

# Global-Active Device Cloud Quorum in AWS

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. Remove the need to have a third site to host the quorum by deploying it in the cloud.

**Hitachi Vantara**

**MK-92RD8087-00**

**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>Table of Contents .....</b>	<b>3</b>
<b>Preface .....</b>	<b>4</b>
About this document .....	4
Document conventions .....	4
Intended audience .....	4
Referenced documents .....	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 Tunnel .....	7
AWS Virtual Machine.....	7
<b>Amazon Virtual Machine .....</b>	<b>8</b>
Deployment .....	8
Firewall Exemption .....	11
Access Quorum VM.....	12
<b>Global-Active Device Quorums.....</b>	<b>14</b>
Create iSCSI Paths .....	14
Discover External Volumes .....	16
Define GAD Quorums.....	19
<b>Appendix A: Mutual CHAP Authentication .....</b>	<b>21</b>
Enable on targetcli.....	21
Enable on iSCSI Ports.....	22
Create iSCSI Paths .....	23

# Preface

## About this document

This guide provides instructions to deploy a virtual machine on the Amazon Web Services (AWS) 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 AWS as quorum volumes for Global-active device (GAD).

This guide does not include instructions for establishing a VPN connection to AWS. Refer to the AWS documentation, such as [AWS Site-to-Site VPN](#).

## 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's 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 Amazon Web Services.

# 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 AWS cloud.

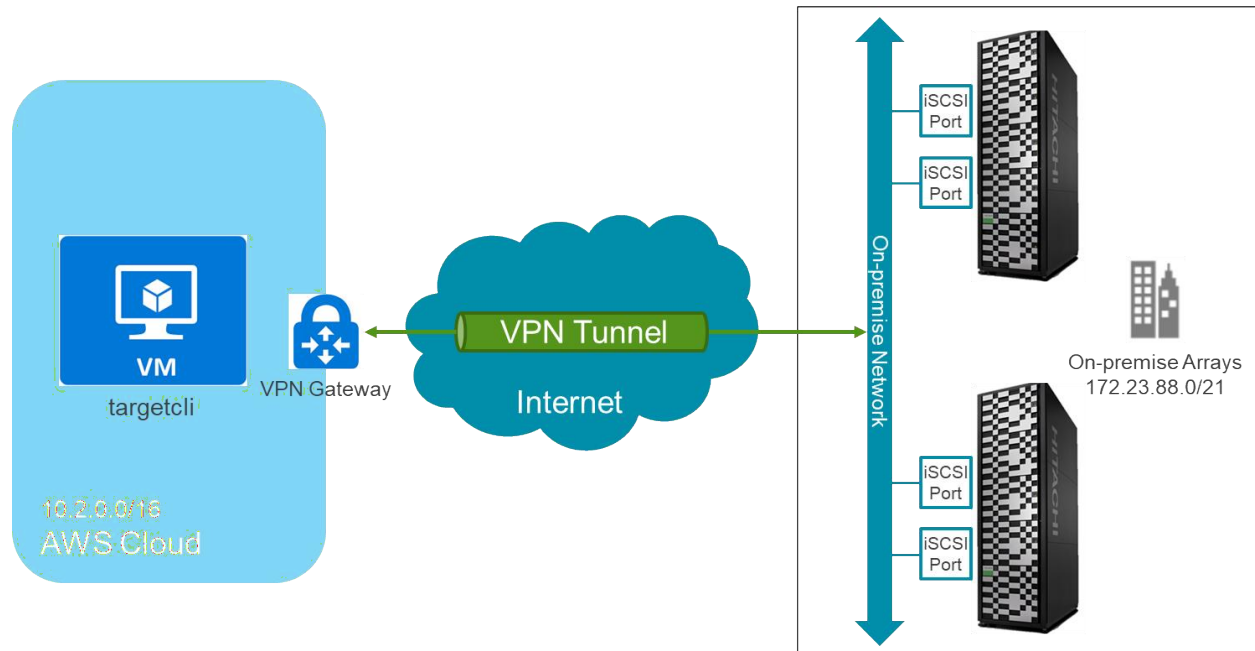


Figure 1: Test Environment

## VPN Tunnel

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

## AWS Virtual Machine

The following settings were used for the virtual machine image:

- Operating system: Amazon Linux 2
- Kernel: Linux Kernel 5.10
- Instance type: t2.micro
  - CPU: 1 virtual CPU
  - Memory: 1 GB
  - Disks: Premium SSD 67 GB
- Targetcli version: 2.1.53

# Amazon Virtual Machine

## Deployment

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

We assume that you are familiar with using an SSH public key for authentication, so we do not cover this topic. For this testing, you must use a Region located within 40ms ping of your VSP storage systems.

Our testing was performed in the western portion of the US connected to our lab in Denver, CO, with a ping of ~30ms. In this testing, under Availability options, no infrastructure redundancy was used.

1. In the page **Step 2: Choose an Instance Type**, select the following:

- **Family:** t2
- **Type:** t2.micro

### Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All instance families** **Current generation** [Show/Hide Columns](#)

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)					
	Family	Type	vCPUs	Memory (GiB)	
<input type="checkbox"/>	t2	t2.nano	1	0.5	
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	
<input type="checkbox"/>	t2	t2.small	1	2	
<input type="checkbox"/>	t2	t2.medium	2	4	
<input type="checkbox"/>	t2	t2.large	2	8	
<input type="checkbox"/>	t2	t2.xlarge	4	16	
<input type="checkbox"/>	t2	t2.2xlarge	8	32	
<input type="checkbox"/>	t3	t3.nano	2	0.5	
<input type="checkbox"/>	t3	t3.micro	2	1	
<input type="checkbox"/>	t3	t3.small	2	2	
<input type="checkbox"/>	t3	t3.medium	2	4	



2. On the Configure Instance Details page enter the details and then select the **Network** from the list.

For the initial configuration, we selected **Enable** from the **Auto-assign Public IP** list to remotely access the virtual machine.

