



Cloud Manager release notes

Release Notes

NetApp
July 19, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-relnotes/index.html> on July 19, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Cloud Manager release notes 1
- Recent changes in Cloud Manager 2
 - Administrative features 2
 - Azure NetApp Files 4
 - Amazon FSx for ONTAP 5
 - Application Template 6
 - Cloud Backup 7
 - Cloud Data Sense 9
 - Cloud Sync 11
 - Cloud Tiering 14
 - Cloud Volumes ONTAP 15
 - Cloud Volumes Service for GCP 19
 - Compute 20
 - Global File Cache 20
 - Kubernetes 21
 - Monitoring 22
 - On-prem ONTAP clusters 23
 - Ransomware Protection 23
 - Replication 24
 - SnapCenter Service 25
- Release notes index 26
 - Storage 26
 - Data services 26
 - Administration 26

Cloud Manager release notes

Recent changes in Cloud Manager

Learn about the most recent changes to the cloud services that are part of the Cloud Manager platform. For more details, go to the [full set of release notes](#) for each individual service.

Administrative features

This section describes new features related to Cloud Manager's administration features: Accounts, Connectors, cloud provider credentials, and more.

15 July 2022

Policy changes

We updated the documentation by adding the Cloud Manager policies directly inside the docs. This means you can now view the required permissions for the Connector and Cloud Volumes ONTAP right alongside the steps that describe how to set them up. These policies were previously accessible from a page on the NetApp Support Site.

[Here's an example that shows the AWS IAM role permissions used to create a Connector.](#)

We also created a page that provides links to each of the policies. [View the permissions summary for Cloud Manager.](#)

3 July 2022

Connector 3.9.20

- We've introduced a new way to navigate to the growing list of features in the Cloud Manager interface. All the familiar Cloud Manager capabilities can now be easily found by hovering over the left panel.



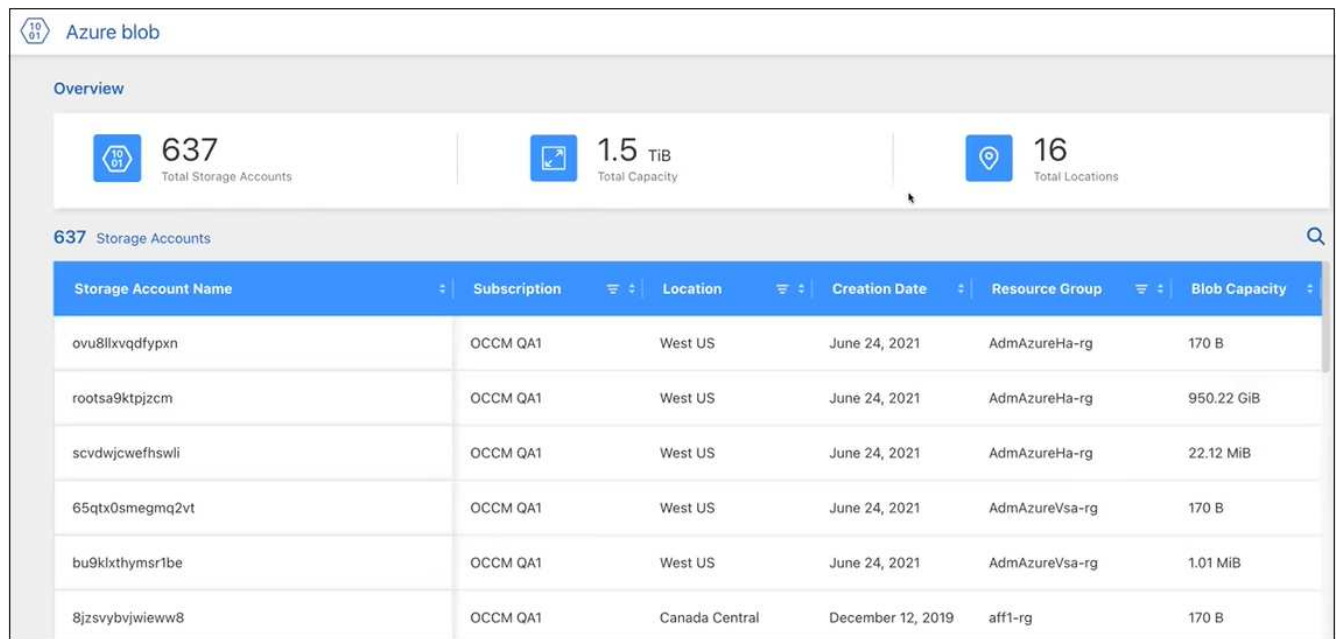
- You can now configure Cloud Manager to send notifications by email so you can be informed of important system activity even when you're not logged into the system.

[Learn more about monitoring operations in your account.](#)

- Cloud Manager now supports Azure Blob storage and Google Cloud Storage as working environments, similar to Amazon S3 support.

After you install a Connector in Azure or Google Cloud, Cloud Manager now automatically discovers information about Azure Blob storage in your Azure subscription or the Google Cloud Storage in the project where the Connector is installed. Cloud Manager displays the object storage as a working environment that you can open to view more detailed information.

Here's an example of an Azure Blob working environment:



- We redesigned the resources page for an Amazon S3 working environment by providing more detailed information about S3 buckets, such as capacity, encryption details, and more.
- The Connector is now supported in the following Google Cloud regions:
 - Madrid (europe-southwest1)
 - Paris (europe-west9)
 - Warsaw (europe-central2)
- The Connector is now supported in the Azure West US 3 region.

[View the full list of supported regions](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

28 June 2022

Log in with NetApp credentials

When new users sign up to Cloud Central, they can now select the **Log in with NetApp** option to log in with their NetApp Support Site credentials. This is an alternative to entering an email address and password.



Existing logins that use an email address and password need to keep using that login method. The Log in with NetApp option is available for new users who sign up.

Azure NetApp Files

11 April 2021

Support for volume templates

A new Application Templates service enables you to set up a volume template for Azure NetApp Files. The template should make your job easier because certain volume parameters will already be defined in the template, such as capacity pool, size, protocol, VNet and subnet where the volume should reside, and more. When a parameter is already predefined, you can just skip to the next volume parameter.

- [Learn about Application Templates and how you can use them in your environment](#)
- [Learn how to create an Azure NetApp Files volume from a template](#)

8 March 2021

Dynamically change service levels

You can now dynamically change the service level for a volume to meet workload needs and optimize your costs. The volume is moved to the other capacity pool with no impact to the volume.

