Learn about Cloud Compliance

Cloud Manager

Tom Onacki
February 16, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/concept_cloud_compliance.html on February 28, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Learn about Cloud Compliance

Cloud Compliance is a data privacy and compliance service for Cloud Manager that scans your volumes, Amazon S3 buckets, databases, and OneDrive accounts to identify the personal and sensitive data that resides in those files. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data.

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)
- Notify Cloud Manager users through email when files contain certain PII (you define this criteria using highlights)
- View and modify Azure Information Protection (AIP) labels in your files
- Delete individual files

Supported working environments and data sources

Cloud Compliance can scan data from the following types of data sources:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure
- On-premises ONTAP clusters
- Azure NetApp Files
- Amazon S3
- Databases that reside anywhere (there is no requirement that the database resides in a working environment)
- OneDrive accounts

A Beta feature released in January 2021 allows you to run Compliance scans for free on the backup files created from your on-prem ONTAP volumes (created using Cloud Backup). This gives you a choice whether you want to have Cloud Compliance scan your on-prem ONTAP volumes directly, or scan the backup files made from those volumes.

Cost

- The cost to use Cloud Compliance depends on the amount of data that you're scanning. The first 1 TB of

data that Cloud Compliance scans in a Cloud Manager workspace is free. This includes all data from all working environments and data sources. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point. See pricing for details.

Learn how to subscribe.

Note: This subscription is not needed to scan backup files created from your on-prem ONTAP systems.

- Installing Cloud Compliance in the cloud requires deploying a cloud instance, which results in charges from the cloud provider where it is deployed. See the the type of instance that is deployed for each cloud provider. There is no cost if you install Cloud Compliance on an on-premises system.
- Cloud Compliance requires that you have deployed a Connector. In many cases you already have a Connector because of other storage and services you are using in Cloud Manager. The Connector instance results in charges from the cloud provider where it is deployed. See the type of instance that is deployed for each cloud provider.

Data transfer costs

Data transfer costs depend on your setup. If the Cloud Compliance instance and data source are in the same Availability Zone and region, then there are no data transfer costs. But if the data source, such as a Cloud Volumes ONTAP cluster or S3 Bucket, 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

How Cloud Compliance works

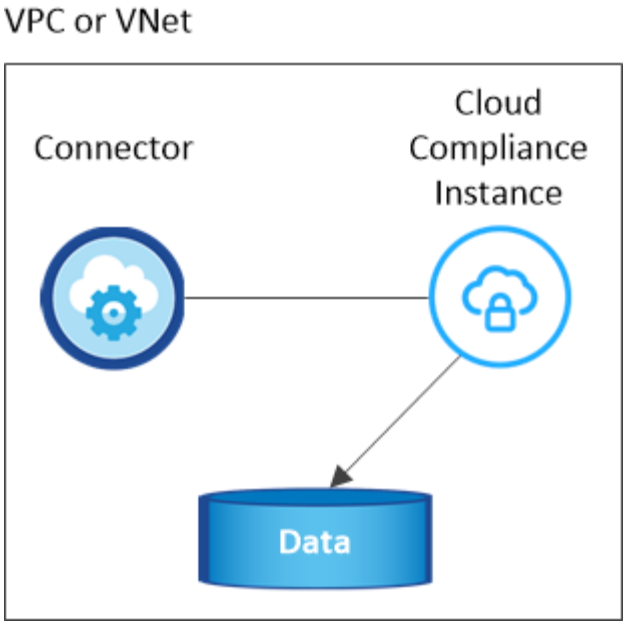
At a high-level, Cloud Compliance works like this:

1. You deploy an instance of Cloud Compliance in Cloud Manager.
2. You enable it on one or more working environments, databases, or OneDrive accounts.
3. Cloud Compliance scans the data using an AI learning process.
4. You click **Compliance** and use the provided dashboard and reporting tools to help in your compliance efforts.

The Cloud Compliance instance

When you deploy Cloud Compliance in the cloud, Cloud Manager deploys the instance in the same subnet as the Connector. Learn more about Connectors.

If the Connector 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 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 Connector.
- 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.

How scans work

After you enable Cloud Compliance and select the volumes, buckets, database schemas, or OneDrive users you want to scan, it immediately starts scanning the data to identify personal and sensitive data. 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, data categories, and file types.

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.

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

You can enable and disable scans at the volume level, at the bucket level, the database schema level, and at the OneDrive user level.

Information that Cloud Compliance indexes

Cloud Compliance collects, indexes, and assigns categories to your 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.

Types

Cloud Compliance takes the data that it scanned and breaks it down by file type. Learn more about types.

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 security group that enables inbound HTTP connections from the Connector instance.

When using Cloud Manager in SaaS mode, the connection to Cloud Manager is served over HTTPS, and the private data sent between your browser and the Cloud Compliance instance are secured with end-to-end encryption, which means NetApp and third parties can't read it.

If you need to use the local user interface instead of the SaaS user interface for any reason, you can still access the local UI.

Outbound rules are completely open. Internet access is needed to install and upgrade the Cloud Compliance software and to send usage metrics.

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

User access to compliance information

The role each user has been assigned provides different capabilities within Cloud Manager and within Cloud Compliance:

- **Account Admins** can manage compliance settings and view compliance information for all working environments.
- **Workspace Admins** can manage compliance settings and 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.
- Users with the **Cloud Compliance Viewer** role can only view compliance information and generate reports for systems that they have permission to access. These users cannot enable/disable scanning of volumes, buckets, or database schemas.

Learn more about Cloud Manager roles and how to add users with specific roles.

Copyright Information

Copyright © 2021 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.