

# Global-Active Device Cloud Quorum in Azure

v1.0

---

## Implementation Guide

Reduce the costs of Global-Active Device by using a virtual machine instead of a physical storage system as the quorum and remove the need for a third site to host the quorum by deploying it in the cloud.

**Hitachi Vantara**

**MK-92RD8088-00**

**February 2022**

© 2022 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](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

<b>Preface .....</b>	<b>4</b>
About this document.....	4
Document conventions.....	4
Intended audience .....	4
References .....	4
Accessing product downloads.....	4
Comments .....	5
Getting Help.....	5
<b>Executive Summary .....</b>	<b>6</b>
<b>Configuration and Specifications .....</b>	<b>7</b>
VPN Gateway .....	7
Azure Virtual Machine .....	8
<b>Azure Virtual Machine.....</b>	<b>9</b>
Deployment .....	9
Firewall Exemption .....	11
Access Quorum VM .....	11
<b>Global-Active Device Quorums .....</b>	<b>13</b>
Create iSCSI Paths .....	13
Discover External Volumes .....	15
Define GAD Quorums .....	18
<b>Appendix I: Mutual CHAP Authentication.....</b>	<b>20</b>
Enable on targetcli.....	20
Enable on iSCSI Ports.....	21
Create iSCSI Paths .....	22

# Preface

## About this document

This document provides instructions to deploy a virtual machine in the Microsoft Azure cloud and configure it to be an iSCSI target. We will use the Linux package “targetcli” to create and manage block devices on the virtual machine. The objective is to leverage volumes from the iSCSI target virtual machine running on Azure as quorum volumes for Global-Active Device.

This guide does not include instructions for establishing a VPN connection to Azure. Refer to the Azure documentation, such as [Tutorial: Create a Site-to-Site connection in the Azure portal](#).

## Document conventions

This document uses the following typographic convention:

Convention	Description
<b>Bold</b>	<ul style="list-style-type: none"><li>Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: <b>Click OK</b>.</li><li>Indicates emphasized words in list items.</li></ul>
<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 interest in hosting their quorum on the cloud.

## Referenced documents

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

## 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 [doc.comments@hitachivantara.com](mailto:doc.comments@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](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](https://community.hitachivantara.com), register, and complete your profile.

# Executive Summary

Global-active device cloud quorum is a virtual machine image provided by Hitachi Vantara through the cloud marketplace. Its purpose is to simplify and enhance Global-Active Device (GAD) by replacing an on-premise quorum with an automatically configured, easy-to-use cloud quorum. In addition to being easier and faster to deploy, a cloud quorum also makes GAD more resilient against outages: Quorums hosted at the same location as their storage systems create a single point of failure. For on-premise deployments, this is avoided by hosting the quorum disk at a separate datacenter, but with global-active device cloud quorum, you can achieve the same result without the associated overhead. This guide provides instructions on how to set up and use global-active device cloud quorum on Microsoft Azure.

# Configuration and Specifications

Figure 1 provides a high-level illustration of the connectivity between on-premise Virtual Storage Platform (VSP) storage systems and an iSCSI target virtual machine in the Azure cloud.

