

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

2024

TECHNICAL PAPERS



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



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 (OVF Version 20230901 Version V8 (build 15260) or earlier.)

For newer versions of StarWind Virtual SAN (CVM Version 20231016 and later), please refer to this configuration guide:

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

Purpose

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

For more information about StarWind VSAN architecture and available installation options, please refer to the StarWind Virtual (VSAN) Getting Started Guide.

Audience

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

Expected result

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

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

Prerequisites



Starwind Virtual San System Requirements

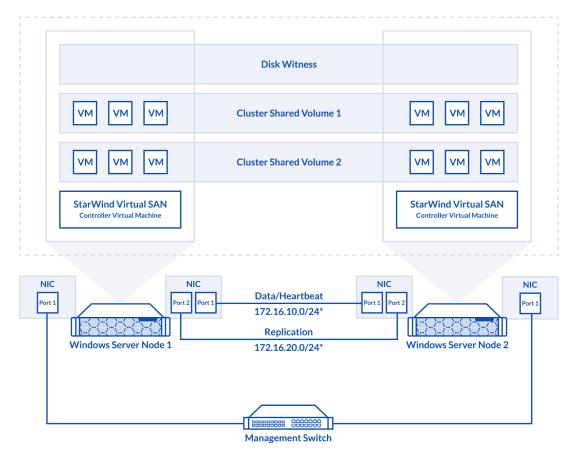
Prior to installing StarWind Virtual SAN, please make sure that the system meets the requirements, which are available via the following link: https://www.starwindsoftware.com/system-requirements

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

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

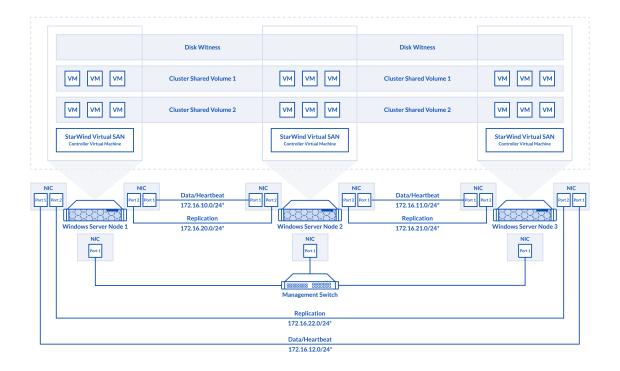
Solution Diagram

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



2-node cluster





3-node cluster

Preconfiguring cluster nodes

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

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

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

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

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



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

Virtual Switches	🚜 Virtual Switch Properties
² New virtual network switch	
MGMT	Name:
Intel(R) 82574L Gigabit Network C	MGMT
Intel(R) 82574L Gigabit Network C	Notes:
L iSCSI	,
Intel(R) 82574L Gigabit Network C	
Global Network Settings	
MAC Address Range 00-15-5D-0C-39-00 to 00-15-5D-0	Connection type
00-13-30-00-39-00 10 00-13-30-0	What do you want to connect this virtual switch to?
	External network:
	Intel(R) 82574L Gigabit Network Connection
	Allow management operating system to share this network adapter
	Enable single-root I/O virtualization (SR-IOV)
	O Internal network
	O Private network
	VLAN ID
	Enable virtual LAN identification for management operating system
	The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
	Remove SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.

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

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

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

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



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

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

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

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

mpiocpl

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



MPIO Properti	es			×
MPIO Devices	Discover Multi-Paths	DSM Install	Configuration Snapshot	t
SPC-3 comp	bliant			
Device Ha	ardware Id			
Add sup	port for iSCSI devices			
Add sup	port for SAS devices			
			Add	
Others				
Device Ha	ardware Id			
			Add	
			OK Cancel	

- 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:

📥 Add Roles and Features Wizard		- 🗆 X
Select server roles Before You Begin Installation Type	Select one or more roles to install on the selected server.	DESTINATION SERVER SW1.stanwind.local
Server Selection Server Roles Features Confirmation Results	Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server Fax Server File and Storage Services (1 of 12 installed) ✓ File and iSCSI Services ✓ File and iSCSI Services ✓ File Server BranchCache for Network Files Data Deduplication DFS Namespaces DFS Replication File Server VSS Agent Service iSCSI Target Server iSCSI Target Server iSCSI Target Server Server for NFS Work Folders ✓ Storage Service (Installed) ✓	File Server manages shared folders and enables users to access files on this computer from the network.
	< <u>P</u> revious <u>N</u> ext >	Cancel

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

File Server For General Use With Smb Share

- 1. Open Server Manager: Start -> Server Manager.
- 2. Select: Manage -> Add Roles and Features.

3. Follow the installation wizard steps to install the roles selected in the screenshot below:



🔁 Add Roles and Features Wizard		- 🗆 X
Select server roles		DESTINATION SERVER SW1.stanwind.local
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection Server Roles Features Confirmation Results	Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server File and Storage Services (1 of 12 installed) File and Storage Services (1 of 12 installed) File and Storage Services File Server BranchCache for Network Files Data Deduplication DFS Replication DFS Replication File Server WSS Agent Service iSCSI Target Server iSCSI Target Server Work Folders Work Folders Storane Service (Installed)	File Server manages shared folders and enables users to access files on this computer from the network.
	< Previous Next >	Install Cancel

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

File Server For General Use With Nfs Share

- 1. Open Server Manager: Start -> Server Manager.
- 2. Select: Manage -> Add Roles and Features.

3. Follow the installation wizard steps to install the roles selected in the screenshot below:



Add Roles and Features Wizard		- 🗆 X
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select one or more roles to install on the selected server. Roles Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server Fax Server File and Storage Services (1 of 12 installed) File and Storage Services File Server Fi	DESTINATION SERVER SW1.stanwind.local Description Server for NFS enables this computer to share files with UNIX- based computers and other computers that use the network file system (NFS) protocol.
	Data Deduplication DFS Namespaces DFS Replication File Server Resource Manager File Server VSS Agent Service iSCSI Target Server iSCSI Target Storage Provider (VDS and VSS Server for NFS Work Folders Storane Service (Installed) <	Install

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\



🖳 New Virtual Machine Wizar	d	×
🕮 Specify Name	e and Location	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Summary	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easi identify this virtual machine, such as the name of the guest operating system or workload. Name: SW1 You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server. Store the virtual machine in a different location Location: C:\SW1\ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.	
	< Previous Next > Finish Cancel	

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.



🖳 New Virtual Machine Wizar	d	×
💷 Specify Gene	ration	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Summary	 Choose the generation of this virtual machine. Generation 1 This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V. Generation 2 This virtual machine generation provides support for newer virtualization features, has UEFI-base firmware, and requires a supported 64-bit guest operating system. More a virtual machine has been created, you cannot change its generation. 	
	< Previous Next > Einish Cancel	

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 Wizar	d	×
💹 🛛 Assign Memo	σгγ	
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: 8192 MB Use Dynamic Memory for this virtual machine. 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 > Einish Cancel	

8. Choose the management network for the VM.

🖳 New Virtual Machine Wizar	d X
🛄 Configure Ne	tworking
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: MGMT
	< <u>P</u> revious <u>N</u> ext > <u>F</u> inish Cancel



9. Connect .vhdx to the VM.

🖳 New Virtual Machine Wiza	rd	×
🦉 Connect Vir	tual Hard Disk	
Before You Begin Specify Name and Location Specify Generation Assign Memory	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. O <u>C</u> reate a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk.	
Configure Networking Connect Virtual Hard Disk	Name: SW1.vhdx Location: C:\SW1\SW1\Virtual Hard Disks\ Browse	ł.
Summary	Size: 127 GB (Maximum: 64 TB) Image: Size: Use an existing virtual hard disk	
	Use this option to attach an existing VHDX virtual hard disk. Location: C:\SW1\Virtual Hard Disk\sw-vsa-hyper-v-build-15020.vhdx Browse	
	 <u>A</u>ttach 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	

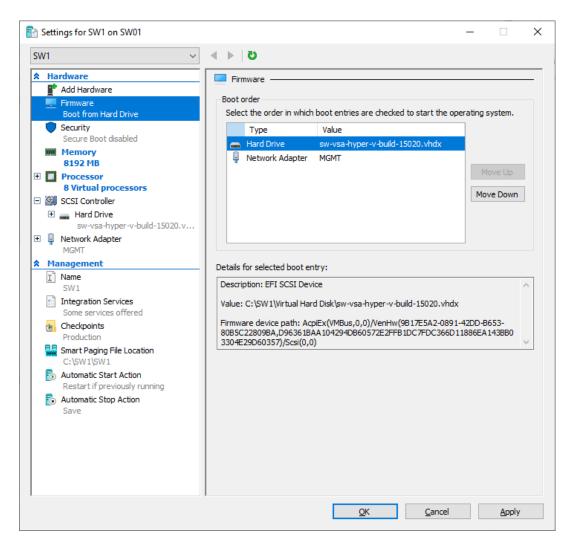
10. Review the Summary and click Finish to create the VM.



🖳 New Virtual Machine Wiza	rd	×
💴 Completing 🕯	the New Virtual Machine Wizard	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description: Name: SW1 Generation: Generation 2 Memory: 8192 MB	
Connect Virtual Hard Disk Summary	Network: MGMT Hard Disk: C:\SW1\Virtual Hard Disk\sw-vsa-hyper-v-build-15020.vhdx (VHDX, dynamically expansion) To create the virtual machine and close the wizard, click Finish.	and >
	< Previous Next > Einish Cancel	

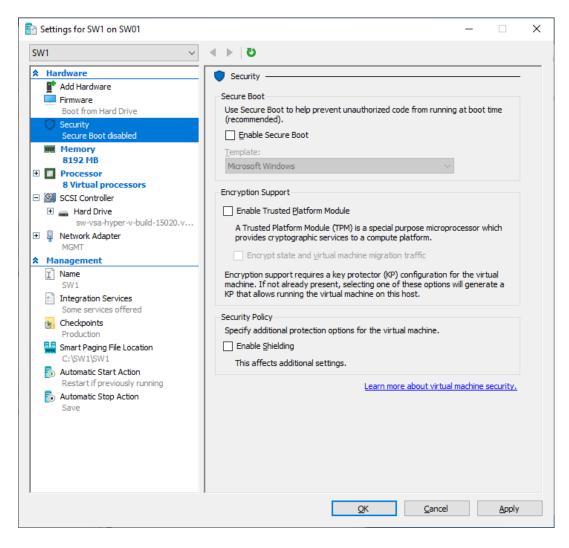
11. Right-click on the VM and choose Settings. Open Firmware and move the option Hard Drive to the first place in the list.





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





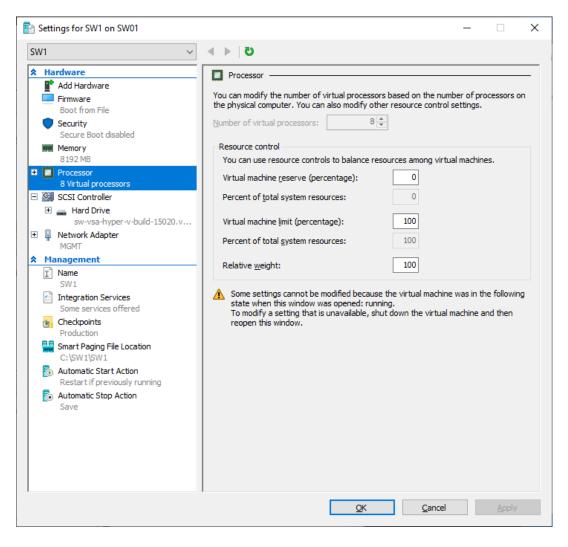
13. Go to Memory and move the slider for Memory weight to High.



