Deploy Cloud Compliance

Cloud Manager

Tom Onacki
February 04, 2021

Table of Contents

Deploy Cloud Compliance

Complete a few steps to deploy the Cloud Compliance instance in your Cloud Manager workspace. You can deploy Cloud Compliance in the cloud or on an on-premises system.

The on-prem installation may be a good option if you prefer to scan on-premises ONTAP working environments using a Compliance instance that is also located on premises. But this this not a requirement. The Compliance software functions exactly the same way regardless of which installation method you choose.

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.

You can also deploy the Connector on-premises on an existing Linux host in your network or in the cloud.

Review prerequisites

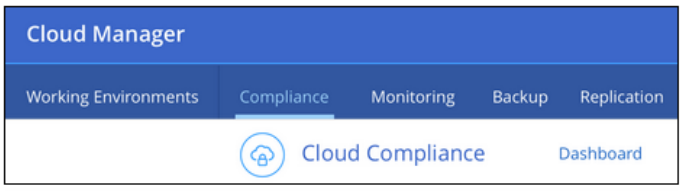
Ensure that your environment can meet the prerequisites. This includes outbound internet access for the instance, connectivity between the Connector and Cloud Compliance over port 80, and more. See the complete list.

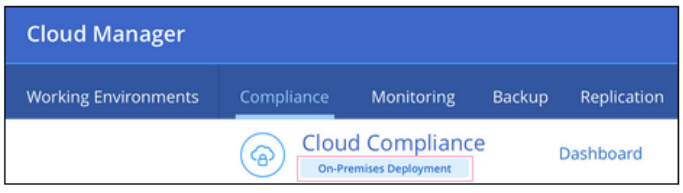
- When installed in the cloud, you need 16 vCPUs for the Cloud Compliance instance. See more details about the instance type.
- When installed on premises, you need a Linux system that meets the following requirements.

Deploy Cloud Compliance

Launch the installation wizard to deploy the Cloud Compliance instance.

You can deploy Cloud Compliance in the cloud or in an on-premises location. The only difference you'll notice in the UI is the words "On-Premises Deployment".





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, OneDrive folders, and on-prem ONTAP systems can be scanned using either Connector.

Note that you can also deploy the Connector on-premises on an existing Linux host in your network or in the cloud. Some users planning to install Cloud Compliance on-prem may also choose to install the Connector on-prem.

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 from Cloud Compliance

Cloud Compliance requires outbound internet access. If your virtual or physical network uses a proxy server for internet access, ensure that the Cloud Compliance instance has outbound internet access to contact the following endpoints. When you deploy Cloud Compliance in the cloud, it is located in the same subnet as the Connector.

Review the appropriate table below depending on whether you are deploying Cloud Compliance in AWS, Azure, or on-premises.

Required endpoints for AWS deployments:

Endpoints	Purpose
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.

Endpoints	Purpose
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 https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.

Required endpoints for Azure and On-Prem deployments:

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://support.compliance.cloudmanager.cloud.netapp.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://support.compliance.cloudmanager.cloud.netapp.com/	Enables NetApp to stream data from audit records.
https://support.compliance.cloudmanager.cloud.netapp.com/	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.

Endpoints	Purpose
On-premises installs only: https://github.com/docker https://download.docker.com https://rhui3.us-west-2.aws.ce.redhat.com https://github-production-release-asset-2e65be.s3.amazonaws.com https://pypi.org https://pypi.python.org https://files.pythonhosted.org http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Provides prerequisite packages for installation.

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

When installed in the cloud, 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.

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.