### Step 3: Configure Instance Details

Number of Instances <sup>(i)</sup> 1 Launch into Auto Scaling Group <sup>(i)</sup>

Purchasing option <sup>(i)</sup> ☐ Request Spot instances

Network <sup>(i)</sup> vpc-075201acbaecd164c | VPC\_Denver <sup>(i)</sup> Create new VPC  
No default VPC found. [Create a new default VPC.](#)

Subnet <sup>(i)</sup> subnet-0ab744f22f29e89a8 | us-west-1a <sup>(i)</sup> Create new subnet  
65521 IP Addresses available

Auto-assign Public IP <sup>(i)</sup> **Enable**

Hostname type <sup>(i)</sup> Use subnet setting (IP name) <sup>(i)</sup>

DNS Hostname <sup>(i)</sup> ☒ Enable IP name IPv4 (A record) DNS requests  
☒ Enable resource-based IPv4 (A record) DNS requests  
☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group <sup>(i)</sup> ☐ Add instance to placement group

Capacity Reservation <sup>(i)</sup> Open <sup>(i)</sup>

Domain join directory <sup>(i)</sup> No directory <sup>(i)</sup> Create new directory

IAM role <sup>(i)</sup> None <sup>(i)</sup> Create new IAM role

Shutdown behavior <sup>(i)</sup> Stop <sup>(i)</sup>

Stop - Hibernate behavior <sup>(i)</sup> ☐ Enable hibernation as an additional stop behavior

Enable termination protection <sup>(i)</sup> ☐ Protect against accidental termination

Monitoring <sup>(i)</sup> ☐ Enable CloudWatch detailed monitoring  
Additional charges apply.

Tenancy <sup>(i)</sup> Shared - Run a shared hardware instance <sup>(i)</sup>  
Additional charges will apply for dedicated tenancy.

Credit specification <sup>(i)</sup> ☐ Unlimited  
Additional charges may apply

3. In the Advanced tab, under User data, enter the following lines:

```
#!/bin/bash
/home/ec2-user/quorum_setup/quorum_setup.sh
```

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

### Advanced Details

Enclave <sup>(i)</sup> ☐ Enable

Metadata accessible <sup>(i)</sup> Enabled <sup>(i)</sup>

Metadata version <sup>(i)</sup> V1 and V2 (token optional) <sup>(i)</sup>

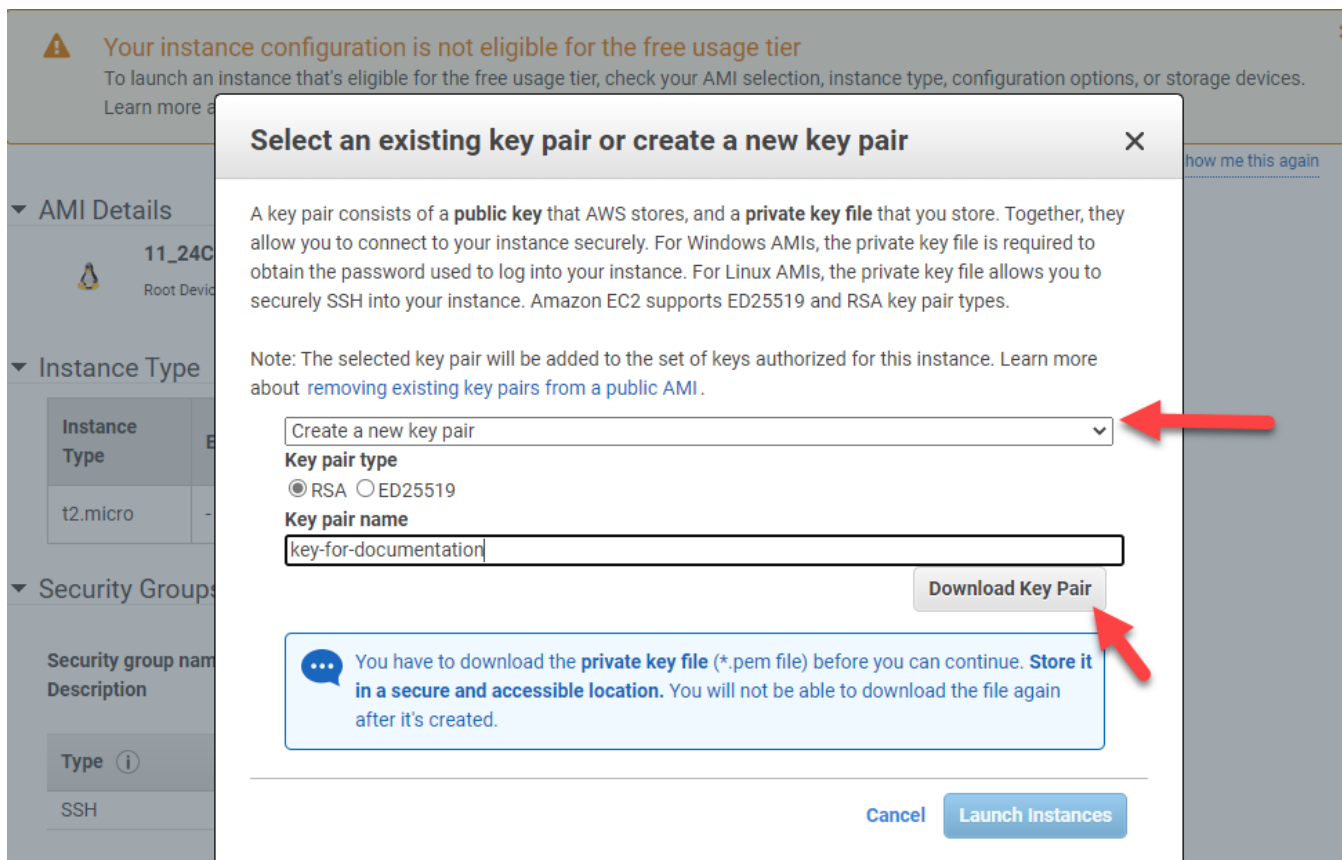
Metadata token response hop limit <sup>(i)</sup> 1 <sup>(i)</sup>

