Getting started with Cloud Compliance for Cloud Volumes ONTAP and Azure NetApp Files

Cloud Manager

Ben Cammett, Tom Onacki
August 28, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_getting_started_compliance.html on November 10, 2020. Always check docs.netapp.com for the latest.

Table of Contents

Getting started with Cloud Compliance for Cloud Volumes ONTAP and Azure NetApp Files

Complete a few steps to get started with Cloud Compliance for Cloud Volumes ONTAP or Azure NetApp Files.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1 Deploy the Cloud Compliance instance

Deploy Cloud Compliance in Cloud Manager if there isn’t already an instance deployed.

2 Enable Cloud Compliance in your working environments

Click **Cloud Compliance**, select the **Configuration** tab, and activate compliance scans for specific working environments.

3 Ensure access to volumes

Now that Cloud Compliance is enabled, ensure that it can access volumes.

- The Cloud Compliance instance needs a network connection to each Cloud Volumes ONTAP subnet or Azure NetApp Files subnet.
- Security groups for Cloud Volumes ONTAP must allow inbound connections from the Cloud Compliance instance.
- NFS volume export policies must allow access from the Cloud Compliance instance.
- Cloud Compliance needs Active Directory credentials to scan CIFS volumes.

  Click **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** and provide the credentials. The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read data that requires elevated permissions.

4 **Configure volumes to scan**

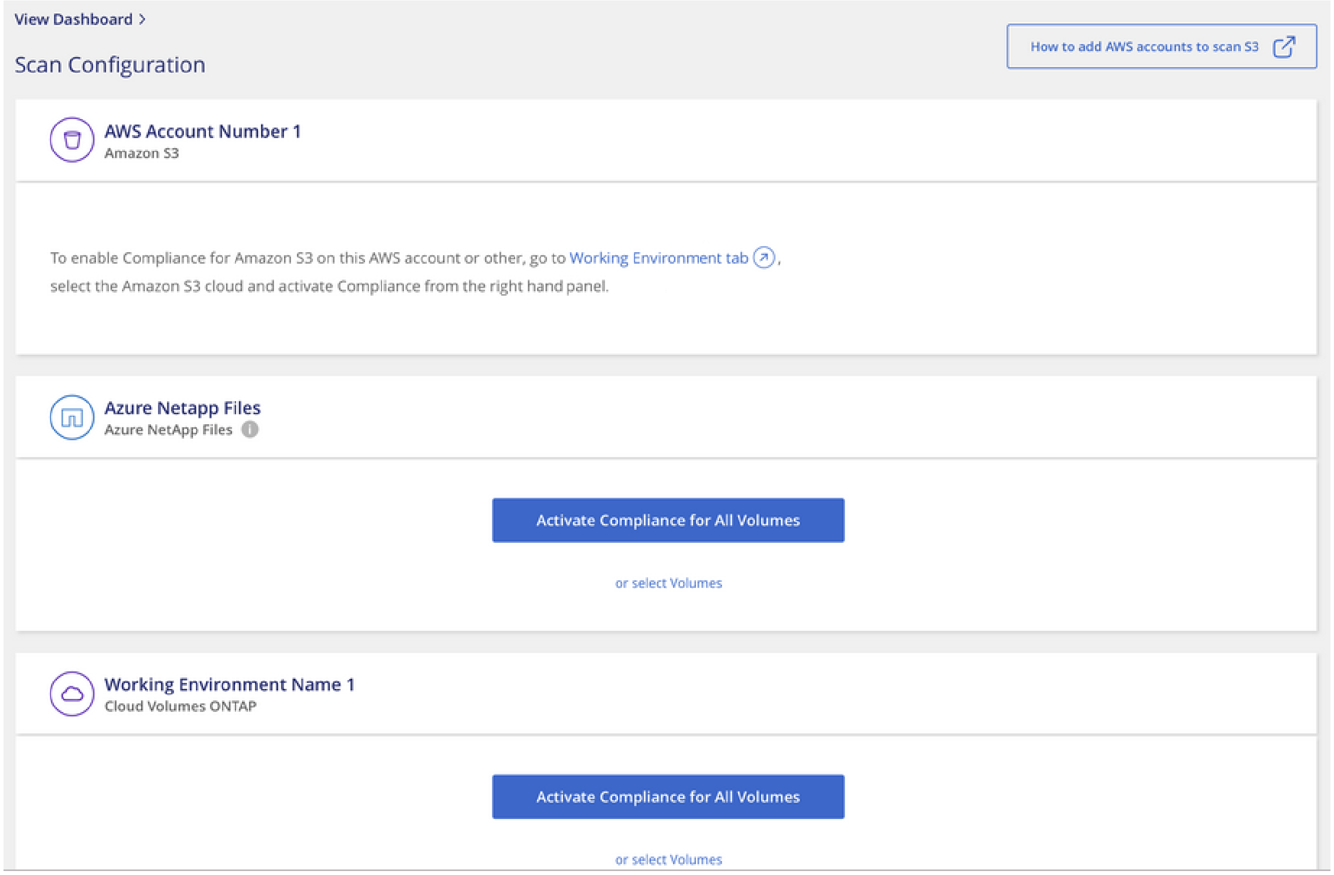
Select the volumes that you’d like to scan and Cloud Compliance will start scanning them.

