



Cloud Manager

Cloud Manager

NetApp

June 15, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/reference_new_occm.html on June 15, 2020.
Always check docs.netapp.com for the latest.

Table of Contents

- Cloud Manager 1
 - What’s new in Cloud Manager 3.8 1
 - Known issues 14
 - Known limitations 14

Cloud Manager

What's new in Cloud Manager 3.8

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



Looking for a previous release?

[What's new in 3.7](#)

[What's new in 3.6](#)

[What's new in 3.5](#)

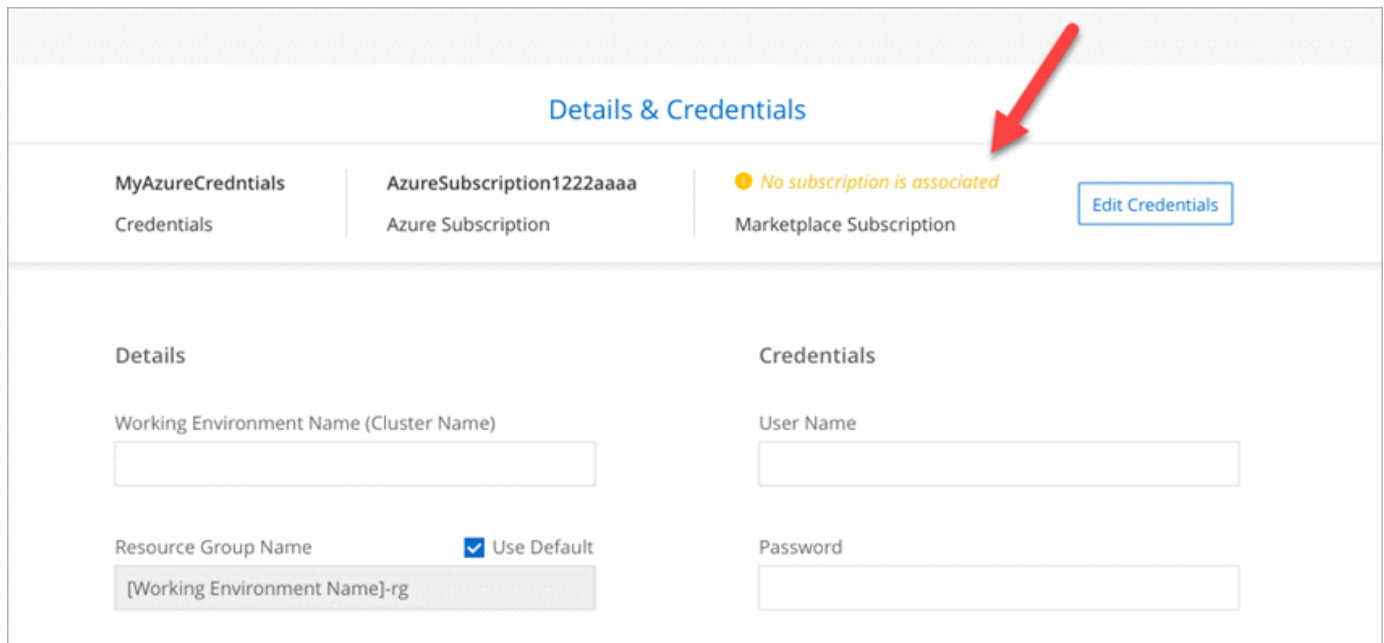
Cloud Manager 3.8.5 (31 May 2020)

- [New subscription required in the Azure Marketplace](#)
- [Backup to Cloud enhancements](#)
- [Cloud Compliance enhancements](#)

New subscription required in the Azure Marketplace

A new subscription is available in the Azure Marketplace. This one-time subscription is required to deploy Cloud Volumes ONTAP 9.7 PAYGO (except for your 30-day free trial system). The subscription also enables us to offer add-on features for Cloud Volumes ONTAP PAYGO and BYOL. You'll be charged from this subscription for every Cloud Volumes ONTAP PAYGO system that you create and each add-on feature that you enable.

