# 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**

# Table of Contents

# 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** | • Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: **Click OK**.<br>• Indicates emphasized words in list items. |
| *Italic* | Indicates a document title or emphasized words in text. |
| `Monospace` | Indicates text that is displayed on screen or entered by the user.<br>Example: `pairdisplay -g oradb` |

## 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.

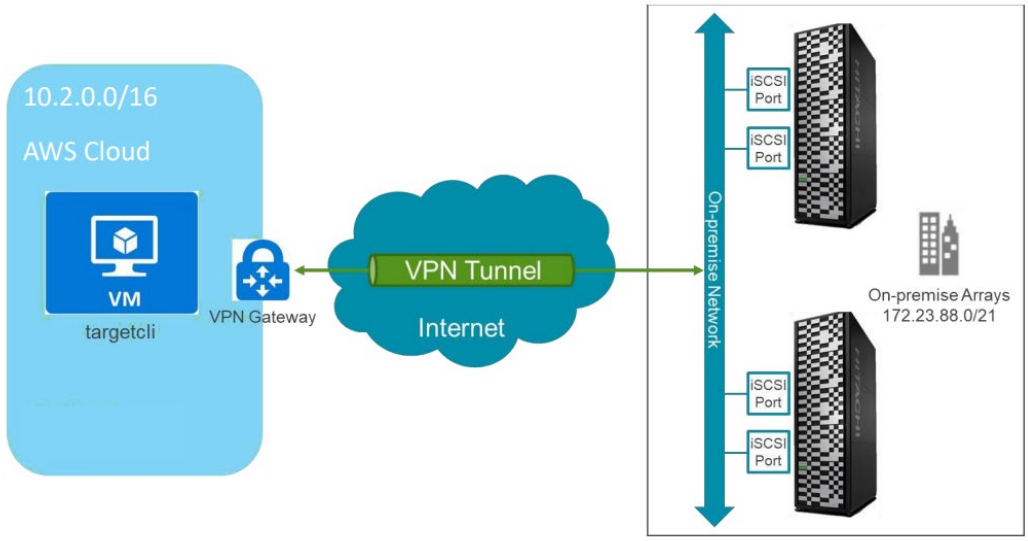



*Figure 1: Test Environment*

## 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

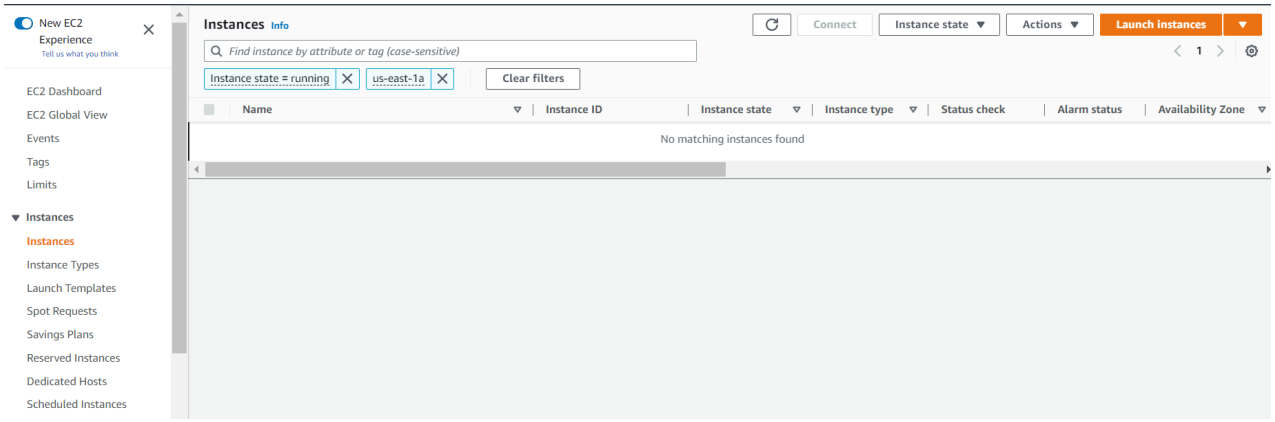
## Deployment

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

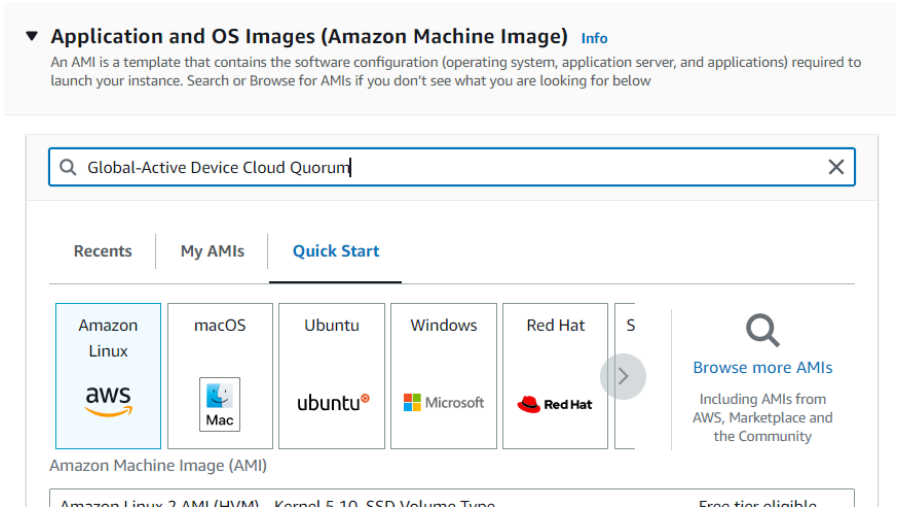
We assume that you are familiar with using an SSH public key for authentication, so we do not cover this topic. For this deployment, we recommend you use an AWS Region and Availability Zone located within 40ms ping of your VSP storage systems.

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

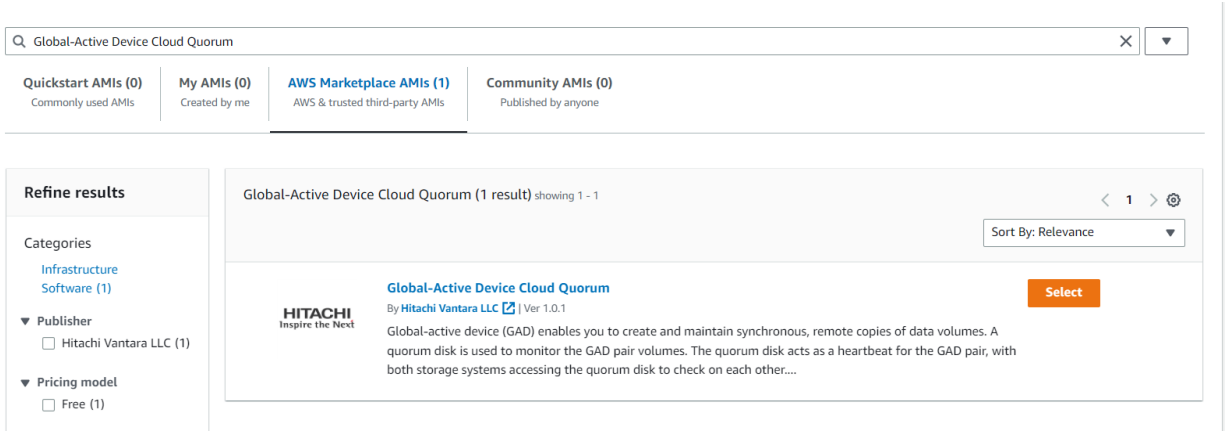
1. To use Amazon EC2 services, navigate to the Instances screen and click **Launch instances**.



