Get started

Cloud Manager

NetApp
June 15, 2020

Table of Contents

Get started

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 DSv3 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**.
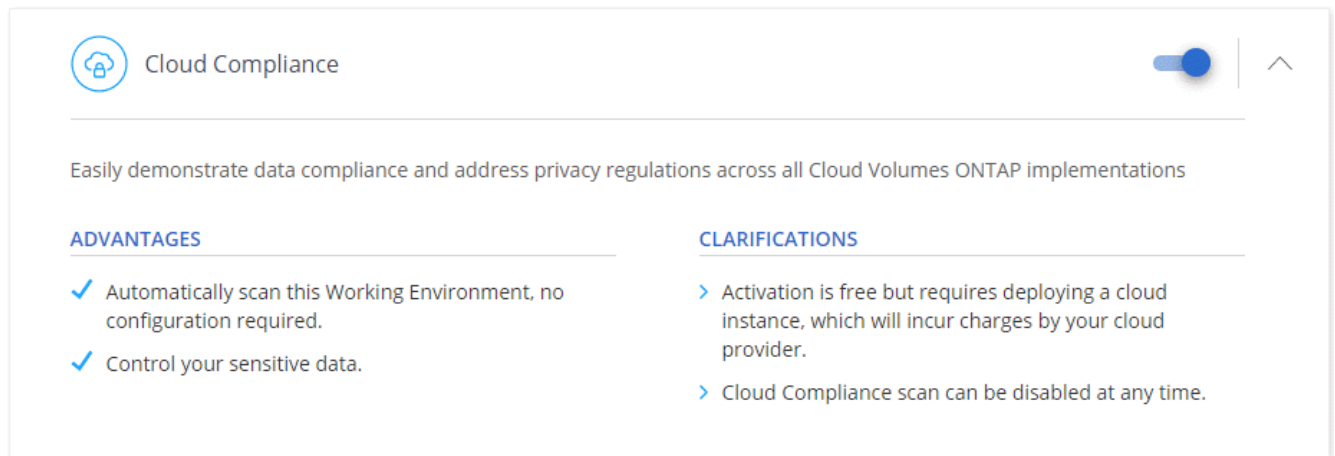
5. Complete the pages in the wizard to deploy the system.

