Dell EMC Cloud Mobility for Storage

Product Overview

Dell EMC Cloud Mobility for Storage enables you to view and analyze snapshots in the cloud and, when needed, move them back to external storage. A virtual application within the AWS Marketplace, Cloud Mobility for Storage provides access to snapshots you have shipped to the cloud from your storage array.

Storing your array snapshots in the cloud reduces the number of live workloads running on local infrastructure. On the Cloud Mobility for Storage interface, you can see and analyze read-only snapshots for testing and development purposes.

Once deployed, Cloud Mobility for Storage provides read-only access to snapshots sent to the cloud. You access snapshots by using a separate iSCSI initiator in the cloud, moving snapshots back to other storage.

Requiring no separate license, Cloud Mobility for Storage also provides multipath I/O support for path redundancy and better performance to ensure continued access to your resources.

Supported configurations

Within the AWS EC2 environment, you can use Cloud Mobility for Storage to manage snapshots from the following cloud providers:

- Amazon S3
- Dell EMC Elastic Cloud Storage (ECS)
- Microsoft Azure

You can have up to 4,000 volumes in the cloud, with a maximum of 32,000 snapshots spread over those 4,000 volumes.

Cloud Mobility for Storage instances

You can have as many instances of Cloud Mobility for Storage as you need. As a best practice, you create the instance and then delete it after you have retrieved the data that you need. When you need access to snapshots again, simply deploy a new backup from the array to Amazon Elastic Compute Cloud (EC2).

Disaster recovery

Although it is not primarily used as a disaster recovery solution, Cloud Mobility for Storage provides disaster recovery capability for snapshots. In the event of a disaster, you use cloud snapshots to

reconstruct and pull snapshots from the cloud and restore them to local storage that is directly attached to the iSCSI initiator.

Deployment

Prerequisites for Cloud Mobility for Storage

The compute environment for Cloud Mobility for Storage resides entirely within AWS EC2. Cloud Mobility for Storage cannot be run as a VMware instance inside your data center or within Azure Compute.

To deploy Cloud Mobility for Storage, you need the following:

- A PowerMax backup configuration
- Amazon AWS account credentials
- An Amazon Machine Instance (AMI)
- An EC2 key pair for Windows or Linux
    - The key pair allows you to use SSH to securely connect to the AMI.
- A basic understanding of how to use Amazon Elastic Cloud; for more information, see Amazon how-to documentation in Amazon Marketplace.
- Either m4large or m4xlarge machine instances within EC2

Firewall rules

Before deploying Cloud Mobility for Storage, the following inbound firewall rules must be configured in EC2:

Protocol	TCP Port	Default Route
SSH	22	0.0.0.0/0
SSH	22	::/0
Custom TCP	3260	0.0.0.0/0
Custom TCP	3260	::/0
HTTPS	443	0.0.0.0/0
HTTPS	443	::/0

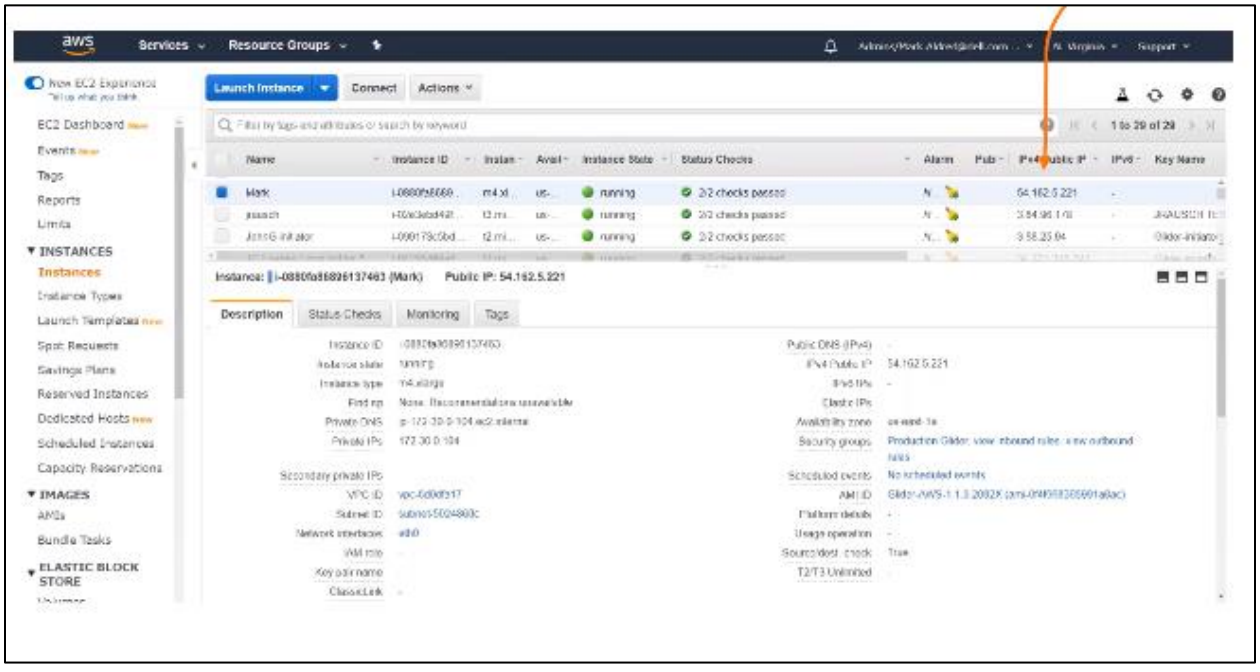
Creating a configuration backup from the array

