Technical White Paper

Cloud Mobility for Dell EMC PowerMax

Abstract

This document describes how Cloud Mobility for Dell EMC™ PowerMax connects to public and private cloud with ease. This feature enables creating policy-based, automated snapshots in seconds for archiving and long-term retention.

September 2020

Revisions

Date	Description
September 2020	Initial release: PowerMaxOS Q3 2020

Acknowledgments

Author: Kevin Vaillancourt

Support: Dell EMC Storage Technical Marketing Engineering Team

Table of contents

Executive summary

Dell EMC™ storage systems address rapid data growth and optimize data-center resources with simple and efficient data mobility to and from public and private clouds. Cloud Mobility for Dell EMC PowerMax offers seamless and transparent movement of application data copies from on-premises to cloud, enabling PowerMax customers to leverage public cloud for agile and economical storage. Archiving and long-term retention are primary examples of how PowerMax customers can leverage Amazon Web Services (AWS), Microsoft® Azure®, and Dell EMC ECS™ for low-cost storage. PowerMax data can be recovered back to the source PowerMax if needed. Archiving to the cloud frees capacity for on-premises PowerMax arrays to support higher priority applications.

PowerMax data stored in the cloud can be made available to an AWS system for secondary processing. For example, a Linux® image can run Oracle® in AWS, which in turn can mount a PowerMax database copy and perform reporting, analytics, or development/test on that database. When the secondary processing is complete, the data can be exported, and the infrastructure can be removed. This ability allows the customer to realize the inherent cost savings of a flexible public-cloud consumption model.

1 Overview

Cloud Mobility for Dell EMC PowerMax is configured within an embedded guest running on the PowerMaxOS hypervisor. Management of Cloud Mobility is performed using the Embedded Management (eManagement) Unisphere™ for PowerMax. Communication between the embedded Unisphere and Cloud Mobility is through REST API over a PowerMax internal private network connection. More details about the PowerMax hypervisor that also powers Embedded Management, Embedded NAS, and the new Embedded VASA provider are in appendix A.

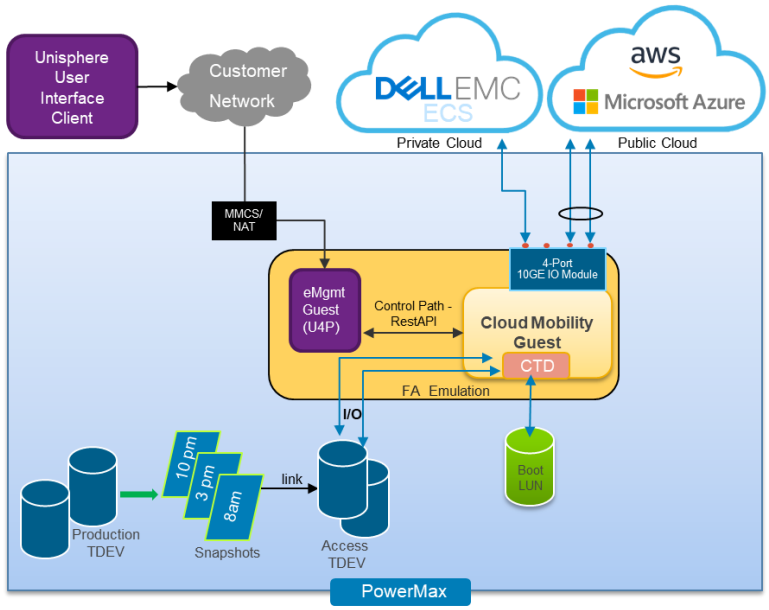


Figure 1 Cloud Mobility for PowerMax high-level architecture

A single dedicated 4-port 10 Gb Ethernet I/O module is connected to the Cloud Mobility guest to provide external IP connectivity to the cloud providers. These ports can be configured as individual ports or as teams to provide resiliency, which is recommended.

Cloud Mobility uses the following resources from the PowerMax:

- 2 vCPU
- 4 GB memory
- (1) 4-port 10 GbE I/O Module
- ~180 GB storage space for boot or data volumes

1.1 Supported configurations

The following are requirements for using Cloud Mobility:

- PowerMax storage platform
- PowerMaxOS Q3 2020 release or later
- Embedded Unisphere for PowerMax V9.2 or later
- (1) 4-port 10 GbE I/O module, used by the guest for cloud provider connectivity.
- Dell EMC ECS, Amazon S3, or Microsoft Azure Blob Storage as a cloud storage provider

1.2 Cloud Mobility scale

You can have up to 4,096 volumes in the cloud, with a maximum of 32,000 snapshots spread over those 4,096 volumes.

1.3 Cloud Mobility Dashboard

Management of Cloud Mobility is performed on the Cloud Mobility Dashboard in Unisphere for PowerMax shown in Figure 2. The dashboard is available by selecting a storage system and going to **System > Cloud.** The Cloud Mobility dashboard is only available through embedded Unisphere for PowerMax.

The dashboard provides the following:

- View Cloud System Health, Jobs, Alerts, and manage cloud system configuration
- View Cloud Storage Groups
- Configure and view Cloud Providers
- Configure and manage Cloud Snapshot Policies
- Performance chart for Cloud Provider Total Used Capacity
- Performance chart for Cloud Provider Throughput Mbs/sec

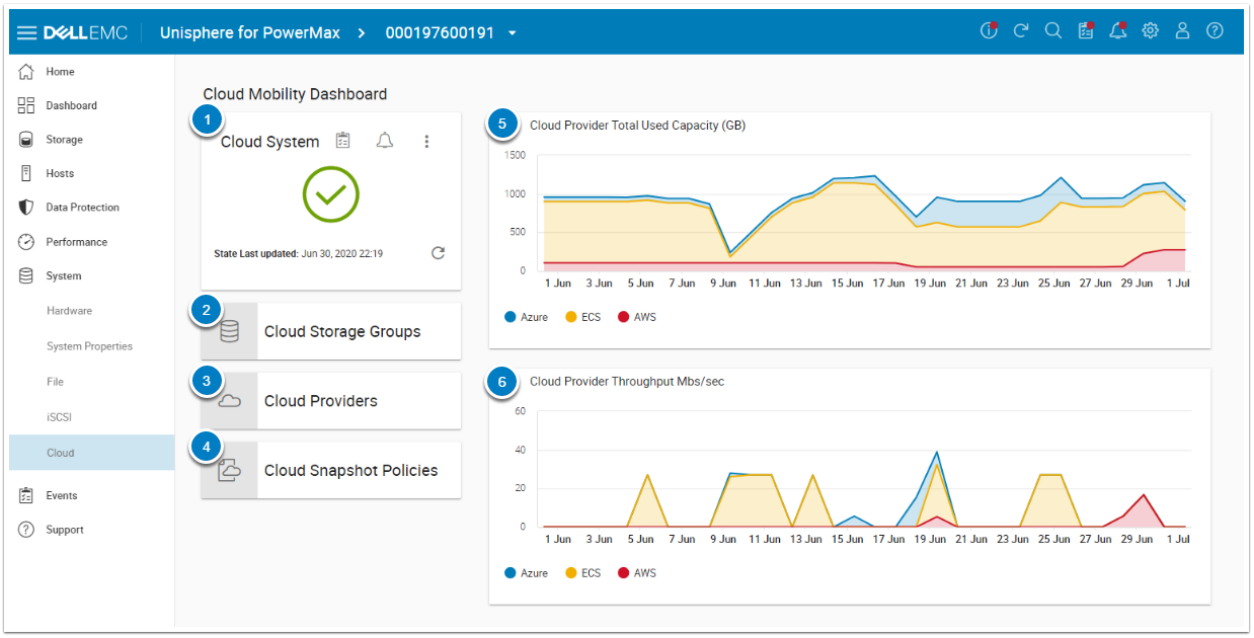


Figure 2 Cloud Mobility Dashboard

2 Cloud Mobility operations

2.1 Managing cloud system configuration

Additional cloud system management options are available by clicking on the three-vertical ellipsis as shown in Figure 3.

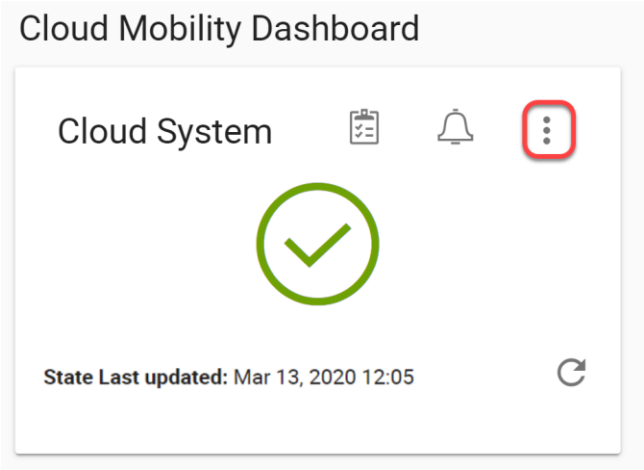


Figure 3 Other cloud management options

The additional management options are:

- Network Configuration – Modify interfaces, IP addresses, DNS, and Routes
- Set Bandwidth Limits – Configure network bandwidth limit for the cloud system
- Download Cloud Configuration Backup – Encrypted file that holds the cloud system configuration
- Advanced Cloud Snapshot Management – Viewing advanced snapshot management information
- Cloud Certification Management – Add/Modify cloud certificates
- Remove Cloud System – Remove cloud system

2.1.1 Network configuration

After the initial cloud system setup, networking details can be viewed and changed in the network configuration page.

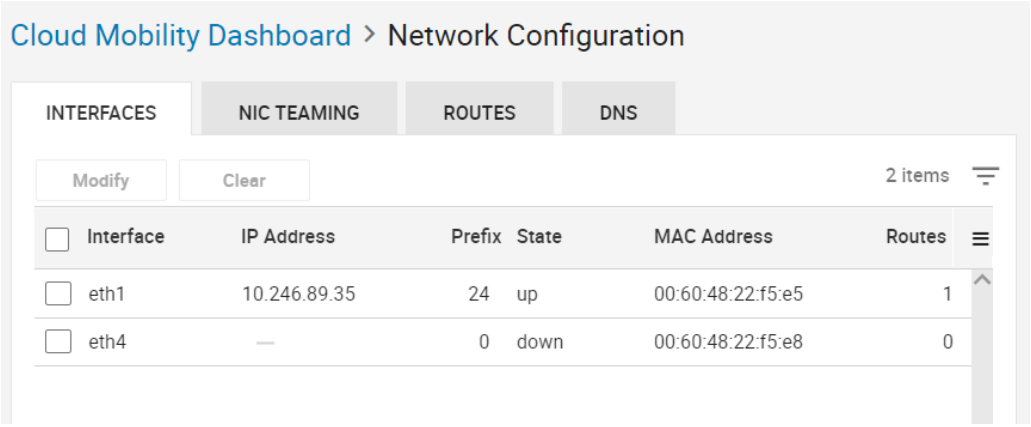


Figure 4 Network configuration

Each port on the four ports on the 10 GbE network I/O module can be configured as network interfaces individually or can be teamed together providing redundancy. Network teaming may also be known as link aggregation, NIC teaming, or ethernet bonding. The interface names, eth1 to eth4, correspond to the I/O modules ports 0 to 3, respectively. In Figure 4 above, eth1 and eth2 interfaces are not displayed because they are configured as part of a NIC team.

