

StarWind SAN & NAS CVM 2-node Converged Scenario with Windows Server

2026

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.

Introduction

StarWind SAN & NAS Controller Virtual Machine (CVM) comes as a prepackaged Linux Virtual Machine (VM) to be deployed on any industry-standard hypervisor. The solution is a fully certified shared storage for Windows Server and Microsoft Hyper-V Server, allowing you to repurpose your existing hardware running industry-standard hypervisor into high-performing storage.

StarWind SAN & NAS supports hardware and software-based storage redundancy configurations. The solution allows turning your server with internal storage into a redundant storage array presented as NAS or SAN, exposing standard protocols such as iSCSI, SMB, and NFS. It features Web-based UI, Text-based UI, and Command-line interface for your cluster-wide operations.

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

Starwind San & Nas Virtual Machine Requirements

Prior to installing StarWind SAN & NAS virtual storage appliance, please make sure that the system meets the requirements, which are available at the following link:

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

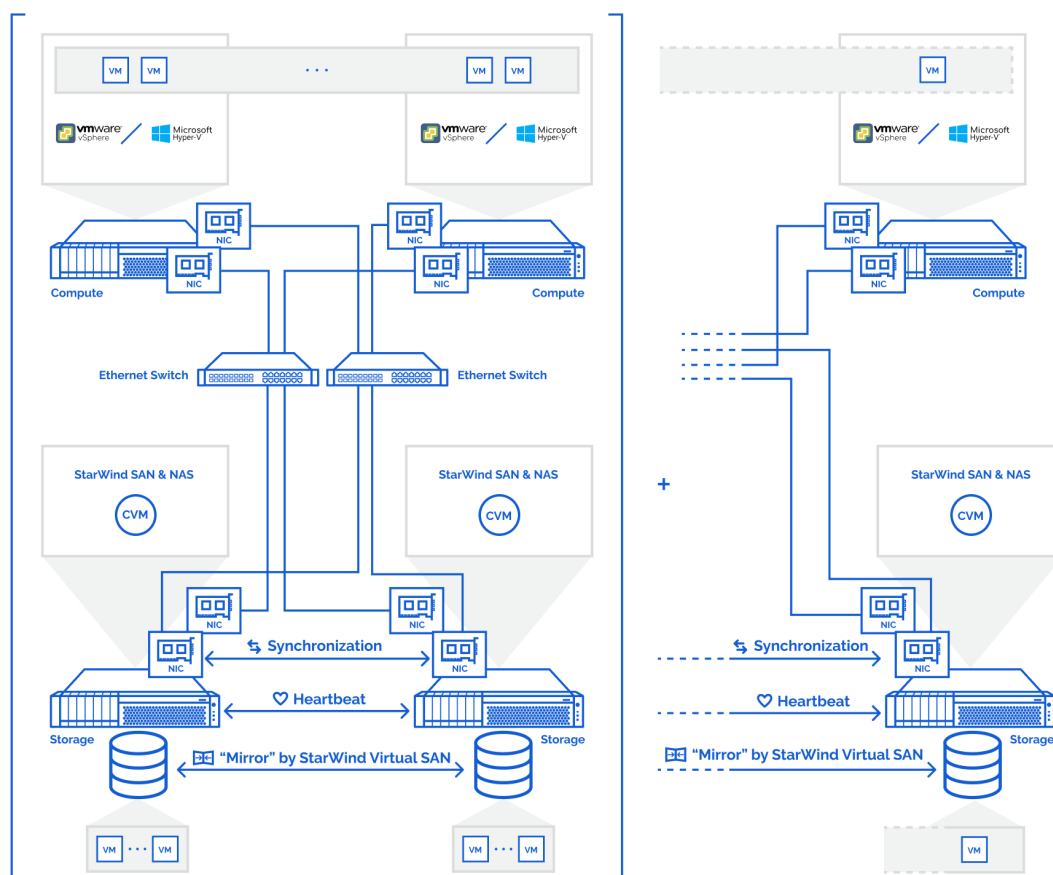
Pre-Configuring The Servers

The diagrams below illustrate the common network and storage configurations of the solution for specific deployment configurations.

Please select your deployment scenario:

Highly Available Shared Storage Servers

- Dedicated 2 storage servers expose highly available shared storage for vSphere and Hyper-V clusters:



1. Install the hypervisor of your choice, VMware vSphere Hypervisor ESXi or Hyper-V Server, on two dedicated storage servers, and on the compute servers that are intended to connect and utilize the shared storage provisioned by the appliance.

2. StarWind SAN & NAS CVM is deployed on each Hyper-V Server or VMware ESXi server with commodity direct-attached storage.

3. The network interfaces on each node for Management, Data/iSCSI, and Replication interfaces should be connected to different subnets and connected directly according to the network diagram above. Here, the 172.16.10.x subnet is used for the Data (iSCSI) storage traffic, and 172.16.20.x subnet is used for the Replication storage traffic.

NOTE: The vCenter server is recommended for the deployment of multiple ESXi servers.

NOTE: The Failover Cluster feature is recommended for the deployment of multiple Hyper-V servers.

Setting Up Starwind San & Nas

This part describes how to prepare the environment to deploy and install StarWind SAN & NAS using your hypervisor of choice, either VMware ESXi and VMware vSphere web clients or Microsoft Hyper-V Server.

Please select the required option:

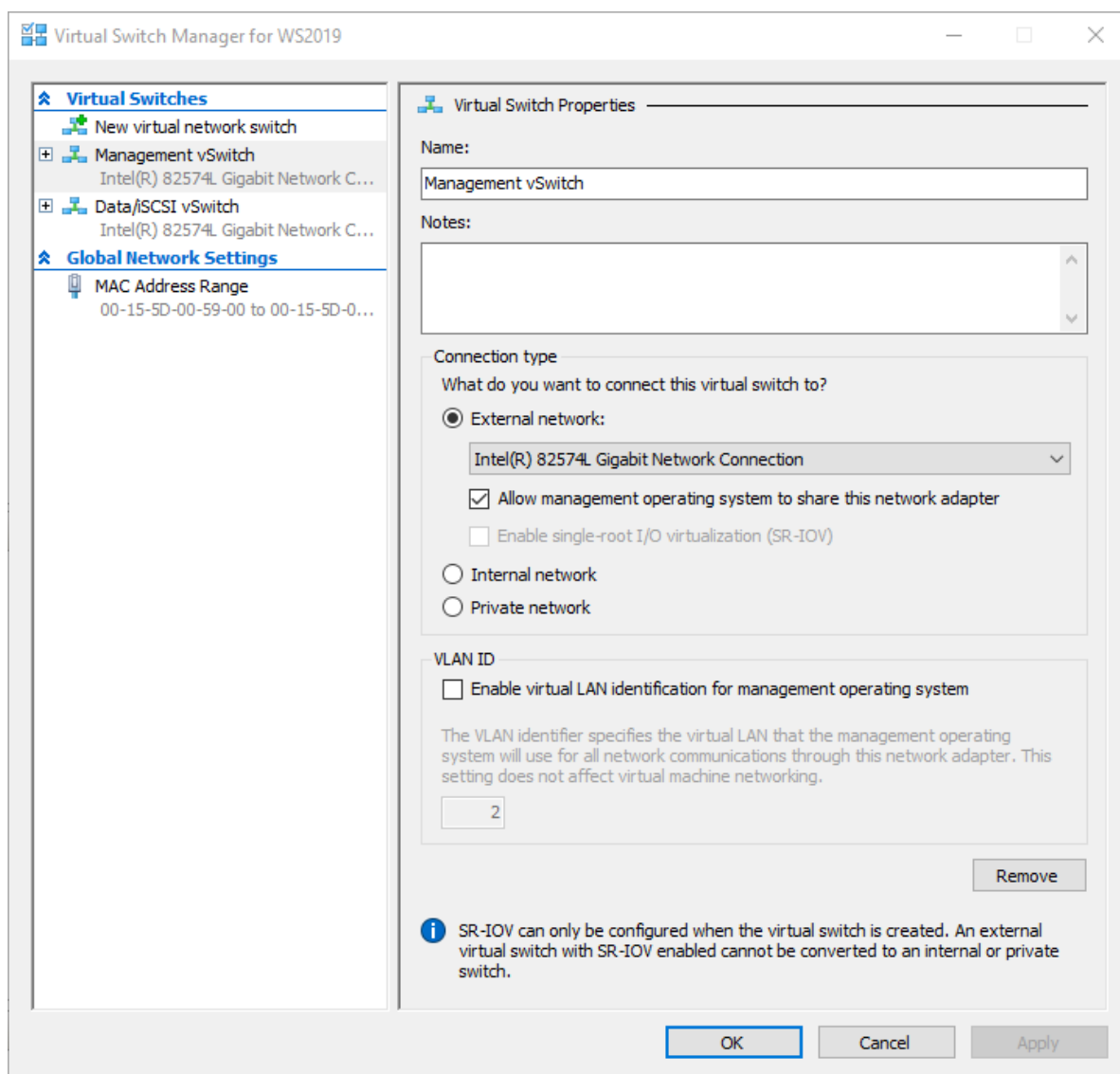
Configuring Converged Storage Server With Hyper-V Server

Configuring Networks On Microsoft Hyper-V Server

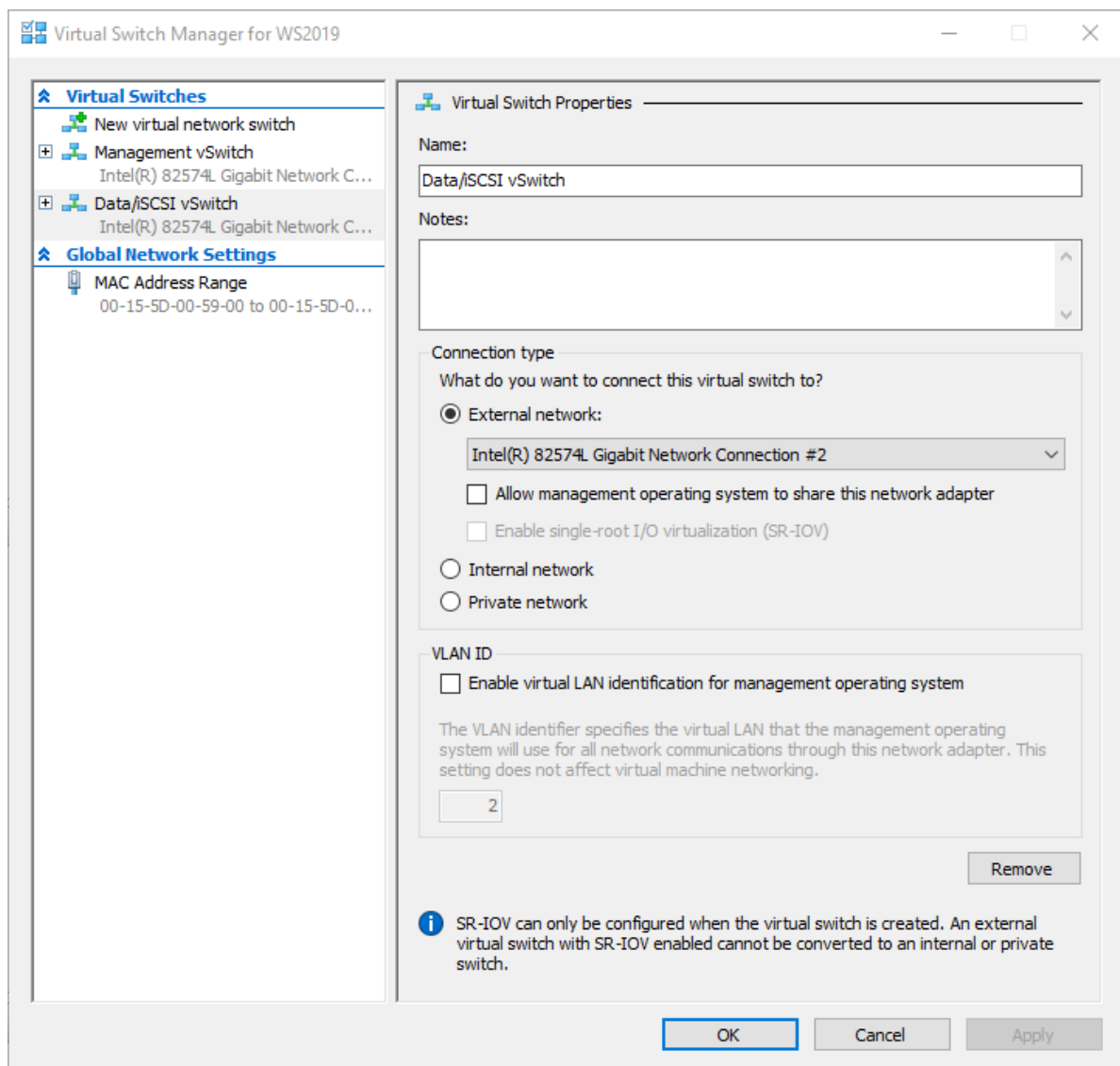
Configure external virtual switches on a hypervisor server, at least one for Management, one for Data, and one for Replication. Ensure the interfaces are in different subnets and connected physically according to the network diagram above. All actions below should be applied to each Hyper-V server for running StarWind SAN & NAS. In this document, the 172.16.10.x subnet is used for Data traffic and 172.16.20.x subnet is used for Replication traffic.

NOTE: It is recommended to set jumbo frames to 9000 on the virtual switch and network interfaces used for Data/iSCSI traffic.

1. Using Virtual Switch Manager create a new external virtual switch for the Management network.



2. Create a second external virtual switch for the Data network.

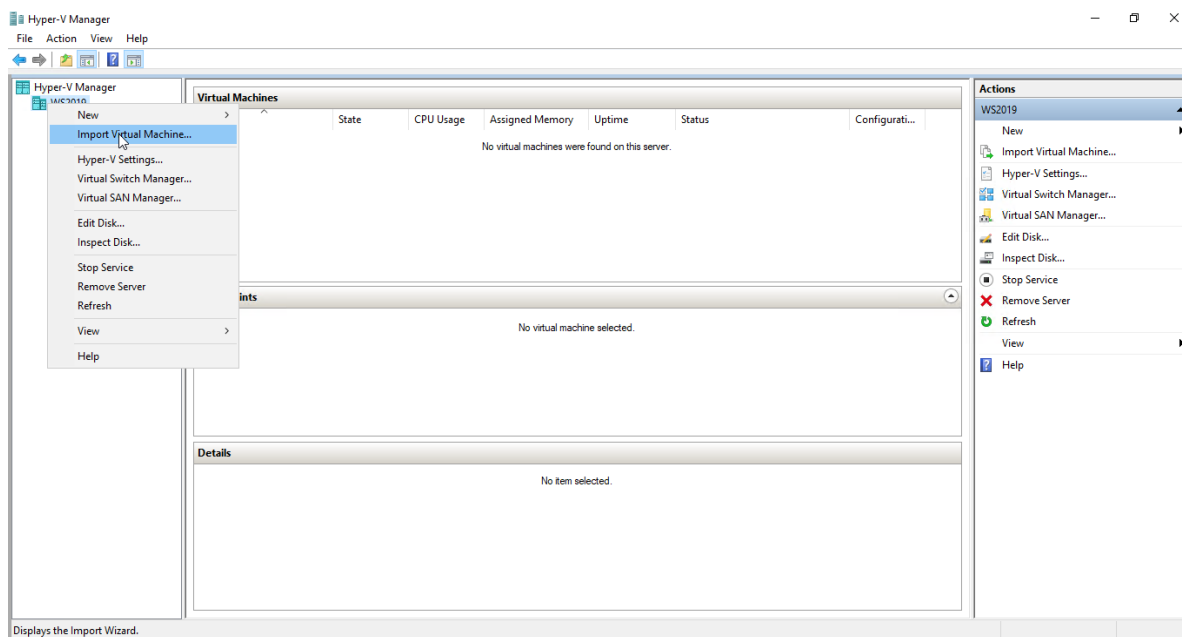


3. Repeat the procedure, create a third external virtual switch for the Replication (Synchronization) network.

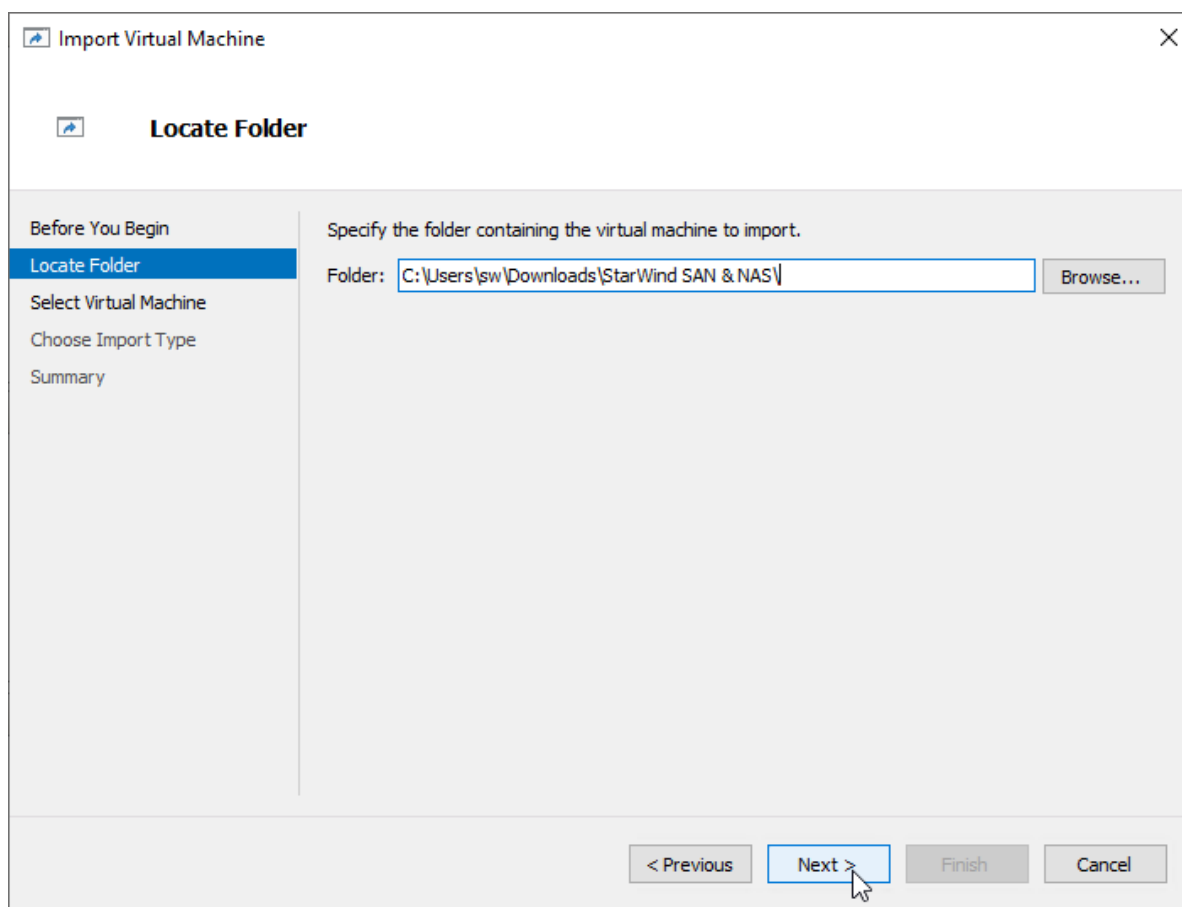
Deploying Starwind San & Nas Cvm On Hyper-V Servers

1. Download the zip archive that contains StarWind SAN & NAS CVM
<https://www.starwindsoftware.com/san-and-nas#download>
2. Extract the virtual machine files.

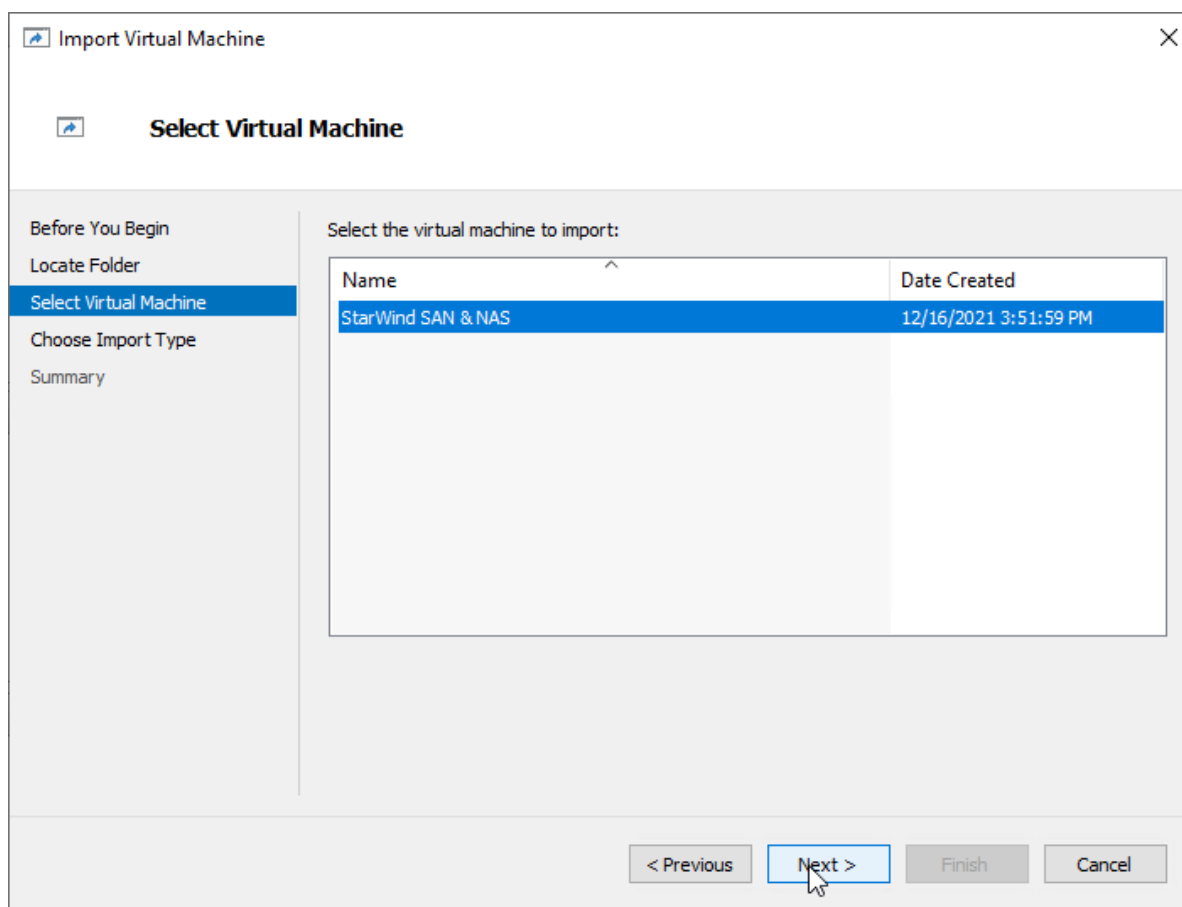
3. Deploy the control virtual machine to the Microsoft Hyper-V Server using the “Import Virtual Machine” wizard in Hyper-V Manager.



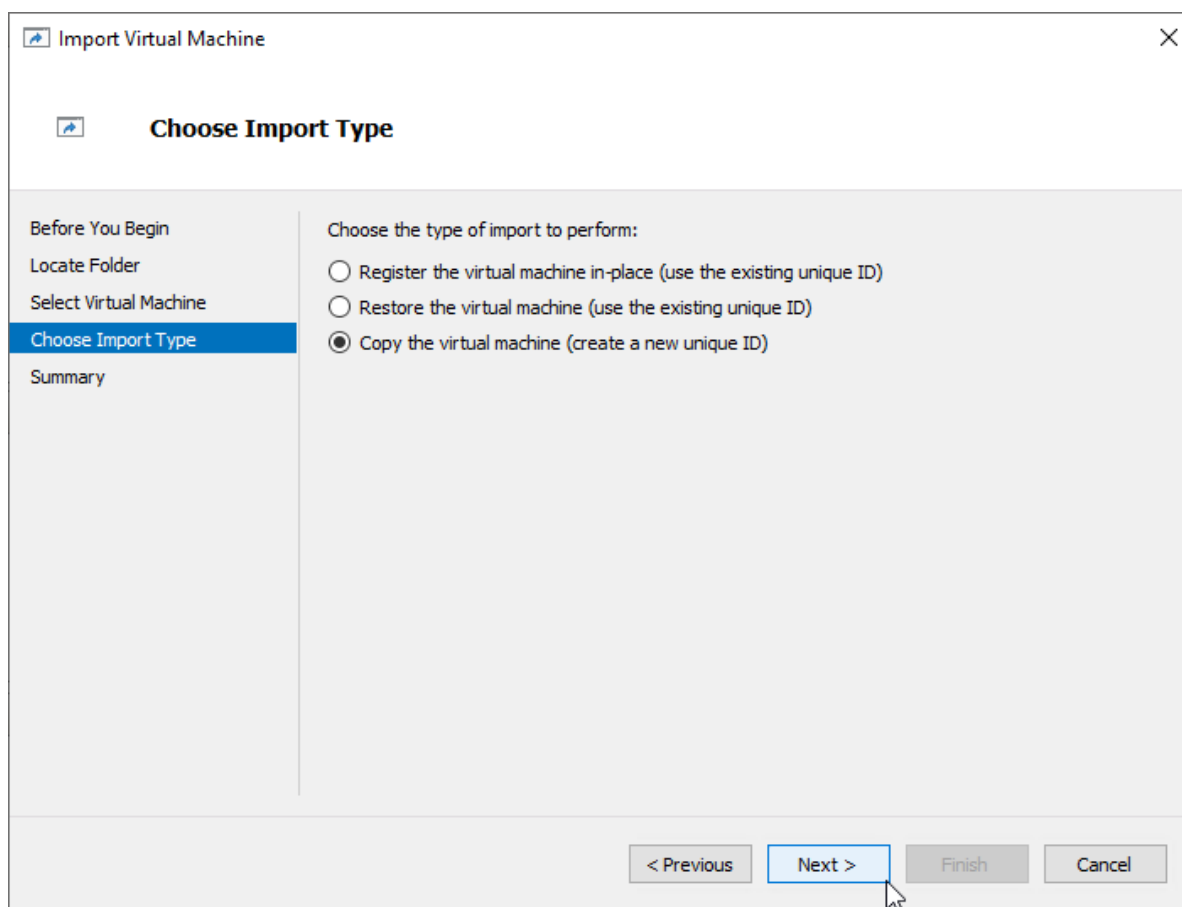
4. On the second page of the wizard, point to the location of the VM template. Select the VM folder and click Next.



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



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



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

Import Virtual Machine

Choose Folders for Virtual Machine Files

Before You Begin

Locate Folder

Select Virtual Machine

Choose Import Type

Choose Destination

Choose Storage Folders

Summary

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

☒ Store the virtual machine in a different location

Virtual machine configuration folder:

Checkpoint store:

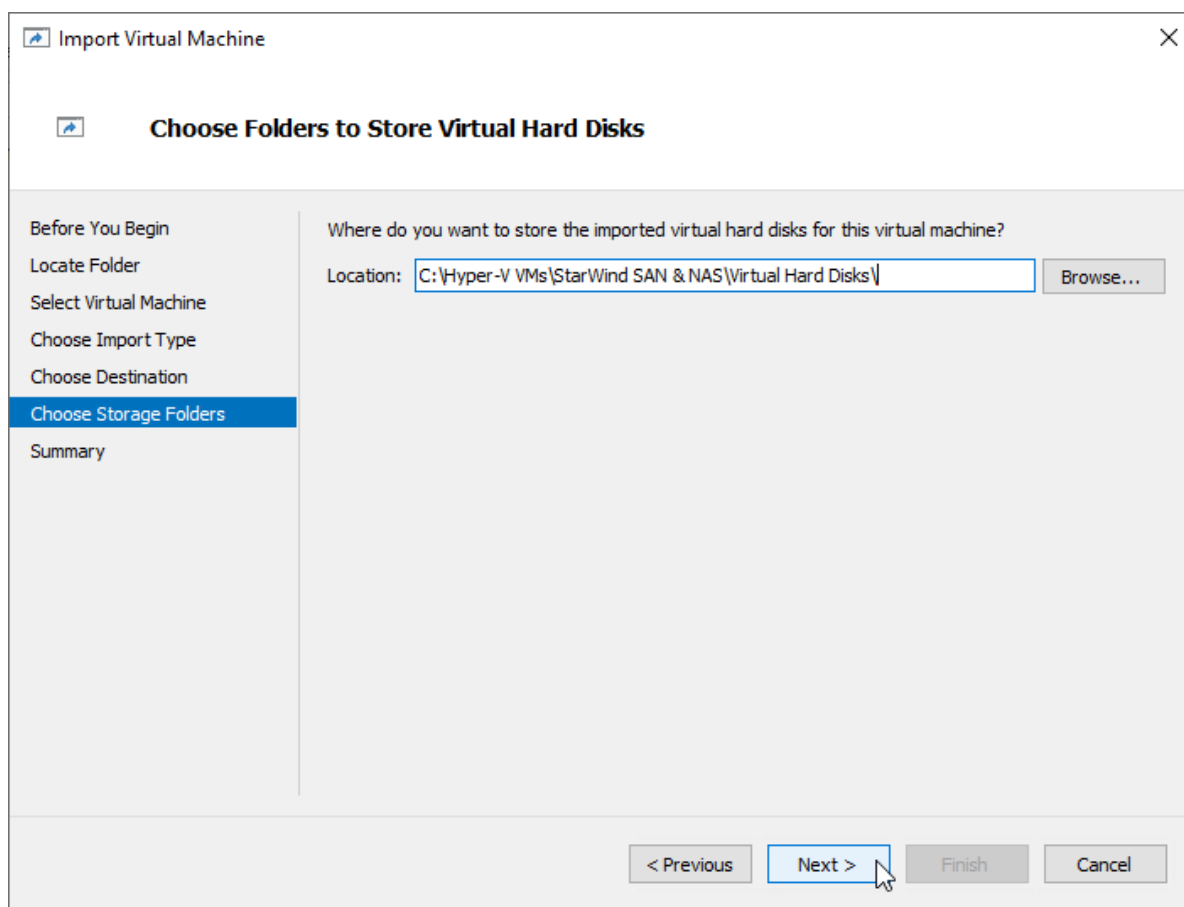
Smart Paging folder:

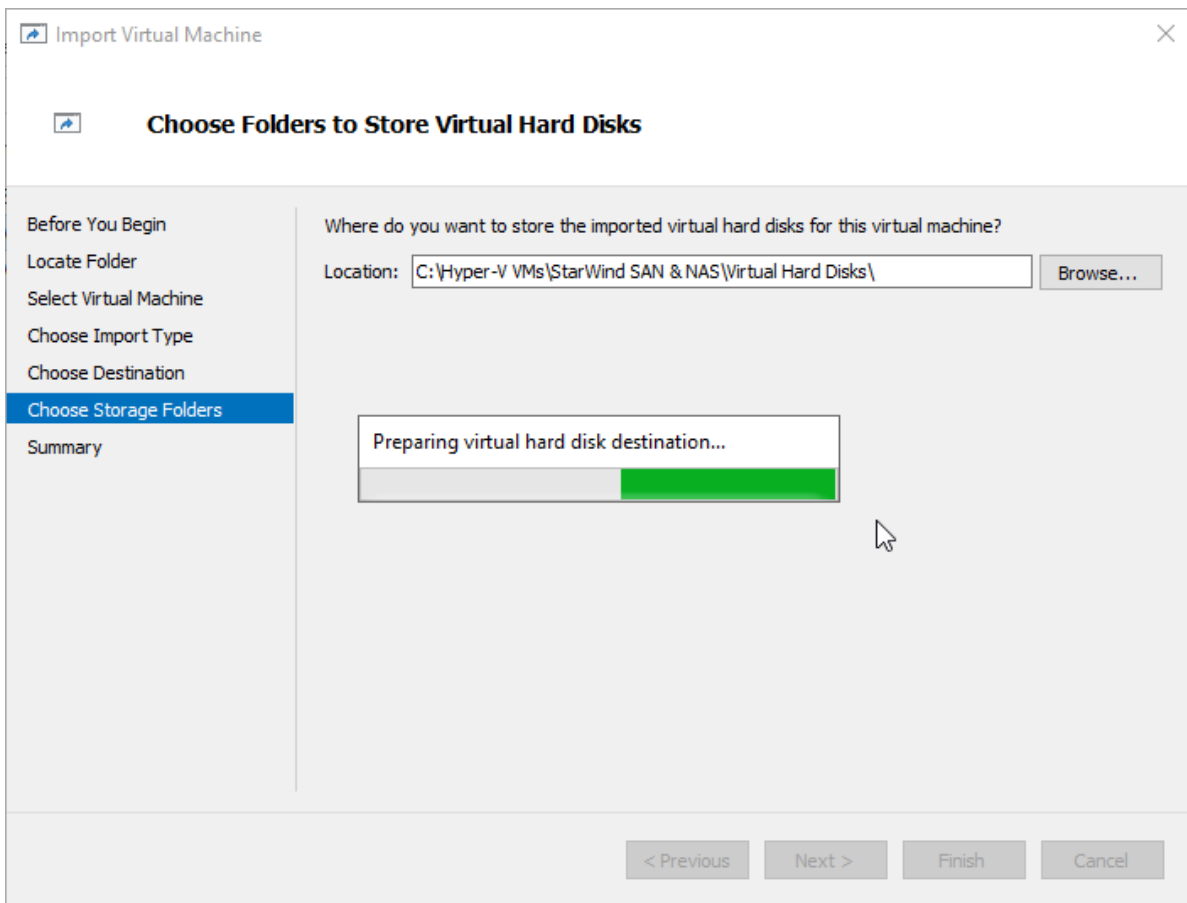
< Previous

Next >

Finish

Cancel



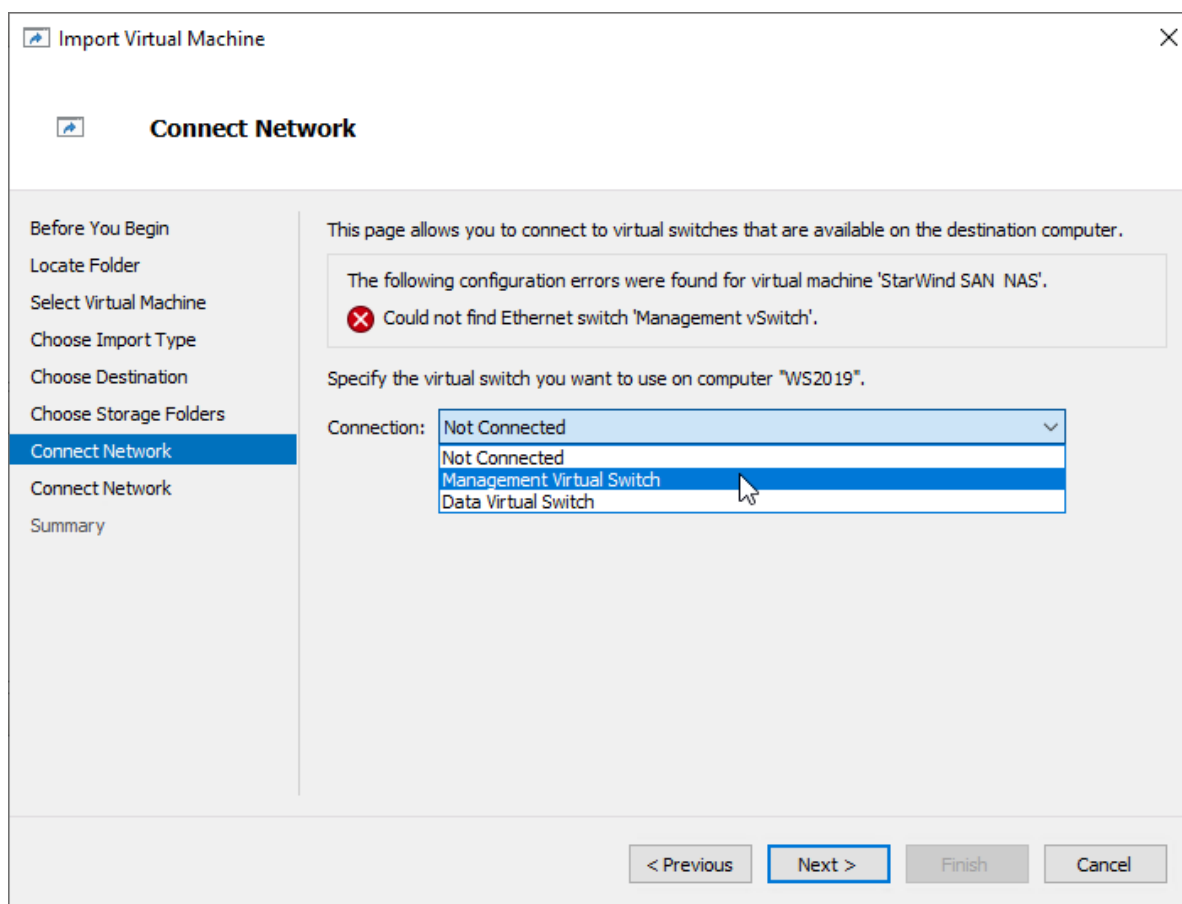


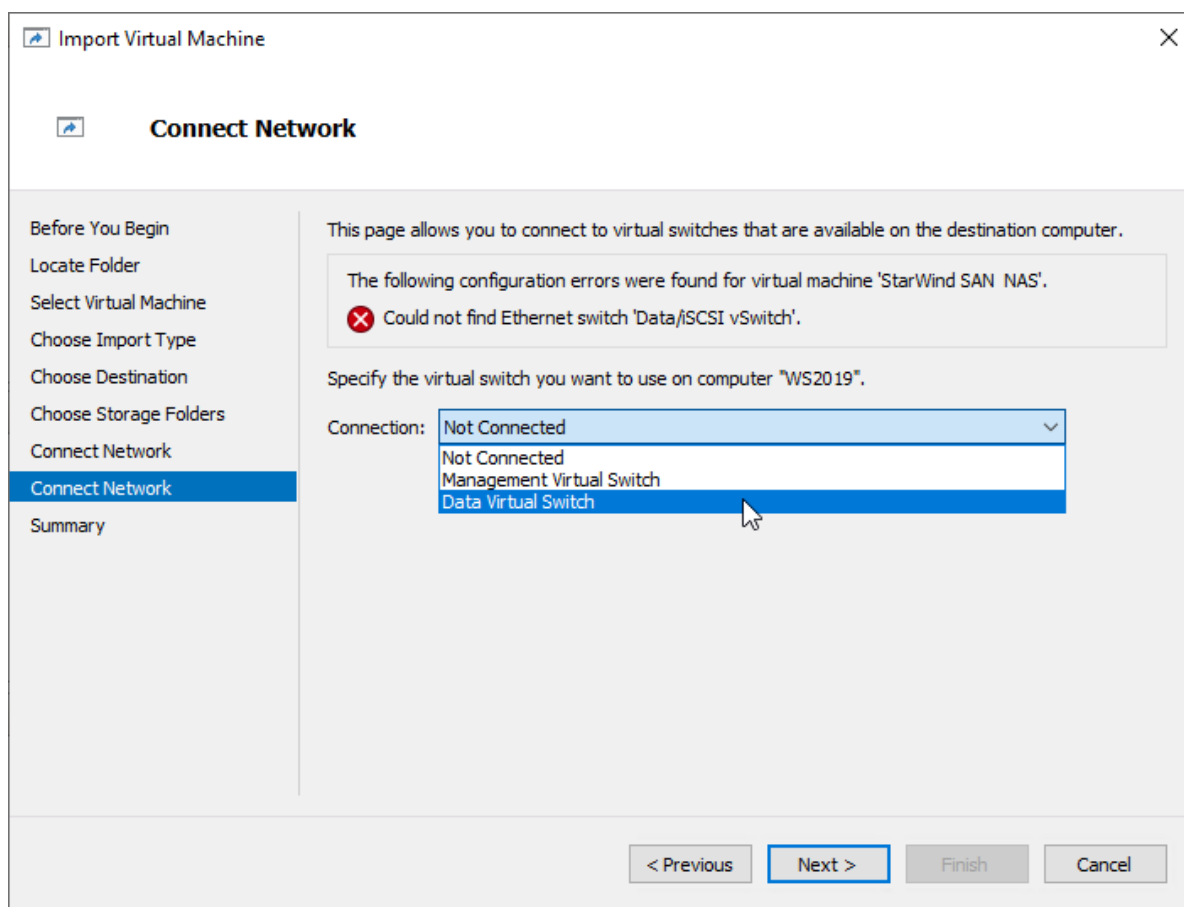
8. In the second step of the wizard, the “VM import” wizard will validate the network.

