



Activate scanning on your data sources

Cloud Manager

NetApp

December 07, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_getting_started_compliance.html on December 07, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Activate scanning on your data sources 1
 - Getting started with Cloud Compliance for Cloud Volumes ONTAP, on-premises ONTAP, or Azure NetApp Files. 1
 - Getting started with Cloud Compliance for Amazon S3 7
 - Scanning database schemas 15

Activate scanning on your data sources

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 working environments at this time.

Your Cloud Volumes ONTAP systems should already be available in working environments 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

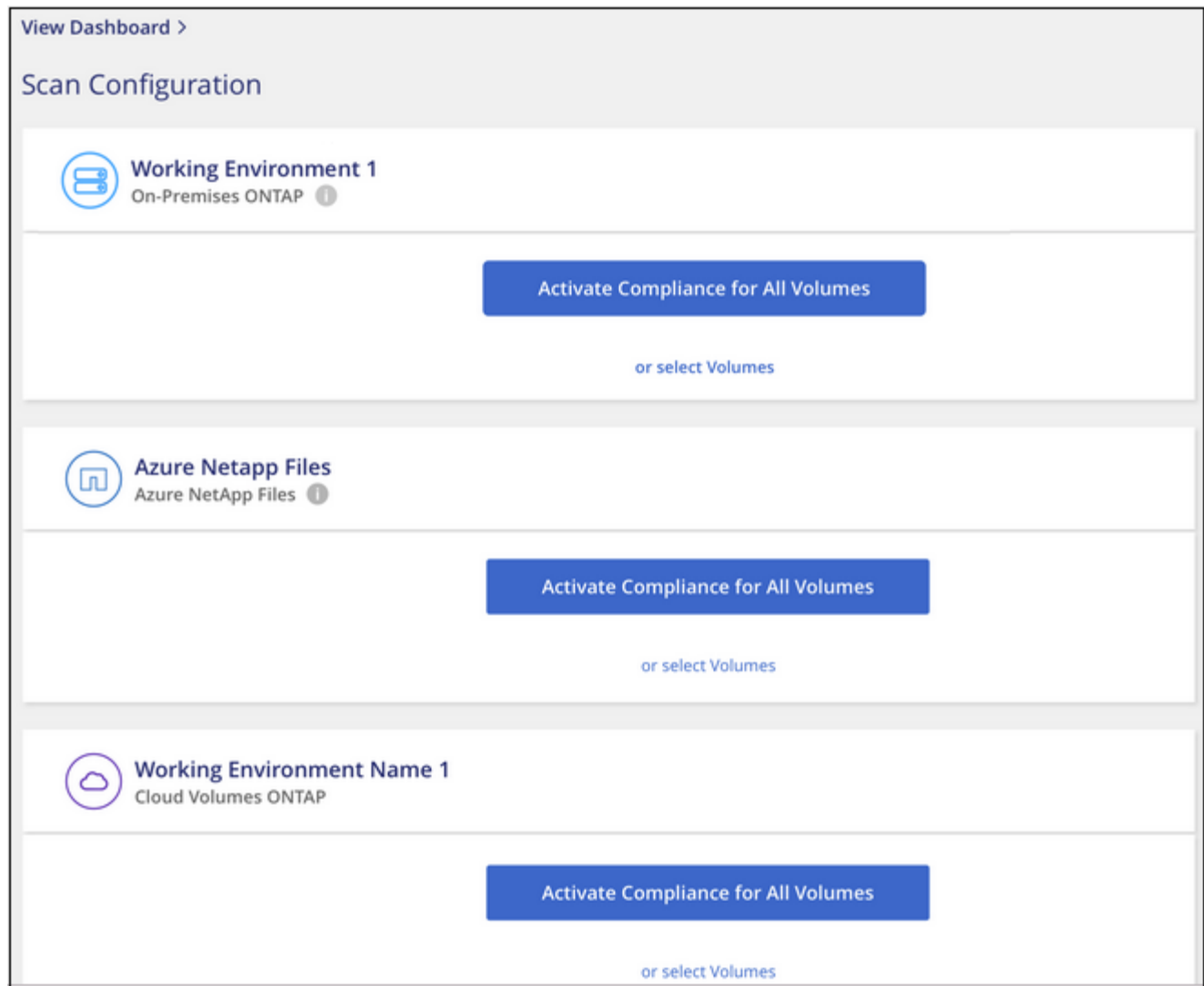
[Deploy Cloud Compliance](#) if there isn't already an instance deployed.

