



Getting started with Cloud Compliance

Cloud Manager

Ben Cammett, Tom Onacki

June 03, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_getting_started_compliance.html on June 15, 2020. Always check docs.netapp.com for the latest.



Table of Contents

- Getting started with Cloud Compliance..... 1
 - Quick start 1
 - Reviewing prerequisites 2
 - Enabling Cloud Compliance on a new working environment..... 4
 - Enabling Cloud Compliance on existing working environments 5
 - Verifying that Cloud Compliance has access to volumes 6

Getting started with Cloud Compliance

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.



Review prerequisites

Ensure that your cloud environment can meet the prerequisites, which includes 16 vCPUs for the Cloud Compliance instance, outbound internet access for the instance, connectivity between Cloud Manager and Cloud Compliance over port 80, and more. [See the complete list.](#)



Enable Cloud Compliance

- New working environments: Be sure to keep Cloud Compliance enabled when you create the working environment (it's enabled by default).
- Existing working environments: Click **Compliance**, optionally edit the list of working environments, and click **Show Compliance Dashboard**.



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 **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.

Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance. You'll need to ensure connectivity to volumes after you enable Cloud Compliance. That's covered below.

Enable outbound internet access

Cloud Compliance requires outbound internet access. If your virtual network uses a proxy server for internet access, ensure that the Cloud Compliance instance has outbound internet access to contact the following endpoints. Note that Cloud Manager deploys the Cloud Compliance instance in the same subnet as Cloud Manager.

Endpoints	Purpose
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.
https://netapp-cloud-account.auth0.com https://auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Provides access to software images, manifests, and templates.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.

Ensure that Cloud Manager has the required permissions

Ensure that Cloud Manager has permissions to deploy resources and create security groups for the Cloud Compliance instance. You can find the latest Cloud Manager permissions in [the policies provided by NetApp](#).

Check your vCPU limits

Ensure that your cloud provider's vCPU limit allows for the deployment of an instance with 16 cores. You'll need to verify the vCPU limit for the relevant instance family in the region where Cloud Manager is running.

In AWS, the instance family is *On-Demand Standard instances*. In Azure, the instance family is *Standard D5v3 Family*.

For more details on vCPU limits, see the following:

- [AWS documentation: Amazon EC2 Service Limits](#)
- [Azure documentation: Virtual machine vCPU quotas](#)

Ensure that Cloud Manager can access Cloud Compliance

Ensure connectivity between Cloud Manager and the Cloud Compliance instance:

- The security group for Cloud Manager must allow inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.

This connection enables deployment of the Cloud Compliance instance and enables you to view information in the Compliance tab.

- If your AWS network doesn't use a NAT or proxy for internet access, modify the security group for Cloud Manager to allow inbound traffic over TCP port 3128 from the Cloud Compliance instance.

This is required because the Cloud Compliance instance uses Cloud Manager as a proxy to access the internet.



This port is open by default on all new Cloud Manager instances, starting with version 3.7.5. It's not open on Cloud Manager instances created prior to that.

Set up discovery of Azure NetApp Files

Before you can scan volumes for Azure NetApp Files, [Cloud Manager must be set up to discover the configuration](#).

Ensure that you can keep Cloud Compliance running

The Cloud Compliance instance needs to stay on to continuously scan your data.

Ensure web browser connectivity to Cloud Compliance

After Cloud Compliance is enabled, ensure that users access the Cloud Manager interface from a host that has a connection to the Cloud Compliance instance.

The Cloud Compliance instance uses a private IP address to ensure that the indexed data isn't accessible to the internet. As a result, the web browser that you use to access Cloud Manager must have a connection to that private IP address. That connection can come from a direct connection to AWS or Azure (for example, a VPN), or from a host that's inside the same network as the Cloud Compliance instance.