   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.
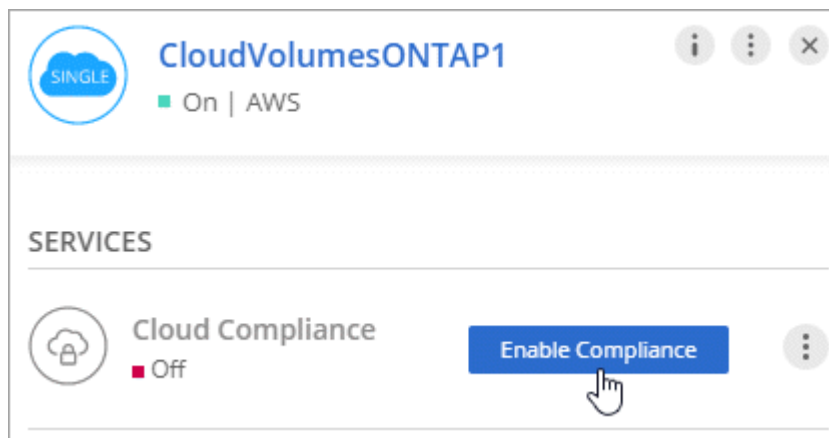
   Otherwise, Cloud Manager is set to enable Cloud Compliance on all working environments to which you have access.
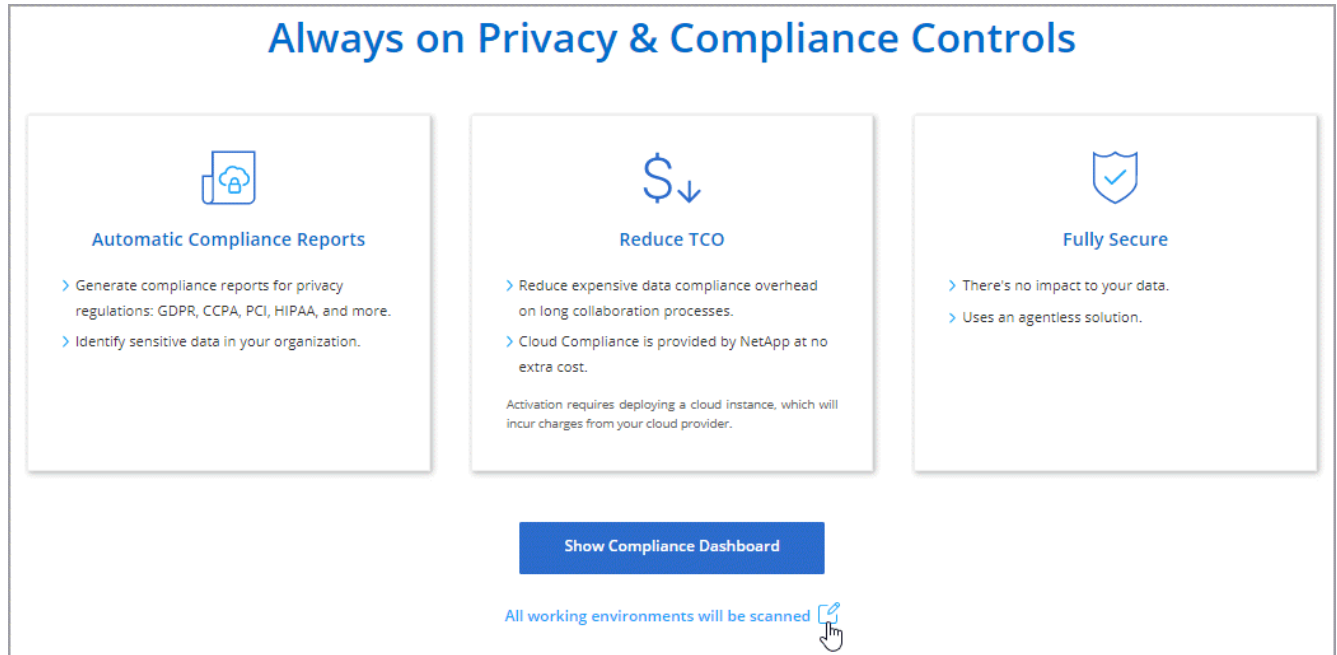
3. Click **Show Compliance Dashboard**.

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 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**.
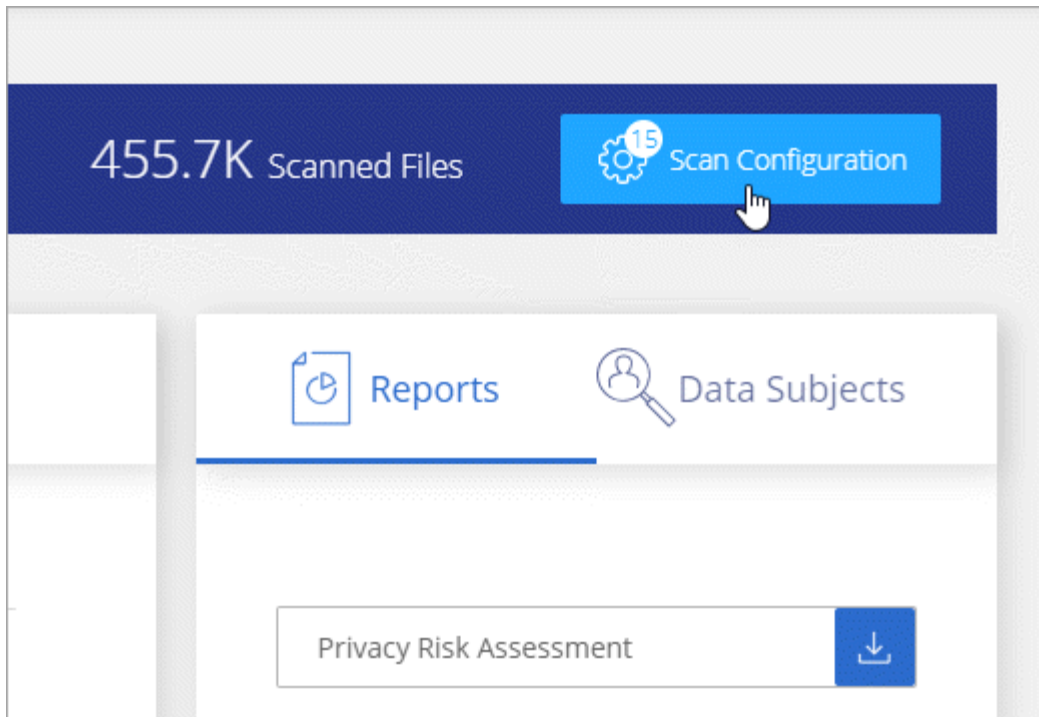
c. For each working environment, click **Edit CIFS Credentials** and enter the user name and password that Cloud Compliance needs to access CIFS volumes on the system.

