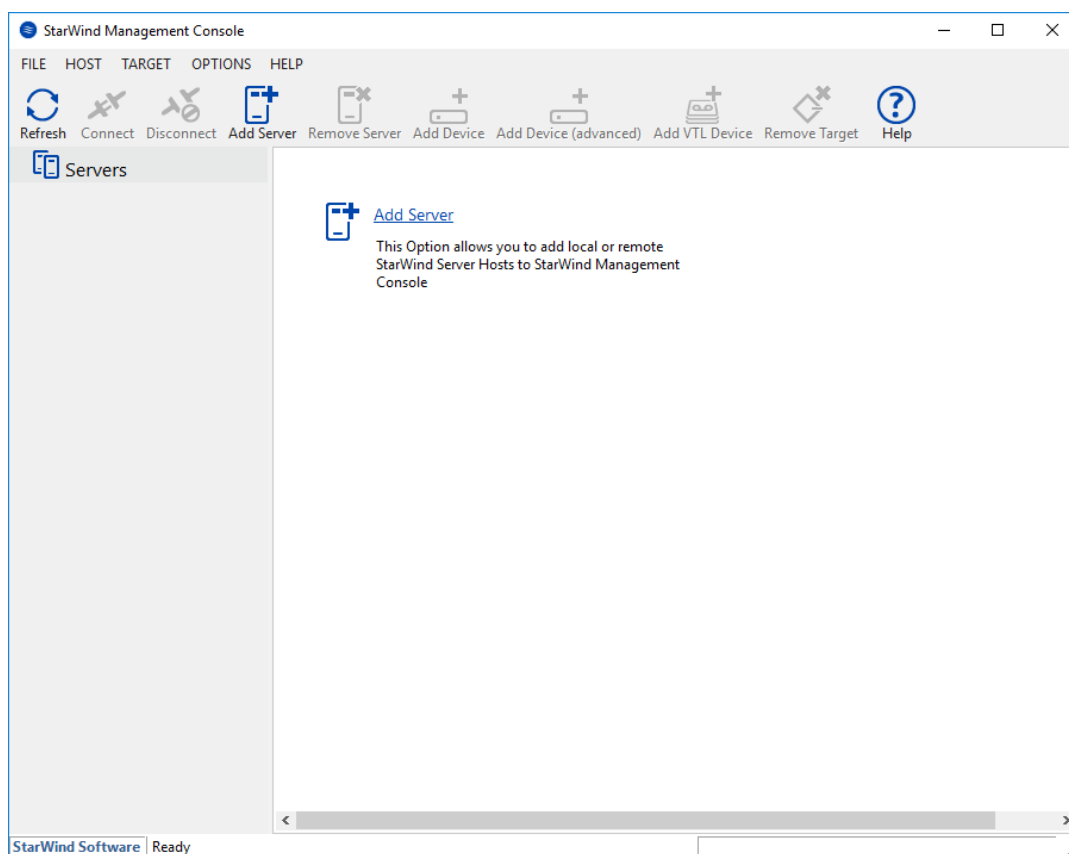
1. Install StarWind Management Console on each server or on a separate workstation with Windows OS (Windows 7 or higher, Windows Server 2008 R2 and higher) using the installer available here.

NOTE: StarWind Management Console and PowerShell Management Library components are required.

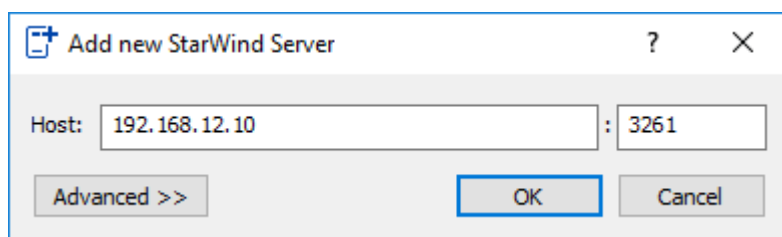
2. Select the appropriate option to apply the StarWind License key.

Once the appropriate license key has been received, it should be applied to StarWind Virtual SAN service via Management Console or PowerShell.

3. Open StarWind Management Console and click Add Server.

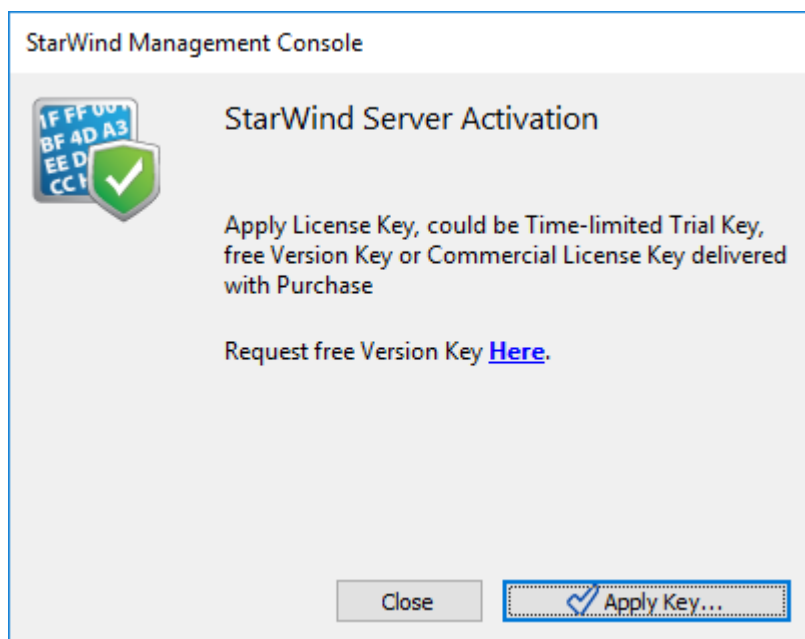


4. Type the IP address of the StarWind Virtual SAN in the pop-up window and click OK.



5. Select the server and click Connect.

6. Click Apply Key... on the pop-up window.



7. Select Load license from file and click the Load button.

8. Select the appropriate license key.

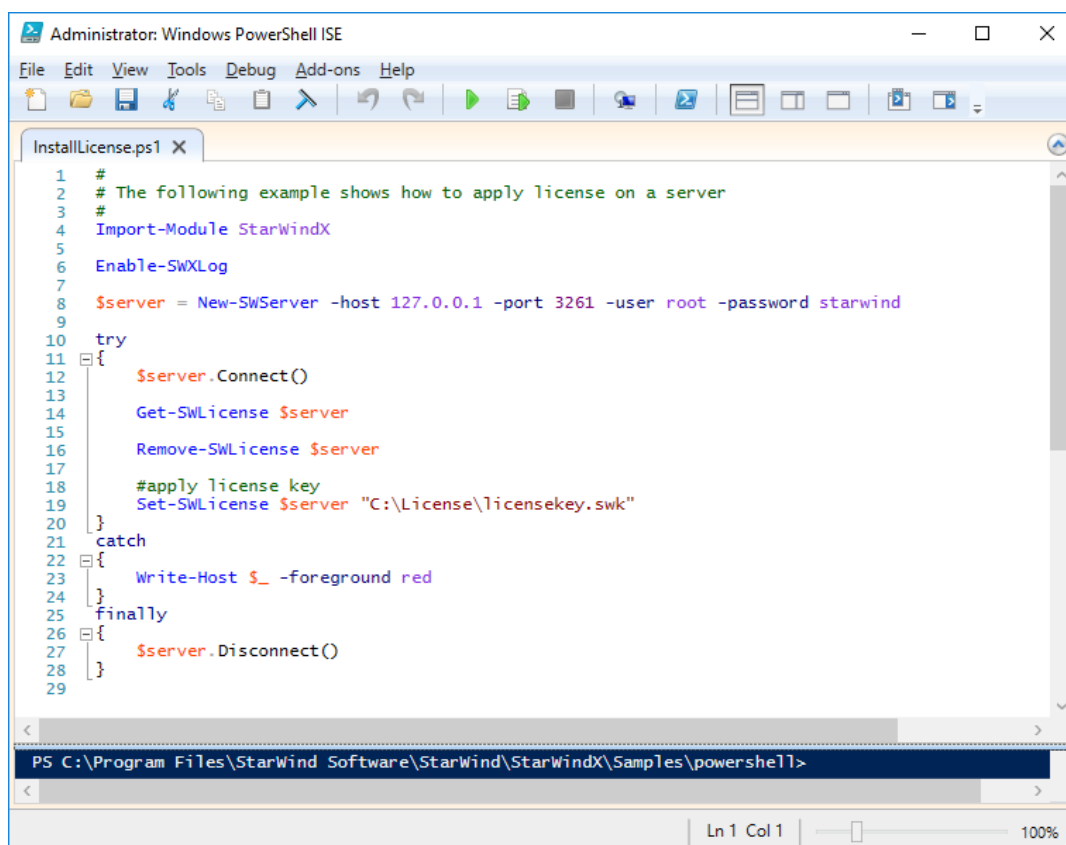
As an alternative, PowerShell can be used. Open StarWind InstallLicense.ps1 script with PowerShell ISE as administrator. It can be found here:

C:\Program Files\StarWind

Software\StarWind\StarWindX\Samples\powershell\InstallLicense.ps1

Type the IP address of StarWind Virtual SAN VM and credentials of StarWind Virtual SAN service (defaults login: root, password: starwind).

Add the path to the license key.



```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
InstallLicense.ps1 X
1 #
2 # The following example shows how to apply license on a server
3 #
4 Import-Module StarWindX
5
6 Enable-SWXLog
7
8 $server = New-SWServer -host 127.0.0.1 -port 3261 -user root -password starwind
9
10 try
11 {
12     $server.Connect()
13
14     Get-SWLicense $server
15
16     Remove-SWLicense $server
17
18     #apply license key
19     Set-SWLicense $server "C:\License\licensekey.swk"
20 }
21 catch
22 {
23     Write-Host $_ -foreground red
24 }
25 finally
26 {
27     $server.Disconnect()
28 }
29
PS C:\Program Files\StarWind Software\StarWind\StarWindX\Samples\powershell>
  
```

9. After the license key is applied, StarWind devices can be created.  
 NOTE: In order to manage StarWind Virtual SAN service (e.g. create ImageFile devices, VTL devices, etc.), StarWind Management Console can be used.

## Creating Starwind Ha Luns Using Powershell

1. Open PowerShell ISE as Administrator.
2. Open StarWindX sample CreateHA\_2.ps1 using PowerShell ISE. It can be found here:  
 C:\Program Files\StarWind Software\StarWind\StarWindX\Samples\

```

1 param($addr="192.168.12.10", $port=3261, $user="root", $password="starwind",
2 $addr2="192.168.12.11", $port2=$port, $user2=$user, $password2=$password,
3
4 #common
5 $initMethod="Clear",
6 $size=2048,
7 $sectorSize=512,
8 $failover=0,
9 $bmpType=1,
10 $bmpStrategy=0,
11
12 #primary node
13 $ImagePath="VSA Storage\mnt\crypted1",
14 $imageName="testha02",
15 $createImage=$true,
16 $storageName="",
17 $targetAlias="target02",
18 $autoSynch=$true,
19 $poolName="pool1",
20 $syncSessionCount=1,
21 $luaOptimized=$true,
22 $cacheMode="none",
23 $cacheSize=0,
24 $syncInterface="#p2={0}:3260" -f "172.16.10.20",
25 $hbInterface="#p2=172.16.20:3260",
26 $createTarget=$true,
27 $bmpFolderPath="",
28
29 #secondary node
30 $ImagePath2="VSA Storage\mnt\crypted1",
31 $imageName2="testha02",
32 $createImage2=$true,
33 $storageName2="",
34 $targetAlias2="target02",
35 $autoSynch2=$true,
36 $poolName2="pool1",
37 $syncSessionCount2=1,
38 $luaOptimized2=$false,
39 $cacheMode2=$cacheMode,
40 $cacheSize2=$cacheSize,
41 $syncInterface2="#p1={0}:3260" -f "172.16.10.10",
42 $hbInterface2="#p1=172.16.10.10:3260",
43 $createTarget2=$true,
44 $bmpFolderPath2="",
45
46 )
47
48 Import-Module StarWindX
49
50 try
51 {
52     Enable-SWLog -level SW_LOG_LEVEL_DEBUG
53     $server = New-SWServer -host $addr -port $port -user $user -password $password
54     $server.Connect()
55 }
56 catch
57 {
58     #Error handling
59 }

```

2. Configure script parameters according to the following example:

```

param($addr="192.168.12.10", $port=3261, $user="root",
$password="starwind",
    $addr2="192.168.12.11", $port2=$port, $user2=$user,
$password2=$password,
#common
    $initMethod="Clear",
    $size=2048,
    $sectorSize=512,
    $failover=0,
    $bmpType=1,
    $bmpStrategy=0,
#primary node
    $ImagePath="VSA Storage\mnt\crypted1",
    $imageName="testha02",
    $createImage=$true,
    $storageName="",
    $targetAlias="target02",
    $autoSynch=$true,

```



```

    $poolName="pool1",
    $syncSessionCount=1,
    $aluaOptimized=$true,
    $cacheMode="none",
    $cacheSize=0,
    $syncInterface="#p2={0}:3260" -f "172.16.20.20",
    $hbInterface="#p2={0}:3260" -f "172.16.10.20",
    $createTarget=$true,
    $bmpFolderPath="",
#secondary node
    $imagePath2="VSA Storage\mnt\crypted1",
    $imageName2="testtha02",
    $createImage2=$true,
    $storageName2="",
    $targetAlias2="target02",
    $autoSynch2=$true,
    $poolName2="pool1",
    $syncSessionCount2=1,
    $aluaOptimized2=$false,
    $cacheMode2=$cacheMode,
    $cacheSize2=$cacheSize,
    $syncInterface2="#p1={0}:3260" -f "172.16.20.10",
    $hbInterface2="#p1={0}:3260" -f "172.16.10.10",
    $createTarget2=$true,
    $bmpFolderPath2=""
  )
Import-Module StarWindX

try
{
    Enable-SWXLog -level SW_LOG_LEVEL_DEBUG

    $server = New-SWServer -host $addr -port $port -user
$user -password $password

    $server.Connect()

    $firstNode = new-Object Node

    $firstNode.HostName = $addr
    $firstNode.HostPort = $port
    $firstNode.Login = $user
    $firstNode.Password = $password
    $firstNode.ImagePath = $imagePath

```

```

$firstNode.ImageName = $imageName
$firstNode.Size = $size
$firstNode.CreateImage = $createImage
$firstNode.StorageName = $storageName
$firstNode.TargetAlias = $targetAlias
$firstNode.AutoSynch = $autoSynch
$firstNode.SyncInterface = $syncInterface
$firstNode.HBInterface = $hbInterface
$firstNode.PoolName = $poolName
$firstNode.SyncSessionCount = $syncSessionCount
$firstNode.ALUAOptimized = $aluaOptimized
$firstNode.CacheMode = $cacheMode
$firstNode.CacheSize = $cacheSize
$firstNode.FailoverStrategy = $failover
$firstNode.CreateTarget = $createTarget
$firstNode.BitmapStoreType = $bmpType
$firstNode.BitmapStrategy = $bmpStrategy
$firstNode.BitmapFolderPath = $bmpFolderPath
#
# device sector size. Possible values: 512 or 4096(May
be incompatible with some clients!) bytes.
#
$firstNode.SectorSize = $sectorSize
$secondNode = new-Object Node

$secondNode.HostName = $addr2
$secondNode.HostPort = $port2
$secondNode.Login = $user2
$secondNode.Password = $password2
$secondNode.ImagePath = $imagePath2
$secondNode.ImageName = $imageName2
$secondNode.CreateImage = $createImage2
$secondNode.StorageName = $storageName2
$secondNode.TargetAlias = $targetAlias2
$secondNode.AutoSynch = $autoSynch2
$secondNode.SyncInterface = $syncInterface2
$secondNode.HBInterface = $hbInterface2
$secondNode.SyncSessionCount = $syncSessionCount2
$secondNode.ALUAOptimized = $aluaOptimized2
$secondNode.CacheMode = $cacheMode2
$secondNode.CacheSize = $cacheSize2
$secondNode.FailoverStrategy = $failover
$secondNode.CreateTarget = $createTarget2
$secondNode.BitmapFolderPath = $bmpFolderPath2

```

```

    $device = Add-HADevice -server $server -firstNode
$firstNode -secondNode $secondNode -initMethod $initMethod
    while ($device.SyncStatus -ne
[SwHaSyncStatus]::SW_HA_SYNC_STATUS_SYNC)
    {
        $syncPercent =
$device.GetPropertyValue("ha_synch_percent")
        Write-Host "Synchronizing: $($syncPercent)%" -
foreground yellow

        Start-Sleep -m 2000

        $device.Refresh()
    }
}
catch
{
    Write-Host $_ -foreground red
}
finally
{
    $server.Disconnect()
}

```

Detailed explanation of script parameters:

-addr, -addr2 — partner nodes IP address.

Format: string. Default value: 192.168.0.1, 192.168.0.1

allowed values: localhost, IP-address

-port, -port2 — local and partner node port.

Format: string. Default value: 3261

-user, -user2 — local and partner node user name.

Format: string. Default value: root

-password, -password2 — local and partner node user password.

Format: string. Default value: starwind

#common

-initMethod -

Format: string. Default value: Clear

-size - set size for HA-devcie (MB)

Format: integer. Default value: 12

-sectorSize - set sector size for HA-device

Format: integer. Default value: 512

allowed values: 512, 4096

-failover – set type failover strategy  
 Format: integer. Default value: 0 (Heartbeat)  
 allowed values: 0, 1 (Node Majority)  
 -bmpType – set bitmap type, is set for both partners at once  
 Format: integer. Default value: 1 (RAM)  
 allowed values: 1, 2 (DISK)  
 -bmpStrategy – set journal strategy, is set for both partners at once  
 Format: integer. Default value: 0  
 allowed values: 0, 1 – Best Performance (Failure), 2 – Fast Recovery (Continuous)

#primary node

-imagePath – set path to store the device file  
 Format: string. Default value: My computer\C\starwind". For Linux the following format should be used: "VSA Storage\mnt\mount\_point"  
 -imageName – set name device  
 Format: string. Default value: masterImg21  
 -createImage – set create image file  
 Format: boolean. Default value: true  
 -targetAlias – set alias for target  
 Format: string. Default value: targetha21  
 -poolName – set storage pool  
 Format: string. Default value: pool1  
 -aluaOptimized – set Alua Optimized  
 Format: boolean. Default value: true  
 -cacheMode – set type L1 cache (optional parameter)  
 Format: string. Default value: wb  
 allowed values: none, wb, wt  
 -cacheSize – set size for L1 cache in MB (optional parameter)  
 Format: integer. Default value: 128  
 allowed values: 1 and more  
 -syncInterface – set sync channel IP-address from partner node  
 Format: string. Default value: "#p2={0}:3260"  
 -hbInterface – set heartbeat channel IP-address from partner node  
 Format: string. Default value: ""  
 -createTarget – set creating target  
 Format: string. Default value: true  
 Even if you do not specify the parameter -createTarget, the target will be created automatically.  
 If the parameter is set as -createTarget \$false, then an attempt will be made to create the device with existing targets, the names of which are specified in the -targetAlias (targets must already be created)  
 -bmpFolderPath – set path to save bitmap file  
 Format: string.

#secondary node

- imagePath2 – set path to store the device file  
 Format: string. Default value: “My computer\C\starwind”. For Linux the following format should be used: “VSA Storage\mnt\mount\_point”
- imageName2 – set name device  
 Format: string. Default value: masterImg21
- createImage2 – set create image file  
 Format: boolean. Default value: true
- targetAlias2 – set alias for target  
 Format: string.  
 Default value: targetha22
- poolName2 – set storage pool  
 Format: string. Default value: pool1
- aluaOptimized2 – set Alua Optimized  
 Format: boolean. Default value: true
- cacheMode2 – set type L1 cache (optional parameter)  
 Format: string. Default value: wb  
 allowed values: wb, wt
- cacheSize2 – set size for L1 cache in MB (optional parameter)  
 Format: integer. Default value: 128  
 allowed values: 1 and more
- syncInterface2 – set sync channel IP-address from partner node  
 Format: string. Default value: “#p1={0}:3260”
- hbInterface2 – set heartbeat channel IP-address from partner node  
 Format: string. Default value: “”
- createTarget2 – set creating target  
 Format: string. Default value: true

Even if you do not specify the parameter -createTarget, the target will be created automatically. If the parameter is set as -createTarget \$false, then an attempt will be made to create the device with existing targets, the names of which are specified in the -targetAlias (targets must already be created)

- bmpFolderPath2 – set path to save bitmap file  
 Format: string.

## 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.

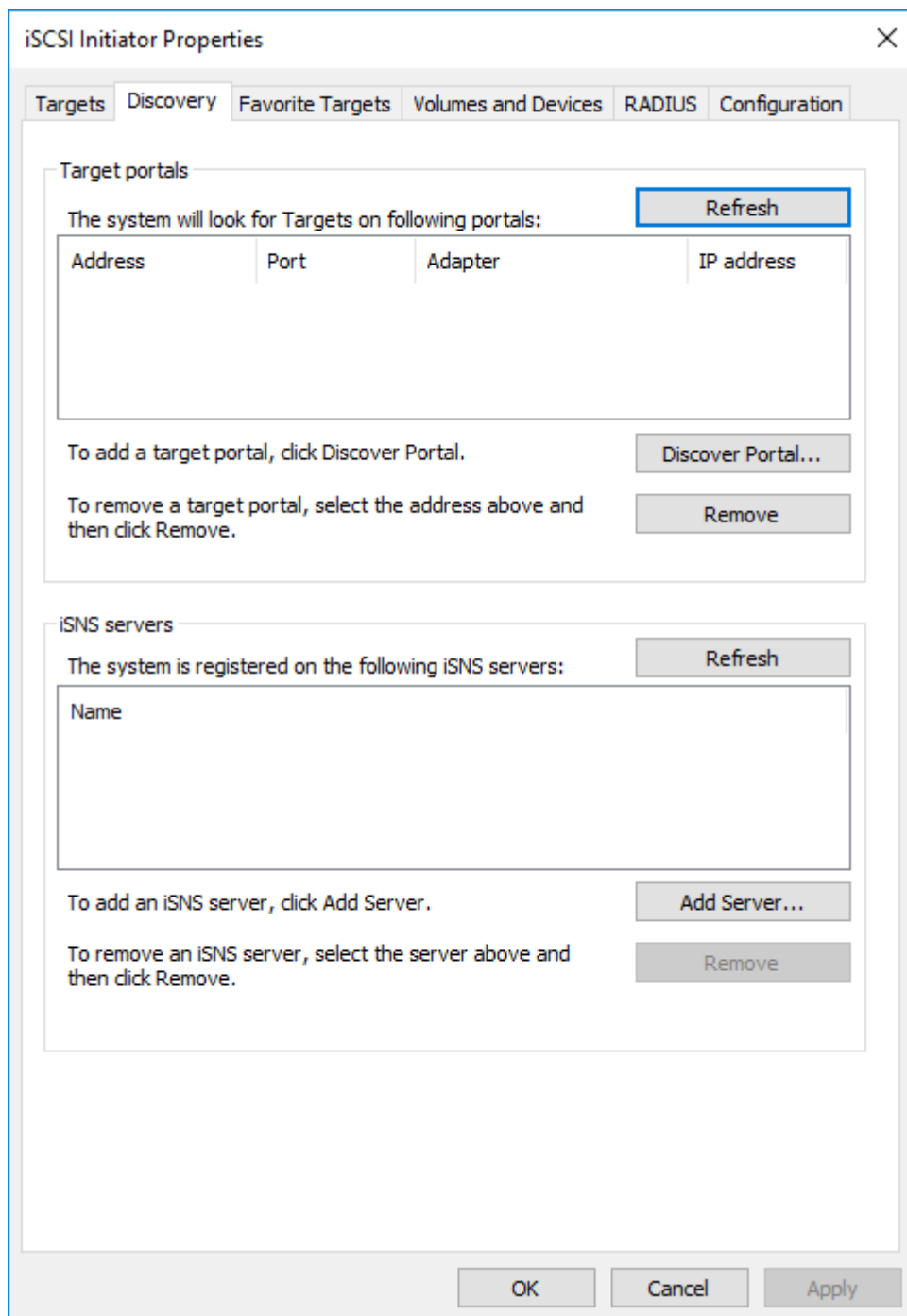
Please select the required option:

## Provisioning Starwind Ha Storage To Windows Server Hosts

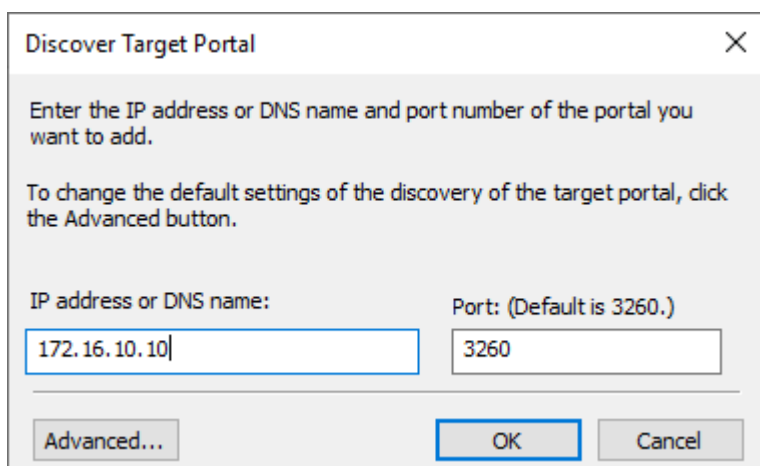
1. Launch Microsoft iSCSI Initiator: Start -> Windows Administrative Tools -> iSCSI Initiator. Alternatively, launch it using the command below in the command line interface:

```
iscsicpl
```

2. Navigate to the Discovery tab.



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



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

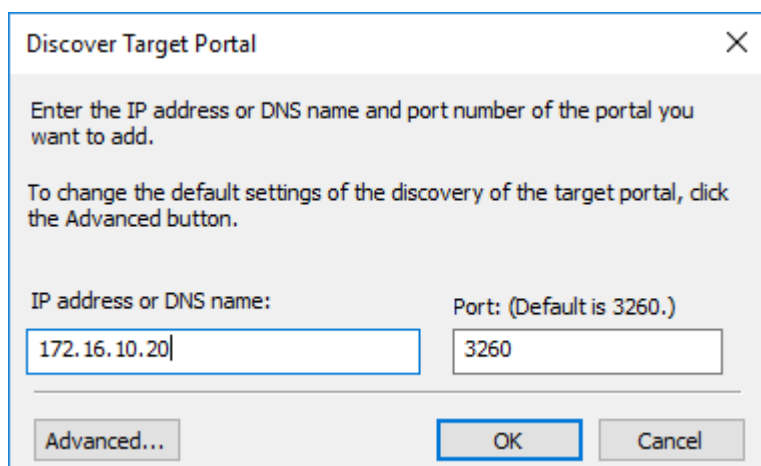
4. Click the Advanced button. Select Microsoft iSCSI Initiator as a Local adapter and select Initiator IP. Confirm the actions to complete the Target Portal discovery.



