Cloud Manager

Cloud Manager 3.5

NetApp
April 21, 2020

Table of Contents

Cloud Manager

What's new in Cloud Manager 3.5

OnCommand Cloud Manager typically introduces a new release every month to bring you new features, enhancements, and bug fixes.

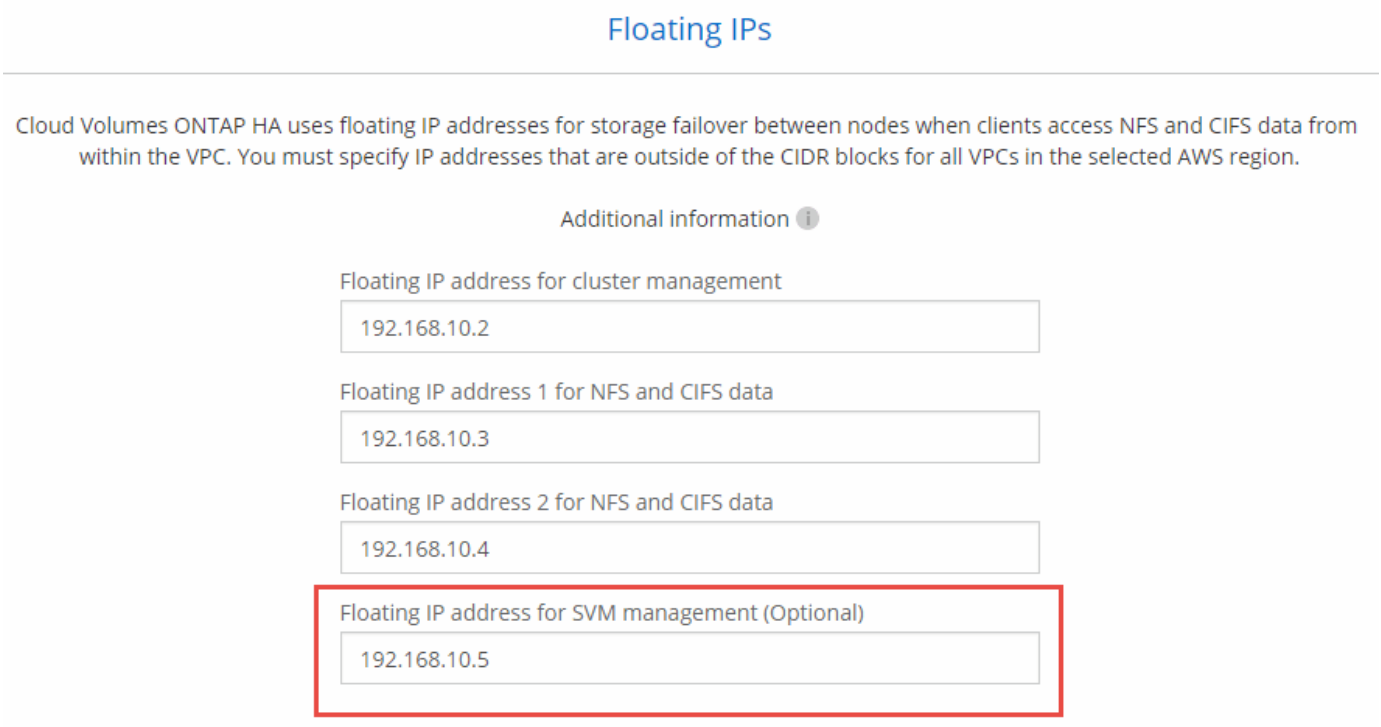
Cloud Manager 3.5.3 (2 Sept 2018)

Cloud Manager 3.5.3 includes a few enhancements.

- Creation of SVM management LIF for HA systems in multiple AZs
- Ability to break SMB/CIFS locks

Creation of SVM management LIF for HA systems in multiple AZs

When deploying Cloud Volumes ONTAP HA systems in multiple Availability Zones, you can now specify the floating IP address for an SVM management network interface (LIF). The SVM management LIF enables you to use SnapCenter or SnapDrive for Windows with the HA system.



Ability to break SMB/CIFS locks

In previous releases, upgrading or modifying the instance type and license type for a Cloud Volumes ONTAP HA system could fail if locks were present on SMB/CIFS files. Starting in this release, Cloud Manager can detect and break the locks before it proceeds with the operation. You simply need to

confirm when prompted.

Cloud Manager 3.5.2 (1 Aug 2018)

Cloud Manager 3.5.2 includes new features and enhancements.

Changes in this release require a new Azure permission for Cloud Manager. Read the changes below.