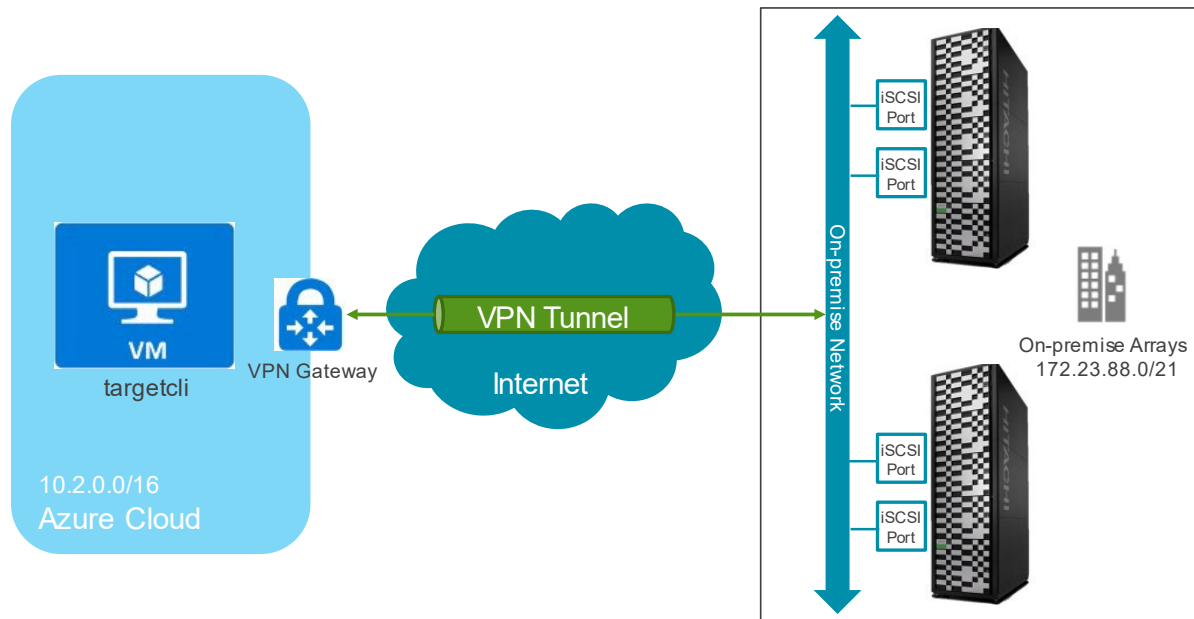


Figure 1: Test Environment

## VPN Gateway

During certification of this solution, we determined that the Azure VPN Gateway plays a substantial role. You must use a sufficiently large gateway type to support quorum traffic. Otherwise, the iSCSI paths between the storage systems and Azure virtual machine experience frequent timeouts and disconnects.

We experienced these issues while testing with 16 GAD quorums using the two smallest gateway types, Basic and VpnGw1. The timeout and disconnect problems were resolved when we upgraded the Azure VPN Gateway to a VpnGw2 type.

For a complete list of available gateway types, see: <https://azure.microsoft.com/en-us/pricing/details/vpn-gateway/>.

A tip for identifying the Azure VPN Gateway as a bottleneck is to ask Azure Support to review the object CPU utilization. High utilization is a sign that the gateway is a potential problem. Unfortunately, you cannot currently check this metric yourself.

# Azure Virtual Machine

The following settings were used for the virtual machine image:

- Operating system: SUSE Linux Enterprise Server 15 SP1
- Kernel: 4.12.14-8.33-azure
- Instance type: Standard\_B2s
  - CPU: 2 virtual CPUs
  - Memory: 4 GB
  - Disks: Standard HDD 30 GB, Premium SSD 66 GB
- Targetcli version: 2.1.fb49



# Azure Virtual Machine

## Deployment


This section provides instructions for creating the virtual machine in Azure that will function as the iSCSI target.

We assume you are familiar with using an SSH public key for authentication, so we do not cover this topic. For a refresher, see: [Generate and store SSH keys in the Azure portal](#).

1. On the landing page of the Azure Portal, use the top-left shortcut to expand the portal menu, click **Virtual machines**, click **Add**, and then click **Virtual machine**.
2. Enter a name for your quorum VM. Then, click **See all images** and search the Azure marketplace for **Global-Active Device Cloud Quorum**.

**Create a virtual machine** ...


Instance details

Virtual machine name \* ⓘ 

Region \* ⓘ (US) West US ▼

Availability options ⓘ No infrastructure redundancy required ▼

Security type ⓘ Standard ▼

Image \* ⓘ  [See all images](#) | Configure VM generation ▼

Azure Spot instance ⓘ ☐

Size \* ⓘ Standard\_B2s - 2 vcpus, 4 GiB memory (\$29.71/month) ▼  
[See all sizes](#)

3. Set the Region located within a 40ms ping of your VSP storage systems. Our testing was done in the western portion of the US connected to our lab in Denver, CO with a ping of ~30ms. Under Availability options, no infrastructure redundancy was used in our testing.
4. From the top of the page, select the Networking tab, and enter values for the following options:
  - **Virtual network** (The virtual network must be able to pass traffic to and from the on-premise networks where the storage systems are located).
  - **Subnet**
  - **Public IP**

- **Configure network security group**

5. In the Advanced tab, under Custom data type, enter the following lines:

```
#!/bin/bash
./quorum_setup.sh
```

After these lines, add the IQNs of your GAD storage system ports separated by spaces.

#### Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#)

Custom data



```
#!/bin/bash
./quorum_setup.sh iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c42.1g iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c42.3g iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c4a.1e iqn.1994-04.jp.co.hitachi:rsd.r90.i.089c4a.2e
```

You can find your VSP IQNs by using Storage Navigator as follows:

Port ID	Type	Mode	iSCSI Virtual Port Mode	WWN / iSCSI Name	IPv4
CL1-A	Fibre	SCSI	-	50060E8008775400	-
CL3-A	Fibre	SCSI	-	50060E8008775420	-
CL1-G	iSCSI	-	Disabled	iqn.1994-04.jp.co.hitachi:rsd.r90.i.087754.1g	172.23.90.177
CL3-G	iSCSI	-	Disabled	iqn.1994-04.jp.co.hitachi:rsd.r90.i.087754.3g	192.168.0.14
CL1-C	Fibre	SCSI	-	50060E8008775402	-

No additional settings are required on the remaining pages.

6. Click **Review + create**, verify that the final details are correct, and then click **Create**.

# Firewall Exemption

This section provides instructions for creating a firewall exemption on the Azure network so that iSCSI traffic can get to the GAD quorum virtual machine from the on-premise storage systems.

