



Backing up on-premises ONTAP data to Azure Blob storage

Cloud Manager

Tom Onacki
September 08, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/task_backup_onprem_to_azure.html on September 09, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Backing up on-premises ONTAP data to Azure Blob storage 1
 - Quick start 1
 - Requirements 3
 - Enabling Cloud Backup 6

Backing up on-premises ONTAP data to Azure Blob storage

Complete a few steps to get started backing up data from your on-premises ONTAP systems to Azure Blob storage.

TIP

In most cases you'll use Cloud Manager for all backup and restore operations. However, starting with ONTAP 9.9.1 you can initiate volume backup operations of your on-premises ONTAP clusters using ONTAP System Manager. [See how to use System Manager to back up your volumes to the cloud using Cloud Backup.](#)

A Beta feature released in January 2021 allows you to run compliance scans on the backed up volumes from your on-premises systems. Typically, compliance scans are free up to 1 TB of data, and then a cost for the service is applied for data over 1 TB. When combining Backup and Data Sense for your on-premises volumes, the cost for scans on those on-prem volumes is free. Learn more about how [Cloud Data Sense](#) can get your business applications and cloud environments privacy ready.

Quick start

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



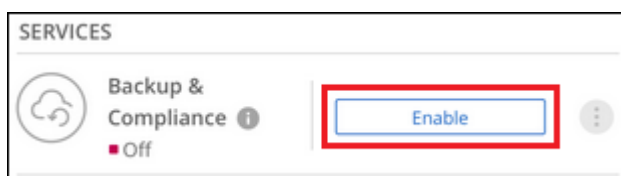
Verify support for your configuration

- You have discovered the on-premises cluster and added it to a working environment in Cloud Manager. See [Discovering ONTAP clusters](#) for details.
 - The cluster is running ONTAP 9.7P5 or later.
 - The cluster has a SnapMirror license — it is included as part of the Premium Bundle or Data Protection Bundle.
- The cluster must have the required network connections to Blob storage and to the Connector.
- The Connector must have the required network connections to Blob storage and to the cluster, and the required permissions.
- You have a valid Azure subscription for the object storage space where your backups will be located.



Enable Cloud Backup on the system

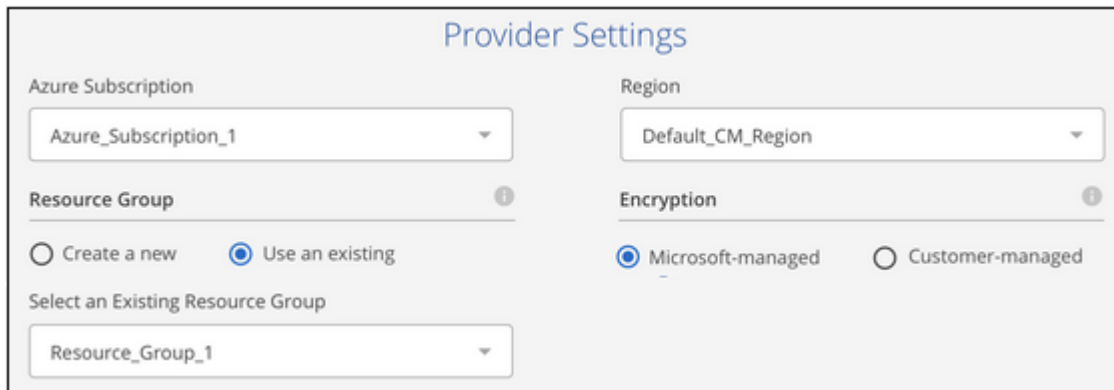
Select the working environment and click **Enable** next to the Backup & Compliance service in the right-panel, and then follow the setup wizard.



3

Select the cloud provider and enter the provider details

Select Microsoft Azure as your provider and then enter the provider details. You'll need to select the Azure Subscription and the region where you want to create the backups. You can also choose your own customer-managed key for data encryption instead of using the default Microsoft-managed encryption key.