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

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

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

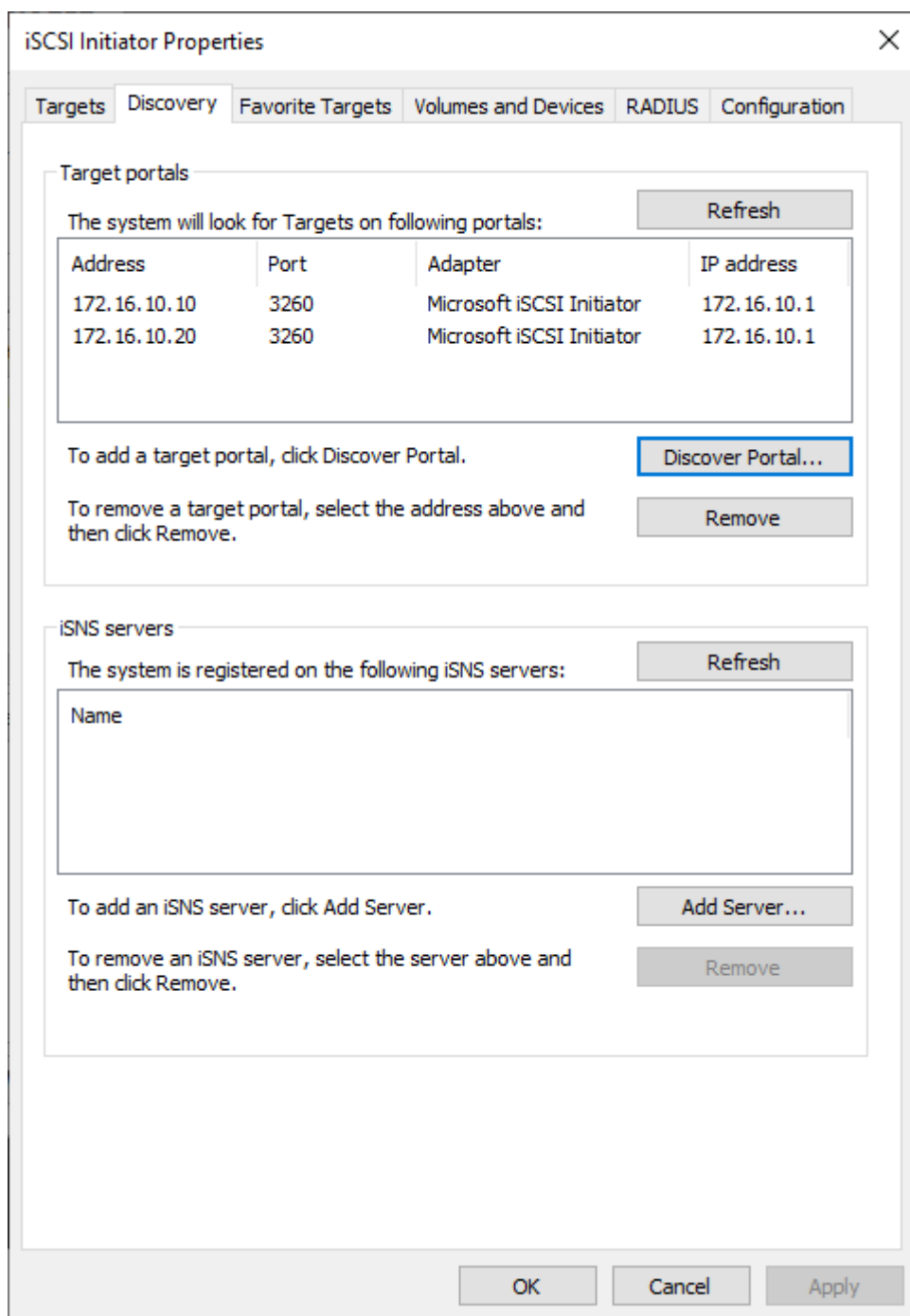


The image shows a 'Discover Target Portal' dialog box with a close button (X) in the top right corner. Inside the dialog, there is instructional text: 'Enter the IP address or DNS name and port number of the portal you want to add.' and 'To change the default settings of the discovery of the target portal, click the Advanced button.' Below this text are two input fields. The first field is labeled 'IP address or DNS name:' and contains the text '172.16.10.20'. The second field is labeled 'Port: (Default is 3260.)' and contains the text '3260'. At the bottom of the dialog, there are three buttons: 'Advanced...', 'OK', and 'Cancel'. The 'OK' button is highlighted with a blue border.

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

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

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



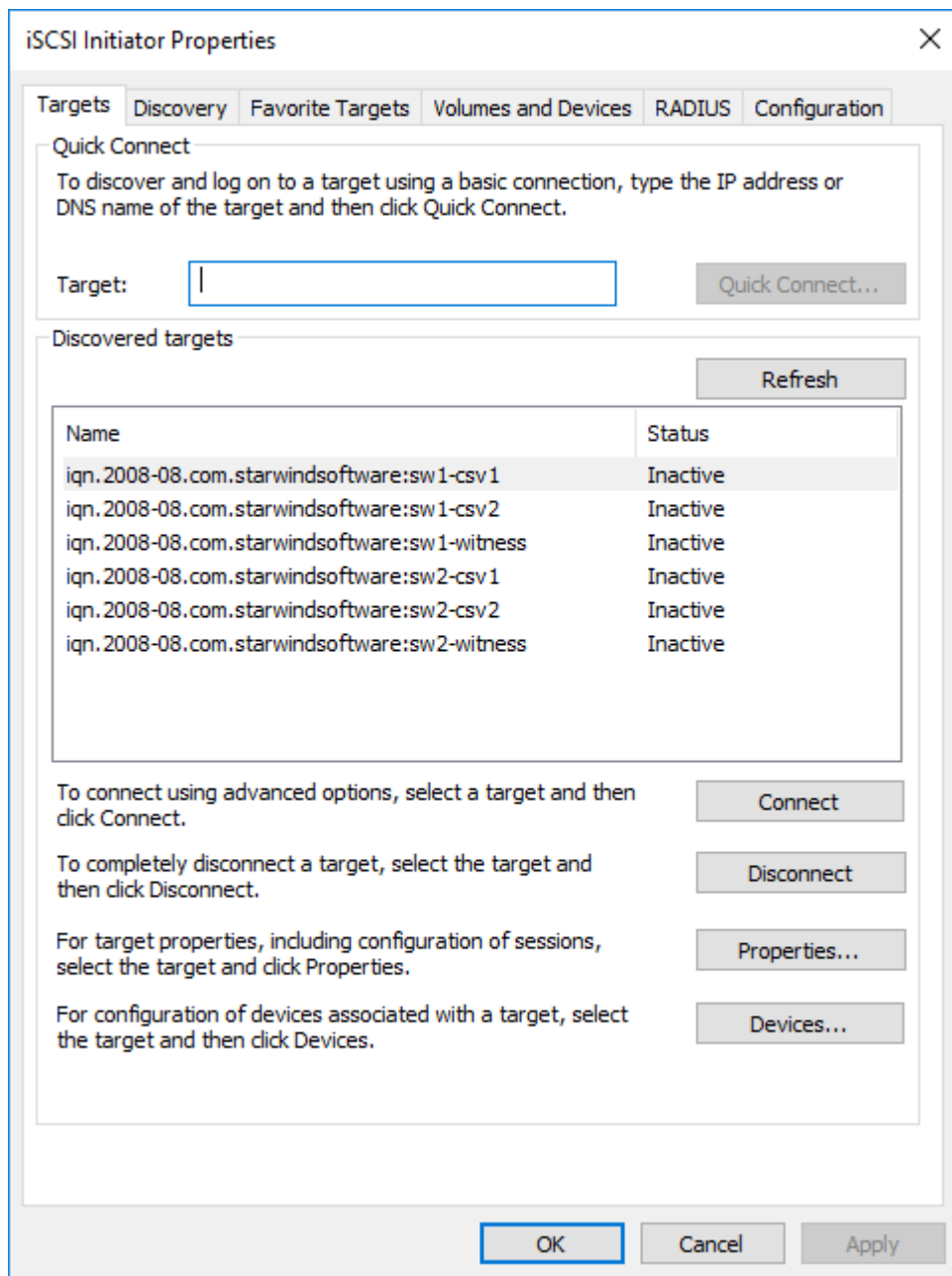
9. Repeat the steps 1-8 on the partner node.

### Connecting Targets

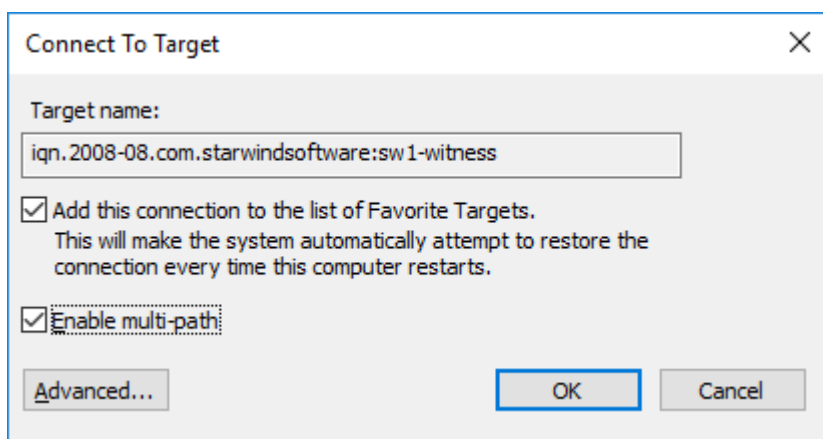
1. Click the Targets tab. The previously created targets are listed in the Discovered Targets section.

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

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



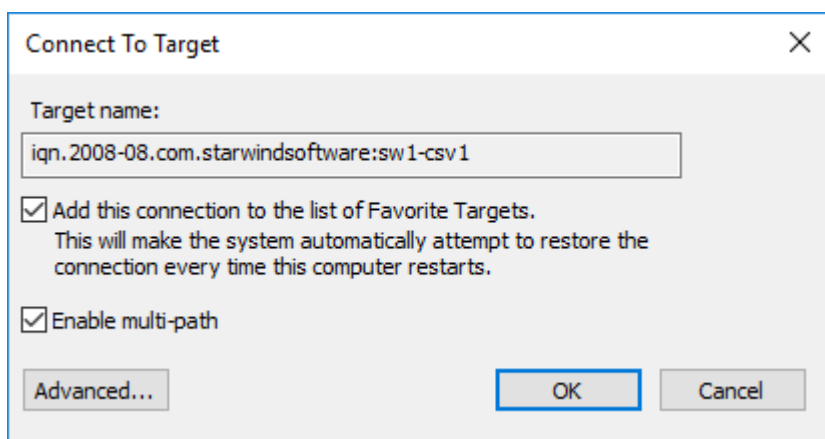
2. Select the Witness target from the local server and click Connect.
3. Enable checkboxes as shown in the image below. Click Advanced.



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

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

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



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

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

10. Repeat the step 6.

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



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

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

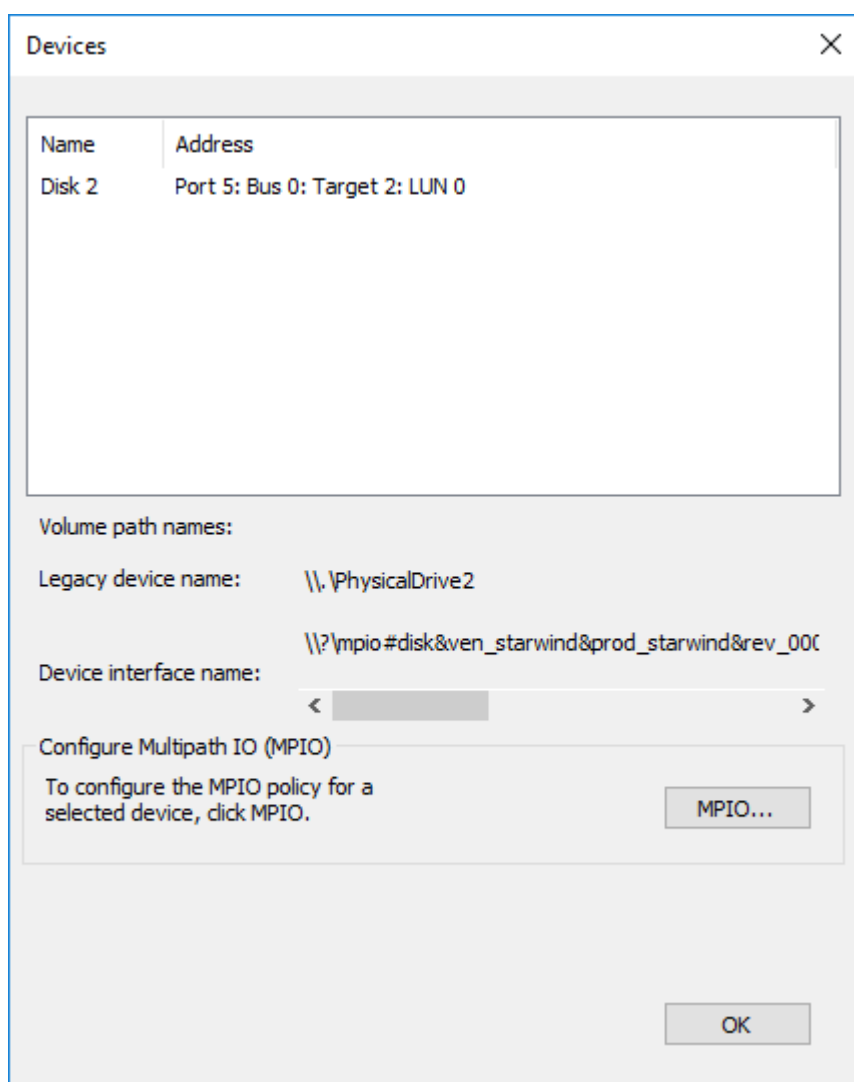
12. Repeat the steps 1-11 on the other StarWind node, specifying corresponding data channel IP addresses.

### Configuring Multipath

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

load balancing policy.

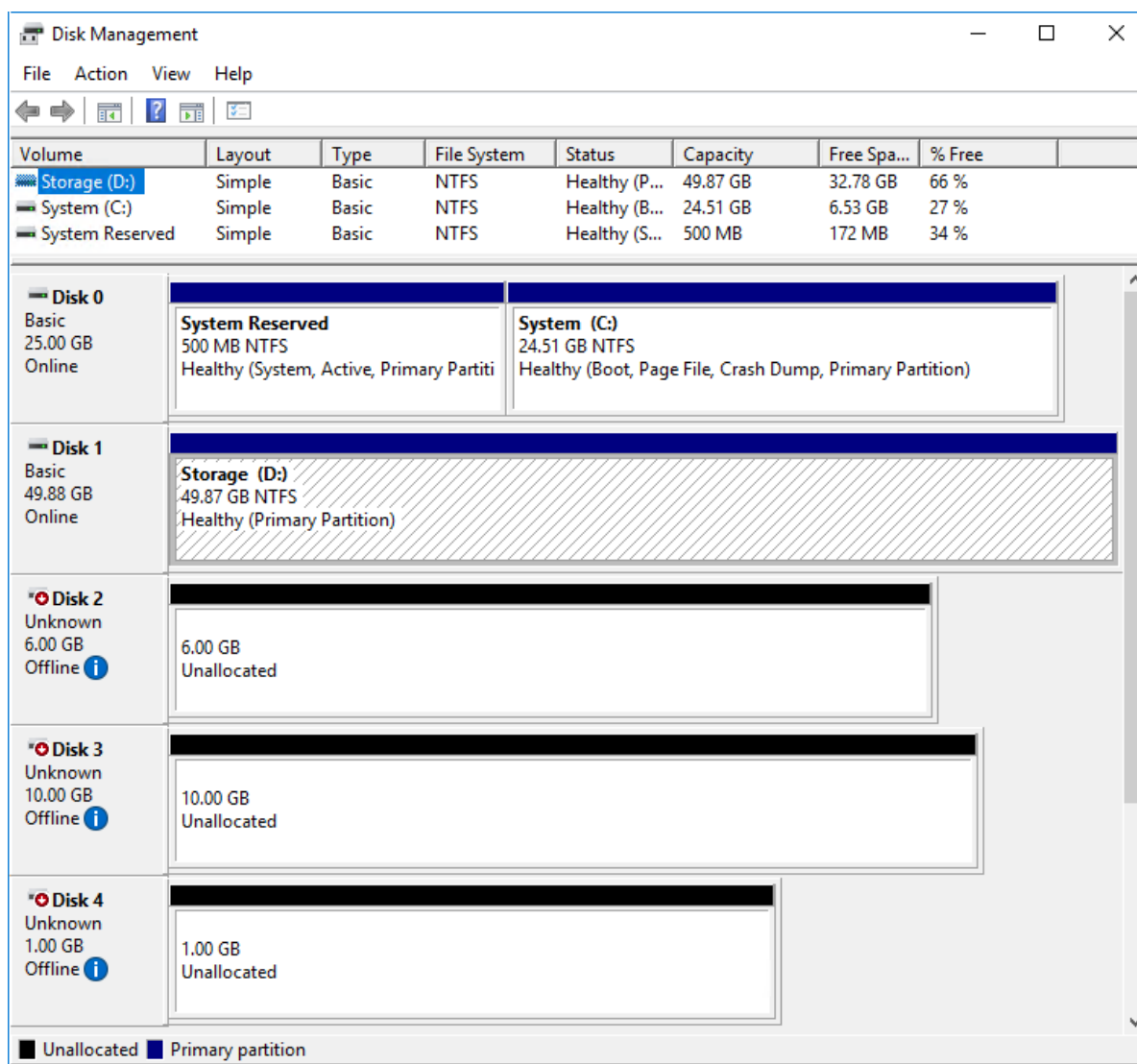
1. Configure the MPIO policy for each target with the load balance policy of choice. Select the Target located on the local server and click Devices.
2. In the Devices dialog, click MPIO.



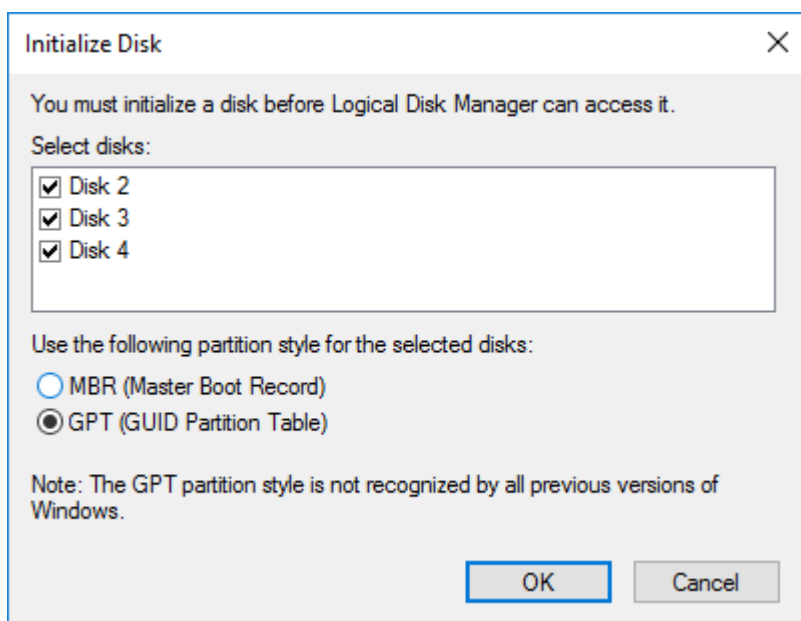
3. Select the appropriate load balancing policy.
4. Repeat the steps 1-3 for configuring the MPIO policy for each remaining device on the current node and on the partner node.

### Connecting Disks to Servers

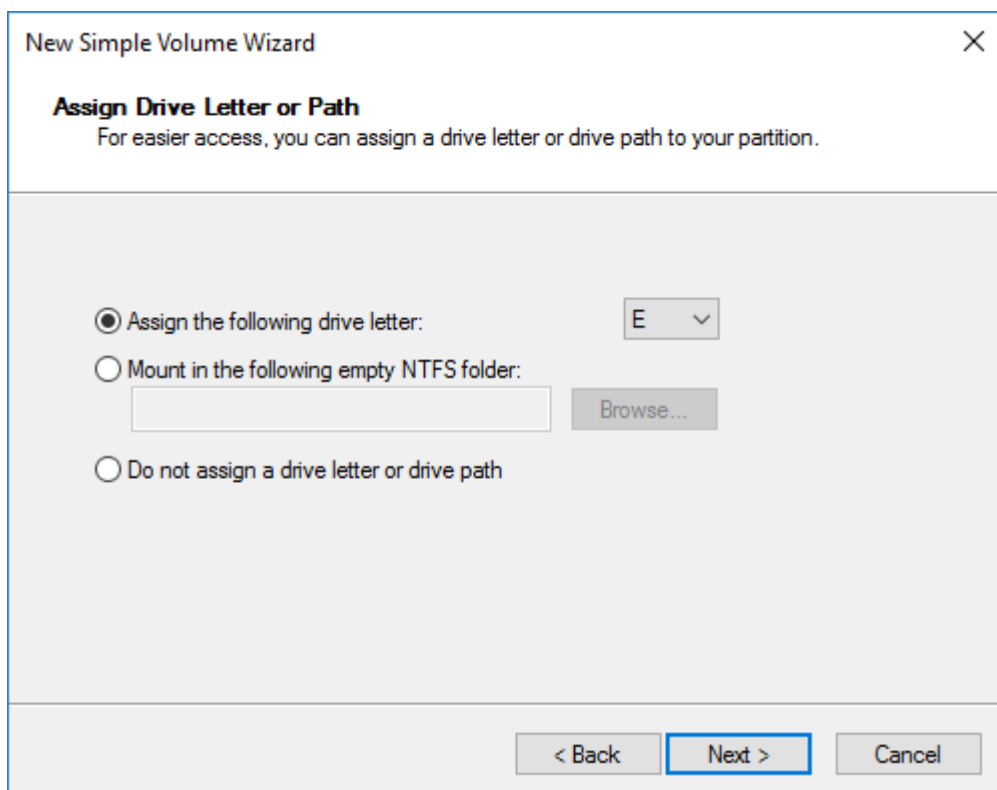
1. Open the Disk Management snap-in. The StarWind disks will appear as unallocated and offline.



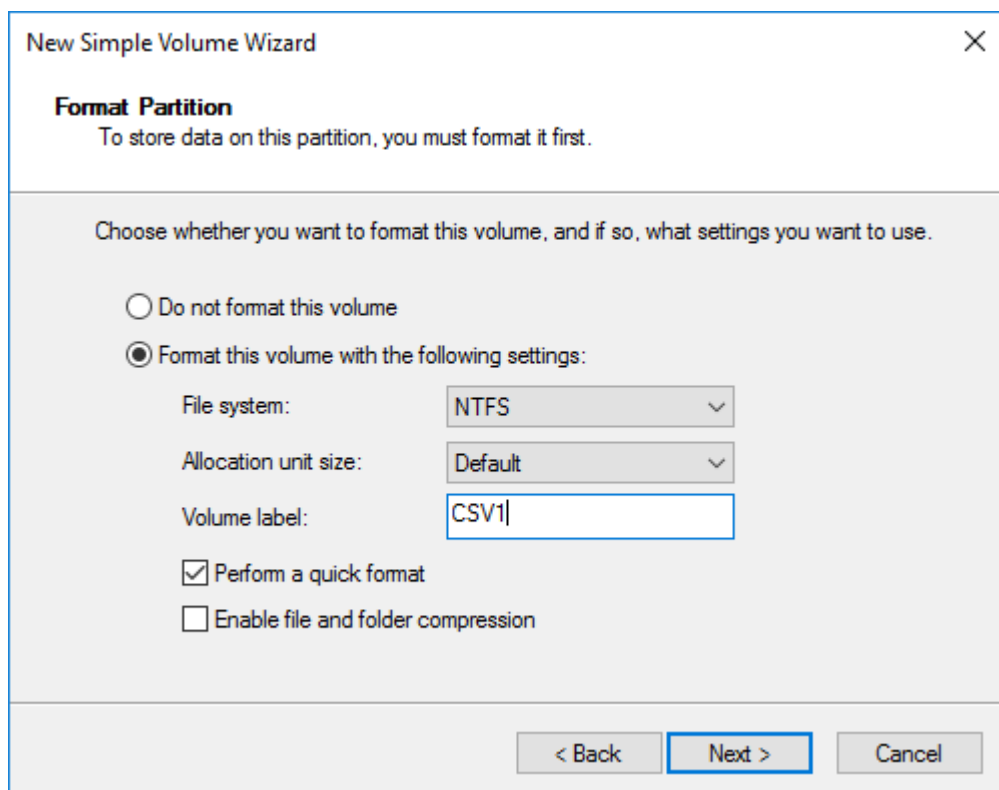
2. Bring the disks online by right-clicking on them and selecting the Online menu option.
3. Select the CSV disk (check the disk size to be sure) and right-click on it to initialize.
4. By default, the system will offer to initialize all non-initialized disks. Use the Select Disks area to choose the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



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



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



**New Simple Volume Wizard** [X]

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

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

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS [v]

Allocation unit size: Default [v]