The default naming for virtual switches:

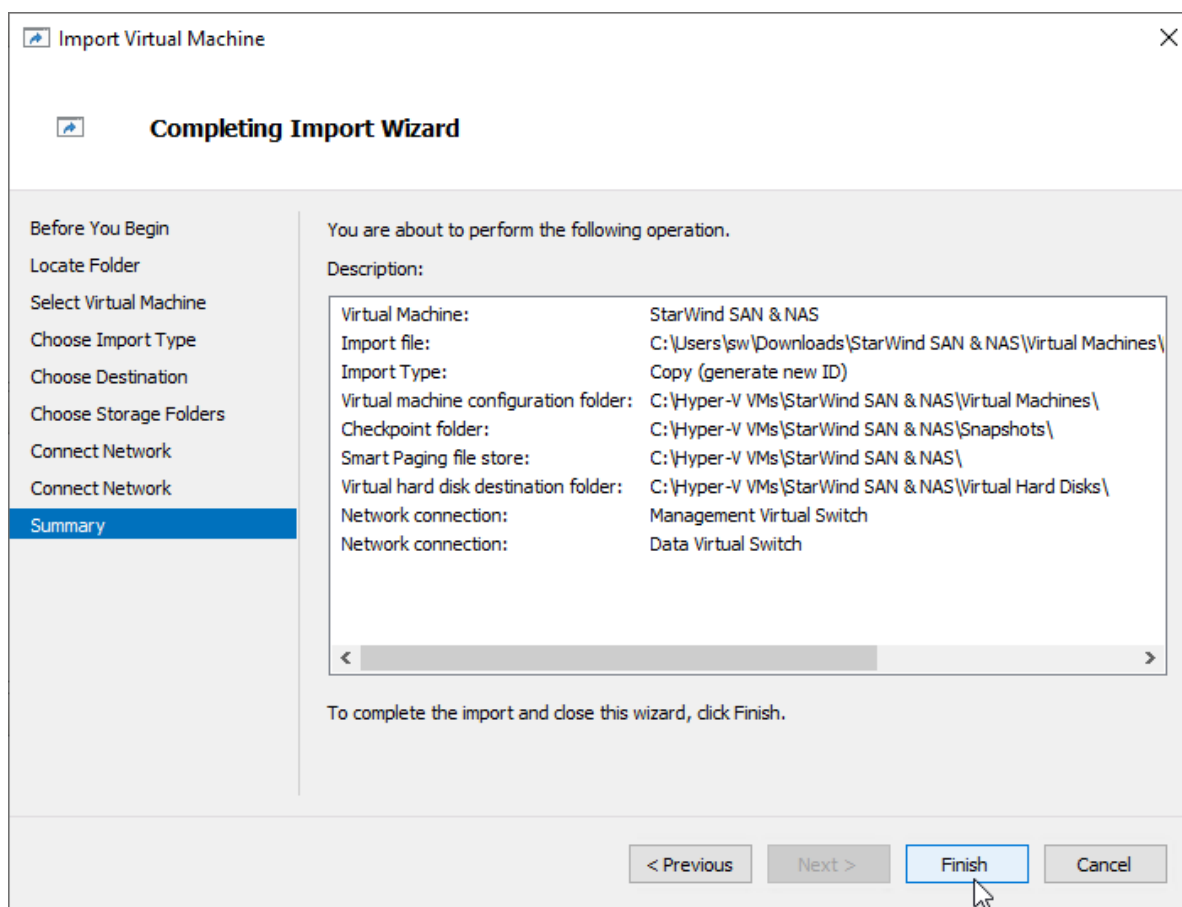
- the Management virtual switch is “Management vSwitch”,
- the iSCSI virtual switch is “Data/iSCSI vSwitch”,
- the Synchronization virtual switch is “Replication/Sync vSwitch”.

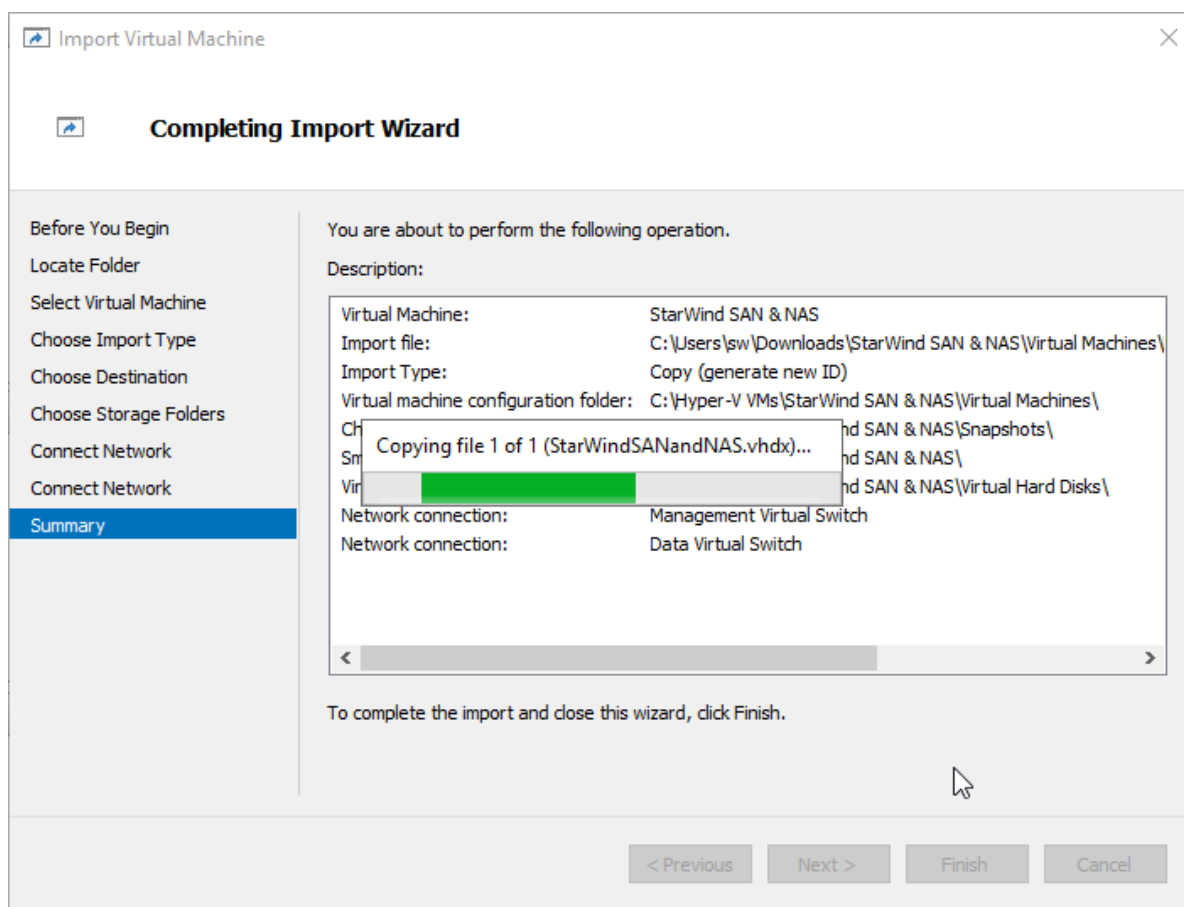
If existing virtual switches have different names, specify corresponding network connections. Click Next.





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



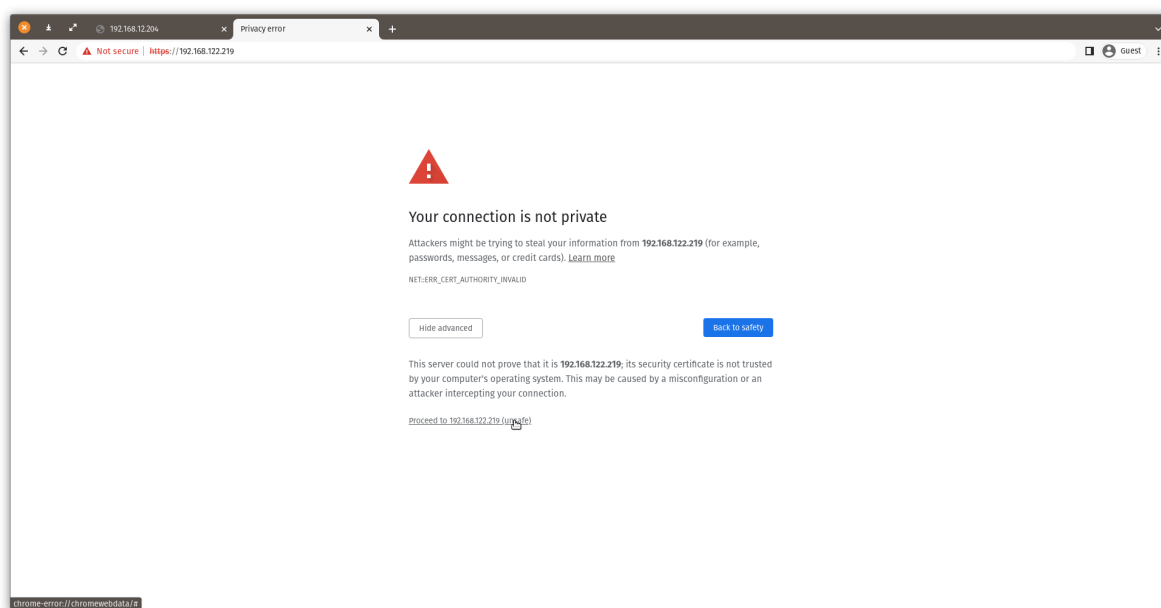


10. Repeat the VM deployment on each partner server which is used for configuring 2-node or 3-node highly available storage according to your licensing.

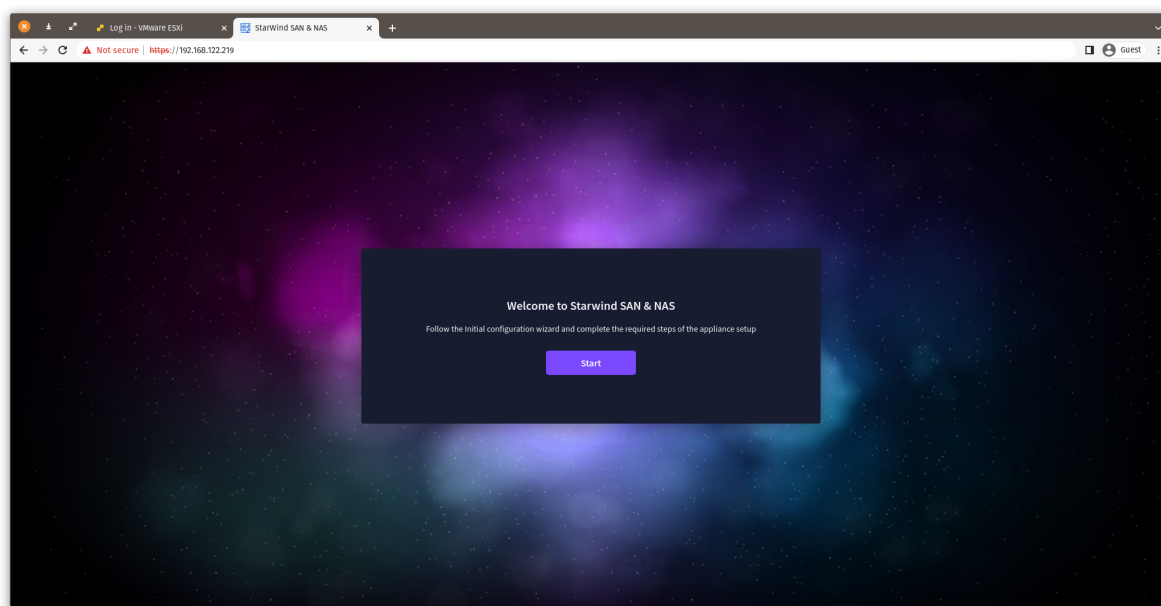
Configuring Appliances

Getting Started With Starwind San & Nas

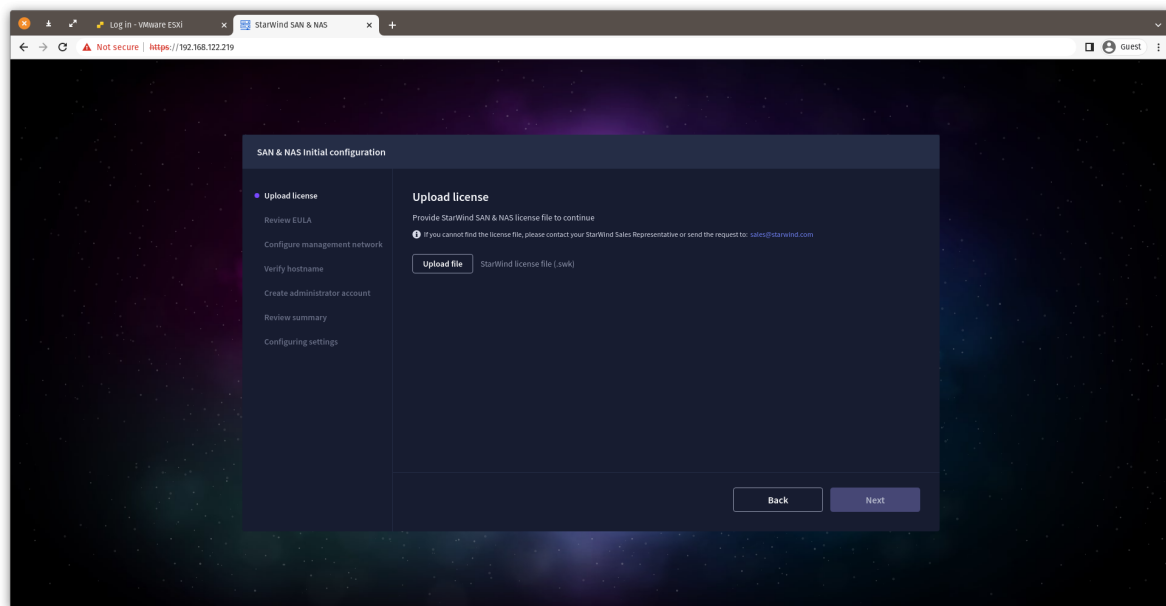
1. Start StarWind SAN & NAS CVM.
2. Launch Console to see the VM boot process and get the IPv4 address of the Management network interface.
Note: in case VM has no IPv4 address obtained from a DHCP server, use the Text-based User Interface (TUI) to set up a Management network.
3. Using the web browser, open a new tab and enter the VM IPv4 address to open StarWind SAN & NAS Web Interface. Click "Advanced" and then "Continue to..."



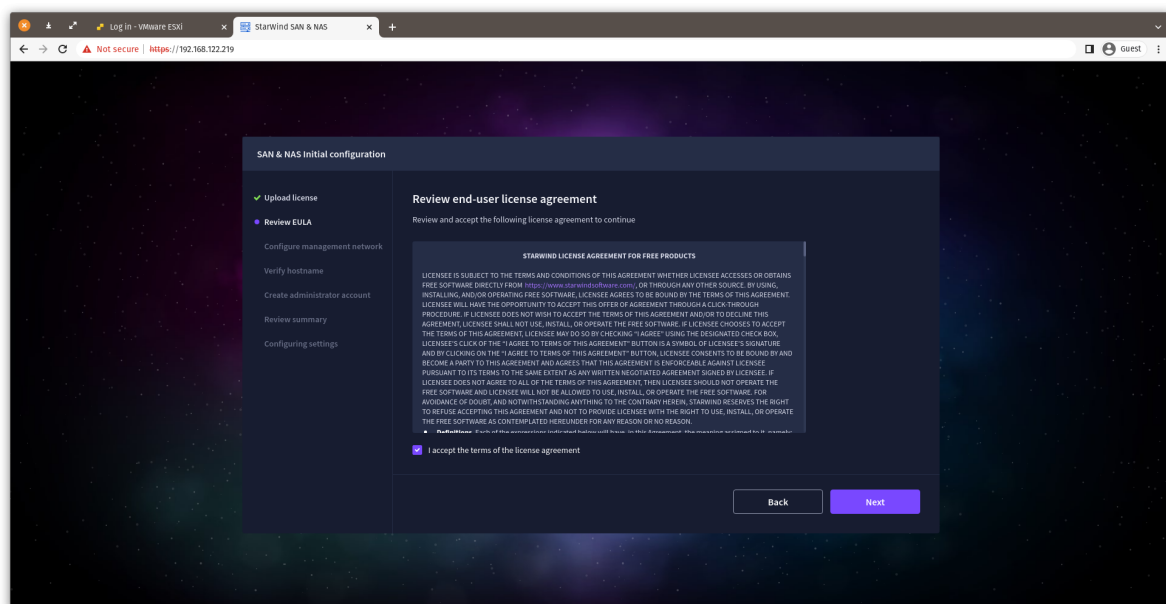
4. StarWind SAN & NAS welcomes you, and the “Initial configuration” wizard will guide you through the deployment process.



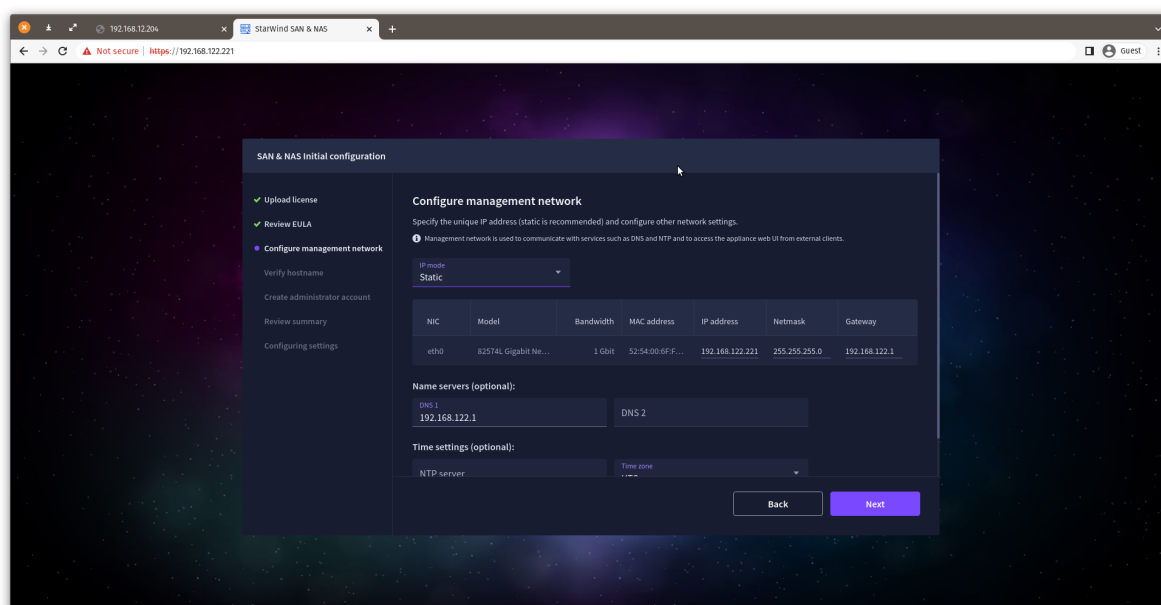
5. In the following step, upload the license file.



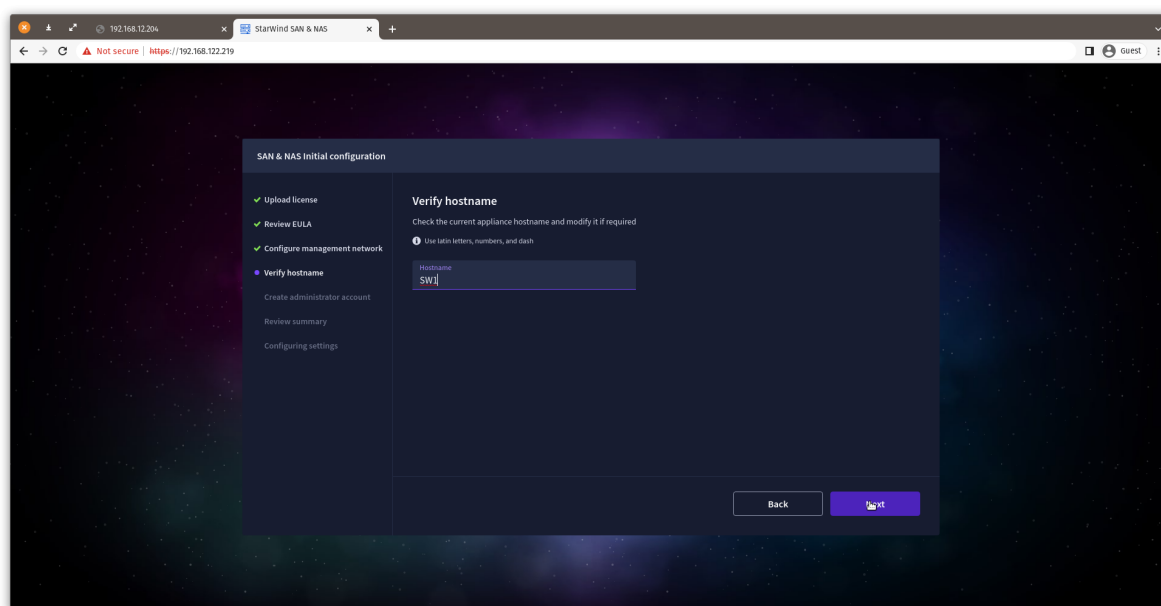
6. Read and accept the End User License Agreement to proceed.



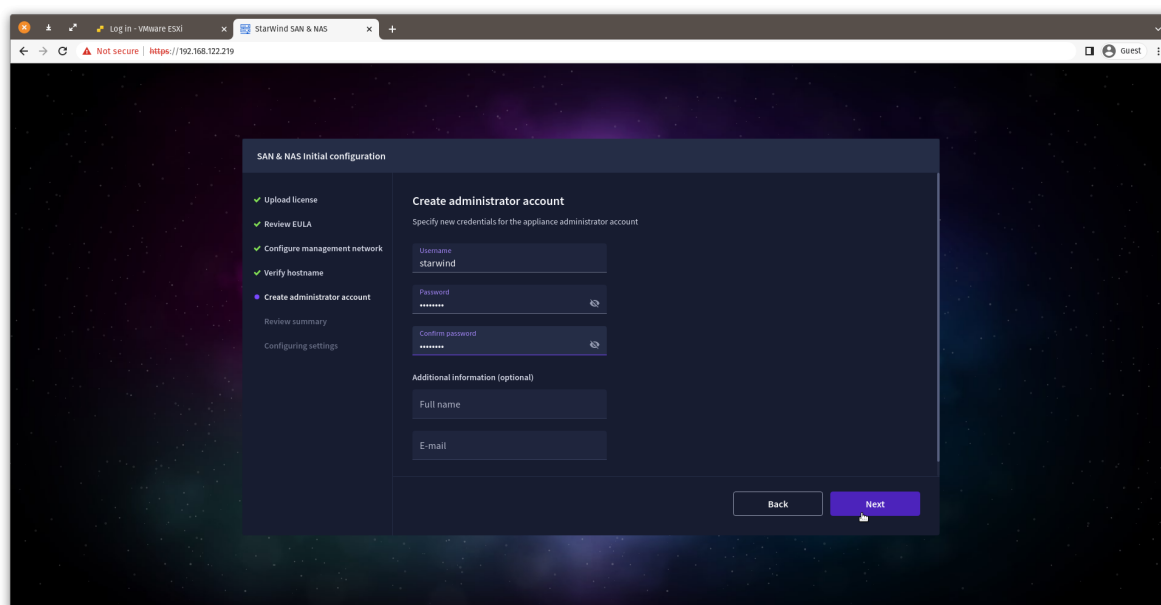
7. Review or edit the Network settings and click Next.
Note: Static network settings are recommended for the configuration.



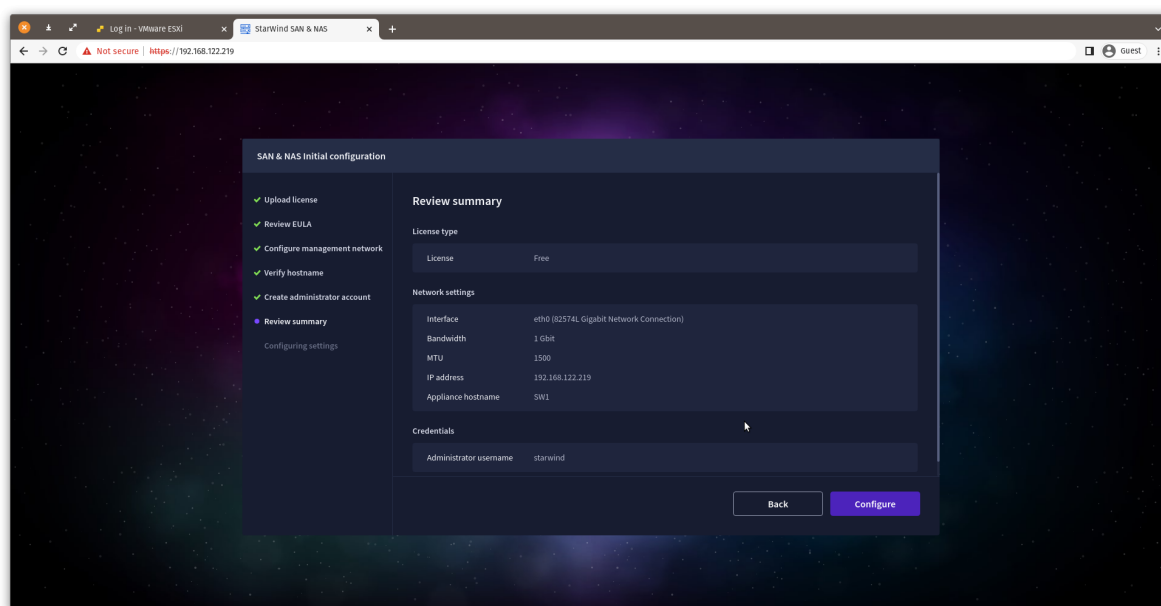
8. Specify the hostname for the virtual machine and click Next.



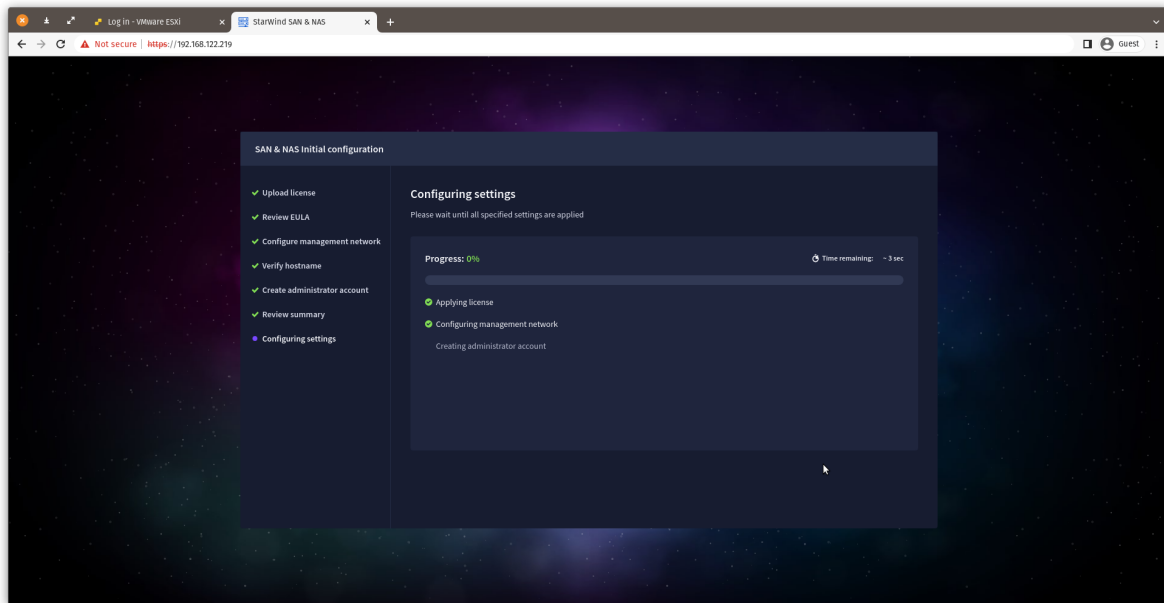
9. Create an administrator account. Click Next.



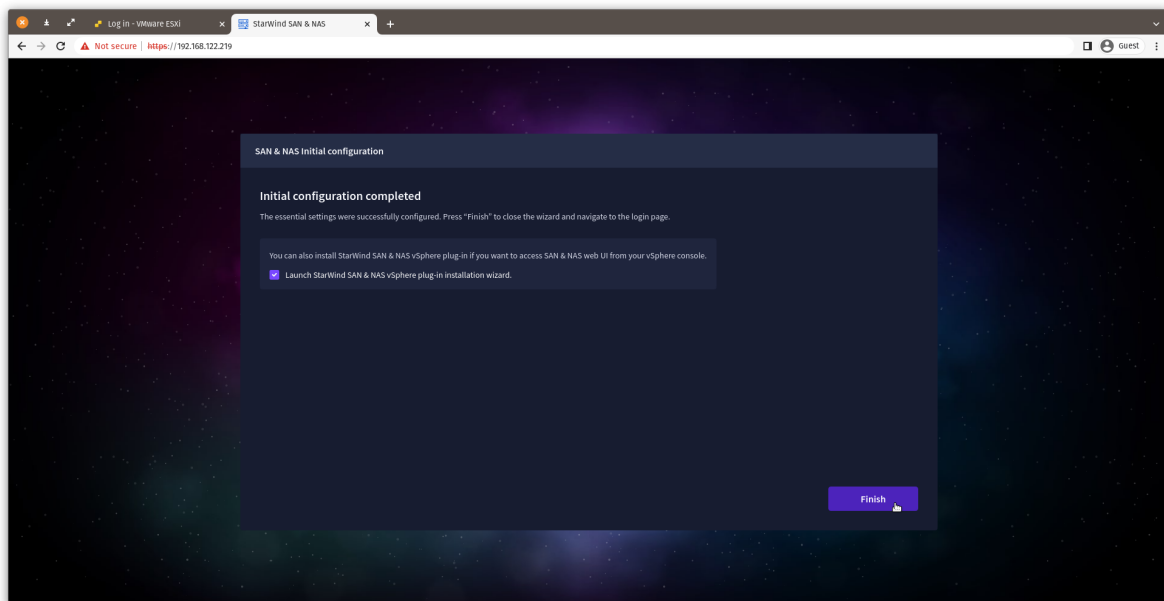
10. Review your settings selection before setting up StarWind SAN & NAS.



11. Please standby until the Initial Configuration Wizard configures StarWind SAN & NAS for you.



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

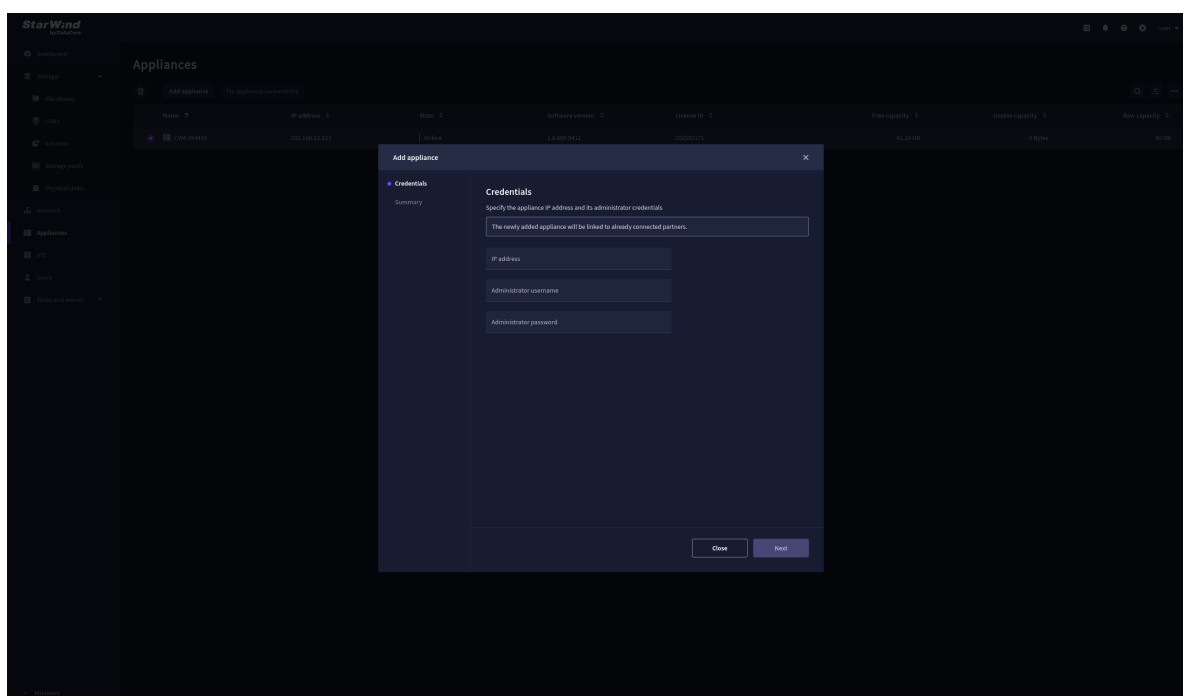


13. Repeat the initial configuration on other StarWind SAN & NAS CVMs that will be used to create 2-node or 3-node HA shared storage.

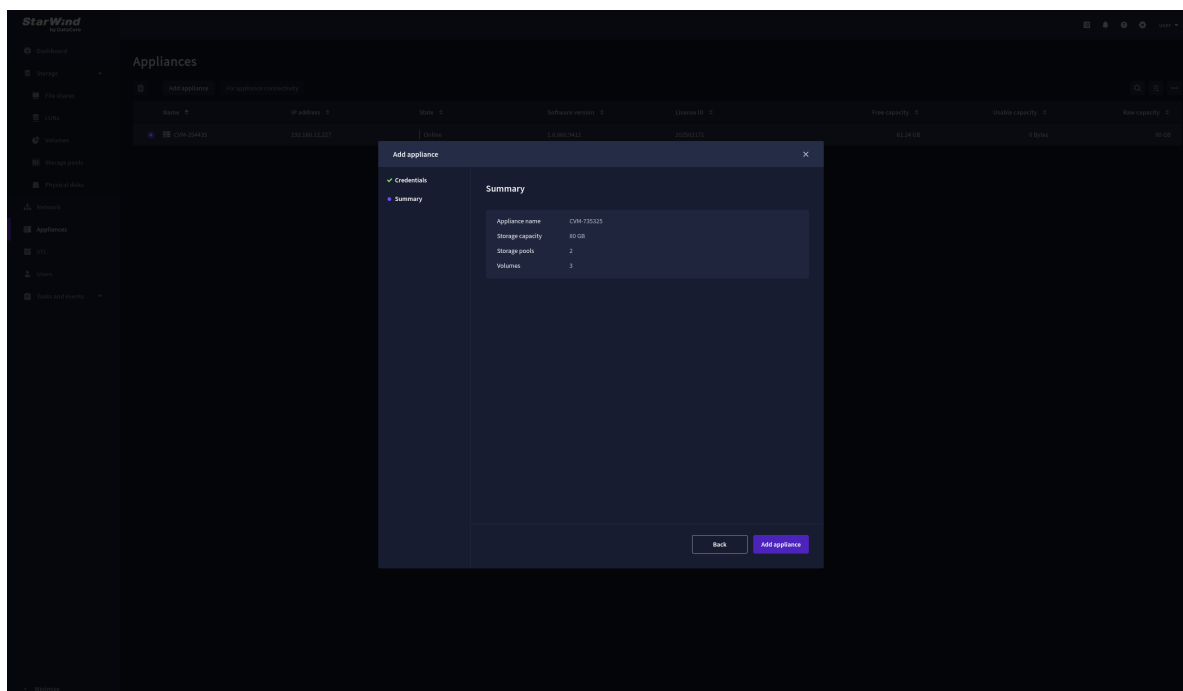
Add Appliance

To create replicated, highly available storage, add partner appliances that use the same StarWind Virtual SAN license key.

1. Navigate to the Appliances page and click Add to open the Add appliance wizard.
2. On the Credentials step, enter the IP address and credentials for the partner StarWind Virtual SAN appliance, then click Next.



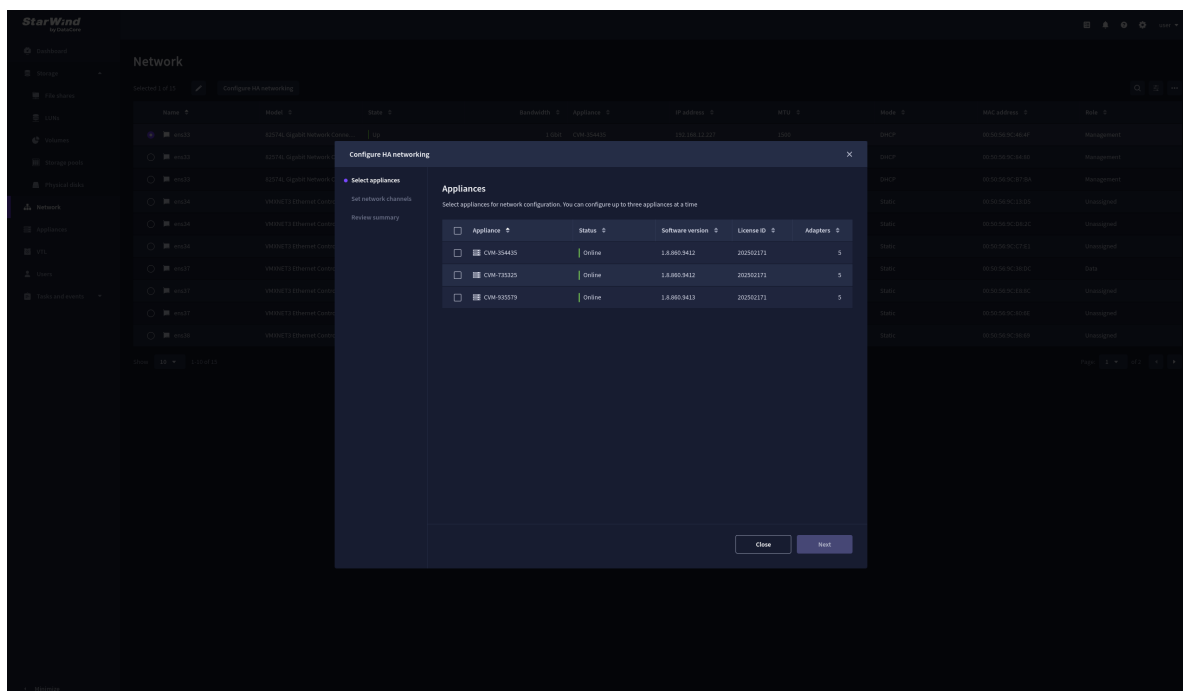
3. Wait for the connection to be established and the settings to be validated
4. On the Summary step, review the properties of the partner appliance, then click Add Appliance.



