

Global-Active Device Cloud Quorum in AWS

V3.0.0

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 for a third site to host the quorum by deploying it in the cloud.

Hitachi Vantara

MK-92RD8087-03

April 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

Table of Contents	3
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
VPN Tunnel	7
AWS Virtual Machine	7
Amazon Virtual Machine.....	8
Deployment	8
Firewall Exemption	13
Access Quorum VM	14
Global-Active Device Quorums.....	16
Create iSCSI Paths	16
Discover External Volumes	18
Define GAD Quorums	21
Upgrade Instructions	22
Upgrade Steps	22
Clean up	23
Appendix A: Mutual CHAP Authentication (Optional).....	24
Enable on targetcli.....	24
Enable on iSCSI Ports.....	25
Create iSCSI Paths	26

Preface

About this document

This guide provides instructions for deploying Global-Active Device Cloud Quorum in AWS version 2.0.0 as well as upgrading from a previous version to 2.0.0. The main difference in the new version is a change in the operating system from Amazon Linux 2 to SUSE Linux 15 SP4.

Document conventions

This document uses the following typographic convention:

Convention	Description
Bold	<ul style="list-style-type: none">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 or upgrading GAD Cloud Quorum running AWS Linux OS to the latest version of GAD Cloud Quorum (v2.0.0) running SUSE Linux 15 SP4.

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) Cloud Quorum is a virtual machine image provided by Hitachi Vantara through the Amazon Web Services (AWS) Marketplace. Its purpose is to simplify and enhance GAD by replacing an on-premises 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. This is avoided by hosting the quorum disk on-premises at a separate datacenter; however, with GAD Cloud Quorum, you can achieve the same result without the associated overhead. This guide provides instructions on how to set up, upgrade, and use GAD Cloud Quorum on AWS.

If you are running an existing GAD Cloud Quorum that is older than v2.0.0 and want to upgrade to the latest GAD Cloud Quorum in AWS (v2.0.0) running SUSE Linux 15 SP4, you must run a few `raidcom` commands to complete the upgrade process. Overall, the upgrade process is very simple and non-disruptive to your GAD environment.

Configuration and Specifications

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

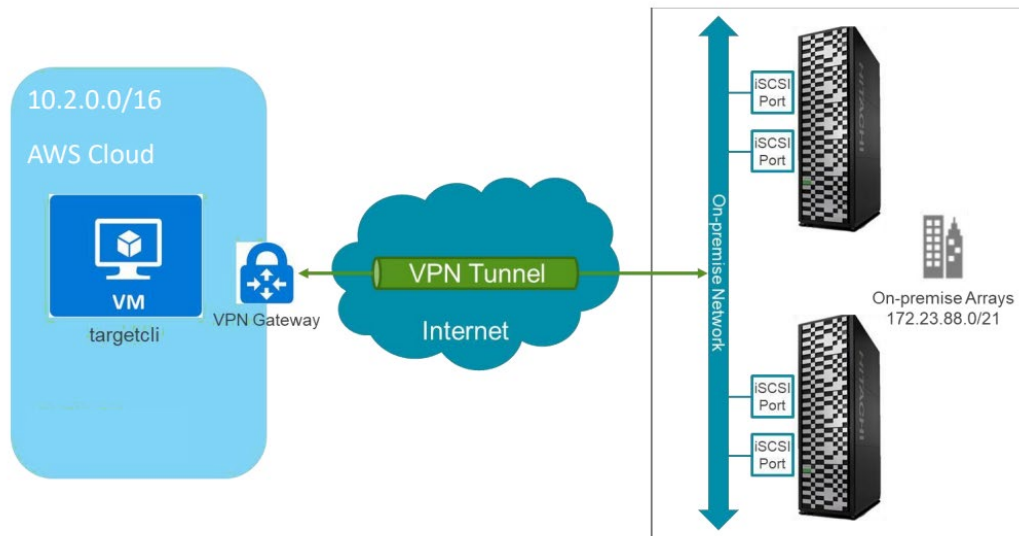


Figure 1: Test Environment

VPN Gateway

During the certification of this solution, we determined that the AWS VPN Gateway plays an important role. You must use a sufficiently large VPN Gateway 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: SUSE Linux Enterprise Server 15 SP4
- Kernel: 4.12.14-197.83-default
- Instance type: t2.micro
 - CPU: 1 virtual CPU
 - Memory: 1 GB
 - Disks: Premium SSD 67 GB
- Targetcli version: 2.1.fb49

Amazon Virtual Machine

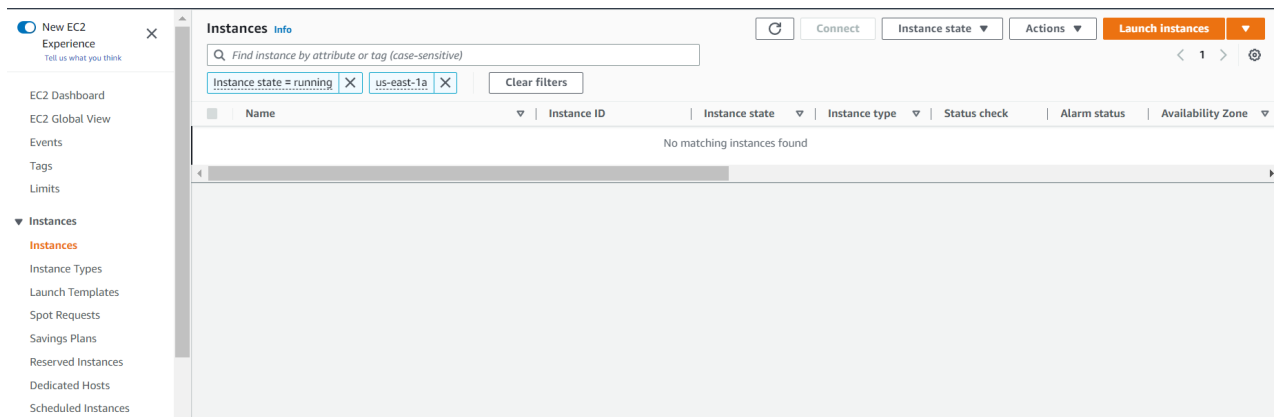
Deployment

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 deployment, we recommend you use an AWS Region and Availability Zone located within 40ms ping of your VSP storage systems.