[Learn how to change a volume's service level.](#)

3 August 2020

Azure NetApp Files set up and management

Set up and manage Azure NetApp Files directly from Cloud Manager. After you create an Azure NetApp Files working environment, you can complete the following tasks:

- Create NFS and SMB volumes.
- Manage capacity pools and volume snapshots

Cloud Manager enables you to create, delete, and restore volume snapshots. You can also create new capacity pools and specify their service levels.

- Edit a volume by changing its size and managing tags.

The ability to create and manage Azure NetApp Files directly from Cloud Manager replaces the previous data migration functionality.

Amazon FSx for ONTAP

3 July 2022

- You can now select a single or multiple Availability Zone HA deployment model.

[Create an FSx for ONTAP working environment](#)

- AWS GovCloud account authentication is now supported in Cloud Manager.

[Set up the IAM role](#)

27 February 2022

Assume IAM role

When you create an FSx for ONTAP working environment, you now must provide the ARN of an IAM role that Cloud Manager can assume to create an FSx for ONTAP working environment. You previously needed to provide AWS access keys.

[Learn how to set up permissions for FSx for ONTAP.](#)

31 October 2021

Create iSCSI volumes using Cloud Manager API

You can create iSCSI volumes for FSx for ONTAP using the Cloud Manager API and manage them in your working environment.

Select volume units when creating volumes

You can [select volume units \(GiB or TiB\) when creating volumes](#) in FSx for ONTAP.

Application Template

3 March 2022

Now you can build a Template to find specific working environments

Using the "Find Existing Resources" action you can identify the working environment, and then use other template actions, such as creating a volume, to easily perform actions on existing working environments. [Go here for details.](#)

Ability to create a Cloud Volumes ONTAP HA working environment in AWS

The existing support for creating a Cloud Volumes ONTAP working environment in AWS has been expanded to include creating a high-availability system in addition to a single-node system. [See how to create a template for a Cloud Volumes ONTAP working environment.](#)

9 February 2022

Now you can build a Template to find specific existing volumes and then enable Cloud Backup

Using the new "Find Resource" action you can identify all the volumes on which you want to enable Cloud Backup, and then use the Cloud Backup action to enable backup on those volumes.

Current support is for volumes on Cloud Volumes ONTAP and on-premises ONTAP systems. [Go here for details.](#)

31 October 2021

Now you can tag your Sync relationships so you can group or categorize them for easy access

[Learn more about resource tagging.](#)

Cloud Backup

13 July 2022

Support has been added to back up SnapLock Enterprise volumes

Now you can use Cloud Backup to back up SnapLock Enterprise volumes to public and private clouds. This feature requires that your ONTAP system is running ONTAP 9.11.1 or later. SnapLock Compliance volumes, however, aren't currently supported.

Now you can create backup files in the public cloud when using an on-premises Connector

In the past you needed to deploy the Connector in the same cloud provider as where you were creating backup files. Now you can use a Connector deployed in your premises to create backup files from on-prem ONTAP systems to Amazon S3, Azure Blob, and Google Cloud Storage. (An on-prem Connector was always required when creating backup files on StorageGRID systems.)

Additional features are available when creating backup policies for ONTAP systems

- Backup on a yearly schedule is now available. The default retention value is 1 for yearly backups, but you can change this value if you want to have access to many previous years' backup files.
- You can name your backup policies so you can identify your policies with more descriptive text.

14 June 2022

Support has been added to back up on-premises ONTAP cluster data in sites without internet access

If your on-prem ONTAP cluster resides in a site with no internet access, also known as a dark site or offline site, now you can use Cloud Backup to back up volume data to a NetApp StorageGRID system that resides in the same site. This functionality requires that the Cloud Manager Connector (version 3.9.19 or greater) is also deployed in the offline site.

[See how to install the Connector in your offline site.](#)

[See how to back up ONTAP data to StorageGRID in your offline site.](#)

8 June 2022

Cloud Backup for Virtual Machines 1.1.0 is now GA

You can protect data on your virtual machines by integrating the SnapCenter Plug-in for VMware vSphere with Cloud Manager. You can back up datastores to the cloud and restore virtual machines back to the on-premises SnapCenter Plug-in for VMware vSphere with ease.

[Learn more about protecting virtual machines to cloud.](#)

Cloud Restore instance is not needed for ONTAP Browse & Restore functionality

A separate Cloud Restore instance/virtual machine used to be required for file-level Browse & Restore operations from S3 and Blob storage. This instance shut down when not in use — but it still added some time and cost when restoring files. This functionality has been replaced with a no-cost container that gets deployed on the Connector when needed. It provides the following advantages:

- No added cost for file-level restore operations
- Faster file-level restore operations
- Support for Browse & Restore operations for files from the cloud when the Connector is installed on your premises

Note that the Cloud Restore instance/VM will be removed automatically if you were previously using it. A Cloud Backup process will run once a day to delete all old Cloud Restore instances. This change is completely transparent — there is no effect on your data, and you won't notice any changes to your backup or restore jobs.

Browse & Restore support for files from Google Cloud and StorageGRID storage

With the addition of the container for Browse & Restore operations (as described above), file restore operations now can be performed from backup files stored in Google Cloud and StorageGRID systems. Now Browse & Restore can be used to restore files across all public cloud providers and from StorageGRID. [See how to use Browse & Restore to restore volumes and files from your ONTAP backups.](#)

Drag and drop to enable Cloud Backup to S3 storage

If the Amazon S3 destination for your backups exists as a working environment on the Canvas, you can drag your on-prem ONTAP cluster or Cloud Volumes ONTAP system (installed in AWS) onto the Amazon S3 working environment to initiate the setup wizard.

Automatically apply a backup policy to newly created volumes in Kubernetes clusters

If you added new persistent volumes to your Kubernetes clusters after Cloud Backup was activated, in the past you needed to remember to configure backups for those volumes. Now you can select a policy that will be applied automatically to newly created volumes [from the Backup Settings page](#) for clusters that have already activated Cloud Backup.

Cloud Backup APIs are now available for managing backup and restore operations

The APIs are available at <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>. See [this page](#) for an overview of the APIs.

2 May 2022

Search & Restore is now supported with backup files in Google Cloud Storage

The Search & Restore method of restoring volumes and files was introduced in April for users who store their backup files in AWS. Now the capability is available for users who store their backup files in Google Cloud Storage. [See how to restore your volumes and files using Search & Restore.](#)

Configure a backup policy to be applied automatically to newly created volumes in Kubernetes clusters

If you added new persistent volumes to your Kubernetes clusters after Cloud Backup was activated, in the past you needed to remember to configure backups for those volumes. Now you can select a policy that will be applied automatically to newly created volumes. This option is available in the setup wizard when activating Cloud Backup for a new Kubernetes cluster.

