Getting started with Cloud Compliance for Cloud Volumes ONTAP, on-premises ONTAP, or Azure NetApp Files

Cloud Manager

Tom Onacki, Ben Cammett
February 16, 2021

Table of Contents

Getting started with Cloud Compliance for Cloud Volumes ONTAP, on-premises ONTAP, or Azure NetApp Files

Complete a few steps to get started with Cloud Compliance for Cloud Volumes ONTAP, on-premises ONTAP systems, or Azure NetApp Files.

Quick start

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

Discover the data sources that contain the data you want to scan

Before you can scan volumes, you must add the systems to working environments in Cloud Manager:

- For Cloud Volumes ONTAP systems, these working environments should already be available in Cloud Manager
- For on-premises ONTAP systems, Cloud Manager must discover the ONTAP clusters
- For Azure NetApp Files, Cloud Manager must be set up to discover the configuration.

Deploy the Cloud Compliance instance

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

Enable Cloud Compliance in your working environments and select the volumes to scan

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

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, Azure NetApp Files subnet, or on-prem ONTAP system.
- 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 **Compliance** > **Scan Configuration** > **Edit CIFS Credentials** and provide the credentials.

Manage the volumes you want to scan

Select or deselect the volumes that you want to scan and Cloud Compliance will start or stop scanning them.

Discovering the data sources that you want to scan

If the data sources you want to scan are not already in your Cloud Manager environment, you can add them to the canvas at this time.

Your Cloud Volumes ONTAP systems should already be available in the Canvas in Cloud Manager. For on-premises ONTAP systems you need to have Cloud Manager discover these clusters. And for Azure NetApp Files, Cloud Manager must be set up to discover the configuration.

Deploying the Cloud Compliance instance

Deploy Cloud Compliance if there isn't already an instance deployed.

Cloud Compliance can be deployed in the cloud or in an on-premises location when scanning Cloud Volumes ONTAP or on-premises ONTAP systems.

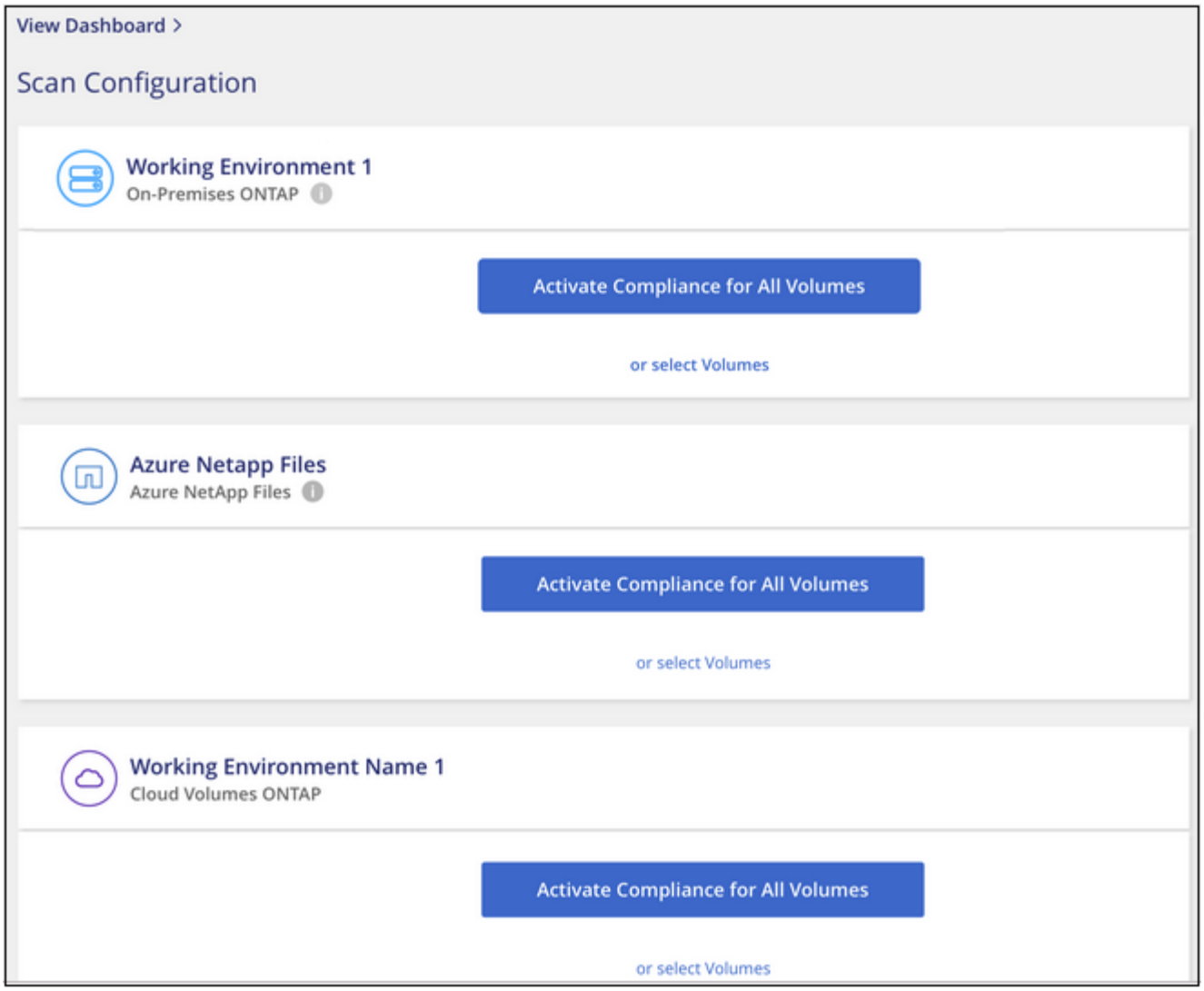
Cloud Compliance must be deployed in the cloud when scanning Azure NetApp Files volumes, and it must be deployed in the same region as the volumes you wish to scan.