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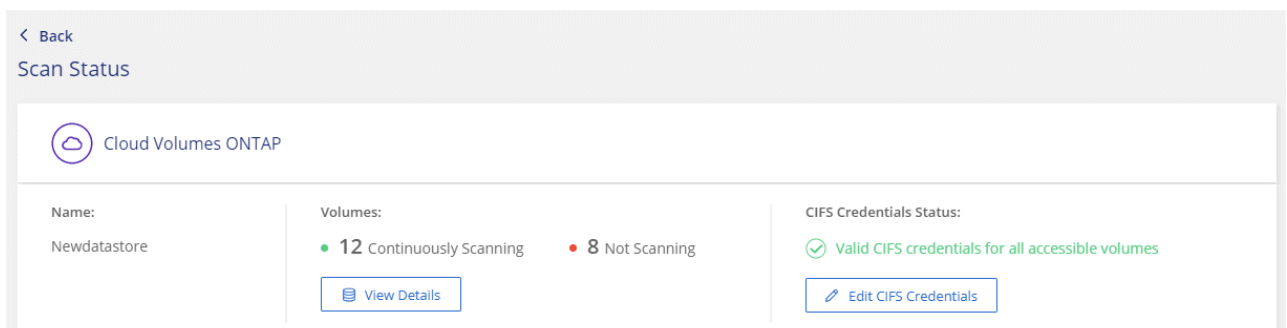
5. On the **Scan Configuration** page, click **View Details** to review the status for each CIFS and NFS volume and correct any errors.

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.

Back

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...

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.

Pricing

You need to pay to scan your Amazon S3 buckets. Learn about pricing.

A 30-day free trial is available to scan Amazon S3 data with Cloud Compliance. A subscription to the AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends. Learn how to subscribe.

Quick start

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

① Deploy Cloud Manager in AWS

If you haven't already done so, log in to Cloud Central and deploy Cloud Manager in AWS.

Cloud Manager automatically discovers the S3 buckets in this AWS account and displays them in an Amazon S3 working environment.

② Set up your cloud environment

Ensure that your cloud environment can meet the requirements for Cloud Compliance, which includes preparing an IAM role, setting up connectivity from Cloud Compliance to S3, and more. See the complete list.

3 **Subscribe from the AWS Marketplace**

A subscription to the AWS Marketplace is required to scan Amazon S3 after the 30-day free trial ends.

Click **Settings** > **Credentials** and click **Add Subscription** for the Instance Profile.

4 **Enable Cloud Compliance**

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

5 **Configure buckets**

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

Reviewing prerequisites

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

Requirements specific to S3

The first two 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.

General requirements

The requirements in this section apply to Cloud Compliance in general, whether you're scanning Amazon S3, Cloud Volumes ONTAP, or Azure NetApp Files. If you've already enabled Cloud Compliance (for Cloud Volumes ONTAP or Azure NetApp Files), then you can skip these requirements and Subscribe from the AWS Marketplace.

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 DSv3 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.

  > **ℹ** 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.

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.