In our testing performed in the western US connected to our lab in Denver, CO, we saw a ping of ~30ms. In this testing, under Availability options, no infrastructure redundancy was used. For more ways to improve the redundancy, see [Higher Availability with Global-Active Device Cloud Quorum Using AWS Auto Scaling](#)

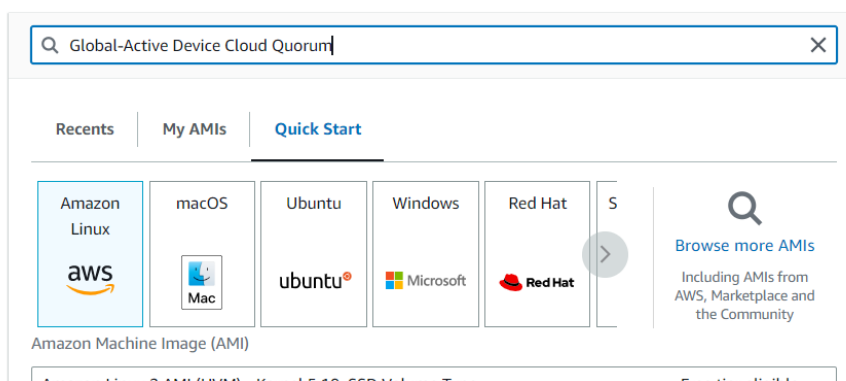
1. To use Amazon EC2 services, navigate to the Instances screen and click **Launch instances**.



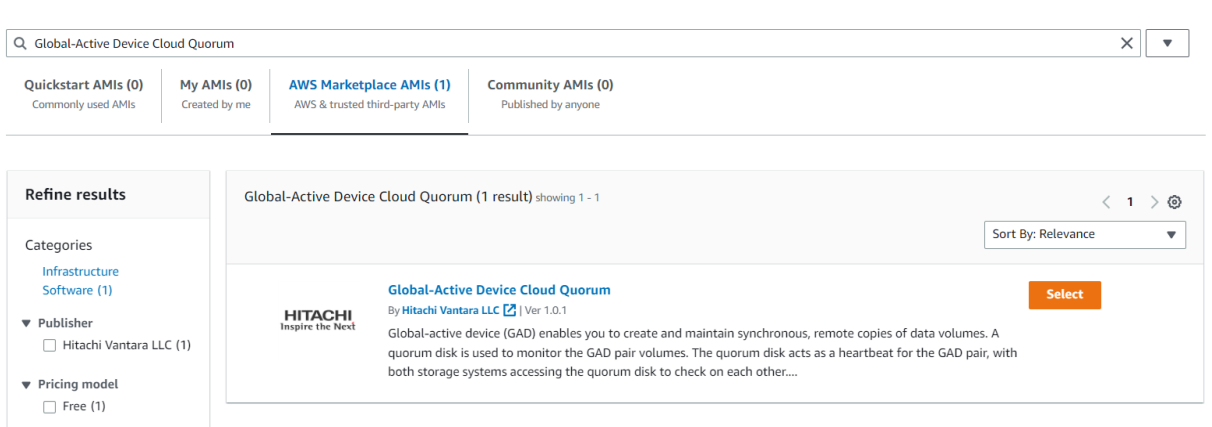
2. Under Application and OS Images (Amazon Machine Image), enter Global-Active Device Cloud Quorum.

▼ Application and OS Images (Amazon Machine Image) Info

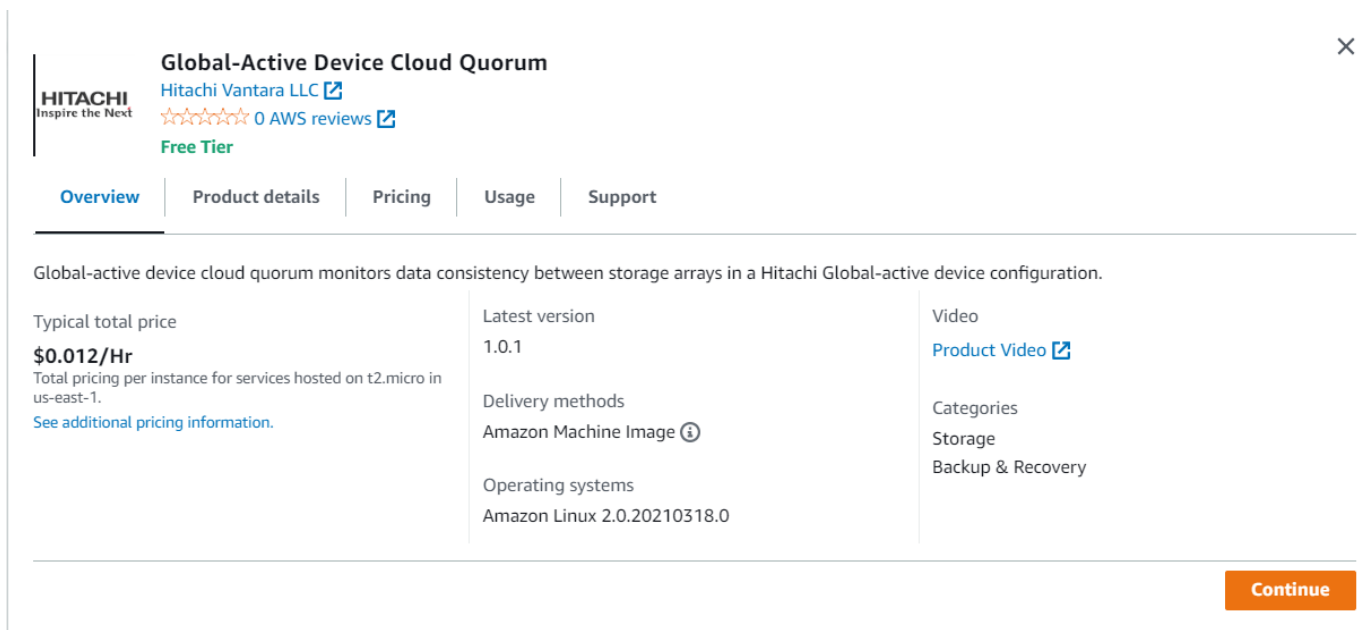
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below