Enabling Cloud Compliance in your working environments

You can enable Cloud Compliance on Cloud Volumes ONTAP systems (in AWS and Azure), on-premises ONTAP clusters, and Azure NetApp Files.

Following these steps for on-prem ONTAP systems scans the volumes directly on the on-prem ONTAP system. If you are already creating backup files from those on-prem systems using Cloud Backup, you can run compliance scans on the backup files in the cloud instead. Go to Scanning backup files from on-premises ONTAP systems to scan the volumes by scanning the backup files.

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



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 volumes you selected in the 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

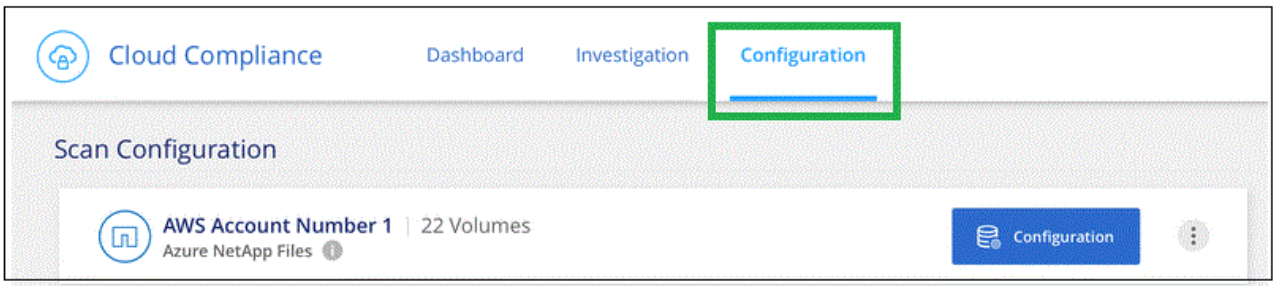
1. Make sure that there's a network connection between the Cloud Compliance instance and each network that includes volumes for Cloud Volumes ONTAP, Azure NetApp Files, or on-prem ONTAP clusters.

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.