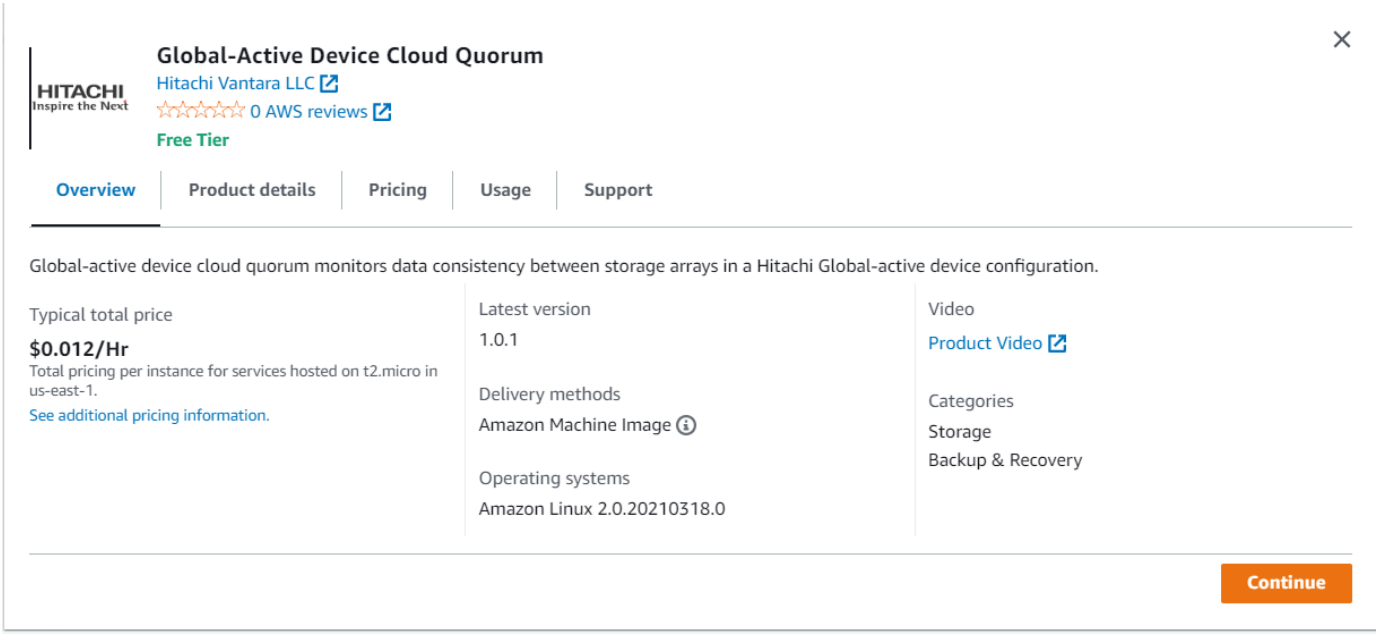

2. Under Application and OS Images (Amazon Machine Image), enter Global-Active Device Cloud Quorum.



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

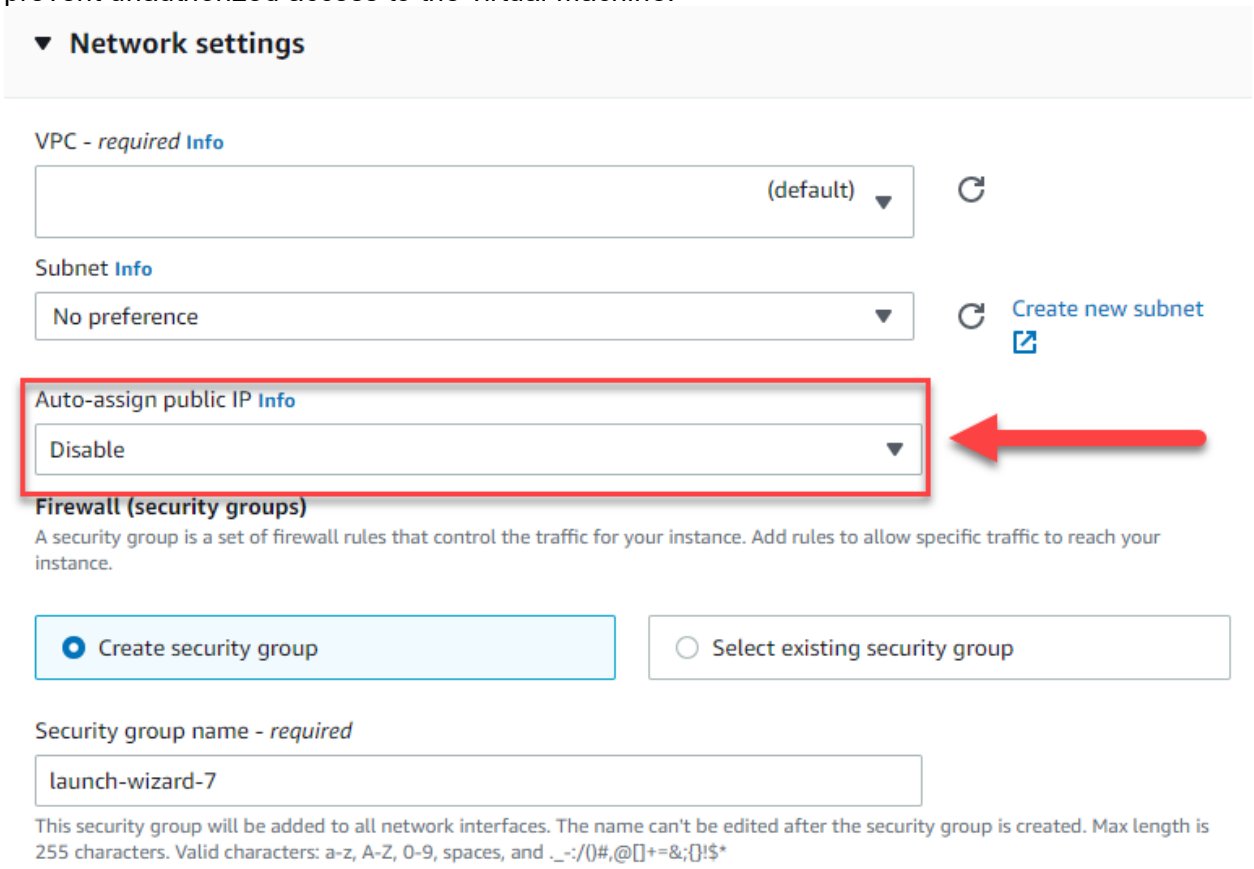



3. Select the image and click **Continue**.



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.




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

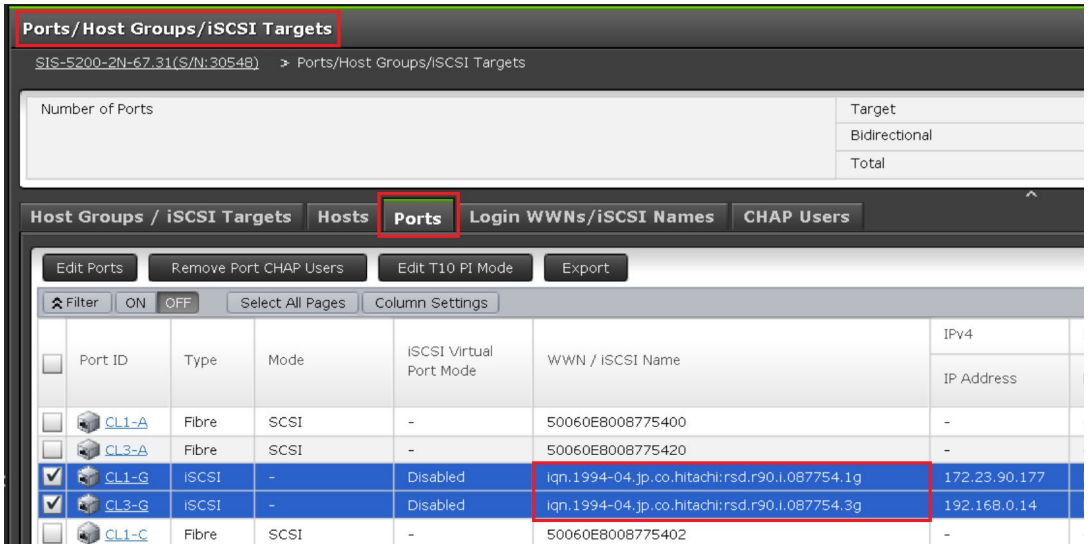
Allow tags in metadata Info

Select

User data Info

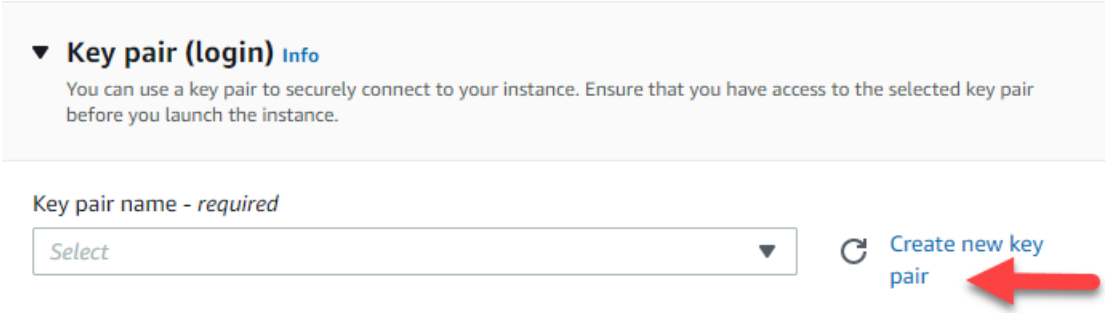
```
#!/bin/bash
/home/ec2-user/quorum_setup/quorum_setup.sh
```