Settings for SW1 on SW01				-		>
SW1 ~	G ∢ ▶					
A Hardware	Memory					
Add Hardware	Specify the amount of me	mory that this virtual m	achine can use			
Firmware Boot from File			denine can use.			
Security	RAM:	8192 MB				
Secure Boot disabled	Dynamic Memory					
Memory 8192 MB	You can allow the amou dynamically within the r		to this virtual machin	ne to cha	ange	
 Processor 8 Virtual processors 	Enable Dynamic Me	mory				
🖃 🔄 SCSI Controller	Minimum RAM:	512 MB				
🛨 🚃 Hard Drive						
sw-vsa-hyper-v-build-15020.v	Maximum RAM:	1048576 MB				
 Wetwork Adapter MGMT Management 	Specify the percentage Hyper-V uses the perce amount of memory for	ntage and the current				
Name SW1	Memory <u>b</u> uffer:	20 - %				
Integration Services Some services offered	Memory weight					
Checkpoints Production	Specify how to prioritize compared to other virtu			achine		
Smart Paging File Location C:\SW1\SW1	Low		High			
Automatic Start Action Restart if previously running	G Specifying a lower	setting for this virtual				
Automatic Stop Action Save		er virtual machines are	-			
	state when this wind	t be modified because t ow was opened: runnin hat is unavailable, shut	ıg.			Ig
	,	<u>О</u> К	<u>C</u> ancel			

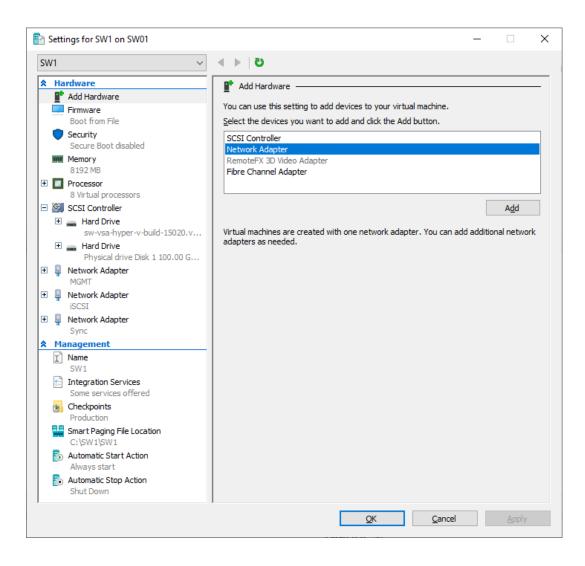
14. Go to Processor and assign 8 vCPUs to the VM.





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



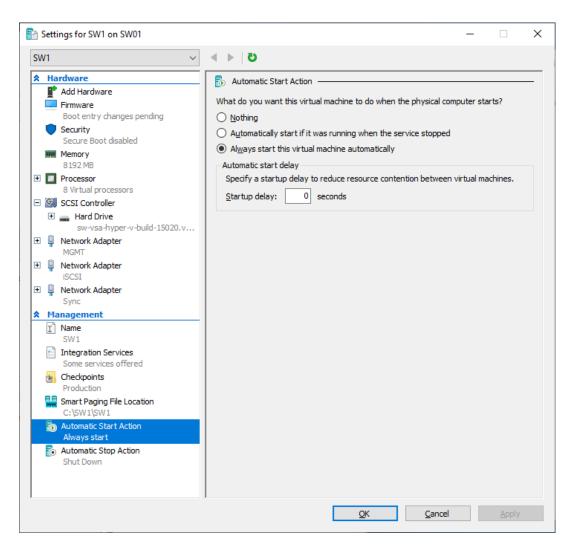




音 Settings for SW1 on SW01	- 🗆 X
SW1 ~	د ⊳ 5
 Hardware Add Hardware Firmware Boot entry changes pending Security Secure Boot disabled Memory 8 192 MB Processor 8 Virtual processors SCSI Controller Hard Drive sw-vsa-hyper-v-build-15020.v Network Adapter MGMT Network Adapter iSCSI Network Adapter Sync Management Name SW1 Integration Services Some services offered 	Network Adapter Specify the configuration of the network adapter or remove the network adapter. Virtual gwitch: Sync VLAN ID Enable girtual LAN identification The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter. 2 Bandwidth Management Enable bandwidth management Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth are measured in Megabits per second. Minimum bandwidth: 0 Mbps To leave the minimum or maximum unrestricted, specify 0 as the value.
 Checkpoints Production Smart Paging File Location C:\SW1\SW1 Automatic Start Action Always start Automatic Stop Action Save 	
	OK Cancel Apply

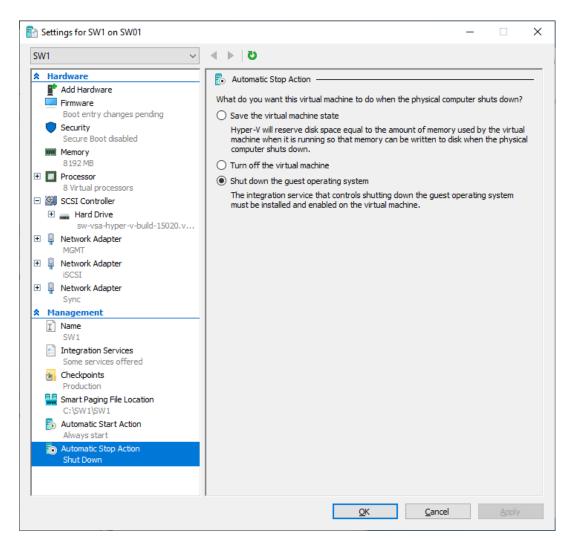
16. Configure Automatic Start and Stop actions, so the VM will always start automatically.





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).

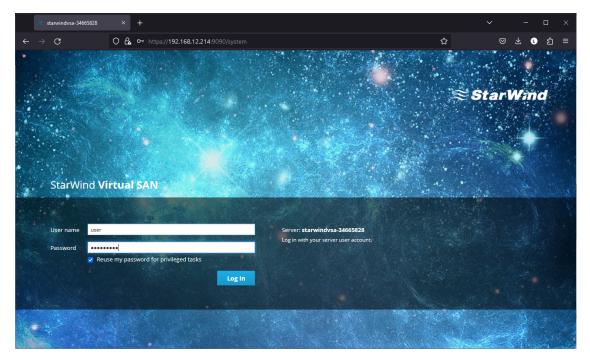


🕎 SW1 on SW01 - V	irtual Machine Conne	ection	
File Action M	fedia Clipboard 1	View Help	
🖿 🛛 🕲 🕲 🕲) III IÞ 🔂 D	1 <u>1</u>	
Codename: Siler			e https://192.168.12.214:9896/
Hint: Num Lock			
starwindusa-346	65828 login:		

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.



accounts - starwindvs -	a-346658.× +			~	-		×
$\leftarrow \rightarrow \mathbf{G}$	O 🔓 https://192.168.12.214:9090/us		☆	Ø	⊻ เ	பி	≡
STARWIND VIRTUAL SAN						1 u	ser 🗸
🗐 starwindvsa-34	Accounts > user	t Password					
System	user	Old Password		Termina	te Session	Delet	te
Logs	Full Name user	New Password					
Storage	User Name user						
Networking	Roles 🗹 Server Administrator						
Accounts	Last Login Invalid Date		Cancel Set				
Services	Access 🔲 Lock Account	Never lock account	_				
Terminal	Password Set Password Force Change	e Never expire password					
	Authorized Public SSH Keys					ľ	÷
	There are no authorized public keys for this a	account.					

5. On the left sidebar, click Networking.

📚 Networking - starwind	vsa-3466:× +			∽ - □ ×
$\leftarrow \rightarrow G$	O 🔒 https://192.168.12.2	214:9090/network	☆	⊠ ± 🕻 දා =
STARWIND VIRTUAL SAN				🔒 Privileged 💄 user 🗸
🗐 starwindvsa-34	Kbps Sending		Kbps Receiving	
System Logs	400		400	
Storage	0 20:32	20:33 20:34 20:35	20:32 20:33	20:34 20:35
Networking	Firewall			0
Accounts	0 Active Rules			
Services	Interfaces		Add Bond	Add Team Add Bridge Add VLAN
Terminal	Name	IP Address	Sending	Receiving
	eth0	192.168.12.214/23	8.36 Kbps	8.46 Kbps
	eth1	172.16.10.10/24	0 bps	14.8 Kbps
	eth2	172.16.20.10/24	3.23 Kbps	11.4 Kbps
	Networking Logs			
	May 8, 2023			
		57.4612] audit: op="checkpoint-destroy" arg="/or		
	20:35 <info> [16835673</info>	57.4607] checkpoint[0x561a96b655b0]: destroy /or	rg/freedesktop/NetworkManager/Checkpoint/4	NetworkManager

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).



📚 Networking - starwin	dvsa-3466: × +			✓ - □ ×
$\leftarrow \ \rightarrow \ \mathbf{C}$	O A https://192.168.12.214:90		☆	ල ් € ව් ≡
STARWIND VIRTUAL SAN				🔓 Privileged 💄 user 🗸
🗐 starwindvsa-34	Networking → eth0	IPv4 Settings		
System	Kbps Sending	Addresses	Automatic (DHCP) v	
Logs Storage	400	DNS	Automatic (DHCP) Link local + Manual	
Networking	0 20:21 20:22	DNS Search Domains		20:23 20:24 20:25
Accounts Services	eth0 hv_netvsc 00:15:5D:0C:39:00	Routes	Automatic 🗸 +	
Terminal	Status 192.168.12.214/23, fe80:0:0 Carrier 1 Gbps General I Connect automatically			
	IPv4 Automatic (DHCP)		Cancel Apply	
	IPv6 Automatic MTU Automatic			

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

Networking - starwin	ndvsa-3466°× +			~	-	o ×
$\leftarrow \ \rightarrow \ \mathbf{G}$	O 🔒 https://192.16	8.12.214:9090/network		☆	◎★○	ເ ປ ≡
STARWIND VIRTUAL SAN						ed 💄 user 🗸
starwindvsa-34 System Logs Storage Networking Accounts	Klapps Sending	2033 2034 2	κερε Receiving 500 000 000 000 000 000 2032	2033 2034	20:35	
Services						
Terminal	Interfaces				Add Bridge	Add VLAN
	Name eth0	IP Address 192.168.12.214/23	Sending 8.36 Kbps	Receiv 8.46 K	-	
	eth1	172.16.10.10/24	0 bps	14.8 K	ops	
	eth2	172.16.20.10/24	3.23 Kbps	11.4 K	ops	
	Networking Logs May 8, 2023					
			-destroy" arg="/org/freedesktop/NetworkManager/C 55b0]: destroy /org/freedesktop/NetworkManager/C		kManager kManager	

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



📚 Networking - starwing	Avsa-3466/ × +		✓ – □ ×
$\leftarrow \ \rightarrow \ \mathbf{G}$	O A https://192.168.12.214:9090/network#/eth1	☆	ල ් € ව =
STARWIND VIRTUAL SAN			🔒 Privileged 💄 user 🗸
🗐 starwindvsa-34	Networking > eth1		
System	Kbps Sending Kbps Receiv	ving	
Logs			
Storage	400 400		
Networking	0 20:34 20:35 20:36 20:37 20:38	20:34 20:35	20:36 20:37 20:38
Accounts	eth1 hv_netvsc 00:15:5D:00:39:03		
Services	Status 172.16.10.10/24, fe80:0:0:0:5804:44b8:3955:e9bc/64		
Terminal	Carrier 1 Gbps		
Terminal	General 🗸 Connect automatically		
	IPv4 Address 172.16.10.10/24		
	IPv6 Automatic MTU 9000		

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:



📚 System - starwindvsa	-34665828 × +					~	-		×
$\leftarrow \ \rightarrow \ \mathbf{G}$	O 🔓 https://192.1	.168.12.214:9090/system			☆		⊠ ± €	பி	≡
STARWIND VIRTUAL SAN								1 u	iser ~
🗐 starwindvsa-34	Hardware Micro Asset Tag 4089	Channes Hand Manual	e of 9 CDU correct						
System	Machine ID fa6b	Pretty Host Name	sw1						
Logs	Operating System Cent	tOS Linux 7 (Co Real Host Name	sw1			20:36	20:37		
Storage	Secure Shell Keys Show	w fingerprints							
Networking	Host Name starv	windvsa-34665							
Accounts	Domain Join E				Cancel Change				
Services	System Time 2023 Power Options Res		0					_	
Terminal	Performance Profile none	ne	20:33 KiB/s Disk I/O	20:34	20:35	20:36	20:37		
			192						
			64						
			20:33	20:34	20:35	20:36	20:37		
			Mbps Network Traffic						
			800						
			400		Annelika	<u>h h</u>		• • • •	

13. Change System time and NTP settings if required:

≈ System - starwindvs	iar-34665828 × +		~ - • ×
$\leftarrow \rightarrow \mathbf{G}$	O 🔒 https://192.168.12.214:9090/system	☆	ල ± i දා ≡
STARWIND VIRTUAL SAN			🔒 Privileged 💄 user 🗸
🖹 starwindvsa-34 System	Hardware Microsoft Corporation Virtual Machine Charge System Time Asset Tag. 4089-0074-9445-9761-6594-9417-84 Machine ID Fa6b289621d243798a9F5d8abc790 Operating System CentOS Linux 7 (Core) America/New York		
Logs Storage Networking	Secure Shell Keys Show fingerprints Host Name starwindvsa-34665828 Cancel Change	20:36	20:37 20:38
Accounts Services	Domain Join Domain System Time 2023-05-08 13:38 Power Options Restart V 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	_	
Terminal	Performance Profile none KBIs Disk I/O	20:36	20.37 20.38
	528 0 2034 Mtes Network Traffic	20:36	20:37 20:38
			Ma

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.