- Support for WORM storage
- Support for the auto tiering policy with Cloud Volumes ONTAP Standard
- Cloud Manager deployment in Azure from NetApp Cloud Central
- Animation added to used capacity charts
- Locks on Azure disks
- Tags on AWS CloudFormation stacks
- Deprecation of Cloud Volumes ONTAP encryption in AWS

Support for WORM storage

You can now activate WORM storage on new Cloud Volumes ONTAP systems. Write once, read many (WORM) storage enables you to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level.

Learn more about WORM storage.

Support for the auto tiering policy with Cloud Volumes ONTAP Standard

The *auto* volume tiering policy is now supported with the pay-as-you-go Standard license for Cloud Volumes ONTAP. You can select the auto tiering policy when creating, modifying, or replicating a volume. Data tiering enables automated tiering of cold data to low-cost object storage.

Auto is the default policy when creating new volumes for Cloud Volumes ONTAP Standard, Premium, and BYOL.

Learn more about data tiering.

Cloud Manager deployment in Azure from NetApp Cloud Central

You can now deploy new Cloud Manager systems in Microsoft Azure directly from NetApp Cloud Central. Cloud Central simplifies the deployment experience and provides a single location to view and manage multiple Cloud Manager systems. Providing your Azure credentials is secure and private because they are entered in an Azure pop-up window.

Learn more about Cloud Central.

Animation added to used capacity charts

An animation now shows you the amount of used capacity when you view volumes or aggregates.

Locks on Azure disks

Cloud Manager can now add locks to the Azure disks that it allocates to Cloud Volumes ONTAP. The locks help to ensure that the disks are not accidently deleted. This change requires a new permission so Cloud Manager can add, delete, and query the locks:

"Microsoft.Authorization/locks/*"

You should add this permission to the custom role that provides Cloud Manager with the required permissions.

Tags on AWS CloudFormation stacks

Cloud Manager now adds user tags to the AWS CloudFormation stacks that it creates. The tags can help to ensure that the stacks are not deleted by automated processes.

Deprecation of Cloud Volumes ONTAP encryption in AWS

Data-at-rest encryption of aggregates using external key managers is no longer supported when launching new Cloud Volumes ONTAP systems in AWS. Existing systems that use this feature are still supported; however, Cloud Volumes ONTAP encryption will be deprecated in the 9.5 release. NetApp will contact you to discuss how to upgrade those systems to the 9.5 release and how to implement a replacement encryption feature.

You can still enable data encryption on new systems by using the AWS Key Management Service (KMS).

Cloud Manager 3.5.1 (2 July 2018)

Cloud Manager 3.5.1 includes new features and enhancements.

- Support for pay-as-you-go in the AWS GovCloud (US) region
- Tiering levels for cold data
- Providing Azure permissions using a Managed Service Identity
- New used capacity charts

Support for pay-as-you-go in the AWS GovCloud (US) region

The pay-as-you-go version of Cloud Volumes ONTAP is now supported in the AWS GovCloud (US) region. This is in addition to supporting Cloud Volumes ONTAP BYOL in the GovCloud (US) region.

You can deploy Cloud Volumes ONTAP in the GovCloud (US) region just like any other region. Go to

NetApp Cloud Central and launch Cloud Manager in GovCloud (US). Then launch Cloud Volumes ONTAP PAYGO or BYOL by creating a new working environment in Cloud Manager.

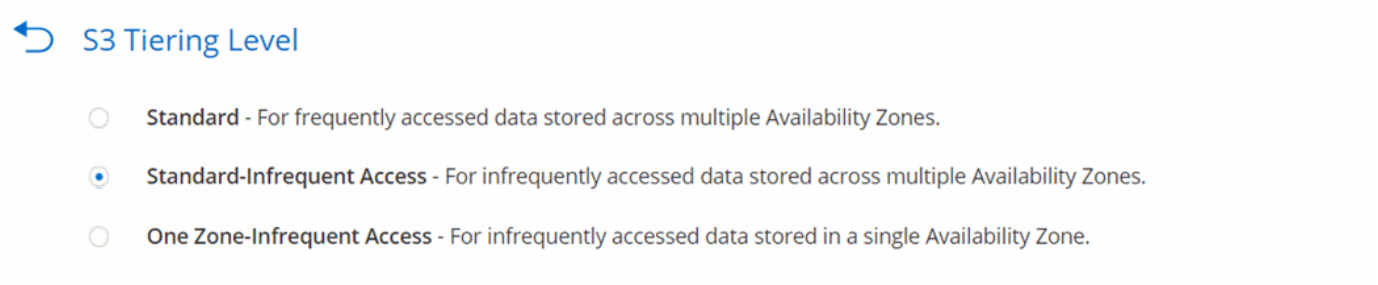
Tiering levels for cold data

After you deploy Cloud Volumes ONTAP, you can change the Amazon S3 storage class or the Azure Blob storage tier in which you want to store cold data. Changing the tiering level can reduce your storage costs, if you do not plan to access the data. The access costs are higher if you do access the data, so you must take that into consideration before you change the tiering level.