User data has already been base64 encoded

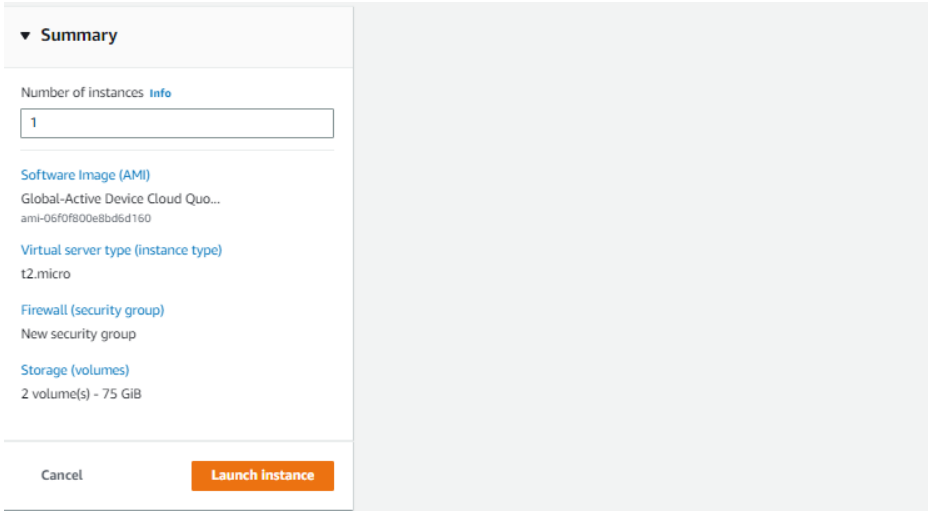



**Note**: You can find your VSP IQNs by using Storage Navigator.

6. 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.**



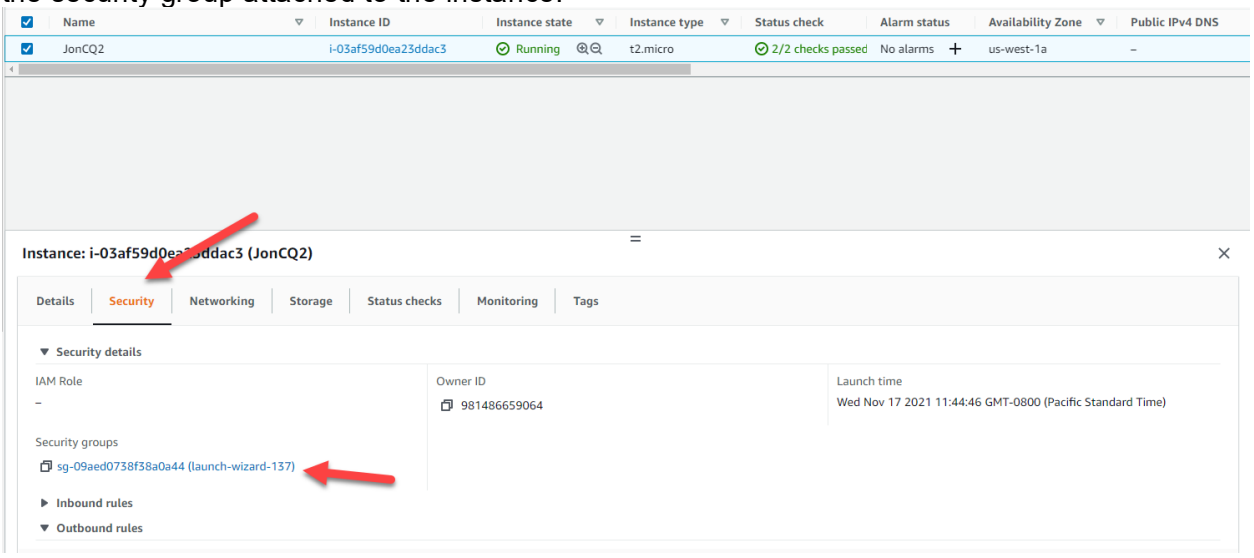

7. Click **Launch instance**.



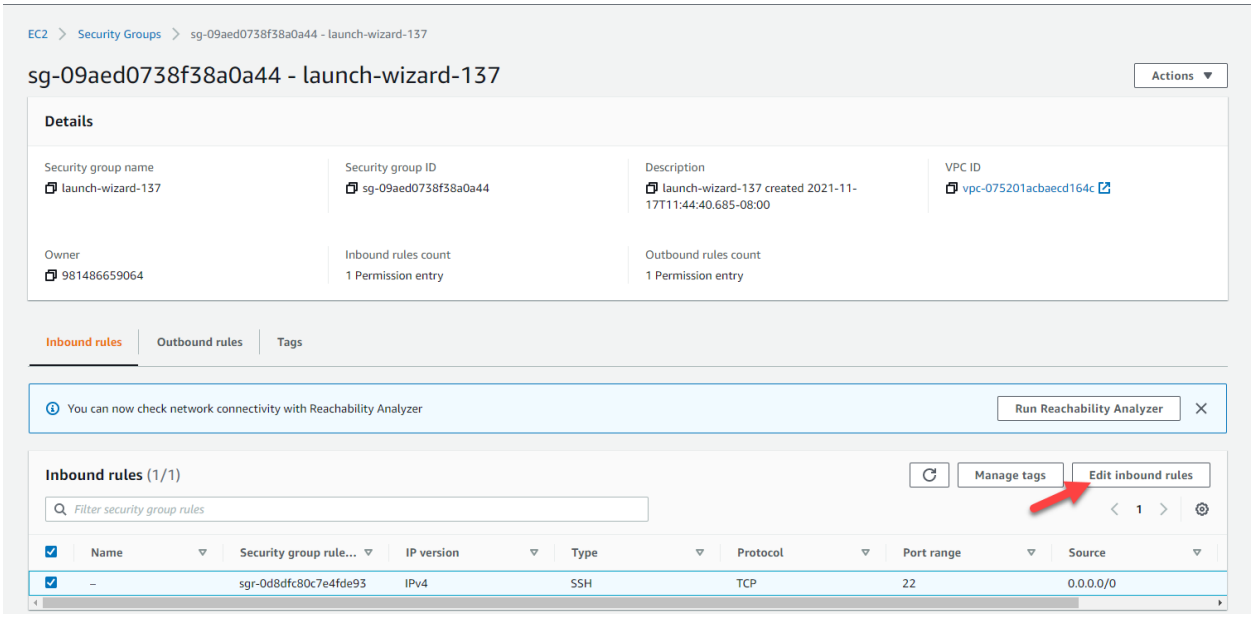
# Firewall Exemption

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.