After clicking enter, you will see the following image under AWS Marketplace AMIs:



3. Select the image and click **Continue**.




4. From the **Network setting** drop-down menu, click **Edit**.



For the initial configuration, we recommend **Disable** from the **Auto-assign Public IP** list to prevent unauthorized access to the virtual machine.

▼ **Network settings**


VPC - required [Info](#)

(default) ▼ 

Subnet [Info](#)

No preference ▼  [Create new subnet](#) 

Auto-assign public IP [Info](#)

Disable ▼ 

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

launch-wizard-7

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and . _ - / () # , @ [] + = & ; ! \$ *

5. From the **Advanced details** drop-down menu, under user data, enter the following and then add the iSCSI Qualified Names (IQN) of your GAD storage system ports separated by spaces:

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

Metadata version [Info](#)

Select

Metadata response hop limit [Info](#)

Select

Allow tags in metadata [Info](#)

Select

User data [Info](#)

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

☐ User data has already been base64 encoded

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 Targets Hosts **Ports** Login WWNs/iSCSI Names CHAP 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.i.087754.1g	172.23.90.177
<input checked="" type="checkbox"/> CL3-G	iSCSI	-	Disabled	iqn.1994-04.jp.co.hitachi.rsd.r90.i.087754.3g	192.168.0.14
<input type="checkbox"/> CL1-C	Fibre	SCSI	-	50060E8008775402	-

Note: You can find your VSP IQNs by using Storage Navigator.


- 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 **Key pair (login)** drop-down menu, enter a name for the pair, and then click **Create Key Pair**.


▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼

 [Create new key pair](#)



- Click **Launch instance**.

▼ **Summary**

Number of instances [Info](#)

1

[Software Image \(AMI\)](#)

Global-Active Device Cloud Quo...
ami-06f0f800e8bd6d160

[Virtual server type \(instance type\)](#)

t2.micro

[Firewall \(security group\)](#)

New security group

[Storage \(volumes\)](#)