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

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.

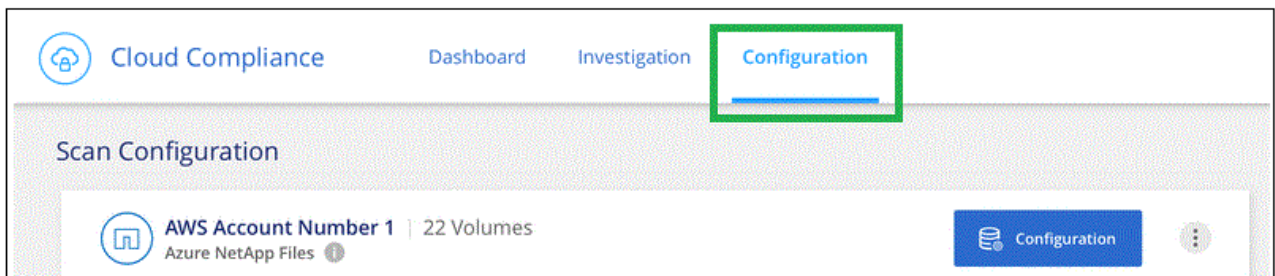


For Azure NetApp Files, Cloud Compliance can only scan volumes that are in the same region as Cloud Manager.

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.

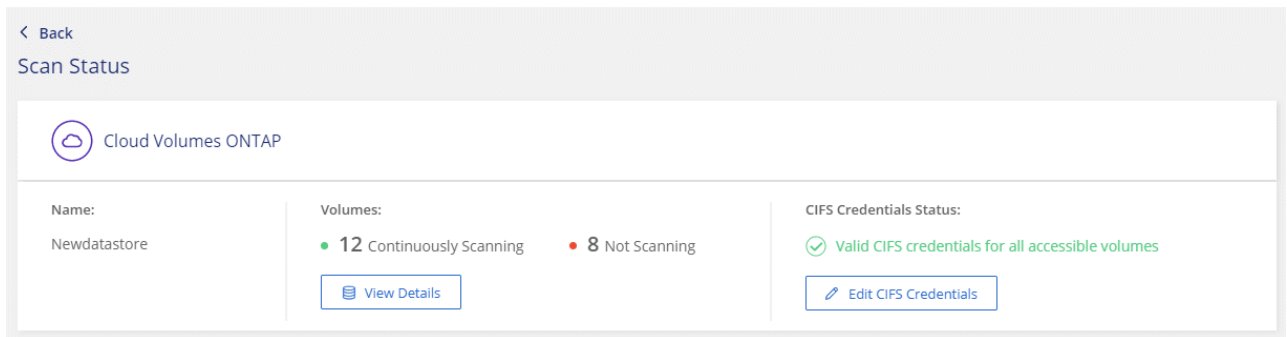
3. Ensure that NFS volume export policies include the IP address of the Cloud Compliance instance so it can access the data on each volume.
4. If you use CIFS, provide Cloud Compliance with Active Directory credentials so it can scan CIFS volumes.
 - a. At the top of Cloud Manager, click **Compliance**.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