Volume label: CSV1

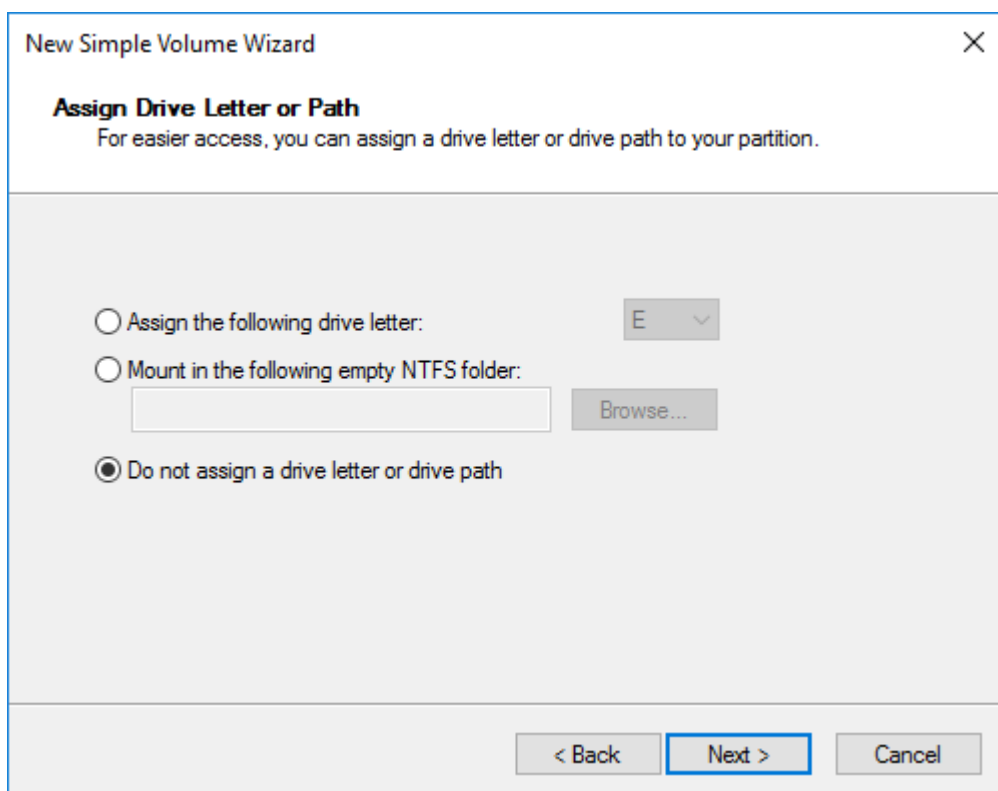
☒ Perform a quick format

☐ Enable file and folder compression

< Back   **Next >**   Cancel

9. Press Finish to complete.

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



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

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

## Creating A Failover Cluster In Windows Server

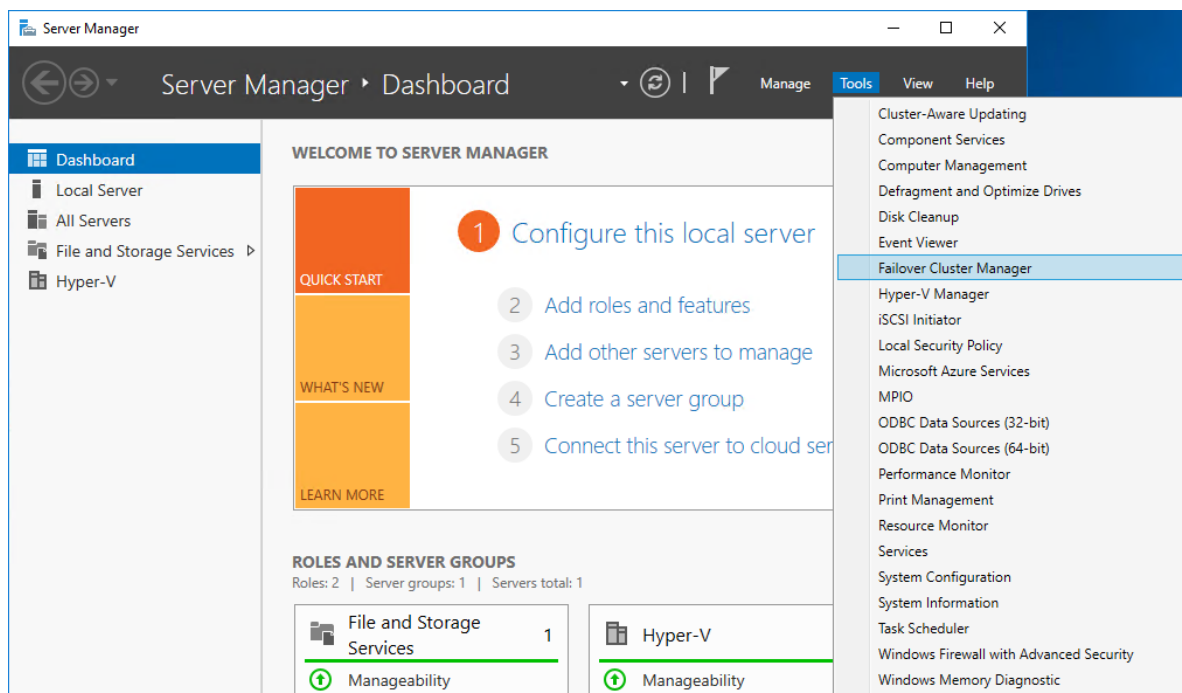
NOTE: To avoid issues during the cluster validation configuration, it is recommended to install the latest Microsoft updates on each node.

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

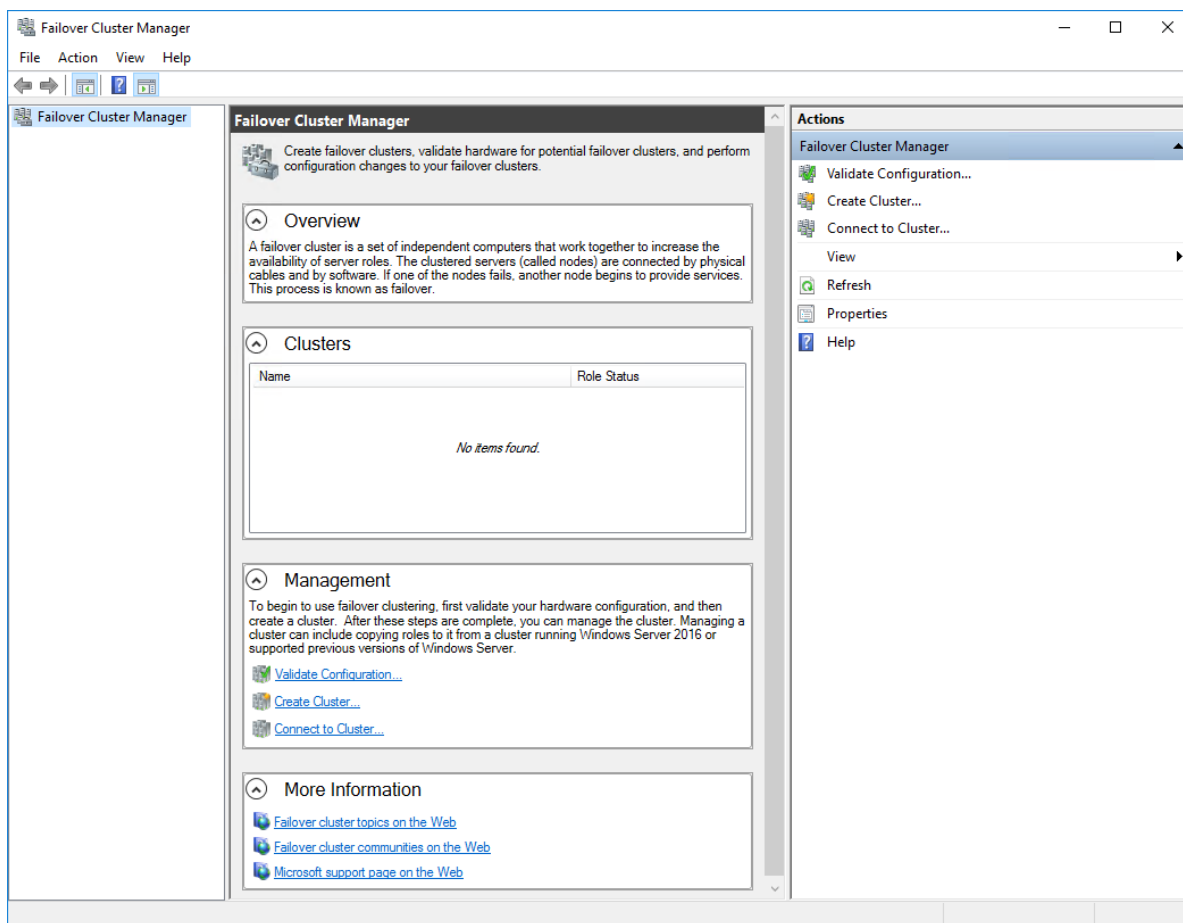
<https://docs.microsoft.com/en-us/windows-server/remote/remote-server-administration-tools>

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

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

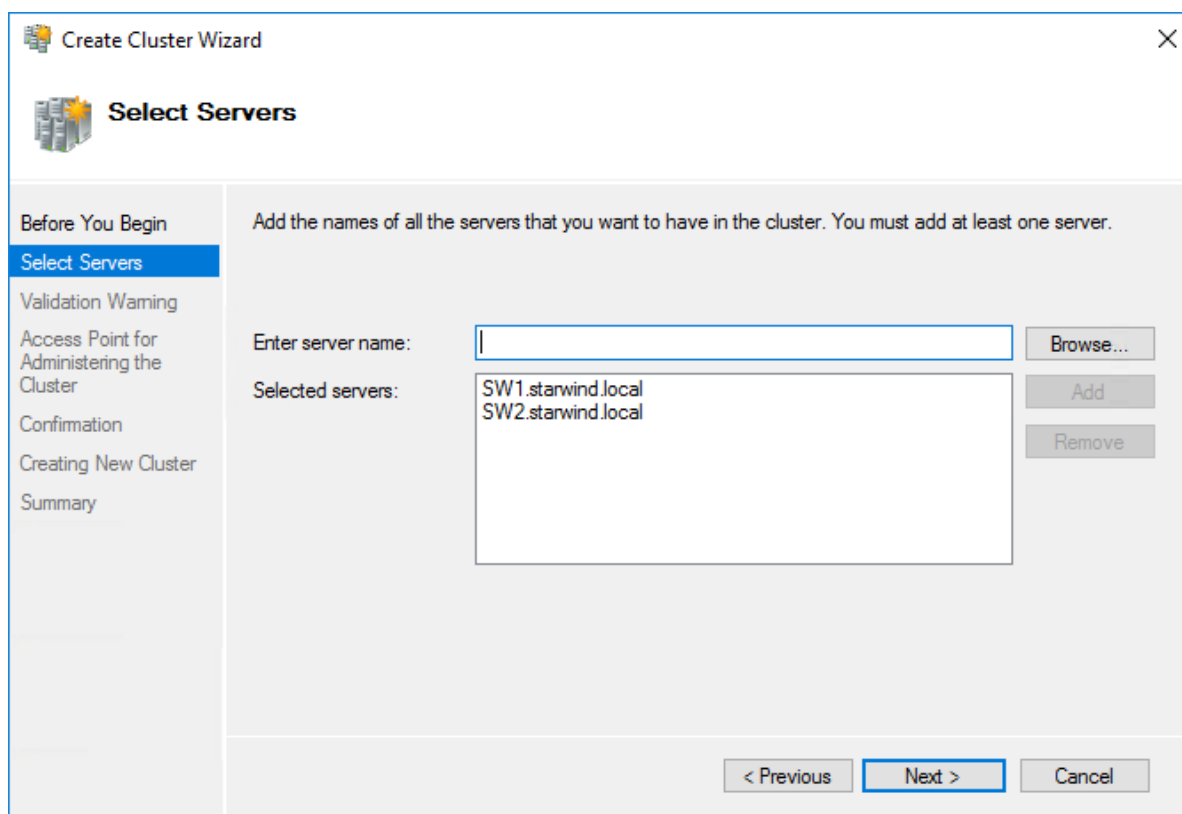


2. Click the Create Cluster link in the Actions section of Failover Cluster Manager.

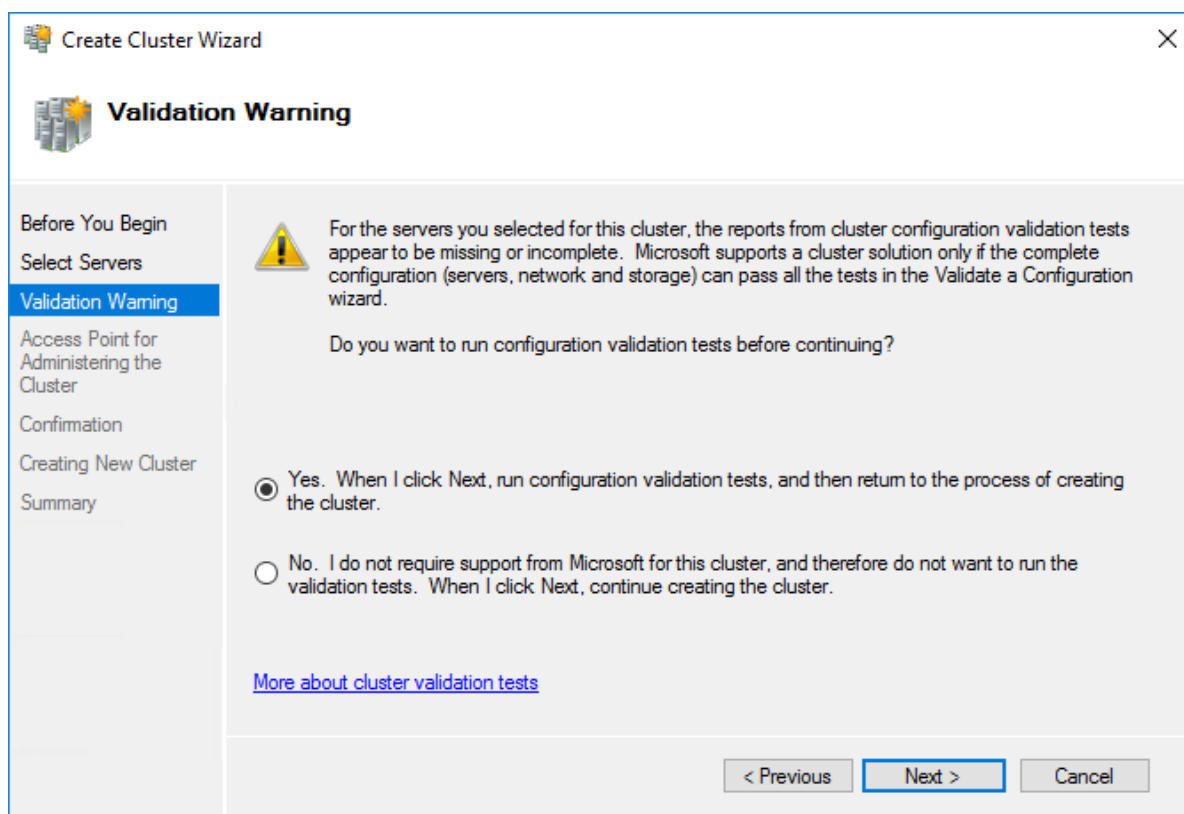


3. Specify the servers to be added to the cluster. Click Next to continue.



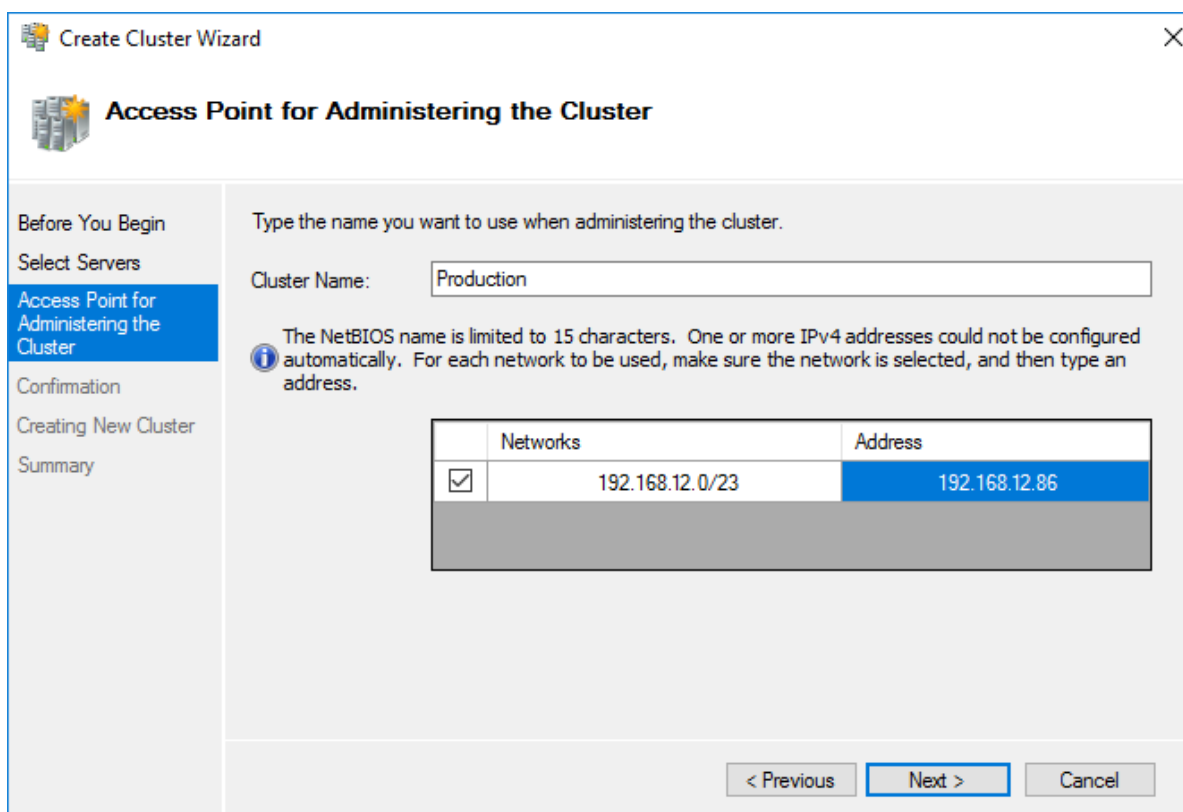


4. Validate the configuration by running the cluster validation tests: select Yes... and click Next to continue.



5. Specify the cluster name.

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



**Create Cluster Wizard**

**Access Point for Administering the Cluster**

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

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

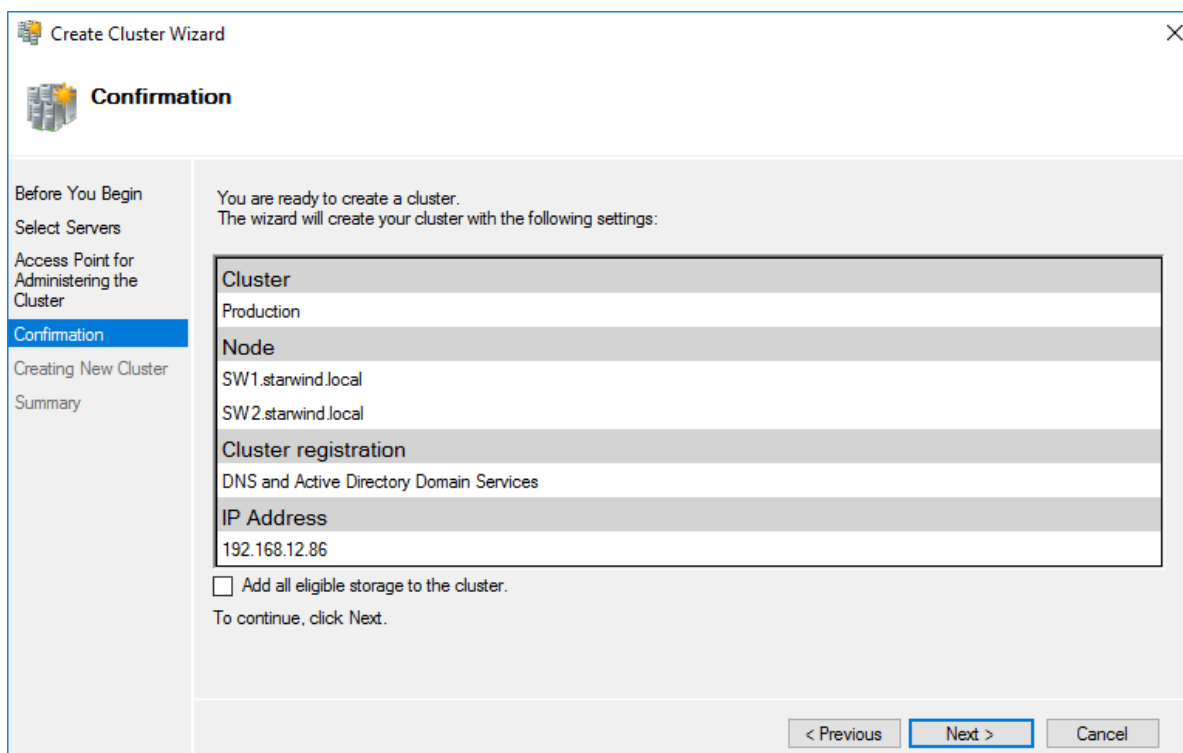
Cluster Name:

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

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

< Previous   **Next >**   Cancel

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



**Create Cluster Wizard**

**Confirmation**

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

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

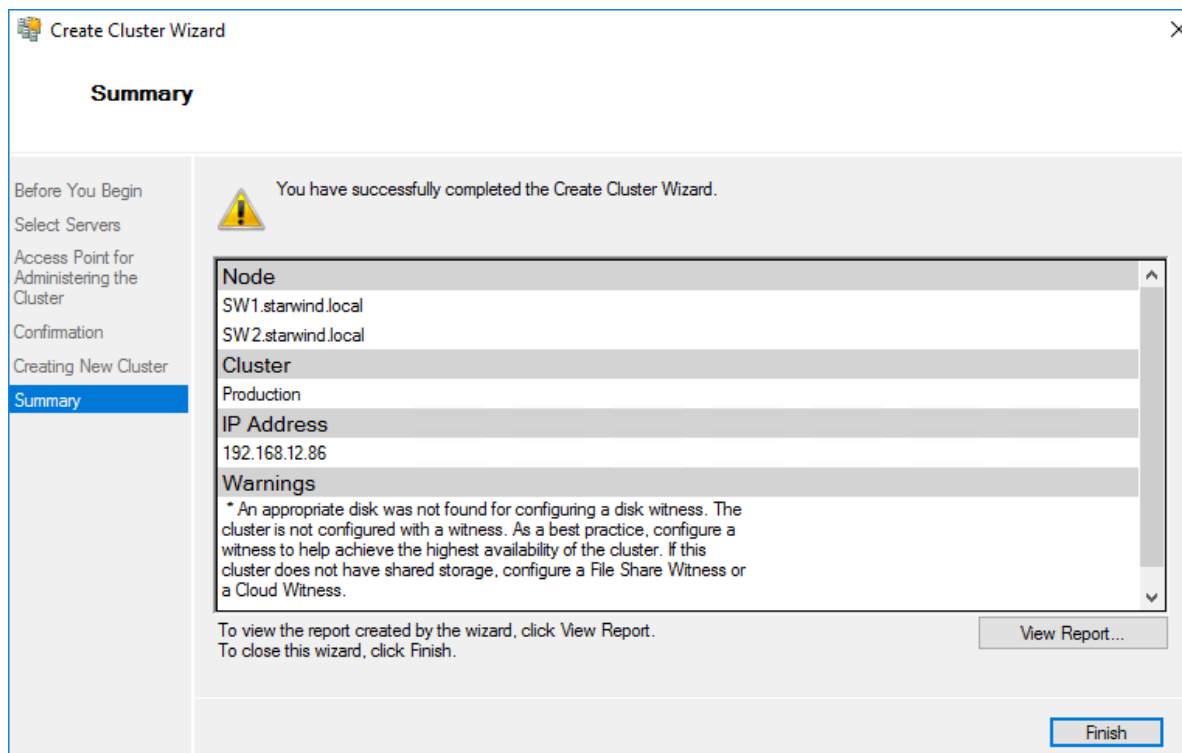
<b>Cluster</b>	Production
<b>Node</b>	SW1.starwind.local SW2.starwind.local
<b>Cluster registration</b>	DNS and Active Directory Domain Services
<b>IP Address</b>	192.168.12.86

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

< Previous   **Next >**   Cancel

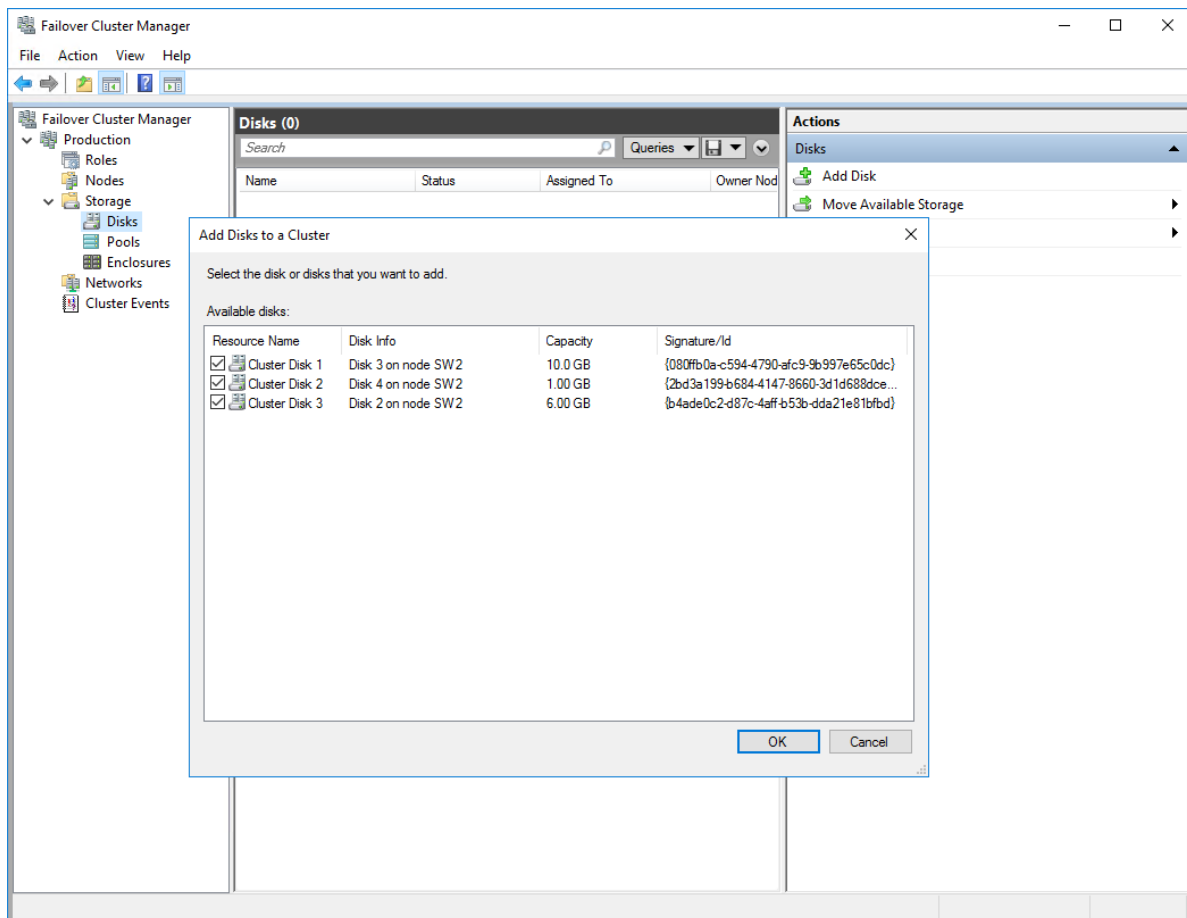
NOTE: If checkbox Add all eligible storage to the cluster is selected, the wizard will add all disks to the cluster automatically. The device with the smallest storage volume will be assigned as a Witness. It is recommended to uncheck this option before clicking Next and add cluster disks and the Witness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