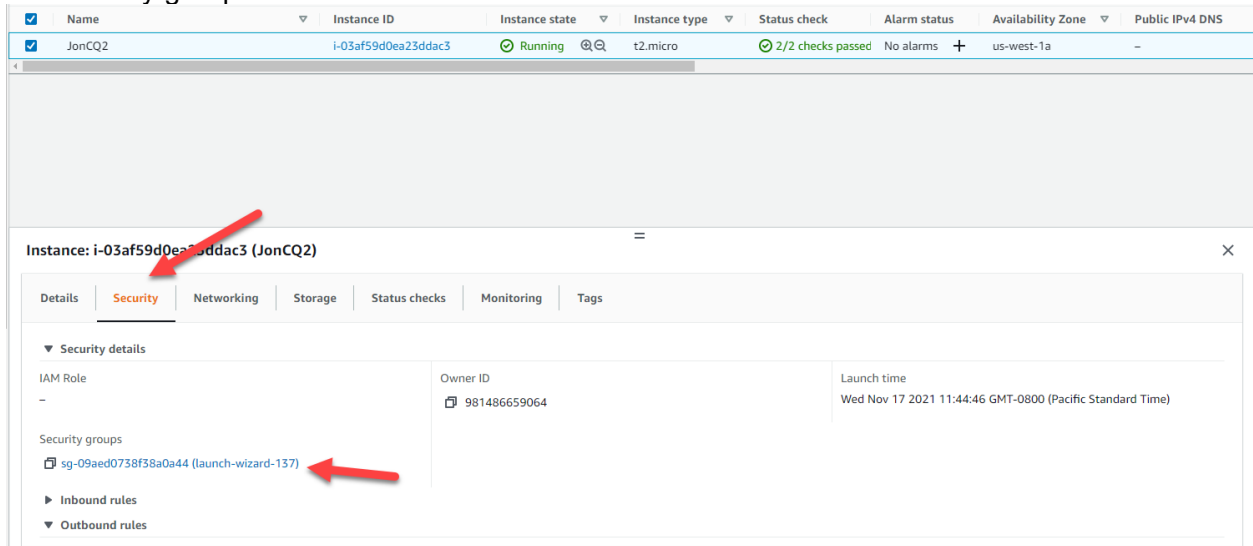
2 volume(s) - 75 GiB

Cancel **Launch instance**

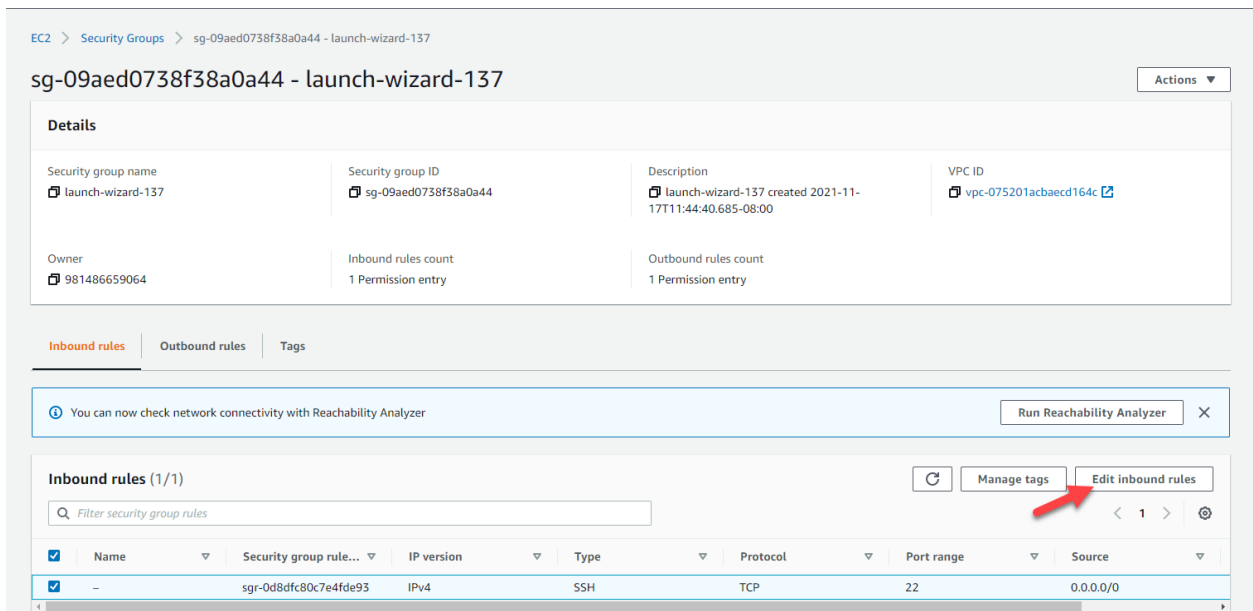
Firewall Exemption

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, and 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		Delete
-	Custom TCP	TCP	3260	Custom	iSCSI traffic	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 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 ec2-user.
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).

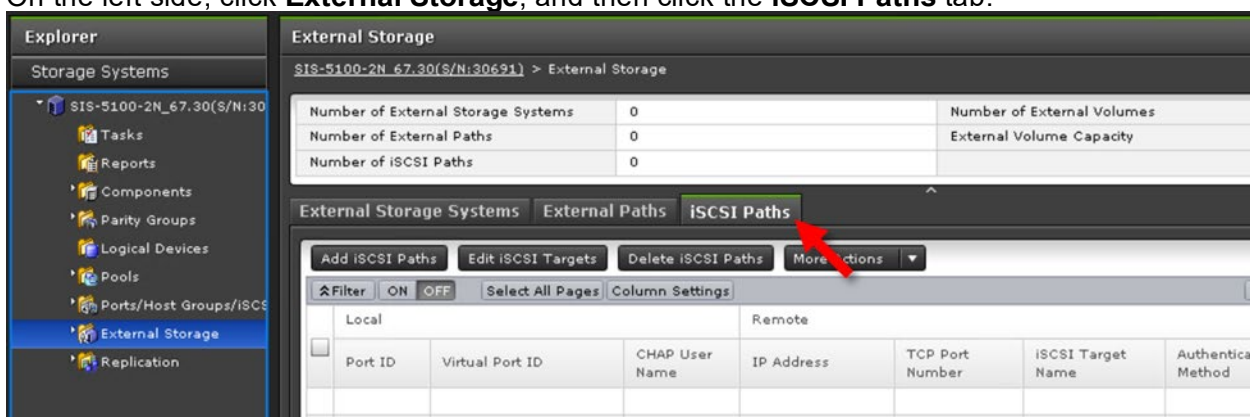
Note: If you intend to use CHAP, ensure to enable it during initial configuration because making changes to CHAP settings in the future may be difficult or not possible.

Global-Active Device Quorums

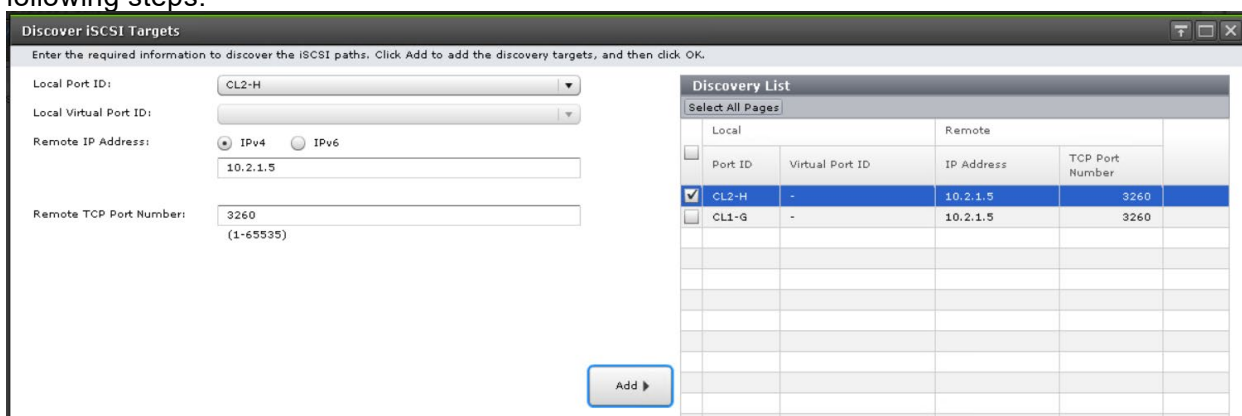
This section describes how to discover the volumes from the iSCSI target virtual machine and turn them into GAD quorums. The procedure is the same as it is to virtualize a physical Fibre Channel or iSCSI storage system.

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 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**.

