

Global-Active Device Quorum on Azure Cloud

iSCSI Target Using Azure Virtual Machine

Hitachi Vantara

May 2022

Table of Contents

Notices and Disclaimer	2
About This Guide	3
Intended Audience	3
Document Revisions	3
References	3
Comments	3
Configuration and Specifications	4
Introduction	4
VPN Gateway	4
Azure Virtual Machine	5
Azure Virtual Machine	6
Deployment	6
Storage Repository	7
Firewall Exemption	9
Targetcli	10
Auto-start	10
Configuration	10
Global-Active Device Quorums	14
Create iSCSI Paths	14
Discover External Volumes	16
Define GAD Quorums	19
Appendix I: Mutual CHAP Authentication	21
Enable CHAP Authentication in targetcli	21
Enable CHAP Authentication on iSCSI Ports	21
Create iSCSI Paths for CHAP Authentication	22

Notices and Disclaimer

© 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 (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 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.

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, BCPii™ 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 screenshots 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.

Global-Active Device Quorum on Azure Cloud

About This Guide

This guide provides instructions for deploying a virtual machine in the Microsoft Azure cloud and configuring it as an iSCSI target.



After the original publication of this whitepaper, Hitachi Vantara released a virtual machine image on Azure Marketplace that automates the process of configuring targetcli. The solution is available for free on the Azure Marketplace. However, you must pay for various Azure fees relating to running the virtual machine. The solution can be found at https://azuremarketplace.microsoft.com/en-us/marketplace/apps/hitachivantara.hv-gadcloudquorum?ocid=GTMRewards_WhatsNewBlog_hv-gadcloudquorum_031022.

Intended Audience

This document is intended for Hitachi Vantara and Hitachi partner representatives who need a foundation of knowledge on this product to best represent it to potential buyers.

Document Revisions

Revision Number	Date	Details
1.0	April 2021	Initial release.
1.1	May 2022	Added recommendation to remove public IP address on the Azure virtual machine and added GAD Cloud Quorum solution. Also made wording corrections and formatting updates.

References

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

Comments

Please send your comments on this document to gpse.replicationsoftware@hitachivantara.com. Include the document title and number, including the revision level, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara.

Thank You!

Configuration and Specifications

Introduction

This guide provides instructions for deploying a virtual machine on the Microsoft Azure cloud and configuring it as 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 (GAD).



Only use volumes from an iSCSI target virtual machine for global-active device quorums. Do not use them as data volumes.



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](#).

Figure 1 illustrates the test environment. The on-premises datacenter is connected to the Azure cloud using a VPN tunnel. Network traffic is passed between the on-premises storage systems and the iSCSI target virtual machine in Azure using the VPN tunnel.

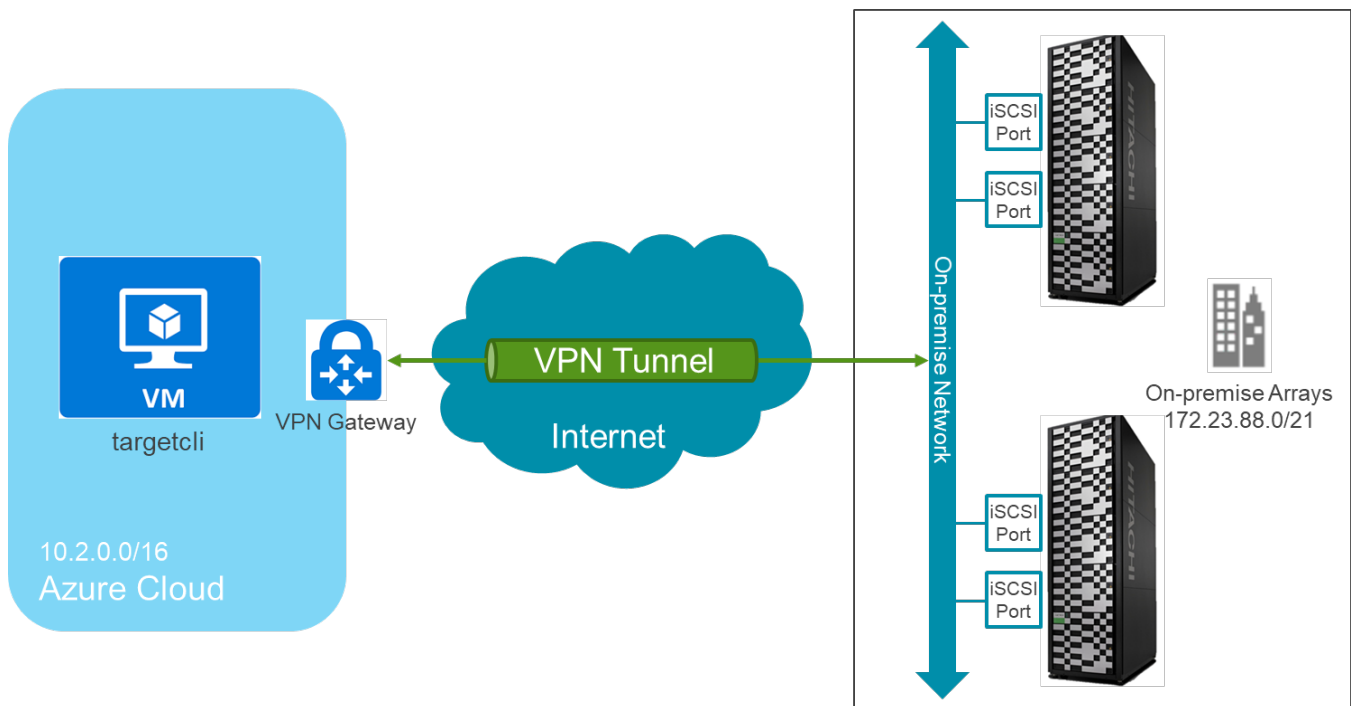


Figure 1. Test Environment

VPN Gateway



While certifying this solution, we determined that the type of the Azure 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 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.