Cloud Manager will prompt you to subscribe to this offering when you deploy a new Cloud Volumes ONTAP system (9.7 P1 or later).



The screenshot shows a web interface titled "Details & Credentials". At the top, there are three sections: "MyAzureCredntials Credentials", "AzureSubscription1222aaaa Azure Subscription", and "No subscription is associated Marketplace Subscription". A red arrow points to the "No subscription is associated" message. To the right of these sections is an "Edit Credentials" button. Below the top bar, there are two columns: "Details" and "Credentials". The "Details" column contains a "Working Environment Name (Cluster Name)" text box, a "Resource Group Name" text box with a "Use Default" checkbox, and a placeholder "[Working Environment Name]-rg". The "Credentials" column contains a "User Name" text box and a "Password" text box.

Backup to Cloud enhancements

The following enhancements are now available for Backup to Cloud.

- In Azure, you can now create a new resource group or select an existing resource group instead of having Cloud Manager create one for you. The resource group can't be changed after you enable Backup to Cloud.
- In AWS, you can now back up Cloud Volumes ONTAP instances that reside on a different AWS account than your Cloud Manager AWS account.
- Additional options are now available when selecting the backup schedule for volumes. In addition to daily, weekly, and monthly backup options, you can now select one of the system-defined policies that provide combination policies such as 30 daily, 13 weekly, and 12 monthly backups.
- After deleting all backups for a volume, you can now start creating backups again for that volume. This was a known limitation in the previous release.

Cloud Compliance enhancements

The following enhancements are available for Cloud Compliance.

- You can now scan S3 buckets that are in different AWS accounts than the Cloud Compliance instance. You just need to create a role on that new account so that the existing Cloud Compliance instance can connect to those buckets. [Learn more](#).

If you configured Cloud Compliance before release 3.8.5, you will need to modify the existing [IAM role for the Cloud Compliance instance](#) to use this functionality.

- You can now filter the contents of the investigation page to display only the results you want to see. Filters include working environment, category, private data, file type, last modified date, and whether the S3 object's permissions are open to public access.

Dashboard Investigation		3011 Results Found					
FILTERS:		File Name ↓↑	Personal ↓↑	Sensitive Personal ↓↑	Data Subjects ↓↑	File Type ↓↑	
Working Environment	+	> Expense Report EXP-TPO-1060388	6	3	16	PDF	
Storage Repository	+	> Expense Report EXP-TPO-1060388	9	2	11	PDF	
Category	+	> Expense Report EXP-TPO-1060388	4	1	7	PDF	
Private Data 6	+	> Expense Report EXP-TPO-1060388	9	1	6	PDF	
File Type	+	> Expense Report EXP-TPO-1060388	8	6	4	PDF	

- You can now activate and deactivate Cloud Compliance on a working environment directly from the Cloud Compliance tab.

Cloud Manager 3.8.4 update (10 May 2020)

We released an enhancement to Cloud Manager 3.8.4.

Cloud Insights integration

By leveraging NetApp's Cloud Insights service, Cloud Manager gives you insights into the health and performance of your Cloud Volumes ONTAP instances and helps you troubleshoot and optimize the performance of your cloud storage environment. [Learn more.](#)

Cloud Manager 3.8.4 (3 May 2020)

Cloud Manager 3.8.4 includes the following improvement.

Backup to Cloud enhancements

The following enhancements are now available for Backup to Cloud (previously called *Backup to S3* for AWS):

- **Backing up to Azure Blob storage**

Backup to Cloud is now available for Cloud Volumes ONTAP in Azure. Backup to Cloud provides backup and restore capabilities for protection, and long-term archive of your cloud data. [Learn more.](#)

- **Deleting backups**

You can now delete all backups for a specific volume directly from the Cloud Manager interface. [Learn more.](#)

Cloud Manager 3.8.3 (5 Apr 2020)

- [Cloud Tiering integration](#)
- [Data migration to Azure NetApp Files](#)
- [Cloud Compliance enhancements](#)
- [Backup to S3 enhancements](#)
- [iSCSI volumes using APIs](#)

Cloud Tiering integration

NetApp's Cloud Tiering service is now available from within Cloud Manager. Cloud Tiering enables you to tier data from an on-premises ONTAP cluster to lower-cost object storage in the cloud. This frees up high-performance storage space on the cluster for more workloads.