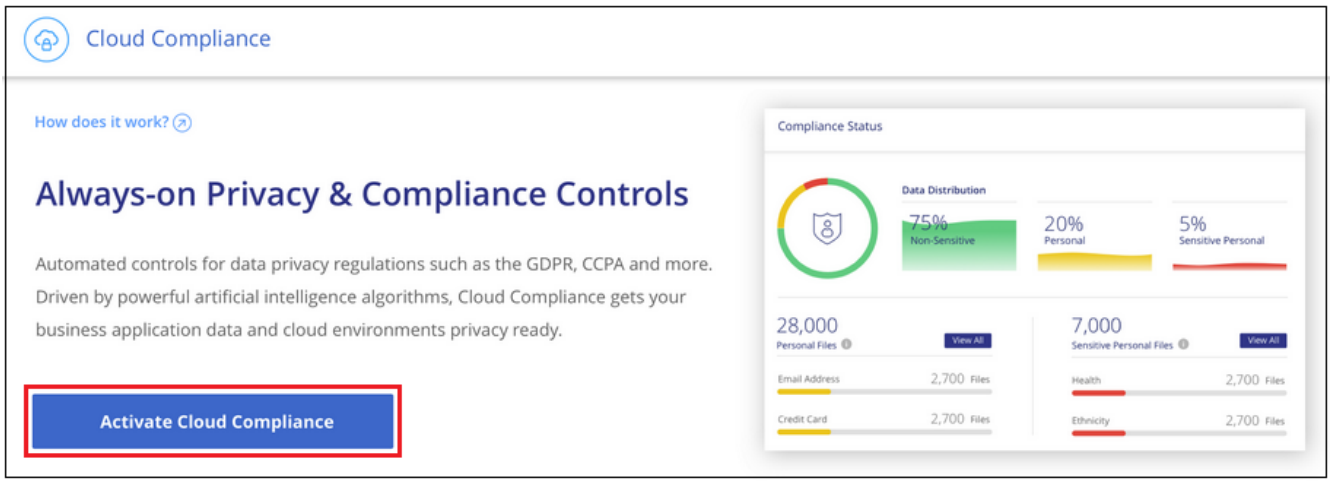
Deploying the Cloud Compliance instance in the cloud

Deploying an instance of Cloud Compliance in the cloud is the most common deployment model. But you have the option to deploy the Compliance software on a Linux host in your network or in the cloud.

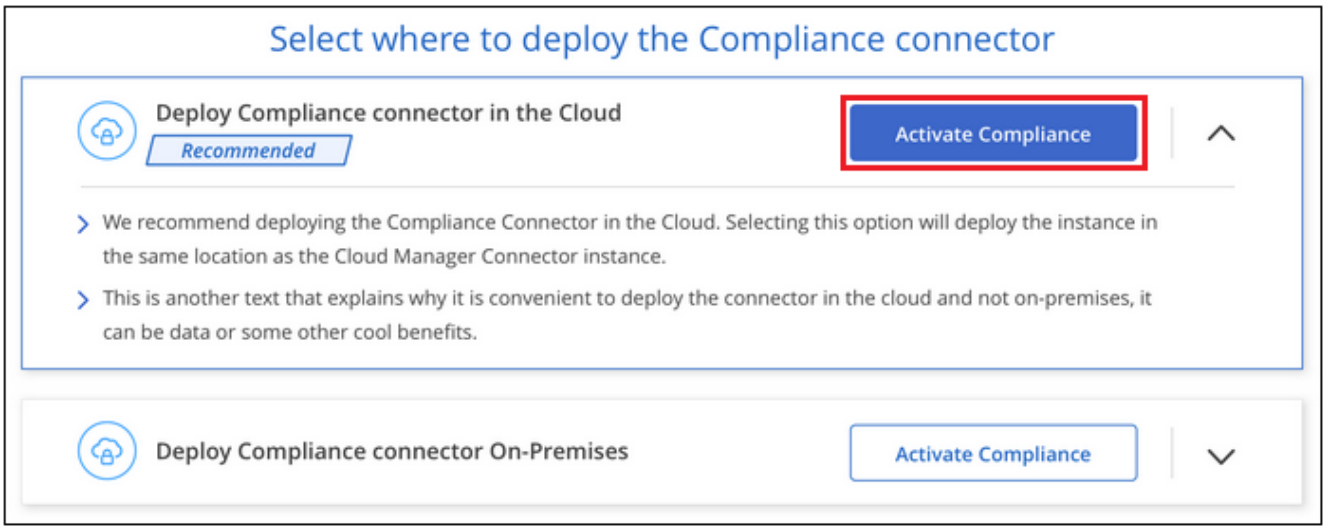
The Compliance software functions exactly the same way regardless of which installation method you choose.