1. On the landing page of Azure Portal, use the top-left shortcut to expand the portal menu, click **Virtual machines**, and then click the newly created virtual machine.
2. On the left, under **Settings**, click **Networking**, and then click **Add inbound port rule**.
3. Enter the following values and then click **Add**:
  - **Source**: IP addresses
  - **Source IP addresses/CIDR ranges**: subnets of the on-premise arrays' iSCSI ports
  - **Source port ranges**: \* (asterisk)
    - **Destination**: IP addresses
    - **Destination IP addresses/CIDR ranges**: private IP of the VM
    - **Service**: custom
    - **Destination port ranges**: 3260
    - **Protocol**: TCP

You do not need to add an outbound rule for TCP 3260.

## Quorum VM Access

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

1. Use an SSH client (such as putty) to log into your quorum VM. Use the public IP and SSH key assigned to your VM.
2. Log in to the quorum. The default username is azureuser.

3. Open the configuration script: `./menu.sh`

```
azureuser@q-code:~> ./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. Enter 7 to view the current configuration

```
*****
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 array 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).

# Global-Active Device Quorums

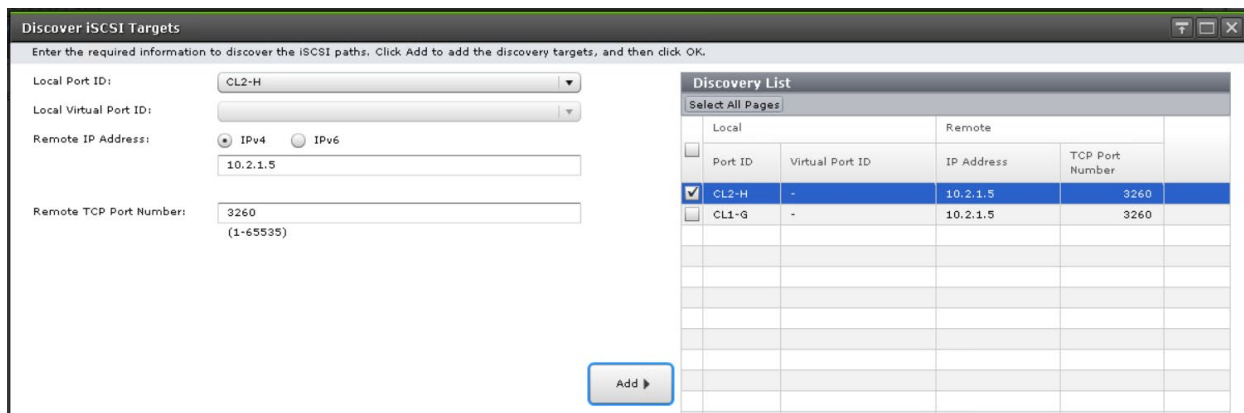
This section describes how to discover the volumes from the iSCSI target virtual machine and turn them into GAD quorums. The procedure is the same as it is to virtualize a physical Fibre Channel or iSCSI storage system.

## 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 Azure VM, complete the following steps:



- a. Enter the following:

- **Local Port ID:** iSCSI port

- **Remote IP Address:** private IP address of the Azure 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**.

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

**Add iSCSI Paths**

1. Add iSCSI Paths > 2. Confirm

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.

Available iSCSI Paths

Local		Remote	
Port ID	Virtual Port ID	IP Address	TCP Port Number
<input checked="" type="checkbox"/>	CL2-H	-	10.2.1.5
<input checked="" type="checkbox"/>	CL1-G	-	10.2.1.5

Selected iSCSI Paths

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

Authentication Method: **None**

Mutual CHAP: ☐ Enable ☒ Disable

User Name: (-)

Secret: (-)

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

The following screenshot shows the iSCSI paths after creation:

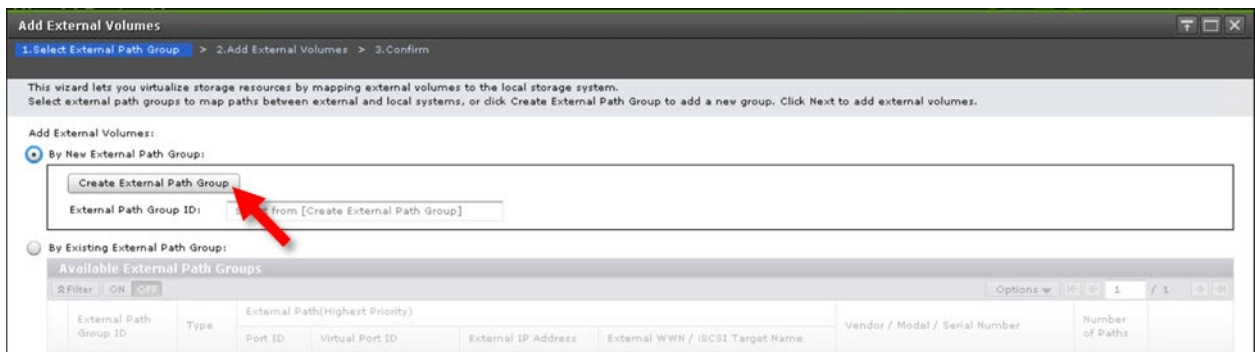
External Storage Systems External Paths <b>iSCSI Paths</b>								
Add iSCSI Paths Edit iSCSI Targets Delete iSCSI Paths More Actions Sel								
Filter ON OFF Select All Pages Column Settings Options 1								
Local			Remote					
<input type="checkbox"/>	Port ID	Virtual Port ID	CHAP User Name	IP Address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