The tiering level is system wide—it is not per volume. For details about changing the tiering level, see Tiering cold data to low-cost object storage.

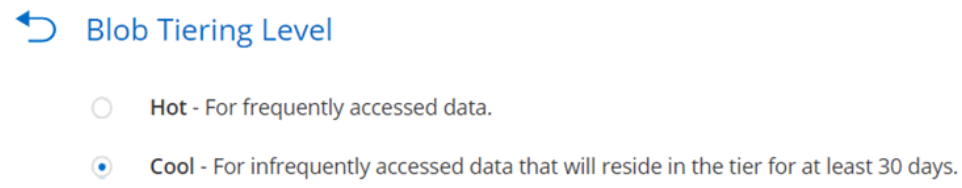
AWS tiering levels

In AWS, Cloud Volumes ONTAP uses **Standard** as the default storage class for data tiering to Amazon S3. You can change the storage class to either **Standard-Infrequent Access** or **One Zone-Infrequent Access**. When you change the tiering level, cold data starts in the **Standard** storage class and moves to the storage class that you selected, if the data is not accessed after 30 days. For details about S3 storage classes, refer to AWS documentation.



Azure tiering levels

In Azure, Cloud Volumes ONTAP uses the Azure **hot** storage tier as the default for data tiering to Blob storage. You can change to the Azure **cool** storage tier. When you change the tiering level, cold data starts in the **hot** storage tier and moves to the **cool** storage tier, if the data is not accessed after 30 days. For details about Azure Blob storage tiers, refer to Azure documentation.



Providing Azure permissions using a Managed Service Identity

You can now provide Azure permissions to Cloud Manager by using a Managed Service Identity. A Managed Service Identity allows a Cloud Manager virtual machine in Azure to identify itself to Azure

Active Directory without providing any credentials. This method is simpler than manually setting up an Azure service principal and providing the credentials to Cloud Manager.

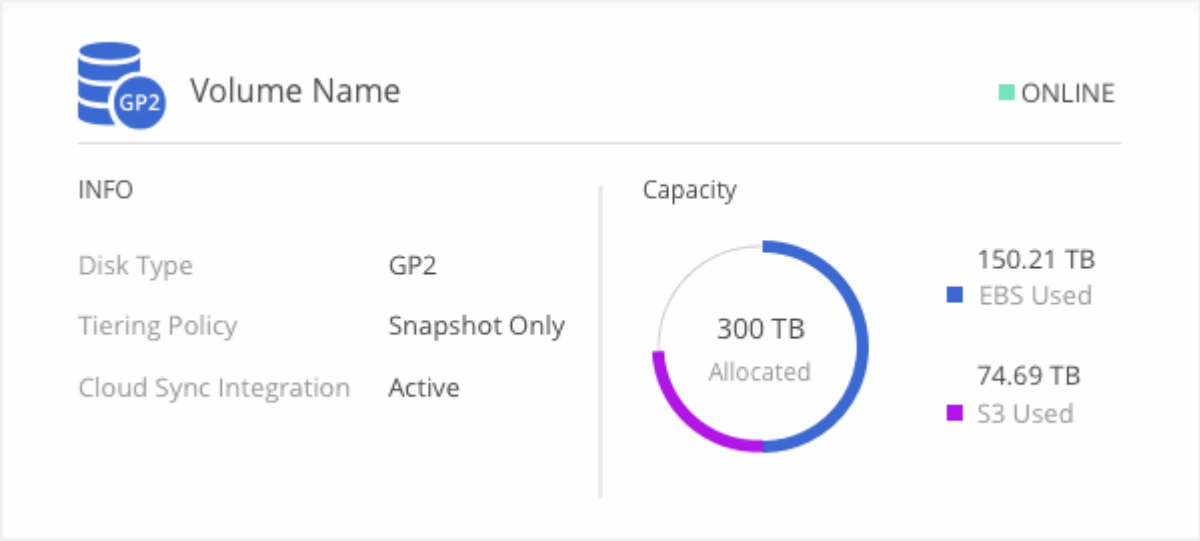
To use a Managed Service Identity with Cloud Manager, follow instructions for new Cloud Manager virtual machines or instructions for existing Cloud Manager virtual machines.