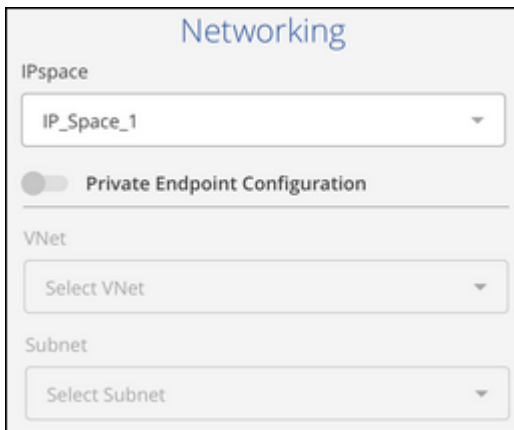


The screenshot shows the 'Provider Settings' form. It has two columns. The left column contains 'Azure Subscription' (dropdown with 'Azure_Subscription_1'), 'Resource Group' (radio buttons for 'Create a new' and 'Use an existing', with 'Use an existing' selected, and a dropdown for 'Select an Existing Resource Group' with 'Resource_Group_1'). The right column contains 'Region' (dropdown with 'Default_CM_Region') and 'Encryption' (radio buttons for 'Microsoft-managed' and 'Customer-managed', with 'Microsoft-managed' selected). Information icons are present next to the 'Resource Group' and 'Encryption' sections.

4

Select the cluster IPspace and optional use of a private VNet endpoint

Select the IPspace in the ONTAP cluster where the volumes reside. You can also choose to use an existing Azure Private Endpoint for a more secure connection to the VNet from your on-prem data center.



The screenshot shows the 'Networking' form. It contains 'IPspace' (dropdown with 'IP_Space_1'), a toggle for 'Private Endpoint Configuration' (currently off), 'VNet' (dropdown with 'Select VNet'), and 'Subnet' (dropdown with 'Select Subnet').

5

Define the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to hourly, daily, weekly, or monthly backups, or select one of the system-defined policies that provide more options. You can also change the number of backup copies to retain.

Define Policy

Policy - Retention & Schedule

☐ Create a New Policy

☒ Select an Existing Policy

Select Policy

Default Policy (30 Daily)

DP Volumes

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

6 Select the volumes that you want to back up

Identify which volumes you want to back up from the cluster.

7 Activate Compliance scans on the backed up volumes (optional)

Choose whether you want to have Cloud Data Sense scan the volumes that are backed up in the cloud.