# Discover External Volumes

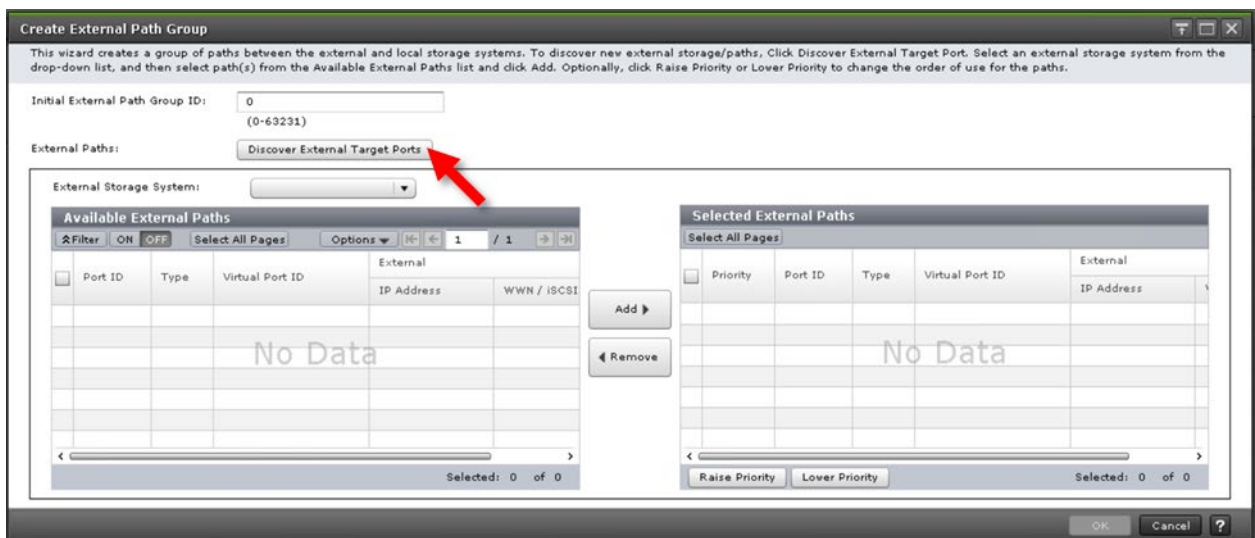
1. Click the **External Storage Systems** tab and then click **Add External Volumes**.



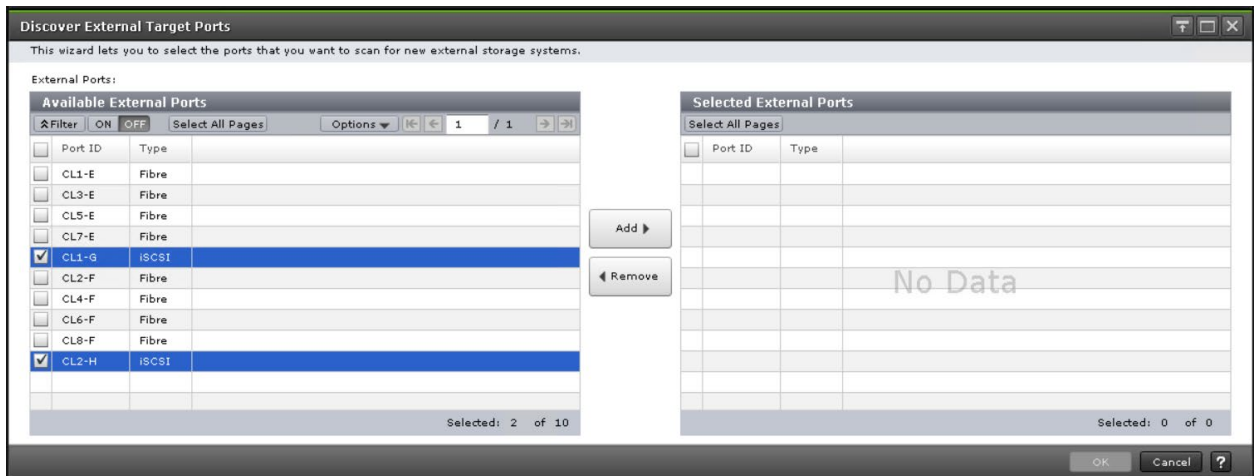
2. Click **Create External Path Group**.