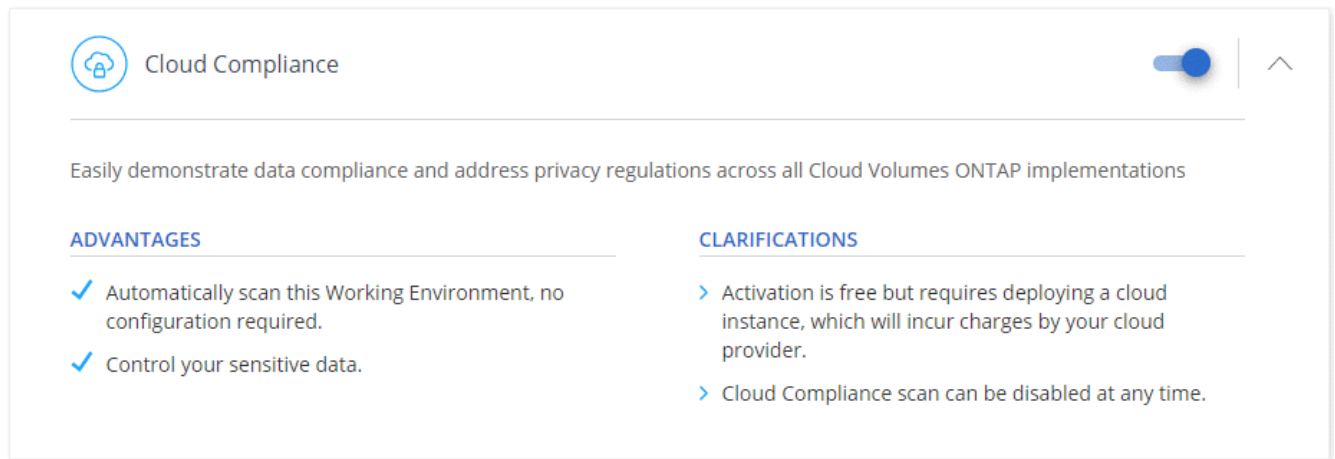
If you're accessing Cloud Manager from a public IP address, then your web browser probably isn't running on a host inside the network.

Enabling Cloud Compliance on a new working environment

Cloud Compliance is enabled by default in the Cloud Volumes ONTAP working environment wizard. Be sure to keep the option enabled.

Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services or Microsoft Azure as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave Cloud Compliance enabled and click **Continue**.



5. Complete the pages in the wizard to deploy the system.

For help, see [Launching Cloud Volumes ONTAP in AWS](#) and [Launching Cloud Volumes ONTAP in Azure](#).

Result

Cloud Compliance is enabled on the Cloud Volumes ONTAP system. If this is the first time that you enabled Cloud Compliance, Cloud Manager deploys the Cloud Compliance instance in your cloud provider.

As soon as the instance is available, Cloud Compliance starts scanning the data in the working environment. Results will be available in the Compliance dashboard as soon as Cloud Compliance finishes the initial scans.

Enabling Cloud Compliance on existing working environments

If you haven't enabled Cloud Compliance yet, enable it on existing Cloud Volumes ONTAP or Azure NetApp Files working environments from the **Compliance** tab in Cloud Manager.


Another option is to enable Cloud Compliance from the **Working Environments** tab by selecting each working environment individually.

Steps for multiple working environments (first time only)

1. At the top of Cloud Manager, click **Compliance**.
2. If you want to enable Cloud Compliance on specific working environments, click the edit icon.


Otherwise, Cloud Manager is set to enable Cloud Compliance on all working environments to which you have access.

Always on Privacy & Compliance Controls



Automatic Compliance Reports


- > Generate compliance reports for privacy regulations: GDPR, CCPA, PCI, HIPAA, and more.
- > Identify sensitive data in your organization.



Reduce TCO

- > Reduce expensive data compliance overhead on long collaboration processes.
- > Cloud Compliance is provided by NetApp at no extra cost.


Activation requires deploying a cloud instance, which will incur charges from your cloud provider.



Fully Secure

- > There's no impact to your data.
- > Uses an agentless solution.

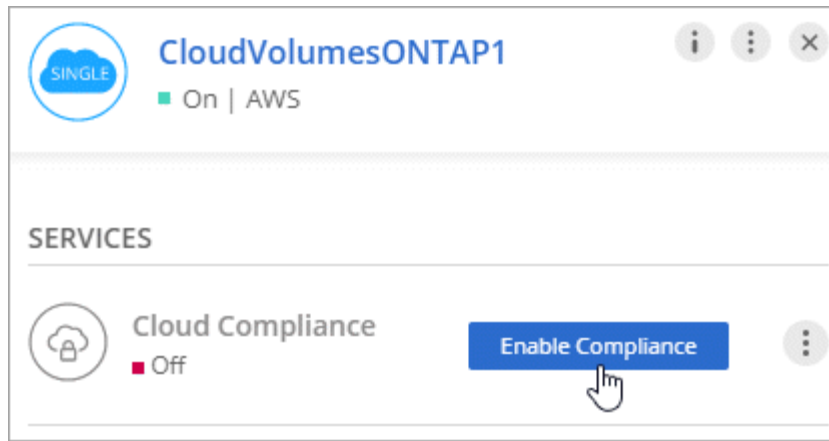
Show Compliance Dashboard

All working environments will be scanned 

3. Click **Show Compliance Dashboard**.

Steps for a single working environment

1. At the top of Cloud Manager, click **Working Environments**.
2. Select a working environment.
3. In the pane on the right, click **Enable Compliance**.



