Technical White Paper

Dell EMC PowerProtect Cloud Snapshot Manager: Architecture and Security

Abstract

This document provides an overview of the architecture and security features of Dell EMC's PowerProtect Cloud Snapshot Manager

February 2021

Revisions

Date	Description
September 2019	Initial release
June 2020	Included new security features pertaining to AWS and Role Based Access Control
January 2021	Included cross region support for Azure
February 2021	CSM Integration with DDVE in AWS

Acknowledgments

Author: Parimala Guruprasad

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third party content is updated by the relevant third parties, this document will be revised accordingly.

Table of Contents

Revisions....2
Acknowledgments....2
Table of Contents....3
1 Introduction....4
1.1 PowerProtect Cloud Snapshot Manager....4
1.2 Features....4
2 Architecture....5
2.1 Overall CSM Architecture....5
2.2 Copy Snapshots to DDVE in AWS to reduce storage costs....7
3 Security....10
3.1 CSM Access to the customer's cloud accounts....10
3.2 Federated Identification....10
3.3 Role Based Access Control....11
3.4 Expanded Security with Copying Snapshots to a Restricted Account....11
4 Conclusion....12
A Technical support and resources....13
A.1 Related resources....13

1 Introduction

1.1 PowerProtect Cloud Snapshot Manager

Dell EMC PowerProtect Cloud Snapshot Manager (CSM) is an enterprise-grade Software-as-a-Service (SaaS) solution that makes it easy for customers to protect workloads in public cloud environments (AWS, Azure). CSM leverages the underlying snapshot technology of the cloud providers – without requiring installation or infrastructure. Customers can discover, orchestrate and automate the protection of workloads across multiple clouds based on policies for seamless backup, compliance and disaster recovery from a single pane of glass. CSM supports secure multitenancy.

1.2 Features

- Policy based creation and deletion of snapshots for AWS and Azure
- Protection across many cloud accounts and regions
- Replication and restore of snapshots across regions for disaster recovery
- Replication and restore of snapshots across accounts in AWS for disaster recovery and enhanced security
- Discovery of existing snapshots in AWS for better control over snapshot sprawl
- Tag based protection policy assignment to resources in AWS and Azure
- Support for Federated Identification with Security Assertion Mark-up Language (SAML) to enable Single sign-on *(*SSO)
- Role Based Access Control to help enterprises restrict access to authorized administrators and assign specific level of privileges to different roles
- Copy snapshots to PowerProtect DDVE in AWS to retain them for a longer period
- Application Consistency backups using pre and post scripts
- Extensive data sources:
  - AWS: EC2, EBS volumes, RDS Database, Aurora, Redshift, DynamoDB
  - Azure: VMs with managed disks and Blob storage containers
- One-click restore of one or a group of resources with its configuration
- File Level Recovery (FLR) capabilities for AWS and Azure resources
- Group restore of multiple VMs
- Auto scale to protect thousands of resources across multiple cloud providers
- Audit logging, secure multi-tenancy, and automated reports
- Extensive REST API support

2 Architecture

2.1 Overall CSM Architecture

CSM leverages the cloud providers' (AWS and Azure) existing snapshot technology to protect workloads in the cloud. More enterprises want to use native snapshots for data protection over traditional backups because it provides faster backups and restores. While snapshot capabilities exist in the cloud, they are not automated and need to be manually managed. As a result, they are typically managed and run using scripts and homegrown tools.

The lack of snapshot automation and management results in snapshot proliferation, which quickly becomes expensive and cumbersome to manage. It also adds complexity to the recovery process because users find it difficult to identify the "right" snapshot to recover, among so many snapshots. These challenges exist in single cloud instances, and when an organization goes multi-cloud it exacerbates the problems.

CSM solves this problem by orchestrating and managing snapshot creation and deletion per policy across multiple clouds, multiple accounts and regions through a single pane of glass.