Global-Active Device Quorum on Azure Cloud

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
- 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 that 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, then select **Virtual machines > Add > Virtual machine**.
2. On the Basics page, for image option, select **SUSE Enterprise Linux**.

We recommend that you use **Standard_B2s** or larger for the virtual machine size. This type has 2 virtual CPUs and 4 GiB memory. You can set the remaining options on this page based on your requirements.

3. Click **Next: Disks >**.

On the Disks page, add a data disk for the type of **Premium SSD**. The minimum capacity for a quorum is 12,292 MB; therefore, you must size the data disk based on this requirement. You can set the OS disk type to **Standard HDD**. In our testing, we found this was sufficient in our testing. Click **Next: Networking >**.

Disk options

OS disk type * ⓘ Standard HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type * (Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility ⓘ ☐
 Ultra disk is available only for Availability Zones in centralus.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
0	quorum-1_DataDisk_0	256	Premium SSD LRS	None

4. Click **Next: Networking >**.

On the Networking page, enter values (based on your cloud infrastructure—the process of setting up the infrastructure is not included in this paper) for the following options:

- **Virtual network** (The virtual network must be able to pass traffic to and from the on-premises networks where the storage systems are located.)
- **Subnet**
- **Public IP** (Not required nor recommended.)
- **Configure network security group**

Global-Active Device Quorum on Azure Cloud



A public IP address is not required for the virtual machine to function as an iSCSI target. The virtual machine communicates with the on-premises storage systems using the private IP address, which passes through the VPN tunnel. We recommend that you do not assign a public IP address to improve the solution security.

No additional settings are required on the remaining pages: Management, Advanced, and Tags.

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

Storage Repository

This section provides instructions for configuring a storage repository on the virtual machine to hold the volumes to use as GAD Quorum devices.

1. Log in to the virtual machine using SSH.
2. List all disks and identify the data disk using the size by running the following command:

```
sudo fdisk -l | grep "Disk /dev"
```

" command. The output lists three disks: /dev/sda (30 GiB), /dev/sdc (256 GiB), and /dev/sdb (8 GiB)."/>

```
13.77.209.233 - PuTTY
azureuser@quorum-1:~> sudo fdisk -l | grep "Disk /dev"
Disk /dev/sda: 30 GiB, 32212254720 bytes, 62914560 sectors
Disk /dev/sdc: 256 GiB, 274877906944 bytes, 536870912 sectors
Disk /dev/sdb: 8 GiB, 8589934592 bytes, 16777216 sectors
azureuser@quorum-1:~>
```

3. Create a partition on the data disk by running the following command:

```
sudo fdisk /dev/sdc
```

- a. On the fdisk main menu, enter: **n**
- b. For Partition type, enter: **p**
- c. For Partition number, enter: **1**
- d. To accept default of 2048 for the first sector, press **Enter**.
- e. To accept default of max for the last sector, press **Enter**.

```
azureuser@quorum-1:~> sudo fdisk /dev/sdc
Welcome to fdisk (util-linux 2.33.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x8e8eb131.

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (2048-536870911, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-536870911, default 536870911):

Created a new partition 1 of type 'Linux' and of size 256 GiB.

Command (m for help):
```

Global-Active Device Quorum on Azure Cloud

4. To verify the new partition, enter **p**.

```
Command (m for help): p
Disk /dev/sdc: 256 GiB, 274877906944 bytes, 536870912 sectors
Disk model: Virtual Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0x8e8eb131

Device      Boot Start      End  Sectors  Size Id Type
/dev/sdc1                2048 536870911 536868864 256G 83 Linux

Command (m for help):
```

5. To write changes and close fdisk, enter **w**.

```
Command (m for help): w

The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

azureuser@quorum-1:~>
```

6. Create a volume group on top of the new partition by running the following command:

```
sudo vgcreate vg_quorums /dev/sdc1
```

```
azureuser@quorum-1:~> sudo vgcreate vg_quorums /dev/sdc1
Physical volume "/dev/sdc1" successfully created.
Volume group "vg_quorums" successfully created
azureuser@quorum-1:~>
```

7. Create a logical volume in the new volume group that uses 100% of the capacity by running the following command:

```
sudo lvcreate -l 100%VG vg_quorums
```

```
azureuser@quorum-1:~> sudo lvcreate -l 100%VG vg_quorums
Logical volume "lvol0" created.
azureuser@quorum-1:~>
```

8. Create an XFS file system on top of the new logical volume by running the following command:

```
sudo mkfs.xfs /dev/vg_quorums/lvol0
```

```
azureuser@quorum-1:~> sudo mkfs.xfs /dev/vg_quorums/lvol0
meta-data=/dev/vg_quorums/lvol0 isize=512    agcount=4, agsize=16776960 blks
        =                               sectsz=4096  attr=2, projid32bit=1
        =                               crc=1        finobt=1, sparse=0, rmapbt=0
        =                               reflink=0
data      =                               bsize=4096   blocks=67107840, imaxpct=25
        =                               sunit=0      swidth=0 blks
naming    =version 2                      bsize=4096   ascii-ci=0, ftype=1
log       =internal log                   bsize=4096   blocks=32767, version=2
        =                               sectsz=4096  sunit=1 blks, lazy-count=1
realtime  =none                           extsz=4096   blocks=0, rtextents=0
azureuser@quorum-1:~>
```