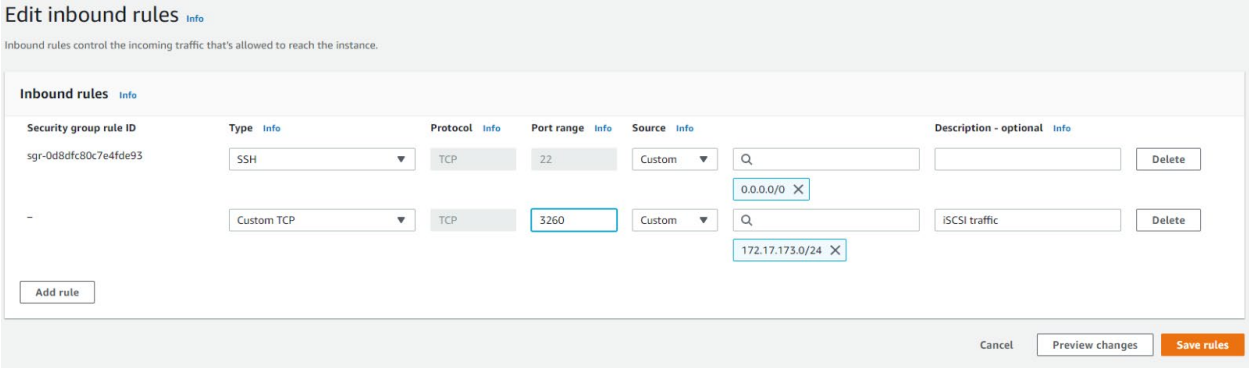
1. On the **Instances** page, select the virtual machine, click the **Security** tab, and then select the security group attached to the instance.




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**:




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

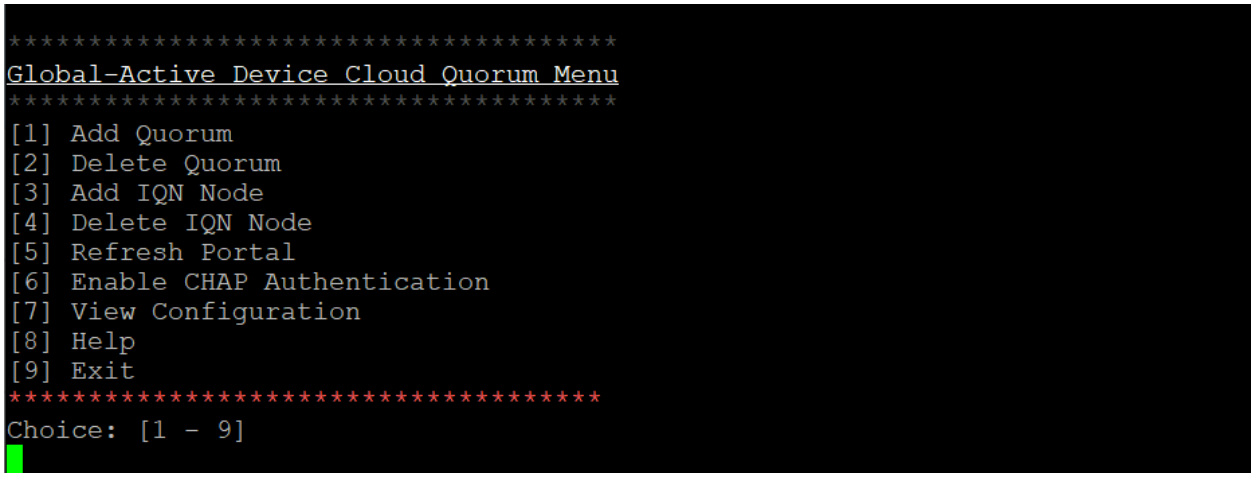
5. Click **Save rules**.

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`



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.

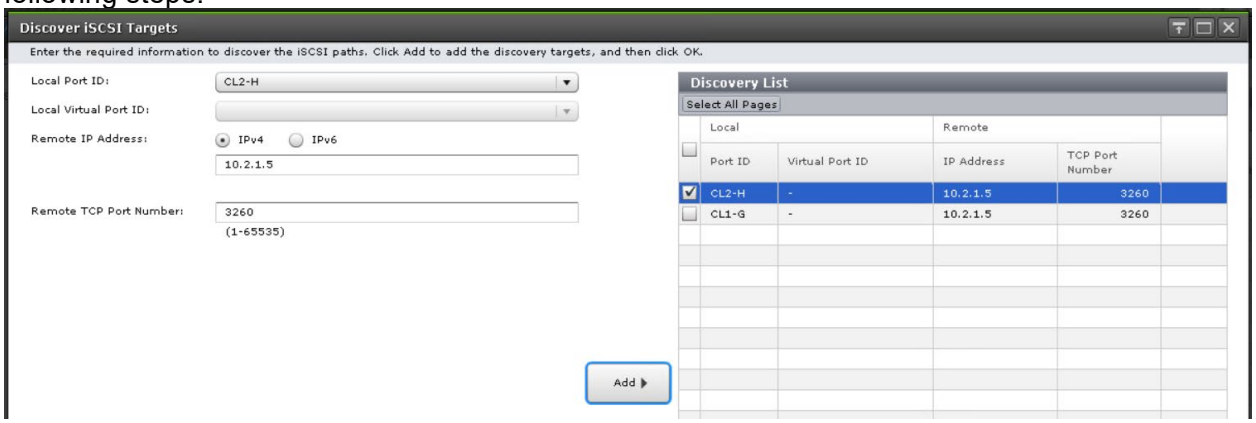
# Global-Active Device Quorums

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

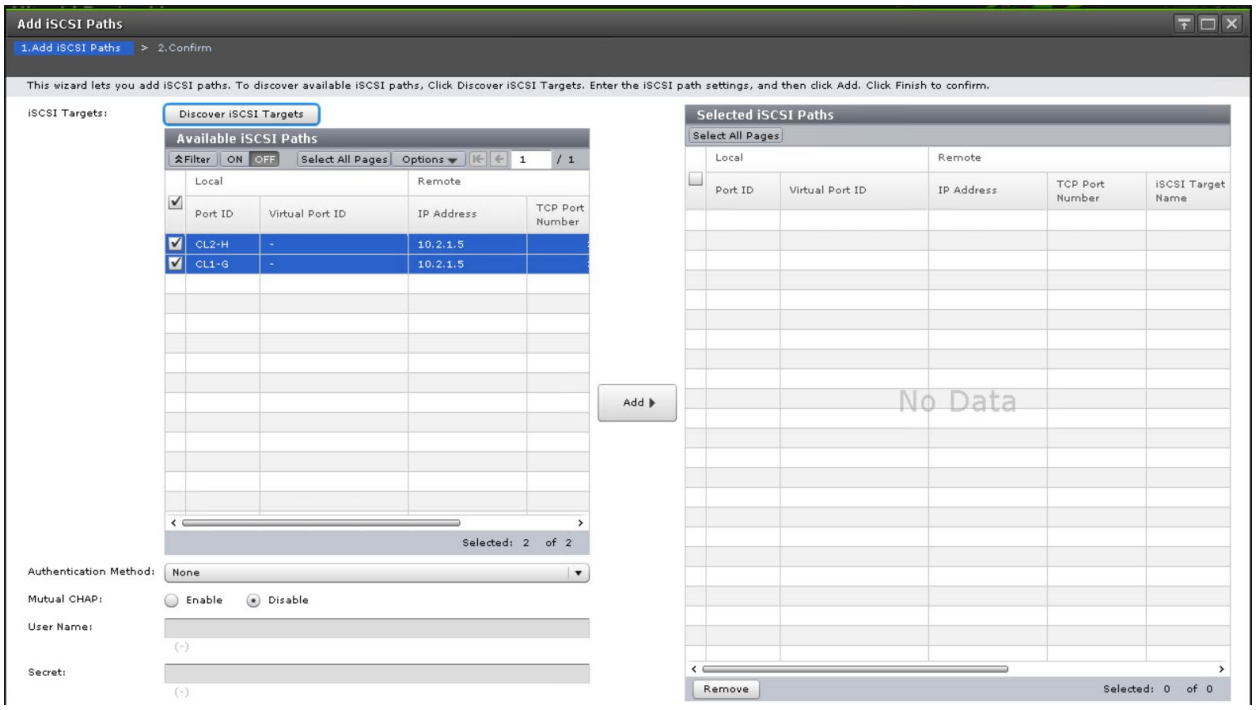
1. Log in to Storage Navigator.
2. On the left side, click **External Storage**, and then click the **iSCSI Paths** tab.