Cloud Backup now requires a license before being activated on a working environment

There are a few changes to how licensing is implemented with Cloud Backup:

- You must sign up for a PAYGO Marketplace subscription from your cloud provider, or purchase a BYOL license from NetApp, before you can activate Cloud Backup.
- The 30-day Free Trial is available only when using a PAYGO subscription from your cloud provider - it is not available when using the BYOL license.
- The Free Trial starts the day the Marketplace subscription starts. For example, if you activate the Free Trial after you have been using a Marketplace subscription for 30 days for a Cloud Volumes ONTAP system, the Cloud Backup Trial will not be available.

[Learn more about the available licensing models.](#)

Cloud Data Sense

6 July 2022 (version 1.14)

Now you can view the users and groups who have access to your directories

In the past you could view the types of open permissions granted on individual files. Now you can view a list of all users or groups who have access to directories (folders and file shares), and the types of permissions they have. [See how to view the users and groups that have access to your folders and file shares.](#)

You can "pause" scanning a repository to temporarily stop scanning certain content

Pausing scanning means that Data Sense won't perform future scanning on any additions or changes to a volume or bucket, but that all the current results will still be available in the system. [See how to pause and resume scanning.](#)

US driver's license data from three additional states can be identified by Data Sense

Data Sense can identify and categorize files that contain driver's license data from Indiana, New York, and Texas. [See all the types of personal data that Data Sense can identify in your data.](#)

Policies now return directories that match the search criteria

In the past when you created a custom Policy, the results showed the files that matched the search criteria. Now the results also show the directories (folders and file shares) that match the query. [Learn more about creating policies.](#)

Data Sense can move up to 100,000 files at a time now

If you plan to use Data Sense to move files from a scanned data source to an NFS share, the maximum number of files has been increased to 100,000 files. [See how to move files using Data Sense.](#)

12 June 2022 (version 1.13.1)

Now you can download the results from the Data Investigation page as a .JSON report

After you have filtered the data in the Data Investigation page, now you can save the data as a report in a .JSON file that you can export to an NFS Share, in addition to saving the data to a .CSV file on your local system. Make sure Data Sense has the correct permissions for export access. [See how to create reports from the Data Investigation page.](#)

Ability to uninstall Data Sense from the Data Sense UI

You can uninstall Data Sense to permanently remove the software from the host, and in the case of a cloud deployment, delete the virtual machine / instance on which Data Sense was deployed. Deleting the instance permanently deletes all the indexed information Data Sense has scanned. [See how](#).

Audit logging is now available to track the history of actions that Data Sense has performed

The audit log tracks the management activities that Data Sense has performed on files from all the working environments and data sources that Data Sense is scanning. The activities could be user generated (delete a file, create a policy, etc.) or policy generated (automatically add labels to files, automatically delete files, etc.).

[See more details about the audit log](#).

New Filter for number of sensitive identifiers in the Data Investigation page

The “Number of identifiers” filter enables you to list the files that have a certain number of sensitive identifiers - including both personal data and sensitive personal data. You can select a range like 1-10 or 501-1000 to view only the files that contain that number of sensitive identifiers.

[See the list of all the filters you can use to investigate your data](#).

Now you can edit existing policies that you created

If you need to make a change to a custom policy that you created in the past, now you can edit the policy instead of creating a new policy. [See how to edit a policy](#).

11 May 2022 (version 1.12.1)

Support added for scanning data in Google Drive accounts

Now you can add your Google Drive accounts to Data Sense in order to scan the documents and files from those Google Drive accounts. [See how to scan your Google Drive accounts](#).

Data Sense can identify Personal Identifiable Information (PII) within the following Google file types from the Google Docs suite — Docs, Sheets, and Slides — in addition to the [existing file types](#).

Directory level view added to the Data Investigation page

In addition to viewing and filtering data from all your files and databases, now you can view and filter data based on all the data within folders and shares in the Data Investigation page. Directories will be indexed for scanned CIFS and NFS shares, and for OneDrive, SharePoint, and Google Drive folders. So now you can view permissions and manage your data on the directory level. [See how to select the Directories view of your scanned data](#).

Expand groups to show the users/members that have permissions to access a file

As part the Data Sense permissions capabilities, now you can view the list of users and groups that have access to a file. Each group can be expanded to show the list of users in the group. [See how to view users and groups who have read and/or write permissions to your files](#).

Two new Filters have been added to the Data Investigation page

- The “Directory type” filter enables you to refine your data to see folders or shares only. The results will be

shown in the new **Directories** tab.

- The "User / Group Permissions" filter enables you to list the files, folders, and shares that a specific user or a group has read and/or write permissions to. You can select multiple users and/or group names - or enter a partial name. T

[See the list of all the filters you can use to investigate your data.](#)

Cloud Sync

3 July 2022

Support for Azure Data Lake Storage Gen2

You can now sync data from an NFS server or SMB server to Azure Data Lake Storage Gen2.

When creating a sync relationship that includes Azure Data Lake, you need to provide Cloud Sync with the storage account connection string. It must be a regular connection string, not a shared access signature (SAS).

[View the list of supported sync relationships.](#)

Continuous sync from Google Cloud Storage

The Continuous Sync setting is now supported from a source Google Cloud Storage bucket to a cloud storage target.

After the initial data sync, Cloud Sync listens for changes on the source Google Cloud Storage bucket and continuously syncs any changes to the target as they occur. This setting is available when syncing from a Google Cloud Storage bucket to S3, Google Cloud Storage, Azure Blob storage, StorageGRID, or IBM Storage.

The service account associated with your data broker needs the following permissions to use this setting:

```
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
```

[Learn more about the Continuous Sync setting.](#)

New Google Cloud region support

The Cloud Sync data broker is now supported in the following Google Cloud regions:

- Columbus (us-east5)

- Dallas (us-south1)
- Madrid (europe-southwest1)
- Milan (europe-west8)
- Paris (europe-west9)

New Google Cloud machine type

The default machine type for the data broker in Google Cloud is now n2-standard-4.

6 June 2022

Continuous sync

A new setting enables you to continuously sync changes from a source S3 bucket to a target.

After the initial data sync, Cloud Sync listens for changes on the source S3 bucket and continuously syncs any changes to the target as they occur. There's no need to rescan the source at scheduled intervals. This setting is available only when syncing from an S3 bucket to S3, Google Cloud Storage, Azure Blob storage, StorageGRID, or IBM Storage.

Note that the IAM role associated with your data broker will need the following permissions to use this setting:

```
"s3:GetBucketNotification",
"s3:PutBucketNotification"
```

These permissions are automatically added to any new data brokers that you create.