User data <sup>(i)</sup> ☒ As text ☐ As file ☐ Input is already base64 encoded

#!/bin/bash  
/home/ec2-user/quorum\_setup/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

Cancel Review and Launch Next: Add Storage

- If you do not have an existing key pair or do not want to use an existing key pair, click **Create a new key pair** from the list, enter a name for the pair, and then click **Download Key Pair**.



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

Ports/Host Groups/iSCSI Targets

SIS-5200-2N-67.31(S/N:30548) > Ports/Host Groups/iSCSI Targets

Number of Ports

Target

Bidirectional

Total

Host Groups / iSCSI TargetsHostsPortsLogin WWNs/iSCSI NamesCHAP Users

Edit Ports

Remove Port CHAP Users

Edit T10 PI Mode

Export






Filter

ON

OFF

Select All Pages

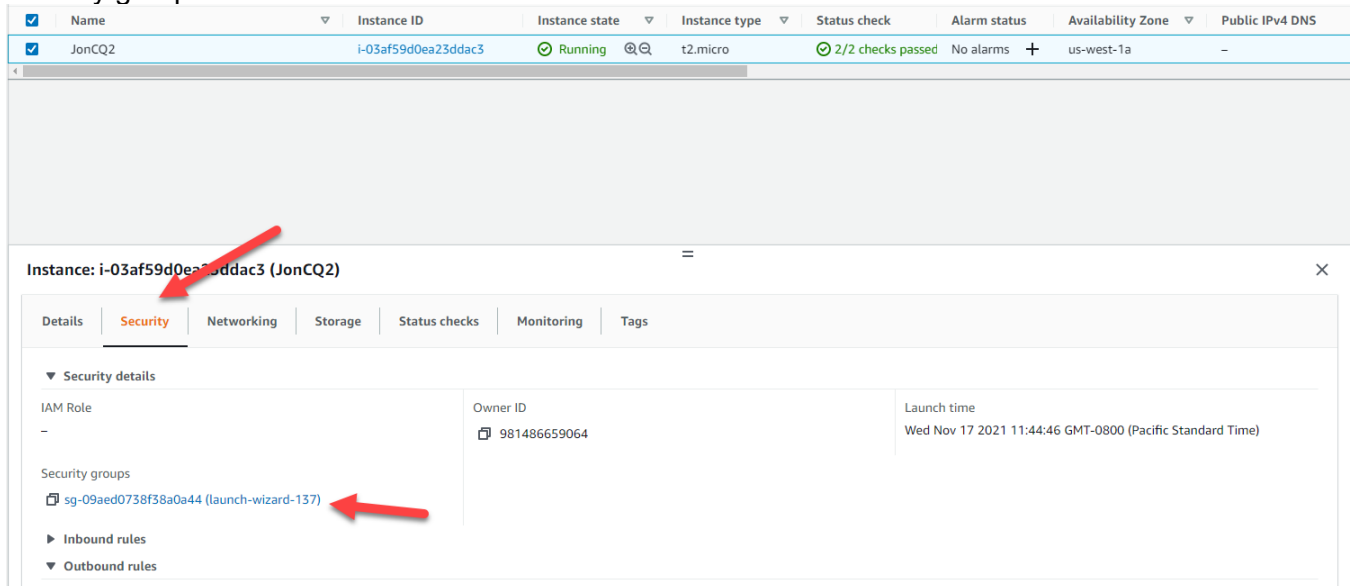
Column Settings

	Port ID	Type	Mode	iSCSI Virtual Port Mode	WWN / iSCSI Name	IPv4
						IP Address
<input type="checkbox"/>	 CL1-A	Fibre	SCSI	-	50060E8008775400	-
<input type="checkbox"/>	 CL3-A	Fibre	SCSI	-	50060E8008775420	-
<input checked="" type="checkbox"/>	 CL1-G	iSCSI	-	Disabled	iqn.1994-04.jp.co.hitachi:rsd.r90.l.087754.1g	172.23.90.177
<input checked="" type="checkbox"/>	 CL3-G	iSCSI	-	Disabled	iqn.1994-04.jp.co.hitachi:rsd.r90.l.087754.3g	192.168.0.14
<input type="checkbox"/>	 CL1-C	Fibre	SCSI	-	50060E8008775402	-