Configure Ha Networking

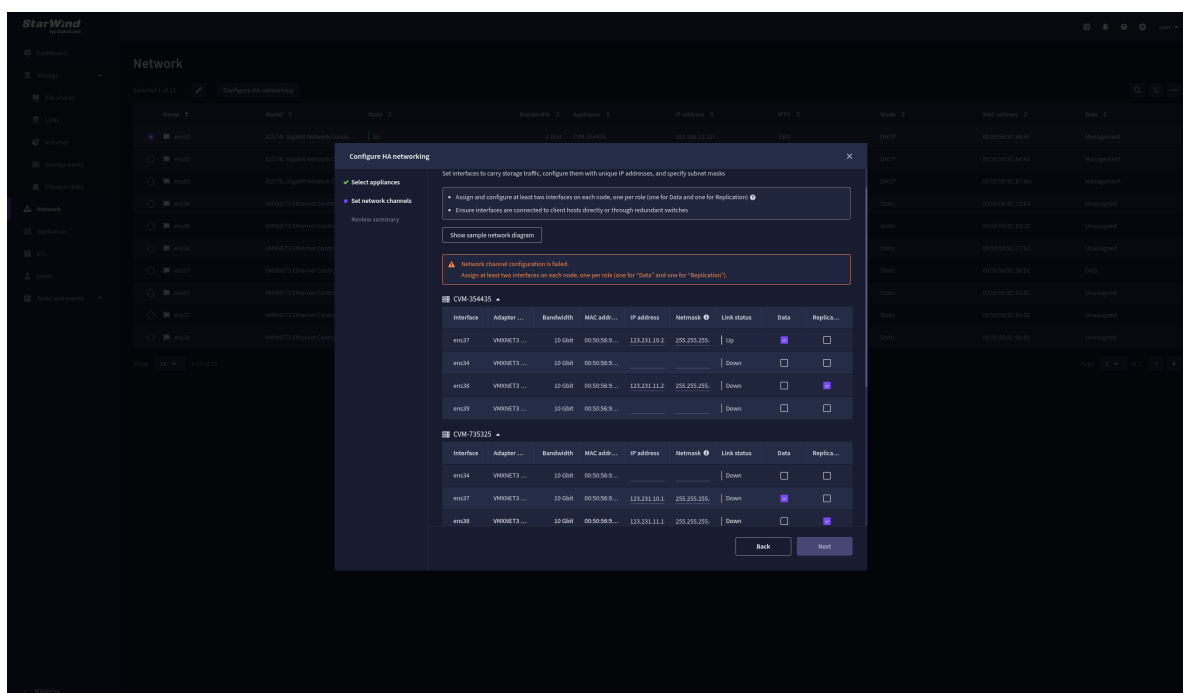
1. Navigate to the Network page and open the Configure HA networking wizard.
2. On the Appliances step, select either 2 partner appliances to configure two-way replication or 3 appliances for three-way replication, then click Next.

NOTE: The number of appliances in the cluster is limited by your StarWind Virtual SAN license.



3. Set Network Channels step combines configuration of Data and Replication Networks. Select the network interfaces designated to carry iSCSI or NVMe-oF storage traffic. Assign and configure at least one interface on each appliance with a static IP address in a unique network (subnet), specify the subnet mask and Cluster MTU size.

4. Select the network interfaces designated to carry the traffic for synchronous replication. Assign and configure at least one interface on each appliance with a static IP address in a unique network (subnet), specify the subnet mask and Cluster MTU size.

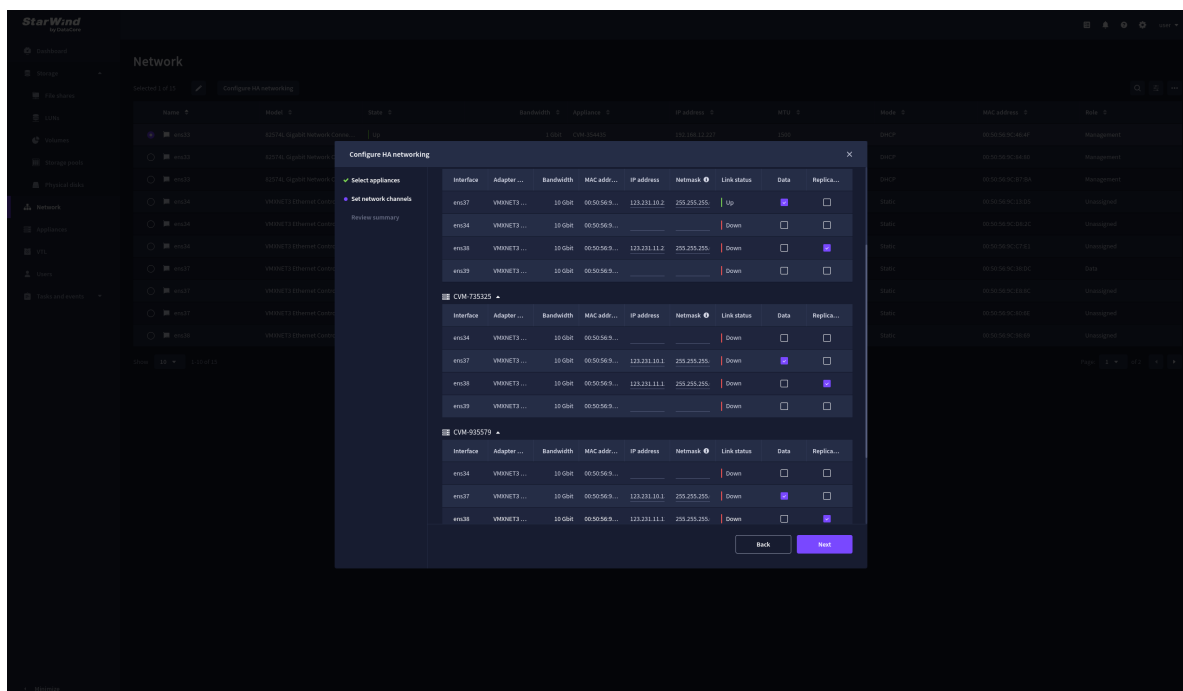


IMPORTANT: For a redundant, high-availability configuration, configure at least 2 network interfaces on each appliance. Ensure that the Data Network interfaces are interconnected between appliances through multiple direct links or via redundant switches.

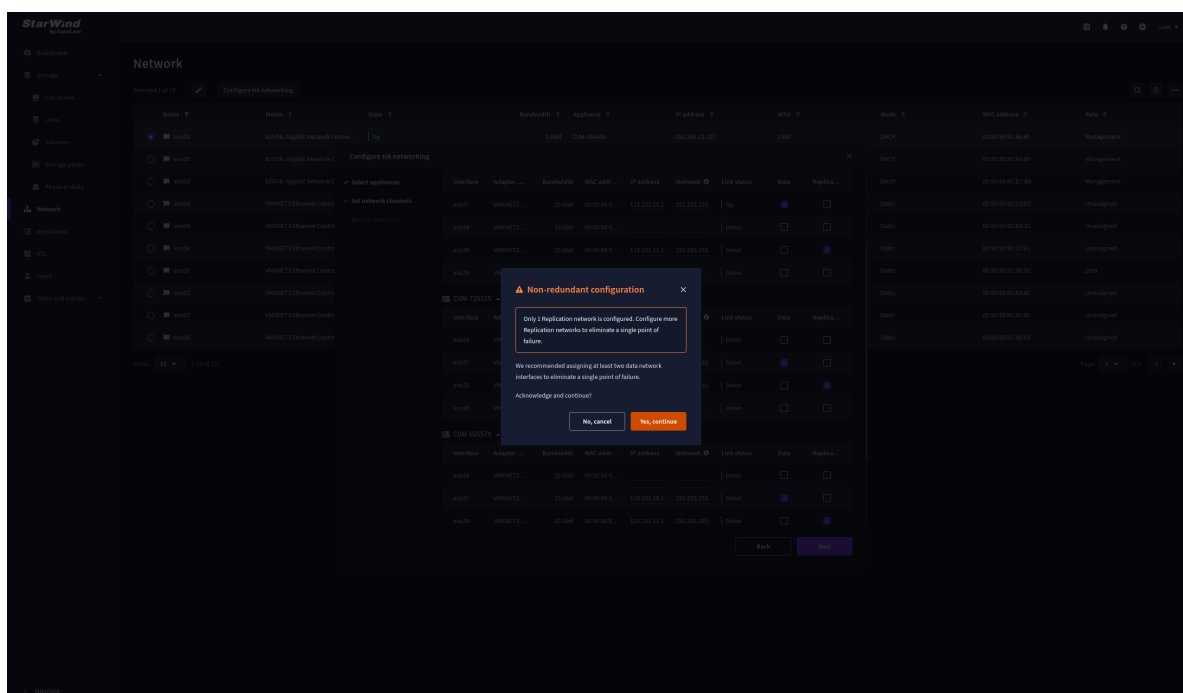
5. Assign an MTU value on all selected network adapters, e.g., 1500 or 9000 bytes. If you are using network switches with the selected Data Network adapters, ensure that they are configured with the same MTU size value. In case of an MTU settings mismatch, stability and performance issues might occur on the whole setup.

NOTE: Setting MTU to 9000 bytes on some physical adapters (like Intel Ethernet Network Adapter X710, Broadcom network adapters, etc.) might cause stability and performance issues depending on the installed network driver. To avoid them, use 1500 bytes MTU size or install the stable version of the driver.

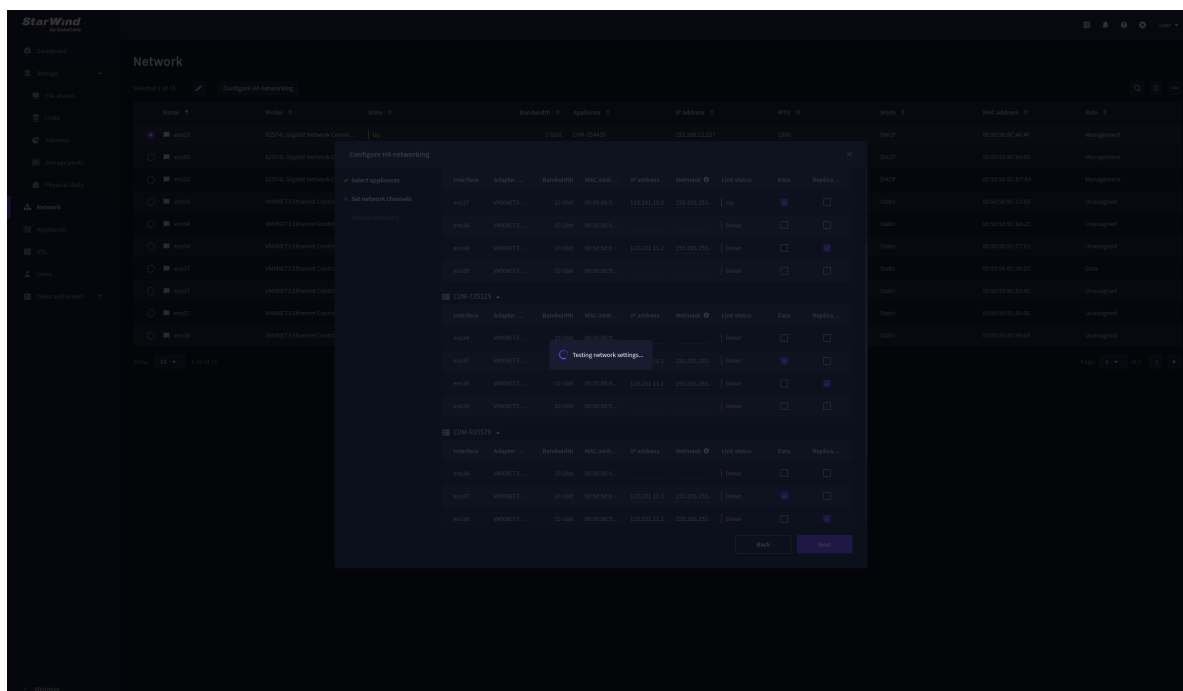
6. Once configured, click Next to validate network settings.



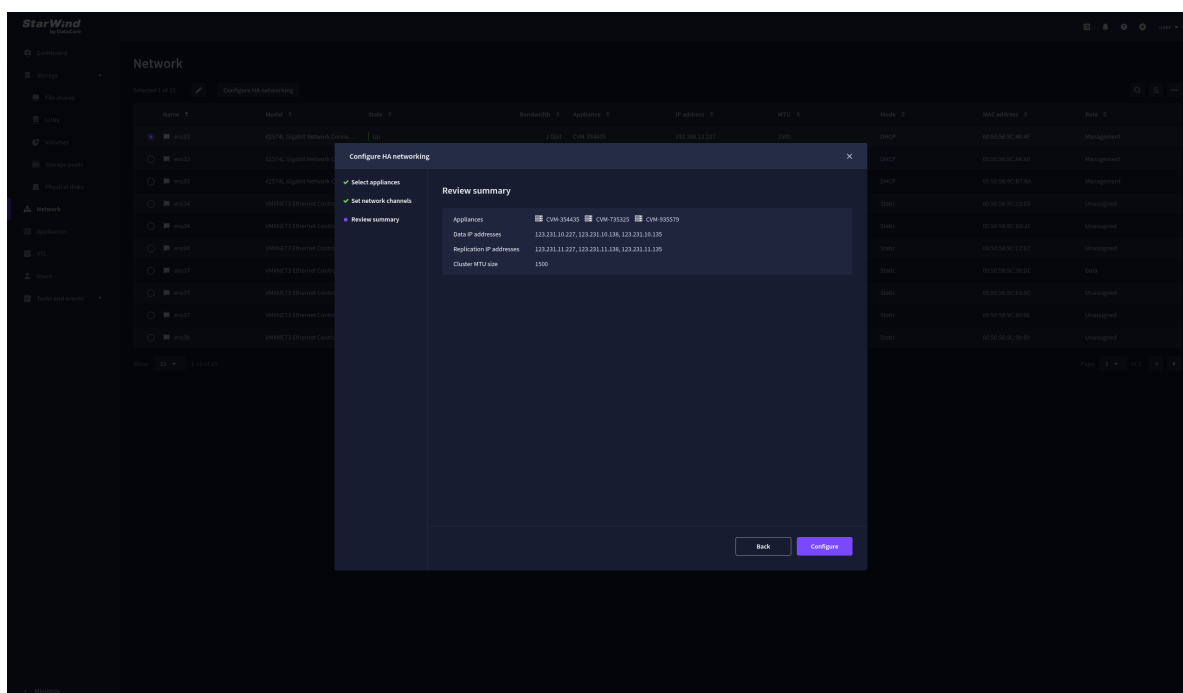
7. The warning might appear if a single data interface is configured. Click Yes, continue to proceed with the configuration.



8. Wait for the configuration to complete.



9. On the Summary step, review the specified network settings and click Configure to apply the changes.



Add Physical Disks

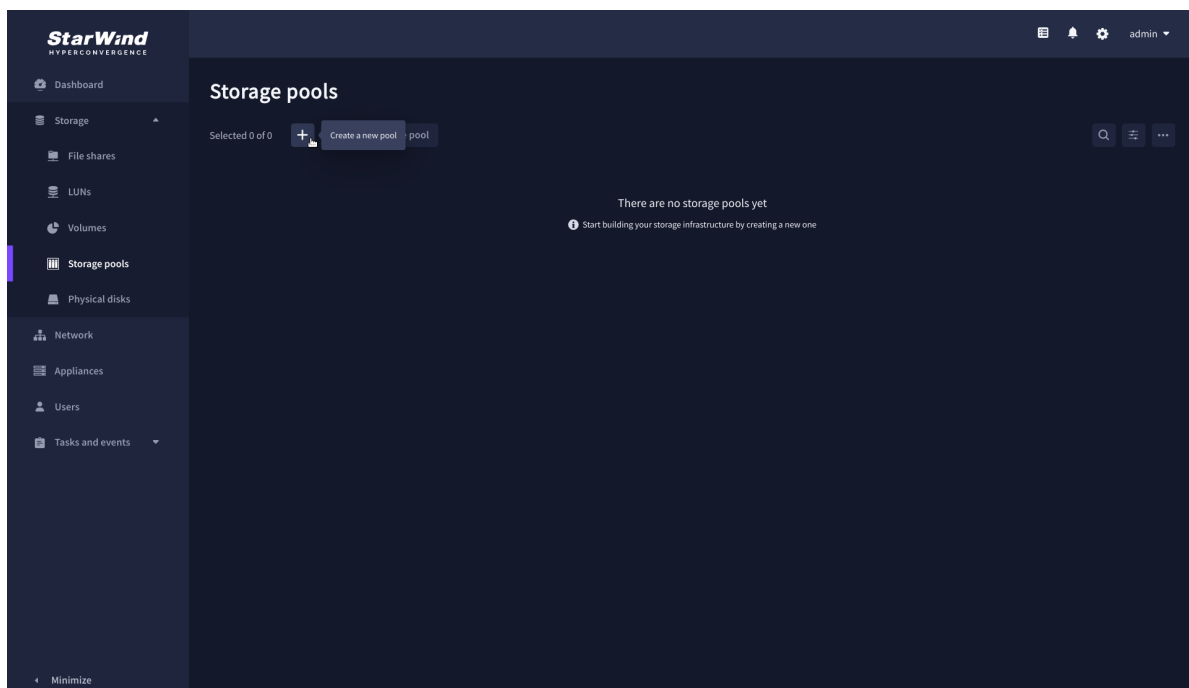
Attach physical storage to StarWind Virtual SAN Controller VM:

- Ensure that all physical drives are connected through an HBA or RAID controller.
- To get optimal storage performance, add HBA, RAID controllers, or NVMe SSD drives to StarWind CVM via a passthrough device.

For detailed instructions, refer to [Microsoft's documentation on DDA](#). Also, find the storage provisioning guidelines in the [KB article](#).

Create Storage Pool

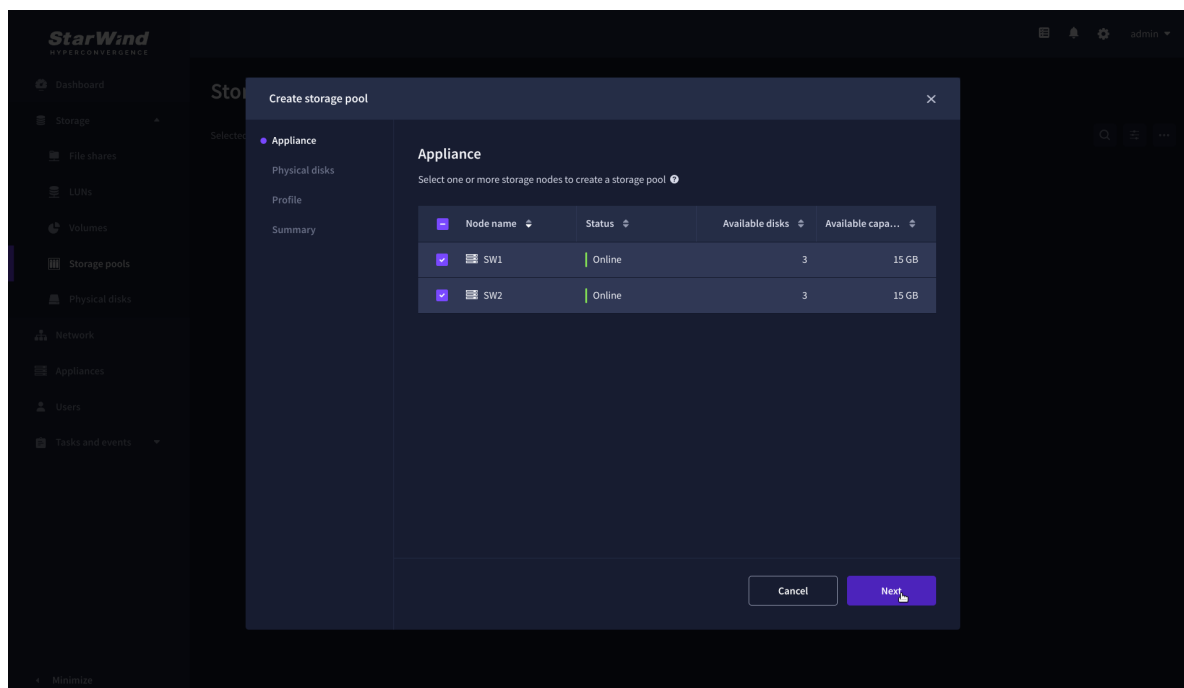
1. Navigate to the Storage pools page and click the + button to open the Create storage pool wizard .



2. On the Appliance step, select partner appliances on which to create new storage pools, then click Next.

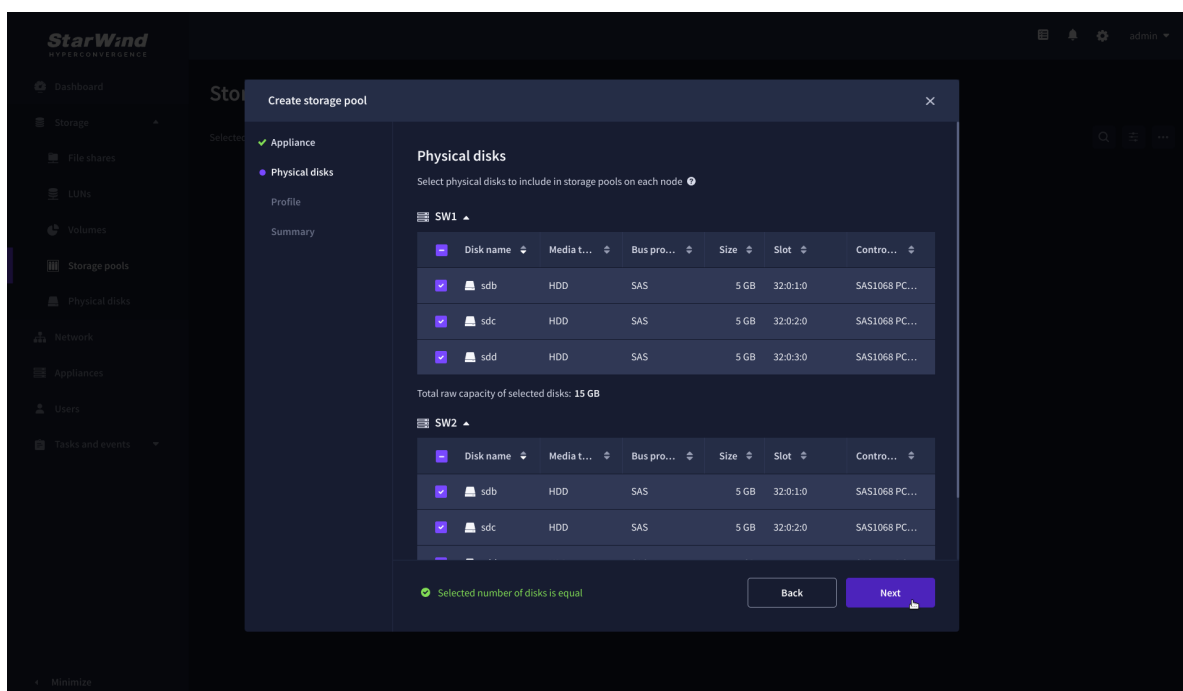
NOTE: Select 2 appliances for configuring storage pools if you are deploying a two-node cluster with two-way replication, or select 3 appliances for configuring a three-node

cluster with a three-way mirror.

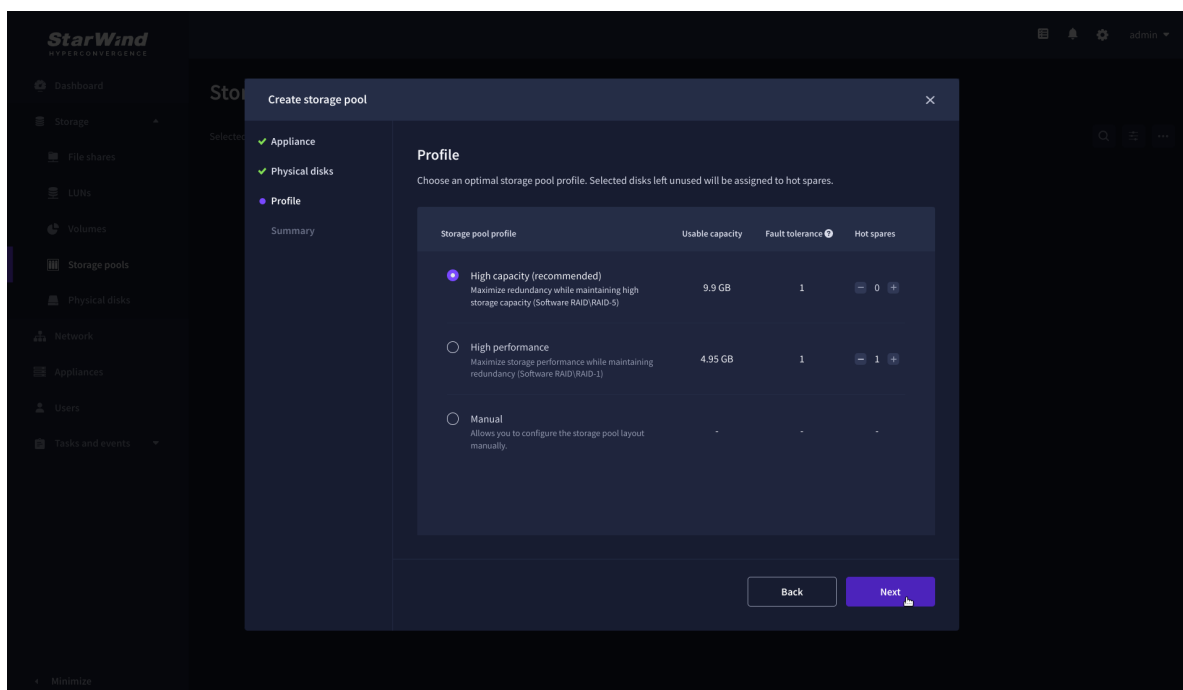


3. On the Physical disks step, select physical disks to be pooled on each node, then click Next.

IMPORTANT: Select an identical type and number of disks on each appliance to create storage pools with a uniform configuration.



4. On the Profile step, select one of the preconfigured storage profiles, or choose Manual to configure the storage pool manually based on your redundancy, capacity, and performance requirements, then click Next.

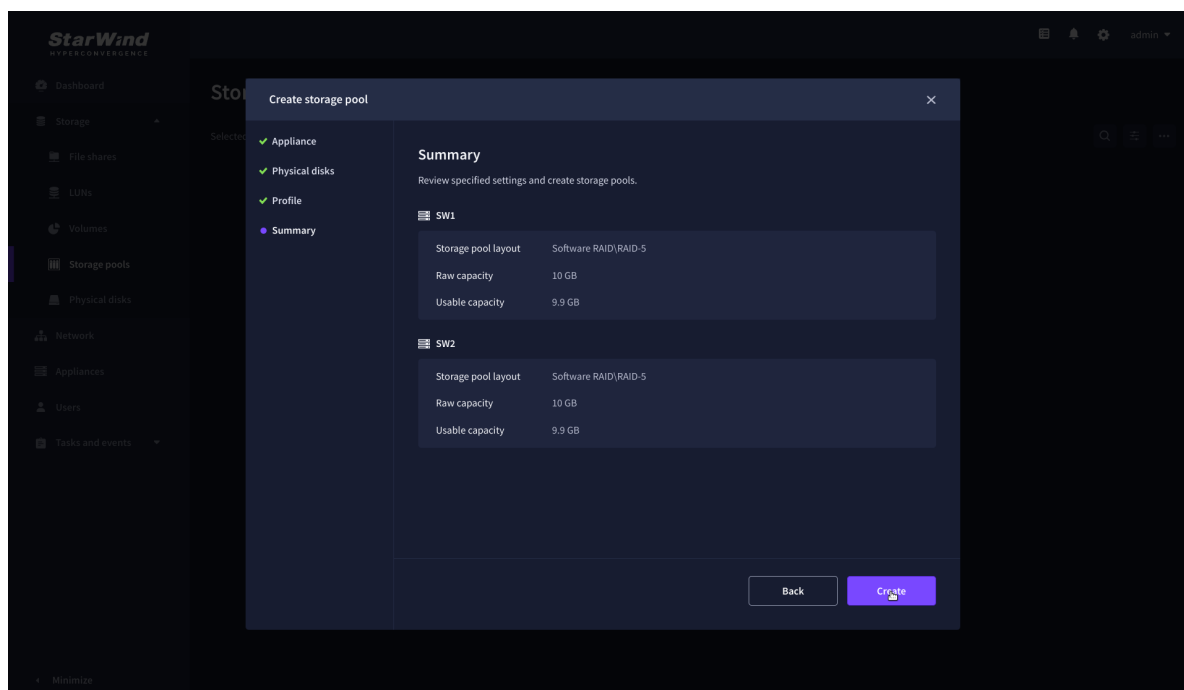


NOTE: Hardware RAID, Linux Software RAID, and ZFS storage pools are supported. To

simplify the configuration of storage pools, preconfigured storage profiles are provided. These profiles recommend a pool type and layout based on the attached storage:

- High capacity – creates Linux Software RAID-5 to maximize storage capacity while maintaining redundancy.
- High performance – creates Linux Software RAID-10 to maximize storage performance while maintaining redundancy.
- Hardware RAID – configures a hardware RAID virtual disk as a storage pool. This option is available only if a hardware RAID controller is passed through to the StarWind Virtual SAN.
- Better redundancy – creates ZFS Striped RAID-Z2 (RAID 60) to maximize redundancy while maintaining high storage capacity.
- Manual – allows users to configure any storage pool type and layout with the attached storage.

5. On the Summary step, review the storage pool settings and click Create to configure new storage pools on the selected appliances.



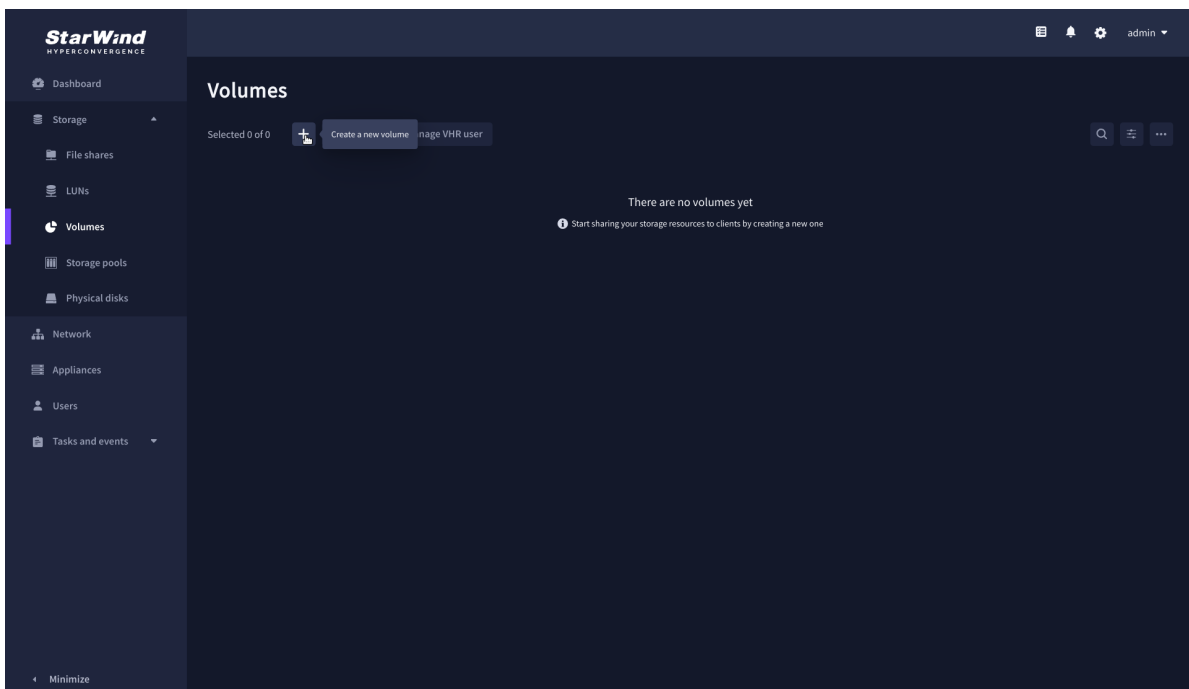
NOTE: The storage pool configuration may take some time, depending on the type of pooled storage and the total storage capacity. Once the pools are created, a notification will appear in the upper right corner of the Web UI.

IMPORTANT for CVM only: In some cases, additional tweaks are required to optimize the storage performance of the disks added to the Controller Virtual Machine. Please follow the steps in this KB to change the scheduler type depending on the disks type:
<https://knowledgebase.starwindsoftware.com/guidance/starwind-vsan-for-vsphere-changi>

[ng-linux-i-o-scheduler-to-optimize-storage-performance/](#)

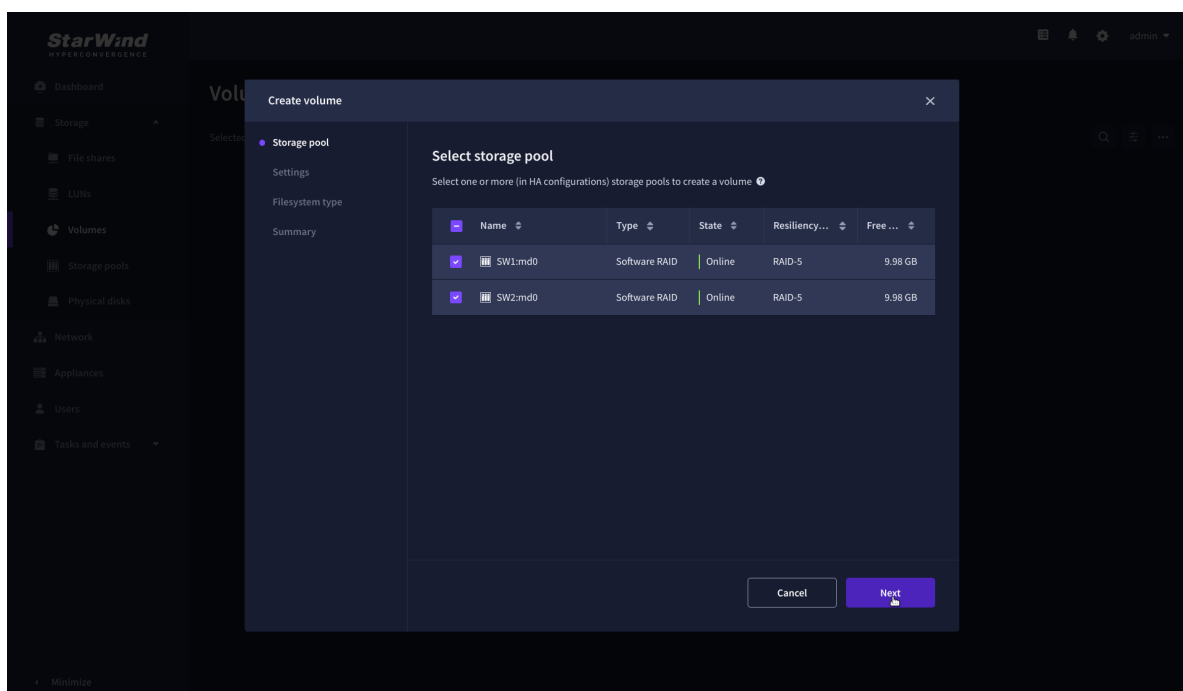
Create Volume

1. Navigate to the Volumes page and click the + button to open the Create volume wizard.

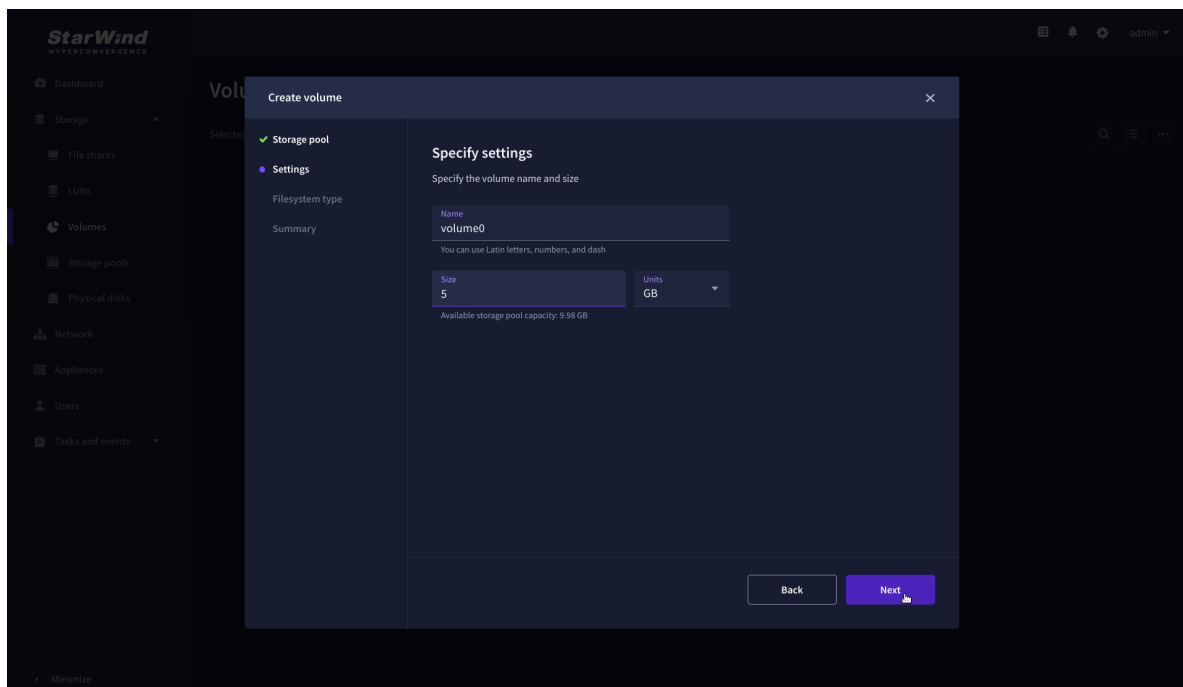


2. On the Storage pool step, select partner appliances on which to create new volumes, then click Next.

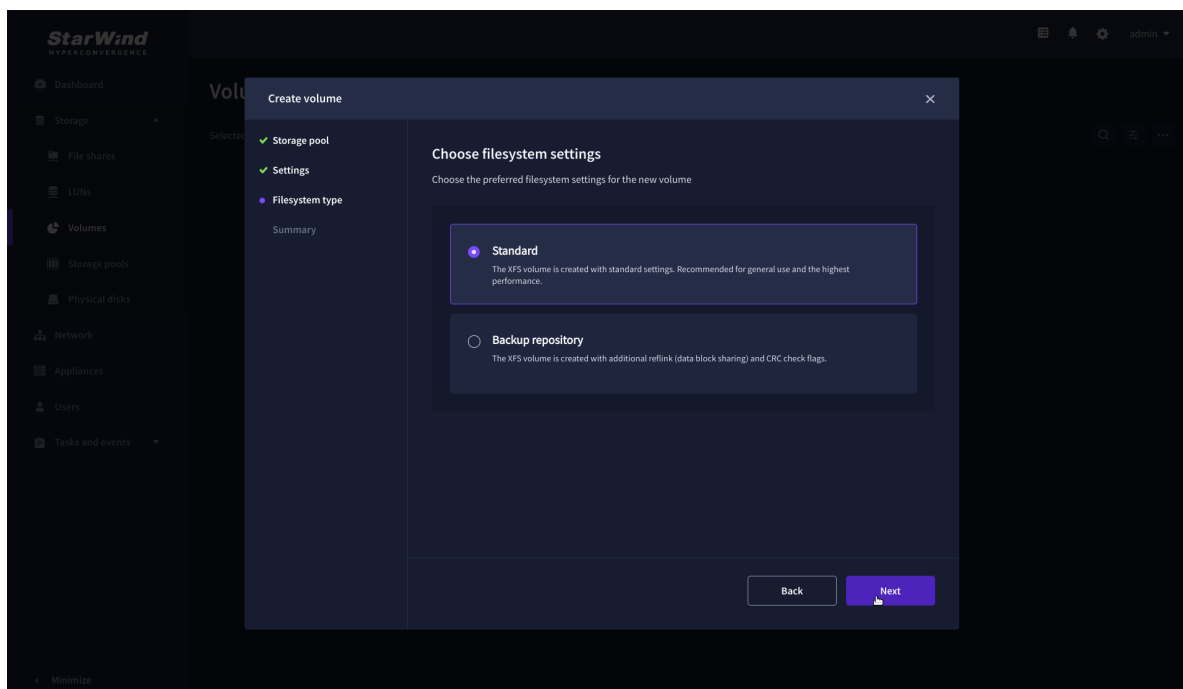
NOTE: Select 2 appliances for configuring volumes if you are deploying a two-node cluster with two-way replication, or select 3 appliances for configuring a three-node cluster with a three-way mirror.