Global-Active Device Quorum on Azure Cloud

9. Create a mount point for the new filesystem by running the following command:

```
sudo mkdir /quorums
```

10. To mount file system automatically during a restart, add the following line in the `/etc/fstab` file:

```
sudo sh -c "echo /dev/vg_quorums/lvol0 /quorums xfs defaults 0 0 >> /etc/fstab"
```

11. Verify that the entry was added correctly by running the following command:

```
sudo cat /etc/fstab
```

```
azureuser@quorum-1:~> sudo cat /etc/fstab
UUID=0eb96096-0cc7-4c16-b15e-8c8777b4f487 / xfs defaults 0 0
UUID=64df4613-87a7-4c51-9cc8-e3ee144a6d2a /boot xfs defaults 0 0
UUID=50BD-2DD9 /boot/efi vfat defaults 0 0
/dev/disk/cloud/azure_resource-part1 /mnt auto defaults,nofail,x-systemd.requires=cloud-init.service,comment=cloudconfig 0 2
/dev/vg_quorums/lvol0 /quorums xfs defaults 0 0
azureuser@quorum-1:~>
```

12. Mount the filesystem by running the following command:

```
sudo mount /quorums; df -h
```

```
azureuser@quorum-1:~> sudo mount /quorums; df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                   2.0G    8.0K    2.0G   1% /dev
tmpfs                      2.0G         0    2.0G   0% /dev/shm
tmpfs                      2.0G    17M    2.0G   1% /run
tmpfs                      2.0G         0    2.0G   0% /sys/fs/cgroup
/dev/sda4                   29G     1.7G    27G   6% /
/dev/sda3                 1014M     92M   923M  10% /boot
/dev/sda2                   512M     3.7M   509M   1% /boot/efi
/dev/sdb1                   7.9G     36M    7.4G   1% /mnt
tmpfs                      393M         0   393M   0% /run/user/1000
/dev/mapper/vg_quorums-lvol0 256G    294M   256G   1% /quorums
azureuser@quorum-1:~>
```

Firewall Exemption

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

1. On the landing page of Azure Portal, use the top-left shortcut to expand the portal menu, select **Virtual machines**, and then select the newly created virtual machine.
2. On the left, under **Settings**, select **Networking > Add inbound port rule**.

Note: Outbound rule is not required.

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

- **Source:** IP addresses
- **Source IP addresses/CIDR ranges:** Subnets of the on-premises storage system iSCSI ports
- **Source port ranges:** * (asterisk)
- **Destination:** IP addresses
- **Destination IP addresses/CIDR ranges:** Private IP address of the virtual machine
- **Service:** custom
- **Destination port ranges:** 3260
- **Protocol:** TCP

Targetcli

The targetcli application is installed by default with Azure SUSE Enterprise Linux 15 SP1. So, there are no additional steps required before using it.

Auto-start

1. Start targetcli and configure it to start automatically after a restart by running the following command:

```
sudo systemctl enable --now targetcli
```

2. Verify that targetcli started successfully by running the following command:

```
sudo systemctl status targetcli
```

```
azureuser@quorum-1:~> sudo systemctl status targetcli
● targetcli.service - "Generic Target-Mode Service (fb)"
   Loaded: loaded (/usr/lib/systemd/system/targetcli.service; enabled; vendor p>
   Active: active (exited) since Tue 2021-03-23 01:38:15 UTC; 34s ago
   Process: 32410 ExecStart=/usr/bin/targetcli restoreconfig $CONFIG_FILE (code=>
  Main PID: 32410 (code=exited, status=0/SUCCESS)
     Tasks: 0
    CGroup: /system.slice/targetcli.service

Mar 23 01:38:13 quorum-1 systemd[1]: Starting "Generic Target-Mode Service (fb)">
Mar 23 01:38:14 quorum-1 targetcli[32410]: Warning: Could not load preferences >
Mar 23 01:38:15 quorum-1 targetcli[32410]: Restore file /etc/target/saveconfig.>
Mar 23 01:38:15 quorum-1 systemd[1]: Started "Generic Target-Mode Service (fb)".
lines 1-12/12 (END)
```

Configuration

This section provides instructions for configuring targetcli to present three 13 GB volumes over iSCSI.



These instructions are for a configuration without authentication. Refer to [Appendix I: Mutual CHAP Authentication](#) if you want to configure CHAP authentication.

1. Log in to targetcli by running the following command:

```
sudo targetcli
```

```
azureuser@quorum-1:~> sudo targetcli
targetcli shell version 2.1.52
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/>
```

2. Create three 13 GB volumes in the /quorums folder by running the following command (change the number after "volume" as you proceed):

```
/backstores/fileio create volume0 /quorums/volume0 13g
```

```
/> backstores/fileio create volume0 /quorums/volume0 13g
Created fileio volume0 with size 13958643712
/> backstores/fileio create volume1 /quorums/volume1 13g
Created fileio volume1 with size 13958643712
/> backstores/fileio create volume2 /quorums/volume2 13g
Created fileio volume2 with size 13958643712
/>
```

Global-Active Device Quorum on Azure Cloud

3. Verify that the volumes were created successfully by running the following command:

```
ls /backstores/fileio
```

```
> ls /backstores/fileio/
o- fileio ..... [Storage Objects: 3]
  o- volume0 ..... [/quorums/volume0 (13.0GiB) write-back activated]
    | o- alua ..... [ALUA Groups: 1]
      | o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
  o- volume1 ..... [/quorums/volume1 (13.0GiB) write-back activated]
    | o- alua ..... [ALUA Groups: 1]
      | o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
  o- volume2 ..... [/quorums/volume2 (13.0GiB) write-back activated]
    | o- alua ..... [ALUA Groups: 1]
      | o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
/>
```