Steps

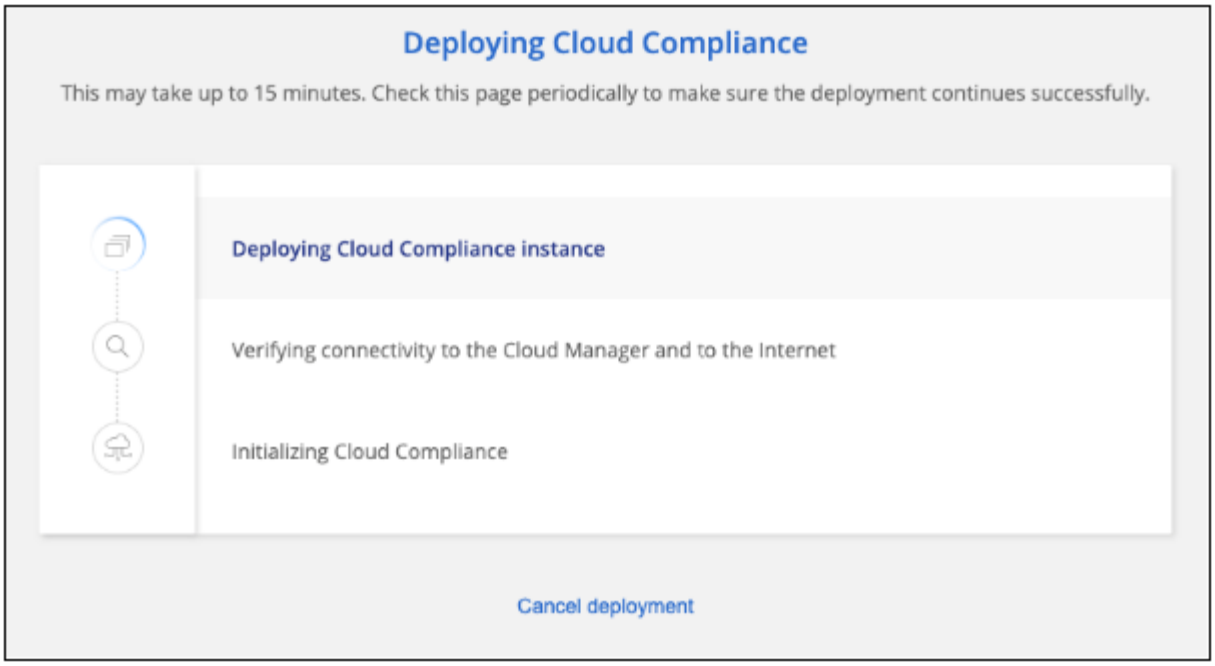
1. In Cloud Manager, click **Compliance**.
2. Click **Activate Cloud Compliance**.



3. Click **Activate Compliance** to start the deployment wizard.



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



5. 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 data sources that you want to scan.

You can also subscribe to the Cloud Compliance service at this time. You will not be charged until the amount of data exceeds 1 TB.

Deploying the Cloud Compliance instance on premises

The most common way to deploy Cloud Compliance is to deploy it in the cloud. But you have the option to download and install the Compliance software on a Linux host in your network.

The Compliance software functions exactly the same regardless of which installation method you choose.

Cloud Compliance is currently unable to scan S3 buckets and Azure NetApp Files when the Compliance instance is installed on premises. In these cases you'll need to deploy a separate Connector and instance of Compliance in the cloud and switch between Connectors for your different data sources.