[Learn more.](#)

Data migration to Azure NetApp Files

You can now migrate NFS or SMB data to Azure NetApp Files directly from Cloud Manager. Data syncs are powered by NetApp's Cloud Sync service.

[Learn how to migrate data to Azure NetApp Files.](#)

Cloud Compliance enhancements

The following enhancements are now available for Cloud Compliance.

- **30-day free trial for Amazon S3**

A 30-day free trial is now available to scan Amazon S3 data with Cloud Compliance. If you previously enabled Cloud Compliance on Amazon S3, your 30-day free trial is active starting today (5 Apr 2020).

A subscription to the AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends. [Learn how to subscribe.](#)

[Learn about pricing to scan Amazon S3.](#)

- **New personal data type**

Cloud Compliance can now find a new national identifier in files: Brazilian ID (CPF).

[Learn more about personal data types.](#)

- **Support for additional metadata categories**

Cloud Compliance can now categorize your data into nine additional metadata categories. [See the](#)

[full list of supported metadata categories.](#)

Backup to S3 enhancements

The following enhancements are now available for the Backup to S3 service.

- **S3 lifecycle policy for backups**

Backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.

- **Deleting backups**

You can now delete backups using a Cloud Manager API. [Learn more.](#)

- **Block public access**

Cloud Manager now enables the [Amazon S3 Block Public Access feature](#) on the S3 bucket where backups are stored.

iSCSI volumes using APIs

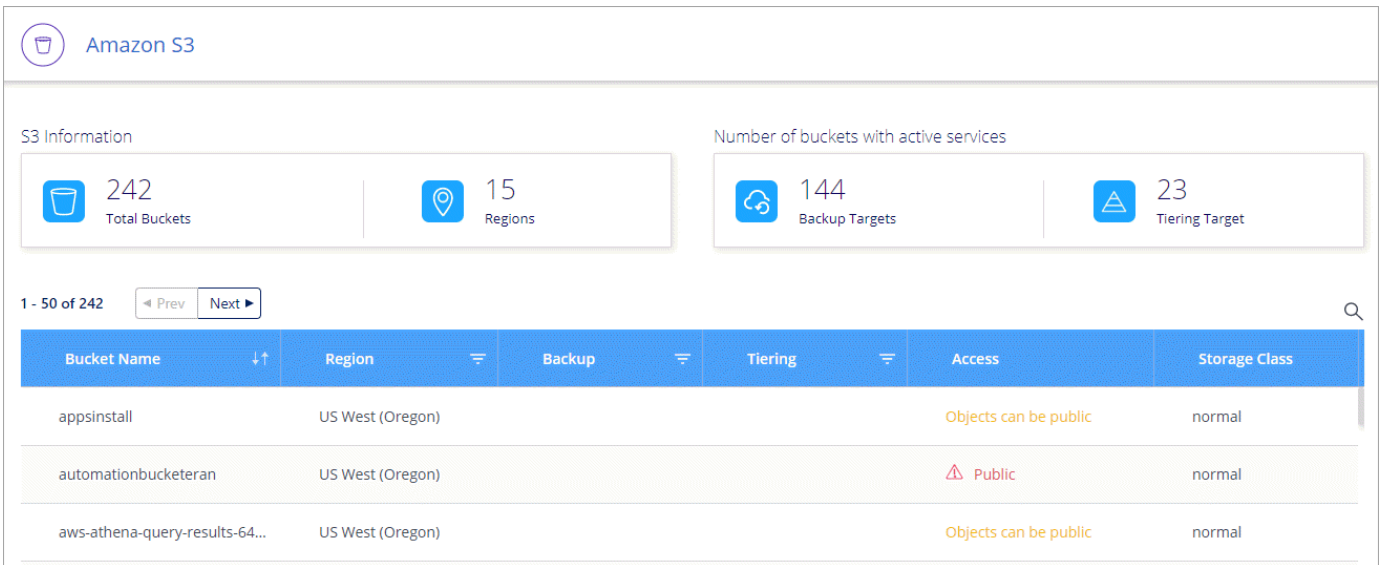
The Cloud Manager APIs now enable you to create iSCSI volumes. [View an example here.](#)