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

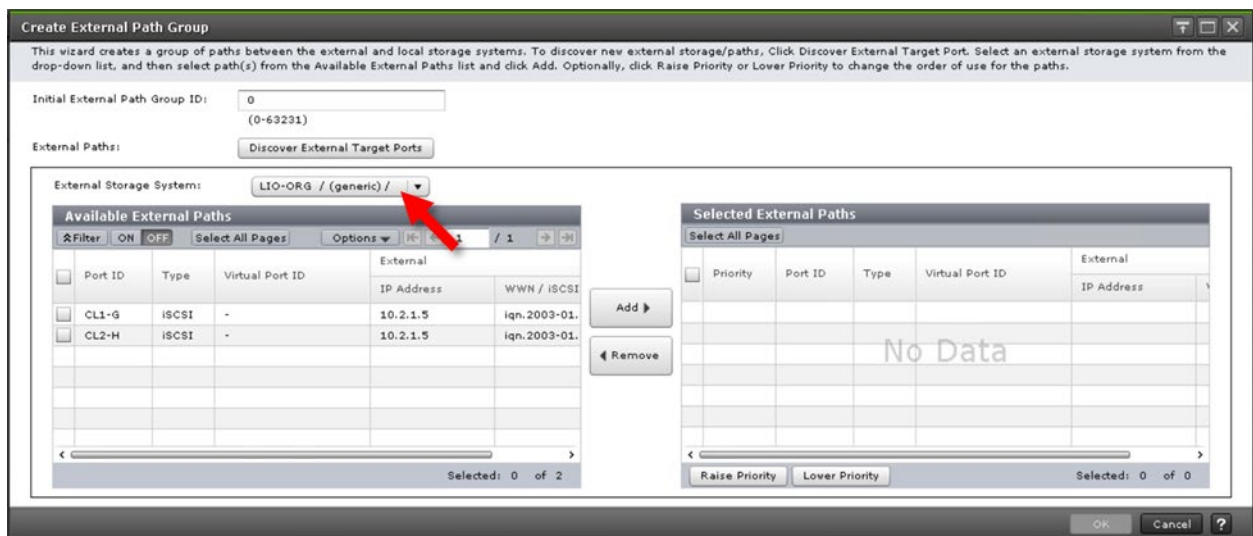


4. Select the iSCSI ports that defined the iSCSI paths in the previous section and then click **Add**.



5. Click **OK**.

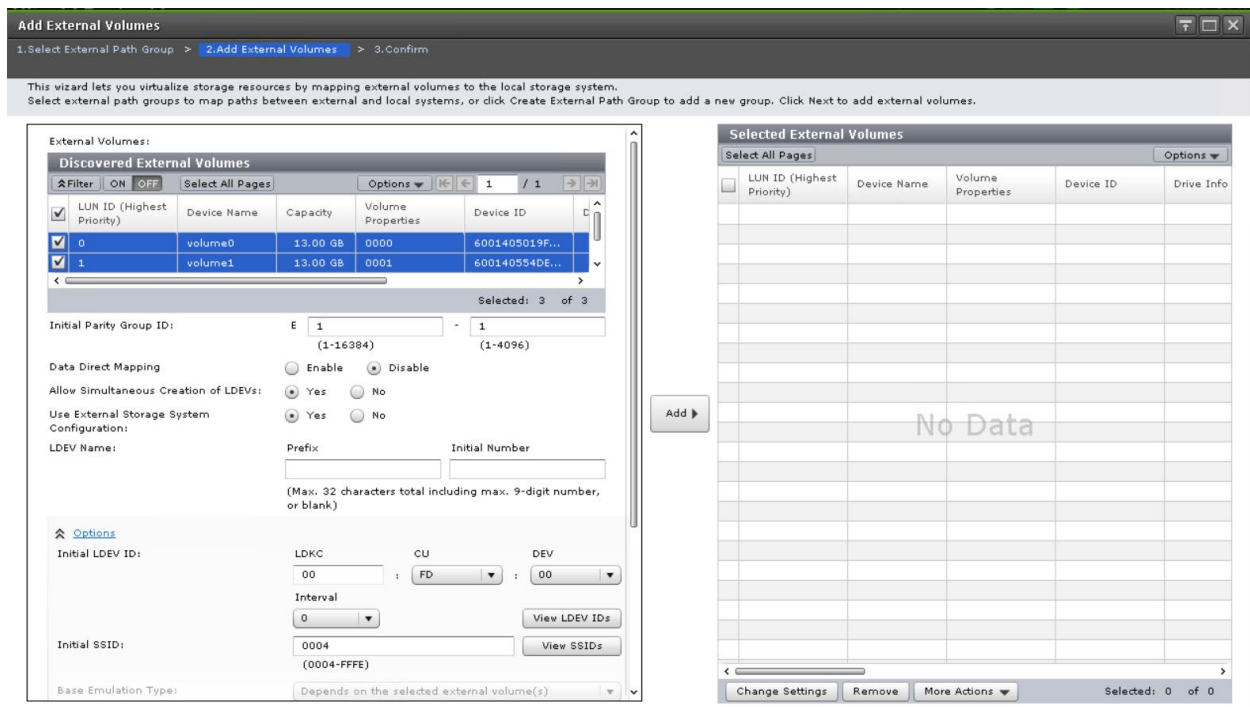
If discovery is successful, LIO-ORG will be listed as an external storage system as follows:



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



The following screenshot shows three external volumes were discovered.

