

StarWind Virtual SAN[®] 3-node Compute and Storage Separated Scenario with Windows Server

2024

TECHNICAL PAPERS





Trademarks

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

Changes

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

Technical Support and Services

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

About StarWind

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

Copyright ©2009-2018 StarWind Software Inc.

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



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

Annotation

Relevant products

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

Purpose

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

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

Audience

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

Expected result

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

Prerequisites

StarWind Virtual SAN system requirements

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

Recommended RAID settings for HDD and SSD disks:

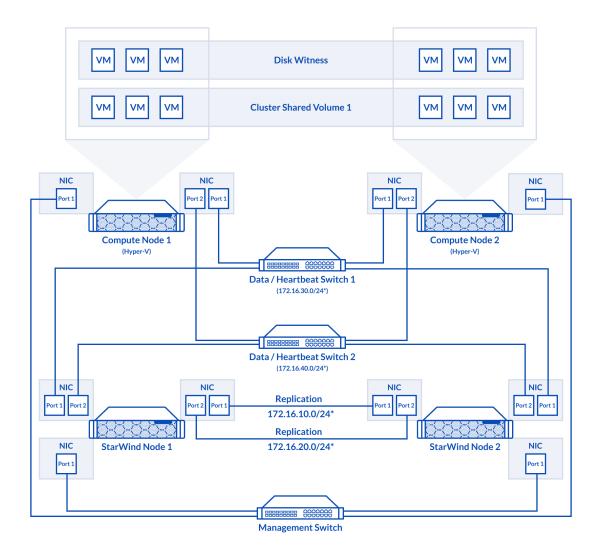


https://knowledgebase.starwindsoftware.com/guidance/recommended-raid-settings-for-h dd-and-ssd-disks/

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

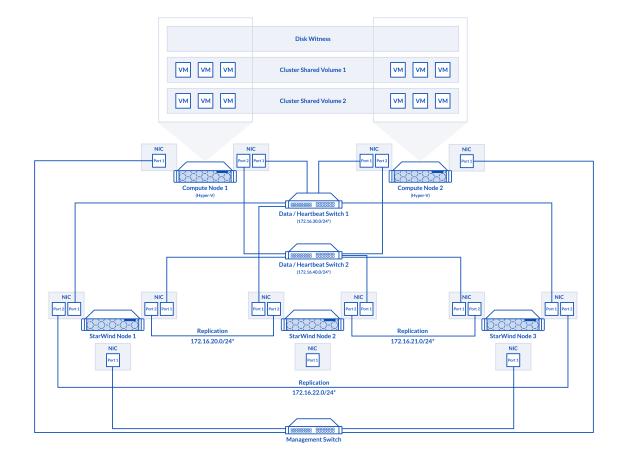
Solution diagram

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. Install Failover Clustering and Multipath I/O features, as well as the Hyper-V role on both cluster nodes. This can be done through the Server Manager (Add Roles and Features) menu item.

3. For a 2-node StarWind setup, configure network interfaces on each node to make sure that Synchronization and iSCSI/StarWind heartbeat interfaces are in different subnets and connected according to the network diagram above. In this document, 172.16.10.x and 172.16.20.x subnets are used for the Synchronization traffic, while 172.16.30.x and 172.16.40.x subnets are used for iSCSI/StarWind heartbeat traffic.

For a 3-node StarWind setup, configure the network interfaces on each node to make sure that the Synchronization and iSCSI/StarWind heartbeat interfaces are in different subnets and connected according to the network diagram above. In this document, 172.16.30.x, 172.16.40.x, subnets are used for the iSCSI/StarWind heartbeat traffic, while 172.16.20.x,172.16.21.x, 172.16.22.x subnets are used for the Synchronization traffic.

4. In order to allow iSCSI Initiators to discover all StarWind Virtual SAN interfaces, the StarWind configuration file (StarWind.cfg) should be changed after stopping the StarWind service on the node where it will be edited. Locate the StarWind Virtual SAN configuration file (the default path is "C:\Program Files\StarWind StarWind StarWind\StarWind.cfg") and open it via WordPad as Administrator. Find the *<iScsiDiscoveryListInterfaces value="0"/>* string and change the value from 0 to 1 (should look as follows: *<iScsiDiscoveryListInterfaces value="1"/>*). Save the changes and exit Wordpad. Once StarWind.cfg is changed and saved, the StarWind service can be restarted.

Enabling Multipath Support

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

mpiocpl

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



MPIO Properti	es			\times
MPIO Devices	Discover Multi-Paths	DSM Install	Configuration Snapsho	ot
SPC-3 comp	liant			
Device Ha	ardware Id			
Add sup	port for iSCSI devices			
	port for SAS devices			
			Add	
Others				
Device Ha	ardware Id			
			Add	
			nuu	
			OK Cancel	

- 7. When prompted to restart the server, click Yes to proceed.
- 8. 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 Server Selection Server Roles Features Confirmation	Select one or more roles to install on the selected server. Roles Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Sax Server	DESTINATION SERVER SW1.stanwind.local Description File Server manages shared folders and enables users to access files on this computer from the network.
Results	File and Storage Services (1 of 12 installed) File and Storage Services File Server BranchCache for Network Files Data Deduplication DFS Namespaces DFS Replication File Server VSS Agent Service ScSI Target Server ScSI Target Server ScSI Target Server Server for NFS Work Folders Vork Folders Storane Service (Installed)	

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.stanvind.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 Fax Server File and Storage Services (1 of 12 installed) File and Storage Services File Server BranchCache for Network Files Data Deduplication DFS Namespaces DFS Replication File Server Resource Manager File Server VSS Agent Service iSCSI Target Server iSCSI Target Server Server for NFS Work Folders Vork Folders Storage Services (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
Select server roles		DESTINATION SERVER SW1.starwind.local
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 Structure Fax 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 Structure File Server File Server File Server VSS Agent Service ScSI Target Storage Provider (VDS and VSS Server for NFS Work Folders File Server (Installed)	Description Server for NFS enables this computer to share files with UNIX- based computers and other computers that use the network file system (NFS) protocol.
	< <u>Previous</u> <u>N</u> ext >	Install Cancel

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

Installing Starwind Vsan For Hyper-V

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

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



Setup - StarWind Virtual SAN —	×
License Agreement Please read the following important information before continuing.	
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.	
STARWIND® LICENSE AGREEMENT	^
This StarWind License Agreement (the "Agreement") is a legal agreement between the entity indicated on the signature page as 'Licensee' or the licensee entity on whose behalf this Agreement is electronically executed by the authorized user (the "Licensee") and StarWind Software, Inc., a State of Delaware, USA corporation ("StarWind," and collectively with Licensee, the "Parties" and each, (a "Party")), that is entered into as of the date of acceptance hereof by both Parties hereto (the "Effective	
 I accept the agreement ○ I do not accept the agreement 	
<u>N</u> ext >	Cancel

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

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



Setup - StarWind Virtual SAN	_		×
Select Destination Location Where should StarWind Virtual SAN be installed?		Q	
Setup will install StarWind Virtual SAN into the following fol	der.		
To continue, click Next. If you would like to select a different folder	, click Br	owse.	
C: \Program Files \StarWind Software \StarWind	В	rowse	
At least 2.4 MB of free disk space is required.			
< <u>B</u> ack <u>N</u> ex	d >	Can	icel

5. Select the following components for the minimum setup:

- StarWind Virtual SAN Service. The StarWind Virtual SAN service is the "core" of the software. It can create iSCSI targets as well as share virtual and physical devices. The service can be managed from StarWind Management Console on any Windows computer that is on the same network. Alternatively, the service can be managed from StarWind Web Console deployed separately.
- StarWind Management Console. Management Console is the Graphic User Interface (GUI) part of the software that controls and monitors all storage-related operations (e.g., allows users to create targets and devices on StarWind Virtual SAN servers connected to the network).

NOTE: To manage StarWind Virtual SAN installed on a Windows Server Core edition with no GUI, StarWind Management Console should be installed on a different computer running the GUI-enabled Windows edition.



Setup - StarWind Virtual SAN	- 🗆	×			
Select Components					
Which components should be installed?					
which components should be installed?					
Select the components you want to install; clear the components you d	o not want t	o			
install. Click Next when you are ready to continue.					
StarWind Virtual SAN Server		\sim			
Service	170,8 MB				
Loopback Accelerator Driver	27070110				
Cloud Replicator for VTL	158,8 MB				
SPTD Driver (Alternative driver for exporting physical devices)	10010100				
StarWind Management Console	29,4 MB				
Configure user account for Web-access to Management Console	0,1 MB				
✓ Integration Component Library	7,8 MB				
	2,6 MB				
SMI-S Agent	51.5 MB	¥			
Current selection requires at least 207,3 MB of disk space.					
	_				
< <u>B</u> ack <u>N</u> ext >	C	ancel			
6. Specify Start Menu Folder.					
Setup - StarWind Virtual SAN	- 🗆	Х			
Select Start Menu Folder					
Where should Setup place the program's shortcuts?		a A			
Setup will create the program's shortcuts in the following Start	Menu folde	r .			
To continue, click Next. If you would like to select a different folder, clic	To continue, dick Next. If you would like to select a different folder, dick Browse				
StarWind Software\StarWind	Browse				

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

< <u>B</u>ack

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

<u>N</u>ext >

Cancel

StarWind Virtual SAN ® 3-node Compute and Storage Separated Scenario with Windows Server



- request time-limited fully functional evaluation key.
- request FREE version key.
- relect the previously purchased commercial license key.
- 9. Click on the Browse button to locate the license file.
- 10. Review the licensing information.