[Learn more about the Continuous Sync setting.](#)

Show all ONTAP volumes

When you create a sync relationship, Cloud Sync now displays all volumes on a source Cloud Volumes ONTAP system, on-premises ONTAP cluster, or FSx for ONTAP file system.

Previously, Cloud Sync would only display the volumes that matched the selected protocol. Now all of the volumes display, but any volumes that don't match the selected protocol or that don't have a share or export are greyed out and not selectable.

Copying tags to Azure Blob

When you create a sync relationship where Azure Blob is the target, Cloud Sync now enables you to copy tags to the Azure Blob container:

- On the **Settings** page, you can use the **Copy for Objects** setting to copy tags from the source to the Azure Blob container. This is in addition to copying metadata.
- On the **Tags/Metadata** page, you can specify Blob index tags to set on the objects that are copied to the Azure Blob container. Previously, you could only specify relationship metadata.

These options are supported when Azure Blob is the target and the source is either Azure Blob or an S3-compatible endpoint (S3, StorageGRID, or IBM Cloud Object Storage).

1 May 2022

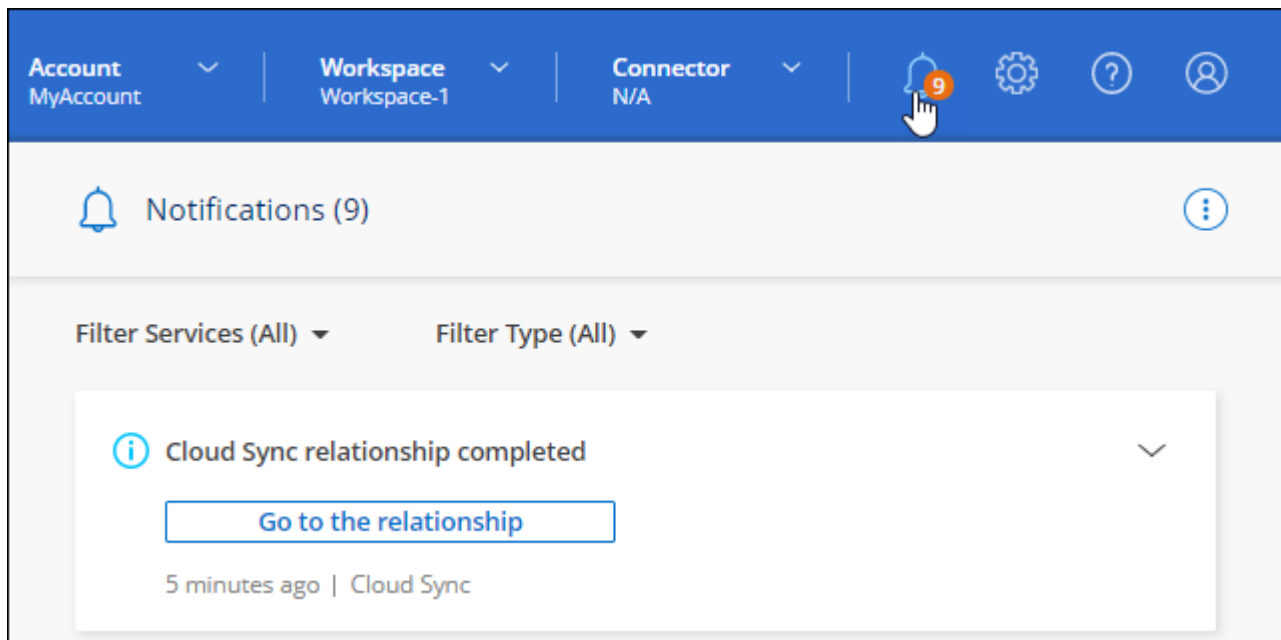
Sync timeout

A new **Sync Timeout** setting is now available for sync relationships. This setting enables you to define whether Cloud Sync should cancel a data sync if the sync hasn't completed in the specified number of hours or days.

[Learn more about changing the settings for a sync relationship.](#)

Notifications

A new **Notifications** setting is now available for sync relationships. This setting enables you to choose whether to receive Cloud Sync notifications in Cloud Manager's Notification Center. You can enable notifications for successful data syncs, failed data syncs, and canceled data syncs.



[Learn more about changing the settings for a sync relationship.](#)

3 April 2022

Data broker group enhancements

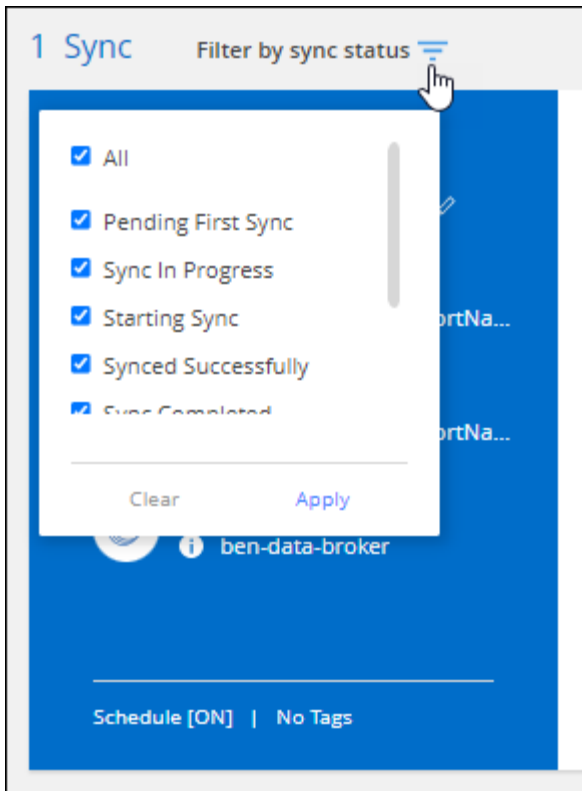
We made several enhancements to data broker groups:

- You can now move a data broker to a new or existing group.
- You can now update the proxy configuration for a data broker.
- Finally, you can also delete data broker groups.

[Learn how to manage data broker groups.](#)

Dashboard filter

You can now filter the contents of the Sync Dashboard to more easily find sync relationships that match a certain status. For example, you can filter on sync relationships that have a failed status



Cloud Tiering

3 May 2022

Cloud Tiering license support for additional cluster configurations

Cloud Tiering licenses can now be shared with your clusters that are in Tiering Mirror configurations (not including MetroCluster configurations) and with clusters that are tiered to IBM Cloud Object Storage. You no longer have to use the deprecated FabricPool licenses for these scenarios. This makes it easier to use the "floating" Cloud Tiering licenses on more of your clusters. [See how to license and configure these types of clusters.](#)

4 April 2022

Amazon S3 Glacier Instant Retrieval storage class is now available

When setting up Cloud Tiering, now you can configure a lifecycle rule so your inactive data transitions from the *Standard* storage class to *Glacier Instant Retrieval* after a certain number of days. This will help reduce your AWS infrastructure costs. [See the supported S3 storage classes.](#)

Cloud Tiering has been fully qualified on ONTAP Select systems

In addition to tiering data from your AFF and FAS systems, now you can tier inactive data from your ONTAP Select systems to cloud storage.