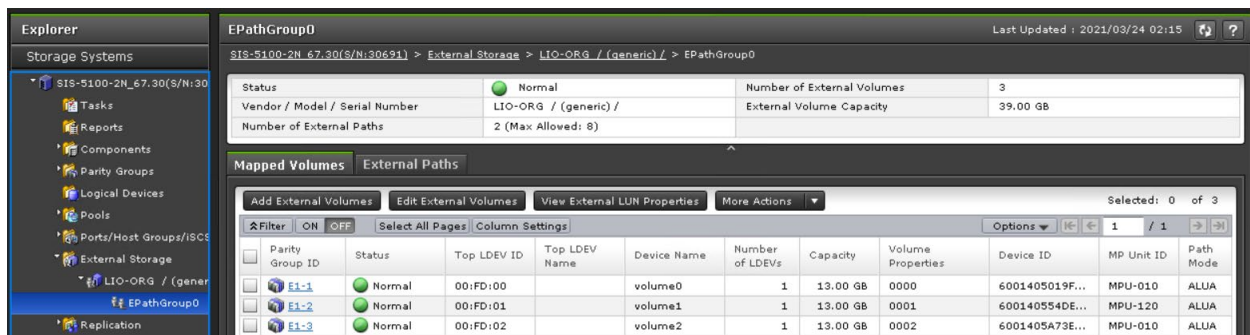


9. Select the discovered volumes and then click **Add**.

These external volumes correlate to the volumes created on your quorum VM. Testing was done with three quorum volumes (the default volume count is one).

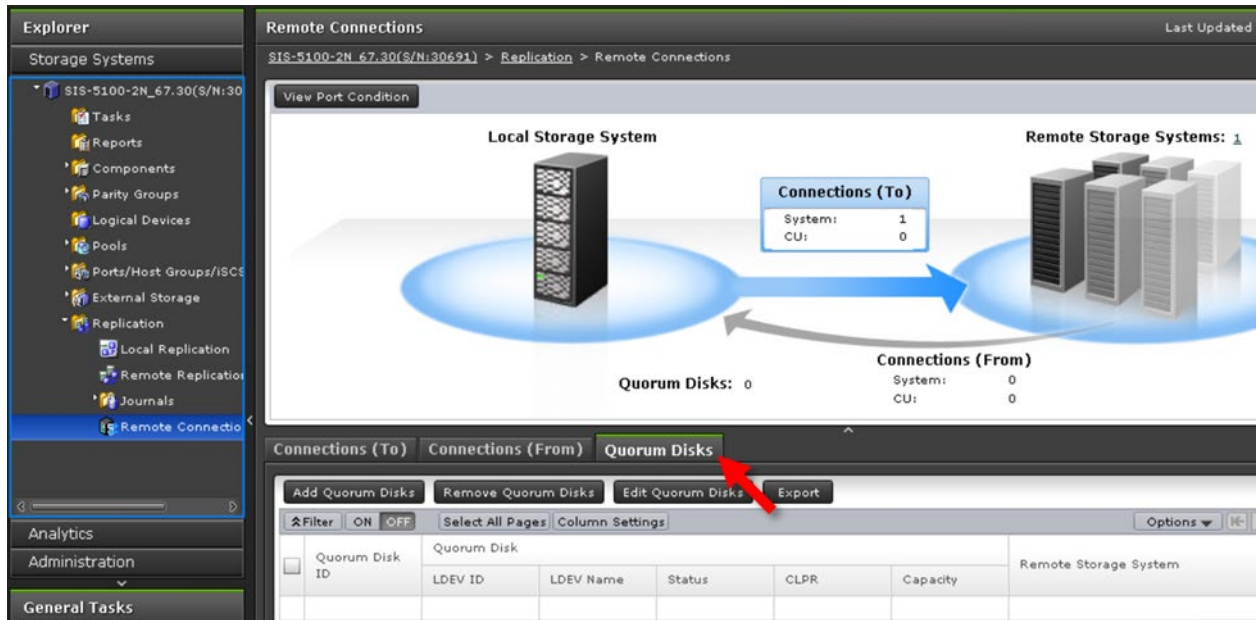
10. Click **Finish** and then click **Apply**.

The following screenshot shows the external volumes after they have been successfully virtualized.