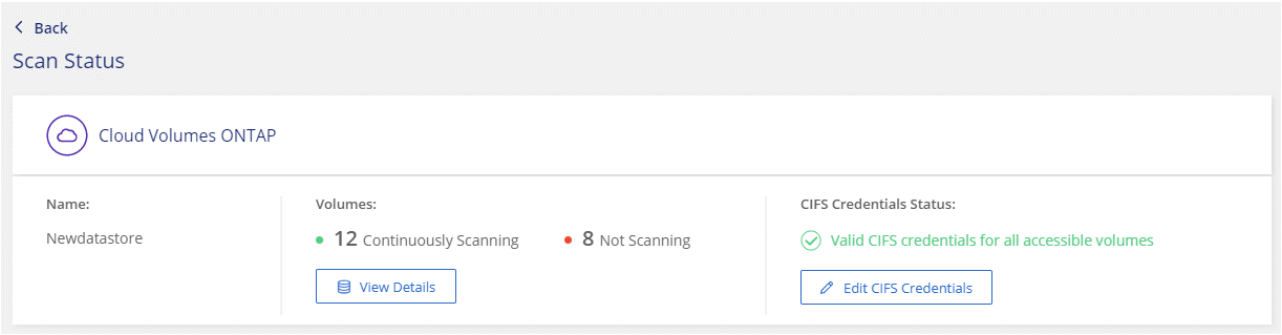
3. Ensure that NFS volume export policies include the IP address of the Cloud Compliance instance so it can access the data on each volume.
4. If you use CIFS, provide Cloud Compliance with Active Directory credentials so it can scan CIFS volumes.
   a. At the top of Cloud Manager, click **Compliance**.
   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.

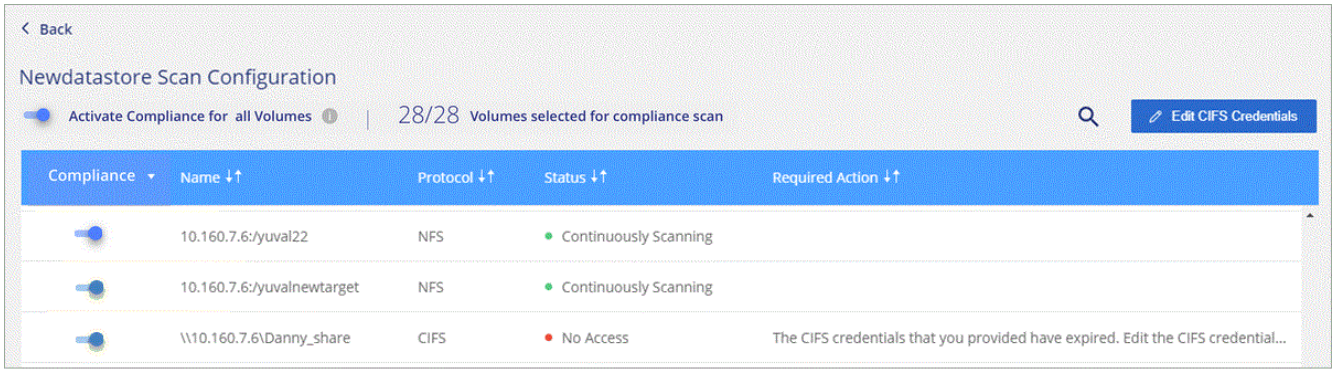
      The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read any data that requires elevated permissions. The credentials are stored on the Cloud Compliance instance.

