Deploy Cloud Compliance

Cloud Manager

Tom Onacki
October 09, 2020

Table of Contents

Deploy Cloud Compliance . . . 1
- Quick start . . . 1
- Creating a Connector . . . 1
- Reviewing prerequisites . . . 2
- Deploying the Cloud Compliance instance . . . 3
- Subscribing to the Cloud Compliance service . . . 5
- Changing to the new Cloud Manager plan in Azure . . . 6

Deploy Cloud Compliance

Complete a few steps to deploy the Cloud Compliance instance in your Cloud Manager workspace.

Quick start

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

 **Create a Connector**

If you don't already have a Connector, create a Connector in Azure or AWS. See creating a Connector in AWS or creating a Connector in Azure.

 **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 the Connector and Cloud Compliance over port 80, and more. See the complete list.

 **Deploy Cloud Compliance**

Launch the installation wizard to deploy the Cloud Compliance instance in Cloud Manager.

 **Subscribe to the Cloud Compliance service**

The first 1 TB of data that Cloud Compliance scans in Cloud Manager is free. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point.

Creating a Connector

If you don't already have a Connector, create a Connector in Azure or AWS. See creating a Connector in AWS or creating a Connector in Azure. In most cases you will probably have a Connector set up before you attempt to activate Cloud Compliance because most Cloud Manager features require a Connector, but there are cases when you need to set one up now.

There are some scenarios where you have to use a Connector in AWS or Azure for Cloud Compliance.

- When scanning data in Cloud Volumes ONTAP in AWS or in AWS S3 buckets, you use a connector in AWS.

- When scanning data in Cloud Volumes ONTAP in Azure or in Azure NetApp Files, you use a connector in Azure.
- Databases can be scanned using either Connector.

As you can see, there may be some situations where you need to use multiple Connectors.

If you are planning on scanning Azure NetApp Files, you need to make sure you're deploying in the same region as the volumes you wish to scan.

Reviewing prerequisites

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

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 the Connector.

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 the Connector and the Cloud Compliance instance. The security group for the Connector 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.

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.

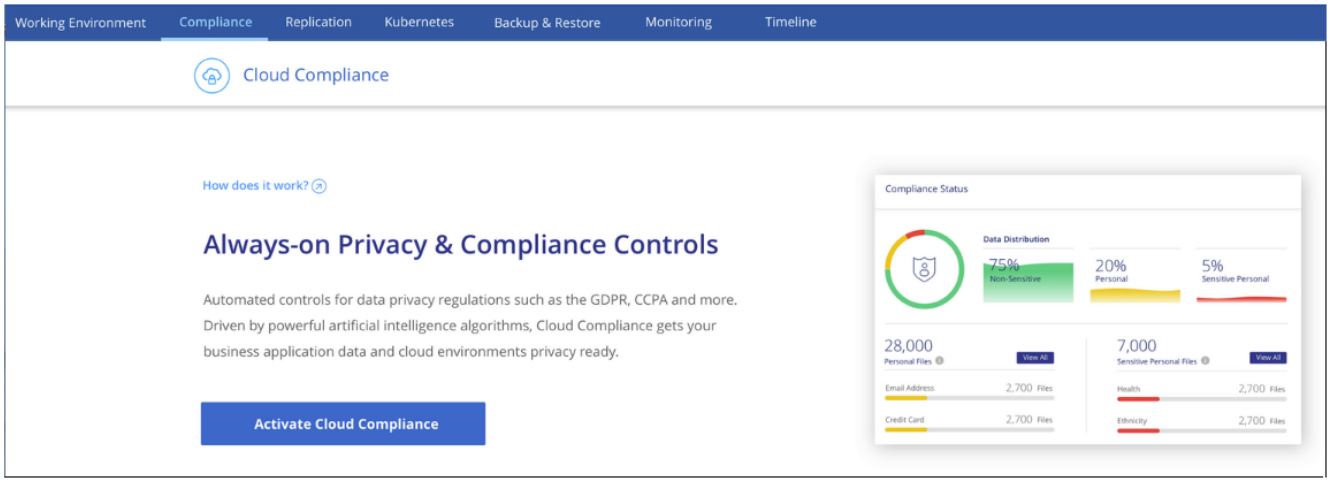
The Cloud Compliance instance uses a private IP address to ensure that the indexed data isn't accessible to the internet. As a result, the web browser that you use to access Cloud Manager must have a connection to that private IP address. That connection can come from a direct connection to AWS or Azure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