Cloud Manager 3.8.2 (1 Mar 2020)

- [Amazon S3 working environments](#)
- [Cloud Compliance enhancements](#)
- [NFS version for volumes](#)
- [Support for Azure US Gov regions](#)

Amazon S3 working environments

Cloud Manager now automatically discovers information about the Amazon S3 buckets that reside in the AWS account where it's installed. This enables you to easily see details about your S3 buckets, including the region, access level, storage class, and whether the bucket is used with Cloud Volumes ONTAP for backups or data tiering. And you can scan the S3 buckets with Cloud Compliance, as described below.



Cloud Compliance enhancements

The following enhancements are now available for Cloud Compliance.

- **Support for Amazon S3**

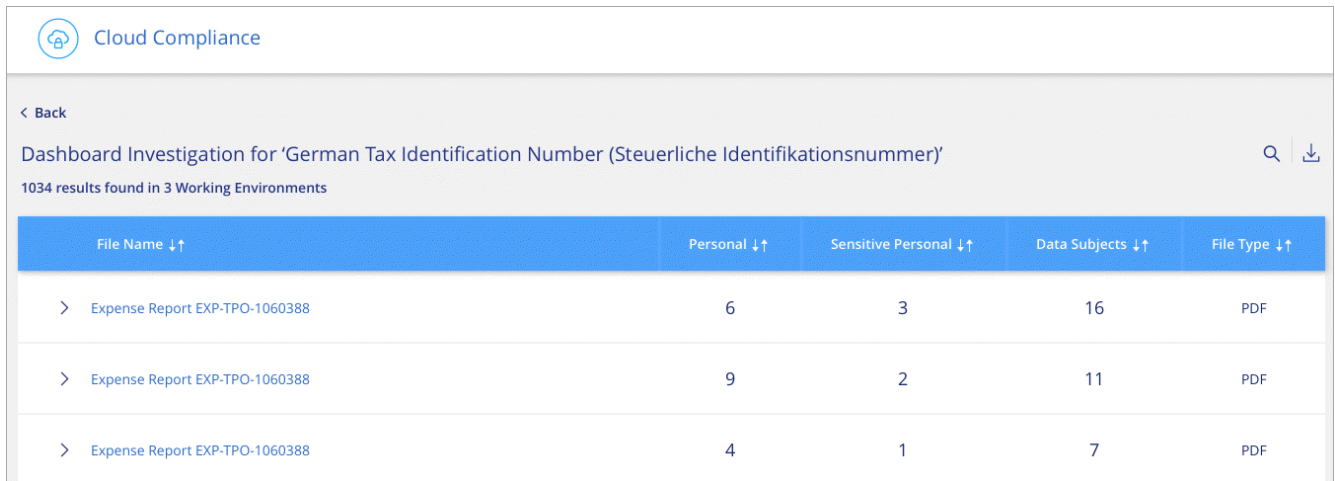
Cloud Compliance can now scan your Amazon S3 buckets to identify the personal and sensitive data that resides in S3 object storage. Cloud Compliance can scan any bucket in the account, regardless if it was created for a NetApp solution.

[Learn how to get started.](#)

- **Investigation page**

A new Investigation page is now available for each type of personal file, sensitive personal file, category, and file type. The page shows details about the affected files and enables you to sort by the files that include the most personal data, sensitive personal data, and names of data subjects. This page replaces the CSV report that was previously available.

Here's a sample:



[Learn more about the Investigation page.](#)

- **PCI DSS Report**

A new Payment Card Industry Data Security Standard (PCI DSS) Report is now available. This report can help you identify the distribution of credit card information across your files. You can view how many files contain credit card information, whether the working environments are protected by encryption or ransomware protection, retention details, and more.