4. Create an iSCSI target by running the following command:

```
/iscsi create
```

```
> /iscsi create
Created target iqn.2003-01.org.linux-iscsi.quorum-1.x8664:sn.e5d4db916f12.
Created TPG 1.
Global pref auto_add_default_portal=true
Created default portal listening on all IPs (0.0.0.0), port 3260.
/>
```

5. Remove the default listening portal and create a new one specific to the virtual machine private IP address as follows:

- a. Enter the portal directory by running the following command (your target will be different):

```
cd /iscsi/iqn.2003-01.org.linux-iscsi.quorum-1.x8664:sn.e5d4db916f12/tpg1/portals/
```

- b. Delete the default portal by running the following command:

```
delete 0.0.0.0 3260
```

- c. Create a new portal specific to the virtual machine private IP address by running the following command:

```
create 10.2.1.5 3260
```

- d. Verify that the new portal was created successfully by running the following command:

```
ls
```

```
o- portals ..... [Portals: 1]
  o- 10.2.1.5:3260 ..... [OK]
/iscsi/iqn.20.../tpg1/portals>
```

6. Map the three volumes:

- a. Enter the LUNs directory by running the following command:

```
cd /iscsi/iqn.2003-01.org.linux-iscsi.quorum-1.x8664:sn.e5d4db916f12/tpg1/luns
```

- b. Map the volumes by running the following command (change the number after "volume" as you proceed):

```
create /backstores/fileio/volume0
```

- c. Verify that the volumes were mapped successfully by running the following command:

Global-Active Device Quorum on Azure Cloud

```
ls
```

```
/iscsi/iqn.20...f12/tpg1/luns> ls
o- luns ..... [LUNs: 3]
  o- lun0 ..... [fileio/volume0 (/quorums/volume0) (default_tg_pt_gp)]
  o- lun1 ..... [fileio/volume1 (/quorums/volume1) (default_tg_pt_gp)]
  o- lun2 ..... [fileio/volume2 (/quorums/volume2) (default_tg_pt_gp)]
/iscsi/iqn.20...f12/tpg1/luns>
```

7. Mask the initiator IQNs of the storage systems to allow access to the LUNs:

- a. Enter the ACLs directory by running the following command:

```
cd /iscsi/iqn.2003-01.org.linux-iscsi.quorum-1.x8664:sn.e5d4db916f12/tpg1/acls
```

- b. Mask each IQN by running the following command (your IQNs will be different):

```
create iqn.1994-04.jp.co.hitachi:rsd.r90.i.0877e3.1g
```

- c. Verify that the masking was successful by running the following command:

```
ls
```

```
/iscsi/iqn.20...f12/tpg1/acls> ls
o- acls ..... [ACLs: 4]
  o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.087754.1g ..... [Mapped LUNs: 3]
    | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
  o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.087754.2h ..... [Mapped LUNs: 3]
    | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
  o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.0877e3.1g ..... [Mapped LUNs: 3]
    | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
  o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.0877e3.2h ..... [Mapped LUNs: 3]
    | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
/iscsi/iqn.20...f12/tpg1/acls>
```

8. Save the changes by running the following commands:

```
cd /
```

```
saveconfig
```

Global-Active Device Quorum on Azure Cloud

9. View the configuration by running the following command:

```
ls
```

```

/> ls
o- / ..... [....]
  o- backstores ..... [....]
    | o- block ..... [Storage Objects: 0]
    | o- fileio ..... [Storage Objects: 3]
    |   | o- volume0 ..... [/quorums/volume0 (13.0GiB) write-back activated]
    |   |   | o- alua ..... [ALUA Groups: 1]
    |   |   |   | o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
    |   |   | o- volume1 ..... [/quorums/volume1 (13.0GiB) write-back activated]
    |   |   |   | o- alua ..... [ALUA Groups: 1]
    |   |   |   |   | o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
    |   | o- volume2 ..... [/quorums/volume2 (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.quorum-1.x8664:sn.e5d4db916f12 .... [TPGs: 1]
    |   | o- tpg1 ..... [no-gen-acls, no-auth]
    |   |   | o- acls ..... [ACLs: 4]
    |   |   |   | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.087754.1g .... [Mapped LUNs: 3]
    |   |   |   |   | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |   |   |   |   | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    |   |   |   |   | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
    |   |   |   | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.087754.2h .... [Mapped LUNs: 3]
    |   |   |   |   | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |   |   |   |   | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    |   |   |   |   | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
    |   |   |   | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.0877e3.1g .... [Mapped LUNs: 3]
    |   |   |   |   | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |   |   |   |   | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    |   |   |   |   | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
    |   |   |   | o- iqn.1994-04.jp.co.hitachi:rsd.r90.i.0877e3.2h .... [Mapped LUNs: 3]
    |   |   |   |   | o- mapped_lun0 ..... [lun0 fileio/volume0 (rw)]
    |   |   |   |   | o- mapped_lun1 ..... [lun1 fileio/volume1 (rw)]
    |   |   |   |   | o- mapped_lun2 ..... [lun2 fileio/volume2 (rw)]
    |   |   | o- luns ..... [LUNs: 3]
    |   |   |   | o- lun0 ..... [fileio/volume0 (/quorums/volume0) (default_tg_pt_gp)]
    |   |   |   | o- lun1 ..... [fileio/volume1 (/quorums/volume1) (default_tg_pt_gp)]
    |   |   |   | o- lun2 ..... [fileio/volume2 (/quorums/volume2) (default_tg_pt_gp)]
    |   |   | o- portals ..... [Portals: 1]
    |   |   |   | o- 10.2.1.5:3260 ..... [OK]
  o- loopback ..... [Targets: 0]
  o- vhost ..... [Targets: 0]
  o- xen-pvscsi ..... [Targets: 0]