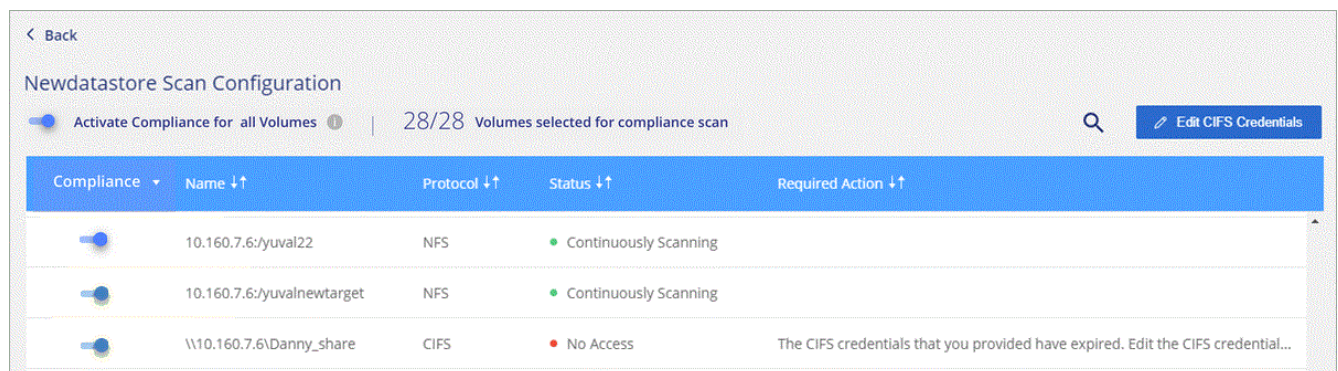
The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read any data that requires elevated permissions. The credentials are stored on the Cloud Compliance instance.

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



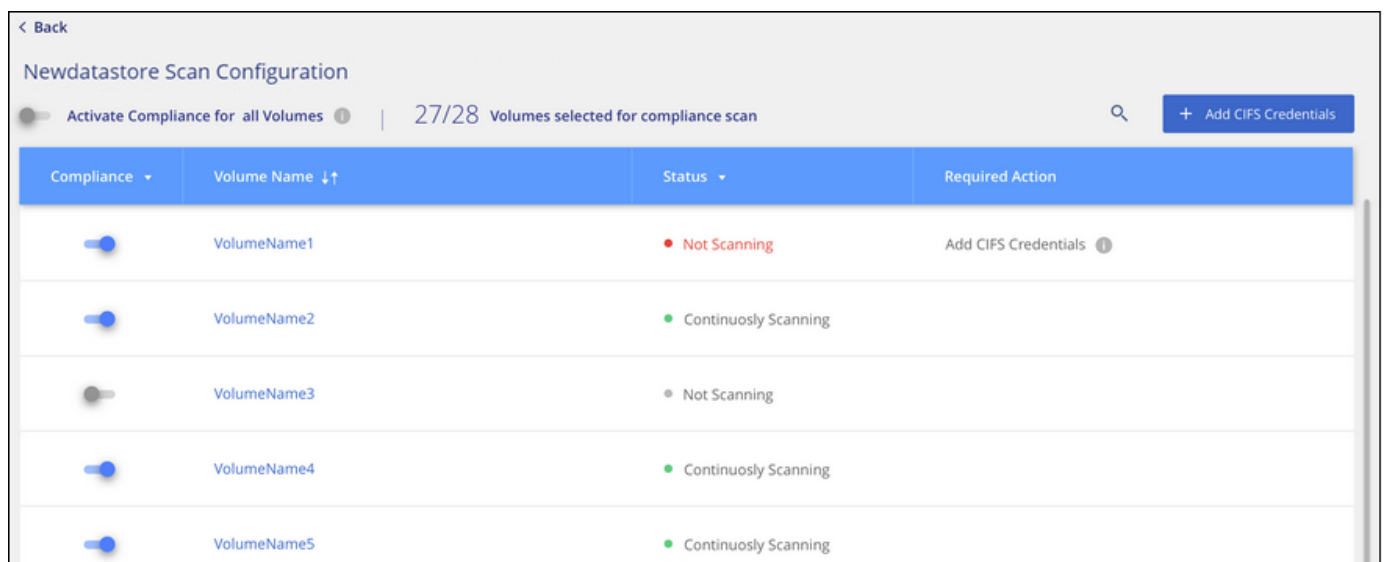
- On the *Scan Configuration* page, click **View Details** to review the status for each CIFS and NFS volume and correct any errors.

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 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*.

'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
<input type="checkbox"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<input checked="" type="checkbox"/>	VolumeName2	NFS	Continuously Scanning	
<input type="checkbox"/>	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. 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.

The image shows two versions of the 'Provide Active Directory Credentials' dialog box. In the left version, the radio button for 'Use existing CIFS Scanning Credentials (user1@domain2)' is selected and highlighted with a red box. In the right version, the radio button for 'Use Custom Credentials' is selected and highlighted with a red box. Both versions contain input fields for 'Active Directory Domain', 'DNS IP Address', 'Username', and 'Password'. A disclaimer text is present below the input fields, and at the bottom are 'Enable Access to DP Volumes' and 'Cancel' buttons.

