

Global-Active Device Private Cloud Quorum in VMware ESXi

v1.0.1

Implementation Guide

Reduce the costs of Global-Active Device by using a virtual machine instead of a physical storage system as the quorum. Remove the complexity of manually deploying a GAD Private Cloud Quorum.

Hitachi Vantara

MK-92RD8089-01

July 2023

© 2023 Hitachi Vantara LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively, "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.HitachiVantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

- 1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and
- 2) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, Flash Copy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, BCPI™ and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or web site are properties of their respective owners.

Table of Contents

Preface	4
About this document.....	4
Document conventions.....	4
Intended audience.....	4
Referenced documents	4
Accessing product downloads.....	4
Comments	5
Getting Help.....	5
Executive Summary	6
Configuration and Specifications	7
VMware Virtual Machine	7
VMware ESXi Virtual Machine	8
Deployment	8
Port Exemption	12
Access Quorum VM	12
Global-Active Device Quorums.....	14
Create iSCSI Paths	14
Discover External Volumes	16
Define GAD Quorums	19
Appendix A: Mutual CHAP Authentication (Optional).....	20
Enable on targetcli.....	20
Enable on iSCSI Ports	21
Create iSCSI Paths	22

Preface

About this document

This guide provides instructions for deploying Global-active device (GAD) Private Cloud Quorum in VMware ESXi.

Document conventions

This document uses the following typographic convention:

Convention	Description
Bold	- Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. - Indicates emphasized words in list items.
<i>Italic</i>	Indicates a document title or emphasized words in text.
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>

Intended audience

This document is intended for Hitachi Vantara and Global-active device users with an interest in installing Private GAD Private Cloud Quorum running SUSE Linux 15 SP4 on VMware ESXi.

Referenced documents

- [Hitachi Global-Active Device User Guide](#)
- [Linux SCSI Target: Targetcli](#)
- [Global-Active Device Cloud Quorum Implementation Guide](#)

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: <https://support.hitachivantara.com/>.

Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Comments

Please send us your comments on this document to GPSE-Docs-Feedback@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara.

Getting Help

[Hitachi Vantara Support Connect](#) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](#) is a global online community for customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Executive Summary

Global-active device (GAD) Private Cloud Quorum is a virtual machine image provided by Hitachi Vantara through the form of OVF files. The purpose is to simplify and enhance GAD by providing an on-premises quorum that is automatically configured and easy-to-use. This guide provides instructions on how to set up and use GAD Private Cloud Quorum on VMware ESXi.

Configuration and Specifications

VMware Virtual Machine

The following settings were used for the virtual machine image:

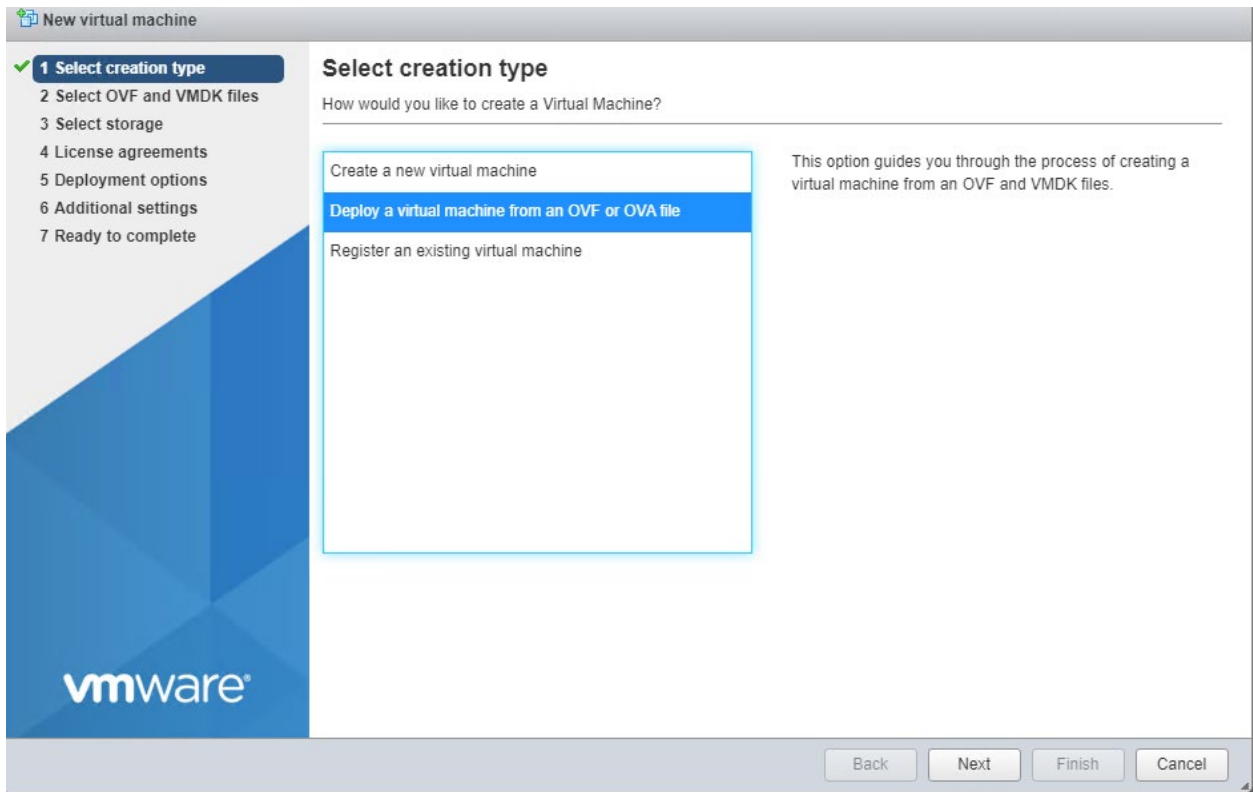
- VMware vSphere version: 7.0U3 +
- Operating system: SUSE Linux Enterprise Server 15 SP4
- Kernel: 5.14.21-150400.22-default
- Instance type:
 - CPU: 1 virtual CPU
 - Memory: 1 GB
 - Disks: Premium SSD 67 GB
- Targetcli version: 2.1.54