Host requirements

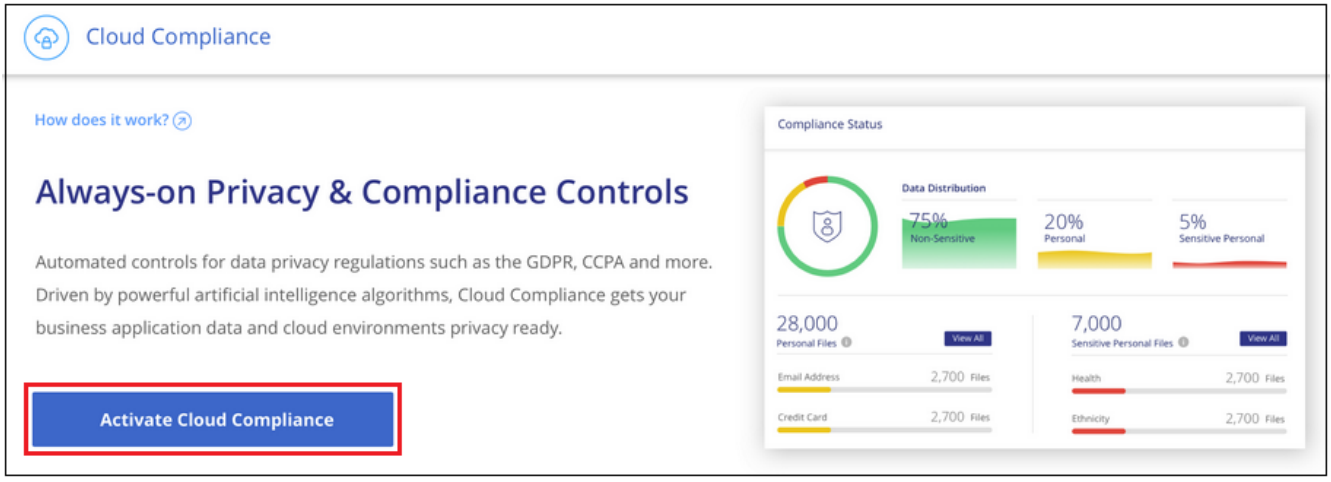
- Operating system: Red Hat Enterprise Linux or CentOS version 8.0 or 8.1
  - Version 7.8 can be used, but the Linux kernel version must be 4.14 or greater
  - The OS must be capable of installing the docker engine (for example, disable the *firewalld* service if needed)
- RAM: 64 GB (swap memory must be disabled on the host)
- CPU: 16 cores

- Disk: 500 GB SSD
- A Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during installation.
- Make sure port 8080 is open so you can see the installation progress in Cloud Manager.
- Root privileges are required to install Cloud Compliance.

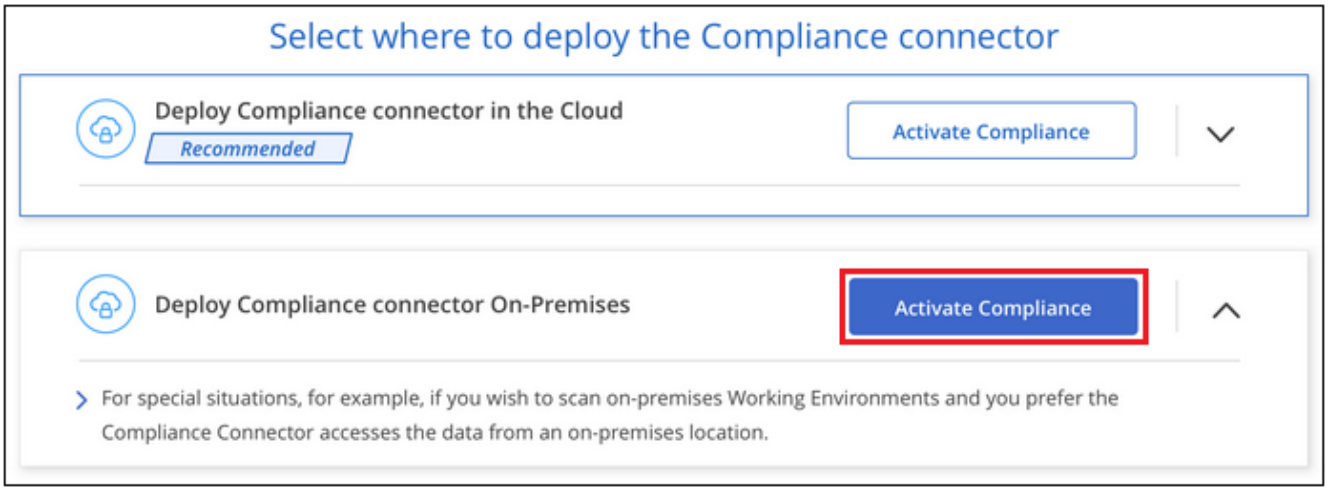
See Reviewing prerequisites for the full list of requirements and endpoints that Cloud Compliance must be able to reach over the internet.