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:



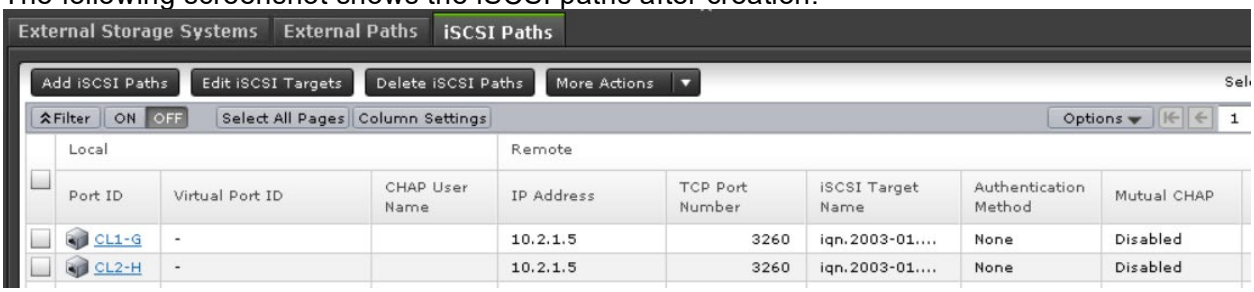

   a. Enter the following:
      - **Local Port ID**: iSCSI port
      - **Remote IP Address**: private IP address of the AWS VM
      - **Remote TCP Port Number**: 3260
   b. Click **Add**.
6. After you finish adding all the required iSCSI ports to the discovery list, click **OK**.

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



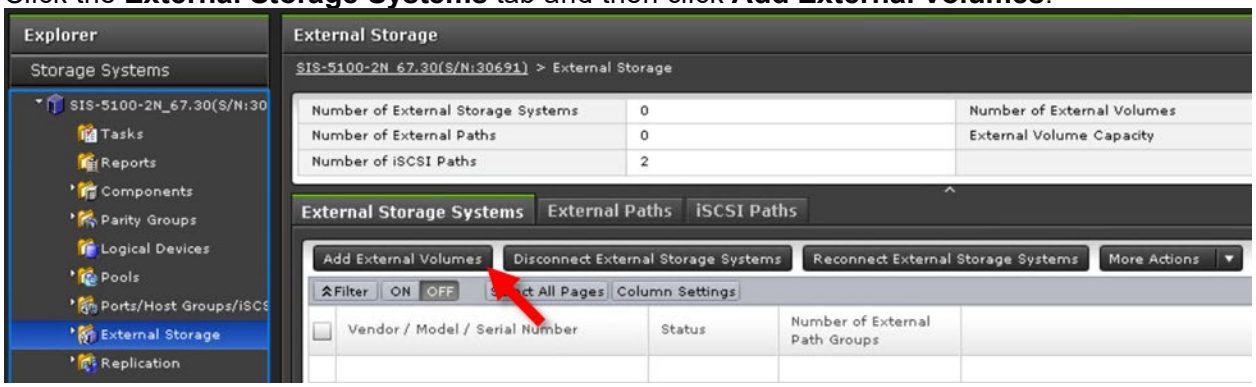

8. Click **Finish** and then click **Apply**.

The following screenshot shows the iSCSI paths after creation:

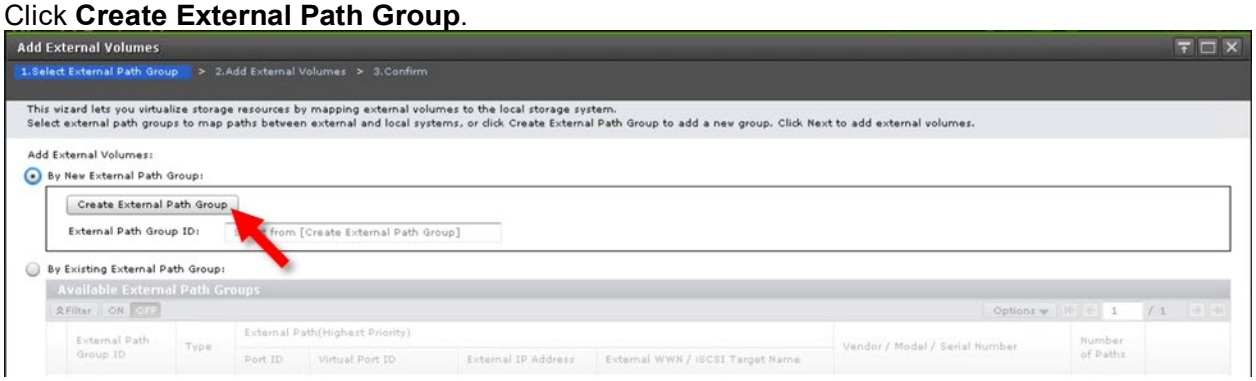


# Discover External Volumes

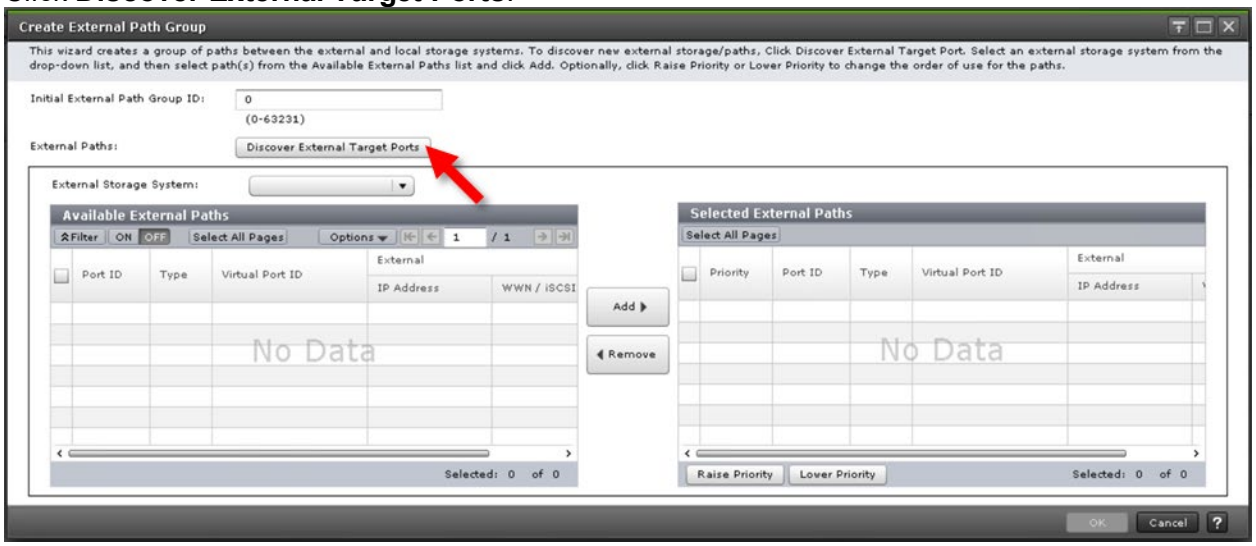
1. Click the **External Storage Systems** tab and then click **Add External Volumes**.