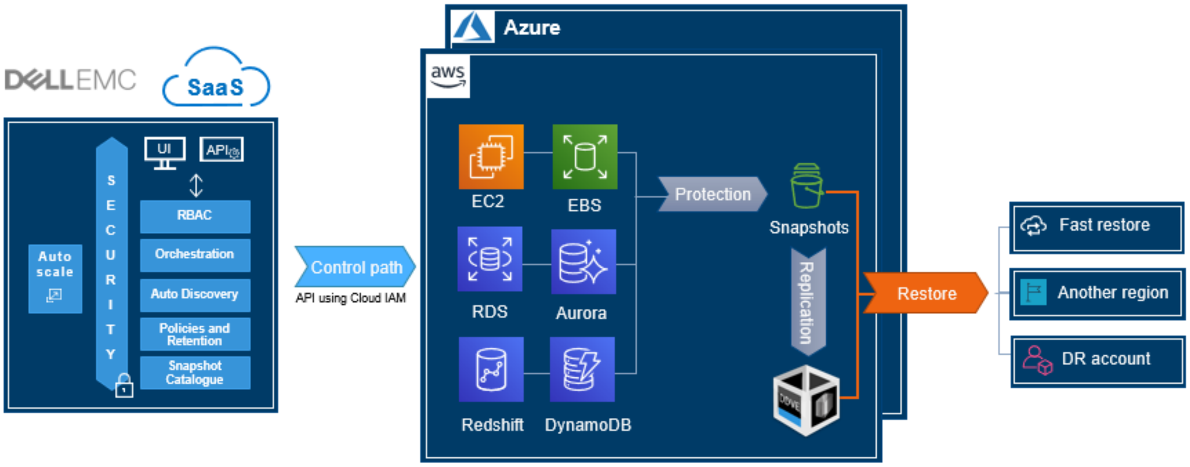


Figure 1 Cloud Snapshot Management for AWS

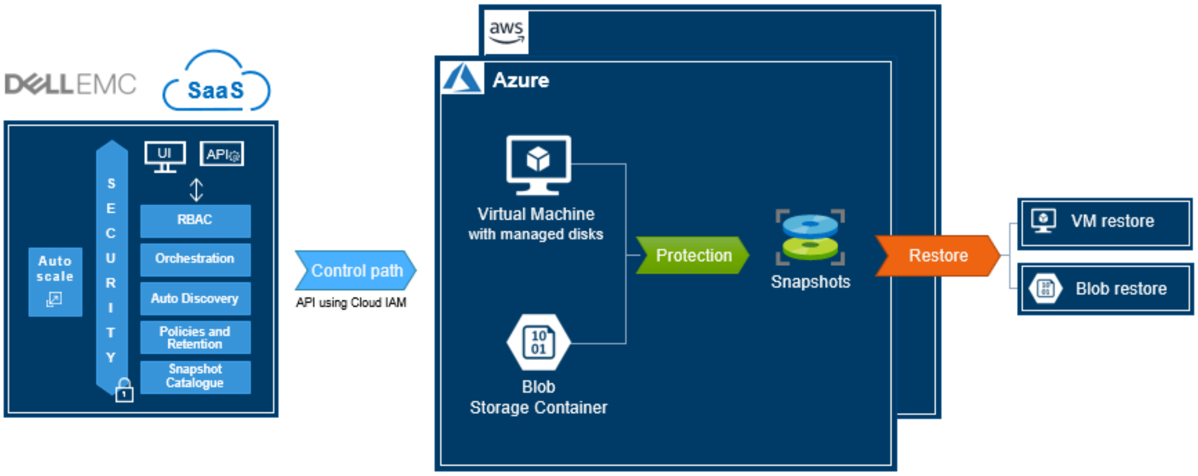


Figure 2 Cloud Snapshot Management for Azure

CSM uses the REST APIs provided by the cloud providers to accomplish tasks like instance discovery, creation, deletion and restoration of snapshots. CSM automates the creation of snapshots through Protection Policies. When the protection policy is run, snapshot creation is triggered for the cloud resources attached to the policy. AWS creates the snapshot of the specified EC2 instance, EBS volumes and RDS databases and stores these snapshots in a special snapshot bucket in S3. This helps separate the copy of the protected data from the primary data. Azure creates snapshots of the Managed Disks and stores the snapshot in the low cost Locally Redundant Storage (LRS).

For AWS, CSM allows copying of snapshots to a different region or a different account other than the region or account where the cloud resources are located for disaster recovery. If the original region snapshot is encrypted, the copied snapshot is encrypted with the AWS default encryption key for the targeted remote region. CSM also enables the users to configure custom encryption keys instead of using the default encryption key.

CSM also helps protect VMs against security attacks and breaches in the customers' AWS accounts. CSM provides disaster recovery by enabling snapshots to be copied to a restricted account in AWS. Snapshots copied across accounts are full backups and therefore, can be restored to the original account or a different AWS account.