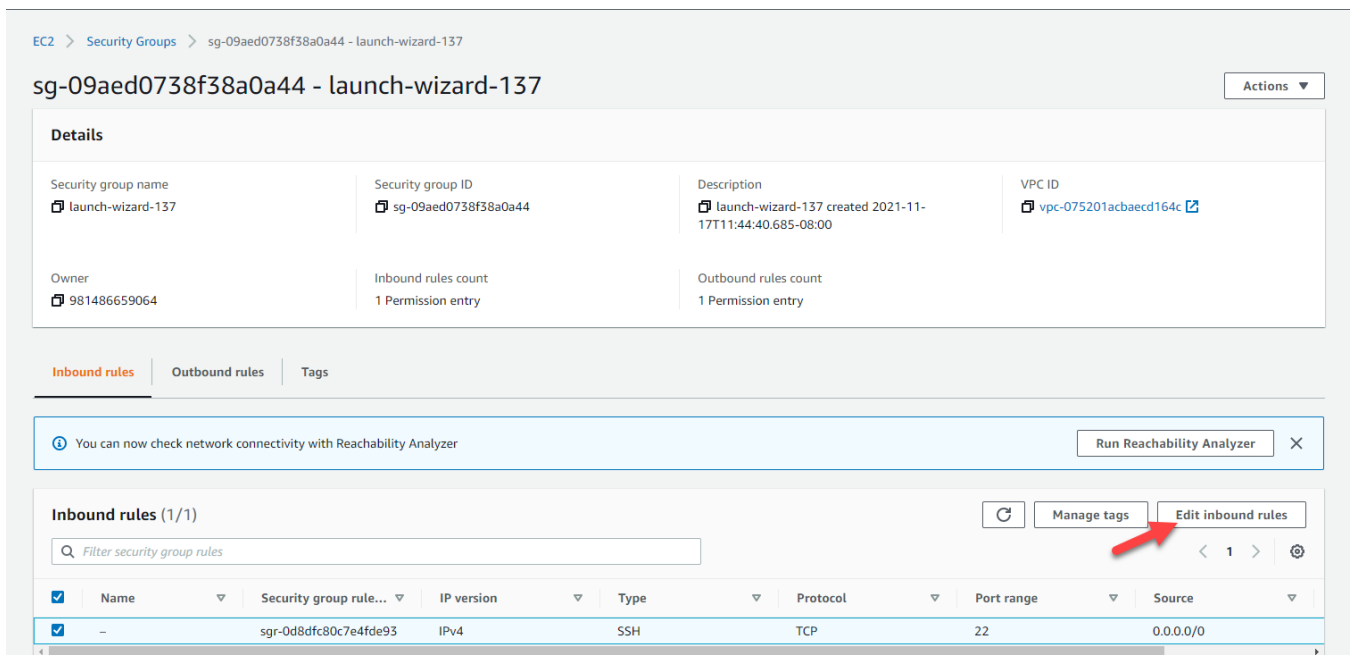
# Firewall Exemption

This section provides instructions for creating a firewall exemption on the AWS network so that the TCP traffic on port 3260 can enter the VCP network. Note that port 3260 is the default port used for iSCSI.

1. On the **Instances** page, select the virtual machine, click the **Security** tab, then select the security group attached to the instance.



2. Select the **Inbound rules** tab and then click **Edit inbound rules**.



3. Click **Add Rule**.
4. Enter the following values and then click **Add**:

**Edit inbound rules** [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional	
sgr-0d8dfc80c7e4fde93	SSH	TCP	22	Custom	0.0.0.0/0	Delete
-	Custom TCP	TCP	3260	Custom	172.17.173.0/24	Delete

[Add rule](#)

[Cancel](#) [Preview changes](#) [Save rules](#)

- **Type:** Custom TCP Rule
- **Port range:** 3260
- **Source:** Click Custom and then enter the subnet of the storage system iSCSI ports.
- **Descriptions:** iSCSI traffic

5. Click **Save rules**.

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

## Access Quorum VM

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 `ec2-user`.
3. Open the configuration script: `/home/ec2-user/quorum_setup/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

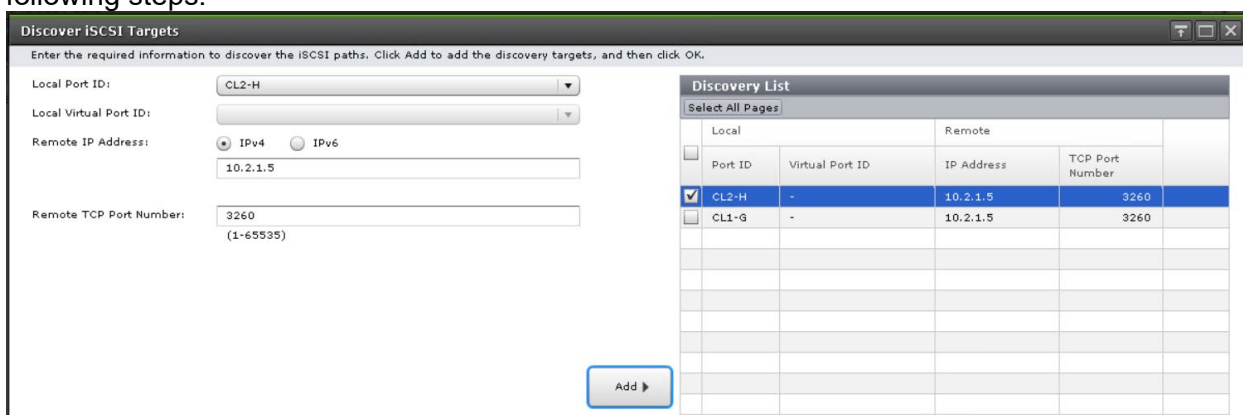
This section describes how to discover the volumes from the iSCSI target virtual machine and turn them into GAD quorums. The procedure is the same as it is to virtualize a physical Fibre Channel or iSCSI storage system.