```

10. Exit targetcli by running the following command:

```
exit
```

Global-Active Device Quorum on Azure Cloud

Global-Active Device Quorums

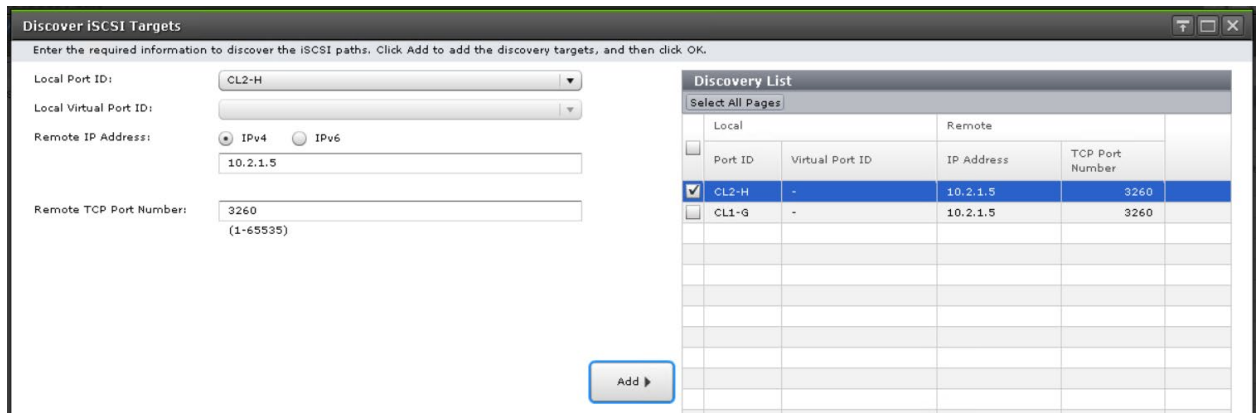
This section describes how to discover volumes from the iSCSI target virtual machine and turn them into GAD quorums. The procedure is the same as it is to virtualize a physical Fibre Channel or iSCSI storage system.

Create iSCSI Paths

1. Log in to Storage Navigator.
2. On the left side, select **External Storage**, and then select 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 virtual machine, complete the following steps:
 - a. Enter the following:
 - **Local Port ID:** Local iSCSI storage port
 - **Remote IP Address:** Private IP address of the Azure virtual machine.
 - **Remote TCP Port Number:** 3260
 - b. Click **Add**.



6. After you finish adding all the required iSCSI ports to the discovery list, click **OK**.

Global-Active Device Quorum on Azure Cloud

7. 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.

iSCSI Targets:

Discover iSCSI Targets

Available iSCSI Paths

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

Selected: 2 of 2

Authentication Method: **None**

Mutual CHAP: ☐ Enable ☒ Disable

User Name: (-)

Secret: (-)

Selected iSCSI Paths

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

Remove

Selected: 0 of 0



If you want to configure CHAP authentication, see: [Appendix I: Mutual CHAP Authentication](#).

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

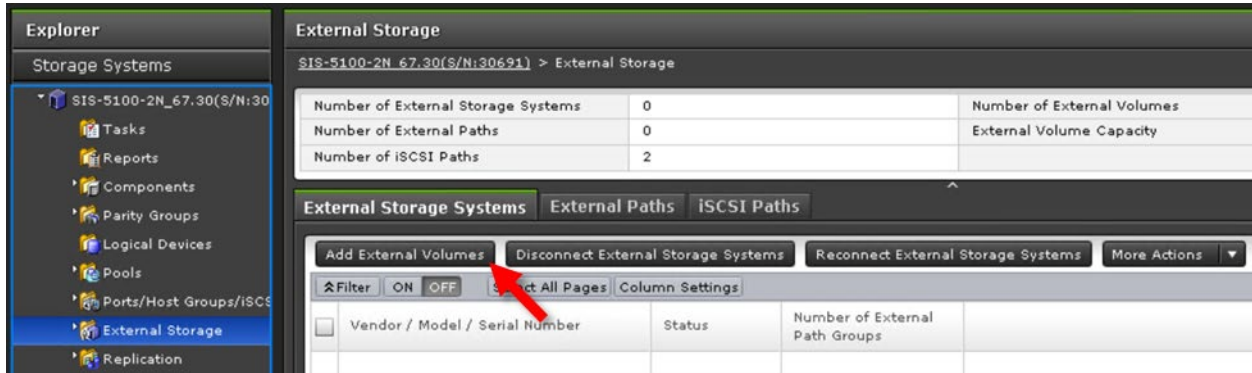
The following screenshot shows the iSCSI paths after they are created:

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

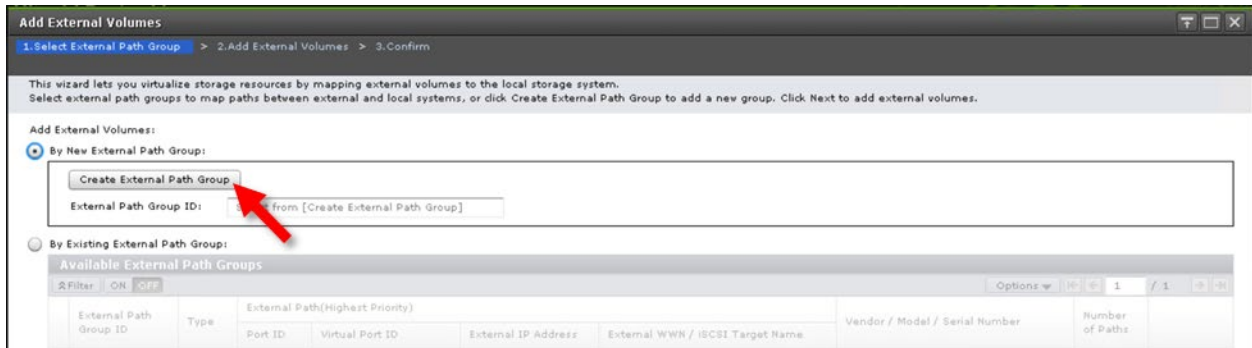
Global-Active Device Quorum on Azure Cloud