VMware ESXi Virtual Machine

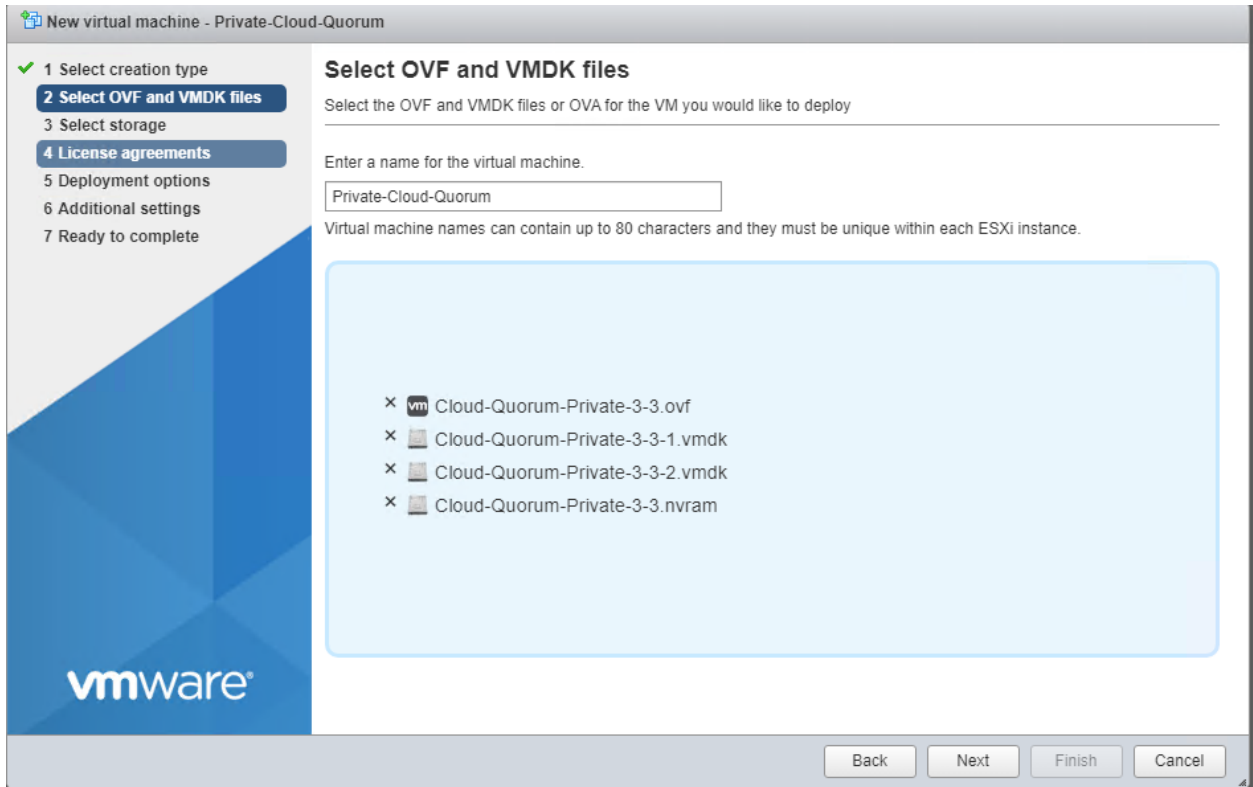
Deployment

This section provides instructions for creating the virtual machine on VMware ESXi that will function as the iSCSI target.

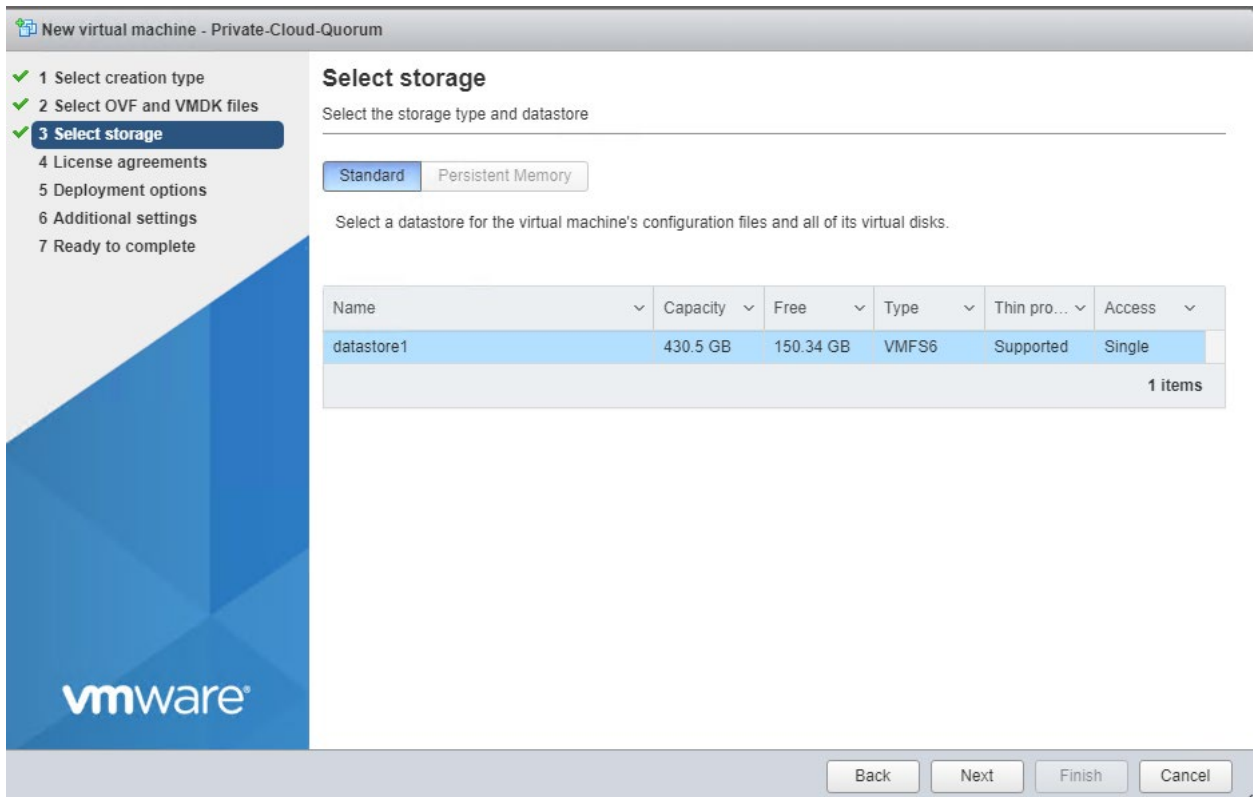
1. To use Private GAD Quorum, navigate to the Create VM screen, select **Deploy a virtual machine from an OVF or OVA file**, and click **Next**.