[Learn more about the PCI DSS report.](#)

- **New sensitive personal data type**

Cloud Compliance can now find ICD-10-CM Medical Codes, which are used in the medical and health industry.

NFS version for volumes

You can now select the NFS version to enable on a volume when you create or edit a volume for Cloud Volumes ONTAP.

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

i Default Policy

Protocol

☒ NFS Protocol ☐ CIFS Protocol

Access Control:

Custom export policy

Advanced options

Select NFS Version: ☒ NFSv3 ☒ NFSv4

Support for Azure US Gov regions

Cloud Volumes ONTAP HA pairs are now supported in Azure US Gov regions.

[See the list of supported Azure regions.](#)

Cloud Manager 3.8.1 update (16 Feb 2020)

We released a few enhancements to Cloud Manager 3.8.1.

Backup to S3 enhancements

- Backup copies are now stored in an S3 bucket that Cloud Manager creates in your AWS account, with one bucket per Cloud Volumes ONTAP working environment.
- Backup to S3 is now supported in all AWS regions [where Cloud Volumes ONTAP is supported](#).
- You can set the backup schedule to daily, weekly, or monthly.
- Cloud Manager no longer needs to set up *private links* to the Backup to S3 service.

Additional S3 permissions are required for these enhancements. The IAM role that provides Cloud Manager with permissions must include permissions from the latest [Cloud Manager policy](#).

[Learn more about Backup to S3.](#)

AWS updates

We've introduced support for new EC2 instances and a change in the number of supported data disks for Cloud Volumes ONTAP 9.6 and 9.7. Check out the changes in the Cloud Volumes ONTAP Release Notes.

- [Cloud Volumes ONTAP 9.7 Release Notes](#)
- [Cloud Volumes ONTAP 9.6 Release Notes](#)

Cloud Manager 3.8.1 (2 Feb 2020)

- [Cloud Compliance enhancements](#)
- [Enhancements to accounts and subscriptions](#)
- [Timeline enhancements](#)

Cloud Compliance enhancements

The following enhancements are now available for Cloud Compliance.

- **Support for Azure NetApp Files**

We're pleased to announce that Cloud Compliance can now scan Azure NetApp Files to identify personal and sensitive data that resides on volumes.

[Learn how to get started.](#)

- **Scan status**

Cloud Compliance now shows you a scan status for each CIFS and NFS volume, including error messages that you can use to correct any issues.

< Back			
Volumes Scan Status for cognigoWE			
2 Volumes found			
Name ↑↑	Protocol ↑↑	Status ↑↑	Details ↑↑
\\172.31.134.172\cifs_vol_share	CIFS	Not Scanning	The CIFS credentials that you provided don't have sufficient per...
172.31.134.172:/parallel_tests	NFS	Continuously Scanning	

- **Filter dashboard by working environment**

You can now filter the contents of the Cloud Compliance dashboard to see compliance data for specific working environments.

Cloud Compliance

All Working Environments (12)

☒ Select all

☒ ANF - Azure NetApp Files ANF

☒ Working Environment Name 1 CVO

☒ Working Environment Name 2 CVS

☒ Working Environment Name 3 CVS

☒ Working Environment Name 4 CVO

View
Cancel

Personal Files ⓘ
View All

Email Address 2,700 Files

Credit Card 2,700 Files

20% Personal

5% Sensitive Personal

7,000 Sensitive Personal Files ⓘ
View All

Health 2,700 Files

Ethnicity 2,700 Files

- **New personal data type**

Cloud Compliance can now identify a California Driver's License when scanning data.

- **Support for additional categories**


Three additional categories are supported: Application data, logs, and database and index files.

[Learn more about categories.](#)

Enhancements to accounts and subscriptions

We've made it easier to select an AWS account or GCP project and an associated marketplace subscription for a pay-as-you-go Cloud Volumes ONTAP system. These enhancements help to ensure that you're paying from the right account or project.