Result

If this is the first time that you enabled Cloud Compliance, Cloud Manager deploys the Cloud Compliance instance in your cloud provider.

As soon as the instance is available, 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.



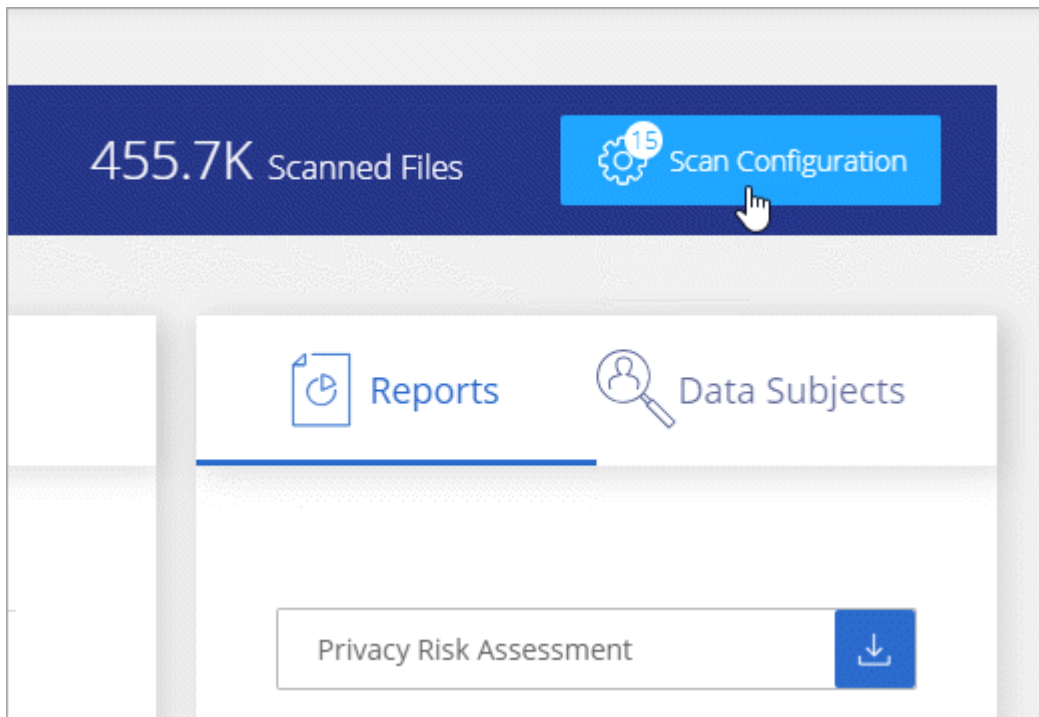
For Azure NetApp Files, Cloud Compliance can only scan volumes that are in the same region as Cloud Manager.

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.

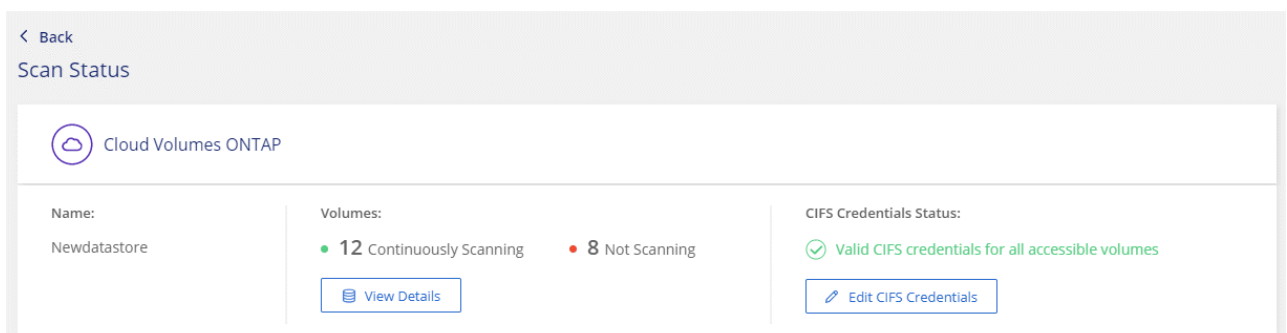
- a. At the top of Cloud Manager, click **Compliance**.
- b. In the top right, click **Scan Configuration**.



- 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.

Newdatastore Scan Configuration

23/23 Volumes selected for compliance scan



[Edit CIFS Credentials](#)

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...

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.