The following are requirements for the cloud system network:

- Only IPv4 Interfaces are supported.
- Netmask Length value must be between 8 and 31
- Only one default route can be configured for the cloud system
- A maximum of three DNS servers can be configured.

2.1.2 Network bandwidth limits

Optional bandwidth limits can be placed on the cloud system network interfaces by enabling this option and defining the maximum Mbps as display in Figure 5.

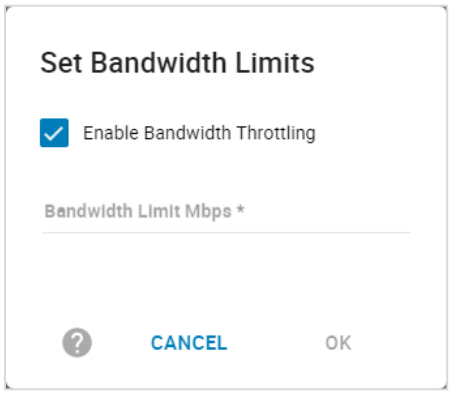


Figure 5 Bandwidth Limits

2.1.3 Cloud configuration backup

The cloud system configuration can be backed up and exported to an encrypted file for use with Dell EMC Cloud Mobility for Storage. Cloud Mobility for Storage is a virtual application in the AWS Marketplace providing access to snapshots that have been shipped from the PowerMax to cloud providers.

The backup operation prompts for a one-time password used to encrypt the configuration backup file. Use of a strong password is recommended and stored in a secure location. The configuration file contains information pertaining to the cloud providers, cloud snapshots, and encryption keys for the data stored on the cloud providers. This password and configuration backup file is required when using Cloud Mobility for Storage.

More details about Cloud Mobility for Storage are in section 5 and in the Cloud Mobility for Storage Guide.

Note: We recommend exporting the cloud configuration regularly for site-recovery situations.

2.1.4 Advanced Cloud Snapshot Management

The Advanced Cloud Snapshot Management page displays all the SnapVX snapshots on the PowerMax tagged as Cloud Snapshots as shown in Figure 6. The list details the snapshot ID, name, creation time on the array, if it was taken as part of a cloud snapshot policy, the storage group the snapshot applies to, if the cloud

snapshot is protected in the cloud, and if the snapshot is a delete candidate. A delete candidate is any snapshot that has been shipped to the cloud, its retention period has expired, or its cloud provider is now invalid or offline.

Snapshots can be selected to view additional details or deleted if the provider is invalid or offline. The cloud snapshots can also be deleted before the assigned expiry time if no longer required.

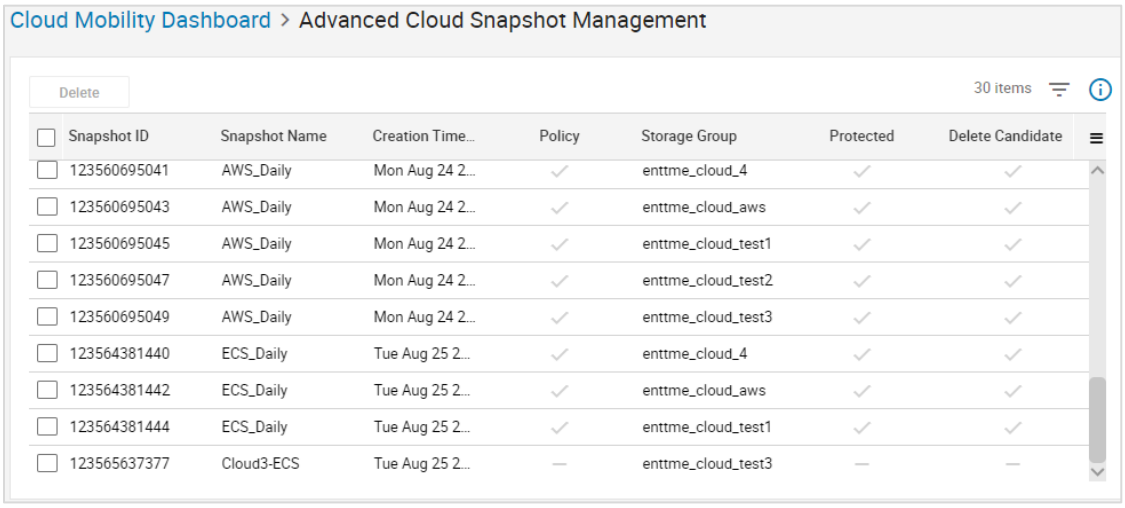


Figure 6 Advanced Cloud Snapshot Management

2.1.5 Cloud Certificate Management

Setting up the cloud system to access ECS over a secure SSL connection may require a valid certification authority (CA) certificate to be imported before adding ECS as a cloud provider.

If your organization is not using a public Certificate Authority service, it may be necessary to internally generate a CA certificate in order to enable an SSL connection from the cloud system to the load balancer which handles traffic for the ECS. In most cases where an internal CA is being used, it is important to install the *root* CA, not the server certificate installed on the load balancer. Even if using a public CA, it is still likely that installing the root CA is required. For purely private networks, such as offsite DR or test locations which may be isolated from public DNS and CA servers, it is possible to create a self-signed certificate which can be imported into the cloud system for use in building the SSL tunnel.

Once a self-signed CA certificate file has been generated in PEM format (x509 with Subject Alternative Name entries), it can be imported into the cloud system as shown in Figure 7.

Figure 7 Cloud Certification Management

2.1.6 Remove Cloud System

Cloud Mobility can be removed to release the allocated CPU and memory back to the PowerMax for array redistribution. The Unisphere Remove Cloud System operation will un-enroll the cloud system but will not release the resources back to the PowerMax. A Dell Technologies™ Professional Services engagement is required to complete the removal of the Cloud Mobility guest and the associated 10 GbE I/O module.

Dell Support will be required to reset the Cloud System enrollment if you wish to re-enroll the Cloud System after running the Remove Cloud System operation and did not have professional services complete the uninstall.

Prior to running Remove Cloud System, all cloud-related objects (Cloud Snapshots, Cloud Policies, and Cloud Providers) must be deleted from the array.

2.2 Cloud jobs

To view a list of the Active Cloud Jobs, click the clipboard icon as shown in Figure 8.

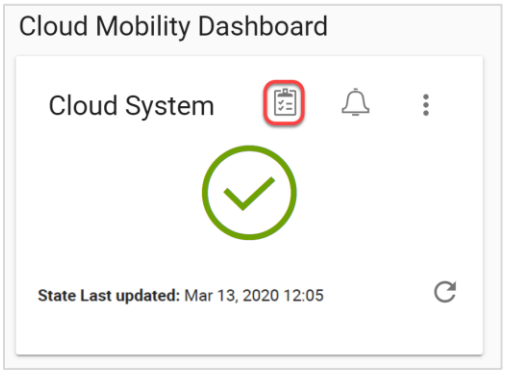


Figure 8 Cloud System Active Jobs

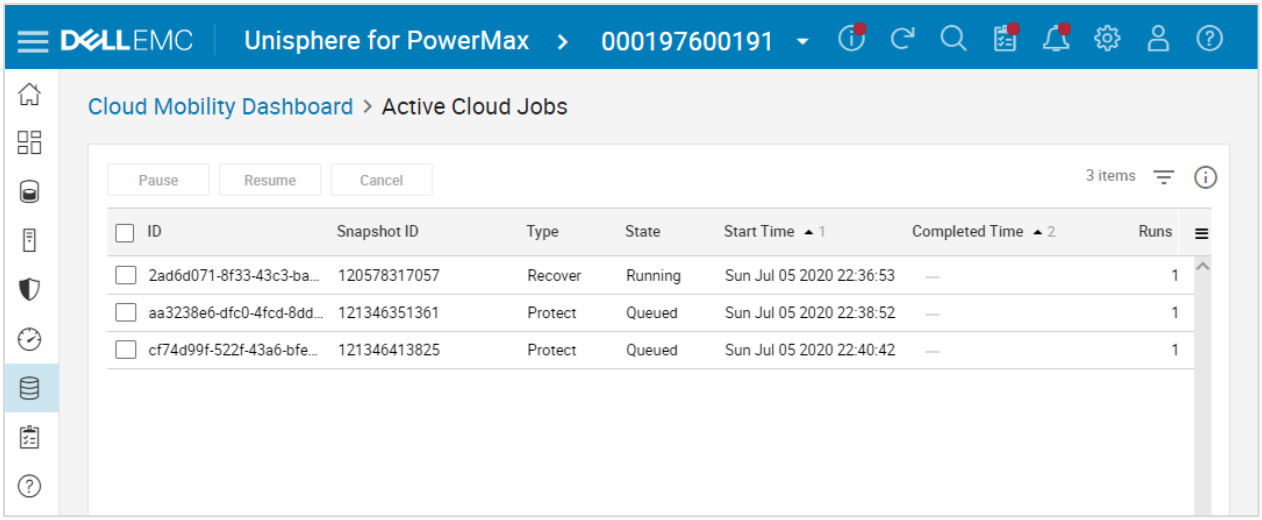


Figure 9 Active Cloud Jobs

The system active cloud jobs window displays the following information:

- Cloud Job ID
- Snapshot ID – ID of the snapshot with which the job is associated.
- Type – Type of the job. Possible values are:
  - Protect
  - Recover
  - Delete
- State – State of the job. Possible values are:
  - Queued
  - Running
  - Completed
  - Cancelling
  - Cancelled
  - Failed
  - Paused
- Start Time – Date and Time the job started.
- Completed Time – Date and time the job completed. This field is blank for incomplete jobs.
- Runs – The number of times the job has been run.

Note: If a cloud-related job fails, the user will need to intervene to resume or cancel the job. Failure to do so will stop future cloud protection jobs from running on the associated Storage Group.

2.3 Cloud providers

The following public and private cloud providers are supported for use with Cloud Mobility:

- Dell EMC ECS
- Amazon S3
- Microsoft Azure

Selecting **Cloud Providers** on the Cloud Mobility Dashboard opens the cloud providers page, as shown in Figure 10. The cloud providers page displays the configured providers, status, capacity used, and additional details. From this page, cloud providers are created, modified, or deleted.