2 September 2021

Cloud Tiering BYOL license replaces FabricPool license

A new **Cloud Tiering** license is now available for tiering configurations that are supported within Cloud Manager using the Cloud Tiering service. It is a floating license that you can use across multiple on-premises ONTAP clusters. The **FabricPool** license that you may have used in the past is retained only for configurations that aren't supported within Cloud Manager.

[Learn more about the new Cloud Tiering license.](#)

Tier inactive data from on-prem ONTAP clusters to S3-compatible object storage

Now you can tier inactive data to any Object Storage service which uses the Simple Storage Service (S3) protocol. [See how to tier data to S3-compatible object storage.](#)

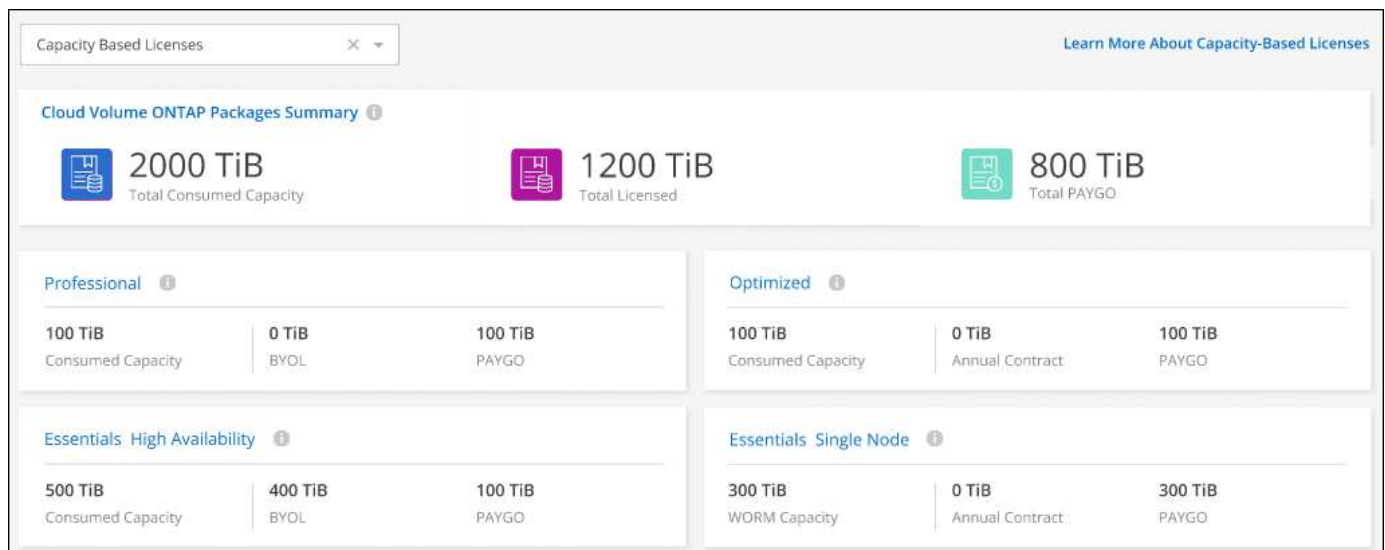
Cloud Volumes ONTAP

3 July 2022

The following changes were introduced with the 3.9.20 release of the Connector.

Digital Wallet

The Digital Wallet now shows you the total consumed capacity in your account and the consumed capacity by licensing package. This can help you understand how you're being charged and whether you need to purchase additional capacity.



Elastic Volumes enhancement

Cloud Manager now supports the Amazon EBS Elastic Volumes feature when creating a Cloud Volumes ONTAP working environment from the user interface. The Elastic Volumes feature is enabled by default when using gp3 or io1 disks. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed.

[Learn more about support for Elastic Volumes in AWS.](#)

ONTAP S3 license in AWS

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.11.0 or later in AWS.

[Learn how to configure and manage S3 object storage services in ONTAP](#)

New Azure Cloud region support

Starting with the 9.10.1 release, Cloud Volumes ONTAP is now supported in the Azure West US 3 region.

[View the full list of supported regions for Cloud Volumes ONTAP](#)

ONTAP S3 license in Azure

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.9.1 or later in Azure.

[Learn how to configure and manage S3 object storage services in ONTAP](#)

7 June 2022

The following changes were introduced with the 3.9.19 release of the Connector.

Cloud Volumes ONTAP 9.11.1

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.11.1, which includes support for new features and additional cloud provider regions.

[Learn about the new features included in this release of Cloud Volumes ONTAP](#)

New Advanced View

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside Cloud Manager so that you don't need to leave Cloud Manager for advanced management.

This Advanced View is available as a Preview with Cloud Volumes ONTAP 9.10.0 and later. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

[Learn more about the Advanced View.](#)

Support for Amazon EBS Elastic Volumes

Support for the Amazon EBS Elastic Volumes feature with a Cloud Volumes ONTAP aggregate provides better performance and additional capacity, while enabling Cloud Manager to automatically increase the underlying disk capacity as needed.

Support for Elastic Volumes is available starting with *new* Cloud Volumes ONTAP 9.11.0 systems and with gp3 and io1 EBS disk types.

[Learn more about support for Elastic Volumes.](#)

Note that support for Elastic Volumes requires new AWS permissions for the Connector:

```
"ec2:DescribeVolumesModifications",  
"ec2:ModifyVolume",
```

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager.
[View the latest Connector policy for AWS.](#)

Support for deploying HA pairs in shared AWS subnets

Cloud Volumes ONTAP 9.11.1 includes support for AWS VPC sharing. This release of the Connector enables you to deploy an HA pair in an AWS shared subnet when using the API.

[Learn how to deploy an HA pair in a shared subnet.](#)

Limited network access when using service endpoints

Cloud Manager now limits network access when using a VNet service endpoint for connections between Cloud Volumes ONTAP and storage accounts. Cloud Manager uses a service endpoint if you disable Azure Private Link connections.

