Learn about Cloud Compliance

Cloud Manager

Ben Cammett, Tom Onacki
June 05, 2020

Table of Contents

Learn about Cloud Compliance

Cloud Compliance is a data privacy and compliance service for Azure NetApp Files and Cloud Volumes ONTAP. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data.

Cloud Compliance is currently available as a Controlled Availability release.

Learn about the use cases for Cloud Compliance.

Features

Cloud Compliance provides several tools that can help you with your compliance efforts. You can use Cloud Compliance to:

- Identify Personal Identifiable Information (PII)
- Identify a wide scope of sensitive information as required by GDPR, CCPA, PCI, and HIPAA privacy regulations
- Respond to Data Subject Access Requests (DSAR)

Supported working environments

Cloud Compliance can scan data from the following types of working environments:

- Cloud Volumes ONTAP in AWS and Azure
- Amazon S3
- Azure NetApp Files

  For Azure NetApp Files, Cloud Compliance can scan volumes that are in the same region as Cloud Manager. When you activate compliance scans on an Azure NetApp Files working environment, Cloud Compliance scans *all* of the volumes in the region.

Cost

The cost to use Cloud Compliance depends on the type of working environment that you're scanning.

Cloud Volumes ONTAP and Azure NetApp Files

Cloud Compliance is an add-on service provided by NetApp at no extra cost. Activating Cloud Compliance requires deploying a cloud instance, which results in charges from your cloud provider.

Data transfer costs depend on your setup. If Cloud Compliance and Cloud Volumes ONTAP are in the same Availability Zone and region, then there are no data transfer costs. But if Cloud Volumes ONTAP is in a *different* Availability Zone or region, then you'll be charged by your cloud provider for data transfer costs. See these links for more details:

- AWS: Amazon EC2 Pricing
- Microsoft Azure: Bandwidth Pricing Details

Amazon S3

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.

How Cloud Compliance works

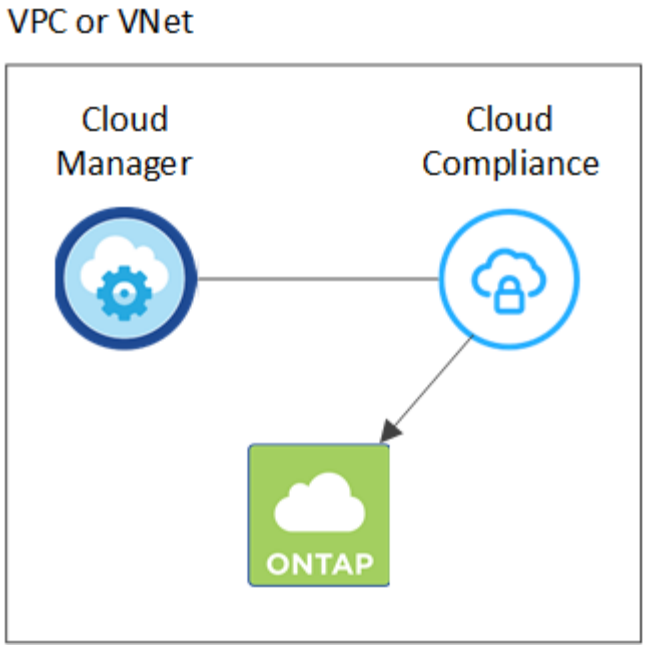
At a high-level, Cloud Compliance works like this:

1. You enable Cloud Compliance on one or more working environments.
2. Cloud Compliance scans the data using an AI learning process.
3. In Cloud Manager, you click **Compliance** and use the provided dashboard and reporting tools to help you in your compliance efforts.

The Cloud Compliance instance

When you enable Cloud Compliance, Cloud Manager deploys a Cloud Compliance instance in the same subnet as Cloud Manager.

If Cloud Manager is installed on-prem, it deploys the Cloud Compliance instance in same VPC or VNet as the first Cloud Volumes ONTAP system in the request.



Note the following about the instance:

- In Azure, Cloud Compliance runs on a Standard_D16s_v3 VM with a 512 GB disk.
- In AWS, Cloud Compliance runs on an m5.4xlarge instance with a 500 GB GP2 disk.

  In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.

  Changing or resizing the instance/VM type isn't supported. You need to use the default size that's provided.

