



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 1
 - Quick start 1
 - Deploying the Cloud Compliance instance..... 2
 - Enabling Cloud Compliance in your working environments 2
 - Verifying that Cloud Compliance has access to volumes 3
 - Enabling and disabling compliance scans on volumes..... 4
 - Scanning data protection volumes..... 5

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.



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

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

The screenshot shows the 'Scan Configuration' page in Cloud Manager. At the top, there is a 'View Dashboard >' link and a button 'How to add AWS accounts to scan S3' with an external link icon. The page is divided into three main sections for different environments:

- AWS Account Number 1** (Amazon S3): Includes a note: '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.'
- Azure Netapp Files** (Azure NetApp Files): Features a blue button 'Activate Compliance for All Volumes' and a link 'or select Volumes' below it.
- Working Environment Name 1** (Cloud Volumes ONTAP): Features a blue button 'Activate Compliance for All Volumes' and a link 'or select Volumes' below it.

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.

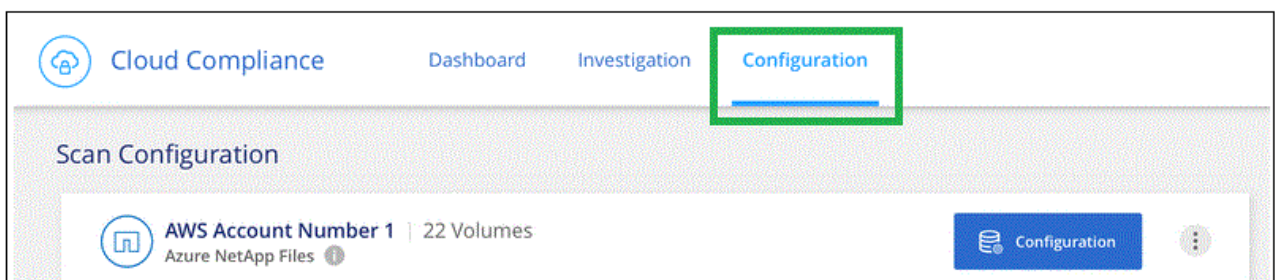


For Azure NetApp Files, Cloud Compliance can only scan volumes that are in the same region as Cloud Manager.

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.

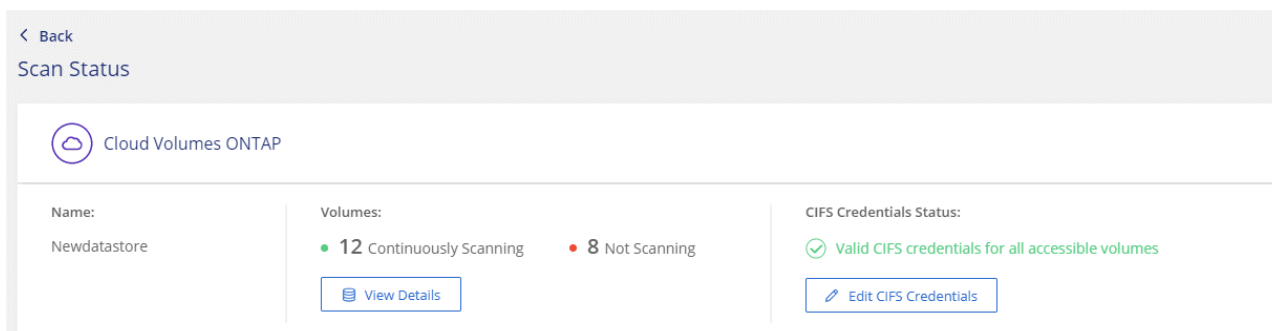
3. Ensure that NFS volume export policies include the IP address of the Cloud Compliance instance so it can access the data on each volume.
4. If you use CIFS, provide Cloud Compliance with Active Directory credentials so it can scan CIFS volumes.
 - a. At the top of Cloud Manager, click **Cloud Compliance**.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

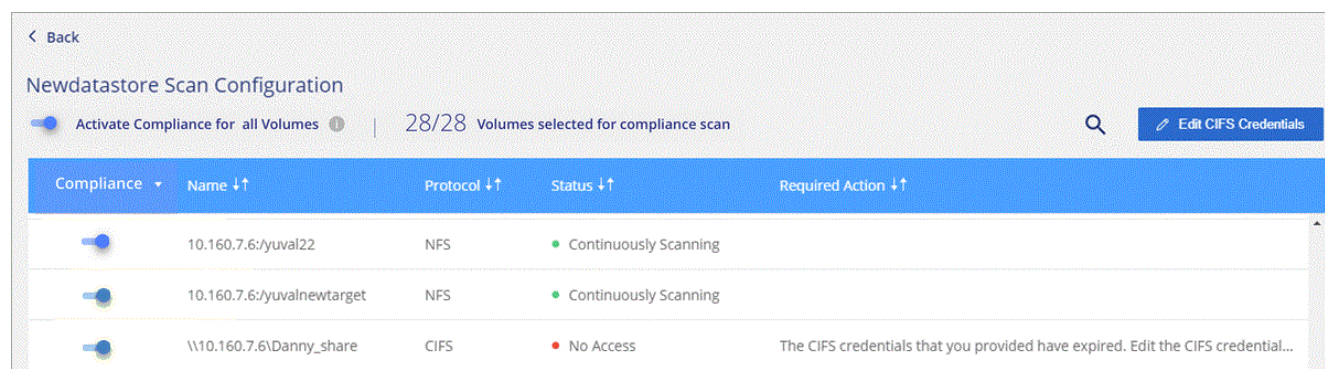
The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read any data that requires elevated permissions. The credentials are stored on the Cloud Compliance instance.

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



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.

< Back

Newdatastore Scan Configuration

Activate Compliance for all Volumes

27/28 Volumes selected for compliance scan

+ Add CIFS Credentials

Compliance	Volume Name	Status	Required Action
<div><div></div></div>	VolumeName1	<div><div></div>Not Scanning</div>	<div>Add CIFS Credentials</div>
<div><div></div></div>	VolumeName2	<div><div></div>Continuously Scanning</div>	
<div><div></div></div>	VolumeName3	<div><div></div>Not Scanning</div>	
<div><div></div></div>	VolumeName4	<div><div></div>Continuously Scanning</div>	
<div><div></div></div>	VolumeName5	<div><div></div>Continuously Scanning</div>	

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

Enable Access to DP Volumes

Edit CIFS Credentials

Compliance	Volume Name	Type	Status	Required Action
<div></div>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<div></div>	VolumeName2	NFS	Continuously Scanning	
<div></div>	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

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.