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

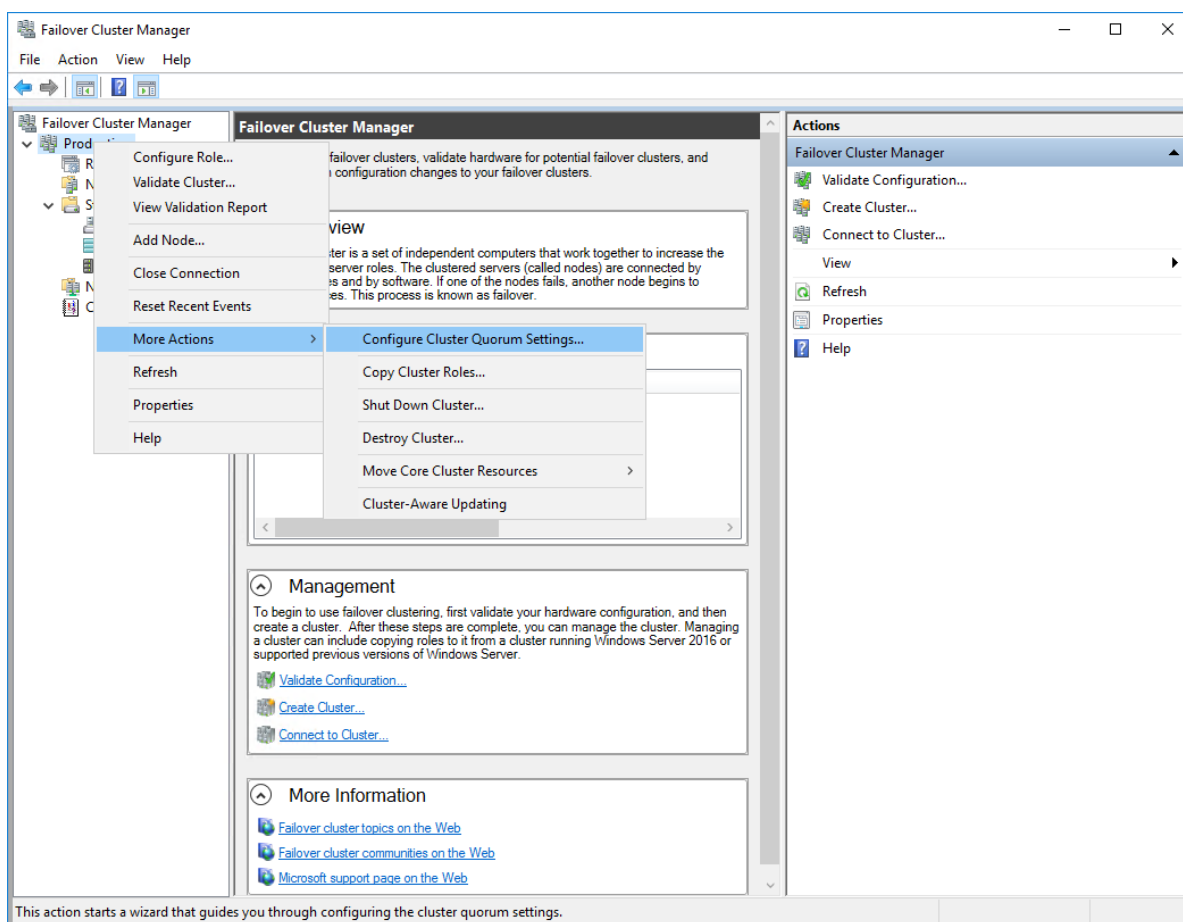


## Adding Storage to the Cluster

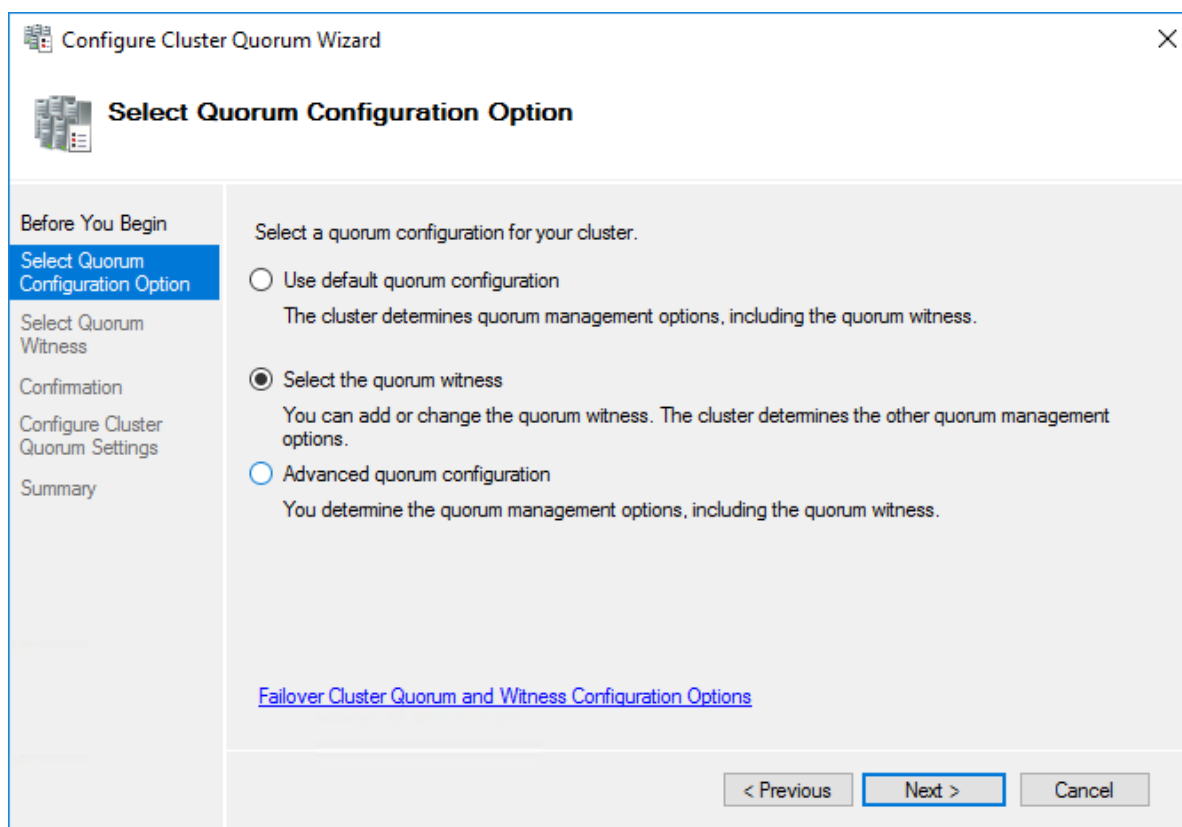
1. In Failover Cluster Manager, navigate to Cluster -> Storage -> Disks. Click Add Disk in the Actions panel, choose StarWind disks from the list and confirm the selection.



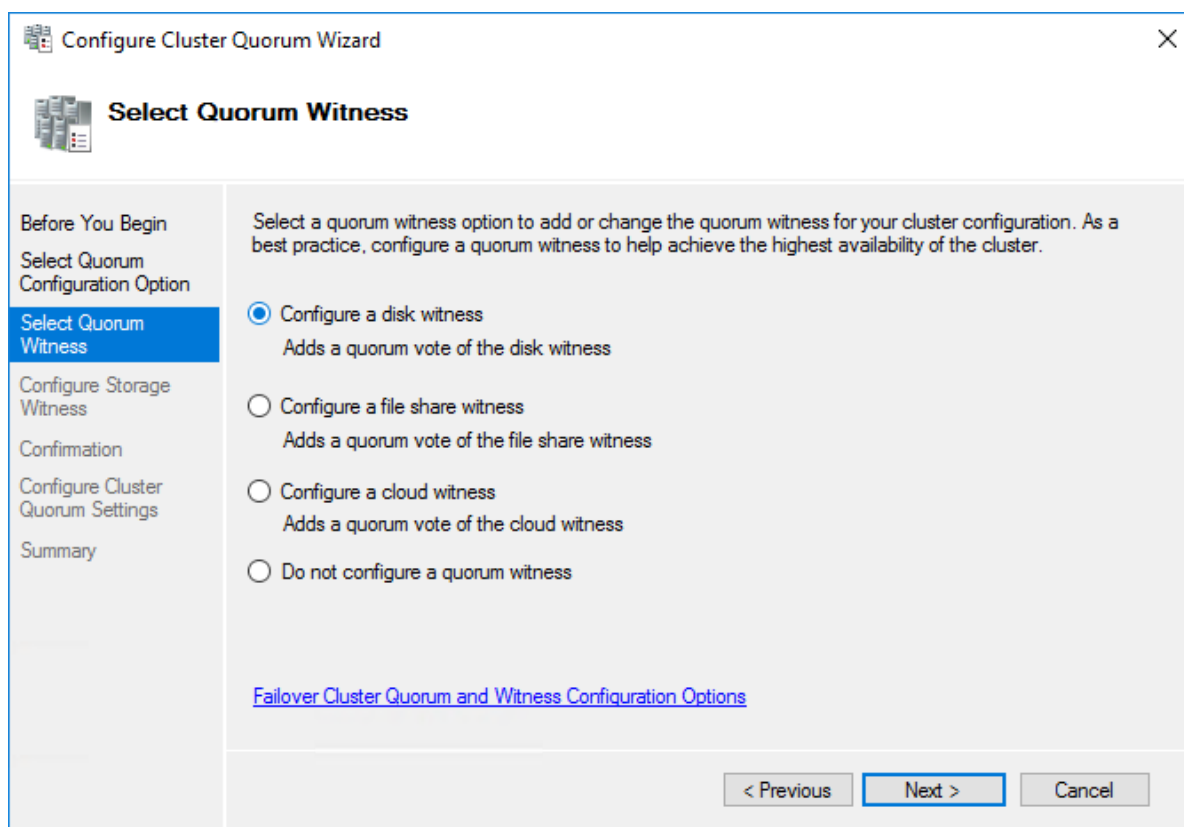
2. To configure the cluster witness disk, right-click on Cluster and proceed to More Actions -> Configure Cluster Quorum Settings.



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

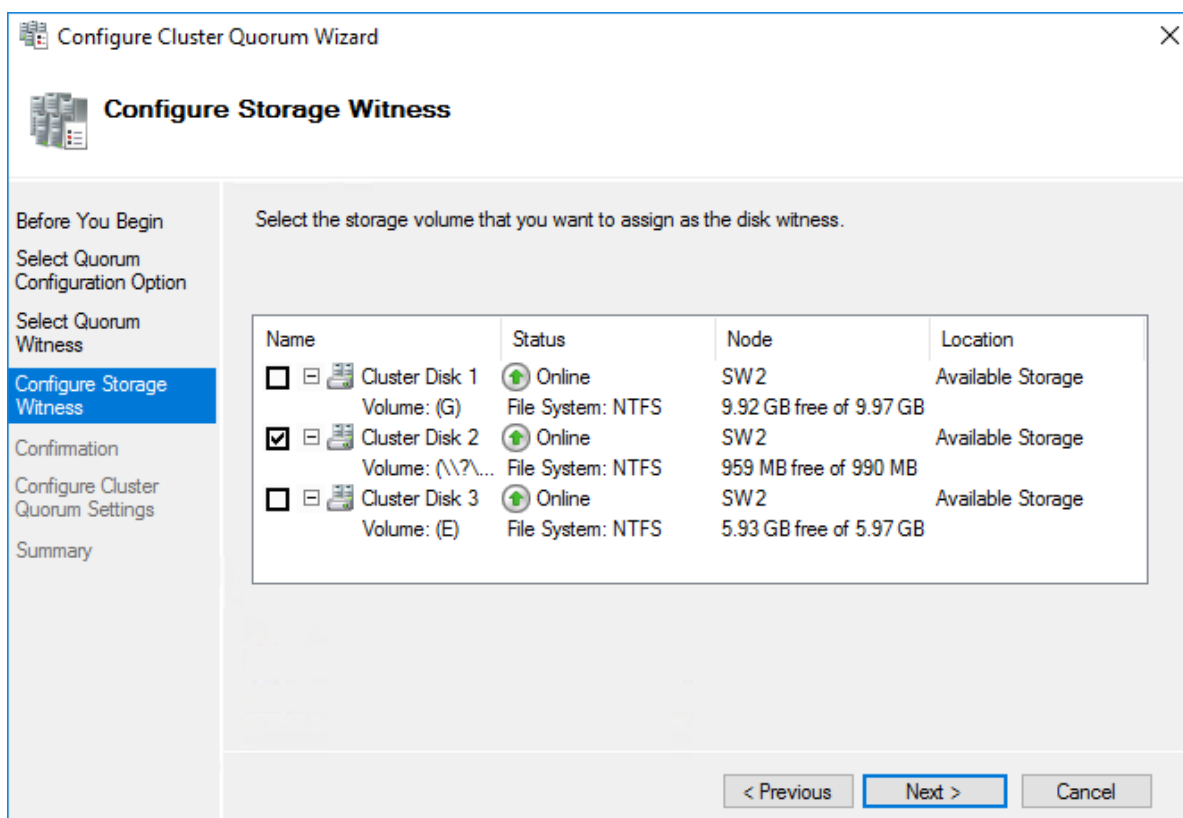


4. Select Configure a disk witness. Click Next.

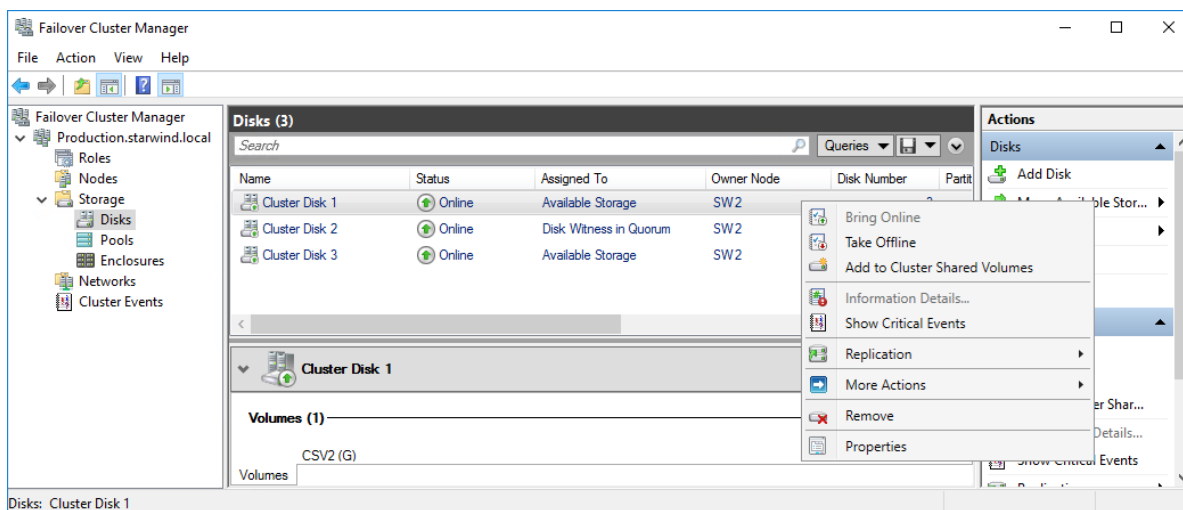


5. Select the Witness disk to be assigned as the cluster witness disk. Click Next and press Finish to complete the operation.

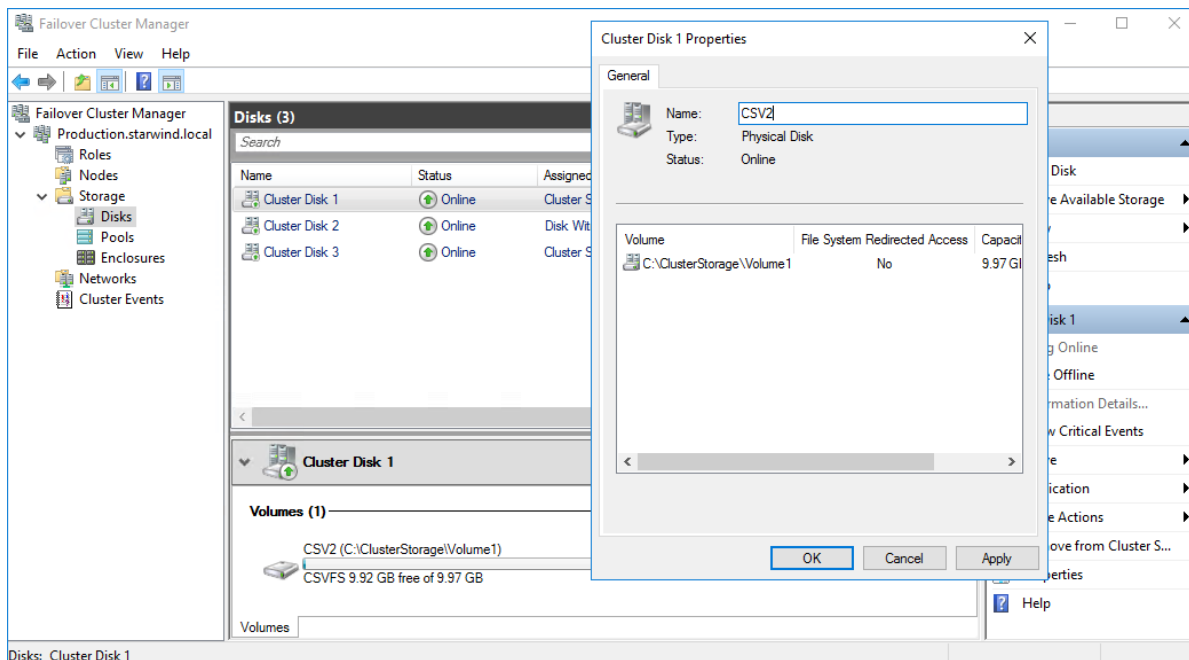




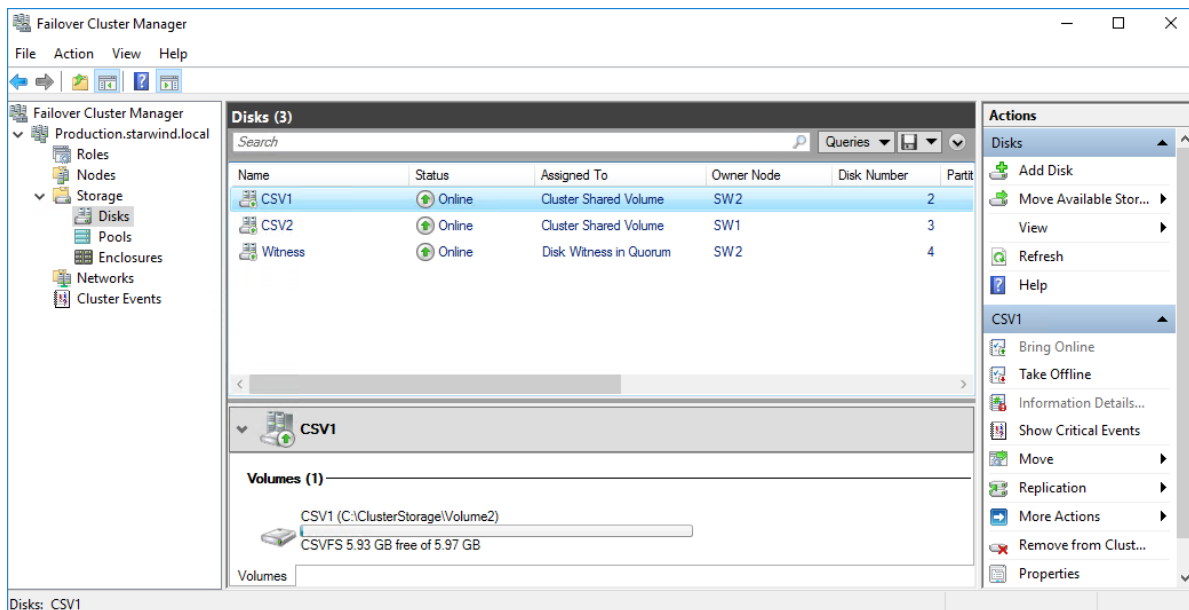
6. In Failover Cluster Manager, Right-click the disk and select Add to Cluster Shared Volumes.



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



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

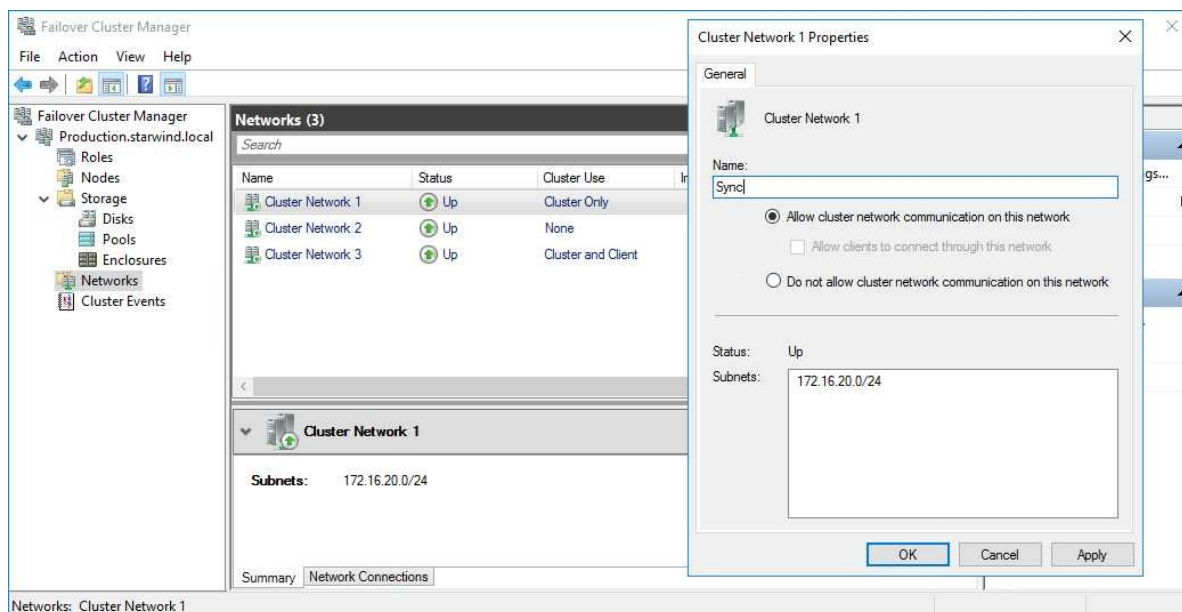


## Configuring Cluster Network Preferences

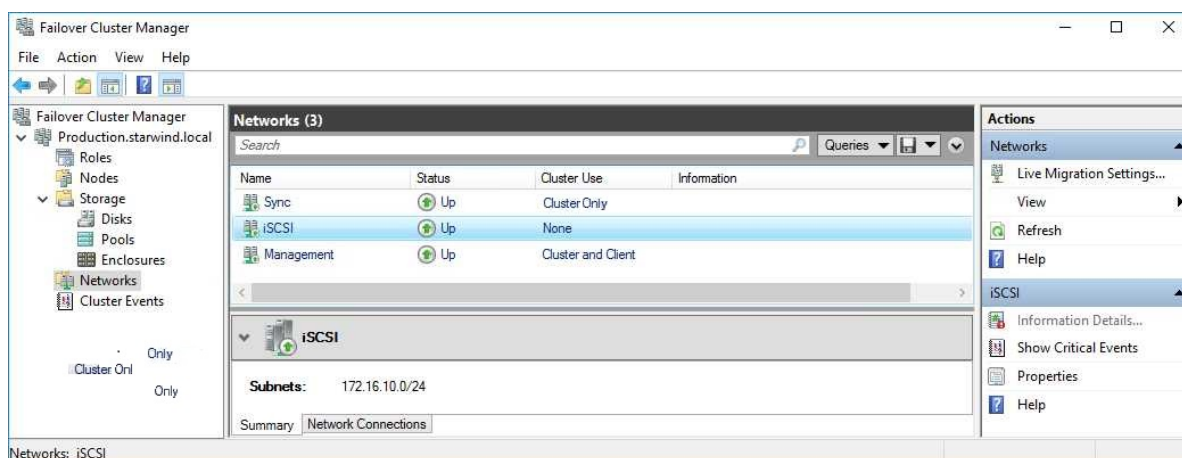
1. In the Networks section of the Failover Cluster Manager, right-click on the network from the list. Set its new name if required to identify the network by its subnet. Apply the change and press OK.