2. Under Select OVF and VMDK files, enter a name for the virtual machine.
After selecting the required files from the ISO, you will see the following screen:



3. Select a datastore and click **Next**.



- From the **VM Network** drop-down menu, click the network you have set up.

For disk provisioning, we recommend **Thin**.

New virtual machine - Private-Cloud-Quorum

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 **Deployment options**
- ✓ 5 Ready to complete

Deployment options

Select deployment options

Network mappings	VM Network	VM Network
Disk provisioning	☒ Thin ☐ Thick	
Power on automatically	☒	

Back Next Finish Cancel

- Click **Finish**.

New virtual machine - Private-Cloud-Quorum

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 **Ready to complete**

Ready to complete

Review your settings selection before finishing the wizard

Product	Cloud-Quorum-Private-3-3
VM Name	Private-Cloud-Quorum
Files	Cloud-Quorum-Private-3-3-1.vmdk Cloud-Quorum-Private-3-3-2.vmdk Cloud-Quorum-Private-3-3.nvram
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

 Do not refresh your browser while this VM is being deployed.

Back Next Finish Cancel

6. After you log on to the console, enter the following and then add the iSCSI Qualified Names (IQN) of your GAD storage system ports separated by spaces:

Login: admin

Password: Hitachi123!

/home/admin/quorum_setup.sh

```
localhost login: admin
Password:
No mail.
Last login: Thu Mar 16 16:08:03 on tty1
admin@localhost:~$ /home/admin/quorum_setup.sh iqn.1234-99.jj.co.hitachi.rsd.r77.i.07777.1a_
```

Port Exemption

Ensure that port 3260 is the default port used for iSCSI.

Access Quorum VM

This section provides instructions for verifying whether the quorum was set up properly and for configuring the quorum after setup.

1. Use an SSH client (such as putty) to log in to your quorum VM. Use the private IP and SSH key assigned to your VM.
2. Log in to the quorum. The default username is admin.
3. Run the configuration script: `./menu.sh`

```
*****
Global-Active Device Cloud Quorum Menu
*****
[1] Add Quorum
[2] Delete Quorum
[3] Add IQN Node
[4] Delete IQN Node
[5] Refresh Portal
[6] Enable CHAP Authentication
[7] View Configuration
[8] Help
[9] Exit
*****
Choice: [1 - 9]
```

4. To view the current configuration, enter 7.

```
*****
Choice: [1 - 9]
7
targetcli shell version 2.1.fb49
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/> o- / ..... [.]
..]
  o- backstores ..... [...]
    | o- block ..... [Storage Objects: 0]
    | o- fileio ..... [Storage Objects: 1]
    | | o- volume0 ..... [/quorums/volume0 (13.0GiB) write-back activated]
    | |   o- alua ..... [ALUA Groups: 1]
    | |     o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
    | o- pscsi ..... [Storage Objects: 0]
    | o- ramdisk ..... [Storage Objects: 0]
    | o- rbd ..... [Storage Objects: 0]
  o- iscsi ..... [Targets: 1]
    | o- iqn.2003-01.org.linux-iscsi.q-code.x8664:sn.9bdf33afba5e ..... [TPGs: 1]
    |   o- tpg1 ..... [no-gen-acls, no-auth]
    |     o- acls ..... [ACLs: 4]
    |       | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c42.1g .... [Mapped LUNs: 1]
    |       | | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |       | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c42.3g .... [Mapped LUNs: 1]
    |       | | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |       | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c4a.1e .... [Mapped LUNs: 1]
    |       | | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |       | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c4a.2e .... [Mapped LUNs: 1]
    |       | | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |     o- luns ..... [LUNs: 1]
    |       | o- lun0 ..... [fileio/volume0 (/quorums/volume0) (default_tg_pt_gp)]
    |     o- portals ..... [Portals: 1]
    |       o- 172.30.255.6:3260 ..... [OK]
```

If the setup was successful, you will see volume0 and your storage system IQNs listed under the acls directory.

From the configuration menu, you can also add and remove quorum volumes and IQNs, refresh the portal, and enable Challenge Handshake Authentication Protocol (CHAP).

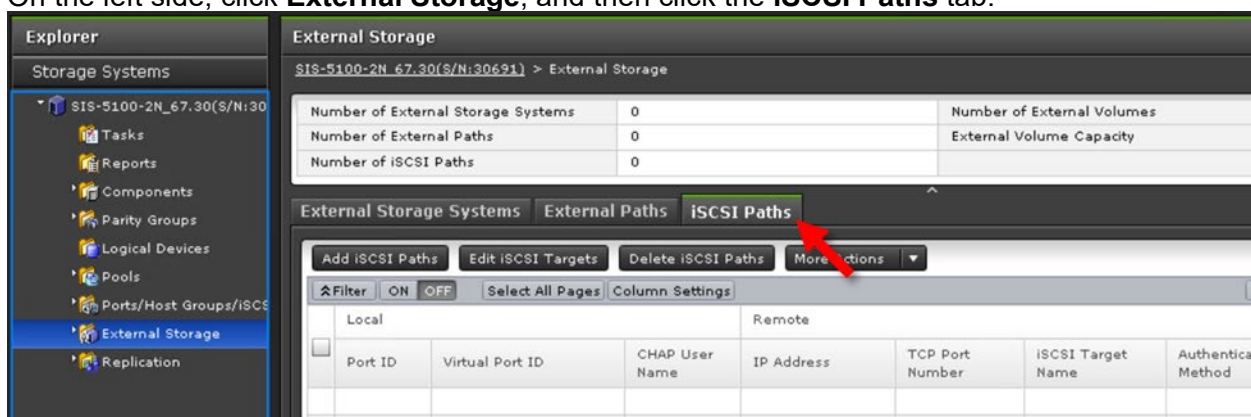
Note: If you intend to use CHAP, ensure to enable it during initial configuration because making changes to CHAP settings in the future may be difficult or not possible.