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

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

13. Repeat the installation steps on the partner node.

Creating Starwind Devices

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

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



			?	×
\leftarrow	Add D	evice Wizard		
	Select [Device Type you want to create or export as iSCSI Target		
		Hard Disk Device		
	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></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 Dev	vice Wizard		
Sp	ecify [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 M	1aximum available Size		
	Size:	128 MB ~		
		Next	Cano	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	icel

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.

Refresh Add Replica Replication Partner Click to add replication partner PROPERTIES Host Name	😴 Replication Manager for imagefile1	?	×
Replication Partner Click to add replication partner PROPERTIES	Refresh Add Replica Remove Replica		
PROPERTIES			
	Click to add replication partner		
Host Name	PROPERTIES		
	Host Name		
Target Name	Target Name		
Mode			
Priority			
Synchronization Status			
Synchronization Channel	Synchronization Channel		
Close		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 channel (heartbeat). At least one synchronization or heartbeat channel must be functio proper failover processing. Loss of all communication channels may lead to split issue, so it's recommended to use client iSCSI connection interfaces as heartbeat channel. Node Majority Process node and communication failures using majority policy: node stays activisees more than half of nodes including itself. In case of 2 storage nodes, requir configuring additional witness node. Does not require additional heartbeat channel 	nal for brain at e while i es	t
	Next	Can	cel

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 with 2-way replication and 4MB per 1 TB of HA device size for 3-way replication.

Failure journal

The strategy 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

The strategy 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.

		AM-based journal synchronization journal placed in RAM. Synchronization with RAM journal provides good O performance in any scenario. Disk-based journal synchronization journal placed on disk. Failure journal The strategy provides good IO performance while all device nodes are in a healthy state. Continuous journal The strategy guarantees fast synchronization and data consistency in all cases.	
←	Replication Wizard		
	Synchronization Journal Setup		
	RAM-based journal Synchronization journal placed in RAM. Synchronization with RAM journa IO performance in any scenario.	al provides good	
	 Disk-based journal Synchronization journal placed on disk. 		
	The strategy provides good IO performance while all device node	s are in a healthy	
		ncy in all cases.	
	Current Node My Computer\C\		
	Partner Node My Computer\C\		
	<u>N</u> (ext Can	cel

5. Click Change Network Settings and specify the interfaces for Synchronization and



Heartbeat Channels. Click OK and then click Next.

I		
172.16.20.0	v	
172.16.22.0		
172.16.30.0		v
172.16.40.0		v
192.168.12.0		v
172 16 20 0		
192.168.12.0		v
	172.16.22.0 172.16.30.0 172.16.40.0 192.168.12.0 172.16.20.0 172.16.21.0 172.16.30.0 172.16.40.0	172.16.22.0 172.16.30.0 172.16.40.0 192.168.12.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 I72.16.20.0 I72.16.20.0

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

- 7. Click Create Replica. Click Finish to close the wizard.
- 8. The successfully added device appears in StarWind Management Console.
- 9. Choose device, open Replication Manager and click Add replica again.



😴 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	æ

10. Select Synchronous "Two-Way" Replication as a replication mode. Click Next to proceed.



	?	?	×
\leftarrow	Replication Wizard		
	Replication Mode		
	Synchronous "Two-Way" Replication Replication Partner must be connected to Client as Source Device as well, MPIO on C must be enabled, needs dedicated high Performance Network Connection for Synchronization.	Client	
	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 mus added to cluster to make number of nodes odd number and enable proper functionin Node Majority policy.	st be	
	Next	Canc	el

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



	?	\times
Replication Wizard		
Add Partner Node		
Specify Partner Host Name or IP Address where Replication Node would be created	l	
Host Name or IP Address SW3 🗸 🗸		
Port Number 3261		
Next	(Cancel

12. 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 sp issue, 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 as sees more than half of nodes including itself. In case of 2 storage nodes, recomfiguring additional witness node. Does not require additional heartbeat channel. 	tional for blit brain beat ctive while i quires	it
	Next	Can	icel

13. Select Create new Partner Device and click Next.

14. Select a partner device Location and Synchronization Journal Strategy and click Next.

15. Click Change Network Settings.



		?	×
←	Replication Wizard		
	Network Options for Replication		
	Networks for Synchronization and Heartbeat		1
	Press "Change Network Settings" to configure Interfaces		
	Networks for Heartbeat		1
	Press "Change Network Settings" to configure Interfaces		
	Change Network Settings		
	ALUA preferred SW1, SW2, SW3		
	Change ALUA Settings		
	Next	Can	cel

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

Select synchronization channel					
Interfaces	Networks	Synchronization and	Heartbeat	^	
172.16.30.10	172.16.30.0		•		
172.16.40.10	172.16.40.0		•		
192.168.12.10	192.168.12.0		v	- 11	
🖃 Host Name: SV	V2				
172.16.20.20	172.16.20.0	\checkmark	Γ		
172.16.21.20	172.16.21.0				
172.16.30.20	172.16.30.0		V		
172.16.40.20	172.16.40.0		V		
192.168.12.20	192.168.12.0		\checkmark		
🖃 Host Name: SV	V3				
172.16.21.30	172.16.21.0	v			
172.16.22.30	172.16.22.0				
172.16.30.30	172.16.30.0		~		
172.16.40.30	172.16.40.0		•		
192.168.12.30	192.168.12.0		v		
				\checkmark	

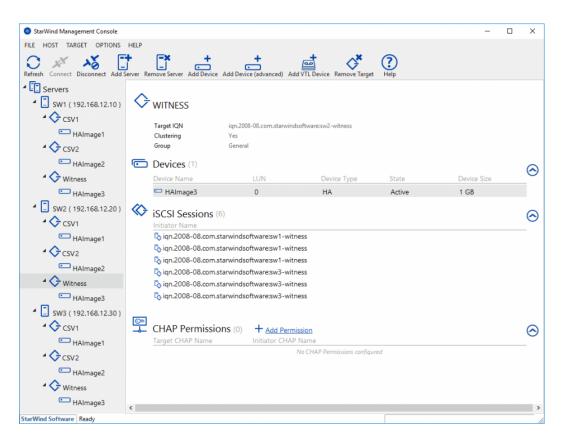
NOTE: It is not recommended to configure the Heartbeat and iSCSI channels on the same interfaces to avoid the split-brain issue. If the Synchronization and Heartbeat interfaces are located on the same network adapter, it is recommended to assign one more Heartbeat interface to a separate adapter.

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

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

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





NOTE: To extend an Image File or a StarWind HA device to the required size, please check the article below:

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

Node Majority

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



			?	×
÷	Replication Wizard			
	Failoura	r Stratagy		
	railove	r Strategy		
	Heartbeat Process node and communication failures using additional communication channel (heartbeat). At least one synchronization or heartbeat channel must be functional proper failover processing. Loss of all communication channels may lead to split brai issue, so it's recommended to use client iSCSI connection interfaces as heartbeat channel.		rain	
	٢	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, require configuring additional witness node. Does not require additional heartbeat channe	s	
		Net	Com	
		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.

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 with 2-way replication and 4MB per 1 TB of HA device size for 3-way replication.

Failure journal

The strategy 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

The strategy 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.

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

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

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

- 8. Press the Create Replica button and close the wizard.
- 9. The added devices will appear in StarWind Management Console.
- 10. Choose device, open Replication Manager and click Add replica again.