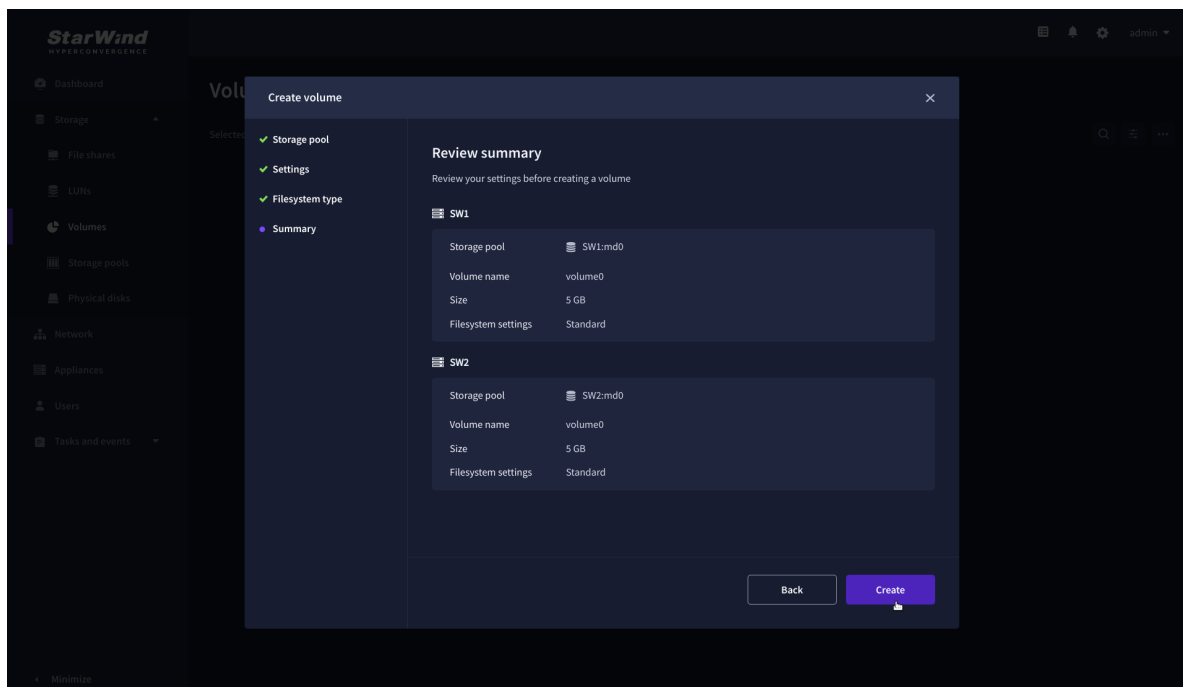
3. On the Settings step, specify the volume name and size, then click Next.



4. On the Filesystem type step, select Standard, then click Next.



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

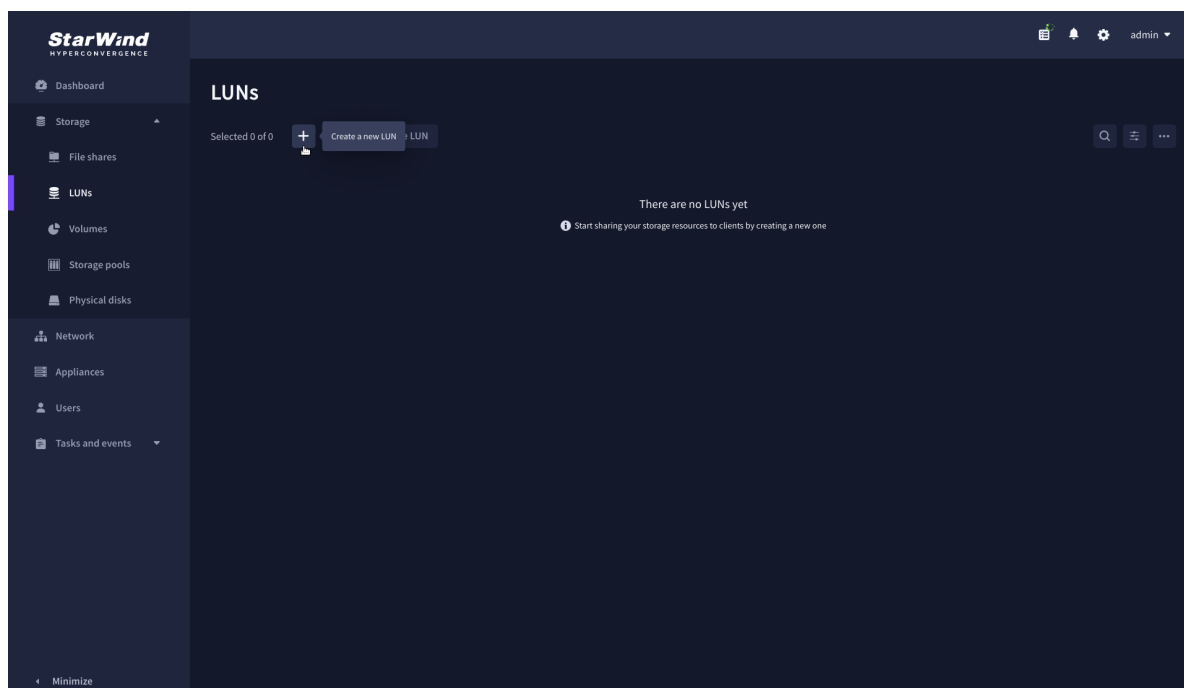


Create Ha Lun Using Webui

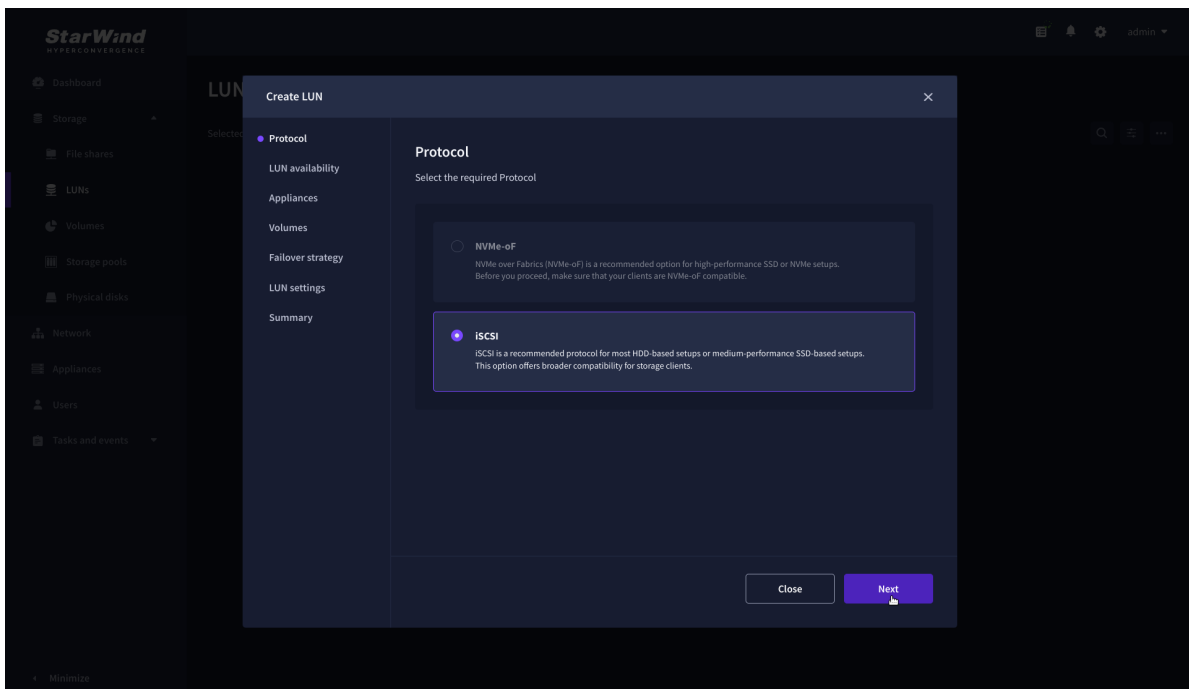
This section describes how to create LUN in Web UI. This option is available for the setups with Commercial, Trial, and NFR licenses applied.

For setups with a Free license applied, the PowerShell script should be used to create the LUN – please follow the steps described in the section: Create StarWind HA LUNs using PowerShell

1. Navigate to the LUNs page and click the + button to open the Create LUN wizard.



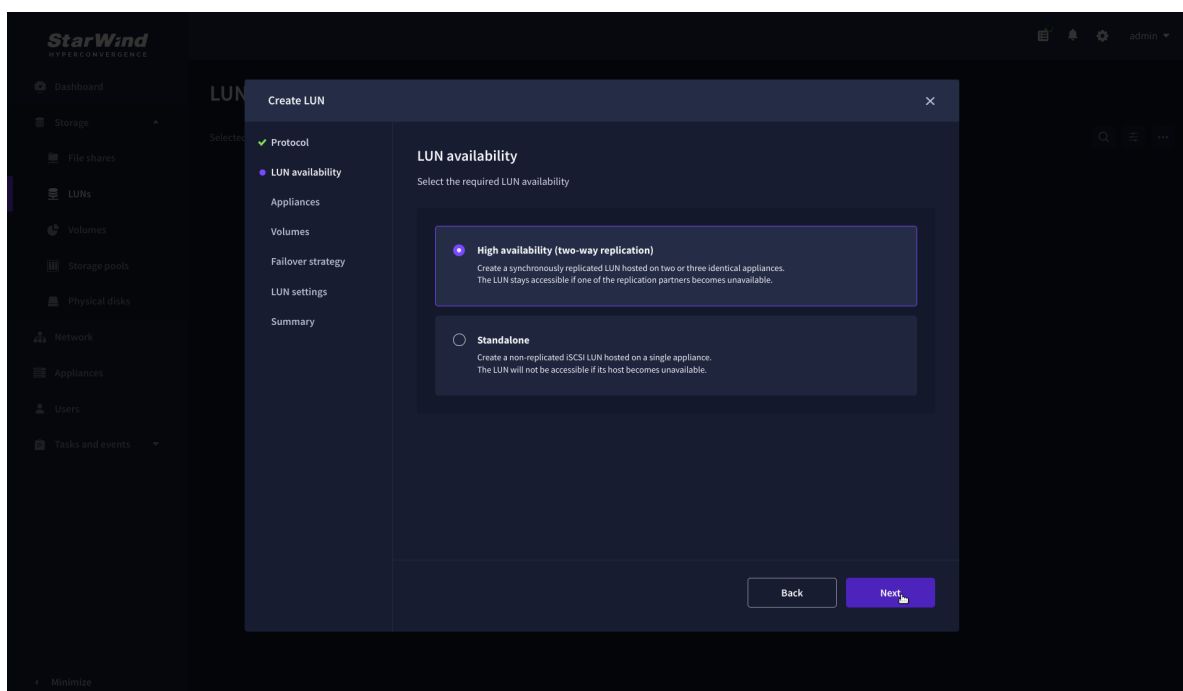
2. On the Protocols step, select the preferred storage protocol and click Next.



3. On the LUN availability step, select the High availability and click Next.

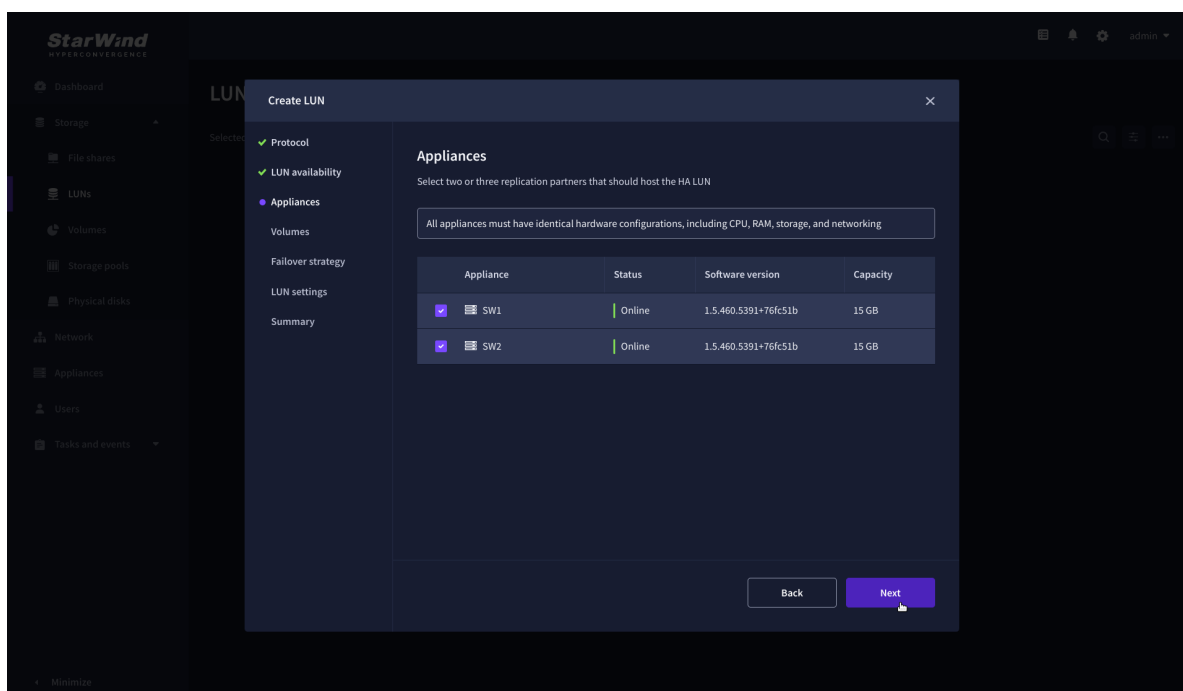
NOTE: The availability options for a LUN can be Standalone (without replication) or High Availability (with 2-way or 3-way replication), and are determined by the StarWind Virtual SAN license.

Below are the steps for creating a high-availability iSCSI LUN.



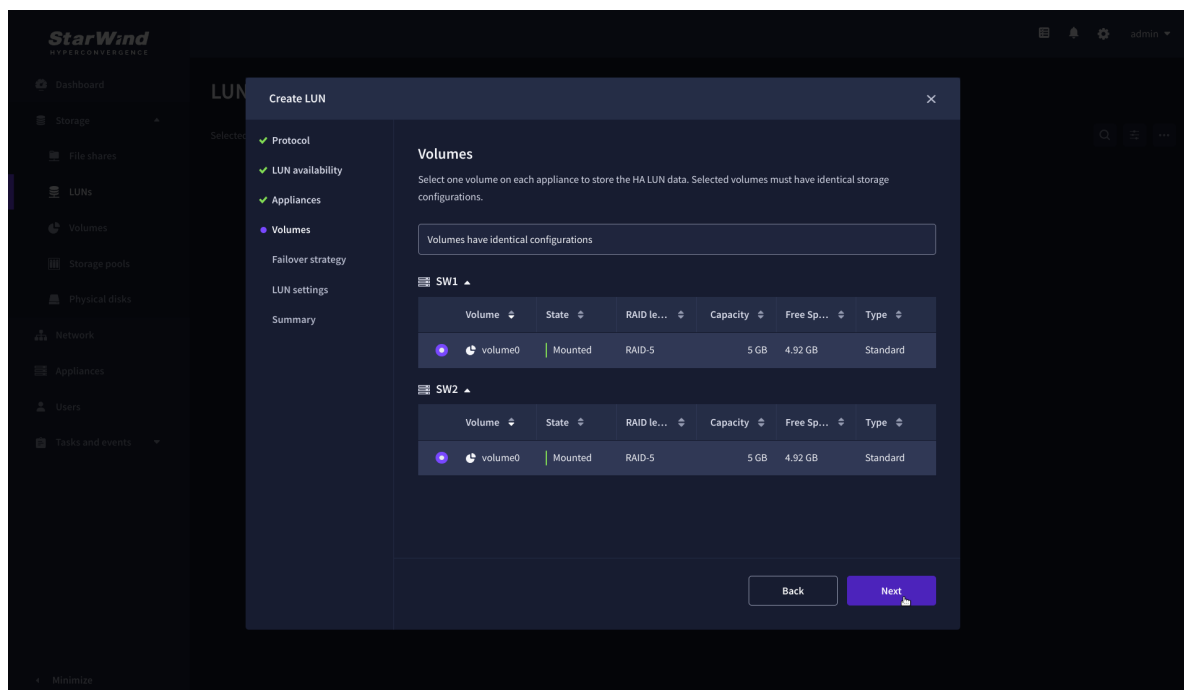
4. On the Appliances step, select partner appliances that will host new LUNs and click Next.

IMPORTANT: Selected partner appliances must have identical hardware configurations, including CPU, RAM, storage, and networking.



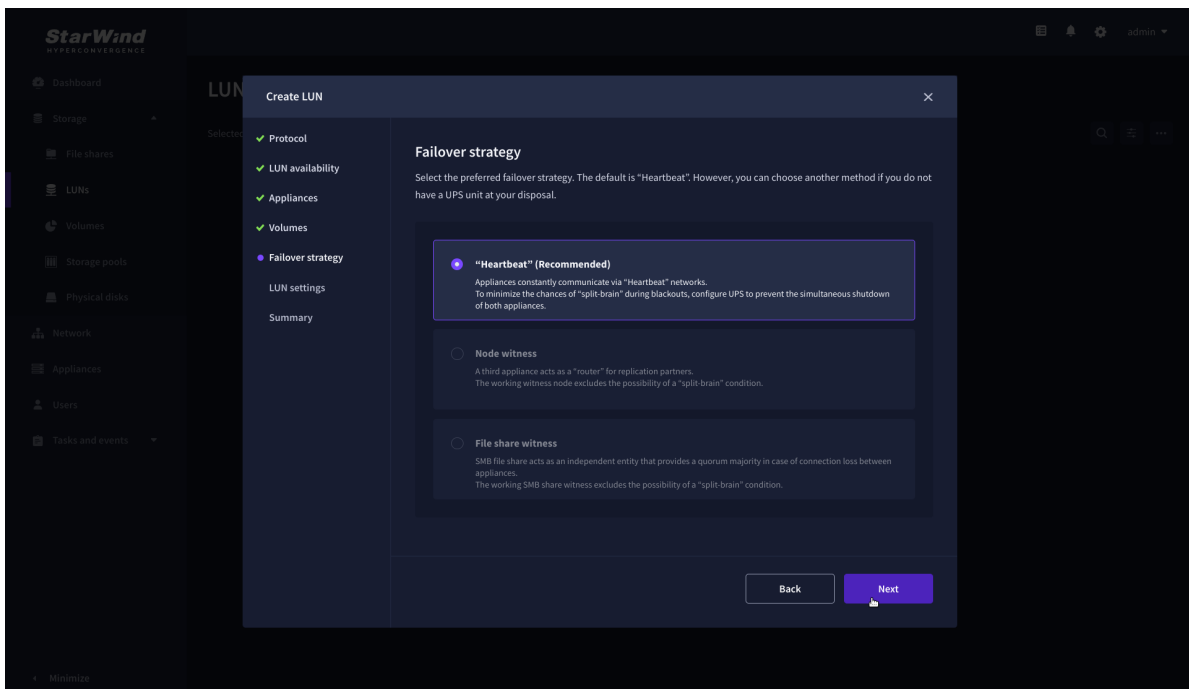
5. On the Volumes step, select the volumes for storing data on the partner appliances and click Next.

IMPORTANT: For optimal performance, the selected volumes must have identical underlying storage configurations.



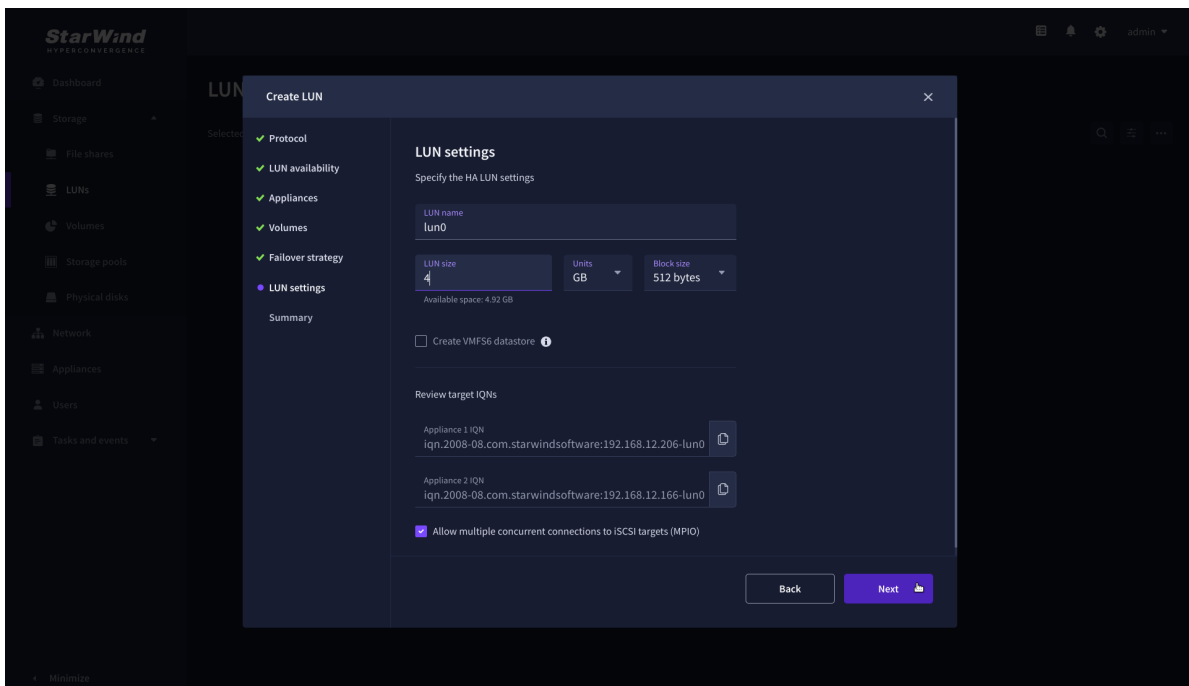
6. On the Failover strategy step, select the preferred failover strategy and click Next.

NOTE: The failover strategies for a LUN can be Heartbeat or Node Majority. In case of 2-nodes setup and None Majority failover strategy, Node witness (requires an additional third witness node), or File share witness (requires an external file share) should be configured. These options are determined by StarWind Virtual SAN license and setup configuration. Below are the steps for configuring the Heartbeat failover strategy in a two-node cluster.

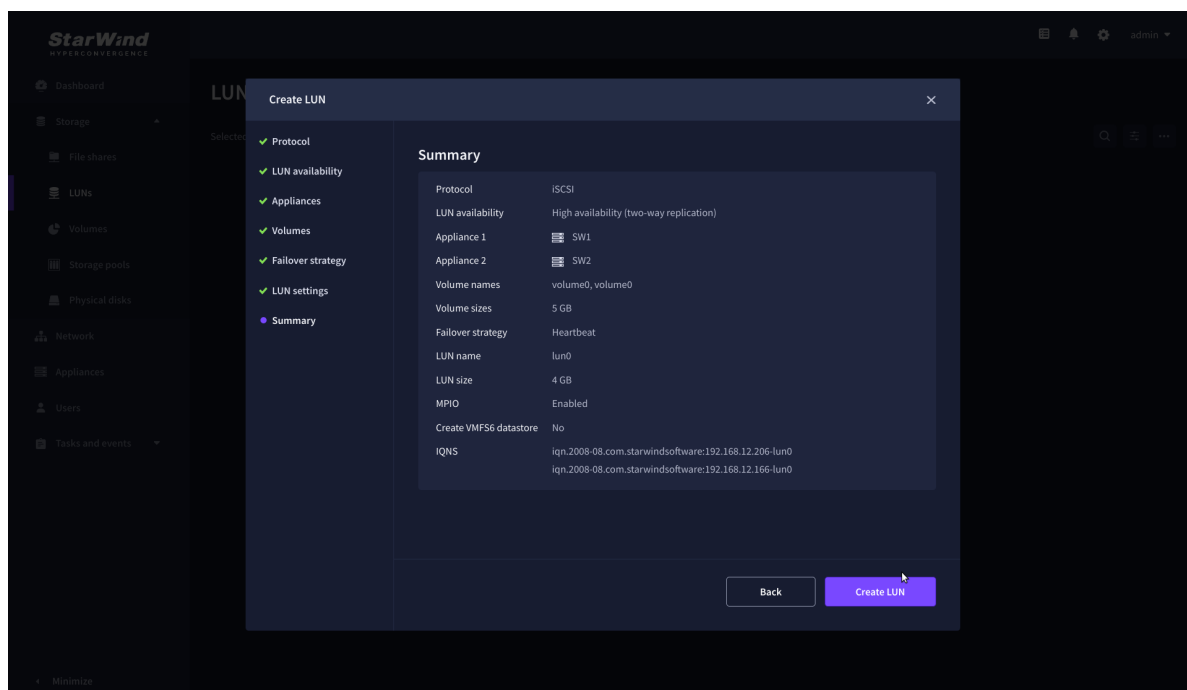


7. On the LUN settings step, specify the LUN name, size, block size, then click Next.

NOTE: For high-availability configurations, ensure that MPIO checkbox is selected.



8. On the Summary step, review the LUN settings and click Create to configure new LUNs on the selected volumes.



Connecting Starwind Virtual Disk To Hyper-V Servers

Enabling Multipath Support on Hyper-V Servers

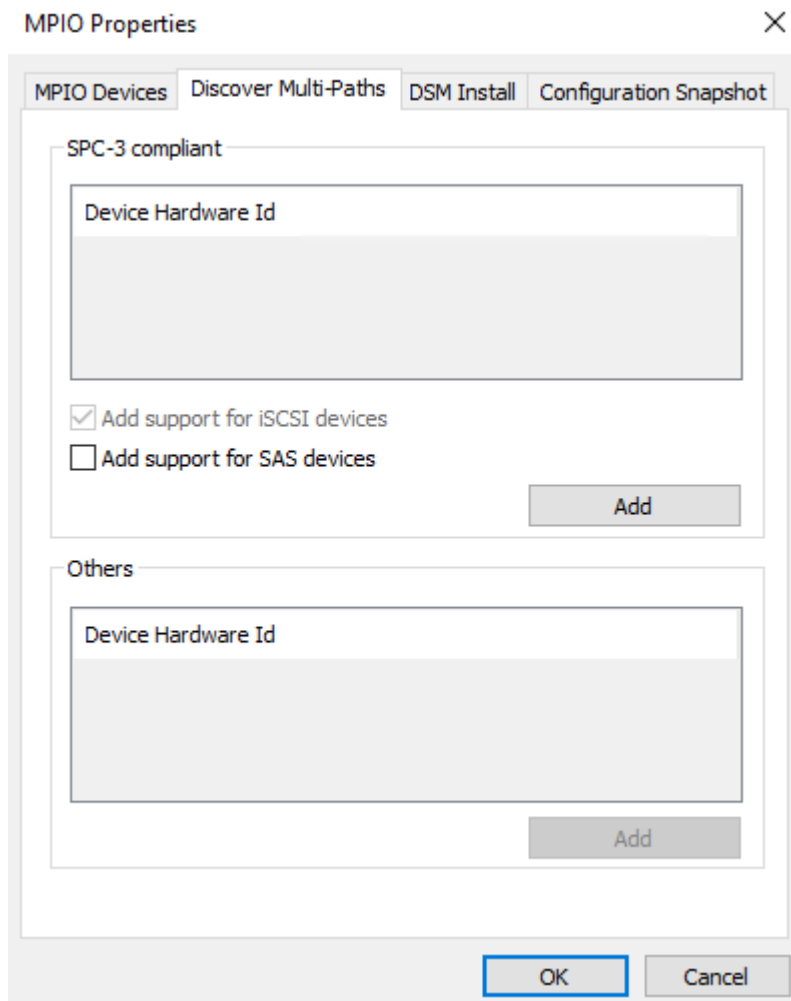
1. Install the Multipath I/O feature by executing the following command in the PowerShell window:

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

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

```
mpioctl
```

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



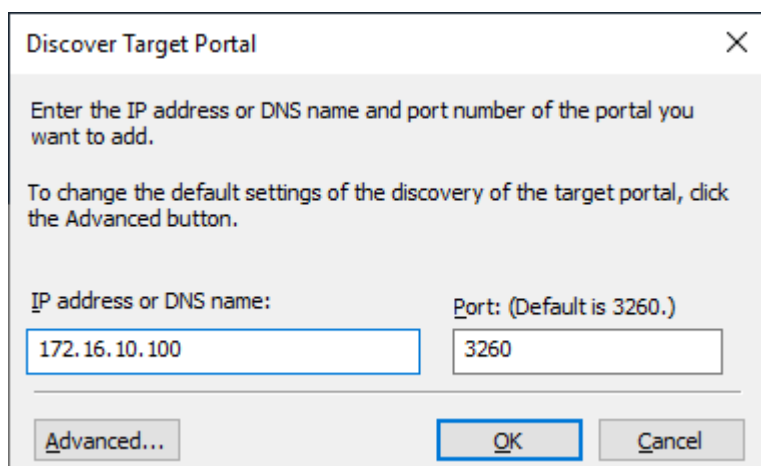
4. When prompted to restart the server, click Yes to proceed.
5. Repeat the same procedure on the other compute server that will be connected to SAN & NAS appliance.

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

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

```
iscsicpl
```

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



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

Discover Target Portal

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

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

IP address or DNS name: 172.16.10.100

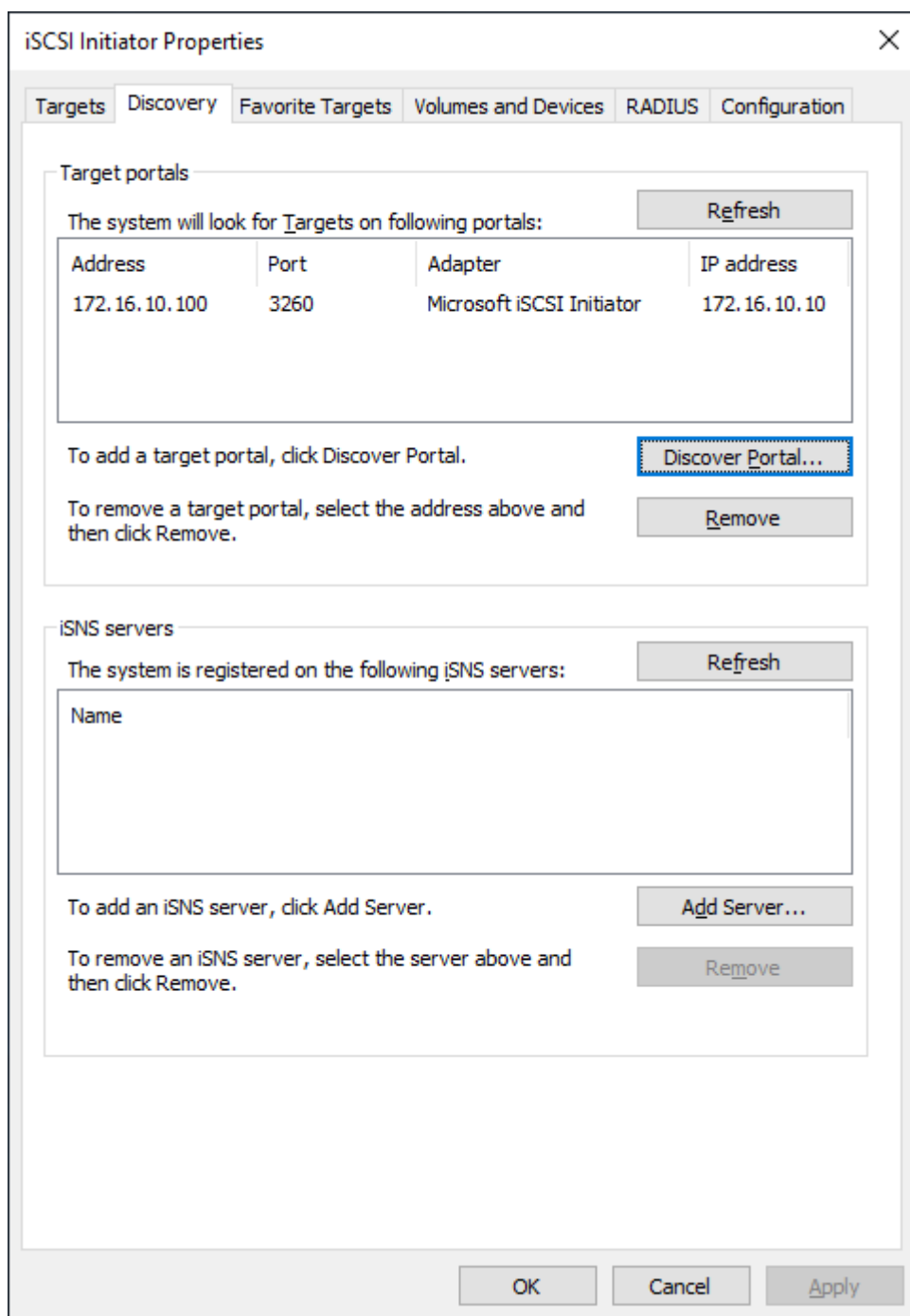
Port: (Default is 3260.) 3260

Advanced... OK Cancel

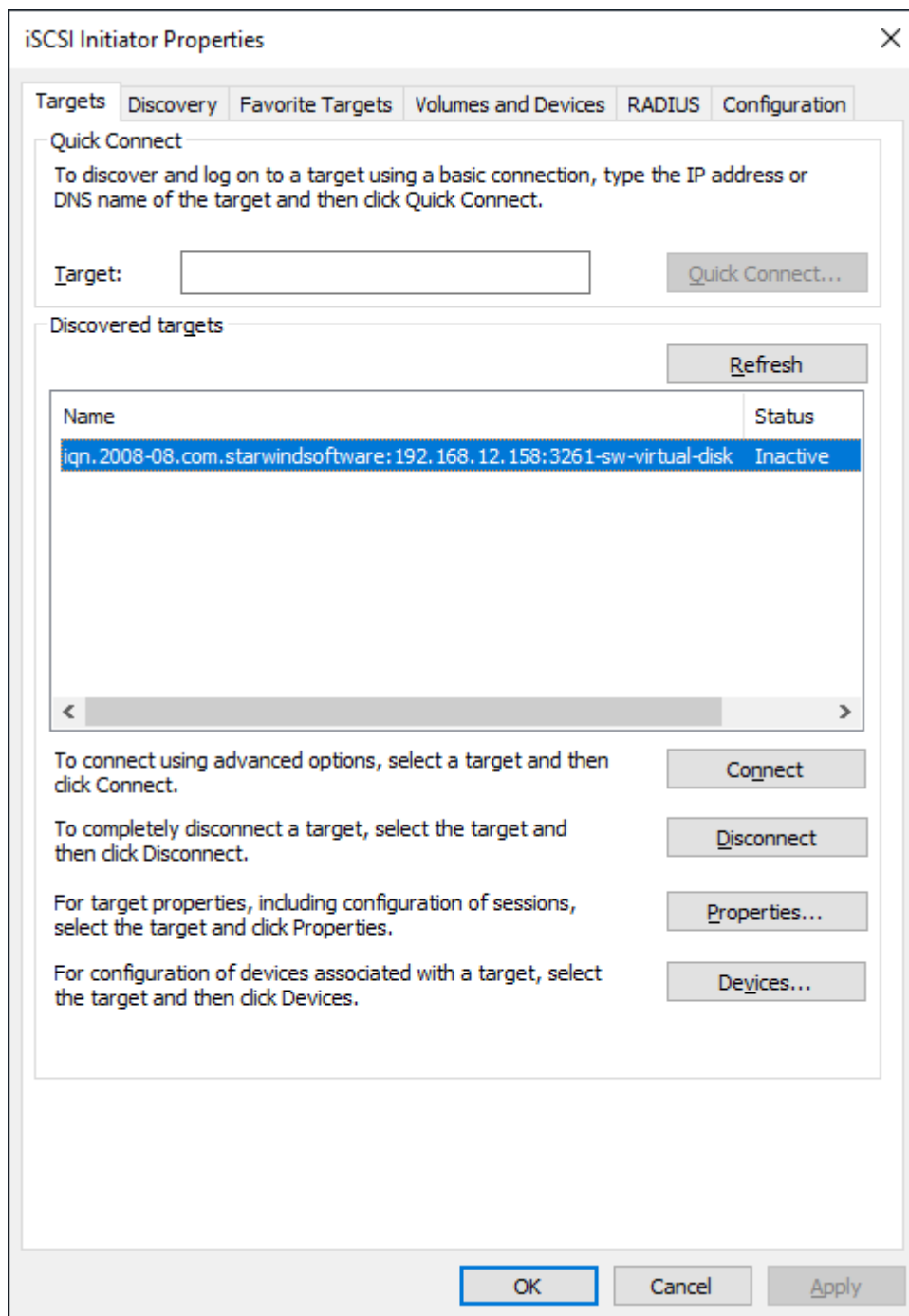
4. Click the Advanced button. Select Microsoft iSCSI Initiator as a Local adapter and as Initiator IP select the IP address of a network adapter connected to the Data\iSCSI virtual switch. Confirm the actions to complete the Target Portal discovery.

The screenshot shows the 'Advanced Settings' dialog box with the 'IPsec' tab selected. The 'Connect using' section has three dropdown menus: 'Local adapter' set to 'Microsoft iSCSI Initiator', 'Initiator IP' set to '172.16.10.10', and 'Target portal IP' which is empty. The 'CRC / Checksum' section has two unchecked checkboxes: 'Data digest' and 'Header digest'. The 'Enable CHAP log on' checkbox is also unchecked. Below this is the 'CHAP Log on information' section, which includes a text box for 'Name' containing 'iqn.1991-05.com.microsoft:ws2019' 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.

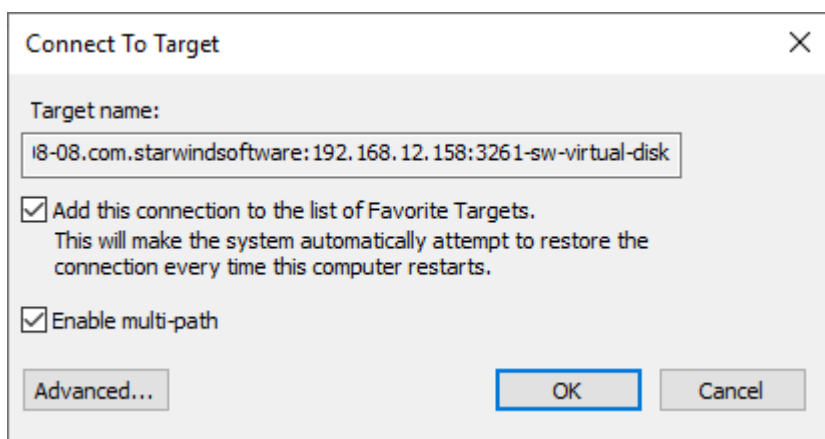
5. The target portals are added on this server.



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



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



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

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

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

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

Connecting Disks to Servers

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

1. Run diskpart in the CMD window:

List disk

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

Online disk

Clean

Attributes disk clear readonly

Convert GPT

Create Partition Primary

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

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

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

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

DISKPART> list disk

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

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

DISKPART> online disk
DiskPart successfully onlined the selected disk.

DISKPART> attributes disk clear readonly
Disk attributes cleared successfully.