Steps

1. Download the Cloud Compliance software from the NetApp Support Site.
2. Copy the installer file to the Linux host you plan to use (using `scp` or some other method).
3. In Cloud Manager, click **Compliance**.
4. Click **Activate Cloud Compliance**.



5. Click **Activate Compliance**.



6. In the *Deploy Cloud Compliance On Premises* dialog, copy the provided command and paste it in a text file so you can use it later. For example:

   sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq

7. Unzip the installer file on the host machine:

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

8. When prompted by the installer, you can enter the required values in a series of prompts, or you can enter the complete command in the first prompt:

Enter parameters as prompted:	Enter the full command:
1. Paste the information you copied from step 6: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token>` 2. Enter the IP address or host name of the Compliance host machine so it can be accessed by the Connector instance. 3. Enter the IP address or host name of the Cloud Manager Connector host machine so it can be accessed by the Cloud Compliance instance. 4. Enter proxy details as prompted. If your Cloud Manager already uses a proxy, there is no need to enter this information again here since Cloud Compliance will automatically use the proxy used by Cloud Manager.	Alternatively, you can create the whole command in advance and enter it in the first prompt: `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <cc_host> --cm-host <cm_host> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy-user <proxy_user> --proxy-password <proxy_password>`

   Variable values:

   - *account_id* = NetApp Account ID
   - *agent_id* = Connector ID
   - *token* = jwt user token
   - *cc_host* = IP address or host name of the Cloud Compliance Linux system.
   - *cm_host* = IP address or host name of the Cloud Manager Connector system.
   - *proxy_host* = IP or host name of the proxy server if the host is behind a proxy server.
   - *proxy_port* = Port to connect to the proxy server (default 80).
   - *proxy_scheme* = The connection schema: https or http (default http).
   - *proxy_user* = Authenticated user to connect to the proxy server, if basic authentication is required.
   - *proxy_password* = Password for the user name that you specified.

Result

The Cloud Compliance installer installs packages, installs docker, registers the installation, and installs Cloud Compliance. Installation can take 10 to 20 minutes.

If there is connectivity over port 8080 between the host machine and the Connector instance, you will see the installation progress in the Compliance tab in Cloud Manager.

What's Next

From the Scan Configuration page you can select the data sources that you want to scan.

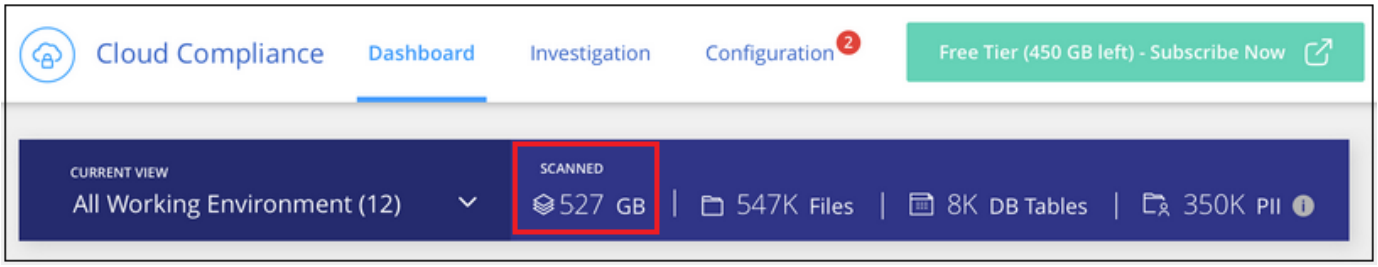
You can also subscribe to the Cloud Compliance service at this time. You will not be charged until the amount

of data exceeds 1 TB. A subscription to either the AWS or Azure Marketplace can be used when you have deployed Cloud Compliance on an on-premises system.