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



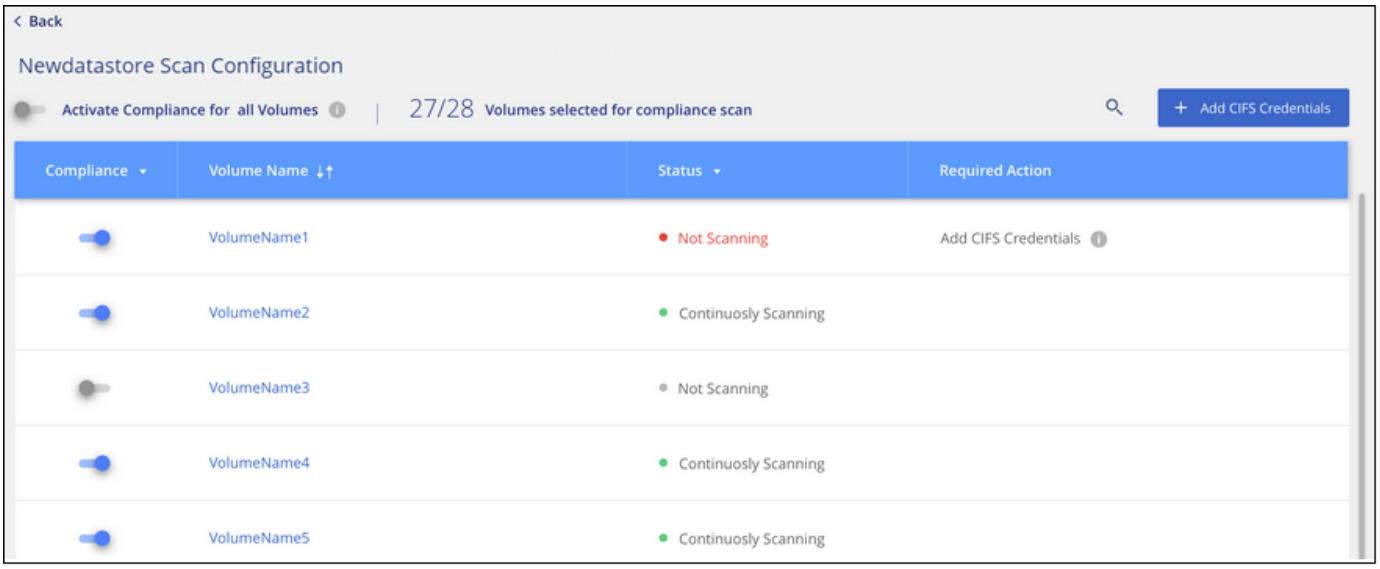
5. On the *Scan Configuration* page, click **View Details** to review the status for each CIFS and NFS volume and correct any errors.

   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.



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.



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 backup files from on-premises ONTAP systems

If you don't want Cloud Compliance to scan volumes directly on your on-prem ONTAP systems, a new Beta

feature released in January 2021 allows you to run compliance scans on backup files created from your on-prem ONTAP volumes. So if you are already creating backup files using Cloud Backup, you can use this new feature to run compliance scans on those backup files.

The Compliance scans you run on backup files are **free** - no Cloud Compliance subscription or license is needed.

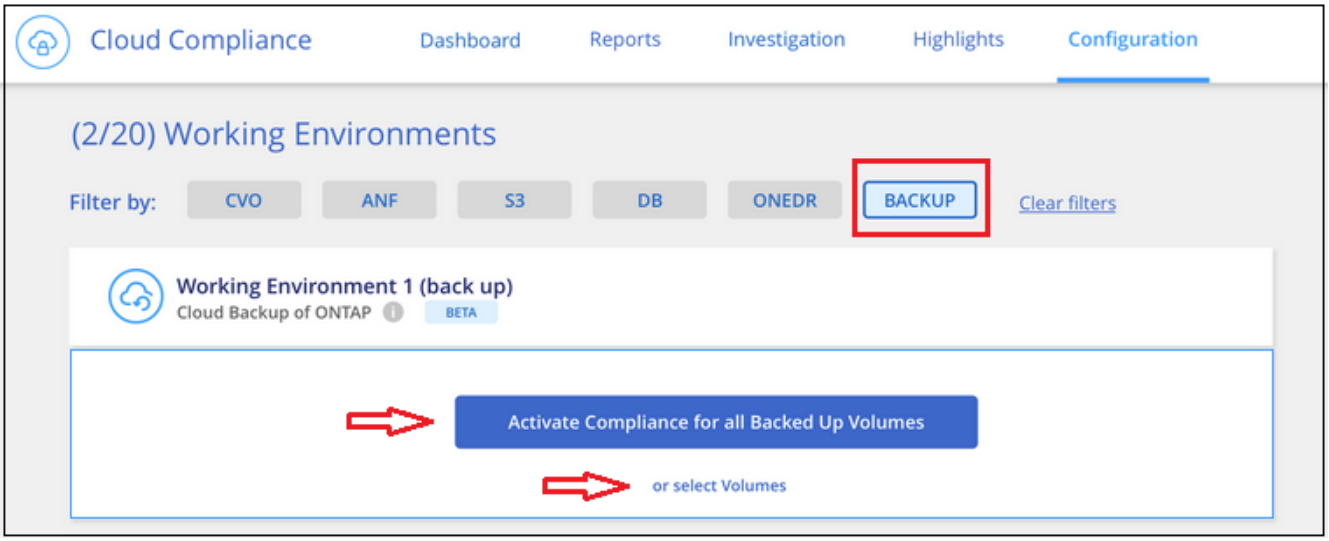
Note: When Compliance scans backup files it uses permissions granted through the Restore instance to access the backup files. Typically the Restore instance powers down when not actively restoring files, but it remains on when scanning backup files. See more information about the Restore instance.