📸 Settings for SW1 on SW01		– 🗆 X
SW1 ~	ن (♦	
Hardware Add Hardware Firmware Boot entry changes pending Security Secure boot disabled	Hard Drive — You can change how this virtual hard disk is a operating system is installed on this disk, cha virtual machine from starting. Controller:	
Memory	SCSI Controller	1 (in use) 🗸 🗸
8192 MB Processor 8 Virtual processors SCSI Controller	Media You can compact, convert, expand, merge by editing the associated file. Specify the	
Hard Drive sw-vsa-hyper-v-build-15020.v Hard Drive	O <u>V</u> irtual hard disk:	
Physical drive Disk 1 100.0	<u>N</u> ew <u>E</u>	dit <u>I</u> nspect <u>B</u> rowse
Network Adapter MGMT	Physical hard disk:	• ••
Network Adapter ISCSI	Disk 1 100.00 GB Bus 0 Lun 0 Target	
Vetwork Adapter Sync		It to use is not listed, make sure that the ent on the physical computer to manage
A Management	To remove the virtual hard disk, click Remove	 This disconnects the disk but does not
I Name SW1	delete the associated file.	
Some services		<u>R</u> emove
Checkpoints Production		
Smart Paging File Location C:\SW1\SW1		
Automatic Start Action Always start		
Automatic Stop Action Shut Down		
	<u>O</u> K	<u>C</u> ancel <u>Apply</u>



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.

📚 Storage - starwindvsa-34	≋ Storage - starwindvsa-34655828 × +										~		-		×
$\leftarrow \rightarrow G$	O 🔒 https://192.168	12.214:9090/storage							☆		C	9	¥ (ර	≡
STARWIND VIRTUAL SAN														1 1	user ~
🗐 starwindvsa-34	KiB/s Reading		KiB/s V 96	Vriting					RAID Dev		rage set i		PAID		•
System	64 32		64						Volume		rage set i	ip as i	KAID		+
Logs Storage	0 20:37 20:38	20:39 20:40	20:41	20:37	20:38	20:39	20:40 2	0:41		centos 14.8 GiB					
Networking	Filesystems														
Accounts	Name	Mount Point	Size						VDO Dev	ices					+
Services	/dev/centos/root	/				2.9	92 / 13.2 GiB			No sto	rage set i	up as l	VDO		
Terminal	/dev/sda2	/boot				235	5 / 1014 MiB		Drives						
	Storage Logs								R	Msft Virtu 16 GiB Ha R: 0 B/s	ard Disk		4806		
	May 8, 2023														
		y: object class 'UDis		-		_	_		2	VMware 100 GiB H			00c2		
		y: object class 'UDis y: object class 'UDis				2	_			R: 0 B/s	W: 0 B/	s			
		y: object class 'UDis				2									
		y: object class 'UDis													
	20:40 g_object_notif	y: object class 'UDis	ksObjectSke	eleton' ud	isksd										
	20:40 Loading module	libudisks2_lvm2.so		ud	isksd										

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

📚 Storage - starwindvsa	34665828 × +				~	-		×
$\leftarrow \ \rightarrow \ \mathbf{G}$	O A https://192.168.12.214:90	90/storage#/sdb		☆	\bigtriangledown	⊻ เ	பி	≡
STARWIND VIRTUAL SAN							💄 us	er 🗸
🗐 starwindvsa-34	Storage > VMware Virtual disk (6000c292	22debd1cf1f227ad Format Disk /						
System		Erase [Don't overwrite existing data	~				
Logs	Model Virtual disk	Partitioning C	compatible with modern system and hard disks > 2TB (GPT)	~				
Storage	Serial Number 6000c2922debd1							
Networking	World Wide Name 0x6000c2922deb		Formatting a disk	will erase all data on it.				
Accounts	Capacity 100 GiB, 107 GB,			Cancel Format				
Services	Device File /dev/sdb							
Terminal								
	Content				Creat	e Partition	n Table	
	> 100 GiB Unrecognized Data		/dev	//sdb				

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



Storage - starwindvsa-34665828 × +					~		-		×
$\leftarrow \rightarrow \mathbf{G}$	O 🔓 https://192.168.12.214:90	190/storage#/sdb		☆		◙	⊻ เ	பி	≡
STARWIND VIRTUAL SAN								1 u	iser 🗸
🗟 starwindvsa-34	Storage > VMware Virtual disk (6000c29)	22debd1cf1f227ad00 Create Partitio							
System Logs Storage Networking Accounts Services Terminal	Drive Model Virtual disk Firmware Version 2.0 Serial Number 6000c2922debd World Wide Name 0x6000c2922deb Gapacity 100 GiB, 107 Gs Device File /dev/sdb	Type Name Mounting Mount Point Mount Options	Don't overwrite existing data XFS - Recommended default disk1 Encrypt data Custom /mnt/disk1 Mount read only Custom mount options noatime	100 GiB v v v		Cre	ate Partitio		

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

📚 Storage - starwindvsa-	44665828 × +		~ - ¤ ×
$\leftarrow \rightarrow C$	O ♣ https://192.168.12.214:9090/storage#/sdb	ن ک	ල ± 0 දා ≡
STARWIND VIRTUAL SAN			🔒 Privileged 💄 user 🗸
starwindvsa-34	Storage > VMware Virtual disk (6000c2922debd1cf1f227ad001f11438)		
System	Drive		
Logs	Model Virtual disk Firmware Version 2.0		
Storage	Serial Number 6000c2922debd1cf1f227ad001f11438		
Networking	World Wide Name 0x6000c2922debd1cf1f227ad001f11438		
Accounts	Capacity 100 GiB, 107 GB, 107374182400 bytes Device File /dev/sdb		
Services			
Terminal	Content		Create Partition Table
	✓ 100 GiB xfs File System	/dev/sdb1	
	Partition Filesystem		Delete Format
	Name disk1 Mount Point /mnt/disk1 Mount Options noatime Used -		



Configuring Starwind Management Console

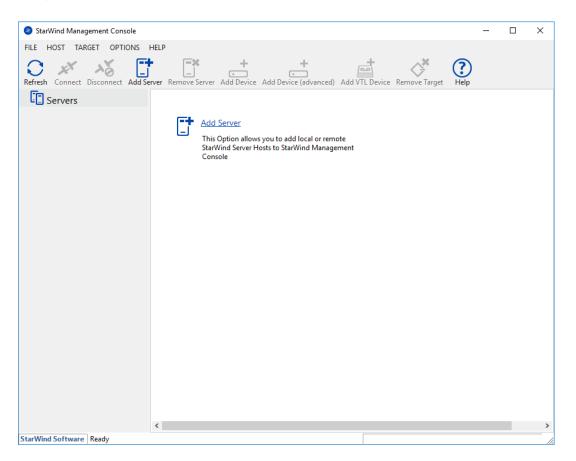
1. Install StarWind Management Console on each server or on a separate workstation with Windows OS (Windows 7 or higher, Windows Server 2008 R2 and higher) using the installer available here.

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.



Add new StarWind Server				×
Host:	192. 168. 12. 10		: 3261	
Advanced >>		OK	Ca	ncel

- 5. Select the server and click Connect.
- 6. Click Apply Key... on the pop-up window.

StarWind Management Console					
IF FF 00 BF 4D A3 EE D CC1	StarWind Server Activation				
	Apply License Key, could be Time-limited Trial Key, free Version Key or Commercial License Key delivered with Purchase				
	Request free Version Key <u>Here</u> .				
	Close Apply Key				

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	
	F
InstallLicense.ps1 X	<u></u>
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>	
	>
Ln 1 Col 1	100%

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 Devices

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

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



			?	×
\leftarrow	Add [Device Wizard		
	Select I	Device Type you want to create or export as iSCSI Target		
	۲	Hard Disk Device		
	0	Tape Device		
	0	Optical Disc Drive		
		<u>N</u> ext	Car	ncel

3. Select Virtual Disk.



			?	×
←	Add [Device Wizard		
	Select I	Disk Device Type		
	۲	Virtual Disk		
		Virtual Disk stores User Data in File		
	0	Physical Disk		
		Export existing physical Disk as iSCSI Target		
	0	RAM Disk		
		Virtual Disk with Memory Storage		
		Next	Can	cel

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



			?	×
←	Add Device Wiza	rd		
	Virtual Disk Loo	ation		
	Create a New	/irtual Disk		
	Name:	<pre><device name=""></device></pre>]	
	Location:	My Computer\D\		
	Size:	<size> GB ~</size>		
	OUse an Existing	Virtual Disk		
	Location:	~		
	Read-On	ly Mode		
		Next	Cano	cel
		Next	Cano	:el

5. Select the Thick provisioned disk type and block size.

NOTE: Use 4096 sector size for targets, connected on Windows-based systems and 512 bytes sector size for targets, connected on Linux-based systems (ESXi/Xen/KVM).

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



			?	×
←	Add De	vice Wizard		
	Specify I	Device RAM Cache Parameters		
	Mode			
	0	Write-Back Writes are performed asynchronously, actual Writes to Disk are delayed, Read are cached	S	
	0	Write-Through Writes are performed synchronously, Reads are cached		
	۲	N/A Reads and Writes are not cached		
	Set	1aximum available Size		
	Size:	128 MB ~		
		<u>N</u> ext	Can	cel

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



		?	×
←	Add Device Wizard		
	Target Parameters		
	Choose a Target Attachment Method		_
	Create new Target	~	
	Target Alias		_
	<target alias="" name=""></target>		
	Target Name		
	iqn.2008-08.com.starwindsoftware:sw1- <target alias="" name=""></target>		
	Allow multiple concurrent iSCSI Connections		
	<u>N</u> ext	Car	ncel

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



	?)	<
←	Add Device Wizard	
	Creation Page	
	Press "Create" to add new Device and attach it to new Target	
	Progress	
	Creating Device Folder	
	Creating Image File	
	Creating Header	
	Creating Device	
	Creating Target and attaching Device	
		_
	Create Cancel	

9. Click Close to finish the device creation.

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

Select The Required Replication Mode

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



Synchronous "Two-Way" Replication

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

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

😴 Replication Manager for imagefile1	?	×
Refresh Add Replica Remove Replica		
Replication Partner		
Click to add replication partner		
PROPERTIES		
Host Name		
Target Name		
Mode		
Priority		
Synchronization Status		
Synchronization Channel		
	Clos	e .

3. Select Synchronous "Two-Way" replication as a replication mode.



		?	×
~	Replication Wizard		
	Replication Mode		
	Synchronous "Two-Way" Replication Replication Partner must be connected to Client as Source Device as well, MPIO or must be enabled, needs dedicated high Performance Network Connection for Synchronization.	n Client	
	Witness Node Witness node doesn't contain user data. In case when Node Majority policy is set Synchronous replication device and there are two storage nodes, Witness Node m added to cluster to make number of nodes odd number and enable proper function Node Majority policy.	ust be	
	Next	Canc	el

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

Selecting The Failover Strategy

StarWind provides 2 options for configuring a failover strategy:

Heartbeat

The Heartbeat failover strategy allows avoiding the "split-brain" scenario when the HA cluster nodes are unable to synchronize but continue to accept write commands from the initiators independently. It can occur when all synchronization and heartbeat channels disconnect simultaneously, and the partner nodes do not respond to the node's requests. As a result, StarWind service assumes the partner nodes to be offline and continues operations on a single-node mode using data written to it.