For Azure, CSM allows copying snapshots to remote or cross-regions, hence enabling quick recovery of protected VMs in other regions. CSM supports the use of both Disk level encryption (Managed Disk Server-Side Encryption with Customer Managed Keys) and Operating System level encryption (Azure Disk Encryption (ADE)) for copy and restore of snapshots across regions.

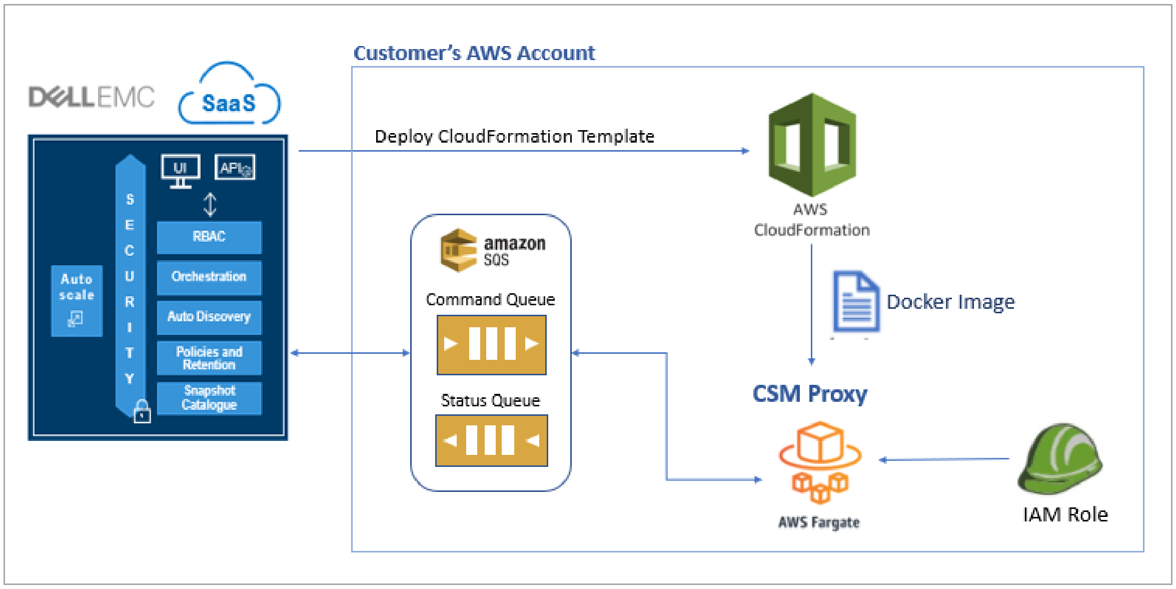
2.2 Copy Snapshots to DDVE in AWS to reduce storage costs

Cloud Snapshot Manager supports integration with PowerProtect Data Domain Virtual Edition (DDVE) deployed in AWS. This feature enables saving copies of snapshots to S3 for a longer duration. By leveraging the high-speed, variable length industry-leading deduplication capability of Data Domain Series, the snapshot storage costs are highly reduced.

This solution uses CSM Proxy to enable data transfer to and from the DDVE on AWS. CSM Proxy acts as a data mover enabling

- Replicating snapshots to DDVE
- Restoring snapshots from DDVE
- Deleting expired snapshot copies from DDVE.

CSM Proxy is a container instance created by CSM using AWS Fargate. CSM Proxy is ephemeral and is created on-demand by CSM during data transfer and is cleaned up by CSM after use thereby minimizing costs.



CSM uses AWS CloudFormation Stack to orchestrate the creation of the container instance (CSM Proxy). CSM uses the AWS ECS for the container. The container is created off a Docker image that is hosted on docker.io.

CSM also uses AWS SQS, to communicate with the CSM services hosted in the Dell Data Center. AWS SDK interfaces are used to create/delete the queues and send/receive messages. The communication with AWS SQS service happens over HTTPS protocol. CSM internally uses 2 queues:

- Command Queue – Used by CSM services to send commands to the CSM Proxy. Ex. Start copying snapshots to DDVE, retrieve snapshots from DDVE, delete expired snapshots from DDVE.
- Status Queue - Used by the CSM proxy will send the status of the jobs back to CSM services

