Release Notes

Dell PowerProtect Cloud Snapshot Manager

Release Notes

Rev. 38

October 2024

These release notes contain supplemental information. Topics include:

Introduction

PowerProtect Cloud Snapshot Manager (CSM) is a Software-as-a-Service (SaaS) solution for backup and disaster recovery of cloud workloads, enabling organizations to manage and protect application data in AWS, Azure and GCP cloud environments seamlessly without requiring installation or infrastructure.

AWS, Azure and GCP users can discover instances and automate native application consistent snapshots across multiple cloud accounts and regions that are based on policies.

This document provides a summary of all new features, resolved issues, and known issues in various PowerProtect Cloud Snapshot Manager releases. For details about the documents available for the latest release of PowerProtect Cloud Snapshot Manager and for support information, go to the Support page.

Release for October 23, 2024

Learn about new and changed features in this release of Cloud Snapshot Manager

Changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

AWS accounts configured to use old trusted account number becomes nonoperational

Cloud Snapshot Manager has moved to a new trusted account number for creating AWS Role-Based accounts. You must migrate AWS cloud accounts to use new trusted account number. For more information, see Steps to migrate to a new AWS-Trusted Account in PowerProtect Cloud Management Software. Failing to migrate results in operation failures for such AWS cloud accounts.

Update to AWS permissions for ECS resources

Amazon ECS introduced tagging authorization for creating resource on April 18, 2023. This security control empowers AWS customers to deny or allow tagging of ECS resources when they are created. To prevent service interruption, you must update your AWS IAM policies to explicitly allow the `ecs:TagResource` action. If you have not updated your AWS Identity and Access Management (IAM) policy to grant explicit `ecs:TagResource` permissions, you will experience interruptions in your workloads that rely on the ability to tag ECS resources during creation. Failure in updating IAM policy results in failure of DDVE-related operations.

```
{
 "Sid": "AllowTagging",
 "Effect": "Allow",
 "Action":[
 "ecs:TagResource"
 ],
 "Resource":"*"
 }
```

For more information, see AWS minimum permissions.

Fixed Issues

Learn about the following fixed issues in this release of Cloud Snapshot Manager.

GET Snapshots REST API call is not returning the expected output

Unique values are returned for fields **id** and **created_time**.

Azure cross-region snapshot job fails when VM disk is resized

Cloud Snapshot Manager performs full snapshot instead of incremental if Azure fails to do incremental snapshot on resized disk.

Aurora database backup fails for large database size

Cloud Snapshot Manager uses **DurationSeconds** parameter when calling `IAM:AssumeRole` operation for generating temporary credentials.

Customer can edit IAM Role (Default 1 hour and Maximum 12 hours) to increase value for **Maximum session duration**.

Unable to activate full license

A new license can be activated.

VSS App consistent snapshot job fails for Azure Cloud

Provide an appropriate script for VSS App consistent snapshots.

Aurora protection plan job fails when Aurora instances are created using Cloud Formation Stack

Protection Plan Run and On-Demand Snapshot operation succeeds for Aurora instances that are created using Cloud Formation Stack.

Duplicate expiry jobs created for single snapshot

Cloud Snapshot Manager prevents creation of duplicate job for snapshot if the earlier expiry job is not finished.

Expiry operation fails with throttling error

Cloud Snapshot Manager avoids unnecessary cloud API calls to limit API throttling.

Known Issues

Learn about the following known issues in this release of Cloud Snapshot Manager and get acknowledged on how to work around them.

Protection plans run simultaneously regardless of daylight saving

Protection plans do not consider daylight saving time while running jobs.

Release for June 26, 2024

Learn about new and changed features in this release of Cloud Snapshot Manager

Fixed Issues

Learn about the following fixed issues in this release of Cloud Snapshot Manager.

Container instance memory is configurable to address the SCBT issue

The container instance memory size is now configurable according to requirements. You can configure the 1 GB default memory depending on use cases.

ⓘ **NOTE:** Permission for this configuration is granted to the Cloud Snapshot Manager admin team only.

Azure App Consistent Snapshot Mechanism improvement

Optimized azure app consistent snapshot of large disk VMs using resource-based and tag-based protection plans in comparison to the existing mechanism.

Fixed an error message `csm-proxy-configuration not found` in the SCBT expiry process

The DDVE expiry code workflow has been enhanced to fix the DDVE expiry-related errors.

Known Issues

Learn about the following known issues in this release of Cloud Snapshot Manager and get acknowledged on how to work around them.

Protection plans run simultaneously regardless of daylight saving

Protection plans do not consider daylight saving time while running jobs.

Release for February 27, 2024

Learn about new and changed features in this release of Cloud Snapshot Manager.

Fixed Issues

Learn about the issues that have been fixed in this release of Cloud Snapshot Manager.

False failure events generated for all the resources in the protection plan

If the cross-region native snapshot fails, event is generated only for the failed resources attached to the protection plan.

Unprotected resource report gives error - Error encountered while processing the request

A scheduled report is generated for each **unprotected resources** resource type.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Protection plans should run at the same time regardless of daylight saving

Protection plans will not consider daylight savings time while running jobs.

Release for November 01, 2023

Learn about new and changed features in this release of Cloud Snapshot Manager.

Fixed Issues

Learn about the issues that have been fixed in this release of Cloud Snapshot Manager.

Unable to create RBAC policy by selecting specific cloud account

You can create an RBAC policy by selecting a specific cloud account.

Cross region snapshot failure not reporting as an event in Cloud Snapshot Manager

Cloud Snapshot Manager generates an event if Cross region native snapshot operation fails.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Protection plans should run simultaneously regardless of daylight saving

Protection plans do not consider daylight savings time while running jobs.

Unprotected resource report gives error - Error encountered while processing the request

Scheduled/Adhoc report will not be generated for each **unprotected resources** resource type.

Release for July 11, 2023

Learn about fixes and known issues in this release of Cloud Snapshot Manager.

Fixed issues

Learn about the issues that have been fixed in this release of Cloud Snapshot Manager.

Azure/AWS copy jobs fail intermittently due to " [5056] The object exists" error

Issue has been fixed and copy jobs are successful without error.

Volume IOPS and throughput values are not getting preserved on VM restore

The settings are now preserved after VM restore.

Customer is unable to see DD information under protection plans since March 2023 update for CSM has been published

Issue has been fixed and customer can see the DD information under protection plans.

Update "GCP Custom Role Permissions" link on GCP Create Account page not available

GCP Custom Role Permissions link has been added in the GCP **Create** and **Edit** Account page.

Upgrade dgrijalva/jwt-go:v3.2.0 to golang-jwt v3.2.1 to fix security vulnerability

Issue has been fixed in golang-jwt v3.2.1 for security vulnerability.

Error when taking large VM snapshot on AWS

Monitor time while creating snapshot and monitor interval to check snapshot completion have been increased to fix the issue.

Banner on CSM page if the AWS role based accounts not migrated to new trusted account

The banner is displayed for AWS role based accounts not migrated to new trusted account.

On demand snapshot job/Protection Plan job run on VM with public IP after removing public IP permissions should show as partially completed

Issue is fixed to show partially completed when running jobs with public IP without public IP permissions.

Warning icon must be displayed beside every AWS role-based cloud account if they are using old trusted number

Issue is fixed and is displaying warning icon next to AWS role-based cloud account if they are using old trusted number.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Protection plans should run at the same time regardless of daylight saving

Protection plans will not consider daylight savings time while running jobs.

Unable to create RBAC policy by selecting specific cloud account

Customer can create RBAC policy by selecting **All AWS accounts/All AZURE accounts/All GCP accounts/All accounts** option.

Release for March 21, 2023

Learn about new and changed features in this release of Cloud Snapshot Manager.

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Support for Google Cloud Platform (GCP)

The following are the features supported on Google Cloud Platform:

- Dashboard - Provides Dashboard data to show protected and unprotected VMs for GCP jobs.
- VM Discovery - Automatic discovery of resources for taking on-demand snapshots.
- On-demand and Policy based protection of VMs - Ability to set policies for protecting selected VMs in GCP.
- On-demand restore of snapshots - Provides advanced restore capability for Advanced and FLR VMs in GCP.
- Expiry of snapshots - Ability to expire the snapshots in GCP based on the set retention period or on-demand.
- Jobs - Provides status of jobs that ran for protecting VMs in GCP.
- Ad-hoc and scheduled reports - Provides CSM reporting for backups of GCP VMs.
- RBAC - Provides RBAC support for GCP cloud account.
- Alerts - Provides alerts for backups and restores done in GCP.

Support to configure CSM Proxy image from the private repository for Azure

Allows the user to store CSM proxy container image for Azure, in their repository.

Select alternate region for AWS DR cloud account restore

Allows selection of alternate regions for AWS DR cloud account restore.

Added email based MFA support

Now CSM supports MFA via device based authentication with OTP over email. New login screen will appear for non-federated users.

Added resource name to the Protection Plan failure event notifications for VM and Volumes

Allows user to see the resource name of the VM and volume in Protection Plan failure event notifications.

Support to Undelete the Blob containers during restore already deleted from Azure

Allows user to **Undelete** the Blob containers during restore already deleted from Azure.

New AWS trusted account will be used for new AWS role based accounts

Dell has moved to a new trusted account which will be used while creating new AWS Role Based accounts going forward.

Fixed issues

Learn about the issues that have been fixed in this release of Cloud Snapshot Manager.

DDVE bug fixes

Following are the errors that relate to DDVE that have been fixed:

1. DDVE copy job marked as successful but appears to have failed.
2. Not able to create DD storage with valid FQDN.
3. Not able to fetch queue message for copy jobs when multiple copy jobs are run on a specific container.

Concurrent snapshot copy limit preventing job execution for AWS cross-region/ account snapshots

Retries are spanned out for more duration with more elapsed time between each other to fix the concurrent execution limit.

API 2002 error on GET API when running Protection Plan in V2

Issue has been fixed and will be able to retrieve GET API details for Protection Plan Run in V2.

Switzerland regions are missing from the regions list for Azure

Azure regions list has been updated with Switzerland North and West regions.

RBAC policies audit not displaying Roles name and instead shows ID

Issue has been fixed to display Role names in RBAC policy audit.

Application Consistency and Copy Details are not working for existing Protection Plan when ownership is changed

Issue has been fixed and now Application Consistency and Copy details are retained when Protection Plans when ownership changes.

