



# Scanning on-premises ONTAP data with Cloud Compliance

## Cloud Manager

Tom Onacki, Ben Cammett  
December 07, 2020

This PDF was generated from [https://docs.netapp.com/us-en/occm/task\\_scanning\\_onprem.html](https://docs.netapp.com/us-en/occm/task_scanning_onprem.html) on December 07, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

- Scanning on-premises ONTAP data with Cloud Compliance ..... 1
  - Scanning data in on-premises ONTAP working environments..... 1
  - Verifying that Cloud Compliance has access to volumes ..... 2
  - Scanning on-premises ONTAP data by using SnapMirror ..... 4

# Scanning on-premises ONTAP data with Cloud Compliance

You can scan data on your on-premises ONTAP systems directly using Cloud Compliance. You can also replicate the on-prem NFS or CIFS data to a Cloud Volumes ONTAP working environment and then enable compliance for those data protection volumes. Choose whichever way works best for you.

## Scanning data in on-premises ONTAP working environments

If you have [discovered your ONTAP clusters](#) and added them to a working environment in Cloud Manager, you can scan volume data directly from those on-prem clusters.

Complete a few steps to get started with Cloud Compliance for on-premises ONTAP clusters.

### 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 on-prem working environments and select the volumes to scan

Click **Compliance**, select the **Configuration** tab, and activate compliance scans for all volumes or just specific volumes.



#### Ensure access to volumes

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

- The Cloud Compliance instance needs a network connection to each on-prem ONTAP system.
- Security groups 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 are scanning

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

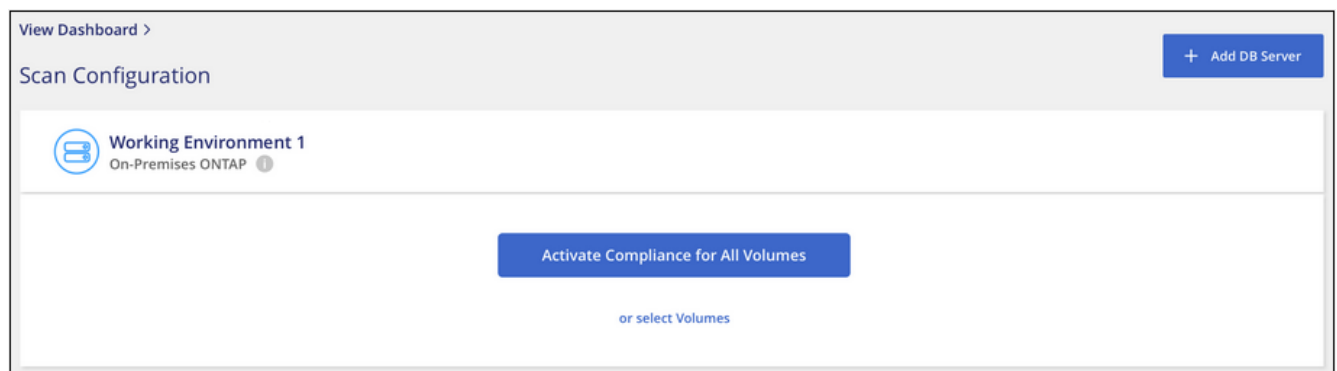
## Deploying the Cloud Compliance instance

[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 on-premises ONTAP clusters.

## Enabling Cloud Compliance in your working environments

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

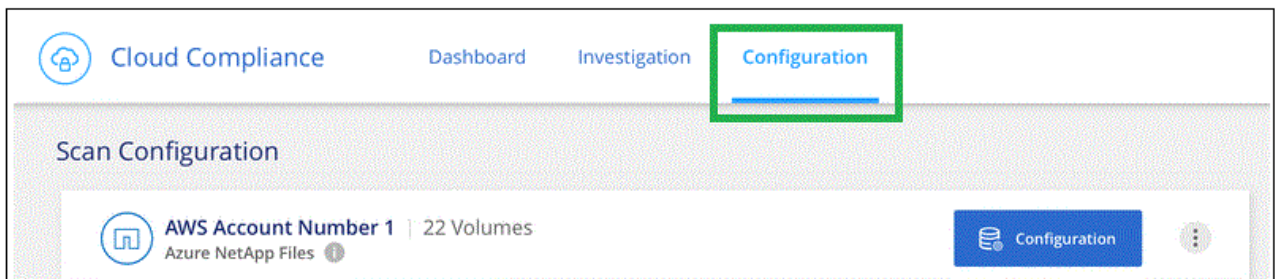
volumes.

### Steps

1. Make sure that there's a network connection between the Cloud Compliance instance and each network that includes volumes for on-prem ONTAP systems.
2. Ensure that the security group for the on-prem ONTAP systems allow inbound traffic from the Cloud Compliance instance.

You can do this by opening the security group for traffic from the IP address of the Cloud Compliance instance.