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
<input checked="" type="checkbox"/>	CL2-H	-	10.2.1.5
<input checked="" type="checkbox"/>	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

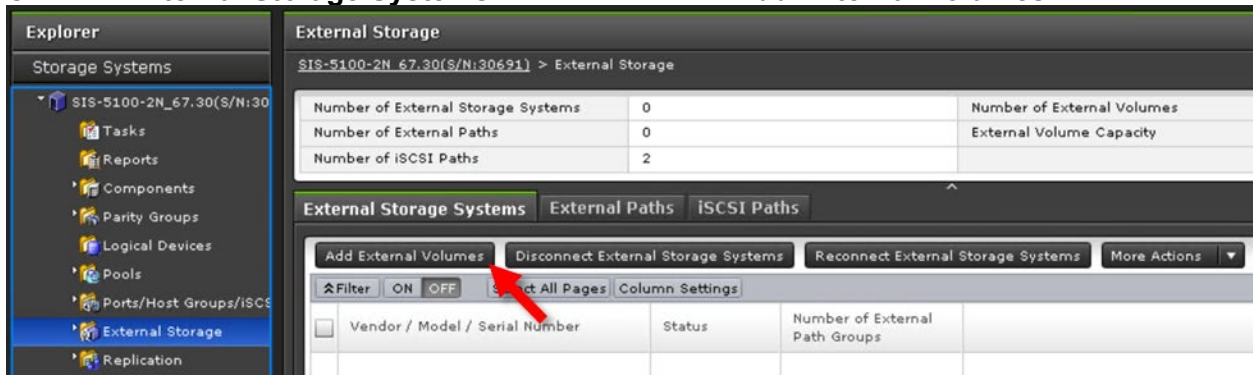
- Click **Finish** and then click **Apply**.

The following screenshot shows the iSCSI paths after creation:

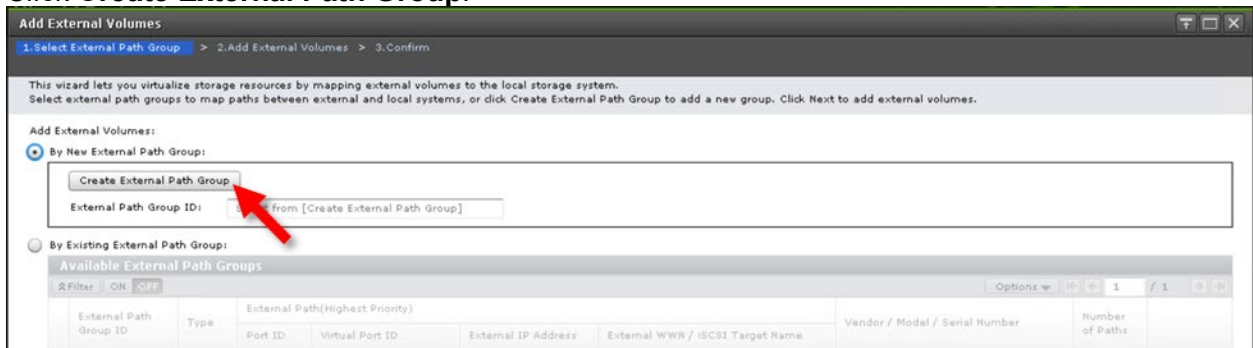
External Storage Systems External Paths iSCSI Paths								
Add iSCSI Paths Edit iSCSI Targets Delete iSCSI Paths More Actions								
Filter ON OFF Select All Pages Column Settings Options 1								
Local	Remote							
Port ID	Virtual Port ID	CHAP User Name	IP Address	TCP Port Number	iSCSI Target Name	Authentication Method	Mutual CHAP	
<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

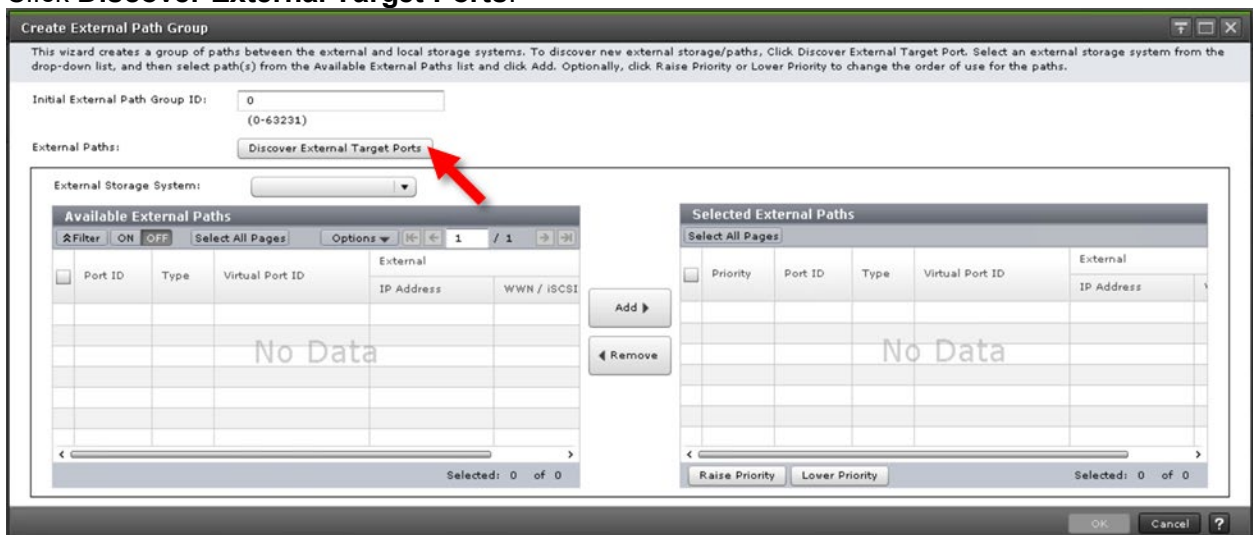
1. Click the **External Storage Systems** tab and then click **Add External Volumes**.