- The instance is named *CloudCompliance* with a generated hash (UUID) concatenated to it. For example: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Only one Cloud Compliance instance is deployed per Cloud Manager system.
- Upgrades of Cloud Compliance software is automated—you don't need to worry about it.

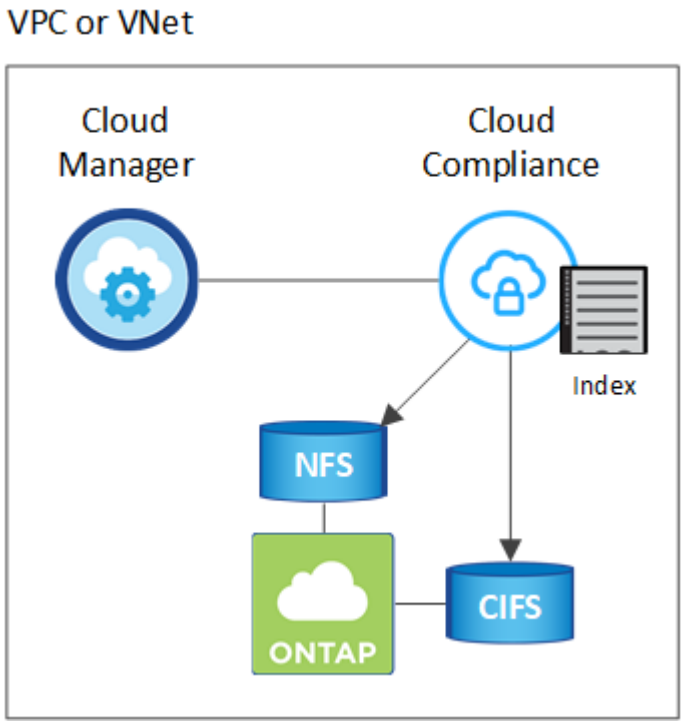
  The instance should remain running at all times because Cloud Compliance continuously scans the data on volumes.

How scans work

After you enable Cloud Compliance, it immediately starts scanning your data to identify personal and sensitive data.

Cloud Compliance connects to the data like any other client by mounting NFS and CIFS volumes. NFS volumes are automatically accessed as read-only, while you need to provide Active Directory credentials to scan CIFS volumes.

Cloud Compliance scans the unstructured data on each volume for a range of personal information. It maps your organizational data, categorizes each file, and identifies and extracts entities and predefined patterns in the data. The result of the scan is an index of personal information, sensitive personal information, and data categories.



After the initial scan, Cloud Compliance continuously scans each volume to detect incremental changes (this is why it's important to keep the instance running).

You can turn scans on and off at the working environment level, but not at the volume level. Learn how.

Information that Cloud Compliance indexes

Cloud Compliance collects, indexes, and assigns categories to unstructured data (files). The data that Cloud Compliance indexes includes the following:

Standard metadata

Cloud Compliance collects standard metadata about files: the file type, its size, creation and modification dates, and so on.

Personal data

Personally identifiable information such as email addresses, identification numbers, or credit card numbers. Learn more about personal data.

Sensitive personal data

Special types of sensitive information, such as health data, ethnic origin, or political opinions, as

defined by GDPR and other privacy regulations. Learn more about sensitive personal data.

Categories

Cloud Compliance takes the data that it scanned and divides it into different types of categories. Categories are topics based on AI analysis of the content and metadata of each file. Learn more about categories.

Name entity recognition

Cloud Compliance uses AI to extract natural persons' names from documents. Learn about responding to Data Subject Access Requests.

Networking overview

Cloud Manager deploys the Cloud Compliance instance with a private IP address and a security group that enables inbound HTTP connections from Cloud Manager. This connection enables you to access the Cloud Compliance dashboard from the Cloud Manager interface.

Outbound rules are completely open. The instance connects to the internet through a proxy from Cloud Manager. Internet access is needed to upgrade the Cloud Compliance software and to send usage metrics.

If you have strict networking requirements, learn about the endpoints that Cloud Compliance contacts.

The indexed data never leaves the Cloud Compliance instance—the data isn't relayed outside of your virtual network and it isn't sent to Cloud Manager.

User access to compliance information

Cloud Manager Admins can view compliance information for all working environments.

Workspace Admins can view compliance information only for systems that they have permissions to access. If a Workspace Admin can't access a working environment in Cloud Manager, then they can't see any compliance information for the working environment in the Compliance tab.

Learn more about Cloud Manager roles.