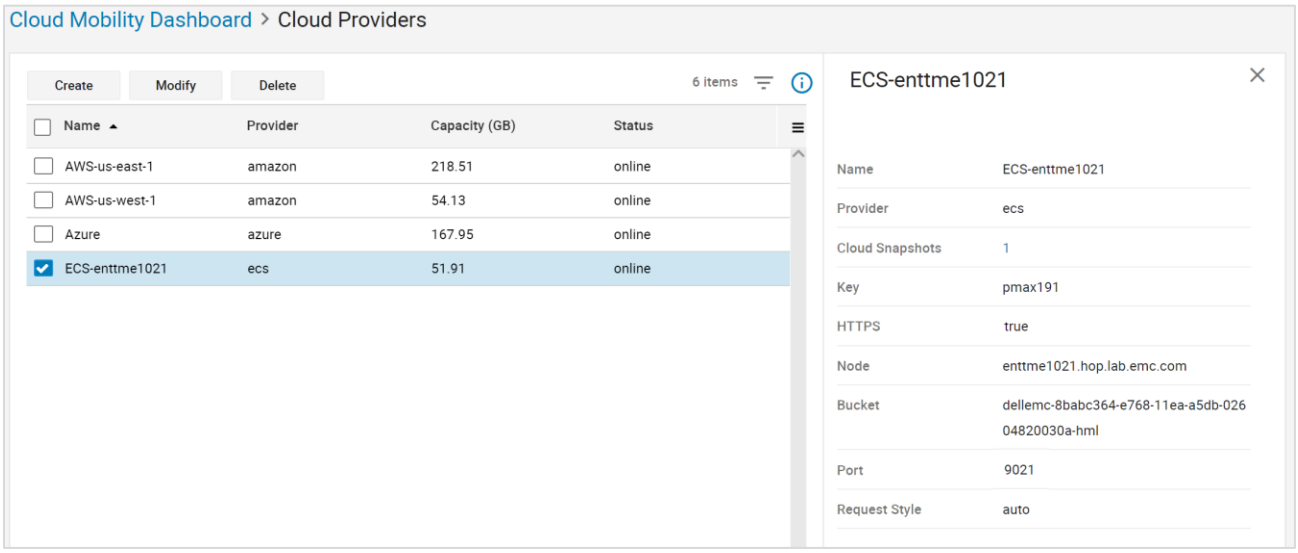


Figure 10 Cloud Providers

2.3.1 Creating cloud providers

To create a new cloud provider:

1. Click **Create.**
2. Choose the type of Cloud Provider (ECS, Amazon S3, or Microsoft Azure).
3. Enter the appropriate fields. Each of the cloud provider types has specific fields as shown in Table 1.
4. Click **Run Now**.

Table 1 Cloud provider creation fields

Cloud provider type	Fields
ECS	• Name * • Node * • Key * (Object Username) • Secret * (Secret Key) • Port • HTTPS • Bucket • Request Style
Amazon S3 (AWS)	• Name * • Access Key ID * • Secret Access Key * • Port • Bucket • Storage Class • Provider Region
Azure	• Name * • Storage Account * • Managed Key * • Port • HTTPS • URL • Container

* Fields are required

Note: If a bucket or container name is not provided, one will be generated using the prefix of **"dellemc-<cloud_provider_id>".**

After successfully adding the provider, a window is presented to create a snapshot policy for the cloud provider as shown in Figure 11.

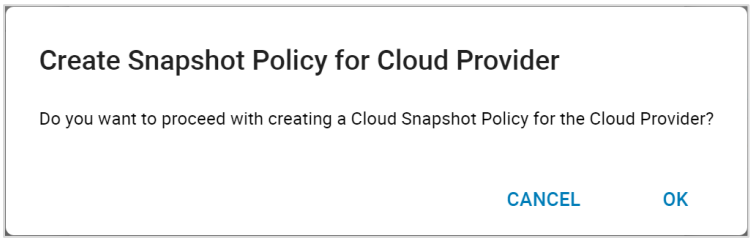


Figure 11 Create Snapshot Policy Popup

2.3.2 Modify cloud providers

It may be necessary to modify the cloud provider name or connection details after creation. Performing rotations of the keys used is a best practice. Depending on the cloud provider type, only the following parameters as shown in Table 2 are available to be modified.

Table 2 Cloud provider modify fields

Cloud provider type	Modify fields
ECS	• Name • Secret • Port • Node • Request Style
Amazon S3	• Name • Secret Access Key • Port
Azure	• Name • Managed Key • Port • URL

2.3.3 Delete cloud providers

Once a cloud provider is no longer in use it can be deleted from the cloud system. Before deleting a provider, all associated cloud snapshot policies and cloud snapshots must be deleted.

2.4 Cloud snapshot policies

Snapshot policies allow the automated scheduling of snapshots for Storage Groups. Cloud Mobility snapshot policies can be managed using Unisphere for PowerMax and REST API and can only be created and modified with Embedded Management Unisphere. External Unisphere instances can add and remove Storage Groups from existing cloud snapshot policies.

The snapshot policy creation wizard is launched either after creating a cloud provider or from the Cloud Mobility Dashboard selecting **Cloud Snapshot Policies** and clicking **Create Snapshot** Policy as shown in Figure 12.

Note: The Snapshot Policies page is also available by going to **Data Protection** > **Snapshot Policies**.

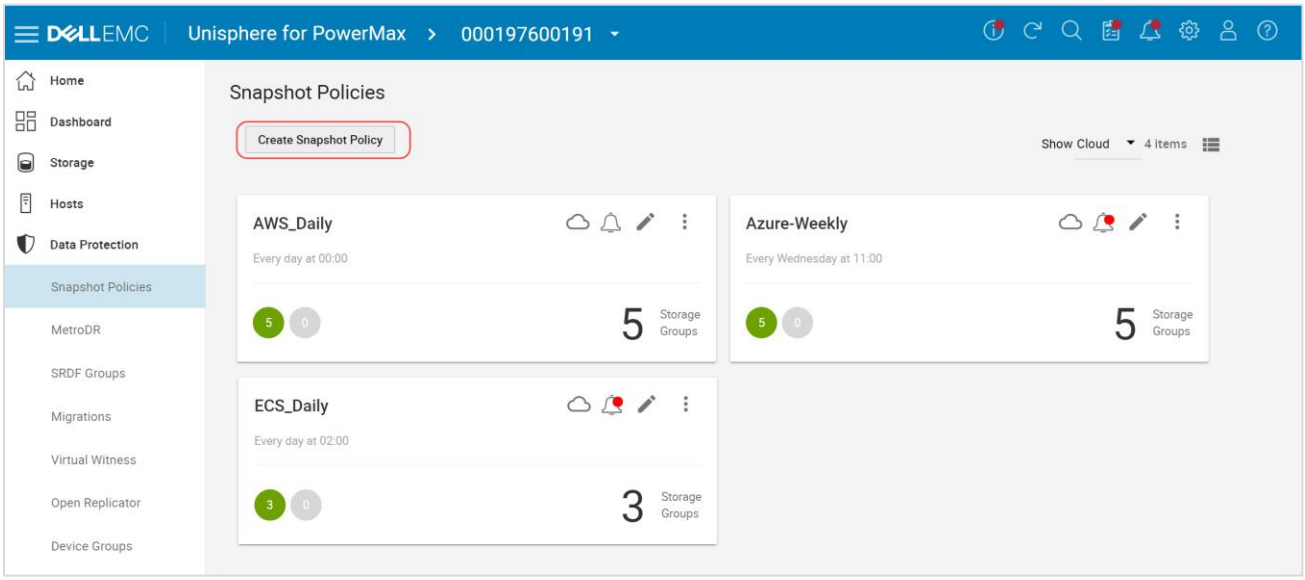


Figure 12 Snapshot Policies

In the Create Snapshot Policy as seen in Figure 13, the cloud snapshot policy parameters include:

- Cloud Provider selection
- RPO Options:
  - Daily or Weekly
- Keep For:
  - 3 Days
  - 1 Week
  - 1, 3, or 6 Months
  - 1, 7, or 14 Years
    Until Specific Date
- Compliance:
  - Warning – minimum number of snapshots required for Warning threshold
  - Error – minimum number of snapshots required for Error threshold

Note: The **Keep Until Specific Date** must be greater than 3 days but less than 14 years.

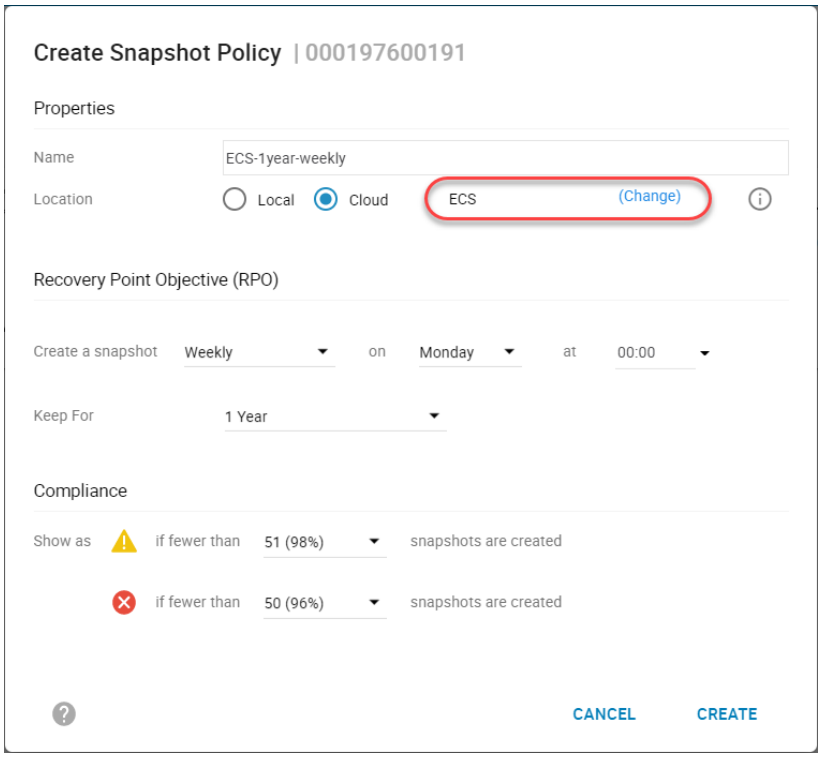


Figure 13 Create Cloud Snapshot Policy

For additional information about managing snapshot policies, see the Dell EMC PowerMax and VMAX All Flash Snapshot Policies Best Practices document.