[Learn more about Azure Private Link connections with Cloud Volumes ONTAP.](#)

Support for creating storage VMs in Google Cloud

Multiple storage VMs are now supported with Cloud Volumes ONTAP in Google Cloud, starting with the 9.11.1 release. Starting with this release of the Connector, Cloud Manager enables you to create storage VMs on Cloud Volumes ONTAP HA pairs in Google Cloud by using the API.

Support for creating storage VMs requires new Google Cloud permissions for the Connector:

```
- compute.instanceGroups.get  
- compute.addresses.get
```

Note that you must use the ONTAP CLI or System Manager to create a storage VM on a single node system.

- [Learn more about storage VM limits in Google Cloud](#)
- [Learn how to create data-serving storage VMs for Cloud Volumes ONTAP in Google Cloud](#)

2 May 2022

The following changes were introduced with the 3.9.18 release of the Connector.

Cloud Volumes ONTAP 9.11.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.11.0.

[Learn about the new features included in this release of Cloud Volumes ONTAP.](#)

Enhancement to mediator upgrades

When Cloud Manager upgrades the mediator for an HA pair, it now validates that a new mediator image is available before it deletes the boot disk. This change ensures that the mediator can continue to operate successfully if the upgrade process is unsuccessful.

K8s tab has been removed

The K8s tab was deprecated in a previous and has now been removed. If you want to use Kubernetes with Cloud Volumes ONTAP, you can add managed-Kubernetes clusters to the Canvas as a working environment for advanced data management.

[Learn about Kubernetes data management in Cloud Manager](#)

Annual contract in Azure

The Essentials and Professional packages are now available in Azure through an annual contract. You can contact your NetApp sales representative to purchase an annual contract. The contract is available as a private offer in the Azure Marketplace.

After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Azure Marketplace during working environment creation.

[Learn more about licensing.](#)

S3 Glacier Instant Retrieval

You can now store tiered data in the Amazon S3 Glacier Instant Retrieval storage class.

[Learn how to change the storage class for tiered data.](#)

New AWS permissions required for the Connector

The following permissions are now required to create an AWS spread placement group when deploying an HA pair in a single Availability Zone (AZ):