Global-Active Device Quorums

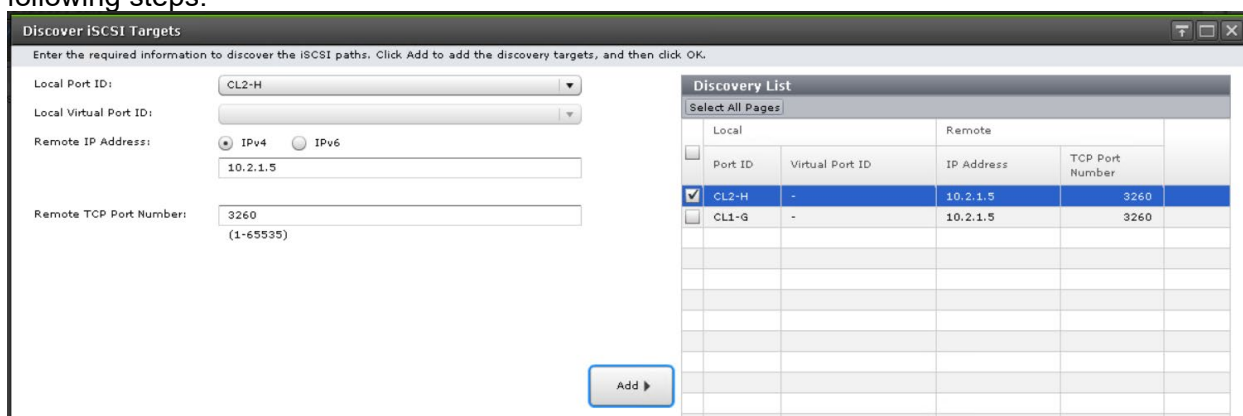
This section describes how to discover the volumes from the iSCSI target virtual machine and turn them into GAD quorums. The procedure is the same as it is to virtualize a physical Fibre Channel or iSCSI storage system.

Create iSCSI Paths

1. Log in to Storage Navigator.
2. On the left side, click **External Storage**, and then click the **iSCSI Paths** tab.



3. Click **Add iSCSI Paths**.
4. Click **Discover iSCSI Targets**.
5. For each storage system iSCSI port that will connect to the VMware VM, complete the following steps:



- a. Enter the following:
 - **Local Port ID:** iSCSI port
 - **Remote IP Address:** private IP address of the VMware VM
 - **Remote TCP Port Number:** 3260
 - b. Click **Add**.
6. After you finish adding all the required iSCSI ports to the discovery list, click **OK**.

- Back in the Add iSCSI Paths window, leave **Authentication Method=None** and **Mutual CHAP=Disable**, and then click **Add**.

This wizard lets you add iSCSI paths. To discover available iSCSI paths, Click Discover iSCSI Targets. Enter the iSCSI path settings, and then click Add. Click Finish to confirm.

iSCSI Targets: [Discover iSCSI Targets](#)

Available iSCSI Paths

Local		Remote	
Port ID	Virtual Port ID	IP Address	TCP Port Number
☒	CL2-H	-	10.2.1.5
☒	CL1-G	-	10.2.1.5

Selected: 2 of 2

Authentication Method: **None**

Mutual CHAP: ☐ Enable ☒ Disable

User Name: (-)

Secret: (-)

Selected iSCSI Paths

Local		Remote		
Port ID	Virtual Port ID	IP Address	TCP Port Number	iSCSI Target Name
No Data				

Remove Selected: 0 of 0

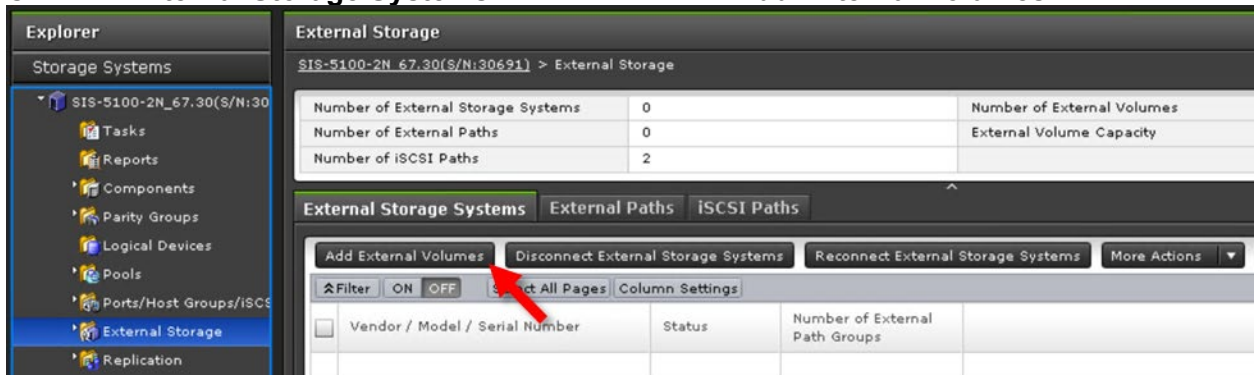
- Click **Finish** and then click **Apply**.