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

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

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

DISKPART> _
```

2. Perform the steps above on other compute servers.

Creating A Failover Cluster In Windows Server

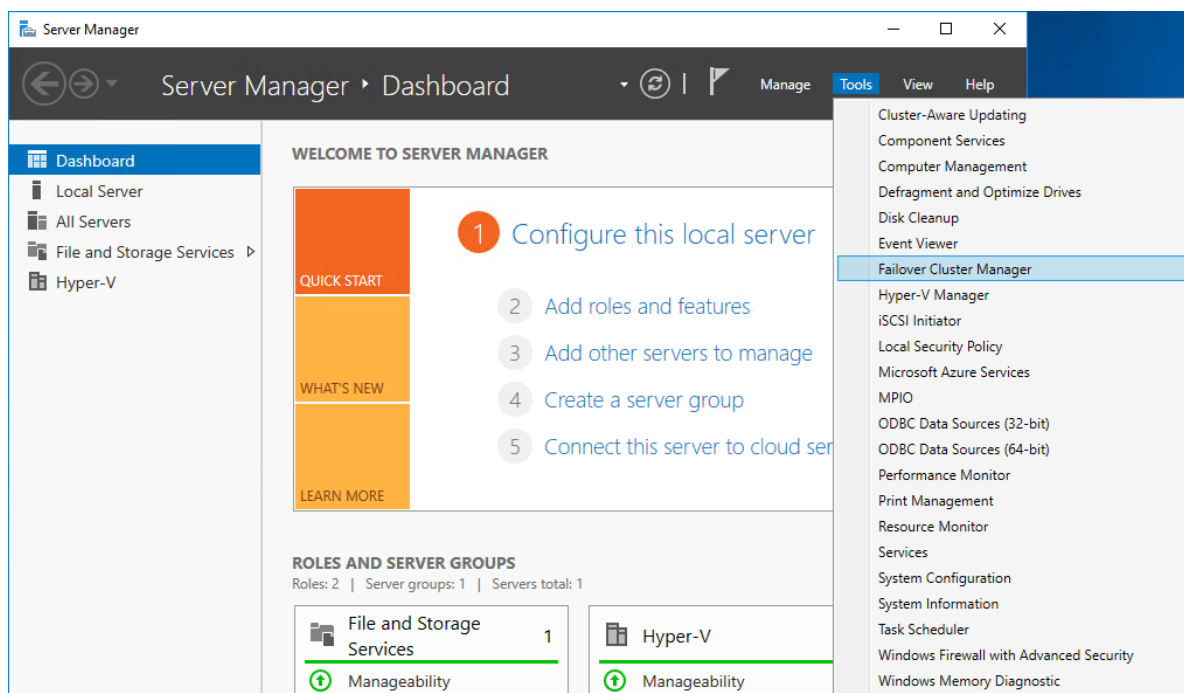
NOTE: To avoid issues during the cluster validation configuration, it is recommended to install the latest Microsoft updates on each node.

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

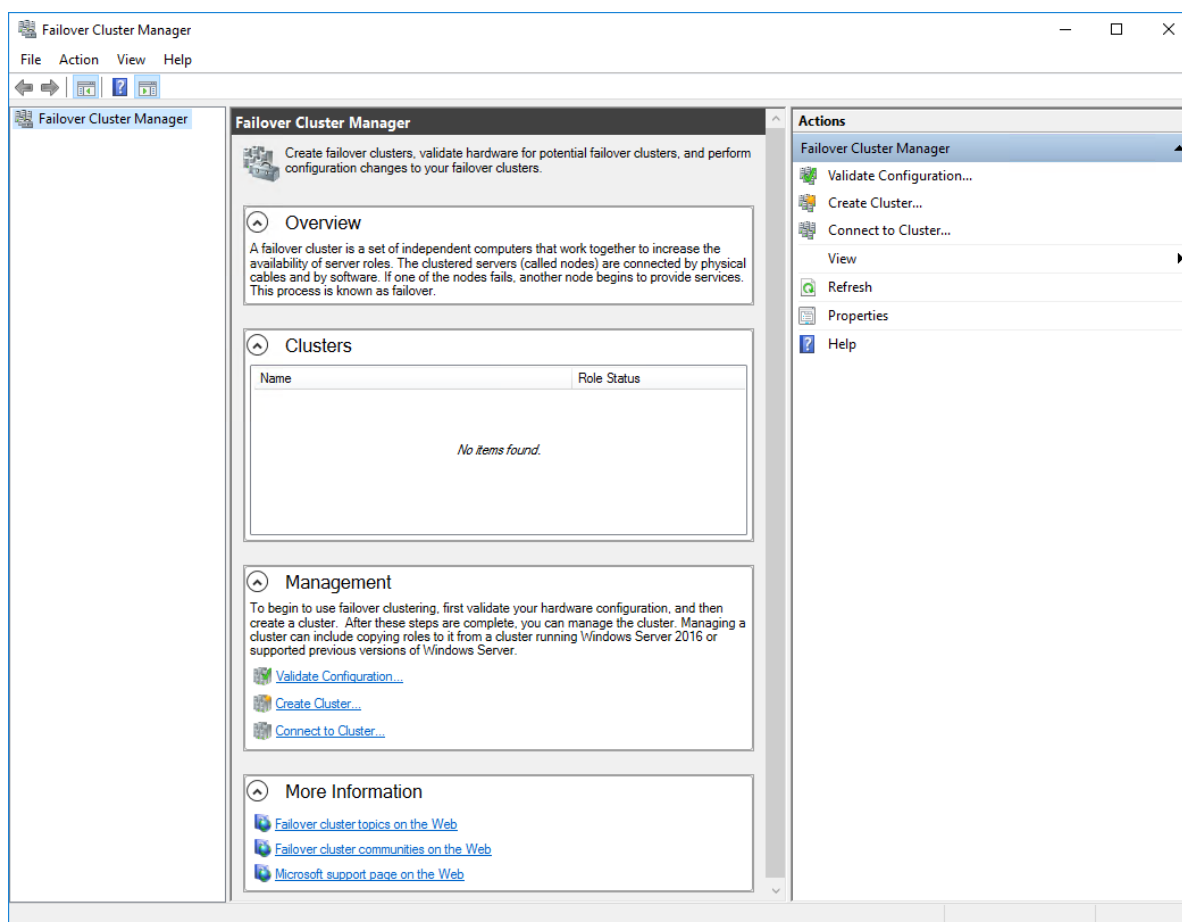
<https://docs.microsoft.com/en-us/windows-server/remote/remote-server-administration-tools>

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

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



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



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

Create Cluster Wizard

Select Servers

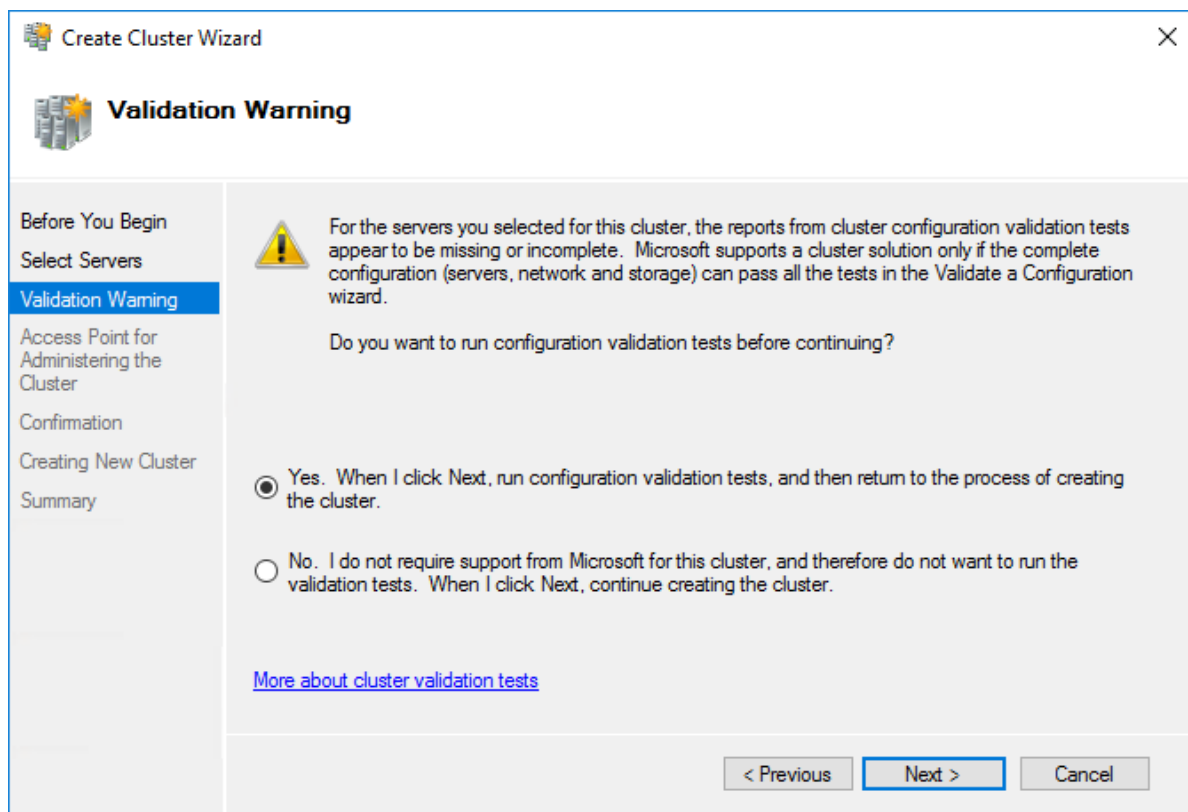
Add the names of all the servers that you want to have in the cluster. You must add at least one server.

Enter server name:

Selected servers:

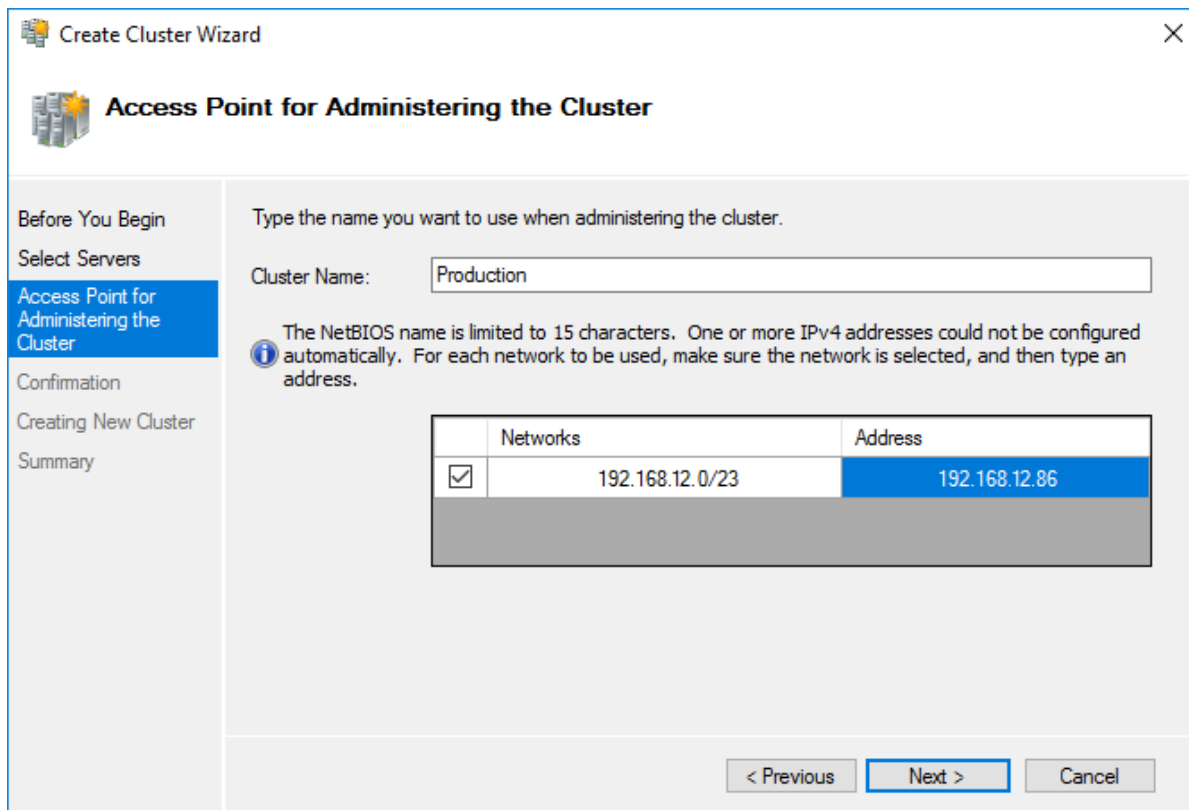
- SW1.starwind.local
- SW2.starwind.local

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



5. Specify the cluster name.

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



Create Cluster Wizard

Access Point for Administering the Cluster

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

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

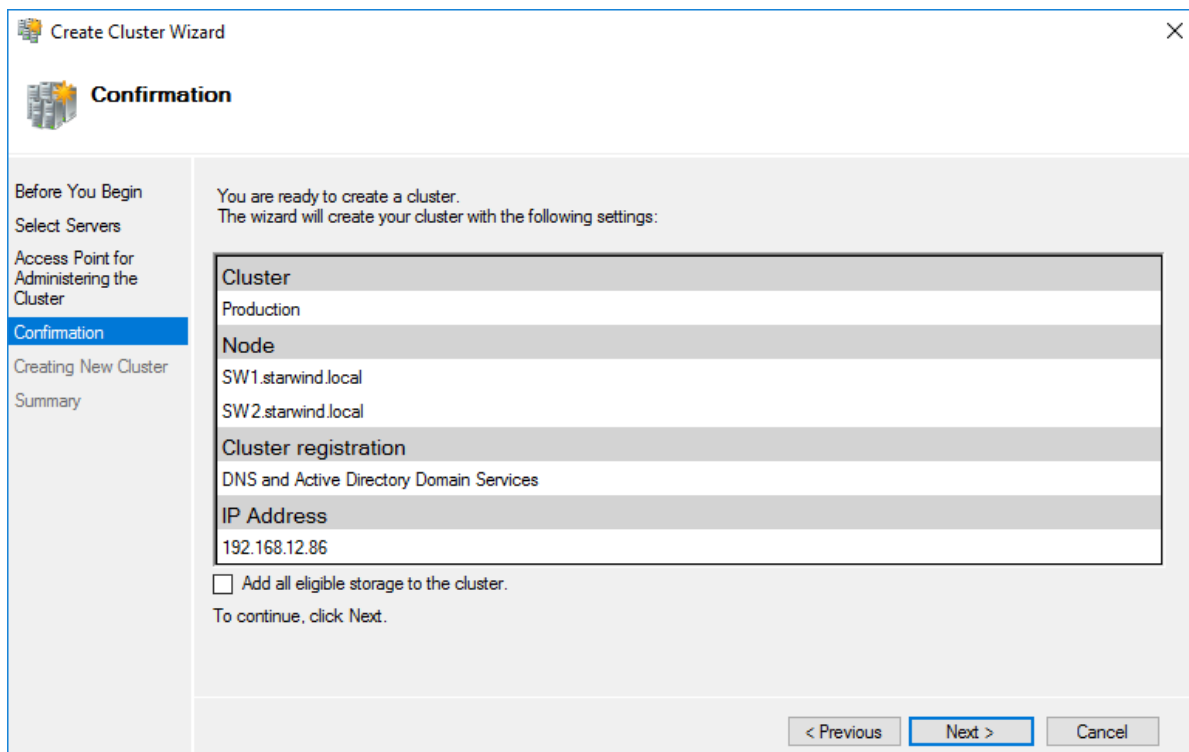
Cluster Name:

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

	Networks	Address
☒	192.168.12.0/23	192.168.12.86

< Previous **Next >** Cancel

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



Create Cluster Wizard

Confirmation

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

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

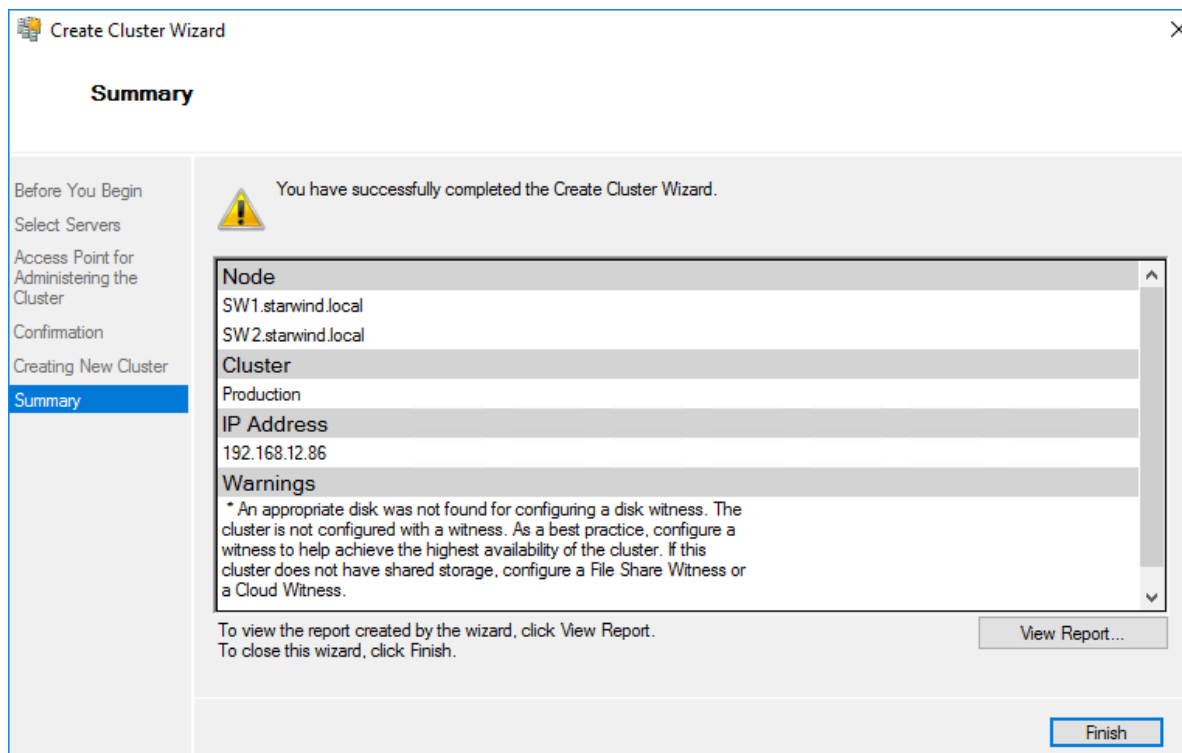
Cluster	Production
Node	SW1.starwind.local SW2.starwind.local
Cluster registration	DNS and Active Directory Domain Services
IP Address	192.168.12.86

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

< Previous **Next >** Cancel

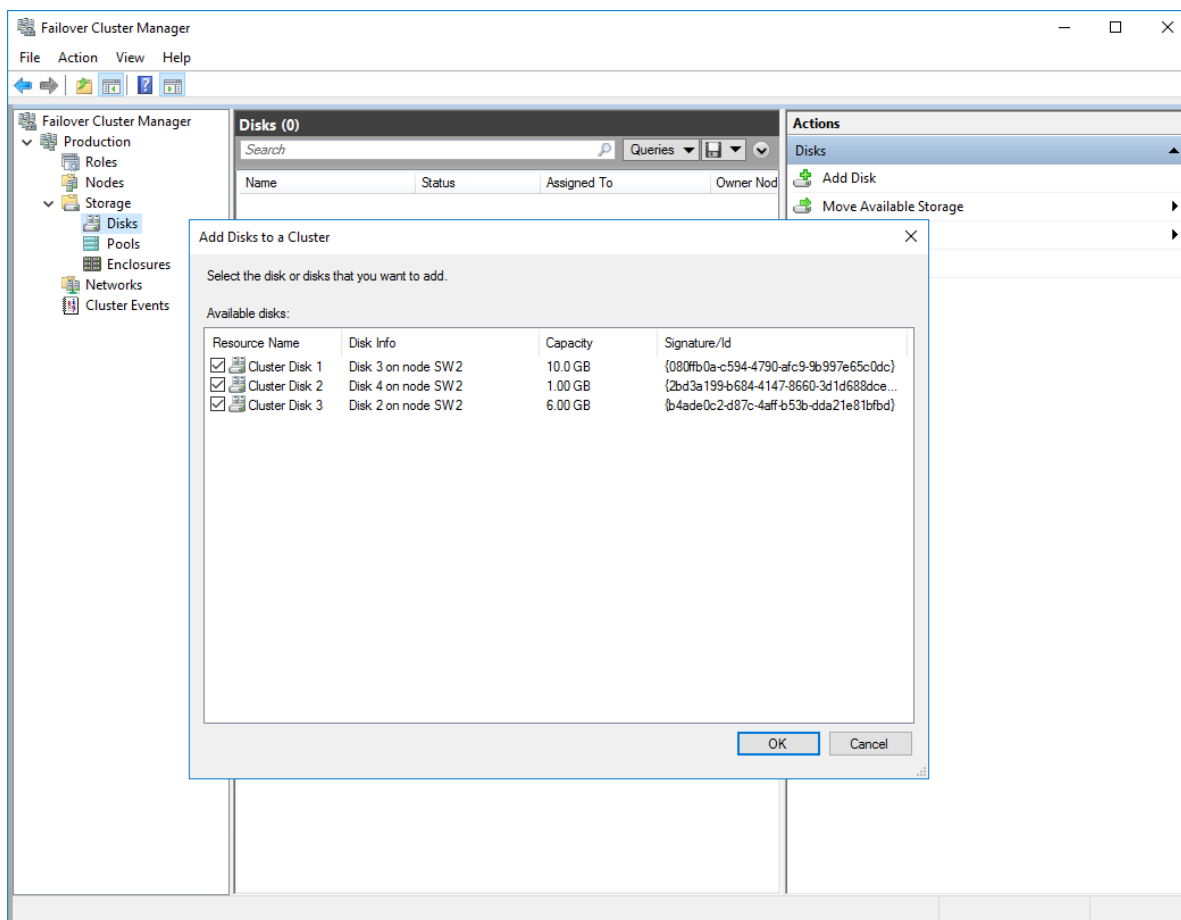
NOTE: If checkbox Add all eligible storage to the cluster is selected, the wizard will add all disks to the cluster automatically. The device with the smallest storage volume will be assigned as a Witness. It is recommended to uncheck this option before clicking Next and add cluster disks and the Witness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

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

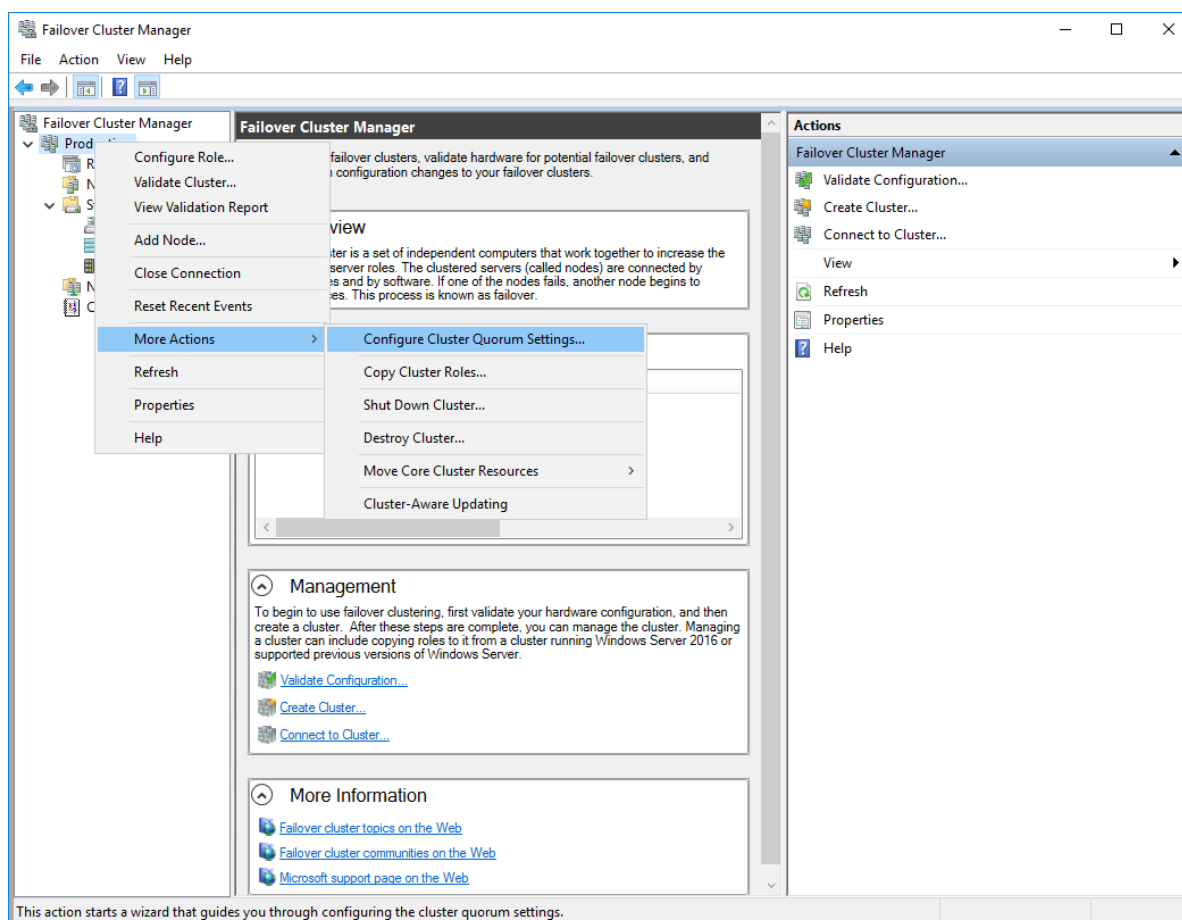


Adding Storage to the Cluster

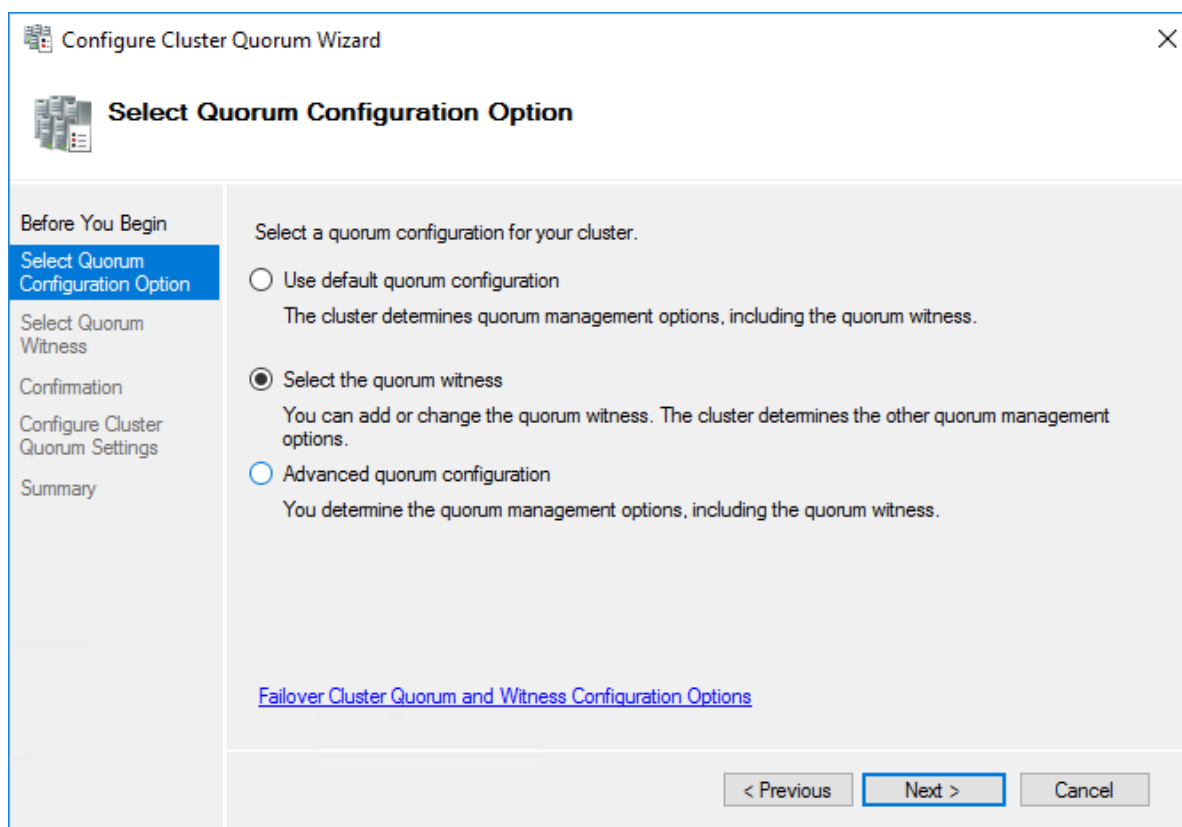
1. In Failover Cluster Manager, navigate to Cluster -> Storage -> Disks. Click Add Disk in the Actions panel, choose StarWind disks from the list and confirm the selection.



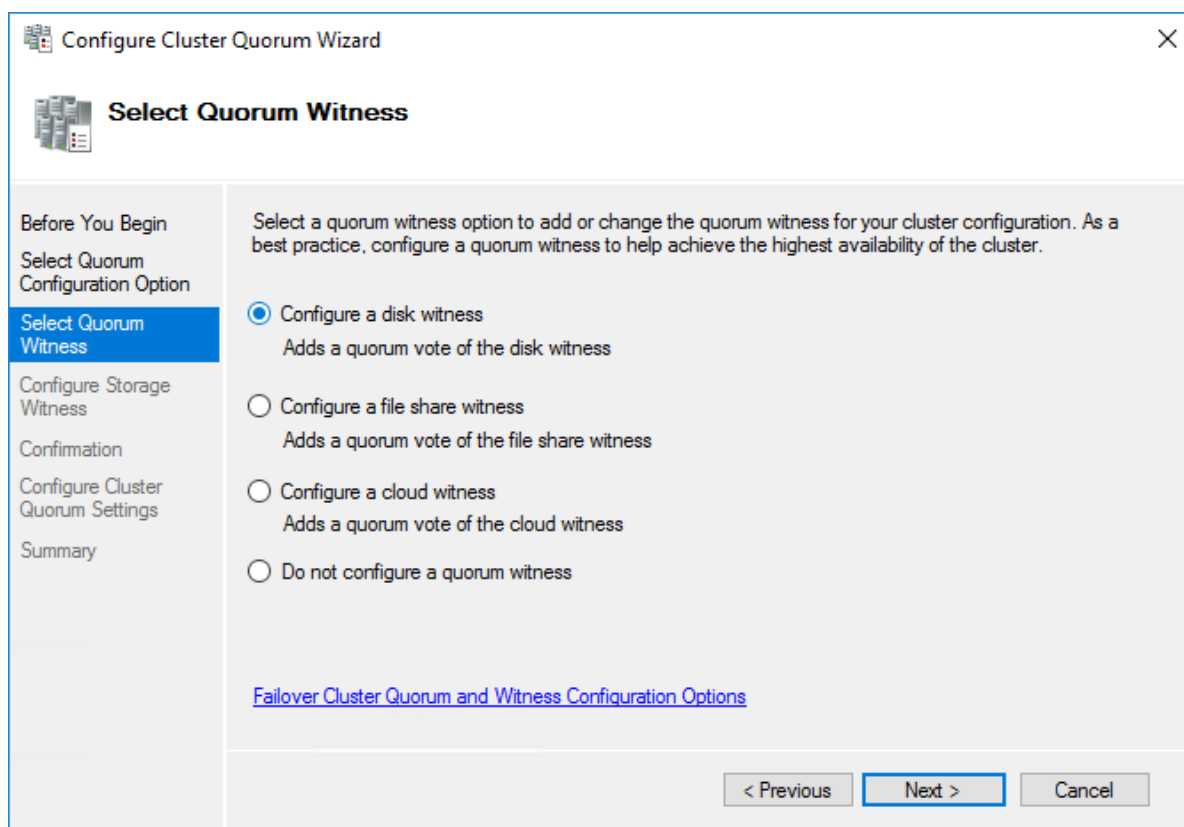
2. To configure the cluster witness disk, right-click on Cluster and proceed to More Actions -> Configure Cluster Quorum Settings.



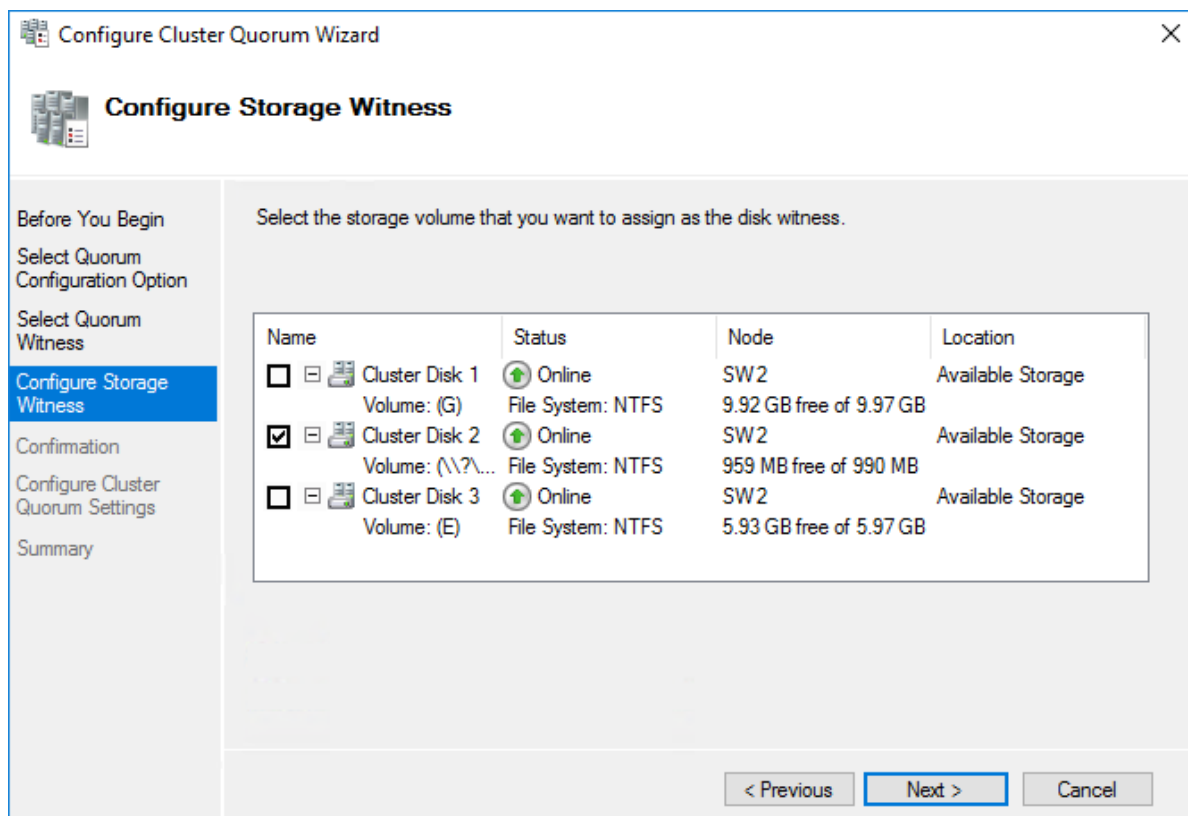
3. Follow the wizard and use the Select the quorum witness option. Click Next.



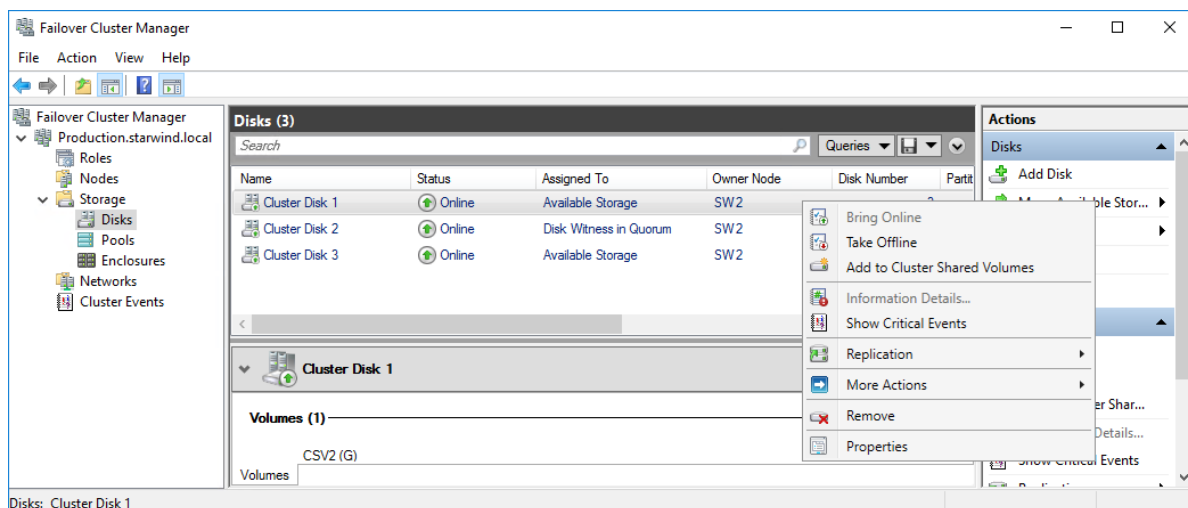
4. Select Configure a disk witness. Click Next.



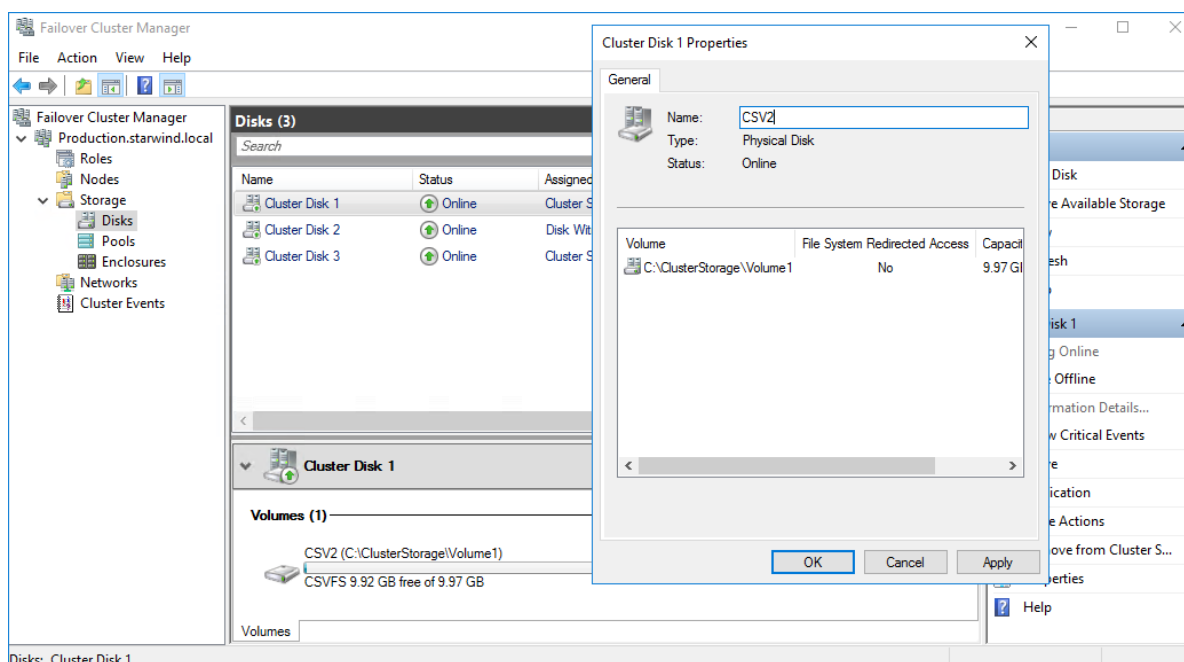