Deploying the Cloud Compliance instance

Deploy Cloud Compliance in Cloud Manager if there isn’t already an instance deployed.

Enabling Cloud Compliance in your working environments

1. At the top of Cloud Manager, click **Cloud Compliance** and then select the **Configuration** tab.



To enable Compliance for Amazon S3 on this AWS account or other, go to Working Environment tab, select the Amazon S3 cloud and activate Compliance from the right hand panel.

2. To scan all volumes in a working environment, click **Activate Compliance for All Volumes**.

   To scan only certain volumes in a working environment, click **or select Volumes** and then choose the volumes you want to scan.

See Enabling and disabling compliance scans on volumes for details.

Result

Cloud Compliance starts scanning the data on each working environment. Results will be available in the Compliance dashboard as soon as Cloud Compliance finishes the initial scans. The time that it takes depends on the amount of data—it could be a few minutes or hours.

Verifying that Cloud Compliance has access to volumes

Make sure that Cloud Compliance can access volumes by checking your networking, security groups, and export policies. You'll need to provide Cloud Compliance with CIFS credentials so it can access CIFS volumes.

Steps

1. Make sure that there's a network connection between the Cloud Compliance instance and each network that includes volumes for Cloud Volumes ONTAP or Azure NetApp Files.

   > For Azure NetApp Files, Cloud Compliance can only scan volumes that are in the same region as Cloud Manager.

2. Ensure that the security group for Cloud Volumes ONTAP allows inbound traffic from the Cloud Compliance instance.

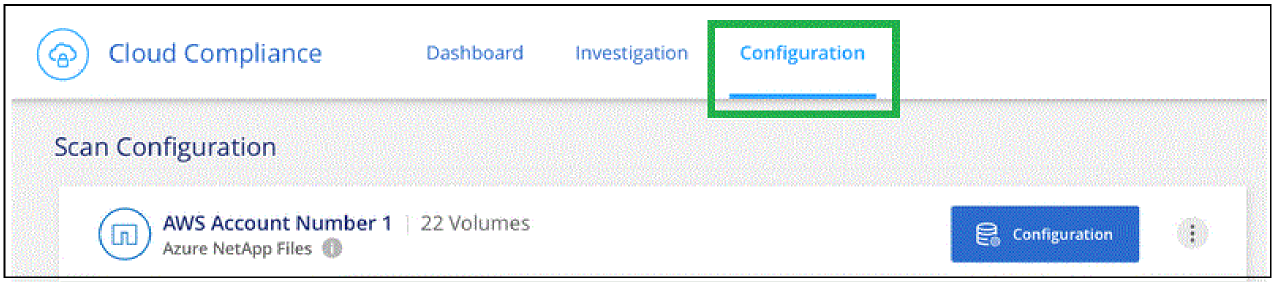
   You can either open the security group for traffic from the IP address of the Cloud Compliance instance, or you can open the security group for all traffic from inside the virtual network.