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.

Getting started with Cloud Compliance for Amazon S3

Cloud Compliance can scan your Amazon S3 buckets to identify the personal and sensitive data that resides in S3 object storage. Cloud Compliance can scan any bucket in the account, regardless if it was created for a NetApp solution.

Quick start

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



Set up the S3 requirements in your cloud environment

Ensure that your cloud environment can meet the requirements for Cloud Compliance, including preparing an IAM role and setting up connectivity from Cloud Compliance to S3. [See the complete list.](#)



Deploy the Cloud Compliance instance

Deploy [Cloud Compliance](#) if there isn't already an instance deployed.



Activate Compliance on your S3 working environment

Select the Amazon S3 working environment, click **Enable Compliance**, and select an IAM role that includes the required permissions.



Select the buckets to scan

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

Reviewing S3 prerequisites

The following requirements are specific to scanning S3 buckets.

Set up an IAM role for the Cloud Compliance instance

Cloud Compliance needs permissions to connect to the S3 buckets in your account and to scan them. Set up an IAM role that includes the permissions listed below. Cloud Manager prompts you to select an IAM role when you enable Cloud Compliance on the Amazon S3 working environment.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}

```

Provide connectivity from Cloud Compliance to Amazon S3

Cloud Compliance needs a connection to Amazon S3. The best way to provide that connection is through a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Compliance instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Compliance can't connect to the S3 service.

If you experience any issues, see [AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?](#)

An alternative is to provide the connection by using a NAT Gateway.



You can't use a proxy to get to S3 over the internet.

Deploying the Cloud Compliance instance

[Deploy Cloud Compliance in Cloud Manager](#) if there isn't already an instance deployed.

You need to deploy the instance in an AWS Connector so that Cloud Manager automatically discovers the S3 buckets in this AWS account and displays them in an Amazon S3 working environment.

Note: Deploying Cloud Compliance in an on-premises location is not currently supported when scanning S3 buckets.

Activating Compliance on your S3 working environment