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy",
```

These permissions are now required to optimize how Cloud Manager creates the placement group.

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager.

[View the latest Connector policy for AWS.](#)

New Google Cloud region support

Cloud Volumes ONTAP is now supported in the following Google Cloud regions starting with the 9.10.1 release:

- Delhi (asia-south2)
- Melbourne (australia-southeast2)
- Milan (europe-west8) - single node only

- Santiago (southamerica-west1) - single node only

[View the full list of supported regions for Cloud Volumes ONTAP](#)

Support for n2-standard-16 in Google Cloud

The n2-standard-16 machine type is now supported with Cloud Volumes ONTAP in Google Cloud, starting with the 9.10.1 release.

[View supported configurations for Cloud Volumes ONTAP in Google Cloud](#)

Enhancements to Google Cloud firewall policies

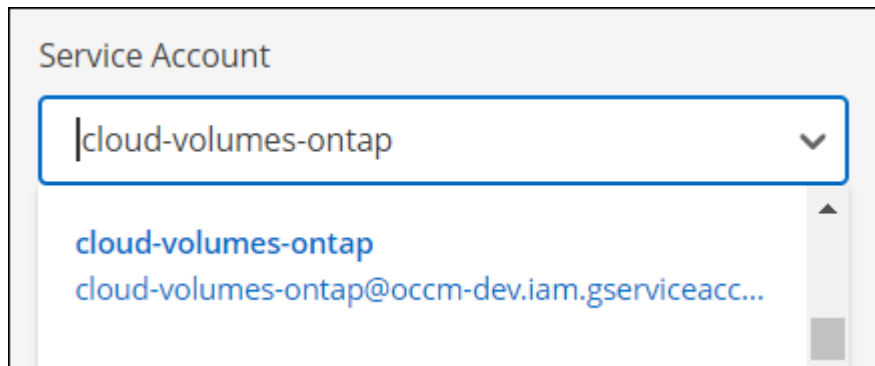
- When you create a Cloud Volumes ONTAP HA pair in Google Cloud, Cloud Manager will now display all existing firewall policies in a VPC.

Previously, Cloud Manager wouldn't display any policies in VPC-1, VPC-2, or VPC-3 that didn't have a target tag.

- When you create a Cloud Volumes ONTAP single node system in Google Cloud, you can now choose whether you want the predefined firewall policy to allow traffic within the selected VPC only (recommended) or all VPCs.

Enhancement to Google Cloud service accounts

When you select the Google Cloud service account to use with Cloud Volumes ONTAP, Cloud Manager now displays the email address that's associated with each service account. Viewing the email address can make it easier to distinguish between service accounts that share the same name.



Cloud Volumes Service for GCP

9 September 2020

Support for Cloud Volumes Service for Google Cloud

You can now manage Cloud Volumes Service for Google Cloud directly from Cloud Manager:

- Set up and create a working environment
- Create and manage NFSv3 and NFSv4.1 volumes for Linux and UNIX clients
- Create and manage SMB 3.x volumes for Windows clients

- Create, delete, and restore volume snapshots

Compute

7 December 2020

Navigation between Cloud Manager and Spot

It's now easier to navigate between Cloud Manager and Spot.

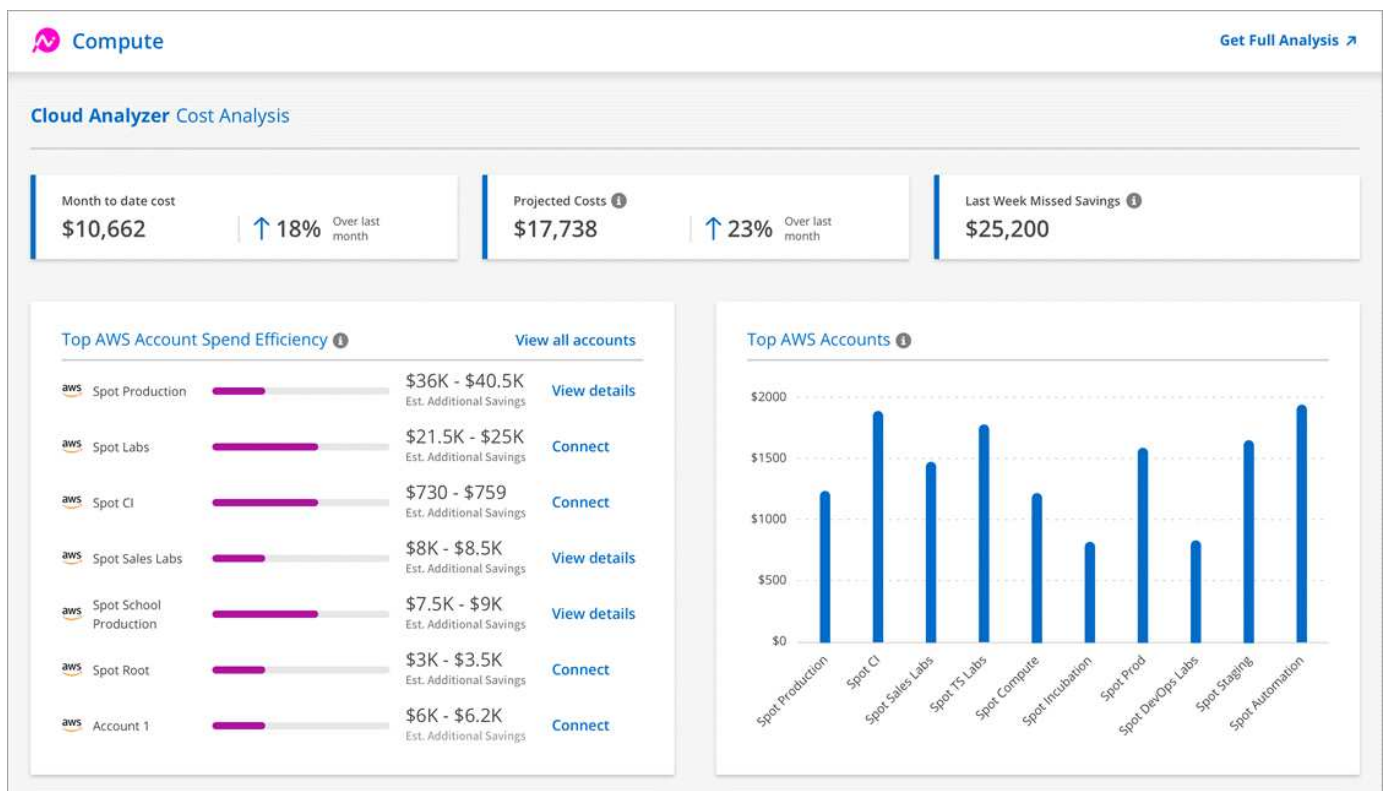
A new **Storage Operations** section in Spot enables you to navigate directly to Cloud Manager. After you're done, you can get back to Spot from the **Compute** tab in Cloud Manager.

18 October 2020

Introducing the Compute service

By leveraging [Spot's Cloud Analyzer](#), Cloud Manager can now provide a high-level cost analysis of your cloud compute spending and identify potential savings. This information is available from the **Compute** service in Cloud Manager.

[Learn more about the Compute service.](#)



Global File Cache

23 June 2022 (version 1.3.1)

Global File Cache Edge software for version 1.3.1 is available at [this page](#). This release fixes the issues

described in the [Fixed Issues](#).

19 May 2022 (version 1.3.0)

Global File Cache Edge software for version 1.3.0 is available at [this page](#).

New Metadata Edge Sync feature

This "Metadata Edge Sync" feature uses the Edge Synchronization feature as its core framework. Only Metadata information is updated on all subscribed Edges and the files/folders get created on the Edge machines.

License Manager Service enhancements

The Global File Cache License Management Server (LMS) service is enhanced to auto detect proxy settings. This enables a seamless configuration.

17 December 2021 (version 1.2.0)

The OpenSSL module has been upgraded to version 1.1.1l.

This is the latest version and it is more secure. This module is used for secure communication between GFC Edge and GFC Core.

The logging infrastructure has been enhanced.

9 June 2021 (version 1.1.0)

The "Edge Synchronization" feature has been added.

This feature keeps multiple Edges at a remote office in sync and the data is always cached/warm. When a file is flushed/fetched at one Edge, then the same file on all Edges participating in Edge Sync is updated and cached. See section 8.4 in the [NetApp Global File Cache User Guide](#) for details.

The OpenSSL module has been upgraded to version 1.1.1k.

This is the latest version and it is more secure. This module is used for secure communication between GFC Edge and GFC Core.

Updated License Registration Page.

The GFC License Registration Page now displays the number of licenses when activated through a NetApp subscription.

Kubernetes

3 July 2022

- If Astra Trident was deployed using the Trident operator, you can now upgrade to the latest version of Astra Trident using Cloud Manager.

[Install and manage Astra Trident](#)

- You can now drag your Kubernetes cluster and drop it onto the AWS FSx for ONTAP working environment to add a storage class directly from the Canvas.

[Add storage class](#)

6 June 2022

Cloud Manager now supports Amazon FSx for ONTAP as backend storage.

4 May 2022

Drag and drop to add storage class

You can now drag your Kubernetes cluster and drop it onto the Cloud Volumes ONTAP working environment to add a storage class directly from the Canvas.

[Add storage class](#)

Monitoring

1 August 2021

Change to Acquisition Unit name

We changed the default name of the Acquisition Unit instance to `CloudInsights-AU-UUID` so that the name is more descriptive (the UUID is a generated hash).

Cloud Manager deploys this instance when you enable the Monitoring service on a Cloud Volumes ONTAP working environment.

5 May 2021

Support for existing tenants

You can now enable the Monitoring service on a Cloud Volumes ONTAP working environment even if you have an existing Cloud Insights tenant.

Free Trial transition

When you enable the Monitoring service, Cloud Manager sets up a free trial of Cloud Insights. On the 29th day, your plan now automatically transitions from the Trial Version to the [Basic Edition](#).

9 February 2021

Support in Azure