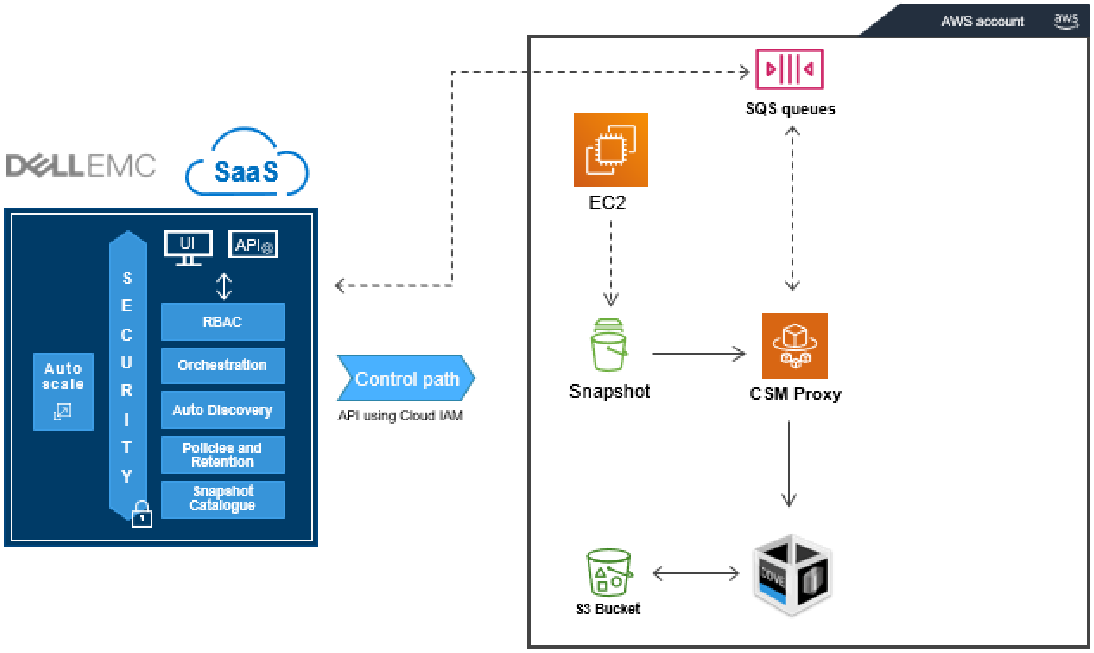
These two queues are created by the CSM copy engine and are associated to the CSM Proxy that is has been created. The queues are removed as soon as the data movement is completed and the CSM Proxy is torn down. The Fargate container is granted permission to access these queues through the role assigned to it during its creation.

To enable this communication between the Proxy and CSM services, the subnet should either be a public or a private one with Network Address Translation (NAT) for access to internet.

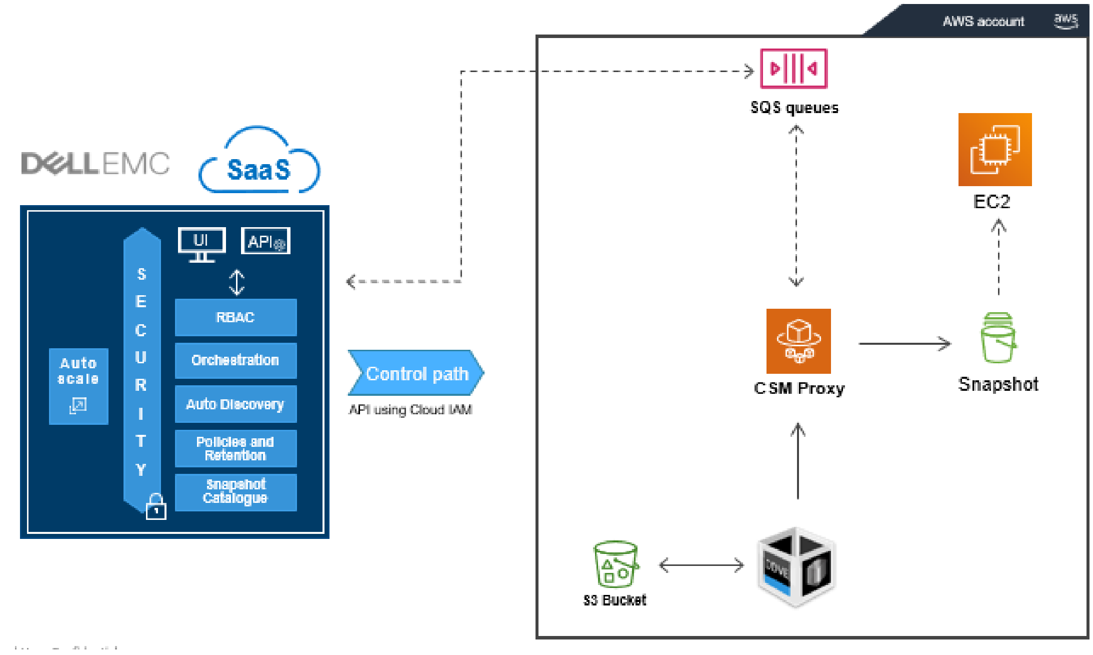
An IAM role is attached to the container. Through the IAM role, the container will be granted minimum permissions required to access EBS to list and get snapshot blocks and to SQS to send and receive messages. With IAM role, the container doesn't require AWS credentials to be passed to it to perform the necessary operations.