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

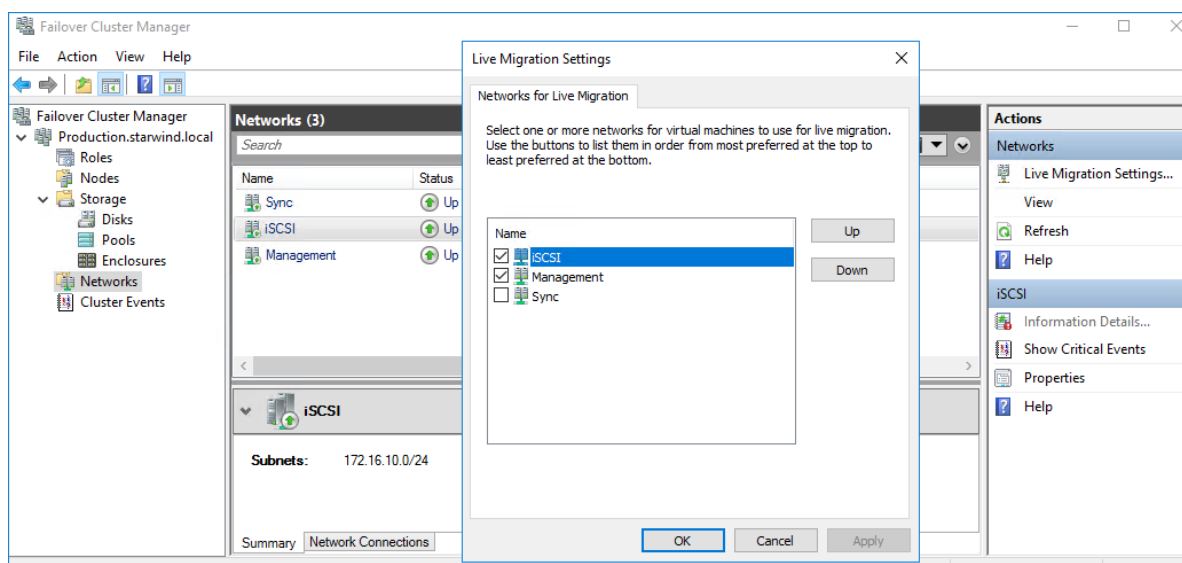
<https://docs.microsoft.com/en-us/windows-server/failover-clustering/smb-multichannel>



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



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



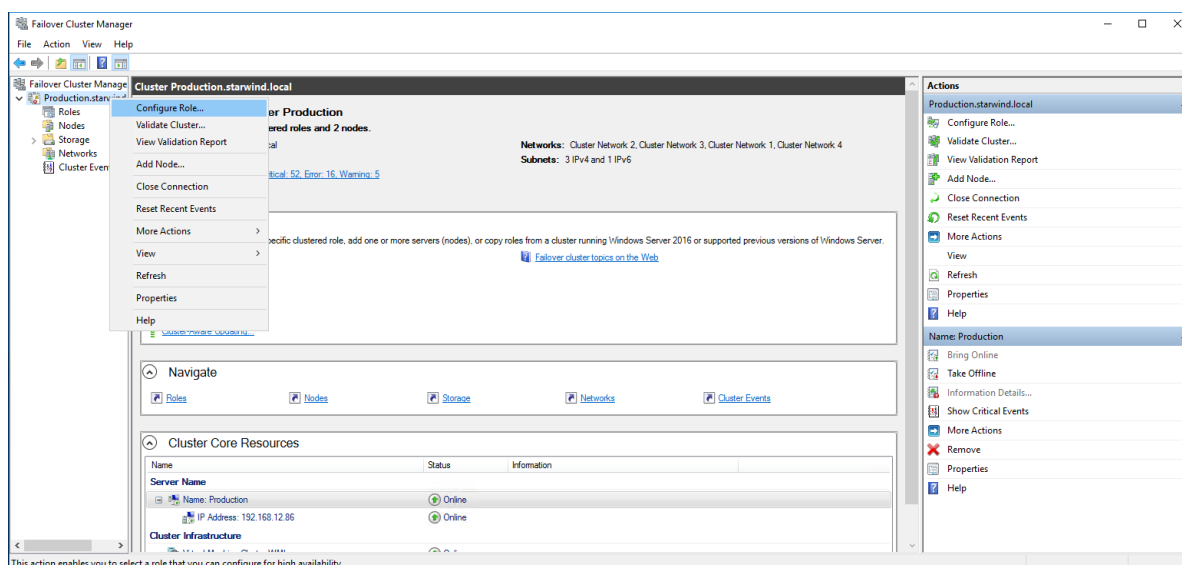
The cluster configuration is completed and it is ready for virtual machines deployment. Select Roles and in the Action tab, click Virtual Machines -> New Virtual Machine. Complete the wizard.

## Configuring File Shares

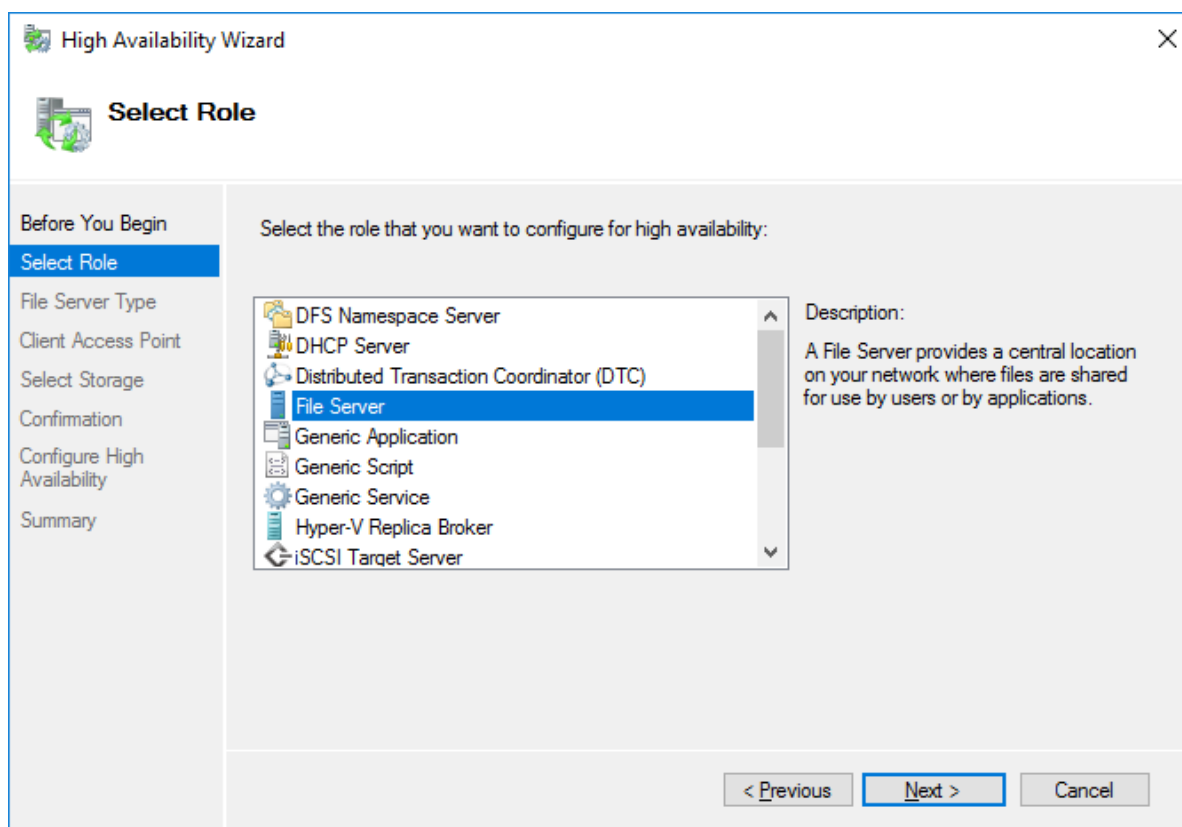
Please follow the steps below if file shares should be configured on cluster nodes.

## Configuring The Scale-Out File Server Role

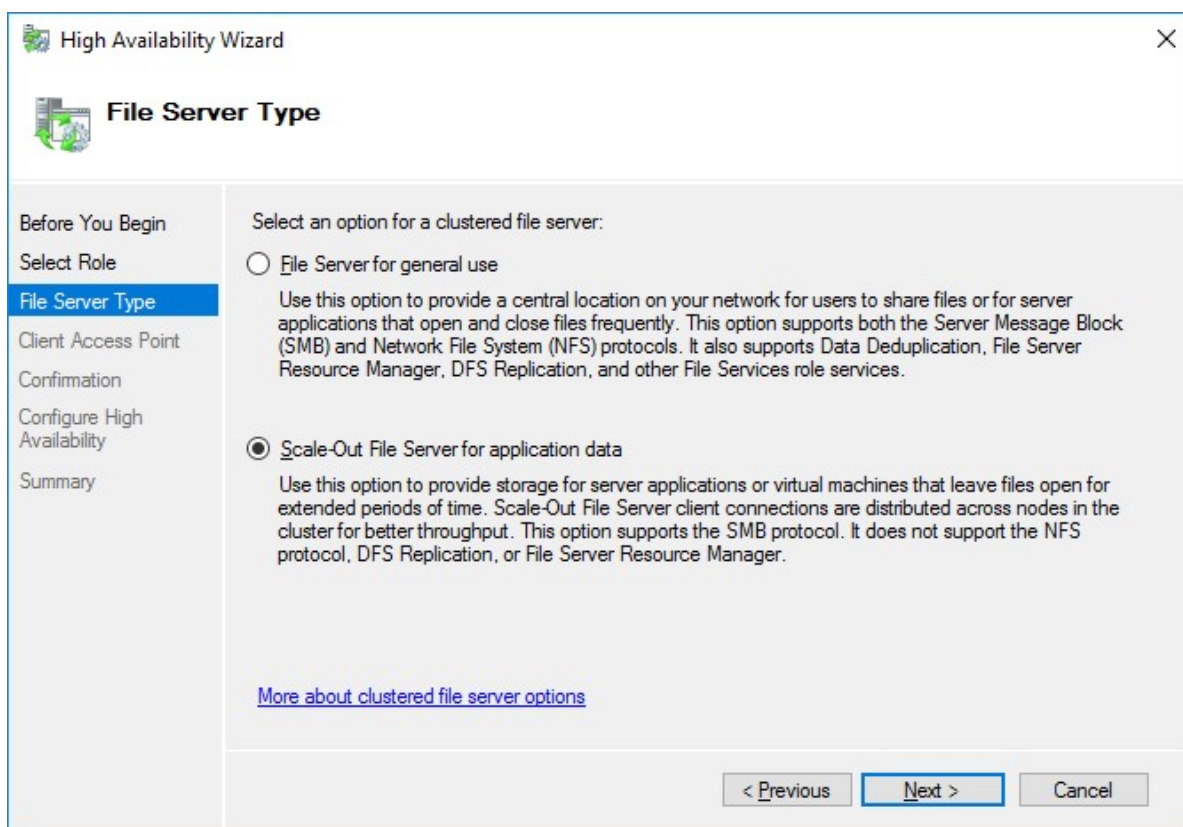
1. To configure the Scale-Out File Server Role, open Failover Cluster Manager.
2. Right-click the cluster name, then click Configure Role and click Next to continue.



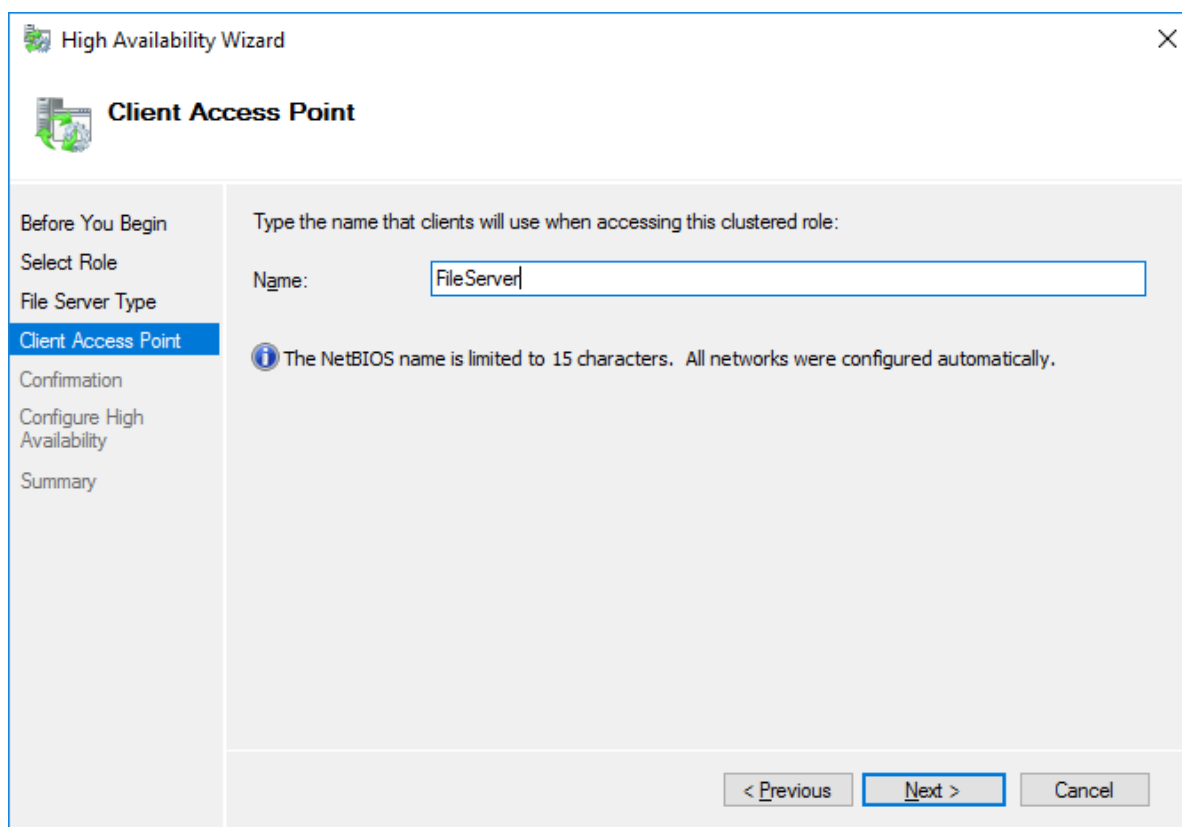
3. Select the File Server item from the list in High Availability Wizard and click Next to continue.



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



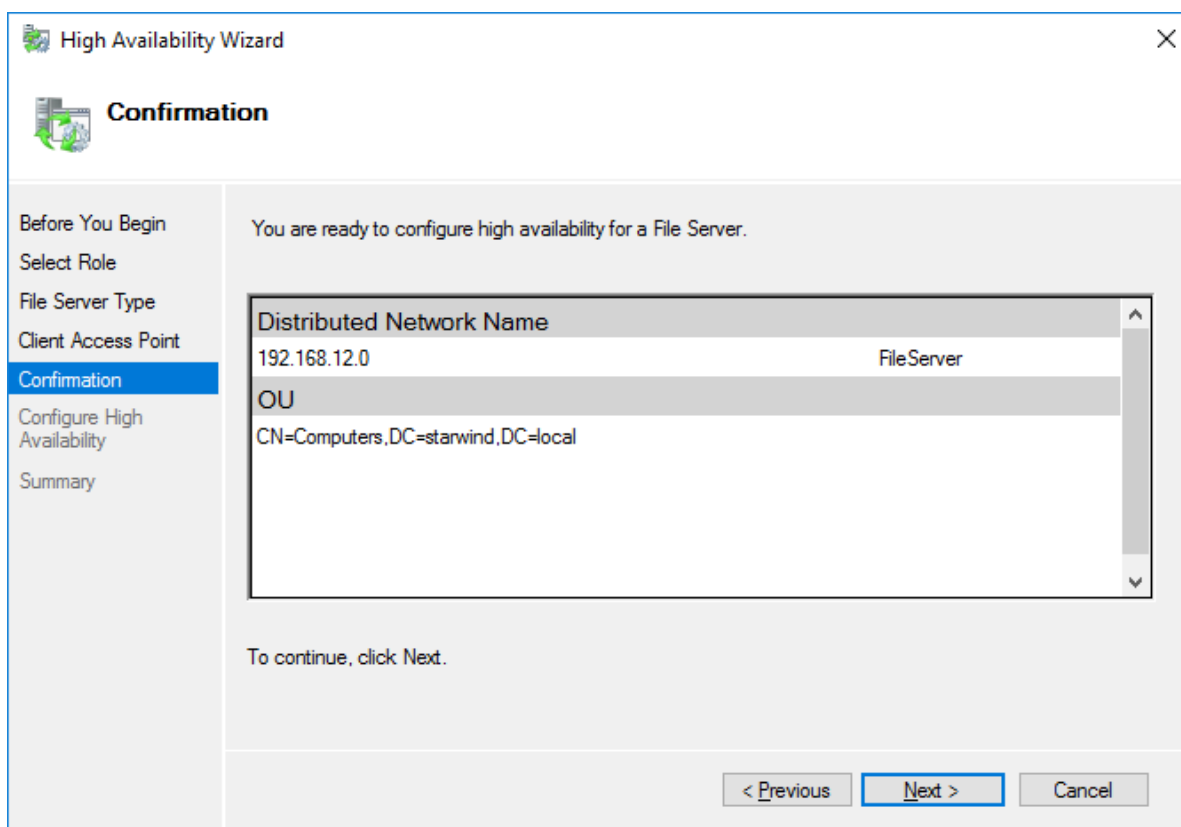
5. On the Client Access Point page, in the Name text field, type the NetBIOS name that will be used to access a Scale-Out File Server.



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

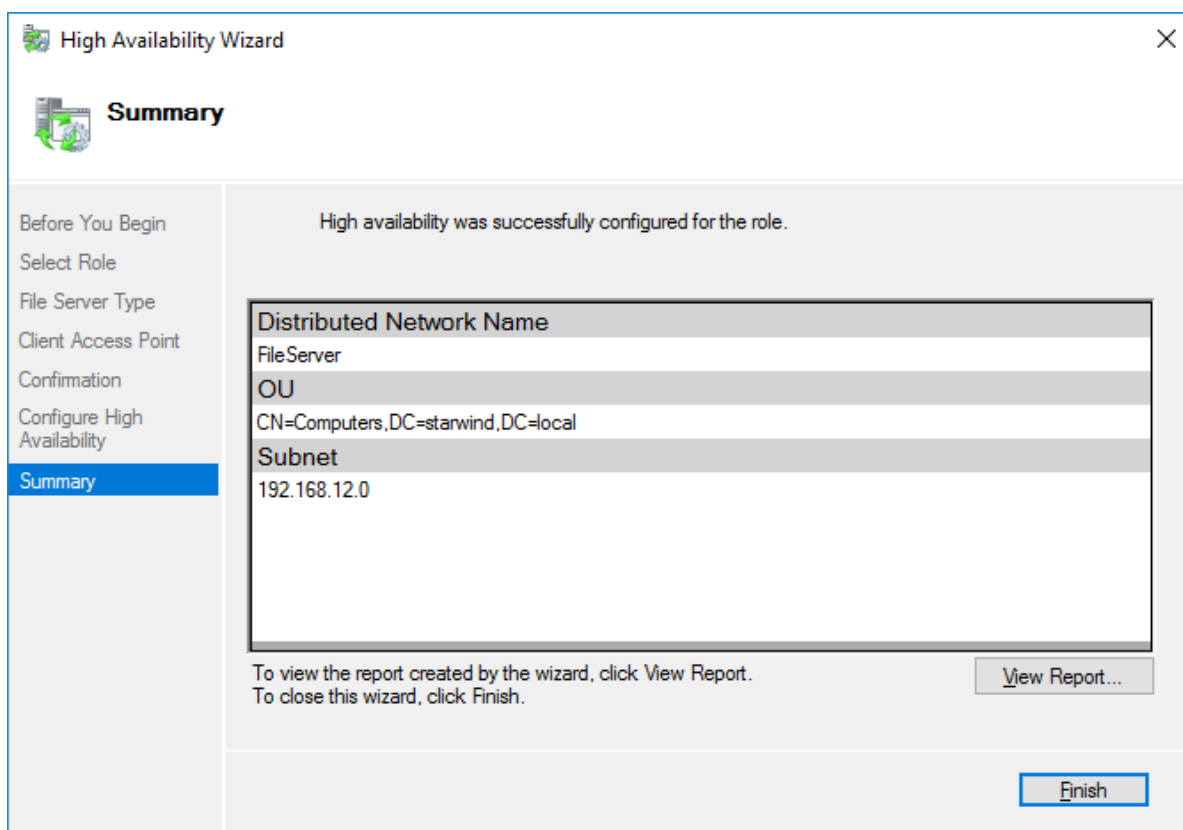
Click Next to continue.

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

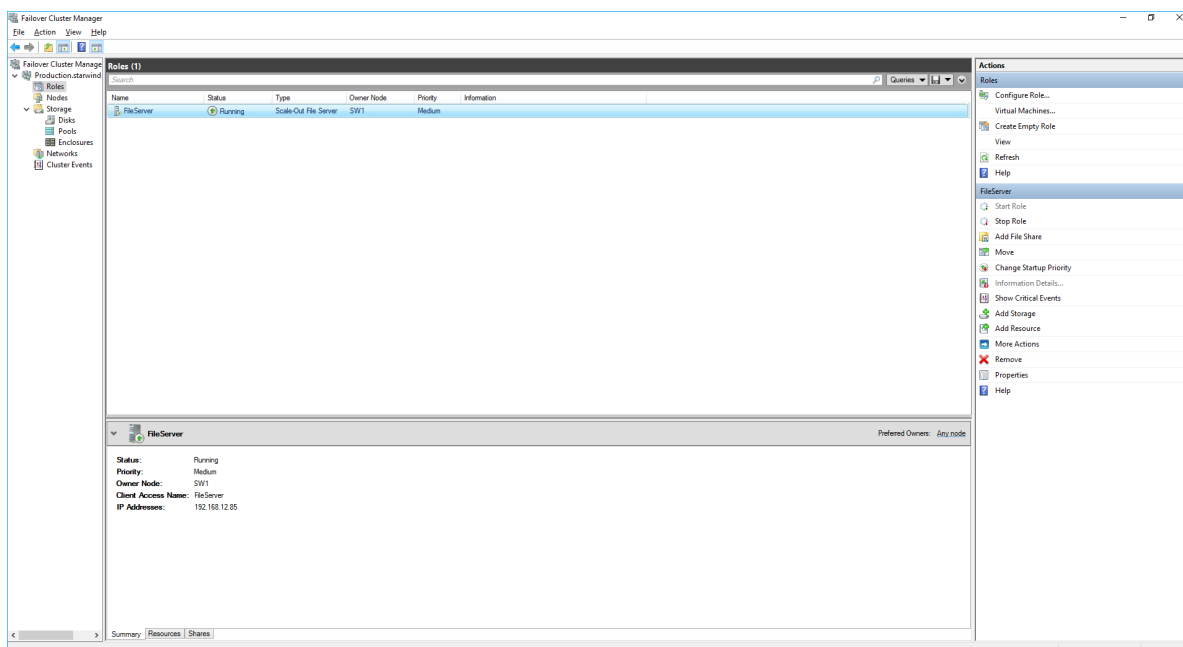


7. Once the installation is finished successfully, the Wizard should now look like the screenshot below.  
Click Finish to close the Wizard.

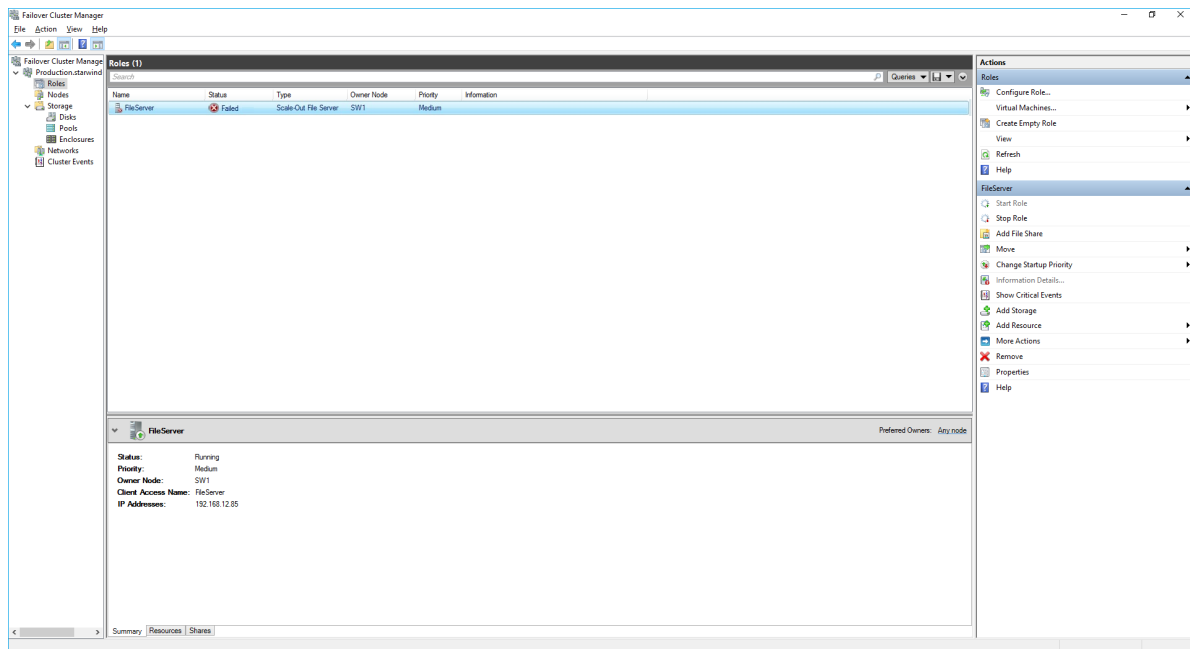




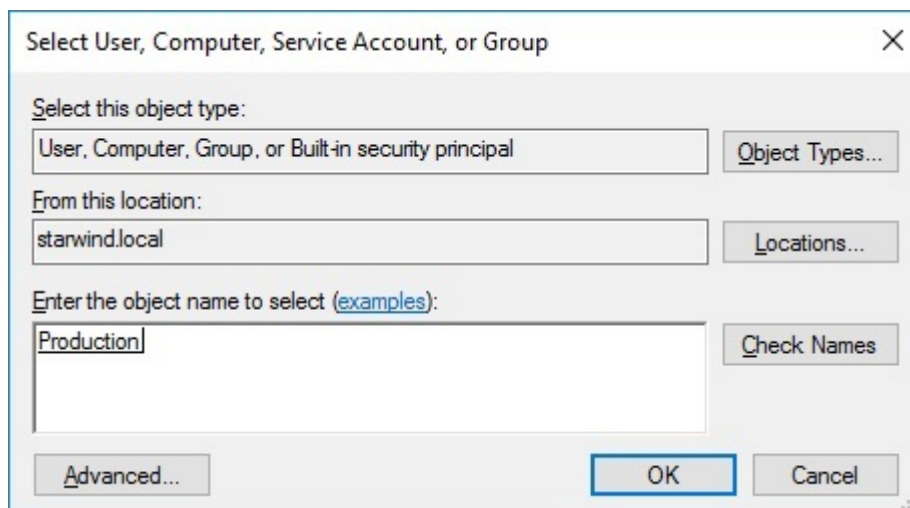
8. The newly created role should now look like the screenshot below.