The following screenshot shows the iSCSI paths after creation:

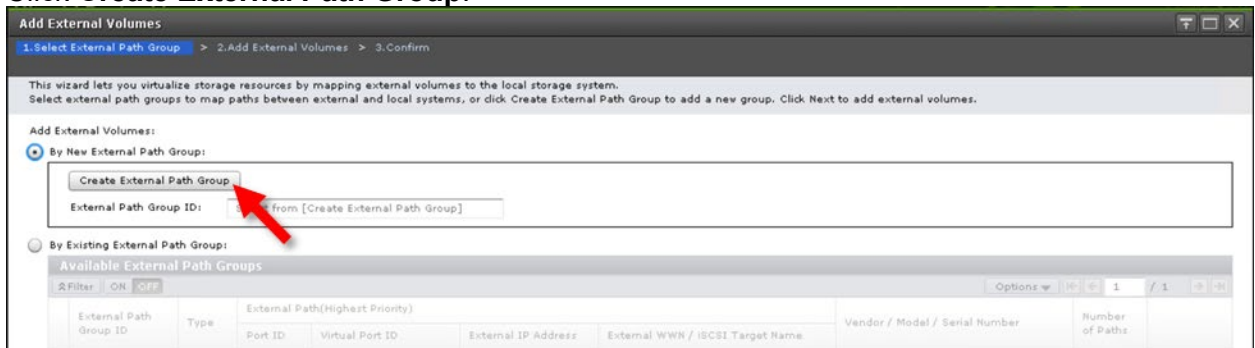
External Storage Systems External Paths iSCSI Paths								
Add iSCSI Paths Edit iSCSI Targets Delete iSCSI Paths More Actions								
Filter ON OFF Select All Pages Column Settings Options 1								
Local	Remote							
Port ID	Virtual Port ID	CHAP User Name	IP Address	TCP Port Number	iSCSI Target Name	Authentication Method	Mutual CHAP	
☐ CL1-G	-		10.2.1.5	3260	iqn.2003-01....	None	Disabled	
☐ CL2-H	-		10.2.1.5	3260	iqn.2003-01....	None	Disabled	

Discover External Volumes

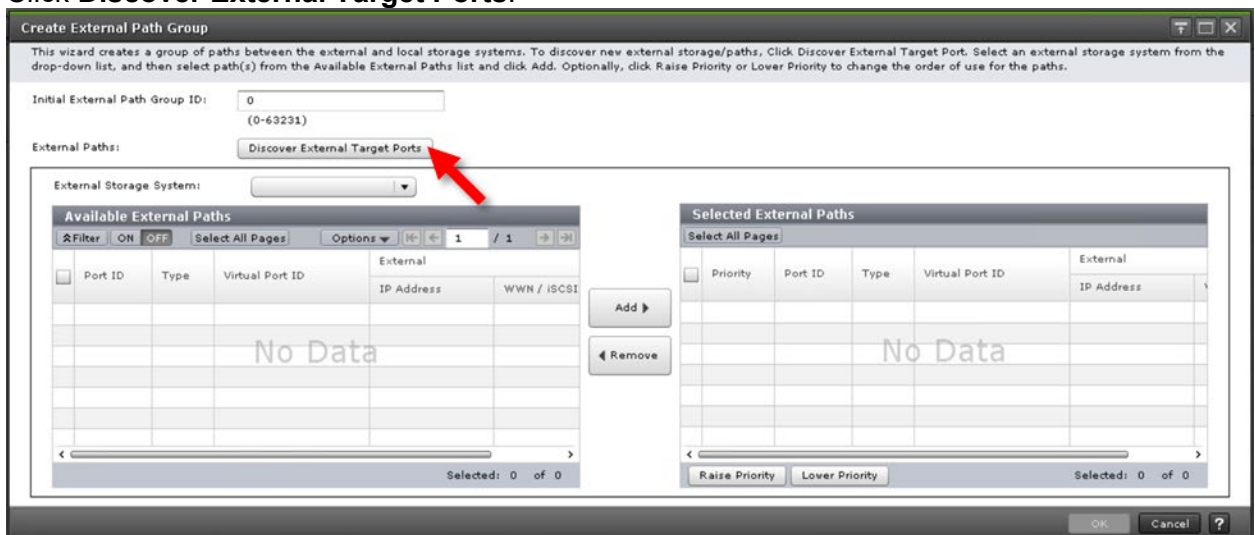
1. Click the **External Storage Systems** tab and then click **Add External Volumes**.



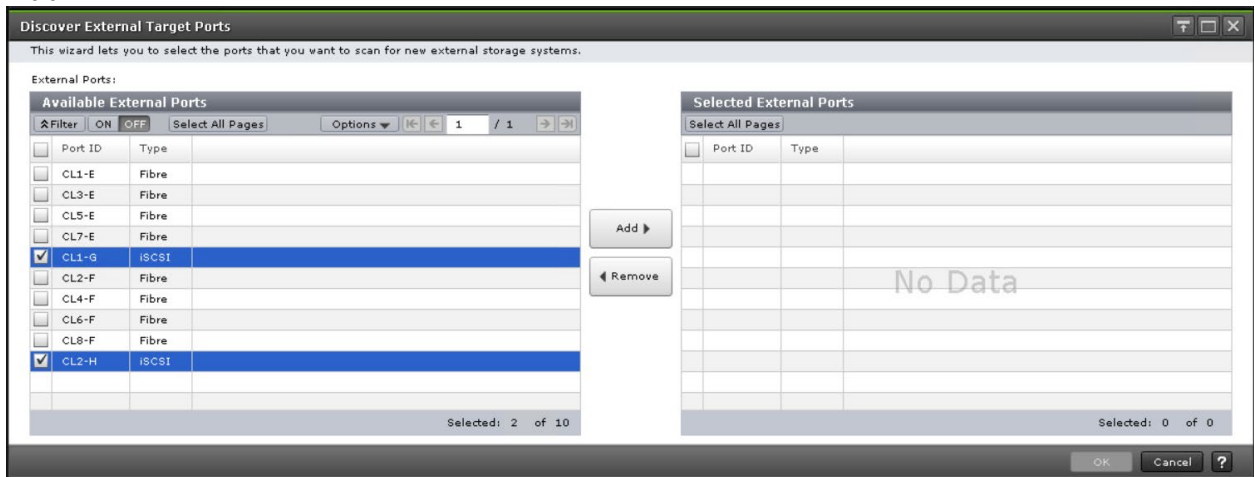
2. Click **Create External Path Group**.