For the permissions required to enable integration between CSM and DDVE, refer to AWS Permission Policy.

For replication to DDVE, the CSM Proxy is created in the cloud account and region where the snapshot to be copied is present.



Likewise, the Proxy is created in the cloud account and the region where data is to be restored, in case of a recovery scenario.



The CSM proxy requires the VPC and subnet details for its configuration during creation. So, it is required that a VPC and Subnet is configured per region for each AWS cloud account.

Topologies supported:

1. DDVE and CSM Proxy in the same VPC but different subnets
2. DDVE and CSM Proxy in different VPCs but in the same region and cloud account
3. DDVE and CSM Proxy in different VPCs and regions but the same cloud account
4. DDVE and CSM Proxy in different VPCs, regions, and cloud accounts

For topologies with the Proxy and DDVE in different VPCs, VPC peering, if required, should be set-up by the customers. CSM uses secure VPC peering to transfer data to/from DDVE.

DDVE details required by CSM:

- Cloud account and region where DDVE is deployed
- The VPC and subnet details where DDVE is deployed
- IP address or FQDN of DDVE
- DDVE administrator username and password
- DDVE Storage Unit (STU) username and password
- Default DDVE TCP Port 3009 to be open. For details on DDVE, refer to PowerProtect DD Virtual Edition on Amazon Web Services - Installation and Administration Guide

The DDVE admin user is used to collect DDVE metadata required for this integration. The Storage Unit credentials are used to read and write data into the STU. These credentials are kept secure by encryption with AES256 algorithm.

Replicating of snapshot copies to DDVE can be scheduled in CSM. CSM allows the user to specify the frequency at which snapshots are to be copied to DDVE and the retention time for these copies. DDVE snapshots can be restored to the same cloud account and region or a different cloud account and region.

3 Security

CSM is hosted in secured Dell EMC IT infrastructure and provides secure multitenancy. Dell has implemented corporate information security practices and standards that are designed to safeguard the Dell corporate environment and to address: (1) information security; (2) system and asset management; (3) development; and (4) governance. These practices and standards are approved by the Dell CIO and undergo a formal review on an annual basis. Dell has a formalized risk management program and processes that focus on continuous improvement. Where applicable to Dell business, Dell Cybersecurity performs on-going risk reviews and assessments for the continuous improvement of Dell's information security. Dell policies and standards are reviewed on an annual basis.

Dell EMC conducts security assessment of Cloud Snapshot Management regularly to assess and fix any vulnerabilities if detected. Detailed threat modeling helps proactively identify potential issues and fix them before they become an issue.

Users' cloud account credentials required by CSM are protected using AES 256-bit encryption.

3.1 CSM Access to the customer's cloud accounts

CSM discovers and protects resources in AWS or Azure by using the minimal set of permissions to enable discovery, instance protection, and recovery. To provide CSM, access to the cloud accounts, the user should create either a role with permissions described in an Identity Access Management (IAM) policy or a user for AWS or cloud accounts using custom roles for Azure. The minimum permissions that CSM requires to function are provided in the Online Help in CSM – AWS permission policy and Azure custom role permissions.

CSM orchestrates the creation and deletion of snapshots by using the cloud providers' native APIs. AWS or Azure remains the custodian of the data.