😴 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

11. Select Synchronous "Two-Way" Replication as a replication mode. Click Next to proceed.



		?	×
\leftarrow	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.	1 Client	
	Witness Node Witness node doesn't contain user data. In case when Node Majority policy is set f 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

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



		?	×
 Replication Wizard 			
Add Partner Node			
Specify Partner Host N	ame or IP Address where Replication Node would be created		
Host Name or IP Addre	ss SW3		
Port Number	3261		
	Next	Can	cel

13. 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 function: proper failover processing. Loss of all communication channels may lead to split bi issue, so it's recommended to use client iSCSI connection interfaces as heartbeat channel.	rain	
	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, require configuring additional witness node. Does not require additional heartbeat chann	s	
		Next	Cano	cel

14. Choose Create new Partner Device and click Next.

15. Specify the partner device Location and modify the target name if necessary. Click Next.

16. Select Synchronization Journal Strategy and click Next.

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

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

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

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

21. The added devices will appear in StarWind Management Console.

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



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

Provisioning Starwind Ha Storage To Windows Server Hosts

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

iscsicpl

2. Navigate to the Discovery tab.



iSC	SI Initiator Prope	rties			×
Та	argets Discovery	Favorite Targets	Volumes and Devices	RADIUS Configuratio	n
	Target portals				
	The system will lo	ok for Targets on fo	ollowing portals:	Refresh	
	Address	Port	Adapter	IP address	
	To add a target p	oortal, click Discover	Portal.	Discover Portal	
	To remove a targ then click Remove		address above and	Remove	
	iSNS servers			Refresh	
	The system is reg	istered on the follow	wing iSNS servers:	Refresh	1
	To add an iSNS se	erver, dick Add Serv	/er.	Add Server	
	To remove an iSN then click Remove	IS server, select the e.	e server above and	Remove	
			ОК	Cancel Ap	ply

3. Click the Discover Portal button. In the Discover Target Portal dialog, type in the iSCSI interface IP address of the first StarWind node that will be used to connect the StarWind provisioned targets. The steps below provide instructions how to discover targets within 172.16.30.X subnet. The same should be done for 172.16.40.X subnet Click Advanced...



Discover Target Portal	×			
Enter the IP address or DNS name and port number of the portal you want to add.				
To change the default settings of the disc the Advanced button.	overy of the target portal, dick			
IP address or DNS name:	<u>P</u> ort: (Default is 3260.) 3260			
Advanced	<u>O</u> K <u>C</u> ancel			

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



dvanced Settings	?	×
eneral IPsec		
Connect using		
-		1
Local adapter:	Microsoft iSCSI Initiator V	
Initiator <u>I</u> P:	172.16.30.40 ~	
Target portal IP:	~	
CRC / Checksum		
Data digest	<u>H</u> eader digest	
initiator. The name will specified.	ign. 1991-05.com.microsoft:compute1.starwind.local	
Name:	Iqn 1991 ostonning osori computer i star vinano car	
Target <u>s</u> ecret:		
RADIUS.	entication ther specify an initiator secret on the Configuration page or use erate user authentication credentials enticate target credentials	
	OK Cancel A	<u>pply</u>

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



Discover Target Portal	×			
Enter the IP address or DNS name and port number of the portal you want to add.				
To change the default settings of the discovery of the target portal, dick the Advanced button.				
IP address or DNS name: 172.16.30.20	Port: (Default is 3260.) 3260			
<u>A</u> dvanced	<u>Q</u> K <u>C</u> ancel			

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



vanced Settings	?	>
eneral IPsec		
Connect using		
_	Microsoft iSCSI Initiator	
Local adapter:		
Initiator <u>I</u> P:	172.16.30.40 ~	
Target portal IP:	\sim	
CRC / Checksum		
Data digest	Header digest	
specified.	iqn.1991-05.com.microsoft:compute1.starwind.local	
– Target <u>s</u> ecret:		
RADIUS.	thentication either specify an initiator secret on the Configuration page or use nerate user authentication credentials thenticate target credentials	
	OK Cancel A	pply

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



Discover Target Portal	×			
Enter the IP address or DNS name and port number of the portal you want to add.				
To change the default settings of the dis the Advanced button.	covery of the target portal, dick			
IP address or DNS name: 172.16.30.30	<u>P</u> ort: (Default is 3260.) 3260			
<u>A</u> dvanced	<u>OK</u> _ancel			

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



Connect using	
ocal adapter:	Microsoft iSCSI Initiator \checkmark
initiator IP:	172.16.30.40 ~
arget portal IP:	~
CRC / Checksum	
Data digest	<u>H</u> eader digest
an initiator. To use, specify the sa nitiator. The name wi	
CHAP Log on informa CHAP helps ensure co an initiator. To use, specify the sa nitiator. The name wi specified.	ation Innection security by providing authentication between a target and Imme name and CHAP secret that was configured on the target for this
CHAP Log on informa CHAP helps ensure co an initiator. To use, specify the sa	ation Innection security by providing authentication between a target and Imme name and CHAP secret that was configured on the target for this Ill default to the Initiator Name of the system unless another name is
CHAP Log on informa THAP helps ensure co an initiator. To use, specify the sa initiator. The name wi specified. Mame: Mame: Perform mutual au	ation Innection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this ill default to the Initiator Name of the system unless another name is iqn.1991-05.com.microsoft:compute1.starwind.local

- 9. Repeat the steps 1-8 on for the 172.16.40.X subnet.
- 10. Repeat the steps 1-9 on the partner node
- 11. All the target portals are added on the first Compute node.



iSCSI Initiator Prope	SCSI Initiator Properties				×
Targets Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration	
Target portals					
	ok for <u>T</u> argets on fo	ollowing portals:		R <u>e</u> fresh	
Address	Port	Adapter	I	P address	
172.16.30.30	3260	Microsoft iSCSI Initia	tor	172.16.30.4	
172.16.40.10	3260	Microsoft iSCSI Initia	tor 1	172.16.40.4	
172.16.40.20	3260	Microsoft iSCSI Initia	tor 1	172.16.40.4 🗸	
<				>	
To add a target p	ortal, click Discover	Portal.	Disco	over <u>P</u> ortal	
To remove a targ then click Remove		address above and		<u>R</u> emove	
iSNS servers The system is reg Name	The system is registered on the following iSNS servers: Refresh				
	erver, click Add Serv IS server, select the e.			d Server Re <u>m</u> ove	
		ОК	Cance	L Apply	,

Address	Port	Adapter	IP Adress
172.16.30.10	3260	Microsoft iSCSI initiator	172.16.30.40
172.16.30.20	3260	Microsoft iSCSI initiator	172.16.30.40
172.16.30.30	3260	Microsoft iSCSI initiator	172.16.30.40
172.16.40.10	3260	Microsoft iSCSI initiator	172.16.30.40



172.16.40.20 3260 Microsoft iSCSI initiator 172.16.30.40

172.16.40.30 3260 Microsoft iSCSI initiator 172.16.30.40

12. All the target portals are added on the second Compute node.

ets Dis	covery	Favorite Targe	ts Volu	mes and Devices	RADIUS	Configur	ation
		-				-	
rget por	tals —						
'he syste	em will lo	ok for <u>T</u> argets o	n followir	ng portals:		R <u>e</u> fresh	
ddress		Port	Ada	apter	IP	address	^
72.16.30	.20	3260	Mici	rosoft iSCSI Initiato	or 13	72.16.30.5	50
72.16.30	.30	3260	Mic	rosoft iSCSI Initiato	or 13	72.16.30.5	50
72.16.40). 10	3260	Mici	rosoft iSCSI Initiato	or 13	72.16.40.5	50 🗸
2						2	>
o add a t	target p	ortal, <mark>cl</mark> ick Disco	ver Porta	al.	Disco	ver <u>P</u> ortal	I
o remove nen click		et portal, select	the addr	ess above and		<u>R</u> emove	
	ers em is reg	istered on the fo	ollowing <u>i</u>	SNS servers:		Re <u>f</u> resh	
		istered on the fo	ollowing <u>i</u>	SNS servers:		Refresh	
Name	em is reg	erver, click Add S		SNS servers:		Re <u>f</u> resh	
To add an	m is reg	rver, dick Add S S server, select	Gerver.		Ad		•
Name To add an	m is reg	rver, dick Add S S server, select	Gerver.		Ad	d Server Remove	<u>Apply</u>
iame o add an	n iSNS se e an iSN Remove	erver, click Add S S server, select	Gerver. the serv	er above and	Ad	d Server Remove	Apply
lame o add an o remove	n iSNS se e an iSN Remove	erver, click Add S S server, select	Gerver.	er above and	Ad	d Server Remove	



172.16.30.20	3260	Microsoft iSCSI initiator	172.16.30.50
172.16.30.30	3260	Microsoft iSCSI initiator	172.16.30.50
172.16.40.10	3260	Microsoft iSCSI initiator	172.16.30.50
172.16.40.20	3260	Microsoft iSCSI initiator	172.16.30.50
172.16.40.30	3260	Microsoft iSCSI initiator	172.16.30.50
 Tawasha			