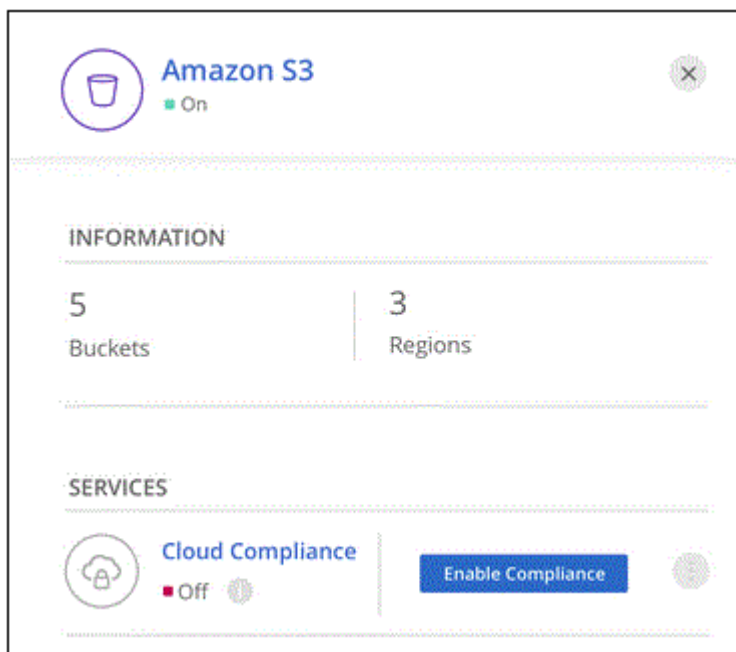
Enable Cloud Compliance on Amazon S3 after you verify the prerequisites.

Steps

1. At the top of Cloud Manager, click **Canvas**.
2. Select the Amazon S3 working environment.



3. In the pane on the right, click **Enable Compliance**.



4. When prompted, assign an IAM role to the Cloud Compliance instance that has [the required permissions](#).

Assign an AWS IAM Role for Cloud Compliance

To enable Cloud Compliance on Amazon S3 buckets, select an existing IAM role. Make sure that your AWS IAM role has the permission defined in the [Policy Requirements](#).

Select IAM Role

NetAppCloudCompliance

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so Cloud Compliance can securely scan the data.

Alternatively, ensure that the Cloud Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.


Free for the 1st TB

Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable ComplianceCancel

5. Click **Enable Compliance**.



You can also enable compliance scans for a working environment from the Scan Configuration page by clicking the  button and selecting **Activate Compliance**.

Result

Cloud Manager assigns the IAM role to the instance.

Enabling and disabling compliance scans on S3 buckets

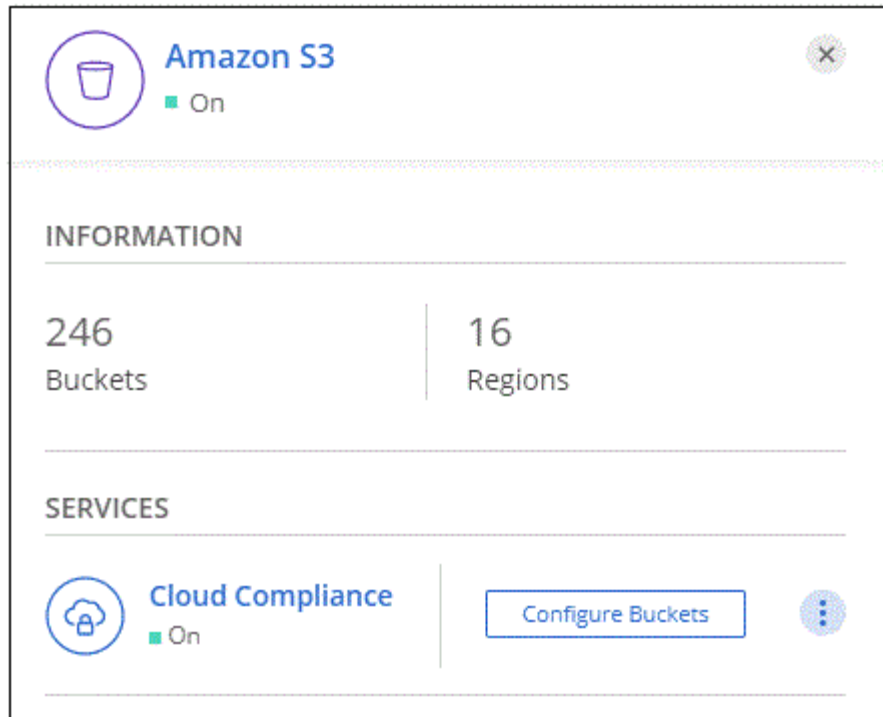
After Cloud Manager enables Cloud Compliance on Amazon S3, the next step is to configure the buckets that you want to scan.

When Cloud Manager is running in the AWS account that has the S3 buckets you want to scan, it discovers those buckets and displays them in an Amazon S3 working environment.

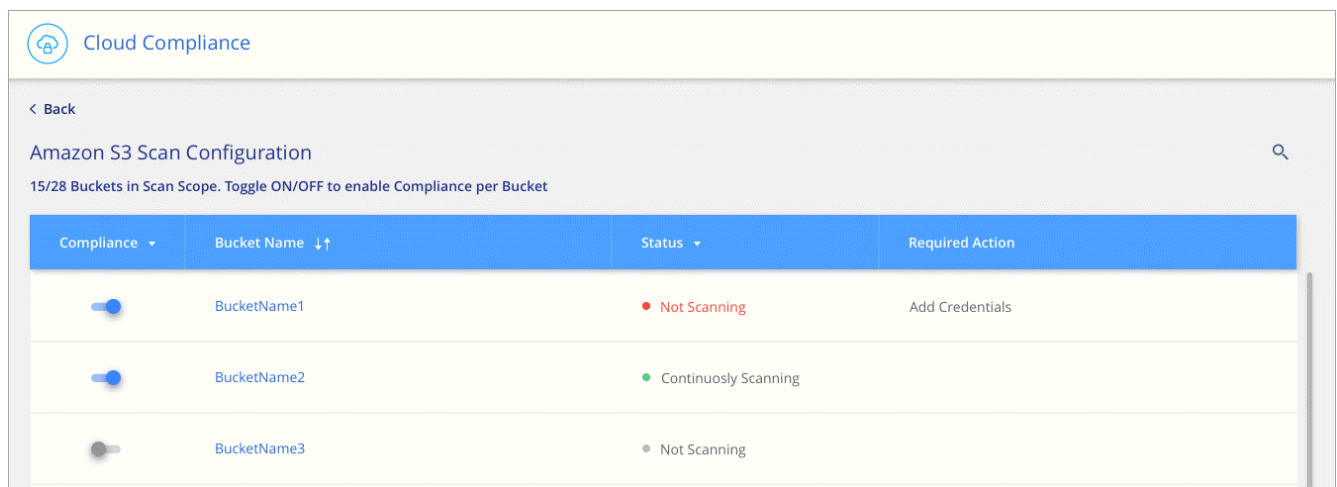
Cloud Compliance can also [scan S3 buckets that are in different AWS accounts](#).

Steps

1. Select the Amazon S3 working environment.
2. In the pane on the right, click **Configure Buckets**.



3. Enable compliance on the buckets that you want to scan.



Result

Cloud Compliance starts scanning the S3 buckets that you enabled. If there are any errors, they'll appear in the Status column, alongside the required action to fix the error.

Scanning buckets from additional AWS accounts

You can scan S3 buckets that are under a different AWS account by assigning a role from that account to access the existing Cloud Compliance instance.

Steps

1. Go to the target AWS account where you want to scan S3 buckets and create an IAM role by selecting **Another AWS account**.

Create role





1

2

3

4


Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
 - ☐ Require MFA 

Be sure to do the following:

- Enter the ID of the account where the Cloud Compliance instance resides.
- Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
- Attach the Cloud Compliance IAM policy. Make sure it has the required permissions.

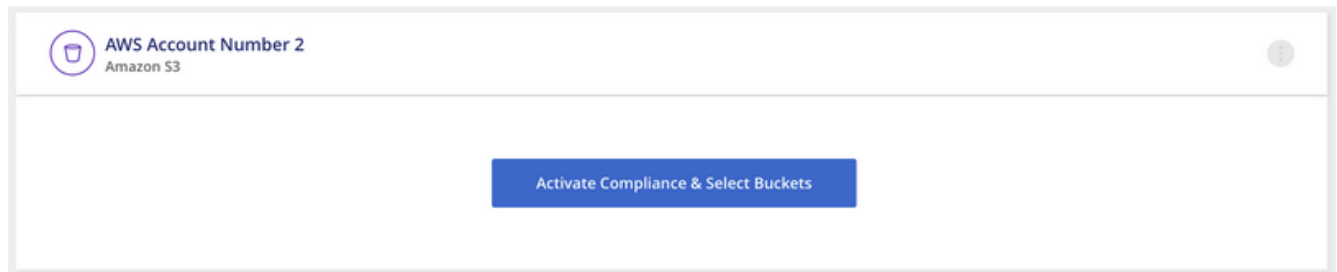
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

- Go to the source AWS account where the Cloud Compliance instance resides and select the IAM role that is attached to the instance.
 - Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
 - Click **Attach policies** and then click **Create policy**.
 - Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

The Cloud Compliance instance profile account now has access to the additional AWS account.

3. Go to the **Amazon S3 Scan Configuration** page and the new AWS account is displayed. Note that it can take a few minutes for Cloud Compliance to sync the new account's working environment and show this information.



4. Click **Activate Compliance & Select Buckets** and select the buckets you want to scan.

Result

Cloud Compliance starts scanning the new S3 buckets that you enabled.

Scanning database schemas

Complete a few steps to start scanning your database schemas with Cloud Compliance.

Quick start

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



Review database prerequisites

Ensure that your database is supported and that you have the information necessary to connect to the database.



Deploy the Cloud Compliance instance

Deploy [Cloud Compliance](#) if there isn't already an instance deployed.



Add the database server

Add the database server that you want to access.



Select the schemas

Select the schemas that you want to scan.

Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance.

Supported databases

Cloud Compliance can scan schemas from the following databases:

- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA

- SQL Server (MSSQL)



The statistics gathering feature **must be enabled** in the database.

Database requirements

Any database with connectivity to the Cloud Compliance instance can be scanned, regardless of where it is hosted. You just need the following information to connect to the database:

- IP Address or host name
- Port
- Service name (only for accessing Oracle databases)
- Credentials that allow read access to the schemas

When choosing a user name and password, it's important to choose one that has full read permissions to all the schemas and tables you want to scan. We recommend that you create a dedicated user for the Cloud Compliance system with all the required permissions.