3. Click **Discover External Target Ports**.

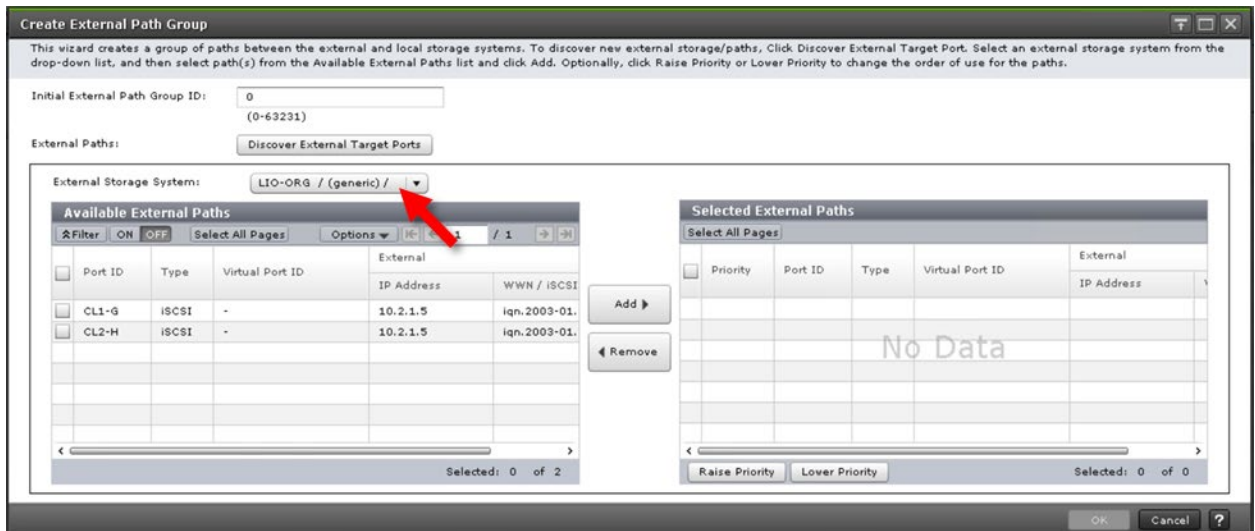


4. Select the iSCSI ports that defined the iSCSI paths in the previous section and then click **Add**.



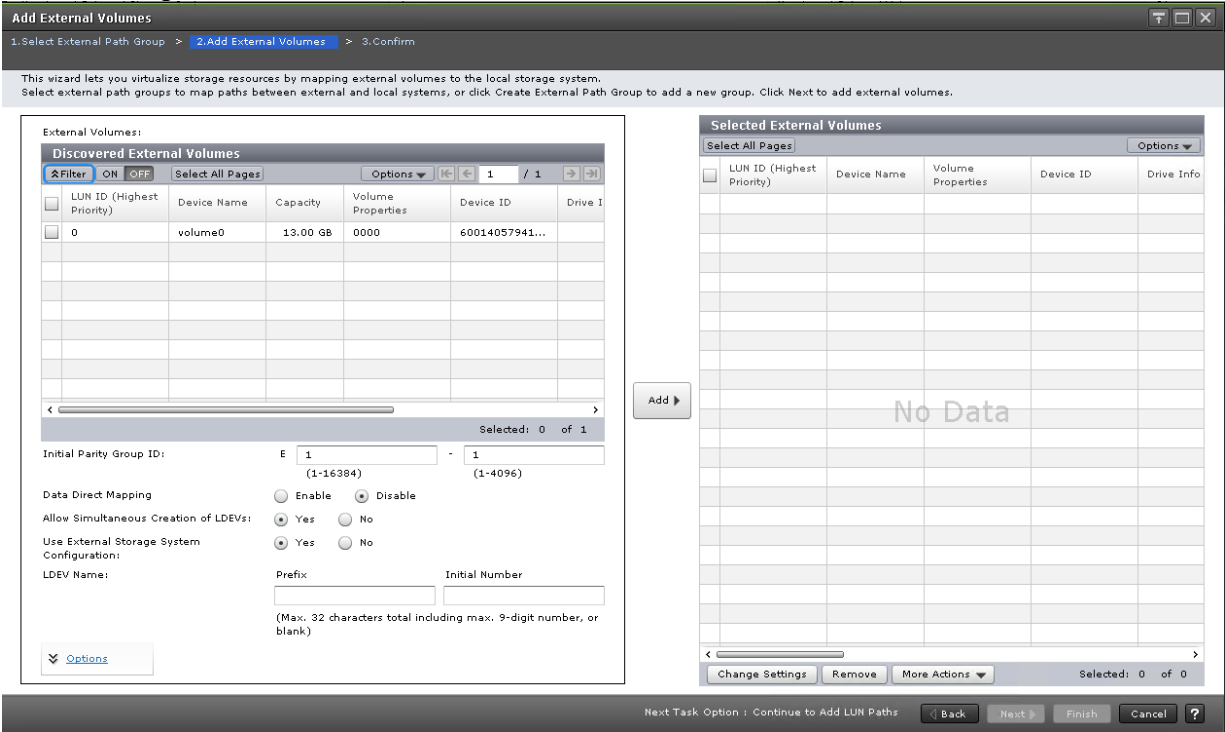
5. Click **OK**.

If the discovery is successful, LIO-ORG will be listed as an external storage system as follows:



6. Select the discovered external paths and click **Add**.
7. Click **OK**.
8. Back in the Add External Volumes screen, click **Next**.

The following screenshot shows the external volume that was discovered:

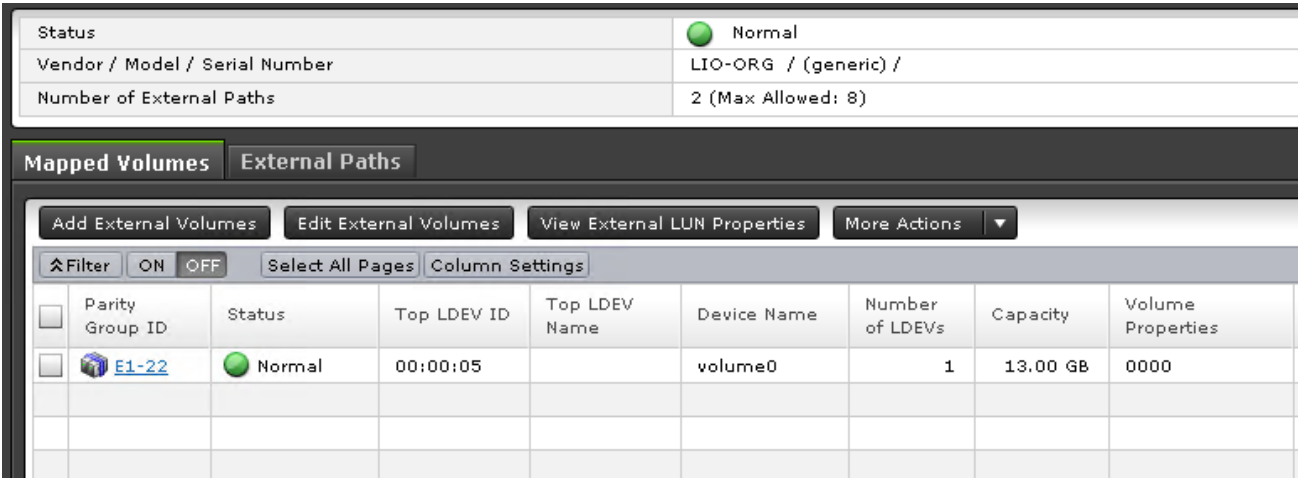


9. Select the discovered volume and then click **Add**.

Note: This external volume corresponds to the volume created on your quorum VM.

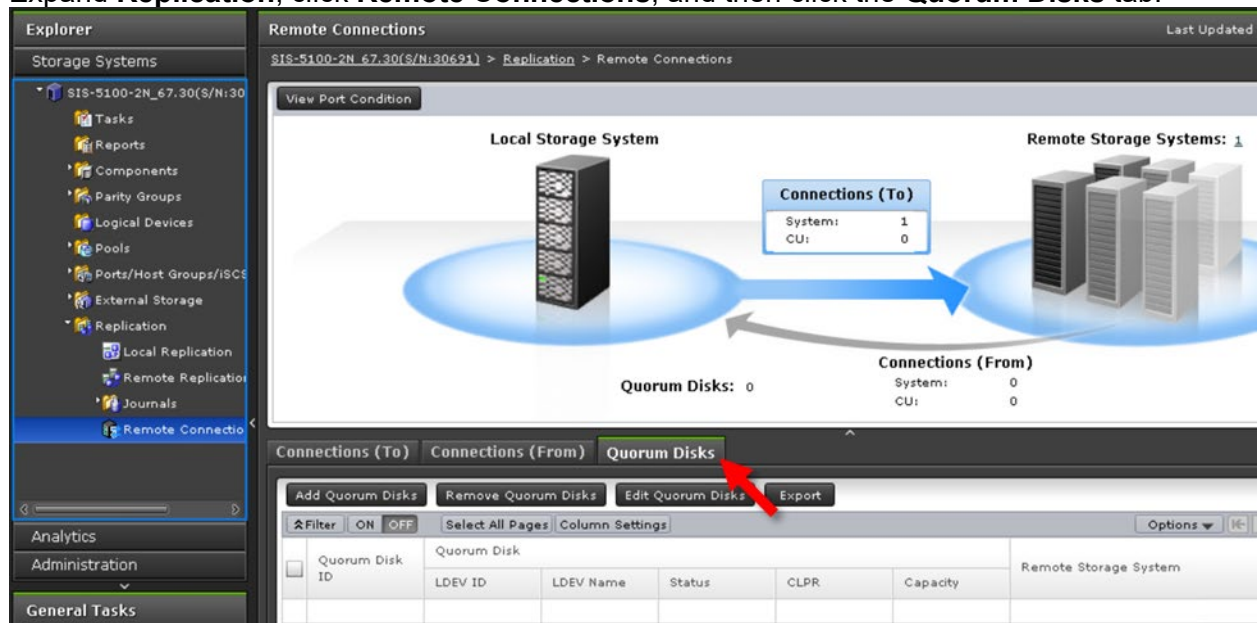
10. Click **Finish** and then click **Apply**.

The following screenshot shows the external volume after it has been successfully virtualized:



Define GAD Quorums

1. Expand **Replication**, click **Remote Connections**, and then click the **Quorum Disks** tab.



2. Click **Add Quorum Disks**.
3. For each quorum that you are creating, complete the following steps:
 - a. Enter the following:
 - **Quorum Disk ID:** a value from the available list
 - **Available LDEVs:** external volume to use as a quorum
 - **Remote Storage System:** remote array to pair with this new quorum
 - b. Click **Add**.
4. Click **Finish** and then click **Apply**.

The following screenshot shows the quorum after it has been successfully created:

Quorum Disks						
Add Quorum Disks Remove Quorum Disks Edit Quorum Disks Export						
Filter ON OFF Select All Pages Column Settings Options						
Quorum Disk ID	LDEV ID	LDEV Name	Status	CLPR	Capacity	Remote Storage System
☐ 00	00:00:02		● Normal	0:CLPR0	13.00 GB	VSP 5000 series / 30548

Appendix A: Mutual CHAP Authentication (Optional)

This section describes how to configure mutual (bidirectional) authentication with Challenge Handshake Authentication Protocol (CHAP). Mutual CHAP authentication means that the on-premises storage systems must authenticate with the VMware ESXi virtual machine and vice-versa. This extra security prevents unintended access from other devices on the same network.