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 Node as well as the list of networks served by the StarWind Node (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	RADIUS Configuration
Quick Connect	
To discover and log on to a target using a basic connection, to DNS name of the target and then click Quick Connect.	type the IP address or
Target:	Quick Connect
Discovered targets	
	<u>R</u> efresh
Name	Status ^
iqn.2008-08.com.starwindsoftware:sw1-csv1	Inactive
iqn.2008-08.com.starwindsoftware:sw1-cvs2	Inactive
iqn.2008-08.com.starwindsoftware:sw1-witness	Inactive
iqn.2008-08.com.starwindsoftware:sw2-csv1	Inactive
iqn.2008-08.com.starwindsoftware:sw2-cvs2	Inactive
iqn.2008-08.com.starwindsoftware:sw2-witness	Inactive
iqn.2008-08.com.starwindsoftware:sw3-csv1	Inactive
ign.2008-08.com.starwindsoftware:sw3-cvs2	Inactive 💙
<	>
To connect using advanced options, select a target and then click Connect.	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.	De <u>v</u> ices
24	Canad
OK	Cancel Apply

- 2. Select the Witness target from the first StarWind Node 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	
<u>A</u> dvanced OK	Cancel

4. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Initiator IP, select 172.16.30.40, in Target portal IP, select 172.16.30.10. Confirm the action



Connect using		
Local adapter:	Microsoft iSCSI Initiator $\qquad \checkmark$	
Initiator <u>I</u> P:	172.16.30.40 ~	
Target portal IP:	172.16.30.10 / 3260 ~	
CRC / Checksum		
Data digest	Header digest	
an initiator. To use, specify the si nitiator. The name w	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 helps ensure co an initiator. To use, specify the si initiator. The name w specified.	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 helps ensure co an initiator. To use, specify the si initiator. The name w	onnection security by providing authentication between a target and a me name and CHAP secret that was configured on the target for this	
CHAP helps ensure co an initiator. To use, specify the si initiator. The name w specified.	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. Select the Witness target from the first StarWind Node again and click Connect.

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



Connect To Target	×
Target name: ign.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 Cance	el

7. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Initiator IP, select 172.16.40.40, in Target portal IP, select 172.16.40.10. Confirm the action



Connect using	
ocal adapter:	Microsoft iSCSI Initiator $\qquad \sim$
initiator <u>I</u> P:	172.16.40.40 ~
[arget portal IP:	172.16.40.10 / 3260 🗸
CRC / Checksum	
Data digest	Header digest
CHAP Log on inform CHAP helps ensure co an initiator. To use, specify the sa nitiator. The name w	
THAP 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. To use, specify the sa	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

- 8. Select the Witness target from the second StarWind Node and click Connect.
- 9. Enable checkboxes as shown in the image below. Click Advanced...



Connect To Target		×
Target name:		
iqn.2008-08.com.starwindsoftware:sw2-witnes	s	
Add this connection to the list of Favorite Tar This will make the system automatically attem connection every time this computer restarts	pt to restore the	
⊡ <u>E</u> nable multi-path		
<u>A</u> dvanced	ОК	Cancel

10. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Initiator IP, select 172.16.30.40, in Target portal IP, select 172.16.30.20. Confirm the action



Connect using	
Local adapter:	Microsoft iSCSI Initiator $\qquad \checkmark$
Initiator <u>I</u> P:	172.16.30.40 ~
Target portal IP:	172.16.30.20 / 3260 🗸 🗸
CRC / Checksum	
Data digest	<u>H</u> eader digest
an initiator. To use, specify the sa nitiator. The name w	
CHAP Log on inform CHAP helps ensure co an initiator. To use, specify the sa initiator. 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 vill default to the Initiator Name of the system unless another name is
CHAP Log on inform CHAP helps ensure co an initiator. To use, specify the sa initiator. The name w specified. <u>N</u> ame:	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, To use, specify the sa	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

11. Select the Witness target from the second StarWind Node once again and click Connect.

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



Connect To Target		×
Target name:		1
iqn. 2008-08.com.starwindsoftware:sw2-witnes]
Add this connection to the list of Favorite Tar. This will make the system automatically attem connection every time this computer restarts.	pt to restore the	
∑ <u>E</u> nable multi-path		
<u>A</u> dvanced	ОК	Cancel

13. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Initiator IP, select 172.16.40.40, in Target portal IP, select 172.16.40.20. Confirm the action.



Connect using	
ocal adapter:	Microsoft iSCSI Initiator \sim
nitiator <u>I</u> P:	172.16.40.40 ~
arget portal IP:	172.16.40.20 / 3260 🗸
CRC / Checksum	
Data digest	Header digest
CHAP Log on inform CHAP helps ensure co in initiator. To use, specify the sa nitiator. The name w	
THAP helps ensure co an initiator. To use, specify the sa hitiator. 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

14. Select the Witness target from the third StarWind Node and click Connect.

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



Connect To Target	×
Target name:	
iqn.2008-08.com.starwindsoftware:sw3-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	
<u>A</u> dvanced OK	Cancel

16. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Initiator IP, select 172.16.30.40, in Target portal IP, select 172.16.30.30. Confirm the action.



dvanced Settings	?	×
eneral IPsec		
Connect using		
Local adapter:	Microsoft iSCSI Initiator	
Initiator <u>I</u> P:	172.16.30.40 ~	
Target portal IP:	172.16.30.30 / 3260 ~	
CRC / Checksum		
	Header digest	
specified.	vill default to the Initiator Name of the system unless another name is	
<u>N</u> ame:	iqn.1991-05.com.microsoft:compute1.starwind.local	
Target <u>s</u> ecret:		
RADIUS.	uthentication either specify an initiator secret on the Configuration page or use enerate user authentication credentials uthenticate target credentials	
	OK Cancel A	pply

17. Select the Witness target from the third StarWind Node one more and click Connect.

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



Connect To Target	×		
Target name: iqn.2008-08.com.starwindsoftware:sw3-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			
<u>A</u> dvanced OK	Cancel		

19. Select Microsoft iSCSI Initiator in the Local adapter dropdown menu. In Initiator IP, select 172.16.40.40, in Target portal IP, select 172.16.40.30. Confirm the action.



Ivanced Settings		?	×
eneral IPsec			
Connect using			
Local adapter:	Microsoft iSCSI Initiator	\sim	
	172.16.40.40		
Initiator <u>I</u> P:		~	
Target portal IP:	172.16.40.30 / 3260	\sim	
CRC / Checksum			
Data digest	Header digest		
specified.	vill default to the Initiator Name of the system unless another name is		
<u>N</u> ame:	iqn.1991-05.com.microsoft:compute1.starwind.local		
Target <u>s</u> ecret:			
RADIUS.	uthentication either specify an initiator secret on the Configuration page or use enerate user authentication credentials uthenticate target credentials		

20. Repeat the steps 1-19 for all remaining HA device targets.

21. Repeat the steps 1-19 on the other Compute node, specifying the corresponding local and data channel IP addresses. The result should look like in the screenshot below.



iSCSI Init	iator Prope	rties				×
Targets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuratio	n
-	Connect					
		g on to a target usin arget and then click	ng a basic connection, t Quick Connect.	ype the IP	address or	
<u>T</u> arget	:			Qu	uick Connect	
Discove	ered targets					_
					<u>R</u> efresh	
Name	1			Status		^
iqn.2	008-08.com.	starwindsoftware:s	w1-csv1	Connecte	d	
iqn.2	008-08.com.	starwindsoftware:s	w1-cvs2	Connecte	d	
iqn.2	008-08.com.	starwindsoftware:s	w1-witness	Connecte	d	
		starwindsoftware:s		Connecte	-	
		starwindsoftware:s		Connecte	-	
iqn.2	008-08.com.	starwindsoftware:s	w2-witness	Connecte	d	
		starwindsoftware:s		Connecte	-	
	008-08.com.	starwindsoftware:s	w3-cvs2	Connecte	d	~
<					>	
	nect using a onnect.	dvanced options, se	elect a target and then		Co <u>n</u> nect	
	npletely disco lick Disconne	onnect a target, sele ct.	ect the target and		Disconnect	
		es, including configu nd click Properties.	uration of sessions,	ļ	Properties	
	For configuration of devices associated with a target, select the target and then dick Devices.				De <u>v</u> ices	
			ОК	Cancel	Ар	ply

Configuring Multipath

NOTE: It is recommended to set the Round Robin or Least Queue Depth MPIO load balancing policy.