5. Select the Witness disk to be assigned as the cluster witness disk. Click Next and press Finish to complete the operation.



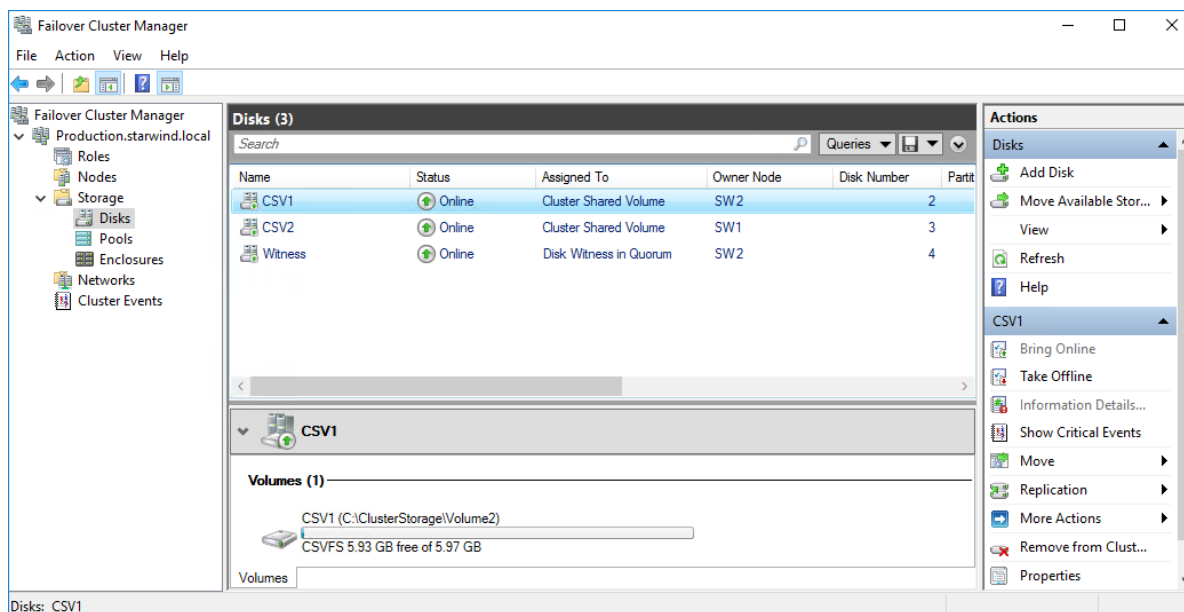
6. In Failover Cluster Manager, Right-click the disk and select Add to Cluster Shared Volumes.



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



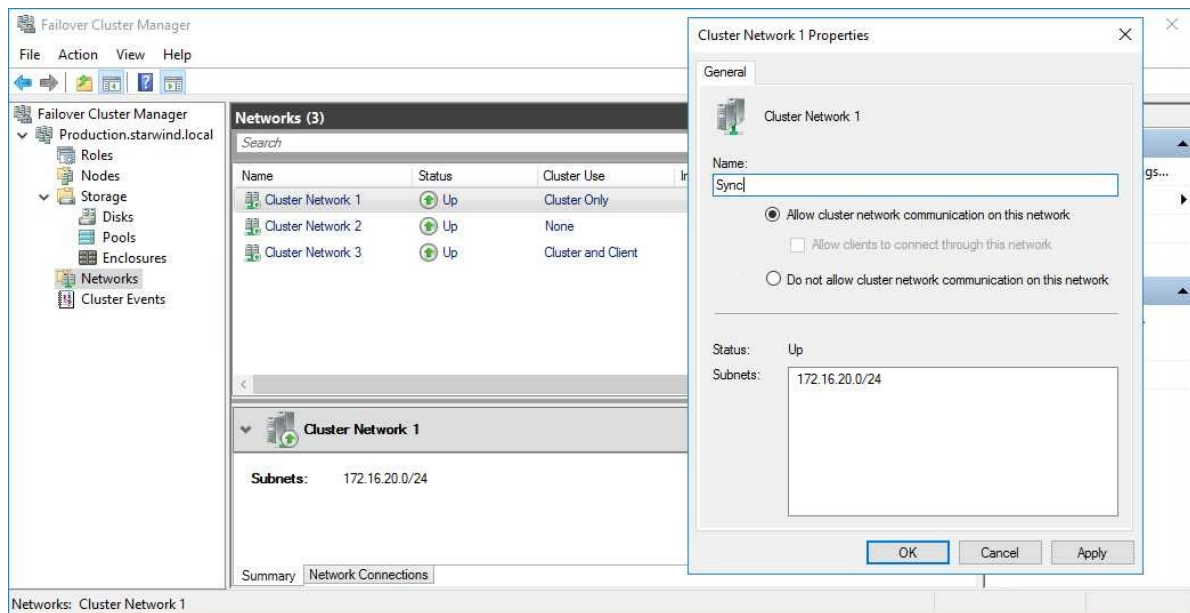
8. Perform the steps 6-7 for any other disk in Failover Cluster Manager. The resulting list of disks will look similar to the screenshot below.



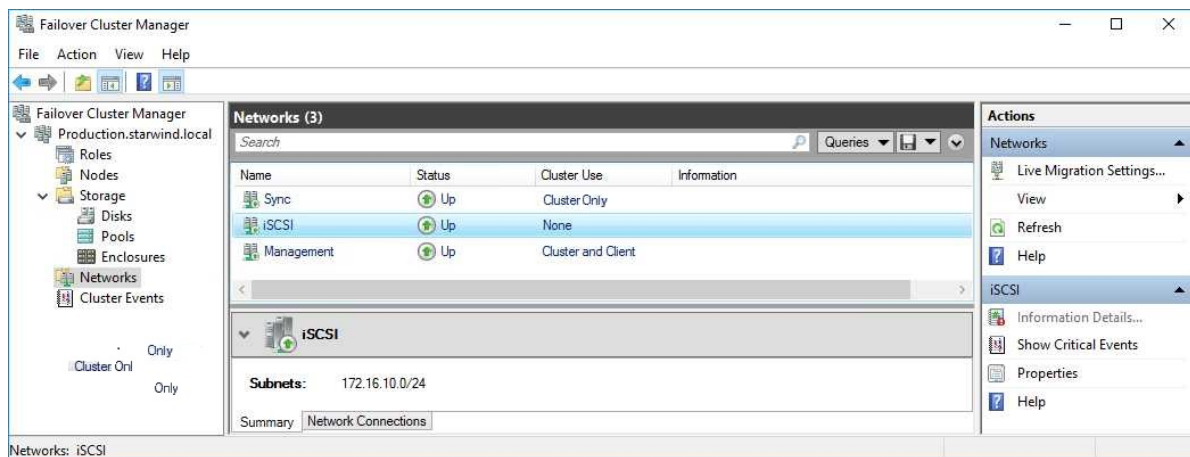
Configuring Cluster Network Preferences

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

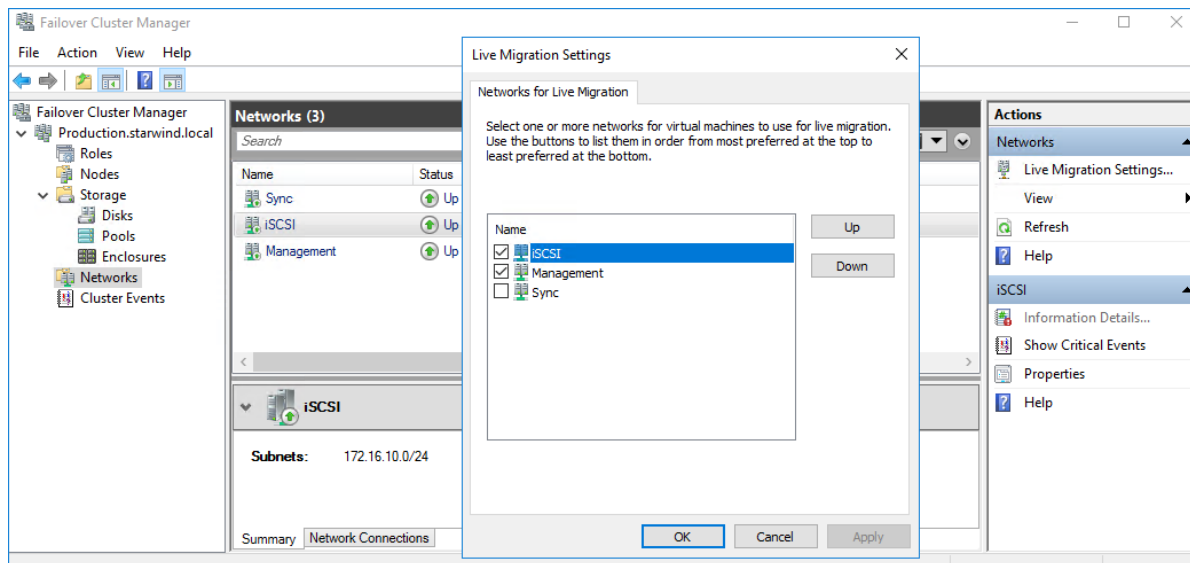
NOTE: Double-check that cluster communication is configured with redundant networks:
<https://docs.microsoft.com/en-us/windows-server/failover-clustering/smb-multichannel>



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.



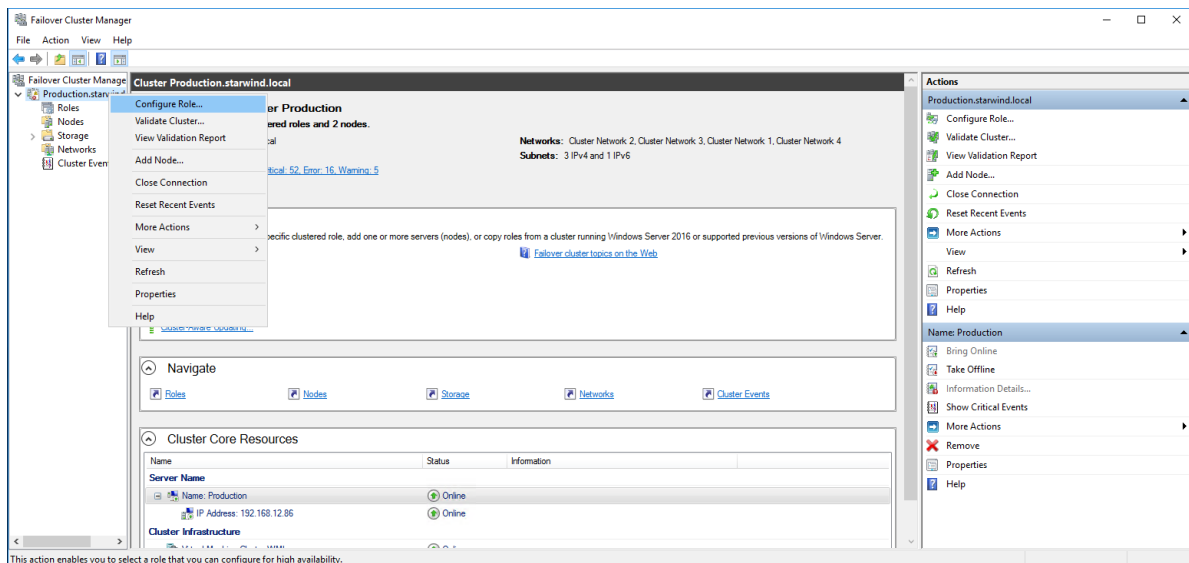
The cluster configuration is completed and it is ready for virtual machines deployment. Select Roles and in the Action tab, click Virtual Machines -> New Virtual Machine. Complete the wizard.

Configuring File Shares

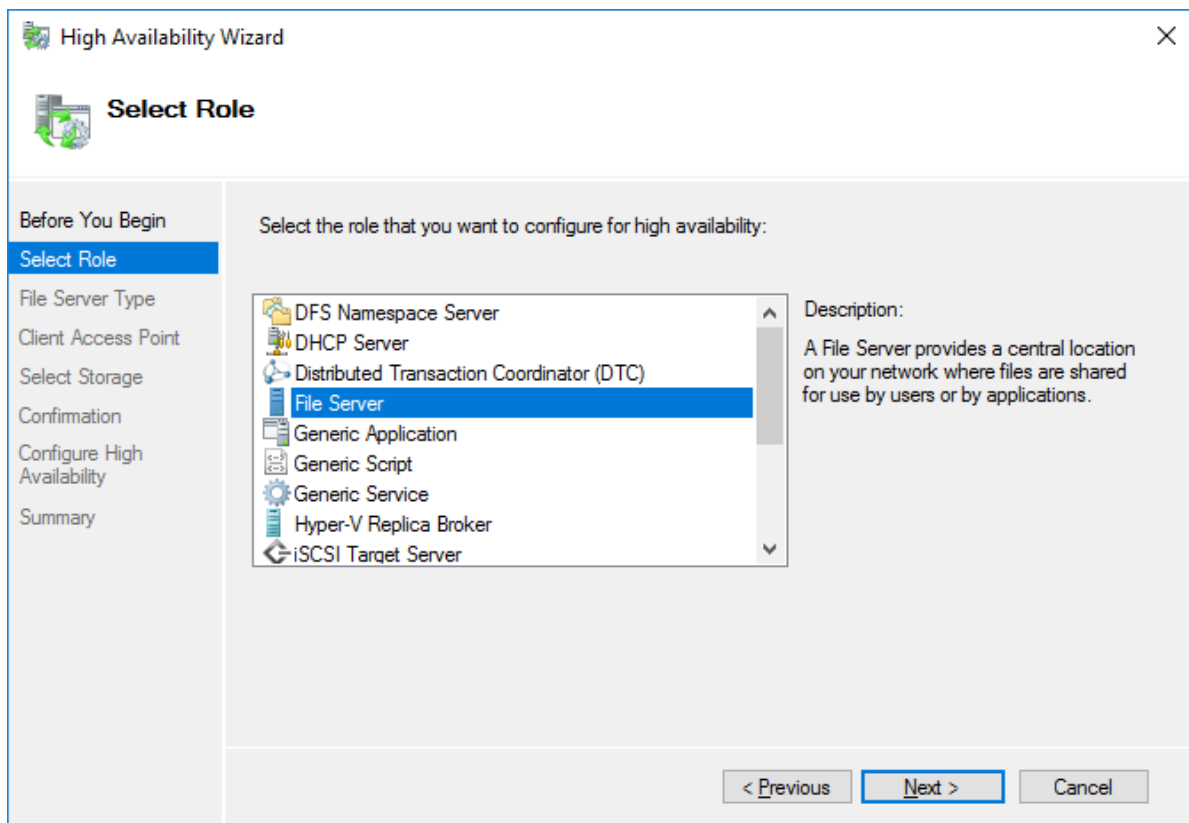
Please follow the steps below if file shares should be configured on cluster nodes.

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.

High Availability Wizard

File Server Type

Select an option for a clustered file server:

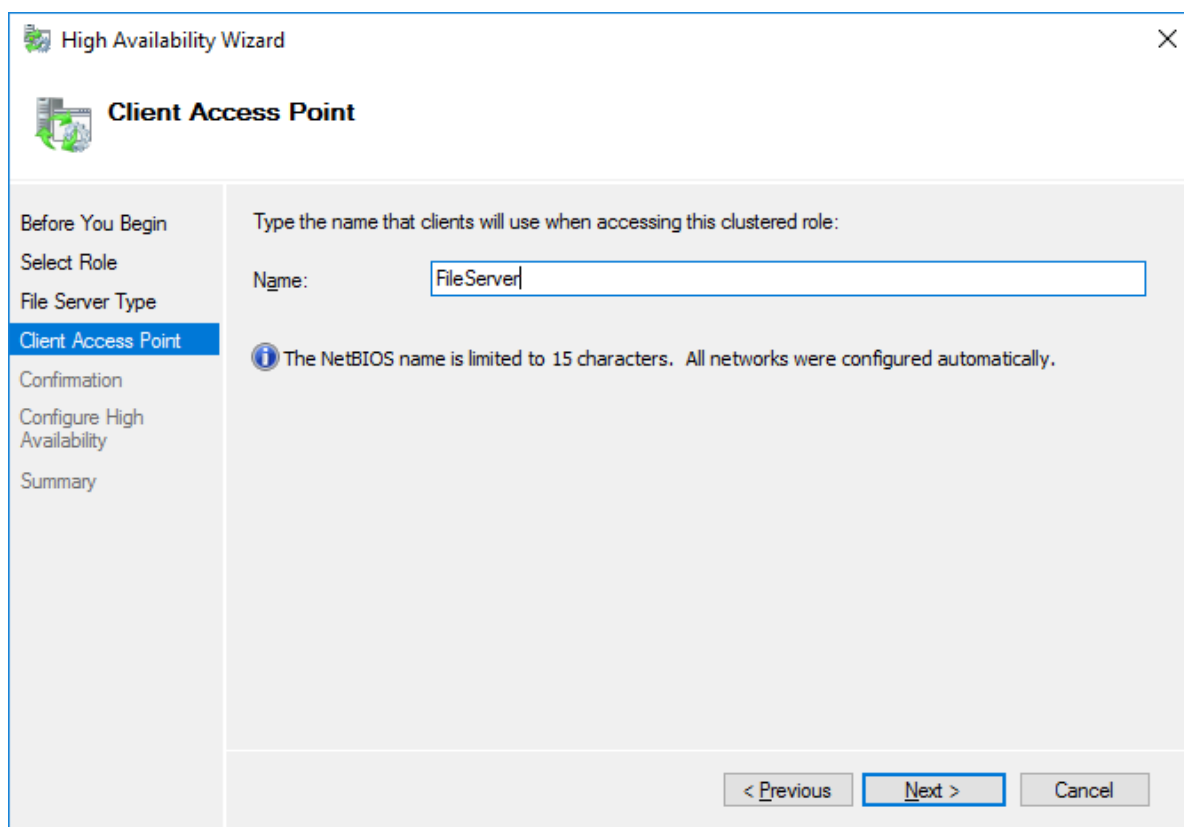
☐ File Server for general use
Use this option to provide a central location on your network for users to share files or for server applications that open and close files frequently. This option supports both the Server Message Block (SMB) and Network File System (NFS) protocols. It also supports Data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

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

[More about clustered file server options](#)

< Previous **Next >** Cancel

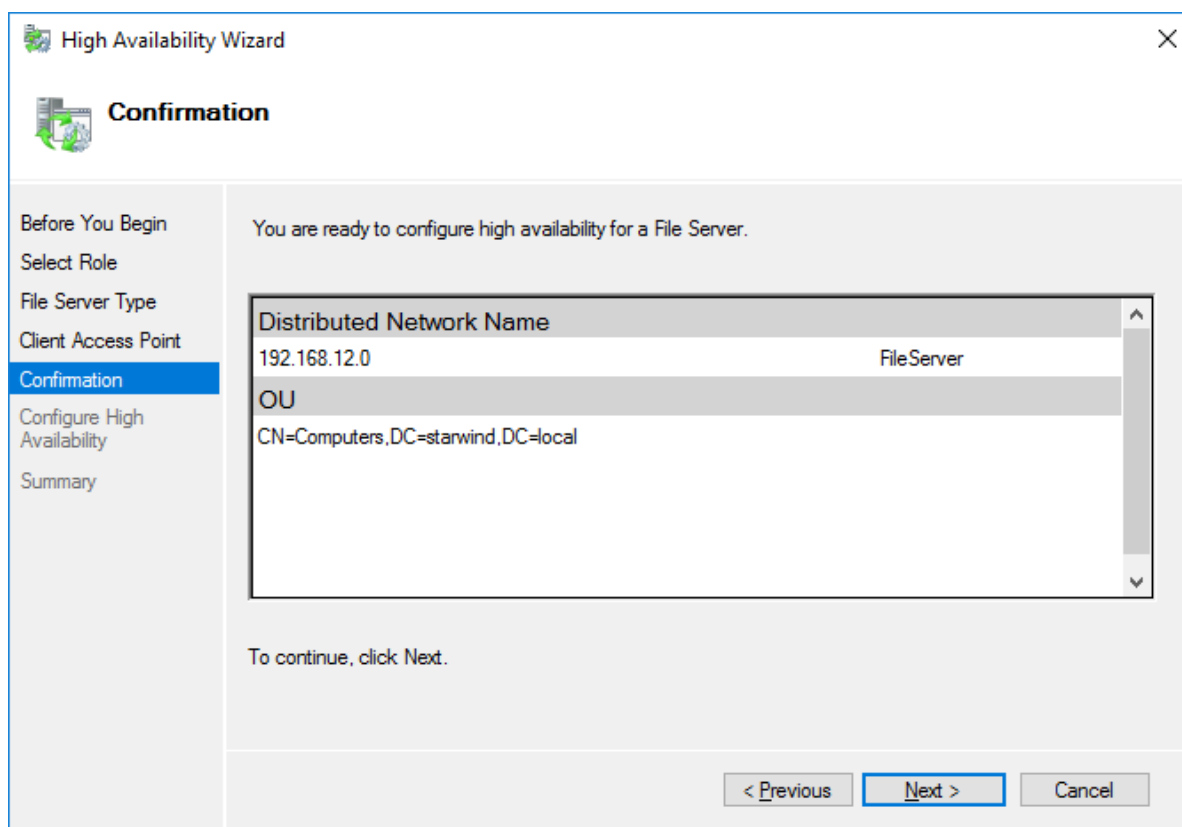
5. On the Client Access Point page, in the Name text field, type the NetBIOS name that will be used to access a Scale-Out File Server.



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. Below the title bar is a header area with a server icon and the text 'Client Access Point'. 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 highlighted with a blue background), 'Confirmation', 'Configure High Availability', and 'Summary'. The main area of the wizard contains the text 'Type the name that clients will use when accessing this clustered role:' followed by a text input field with the value 'FileServer'. Below the input field is an information icon (a blue circle with an 'i') and the text 'The NetBIOS name is limited to 15 characters. All networks were configured automatically.' At the bottom right of the main area, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

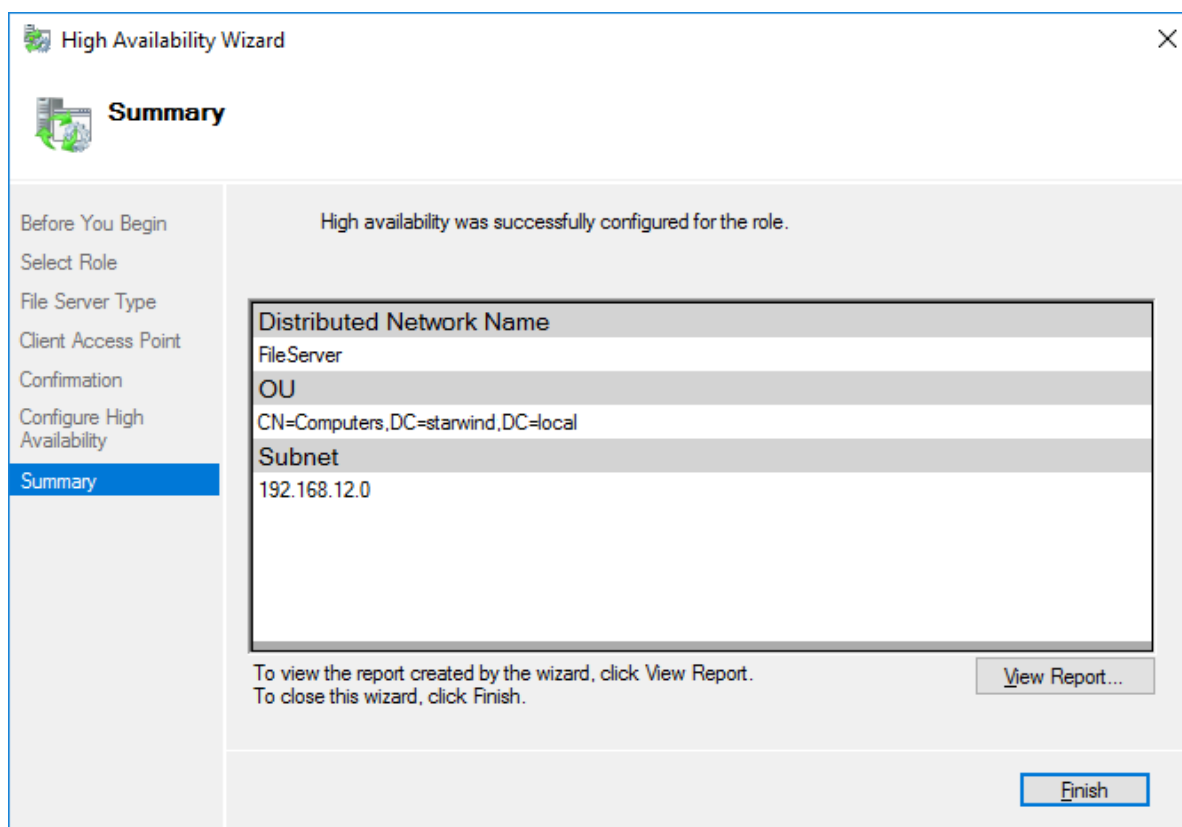
Click Next to continue.

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

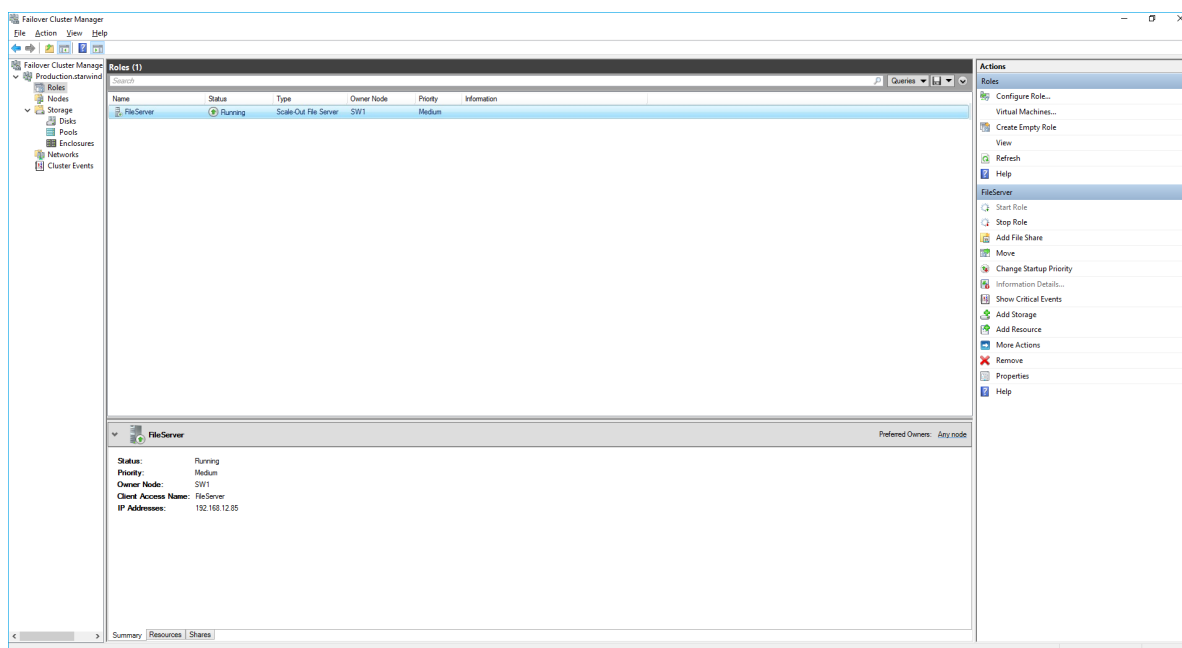


7. Once the installation is finished successfully, the Wizard should now look like the screenshot below.

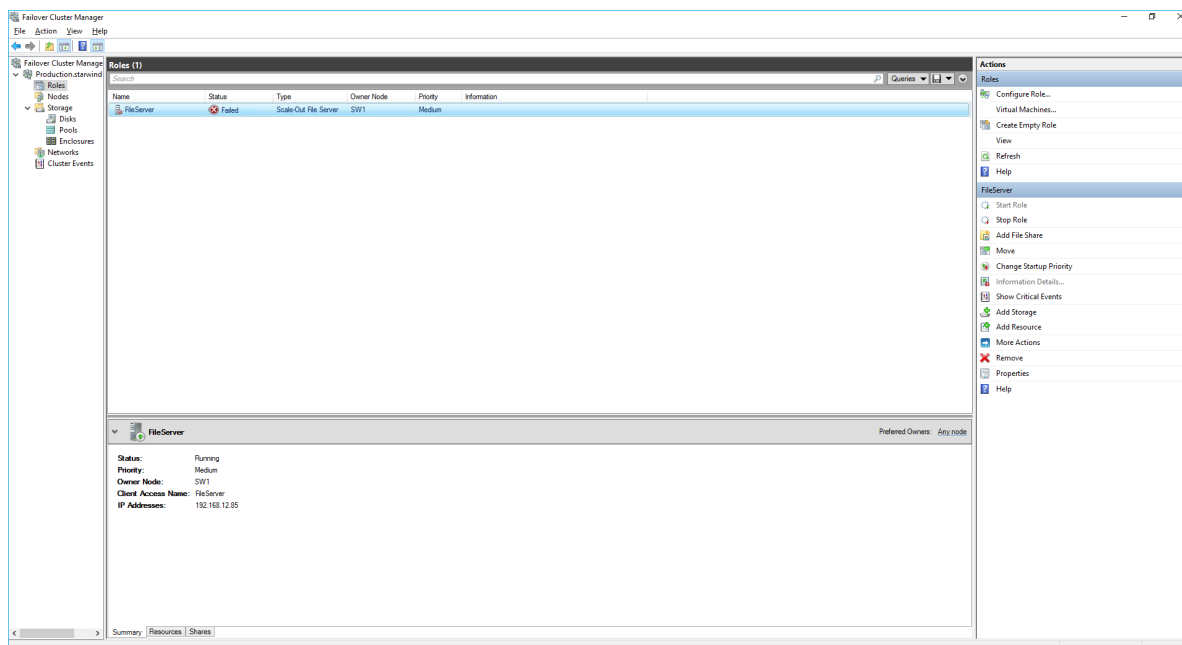
Click Finish to close the Wizard.



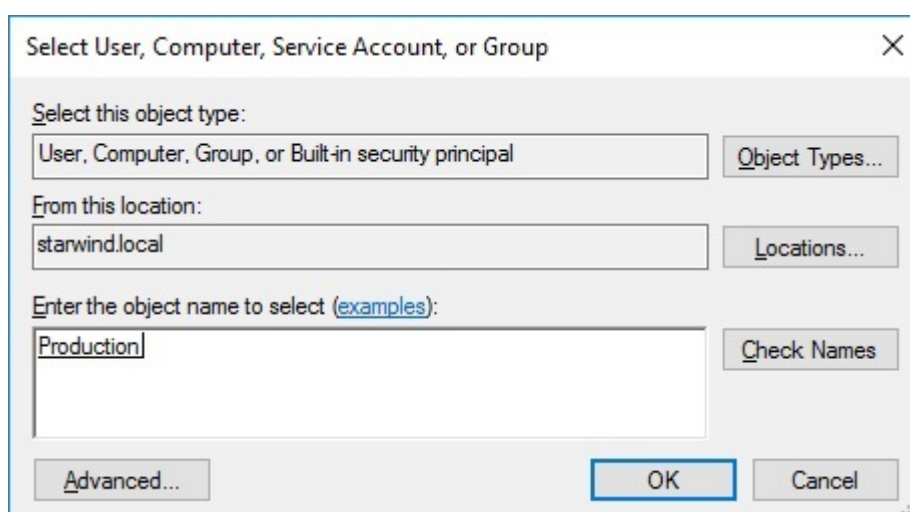
8. The newly created role should now look like the screenshot below.



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

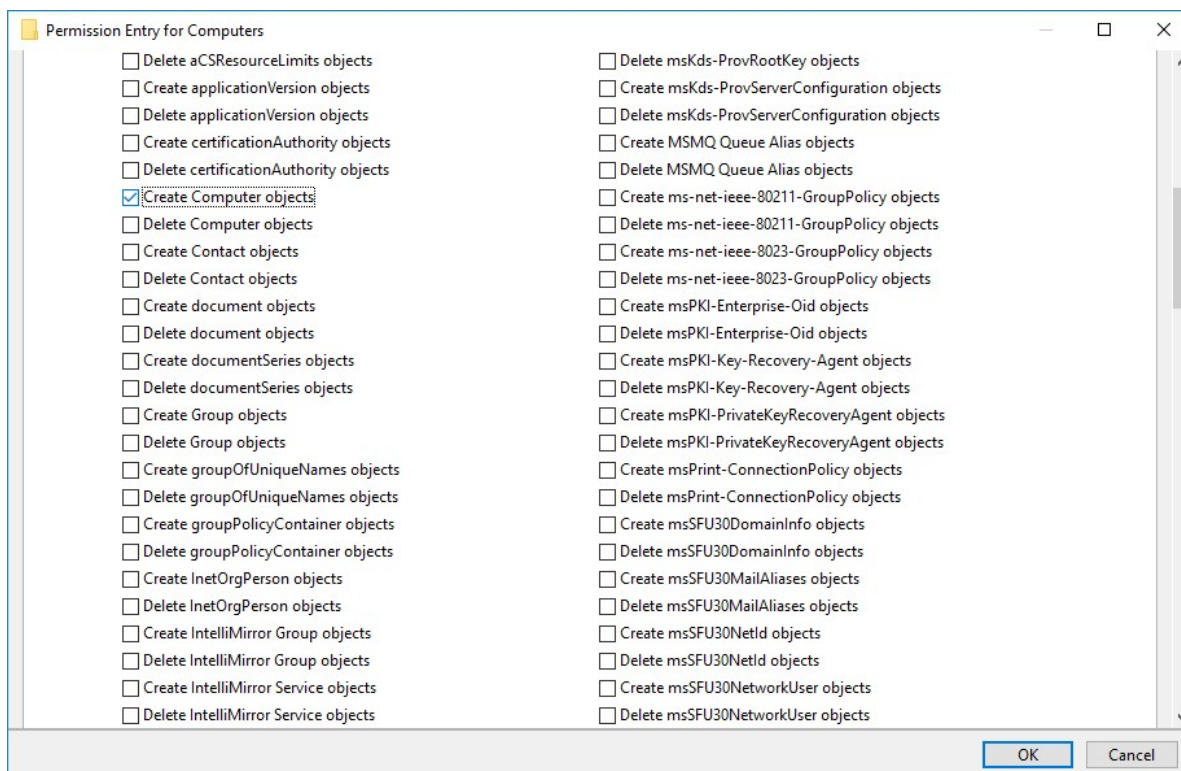