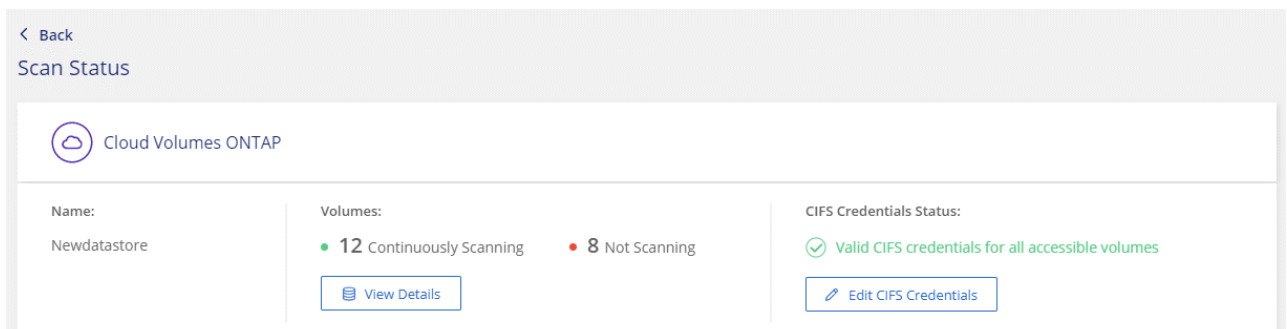
3. Ensure that NFS volume export policies include the IP address of the Cloud Compliance instance so it can access the data on each volume.
4. If you use CIFS, provide Cloud Compliance with Active Directory credentials so it can scan CIFS volumes.
  - a. At the top of Cloud Manager, click **Compliance**.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

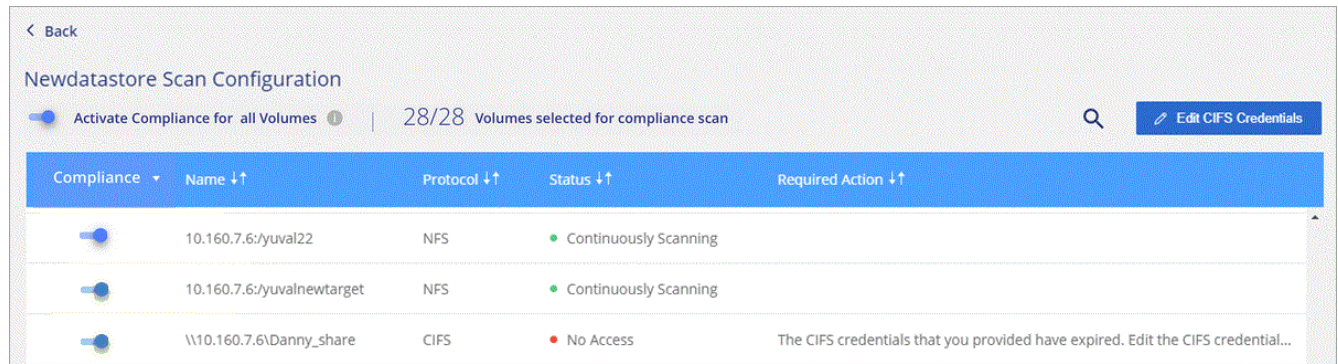
The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read any data that requires elevated permissions. The credentials are stored on the Cloud Compliance instance.

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.



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...

## Scanning on-premises ONTAP data by using SnapMirror

You can scan your on-premises ONTAP data with Cloud Compliance by replicating the on-prem NFS or CIFS data to a Cloud Volumes ONTAP working environment and then enabling compliance on those data protection volumes.

### TIP

We recommend that you discover your on-prem ONTAP systems in Cloud Manager to add them to a working environment so that you can [scan data on those system directly from Cloud Compliance](#).

You must have [deployed an instance of Cloud Compliance in Cloud Manager already](#).

### Steps

1. From Cloud Manager, create a SnapMirror relationship between the on-premises ONTAP cluster and Cloud Volumes ONTAP.
  - a. [Discover the on-premises cluster in Cloud Manager](#).
  - b. [Create a SnapMirror replication between the on-premises ONTAP cluster and Cloud Volumes ONTAP from Cloud Manager](#).
2. From Cloud Manager, activate Cloud Compliance on the Cloud Volumes ONTAP working environment that contains the SnapMirror data:
  - a. Click **Canvas**.
  - b. Select the working environment that contains the SnapMirror data and click **Enable Compliance**.

[Click here if you need help with enabling Cloud Compliance on a Cloud Volumes ONTAP system.](#)

3. Click the **Enable Access to DP volumes** button at the top of the *Scan Configuration* page so that

Cloud Compliance can access the DP volumes.

NFS volumes are enabled, but CIFS volumes require that you enter Active Directory Admin credentials.

4. 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.

See [Scanning data protection volumes](#) for more information.

## 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.