Managed Service Identities are not supported in the Azure US Gov regions and in the Germany regions. You must grant Azure permissions to Cloud Manager using a service principal and credentials.

For more information about Managed Service Identities, refer to Azure documentation.

New used capacity charts

Cloud Manager now provides a graphical representation of used capacity when viewing volumes and aggregates.



Cloud Manager 3.5 (3 June 2018)

Cloud Manager 3.5 includes new features and enhancements.

- Support for Cloud Volumes ONTAP 9.4
- New permissions required for Cloud Volumes ONTAP 9.4
- Cloud Manager integration with NetApp Cloud Central
- Support for the m4.large instance type
- Marketplace image now based on RHEL 7.4

Support for Cloud Volumes ONTAP 9.4

You can now deploy new Cloud Volumes ONTAP 9.4 systems from Cloud Manager and upgrade your

existing systems to the 9.4 release. Cloud Manager also provides support for the new features introduced in Cloud Volumes ONTAP 9.4.

New permissions required for Cloud Volumes ONTAP 9.4

Cloud Manager requires new permissions for key features in the Cloud Volumes ONTAP 9.4 release. To ensure that your Cloud Manager systems can deploy and manage Cloud Volumes ONTAP 9.4 systems, you must update your Cloud Manager policy by adding the following permissions:

- For AWS: "ec2:DescribeInstanceAttribute",

  Cloud Manager uses this permission to verify that enhanced networking is enabled for supported instance types.

- For Azure: "Microsoft.Network/virtualNetworks/subnets/write",

  Cloud Manager uses this permission to enable VNet service endpoints for data tiering.

You can find the entire list of required permissions in the latest policies provided by NetApp.

Cloud Manager integration with NetApp Cloud Central

When upgrading to Cloud Manager 3.5, NetApp will choose specific Cloud Manager systems to integrate with NetApp Cloud Central, if they are not already integrated. During this process, NetApp migrates all local user accounts in your Cloud Manager system to the centralized user authentication available in Cloud Central. After the upgrade is complete, you simply need to log in.

If you have questions, refer to this FAQ.

Support for the m4.large instance type

Cloud Manager is now supported with the m4.large EC2 instance type. m3.large is no longer supported.

For a list of supported Cloud Manager configurations, see Cloud Manager host requirements.

Marketplace image now based on RHEL 7.4

The operating system for the Cloud Manager marketplace image in AWS and Azure is now Red Hat Enterprise Linux 7.4.

Known issues

Known issues identify problems that might prevent you from using this release of the product successfully.

There are no known issues in this release of Cloud Manager.

You can find known issues for Cloud Volumes ONTAP in the Cloud Volumes ONTAP Release Notes and for ONTAP software in general in the ONTAP Release Notes.

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

Active Directory not supported by default with new installations of Cloud Manager

Starting with version 3.4, new installations of Cloud Manager do not support using your organization's Active Directory authentication for user management. If needed, NetApp can help you set up Active Directory with Cloud Manager. Click the chat icon in the lower right of Cloud Manager to get assistance.

Limitations with the AWS GovCloud (US) region

- Cloud Manager must be deployed in the AWS GovCloud (US) region if you want to launch Cloud Volumes ONTAP instances in the AWS GovCloud (US) region.
- When deployed in the AWS GovCloud (US) region, Cloud Manager cannot discover ONTAP clusters in a NetApp Private Storage for Microsoft Azure configuration or a NetApp Private Storage for SoftLayer configuration.

Volume View limitations

- The Volume View is not supported in the AWS GovCloud (US) region, in the AWS Commercial Cloud Services environment, and in Microsoft Azure.
- The Volume View enables you to create NFS volumes only.
- Cloud Manager does not launch Cloud Volumes ONTAP BYOL instances in the Volume View.

Cloud Manager does not verify IP addresses of key managers

When you add a key manager to Cloud Manager, it does not verify the IP address that you entered because Cloud Manager does not communicate with key managers. If the IP address is incorrect, you are notified later when you try to create a Cloud Volumes ONTAP working environment. Be sure to verify key manager IP addresses after you enter them.

Cloud Manager does not set up iSCSI volumes

When you create a volume in Cloud Manager using the Storage System View, you can choose the NFS or CIFS protocol. You must use OnCommand System Manager to create a volume for iSCSI.

Storage Virtual Machine (SVM) limitation

Cloud Volumes ONTAP supports one data-serving SVM and one or more SVMs used for disaster recovery.

Cloud Manager does not provide any setup or orchestration support for SVM disaster recovery. It also does not support storage-related tasks on any additional SVMs. You must use System Manager or the CLI for SVM disaster recovery.