If at least one heartbeat link is online, StarWind services can communicate with each other via this link. The device with the lowest priority will be marked as not synchronized and get subsequently blocked for the further read and write operations until the synchronization channel resumption. At the same time, the partner device on the



synchronized node flushes data from the cache to the disk to preserve data integrity in case the node goes down unexpectedly. It is recommended to assign more independent heartbeat channels during the replica creation to improve system stability and avoid the "split-brain" issue.

With the heartbeat failover strategy, the storage cluster will continue working with only one StarWind node available.

Node Majority

The Node Majority failover strategy ensures the synchronization connection without any additional heartbeat links. The failure-handling process occurs when the node has detected the absence of the connection with the partner.

The main requirement for keeping the node operational is an active connection with more than half of the HA device's nodes. Calculation of the available partners is based on their "votes".

In case of a two-node HA storage, all nodes will be disconnected if there is a problem on the node itself, or in communication between them. Therefore, the Node Majority failover strategy requires the addition of the third Witness node or file share (SMB) which participates in the nodes count for the majority, but neither contains data on it nor is involved in processing clients' requests. In case an HA device is replicated between 3 nodes, no Witness node is required.

With Node Majority failover strategy, failure of only one node can be tolerated. If two nodes fail, the third node will also become unavailable to clients' requests. Please select the required option:

Heartbeat

1. Select Failover Strategy.



		?	×
←	Replication Wizard		
	Failover Strategy		
	 Heartbeat Process node and communication failures using additional communication chan (heartbeat). At least one synchronization or heartbeat channel must be fund proper failover processing. Loss of all communication channels may lead to sissue, so it's recommended to use client iSCSI connection interfaces as heart channel. Node Majority Process node and communication failures using majority policy: node stays a sees more than half of nodes including itself. In case of 2 storage nodes, recomfiguring additional witness node. Does not require additional heartbeat destinations. 	ctional for plit brain tbeat ctive while i quires	it
	Next	Car	icel

2. Select Create new Partner Device and click Next.

3. Select a partner device Location and click Next.

4. Select Synchronization Journal Strategy and click Next.

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

RAM-based (default) synchronization journal is placed in RAM. Synchronization with RAM journal provides good I/O performance in any scenario. Full synchronization could occur in the cases described in this KB:

https://knowledgebase.starwindsoftware.com/explanation/reasons-why-full-synchronizati on-may-start/

Disk-based journal placed on a separate disk from StarWind devices. It allows to avoid full synchronization for the devices where it's configured even when StarWind service is being stopped on all nodes.

Disk-based synchronization journal should be placed on a separate, preferably faster disk from StarWind devices. SSDs and NVMe disks are recommended as the device



performance is defined by the disk speed, where the journal is located. For example, it can be placed on the OS boot volume.

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

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

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

	?	×
←	Replication Wizard	
	Synchronization Journal Setup	
	RAM-based journal Synchronization journal placed in RAM. Synchronization with RAM journal provides good IO performance in any scenario.	1
	O Disk-based journal Synchronization journal placed on disk.	
	 Failure journal The strategy provides good IO performance while all device nodes are in a healt state. 	hy
	 Continuous journal The strategy guarantees fast synchronization and data consistency in all cases. 	
	Current Node My Computer\C\	
	Partner Node My Computer\C\	
	<u>N</u> ext Ca	ancel

5. Click Change Network Settings.



		?	×
÷	Replication Wizard		
r	Network Options for Replication		
	Networks for Synchronization and Heartbeat		-
	Press "Change Network Settings" to configure Interfaces		
	Networks for Heartbeat		_
	Press "Change Network Settings" to configure Interfaces		
	Change Network Settings		
	ALUA preferred		
	Change ALUA Settings		
	Next	Can	cel

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



elect synchronizatior	n channel		
nterfaces	Networks	Synchronization and H	Heartbeat
- Host Name: 12	7.0.0.1		
172.16.10.10	172.16.10.0		~
172.16.20.10	172.16.20.0		
192.168.12.10	192.168.12.0		v
Host Name: SW	12		
172.16.10.20	172.16.10.0		~
172.16.20.20	172.16.20.0		
192.168.12.20	192.168.12.0		~

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

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

9. Follow the same procedure for the creation of other virtual disks that will be used as storage repositories.

Node Majority

There are two ways to configure Witness for 2-nodes StarWind HA device, created with Node Majority Failover Strategy: File Share (SMB) as Witness and additional server as Witness Node.

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

SMB Witness is a file, located on SMB share, which can be accessed by both nodes and help them to eliminate the split-brain issue in case of synchronization connection



interruption between the nodes. To set up the SMB file share as a Witness for 2-nodes HA device with Node Majority Failover Strategy, perform the actions, described on this page:

https://www.starwindsoftware.com/help/ConfiguringFileShareSMBasWitness.html

- Creating HA device with Witness Node:

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

			?	Х	
←	Replie	cation Wizard			
	Failove	r Strategy			
	0	Heartbeat Process node and communication failures using additional communication channel (heartbeat). At least one synchronization or heartbeat channel must be functiona proper failover processing. Loss of all communication channels may lead to split br issue, so it's recommended to use client iSCSI connection interfaces as heartbeat channel.			
	۲	Node Majority Process node and communication failures using majority policy: node stays active sees more than half of nodes including itself. In case of 2 storage nodes, requires configuring additional witness node. Does not require additional heartbeat channe			
		Next	Can	cel	

2. Choose Create new Partner Device and click Next.

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

4. In Network Options for Replication, press the Change network settings button and select the synchronization channel for the HA device.

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

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



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

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

Adding Witness Node

Witness node can be configured on a separate host or as a virtual machine in a cloud. It requires StarWind Virtual SAN service installed on it.

NOTE: Since the device created in this guide is replicated between 2 active nodes with the Node Majority failover strategy, a Witness node must be added to it.

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

📑 Ad	d new StarWind Server			?	×
Host:	witness-sw]:[3261	
Adva	anced >>	ОК] [Can	cel

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

3. Select Witness Node.



		? >	×
÷	Repli	cation Wizard	
	Replica	ation Mode	
	0	Synchronous "Two-Way" Replication Replication Partner must be connected to Client as Source Device as well, MPIO on Client must be enabled, needs dedicated high Performance Network Connection for Synchronization	
	0	Asynchronous "One-Way" Replication Replica is used to store replicated Data, Data is stored as Snapshots, Client cannot connect to Replication Partner, mount Snapshot from Replica to get Access to replicated Data	
	۲	Witness Node Witness node doesn't contain user data. In case when Node Majority policy is set for Synchronous replication device and there are two storage nodes, Witness Node must be added to cluster to make number of nodes odd number and enable proper functioning of Node Majority policy.	
		Next Cancel	

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



		?	×
Replication Wizard			
Add Partner Node			
Specify Partner Host Name	e or IP Address where Replication Node would be created		
Host Name or IP Address	witness-sw 🗸		
Port Number	3261		
	Next	Car	ncel

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

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

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

8. Click Create Replica and then close the wizard.

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

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



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.



iSC	SI Initiator Pro	opert	ies					Х
Ta	argets Discov	ery	Favorite Targets	Volumes and	Devices	RADIUS	Configuration	
	Target portals							
	The system w	ill loo	k for Targets on f	ollowing portals	:		Refresh	
	Address		Port	Adapter		I	P address	
	To add a targ	jet po	rtal, click Discove	r Portal.		Disco	ver Portal	
	To remove a then click Rem		t portal, select th	e address abov	e and	ļ	Remove	
	iSNS servers	reals	stered on the follo	wing iSNS serv	ers:		Refresh	
	Name							
	To add an iSN	IS ser	ver, click Add Ser	ver.		Ade	d Server	
	To remove ar then dick Ren		server, select th	e server above	and	I	Remove	
				0	<	Cancel	Apply	(

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



Discover Target Portal	×
Enter the IP address or DNS name and p want to add.	ort number of the portal you
To change the default settings of the dis the Advanced button.	covery of the target portal, dick
IP address or DNS name: 172.16.10.10	Port: (Default is 3260.) 3260
Advanced	OK 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.



vanced Settings	?	
neral IPsec		
Connect using		
Local adapter:	Microsoft iSCSI Initiator	/
Initiator IP:	172.16.10.1	
Target portal IP:	~	1
CRC / Checksum		
Data digest	Header digest	
	ame name and CHAP secret that was configured on the target for this vill default to the Initiator Name of the system unless another name is	
Name:	iqn.1991-05.com.microsoft:sw01	
Target secret:		
Perform mutual au	theatication	
RADIUS.	either specify an initiator secret on the Configuration page or use enerate user authentication credentials ithenticate target credentials	

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

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



Discover Target Portal	×
Enter the IP address or DNS name and p want to add.	ort number of the portal you
To change the default settings of the dis the Advanced button.	covery of the target portal, dick
IP address or DNS name: 172.16.10.20	Port: (Default is 3260.) 3260
Advanced	OK Cancel

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



Connect using	
ocal adapter:	Microsoft iSCSI Initiator \sim
nitiator IP:	172.16.10.1 ~
arget portal IP:	\sim
CRC / Checksum	
Data digest	Header digest
n initiator. o use, specify the sa nitiator. The name w	
CHAP Log on inform CHAP helps ensure co in initiator. To use, specify the sa nitiator. The name w pecified.	nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this vill default to the Initiator Name of the system unless another name is
CHAP Log on inform CHAP helps ensure co an initiator.	nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this

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



iSC	SI Initi	ator Proper	ties				×
Та	rgets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration	
	Targe	t portals					
	The s	ystem will lo	ok for Targets on fo	llowing portals:		Refresh	
	Addr	ess	Port	Adapter	1	IP address	
	172.	16.10.10	3260	Microsoft iSCSI Initia	tor	172.16.10.1	
	172.	16.10.20	3260	Microsoft iSCSI Initia	tor	172.16.10.1	
	To re			Portal. address above and		over Portal Remove	
			istered on the follov	ving iSNS servers:		Refresh	
	To ad	d an iSNS se	erver, click Add Serv	er.	Ad	d Server	
	To re		S server, select the			Remove	
				OK	Cance	Apply	

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

Connecting Targets

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

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



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

iSCSI Initiator Properties	×
Targets Discovery Favorite Targets Volumes and Devices Quick Connect To discover and log on to a target using a basic connection,	
DNS name of the target and then click Quick Connect.	type the 1P address of
Target:	Quick Connect
Discovered targets	
	Refresh
Name	Status
iqn.2008-08.com.starwindsoftware:sw1-csv1	Inactive
iqn.2008-08.com.starwindsoftware:sw1-csv2	Inactive
iqn.2008-08.com.starwindsoftware:sw1-witness	Inactive
iqn.2008-08.com.starwindsoftware:sw2-csv1	Inactive
iqn.2008-08.com.starwindsoftware:sw2-csv2	Inactive
iqn.2008-08.com.starwindsoftware:sw2-witness	Inactive
To connect using advanced options, select a target and ther click Connect.	n Connect
To completely disconnect a target, select the target and then click Disconnect.	Disconnect
For target properties, including configuration of sessions, select the target and click Properties.	Properties
For configuration of devices associated with a target, select the target and then click Devices.	Devices
ОК	Cancel Apply

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

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



Connect To Target	×
Target name:	
iqn.2008-08.com.starwindsoftware:sw1-witness	
Add this connection to the list of Favorite Targets. This will make the system automatically attempt to restore the connection every time this computer restarts.	
∑ Enable multi-path	
Advanced OK	Cancel

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.



Connect using	
ocal adapter:	Microsoft iSCSI Initiator \checkmark
nitiator IP:	172.16.10.1 ~
Farget portal IP:	172.16.10.10 / 3260 🗸
CRC / Checksum	
Data digest	Header digest
n initiator. o use, specify the sa nitiator. The name w	
CHAP Log on inform CHAP helps ensure co an initiator. To use, specify the sa nitiator. The name w specified.	nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this
CHAP Log on inform CHAP helps ensure co an initiator.	nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this vill default to the Initiator Name of the system unless another name is

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



Connect To Target	×
Target name:	
iqn.2008-08.com.starwindsoftware:sw1-csv1	
Add this connection to the list of Favorite Targets. This will make the system automatically attempt to restore the connection every time this computer restarts.	
Enable multi-path	
Advanced OK	Cancel

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.



eral IPsec	
Connect using	
.ocal adapter:	Microsoft iSCSI Initiator $\qquad \qquad \lor$
nitiator IP:	172.16.10.1 ~
Farget portal IP:	172.16.10.20 / 3260 🗸
CRC / Checksum	
Data digest	Header digest
CHAP Log on inform CHAP helps ensure c in initiator. To use, specify the s nitiator. The name v	
CHAP helps ensure c an initiator. To use, specify the s nitiator. The name v	nation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is
CHAP Log on inform CHAP helps ensure c an initiator. Fo use, specify the s	nation connection security by providing authentication between a target and came name and CHAP secret that was configured on the target for this
CHAP Log on inform CHAP helps ensure c an initiator. To use, specify the s nitiator. The name w specified.	nation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is

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

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

Configuring Multipath

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



load balancing policy.