2.5 Assigning storage groups to policies

You can assign up to four policies to each Storage Group (SG). There is no limit to the number of SGs that can be assigned to a single policy.

The child SGs inherit the policies assigned to a parent SG. When a policy is assigned to a parent SG, the policy takes a snapshot at the parent-SG level and the snapshot is consistent across all child SGs. Conversely, if the policy is individually assigned to each child SG, the child SGs are snapped separately, and the snapshots are not consistent across all child SGs.

SGs that contain common volumes should not be assigned to the same policy because only one SG will be snapped.

To add a Storage Group to a cloud snapshot policy:

1. **Click** the **three vertical ellipsis** to expand the extra controls window (Figure 14).
2. Select **Add Storage Group.**
3. Select **Storage Group** names (Figure 15).
4. Click **Add.**

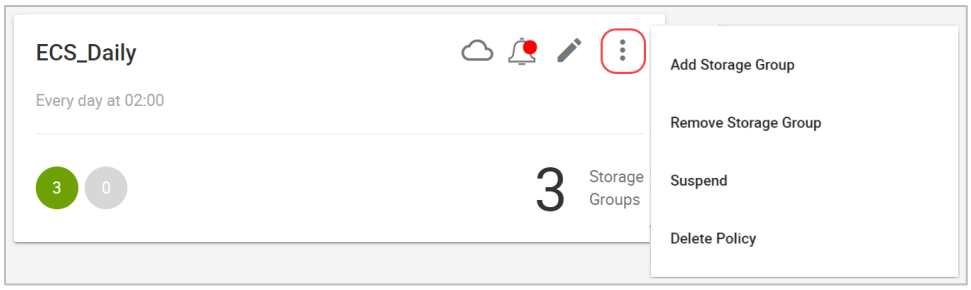


Figure 14 Snapshot Policies Extra Controls

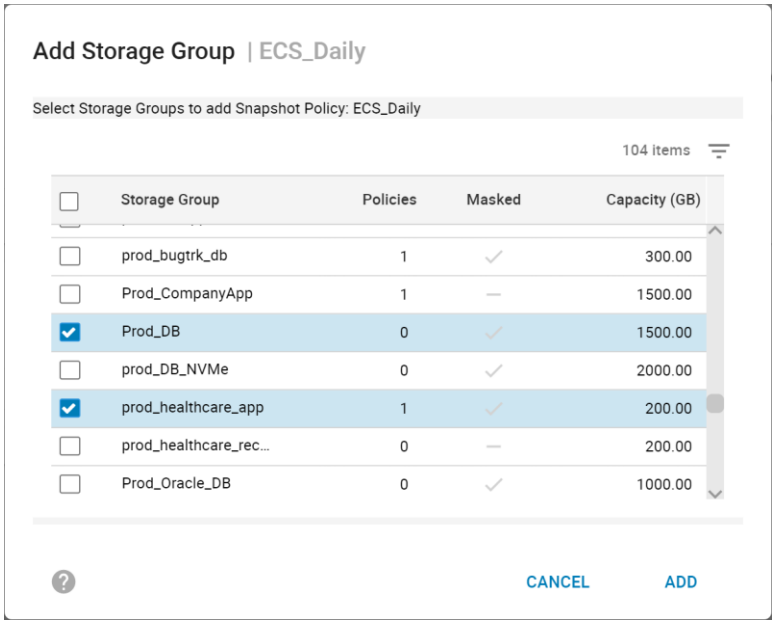


Figure 15 Snapshot Policy: Add Storage Group

2.6 Create on-demand cloud snapshots

In addition to the scheduled snapshots taken as part of the cloud snapshot policies, on-demand cloud snapshots can be taken.

To take an on-demand cloud snapshot:

1. Select **Storage** > **Storage Groups**.
2. Click on the storage group name to view all details.
3. Select **Data Protection** tab.
4. Select **Cloud Snapshots** tab (as shown in Figure 16).
5. Click **Create**, the Create Cloud Snapshot dialog box is displayed (Figure 17).
6. Type a **New Snapshot Name**.
7. Optional: Change the default **Cloud Provider**.
    a. Click **Change**.
    b. In the **Select Cloud Provider** dialog box, select a cloud provider.
    c. Click **OK.**
8. Select a value for **Keep For**. This is the length of time for which to keep the snapshot.

9. Click **Next.**
10. Review the summary.
11. Click **Add to Job List** or expand Add to Job List and click **Run Now**.

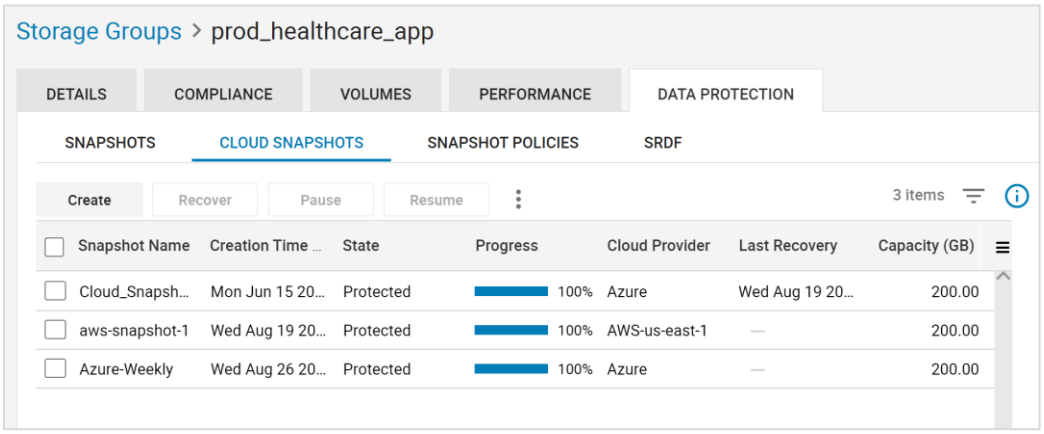


Figure 16 Storage Group Details > Cloud Snapshots

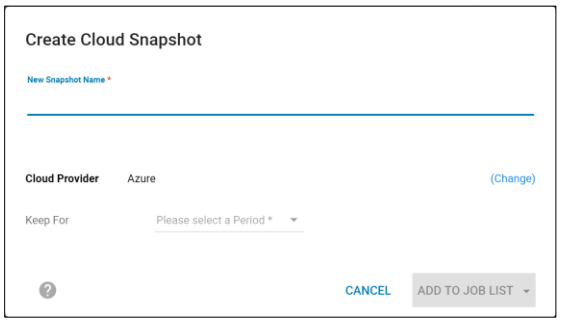


Figure 17 Create Cloud Snapshot

2.7 Recover from cloud snapshot

The recovery of data from a cloud snapshot is performed for the entire Storage Group. A new storage group and volumes will be created with a user provided SRP and Service Level. Cloud Mobility will restore the data from the cloud provider directly to the new volumes. The new volumes will have volume identifier of source volume number. Recovering the parent of a cascaded storage group will restore the individual volumes into a single new storage group.

To recover from a cloud snapshot:

1. Go to the Cloud Mobility Dashboard: Select **System > Cloud**
2. Select Cloud Storage Groups.
3. Select a storage group.
4. In the storage group details view, click the number of **Cloud Snapshots** (Figure 18).
5. Select the cloud snapshot that you want to recover (Figure 19).
6. Click **Recover.** The **Recover Cloud Snapshot** dialog box is displayed (Figure 20).
7. Type a **Storage Group Name**.
8. Select an **SRP.**
9. Select a Service Level.
10. Click **Apply.**

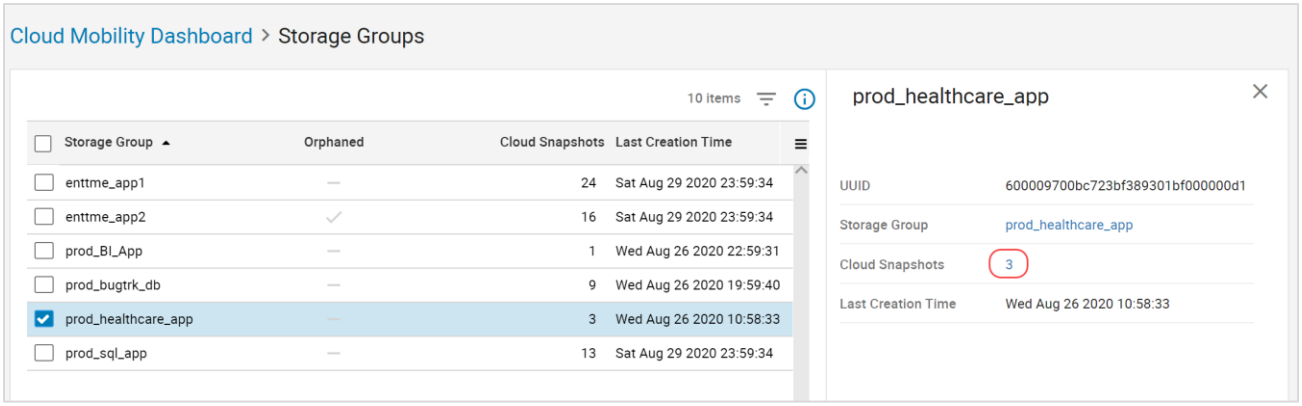


Figure 18 Cloud Storage Groups

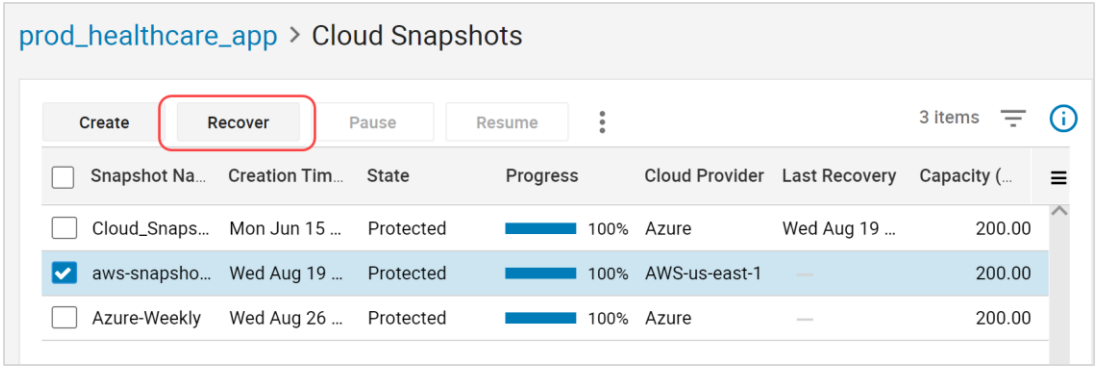


Figure 19 Storage Group Cloud Snapshots

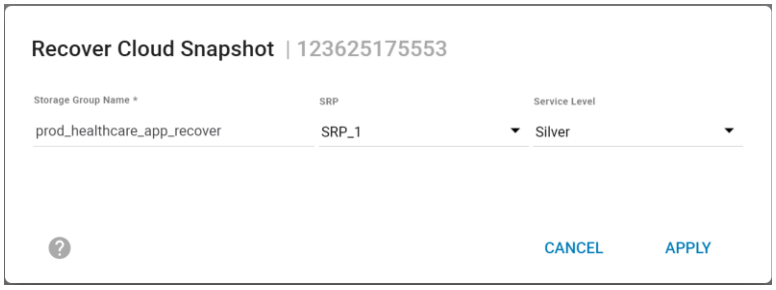


Figure 20 Recover Cloud Snapshot

2.8 Orphaned storage groups

When a storage group with cloud snapshots is deleted from the array, the cloud snapshots are preserved until their expiration date. These storage groups are then known as orphaned storage groups. They are visible in the Cloud Storage Groups page found from the Cloud Mobility Dashboard as seen in Figure 21.