- open Active Directory Users and Computers
- enable the Advanced view if it is not enabled
- edit the properties of the OU containing the cluster computer object (in this case – Production)
- open the Security tab and click Advanced
- in the appeared window, press Add (the Permission Entry dialog box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

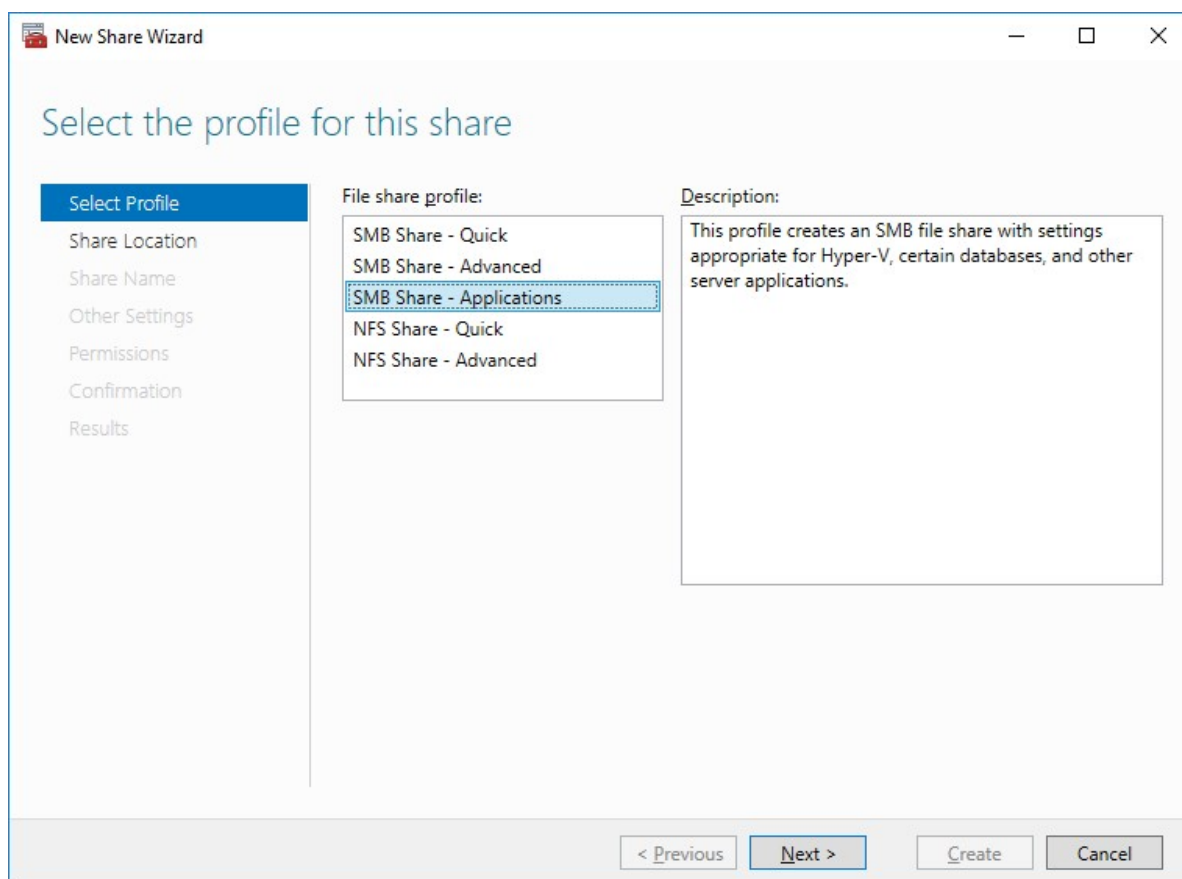


- click OK on all opened windows to confirm the changes
- open Failover Cluster Manager, right-click SOFS role and click Start Role

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:

< Previous

Next >

Create

Cancel

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

New Share Wizard

Specify share name

Select Profile
Share Location
Share Name
Other Settings
Permissions
Confirmation
Results

Share name:

Share description:

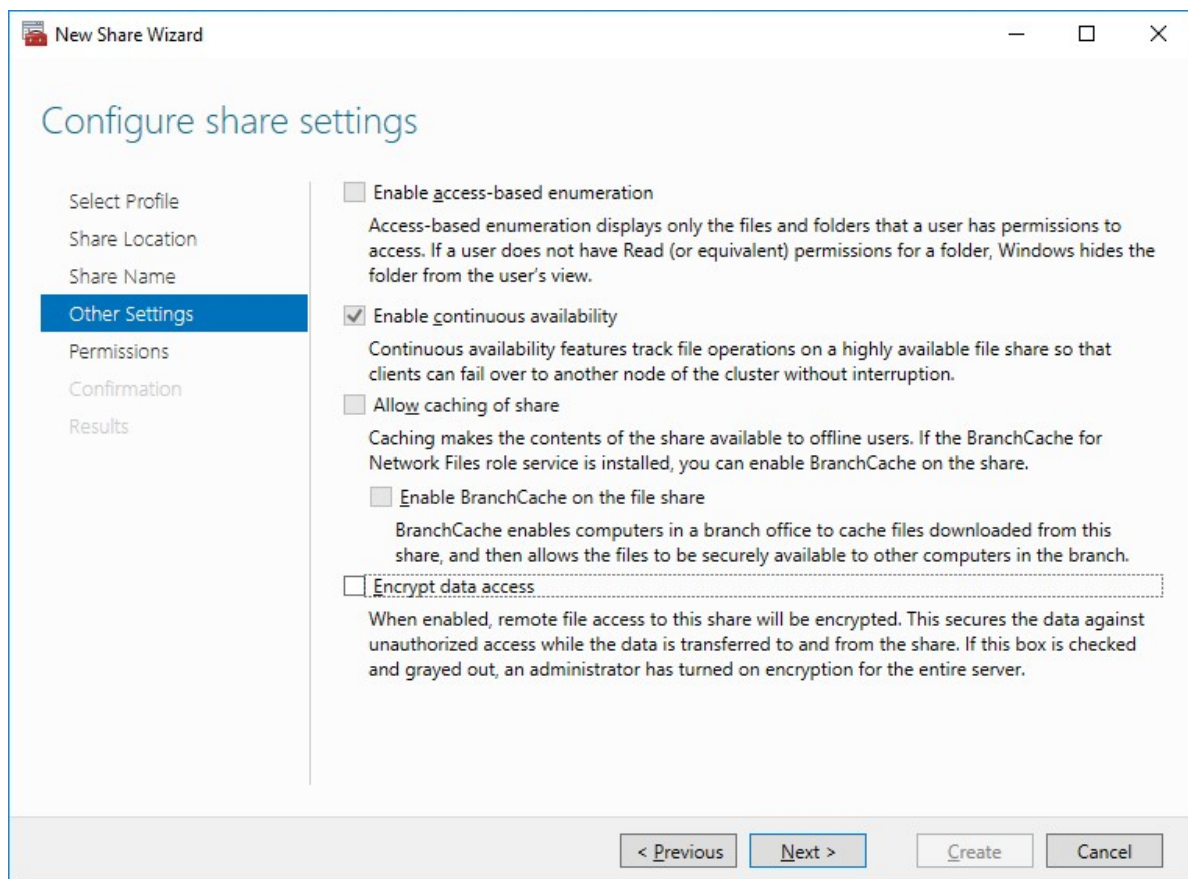
Local path to share:

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

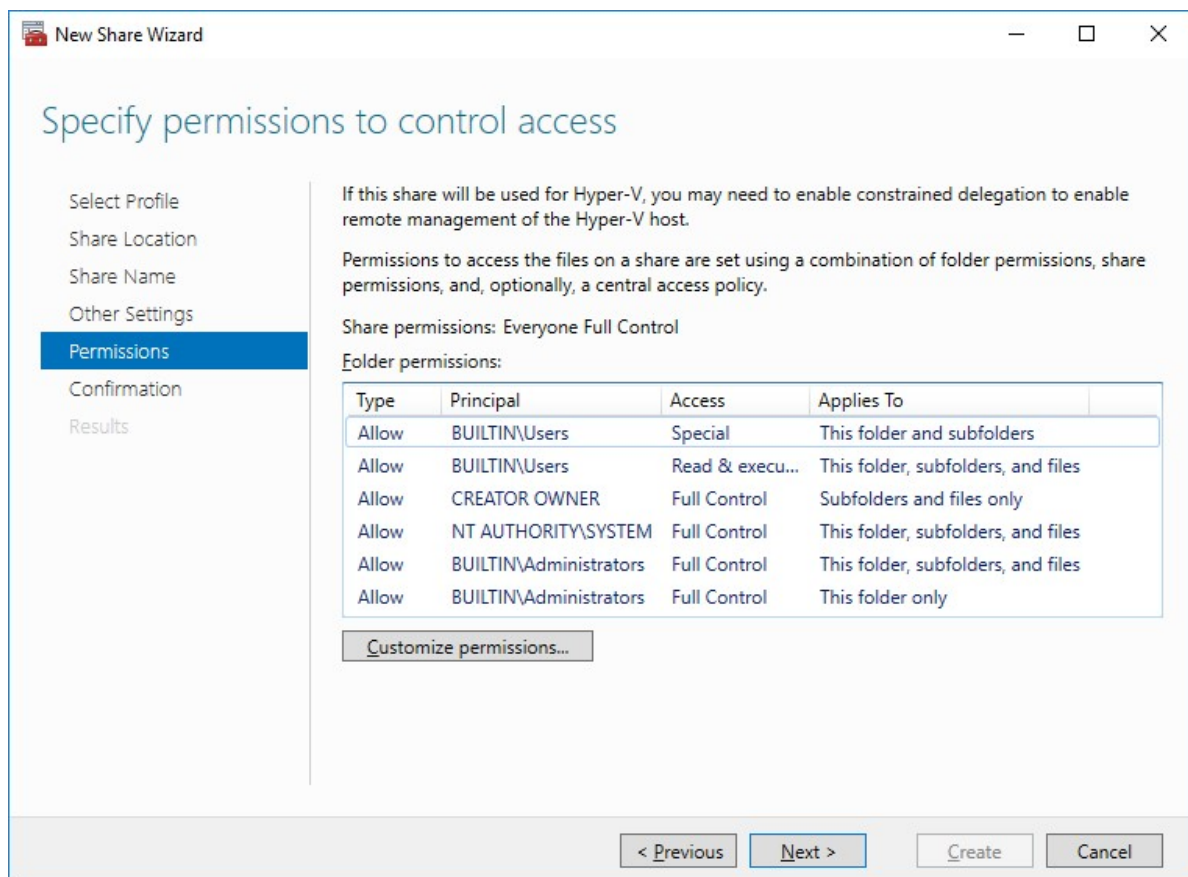
Remote path to share:

< Previous Next > Create Cancel

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



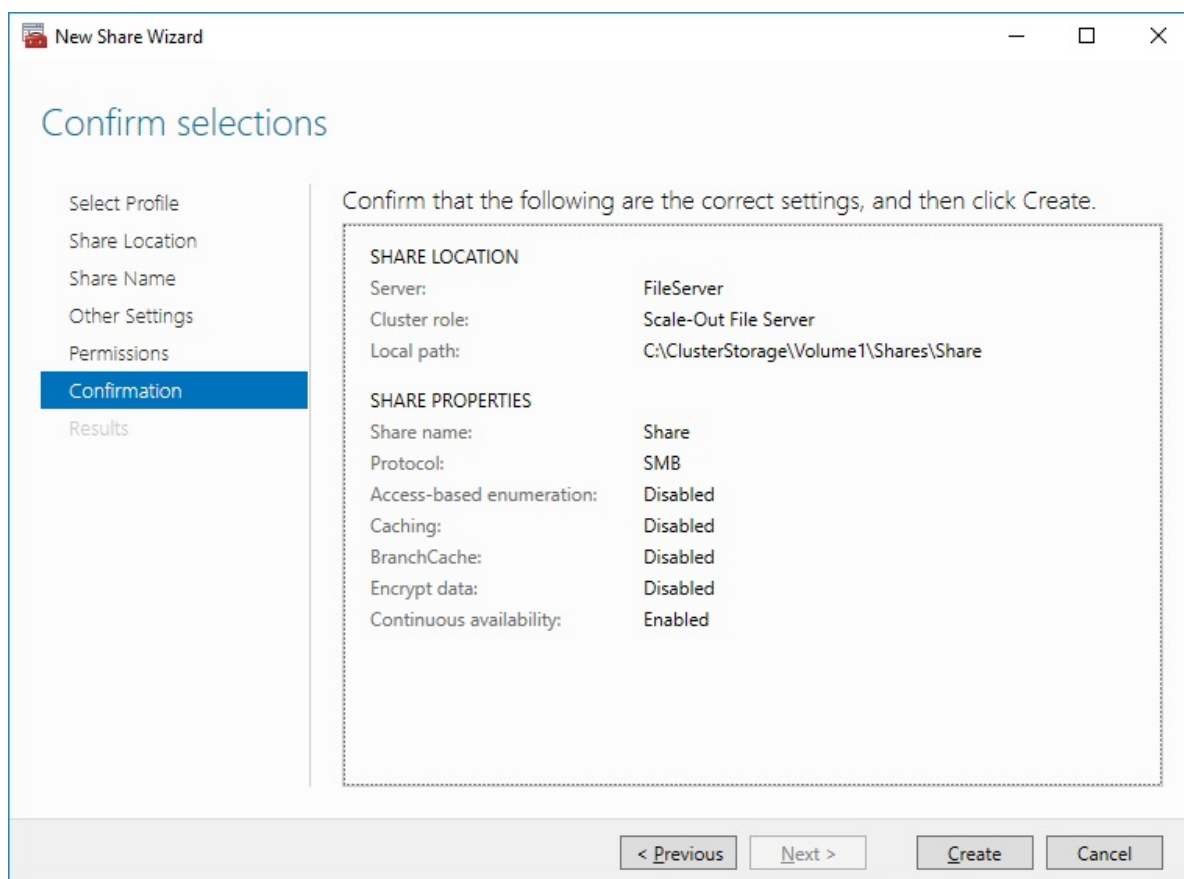
8. Specify the access permissions for the file share.



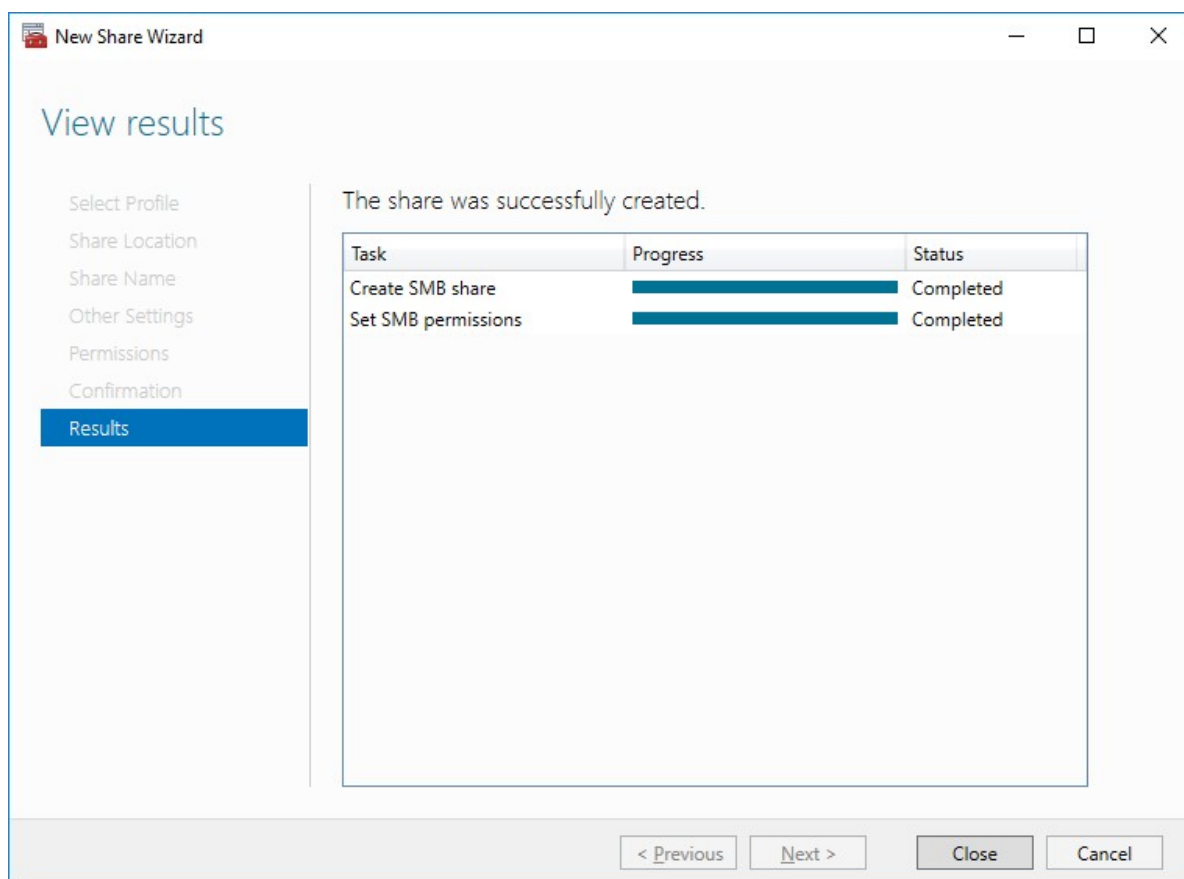
NOTE:

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

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

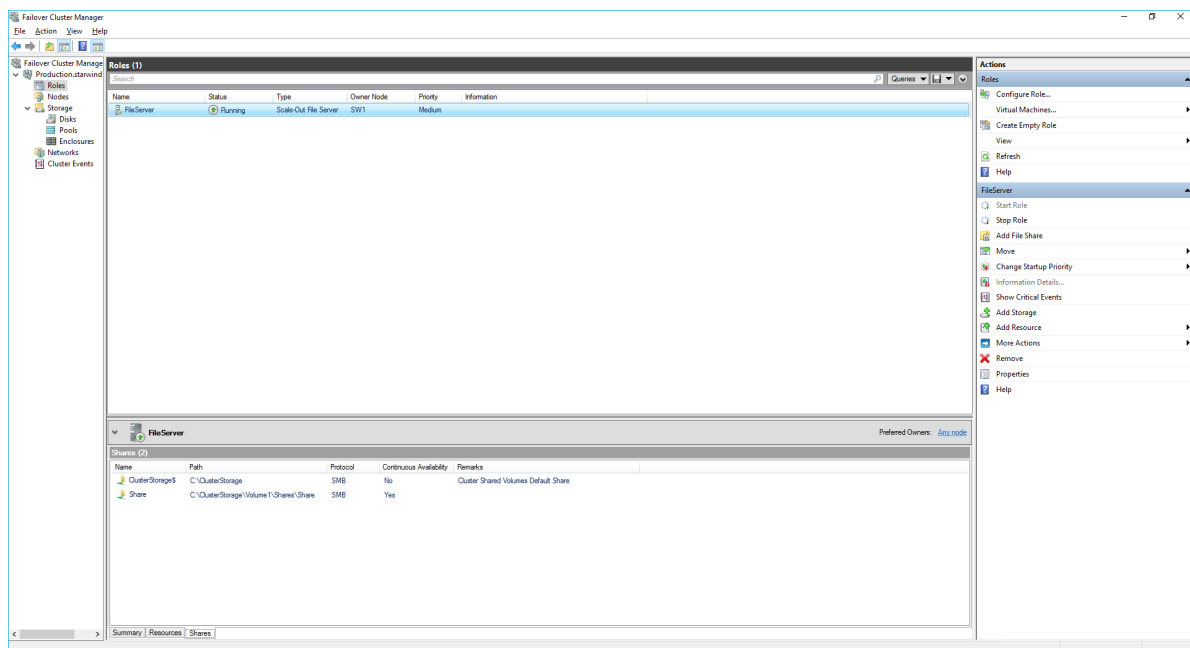


10. Check the summary and click Close to close the Wizard.



To Manage Created File Shares:

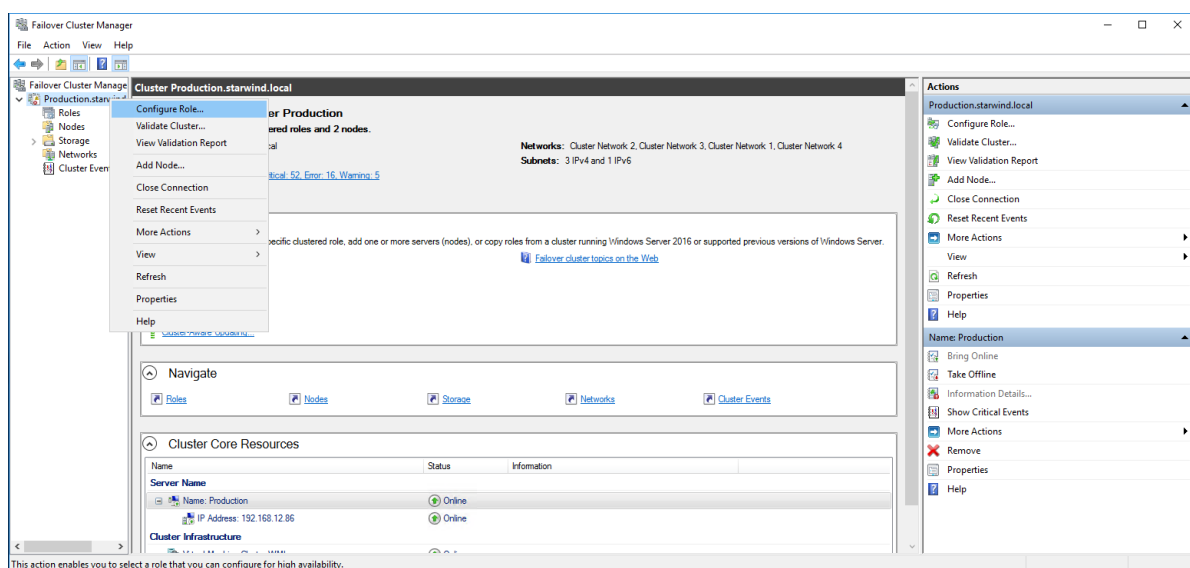
- open Failover Cluster Manager
- expand the cluster and click Roles
- choose the file share role, select the Shares tab, right-click the created file share, and select Properties:



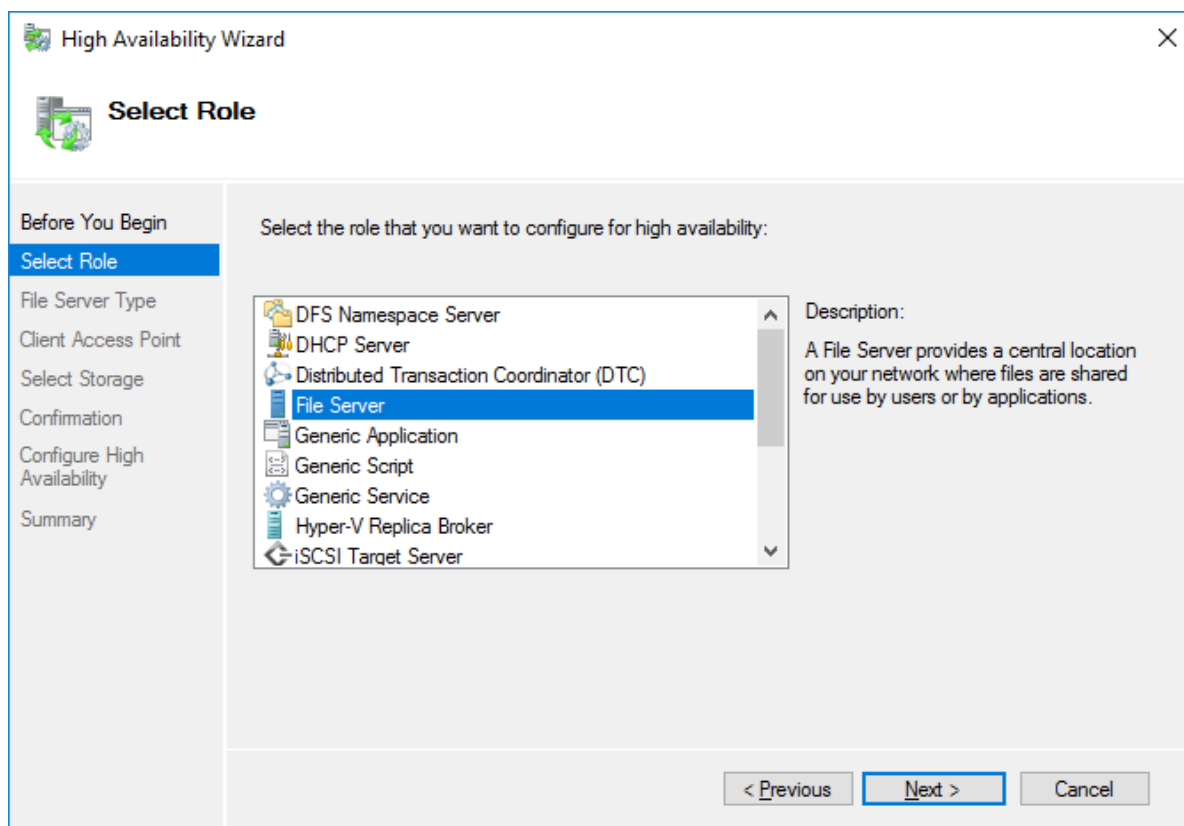
Configuring The File Server For General Use Role

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

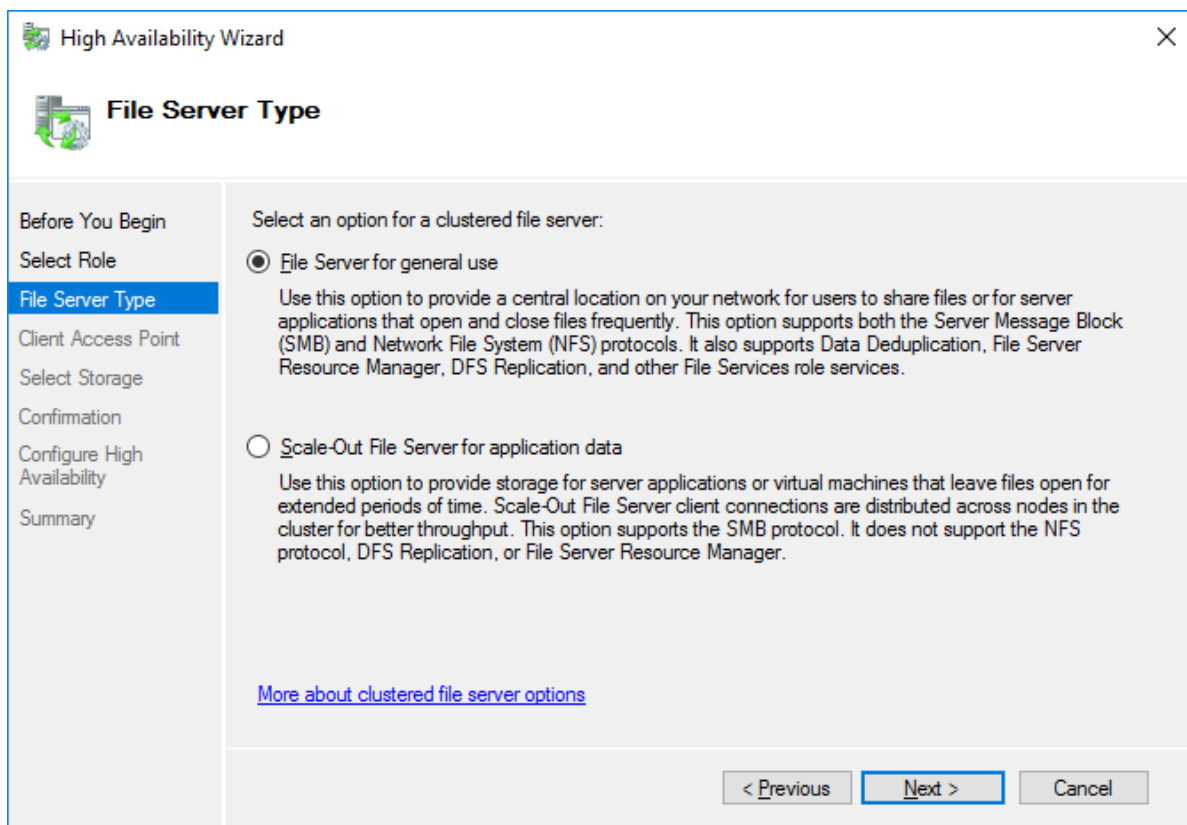
1. To configure the File Server for General Use role, open Failover Cluster Manager.
2. Right-click on the cluster name, then click Configure Role and click Next to continue.



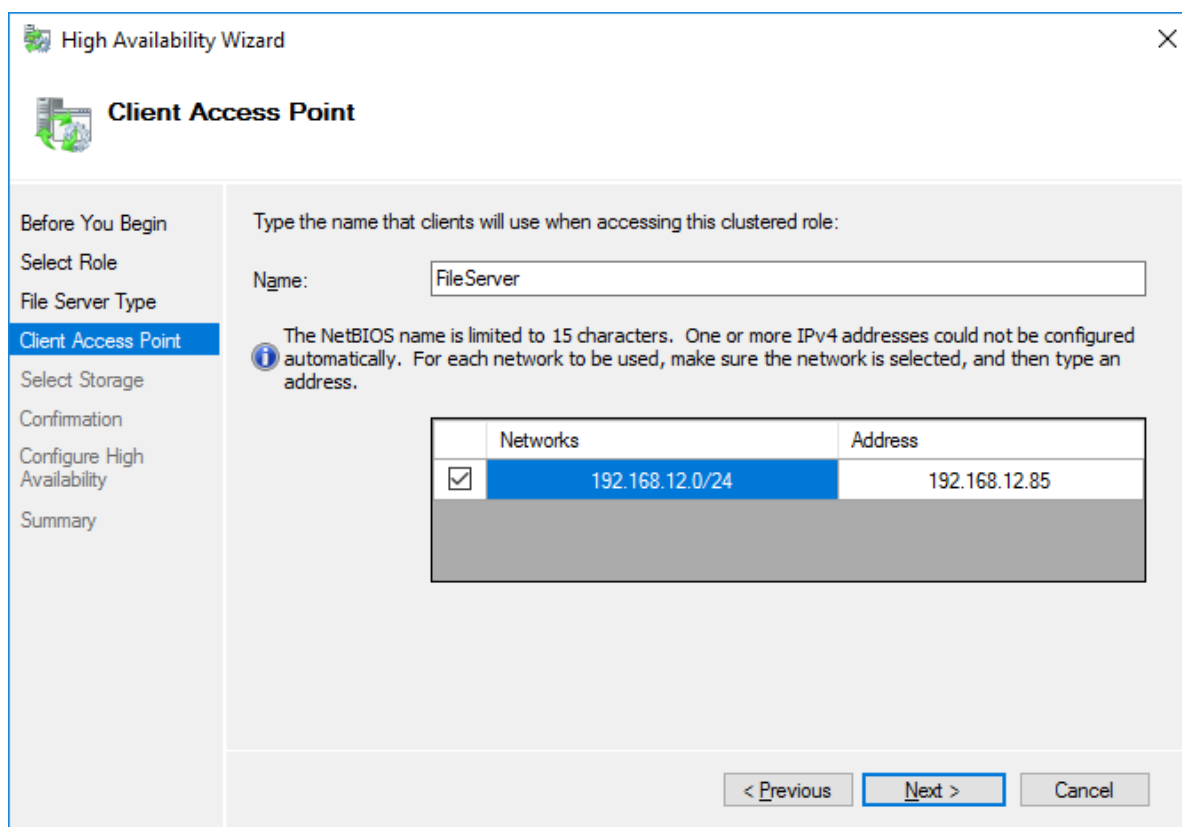
3. Select the File Server item from the list in High Availability Wizard and click Next to continue.



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



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



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

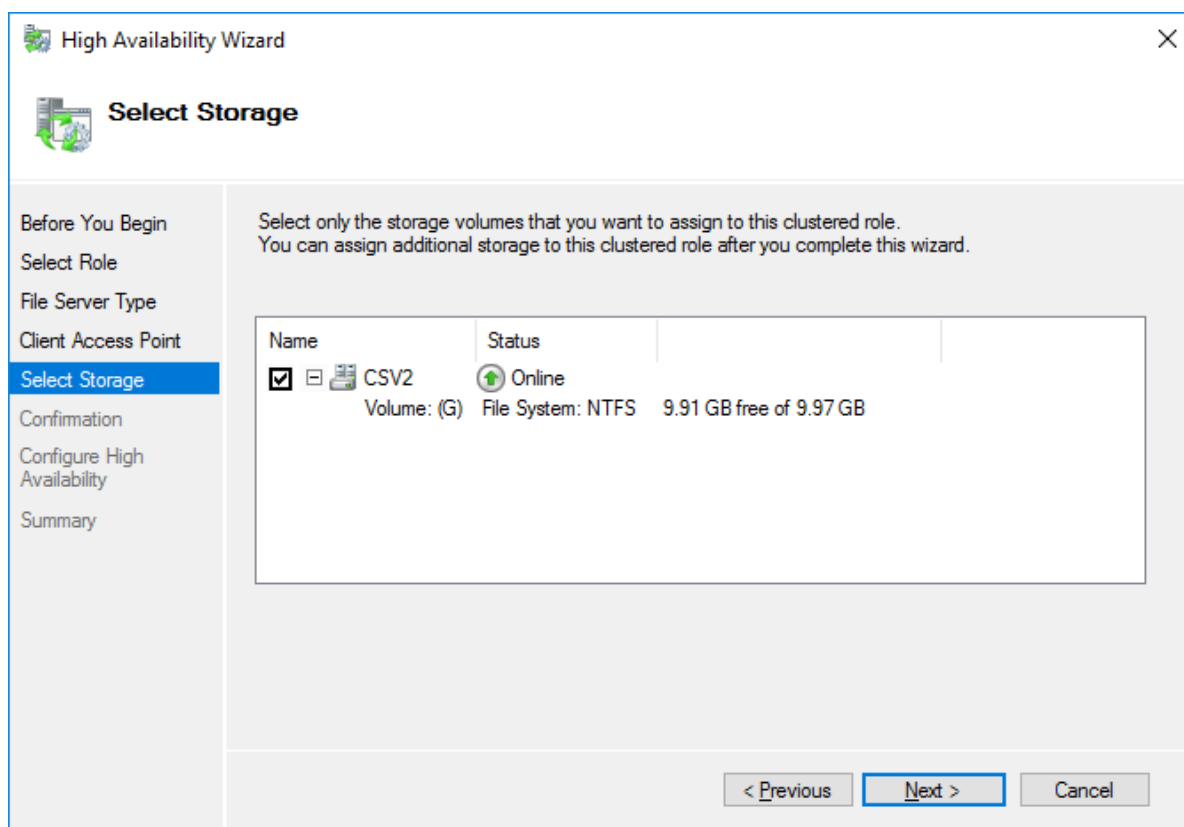
i The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

	Networks	Address
☒	192.168.12.0/24	192.168.12.85

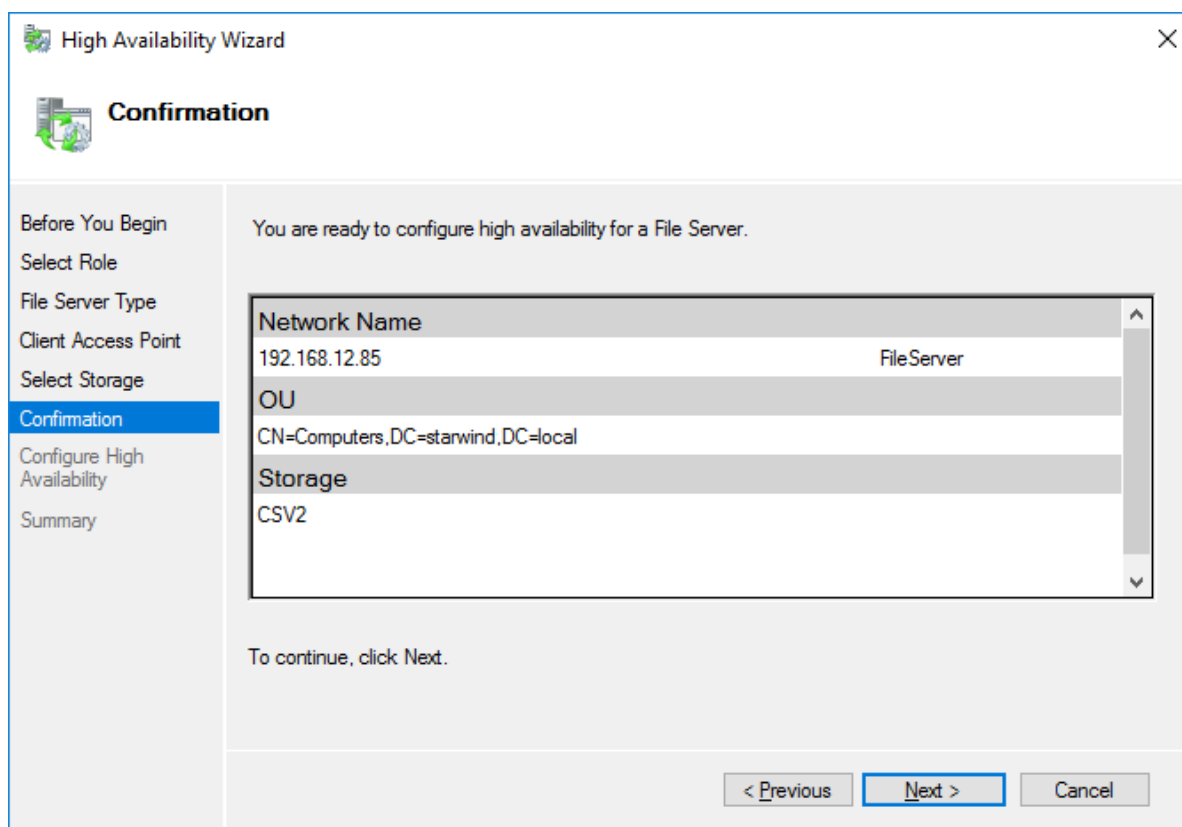
< Previous **Next >** Cancel

Click Next to continue.

6. Select the Cluster disk and click Next.

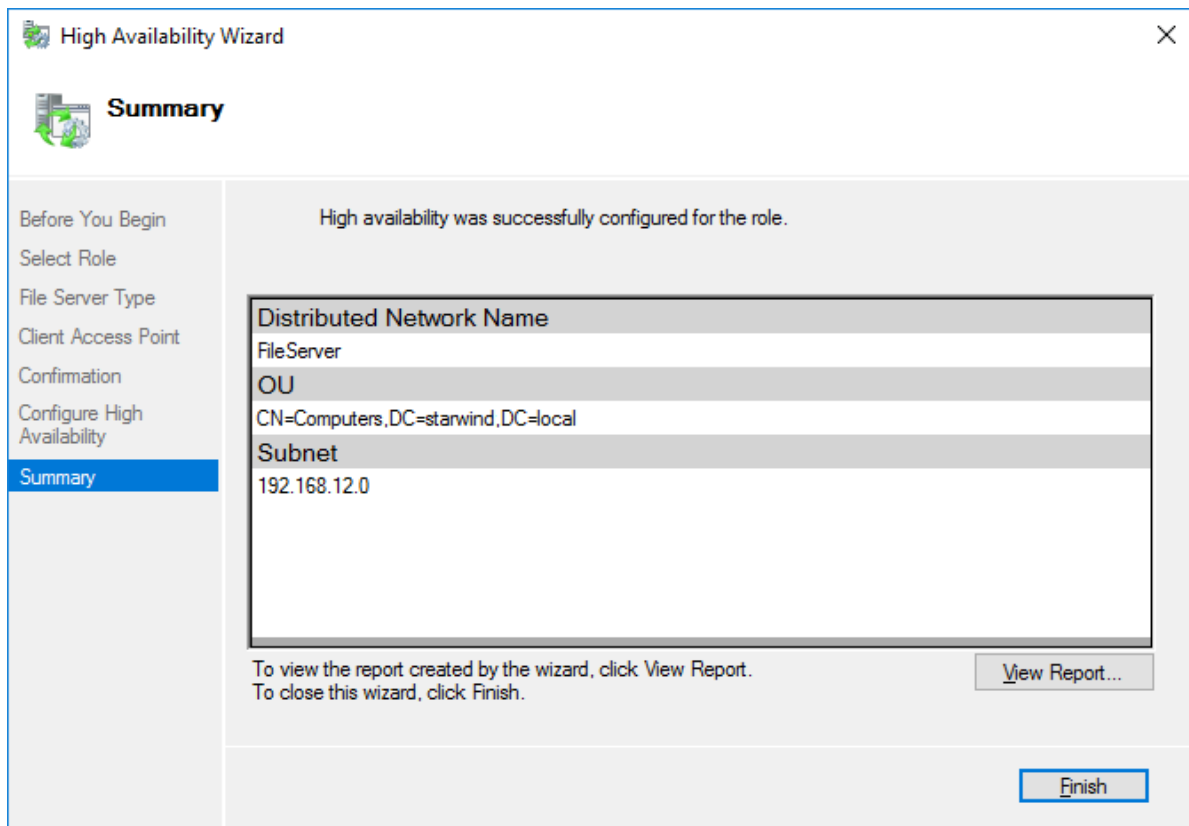


7. Check whether the specified information is correct. Click Next to proceed or Previous to change the settings.

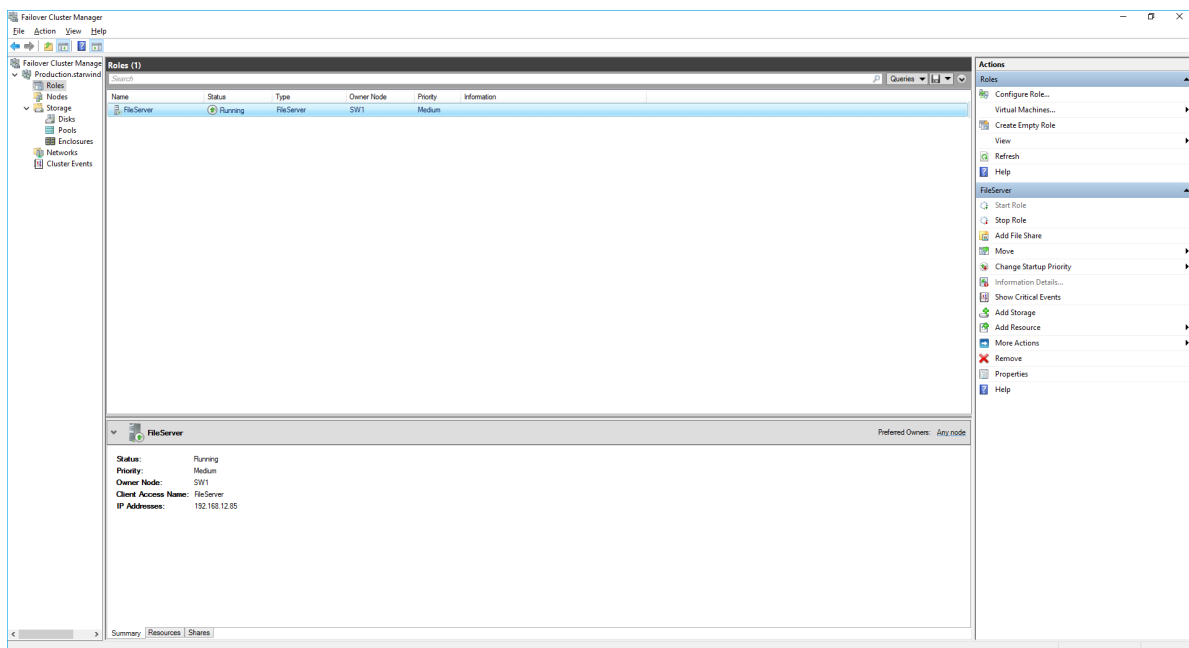


8. Once the installation has been finished successfully, the Wizard should now look like the screenshot below.

Click Finish to close the Wizard.

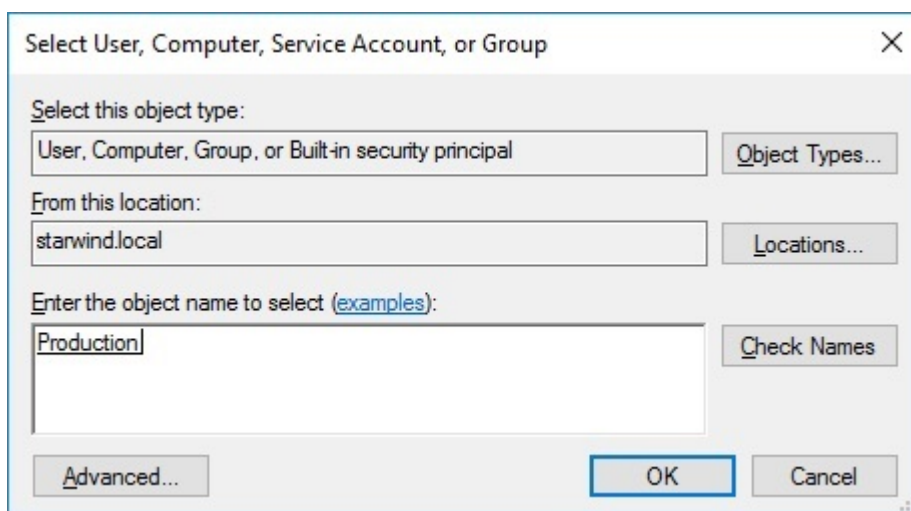


9. The newly created role should now look like the screenshot below.

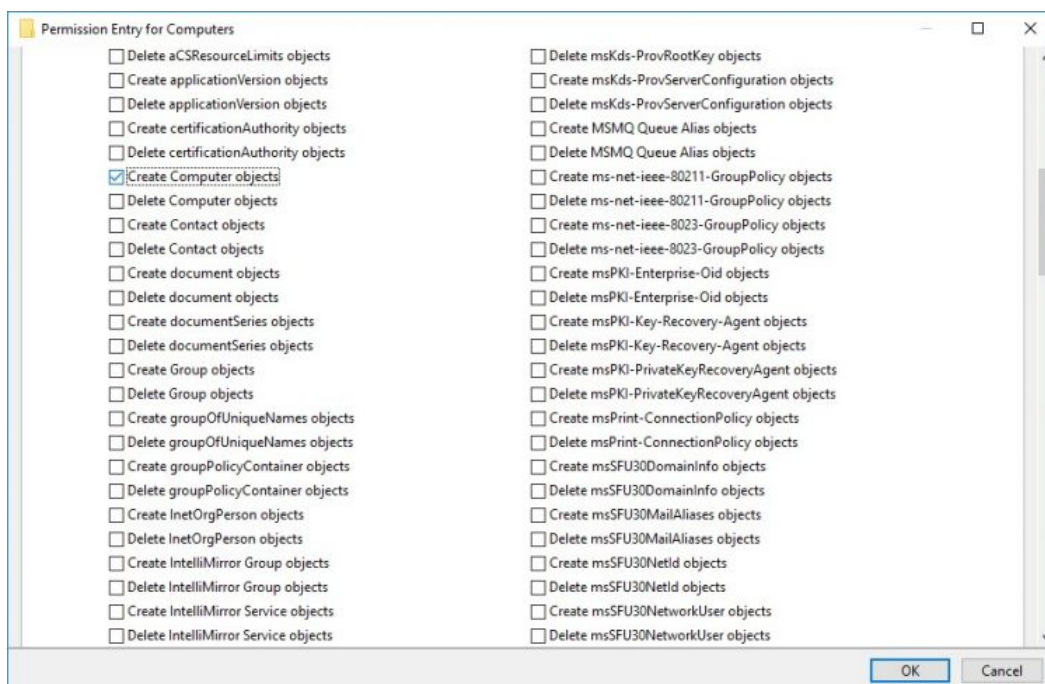


NOTE: If the role status is Failed and it is unable to Start, please, follow the next steps:

- 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

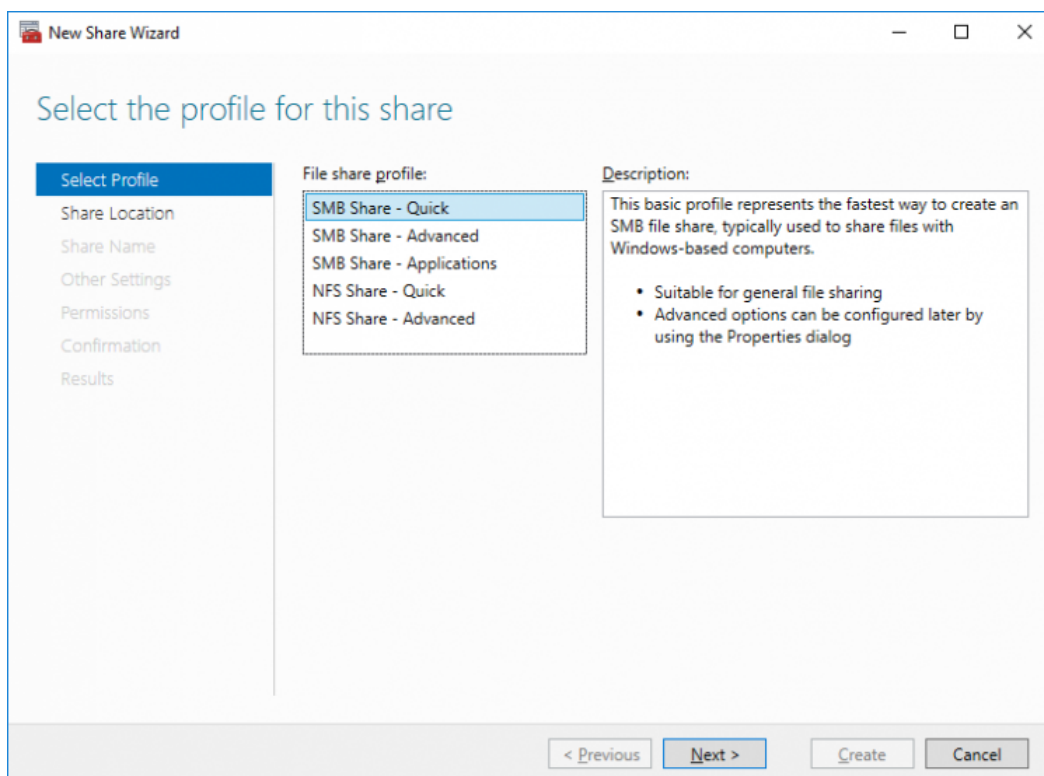