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

2. In the Devices dialog, click MPIO.

Devices			×
	1		
Name	Address		
Disk 2	Port 5: Bus	0: Target 2: LUN 0	
Volume path	names:		
Legacy devic	e name:	\\.\PhysicalDrive2	
Device interf	face name:	\\?\mpio#disk&ven_starwind&pro	od_starwind&rev_000
Device interi	ace name.	<	>
Configure Mu	ultipath IO (M	IPIO)	
	e the MPIO po vice, click MPI		MPIO
			ОК

3. Select the appropriate load balancing policy.

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

Connecting Disks to Servers

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



📅 Disk Managen	nent							_	×
File Action Vi	ew Help								
🔶 🔿 📰 👔									
Volume	Layout	Туре	File Syste	m	Status	Capacity	Free Spa	% Free	
Storage (D:)	Simple	Basic	NTFS		Healthy (P	49.87 GB	32.78 GB	66 %	
- System (C:)	Simple	Basic	NTFS		Healthy (B		6.53 GB	27 %	
 System Reserve 	d Simple	Basic	NTFS		Healthy (S	500 MB	172 MB	34 %	
- Disk 0									^
Basic 25.00 GB Online	System Reserv 500 MB NTFS Healthy (System		mary Partiti	24.5	em (C:) 1 GB NTFS Ithy (Boot, Page	e File, Crash D	ump, Primary Pa	rtition)	
Disk 1 Basic 49.88 GB Online	Storage (D:) 49.87 GB NTFS Healthy (Primat	y Partition)							
O Disk 2 Unknown 6.00 GB Offline	6.00 GB Unallocated							_	
O Disk 3 Unknown 10.00 GB Offline	10.00 GB Unallocated								1
*O Disk 4 Unknown 1.00 GB Offline i	1.00 GB Unallocated								
Unallocated	Primary partition]			~

2. Bring the disks online by right-clicking on them and selecting the Online menu option.

3. Select the CSV disk (check the disk size to be sure) and right-click on it to initialize.

4. By default, the system will offer to initialize all non-initialized disks. Use the Select Disks area to choose the disks. Select GPT (GUID Partition Style) for the partition style to be applied to the disks. Press OK to confirm.



Initialize Disk	×
You must initialize a disk before Logical Disk Manager can access it. Select disks:	
 ✓ Disk 2 ✓ Disk 3 ✓ Disk 4 	
Use the following partition style for the selected disks: MBR (Master Boot Record) ORT (GUID Partition Table)	_
Note: The GPT partition style is not recognized by all previous versions of Windows.	
OK Cancel	

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

New Simple Volume Wizard	×
Assign Drive Letter or Path For easier access, you can assign a drive letter or drive path to your partition.	
 Assign the following drive letter: Mount in the following empty NTFS folder: 	
O Do not assign a drive letter or drive path	
< Back Next > Ca	incel



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

New Simple Volume Wizard		×
Format Partition To store data on this partition, you m	ust format it first.	
Choose whether you want to format	this volume, and if so, what settings you want to use.	
O Do not format this volume		
Format this volume with the format	llowing settings:	
File system:	NTFS ~	
Allocation unit size:	Default ~	
Volume label:	CSV1	
Perform a quick format		
Enable file and folder co	ompression	
	< 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.



New Simple Volume Wizard	×
Assign Drive Letter or Path For easier access, you can assign a drive lette	r or drive path to your partition.
○ Assign the following drive letter:	E v
O Mount in the following empty NTFS folder:	Browse
Do not assign a drive letter or drive path	
	< Back Next > Cancel

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-t ools

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.



ᡖ Server Manager		– 🗆 X
Server Ma	anager 🕨 Dashboard 🛛 🗸 🕫 l 🚩 🕬	age <u>Tools</u> View Help
Dashboard	WELCOME TO SERVER MANAGER	Cluster-Aware Updating Component Services Computer Management
Local Server All Servers File and Storage Services ▷	1 Configure this local serv	
🖪 Hyper-V	2 Add roles and features	Failover Cluster Manager Hyper-V Manager iSCSI Initiator
	3 Add other servers to mana WHAT'S NEW 4 Create a server group	Microsoft Azure Services MPIO
	5 Connect this server to clou	d Ser ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor
	LEARN MORE	Print Management Resource Monitor Services
	Roles: 2 Server groups: 1 Servers total: 1	System Configuration System Information Task Scheduler
	Services Image: Triper v Image: Triper v Triper v <td< td=""><td>Windows Firewall with Advanced Security Windows Memory Diagnostic</td></td<>	Windows Firewall with Advanced Security Windows Memory Diagnostic

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

🗟 Failover Cluster Manager						_	×
File Action View Help							
💐 Failover Cluster Manager	Failover Cluster Manager		^	Act	ons		
	Create failover clusters, validate hardware for potential	failover clusters, and perform		Fail	over Cluster Manager		-
	configuration changes to your failover clusters.			N.	Validate Configuration		
				鷝	Create Cluster		
	Overview			暳	Connect to Cluster		
	A failover cluster is a set of independent computers that work availability of server roles. The clustered servers (called node	s) are connected by physical			View		•
	cables and by software. If one of the nodes fails, another nod This process is known as failover.	e begins to provide services.		Q	Refresh		
					Properties		
	Clusters			?	Help		
	Name R	ole Status					
	No items found.						
	Management]					
	Management	Farmelian and them					
	To begin to use failover clustering, first validate your hardwar create a cluster. After these steps are complete, you can ma	nage the cluster. Managing a					
	cluster can include copying roles to it from a cluster running V supported previous versions of Windows Server.	Vindows Server 2016 or					
	Validate Configuration						
	Create Cluster						
	Connect to Cluster						
	More Information						
	Failover cluster topics on the Web						
	Failover cluster communities on the Web						
	Microsoft support page on the Web						
			~				



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

📳 Create Cluster Wiz	zard		Х
Select Se	ervers		
Before You Begin Select Servers Validation Warning	Add the names of all the s	ervers that you want to have in the cluster. You must add at least one server.	
Access Point for Administering the Cluster Confirmation Creating New Cluster Summary	Enter server name: Selected servers:	SW1.starwind local Add SW2.starwind local Remove	
		< Previous Next > Cancel	

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



🚏 Create Cluster Wi	zard	×
Validation	n Warning	
Before You Begin Select Servers Validation Warning	For the servers you selected for this cluster, the reports from cluster configuration validation tests appear to be missing or incomplete. Microsoft supports a cluster solution only if the complete configuration (servers, network and storage) can pass all the tests in the Validate a Configuration wizard.	
Access Point for Administering the Cluster	Do you want to run configuration validation tests before continuing?	
Confirmation		
Creating New Cluster	• Yes. When I click Next, run configuration validation tests, and then return to the process of creating	
Summary	the cluster.	
	No. I do not require support from Microsoft for this cluster, and therefore do not want to run the validation tests. When I click Next, continue creating the cluster.	
	More about cluster validation tests	
	< Previous Next > Cancel]

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 Wi	zard				×
Access P	oint for Adminis	tering the Clus	ter		
Before You Begin	Type the name you v	vant to use when admi	nistering the cluster.		
Select Servers Access Point for	Cluster Name:	Production			
Access Point for Administering the Cluster Confirmation				addresses could not be conf ork is selected, and then typ	
Creating New Cluster		Networks		Address	
Summary		✓ 19	2.168.12.0/23	192.168.12.86	
			< Previous	Next > Car	ncel

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

🚏 Create Cluster Wiz	zard X
Confirmat	tion
Before You Begin Select Servers	You are ready to create a cluster. The wizard will create your cluster with the following settings:
Access Point for Administering the	Cluster
Cluster	Production
Confirmation	Node
Creating New Cluster	SW1.starwind.local
Summary	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.

🚏 Create Cluster Wiz	zard	×
Summary		
Before You Begin Select Servers	You have successfully completed the Create Cluster Wizard.	
Access Point for Administering the Cluster	Node SW1.starwind.local	^
Confirmation	SW2.starwind.local	
Creating New Cluster	Cluster	
Summary	Production	
	IP Address	
	192.168.12.86	
	Warnings	
	* An appropriate disk was not found for configuring a disk witness. The cluster is not configured with a witness. As a best practice, configure a witness to help achieve the highest availability of the cluster. If this cluster does not have shared storage, configure a File Share Witness or a Cloud Witness.	~
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.	View Report
		Finish

Adding Storage to the Cluster

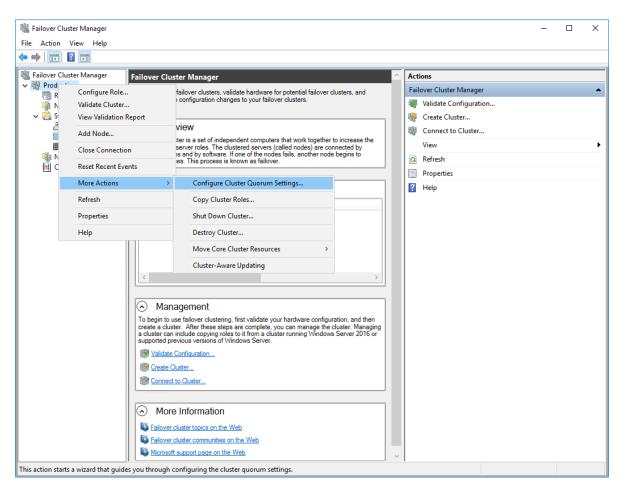
1. In Failover Cluster Manager, navigate to Cluster -> Storage -> Disks. Click Add Disk in the Actions panel, choose StarWind disks from the list and confirm the selection.



Failover Cluster Manager File Action View Help						- □ >
Þ 🧼 🖄 📰 🛛 🖬						
📲 Failover Cluster Manager	Disks (0)				Actions	
✓ Production	Search		<i>P</i> (Queries 🔻 🔒 💌 🔍	Disks	
📷 Roles 📫 Nodes	Name	Status	Assigned To	Owner Nod	🛃 Add Disk	
🗸 <u>ё</u> Storage					📑 Move Available Storage	
Disks	Add Disks to a Cluster				×	
Enclosures						
Networks	Select the disk or disks t	hat you want to add.				
🔢 Cluster Events	Available disks:					
	Resource Name	Disk Info	Capacity	Signature/Id		
	🗹 📇 Cluster Disk 1 🗹 📇 Cluster Disk 2	Disk 3 on node SW2 Disk 4 on node SW2	10.0 GB 1.00 GB	{080ffb0a-c594-4790-a {2bd3a199-b684-4147		
	Cluster Disk 2	Disk 2 on node SW2	6.00 GB	{2003a199-0684-4147 {b4ade0c2-d87c-4aff-t		
				OK	Cancel	

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.