## 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 AWS VM, complete the following steps:



- a. Enter the following:
    - **Local Port ID:** iSCSI port
    - **Remote IP Address:** private IP address of the AWS 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 on 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.

iSCSI Targets: [Discover iSCSI Targets](#)

**Available iSCSI Paths**

Filter: ON OFF Select All Pages Options 1 / 1

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

Add

**Selected iSCSI Paths**

Select All Pages

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

Remove Selected: 0 of 0

Authentication Method: None

Mutual CHAP: ☐ Enable ☒ Disable

User Name: (-)

Secret: (-)

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

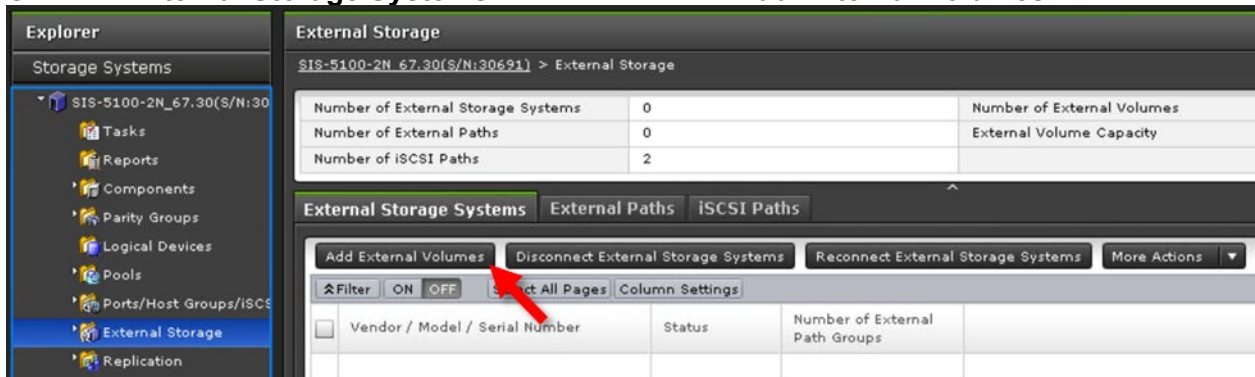
The following screenshot shows the iSCSI paths after creation:

External Storage Systems External Paths <b>iSCSI Paths</b>								
Add iSCSI Paths Edit iSCSI Targets Delete iSCSI Paths More Actions								
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	
<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	

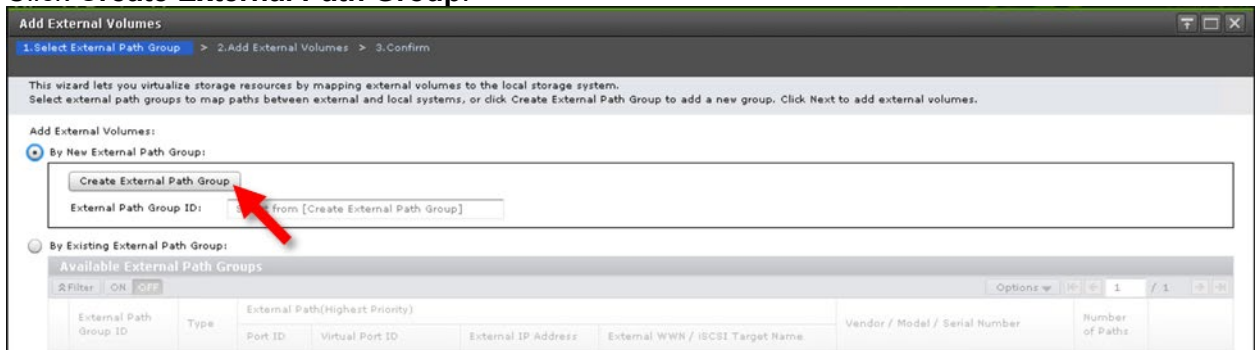


# Discover External Volumes

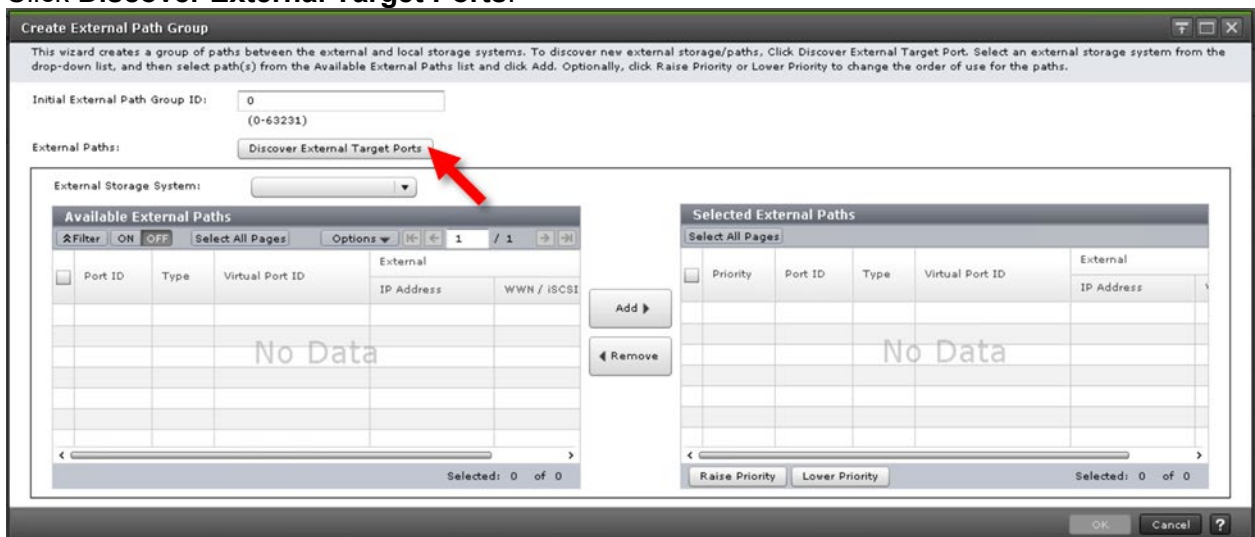
1. Click the **External Storage Systems** tab and then click **Add External Volumes**.