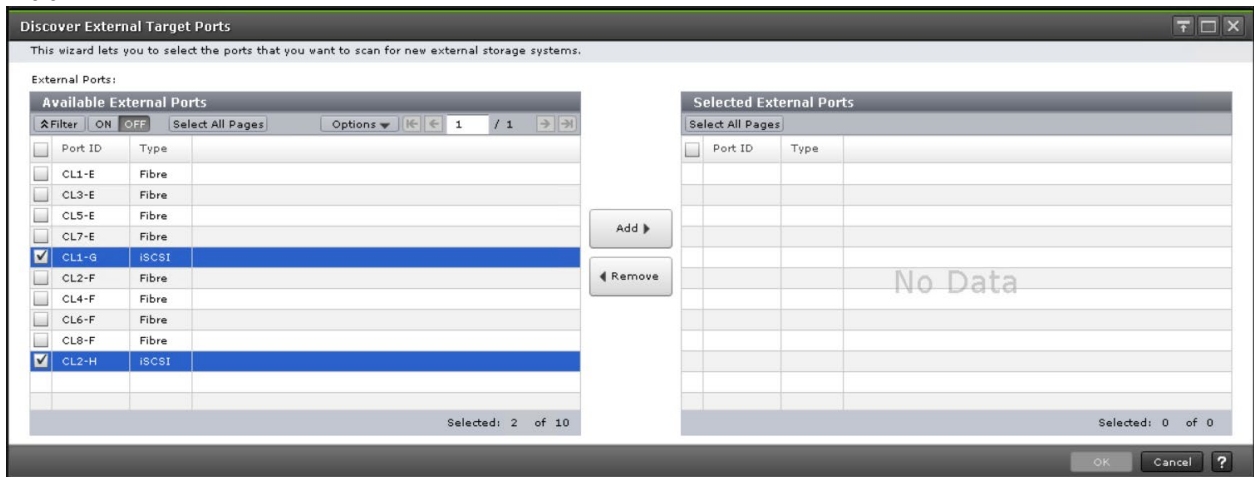
2. Click **Create External Path Group**.



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

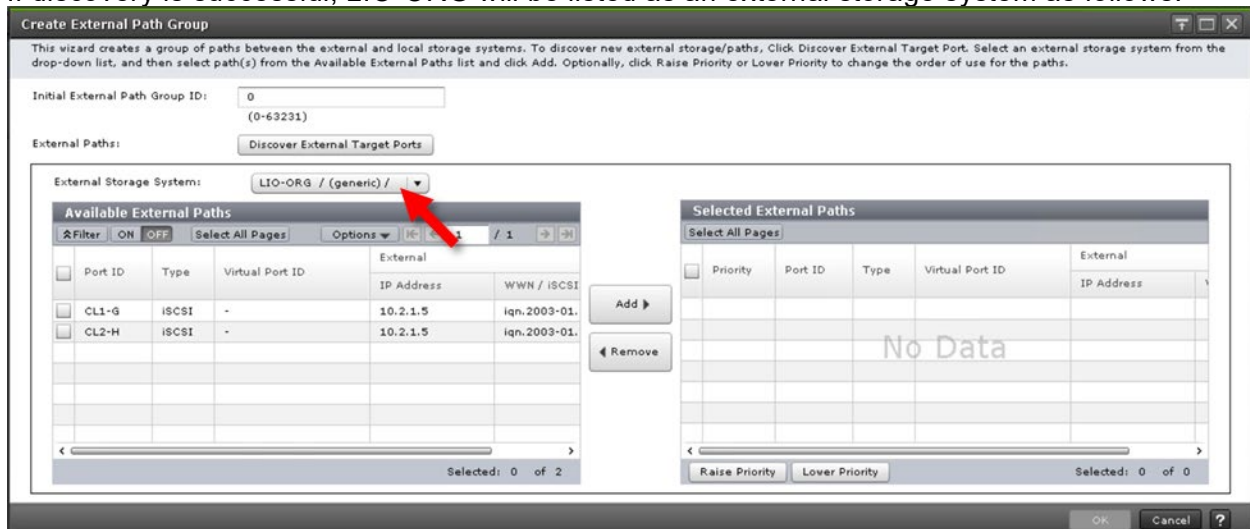


4. Select the iSCSI ports that defined the iSCSI paths in the previous section and then click **Add**.



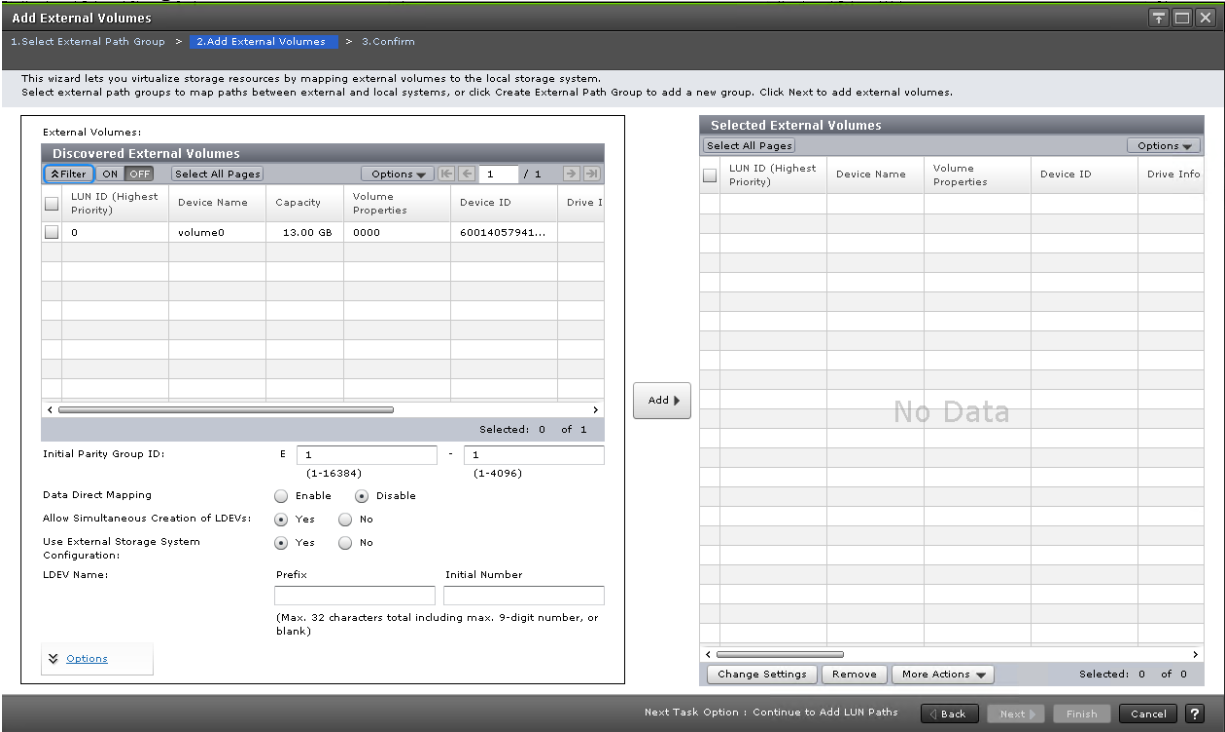
5. Click **OK**.