Restore of the VMs in Azure environment failing with error "Could not find availability set" whereas Availability Set is available

Issue has been fixed to return all the present Availability Sets in the provided region.

Protection plan does not allow adding different storage accounts with same tag name/value for tag based plan

Issue has been fixed to check unique identifiers for storage accounts with same tag name/value when being added to a Protection Plan.

Changes to Resource Type on existing Scheduled Reports are not captured by Audits

Issue has been fixed to check if Resource Type arrays are present in audit details for existing Scheduled Reports.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Volume IOPS and throughput values are not getting preserved on VM restore

The volume IOPS and throughput values are not getting preserved on VM restore. User has to set/update the values manually.

Certain DDVE Copy jobs failing with error "Unable to open DDBoost connection to PowerProtect DD System host : [5075] the user has insufficient access rights"

Some DDVE copy jobs fail with error "Unable to open DDBoost connection to PowerProtect DD System host : [5075] the user has insufficient access rights", observed in some snapshots containing large number of volumes.

Azure/AWS copy jobs fail intermittently due to " [5056] The object exists" error

If copy jobs are retried after a job has failed earlier, the retried job also fails as it is unable to create the backup path with same name. Check if the previous job failed with the errors for Azure/AWS copy. If yes, perform clean up and then copy the snapshot.

Release for October 18, 2022

Learn about new and changed features in this release of Cloud Snapshot Manager.

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Specify a particular Resource Group for snapshots

You can specify a specific Resource Group to store the snapshot while configuring Azure snapshot storage settings.

AWS cross-account snapshot in alternate region

You can also specify an alternate region for storing the snapshots in the AWS DR account.

Fixed issues

Learn about the issues that have been fixed in this release of Cloud Snapshot Manager.

Copy job failures

Following are the errors that relate to copy job failures:

1. Error occurred fetching session from CSM Proxy : Error: Future#WaitForCompletion: context has been cancelled: StatusCode=200 -- Original Error: context deadline exceeded Error code: 3041
2. Copy job fails to get triggered due to error: Could not send job to worker goroutine
3. Copy job failing with error "Cannot convert undefined or null to object"
4. "Unable to get pages within offset(536870912) and count(536870912), pageList is nil: Get &timeout=601: net/http: timeout awaiting response headers"

Dashboard displays incorrect protected resources data for Azure accounts

Now, the correct protected resource data for the Azure account is displayed on the Dashboard.

Incremental restore failure for Azure

You can do incremental restore for Azure.

Protection plan failures

Protection plans was failing with error "One or more snapshots failed 3002." Now, it has been resolved.

Unable to view "In Progress" Protection Plans

In Progress Protect Plan, link was generating "Invalid Request" error but now, you can view the "In Progress" Protection plans.

FLR failures

The following are the FLR failures that are resolved:

- While attempting to attach to an instance with multiple volumes
- Restore was not work on Windows 2019, Datacenter Gen2

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Validation error mismatch while editing and deleting two super admins

There is a validation error mismatch while editing and deleting two super admins. You can delete a super admin by editing and removing super admin role.

Release for June 16, 2022

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Protect PaaS DynamoDB Global tables in AWS

In this release, the Cloud Snapshot Manager has been enhanced to protect the DynamoDB Global Table. You can now protect the DynamoDB Global Table through the Cloud Snapshot Manager. The supported version for DynamoDB Global Table is 2019.11.21.

This release includes the following DynamoDB Global Table features:

- Discovery: You can discover the DynamoDB Global Table.
- On-demand protection: You can protect Global Table with on-demand snapshots.
- Plan-based protection: You can create a resource-based or tag-based protection plan.
- Instant recovery: You can restore the Global Table and its replica to AWS.
- Expiry: You can specify the retention period for Global Table snapshots.
- Auditing and reporting: The Global Table information is captured in the all existing reports and also auditing is added for the Global Table.
- REST API: The REST API support is added for Global Table.

Adding specific regions for cloud accounts

You can add and specify the regions where the resources are available and snapshots can be taken while creating or editing a cloud account, and only those specified regions are automatically listed in all Region drop-down throughout the Cloud Snapshot Manager application. You must edit the account and add the regions for existing accounts.

Search a resource based on its name in Azure

Now, you can search for Azure snapshots by resource name on Snapshots page.

Fixed issues

Learn about the issues that have been fixed in this release of Cloud Snapshot Manager.

The list of subnets are not displayed on the CSM Proxy Network page

On the CSM Proxy Network page, the list of subnets were not displayed. The Cloud Snapshot Manager must lists all subnets from the selected region and resource group on the CSM Proxy Network page while creating the network profile for Azure. Now, the issue has been resolved.

The protection plan fails to add tag-based RDS and Aurora Resources, as well as snapshot Redshift Resources

Issue with adding tag-based RDS, Aurora Resource, and snapshot Redshift Resources in protection plan.

Unable to perform Restore or FLR with io2 volumes

An error occurred while attempting to perform VM restore or FLR using a snapshot created from an AWS io2 volume type.

On the first attempt, the Cross-region snapshot fails

During the cross-region snapshot schedule, several VM resources failed on the first try.

DDVE Copy jobs failing due to wrong cloud account

Copy jobs were failing because of an error in which the job tried to find the resource in the incorrect cloud account.

Release for May 4, 2022

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Support for Azure Germany west region

Displaying volume details like Original and Restored volume IDs in Restore job details so that they can be correlated

Fixed issues

Learn about the issues that have been fixed in this release of Cloud Snapshot Manager.

Copy job failures

Following are the copy job failures that have been fixed:

- AWS Replication Error: Please try calling AWS API again after some time
- Message from the SQS queue could not be retrieved
- Error occurred fetching session from CSM Proxy : Error: stack could not be created after 9 attempts
- Server failed to authenticate the request. Make sure the value of Authorization header is formed correctly including the signature

DD storage streams are not being freed for failed and completed copy jobs

There was an issue with DD storage streams. The streams were not being freed for failed and completed copy jobs.

Dashboard displays incorrect protected resources

There was an issue with the Dashboard showing incorrect protected resources details.

Azure Cross Region Snapshots Failing with checkPlanRunCompletion error

There was an issue with Azure Cross Region Snapshots.

List of subnets fails to populate within the CSM Proxy Network page

There was an issue with the list of subnets failing to populate within the CSM Proxy Network page.

Release for February 10, 2022

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Azure permissions required to list key vaults, keys, and secrets in Cloud Snapshot Manager

As part of the restore operation (advanced recovery) for Azure snapshots, key vaults, keys, and secrets must be listed in the Cloud Snapshot Manager portal. To do that, use one of the permission models, vault access policy, or Azure role based control. Both the permission models require the Azure custom permission role. The following are the permissions that must be added to the **dataActions** section of the Azure custom role:

```
"dataActions"["Microsoft.KeyVault/vaults/secrets/readMetadata/action",
              "Microsoft.KeyVault/vaults/keys/read"
             ]
```

For more information, see Restore from a snapshot.

Update to AWS permissions for RDS, Aurora, Redshift, and DynamoDB resources

Tag based protection plans for RDS, Aurora, Redshift, and DynameDB resources were failing due to a missing AWS permission. After the February 2022 release, for protection plans with AWS resources like RDS, Aurora, Redshift, and DynamoDB to work, the following AWS permission is required:

```
 {
      "Sid": "Stmt1466720176000",
      "Effect": "Allow",
      "Action": [

        "tag:GetResources"
      ],
      "Resource": [
        "*"
      ]
 }
```

The full list of permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/aws-minimum-permission.md.

Shared VPC supported for AWS PowerProtect DD Virtual Edition (DDVE) integration

As part of Cloud Snapshot Manager integration with DDVE, to copy snapshots to DDVE, CSM Proxy is created in the cloud account and region where the snapshots to be copied are present. The proxy is created in a subnet within a VPC. The VPC can be from the same cloud account or a shared VPC from another account.

NOTE: For shared VPC, the account might not have access to the default security group. So, the associated security group for the shared VPC must be added in the proxy configuration page.

Custom path for Docker images supported

In the **CSM Proxy Network** page, the **Image URI** field has been introduced so that you can provide your Docker image path from the private repository to create Fargate containers. If the path is not provided, the latest default image path from the Dell public repository https://hub.docker.com/r/dellemc/powerprotect-csmproxy is used. The image path is supported only for AWS Cloud Snapshot Manager proxy configuration.

Restore report contains details about the snapshot type restored

The Cloud Snapshot Manager restore report contains details about whether the snapshot that is restored is a DDVE snapshot, a normal AWS snapshot, or an Azure snapshot.

Read and write streams supported for Azure PowerProtect DD Virtual Edition (DDVE)

You can now set the stream concurrence limits to control incoming and outgoing connections between Cloud Snapshot Manager and Azure DDVE.

Protection Plans with many tags or resources supported

You can now successfully create or update protection plans with many tags or resources. The number must not exceed 1000 tags or resources.

Time period in the Job, Event, and Report pages

In the Job, Event, and Report pages, the records that are listed are only for a time period that does not exceed 60 days.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

ⓘ **NOTE:** All the known issues in the September 02, 2021 release have been resolved.

RDS instances cannot be queried

The issue has been resolved. For more details, see *Update to AWS permissions for RDS, Aurora, Redshift, and DynameDB* in the *New and changed features* section.

Unable to perform file level recovery due to tag restrictions

Tags are attached at the time of volume creation instead of after volume creation and the issue has been resolved.

Cannot use advanced restore to restore VM having SSE with PMK and ADE disk encryption

The issue has been resolved. Additional permissions are required to list key vaults, keys, and secrets for advanced recovery of Azure VMs. For more information, see *Azure permissions required to list key vaults, keys, and secrets in Cloud Snapshot Manager* in the *New and changed features* section.

RDS Protection Plan jobs fail for instances created using Cloud Formation Stack

The issue has been resolved.

Protection Plan status is incorrectly reported as successful when cross-region copy fails

The issue has been resolved. Cross-region copying of snapshots is successful. The correct message is displayed if the copy operation fails.

Resources cannot be searched using resource name on the Plan Run Details page of a Protection Plan

The issue has been resolved and you can search using the resource name.

