Global-Active Device Cloud Quorum in AWS

v1.0

Implementation Guide

Reduce the costs of Global-Active Device by using a virtual machine instead of a physical storage system as the quorum. Remove the need to have a third site to host the quorum by deploying it in the cloud.
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 .............................................................................................................. 11
   Access Quorum VM ............................................................................................................. 12
Global-Active Device Quorums .................................................................................................. 14
   Create iSCSI Paths ............................................................................................................... 14
   Discover External Volumes ................................................................................................. 16
   Define GAD Quorums ......................................................................................................... 19
Appendix A: Mutual CHAP Authentication ............................................................................... 21
   Enable on targetcli ............................................................................................................... 21
   Enable on iSCSI Ports ......................................................................................................... 22
   Create iSCSI Paths ............................................................................................................... 23
Preface

About this document

This guide provides instructions to deploy a virtual machine on the Amazon Web Services (AWS) cloud and configure it to be an iSCSI target. We will use the Linux package “targetcli” to create and manage block devices on the virtual machine. The objective is to leverage volumes from the iSCSI target virtual machine running on AWS as quorum volumes for Global-active device (GAD).

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

Document conventions

This document uses the following typographic convention:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Bold**   | • Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK.  
             • 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.  
Example: `pairdisplay -g oradb` |

Intended audience

This document is intended for Hitachi Vantara and Global-Active Device users with interest in hosting their quorum on the cloud.

Referenced documents

- Hitachi’s Global-Active Device User Guide
- Linux SCSI Target: Targetcli

Accessing product downloads

Product software, drivers, and firmware downloads are available on Hitachi Vantara Support Connect: [https://support.hitachivantara.com/](https://support.hitachivantara.com/).
Log in and select Product Downloads to access the most current downloads, including updates that may have been made after the release of the product.

Comments

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

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

![Figure 1: Test Environment](image)

VPN Tunnel

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

AWS Virtual Machine

The following settings were used for the virtual machine image:

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

Deployment

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

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

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

1. In the page Step 2: Choose an Instance Type, select the following:
   - **Family**: t2
   - **Type**: t2.micro
2. On the Configure Instance Details page enter the details and then select the **Network** from the list.

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

### Step 3: Configure Instance Details

![Screenshot of Configure Instance Details page]

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

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

After these lines, add the IQNs of your GAD storage system ports separated by spaces.
4. If you do not have an existing key pair or do not want to use an existing key pair, click **Create a new key pair** from the list, enter a name for the pair, and then click **Download Key Pair**.

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

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

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

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

3. Click **Add Rule**.

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

   - **Protocol**: TCP
   - **Port range**: 3260
   - **IP version**: IPv4
   - **Source**: 0.0.0.0/0
   - **Action**: Allow

---

Global-Active Device Cloud Quorum in AWS

Page 11
• **Type:** Custom TCP Rule
• **Port range:** 3260
• **Source:** Click Custom and then enter the subnet of the storage system iSCSI ports.
• **Descriptions:** iSCSI traffic

5. Click **Save rules.**

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

**Access Quorum VM**

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

1. Use an SSH client (such as putty) to log into your quorum VM. Use the public IP and SSH key assigned to your VM.
2. Log in to the quorum. The default username is ec2-user.
3. Open the configuration script: `/home/ec2-user/quorum_setup/menu.sh`
4. Enter 7 to view the current configuration.

```
Choice: [1 - 9]
7
targetcli shell version 2.1.fb49
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.
```

```bash
/> 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- ign.2003-01.org.linux-iscsi.q-code.x8664:sn.9bdf33afba5e [TPGs: 1]
  | o- tpg1 [no-gen-acls, no-auth]
  | o- acls [ACLS: 4]
  | o- ign.1994-04.jp.co.hitachi:r90.i.089c42.1g [Mapped LUNs: 1]
  | o- mapped_lun0 [lun0 fileio/volume0 (rw)]
  | o- ign.1994-04.jp.co.hitachi:r90.i.089c42.3g [Mapped LUNs: 1]
  | o- mapped_lun0 [lun0 fileio/volume0 (rw)]
  | o- ign.1994-04.jp.co.hitachi:r90.i.089c4a.1e [Mapped LUNs: 1]
  | o- mapped_lun0 [lun0 fileio/volume0 (rw)]
  | o- ign.1994-04.jp.co.hitachi:r90.i.089c4a.2e [Mapped LUNs: 1]
  | o- mapped_lun0 [lun0 fileio/volume0 (rw)]
  | o- luns [LUNs: 1]
  | o- lun0 [fileio/volume0 (/quorums/volume0) (default tg pt gp)]
  | o- portals [Portals: 1]
  | o- 172.30.255.6:3260 [OK]
``` 

If the setup was successful, you will see volume0 and your array IQNs listed under the acls directory.

From the configuration menu, you can also add and remove quorum volumes and IQNs, refresh the portal, and enable Challenge Handshake Authentication Protocol (CHAP).
Global-Active Device Quorums

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

Create iSCSI Paths

1. Log in to Storage Navigator.
2. On the left side, click External Storage, and then click the iSCSI Paths tab.
3. Click Add iSCSI Paths.
4. Click Discover iSCSI Targets.
5. For each storage system iSCSI port that will connect to the AWS VM, complete the following steps:
   a. Enter the following:
      - Local Port ID: iSCSI port
      - Remote IP Address: private IP address of the AWS VM
      - Remote TCP Port Number: 3260
   b. Click Add.
6. After you finish adding all the required iSCSI ports to the discovery list, click OK.
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 three external volumes that were discovered.

9. Select the discovered volumes and then click **Add**. These external volumes correlate to the volumes created on your quorum VM. Testing was done with three quorum volumes (the default volume count is one).

10. Click **Finish** and then click **Apply**. The following screenshot shows the external volumes after they have been successfully virtualized.
Define GAD Quorums

1. Expand Replication, click Remote Connections, and then click the Quorum Disks tab.

2. Click Add Quorum Disks.

3. For each quorum that you are creating, complete the following steps:

   a. Enter the following:
      - Quorum Disk ID: a value from the available list
      - Available LDEVs: external volume to use as a quorum
      - Remote Storage System: remote array to pair with this new quorum
   b. Click Add.
4. Click **Finish** and then click **Apply**.

The following screenshot shows the quorums after they have been successfully created.
Appendix A: Mutual CHAP Authentication

This section describes how to configure mutual (bidirectional) authentication with Challenge Handshake Authentication Protocol (CHAP). Mutual CHAP authentication means that the on-premise storage systems must authenticate with the AWS virtual machine and vice-versa. This extra security prevents unintended access from other devices on the same network.

Enable on targetcli

1. Log in to global-active device cloud quorum VM.
2. Enable mutual CHAP authentication by entering the following commands:
   
   ```
   /home/ec2-user/quorum_setup/menu.sh
   ```

3. Follow the prompts to set credentials.
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.