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 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.

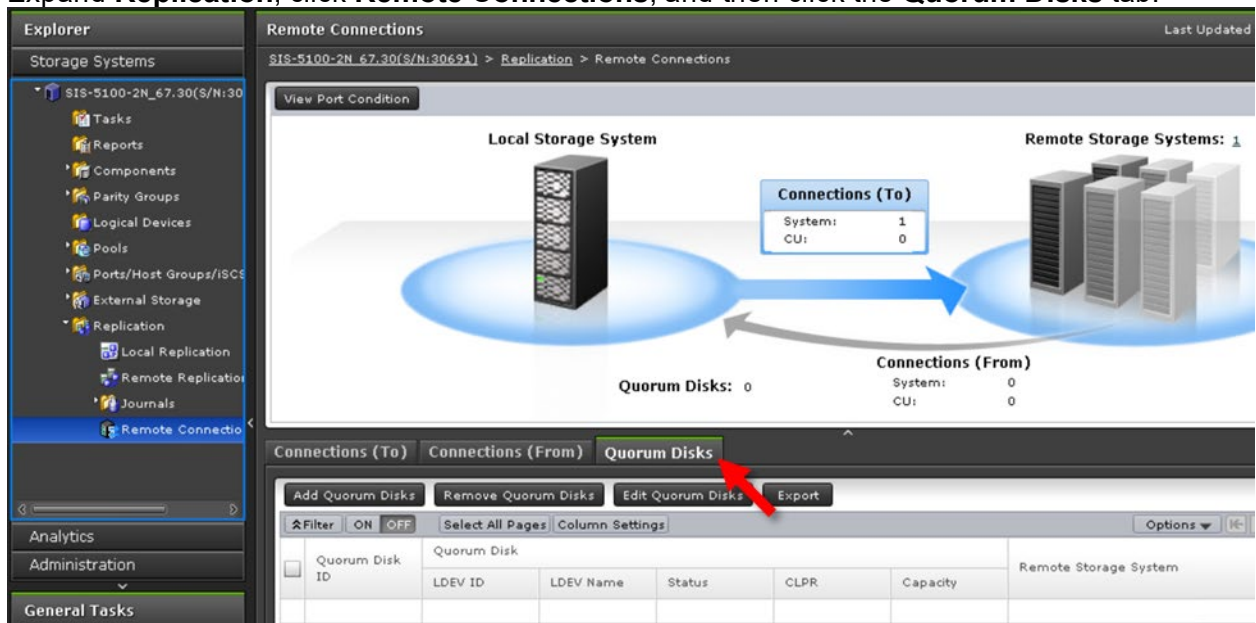
10. Click **Finish** and then click **Apply**.

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.

Connections (To) Connections (From) 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
<input type="checkbox"/> 00	00:00:02		● Normal	0:CLPR0	13.00 GB	VSP 5000 series / 30548

Upgrade Instructions

The following instructions describe how to upgrade an existing GAD Cloud Quorum running an early version to v2.0.0. If you are deploying GAD Cloud Quorum for the first time, ignore these instructions.

Upgrade Steps

1. Disconnect the old quorum by running the following command:

```
raidcom disconnect external_grp -ldev_id <ldev#> | -  
external_grp_id <gno-sgno>
```

Example: `raidcom disconnect external_grp -ldev_id 00:00`

```
[root@sisd51b-04 ~]# raidcom disconnect external_grp -ldev_id 00:00 -IH30  
raidcom: EGRP 1-17(0x1-0x11) will be used for LDEV# 0.
```

2. Replace the old quorum with the newly defined quorum by running the following command:

```
raidcom replace quorum -quorum_id <quorum id> -ldev_id <ldev#>
```

Example: `raidcom replace quorum -quorum_id 0 -ldev_id 00:02`

```
[root@sisd51b-04 ~]# raidcom replace quorum -quorum_id 0 -ldev_id 00:02 -IH30  
[root@sisd51b-04 ~]# raidcom get quorum -quorum_id 0 -I30  
QRDID : 0  
LDEV : 2  
QRP_Serial# : 530548  
QRP_ID : R9  
Timeout(s) : 40  
STS : REPLACING
```

Connections (To)		Connections (From)		Quorum Disks				
Add Quorum Disks		Remove Quorum Disks		Edit Quorum Disks			Export	
Filter ON OFF		Select All Pages		Column Settings			Options 1	
Quorum Disk ID		LDEV ID		LDEV Name		Status	CLPR	Capacity
00		00:00:02				Normal	0:CLPR0	13.00 GB
								VSP 5000 series / 30548

Note: The LDEV ID used in the command refers to the LDEV ID of the new quorum.

The quorum disk is now changed to the new quorum.