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

2. In the Devices dialog, click MPIO

Devices		×
Name Address Disk 1 Port 5:	s Bus 0: Target 0: LUN 0	
Volume path names:		
Legacy device name:	\\. \PhysicalDrive 1	
Device interface name	\\?\mpio#disk&ven_starwind e: «	d∏_starwind&rev_000
Configure Multipath I	O (MPIO)	
To configure the MPI selected device, click		<u>M</u> PIO
		<u>O</u> K

3. Select the appropriate load balancing policy.



evice Details				>
MPIO				
Load balance	policy:			
Least Queu	e Depth			~
Description	1			
distributin processing This device h	g paths.			s to lightly loaded
Path Id	Status	Type	Weight	Session ID
0x7705	Conne	Active	n/a	ffffc90eec43b010-4000
0x7705	Conne	Active	n/a	ffffc90eec43b010-4000
0x7705	Conne	Active	n/a	ffffc90eec43b010-4000
<				>
			De	tails <u>E</u> dit
			ж	Cancel Apply

Configuring Disks to Servers

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



📅 Disk Manager	ment						_		×
File Action V	/iew Help								
🔶 🔿 🔤 🖬									
Volume	Layout	Туре	File Syste		Capacity	Free Spa	% Free		
Storage (D:)	Simple	Basic	NTFS	Healthy (P.,		32.78 GB	66 %		
System (C:)	Simple	Basic	NTFS	Healthy (B.		6.53 GB	27 %		
- System Reserve	ed Simple	Basic	NTFS	Healthy (S	500 MB	172 MB	34 %		
-Disk 0									^
Basic	System Reserv	ed		System (C:)					
25.00 GB Online	500 MB NTFS Healthy (System	Active Pri	many Partiti	24.51 GB NTFS Healthy (Boot, Pa	ge File, Crash Di	ump Primary Pa	rtition)		
	Treating (System	, Active, i fi			gerne, enamer	amp, i innary i a	interesting		
	-		1	,					_
Disk 1 Basic	Storage (D:)						///////////////////////////////////////	77777	777
49.88 GB	49.87 GB NTFS								
Online	Healthy (Primary Partition)								
O Disk 2									
Unknown									
6.00 GB Offline ()	6.00 GB Unallocated								
•	ondirocated								
	·								
Olisk 3 Unknown									
10.00 GB	10.00 GB								
Offline 🚺	Unallocated								
Olisk 4									
Unknown 1.00 GB	1.00 GB								
Offline 1	Unallocated								
-									
Linglic system	Drimono nontiti]				`
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	х
You must initialize a disk before Logical Disk Manager can access it. Select disks:	
 ✓ Disk 2 ✓ Disk 3 ✓ Disk 4 	
Use the following partition style for the selected disks: MBR (Master Boot Record) GPT (GUID Partition Table)	
Note: The GPT partition style is not recognized by all previous versions of Windows.	
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: Browse 	
O Do not assign a drive letter or drive path	
< Back Next > Ca	ancel



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

New Simple Volume Wizard		×			
Format Partition To store data on this partition, you must format it first.					
Choose whether you want to format	this volume, and if so, what settings you want to use.				
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
Mount in the following empty NTFS folder:	-
	Browse
O 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.

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



ᡖ Server Manager		- D X
	anager • Dashboard • 🤅	Cluster-Aware Updating
Image: Dashboard Image: Local Server Image: All Servers Image: File and Storage Services Image: Performance Services Image: Hyper-V	WELCOME TO SERVER MANAGER 1 Configure this line QUICK START 2 Add roles and fe 3 Add other server WHAT'S NEW 0 5	Component Services Computer Management Defragment and Optimize Drives Disk Cleanup Event Viewer Failover Cluster Manager Hyper-V Manager iSCSI Initiator Local Security Policy Microsoft Azure Services
	4 Create a server	ODBC Data Sources (32-bit) Ver to cloud service ODBC Data Sources (64-bit) Performance Monitor Print Management Resource Monitor Services System Configuration
	File and Storage 1 Services 1 Manageability Imageability Events Events Performance Service BPA results Perform	Windows Firewall with Advanced Security Windows Memory Diagnostic Windows PowerShell Windows PowerShell (x86) Windows PowerShell ISE mance Windows PowerShell ISE Windows PowerShell ISE Windows PowerShell ISE

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 Actions		
Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.		•
Configuration changes to your failover clusters. 🛛 💐 Validate Configuration		
Create Cluster		
A failover cluster is a set of independent computers that work together to increase the		
a valiability of server roles. The clustered servers (called nodes) are connected by physical cables and by software. If one of the nodes fails, another node begins to provide services.		•
Cables and by somware. If one of the nodes fails, another node begins to provide services. This process is known as failover.		
Properties		
Clusters		
Name Role Status		
No items found.		
Management To begin to use failover clustering, first validate your hardware configuration, and then create a cluster. After these steps are complete, you can manage the cluster. Managing a		
cluster can include copying roles to it from a cluster running Windows Server 2016 or supported previous versions of Windows Server.		
Validate Configuration		
Create Cluster		
Connect to Cluster		
More Information		
Calover 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		×
Select Se	ervers		
Before You Begin Select Servers Validation Warning Access Point for Administering the Cluster Confirmation Creating New Cluster Summary	Add the names of all the set Enter server name: <u>S</u> elected servers:	ervers that you want to have in the cluster. You must add at least one server. Browse Compute 1.starwind.local Compute 2.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 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 Cluster				
Before You Begin	Type the name you v	vant to use when administering the cluster.				
Select Servers Access Point for	Cluster Name:	Production]		
Administering the Cluster Confirmation		The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an				
Creating New Cluster		Networks	Address			
Summary		192.168.12.0/24	192.168.12.100			
				,		
		< <u>P</u> revious	Next > Cancel]		

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



🚏 Create Cluster Wiz	ard X
Confirmat	ion
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	Compute 1.starwind.local
Summary	Compute2.starwind.local
	Cluster registration
	DNS and Active Directory Domain Services
	Add all eligible storage to the cluster.
	To continue, click Next.
	< <u>P</u> revious <u>N</u> ext > 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.



韂 Create Cluster Wiz	ard	×
Summary		
Before You Begin Select Servers	You have successfully completed the Create Cluster Wizard.	
Access Point for Administering the	Node	^
Cluster	Compute 1.starwind.local	
Confirmation	Compute2.starwind.local	
Creating New Cluster	Cluster	
Summary	Production	
	IP Address	
	192.168.12.100	
	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 biohest availability of the cluster. If this	~
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.	<u>V</u> iew Report
		<u>F</u> inish

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						-	ΟX
					Actions		
Roles Modes Construction Storage	Search Name Add Disks to a Cluster	Status Assign		ries 👻 🔛 👻 👻 Owner Node	Disks 🔮 Add Disk	×	•
Pools Enclosures Networks	Select the disk or disks the Available disks:		1				,
i Networks ा Cluster Events		Disk Info Disk 1 on node COMPUTE1 Disk 2 on node COMPUTE1 Disk 3 on node COMPUTE1	Capacity 1.00 GB 5.00 GB 6.00 GB	Signature/Id {4c8a1108-ca81.4677. {529cbafc-7213.49c8- {7d5635bf-4a89.44b7-	92c1-dd6b9e99f37d}		
					OK Car	ncel	
< >>							

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



📲 Failover Clus	ster Manager				-	\times
File Action	View Help					
🗢 🔿 🔁 🗖						
Hailover Clust	ter Manage Disks (3)				Actions	
V Production	Configure Role	_	P	Queries 🔻 🔛 👻 👻	Disks	-
🃫 Not	Validate Cluster	Status	Assigned To	Owner Node	🛃 Add Disk	
✓ 📇 Sto ∄	View Validation Report	Online	Available Storage	Compute1	📑 Move Available Storage	•
	Add Node	() Online	Available Storage	Compute1	View	•
	Close Connection	Online	Available Storage	Compute1	Refresh	
📫 Net 関 Clu	Reset Recent Events				🛛 Help	
11 CIU						
	More Actions		r Quorum Settings			
	Refresh	Copy Cluster Rol	es			
	Properties	Shut Down Clust	er			
	Help	Destroy Cluster	Destroy Cluster			
		Move Core Clust	er Resources	>		
		Cluster-Aware U	odating			
			-			
	<			>		
	*					
	·					
< .	>					
hese actions are	used less frequently than other o	luster actions.				

3. Follow the wizard and choose 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	r Quorum Wizard	×
Select Qu	uorum Witness	
Before You Begin Select Quorum Configuration Option	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.	
Select Quorum Witness	 Configure a disk witness Adds a quorum vote of the disk witness 	
Configure Storage Witness Confirmation	 Configure a file share witness Adds a quorum vote of the file share witness 	
Configure Cluster Quorum Settings Summary	 Configure a cloud witness Adds a quorum vote of the cloud witness 	
Summary	O Do not configure a quorum witness	
	Failover Cluster Quorum and Witness Configuration Options	
	< Previous Next > Cancel	

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	at you want to assign as ti	he disk witness.		_
Select Quorum Witness	Name	Status	Node	Location	
Configure Storage Witness Confirmation Configure Cluster Quorum Settings Summary	Volume: (\\?\ Cluster Disk 2 Volume: (G)	 Online (Chkdsk sc File System: NTFS Online (Chkdsk sc File System: NTFS Online File System: NTFS 	948 MB free of 990 MB	Available Storage	
			< <u>P</u> revious <u>N</u> e	xt > Cancel	

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

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



Cluster Disk 1 Properties	\times	-	\times
File Action View Help			
🗢 🔿 🔂 🖬 General			
Image: Solower Cluster Manager Disks (3) Name: CSV/2 > mage: Solower Cluster Manager Search Status: CSV/2 Search Status: Onine Status:			•
Nodes Name Status Assigned		Disk	
✓ Storage Image: Cluster Disk 1 Image: Cluster Disk 2 Image: Disks Image: Cluster Disk 2 Image: Cluster Disk 2	_	e Available Storage	+
Pools Couter S Call Couter S C	apacit 97 Gl	esh	,
Networks Cluster Events		, isk 1	_
			-
		g Online Offline	
		mation Details	
		v Critical Events	
Cluster Disk 1	>	re -	►
		ication	►
Volumes (1)		e Actions	►
CSV2 (C:\ClusterStorage\Volume1) OK Cancel Ap	pply	ove from Cluster S	
CSVFS 9.92 GB free of 9.97 GB		erties	
	👔 Helj	р	
Volumes Disks: Cluster Disk 1			

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.