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

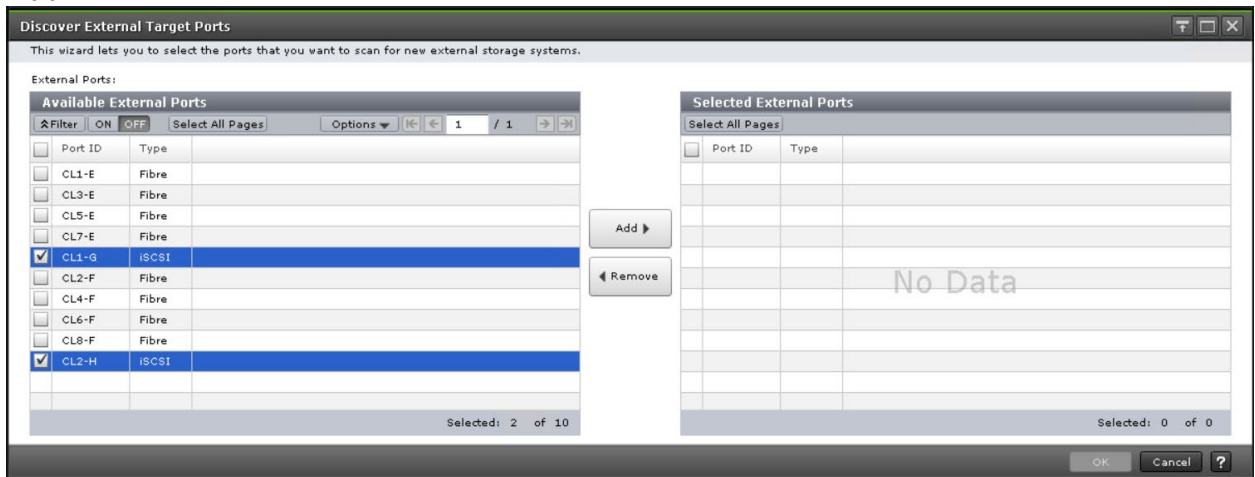


3. Click **Discover External Target Ports**.



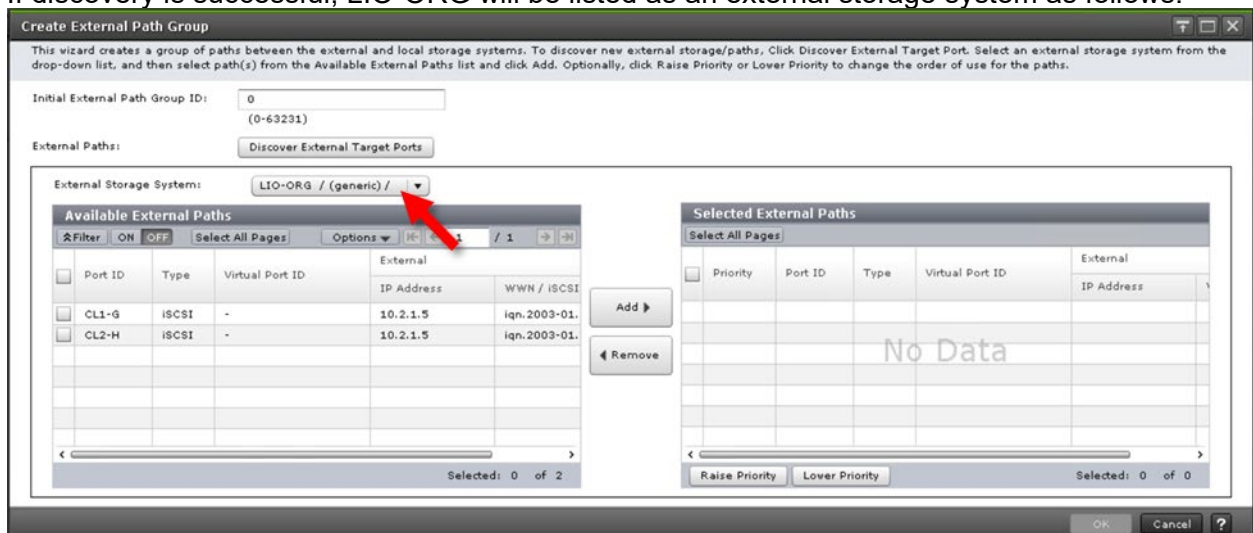


4. Select the iSCSI ports that defined the iSCSI paths in the previous section and then click **Add**.



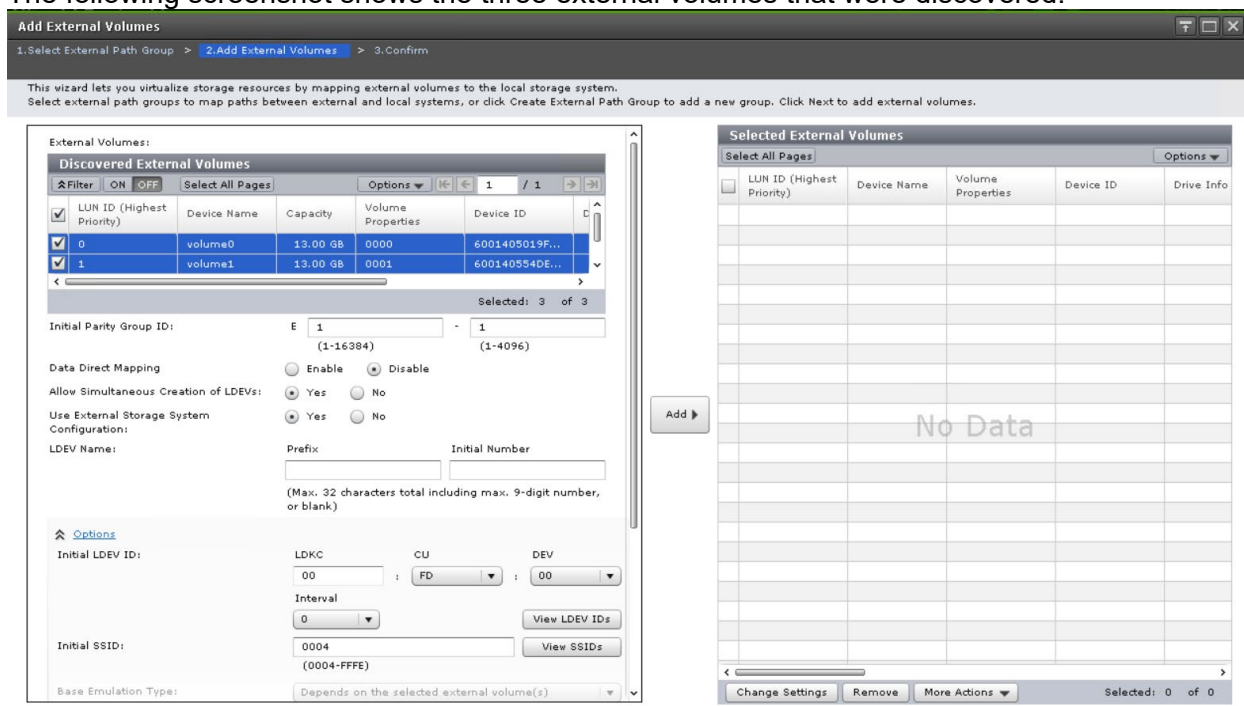
5. Click **OK**.