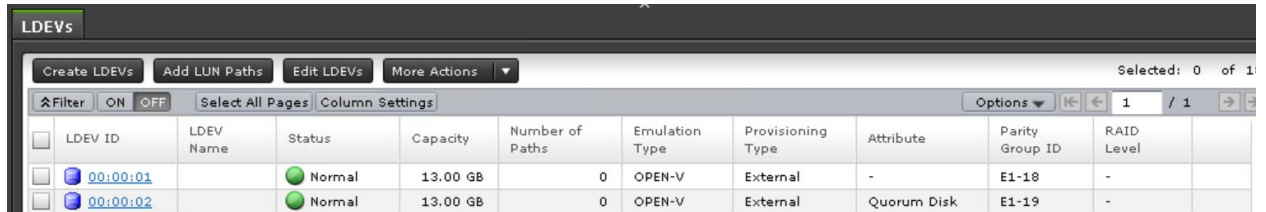
Clean up

1. Delete the old external volume by running the following command:

```
raidcom delete ldev -ldev_id <ldev_id>
```

Example: `raidcom delete ldev -ldev_id 00:00`

```
[root@sisd51b-04 ~]# raidcom delete ldev -ldev_id 00:00 -IH30
[root@sisd51b-04 ~]#
```



LDEV ID	LDEV Name	Status	Capacity	Number of Paths	Emulation Type	Provisioning Type	Attribute	Parity Group ID	RAID Level
00:00:01		Normal	13.00 GB	0	OPEN-V	External	-	E1-18	-
00:00:02		Normal	13.00 GB	0	OPEN-V	External	Quorum Disk	E1-19	-

LDEV 00:00 is no longer shown under LDEVs.

2. Delete the disconnected external groups by running the following command:

```
raidcom delete external_grp -external_grp_id <gno-sgno> [-forcible]
```

Example: `raidcom delete external_grp -external_grp_id`

```
[root@sisd51b-04 ~]# raidcom delete external_grp -external_grp_id 1-17 -IH30
[root@sisd51b-04 ~]#
```

```
# raidcom get external_grp -external_grp_id 1-17 -I30
```

The command should return nothing after properly deleting the disconnected external group.

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 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:

```
./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'.

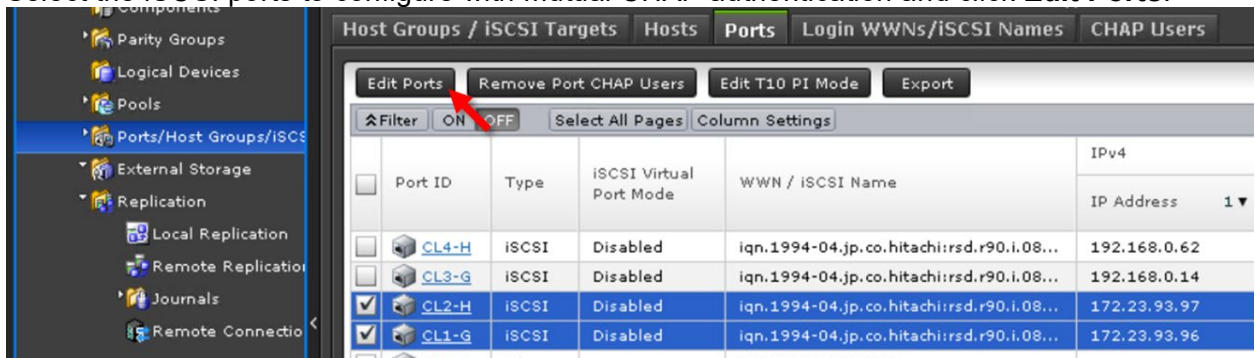
/> /iscsi/iqn.20...0.i.089c42.1g> Parameter userid is now 'uid'.
/iscsi/iqn.20...0.i.089c42.1g> Parameter password is now 'pass'.
/iscsi/iqn.20...0.i.089c42.1g> Parameter mutual_userid is now 'muid'.
/iscsi/iqn.20...0.i.089c42.1g> Parameter mutual_password is now 'mpass'.
/iscsi/iqn.20...0.i.089c42.1g> /> 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)

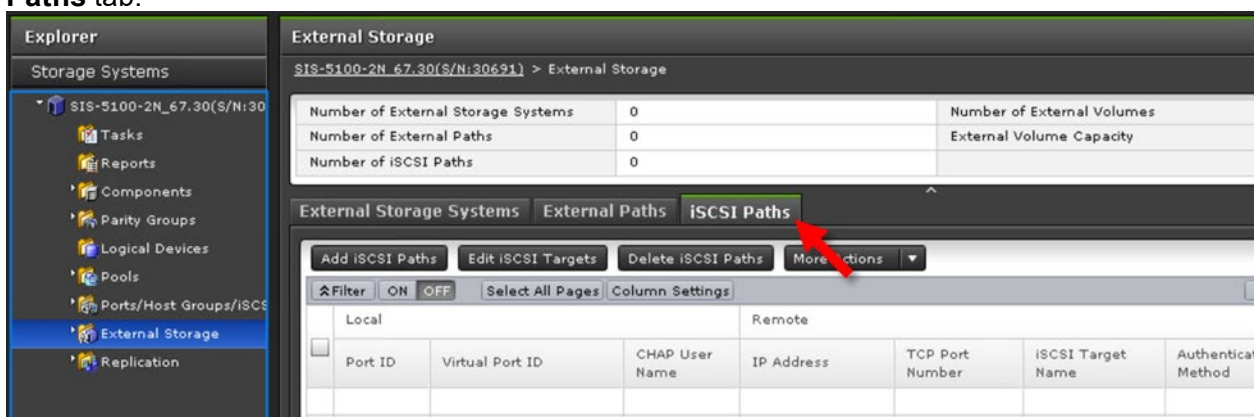
☒ Secret:
 (12 - 32 characters)

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

Discovery List

Local Port ID	Virtual Port ID	IP Address	TCP Port Number
CL2-H	-	10.2.1.5	3260
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:

External Storage Systems External Paths **iSCSI Paths**

Add iSCSI Paths Edit iSCSI Targets Delete iSCSI Paths More Actions ▼

Selected: 0 of

Filter ON OFF Select All Pages Column Settings Options ▼ 1 / 1

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
<input type="checkbox"/>	CL1-G	-		10.2.1.5	3260	iqn.2003-01....	CHAP	Enabled	
<input type="checkbox"/>	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