Release for September 02, 2021

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Copy Azure snapshots to PowerProtect DD Virtual Edition (DDVE) with deduplication to reduce storage cost

The powerful capabilities of Cloud Snapshot Manager are brought together with DDVE, the industry-leading deduplication storage virtual appliance. This integration addresses the requirements of Azure users who want to benefit from the capabilities of snapshots such as fast image level backups and restores while having the flexibility to keep backup data for a longer time period with deduplication in Azure Blobs.

With this integration, users can save on snapshot storage costs by leveraging lower-cost blob storage combined with DDVE block-level deduplication technology. For more information, see *Cloud Snapshot Manager integration with PowerProtect DD Virtual Edition (Azure)* in PowerProtect Cloud Snapshot Manager Online Help.

Cloud Snapshot Manager integration with DDVE is available for all users at no extra cost. Existing users do not require a new or additional purchase to use the feature with Cloud Snapshot Manager.

NOTE: Though Cloud Snapshot Manager does not charge to use DDVE, Azure services charge a fee to run DDVE.

License agreement

Software provided as part of Cloud Snapshot Manager is licensed pursuant to Dell's End User License Agreement, available at https://www.dell.com/learn/us/en/uscorp1/terms-conditions/art-software-license-agreements.

Cloud Snapshot Manager requires the following Azure permissions to create and manage the CSM Proxy network profile and the container for data transfer as part of Cloud Snapshot Manager integration with DDVE. These permissions must be added to the permissions set for the Cloud Snapshot Manager registered application defined in the Cloud Snapshot Manager cloud account configuration:

```
"Actions": [
    "Microsoft.Network/networkProfiles/read",
    "Microsoft.Network/networkProfiles/write",
    "Microsoft.ContainerInstance/containerGroups/read",
    "Microsoft.ContainerInstance/containerGroups/write",
    "Microsoft.ContainerInstance/containerGroups/delete",
    "Microsoft.Storage/storageAccounts/listKeys/action"
 ]
```

The full list of Azure permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/azure-custom-role.md.

Update to the AWS cloud account type and the permissions required to copy snapshots to PowerProtect DD Virtual Edition (DDVE)

A change has been made in this release to the way that the CSM Proxy task runs in AWS. The dynamically created IAM role used to run copy tasks has been changed to a static integrated role dependency. A change to Cloud Snapshot Manager's Minimum Permission policy is required to ensure continued DDVE operation.

An AWS role based cloud account is required to copy AWS snapshots to DDVE. You must also create a trust relationship for the role. Existing IAM roles too require the update to create a trust relationship with the ecs-tasks service. For the IAM role that is associated with the Cloud Snapshot Manager cloud account, in the AWS console, include the following by editing the **Trust Relationship** JSON content:

```
{
"Effect": "Allow",
"Principal": {
"Service": "ecs-tasks.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
```

For more details, see step 5 in the topic, *Configure a role based IAM user for AWS* in PowerProtect Cloud Snapshot Manager Online Help.

The following IAM permissions are no more required. It is recommended that you remove them from the policy list:

```
"Action":   [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:GetRole",
            "iam:PutRolePolicy"
        ]
```

The following permissions have been added to the AWS Minimum Permission Policy and are required to create the CSM Proxy for data transfer into DDVE:

```
    {
      "Sid": "AmazonECSTaskExecutionRolePolicy",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "*"
      ]
    },
```

The following permission has been added to the AWS Minimum Permission Policy. It is required to delete the task definition within the CloudFormation stack that Cloud Snapshot Manager created:

```
 {
         "Sid":"ECSPermissions",
         "Effect":"Allow",
         "Action":[
            "ecs:DescribeTaskDefinition"
         ],
         "Resource":[
            "*"
         ]
      }
```

The full list of AWS permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/aws-minimum-permission.md.

A user with the Super Admin policy has permissions to edit another user's protection plan irrespective of the owner of the plan

Cloud Snapshot Manager now enables a user with the *Super Admin* policy to edit, enable, and disable a protection plan irrespective of the owner of the plan.

Restore Azure VMs with any VNet from any resource group within the same region

Cloud Snapshot Manager enables you to restore VMs with any VNet, security group, disk encryption set, and availability set from any resource group within the same region.

Support to attach disks or volumes permanently to VMs during file level recovery

For AWS and Azure resources, during file level recovery, Cloud Snapshot Manager provides the option, **Never detach** to attach disks or volumes permanently to VMs.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

Unable to create a trial account

An error message was displayed when the user tried to fill in details in the **Request Trial** page. The issue has been resolved and the user is able to create a tenant id.

Unable to successfully restore snapshots from AWS DDVE if the EBS encryption enforcement feature is enabled

During the restore operation, the AWS snapshot that was created from a DDVE copy was never encrypted. Instead, the volume created was encrypted later using the encryption key. The issue is resolved and the restored snapshot can also be encrypted now.

The schedule type is set incorrectly when the retention period is the same for daily and weekly schedule

In the scheduled report, CSM Snapshot Details, data displayed in the *Schedule type* column was incorrect if the daily and the weekly schedule had the same retention period. The issue has been resolved and now the correct schedule type is displayed.

Remove IAM create and delete role permissions dependency while creating AWS cloud formation stack

For more information, in the New and changed features section, see the topic, *Update to the AWS cloud account type and the permissions required to copy snapshots to PowerProtect DD Virtual Edition (DDVE).*

Azure based protection plan does not run successfully

The issue was due to insufficient permissions and has been resolved.

RDS restore operation fails

This issue is resolved.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

The Jobs page shows the status as successful for Azure group restore

The status, 'Successful' is displayed instead of 'Completed' for an Azure group restore job that has been completed successfully.

The protection plan REST API allows a non-super admin user to edit the protection plan of any other user

A non-super admin user with permissions to manage protection plans must not be allowed to edit a protection plan created by another user.

Incorrect resource type shown in the scheduled report email for unprotected resources

Audit views displayed are incorrect when a cloud account is deleted

When a cloud account is deleted, the audit for older entries does not work since the cloud account is not available.

Azure Snapshot Storage Settings page mandates cross region configuration even if you only want to save alternate snapshot resource group

In the Azure Snapshot Storage Settings page, it does not allow you to save the page if you only select the **Use Alternate Snapshot Resource Group** option.

In a protection plan, pre and post scripts are mandatory for application consistency

In a protection plan, the application consistency option does not work if pre and post scripts are not provided. Pre and post scripts are optional and must not be mandatory. The issue exists for both AWS and Azure resources.

Release for May 04, 2021

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

PowerProtect Cloud Snapshot Manager activation with Dell EMC PowerProtect Data Manager perpetual license

As part of tighter integration of Cloud Snapshot Manager with PowerProtect Data Manager, Cloud Snapshot Manager now accepts PowerProtect Data Manager perpetual license for activation. The entitlement to use Cloud Snapshot Manager is tied to a valid support agreement. So you have to enter the end date of the support agreement at the time of activation.

For more information, see *Provision Cloud Snapshot Manager account* in the *Dell EMC PowerProtect Cloud Snapshot Manager Getting Started Guide*.

Tag based protection support for Azure Blob Containers

Cloud Snapshot Manager supports tag based resource selection of Azure Blob Containers as part of creating a protection plan. Every time the protection plan runs, it discovers Blob Containers with the specific tags in the plan and protects them. So you do not have the burden of manually adding new Blob Containers to the resource based plan.

Azure restore enhancements

The following Azure restore enhancements have been added to Cloud Snapshot Manager:

- In the Advanced Restore page:

    Included the **VNet ID** option to restore VMs to a different Azure Virtual Network (VNet) other than the original VNet.

    Enabled the option to select a subnet for each of the Network Interface Cards (NIC) in the VM.

    Enabled the option to restore the VM to a different availability zone other than the original availability zone. This is also applicable for cross-region VMs.
- Added the **Proximity Placement Group** parameter in the Cloud Snapshot Manager REST API for POST /restore API.

Support for DD Operating System 7.5

In this Cloud Snapshot Manager release, for AWS DD Virtual Edition (DDVE) replication or restore of snapshots, Cloud Snapshot Manager supports DDVE 6.0 with DDOS 7.5.

Cloud Snapshot Manager REST APIs

In addition to the existing REST APIs, the following REST APIs are supported in this release of Cloud Snapshot Manager:

- List events
- List jobs

The documented reference to the API specifications is available at https://developer.dell.com/apis/5788/versions/latest and the new APIs are available under **v1**.

Unprotected Resources report for Azure Blob Containers

You can schedule Unprotected Resources reports to generate the list of unprotected Blob Containers in your Azure cloud account so that you can start protecting them.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

Dashboard data displayed for Blob Containers is incorrect

The issue has been resolved. The Cloud Snapshot Manager Dashboard now accurately displays the number of protected Blob Containers.

Release for April 08, 2021

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Azure VM restore enhancements

A new parameter, **Proximity Placement Group** has been added to the Advanced Restore page for Azure VMs. With this enhancement, while restoring Azure VMs, CSM now preserves the VM settings, Proximity Placement Group, Advanced VM Extensions, System Assigned Managed Identity, and Ultra Disk Compatibility on Disks if specified in the Azure portal. This is applicable for original region and cross-region Azure snapshots.

> **NOTE:** The VM settings, Proximity Placement Group, Advanced VM Extensions, System Assigned Managed Identity, and Ultra Disk Compatibility on Disks are preserved during the restore process only for Azure snapshots taken after the CSM April 2021 release.

CSM requires the following Azure permissions to preserve the VM settings mentioned:

```
"Actions": [
             "Microsoft.Compute/proximityPlacementGroups/read",
             "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
            ]
```

The full list of Azure permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/azure-custom-role.md.

VM restore with tags applied

When restoring a VM, CSM first created the VM and then applied the tags on that VM. Some external automation tool in the cloud environment requires tags to be there as VMs are created, and since CSM was not applying the tags at the time of VM creation, the tool would bring down the VM immediately. To address this issue, CSM now applies the VM tags at the time of VM creation.

Release for March 02, 2021

In this release, general stability improvements have been made to the DDVE feature rolled out in the January 2021 release.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

Azure file level recovery to a VM in a different availability zone from the source VM fails

You can now perform file level recovery of disks to a VM in a different availability zone other than the availability zone of the original VM where both the source and the target VM are in the same region.

Resources view returns partially filled pages

Azure does not provide tag-based filtering with proper support for pagination. CSM has addressed this limitation by providing pagination at CSM level.