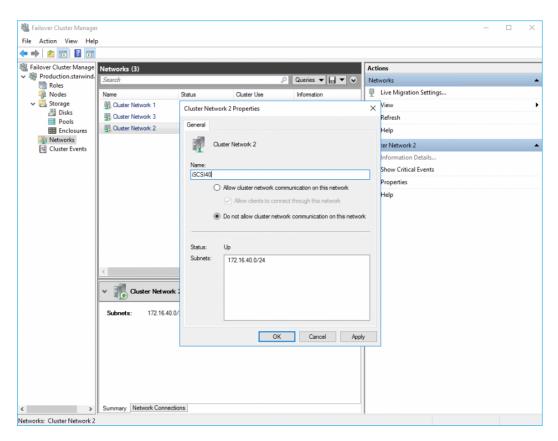
📲 Failover Cluster Manager					>	/
					/	` I
Eile Action View Help	2					
Failover Cluster Manage					Actions	_
 Production.starwind. 	Disks (3) Search		P Qu	ieries 🔻 🔒 🔻 🗸	Actions Disks	•
Roles					Disks	•
🏺 Nodes 🗸 📇 Storage	Name	Status	Assigned To	Owner Node		-
Disks	ESV1	Online Online	Cluster Shared Volume	Compute1 Compute2	Move Available Storage	<u> </u>
Pools	A Witness	Online Online	Disk Witness in Quorum	Compute2 Compute1	View	•
Enclosures 🙀 Networks	C withess	() Online	Disk withess in Quorum	Computer	Q Refresh	
Cluster Events					👔 Help	
	<			>		
	*					
< >						
Disks:						
Configuring	g Cluster I	Vetwork	Preference	es		



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

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

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



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



 Bailover Cluster Manager File Action View Help 	þ						-	□ ×
📲 Failover Cluster Manage	Networks (3)					Act	ions	
 Production.starwind. Roles 	Search			P Q	ueries 🔻 🕞 👻 😔	Net	tworks	
Nodes	Name	Status	Cluster Use	Information		1	Live Migration Settings	
V 📇 Storage	🔢 iSCSI30	Live Migration Se	ettings		×		View	•
Disks	Hanagement					Q	Refresh	
Enclosures	ISCSI40	Networks for Live				?	Help	
Networks Cluster Events		Use the buttons	ore networks for virtu s to list them in order	al machines to use from most preferre	for live migration. d at the top to	Ma	nagement	
En Cluster Events		least preferred	at the bottom.			8	Information Details	
							Show Critical Events	
		Name			Up		Properties	
	Management Subnets: 192.168.12	✓ ²⁰ / ₂ Manage → 9:SCS140 → 0:SCS140)	Cancel	Down	2	Help	
< >	Summary Network Connecti	ons						

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.



Hailover Cluster Manager	r					-	×
<u>File Action View Help</u>							
🗢 🔿 🖄 📰 🖬							
📲 Failover Cluster Manage	Networks (3)				Actions		
 Production.starwind. Roles 	Search			🔎 Queries 🔻 🔛 💌 😪	Networks		
Nodes	Name 🔻	Status	Cluster Use	Information	Live Migration Settings		
✓ Call Storage	Hanagement	💿 Up	Cluster and Client		View		•
Disks	🔢 iSCSI40	💿 Up	None		Refresh		
Enclosures	ISCSI30	💿 Up	None		👔 Help		
Networks					Management		
ing cluster events					Information Details		
					B Show Critical Events		
					Properties		
					👔 Help		
	<			>			
	v 🚺 Management						
	Subnets; 192.168.12	0.04					
	Subnets: 192.168.12						
< >	Summary Network Connect	tions					

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 Manager		- 🗆 X
File Action View Help		
🗢 🔿 🙍 🖬 🖬 🖬		
Hailover Cluster Manage Cluster Produ	oduction.starwind.local	
Production.stary Configure Role	Productions Production	arwind.local
Nodes Validate Cluste		re Role
> 🛃 Storage View Validation	ion Report 🛛 🔰 Networks: Cluster Network 2, Cluster Network 3, Cluster Network 1, Cluster Network 4 😻 Validate	Cluster
Networks Cluster Even Add Node		idation Report
Close Connect	tical: 52. Error: 16. Warring: 5	le
	Close G	nnection
Reset Recent E	S Reset Re	cent Events
More Actions	ns > ecific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2016 or supported previous versions of Windows Server.	tions 🕨
View	Falover duster topics on the Web View	+
Refresh	G. Refresh	
Properties	Properti	25
Help	2 Help	
	Name Produ	action 🔺
	R Bring Or	line
Navi	vigate Take Off	
Roles	s 🖻 Nodes 🖻 Storage 🖻 Networks 🖻 Cluster Events	ion Details
roles	E Proces Proces Prevents Public Proces	itical Events
		tions 🕨
 Clust 	Ister Core Resources	
Name	Status Information	25
Server Nat	Help	
	Name: Production	
	🐩 IP Address: 192.168.12.86 🛞 Online	
This action enables you to select a role that yo		

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

🧞 High Availability	Nizard		×
Select Ro	ble		
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 Corrigination Server	A Fil	cription: e Server provides a central location our network where files are shared se by users or by applications.
		< <u>P</u> revious	<u>N</u> ext > Cancel

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



High Availability	ver Type	×
Before You Begin	Select an option for a clustered file server:	
Select Role File Server Type Client Access Point Confirmation Configure High Availability	 Elle Server for general use Use this option to provide a central location on your network for users to share files or for server applications that open and close files frequently. This option supports both the Server Message Block (SMB) and Network File System (NFS) protocols. It also supports Data Deduplication, File Server Resource Manager, DFS Replication, and other File Services role services. Scale-Out File Server for application data 	
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.	
-	< <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 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	(1) The NetBIOS name is limited to 15 characters. All networks were configured automatically.	
	< Previous Next > 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 \	Vizard		×
tonfirmat	ion		
Before You Begin Select Role	You are ready to configure high availability for a File	e 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 > Cancel	

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

Click Finish to close the Wizard.



🧱 High Availability \	Wizard	Х
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:



A result in the set of the set	🍓 Failover Cluster Manager								-	o ×
Internet Internet <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>										
V Ref Part Ref Re										
Image: State Type OwerHold Parky Menue Parket Over. Hold Parky Me	Failover Cluster Manage	Roles (1)							Actions	
Image: Radia Tapa Tapa Ower tots Note Medica Image: Radia Tapa Tapa Ower tots Note Medica Image: Radia Tapa Tapa	Production.starwind Poler	Search						🔎 Queries 🔻 🔜 👻	Roles	
Pede Image: Section of the section	Nodes			Туре	Owner Node	Priority	Information		Nonfigure Role	
Peder Peder	V 📇 Storage	EleServer	😟 Failed	Scale-Out File Server	SW1	Medium				•
Industry New									Treate Empty Role	
C Outre fores	Enclosures									•
Image: Second Secon	Networks Networks Itil Cluster Events									
✓ Reference ✓ Nores ✓ Reference ✓ Nores ✓	En entre crents								😰 Help	
Senser Sense									FileServer	
Add Statup Priority Monantian Datalian Monantian									🔅 Start Role	
✓ Findement Findement Addression Image: State Priority on the									Stop Role	
Comparing Status Protections: August Comparing Status Protections: A										
Monitor Database Mon									Move Move	•
✓ Telsarer Telsa										•
Add Storage Add Stor										
Image: Base of the Server Reference Propertie Mate: Barring Reference Image: Barring Noney: Modes State State Or encloses ins: reference Image: Barring Image: Barring Noney: Modes State State Image: Barring Modes Image: Barring Noney: Modes State State Image: Barring Modes State Image: Barring State State Image: Barring State State Image: Barring State State Image: Barring State State Image: Barring State <td></td>										
MoreAddown Mereadown Mareadown										
V FinServer Properties Mater: Finserve Properties Mater: Finserve Properties Over Moders: SV11 Over Moders: SV12										•
V Indexer Properties Statu: Burg Math: Burg Control Actions Burg W Addresses 102/101/225										•
V The Server Proteined Ources: Auguste Status: Rursing Modersen:: Status: Outer Access Name: Referent Proteined Ources: Proteined Ources: Addensent:: 192.158.22.55										
V Telserver Pedered Owner: Any sould State: Horing: Mode: None (construction) State: State: Owner Konsens: State: State: IP Addressen: 132.168.12.85										
Sadaz: Pursing Pleafy: Modum Ormer Hode: SPT1 Comer Look: SPT Comer Look: SPT									Help	
Sadaz: Burning Pledity: Modum Ommer Hode: SPT1 Commer Hode: SPT1 C										
Sadaz: Burning Pledity: Modum Ommer Hode: SPT1 Commer Hode: SPT1 C		u III Dieferrer						Performed Comments Amounted		
Piongry Modum Owner Nade: SW1 Claret Access Name: Referent IP Addresser: 192.168.2.285		* The server						Freiened Owners. Any house		
Over Node: SV11 Over Access Mark: Fischer If Addresses: 132.163.12.25										
Over Access Nacc: FreStover IP Addresses: 152-168-12-85										
IF Addresses: 152.163.12.85										
< Summery [Resources [States]										
< Summery Resources Shares										
< Summery Resources (States)										
< Summery [Resources [States]										
< > Summery Resources States										
< >> Summery Resources (States)										
< Summery Resources Shares										
< Summery Resources States										
	<pre></pre>	Summary Resources St	hares							
									1	