Deploying the Cloud Compliance instance

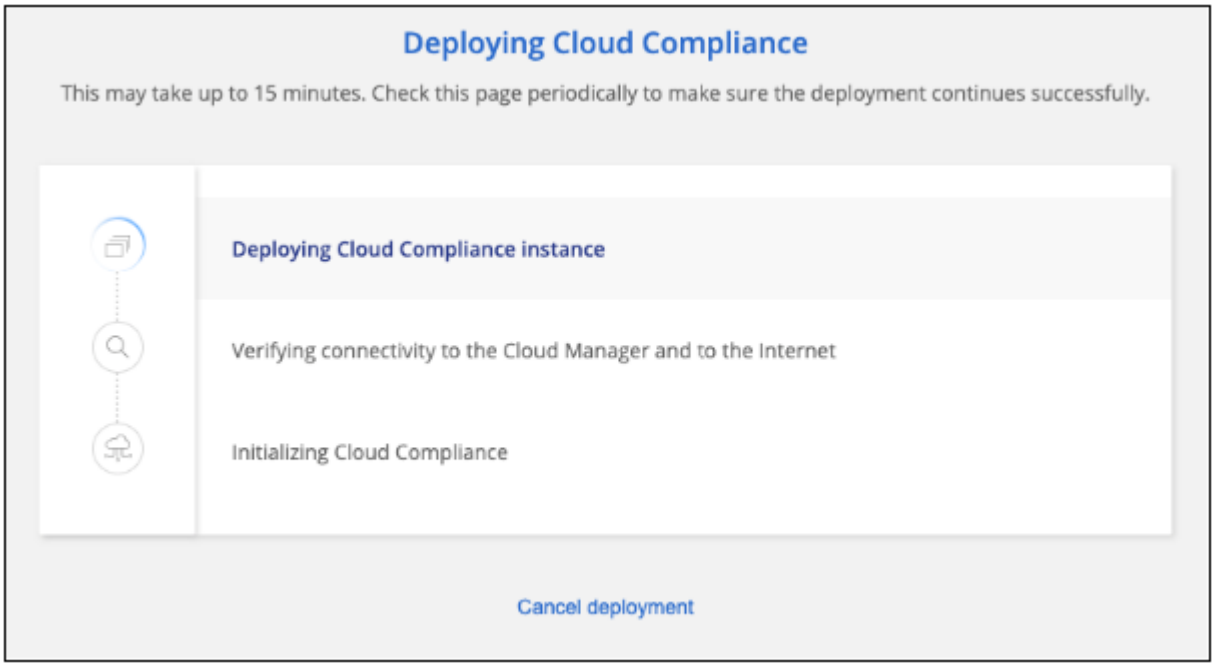
You deploy an instance of Cloud Compliance for each Cloud Manager instance.

Steps

1. In Cloud Manager, click **Cloud Compliance**.
2. Click **Activate Cloud Compliance** to start the deployment wizard.



3. The wizard displays progress as it goes through the deployment steps. It will stop and ask for input if it runs into any issues.



4. When the instance is deployed, click **Continue to configuration** to go to the *Scan Configuration* page.

Result

Cloud Manager deploys the Cloud Compliance instance in your cloud provider.