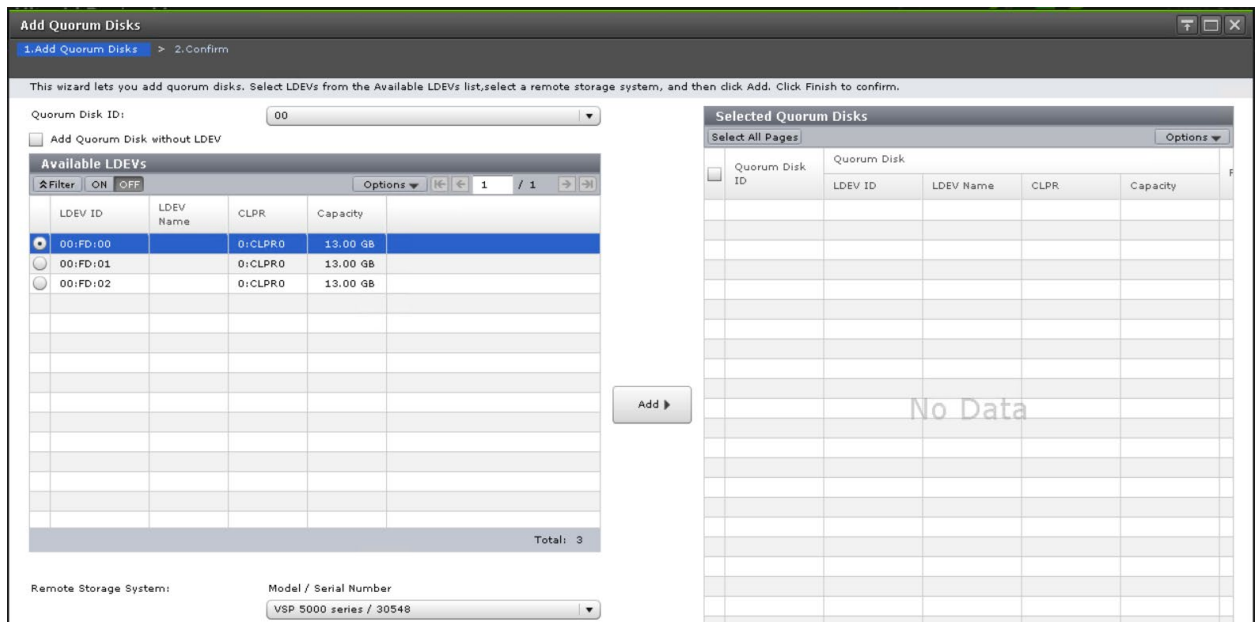


# Define GAD Quorums

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 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 quorums after they have been successfully created.

Connections (To)Connections (From)Quorum Disks

Add Quorum DisksRemove Quorum DisksEdit Quorum DisksExport

FilterONOFFSelect All PagesColumn SettingsOptions

<input type="checkbox"/>	Quorum Disk ID	Quorum Disk					Remote Storage System
		LDEV ID	LDEV Name	Status	CLPR	Capacity	
<input type="checkbox"/>	 00	<a href="#">00:FD:00</a>		 Normal	0:CLPR0	13.00 GB	VSP 5000 series / 30548
<input type="checkbox"/>	 01	<a href="#">00:FD:01</a>		 Normal	0:CLPR0	13.00 GB	VSP 5000 series / 30548
<input type="checkbox"/>	 02	<a href="#">00:FD:02</a>		 Normal	0:CLPR0	13.00 GB	VSP 5000 series / 30548

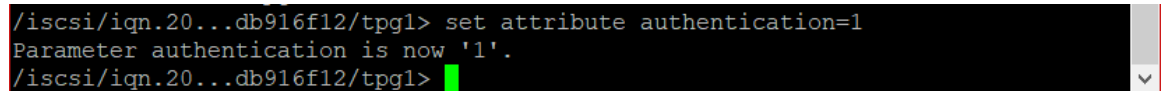
# Appendix I: Mutual CHAP Authentication

This section describes how to configure mutual (bidirectional) authentication with Challenge Handshake Authentication Protocol (CHAP). Mutual CHAP authentication means that the on-premise storage systems must authenticate with the Azure 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 targetcli with the command: `sudo targetcli`
2. Enable mutual CHAP authentication by entering the following commands:

```
cd /iscsi/iqn.2003-01.org.linux-iscsi.quorum-  
1.x8664:sn.e5d4db916f12/tpg1/  
  
set attribute authentication=1
```



```
/iscsi/iqn.20...db916f12/tpg1> set attribute authentication=1  
Parameter authentication is now '1'.  
/iscsi/iqn.20...db916f12/tpg1>
```