Steps

If you want to scan the backup files from on-prem ONTAP systems:

1. At the top of Cloud Manager, click **Compliance** and then select the **Configuration** tab.
2. From the list of working environments, click the **BACKUP** button from the list of filters.

   All the on-premises ONTAP working environments that have backup files are listed. If you don't have any backup files in an on-prem system, then the working environment is not shown.



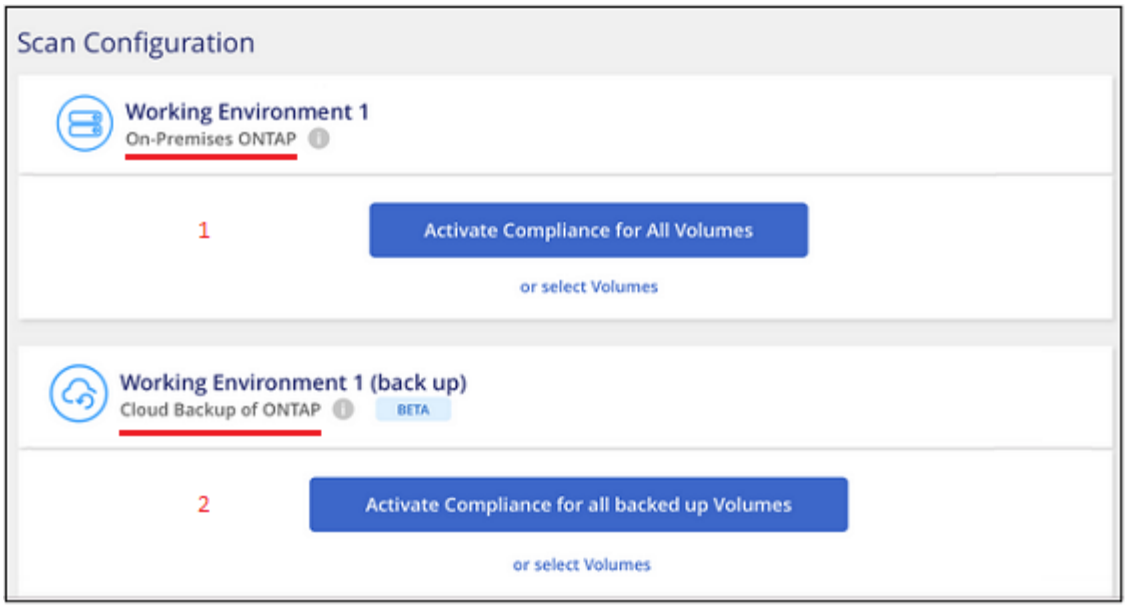
3. To scan all backed up volumes in a working environment, click **Activate Compliance for all backed up Volumes**.

   To scan only certain backed up volumes in a working environment, click **or select Volumes** and then choose the backup files (volumes) that you want to scan.

See Enabling and disabling compliance scans on volumes for details.

Scanning on-prem volumes versus backups of those volumes

When you view the entire list of working environments you will see two listings for each on-prem cluster if they have backed up files.