Discover External Volumes

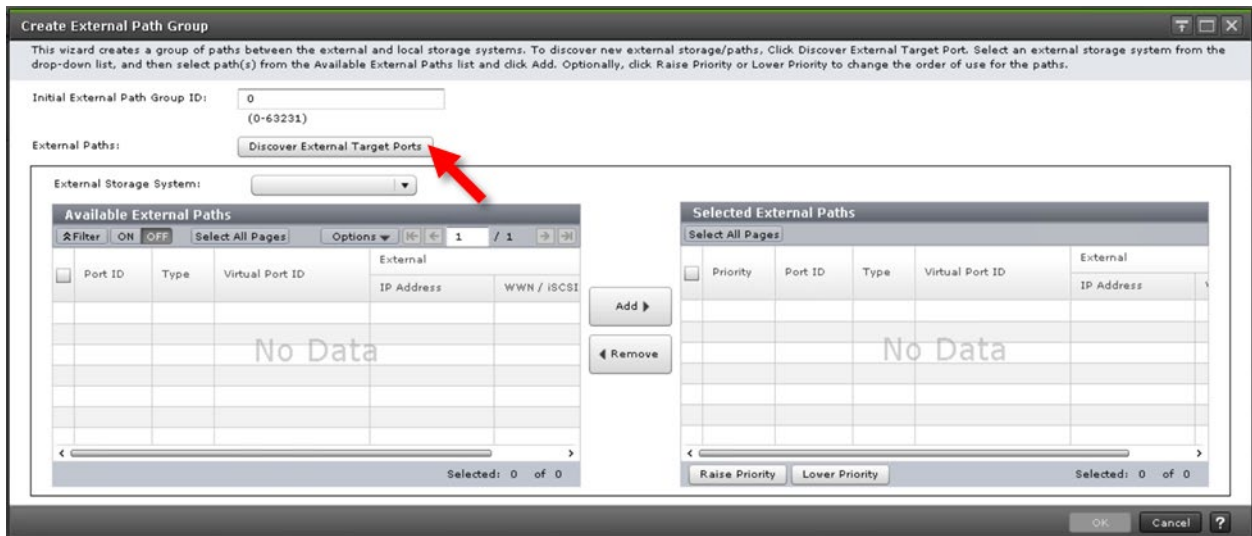
1. Select the **External Storage Systems** tab and then click **Add External Volumes**.



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



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



Global-Active Device Quorum on Azure Cloud

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

Discover External Target Ports

This wizard lets you to select the ports that you want to scan for new external storage systems.

External Ports:

Available External Ports	
Port ID	Type
☐ CL1-E	Fibre
☐ CL3-E	Fibre
☐ CL5-E	Fibre
☐ CL7-E	Fibre
☒ CL1-G	iSCSI
☐ CL2-F	Fibre
☐ CL4-F	Fibre
☐ CL6-F	Fibre
☐ CL8-F	Fibre
☒ CL2-H	iSCSI

Selected: 2 of 10

Buttons: Add, Remove

Selected External Ports	
Port ID	Type
No Data	

Selected: 0 of 0

Buttons: OK, Cancel, ?

- Click **OK**.

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

Create External Path Group

This wizard creates a group of paths between the external and local storage systems. To discover new external storage/paths, Click Discover External Target Port. Select an external storage system from the drop-down list, and then select path(s) from the Available External Paths list and click Add. Optionally, click Raise Priority or Lower Priority to change the order of use for the paths.

Initial External Path Group ID: 0 (0-63231)

External Paths: Discover External Target Ports

External Storage System: LIO-ORG / (generic) /

Available External Paths				
Port ID	Type	Virtual Port ID	External	
			IP Address	WWN / iSCSI
☐ CL1-G	iSCSI	-	10.2.1.5	iqn.2003-01.
☐ CL2-H	iSCSI	-	10.2.1.5	iqn.2003-01.

Selected: 0 of 2

Buttons: Add, Remove

Selected External Paths				
Priority	Port ID	Type	Virtual Port ID	External IP Address
No Data				

Buttons: Raise Priority, Lower Priority

Selected: 0 of 0

Buttons: OK, Cancel, ?

- Select the discovered external paths and click **Add**.
- Click **OK**.
- On the Add External Volumes screen, click **Next**.

Global-Active Device Quorum on Azure Cloud

The following screenshot shows three external volumes were discovered:

Add External Volumes

1. Select External Path Group > **2. Add External Volumes** > 3. Confirm

This wizard lets you virtualize storage resources by mapping external volumes to the local storage system. Select external path groups to map paths between external and local systems, or click Create External Path Group to add a new group. Click Next to add external volumes.

External Volumes:

Discovered External Volumes

LUN ID (Highest Priority)	Device Name	Capacity	Volume Properties	Device ID
0	volume0	13.00 GB	0000	6001405019F...
1	volume1	13.00 GB	0001	600140554DE...
2	volume2	13.00 GB	0002	6001405A73E...