Configure Cluster	r Quorum Wizard	×
Select Qu	uorum Configuration Option	
Before You Begin Select Quorum Configuration Option Select Quorum Witness Confirmation Configure Cluster Quorum Settings Summary	 Select a quorum configuration for your cluster. Use default quorum configuration The cluster determines quorum management options, including the quorum witness. Select the quorum witness You can add or change the quorum witness. The cluster determines the other quorum management options. Advanced quorum configuration You determine the quorum management options, including the quorum witness. 	
	< Previous Next > Cancel	

4. Select Configure a disk witness. Click Next.



Configure Cluster	Quorum Wizard	×
Select Qu	uorum Witness	
Before You Begin Select Quorum Configuration Option Select Quorum	Select a quorum witness option to add or change the quorum witness for your cluster configuration. As a best practice, configure a quorum witness to help achieve the highest availability of the cluster.	
Witness Configure Storage Witness Confirmation Configure Cluster Quorum Settings Summary	Adds a quorum vote of the disk witness Configure a file share witness Adds a quorum vote of the file share witness Configure a cloud witness Adds a quorum vote of the cloud witness 	
	Do not configure a quorum witness Failover Cluster Quorum and Witness Configuration Options <pre></pre>	

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



Configure Cluster	Quorum Wizard			×
Configure	e Storage Witness			
Before You Begin Select Quorum Configuration Option	Select the storage volume the	nat you want to assign a	s the disk witness.	
Select Quorum Witness	Name	Status	Node	Location
Configure Storage Witness Configure Cluster Quorum Settings Summary	 □ I Cluster Disk 1 Volume: (G) ☑ □ I Cluster Disk 2 Volume: (\\?\ □ I Cluster Disk 3 Volume: (E) 	File System: NTFS The Online File System: NTFS	SW2 959 MB free of 990 MB SW2	Available Storage Available Storage Available Storage
			< Previous Ne	xt > Cancel

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

📲 Failover Cluster Manager						-		×
File Action View Help								
🗢 🔿 🞽 🖬 👔 🗊								
📲 Failover Cluster Manager	Disks (3)					Actions		
 Production.starwind.local Roles 	Search				🔎 Queries 🔻 🕁 👻	Disks		<u>^</u> ^
🍯 Nodes	Name	Status	Assigned To	Owner Node	Disk Number Partit	🔮 Add Disk		
 Storage Disks Pools Enclosures Networks Cluster Events 	3 Cluster Disk 1 4 Cluster Disk 2 3 Cluster Disk 3 <	 Online Online Online 	Available Storage Disk Witness in Quorum Available Storage	SW2 SW2 SW2	Image: Second		ble Stor	▶
	Cluster Disk 1 Volumes (1) CSV2 (G) Volumes				Replication More Actions Remove Properties	>	er Shar Details Events	
Disks: Cluster Disk 1] J.							•

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.



闘 Failover Cluster Manager] — П Х	(
File Action View Help				Cluster D	isk 1 Proper	ties		×		
· · · · · · · · · · · · · · · · · · ·				General						_
 Failover Cluster Manager Production.starwind.local Roles Nodes Storage Disks Pools Enclosures 	Disks (3) Search Name 은 Cluster Disk 1 곳 Cluster Disk 2 곳 Cluster Disk 3	Status Online Online Online Online	Assigned Cluster S Disk Wit Cluster S	Volun		CSV2 Physical I Online ge\Volume1	File System Redirected Access	Capacit 9.97 Gl	Disk te Available Storage II y II esh	• •
🍓 Networks 鴡 Cluster Events	<			<u> </u>		ge wordine f		5.57 GI	isk 1 / / / / / / / / / / / / / / / / / /	
	v 🧸 Cluster Disk 1			<				>	re l	۲
									ication I	۲
	Volumes (1)								e Actions I	۲
	CSV2 (C:\ClusterS						OK Cancel	Apply	ove from Cluster S Jerties	
Disks: Cluster Disk 1	Ir									

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.

闂 Failover Cluster Manager							- 0	×	-
File Action View Help									
🗢 🄿 🙍 🖬 🚺									
📲 Failover Cluster Manager	Disks (3)						Actions		-
 Production.starwind.local Roles 	Search			P	Queries 🔻 🕁	• •	Disks	•	^
🖷 Nodes	Name	Status	Assigned To	Owner Node	Disk Number	Partit	🛃 Add Disk		
🗸 🔚 Storage	📇 CSV1	🕜 Online	Cluster Shared Volume	SW2		2	🍰 Move Available St	or 🕨	
Disks	📇 CSV2	Online	Cluster Shared Volume	SW1		3	View	•	
Enclosures	🔠 Witness	💿 Online	Disk Witness in Quorum	SW2		4	Refresh		
Networks							🕐 Help		
<u></u>							CSV1	•	
							🚱 Bring Online		
	<					>	🙀 Take Offline		
	*100						🚯 Information Detail	s	
	👻 🌉 CSV1						Show Critical Ever	its	
							Move Move	•	
	Volumes (1)						🐮 Replication	•	
	CSV1 (C:\Cl	usterStorage\Volume2)					More Actions	•	
	CSVFS 5.93	GB free of 5.97 GB		1			Remove from Clu	st	
	Volumes						Properties		v
Disks: CSV1							-		

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

職 Failover Cluster Manager File Action View Help				Cluster	Netw	vork 1 Properties	Х	×
				Genera				
 Failover Cluster Manager Production.starwind.local Roler 	Networks (3) Search			Ŵ	a	luster Network 1		-
Roles Nodes Storage Brools Enclosures Networks Cluster Events	Name Custer Network 1 Custer Network 2 Custer Network 2 Custer Network 3 Custer Network 3 Custer Network 3 Custer Network 3 Custer Network 2 Subnets: 172.16.2 Summary Network Conn	20.0/24	Cluster Use Cluster Only None Cluster and Client	Ir Sync	((Allow cluster network communication on this network Allow cluster network communication on this network Do not allow cluster network communication on this network Up 172.16.20.0/24 OK Cancel Apply		gs)

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

File Action View Help	1						
 Failover Cluster Manager Production.starwind.local 	Networks (3)					Actions	
Roles	Search			P Quer	ies 🕶 🔐 🕶 😔	Networks	-
Nodes	Name	Status	Cluster Use	Information		Live Migration Settin	gs
✓ 📇 Storage	Sync .	🛞 Up	Cluster Only			View	•
Disks Pools	县 iSCSI	🛞 Up	None			C Refresh	
Enclosures	👫 Management	🛞 Up	Cluster and Client			Help	
Networks	<				>	iSCSI	*
· Only Cluster Onl Only	iSCSI Subnets: 172.1 Summary Network Co	6.10.0/24 nnections				 Information Details Show Critical Events Properties Help 	

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.



💐 Failover Cluster Manager				- 🗆 X
File Action View Help		Live Migration Settings	×	
 Failover Cluster Manager Production.starwind.local Roles Nodes Corrage 	Networks (3) Search Name Stat B Sync (*)			Actions Networks 聲 Live Migration Settings View ▶
 Disks Pools Enclosures Networks Cluster Events 	ISCSI ① ISCSI ④ ISCSI ④	- Turic		Refresh Help isCSI
	<		>	 Information Details Show Critical Events Properties Help
	Subnets: 172.16.10.0/24			
	Summary Network Connections	OK Cancel	Apply	

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.



📲 Failover Cluster Manage	er		– 🗆 ×
File Action View Hel	p		
🗢 🔿 🙍 📰 📓 📼			
📲 Failover Cluster Manage	Cluster Production.starwing	d.local	Actions
Production.stary Roles	Configure Role	er Production	Production.starwind.local
Nodes	Validate Cluster	ered roles and 2 nodes.	ky Configure Role
> 📇 Storage	View Validation Report	al Networks: Cluster Network 2, Cluster Network 3, Cluster Network 1, Cluster Network 4	¥ Validate Cluster
Networks	Add Node	Subnets: 3 IPv4 and 1 IPv6	View Validation Report
ensiter even	Close Connection	- tical: 52, Error: 16, Warning: 5	P Add Node
			Close Connection
	Reset Recent Events		Reset Recent Events
	More Actions >		More Actions
	View >	Failover cluster topics on the Web	View +
	Refresh		Q Refresh
	Properties		Properties
	Help		Help
			Name: Production
			🚱 Bring Online
	Navigate		🙀 Take Offline
	Roles	Nodes	🚯 Information Details
			Show Critical Events
			More Actions
	 Cluster Core Res 	ources	× Remove
	Name	Status Information	Properties
	Server Name	0.00	👔 Help
	Name: Production IP Address: 192.1	Online 12.86 Online	
	Cluster Infrastructure	100, 12.00 (b) Unine	
< >			v
This action enables you to se	lect a role that you can configure	for high availability.	

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

🧞 High Availability	Nizard		×
Select Ro	le		
Before You Begin Select Role	Select the role that you want to configure for high a	vailability:	
File Server Type Client Access Point Select Storage Confirmation Configure High Availability Summary	DFS Namespace Server DHCP Server Distributed Transaction Coordinator (DTC) File Server Generic Application Generic Script Generic Service Hyper-V Replica Broker CSCSI Target Server	on your r	ion: erver provides a central location network where files are shared y users or by applications.
		< <u>P</u> revious	Next > Cancel

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



High Availability	r Wizard ver Type	×
Before You Begin Select Role File Server Type	Select an option for a clustered file server: <u>File</u> Server for general use Use this option to provide a central location on your network for users to share files or for server	
Client Access Point Confirmation Configure High Availability	 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 	
Summary	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	

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.



🧓 High Availability	Wizard	×
Client Ac	cess Point	
Before You Begin Select Role File Server Type	Type the name that clients will use when accessing this clustered role: Name: FileServer]
Client Access Point Confirmation Configure High Availability Summary	(i) The NetBIOS name is limited to 15 characters. All networks were configured automatically.	
	< <u>P</u> revious <u>N</u> ext > Cancel	

Click Next to continue.

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



🧞 High Availability \	Nizard		×
Confirmat	tion		
Before You Begin Select Role	You are ready to configure high availability for a f	īile Server.	
File Server Type	Distributed Network Name		^
Client Access Point	192.168.12.0	FileServer	
Confirmation	OU		
Configure High Availability	CN=Computers,DC=starwind,DC=local		
Summary			
,			
			~
	To continue, click Next.		
		< Previous Next > Can	icel

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

Click Finish to close the Wizard.



🧓 High Availability \	Nizard	×
ty Summary		
Before You Begin Select Role	High availability was successfully configured for the role.	
File Server Type	Distributed Network Name	
Client Access Point	FileServer	
Confirmation	OU	
Configure High Availability	CN=Computers,DC=starwind,DC=local	
-	Subnet	
Summary	192.168.12.0	
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.	
	<u> </u>	

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

📲 Failover Cluster Manager									- 0	×
File Action View Help										
🗢 🔿 🙍 📷 🖬 💼										
🐘 Failover Cluster Manage	Roles (1)								Actions	
 Production.starwind Roles 	Search						ş	Queries 🔻 🛃 👻 😪	Roles	
Nodes	Name	Status	Туре	Owner Node	Priority	Information			😽 Configure Role	
🗸 📇 Storage	Rie Server	Running	Scale-Out File Server	SW1	Medium				Virtual Machines	•
Disks									Treate Empty Role	
Enclosures									View	•
Networks B Cluster Events									Refresh	
Is Cluster Events									👔 Help	
									FileServer	
									🗘 Start Role	
									🙄 Stop Role	
									Add File Share	
									1 Move	•
									😵 Change Startup Priority	•
									information Details	
									Show Critical Events	
									Add Storage	
									Add Resource	•
									More Actions	•
									X Remove	
									Properties	
									I Help	
	Y FileServer							Preferred Owners: Arry node		
		Running								
		Medium SW1								
	Client Access Name:									
	IP Addresses:	192.168.12.85								
< >	Summary Resources 1	Shares							1	

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

🖏 Failover Cluster Manager								-	σ×
File Action View Help									
🗢 🔿 🙍 📅 📓 🖬									
🖏 Failover Cluster Manage	Roles (1)							Actions	
 Production.starwind Roles 	Search						👂 Queries 🔻 🔛 👻 🐼	Roles	-
Nodes	Name	Status	Туре	Owner Node	Priority	Information		89 Configure Role	
🗸 📇 Storage	BileServer	Falled	Scale-Out File Server	SW1	Medium			Virtual Machines	•
Disks								Treate Empty Role	
Enclosures								View	,
Networks Cluster Events								Refresh	
En close trens								🛛 Help	
								FileServer	
								🗘 Start Role	
								🗘 Stop Role	
								Add File Share	
								Move Move	,
								😵 Change Startup Priority	,
								🚮 Information Details	
								Show Critical Events	
								Add Storage	
								Add Resource	•
								More Actions	,
								🗙 Remove	
								Properties	
								👔 Help	
	👻 🕌 FileServer						Preferred Owners: Any node		
	· III · IIII · IIII						Therefore of the second s		
		Running							
		Medium SW1							
	Client Access Name:								
		192.168.12.85							
< >	Summary Resources S	ihares							

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

Select User, Computer, Service Account, or Group	×
Select this object type:	
User, Computer, Group, or Built-in security principal	Object Types
From this location:	
starwind.local	Locations
Enter the object name to select (<u>examples</u>):	
Production	Check Names
I	
Advanced	OK Cancel