Enable on targetcli

1. Log in to the GAD Private Cloud Quorum VM.
2. Enable mutual CHAP authentication by entering the following commands:

```
./menu.sh
```

```
6
```
3. Follow the prompts to set the credentials.

```

*****
Global-Active Device Cloud Quorum Menu
*****
[1] Add Quorum
[2] Delete Quorum
[3] Add IQN Node
[4] Delete IQN Node
[5] Refresh Portal
[6] Enable CHAP Authentication
[7] View Configuration
[8] Help
[9] Exit
*****
Choice: [1 - 9]
6
targetcli shell version 2.1.fb49
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/> /iscsi/iqn.20...5d6ac0c7/tpg1> Parameter authentication is now '1'.
/iscsi/iqn.20...5d6ac0c7/tpg1> /> Global pref auto_save_on_exit=true
Configuration saved to /etc/target/saveconfig.json
Please input Authentication UserID: uid
Please input Authentication Password: pass
Please input Authentication Mutual UserID: muid
Please input Authentication Mutual Password: mpass
Apply credentials to all connections? (y/n, default: y) y
0
targetcli shell version 2.1.fb49
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

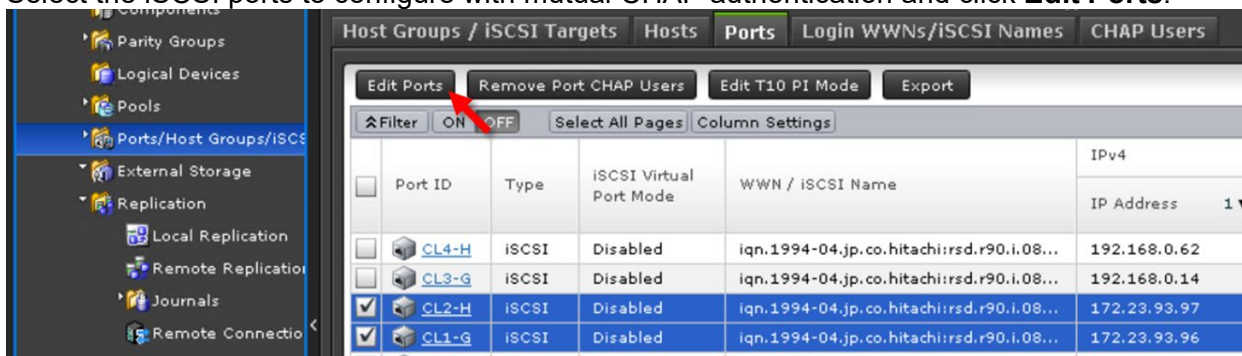
/> /iscsi/iqn.20...0.i.089c42.1g> Parameter userid is now 'uid'.
/iscsi/iqn.20...0.i.089c42.1g> Parameter password is now 'pass'.
/iscsi/iqn.20...0.i.089c42.1g> Parameter mutual_userid is now 'muid'.
/iscsi/iqn.20...0.i.089c42.1g> Parameter mutual_password is now 'mpass'.
/iscsi/iqn.20...0.i.089c42.1g> /> Global pref auto_save_on_exit=true
Configuration saved to /etc/target/saveconfig.json

```

Enable on iSCSI Ports

1. Log in to Storage Navigator.
2. From the left side of Storage Navigator, click **Ports/Host Groups/iSCSI Targets**, and then click the **Ports** tab.

3. Select the iSCSI ports to configure with mutual CHAP authentication and click **Edit Ports**.



4. Complete the following fields, click **Finish**, and then click **Apply**.

☒ CHAP User Name:
 (Max. 223 characters)

☒ Secret:
 (12 - 32 characters)

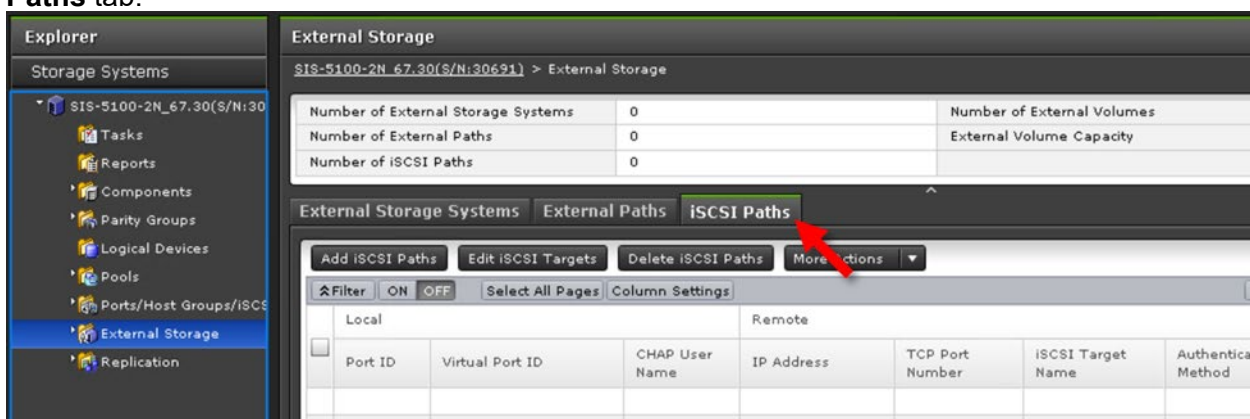
Re-enter Secret:

Back Next **Finish** Cancel ?

- **CHAP User Name:** corresponds to the value for “auth userid” set in targetcli
- **Secret:** corresponds to the value for “auth password” set in targetcli

Create iSCSI Paths

1. Log in to Storage Navigator.
2. From the left side of Storage Navigator, click **External Storage**, and then click the **iSCSI Paths** tab.



3. Click **Add iSCSI Paths**.
4. Click **Discover iSCSI Targets**.

5. For each storage system iSCSI port that will connect to the VMware VM, complete the following steps:

- a. Enter the following:
 - **Local Port ID:** iSCSI port
 - **Remote IP Address:** private IP address of the VMware VM
 - **Remote TCP Port Number:** 3260
 - b. Click **Add**.
6. After adding all the required iSCSI ports to the discovery list, click **OK**.
 7. Back in the Add iSCSI Paths window, complete the following steps:

- a. Enter the following:
 - **Authentication Method:** CHAP
 - **Mutual CHAP:** Enable
 - **User Name:** corresponds to the value for “auth mutual_userid” set in targetcli
 - **Secret:** corresponds to the value for “auth mutual_password” set in targetcli
 - b. Click **Add**.
8. Click **Finish**, and then click **Apply**.

The following screenshot shows the iSCSI paths after creation:



Local		Remote						
Port ID	Virtual Port ID	CHAP User Name	IP Address	TCP Port Number	iSCSI Target Name	Authentication Method	Mutual CHAP	CHAP User Name
CL1-G	-		10.2.1.5	3260	iqn.2003-01....	CHAP	Enabled	
CL2-H	-		10.2.1.5	3260	iqn.2003-01....	CHAP	Enabled	

The remaining steps to discover external volumes and define GAD quorums are the same as without mutual CHAP authentication.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com

Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com