For example, when you create a system in AWS, click **Edit Credentials** if you don't want to use the default account and subscription:

Details & Credentials		
Instance Profile Credentials	 Account ID	QA Subscription Marketplace Subscription
Edit Credentials		


From there, you can choose the account credentials that you want to use and the associated AWS marketplace subscription. You can even add a marketplace subscription, if you need to.

Edit Account & Add Subscription

Credentials

Instance Profile | Account ID: [REDACTED]

Associated Subscription

 QA Subscription

Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.


 [Add Subscription](#)

Apply


Cancel

And if you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page in the settings:

 IT

 Add Subscription

 Edit

 Delete



[REDACTED]
AWS Account ID

[REDACTED]
AWS Access Key

No Subscription
Subscription

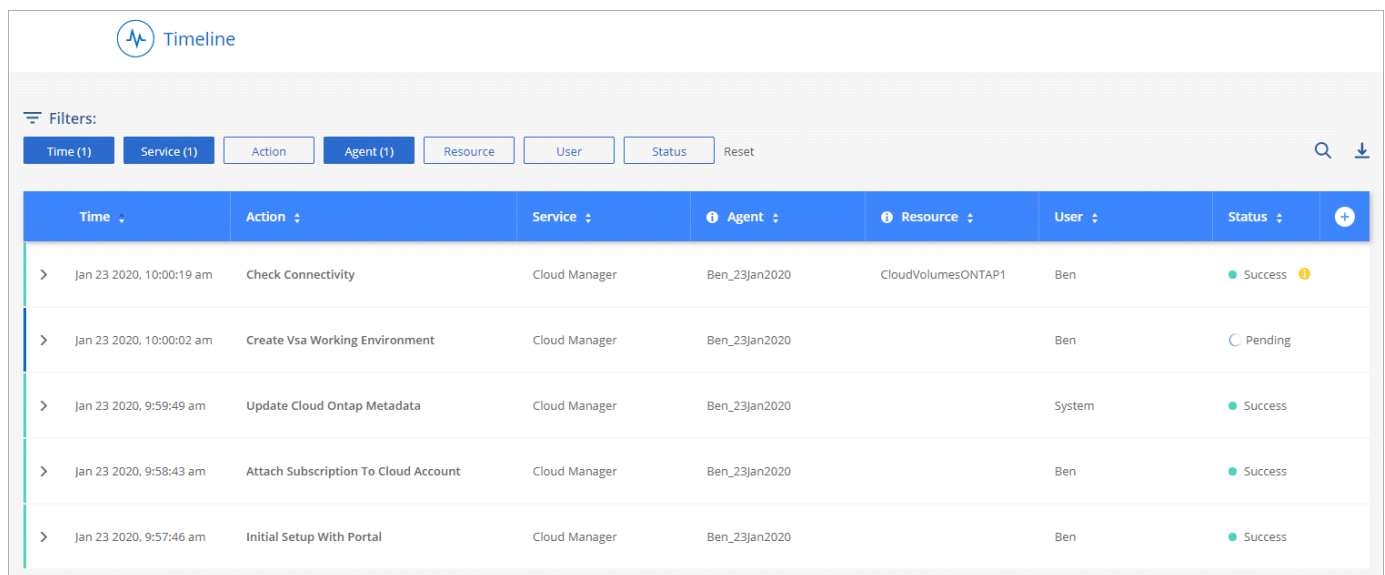
0
Working Environments

[Learn how to manage AWS credentials in Cloud Manager.](#)

Timeline enhancements

The Timeline was enhanced to provide you with more information about the NetApp cloud services that you use.

- The Timeline now shows actions for all Cloud Manager systems within the same Cloud Central account
- You can now find information more easily by filtering, searching, and adding and removing columns
- You can now download the timeline data in CSV format
- In the future, the Timeline will show actions for each NetApp cloud service that you use (but you can filter the information down to a single service)



The screenshot shows the 'Timeline' interface in Cloud Manager. At the top, there's a 'Filters' section with buttons for 'Time (1)', 'Service (1)', 'Action', 'Agent (1)', 'Resource', 'User', and 'Status', along with a 'Reset' button. Below the filters is a table with columns: Time, Action, Service, Agent, Resource, User, Status, and a plus icon for more options. The table contains five rows of events, each with a chevron icon on the left.