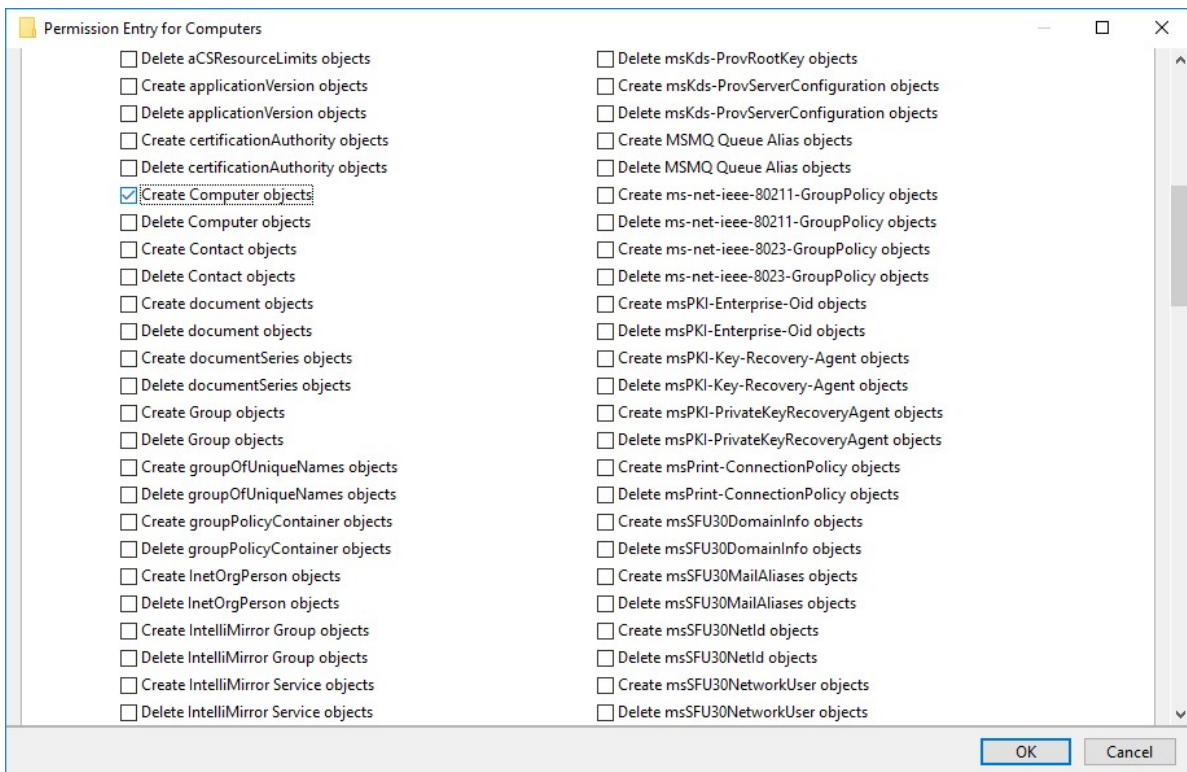
NOTE: If the role status is Failed and it is unable to Start, please, follow the next steps:



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



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

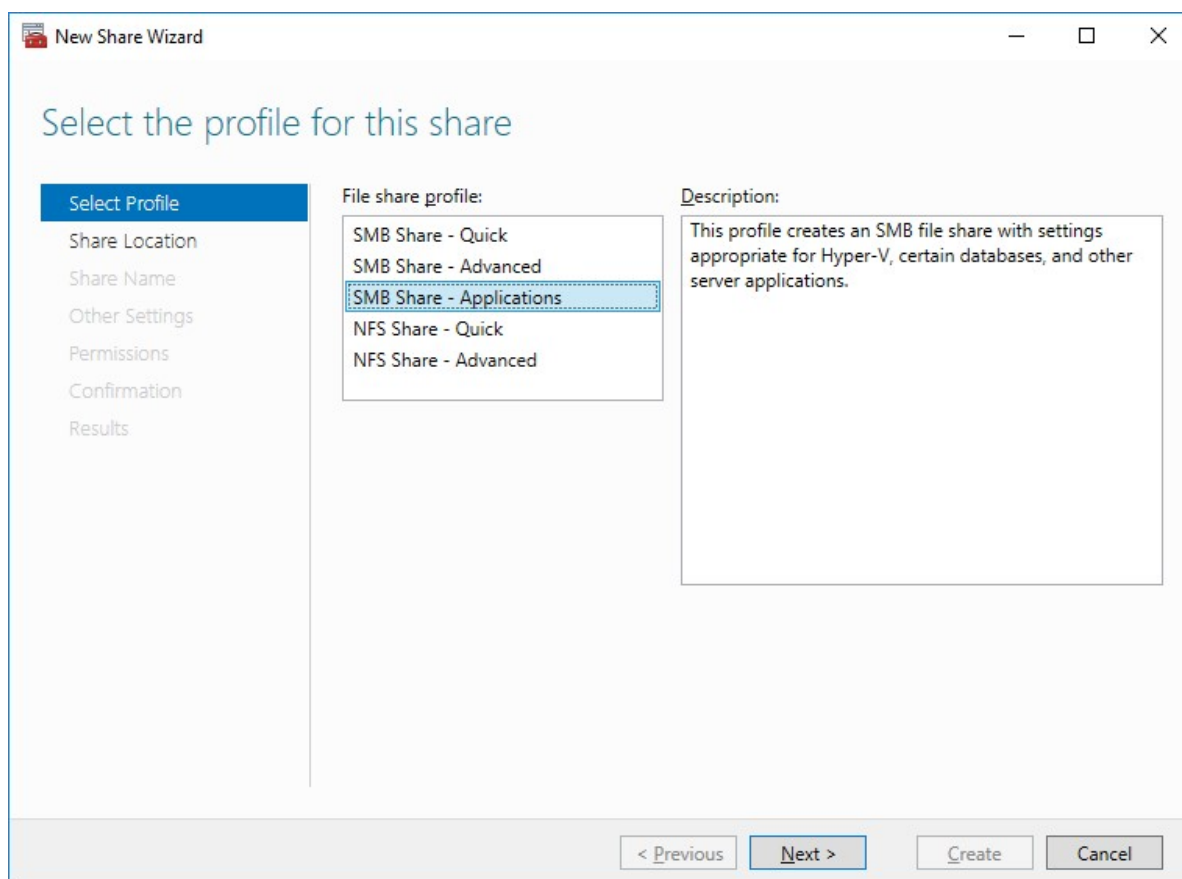


- click OK on all opened windows to confirm the changes
- open Failover Cluster Manager, right-click SOFS role and click Start Role

## Configuring File Share

### To Add File Share:

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



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

**New Share Wizard**

Select the server and path for this share

**Select Profile**

- Share Location
- Share Name
- Other Settings
- Permissions
- Confirmation
- Results

**Server:**

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

**Share location:**

☒ Select by volume:

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

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

☐ Type a custom path:

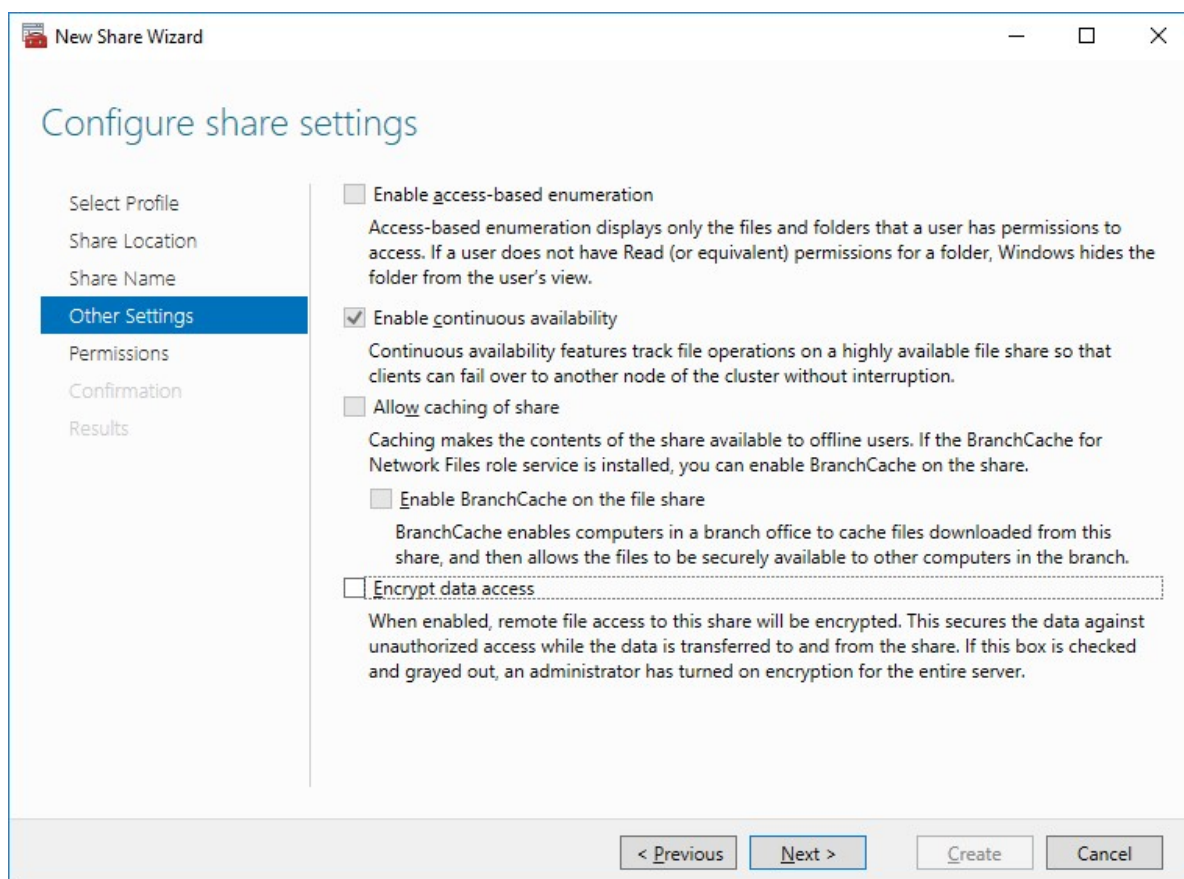
6. Type in the file share name and click Next.

The screenshot shows the 'New Share Wizard' window with the 'Specify share name' step selected in the left sidebar. The main area contains the following fields and options:

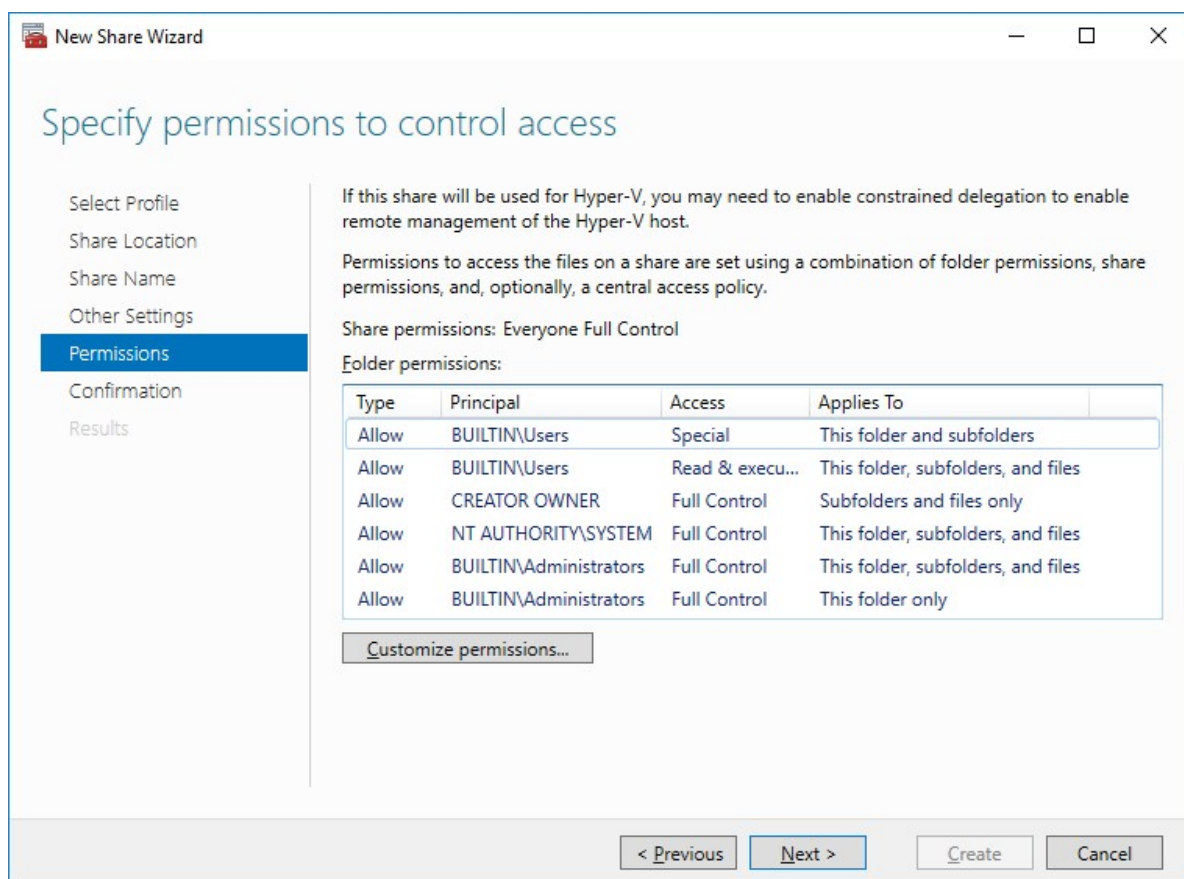
- Share name:** A text box containing the word 'Share'.
- Share description:** An empty text box.
- Local path to share:** A text box containing 'C:\ClusterStorage\Volume1\Shares\Share'. Below this field is a blue information icon and the text: 'If the folder does not exist, the folder is created.'
- Remote path to share:** A text box containing '\\FileServer\Share'.

At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Create', and 'Cancel'.

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



8. Specify the access permissions for the file share.

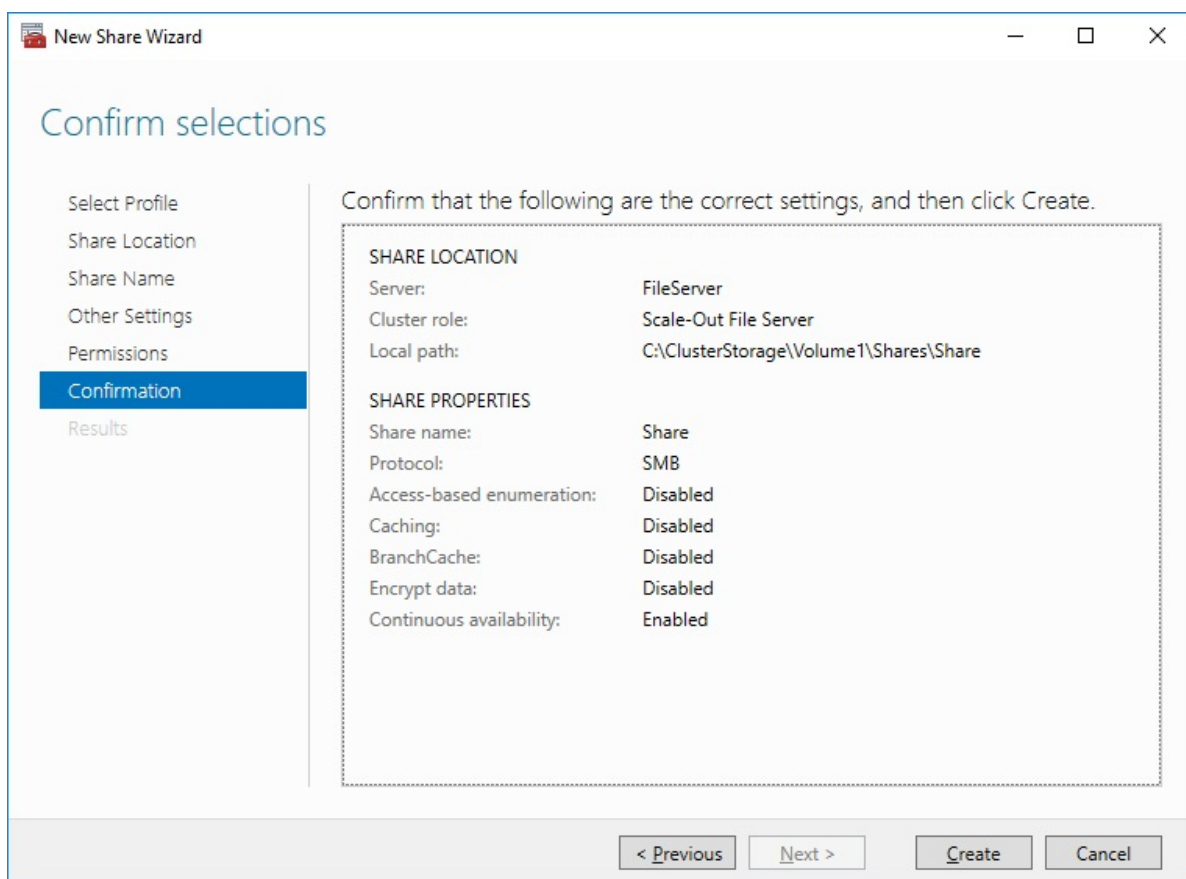


**NOTE:**

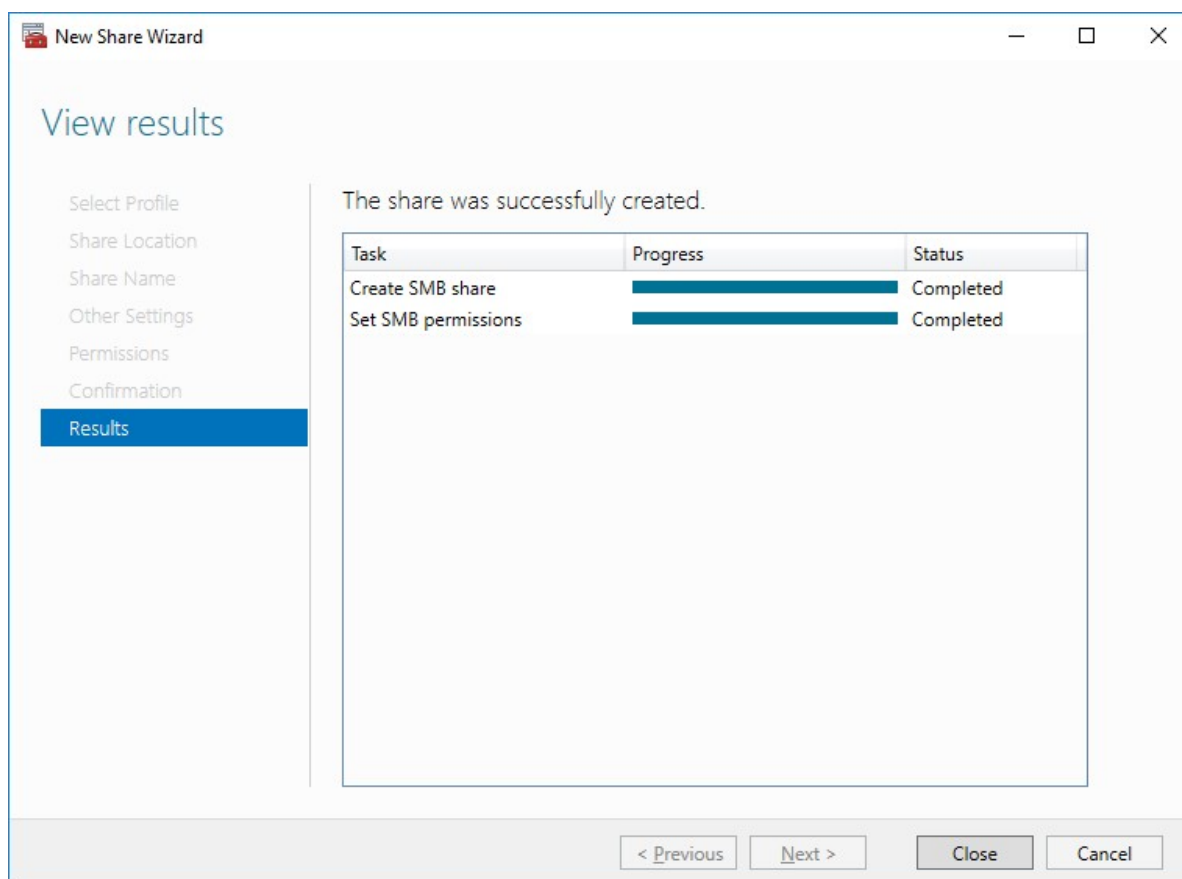
- for the Scale-Out File Server for Hyper-V, all Hyper-V computer accounts, the SYSTEM account, and all Hyper-V administrators must be provided with the full control on the share and file system
- for the Scale-Out File Server on Microsoft SQL Server, the SQL Server service account must be granted full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

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



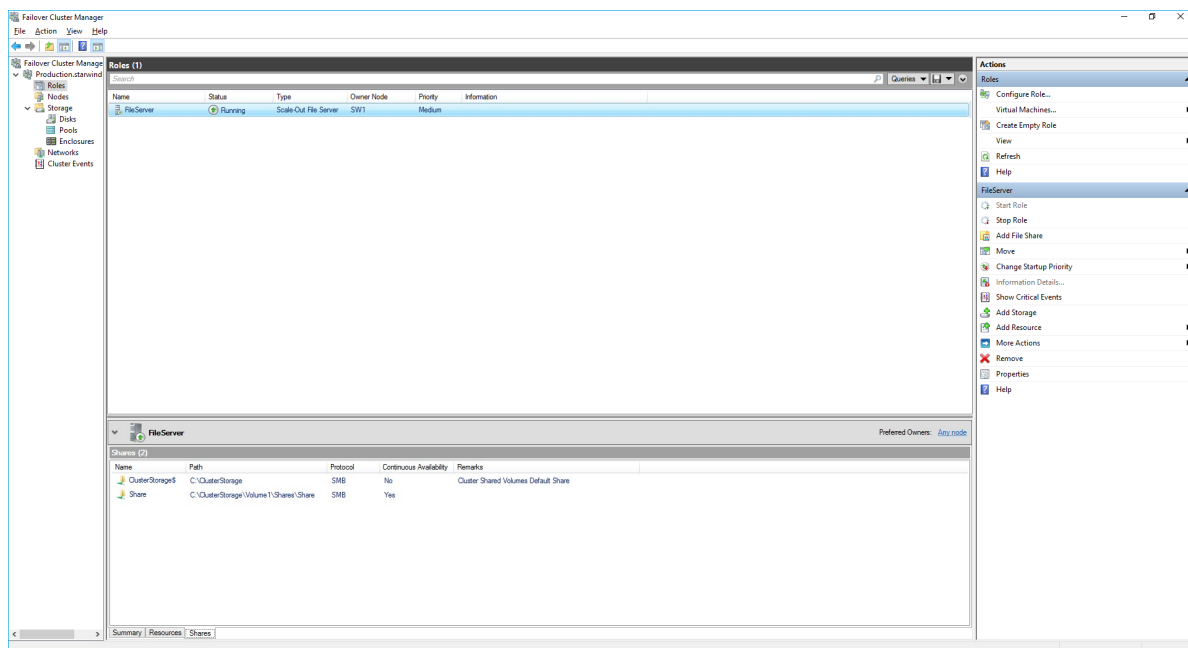


10. Check the summary and click Close to close the Wizard.



To Manage Created File Shares:

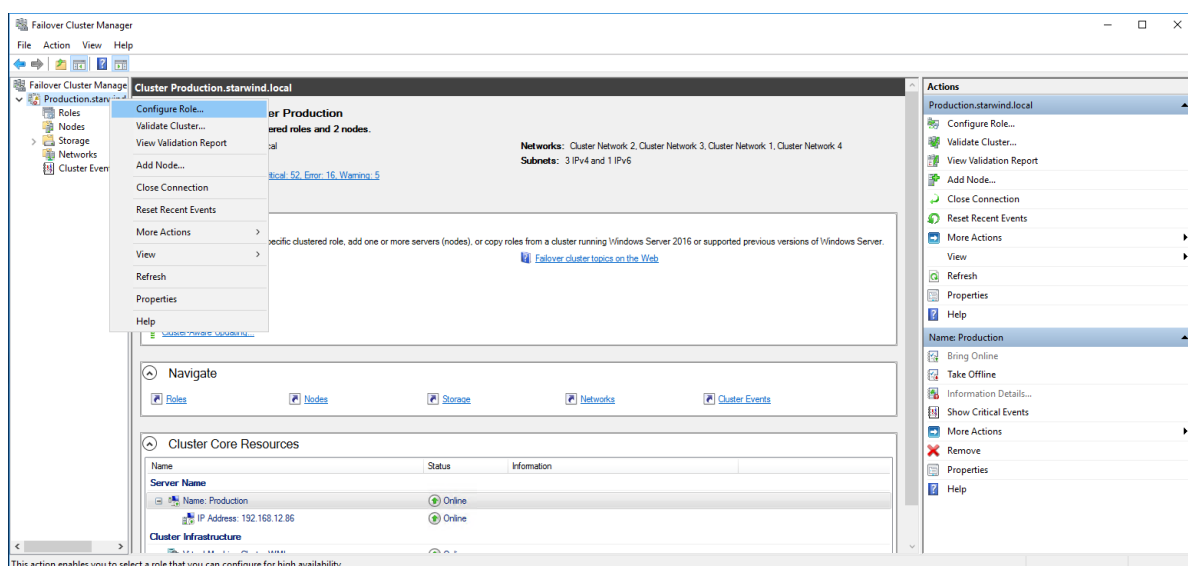
- open Failover Cluster Manager
- expand the cluster and click Roles
- choose the file share role, select the Shares tab, right-click the created file share, and select Properties:



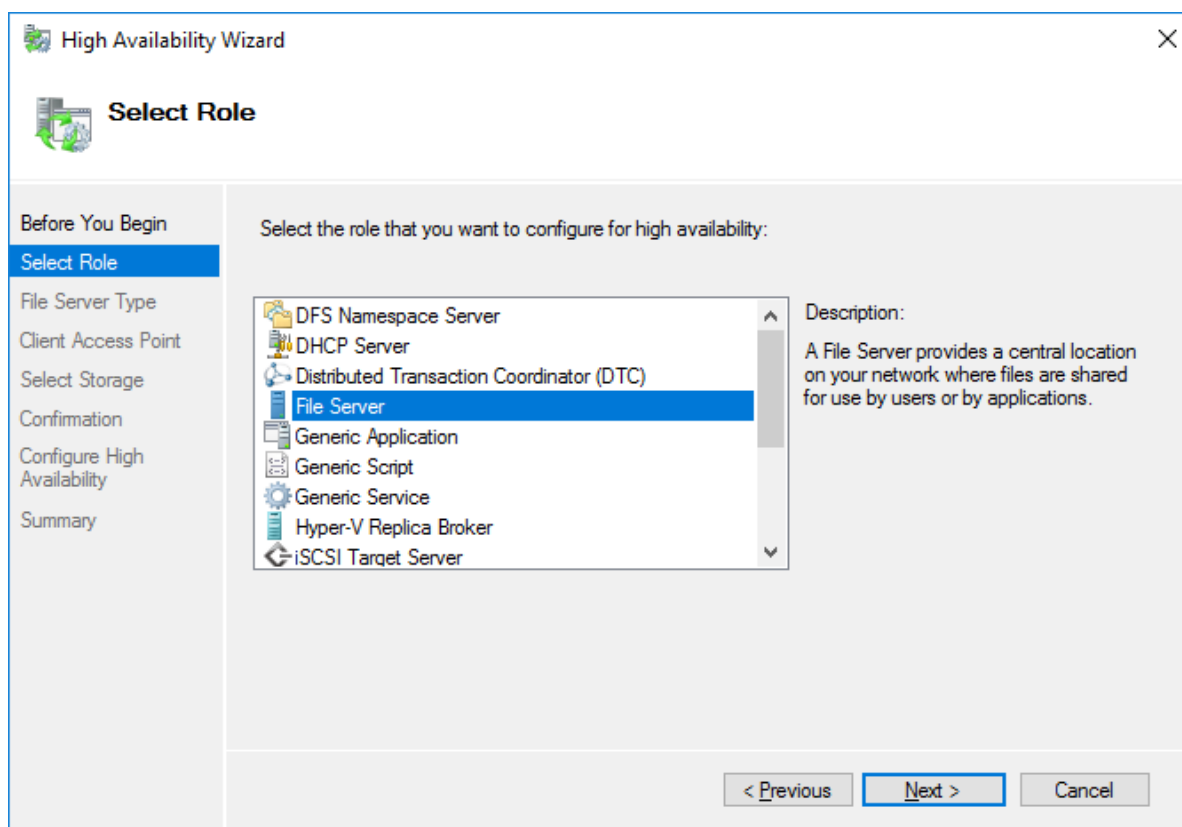
## Configuring The File Server For General Use Role