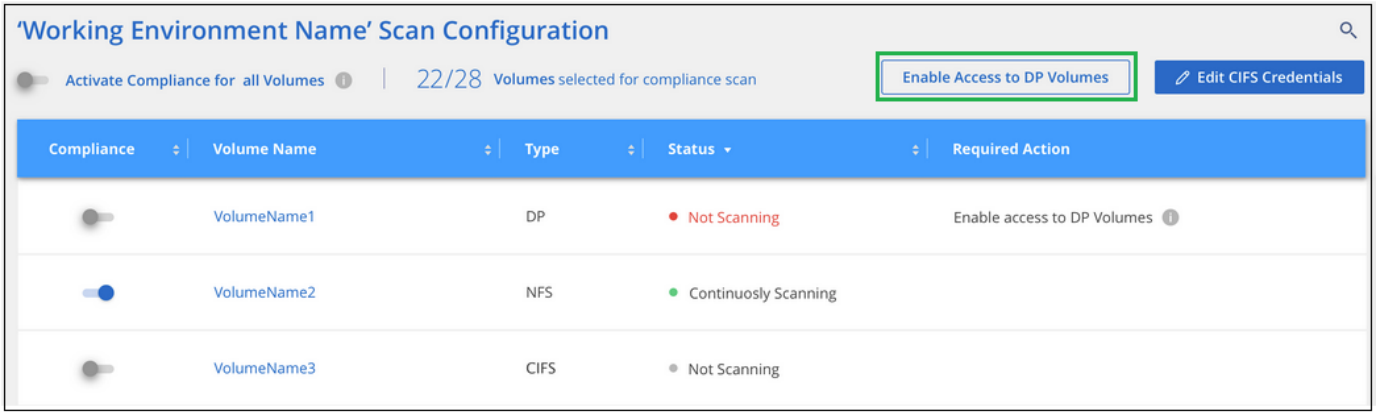
The first item is the on-prem cluster and the actual volumes.
The second item is the backup files from that same on-prem cluster.

Choose the first option to scan the volumes on the on-prem system. Choose the second option to scan the backup files from those volumes. Do not scan both on-prem volumes and backup files of the same cluster.

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 are the destination volumes for SnapMirror operations from an on-premises ONTAP system or from a Cloud Volumes ONTAP system.

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

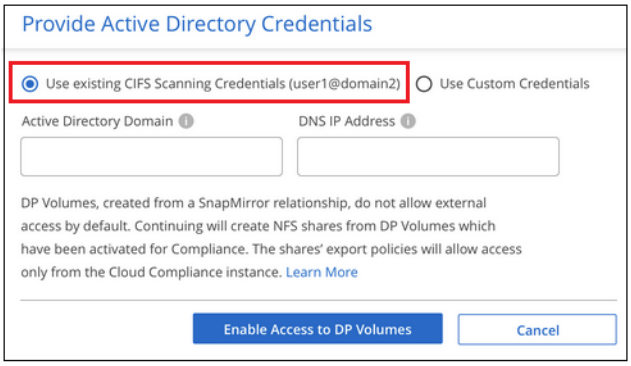


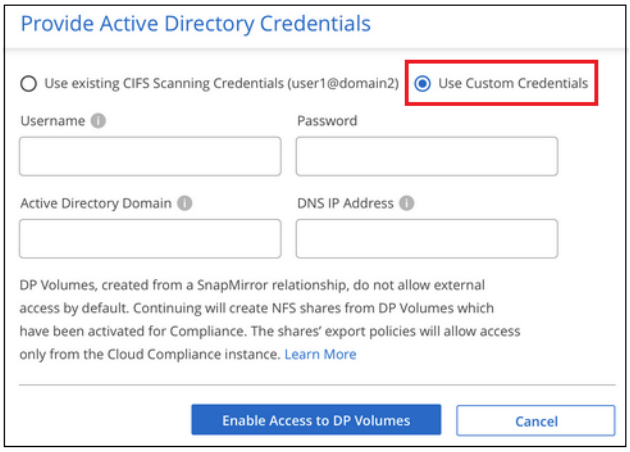
Steps

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. Review the confirmation message and click **Enable Access to DP volumes** again.
    - Volumes that were initially created as NFS volumes in the source ONTAP system are enabled.

- Volumes that were initially created as CIFS volumes in the source ONTAP system require that you enter CIFS credentials to scan those DP volumes. If you already entered Active Directory credentials so that Cloud Compliance can scan CIFS volumes you can use those credentials, or you can specify a different set of Admin credentials.





3. Activate each DP volume that you want to scan the same way you enabled other volumes, or use the **Activate Compliance for all Volumes** control to enable all volumes, including all DP volumes.

Result

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.

Note: If you had no CIFS data protection volumes when you initially enabled access to DP volumes, and later add some, the button **Enable Access to CIFS DP** appears at the top of the Scan Configuration page. Click this button and add CIFS credentials to enable access to these CIFS DP volumes.