Release for January 28, 2021

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Copy snapshots to PowerProtect DDVE with deduplication to reduce storage cost

The powerful capabilities of Cloud Snapshot Manager are brought together with PowerProtect DDVE, the industry-leading deduplication storage appliance. This integration addresses the requirements of users who want to benefit from the capabilities of snapshots such as fast image level backups and restores while having the flexibility to keep backup data for a longer time period with deduplication in S3.

With this integration, you can save on snapshot storage costs and use the deduplication feature of DDVE. For more information, see *Cloud Snapshot Manager integration with PowerProtect DDVE* in *PowerProtect Cloud Snapshot Manager Online Help*.

CSM integration with DDVE is available for all users at no extra cost. Existing users do not require a new or additional purchase to utilize the feature with Cloud Snapshot Manager.

License agreement

Software provided as part of Cloud Snapshot Manager is licensed pursuant to Dell's End User License Agreement, available at https://www.dell.com/learn/us/en/uscorp1/terms-conditions/art-software-license-agreements.

Cloud Snapshot Manager requires the following AWS permissions for data transfer as part of CSM integration with DDVE:

```
    {
       "Sid": "EBSPermissions",
       "Effect": "Allow",
       "Action": [
         "ebs:CompleteSnapshot",
         "ebs:GetSnapshotBlock",
         "ebs:ListChangedBlocks",
         "ebs:ListSnapshotBlocks",
         "ebs:PutSnapshotBlock",
         "ebs:StartSnapshot"
       ],
       "Resource": [
         "*"
       ]
     },
     {
       "Sid": "CloudFormationPermissions",
       "Effect": "Allow",
       "Action": [
         "cloudformation:CreateStack",
         "cloudformation:DeleteStack",
         "cloudformation:DescribeStacks"
       ],
       "Resource": [
         "*"
       ]
     },
     {
          "Sid": "ECSPermissions",
          "Effect": "Allow",
          "Action":   [
               "ecs:CreateCluster",
               "ecs:CreateService",
               "ecs:DeleteCluster",
               "ecs:DeregisterTaskDefinition",
               "ecs:RegisterTaskDefinition",
               "ecs:DeleteService",
               "ecs:DescribeClusters",
               "ecs:DescribeServices"
           ],
           "Resource": [
                "*"
           ]
     },
     {
          "Sid": "IAMPermissions",
          "Effect": "Allow",
          "Action":  [
               "iam:AttachRolePolicy",
               "iam:CreateRole",
               "iam:DeleteRole",
               "iam:DeleteRolePolicy",
               "iam:DetachRolePolicy",
               "iam:GetRole",
               "iam:PassRole",
               "iam:PutRolePolicy"
           ],
           "Resource": [
                "*"
           ]
     },
     {
       "Sid": "SQSPermissions",
       "Effect": "Allow",
       "Action": [
         "sqs:CreateQueue",
         "sqs:DeleteMessage",
         "sqs:DeleteQueue",
         "sqs:ReceiveMessage",
         "sqs:SendMessage"
       ],
       "Resource": [
         "*"
       ]
      }
```

The full list of AWS permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/aws-minimum-permission.md.

Store snapshots in an alternate resource group in Azure

Cloud Snapshot Manager has been enhanced to enable storing Azure snapshots in a different resource group other than the resource group where the original resource resides.

For more information, see *Configure Azure snapshot storage settings* in *PowerProtect Cloud Snapshot Manager Online Help*.

Exclude data volumes for on-demand VM snapshots

In the **Resources** page, CSM has introduced an option to exclude data volumes that are attached to a VM while taking on-demand snapshots. This helps in reducing snapshot storage costs incurred due to large data volumes.

Update to RBAC permissions

A new permission, *Manage Storage Systems*, has been included as part of role based access control (RBAC). The permission manages DDVE configuration in CSM.

Change in email id

The Cloud Snapshot Manager email id that is used for communication regarding user account activation and reports has been changed from no-reply@emc.com to no-reply-cloud-snapshot-manager@dell.com.

Release for October 03, 2020

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager

Copy Azure snapshots to other regions for disaster recovery

Cloud Snapshot Manager has been enhanced to support copying of Azure VM snapshots to other regions. You can now keep copies of Azure snapshots in other regions to quickly recover entire VMs if there is a disaster in one of the Azure regions. The snapshot is created in the same region as the resource, and then can be copied to one or more regions that the cloud account has access to using Azure storage accounts. Configure the regions that you want to copy your snapshot to as part of setting a cross-region policy. You can set the copy schedule and retention in the remote region.

By copying your snapshots from one region to another, you can:

- Recover quickly from regional disasters in Azure by launching applications in a new region.
- Move an application from one region to another.

Cloud Snapshot Manager requires the following Azure permissions to copy and restore snapshots in other regions:

```
"Actions": [
            "Microsoft.KeyVault/vaults/read",
            "Microsoft.KeyVault/vaults/secrets/read",
            "Microsoft.Storage/storageAccounts/blobServices/containers/delete",
            "Microsoft.Compute/diskEncryptionSets/read"
            ]
```

The full list of Azure permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/azure-custom-role.md.

Update to RBAC privileges

The following privileges have been included as part of role based access control (RBAC) to provide administrators with more flexibility to restrict access control:

- **Manage protection plans** - The user assigned the privilege can create, edit, and delete protection plans. All *Super Admins* within a tenant can continue to have full access to all existing protection plans within the tenant. The protection plans may have been created either through the CSM UI or REST API. Protection plans created through REST API continue to run based on the *Super Admin* policy privileges. However, from this release onwards, protection plans created will be editable only by the creator of the plan.
- **Manage policy schedules** - The user assigned the privilege can create, edit, and delete policy schedules.
- **Manage cloud accounts** - The user assigned the privilege can create, edit, and delete cloud accounts.
- The earlier privilege, **View resources and on-demand snapshots**, is now offered as two separate privileges, **View resources** and **Take on-demand snapshots**.

In this release, the integrated role, *Full Access* has been renamed to *Super Admin*. If existing users have created a role and named it *Super Admin*, it will be renamed to *Existing Super Admin* to differentiate between the roles.

Release for August 18, 2020

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Cloud Snapshot Manager activation with PowerProtect Data Manager license

With this release, Cloud Snapshot Manager accepts PowerProtect Data Manager(PPDM) license for activation, enabling organizations to take advantage of the capabilities of both PowerProtect Data Manager and Cloud Snapshot Manager as part of one purchase.

The existing option of purchasing CSM separately is also available for those who only have CSM requirements.

For more information, see *Cloud account management* in the *Dell EMC PowerProtect Cloud Snapshot Manager Getting Started Guide*.

ⓘ **NOTE:** PPDM licensing is based on Front End Tera Byte (FETB) or SOCKETS. CSM licensing is based on the number of resources protected. 1 TB, or 1 SOCKET is equivalent to 10 resources. So a PPDM license with 50 TB or 50 SOCKET capacity translates into a license to protect 500 resources in CSM.

New Azure regions supported

In addition to the existing Azure regions, Cloud Snapshot Manager supports the following new regions:

- Germany West Central (Public)
- Germany North (Public)
- Switzerland North
- Switzerland West
- Norway West
- Norway East
- UAE Central

Exclude data volumes in a protection plan

In the **Protection Plans** page, CSM has introduced an option to exclude data volumes that are attached to a VM while taking snapshots as part of a protection plan. This helps in reducing snapshot storage costs incurred due to large data volumes.

ⓘ **NOTE:** If you exclude volumes from Linux VMs, protection and recovery of the Linux VMs might fail. To avoid the issue, use the *no fail* settings in the */etc/fstab* files. This causes the Linux VM boot sequence to ignore a failure in finding the volume. For example, *UUID=123456-1234-1234-1234-123456789av /mnt/vol1 xfs defaults, nofail 0 2*. For more information, see https://wiki.archlinux.org/index.php/Fstab.

Cloud Snapshot Manager REST APIs

In addition to the existing REST APIs, the following REST APIs are supported in this release of Cloud Snapshot Manager:

- List policies.
- Fetch policy by ID.
- Create protection plan.
- Update protection plan.
- Delete protection plan.

The documented reference to the API specifications is available at https://developer.dell.com/apis/5788/versions/latest and the new APIs are available under version 2.0.0(v2).

Access to failed plan run jobs

The plan run failure email to the user now contains a hyperlink providing easy access to failed plan runs in the Cloud Snapshot Manager portal.

Update to AWS permissions required for RDS

CSM requires the following AWS permission to attach custom tags to snapshot or restore an RDS instance:

```
{
   "Sid": "Stmt1466720176000",
   "Effect": "Allow",
   "Action": [
     "rds:AddTagsToResource",
           ],
   "Resource": [
     "*"
   ]
 }
```

The full list of permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/aws-minimum-permission.md.

Release for June 30, 2020

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Support for AWS DBaaS tag based protection plans

For organizations who want to automate their cloud infrastructure protection using tags, Cloud Snapshot Manager extends its powerful tag based assignment of resources to protection plans, to include AWS DBaaS resources such as RDS, Aurora, Redshift, and DynamoDB.

Cloud Snapshot Manager free trial extended

Cloud Snapshot Manager has extended its free trial offer to 90 days. You get an account with all features of Cloud Snapshot Manager to protect 50 instances. After you make a purchase, you can continue to use the same account. To download the free trial version, go to www.delltechnologies.com/CSMFreeTrial.

New regions supported

Two new regions, Africa (Cape Town) and Europe (Milan) have been added to the list of AWS regions supported by Cloud Snapshot Manager. You can discover resources, create snapshots, and perform restore operations in these regions.

Update to AWS permissions required for Redshift

Cloud Snapshot Manager requires the following AWS permission in addition to the existing permissions for Redshift to take snapshots:

```
{
   "Sid": "redshiftpermissions",
   "Effect": "Allow",
   "Action": [
     "redshift:CreateTags",
           ],
   "Resource": [
     "*"
   ]
 }
```

The full list of permissions is available at https://developer.dell.com/apis/5788/versions/latest/docs/aws-minimum-permission.md.

Enhanced filtering for protection plan list

Cloud Snapshot Manager has been enhanced with a new filtering option, **Enabled** in the **Protection Plans** page to list enabled resource based or tag based protection plans.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

RBAC: Report job is created even if no accessible cloud account exists

If a user had access to a cloud account and later the access was removed, the user could still generate a report for the account. The issue has been fixed, and a report can no longer be generated.