Before you install and deploy Cloud Mobility for Storage, you must create a CMS backup configuration file from the PowerMax array and create a password for that backup.

1. In Unisphere, go to the Cloud Mobility Dashboard.
2. Download a backup of the configuration, which is saved as a `.tgz` file.
3. Set a password for the backup.
4. Place the downloaded file in a folder or location where you can easily access it.

Deploying Cloud Mobility for Storage in Amazon Marketplace

1. Search in the Amazon Marketplace for Dell EMC products.
2. In the search results, select Cloud Mobility for Storage.
3. Click **Subscribe and Deploy**.
   After you deploy the instance inside Amazon Marketplace, use the EC2 console to see the instance you just deployed.



   You should see the IPv4 public IP address, which you need to access the instance of Cloud Mobility for Storage that is running in Amazon EC2.
   Note: Verify the instance is in the Running state; if the instance is still in the Initializing state, wait for it to enter the Running state.
4. Copy and paste the IPv4 address of the instance into the address field of your browser, adding `https` in the address.

The **Getting Started with Cloud Mobility** screen should appear.
(**Note:** Using a self-signed certificate is less secure than accessing the Cloud Mobility for Storage through a VPN client on your system and connecting to an AWS Client VPN endpoint. For more information about using self-signed certificates with PowerMax systems, see the *Dell EMC PowerMax Family Security Configuration Guide*.

Installing Cloud Mobility for Storage

After you deploy Cloud Mobility for Storage, perform the installation by applying the configuration backup that you created. Ensure you have the password that you set for the backup.

Complete the following procedure after you have pasted the IPv4 address into the browser, which has brought you to the **Getting Started with Cloud Mobility** screen.

1. Click **Start** on the **Getting Started with Cloud Mobility** screen.
2. Select the backup configuration file you saved earlier and enter the password for that backup.
3. Create a username and password for managing the Cloud Mobility for Storage instance in EC2.
4. Click **Begin Installation**.
   Note: The installation might take several minutes to complete.
   When the installation finishes, you will see the Cloud Mobility for Storage login screen.
5. Enter the user and password you created during the previous installation step for the Cloud Mobility for Storage instance.

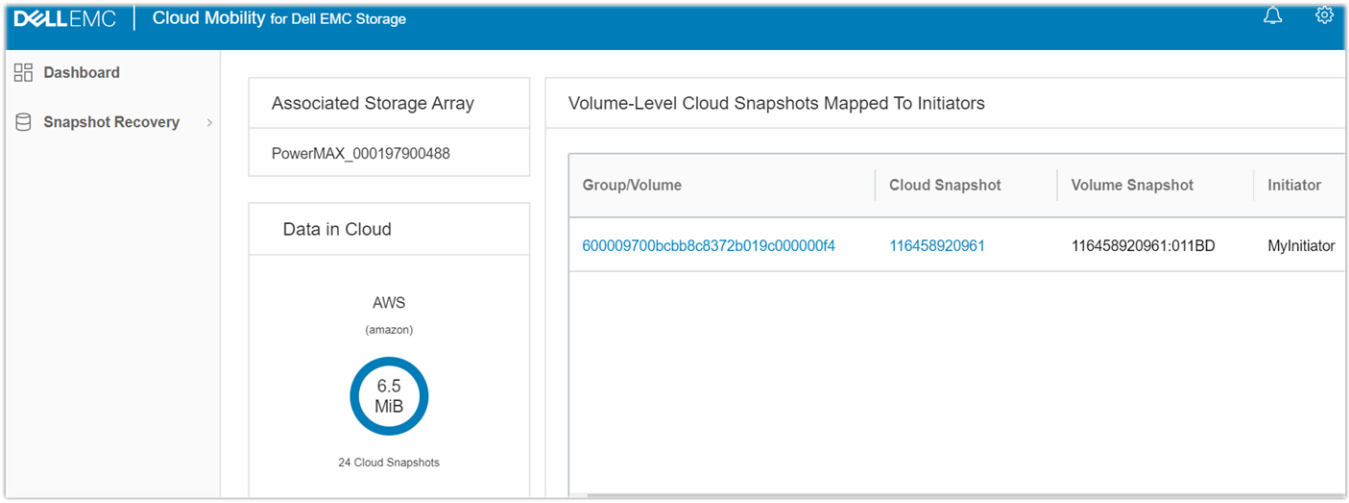
The Cloud Mobility for Storage Dashboard