Subscribing from the AWS Marketplace

A 30-day free trial is available to scan Amazon S3 data with Cloud Compliance. A subscription to the

AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends.

These steps must be completed by a user who has the *Account Admin* role.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Find the credentials for the AWS Instance Profile.

    The subscription must be added to the Instance Profile. Charging won't work otherwise.

    If you already have a subscription, then you're all set—there's nothing else that you need to do.
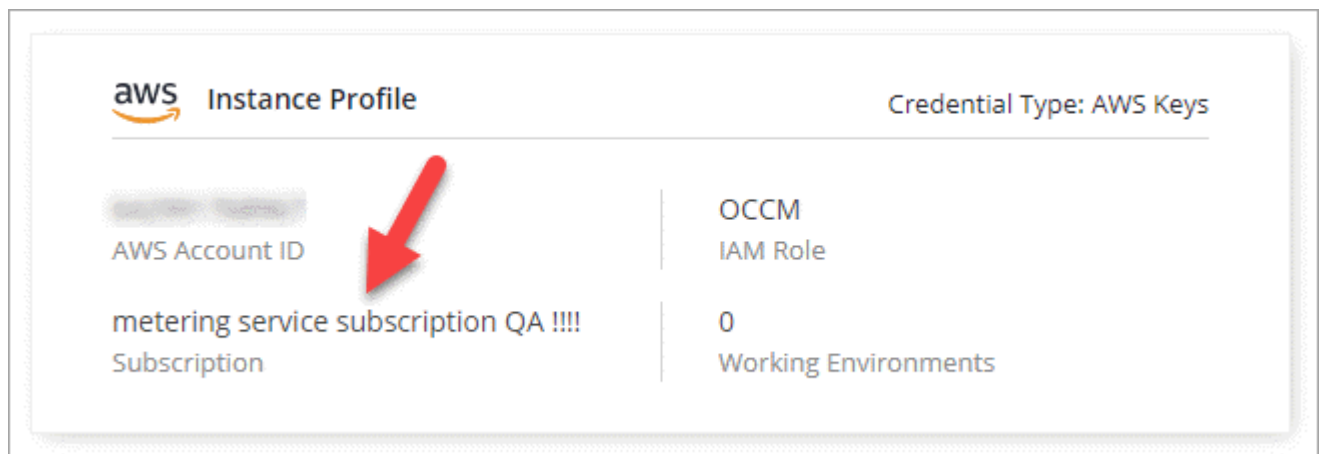
3. If you don't have a subscription yet, hover over the credentials and click the action menu.

4. Click **Add Subscription**.
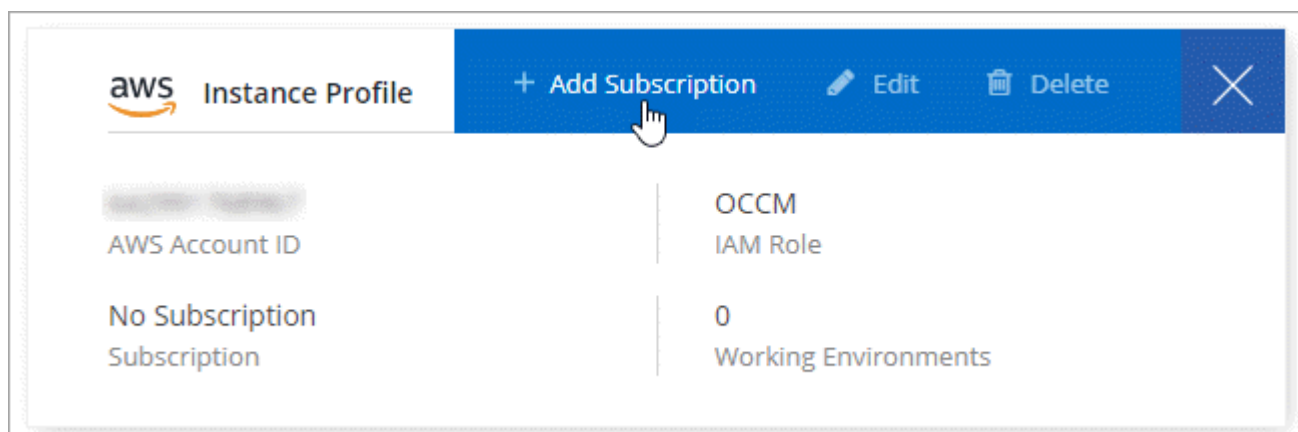
5. Click **Add Subscription**, click **Continue**, and follow the steps.