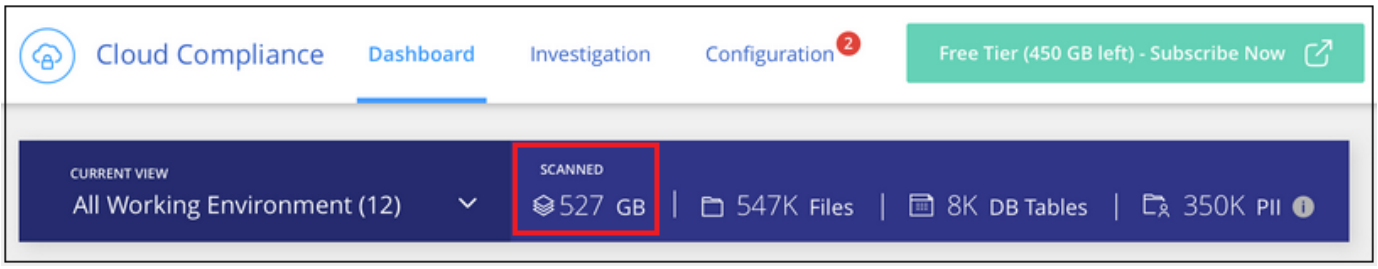
What's Next

From the Scan Configuration page you can select the working environments, volumes, and buckets that you want to scan for compliance. You can also connect to a database server in order to scan specific database schemas. Activate Cloud Compliance on any of these data sources.

Subscribing to the Cloud Compliance service

The first 1 TB of data that Cloud Compliance scans in a Cloud Manager workspace is free. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point.

You can subscribe at any time and you will not be charged until the amount of data exceeds 1 TB. You can always see the total amount of data that is being scanned from the Cloud Compliance Dashboard. And the *Subscribe Now* button makes it easy to subscribe when you are ready.



Note: If you are prompted by Cloud Compliance to subscribe, but you already have an Azure subscription, you're probably using the old **Cloud Manager** subscription and you need to change to the new **NetApp Cloud Manager** subscription. See
Changing to the new NetApp Cloud Manager plan in Azure for details.

Steps

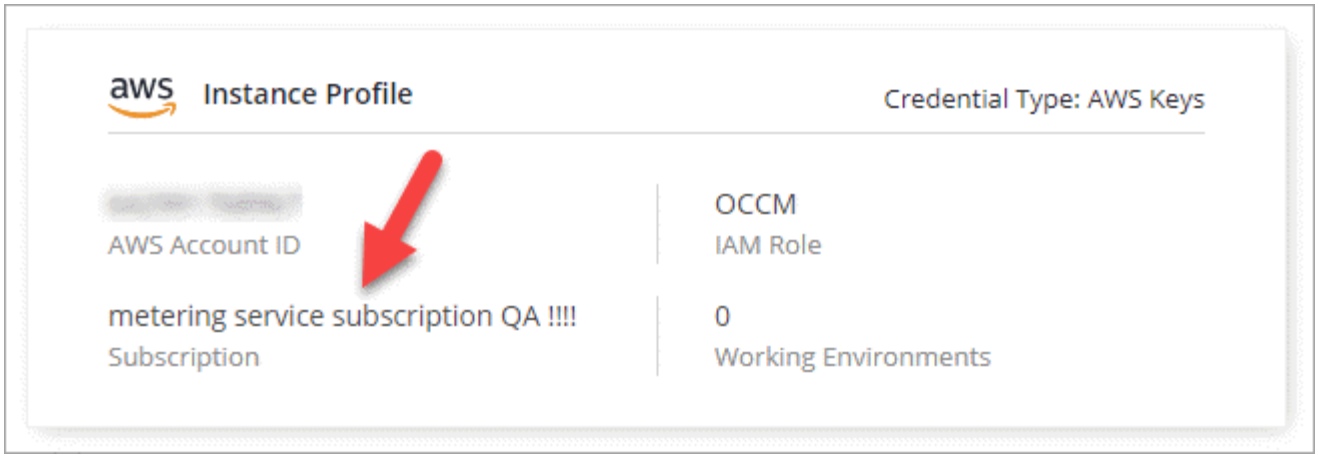
These steps must be completed by a user who has the *Account Admin* role.