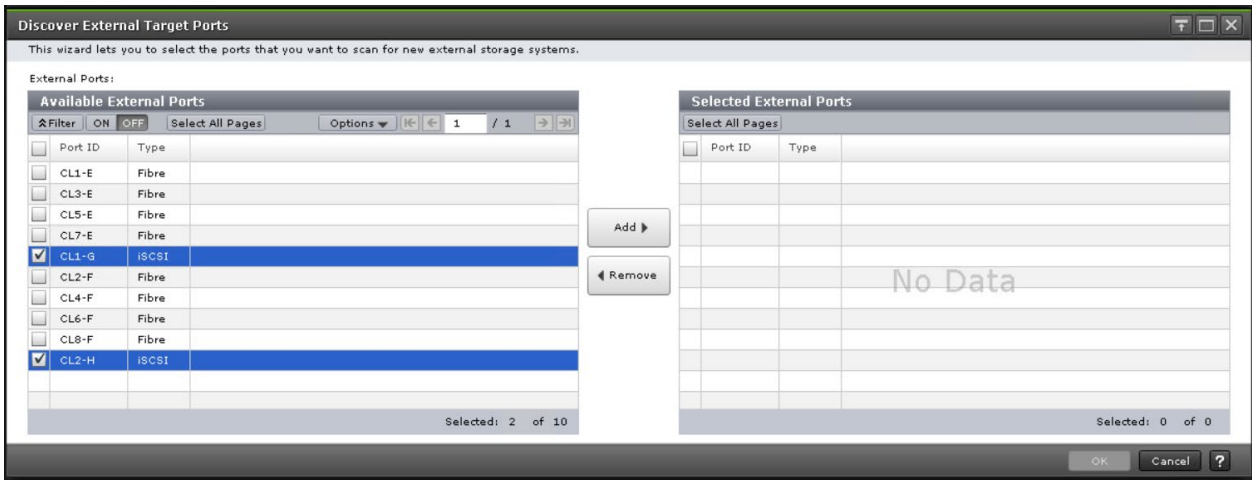

2. Click **Create External Path Group**.




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

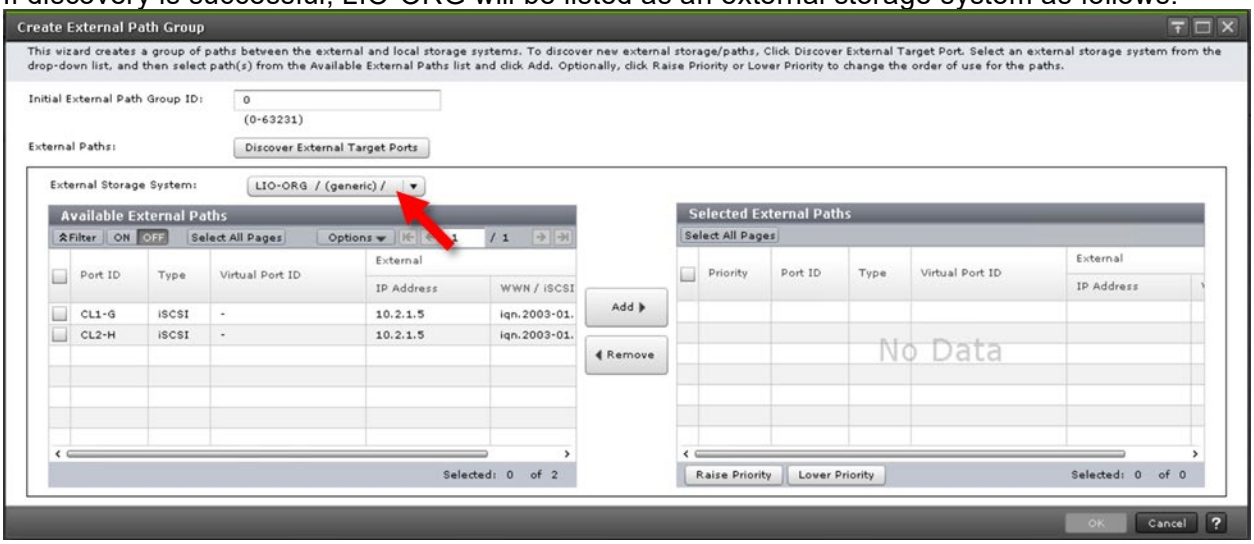


4. Select the iSCSI ports that defined the iSCSI paths in the previous section and then click **Add**.



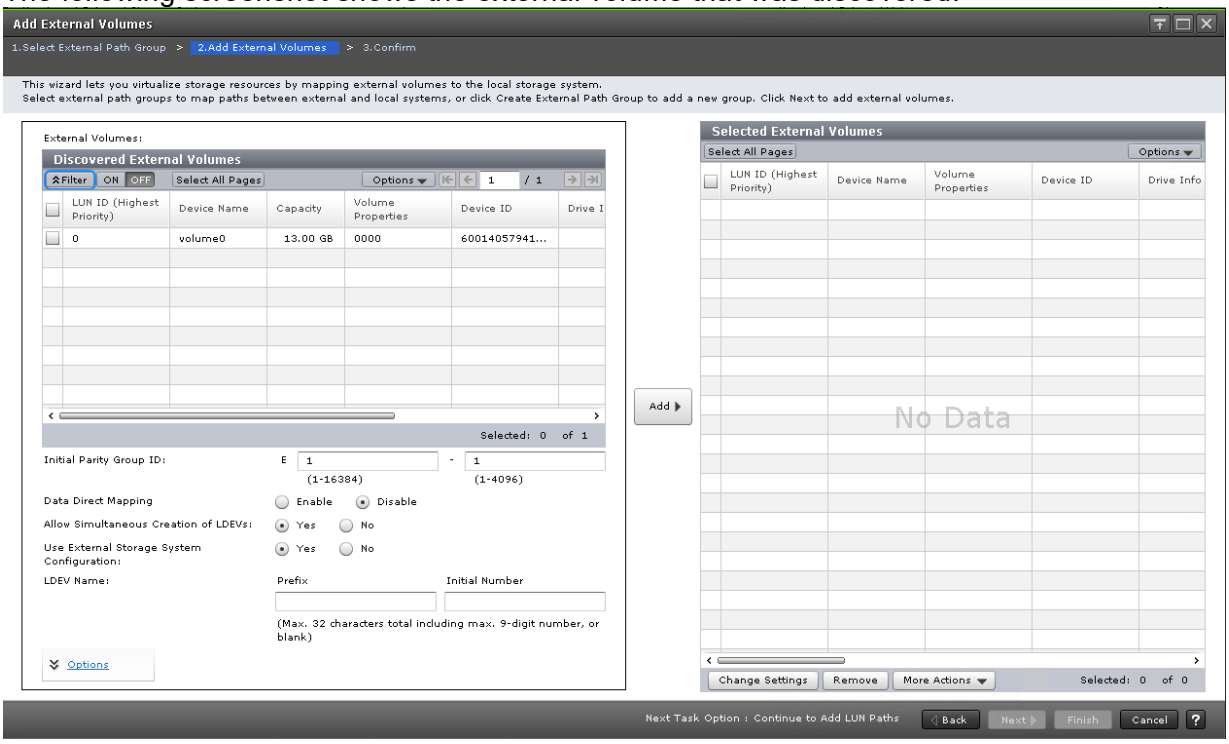

5. Click **OK**.

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.