    ▶ https://docs.netapp.com/us-en/occm/media/video_subscribing_aws.mp4 *(video)*

Enabling Cloud Compliance

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

Steps

1. At the top of Cloud Manager, click **Working Environments**.

2. Select the Amazon S3 working environment.
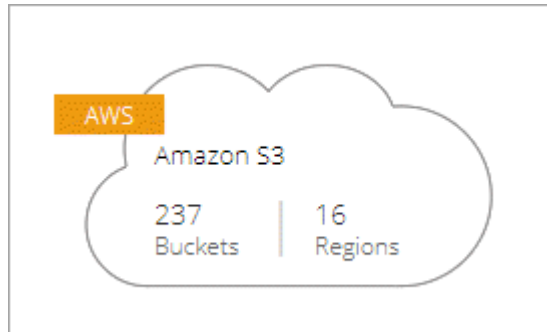
3. In the pane on the right, click **Enable Compliance**.
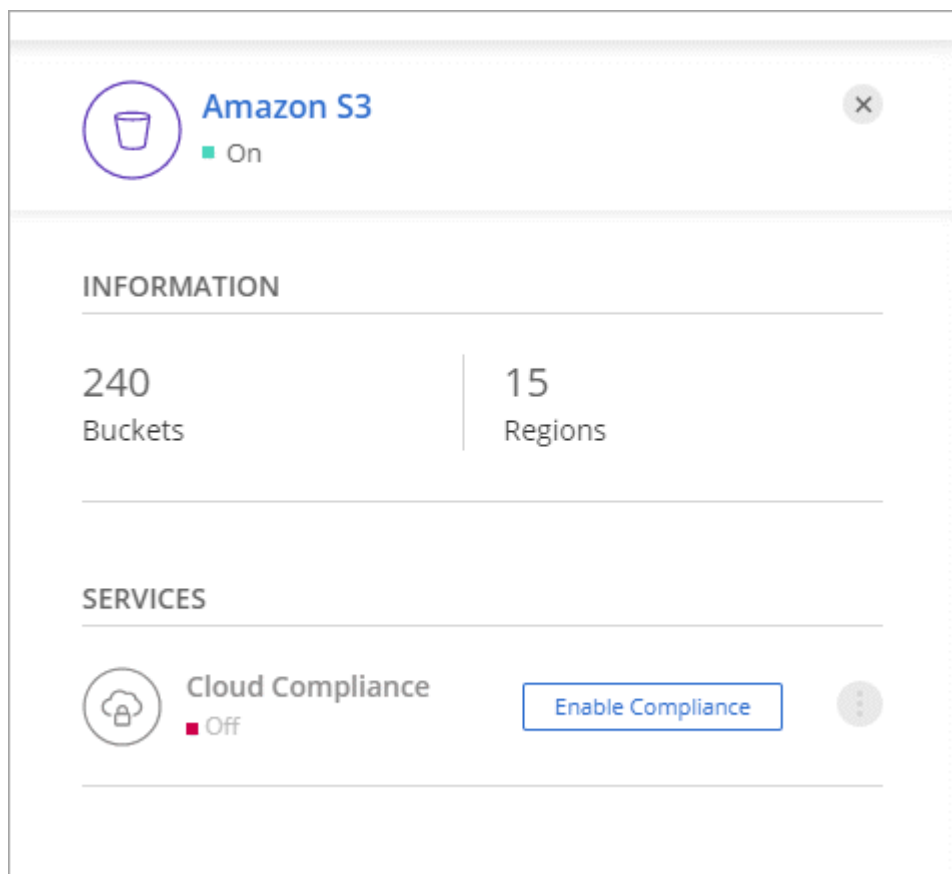
4. When prompted, assign an IAM role to the Cloud Compliance instance that has the required permissions.