The cloud snapshots of the orphaned storage groups can be recovered back to the original PowerMax or through the Dell EMC Cloud Mobility for Storage on AWS for the length of their retention dates. More details about Cloud Mobility for Storage and recovering data on AWS are found on page 28 and in the Cloud Mobility for Storage Guide.

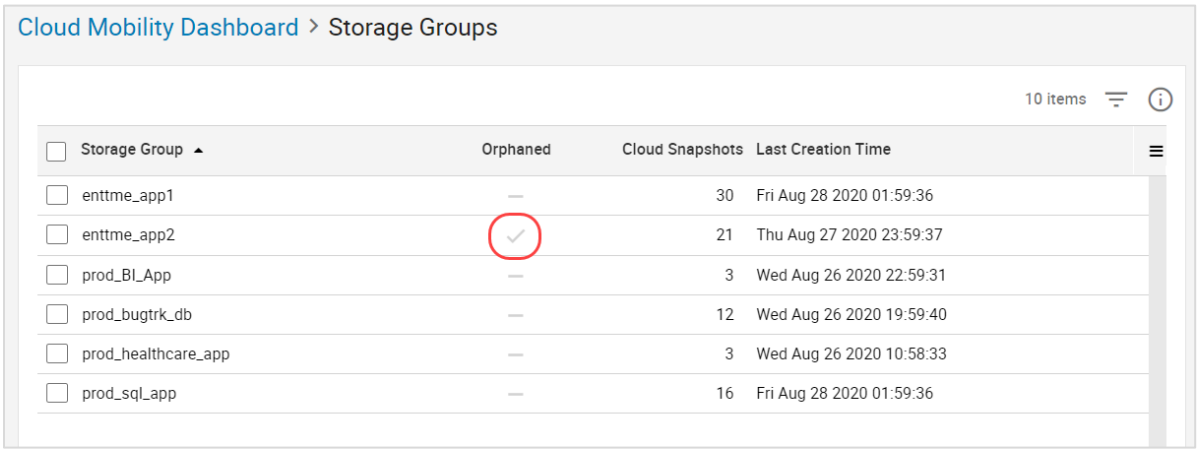


Figure 21 Orphaned Storage Group

3 Setup of Cloud Mobility for Dell EMC PowerMax

Cloud Mobility is configured by following the steps below:

1. NTP Server Verification
2. Setup Cloud System (Enrolling Unisphere for PowerMax with the cloud system and array registration)
3. Cloud System Network Setup Wizard (Interfaces, Routes, and DNS)
4. (Optional) Cloud Certificate Management
5. Setup Cloud Provider
6. Create Snapshot Policy for Cloud Provider
7. (Optional) Create additional Cloud Providers and policies
8. Assign Storage Groups to the Snapshot Policies
9. Enable alerts related to Snapshot Policies
10. (Optional) Set network Bandwidth Limits

3.1 NTP server verification

Prior to configuring the Cloud Mobility feature, the embedded Management and Cloud Mobility applications will need to have their system time synchronized to a Network Time Protocol (NTP) server. The maximum time drift allowed is a 5-minute difference between Cloud Mobility and the cloud providers. The NTP server is configured for both applications in the eManagement vApp Manager.

The NTP server IP address will be configured as part of the PowerMax and Cloud Mobility installation service. The steps below can be used to verify or modify the IP address of the NTP server.

Note: The NTP server should not be changed while snapshots are shipping or recovering. The Reset Config should not be used on systems with Cloud Mobility. To change NTP servers, use the Set Config function**.**

To display the current IP address of the NTP server being used, in the eManagement vApp Manager:

1. Go to **IP Configuration > NTP** click **Get Config** (the system default is 172.18.255.250).
2. To change the current value, type the new address in the text box and click **Set Config.**

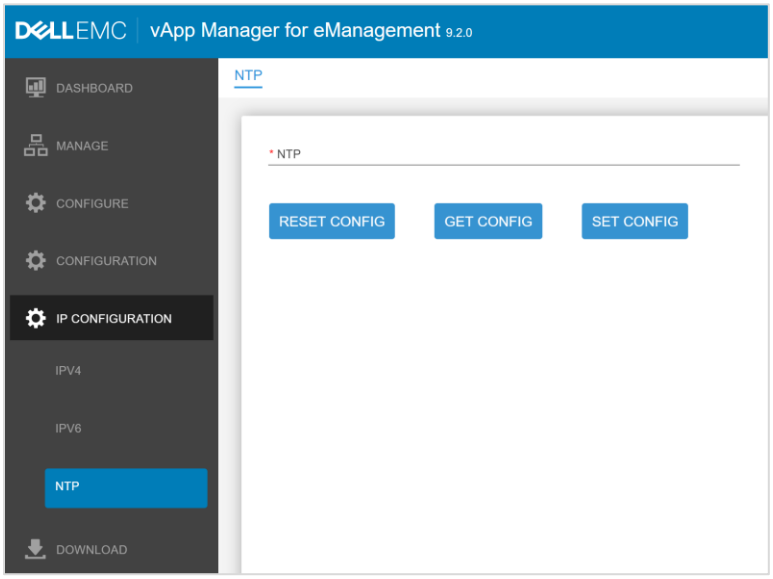


Figure 22 NTP Configuration in eManagement vApp Manager

Note: Changing the IP subnet after the Cloud system has been set up would require Dell Support engineering.

3.2 Set up cloud system

The initial setup of Cloud Mobility is performed with embedded Unisphere using the new Cloud Mobility Dashboard.

The Cloud Mobility Dashboard is available by navigating to **System > Cloud**.

The first time accessing the Cloud Dashboard, the cloud system will be in an unconfigured state and show the link for the Setup Cloud System wizard as shown in Figure 23.

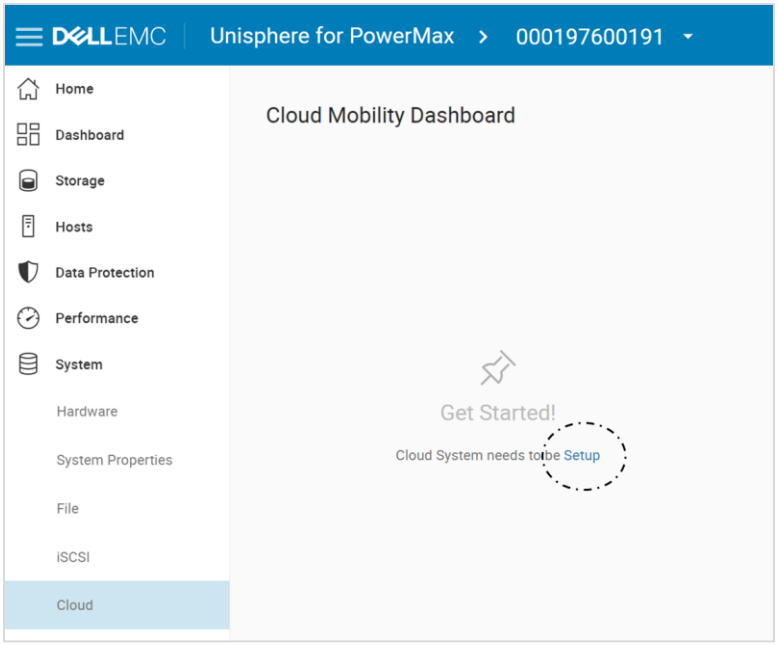


Figure 23 Cloud Mobility Dashboard > Setup

Click **Setup** to open the setup wizard.

Click **OK** on the confirmation window as shown in Figure 24.

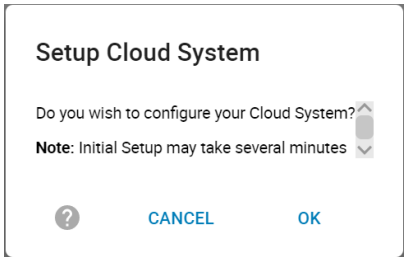


Figure 24 Setup confirmation

The setup wizard will enroll Unisphere with the cloud system and initiate array registration as part of the confirmation of setting up the cloud system.

Figure 25 shows the following tasks as part of the initial setup:

- Enroll Unisphere with Cloud System
- Register Unisphere and the Array on the Cloud System
- Register the Cloud environment into Solutions Enabler
- Synchronize the Cloud System Providers with SE Cloud Providers

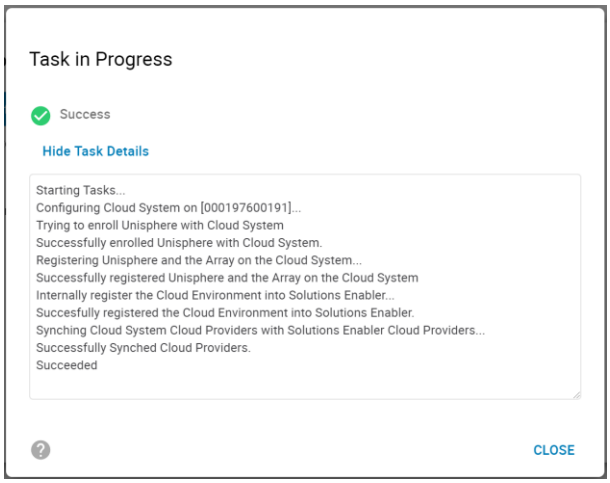


Figure 25 Setup cloud system tasks

Click **Close** to continue to the Setup Cloud System wizard.

3.3 Setup cloud system network

The Setup Cloud System prompts for the network interfaces, routes, and DNS configuration as shown in Figure 26.

Each port on the 4-port 10 GbE network I/O module can be configured as network interfaces individually or can be teamed together providing redundancy. NIC teaming may also be known as link aggregation or Ethernet bonding. The interface names eth1 to eth4 correspond to the I/O module ports 0 to 3, respectively.