The **Dashboard** is the main landing page for Cloud Mobility for Storage within Amazon EC2. This page is where you view and manage your cloud snapshots.

A cloud snapshot can originate from either a volume group or an individual volume. A snapshot of a volume group that Cloud Mobility for Storage sends to the cloud is considered a cloud snapshot. A snapshot of an individual volume Cloud Mobility for Storage sends to the cloud is also considered a cloud snapshot.

You can find the following information in the Dashboard:

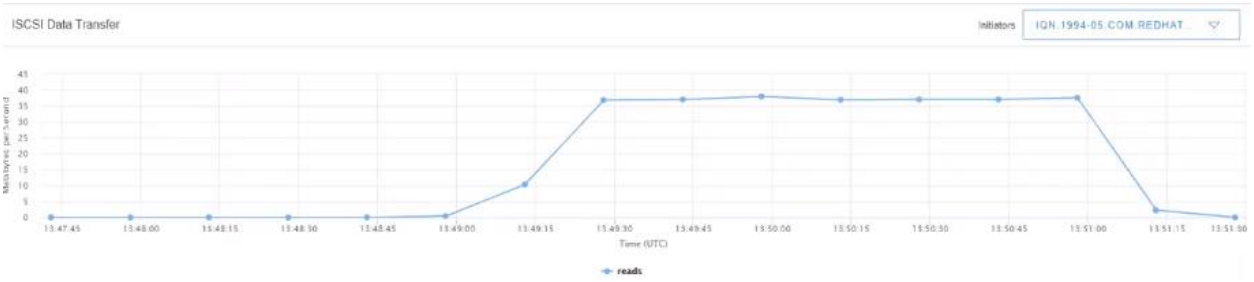
- The storage array from which the cloud snapshots originated
- The amount of data in the cloud for each cloud provider
- The number of volume-level snapshots mapped to iSCSI initiators
- Other cloud providers, if you have them
- Cloud and iSCSI data transfer graphs



Data transfer

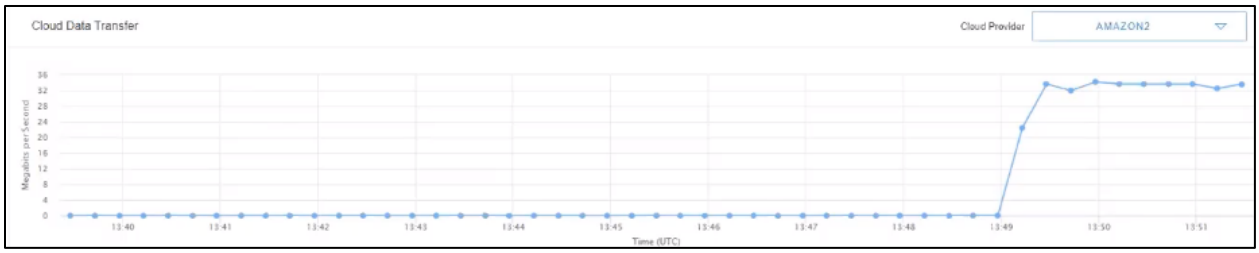
The Dashboard includes a Cloud Data Transfer that describes the data transfer rates for each cloud provider. The graph represents the most recent 15 minutes of data transfer, with a new data point every 15 seconds.

You can see data on both the iSCSI end of the transfer and on the cloud end. The drop-down menu enables you to see graphed data for individual cloud providers or individual iSCSI initiators, or aggregates of all providers or initiators.



Cloud providers

If you navigate to **Snapshot Recovery > Cloud Providers** from the **Dashboard**, you can see the details of each cloud provider that is configured. This data is read-only.



Security Configuration

You can use the AWS Virtual Private Cloud (VPC) to create an isolated network that sends snapshots from your storage array to the Cloud Mobility for Dell EMC Storage instance.