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

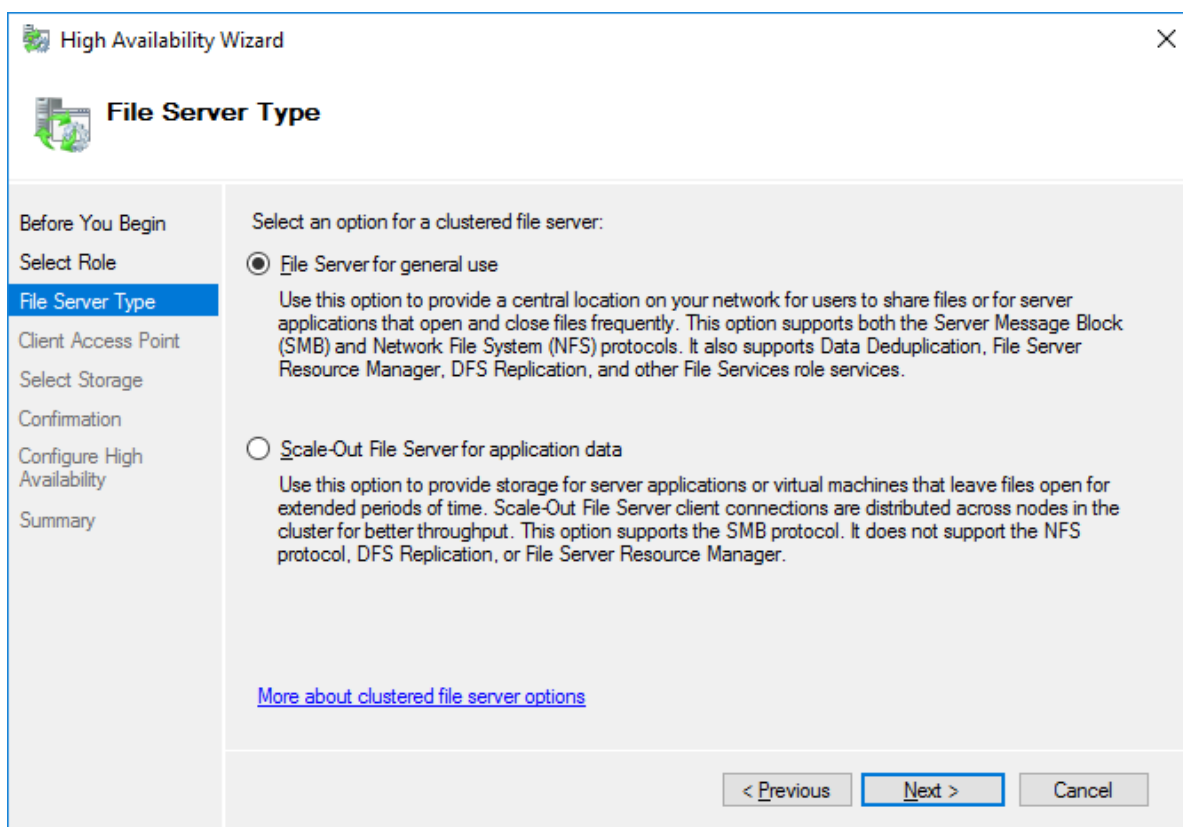
1. To configure the File Server for General Use role, open Failover Cluster Manager.
2. Right-click on the cluster name, then click Configure Role and click Next to continue.



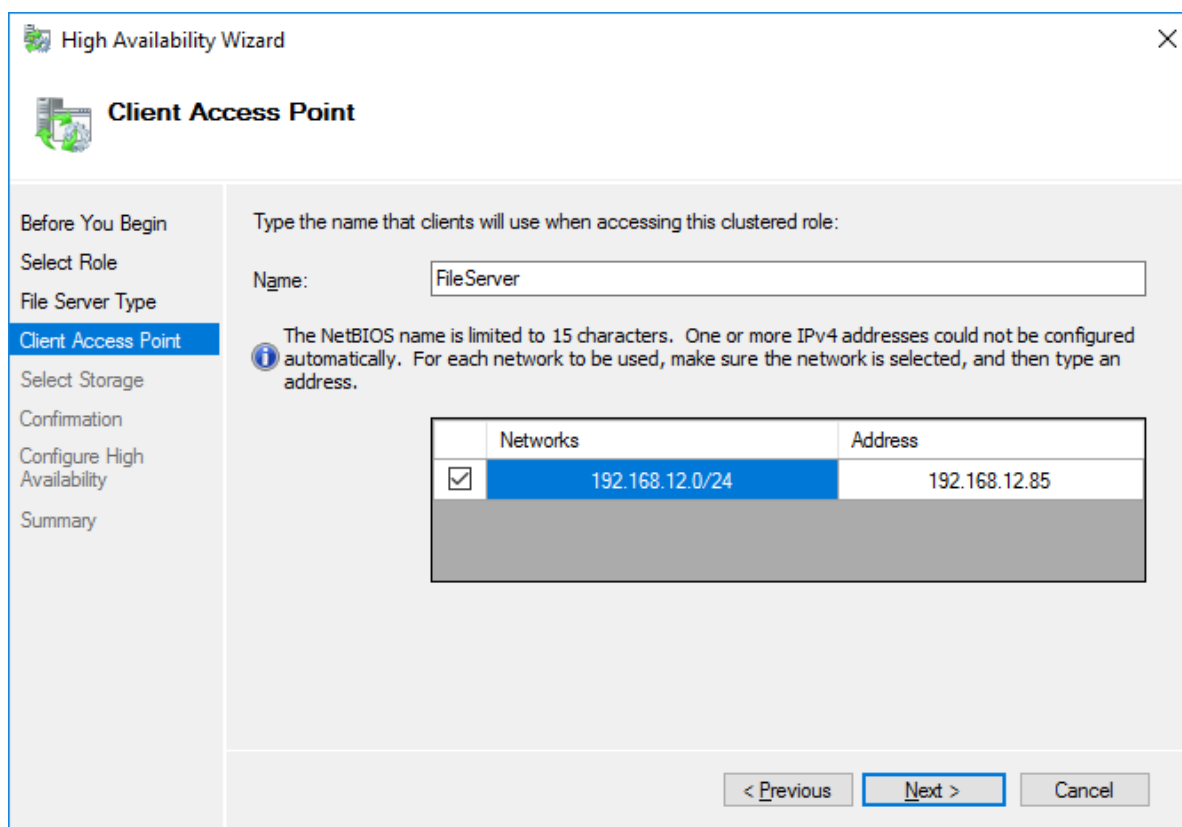
3. Select the File Server item from the list in High Availability Wizard and click Next to continue.



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



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



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

High Availability Wizard

**Client Access Point**

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

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

Name:

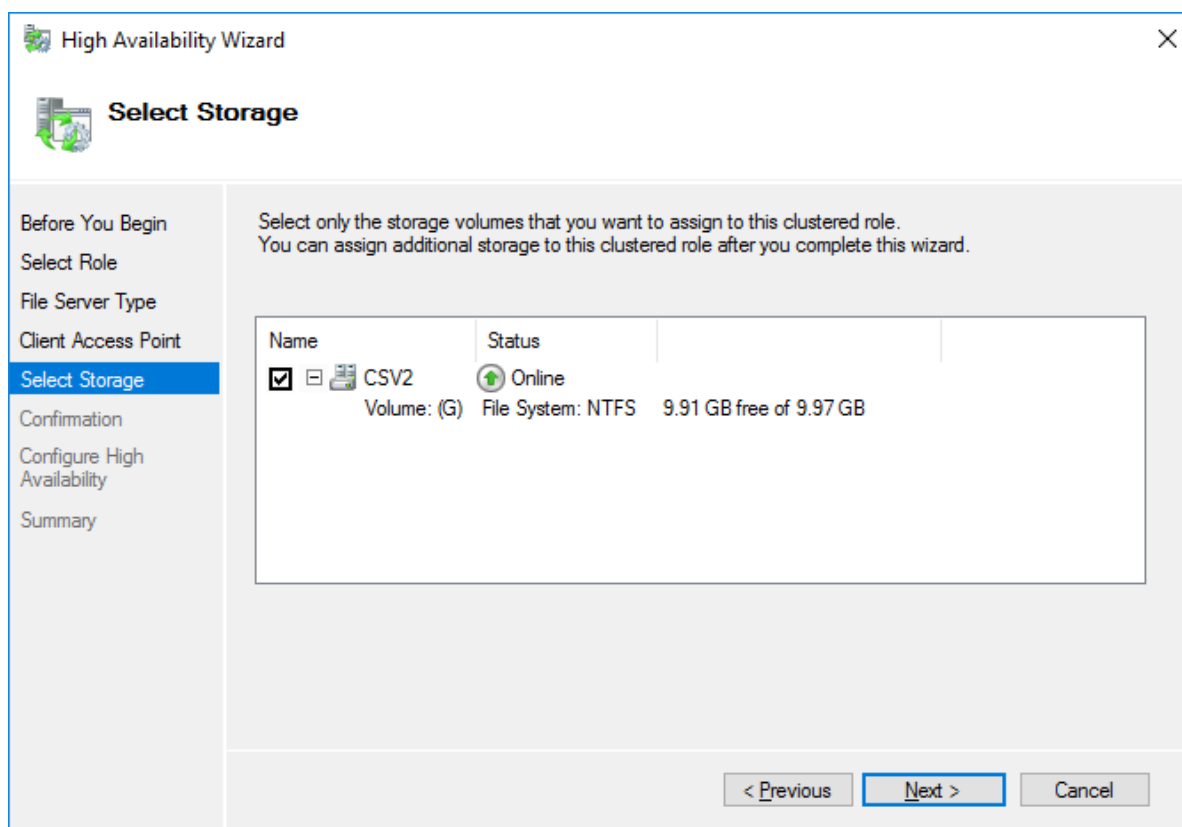
*i* The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

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

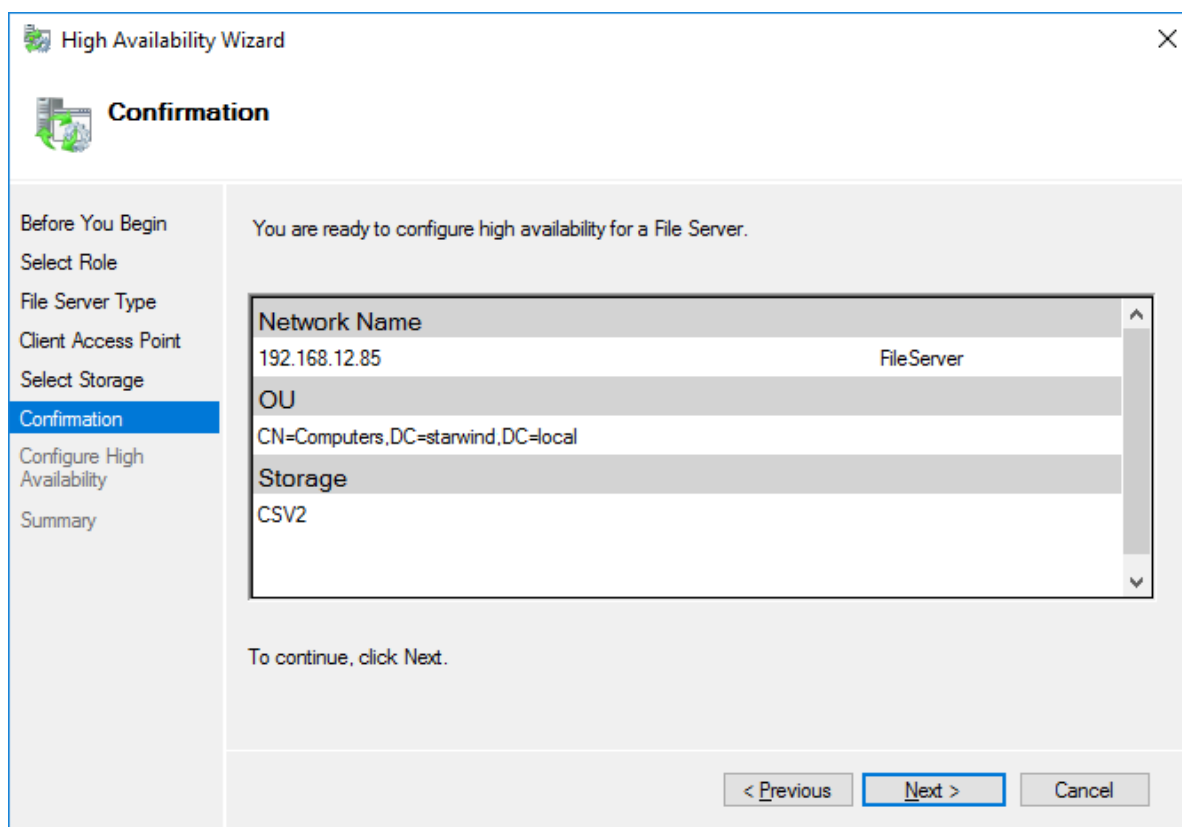
< Previous   **Next >**   Cancel

Click Next to continue.

6. Select the Cluster disk and click Next.



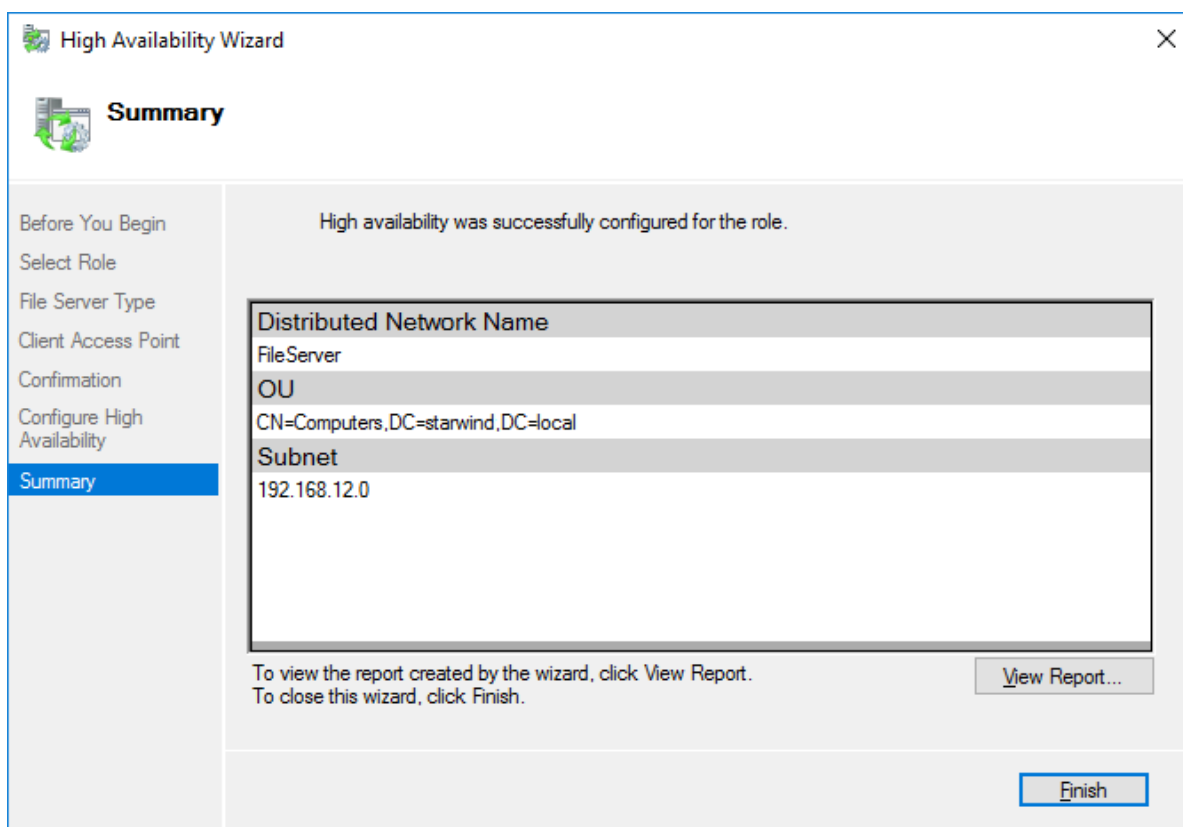
7. Check whether the specified information is correct. Click Next to proceed or Previous to change the settings.



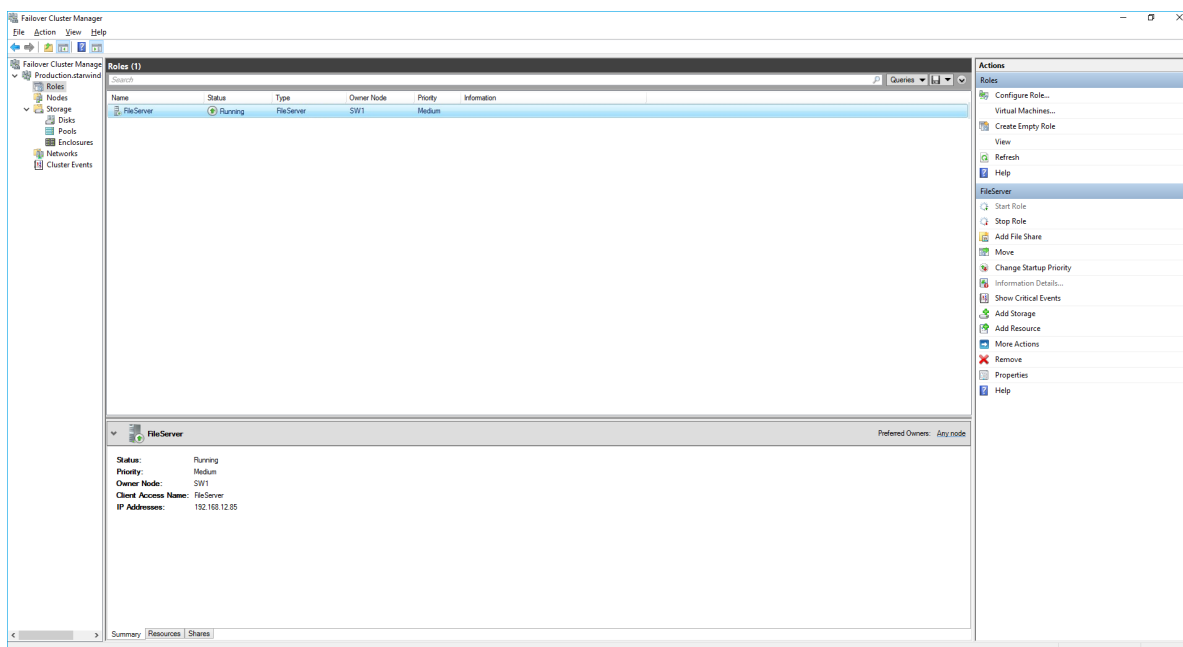
8. Once the installation has been finished successfully, the Wizard should now look like the screenshot below.

Click Finish to close the Wizard.





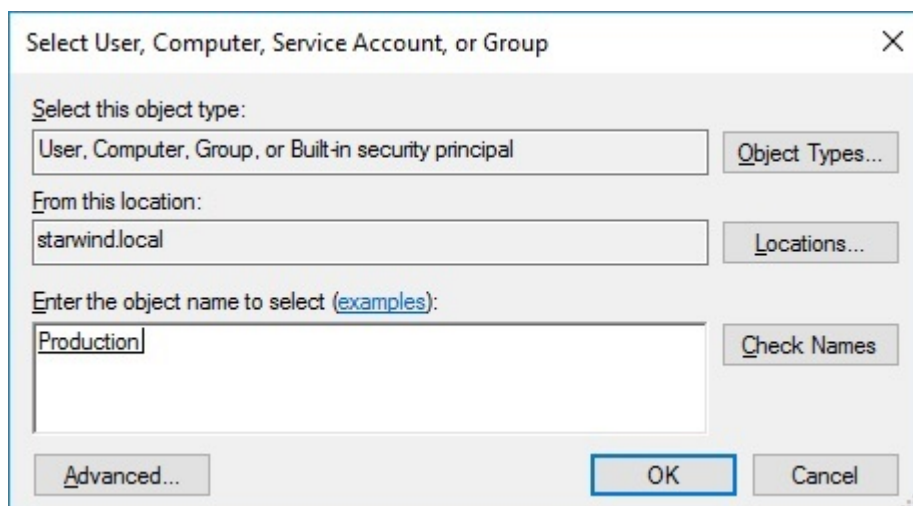
9. The newly created role should now look like the screenshot below.



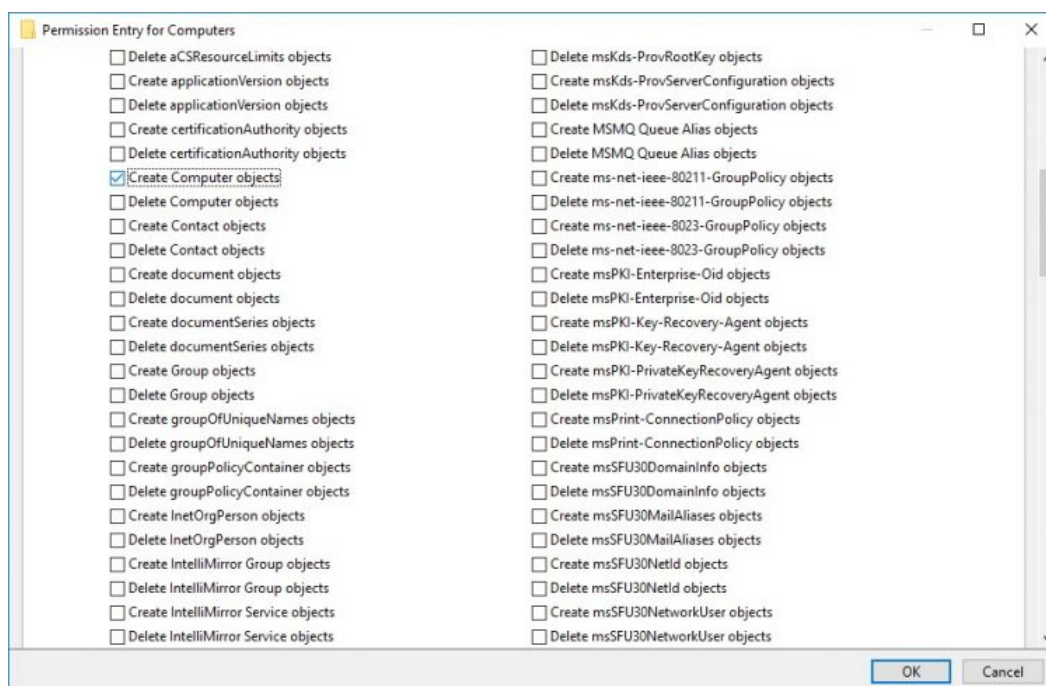
NOTE: If the role status is Failed and it is unable to Start, please, follow the next steps:

- open Active Directory Users and Computers

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



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



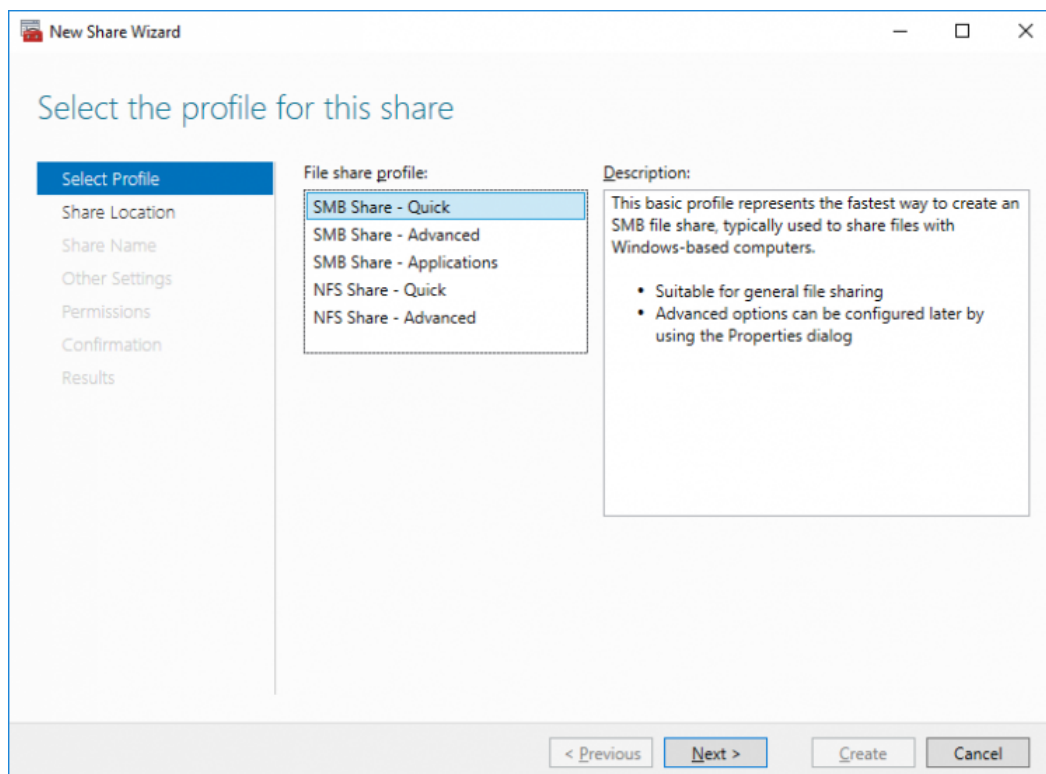
- click OK on all opened windows to confirm the changes

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

## Configuring Smb File Share

To Add SMB File Share

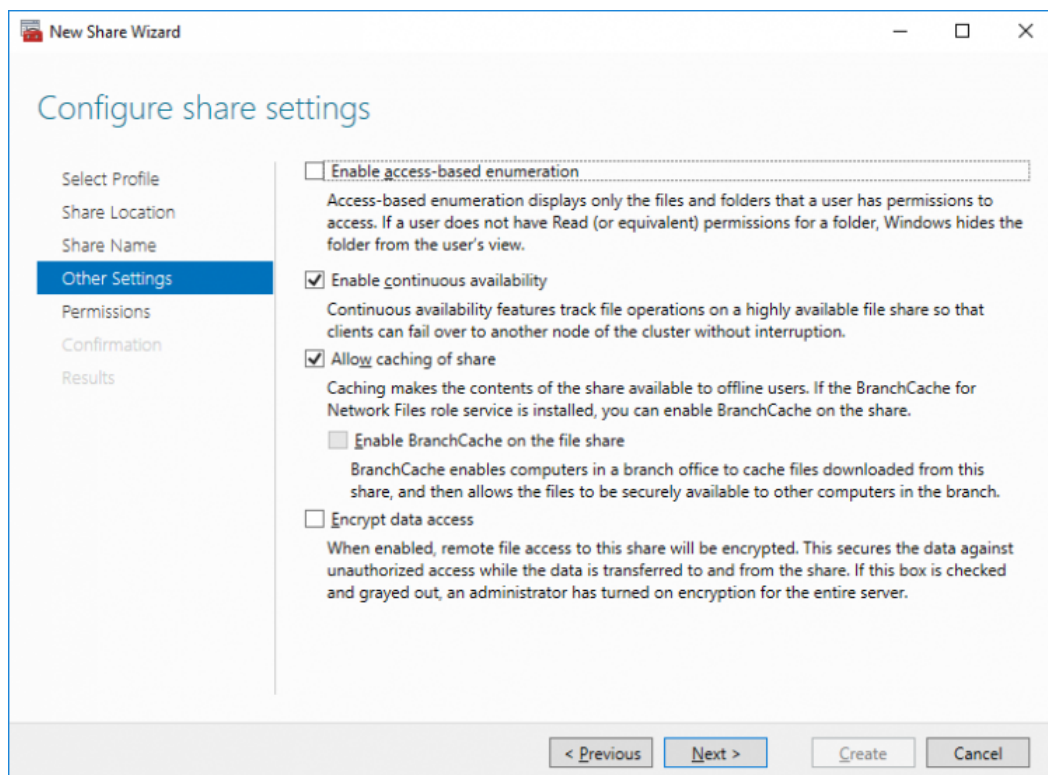
1. Open Failover Cluster Manager.
2. Expand the cluster and then click Roles.
3. Right-click the File Server role and then press Add File Share.
4. On the Select the profile for this share page, click SMB Share – Quick and then click Next.