The Monitoring service is now supported with Cloud Volumes ONTAP for Azure.

Support in Government regions

The Monitoring service is also supported in Government regions in AWS and Azure.

On-prem ONTAP clusters

7 June 2022

The following change was introduced with the 3.9.19 release of the Connector.

New Advanced View

If you need to perform advanced management of an ONTAP on-premises cluster, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside Cloud Manager so that you don't need to leave Cloud Manager for advanced management.

This Advanced View is available as a Preview with on-premises ONTAP clusters running 9.10.0 or later. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

[Learn more about the Advanced View.](#)

27 February 2022

An "On-Premises ONTAP" tab is available in the Digital Wallet.

Now you can view an inventory of your on-prem ONTAP clusters along with their hardware and service contracts expiration dates. Additional details about the clusters are also available.

[See how to view this important on-prem cluster information.](#) You'll need to have a NetApp Support Site account (NSS) for the clusters, and the NSS credentials will need to be attached to your Cloud Manager account.

11 January 2022

Tags that you add to volumes on on-prem ONTAP clusters can be use with the Tagging service.

Tags that you add to a volume are now associated with the tagging feature of the Application Templates service, which can help you organize and simplify the management of your resources.

Ransomware Protection

12 June 2022

NAS file system auditing status is now tracked for your ONTAP storage VMs

An alert is added to the *Cyber Resilience Map* if less than 40% of the storage VMs in the working environment have file system auditing enabled. You can view the exact number of SVMs that are not tracking and logging SMB and NFS events into an audit log in the *Harden your ONTAP environment* panel. Then you can decide whether to enable auditing on those SVMs.

Alerts are now displayed when on-box anti-ransomware is not active for your volumes

This information was being reported for on-prem ONTAP systems in the *Harden your ONTAP environments* panel previously, but now an alert is reported in the *Cyber Resilience Map* when the on-box anti-ransomware feature is turned on in less than 40% of volumes so you can view this information in the Dashboard.

FSx for ONTAP systems are now tracked for enabling volume snapshots

The *Harden your ONTAP environments* panel now provides the status of Snapshot copies for volumes on your FSx for ONTAP systems. When less than 40% of the volumes are being protected by snapshots, you will also get an alert in the *Cyber Resilience Map*.

11 May 2022

New panel to track the security hardening of your ONTAP environments.

A new panel *Harden your ONTAP environments* provides the status of certain settings in your ONTAP systems that track how secure your deployment is according to the [NetApp Security Hardening Guide for ONTAP Systems](#) and to the [ONTAP anti-ransomware feature](#) that proactively detects and warns about abnormal activity.

You can review the recommendations and then decide how you want to address the potential issues. You can follow the steps to change the settings on your clusters, defer the changes to another time, or ignore the suggestion. [Go here for details](#).

New panel to show how different categories of data are being protected using Cloud Backup.

This new *Backup Status* panel shows how comprehensively your most important categories of data are backed up in case you need to recover because of a ransomware attack. This data is a visual representation of how many items of a specific category in an environment are backed up by Cloud Backup. [Go here for details](#).

15 March 2022

New panel to track the permissions status of your business critical data

A new panel *Business critical data permissions analysis* shows the permissions status of data that is critical for your business. That way you can quickly assess how well you are protecting your business-critical data. [Go here for details](#).

Open Permissions area now includes OneDrive and SharePoint accounts

The Open Permissions area in the Ransomware Protection Dashboard now includes the permissions that exist for files that are being scanned in OneDrive accounts and SharePoint accounts.

Replication

2 September 2021

Support for Amazon FSx for ONTAP

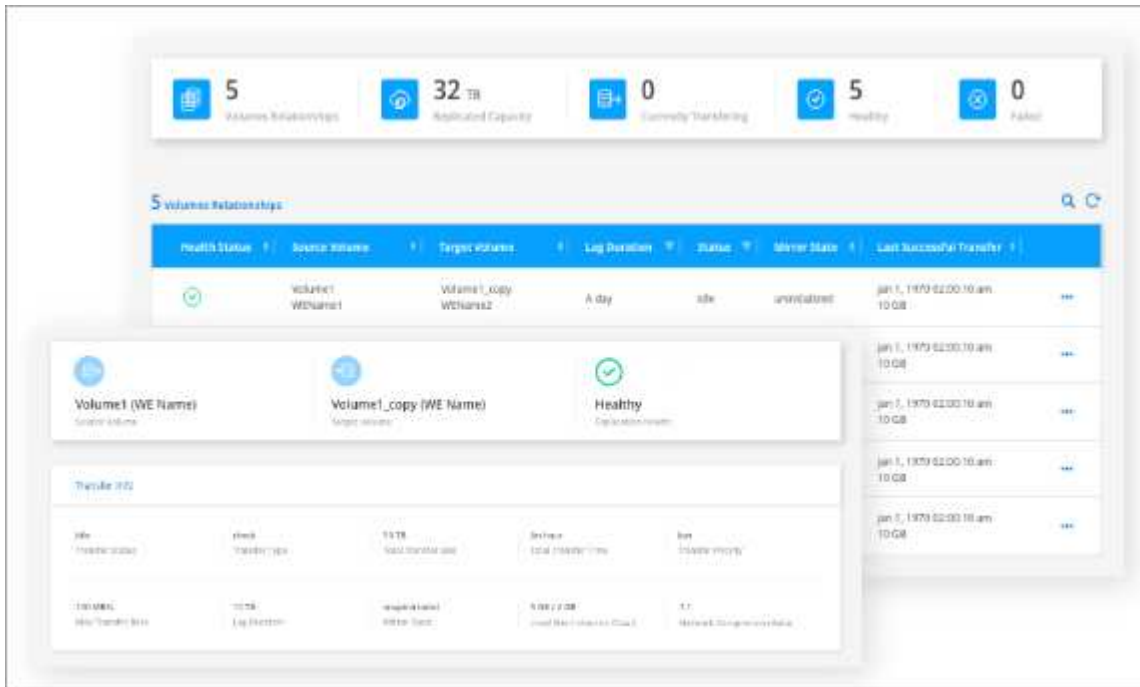
You can now replicate data from a Cloud Volumes ONTAP system or an on-premises ONTAP cluster to an Amazon FSx for ONTAP file system.

[Learn how to set up data replication](#).

5 May 2021

Redesigned interface

We redesigned the Replication tab for ease of use and to match the current look and feel of the Cloud Manager user interface.



SnapCenter Service

21 Dec 2021

Fixes for Apache Log4j vulnerabilities

SnapCenter Service 1.0.1 upgrades Apache Log4j from version 2.9.1 to 2.17 to address the following vulnerabilities: CVE-2021-44228, CVE-2021-4104, and CVE-2021-45105.

The SnapCenter Service cluster should auto-update to the latest version. You should ensure that the version in the SnapCenter Service UI shows that the cluster is 1.0.1.1251 or later.

Release notes index

View the full set of release notes for each individual service.

Storage

- [Azure NetApp Files](#)
- [Amazon FSx for ONTAP](#)
- [Cloud Volumes ONTAP](#)
 - [Release notes for Cloud Volumes ONTAP](#)
 - [Release notes for Cloud Volumes ONTAP management in Cloud Manager](#)
- [Cloud Volumes Service for Google Cloud](#)
- [Kubernetes clusters](#)
- [On-prem ONTAP clusters](#)

Data services

- [AppTemplate](#)
- [Cloud Backup](#)
- [Cloud Data Sense](#)
- [Cloud Sync](#)
- [Cloud Tiering](#)
- [Compute](#)
- [Global File Cache](#)
- [Monitoring](#)
- [Ransomware](#)
- [Replication](#)
- [SnapCenter Service](#)

Administration

- [Set up and administration](#)

Copyright Information

Copyright © 2022 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.