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



Delete aCSResourceLimits objects	Delete msKds-ProvRootKey objects	
	Create mskds-ProvRoticey objects	
Create application Version objects	_	
Delete applicationVersion objects	Delete msKds-ProvServerConfiguration objects Constant MSMO Occurs Alice ship sta	
Create certificationAuthority objects	Create MSMQ Queue Alias objects	
Delete certificationAuthority objects	Delete MSMQ Queue Alias objects	
Create Computer objects	Create ms-net-ieee-80211-GroupPolicy objects	
Delete Computer objects	Delete ms-net-ieee-80211-GroupPolicy objects	
Create Contact objects	Create ms-net-ieee-8023-GroupPolicy objects	
Delete Contact objects	Delete ms-net-ieee-8023-GroupPolicy objects	
Create document objects	Create msPKI-Enterprise-Oid objects	
Delete document objects	Delete msPKI-Enterprise-Oid objects	
Create documentSeries objects	Create msPKI-Key-Recovery-Agent objects	
Delete documentSeries objects	Delete msPKI-Key-Recovery-Agent objects	
Create Group objects	Create msPKI-PrivateKeyRecoveryAgent objects	
Delete Group objects	Delete msPKI-PrivateKeyRecoveryAgent objects	
Create groupOfUniqueNames objects	Create msPrint-ConnectionPolicy objects	
Delete groupOfUniqueNames objects	Delete msPrint-ConnectionPolicy objects	
Create groupPolicyContainer objects	Create msSFU30DomainInfo objects	
Delete groupPolicyContainer objects	Delete msSFU30DomainInfo objects	
Create InetOrgPerson objects	Create msSFU30MailAliases objects	
Delete InetOrgPerson objects	Delete msSFU30MailAliases objects	
Create IntelliMirror Group objects	Create msSFU30NetId objects	
Delete IntelliMirror Group objects	Delete msSFU30NetId objects	
Create IntelliMirror Service objects	Create msSFU30NetworkUser objects	
Delete IntelliMirror Service objects	Delete msSFU30NetworkUser objects	

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

Configuring File Share

To Add File Share:

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



Select Profile	File share profile:	Description:
Share Location Share Name	SMB Share - Quick SMB Share - Advanced	This profile creates an SMB file share with settings appropriate for Hyper-V, certain databases, and other
Share Name Other Settings	SMB Share - Applications	server applications.
	NFS Share - Quick	
Confirmation	NFS Share - Advanced	
Results		

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



Select Profile	Ser	ver:						
Share Location	S	erver Name	Status	Cluster	Role	Owner Node		
Share Name	F	ileServer	Online	Scale-C	ut File			
Other Settings								
Permissions								
Confirmation								
Results								
	Sha	are location:						
	۲	Select by <u>v</u> olume:						
		Volume	Free Space	Capacity	File Syster	n		_
		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 volume.	will be a new fold	ler in the \	Sh <mark>ares dire</mark>	ctory on the se	lected	

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



藩 New Share Wizard				-		×	
Specify share nam	е						
Select Profile	Share name:	Share					
Share Location						_	
Share Name	Share <u>d</u> escription:						
Other Settings							
Permissions							
Confirmation	Local path to share:						
Results	C:\ClusterStorage\Volume1\Shares\Share						
	🕕 If the folder doe	not exist, the folder is created.					
	Remote path to sha	e:					
	\\FileServer\Share						
		< <u>P</u> revious <u>N</u> e	ext > Create	-	Cancel		

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



🖀 New Share Wizard	– 🗆 X
Configure share	settings
Select Profile Share Location Share Name Other Settings Permissions Confirmation Results	 Enable access-based enumeration Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view. Inable continuous availability Continuous availability features track file operations on a highly available file share so that clients can fail over to another node of the cluster without interruption. Allow caching of share Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share. Enable BranchCache on the file share BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch. Encrypt data access When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.
	< Previous Next > Create Cancel

8. Specify the access permissions for the file share.



Select Profile Share Location Share Name Other Settings Permissions	remote ma Permissior permissior	anagement of the Hyper-V h is to access the files on a sha is, and, optionally, a central nissions: Everyone Full Cont	ost. are are set using a access policy.	nable constrained delegation to enable combination of folder permissions, sha
Confirmation	Type	Principal	Access	Applies To
Results		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
	Custor	ize permissions		

NOTE:

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

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

Confirm selections Select Profile Share Location Share Name Other Settings Permissions Confirmation		are the correct settings, and then click Create. FileServer Scale-Out File Server C:\ClusterStorage\Volume1\Shares\Share
Share Location Share Name Other Settings Permissions Confirmation	SHARE LOCATION Server: Cluster role:	FileServer Scale-Out File Server
Share Name Other Settings Permissions Confirmation	SHARE LOCATION Server: Cluster role:	FileServer Scale-Out File Server
Other Settings Permissions Confirmation	Cluster role:	Scale-Out File Server
Permissions Confirmation		
Confirmation	Local path:	C:\ClusterStorage\Volume1\Shares\Share
	SHARE PROPERTIES	
Results	Share name:	Share
	Protocol:	SMB
	Access-based enumeration:	Disabled
	Caching:	Disabled
	BranchCache:	Disabled
	Encrypt data:	Disabled
	Continuous availability:	Enabled
	1	
		< Previous Next > Create Cance

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



藩 New Share Wizard			- 0	×
View results				
Select Profile	The share was success	fully created.		
Share Location	Task	Progress	Status	
Share Name Other Settings	Create SMB share Set SMB permissions		Completed Completed	
Permissions				
Confirmation				
Results				
		< <u>P</u> revious <u>N</u> ext >	Close Canc	el

To Manage Created File Shares:

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

Roles (1)							Actions
Search						P Queries 👻 🔛 👻	Roles
Name	Status Type		Owner Node Pric	fty	Information		89 Configure Role
Rie Server		Out File Server		dum			Virtual Machines
							Create Empty Role
							View
							Refresh
							Help
							FileServer
							🔅 Start Role
							🔅 Stop Role
							Add File Share
							Move
							🐞 Change Startup Priority
							🚯 Information Details
							Show Critical Events
							Add Storage
							Add Resource
							More Actions
							🗙 Remove
							Properties
							👔 Help
							l .
v 🕌 FileServer						Preferred Owners: Any node	
Shares (2)							
Name	Path	Protor	col Continuous Ava	iability R	lemaks		
	C:\OusterStorage	SMB			Juster Shared Volumes Default Share		
🤳 Share	C:\ClusterStorage\Volume1\Shares	Nhare SMB	Yes				
							4

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.

職 Failover Cluster Manag	er							-	×
File Action View He	lp								
🗢 🔿 🙍 📰 🖬 🖬	19								
📲 Failover Cluster Manage	Cluster Production.starwing	i.local				^	Actions		 _
 Production.starv Roles 		er Production					Production.starwind.local		
Nodes	Validate Cluster	ered roles and 2 nodes.					lonfigure Role		
> 📇 Storage	View Validation Report	al		Networks: Cluster Network 2, Cluste	Network 3, Cluster Network 1, Cluster Network 4		¥ Validate Cluster		
Networks	Add Node			Subnets: 3 IPv4 and 1 IPv6			View Validation Report		
en en er er er	Close Connection	tical: 52, Error: 16, Warning: 5					P Add Node		
	Reset Recent Events						Close Connection		
						1	Reset Recent Events		
	More Actions >		More Actions		•				
	View >			Failover cluster topics on the Web			View		•
	Refresh						G Refresh		
	Properties						Properties		
	Help						Help		
							Name: Production		•
							🚱 Bring Online		
	 Navigate 						🙀 Take Offline		
	Roles	Nodes	Storage	Networks	Cluster Events		🚯 Information Details		
							Show Critical Events		
	Cluster Core Res					1	More Actions		•
		ources					🗙 Remove		
	Name		Status I	nformation			Properties		
	Server Name		(Online				Help		
	IP Address: 192.16	69 12 96	Online						
	Cluster Infrastructure		C on the						
< >	Barran in a c		A			~			
This action enables you to s	elect a role that you can configure	for high availability.							

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



퉳 High Availability	Wizard			×
Select Re	ble			
Before You Begin Select Role	Select the role that you want to configure for high	availability:		
File Server Type Client Access Point Select Storage Confirmation Configure High Availability Summary	DFS Namespace Server DHCP Server Distributed Transaction Coordinator (DTC) File Server Generic Application Generic Script Generic Service Hyper-V Replica Broker SCSI Target Server	▲	Description: A File Server provides a central location on your network where files are shared for use by users or by applications.]

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



igh Availability 🎆	Wizard	×
File Serv	ег Туре	
Before You Begin	Select an option for a clustered file server:	
Select Role	<u>Fi</u> le Server for general use	
File Server Type Client Access Point Select Storage Confirmation Configure High Availability Summary	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.	
	< <u>P</u> revious <u>N</u> ext > Cancel	

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



🧞 High Availability	Wizard				×
Client Ac	cess Point				
Before You Begin	Type the name that o	lients will use when	accessing this clustered role:		
Select Role File Server Type	Name:	FileServer]
Client Access Point Select Storage				addresses could not be configured ork is selected, and then type an	
Confirmation		Networks		Address	1
Configure High Availability			192.168.12.0/24	192.168.12.85	
Summary					
					-
			< <u>P</u> revious	Next > Cancel	

Click Next to continue.

6. Select the Cluster disk and click Next.



🧞 High Availability \	Wizard				×
to Select St	orage				
Before You Begin Select Role File Server Type			o assign to this clustered role red role after you complete th		
Client Access Point	Name	Status			
Select Storage Confirmation Configure High Availability Summary	Volume: (G)	Online	9.91 GB free of 9.97 GB		
			< <u>P</u> revious	<u>N</u> ext > Cancel	

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



ligh Availability Wizard					
tonfirmat	ion				
Before You Begin Select Role	You are ready to configure high availability for a File	e Server.			
File Server Type	Network Name		^		
Client Access Point	192.168.12.85	FileServer			
Select Storage	OU				
Confirmation	CN=Computers,DC=starwind,DC=local				
Configure High Availability	Storage				
Summary	CSV2				
			~		
	To continue, click Next.				
		< Previous Next > Canc	el		

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

Click Finish to close the Wizard.



🧓 High Availability \	Nizard	×
ty Summary		
Before You Begin Select Role	High availability was successfully configured for the role.	
File Server Type	Distributed Network Name	
Client Access Point	FileServer	
Confirmation	OU	
Configure High Availability	CN=Computers,DC=starwind,DC=local	
-	Subnet	
Summary	192.168.12.0	
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.	
	<u> </u>	

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

a								- 1	o ×
elp									
1									
e Roles (1)								Actions	
Search						م ر	Queries 🔻 🔜 👻 👽	Roles	
Name	Status	Туре	Owner Node	Priority	nformation			leg Configure Role	
Rie Server	() Running	FileServer	SW1	Medium				Virtual Machines	
								treate Empty Role	
								View	
								Refresh	
								Help	
								FileServer	
								🗘 Start Role	
								😳 Stop Role	
								Add File Share	
								Move Move	
								😵 Change Startup Priority	
								🚯 Information Details	
								Show Critical Events	
								Add Storage	
								Add Resource	
								More Actions	
								× Remove	
								Properties	
								Help	
v 🕌 FileServe	_						Preferred Owners: Any node		
							include of the second s		
Status:									
	Running								
Priority:	Medium								
Priority: Owner Node:	Medium SW1								
Priority:	Medium SW1								
Priority: Owner Node: Client Access Nan	Medium SW1 me: FileServer								
Priority: Owner Node: Client Access Nan	Medium SW1 me: FileServer								
Priority: Owner Node: Client Access Nan	Medium SW1 me: FileServer								
Priority: Owner Node: Client Access Nan	Medium SW1 me: FileServer								
Priority: Owner Node: Client Access Nan	Medium SW1 me: FileServer								
Priority: Owner Node: Client Access Nan	Medium SW1 me: FileServer								
Priority: Owner Node: Client Access Nan	Medium SW1 me: FileServer								

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

• open Active Directory Users and Computers



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

Select User, Computer, Service Account, or Group	×
Select this object type:	
User, Computer, Group, or Built-in security principal	Object Types
From this location:	
starwind.local	Locations
Enter the object name to select (<u>examples</u>):	
Production	Check Names
Advanced	OK Cancel