RBAC: Existing CSM user cannot log in to CSM with the new tenant that the user created

The issue has been fixed. If an existing CSM user creates a tenant using the activation code, the user can now log in to CSM with the new tenant.

Old scheduled reports before May 27 are not getting triggered

Scheduled reports created before May 27, 2020, were not getting triggered after the CSM May 2020 release due to an issue in the scheduler. After the scheduler restarts, the reports should have been fetched but due to an undefined user_id field, they could not be fetched. This issue has been fixed, and the older reports are now getting triggered.

Unprotected resources report for volumes does not display correct data

When snapshots of VMs are taken, it implicitly takes snapshots of the attached volumes only. However, when you generate an Unprotected Resources report for volumes, the protected volumes too are included in the report. The issue has been resolved, and the protected volumes of the VM snapshot do not appear in the report.

Release for May 27, 2020

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Role Based Access Control (RBAC) for enhanced security and restricted access

For organizations that have to control access and set limits to what authorized users can do, Cloud Snapshot Manager introduces Role Based Access Control (RBAC) capability. Cloud Snapshot Manager RBAC enables protection of resources across both AWS and Azure securely through a common set of RBAC policies. A Super Administrator in Cloud Snapshot

Manager can create roles for different types of users, and assign RBAC policies outlining what actions users are allowed to perform and what resources they have access to.

All existing users created in Cloud Snapshot Manager are set up as *Super Admins* with full access control over the CSM account.

With RBAC capabilities along with Federated Identification, Cloud Snapshot Manager provides a comprehensive and secure Identity Access Management environment ensuring that organizations have the security and control to meet their regulatory and compliance requirements.

> ⓘ **NOTE:** Existing Cloud Snapshot Manager users have to use the URL, https://console.dell.com instead of https://console.dell.com/home to access the Cloud Snapshot Manager portal. Another option is to click **DELLEMC** in the blue banner displayed on the upper left side of the browser when the URL, https://console.dell.com/home is used.

> ⓘ **NOTE:** For existing users who still use the URL, https://console.emc.com/ and get redirected to the https://console.dell.com page, the redirect page will no more be available.

Improved resilience and performance

The following improvements have been made to Cloud Snapshot Manager:

- Improved error handling for network operations that timed out.
- Improved performance of filter queries.

Internet Explorer is no more supported

Cloud Snapshot Manager has removed support for the Internet Explorer browser. Mozilla Firefox, Google Chrome, Microsoft Edge, and any Chrome-based browser are supported.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

Orphaned snapshots

Snapshots that were orphaned due to an unknown job completion status are resynchronized with Cloud Snapshot Manager so that their expiration can be managed by Cloud Snapshot Manager.

Release for March 31, 2020

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Copy VM snapshots across AWS accounts for disaster recovery

Cloud Snapshot Manager now offers the ability to protect your VMs against security attacks and breaches in your AWS accounts. With this release, you can copy your snapshots to a restricted account in AWS. Snapshots copied across accounts are full backups enabling a true disaster recovery solution as you can restore these snapshots to the original account or a different AWS account. When snapshots expire as per policy setting, you can control the cleanup by either allowing CSM to automatically delete snapshots or run a script manually as and when needed.

The script, *Delete-CSM-Expired-Snapshots-In-DR-Account* is provided in the **Help** page of the *PowerProtect Cloud Snapshot Manager* portal. For more information about the script, see *Create a cloud account* in *PowerProtect Cloud Snapshot Manager Online Help* available at https://console.dell.com.

AWS Permissions

To support copy and restore snapshot operations to and from a Disaster Recovery (DR) account, CSM requires the following IAM permissions.

The following permissions are required to set up a DR account:

```
{
 "Sid": "Stmt1466719308000",
 "Effect": "Allow",
 "Action": [
   "ec2:CopySnapshot",
   "ec2:CreateTags",
   "ec2:DescribeSnapshots",
   "ec2:ModifySnapshotAttribute"
 ],
 "Resource": [
   "*"
 ]
}
```

The *ec2:ModifySnapshotAttribute* permission enables you to share and stop sharing a snapshot after a snapshot or restore operation is completed.

```
{
 "Sid": "Stmt1466719308001",
 "Effect": "Allow",
 "Action": [
   "kms:ListAliases",
   "kms:ListKeys",
   "kms:Encrypt",
   "kms:Decrypt",
   "kms:ReEncrypt*",
   "kms:GenerateDataKey*",
   "kms:DescribeKey",
   "kms:CreateGrant",
   "kms:ListGrants",
   "kms:RevokeGrant"
 ],
 "Resource": [
   "*"
 ]
}
```

```
{
 "Sid": "CSMCostExplorerPermissions",
 "Effect": "Allow",
 "Action": [
   "ce:GetCostAndUsage"
 ],
 "Resource": [
   "*"
 ]
}
```

The following permissions are required if you want to allow CSM to expire snapshots in the DR account:

```
{
 "Sid": "Stmt1466719308000",
 "Effect": "Allow",
 "Action": [
   "ec2:DeleteSnapshot",
   "ec2:DeleteTags"
 ],
 "Resource": [
   "*"
 ]
}
```

The following permissions are required if you want to run the Lambda script to expire snapshots:

```
{
 "Sid": "Stmt1466719308000",
 "Effect": "Allow",
 "Action": [
   "ec2:DescribeSnapshots",
   "ec2:DeleteSnapshot",
   "ec2:DescribeRegions",
   "logs:CreateLogStream",
   "logs:CreateLogGroup",
   "logs:PutLogEvents"
 ],
 "Resource": [
   "*"
 ]
}
```

The following permission is required for the source account so that snapshots can be shared and copied to the DR account:

```
{
 "Sid": "Stmt1466719308000",
 "Effect": "Allow",
 "Action": [
   "ec2:ModifySnapshotAttribute"
 ],
 "Resource": [
   "*"
 ]
}
```

The following permissions are required for the account to which snapshots are restored:

```
{
 "Sid": "Stmt1466719308000",
 "Effect": "Allow",
 "Action": [
   "ec2:AssociateAddress",
   "ec2:AssociateIamInstanceProfile",
   "ec2:AttachNetworkInterface",
   "ec2:AttachVolume",
   "ec2:CreateNetworkInterface",
   "ec2:CreateTags",
   "ec2:CreateVolume",
   "ec2:DeleteVolume",
   "ec2:DescribeAddresses",
   "ec2:DescribeImages",
   "ec2:DescribeInstances",
   "ec2:DescribeNetworkInterfaces",
   "ec2:DescribeAvailabilityZones",
   "ec2:DescribeSecurityGroups",
   "ec2:DescribeSnapshots",
   "ec2:DescribeSubnets",
   "ec2:DescribeVolumes",
   "ec2:DetachVolume",
   "ec2:ModifyInstanceAttribute",
   "ec2:ModifySnapshotAttribute",
   "ec2:RunInstances",
   "ec2:StartInstances",
   "ec2:StopInstances",
   "ec2:DescribeVpcs",
   "ec2:DescribeKeyPairs",
   "ec2:DescribeIamInstanceProfileAssociations"
 ],
 "Resource": [
   "*"
```

```
       ]
      }
```

```
      {
       "Effect": "Allow",
       "Action": [
         "iam:PassRole"
       ],
       "Resource": [
         "*"
       ]
      }
```

```
      {
       "Sid": "Stmt1466719308001",
       "Effect": "Allow",
       "Action": [
         "kms:ListAliases",
         "kms:Encrypt",
         "kms:Decrypt",
         "kms:ReEncrypt*",
         "kms:ListKeys",
         "kms:GenerateDataKey*",
         "kms:DescribeKey",
         "kms:CreateGrant",
         "kms:ListGrants",
         "kms:RevokeGrant"
       ],
       "Resource": [
         "*"
       ]
      }
```

The above permissions are also provided in Online Help. For more information, see *AWS permissions for cross-account copying of snapshots* in *PowerProtect Cloud Snapshot Manager Online Help*.

Policy creation enhancements

To support cross-account policies, Cloud Snapshot Manager has enhanced the policy creation user experience. CSM now offers three policy types - Backup, Cross-Region, and Cross-Account to enable you to select policies according to your protection needs. When a protection plan is created, a Backup policy is required to create snapshots in the original regions. You can optionally add Cross-Region and Cross-Account policies to the plan.

If you had created a policy with remote region copies, this policy is now migrated to two different types - Backup and Cross-Region. CSM continues to take snapshots as per the specified schedule and no changes are required by you.

Incremental snapshots for Azure Managed Disks is now generally available

With incremental snapshots, you can reduce your backup time and storage costs significantly. With instantaneous access to data, you can achieve shorter recovery time objectives. Additionally, for increased reliability, snapshots are stored on Zone Redundant Storage (ZRS) by default in the regions that support ZRS.

Cloud Snapshot Manager released support for incremental snapshots in preview mode in December 2019. With the general availability announcement, this feature is now supported in all Azure regions.

Enhancements to Cloud Snapshot Manager REST APIs

The following CSM REST APIs have been enhanced to support copying snapshots to a DR account for AWS. These snapshots can also be restored to another AWS account:

- Create cloud account.
- Update cloud account.
- Retrieve cloud account.

- Delete cloud account.
- List protection plans.
- Fetch protection plan by ID.
- Restore from snapshots.

The documented reference to the API specifications is available at https://developer.dell.com/apis/5788/versions/latest.

Release for February 04, 2020

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Enhancements to Cloud Snapshot Manager

The following enhancements have been made to Cloud Snapshot Manager:

- Three new regions, Asia Pacific (Hong Kong), EU (Stockholm), and Middle East (Bahrain) have been added to the list of AWS regions supported by Cloud Snapshot Manager. You can discover resources, create snapshots, and perform restore operations in these regions.
- On the **Entitlements** page, you can view the total number of resources that are protected against all your active entitlements.
- On the **Jobs** page, a new option, *All Jobs*, has been included to list all jobs. The jobs irrespective of the job type are displayed in descending order with the most recent job on top.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

While performing file level recovery(FLR) of an AWS Linux volume, the volume does not mount

During file level recovery of an AWS Linux volume, the volume is attached to the target VM. However, the volume is not mounted to the target VM. The issue is now resolved.

Previously, for Linux, only disk partitions were mounted. With this fix, the CSM SSM document mounts the Linux disk too if it is formatted with File System. The sample SSM document is available in the Cloud Snapshot Manager portal under the **Help** page.