5. Click **Enable Compliance**.

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

Result

If the Cloud Compliance instance hasn't been deployed yet, Cloud Manager deploys it. If it has been deployed, Cloud Manager assigns the IAM role to the instance.

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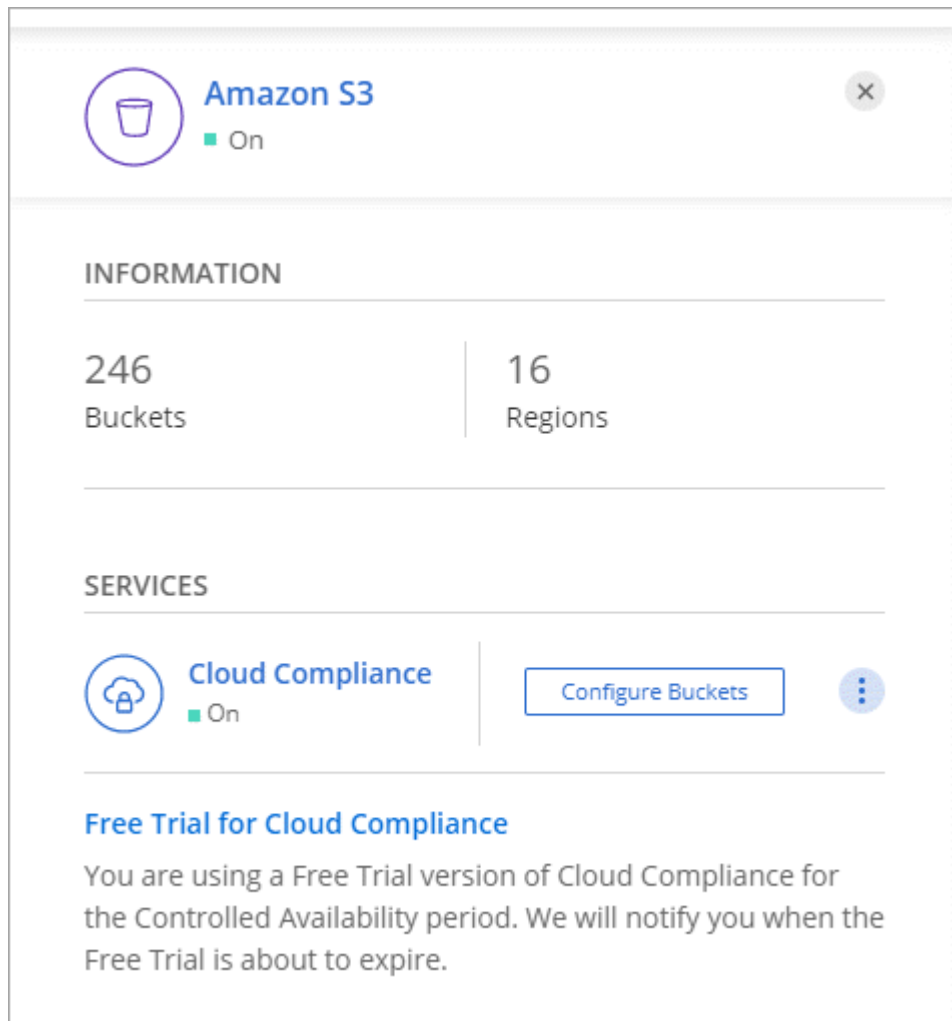
3. Enable compliance on the buckets that you want to scan.
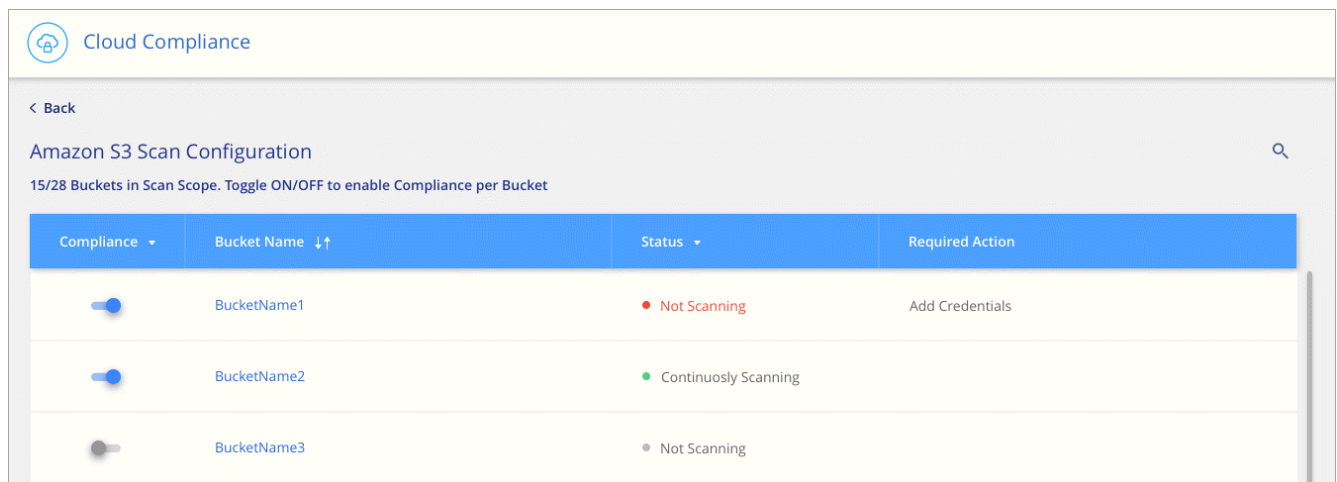
Result