Selected: 3 of 3

Initial Parity Group ID: E 1 (1-16384) - 1 (1-4096)

Data Direct Mapping: ☐ Enable ☒ Disable

Allow Simultaneous Creation of LDEVs: ☒ Yes ☐ No

Use External Storage System Configuration: ☒ Yes ☐ No

LDEV Name: Prefix Initial Number (Max. 32 characters total including max. 9-digit number, or blank)

Initial LDEV ID: LDKC CU DEV Interval View LDEV IDs

Initial SSID: 0004 (0004-FFFE) View SSIDs

Base Emulation Type: Depends on the selected external volume(s)

Selected External Volumes

LUN ID (Highest Priority)	Device Name	Volume Properties	Device ID	Drive Info
No Data				

Add

Change Settings Remove More Actions Selected: 0 of 0

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

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

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

Explorer

Storage Systems

- SIS-5100-2N_67.30(S/N:30691)
 - Tasks
 - Reports
 - Components
 - Parity Groups
 - Logical Devices
 - Pools
 - Ports/Host Groups/ISCS
 - External Storage
 - LIO-ORG / (generic)
 - EPathGroup0**
 - Replication

EPathGroup0 Last Updated : 2021/03/24 02:15

SIS-5100-2N_67.30(S/N:30691) > External Storage > LIO-ORG / (generic) / EPathGroup0

Status: Normal

Vendor / Model / Serial Number: LIO-ORG / (generic) /

Number of External Volumes: 3

External Volume Capacity: 39.00 GB

Number of External Paths: 2 (Max Allowed: 8)

Mapped Volumes External Paths

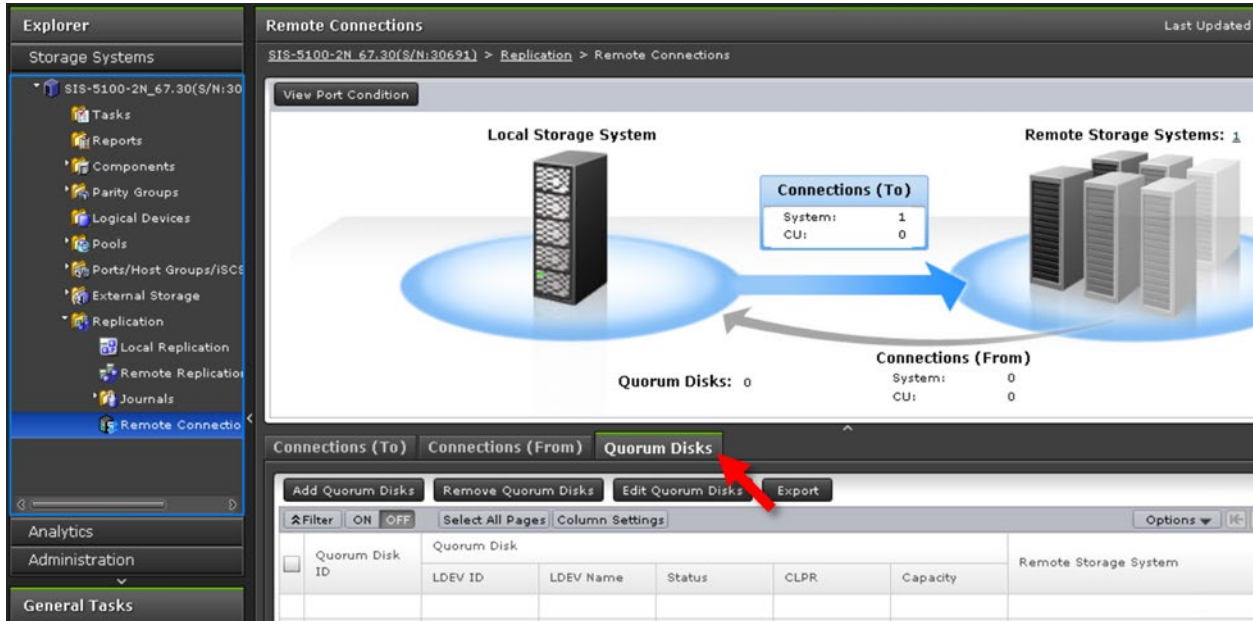
Add External Volumes Edit External Volumes View External LUN Properties More Actions Selected: 0 of 3

Parity Group ID	Status	Top LDEV ID	Top LDEV Name	Device Name	Number of LDEVs	Capacity	Volume Properties	Device ID	MP Unit ID	Path Mode
E1-1	Normal	00:FD:00		volume0	1	13.00 GB	0000	6001405019F...	MPU-010	ALLUA
E1-2	Normal	00:FD:01		volume1	1	13.00 GB	0001	600140554DE...	MPU-120	ALLUA
E1-3	Normal	00:FD:02		volume2	1	13.00 GB	0002	6001405A73E...	MPU-010	ALLUA

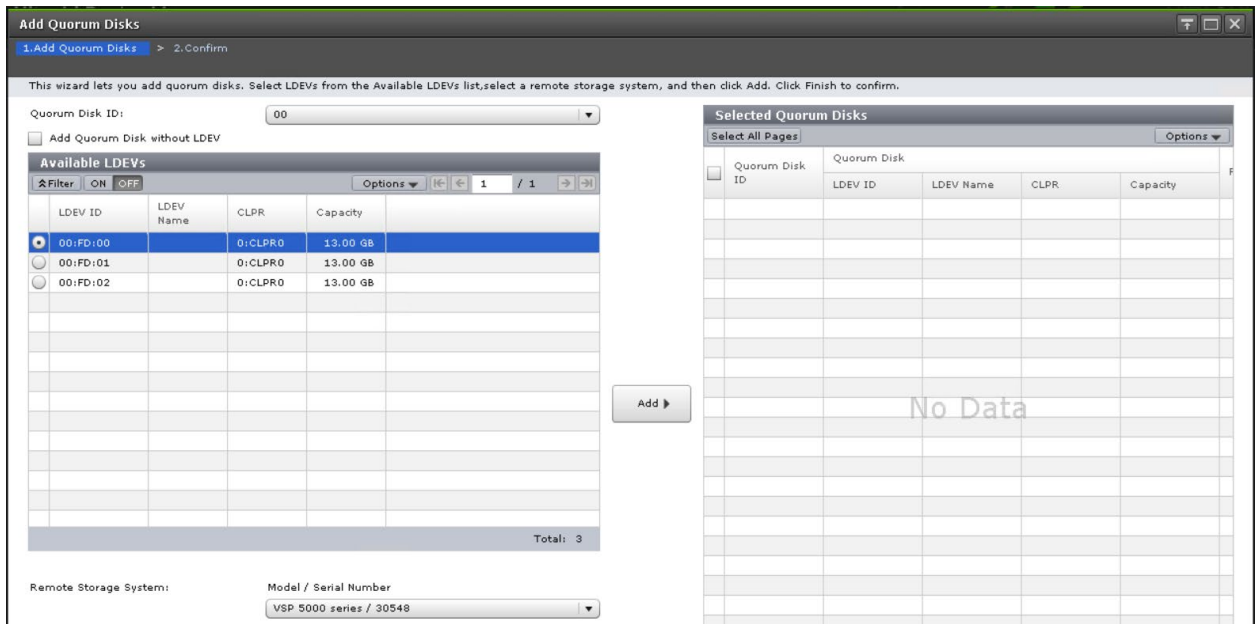
Global-Active Device Quorum on Azure Cloud