- click OK on all opened windows to confirm the changes
- open Failover Cluster Manager, right-click File Share role and click Start Role

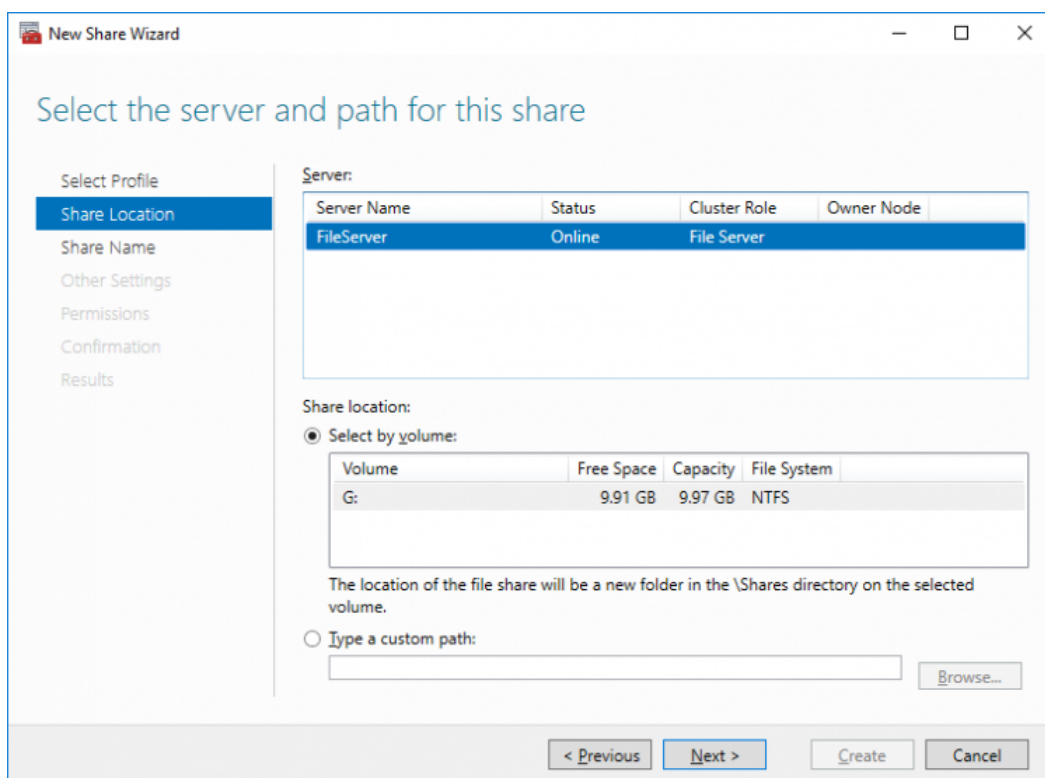
Configuring Smb File Share

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.



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	File Server	

Share location:

☒ Select by volume:

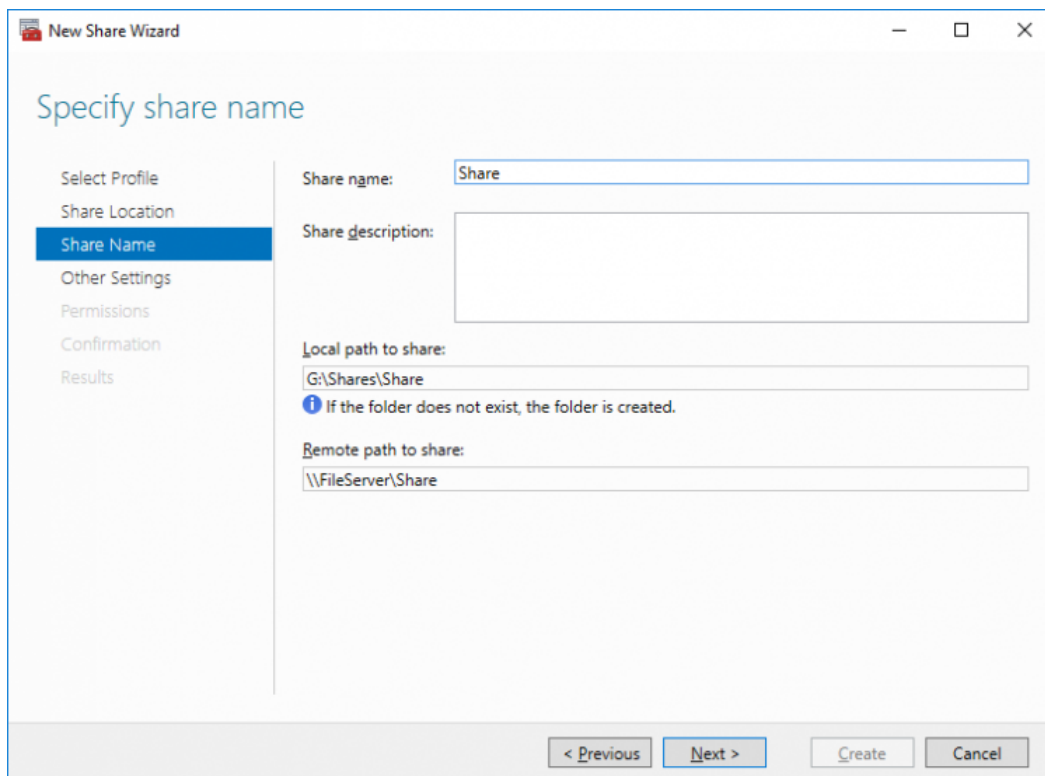
Volume	Free Space	Capacity	File System
G:	9.91 GB	9.97 GB	NTFS

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

☐ Type a custom path:

< Previous Next > Create Cancel

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



New Share Wizard

Specify share name

Select Profile

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

Share name:

Share description:

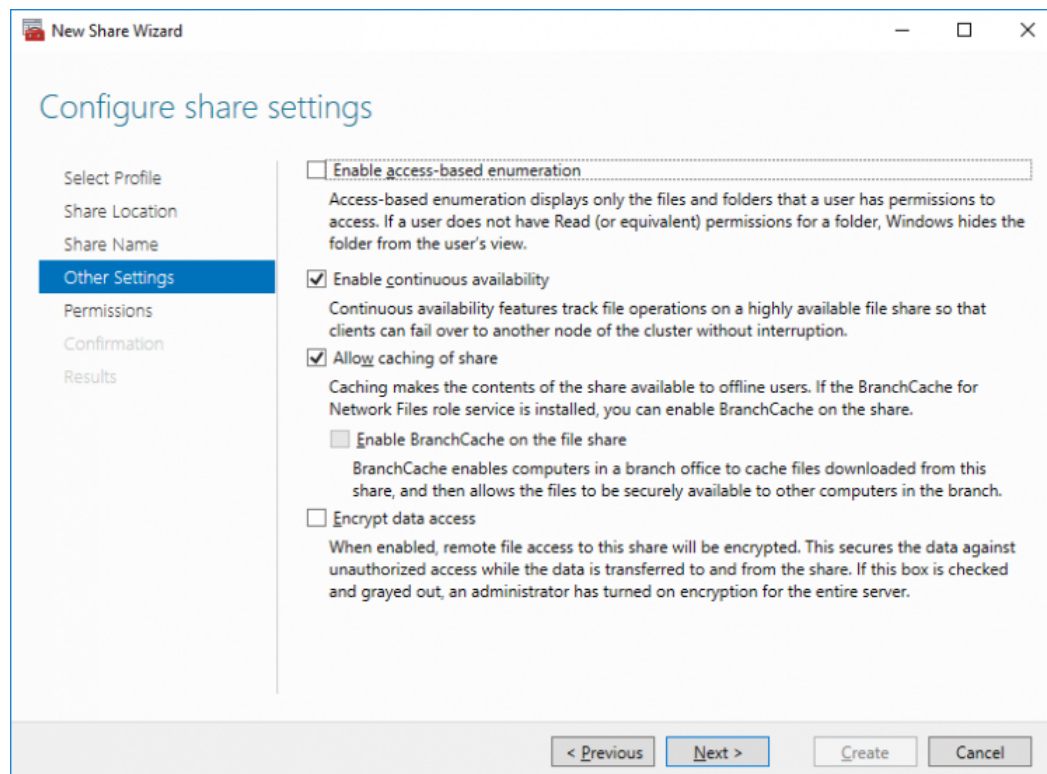
Local path to share:

Remote path to share:

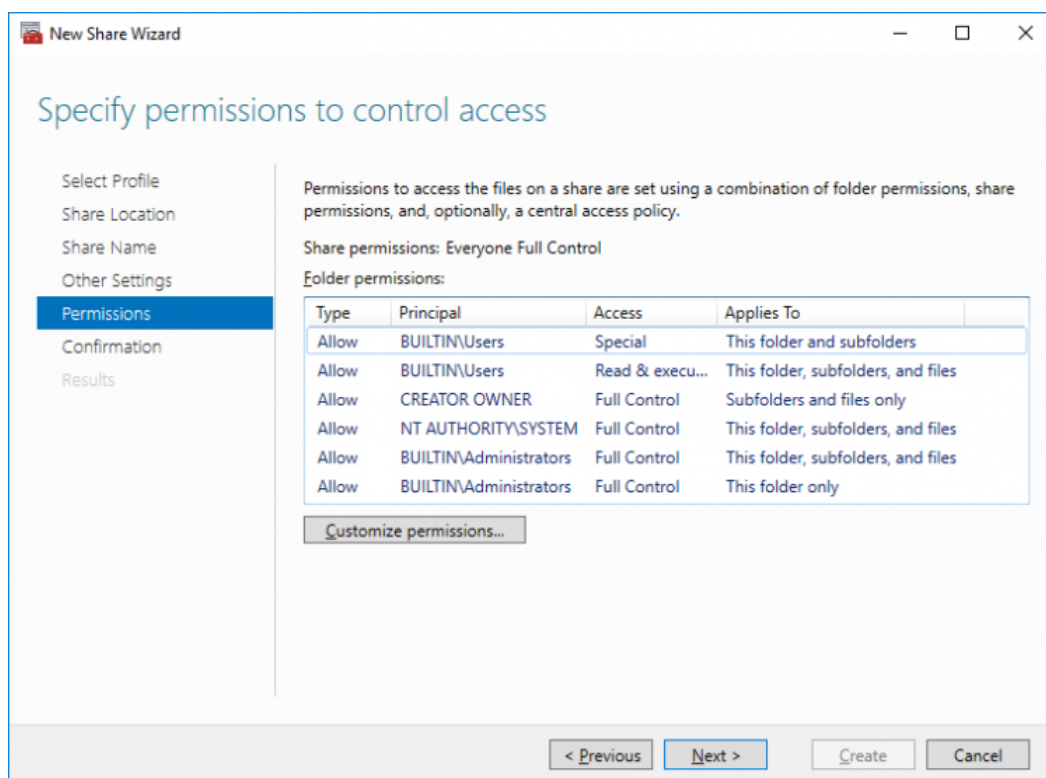
Local path to share:
G:\Shares\Share
If the folder does not exist, the folder is created.

< Previous Next > Create Cancel

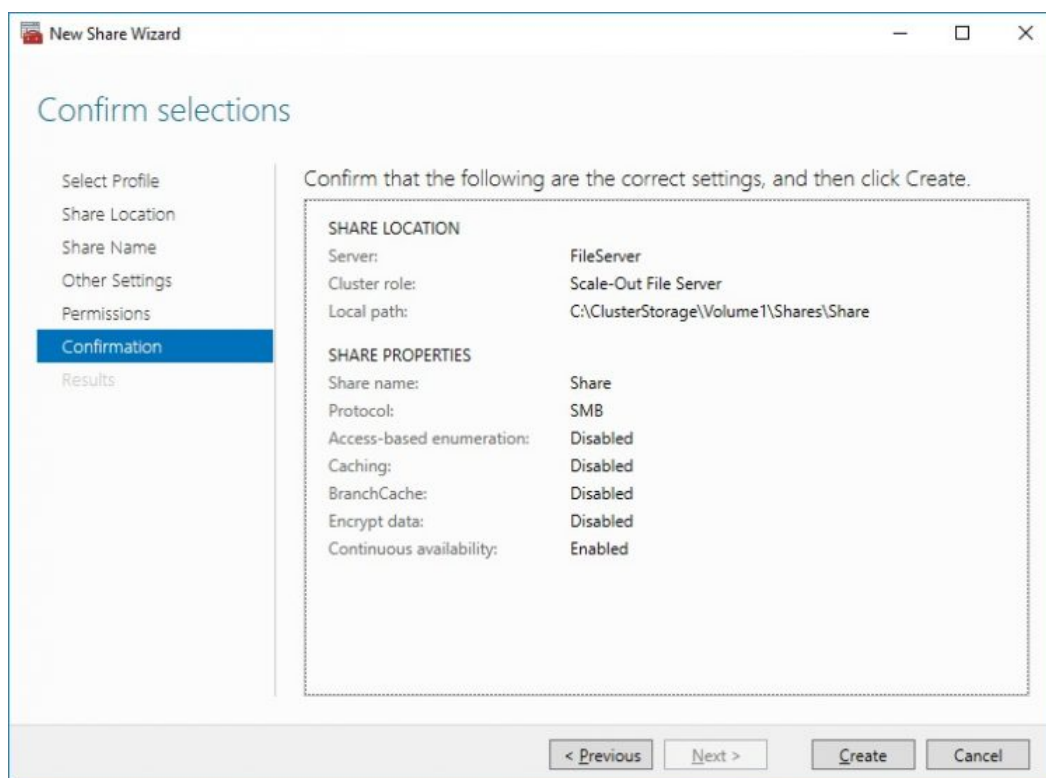
7. Make sure that the Enable Continuous Availability box is checked. Click Next to continue.



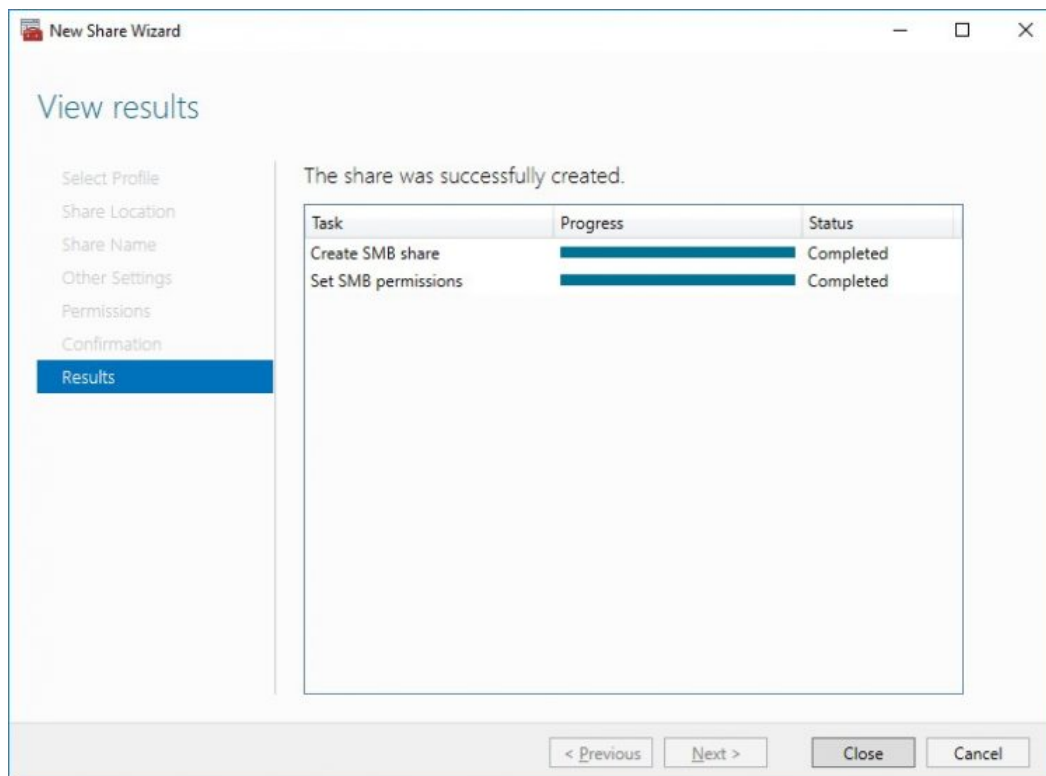
8. Specify the access permissions for the file share.



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



10. Check the summary and click Close.

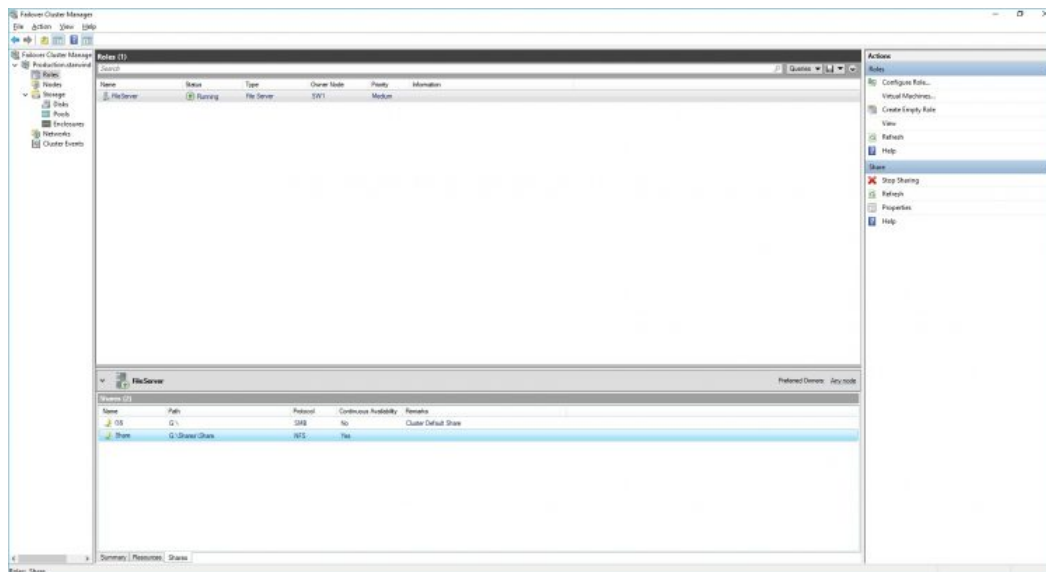


To manage created SMB File Shares

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

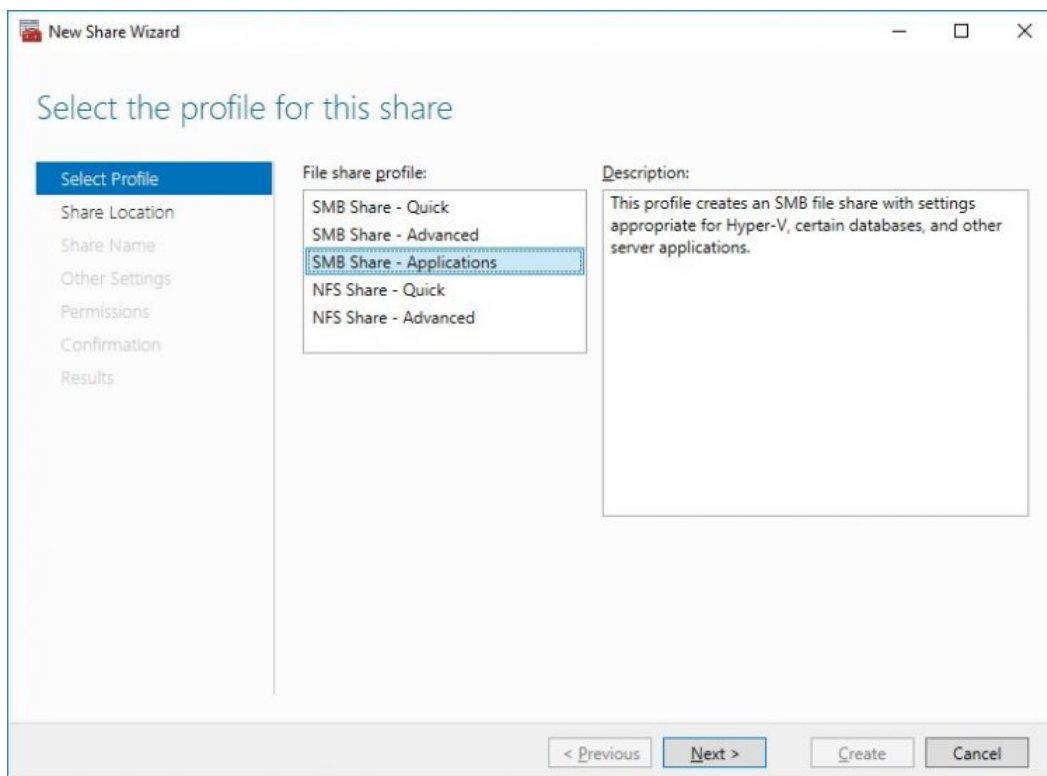
To Add NFS File Share

1. Open Failover Cluster Manager.

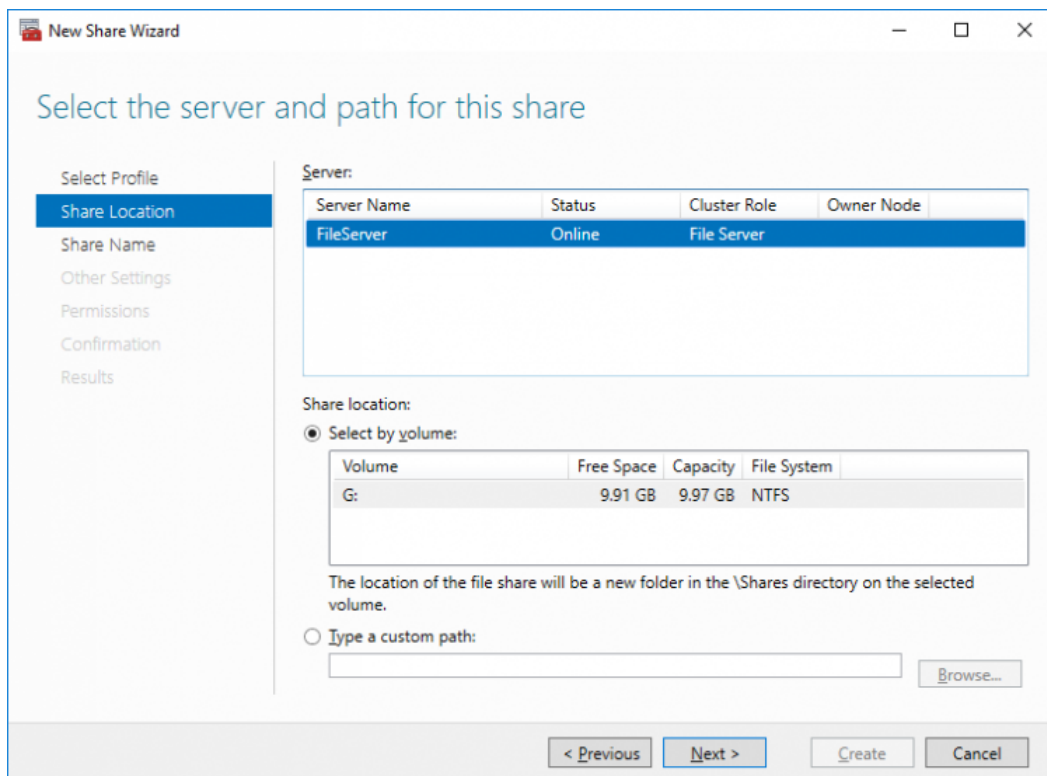
2. Expand the cluster and then click Roles.

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

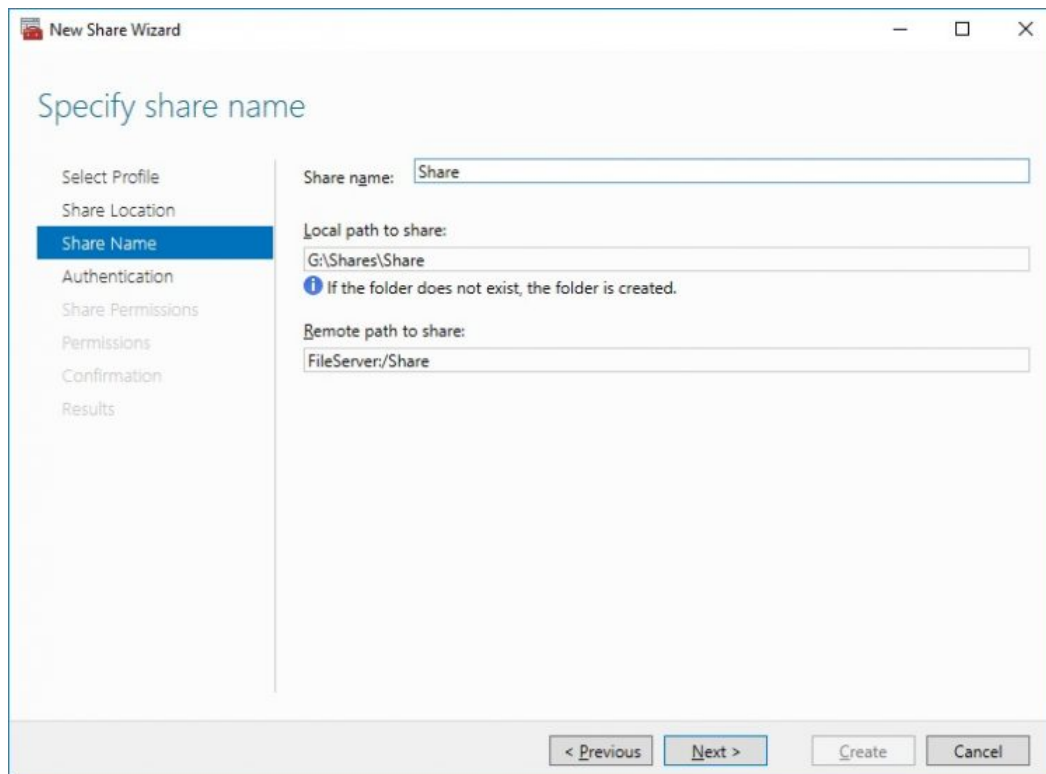
4. On the Select the profile for this share page, click NFS Share - Quick and then click Next.



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



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-hand navigation pane. The main area contains the following fields and options:

- Share name:** A text box containing the word 'Share'.
- Local path to share:** A text box containing 'G:\Shares\Share'.
- Remote path to share:** A text box containing 'FileServer/Share'.
- Information:** A blue information icon followed by the text 'If the folder does not exist, the folder is created.'

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

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

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

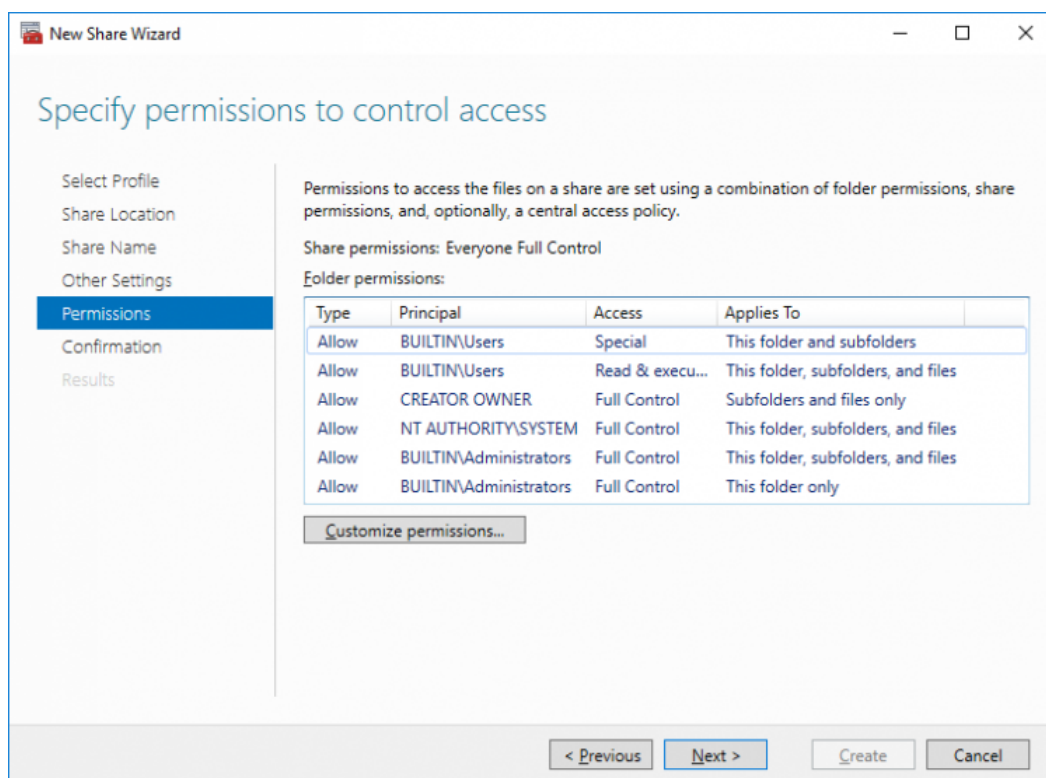
Language encoding: ANSI

Share permissions: No Access

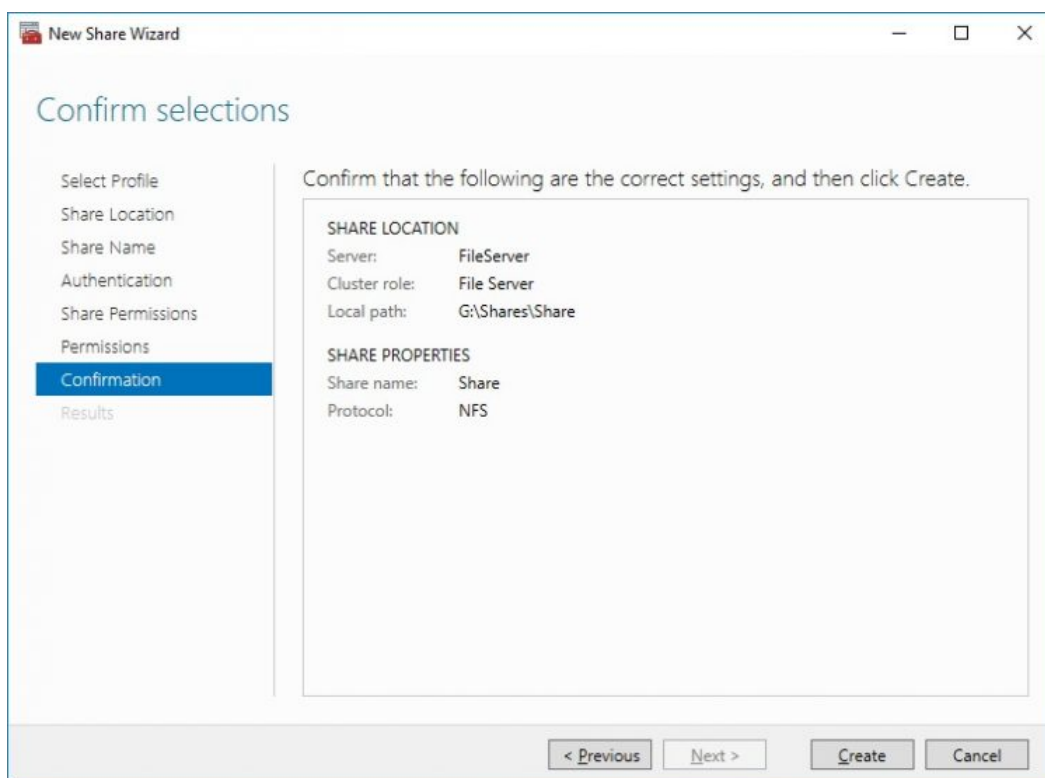
☐ Allow root access (not recommended)

Add Cancel

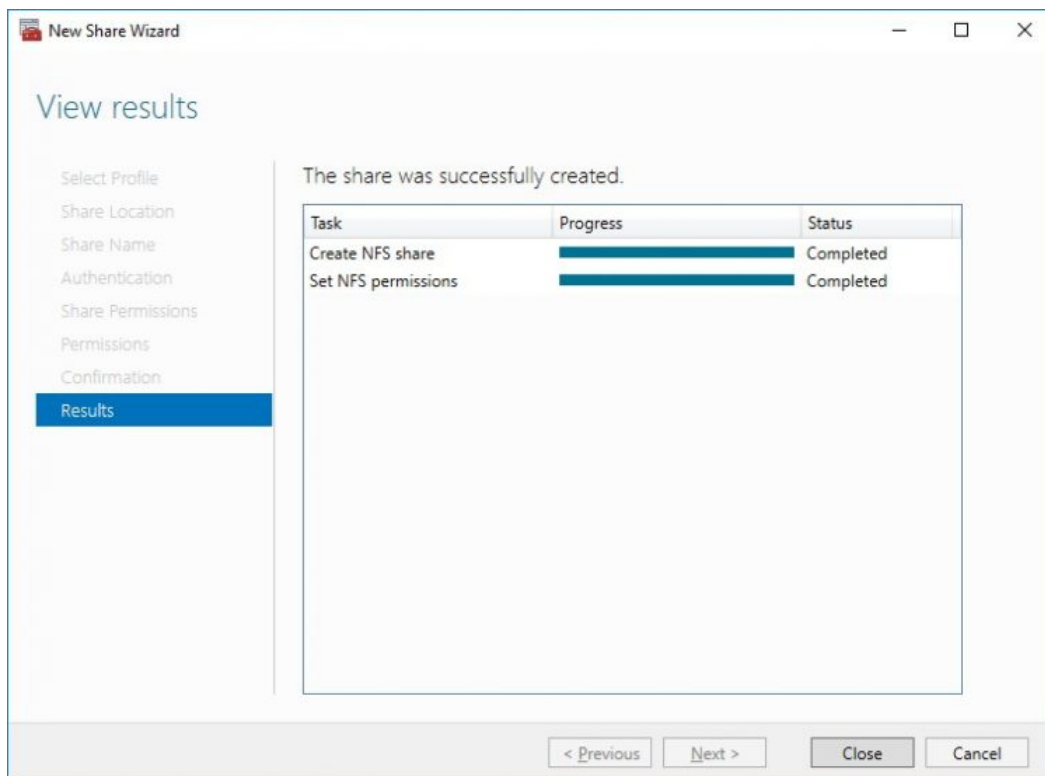
9. Specify the access permissions for the file share.



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

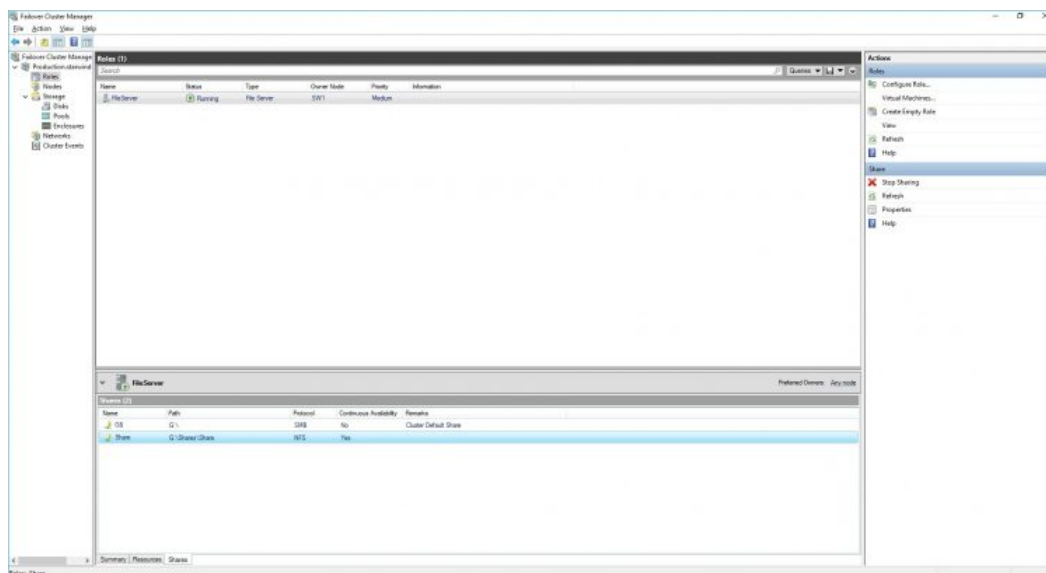


11. Check a summary and click Close to close the Wizard.



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



Contacts

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

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

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

Sales: sales@starwind.com

General Information: info@starwind.com



StarWind Software, Inc. 100 Cummings Center Suite 224-C Beverly MA 01915, USA
www.starwind.com ©2026, StarWind Software Inc. All rights reserved.