Failed to complete plan run for a protection plan

The issue was due to a network failure and has been resolved. Cloud Snapshot Manager has improved resilience around network failures so that multiple attempts are made to complete a plan run before marking the job as failed.

Release for December 17, 2019

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Support for incremental snapshots in Azure

Cloud Snapshot Manager enables you to take incremental snapshots of Azure Managed VMs in the regions Azure supports. This helps you to reduce the amount of storage that is consumed for your backups and reduces your costs drastically. In the regions where Azure incremental snapshots functionality is not supported, full snapshots are taken.

Snapshot reports for Azure

Cloud Snapshot Manager reports that provide enterprises with visibility and insight regarding the status of data protection across all their cloud accounts are expanded to Azure:

- CSM Snapshot Details - This report lists details of all snapshots that Cloud Snapshot Manager generates for a particular tenant.
- Snapshot Summary - This report gives you an insight into the total CSM snapshot counts. It also provides snapshot counts by each resource type.

Recover files from Logical Volume Manager (LVM) volumes using Cloud Snapshot Manager File Level Recovery (FLR)

To recover files from LVM volume snapshots using Cloud Snapshot Manager FLR, see the guide, *File Level Recovery with Logical Volume Manager Snapshots*, available on the Support site.

Restore Azure VM with custom name

Cloud Snapshot Manager has been enhanced to enable you to specify a custom name for a restored Azure VM which makes it easier to identify restored VMs. Earlier, Cloud Snapshot Manager automatically assigned a name to the restored VM using Azure naming conventions. You now have two options, either to select the option to automatically assign a name or to specify a custom name.

Support to reset the API key secret

After generating the API credentials, if at any time you want to change the API key secret for security reasons, it is now possible to do that from the **Access Management** page of the Cloud Snapshot Manager portal.

Usability improvements in the Cloud Snapshot Manager portal

The following usability enhancements have been made to the Cloud Snapshot Manager portal:

- Browsing for snapshots has been made easier with the introduction of tabs. Tabs for CSM and Non-CSM specific filters simplify browsing and selecting snapshots for individual and group restores as well as retrieving Non-CSM snapshots for controlling snapshot sprawl.
- Searching for a cloud account from a list containing many cloud accounts has been made easier with searchable drop-down fields.
- Searching for a cloud account by name, ID, and description is now possible in the **Cloud Accounts** page.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

Scheduled snapshots failing due to iam:SimulatePrincipalPolicy permission

Scheduled snapshots were failing due to the iam:SimulatePrincipalPolicy aws permission which had regional restrictions. The issue has been fixed by removing the permission from the aws permission policy.

Release for November 06, 2019

New and changed features

Learn about new and changed features in this release of PowerProtect Cloud Snapshot Manager.

Support for restoring individual Blob snapshots

Cloud Snapshot Manager has been enhanced to support restoring individual Blob snapshots within a container snapshot. Existing functionality only supports restoring the entire container snapshot.

For information about restoring individual Blob snapshots, see *Restore Azure blob container snapshots or individual blob snapshots* in *PowerProtect Cloud Snapshot Manager Online Help* available at https://console.dell.com/help-and-support.

Dashboard enhancements

The Cloud Snapshot Manager dashboard has a new look and feel. You can now get a consolidated protection summary of all your cloud resources for a cloud type in one place. You can also still choose to view the protection summary only for a particular account.

Information such as the number of AWS and Azure cloud accounts, status of all resources, and regions where they are available is displayed.

Reporting enhancements

The following new report types are available in Cloud Snapshot Manager:

- CSM Snapshot Details - This report lists details of all snapshots that are generated by Cloud Snapshot Manager for a particular tenant.
- Non-CSM Snapshot Details - This report lists details of all snapshots which are not generated by Cloud Snapshot Manager(Non-CSM snapshots) for a particular tenant.
- Snapshot Summary - This report gives you an insight into the total CSM and Non-CSM snapshot counts and storage used across every cloud account. For CSM snapshots, the report also provides snapshot counts by each resource type. The report enables you to gain an understanding on how the protection storage is consumed across your entire cloud environment so that you can manage snapshot sprawl and costs better.

Currently, these report types contain information only for AWS cloud accounts.

AWS permissions required

Additional AWS permissions in the IAM policy are required to use the new report types. The following permissions (JSON format) are required to fetch the storage usage for snapshots from the AWS account and display in the Snapshot Summary report:

```
{
      "Sid": "CSMCostExplorerPermissions",
      "Effect": "Allow",
      "Action": [
        "ce:GetCostAndUsage",
        "ce:GetDimensionValues"
      ],
      "Resource": [
        "*"
       ]
    }
```

The following permission (JSON format) is required in the DynamoDB section of the IAM policy to list all Non-CSM snapshot details from the AWS account in the Non-CSM Snapshot Details report:

```
{
      "Sid": "dynamodbPerms",
      "Effect": "Allow",
      "Action": [
        "dynamodb:ListBackups",
      ],
      "Resource": [
        "*"
      ]
    }
```

For the updated policy which includes all the required permissions, see *AWS minimum permission policy* in *PowerProtect Cloud Snapshot Manager Online Help* available at https://console.dell.com/help-and-support.

PowerProtect Cloud Snapshot Manager REST API Access

PowerProtect Cloud Snapshot Manager REST APIs can be used to manage your cloud accounts, policies, plans, snapshots, and restores in AWS and Azure. Access to the APIs is controlled using credentials.

You can now generate the credentials to access Cloud Snapshot Manager APIs from the **Access Management** page of the PowerProtect Cloud Snapshot Manager portal.

Search snapshots across all regions using tags

Cloud Snapshot Manager has been enhanced to enable you to search for particular instances with specific tags across all regions. This is important if you have replicated snapshots across multiple regions and need to quickly find the restore point for a particular instance or VM to restore.

Fixed issues

Learn about issues that have been fixed in this release of PowerProtect Cloud Snapshot Manager.

For AWS, tag based filter is not working for group restore

In the **Snapshots** page, when a protection plan is selected for group restore, filtering the snapshots by tag does not filter any resources. Issue has been fixed to filter snapshots when a protection plan is selected and the tags are provided.

Displays error when retrieving AWS resources if there are no resources found with matching tags

When retrieving AWS resources with the tags filter, if there are no resources that match the tags, an error is displayed. Now, if there are no resources with matching tags, the message, "No resources found" is displayed.

Report schedules: Monthly scheduled report sent on the day of the week, not according to the schedule

When a monthly report is scheduled for a particular week of the month and day, the report is sent on that day of the week, every week, instead of once in the month. This issue is addressed to send the report only once on that week of the month and the selected day of the week.

Release for August 28, 2019

New and changed features

Learn about new and changed features in this release of PowerProtect Cloud Snapshot Manager.

PowerProtect branding

Cloud Snapshot Manager is now part of Dell EMC PowerProtect Software and is rebranded as PowerProtect Cloud Snapshot Manager. This change is reflected on the User Interface and in all emails and documentation.

Support for Azure Blob Storage

You can discover and protect entire Blob containers within Azure storage accounts using Cloud Snapshot Manager. Blob Storage is the object storage solution of Microsoft for the cloud environment. It enables you to store huge amounts of unstructured data such as text or binary data. Azure Blobs are stored within a container storage structure which functions like a directory.

For information about restoring Blob container snapshots, see *Restore an Azure blob container snapshot* in *PowerProtect Cloud Snapshot Manager Online Help* available at https://console.dell.com/help-and-support.

Automated emails to support trial customers

Cloud Snapshot Manager sends three automated emails to customers during their 30-day free trial period. The first email is sent after the trial account is created and provides customers with links to getting started tutorials. The second email is sent on the 15th day to check on the trial experience.

The final email is sent on the last day to let the customer know that the trial period is over. Also, details to contact sales for purchase of Cloud Snapshot Manager are provided. Customers can opt out anytime by clicking the **Unsubscribe** link in the emails.

PowerProtect Cloud Snapshot Manager REST APIs

In addition to the existing REST APIs, the following REST APIs are supported in this release of Cloud Snapshot Manager:

- Create cloud account.
- Update cloud account.
- Delete cloud account.
- Fetch external ID and trusted account for creating role ARN.
- List encryption keys configuration.
- Create encryption key configuration.
- Fetch encryption key configuration by ID.
- Delete encryption key configuration.

For the entire list of REST APIs supported, see *PowerProtect Cloud Snapshot Manager Public APIs* in *Dell EMC PowerProtect Cloud Snapshot Manager Getting Started Guide* available on the Support page. You can request access to Cloud Snapshot Manager Public APIs at csm.engineering.escalation@dell.com. For requesting credentials to access public APIs, see Generating Credentials. The documented reference to the API Specification is available at https://developer.dell.com/apis/5788/versions/latest.

Fixed issues

Learn about issues that have been fixed in this release of PowerProtect Cloud Snapshot Manager.

File Level Recovery fails to attach volume to the original VM for snapshot of MS Cluster setup

Cloud Snapshot Manager now addresses this issue to attach volumes to a VM in the Microsoft(MS) Cluster environment to recover files. This is applicable only for Azure resources.

Snapshot counts are not reported correctly on the dashboard

Protected, Unprotected, and Protected Inactive resources are reported correctly in the dashboard for a particular cloud account.

Azure snapshots fail because the Azure Disk ID does not match the standard format

When the VM Disk ID is not in the standard format, Cloud Snapshot Manager handles this situation by failing the snapshot and providing the appropriate error message.

PowerProtect Cloud Snapshot Manager UI becomes unresponsive when generating job run history report with many records

The issue has been resolved and reports can be generated successfully.

Snapshot expiry fails after 90 seconds

Cloud Snapshot Manager added retry mechanism to update the job status before marking the job as failed . This ensures that any intermittent communication issues between different services are handled and jobs are updated with the correct status.

Release for June 15, 2019

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Federated Identity support for Cloud Snapshot Manager

Dell EMC now enables you to access Cloud Snapshot Manager using Federated Identity. Federated Identity enables Cloud Snapshot Manager users to be authenticated by their enterprise Identity Provider (IdP) without creating any user accounts at Dell EMC.

For information about how to enable Federated Identity for your enterprise to access Cloud Snapshot Manager, see *Dell EMC Cloud Snapshot Manager Getting Started Guide* available at https://www.dell.com/support/home/en-us/product-support/product/cloud-snapshot-manager.