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 in the Add External Volumes screen, click **Next**.

The following screenshot shows the three external volumes that were discovered.

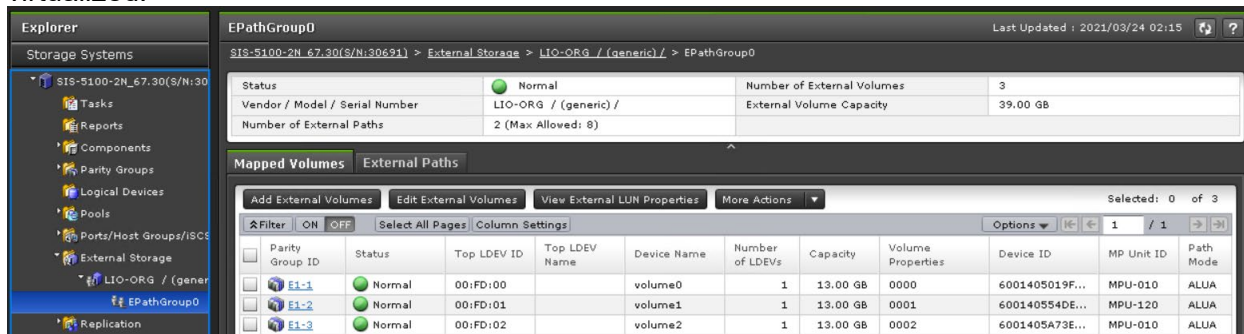


9. Select the discovered volumes and then click **Add**.

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).

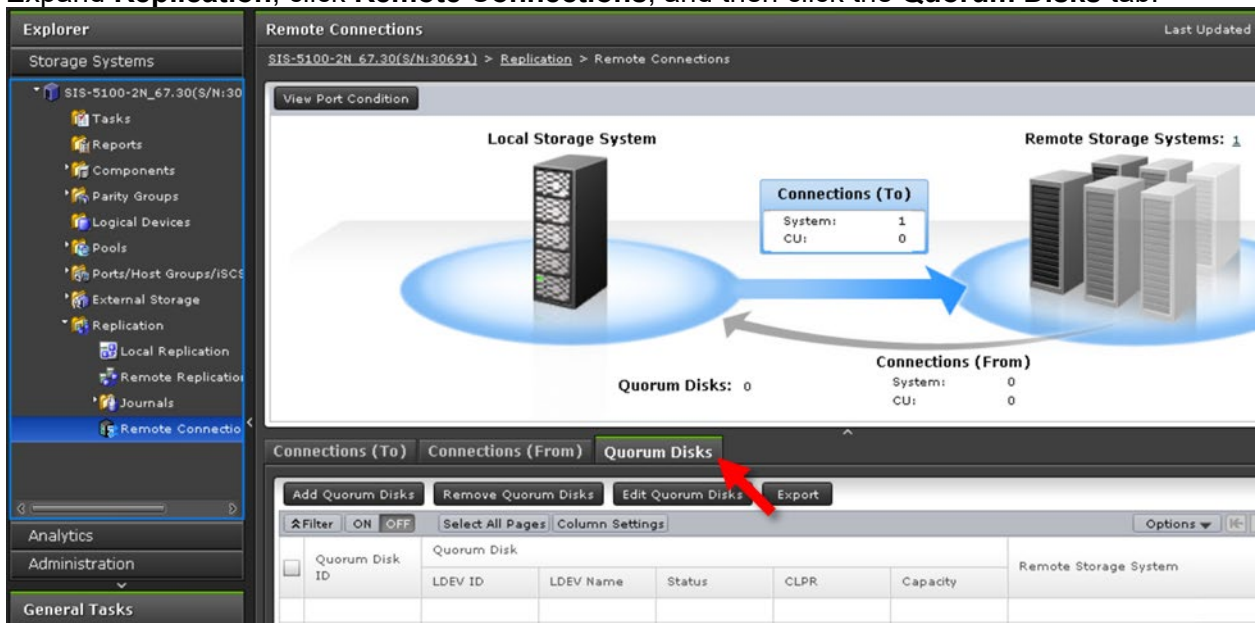
10. Click **Finish** and then click **Apply**.