8 Restore your data, as needed

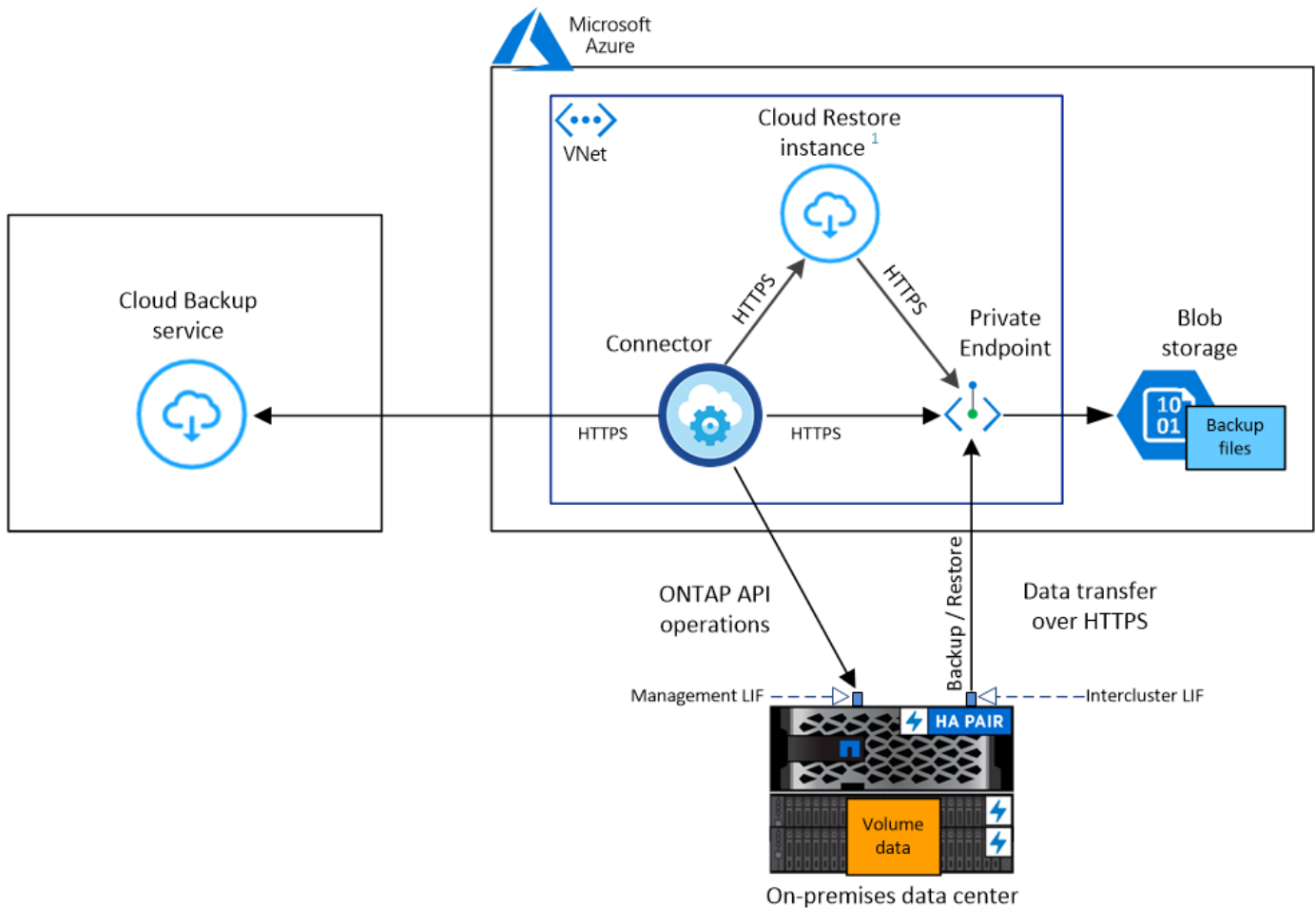
Choose to restore an entire backup to a new volume, or to restore individual files from the backup to an existing volume. You can restore data to a Cloud Volumes ONTAP system in Azure, or to an on-premises ONTAP system.

See [Restoring volume data from backup files](#) for details.

Requirements

Read the following requirements to make sure you have a supported configuration before you start backing up on-premises volumes to Azure Blob storage.

The following image shows each component and the connections that you need to prepare between them:



¹ Cloud Restore instance is active only during single-file restore operations.

Note that when the Cloud Restore instance is deployed in the cloud, it is located in the same subnet as the Connector.

Preparing your ONTAP clusters

You need to discover your on-premises ONTAP clusters in Cloud Manager before you can start backing up volume data.

[Learn how to discover a cluster.](#)

ONTAP requirements

- ONTAP 9.7P5 and later.
- A SnapMirror license (included as part of the Premium Bundle or Data Protection Bundle).

Note: The "Hybrid Cloud Bundle" is not required when using the Cloud Backup service.

See how to [manage your cluster licenses](#).

- Time and time zone are set correctly.

See how to [configure your cluster time](#).

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 from the intercluster LIF to Azure Blob storage for backup and restore operations.

ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

- ONTAP requires an inbound connection from the Connector to the cluster management LIF. The Connector can reside in an Azure VNet.
- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to back up. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage. [Learn more about IPspaces](#).

When you set up Cloud Backup, you are prompted for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.

- The nodes' and intercluster LIFs are able to access the internet.
- DNS servers have been configured for the storage VM where the volumes are located. See how to [configure DNS services for the SVM](#).
- Note that if you are using a different IPspace than the Default, then you might need to create a static route to get access to the object storage.
- Update firewall rules, if necessary, to allow Cloud Backup service connections from ONTAP to object storage through port 443 and name resolution traffic from the storage VM to the DNS server over port 53 (TCP/UDP).