- 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)

elect User, Computer, Service Account, or Group		
elect this object type:		
User, Computer, Group, or Built-in security principal	(Object Types
rom this location:		
starwind.local		Locations
Inter the object name to select (<u>examples</u>):		
Production		Check Names

 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 Occurre Alice alice to	
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



lew Share Wizard		
elect the profi	ile for this share	
Select Profile	File share profile:	Description:
Share Location	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.
Permissions	NFS Share - Quick NFS Share - Advanced	
Confirmation		
Results		
		< Previous Next > Create Cancel

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



	20.	ver:						
Share Location	S	erver Name	Status	Cluster	Role	Owner Node		
Share Name	Fi	ileServer	Online	Scale-C)ut File			
Other Settings								
Permissions								
Confirmation								
Results								
		re location:						
	۲	Select by volume:						
		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	will be a new fold	er in the \	Shares dire	ctory on the se	elected	

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



New Share Wizard			<u> </u>		×
Specify share nam	е				
Select Profile	Share n <u>a</u> me:	Share			
Share Location					_
Share Name	Share <u>d</u> escription:				
Other Settings					
Permissions					
Confirmation	Local path to share:				
Results	C:\ClusterStorage\V	/olume1\Shares\Share			
	If the folder does	s not exist, the folder is created.			
	Remote path to sha	re:			
	\\FileServer\Share				
		< Previous Next >	e	Cancel	

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



New Share Wizard	– 🗆 X
Configure share	e 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. Enable continuous availability Continuous availability features track file operations on a highly available file share so that clients can fail over to another node of the cluster without interruption. Allow caching of share Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share. Enable BranchCache on the file share BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch. Encrypt data access When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.
	< Previous Next > Create Cancel

8. Specify the access permissions for the file share.



elect Profile hare Location hare Name ther Settings ermissions	remote ma Permission permission	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 constrained delegation to enable combination of folder permissions, sha
Confirmation	Type Allow Allow Allow Allow Allow	Principal BUILTIN\Users BUILTIN\Users CREATOR OWNER NT AUTHORITY\SYSTEM BUILTIN\Administrators BUILTIN\Administrators	Access Special Read & execu Full Control Full Control Full Control Full Control	Applies To 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
	Custon	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.



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

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	0	wner Node Priority	Information		Sconfigure Role
Rie Server		Jut File Server SV				Virtual Machines
						Treate Empty Role
						View
						Refresh
						Help
						FileServer
						🔅 Start Role
						🔅 Stop Role
						Add File Share
						😥 Move
						1 Change Startup Priority
						🚯 Information Details
						Show Critical Events
						Add Storage
						Add Resource
						More Actions
						X Remove
						Properties
						Help
v 🕌 FileServer					Preferred Owners: Any node	
Shares (2)						
Name	Path	Protocol	Continuous Availability	Remarks		
🤳 ClusterStorage\$		SMB	No	Cluster Shared Volumes Default Share		
🤳 Share	C:\ClusterStorage\Volume1\Shares\	Share SMB	Yes			
						1

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.

🖏 Failover Cluster Manag	jer							 ×
File Action View H	1							
🗢 🔿 🙇 🗔 🖬	201 1							
📲 Failover Cluster Manag	Cluster Production.starwind	l.local				^	Actions	
Production.stary Roles	Configure Role	er Production					Production.starwind.local	
Nodes		ered roles and 2 nodes.					is Configure Role	
> 📇 Storage iii Networks	View Validation Report	al		Networks: Cluster Network 2, Cluster	Network 3, Cluster Network 1, Cluster Network 4		Validate Cluster	
Retworks	Add Node			Subnets: 3 IPv4 and 1 IPv6			View Validation Report	
	Close Connection	tical: 52, Error: 16, Warning: 5					P Add Node	
	Reset Recent Events						Close Connection	
							Reset Recent Events	
		secific clustered role, add one or more	servers (nodes), or copy ro	oles from a cluster running Windows Serv	er 2016 or supported previous versions of Windows Server.		More Actions	→
	View >			Failover cluster topics on the Web			View	•
	Refresh						Q Refresh	
	Properties						Properties	
	Help						🕜 Help	
	E Custo Award Opdaurig						Name: Production	•
	P					_	🙀 Bring Online	
	 Navigate 						Take Offline	
	Roles	Nodes	Storage	Networks	Cluster Events		🚯 Information Details	
						-	B Show Critical Events	
	Cluster Core Reso						More Actions	•
		burces					🔀 Remove	
	Name Server Name		Status	Information			Properties	
	Mame: Production		Online				🛛 Help	
	IP Address: 192.16	58 12 86	Online					
	Cluster Infrastructure		C state					
< >	Balan an in with		A			~	I	
This action enables you to s	elect a role that you can configure t	for high availability						

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



iigh Availability	Wizard			×
Select Ro	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 Corst 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	er Type	
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 wher	accessing this clustered role:						
Select Role	Name:	FileServer			1				
File Server Type	-				1				
Client Access Point	The NetBIOS name is limited to 15 characters. One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an								
Select Storage	address.	or each network to	be used, make sure the netw	ork is selected, and then type an					
Confirmation		Networks		Address	1				
Configure High Availability		Networks	192.168.12.0/24	Address 192.168.12.85					
Summary			102.100.12.0/24	102.100.12.00					
					1				
			< <u>P</u> revious	<u>N</u> ext > Cancel					

Click Next to continue.

6. Select the Cluster disk and click Next.



🧞 High Availability	Wizard				×
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 File System: NTFS	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.



🧞 High Availability \	Vizard		×
tonfirmat	ion		
Before You Begin Select Role	You are ready to configure high availability for a File	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.		
		< <u>P</u> revious <u>N</u> ext > Cance	4

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.

nager							- 0
Help							
1							
nage Roles (1)							Actions
wind Search						🔎 Queries 🔻 🔛 👻 😪	Roles
Name	Status	Туре	Owner Node	Priority	Information		89 Configure Role
Rie Server	Running	FileServer	SW1	Medium			Virtual Machines
							time Create Empty Role
e							View
							Refresh
							Help
							FileServer
							🗘 Start Role
							🗘 Stop Role
							Add File Share
							Move Move
							1 Change Startup Priority
							🚯 Information Details
							Show Critical Events
							Add Storage
							Add Resource
							More Actions
							× Remove
							Properties
							I Help
👻 🕌 FileServer						Preferred Owners: Any node	
* in Heserver						Preferred Owners: Any node	
Status:	Running						
	Medium						
Owner Node: Client Access Name:	SW1 EleServer						
	192.168.12.85						
> Summary Resources S	haras						
							1

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

sion Entry for Computers		 ×
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 a SMB file share, typically used to share files with
Share Name	SMB Share - Advanced	Windows-based computers.
Other Settings	SMB Share - Applications NFS Share - Ouick	 Suitable for exercise file abasian
	NFS Share - Advanced	 Suitable for general file sharing Advanced options can be configured later by
		using the Properties dialog

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



Share Location	Server Name	Status	Cluster Role	Owner Node	
Share Name	FileServer	Online	File Server		
Other Settings					
	Share location:				
	0.01.11				
	Select by volume:				
	Select by volume: Volume	Free Space	Capacity File Sy	stem	
			Capacity File Sy 9.97 GB NTFS	stem	
	Volume			stem	
	Volume			stem	
	Volume G: The location of the f		9.97 GB NTFS		elected
	Volume G:	9.91 GB	9.97 GB NTFS		elected

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					
Confirmation	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				
		< Previous Next >	eate	Cance	el

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

continue.