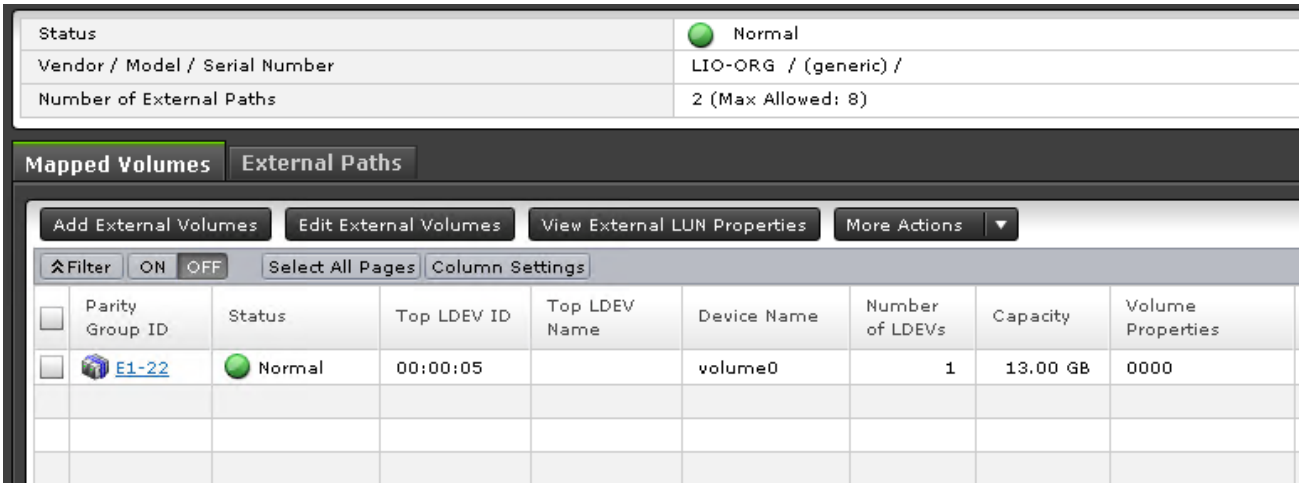



9. Select the discovered volume and then click **Add**.

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

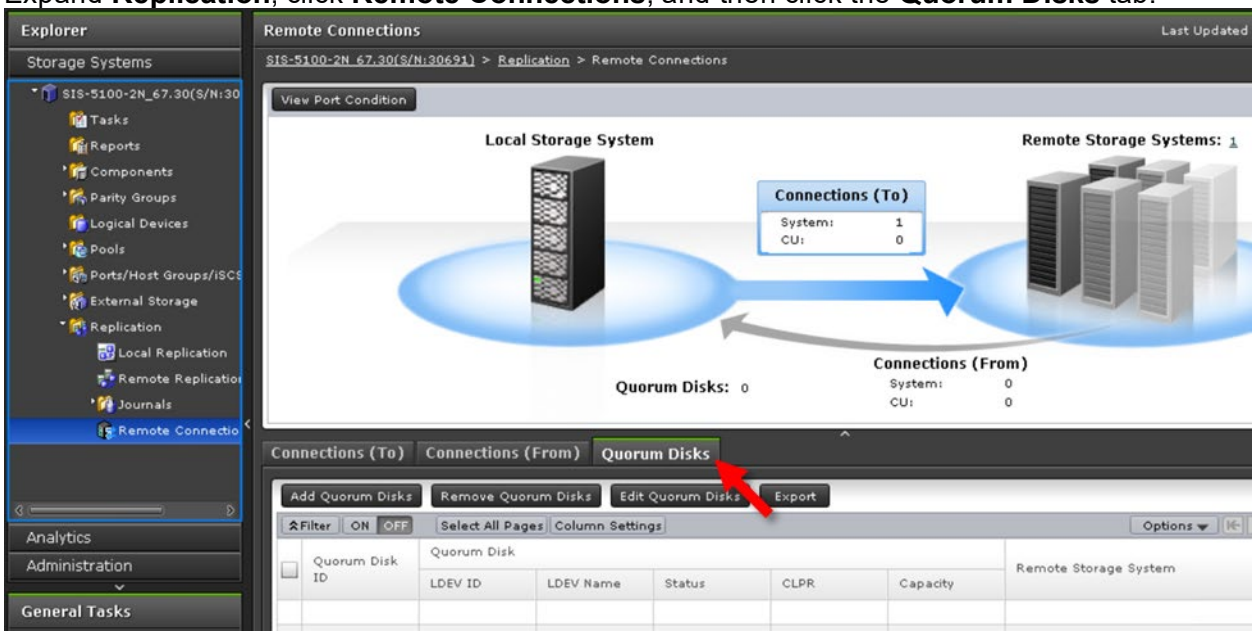
10. Click **Finish** and then click **Apply**.

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.



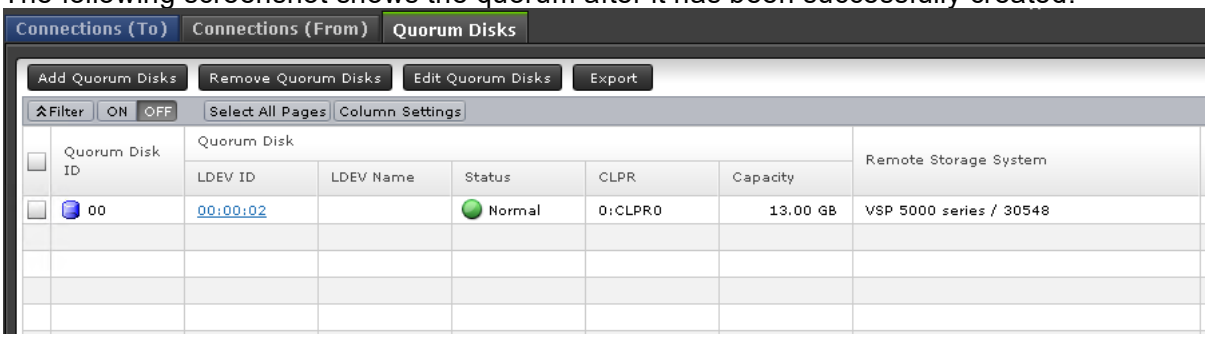

2. Click **Add Quorum Disks**.
3. For each quorum that you are creating, complete the following steps:

    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.



# 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`

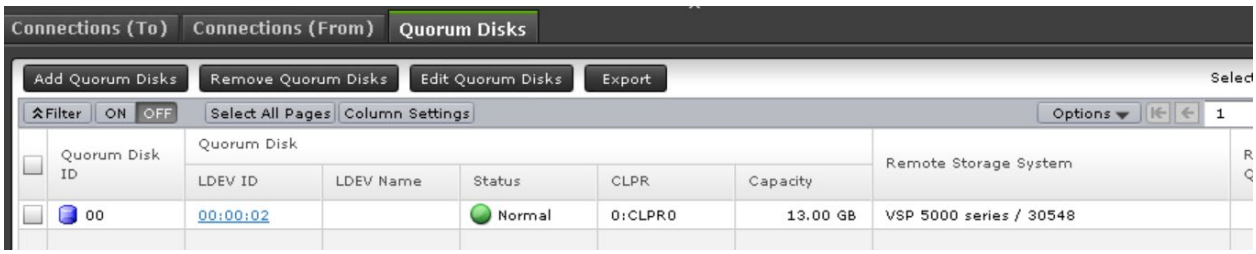
   ```
   [root@sisd51b-04 ~]# raidcom disconnect external_grp -ldev_id 00:00 -IH30
   raidcom: EGRP 1-17(0x1-0x11) will be used for LDEV# 0.
   ```

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
   ```

   **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.

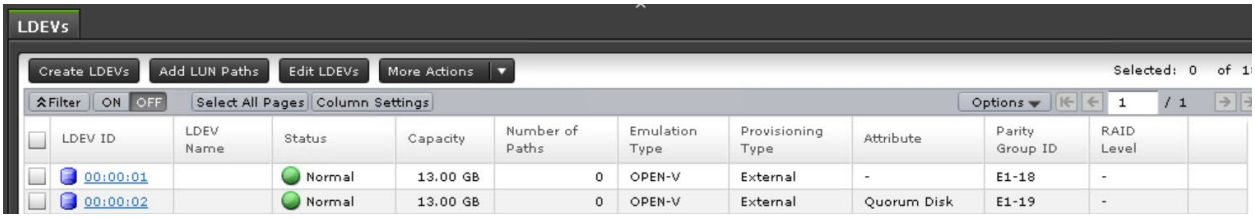
# Clean up

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 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
   ```

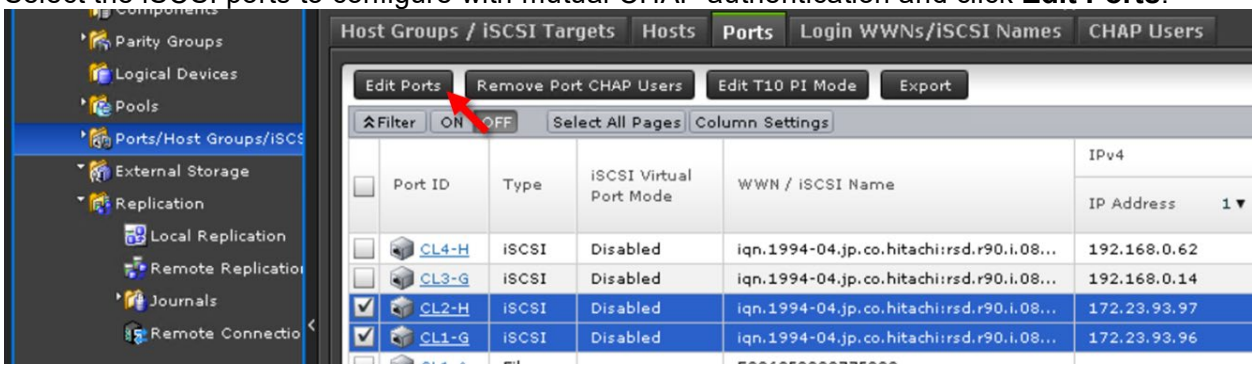
3. Follow the prompts to set credentials.

```
**************************************
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
```