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

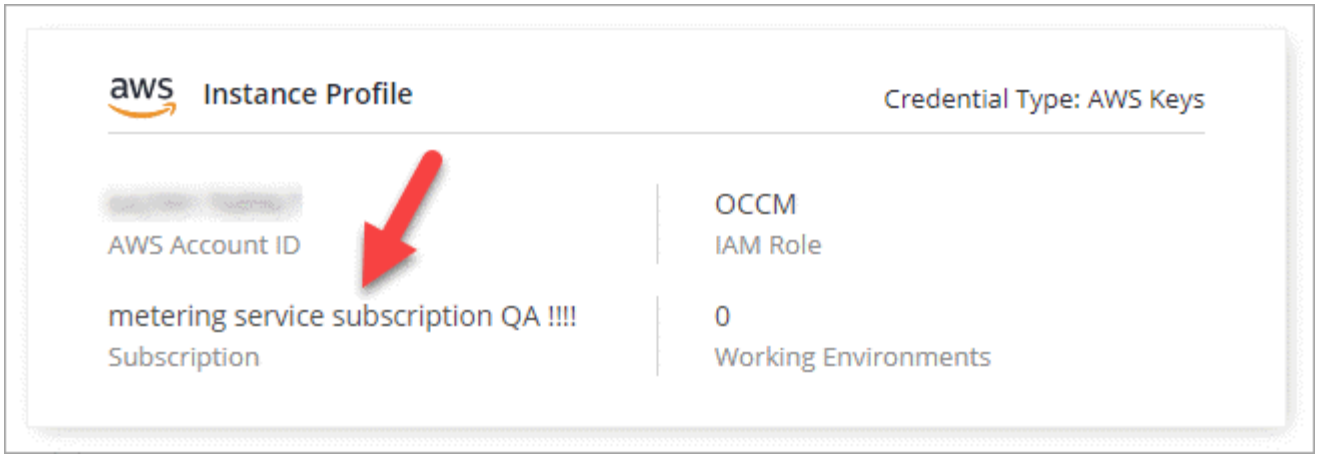
These steps must be completed by a user who has the *Account Admin* role.

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

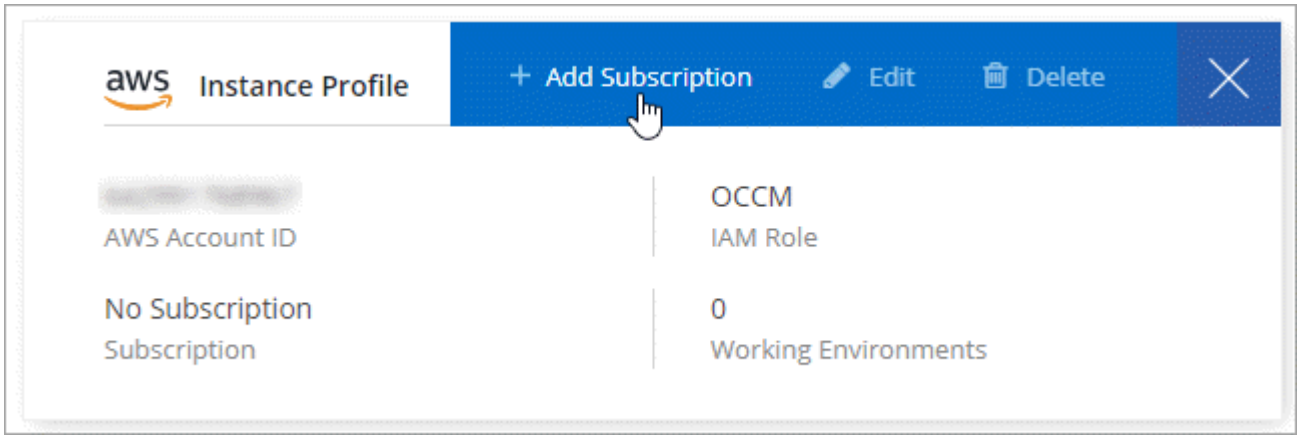
2. Find the credentials for the AWS Instance Profile or Azure Managed Service Identity.