3. Ensure that NFS volume export policies include the IP address of the Cloud Compliance instance so it can access the data on each volume.

4. If you use CIFS, provide Cloud Compliance with Active Directory credentials so it can scan CIFS volumes.

   a. At the top of Cloud Manager, click **Cloud Compliance**.

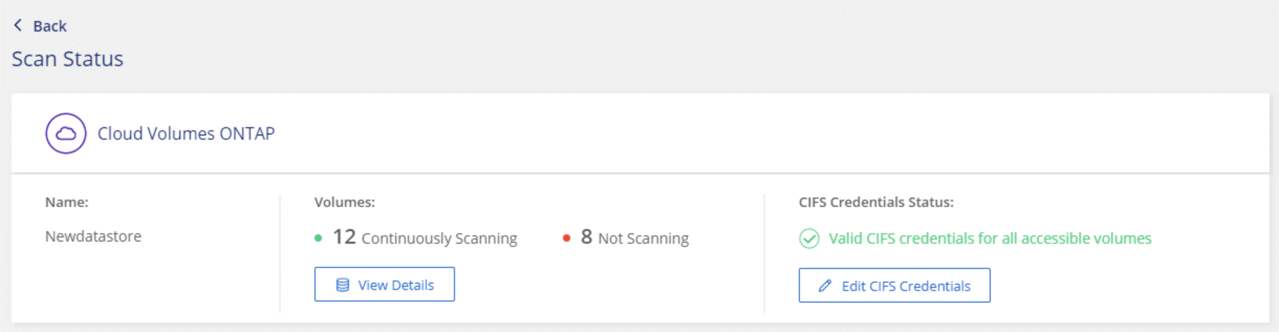
   b. Click the **Configuration** tab.

   c. For each working environment, click **Edit CIFS Credentials** and enter the user name and password that Cloud Compliance needs to access CIFS volumes on the system.

   The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read any data that requires elevated permissions. The credentials are stored on the Cloud Compliance instance.

After you enter the credentials, you should see a message that all CIFS volumes were authenticated successfully.



< Back

Scan Status

Cloud Volumes ONTAP

Name: Newdatastore

Volumes: ● 12 Continuously Scanning ● 8 Not Scanning

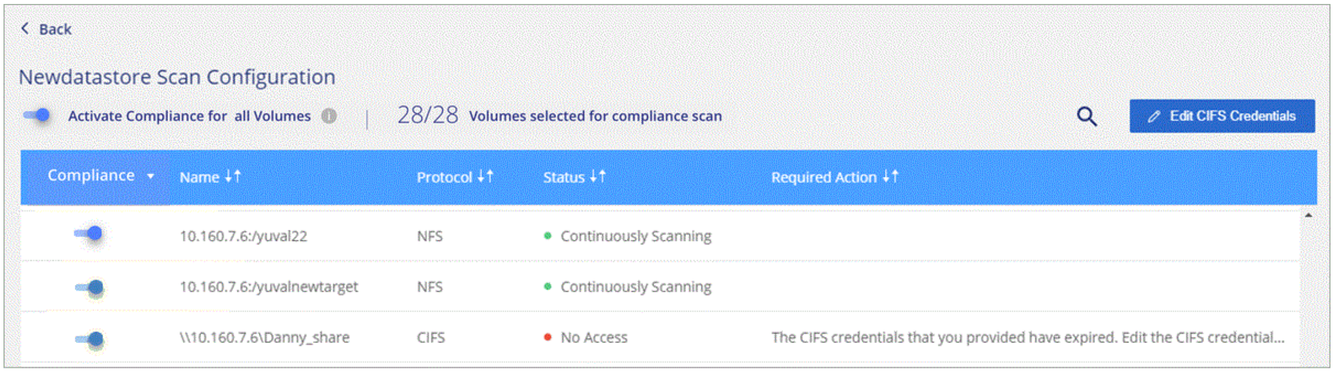
View Details

CIFS Credentials Status: ✓ Valid CIFS credentials for all accessible volumes

Edit CIFS Credentials

5. On the *Scan Configuration* page, click **View Details** to review the status for each CIFS and NFS volume and correct any errors.