Define GAD Quorums

1. Expand **Replication**, select **Remote Connections** and then select 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 dropdown list.
 - Available LDEVs:** External volume (from the previous section) to use as a quorum.
 - Remote Storage System:** Remote storage system to pair with the new quorum.
 - b. Click **Add**.



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

Global-Active Device Quorum on Azure Cloud

The following screenshot shows the quorums after they have 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	Quorum Disk					Remote Storage System
		LDEV ID	LDEV Name	Status	CLPR	Capacity	
☐	00	00:FD:00		 Normal	0:CLPR0	13.00 GB	VSP 5000 series / 30548
☐	01	00:FD:01		 Normal	0:CLPR0	13.00 GB	VSP 5000 series / 30548
☐	02	00:FD:02		 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-premises 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 CHAP Authentication in targetcli

1. Log in to targetcli by running the following command:

```
sudo targetcli
```

2. Enable mutual CHAP authentication by running 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 by running 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 by running the following commands:

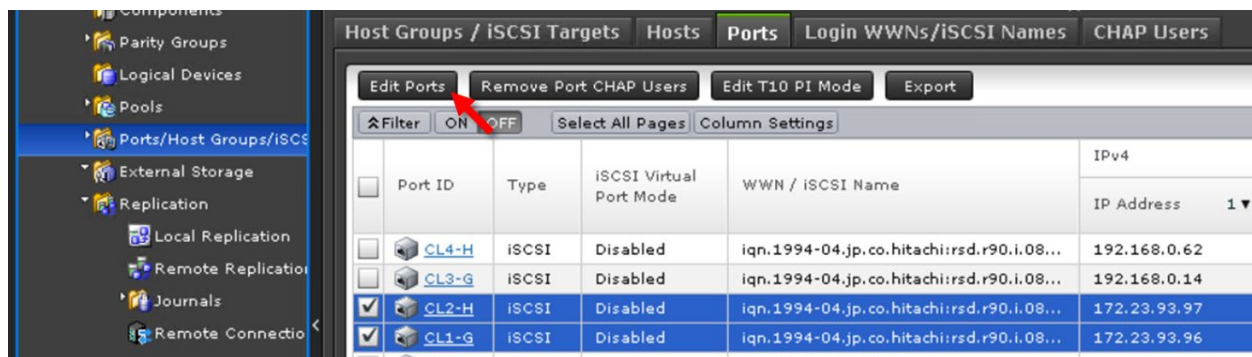
```
cd /
saveconfig
```

6. Exit from targetcli by running the following command:

```
exit
```

Enable CHAP Authentication on iSCSI Ports

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



Global-Active Device Quorum on Azure Cloud

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

- **CHAP User Name:** Value for `auth_userid` set in `targetcli`.
- **Secret:** Value for `auth_password` set in `targetcli`.

Create iSCSI Paths for CHAP Authentication

- Log in to Storage Navigator.
- From the left side of Storage Navigator, select **External Storage**, and then select **iSCSI Paths**.



- Click **Add iSCSI Paths**.
- Click **Discover iSCSI Targets**.
- For each storage system iSCSI port that will connect to the Azure virtual machine, complete the following steps:
 - Enter the following:
 - **Local Port ID:** Local iSCSI storage port.
 - **Remote IP Address:** Private IP address of the Azure virtual machine.
 - **Remote TCP Port Number:** 3260

Global-Active Device Quorum on Azure Cloud

- b. Click **Add**.

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:

Local Virtual Port ID:

Remote IP Address: ☒ IPv4 ☐ IPv6

Remote TCP Port Number:
(1-65535)

Add

Discovery List				
Select All Pages				
Local		Remote		
Port ID	Virtual Port ID	IP Address	TCP Port Number	
☒	CL2-H	-	10.2.1.5	3260
☐	CL1-G	-	10.2.1.5	3260

6. After adding the required iSCSI ports to the discovery list, click **OK**.
7. In the Add iSCSI Paths window, complete the following steps:
- Enter the following:
 - Authentication Method:** CHAP
 - Mutual CHAP:** Enable
 - User Name:** Value for `auth mutual_userid` set in `targetcli`.
 - Secret:** Value for `auth mutual_password` set in `targetcli`.
 - Click **Add**.

Authentication Method:

Mutual CHAP: ☒ Enable ☐ Disable

User Name:
(Max. 223 characters)

Secret:
(12 - 32 characters)

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

The following screenshot shows the iSCSI paths after they are created:

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.