ᡖ New Share Wizard		-		×
Configure share s	settings			
Select Profile	Enable access-based enumeration]
Share Location Share Name	Access-based enumeration displays only the files and folders that a user h access. If a user does not have Read (or equivalent) permissions for a folde folder from the user's view.			the
Other Settings	✓ Enable continuous availability			
Permissions Confirmation Results	Continuous availability features track file operations on a highly available f clients can fail over to another node of the cluster without interruption. Allow caching of share	ile share	so that	
Results	Caching makes the contents of the share available to offline users. If the Bi 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 downl 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 seculurauthorized access while the data is transferred to and from the share. If and grayed out, an administrator has turned on encryption for the entire s	this box i	_	
	< <u>Previous</u> <u>N</u> ext >	ate	Cance	4

8.Specify the access permissions for the file share.

elect Profile hare Location		is to access the files on a sha is, and, optionally, a central	-	combination of folder permissions, s
hare Name	Share perr	missions: Everyone Full Cont	rol	
Other Settings	<u>F</u> older per	missions:		
ermissions	Туре	Principal	Access	Applies To
onfirmation	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
	Custom	nize permissions		



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:	Share SMB
	Access-based enumeration:	Disabled
	Caching:	Disabled
	BranchCache:	Disabled
	Encrypt data:	Disabled
	Continuous availability:	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	
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.

Roles (1)							Actions
Search						D Games + La + v	Roles
Nene	Status Tar	ar Own	v Node Passey	Monatory		and the second	R) Configure Rale
E. Hellever	(1) Ranney Me	le Sever SW1	Medum				Virtual Machines-
121110000							Create Empty Role
							Varue
							E fafeth
							Help
							Share .
							🗶 Stop Sharing
							is Reliegh
							Dipeter
							Halp
						Preferred Demons - Any scole	in .
v 🛃 ReServer							
v 📳 Referen							
Warms (2)	he	Patacol	Continuous Austability	Periate			
New OS	fuer G1	5348	50	Remarks Cluster Default Share			
Name Anno	Patr						
Name Anno	fuer G1	5348	50				



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



Server Name Status Cluster Role Owner Node Ihare Name FileServer Online FileServer Other Settings ermissions FileServer Server Name Confirmation tesults Share location: Select by yolume: Volume Free Space Capacity File System G: 9.91 GB 9.97 GB NTFS	Name r Settings issions				
nare Name Other Settings termissions Confirmation tesults Share location: Select by <u>v</u> olume: Volume Free Space Capacity File System	r Settings issions	FileServer	Online	File Server	r i i i i i i i i i i i i i i i i i i i
ermissions confirmation tesults Share location: Select by <u>v</u> olume: Volume Free Space Capacity File System					
ermissions confirmation tesults Share location: Select by <u>v</u> olume: Volume Free Space Capacity File System					
Share location: Select by <u>v</u> olume: Volume Free Space Capacity File System					
Share location: Image: Select by volume: Volume Free Space Capacity File System					
Share location: Image: Select by volume: Volume Free Space Capacity File System	te				
Volume Free Space Capacity File System		Character Mark			
······		Share location:			
	0				
	Q	Select by volume:	Free Space	ace Capacity File Sys	ile System
	9	Select by <u>v</u> olume: Volume			
	6	Select by <u>v</u> olume: Volume			
The location of the file share will be a new folder in the \Shares directory on the selected	Q	Select by <u>v</u> olume: Volume			
volume.	Q	Select by <u>v</u> olume: Volume G:	9.91 GB	GB 9.97 GB NTFS	ITFS
The location of the file share will be a new folder in the \Shares directory on the selec	6	Select by <u>v</u> olume: Volume			
	Q	Select by <u>v</u> olume: Volume G:	9.91 GB	GB 9.97 GB NTFS	ITFS
	0	Select by volume: Volume G: The location of the file share	9.91 GB	GB 9.97 GB NTFS	ITFS
	6	Select by <u>v</u> olume: Volume			
	Q	Select by <u>v</u> olume: Volume G:	9.91 GB	GB 9.97 GB NTFS	ITFS
	Q	Select by <u>v</u> olume: Volume G:	9.91 GB	GB 9.97 GB NTFS	ITFS
	Q	Select by <u>v</u> olume: Volume			
The location of the file share will be a new folder in the \Shares directory on the selected	6	Select by <u>v</u> olume: Volume			
	6	Select by <u>v</u> olume: Volume			
	9	Select by <u>v</u> olume: Volume			
	0	Select by volume:	Free Space	ace Canacity File Sur	ile Sustem
G: 9.91 GB 9.97 GB NTFS					
······	()				
······	(1)				
······	()				
······	()				
······					
······					
······		Share location:			
······		Share location:			
······		Share location:			
······		Share location:			
Volume Free Space Capacity File System		Share location:			
Volume Free Space Capacity File System	S	Character Caracter			
Select by <u>v</u> olume: Volume Free Space Capacity File System		Character and Character			
Select by <u>v</u> olume: Volume Free Space Capacity File System					
Share location: Image: Select by volume: Volume Free Space Capacity File System	te				
Share location: Select by volume: Volume Free Space Capacity File System					
esults Share location: Select by <u>v</u> olume: Volume Free Space Capacity File System					

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.

pecify authent	ication methods
Select Profile Share Location Share Name Authentication Share Permissions Permissions Confirmation Results	Specify the authentication methods that you want to use for this NFS share. Kerberos v5 authentication Kerberos v5 authentication(Krb5) Kerberos v5 authentication and integrity(Krb5i) Kerberos v5 authentication and privacy(Krb5p) No server authentication No server authentication (AUTH_SYS) Enable unmapped user access Allow unmapped user access by UID/GID Allow unmapped user access
	< Previous Next > Create Cancel

8. Click Add and specify Share Permissions.

wn below. The final a ion both the share po e then applied. Encoding	
Encoding	
	(



Grant permissions to access th netgroup. Select the access an		_	
○ <u>H</u> ost:			
Netgroup:			
			~
Client group:			
			~
All <u>M</u> achines			
Language encoding:		Share permissions:	
ANSI	~	No Access	Ý
Allow root access (not reco	ommend	ed)	

9. Specify the access permissions for the file share.

Select Profile Share Location Share Name Other Settings	Permission permission	ns to access the files on a sha ns, and, optionally, a central missions: Everyone Full Cont	access policy.	combination of folder permissions,	share
Permissions	Туре	Principal	Access	Applies To	
Confirmation Results	Allow Allow Allow Allow Allow <u>C</u> ustom	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	



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

onfirm selectic Select Profile Share Location		ne following are the correct settir	ngs, and then click Create.
Share Name	Server:	FileServer	
Authentication	Cluster role:		
Share Permissions	Local path:	G:\Shares\Share	
Permissions	SHARE PROPER	RTIES	
Confirmation	Share name:	Share	
Results	Protocol:	NFS	

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



New Share Wizard			>	¢
View results				
Select Profile	The share was success	fully created.		
	Task	Progress	Status	
Share Name	Create NFS share		Completed	
	Set NFS permissions		Completed	
Results				
		< Previous Next	> 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

ioles (1)								Actions
Search						 	 Dianas 🕶 🖬 💌 🗢	
Nere	Status	Tipe	Overair Node	Printy	information			R) Configure Rate
E HeSever	(i) Ranneg	He Sever	SM1	Medure				Virtual Machines
								Create Empty Rale
								Vatur
								G fafech
								Help:
								Ghave
								🗙 Stop Sharing
								🚊 Relieph
								Popeties
								Halp-
100							Ref - 17	
- Hasser	•						Performed Dermons Arry mode	
Vieros (2)	10.000						Photomet Derroris - Any node	
Waters (2)	7en			nurus Austability			Philamed Demons. July, mode	
Waters (2)	10.000	9	ndacol Contin Mil No Mil Ta Tak		Receive Cluster Darius Dana		 Philamed Dervers. Jack mode	
Vienes 123	Ann GN	9	342 No				Preferred Derrors: Any node	
Vienes 123	Ann GN	9	342 No				 Performed Demons - Any mode	
Vienes 123	Ann GN	9	342 No				Payloned Durves - Jack rook	
Vienes 123	Ann GN	9	342 No				Netword Denvis . Jes sold	
Vienes 123	Ann GN	9	342 No			 	 Pedered Dennes - Annota	



Conclusion

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



Contacts

US Headquarters	EMEA and APAC
 +1 617 829 44 95 +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.