   For example, the following image shows three volumes; one of which Cloud Compliance can't scan due to network connectivity issues between the Cloud Compliance instance and the volume.



< Back

Newdatastore Scan Configuration

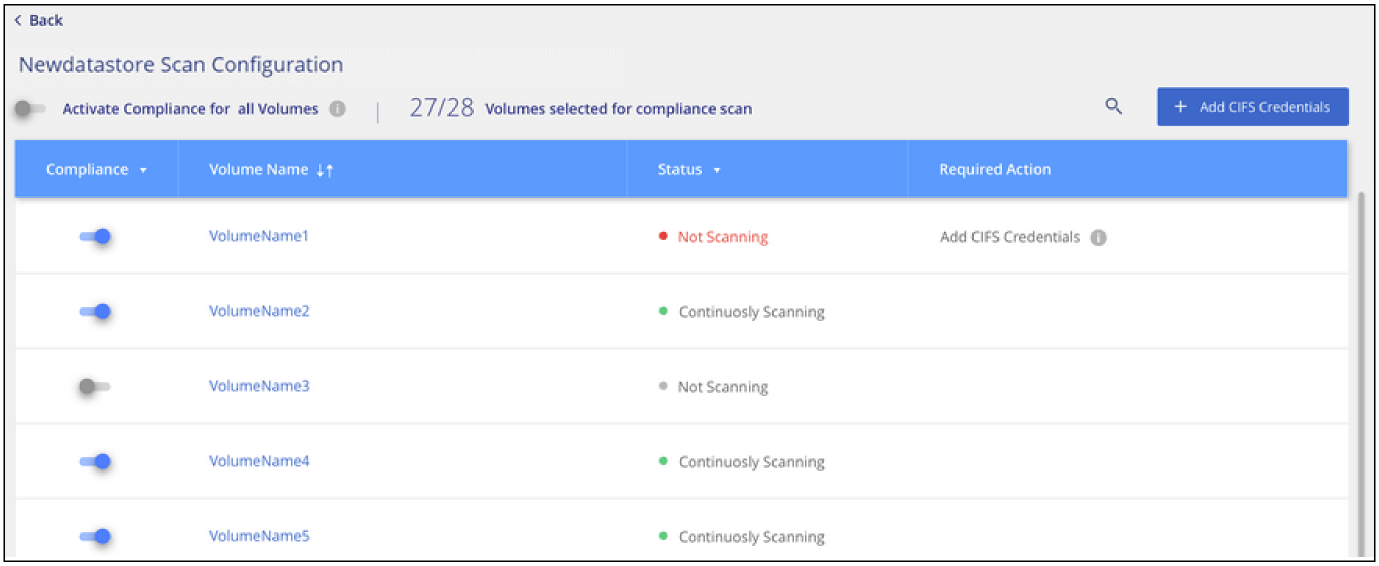
Activate Compliance for all Volumes | 28/28 Volumes selected for compliance scan

Edit CIFS Credentials

Compliance	Name	Protocol	Status	Required Action
●	10.160.7.6:/yuval22	NFS	● Continuously Scanning	
●	10.160.7.6:/yuvalnewtarget	NFS	● Continuously Scanning	
●	\\10.160.7.6\Danny_share	CIFS	● No Access	The CIFS credentials that you provided have expired. Edit the CIFS credential...

Enabling and disabling compliance scans on volumes

You can stop or start scanning volumes in a working environment at any time from the Scan Configuration page. We recommend that you scan all volumes.