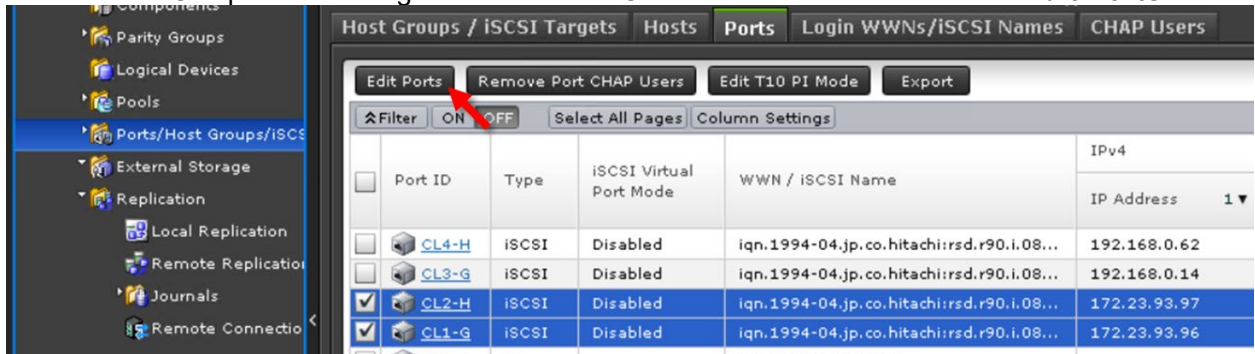
3. Set the user IDs and passwords to use for mutual CHAP authentication with the following commands:

```
cd /iscsi/iqn.2003-01.org.linux-iscsi.quorum-  
1.x8664:sn.e5d4db916f12/tpg1/iqn.1994-  
04.jp.co.hitachi:rsd.r90.i.0877e3.1g/  
  
set auth userid=<chosen_auth_userid>  
set auth password=<chosen_auth_password>  
set auth mutual_userid=<chosen_auth_mutual_userid>  
set auth mutual_password=<chosen_auth_mutual_password>
```

4. Repeat step 3 for the remaining IQNs.
5. Save the changes as follows:
  - a. Go to the root directory with the command: `cd /`
  - b. Save the changes with the command: `saveconfig`
6. Exit from targetcli with the command: `exit`

## Enable on iSCSI Ports

1. From the left side of Storage Navigator, click **Ports/Host Groups/iSCSI Targets**, and then click the **Ports** tab.
2. Select the iSCSI ports to configure with mutual CHAP authentication and click **Edit Ports**.



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

☒ CHAP User Name:   
 (Max. 223 characters)

☒ Secret:   
 (12 - 32 characters)

Re-enter Secret:

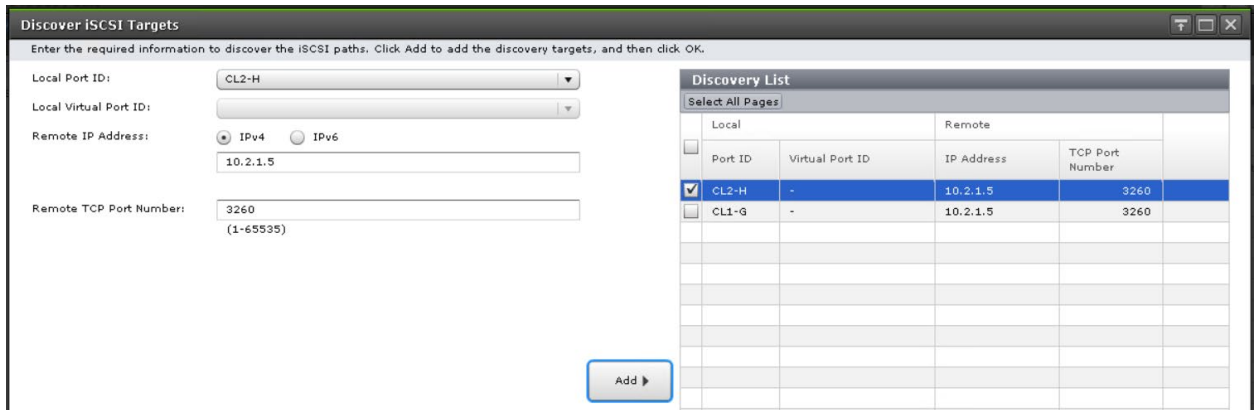
- **CHAP User Name:** corresponds to the value for “auth userid” set in targetcli
- **Secret:** corresponds to the value for “auth password” set in targetcli

# Create iSCSI Paths

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



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



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

6. Back in the Add iSCSI Paths window, complete the following steps:

The screenshot shows the 'Add iSCSI Paths' configuration window. It has the following fields and settings:

- Authentication Method:** A dropdown menu set to 'CHAP'.
- Mutual CHAP:** Two radio buttons, 'Enable' (selected) and 'Disable'.
- User Name:** A text input field containing a redacted name, with a note '(Max. 223 characters)' below it.
- Secret:** A text input field containing a redacted password, with a note '(12 - 32 characters)' below it.

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**.

7. Click **Finish**, and then click **Apply**.

The following screenshot shows the iSCSI paths after creation:

The screenshot shows the 'iSCSI Paths' table in the storage management console. The table has columns for Local and Remote properties. Two paths are listed, both with Mutual CHAP enabled.

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	-	[Redacted]	10.2.1.5	3260	iqn.2003-01....	CHAP	Enabled	[Redacted]
CL2-H	-	[Redacted]	10.2.1.5	3260	iqn.2003-01....	CHAP	Enabled	[Redacted]

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](http://www.HitachiVantara.com) [community.HitachiVantara.com](http://community.HitachiVantara.com)

### Regional Contact Information

Americas: +1 866 374 5822 or [info@hitachivantara.com](mailto:info@hitachivantara.com)

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

Asia Pacific: +852 3189 7900 or [info.marketing.apac@hitachivantara.com](mailto:info.marketing.apac@hitachivantara.com)