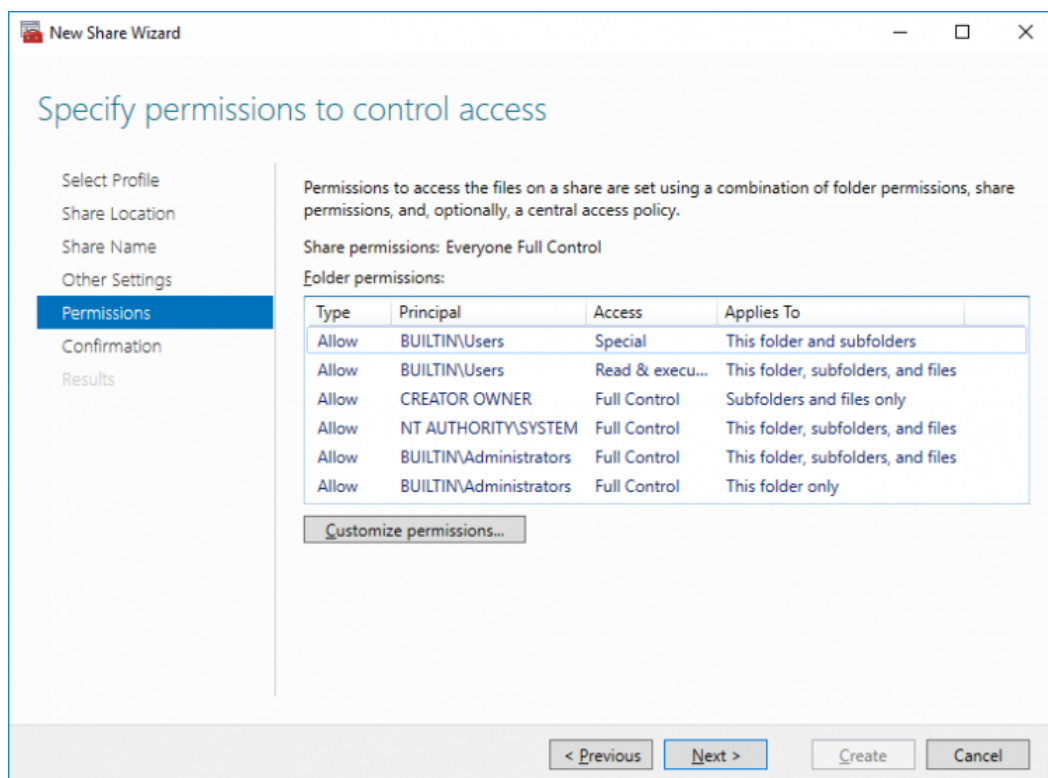
5. Select available storage to host the share. Click Next to continue.



continue.



8.Specify the access permissions for the file share.



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

**New Share Wizard**

### Confirm selections

Select Profile  
Share Location  
Share Name  
Other Settings  
Permissions  
**Confirmation**  
Results

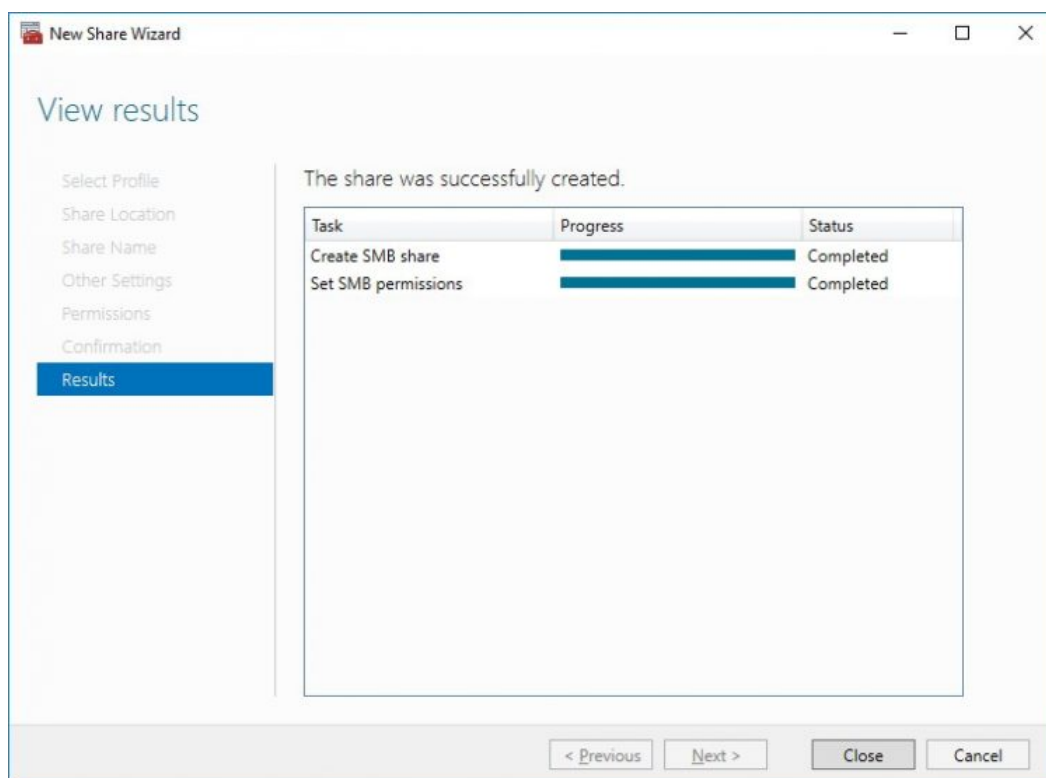
Confirm that the following are the correct settings, and then click Create.

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

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

< Previous   Next >   Create   Cancel

10. Check the summary and click Close.

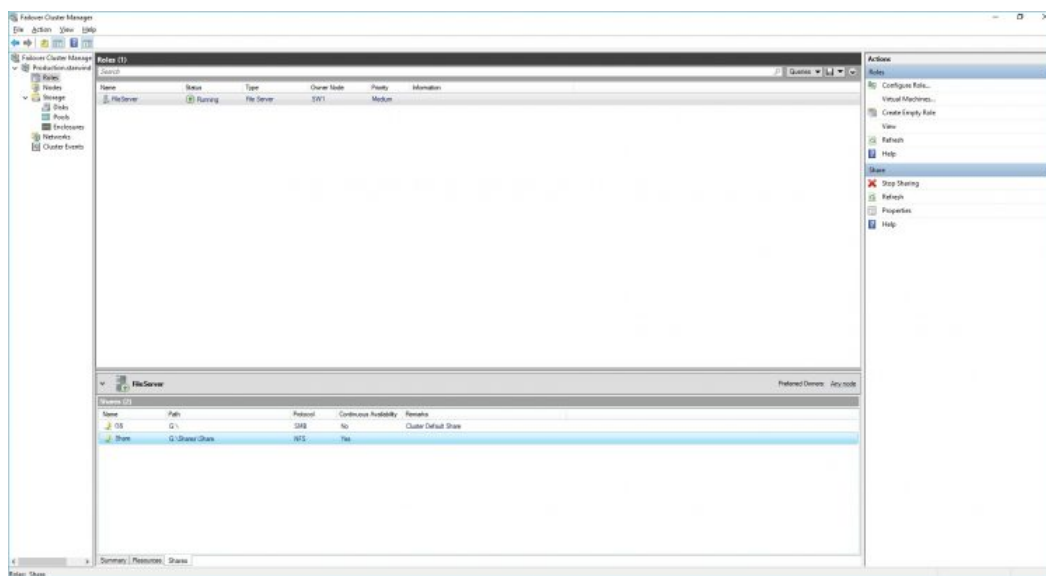


To manage created SMB File Shares

11. Open Failover Cluster Manager.

12. Expand the cluster and click Roles.

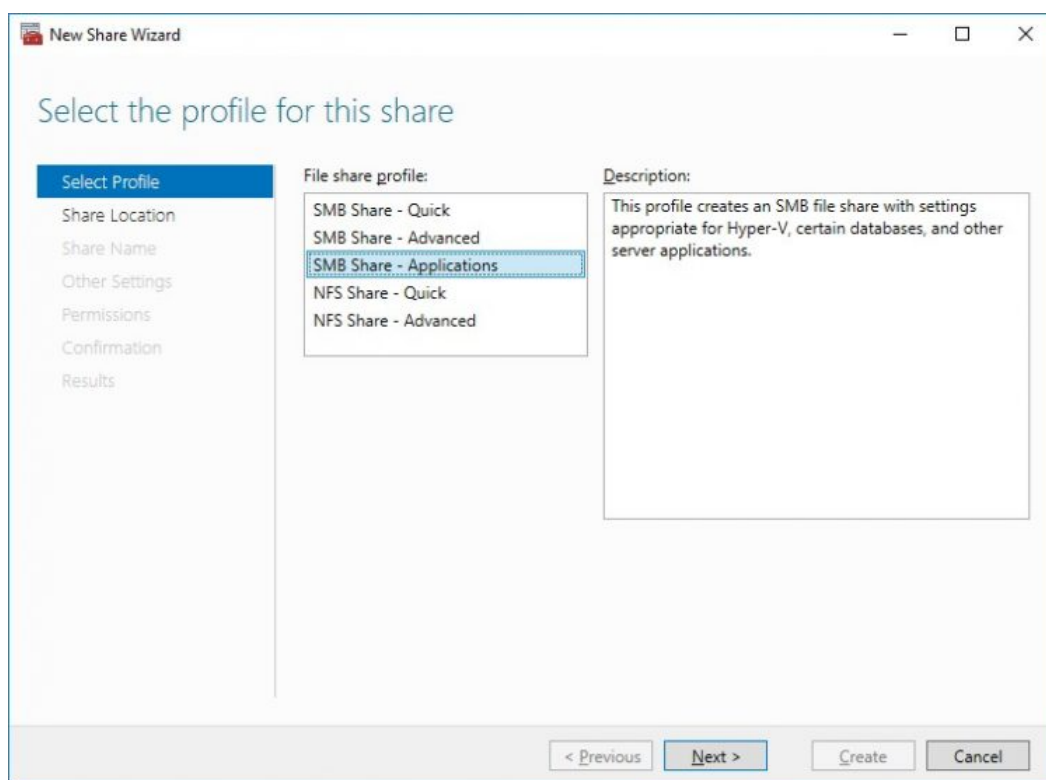
13. Choose the File Share role, select the Shares tab, right-click the created file share, and select Properties.



## Configuring Nfs File Share

To Add NFS File Share

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



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



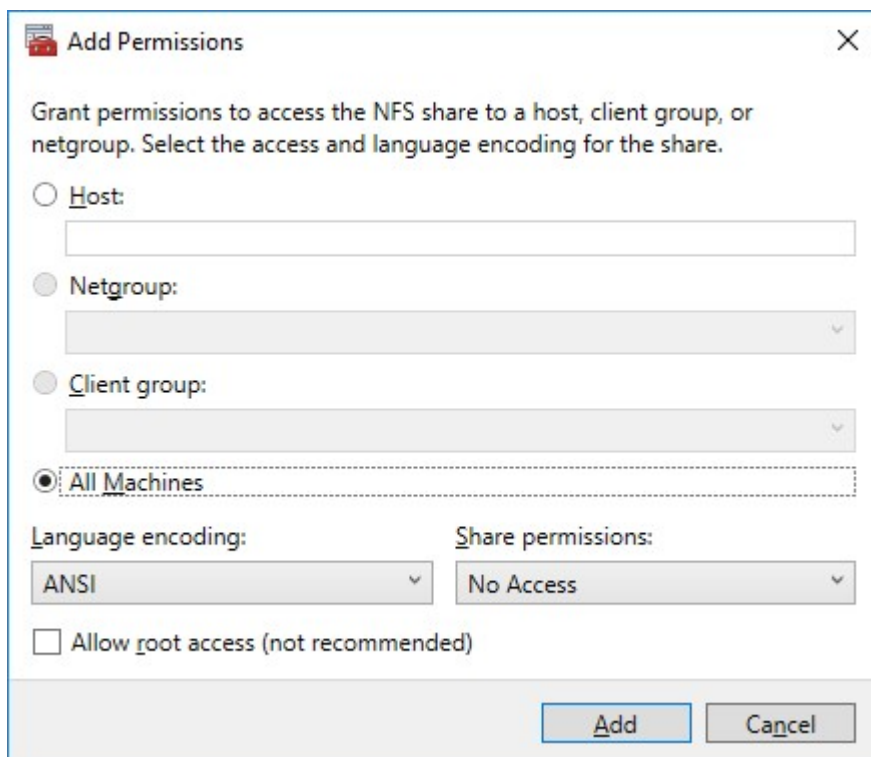


continue.

The screenshot shows the 'New Share Wizard' window at the 'Specify authentication methods' step. The left sidebar lists the steps: Select Profile, Share Location, Share Name, Authentication (highlighted), Share Permissions, Permissions, Confirmation, and Results. The main area has the title 'Specify authentication methods' and the instruction 'Specify the authentication methods that you want to use for this NFS share.' There are two sections: 'Kerberos v5 authentication' with three unchecked checkboxes, and 'No server authentication' with three checked options: 'No server authentication (AUTH\_SYS)', 'Enable unmapped user access', and 'Allow anonymous access' (which is selected with a radio button). At the bottom are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.

8. Click Add and specify Share Permissions.

The screenshot shows the 'New Share Wizard' window at the 'Specify the share permissions' step. The left sidebar highlights 'Share Permissions'. The main area has the title 'Specify the share permissions' and an explanatory text: '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.' Below this is a table with columns: Name, Permissions, Root Access, and Encoding. The table is currently empty. To the right of the table are up and down arrow buttons. Below the table are 'Add...', 'Edit...', and 'Remove' buttons. At the bottom are buttons for '< Previous', 'Next >', 'Create', and 'Cancel'.



**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

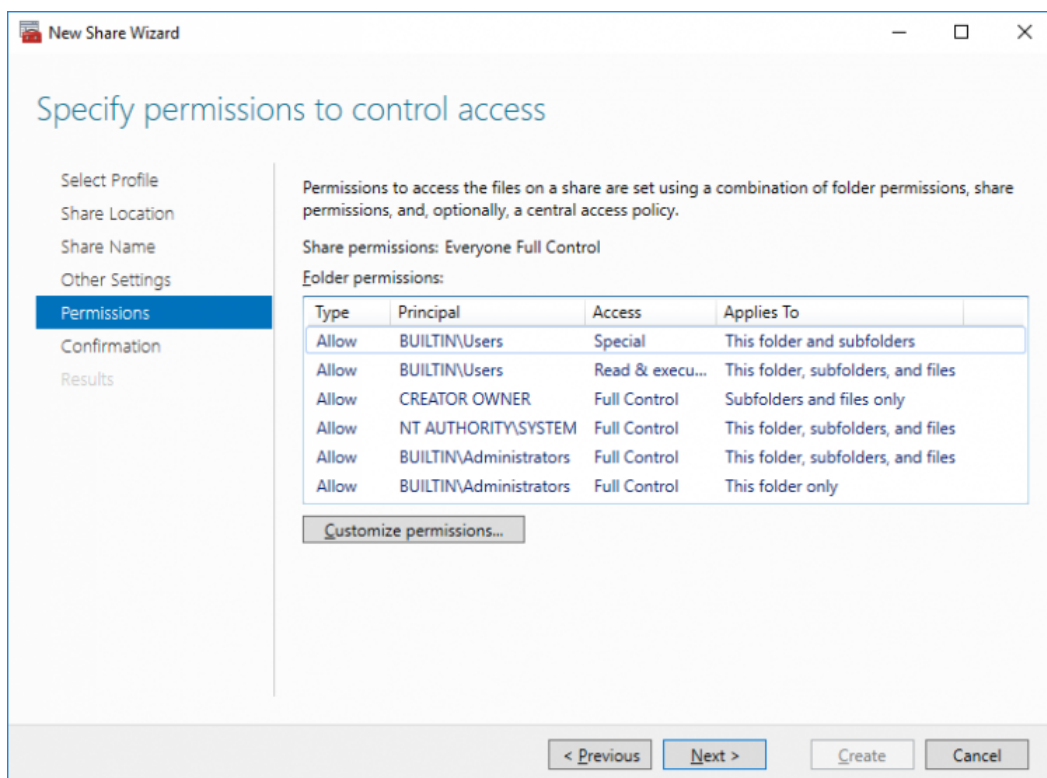
Language encoding: ANSI

Share permissions: No Access

☐ Allow root access (not recommended)

Add Cancel

9. Specify the access permissions for the file share.



**New Share Wizard**

Specify permissions to control access

Select Profile

Share Location

Share Name

Other Settings

**Permissions**

Confirmation

Results

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

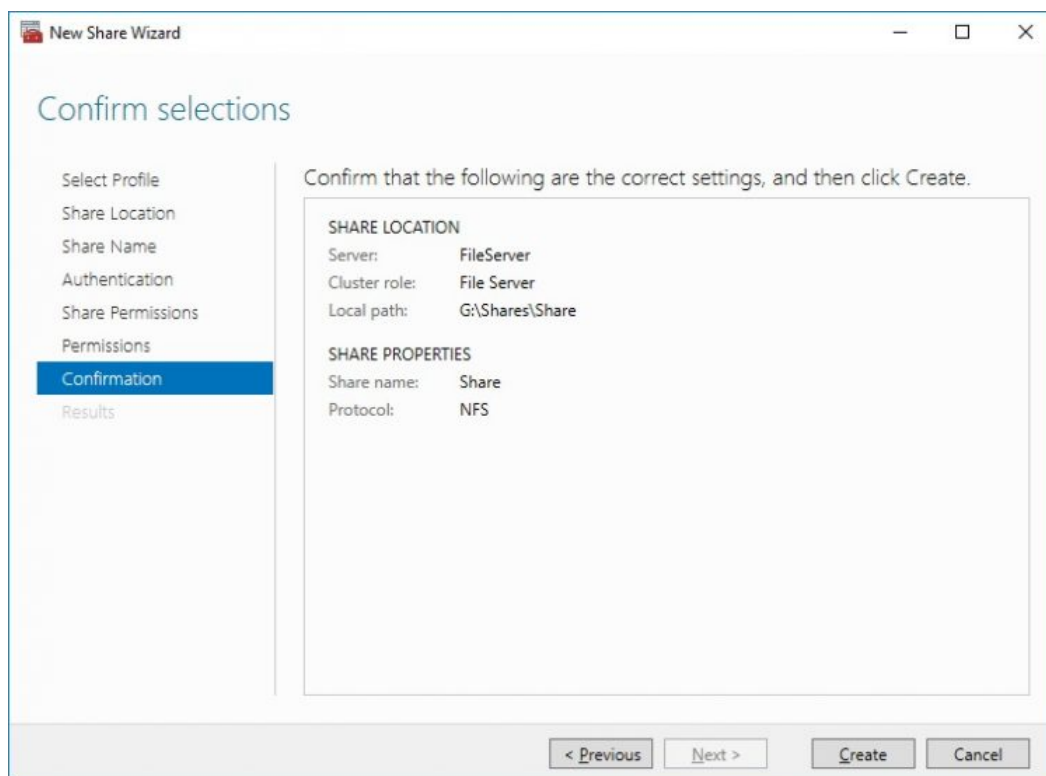
Folder permissions:

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

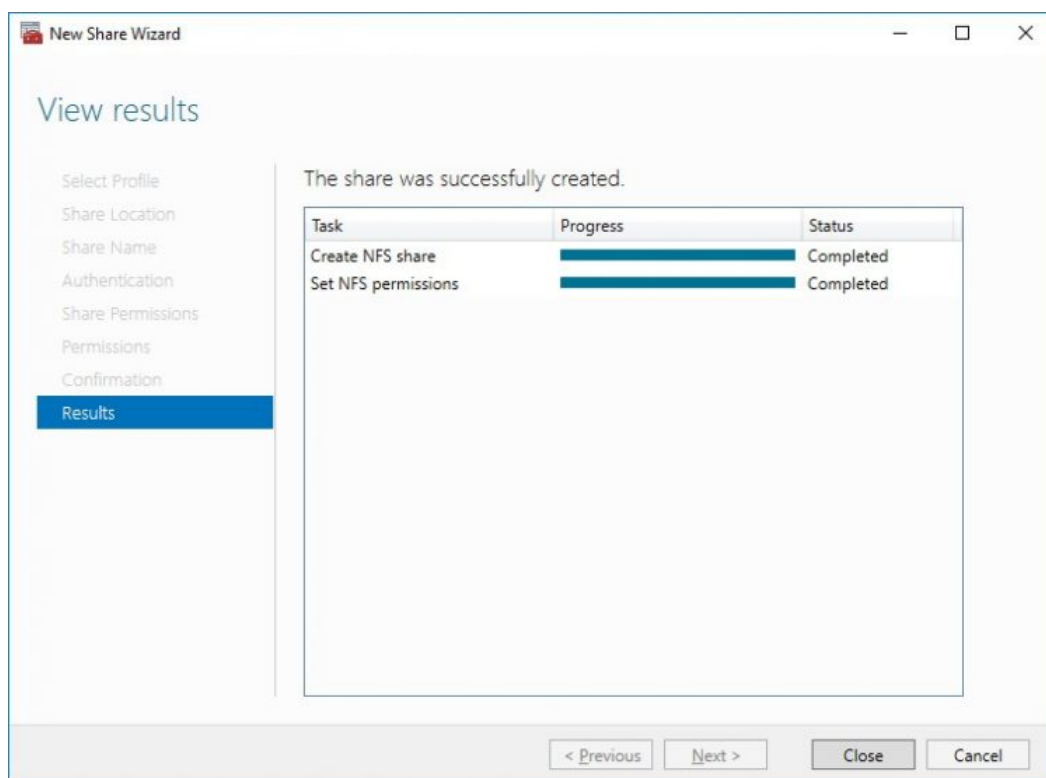
Customize permissions...

< Previous Next > Create Cancel

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

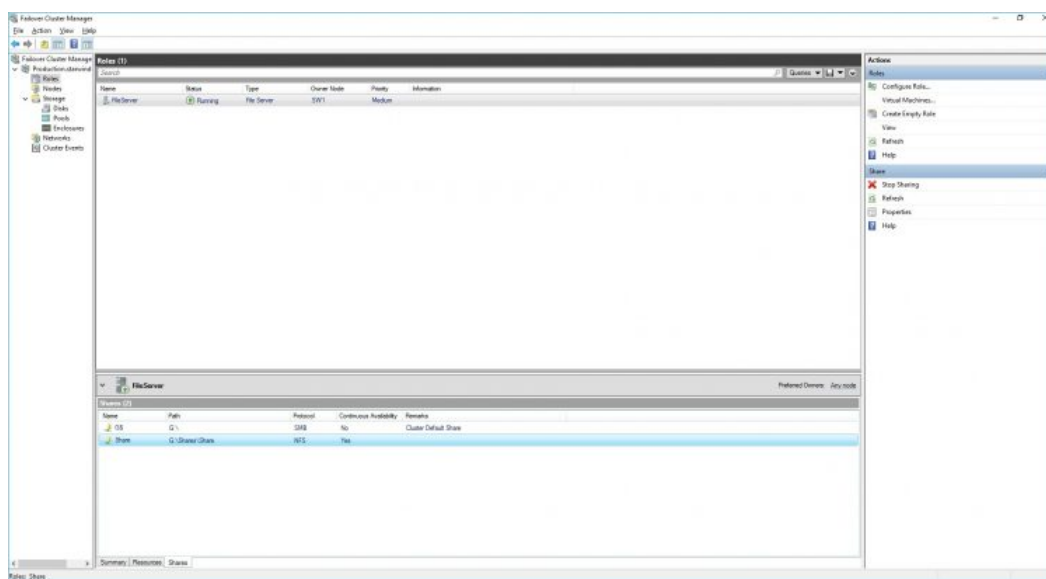


11. Check a summary and click Close to close the Wizard.



To manage created NFS File Shares:








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



## Conclusion

Deploying and configuring Failover Cluster on Microsoft Azure Stack HCI is a crucial process for organizations looking to achieve a high-performing, VM-centric environment. With this guide, IT professionals will have all the necessary resources for a successful cluster deployment with a shared highly-available storage, provided by StarWind VSAN.

## 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](mailto:sales@starwind.com)

General Information: [info@starwind.com](mailto:info@starwind.com)



StarWind Software, Inc. 100 Cummings Center Suite 224-C Beverly MA 01915, USA  
[www.starwind.com](http://www.starwind.com) ©2024, StarWind Software Inc. All rights reserved.