Newdatastore Scan Configuration

○ Activate Compliance for all Volumes | 27/28 Volumes selected for compliance scan

Compliance	Volume Name	Status	Required Action
●	VolumeName1	● Not Scanning	Add CIFS Credentials
●	VolumeName2	● Continuosly Scanning	
○	VolumeName3	● Not Scanning	
●	VolumeName4	● Continuosly Scanning	
●	VolumeName5	● Continuosly Scanning	

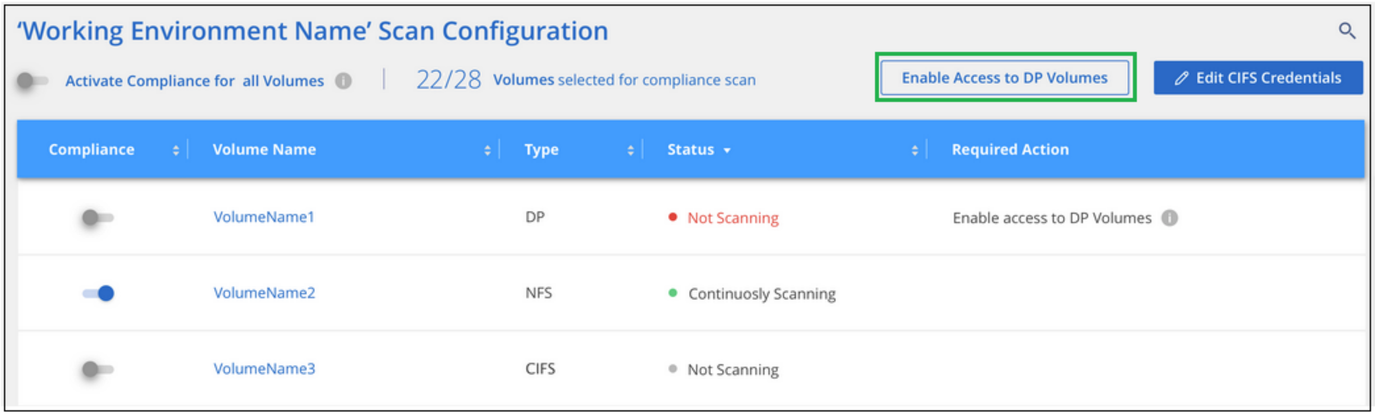
To:	Do this:
Disable scanning for a volume	Move the volume slider to the left
Disable scanning for all volumes	Move the **Activate Compliance for all Volumes** slider to the left
Enable scanning for a volume	Move the volume slider to the right
Enable scanning for all volumes	Move the **Activate Compliance for all Volumes** slider to the right

New volumes added to the working environment are automatically scanned only when the **Activate Compliance for all Volumes** setting is enabled. When this setting is disabled, you’ll need to activate scanning on each new volume you create in the working environment.

Scanning data protection volumes

By default, data protection (DP) volumes are not scanned because they are not exposed externally and Cloud Compliance cannot access them. These volumes are typically the destination volumes for SnapMirror operations from an on-premises ONTAP cluster.

Initially, the Cloud Compliance volume list identifies these volumes as *Type* **DP** with the *Status* **Not Scanning** and the *Required Action* **Enable Access to DP volumes**.



'Working Environment Name' Scan Configuration

Activate Compliance for all Volumes | 22/28 Volumes selected for compliance scan

Compliance	Volume Name	Type	Status	Required Action
○	VolumeName1	DP	● Not Scanning	Enable access to DP Volumes
●	VolumeName2	NFS	● Continuosly Scanning	
○	VolumeName3	CIFS	● Not Scanning	

Steps

If you want to scan these data protection volumes:

1. Click the **Enable Access to DP volumes** button at the top of the page.
2. Activate each DP volume that you want to scan, or use the **Activate Compliance for all Volumes** control to enable all volumes, including all DP volumes.

Once enabled, Cloud Compliance creates an NFS share from each DP volume that was activated for Compliance so that it can be scanned. The share export policies only allow access from the Cloud Compliance instance.

> Only volumes that were initially created as NFS volumes in the source ONTAP system are shown in the volume list. Source volumes that were created initially as CIFS do not currently appear in Cloud Compliance.

Copyright Information

Trademark Information