The following are requirements for the cloud system network:

- Only IPv4 Interfaces are supported.
- Netmask Prefix Length value must be between 8 and 31 (an example prefix length of 24 would be equivalent to a subnet mask of 255.255.255.0).
- Only one default route can be configured for the cloud system.
- A maximum of three DNS servers can be configured.

After configuring network interface, routes, and DNS servers, review the details in the summary and click **Finish** to apply the settings. The wizard closes, and the Cloud Mobility Dashboard is displayed.

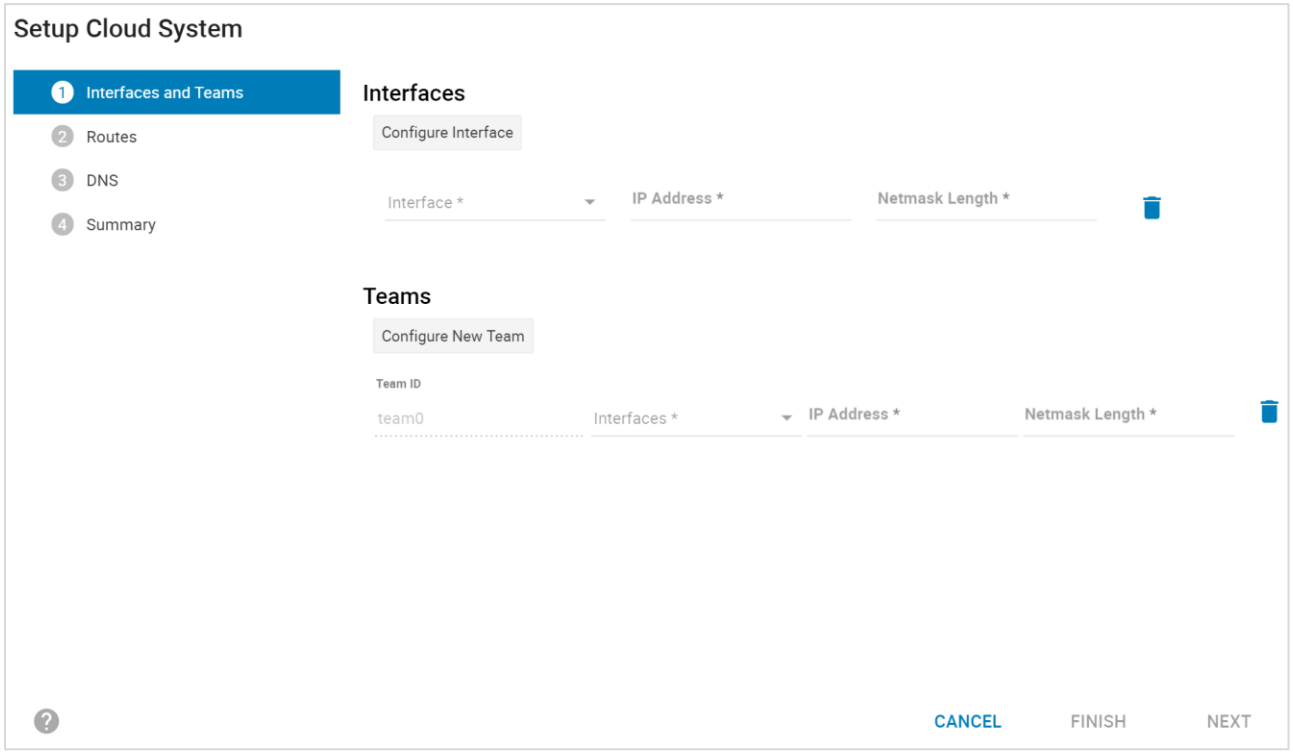


Figure 26 Setup Cloud System Wizard

4 Monitoring Cloud Mobility

Monitoring Cloud Mobility is performed with embedded Unisphere for PowerMax or REST API calls to the embedded Unisphere instance.

4.1 Cloud alerts in Unisphere

Alerts for Cloud Mobility can be enabled in the **Settings > Alerts > Alert Policies**.

Figure 27 displays some of the cloud mobility alerts. These alerts cover apply to cloud system health, cloud provider changes and status, and cloud snapshot shipping status.

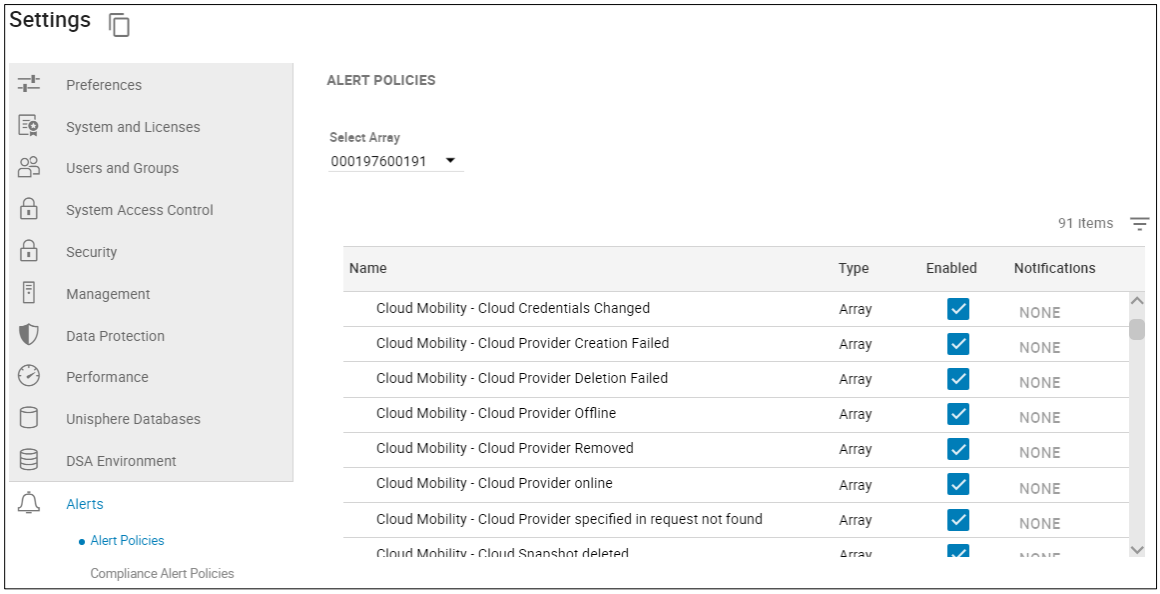


Figure 27 Cloud alert policies

4.2 Performance monitoring

A Cloud Provider performance dashboard is available showing metrics for each of the cloud providers. The dashboard can be made visible in the Dashboard Catalog found in **Settings > Performance > Dashboard Catalog** as seen in Figure 28.

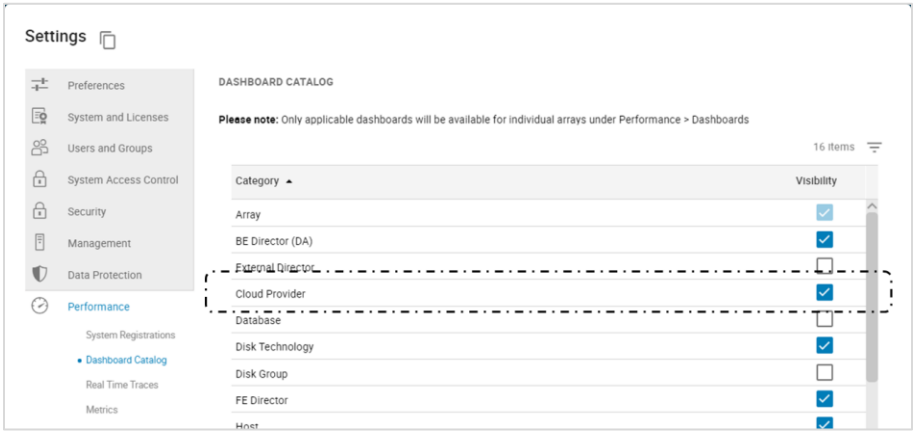
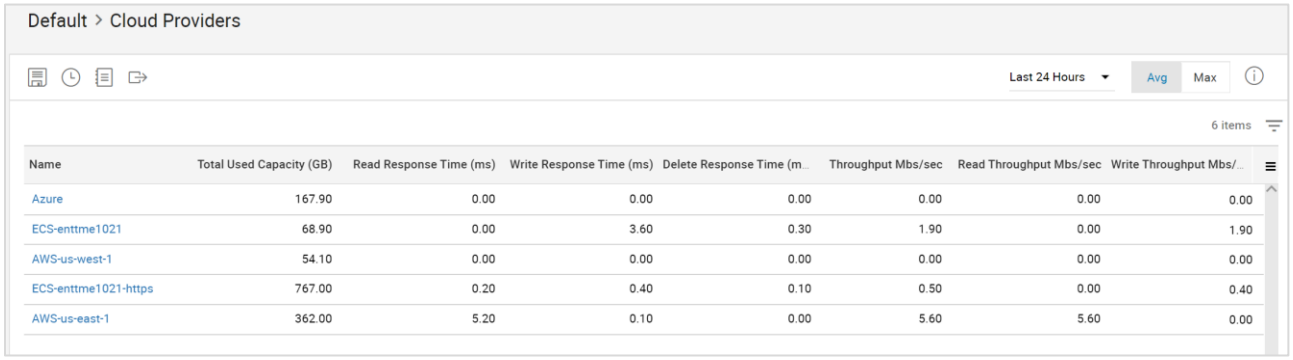


Figure 28 Performance Dashboard Catalog > Cloud Provider

The dashboard listing each of the cloud providers and the following metrics is found at **Performance > Dashboards > Cloud Providers** as seen in Figure 29.

- Total Used Capacity (GB)
- Read Response Time (ms)
- Write Response Time (ms)
- Delete Response Time (ms)
- Throughput Mbs/sec
- Read Throughput Mbs/sec
- Write Throughput Mbs/sec



Name	Total Used Capacity (GB)	Read Response Time (ms)	Write Response Time (ms)	Delete Response Time (m...	Throughput Mbs/sec	Read Throughput Mbs/sec	Write Throughput Mbs/...
Azure	167.90	0.00	0.00	0.00	0.00	0.00	0.00
ECS-enttme1021	68.90	0.00	3.60	0.30	1.90	0.00	1.90
AWS-us-west-1	54.10	0.00	0.00	0.00	0.00	0.00	0.00
ECS-enttme1021-https	767.00	0.20	0.40	0.10	0.50	0.00	0.40
AWS-us-east-1	362.00	5.20	0.10	0.00	5.60	5.60	0.00

Figure 29 Cloud Provider Performance Dashboard

Selecting a specific cloud provider opens a dashboard of charts displaying each of the performance metrics, as shown in Figure 30.