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

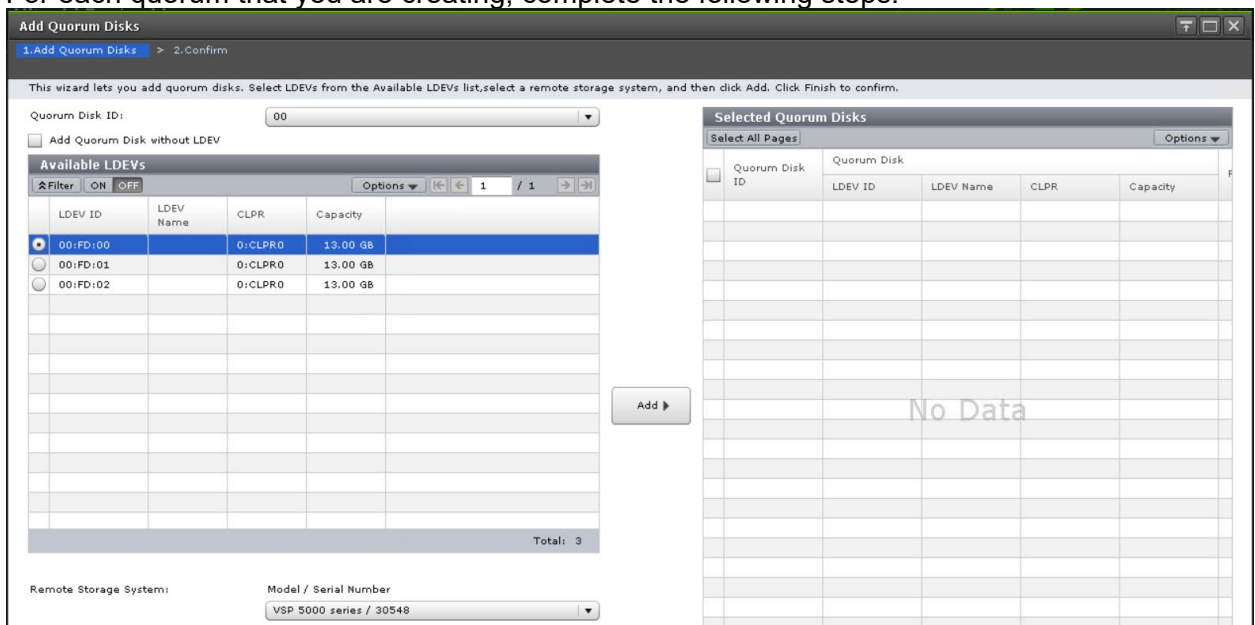


# Define GAD Quorums

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 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 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 A: 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 AWS 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 global-active device cloud quorum VM.
2. Enable mutual CHAP authentication by entering the following commands:  

```
/home/ec2-user/quorum_setup/menu.sh
```

  
6
3. Follow the prompts to set 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

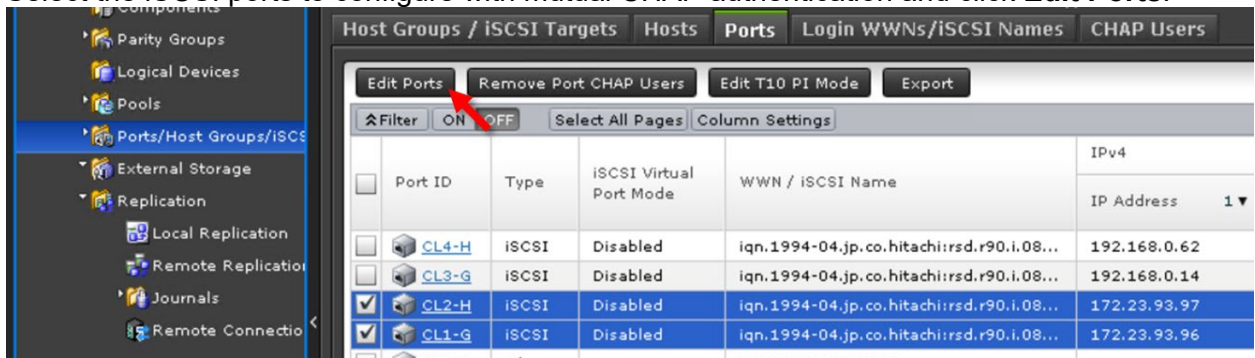
```

## 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:

- **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 AWS VM, complete the following steps:

Discover iSCSI Targets

Enter the required information to discover the iSCSI paths. Click Add to add the discovery targets, and then click OK.

Local Port ID: CL2-H

Local Virtual Port ID:

Remote IP Address: IPv4 IPv6 10.2.1.5

Remote TCP Port Number: 3260 (1-65535)

Add

Local	Remote			
Port ID	Virtual Port ID	IP Address	TCP Port Number	
<input checked="" type="checkbox"/>	CL2-H	-	10.2.1.5	3260
<input type="checkbox"/>	CL1-G	-	10.2.1.5	3260

- a. Enter the following:
  - **Local Port ID:** iSCSI port
  - **Remote IP Address:** private IP address of the AWS 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:

Add iSCSI Paths

Enter the required information to add the iSCSI paths. Click Add to add the iSCSI paths, and then click OK.

Authentication Method: CHAP

Mutual CHAP: Enable Disable

User Name: (Max. 223 characters)

Secret: (12 - 32 characters)

Add

- 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](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)