Time	Action	Service	Agent	Resource	User	Status	
> Jan 23 2020, 10:00:19 am	Check Connectivity	Cloud Manager	Ben_23Jan2020	CloudVolumesONTAP1	Ben	Success	🔔
> Jan 23 2020, 10:00:02 am	Create Vsa Working Environment	Cloud Manager	Ben_23Jan2020		Ben	Pending	
> Jan 23 2020, 9:59:49 am	Update Cloud Ontap Metadata	Cloud Manager	Ben_23Jan2020		System	Success	
> Jan 23 2020, 9:58:43 am	Attach Subscription To Cloud Account	Cloud Manager	Ben_23Jan2020		Ben	Success	
> Jan 23 2020, 9:57:46 am	Initial Setup With Portal	Cloud Manager	Ben_23Jan2020		Ben	Success	

Cloud Manager 3.8 (8 Jan 2020)

- [HA enhancements in Azure](#)
- [Data tiering enhancements in GCP](#)

HA enhancements in Azure

The following enhancements are now available for Cloud Volumes ONTAP HA pairs in Azure.

- **Override CIFS locks for Cloud Volumes ONTAP HA in Azure**

You can now enable a setting in Cloud Manager that prevents issues with Cloud Volumes ONTAP storage failover during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions. [Learn more.](#)

- **HTTPS connection from Cloud Volumes ONTAP to storage accounts**

You can now enable an HTTPS connection from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts when creating a working environment. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

- **Support for Azure general-purpose v2 storage accounts**

The storage accounts that Cloud Manager creates for Cloud Volumes ONTAP 9.7 HA pairs are now general-purpose v2 storage accounts.

Data tiering enhancements in GCP

The following enhancements are available for Cloud Volumes ONTAP data tiering in GCP.

- **Google Cloud storage classes for data tiering**

You can now choose a storage class for data that Cloud Volumes ONTAP tiers to Google Cloud Storage:

- Standard Storage (default)
- Nearline Storage
- Coldline Storage

[Learn more about Google Cloud storage classes.](#)

[Learn how to change the storage class for Cloud Volumes ONTAP.](#)

- **Data tiering using a service account**

Starting with the 9.7 release, Cloud Manager now sets a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. This change provides more security and requires less setup. For step-by-step instructions when deploying a new system, [see step 3 on this page](#).

The following image shows the Working Environment wizard where you can select a storage class and service account:

Data Tiering in Google Cloud Platform

Data tiering can reduce your storage costs by automatically tiering cold data to a Google Cloud Storage bucket.

Tiering data to object storage	Data Tiering Tiering Enabled	Edit	Storage Class Standard Storage	Edit
--	---------------------------------	----------------------	-----------------------------------	----------------------

Select a GCP service account to enable data tiering.
[Learn more about data tiering in GCP.](#)

Service Account

tiering-cloud-volumes-ontap

Cloud Manager requires the following GCP permissions for these enhancements, as shown in the latest [Cloud Manager policy for GCP](#).

- `storage.buckets.update`
- `compute.instances.setServiceAccount`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.list`

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.

Cloud Manager should remain running at all times

Cloud Manager is a key component in the health and billing of Cloud Volumes ONTAP. If Cloud Manager is powered down, Cloud Volumes ONTAP systems will shut down after losing communication

with Cloud Manager for longer than 4 days.

Shared Linux hosts are not supported

Cloud Manager is not supported on a host that is shared with other applications. The host must be a dedicated host.

Cloud Manager does not support FlexGroup volumes

While Cloud Volumes ONTAP supports FlexGroup volumes, Cloud Manager does not. If you create a FlexGroup volume from System Manager or from the CLI, then you should set Cloud Manager's Capacity Management mode to Manual. Automatic mode might not work properly with FlexGroup volumes.

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.

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. The one data-serving SVM spans the entire Cloud Volumes ONTAP system (HA pair or single node).

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.

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.