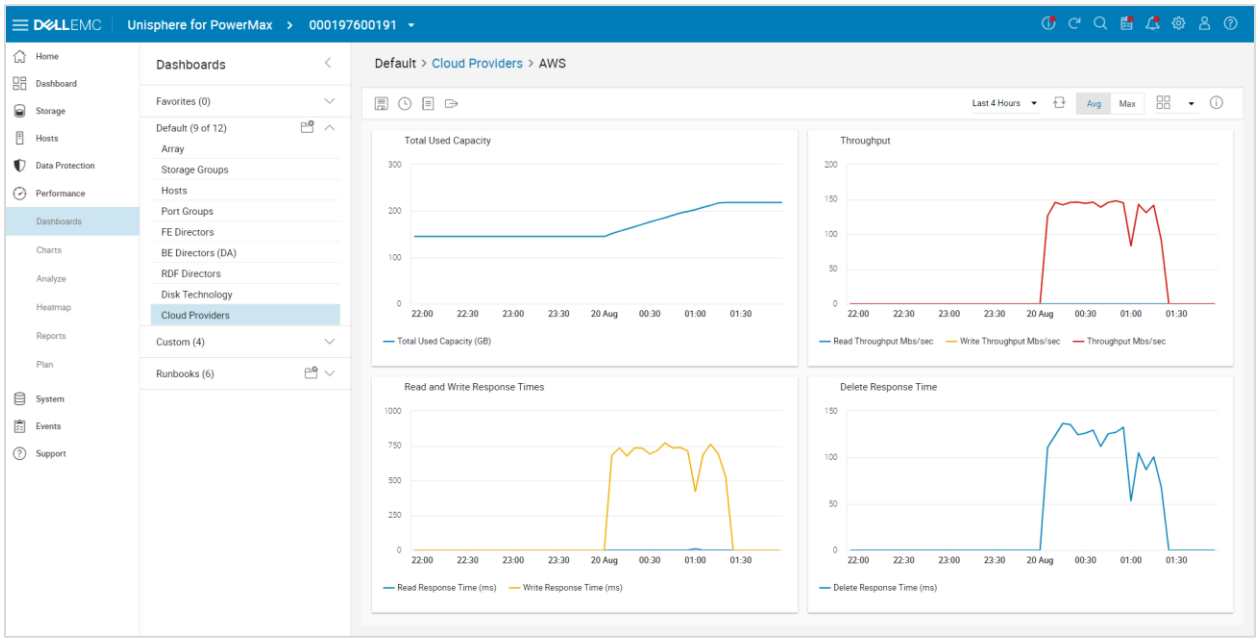


Figure 30 Cloud Provider Performance Dashboard Charts

5 Dell EMC Cloud Mobility for Storage (AWS machine image application)

Dell EMC Cloud Mobility for Storage enables you to view and analyze snapshots in the cloud and, when needed, move them back to your array with ease. 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. Once available to an operating system image, the snapshot images can be recovered to block storage in the cloud (for example, AWS Elastic Block Storage) for use cases such as storage analytics or reporting.

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.

For more details, see the Dell EMC Cloud Mobility for Storage Guide.

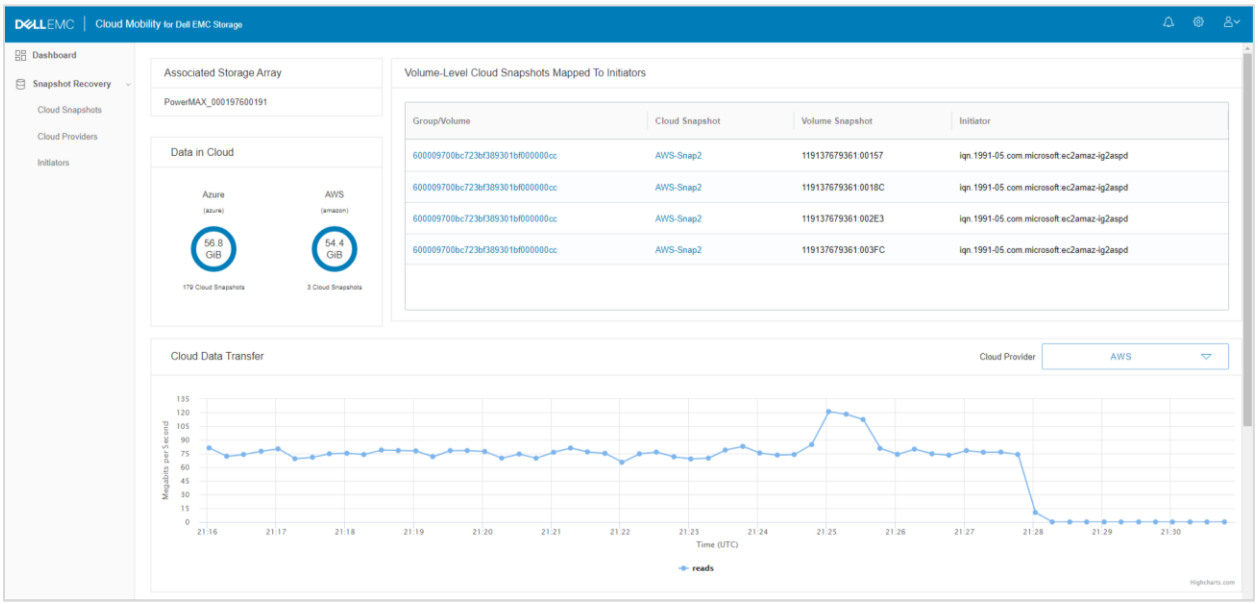


Figure 31 Dell EMC Cloud Mobility for Storage dashboard

A PowerMax hypervisor architecture

PowerMaxOS 5978 runs on the Dynamic Virtual Matrix leveraging its scale out flexibility of cores, cache, and host interfaces. The embedded storage hypervisor reduces external hardware and networking requirements, delivers high levels of availability, and dramatically reduces latency. Hypervisor upgrades are performed non-disruptively.

Within the PowerMax Hypervisor, virtual machines (VMs) provide the host platform that includes CPU processing, memory, network interface card (NIC), ports, data storage by using a Cut-Through Device (CTD), and external network through the Management Module Control Station (MMCS). VMs run within the front-end FA emulation.

Figure 32 shows the primary components of the PowerMax and Hypervisor.

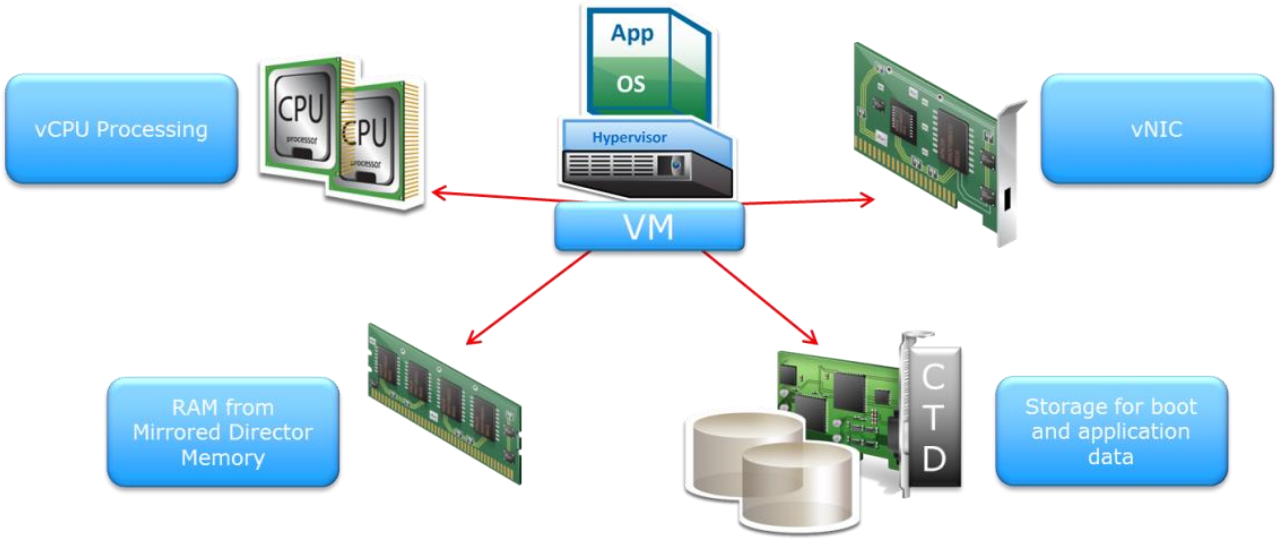


Figure 32 Hypervisor concepts: virtual machines

A.1 Hypervisor CPU core allocation: multicore emulation

Using the multicore emulation capability in PowerMax, the CPU processing is provided using CPU cores from the FA emulation. The cores are pooled for front-end, back-end, and for PowerMaxOS functions as shown in Figure 33. All the CPU cores on the director can work on I/O from all the ports. This helps ensure the directors' ports are always balanced.

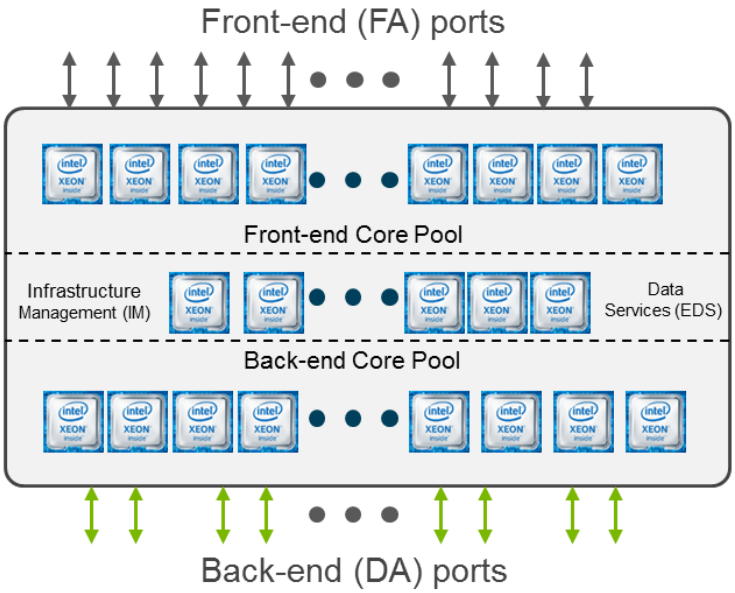


Figure 33 PowerMax multicore emulation

A.2 Hypervisor memory allocation

Memory is allocated to the hypervisor from the director cache during the initial setup as shown in Figure 34. This memory is then allocated to each Virtual Machine (VM) on that director for the purpose of embedded applications. The amount of memory allocated to a VM depends on the type of application, for example Cloud Mobility and Embedded Management.