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

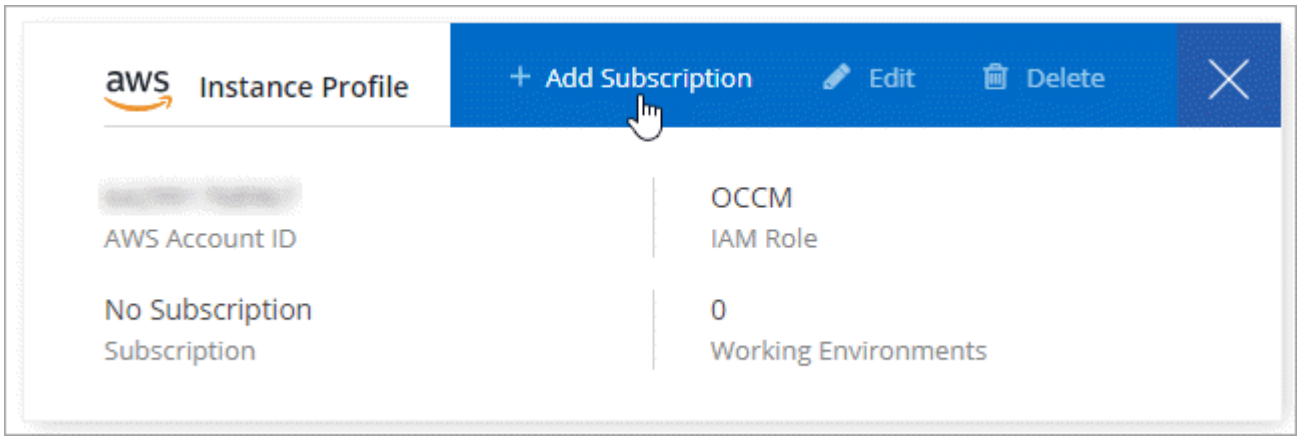
2. Find the credentials for the AWS Instance Profile or Azure Managed Service Identity.

   The subscription must be added to the Instance Profile or Managed Service Identity. 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.

   The following video shows how to associate a Marketplace subscription to an AWS subscription:

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

   The following video shows how to associate a Marketplace subscription to an Azure subscription:

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

Changing to the new Cloud Manager plan in Azure

Cloud Compliance was added to the Azure Marketplace subscription named **NetApp Cloud Manager** as of October 7, 2020. If you already have the original Azure **Cloud Manager** subscription it will not allow you to use Cloud Compliance.

You need to follow these steps and select the new **NetApp Cloud Manager** subscription and then remove the old **Cloud Manager** subscription.

If your existing Subscription was issued with a special private offer, you need to contact NetApp so that we can issue a new special private offer with Compliance included.

Steps

These steps are similar to adding a new subscription as described above, but vary in a few places.

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Find the credentials for the Azure Managed Service Identity that you want to change the subscription for and hover over the credentials and click **Associate Subscription**.

   The details for your current Marketplace Subscription are displayed.

3. Click **Add Subscription**, click **Continue**, and follow the steps. You are redirected to Azure portal in order to create the new subscription.
4. Make sure you select the plan **NetApp Cloud Manager** that provides access to Cloud Compliance and not **Cloud Manager**.
5. Go through the steps in the video to associate a Marketplace subscription to an Azure subscription:

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

6. Return to Cloud Manager, select the new subscription, and click **Associate**.
7. To verify your subscription has changed, hover over the “i” above subscription in the Credentials card.

   Now you can unsubscribe your old subscription from the Azure portal.

8. In the Azure portal, go to Software as a Service (SaaS), select the subscription, and click **Unsubscribe**.