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**.

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": "*"
        },
    ]
}
```

2. Go to the source AWS account where the Cloud Compliance instance resides and select the IAM role that is attached to the instance.

   a. Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.

   b. Click **Attach policies** and then click **Create policy**.

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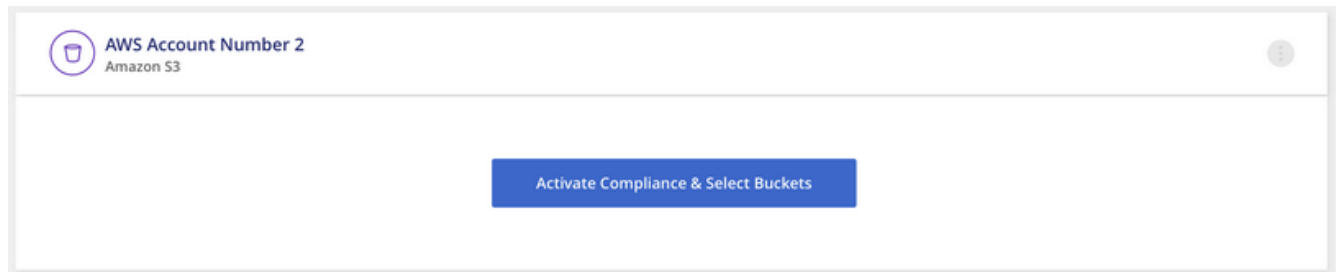
4. Click **Activate Compliance & Select Buckets** and select the buckets you want to scan.

Result

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

Scanning on-premises ONTAP data with Cloud Compliance 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. Scanning the data directly from an on-premises ONTAP working environment isn't supported.

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 the ONTAP CLI, configure the destination volume for data access.

   a. Mount destination volumes to the NAS namespace.

   b. If you're using CIFS:

      ▪ Create a CIFS share on the destination volume.

      ▪ Apply the appropriate ACLs to the CIFS share at the destination volume.

   c. If you're using NFS:

      ▪ Assign NFS export policies to the destination volume.

3. From Cloud Manager, activate Cloud Compliance on the Cloud Volumes ONTAP working environment that contains the SnapMirror data.

   a. Click **Working Environments**.

   b. Select the working environment that contains the SnapMirror data.

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

      Click here if you need help with enabling Cloud Compliance on a Cloud Volumes ONTAP system.