ⓘ **NOTE:** You have to now access Cloud Snapshot Manager using https://console.dell.com instead of https://console.emc.com.

Cloud Snapshot Manager REST APIs

Cloud Snapshot Manager supports additional REST APIs enabling integration of Cloud Snapshot Manager with external systems. The following REST APIs are available in this release:

- List protection plans
- Fetch protection plan by ID
- List protection plan runs
- Fetch protection plan run by ID

Cloud Snapshot Manager Public APIs are in limited availability. You can request access to Cloud Snapshot Manager Public APIs at csm.engineering.escalation@dell.com. For requesting credentials to access public APIs, see Generating Credentials. The documented reference to API Specification is available at https://developer.dell.com/apis/5788/versions/latest.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Accessing support.emc.com through https://console.dell.com is resulting in errors on console.dell.com

When you click **Support** in the **Help** page of https://console.dell.com (Cloud Snapshot Manager portal), you are directed to the Support page. However, when you go back to https://console.dell.com and try to access any page, it results in an error.

As a workaround for the issue, close the browser and log in again into https://console.dell.com.

Release for April 30, 2019

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Group restore of resources

To simplify restoring of a group of VMs that belong to an application to a point in time, Cloud Snapshot Manager has been enhanced to enable you to restore snapshots using a protection plan.

When the protection plan runs, all the resources in that plan have snapshots that are taken around the same time, making group restore possible in a quick, and reliable manner instead of having to restore each individual resource one at a time.

Enhanced report scheduling

Schedule reporting in Cloud Snapshot Manager has been enhanced to enable you to generate daily, weekly, or monthly reports and send them to configured email recipients. You can schedule the following report types:

- Plan Run Detailed
- Restore
- On-Demand Snapshot
- Expiry

You can also edit and delete a report schedule.

Support for Aurora, Redshift, and DynamoDB (AWS only)

Cloud Snapshot Manager now also supports the databases, Aurora, Redshift, and DynamoDB for backup and recovery.

Existing Cloud Snapshot Manager users have to add more permissions in the IAM policy for Cloud Snapshot Manager to support the databases. For the updated policy which includes all the required permissions, see *AWS minimum permission policy* in *Cloud Snapshot Manager Online Help* available at https://console.emc.com/help-and-support.

The following is the JSON format for the permissions:

For Aurora support:

```
    {
      "Sid": "Stmt1466720176000",
      "Effect": "Allow",
      "Action": [
        "rds:CreateDBInstance",
        "rds:AddRoleToDBCluster",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "rds:ModifyDBCluster"
      ],
      "Resource": [
        "*"
      ]
    }
```

For Redshift support:

```
{
      "Sid": "redshiftpermissions",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DeleteClusterSnapshot",
        "redshift:CreateClusterSnapshot",
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "*"
      ]
    }
```

For DynamoDB support:

```
{
      "Sid": "dynamodbPerms",
      "Effect": "Allow",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup",
        "dynamodb:DeleteBackup",
        "dynamodb:describeBackup",
        "dynamodb:ListTables",
        "dynamodb:RestoreTableFromBackup",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem"
      ],
      "Resource": [
        "*"
      ]
    }
```

In addition to the above permissions, the following are required:

```
{
      "Sid": "Stmt1466719308000",
      "Effect": "Allow",
      "Action": [
                 "ec2:DescribeAccountAttributes",
                 "ec2:DescribeInternetGateways"
                ],
               "Resource": [
        "*"
      ]
}
```

where

- ec2:DescribeAccountAttributes - Lists all the attributes for a user account. The attributes include Redshift quotas for the account, such as the number of database instances allowed. The description for a quota includes the quota name, current usage for that quota, and the maximum value of the quota.
- ec2:DescribeInternetGateways - Describes one or more of your internet gateways.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager. The issues were known issues in the previous Cloud Snapshot Manager releases.

Taking VSS snapshot of a VM is partially completed when File Level Recovery (FLR) attached volume is associated with it

To address the issue, AWS has fixed the latest *AWSEC2-CreateVssSnapshot* document and the *AwsVssComponents* package (AWS Systems Manager). Upgrade your VMs to use the latest AwsVssComponents package to resolve the issue.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Azure application consistent snapshot might be partially completed (crash consistent) if multiple jobs run at the same time on a VM

If you try to take multiple application consistent snapshots of an Azure VM at the same time, it might result in partially completed or crash consistent snapshots.

To avoid this issue, take only one application consistent snapshot of a VM at a time.

File level recovery create job is successful even though mounting of the file system fails for AWS

On a Linux VM, when performing file level recovery from the snapshot of a device that has a file system without a partition, Cloud Snapshot Manager displays the file level recovery create job as successful without any error.

However, the mounting of the device on the file level recovery host fails and details of the failure are not provided.

Cloud Snapshot Manager file level recovery of a volume on a Linux OS fails if an application consistent snapshot is created multiple times

After creating application consistent snapshot of an Azure Linux VM multiple times, performing file level recovery of the Operating System (OS) disk of that VM snapshot results in a failure.

The error that is reported is ' VM has reported a failure when processing extension 'RunCommandLinux'. Error message: "Enable failed: failed to execute command: command terminated with exit status=127 Error code: 4032'.

As a workaround for the issue, perform the following steps:

1. Log in to the target machine where the disk was recovered and move all the folders under `/var/lib/waagent/run-command/download` to a backup location or delete them if they are not required. For example, `command: mv /var/lib/waagent/run-command/download/* <destination directory>`
2. After moving the directories in `/var/lib/waagent/run-command/download`, rerun the file level recovery job.

Release for March 6, 2019

New and changed features

Learn about new and changed features in this release of Cloud Snapshot Manager.

Resource name in reports

Cloud Snapshot Manager has been enhanced to display the resource name along with the resource id in reports to make it easier to correlate report data with resources.

Cloud account name included for better troubleshooting

In Cloud Snapshot Manager, the cloud account name has been included in addition to the cloud account id for events, events sent by email, and jobs. When there are several cloud accounts, this enhancement makes it easier to find out which cloud account has an issue.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

CSM snapshot property page shows AWS snapshot resource name under the resource ID section for RDS resource

When AWS RDS resources are listed in the **Resources**, **Snapshots**, and **Protection Plans** detail pages, the identifier and name fields are now displayed with appropriate values.

Expiry failed job is logged every 15 minutes

Cloud Snapshot Manager runs a job every 15 minutes to expire all the snapshots that are past the expiration time. The issue was that when a snapshot was set to expire, it was not listed in the **Snapshots** page. The snapshot would not be listed in the **Snapshots** page even if Cloud Snapshot Manager fails to delete it.

With this fix, the snapshot is listed in the **Snapshots** page until it is deleted from your cloud account. If there is an issue like account authentication failure when Cloud Snapshot Manager tries to expire the snapshot, you can still modify the expiration date, address the issue, and then expire the snapshot.

Release for January 30, 2019

New and changed features

Discovery of Non-CSM snapshots (AWS only)

Cloud Snapshot Manager now allows you to discover and remove (optional) snapshots in AWS cloud accounts that it did not create (referred to as Non-CSM snapshots). You can filter snapshots by date, tags, or volume ids. The feature enables you to have better control over the snapshots and puts an end to redundant snapshots in your environment. This is applicable only for AWS snapshots.

Custom encryption key for remote region snapshots (AWS only)

Cloud Snapshot Manager has been enhanced to support encryption of remote region snapshots using custom encryption keys. You can configure the custom defined encryption key (AWS Customer Master Key) in Cloud Snapshot Manager and copy the AWS snapshot to a remote region with the custom key.

Previously, if the original region snapshot was encrypted, the copied snapshots were encrypted with the AWS default encryption key for the targeted remote region. You could not use a custom encryption key. Currently, custom encryption key support is applicable only for AWS snapshot copies.

Existing Cloud Snapshot Manager users have to add, *kms:ListAliases*, in the IAM policy that is used by the Cloud Snapshot Manager IAM role or IAM user. This new permission is required to enable Cloud Snapshot Manager to list the region specific encryption key aliases in the Cloud Snapshot Manager portal. The following is the JSON format that describes the additional permission that the policy must contain:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1466719308000",
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Azure application consistency using pre and post snapshot scripts

Cloud Snapshot Manager has added support for the creation of application consistent snapshots of Azure Windows and Linux VMs using custom scripts (also referred to as pre and post scripts). You can now use a script to pause read/write operations to the application before the snapshot is taken and resume operations after the snapshot is taken, ensuring consistency of snapshot data for applications.

Support for a new region (AWS only)

Cloud Snapshot Manager now provides support for the AWS Region, Asia Pacific (Osaka-Local) ap-northeast-3. You can use the Asia Pacific (Osaka-Local) Region only with the Asia Pacific (Tokyo) Region. To request access to the Asia Pacific (Osaka-Local) Region for your AWS account, contact your AWS sales representative.

Enhancements to the CSM-Mount-Unmount document

The CSM-Mount-Unmount document for file level recovery has been enhanced for better error handling and multiple partitioned disks mounting. It is recommended to use the latest document though the old version of the document still works. The document is available on the **Help** page of the Cloud Snapshot Manager portal.

Fixed issues

Learn about issues that have been fixed in this release of Cloud Snapshot Manager.

Unable to delete cloud account after removing resources from protection plans

It was not possible to delete the cloud account from the **Cloud Accounts** page of Cloud Snapshot Manager even if there were no protection plans associated with it. With this fix, the issue has been resolved.

Known issues

Learn about known issues that are found in Cloud Snapshot Manager and how to work around them.

Taking VSS snapshot of a VM is partially completed when File Level Recovery (FLR) attached volume is associated with it

Cloud Snapshot Manager uses the AWS provided SSM document, *AWSEC2-CreateVssSnapshot* to take VSS snapshots. When you attach a read-only volume to a VM and attempt to take a VSS snapshot using *AWSEC2-CreateVssSnapshot* , the VSS snapshot is not taken due to a bug in *AWSEC2-CreateVssSnapshot* . The issue has been reported and the AWS team is working on it.

Release for December 11, 2018

New and changed features

It is recommended to include the API, *iam:SimulatePrincipalPolicy* in the IAM policy. Adding the API enables Cloud Snapshot Manager to validate permissions before performing any operation and avoid unnecessary execution and event or email generation. For information about the additional permissions, see *AWS minimum permission policy* in *Cloud Snapshot Manager Online Help*.