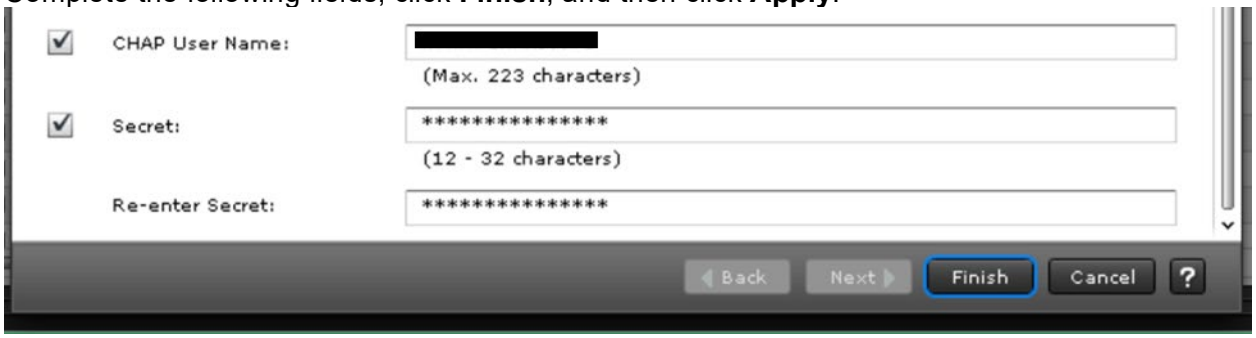
# Enable on iSCSI Ports

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**.



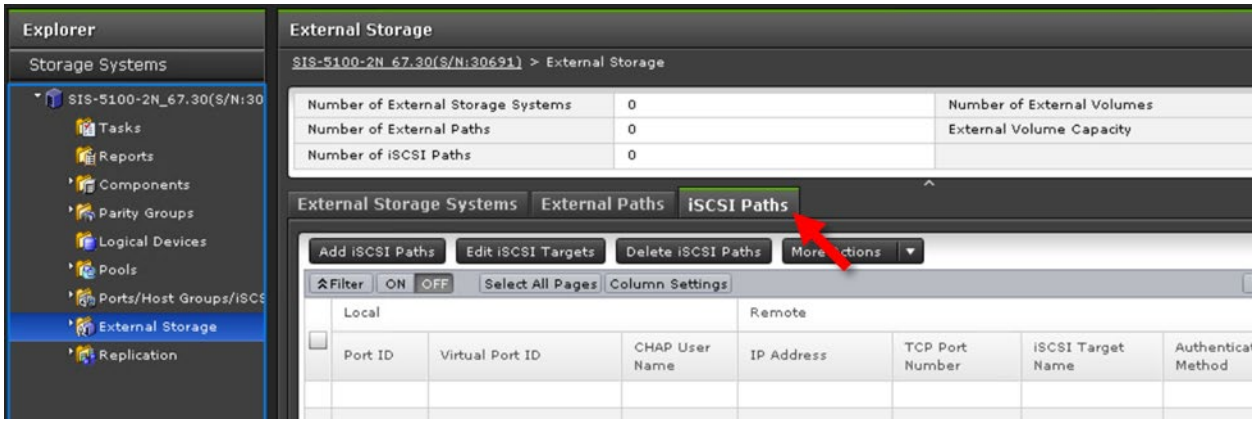

4. Complete the following fields, click **Finish**, and then click **Apply**.




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

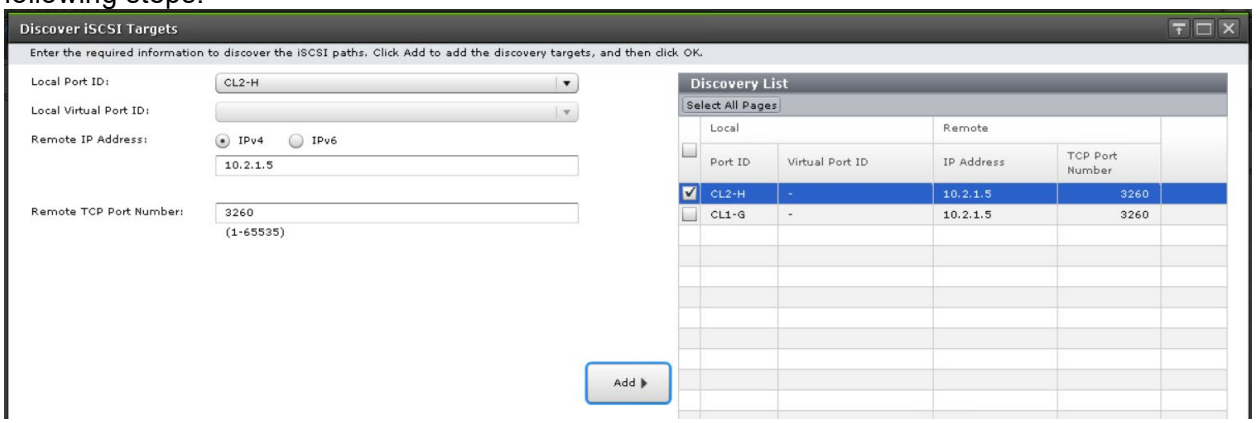
# Create iSCSI Paths

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

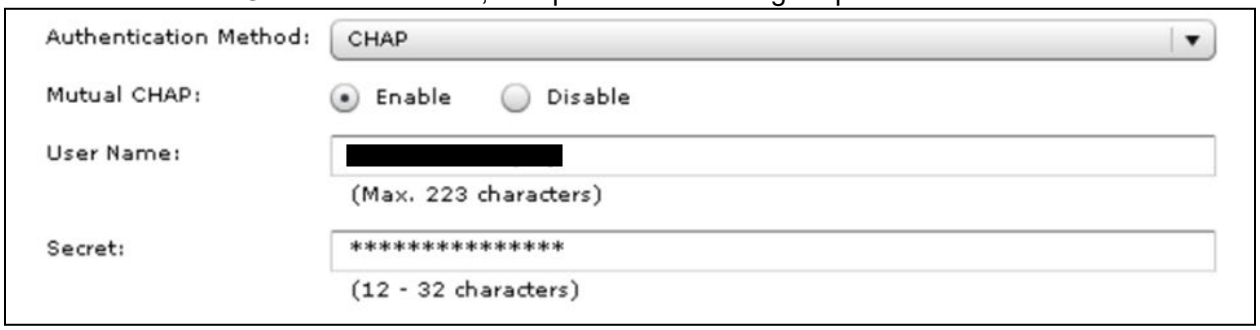



3. Click **Add iSCSI Paths**.
4. Click **Discover iSCSI Targets**.

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

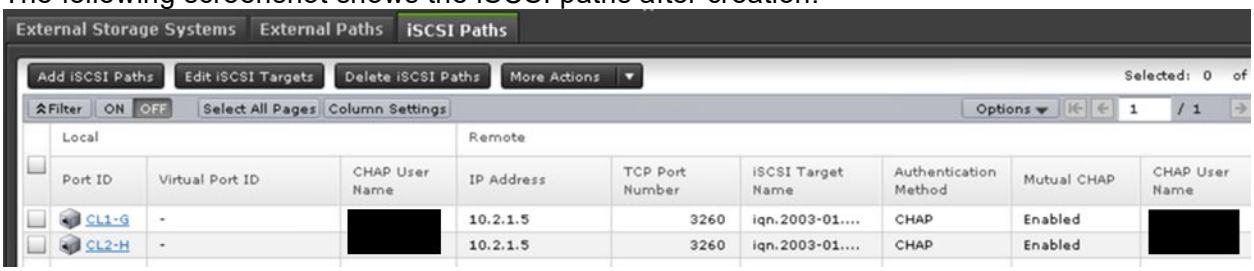



   a. Enter the following:
      - **Local Port ID**: iSCSI port
      - **Remote IP Address**: private IP address of the AWS VM
      - **Remote TCP Port Number**: 3260
   b. Click **Add**.
6. After adding all the required iSCSI ports to the discovery list, click **OK**.
7. Back in the Add iSCSI Paths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




   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:




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