   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 to change to the new **NetApp Cloud Manager** subscription before you can start using Cloud Compliance.

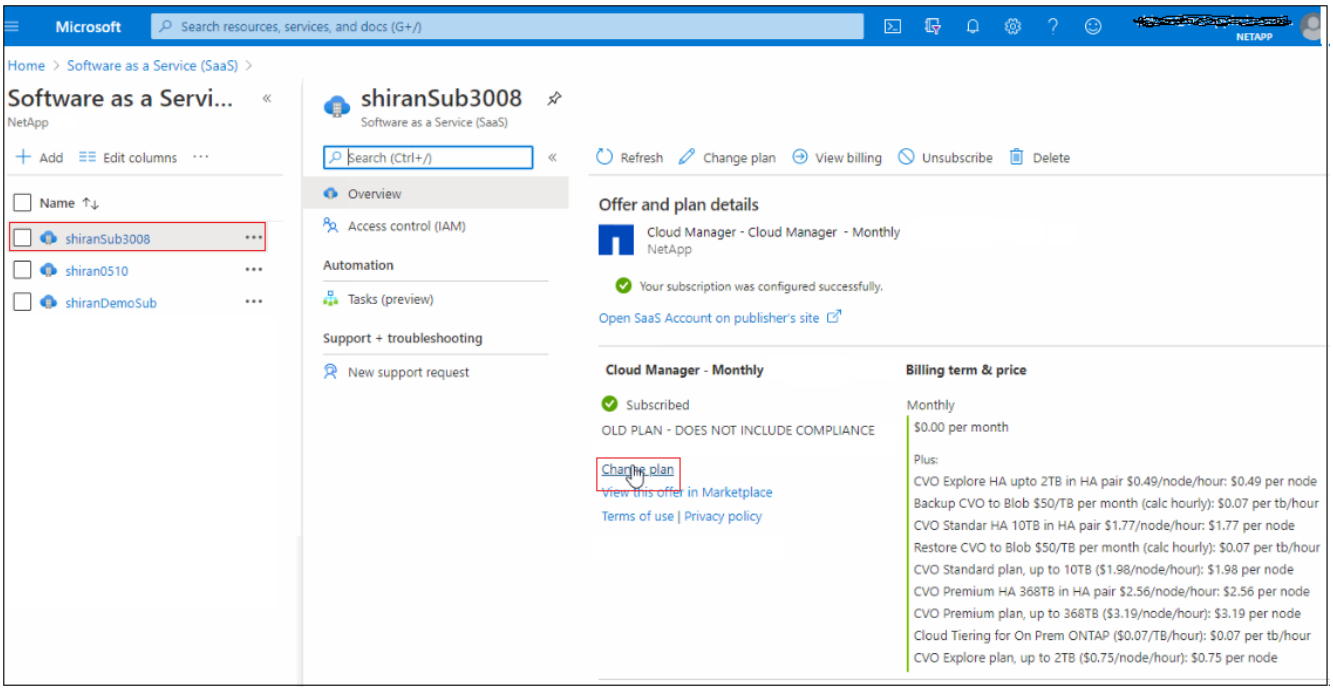
If your existing Subscription was issued with a special private offer, you need to contact NetApp so that we can issue a new special private offer with Compliance included.