Report scheduling

The Reports module of the Cloud Snapshot Manager portal has been enhanced to enable you to schedule reports. You can schedule reports to be generated daily at a set time and sent to configured email recipients. Currently, you can schedule to generate a report of unprotected resources in your cloud accounts.

VM restore changes

When a Virtual Machine (VM) is restored, if there is a Primary Private IPv4 address conflict, that is, if the original VM is present in stopped or running state, the restored VM is assigned a new Primary Private IPv4 address. If you continue with the restore there could be a hostname conflict on the network and domain controller override.

Ensure that there is no hostname conflict before the VM is restored. The changes are applicable for both AWS and Azure resources.

Release for October 30, 2018

New and changed features

AWS application consistency using pre and post snapshot scripts

In Cloud Snapshot Manager, using the AWS SSM (Simple Systems Manager) framework, you can set up a document or a script to pause read/write operations to the application before the snapshot is taken and start it after the snapshot is taken, ensuring consistency of snapshot data for applications. This feature is applicable only for AWS VM snapshots.

For the feature to work seamlessly, you have to update your IAM policy. In the IAM policy, include the permission, ssm:DescribeDocument (describes the specified SSM document) and replace *arn:aws:ssm:*:*:document/CSM-Mount** with *arn:aws:ssm:*:*:document/CSM-**.

For more information, see the topics, *AWS minimum permission policy*, and *Prerequisites for application consistency* in *Online Help*.

Azure File Level Recovery

You can now access files from restored Azure disks. When initiating a file level recovery, you can identify the host to attach the disk to, as well as the number of hours that the disk remains attached. After that, the disk is detached from the host and deleted. The feature is already available for AWS since April, 2018.

Cloud Snapshot Manager REST APIs

Cloud Snapshot Manager introduces the first batch of REST APIs enabling integration of Cloud Snapshot Manager with external systems. The following REST APIs are available in this release:

- Take On-demand snapshots across all AWS and Azure accounts
- Restore from snapshots

Cloud Snapshot Manager Public APIs are in limited availability. You can request access to Cloud Snapshot Manager Public APIs at csm.engineering.escalation@dell.com. For requesting credentials to access public APIs, see Generating Credentials. The documented reference to API Specification is available at https://developer.dell.com/apis/5788/versions/latest.

Event forwarding using email notifications

In Cloud Snapshot Manager, you can now filter the type of the event you want to forward to one or more email addresses. This also enables integration with external event management services or receiving notifications through email when a backup job fails.

Release for September 11, 2018

New and changed features

Sample SSM document is changed

The sample AWS Systems Manager (SSM) document, CSM-Mount, to automate the file level recovery process is deprecated and replaced with CSM-Mount-Unmount. Previously, only details on mounting of volumes was included. The new document contains details on both mounting and unmounting of volumes. Replace the old document with the new one for file level recovery to work correctly. The document is available on the Help page of the Cloud Snapshot Manager portal.

Release for July 31, 2018

New and changed features

Cloud Snapshot Manager support for Azure is Generally Available

This release of Dell EMC Cloud Snapshot Manager extends its in-cloud data protection, delivering support for Microsoft Azure, which enables users to protect workloads in multiple clouds seamlessly from a single pane of glass. Azure support is available with all Cloud Snapshot Manager licenses and includes:

- Protection of Azure VMs with managed disks
- Same powerful policy engine enabling protection through tags and rules
- Cross-cloud job status, audit logging, and reporting
- Simple and modern online help

Release for April 30, 2018

New and changed features

For features that require additional permissions, make sure that your IAM Policy has been updated with the latest permissions. The policy can be updated by copying the Minimum Permission Policy in the Cloud Accounts page of the Cloud Snapshot Manager Portal.

Copy snapshots to remote regions for disaster recovery

CSM now enables you to keep copies of snapshots in remote regions so that you can quickly recover entire VMs or Volumes in other regions in case of a disaster in an AWS region. The snapshot is created in the same region as the resource, and then can be copied to one or more regions that the cloud account has access to. The selected remote regions are configured as part of the policy. The remote region copies and the expiration of those copies can be set based on the backup schedule.

Remote region copies of Databases are not currently supported. For protection plans with Remote Region Copies configured, remote copies are made for VMs and Volumes, but Databases only have the snapshot in the original resource region.

This feature helps you to:

- Back up data across different geographical locations to minimize data loss and recovery time
- Launch applications in new regions
- Move an application from one region to another

To restore these snapshots, CSM requires additional permissions in the AWS IAM policy for the feature to work seamlessly. The required permissions are:

- ec2:DescribeVpcs - Lists the VPCs from a region
- ec2:DescribeKeyPairs - Lists the key pairs from a region

VSS snapshots of Windows instances

Volume Shadow Copy Service (VSS) is a Windows integrated service that enables consistent point-in-time backups of VSS-compatible applications. CSM now provides the option to capture VSS snapshots of compatible VMs while taking on-demand and scheduled snapshots. If you select the option for any non-VSS compatible VM, CSM creates a standard snapshot. CSM leverages native AWS provided VSS capabilities to take VSS snapshots.

To leverage VSS snapshots, CSM requires additional permissions in the AWS IAM policy for the feature to work seamlessly. The required permissions are:

- ssm:SendCommand - Initiates the VSS snapshot
- ssm:GetCommandInvocation - Retrieves the output of the VSS snapshot command
- ssm:DescribeInstanceInformation - Retrieves instances with configuration that is needed for VSS snapshots

File Level Recovery

File Level Recovery (FLR) in CSM provides the capability to access volumes from VMs or Volume snapshots. This enables you to access files from the restored volumes for a period of time. When initiating a file level recovery, you can identify the host to attach the volume to, as well as the number of hours that the volume remains attached. After that, the volume is detached from the host and deleted. The original snapshot remains available for future recovery efforts. This is a powerful feature for VM administrators that enables recovery by files.

To automatically attach and detach the restored volumes, CSM requires additional permissions in the AWS IAM policy for the feature to work seamlessly. The required permissions are:

- ssm:SendCommand - Initiates the attach or detach commands
- ssm:GetCommandInvocation - Retrieves the output of the attach and detach commands that are issued to the instance
- ssm:DescribeInstanceInformation - Retrieves instances with configuration details

Change snapshot expiration time

In CSM, expired snapshots are deleted and are no longer available. You can continue to set the initial expiration of snapshots while creating a policy. In addition, you can now select multiple snapshots and change the expiration to a new date, to expire now, or to never expire.

Snapshot schedule type

In the Snapshot detail section, you can now view whether a snapshot was taken as part of a daily, weekly, or monthly schedule.

Release for January 31, 2018

New and changed features

Metering

CSM now monitors the number of instances you are protecting against what was purchased. It also monitors the entitlement expiration date and suspends the account if the entitlement is not renewed after a grace period of 30 days. During the grace period, all features are available. However, after the period, scheduled activities like snapshot creation, expiry, and dashboard updates cease to work. CSM notifies you about the following events:

- The entitlement expiry date in advance and on the day of expiry.
- The account suspension date in advance and on the day of suspension.
- Protecting more resources than the entitled quantity.

Time zone in protection plan

You can now specify an explicit time zone when creating a new protection plan. The protection plan runs at the specified start date or time for that time zone. Any existing plan is based on Coordinated Universal Time (UTC), and you have the ability to edit the time zone to set an explicit time zone if needed.

Release for November 20, 2017

New and changed features

Free trial

CSM now provides the ability for customers to sign up for a free trial for 30 days. You get an account with all features of CSM to protect 50 instances. After you make a purchase, you can continue to use the same account. To download the free trial version, go to www.dellemc.com/CSMfreetrial.

Support for AWS IAM role

You can create limited access cloud accounts with AWS Identity and Access Management (IAM) role. Previously, only access based on long term IAM user credentials was supported. You have to set up an AWS IAM role with limited permission policy for CSM. The key advantage of the IAM role is that the credentials are not stored in CSM. This is the recommended method of authentication by AWS.

Browse all snapshots of a resource for a duration of time

CSM enables you to browse all snapshots taken for a resource for a duration of time so that you can select a snapshot to delete or to restore. Previously, only the latest snapshots taken for the resource were displayed.

Improved dashboard graph performance

CSM displays charts in the dashboard based on the last poll of AWS resources instead of a real-time poll which could be slow when there are a large number of resources in AWS.

Release for September 26, 2017

This is the first release of Cloud Snapshot Manager and the following features have been introduced.

- Automation and orchestration of snapshots for Amazon Elastic Computer Cloud (EC2), Amazon Elastic Block Store (EBS), and Amazon Relational Database Service (RDS) as per policy.
- Discovery and visibility to resources in all AWS accounts in any region.
- Tag based protection policy assignment to resources.
- Deletion of snapshots as per retention policy to reduce storage costs.
- Easy restoration of EC2 instances including the configuration settings to any availability zone in the region.
- SaaS solution that requires zero infrastructure in the client Virtual Private Cloud (VPC).
- Multi-tenancy capabilities to enable multiple CSM accounts and users.
- Designed for any cloud infrastructure size with auto scaling, audit log, and reporting.

Product limits

Learn about known limitations that are found in Cloud Snapshot Manager or about the limitations of the cloud environment and how to work around them.

- Cloud Snapshot Manager has not been tested on mobile devices.
- Snapshots of Managed VMs in Azure Scale Set are not supported.
- AWS limits the number of RDS snapshots you can have to 100. If you exceed that number of Cloud Snapshot Manager snapshots, they might start failing. As a workaround, if the use case demands more snapshots, follow the steps at https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html to request a limit increase from AWS.
- Using a tag-based search for VMs or Volumes yields a single page of results with a list (limited to as many as 500) of VMs or Volumes. To focus the search result, use more specific tags and then search with those tags only.

- AWS limits the number of EBS snapshots you can have to 10,000. If you exceed that number of Cloud Snapshot Manager snapshots, they might start failing. If the use case demands more snapshots, follow the steps at https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html to request a limit increase from AWS.
- Cloud Snapshot Manager does not support protection of resources with the AWS reserved tags (with prefixes like `aws:`). This limitation is applicable for all AWS resource types except RDS and Aurora.

Notes, cautions, and warnings

ⓘ **NOTE:** A NOTE indicates important information that helps you make better use of your product.

△ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**