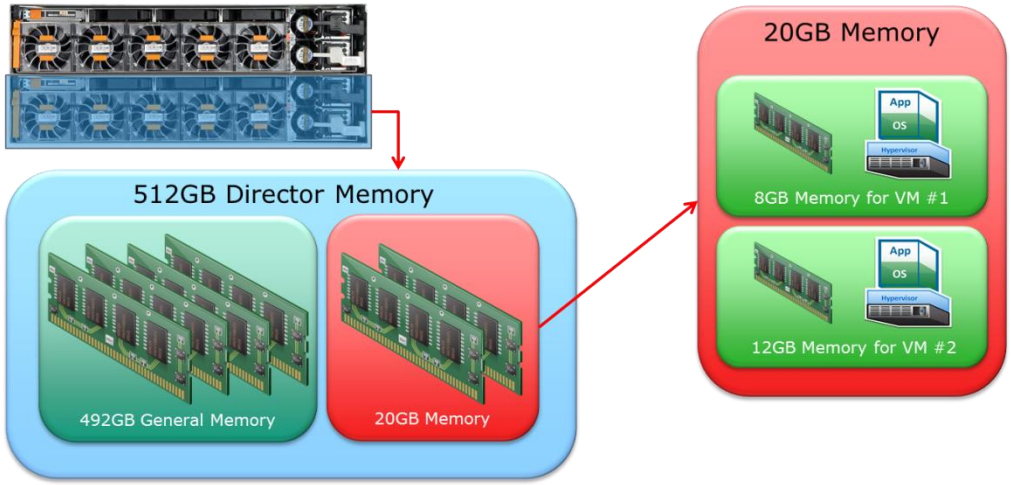


Figure 34 Hypervisor memory allocation

A.3 Hypervisor storage allocation: cut-through device

Data storage for both the boot and application data is provided using a cut-through device (CTD) as shown in Figure 35, which acts like an HBA that accesses LUNs in the PowerMax. The CTD has two components to enable access to the LUNs through an FA port. The first is the CTD Server thread. This runs on the FA emulation and communicates with the CTD Client in the embedded operating system. The second is the CTD Client Driver. The CTD Client Driver is embedded in the host operating system and communicates with the CTD server running on the FA emulation. An operating system running in a VM must have the CTD client driver installed to access the LUNs.

Embedded application ports are virtual ports specifically provided for use by the VMs that contain the applications, such as Cloud Mobility. They are addressed as ports 32 to 63 per director FA emulation. The virtual ports are provided to avoid contention with physical connectivity. As with physical ports, LUNs can be provisioned to the virtual ports.

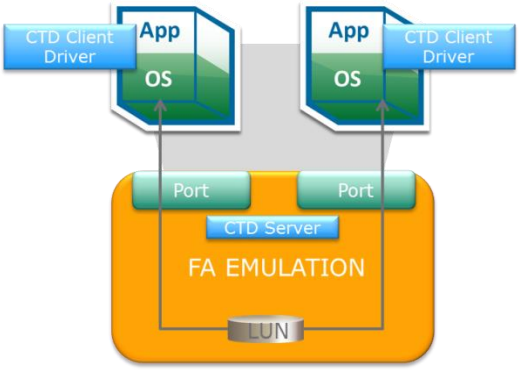


Figure 35 Cut-through device (CTD)

A.4 Hypervisor network connectivity

Network connectivity for the VMs is provided by a virtual NIC (vNIC). The vNIC is connected to the internal network providing communication to PowerMaxOS and other VM instances. The VM management external network connectivity is provided through a PowerMaxOS component called the network address translation (NAT) Gateway which is part of the Infrastructure Manager (IM) emulation. The NAT Gateway provides translation services between external and internal IP addresses and uses a separate network connection on each of the two Management Module Control Stations (MMCS). A PowerMax with eManagement and ESRS connectivity would then require a total of four physical network connections and four IP addresses. More IP addresses would be required if Embedded NAS is also configured. Management of Cloud Mobility is strictly performed through the eManagement in Unisphere and does not require any management IP addresses.

B REST API examples

To help setup and manage Cloud Mobility using the REST API, Unisphere 9.2 adds new endpoints that manage cloud providers, networking, cloud snapshots, and more. The most recent PowerMax REST documentation can found by going to your embedded management instance of Unisphere for PowerMax at:

https://{ip-address|hostname}:8443/univmax/restapi/docs

The versioned calls are under the new branch of the API at the following URL:

https://{ip-address|hostname}:8443/univmax/restapi/restapi/92/

Note: The Dell EMC REST API officially supports up to three versions of the API in a release of Unisphere with N-2 version support. Version 9.2 supports API versions 9.2, 9.1, and 9.0. When Unisphere is upgraded, REST API continues to work the same. However, newer versions of a call may provide extra functionality. Check the REST API change log available on Dell.com/support.

Create a Cloud Provider REST API (POST): Cloud providers can also be viewed or modified with REST GET and PUT calls under https://{ipaddress|hostname}:8443/univmax/restapi/92/system/symmetrix/{symmetrixId}/cloud/cloudprovider/{cloud_provider_id} calls. Figure 36 shows an example to create an ECS cloud provider and Figure 37 shows the details of a cloud provider.

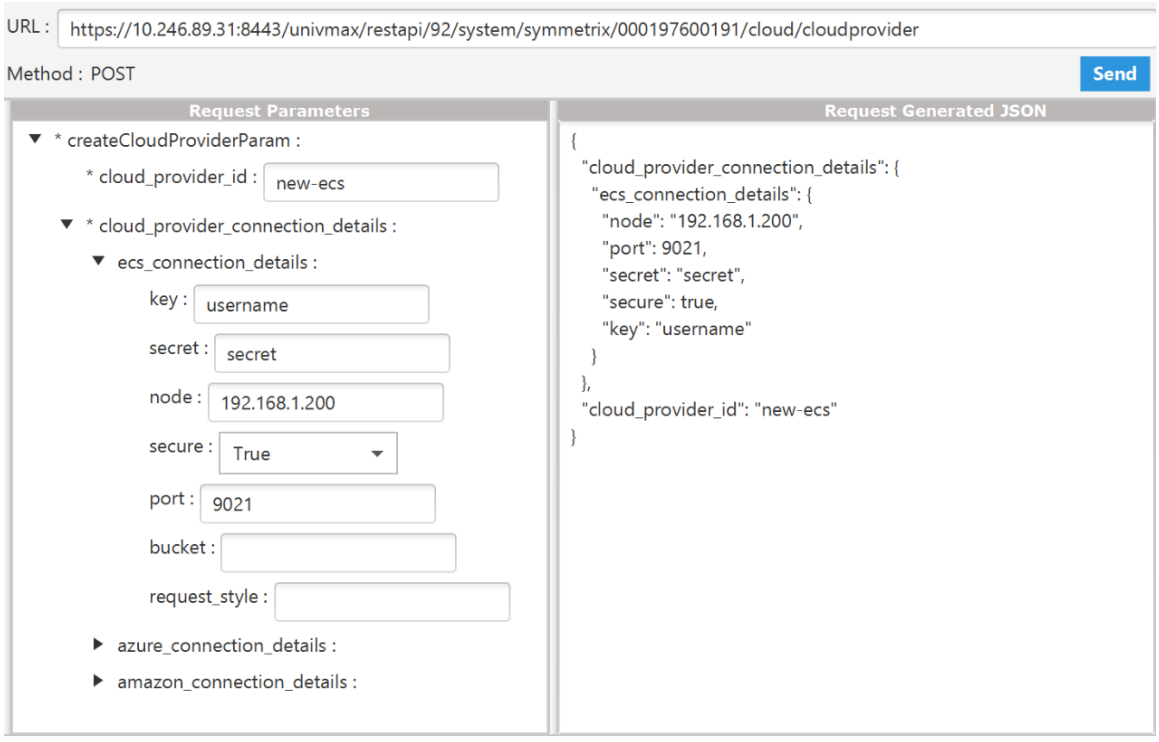


Figure 36 REST API: Create Cloud Provider

Figure 37 REST API: View Cloud Provider Details

Create an On-Demand Cloud Snapshot REST API (POST): Cloud snapshots can be created, modified, or viewed with REST POST, DELETE, LIST, or GET calls under https://{ipaddress|hostname}:8443/univmax/restapi/92/replication/symmetrix/{symmetrixId}/storagegroup/{storageGroupId}/cloudsnapshot Figure 38 shows an example of creating a cloud snapshot for a storage group that will expire in 30 days.

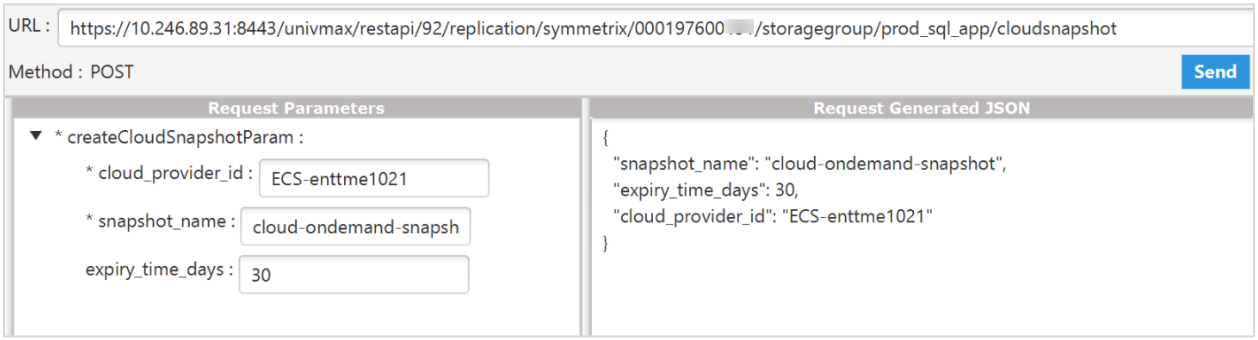


Figure 38 REST API: Create Cloud Snapshot

C Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage and data protection technical white papers and videos provide expertise that helps to ensure customer success with Dell EMC storage and data protection storage products.

C.1 Related resources

- Dell EMC Cloud Mobility for Storage Guide
- Dell EMC PowerMax and VMAX All Flash: Snapshot Policies
- Dell EMC PowerMax Family Overview
- TimeFinder SNAPVX Local Replication
- Frequently Asked Questions about TimeFinder SnapVX on VMAX All Flash Arrays
- Dell EMC PowerMax and VMAX All Flash: Embedded Management
- Dell EMC PowerMax: Reliability, Availability, and Serviceability