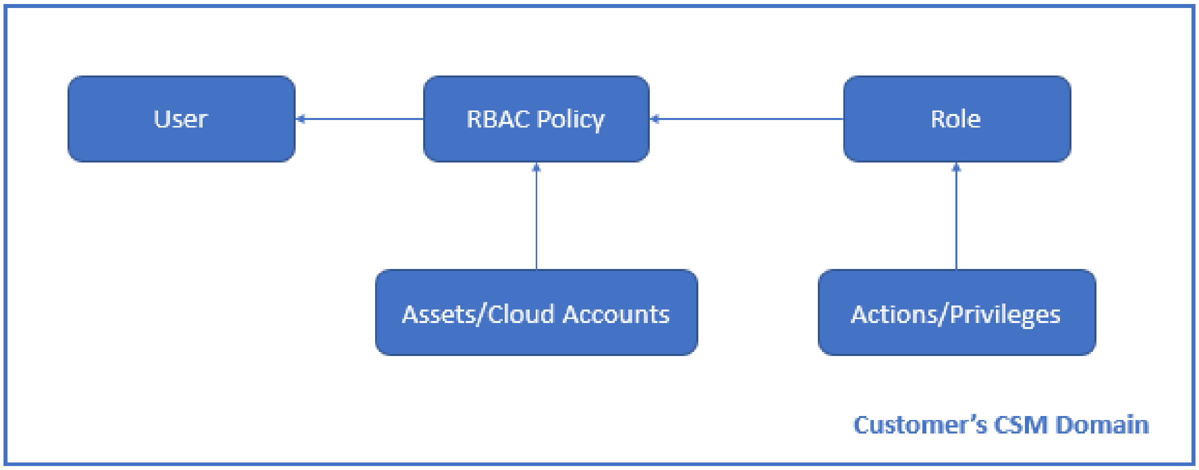
CSM communicates securely with the cloud providers through REST API calls made over HTTPS. The encryption protocol used is TLS 1.2/1.3. CSM uses secure SHA-256 with RSA-2048 encryption for secure transmission of data.

3.2 Federated Identification

CSM also supports **Login through Federated Identity** with Security Assertion Markup Language (SAML) authentication for enterprises to enable SSO. With this option, individual users within an enterprise need not have their Dell accounts created. The users within the enterprise are authenticated by their enterprise Identity Provider (IdP). This feature provides additional security at multiple levels. First, the employees who leave the company are removed from their enterprise Identity Provider and will lose access to CSM immediately. Second, if an enterprise has multifactor authentication policy, the same will be enforced when logging in to CSM. Setup of FedID for an organization can be initiated by contacting Dell support through the Support option in the Help section of Cloud Snapshot Manager. Then, IdP metadata with valid signed certificate and user details from the organization that requires federated authentication and the Service Provider (SP) metadata from Dell EMC is exchanged. Dell EMC and the concerned organization test this configuration and the customer is all set for federated authentication.

3.3 Role Based Access Control

CSM includes Role Based Access Control (RBAC) to restrict access to the customer's CSM account to authorized users. CSM RBAC enables protection of resources across both AWS and Azure securely through a common set of RBAC policies. A super administrator in CSM creates roles, each with privileges to perform a certain set of actions like viewing resources, viewing jobs, generating reports and creating on-demand snapshots. RBAC policies tie these roles to one or more cloud accounts that have already been set up in CSM. All users in CSM are then assigned an appropriate RBAC policy. This process ensures that the super admin has control over what actions the users are authorized to perform and what resources they have access to.



With RBAC capabilities, along with Federated Identification, CSM provides comprehensive and secure Identity Access Management ensuring that enterprises have the security and control to meet their regulatory and compliance requirements.

3.4 Expanded Security with Copying Snapshots to a Restricted Account

CSM has expanded its capability to address the security concerns customers have regarding deletion of backups either by malicious attacks or internal security breaches. CSM supports copying snapshots from primary AWS accounts to another AWS account configured using IAM policies that has restricted access. This feature helps customers protect their data if there is a security breach in their original account, as an isolated copy of the snapshot is available in another account for recovery. CSM also enables customers to control cleanup of snapshots in the restricted account by either allowing CSM to automatically delete expired snapshots or by opting to run a lambda script from within the restricted account for added safeguarding.

4 Conclusion

PowerProtect Cloud Snapshot Manager provides seamless management of snapshots across multiple clouds (AWS and Azure) through a single pane of glass. Dell EMC takes security seriously. CSM is hosted in secure Dell EMC infrastructure, ensures secure multitenancy and protects user’s cloud account credentials with multiple levels of encryption. With enhanced features like Role Based Access Control, federated identification, secured cross-region (AWS and Azure) and cross-account replication (AWS only) of snapshots for disaster recovery and LTR to DDVE in AWS, CSM helps enterprises have the security and control to meet their regulatory and compliance standards.

A 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 products.

A.1 Related resources

- Dell EMC PowerProtect Cloud Snapshot Manager
- Dell EMC PowerProtect Cloud Snapshot Manager – Getting Started Guide