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

ssion Entry for Computers		- 0	×
Delete aCSResourceLimits objects	Delete msKds-ProvRootKey objects		
Create applicationVersion objects	Create msKds-ProvServerConfiguration objects		
Delete applicationVersion objects	Delete msKds-ProvServerConfiguration objects		
Create certificationAuthority objects	Create MSMQ Queue Alias objects		
Delete certificationAuthority objects	Delete MSMQ Queue Alias objects		
Create Computer objects	Create ms-net-ieee-80211-GroupPolicy objects		
Delete Computer objects	Delete ms-net-ieee-80211-GroupPolicy objects		
Create Contact objects	Create ms-net-ieee-8023-GroupPolicy objects		
Delete Contact objects	Delete ms-net-ieee-8023-GroupPolicy objects		
Create document objects	Create msPKI-Enterprise-Oid objects		
Delete document objects	Delete msPKI-Enterprise-Oid objects		
Create documentSeries objects	Create msPKI-Key-Recovery-Agent objects		
Delete documentSeries objects	Delete msPKI-Key-Recovery-Agent objects		
Create Group objects	Create msPKI-PrivateKeyRecoveryAgent objects		
Delete Group objects	Delete msPKI-PrivateKeyRecoveryAgent objects		
Create groupOfUniqueNames objects	Create msPrint-ConnectionPolicy objects		
Delete groupOfUniqueNames objects	Delete msPrint-ConnectionPolicy objects		
Create groupPolicyContainer objects	Create msSFU30DomainInfo objects		
Delete groupPolicyContainer objects	Delete msSFU30DomainInfo objects		
Create InetOrgPerson objects	Create msSFU30MailAliases objects		
Delete InetOrgPerson objects	Delete msSFU30MailAliases objects		
Create IntelliMirror Group objects	Create msSFU30NetId objects		
Delete IntelliMirror Group objects	Delete msSFU30NetId objects		
Create IntelliMirror Service objects	Create msSFU30NetworkUser objects		
Delete IntelliMirror Service objects	Delete msSFU30NetworkUser objects		

• click OK on all opened windows to confirm the changes



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

Configuring Smb File Share

To Add SMB File Share

- 1. Open Failover Cluster Manager.
- 2. Expand the cluster and then click Roles.
- 3. Right-click the File Server role and then press Add File Share.

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

Select Profile	File share profile:	Description:				
Share Location	SMB Share - Quick	This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.				
Share Name	SMB Share - Advanced					
Other Settings	SMB Share - Applications NFS Share - Ouick	Suitable for general file sharing				
	NFS Share - Advanced	 Advanced options can be configured later by 				
		using the Properties dialog				

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



Share Location	Server Name	Status	Cluster Role	Owner Node	
Share Name	FileServer	Online	File Server		
Other Settings					
	Share location:				
	Select by <u>v</u> olume:				
	Volume	Free Space	Capacity File Syst	em	
	G:	9.91 GB	9.97 GB NTFS		
	The location of the f	ile share will be a new fold	der in the \Shares dir	ectory on the ca	lacted
	The location of the f	ie snare will be a new fold	uer in the shares dir	ectory on the se	iecteu
	volume.				

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

🜇 New Share Wizard			-		×
Specify share nan	ne				
Select Profile	Share name:	Share			
Share Location					_
Share Name	Share description:				
Other Settings					
Permissions					
	Local path to share:				
Results	G:\Shares\Share				
	If the folder doe	s not exist, the folder is created.			
	Remote path to sha	re:			
	\\FileServer\Share				
		< <u>P</u> revious <u>N</u> ext > <u>C</u> reated	ate [Cance	ł

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

continue.

🔚 New Share Wizard		-		×
Configure share s	settings			
Select Profile	Enable access-based enumeration]
Share Location	Access-based enumeration displays only the files and folders that a user access. If a user does not have Read (or equivalent) permissions for a fold			the
Share Name	folder from the user's view.			
Other Settings	✓ Enable <u>c</u> ontinuous availability			
Permissions	Continuous availability features track file operations on a highly available clients can fail over to another node of the cluster without interruption.	file share	so that	
Confirmation	Allow caching of share			
Results	Caching makes the contents of the share available to offline users. If the B Network Files role service is installed, you can enable BranchCache on the		he for	
	Enable BranchCache on the file share			
	BranchCache enables computers in a branch office to cache files down share, and then allows the files to be securely available to other compu-			
	Encrypt data access			
	When enabled, remote file access to this share will be encrypted. This sec unauthorized access while the data is transferred to and from the share. If and grayed out, an administrator has turned on encryption for the entire	this box		
	< <u>P</u> revious <u>N</u> ext >	ate [Cance	ł

8.Specify the access permissions for the file share.

New Share Wizard				— C	×		
Specify permise	sions to co	ontrol access					
Select Profile Share Location		is to access the files on a sha is, and, optionally, a central	-	combination of folder permission	s, share		
Share Name		Share permissions: Everyone Full Control					
Other Settings	<u>F</u> older per	missions:					
Permissions	Туре	Principal	Access	Applies To			
Confirmation	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			
	<u>C</u> ustom	ize permissions					
		< 1	Previous <u>N</u> e	xt > Create	Cancel		



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

Select Profile	Confirm that the following	are the correct settings, and then click Create.
Share Location Share Name	SHARE LOCATION Server:	FileServer
Other Settings	Cluster role:	Scale-Out File Server
Permissions	Local path:	C:\ClusterStorage\Volume1\Shares\Share
Confirmation	SHARE PROPERTIES	
	Share name: Protocol: Access-based enumeration: Caching: BranchCache: Encrypt data: Continuous availability:	Share SMB Disabled Disabled Disabled Enabled

10. Check the summary and click Close.



New Share Wizard			- 🗆 X
View results			
Select Profile	The share was success	fully created.	
	Task	Progress	Status
Share Name	Create SMB share		Completed
	Set SMB permissions		Completed
Confirmation			
Results			
		< <u>P</u> revious <u>N</u> ext >	Close Cancel

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.

Jond	Search									Actions	
Indexe Ite laws Ite laws Vool (dybum), Vool (dybum), Indexe Ite laws Ite laws									P Queres w L	I = - Roles	
						information				Rg Co	nfigure Role
v	E Helever	() Ranneg	He Sever	SW1	Medure						
v										- C+	ste Empty Rale
v Refamily Projekti											
V										18 Feb	NUD
v										E He	p .
V Reference Reference Reference										Share .	
v										¥ 9a	p Sharing
v Reference Polense/Drove: Any state Polense/Drove: Any state v Reference Polense/Drove: Any state Polense/Drove: Any state V Polense/Drove: Any state Polense/Drove: Any state										15 10	legih
V Before Protect/Drove: Jog 3085 Texes 00 Texes 00 Texes 00 News 00 Texes 00 Texes 00 10 01 348 S0										E Pa	peter
V Before Protect/Drove: Jog 3085 Texes 00 Texes 00 Texes 00 News 00 Texes 00 Texes 00 10 01 348 S0										10 14	4
States Path Pathon Controvan Andelsky: Fernanta 201 G1 SHR No Caller Undal State	. I. Below						 		Federard Damers	laru note	
Nere Adri Petaco Codiniza Nalisity Renatis											
3 05 G1 SMB No Cultor Default Strate		24		A	the second s	Part of the local data					
										1.1	



Configuring Nfs File Share

To Add NFS File Share

- 1. Open Failover Cluster Manager.
- 2. Expand the cluster and then click Roles.
- 3. Right-click the File Server role and then press Add File Share.

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

New Share Wizard		- 0	×
New Share Wizard Select the profile Share Location Share Name Other Settings Permissions Confirmation Results	for this share File share grofile: SMB Share - Quick SMB Share - Advanced SMB Share - Applications NFS Share - Quick NFS Share - Advanced	Description: This profile creates an SMB file share with settings appropriate for Hyper-V, certain databases, and other server applications.	×
		< <u>P</u> revious <u>N</u> ext > <u>C</u> reate Cancel	

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



Share Location	Server Name				
		Status	Cluster Role	Owner Node	
Share Name	FileServer	Online	File Server		
Other Settings					
	Share location:				
	Select by volume:				
	Volume	Free Space	Capacity File Sys	tem	
			9.97 GB NTES		
	G:	9.91 GB	5.57 00 14175		
	The location of the fi	9.91 GB le share will be a new fol		irectory on the se	elected
				irectory on the se	elected

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

New Share Wizard	- 0	×
Specify share n	ame	
Select Profile Share Location	Share name: Share	
	Local path to share:	
Share Name	G:\Shares\Share	
Authentication Share Permissions	If the folder does not exist, the folder is created. <u>Remote path to share:</u>	
	FileServer:/Share	
	< Previous Next > Create Cancel	-
	Create Cancel	_

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

continue.

New Share Wizard	- D X
Specify authent	ication methods
Select Profile Share Location Share Name Authentication	Specify the authentication methods that you want to use for this NFS share. Kerberos v5 authentication Kerberos v5 authentication(Krb5)
Share Permissions Permissions Confirmation Results	□ Kerberos v5 authentication and privacy(Krb5i) □ Kerberos v5 authentication and privacy(Krb5p) No server authentication ✓ No server authentication (AUTH_SYS) ✓ Enable unmapped user access ○ Allow unmapped user access by UID/GID
	Allow anonymous access
	< <u>P</u> revious <u>N</u> ext > <u>C</u> reate Cancel

8. Click Add and specify Share Permissions.

	the share permissions in the share are determined by tak			
Name	Permissions	Root Access	Encoding	
				(
	permissions on a file	permissions on a file share are determined by tak and the NTFS permission entries. The more restri	permissions on a file share are determined by taking into considerat and the NTFS permission entries. The more restrictive permissions ar	permissions on a file share are determined by taking into consideration both the share and the NTFS permission entries. The more restrictive permissions are then applied.



Grant permissions to access th netgroup. Select the access ar			
O <u>H</u> ost:			
Netgroup:			
			v
Client group:			
			v
All <u>Machines</u>			
Language encoding:		Share permissions:	
ANSI	~	No Access	¥
Allow root access (not rec	ommend	ed)	

9. Specify the access permissions for the file share.

New Share Wizard				- 0	×
Specify permiss	sions to co	ontrol access			
Select Profile Share Location Share Name Other Settings	permission	ns, and, optionally, a central nissions: Everyone Full Cont	access policy.	combination of folder permissions	, share
Permissions	Туре	Principal	Access	Applies To	
Confirmation Results	Allow Allow Allow Allow Allow Allow	BUILTIN\Users BUILTIN\Users CREATOR OWNER NT AUTHORITY\SYSTEM BUILTIN\Administrators BUILTIN\Administrators	Special Read & execu Full Control Full Control Full Control Full Control	This folder and subfolders This folder, subfolders, and files Subfolders and files only This folder, subfolders, and files This folder, subfolders, and files This folder only	
		< [Previous <u>N</u> e	xt > Create Ca	ancel



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

New Share Wizard			- 0
Select Profile Share Location Share Name Authentication Share Permissions Permissions	SHARE LOCATI Server: Cluster role: Local path:	FileServer File Server G:\Shares\Share	gs, and then click Create.
Confirmation	SHARE PROPE Share name:	Share	
	Protocol:	NFS	

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



New Share Wizard			- 0	×
View results				
Select Profile	The share was success	fully created.		
	Task	Progress	Status	
Share Name	Create NFS share		Completed	
	Set NFS permissions		Completed	
Results				
2				
		< <u>P</u> revious <u>N</u> ext	t > Close Cancel	

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

Roles (1)								Actions
Search						2 2	Gueres w La w w	Roles
Nere	Status	Tare	Owner Node	Presty	information			R) Configure Role
E HeSever	(1) Barring	File Server	SW1	Medure				Virtual Machines-
								Create Empty Rale
								Vatw
								a fatien
								Help:
								Ghave
								💥 Stop Sharing
								is Relieph
								Poperies
								Help
· I Beter							Parlament Damanna Janu mode	
	•						Palaned Dimon Ary sole	
Waters (2)	10.000						Preferred Dervers: Any toole	
Waters (2) Name	740			unut Auslahity			Phalamad Dimmons - Any social	
v Findaru States (d) New	740						Phelened Devree: Any scole	
Sinese (2)	10.000	5	felacel Contex DAB 50 DES 764		mmin Lair Dahi Dan		Parlament Dervers - Ann sock	
Vicens (2)	Parts G \	5	5M2 No				Padamat Denara - Alax sode	



Conclusion

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



Contacts

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

General Information: info@starwind.com

Sales: sales@starwind.com



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