Steps

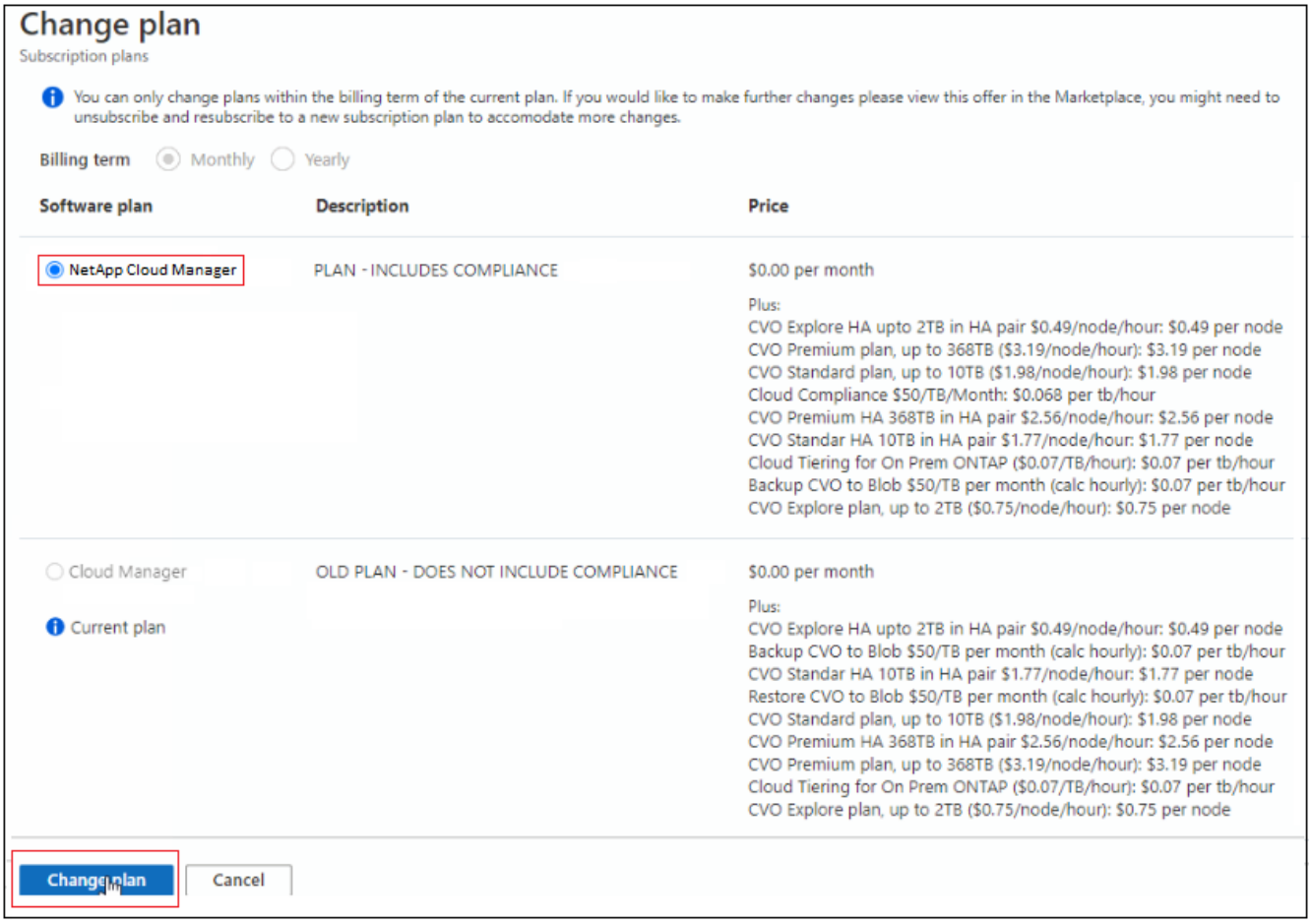
1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Find the credentials for the Azure Managed Service Identity that you want to change the subscription for and hover over the credentials and click **Associate Subscription**.

   The details for your current Marketplace Subscription are displayed.

3. Log in to the Azure portal and select **Software as a Service (SaaS)**.
4. Select the subscription for which you want to change the plan and click **Change Plan**.



5. In the Change Plan page, select the **NetApp Cloud Manager** plan and click the **Change Plan** button.



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