After configuring an AWS Client VPN endpoint, you can access the instance through a VPN client on your system. Configure outbound connections to the internet to allow Cloud Mobility for Storage to connect to your cloud storage. This type of isolated network prevents the following two security threats:

- Man-in-the-middle attacks
- Denial-of-service attacks

If the iSCSI initiator is hosted in EC2 with the Cloud Mobility for Dell EMC Storage instance, configure the networks and security groups to restrict the iSCSI traffic to a private subnet between CMS and the iSCSI initiator. If the initiator is not in the same VPC, you should establish access to the instance through a VPN client on your system.

If you securely connect to a VM that shares a subnet with Cloud Mobility for Dell EMC Storage Instance (not necessarily the same as the initiator), you can use the web browser on that VM to access the Cloud Mobility for Dell EMC Storage instance. Using this approach, you can safely disregard the untrusted certificate warning. If the AWS EC2 subnets are configured properly, no additional configuration is required because insecure traffic remains within these subnets.

If you do not use a VPN, you should manually verify the certificate through SSH. However, the VPN also secures the iSCSI traffic while manually verifying the certificate does not.

Note: Connecting to the Cloud Mobility instance through a VPN client on your system is a best practice.

Managing snapshots

Viewing Volume Groups and Volumes

You manage snapshots at the volume group level.

Within Cloud Mobility for Storage, you can see volume groups, the number of snapshots in each volume group, and the most recent snapshots for those groups. You can view the list of snapshots taken for each volume group and see details for each volume within that snapshot.

1. Select the volume group to see a list of snapshots within that volume group.
2. Select a snapshot to see details for each volume in the snapshot.

Adding an iSCSI initiator

To map volumes within a cloud snapshot to an iSCSI initiator, you must first add the initiator in the Cloud Mobility for Storage instance.

Before mapping the initiator, you must have the iSCSI Qualified Name (IQN) of the initiator.

Note: As a best practice, you should avoid mapping more than 16 snapshots to a single initiator.

1. Under **Snapshot Recovery** in the navigation pane, click **Initiators**.
2. On the iSCSI initiators screen , click **ADD**.
3. In the popup window, specify a name for the initiator you want to add and enter the iSCSI Qualified Name (IQN) of the initiator.
4. Click **ADD**.
   You can also delete initiators from this screen.

Mapping a volume-level cloud snapshot to an initiator

1. On the **Cloud Mobility for Storage Dashboard**, click **Snapshot Recovery > Cloud Snapshots.**
2. Click on a volume group from the ones listed.
   Note: If you have many volume groups, you can filter which volume groups are displayed in the Volumes & Groups table.
3. Click the name of the snapshot that you want to map.
4. On the **Volume-Level Cloud Snapshots** page, check the box next to the volume that you want to map and click **MAP**.
5. Click the radio button to select the initiator.
6. Click **MAP**.
   When the volume is successfully mapped to the initiator, that volume is visible on the volume-level page. That volume is also visible on Initiators when clicking on the mappings link for that initiator. Finally, the volume can be seen on the Dashboard in the Volume-Level Cloud Snapshots Mapped to Initiators table.
   Note: All mappings in CMS to iSCSI initiators provide read-only access to the host. Read-only access prevents any changes from being made to the snapshots that were shipped by the array.

Viewing iSCSI mapping

After you have mapped to initiators, you can view a list of all mapped snapshots and the initiators to which they are mapped.

There are two ways to view details of mapped initiators:

- You can see the initiators in the Volume-Level Cloud Snapshots Mapped to Initiators table on the **Dashboard**.
  You can filter this list if you have mapped snapshots and initiators.
- Click on the Initiators tab in the navigation pane:
  - Select a specific initiator from the list.
  - Click Mappings to see a drop-down list of all devices associated with that initiator.

System Status

You can check the system status on the Cloud Mobility for Storage Dashboard by clicking on the gear icon. In the Settings window, you can see the following information:

- System Status
  - Software version
  - Log level
    Note: The log level is not adjustable from the user interface; only Dell EMC Support can adjust the log level.
  - Local time
  - Up time (how long the instance has been running)
- CA Certificates
  This screen allows you to upload certificates to access other cloud providers, if necessary.
- Support Captures

Generating support captures

If you have an issue that requires support, you can download a support capture to share with Dell EMC Support. A support capture includes all the logs needed to debug an instance as well as other runtime information.

1. Navigate to the **Settings** window and click **Support Captures**.
2. Click **GENERATE SUPPORT CAPTURE**.
   The support capture appears below.
3. Click the radio button next to the support capture to download it.

Deleting a Cloud Mobility for Storage instance

When you have copied the information that you need from the Cloud Mobility for Storage instance to local storage, you can delete the instance from Amazon EC2.

1. Navigate to the EC2 console.
2. In **Instances**, select the instance that you want to delete.
3. Click the **Actions** drop-down menu.
4. Select **Instance State** and **Terminate**.