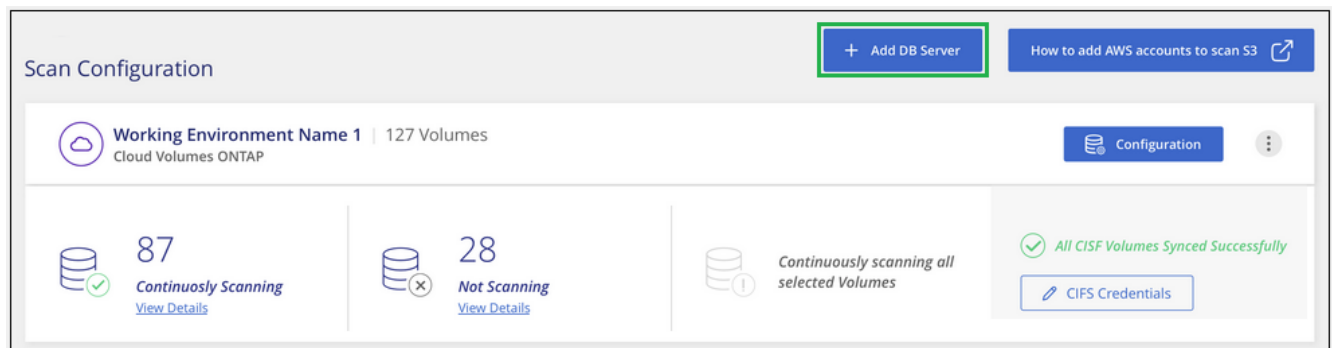
Note: For MongoDB, a read-only Admin role is required.

Adding the database server

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

Add the database server where the schemas reside.

1. From the *Scan Configuration* page, click the **Add DB Server** button.



2. Enter the required information to identify the database server.
 - a. Select the database type.
 - b. Enter the port and the host name or IP address to connect to the database.
 - c. For Oracle databases, enter the Service name.
 - d. Enter the credentials so that Cloud Compliance can access the server.

e. Click **Add DB Server**.

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type

Host Name or IP Address

Port

Service Name

Credentials

Username

Password

Add DB Server

Cancel


The database is added to the list of working directories.


Enabling and disabling compliance scans on database schemas


You can stop or start scanning schemas at any time.


1. From the *Scan Configuration* page, click the **Configuration** button for the database you want to configure.


Scan Configuration

 **Oracle DB 1** | 41 Schemas
Oracle

 Configuration



 No Schemas selected for Compliance

 7
Not Scanning
[View Details](#)

2. Select the schemas that you want to scan by moving the slider to the right.


'Working Environment Name' Scan Configuration			
28/28 Schemas selected for compliance scan			
<div>🔍 Edit Credentials</div>			
Compliance	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	● Not Scanning	Add Credentials ⓘ
<input checked="" type="checkbox"/>	DB1 - SchemaName2	● Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	● Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	● Continuously Scanning	

Result

Cloud Compliance starts scanning the database schemas that you enabled. If there are any errors, they'll appear in the Status column, alongside the required action to fix the error.

Removing a database from Cloud Manager

If you no longer want to scan a certain database, you can delete it from the Cloud Manager interface and stop all scans.

From the *Scan Configuration* page, click the  button in the row for the database, and then click **Remove DB Server**.

Scan Configuration

Oracle DB 1 | 41 Schemas
Oracle

No Schemas selected for Compliance

7
Not Scanning
[View Details](#)

11
No Access - Action Required
[View Details](#)

Configuration ⓘ

Deactivate Compliance

Remove DB Server

+ Credentials

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.