Creating or switching Connectors

A Connector is required to back up data to the cloud, and the Connector must be in an Azure VNet when backing up data to Azure Blob storage. You can't use a Connector that's deployed on-premises. You'll either need to create a new Connector or make sure that the currently selected Connector resides in the correct provider.

- [Learn about Connectors](#)
- [Creating a Connector in Azure](#)
- [Switching between Connectors](#)

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
 - An outbound internet connection to the Cloud Backup service over port 443 (HTTPS)
 - An HTTPS connection over port 443 to your Blob object storage
 - An HTTPS connection over port 443 to your ONTAP clusters
2. Enable a VNet Private Endpoint to Azure storage. This is needed if you have an ExpressRoute or VPN connection from your ONTAP cluster to the VNet and you want communication between the Connector and Blob storage to stay in your virtual private network.

Supported regions

You can create backups from on-premises systems to Azure Blob in all regions [where Cloud Volumes ONTAP is supported](#). You specify the region where the backups will be stored when you set up the service.

License requirements

Before your 30-day free trial of the Cloud Backup service expires, you need to subscribe to a pay-as-you-go (PAYGO) Cloud Manager Marketplace offering from Azure, or purchase and activate a Cloud Backup BYOL license from NetApp. These licenses are for the account and can be used across multiple systems.

- For Cloud Backup PAYGO licensing, you'll need a subscription to the [Azure](#) Cloud Manager Marketplace offering to continue using Cloud Backup. Billing for Cloud Backup is done through this subscription.
- For Cloud Backup BYOL licensing, you don't need a subscription. You need the serial number from NetApp that enables you to use the service for the duration and capacity of the license. [Learn how to manage your BYOL licenses](#).

You need to have an Azure subscription for the object storage space where your backups will be located.

A SnapMirror license is required on the cluster. Note that the "Hybrid Cloud Bundle" is not required when using Cloud Backup.

Preparing Azure Blob storage for backups

1. If your virtual or physical network uses a proxy server for internet access, ensure that the Cloud Restore virtual machine has outbound internet access to contact the following endpoints.

Endpoints	Purpose
http://olcentgbl.trafficmanager.net https://olcentgbl.trafficmanager.net	Provides CentOS packages for the Cloud Restore virtual machine.
http://cloudmanagerinfraprod.azurecr.io https://cloudmanagerinfraprod.azurecr.io	Cloud Restore virtual machine image repository.

2. You use choose your own custom-managed keys for data encryption in the activation wizard instead of using the default Microsoft-managed encryption keys. In this case you will need to have the Azure Subscription, Key Vault name, and the Key. [See how to use your own keys](#).
3. If you want to have a more secure connection over the public internet from your on-prem data center to the VNet, there is an option to configure an Azure Private Endpoint in the activation wizard. In this case you will need to know the VNet and Subnet for this connection. [See details about using a Private Endpoint](#).

Enabling Cloud Backup

Enable Cloud Backup at any time directly from the on-premises working environment.

Steps

1. From the Canvas, select the working environment and click **Enable** next to the Backup & Compliance service in the right-panel.



2. Select Microsoft Azure as your provider and click **Next**.
3. Enter the provider details. Note that you can't change this information after the service has started.
 - a. The Azure subscription used for backups and the Azure region where the backups will be stored.
 - b. The resource group that manages the Blob container - you can create a new resource group or select an existing resource group.
 - c. Whether you will use the default Microsoft-managed encryption key or choose your own customer-managed keys to manage encryption of your data. ([See how to use your own keys](#)).

 A screenshot of the 'Provider Settings' form. It contains four main sections:

- Azure Subscription:** A dropdown menu with 'Azure_Subscription_1' selected.
- Region:** A dropdown menu with 'Default_CM_Region' selected.
- Resource Group:** Includes radio buttons for 'Create a new' (unselected) and 'Use an existing' (selected). Below is a dropdown menu for 'Select an Existing Resource Group' with 'Resource_Group_1' selected.
- Encryption:** Includes radio buttons for 'Microsoft-managed' (selected) and 'Customer-managed' (unselected).

4. Click **Next** after you've entered the provider details.
5. Enter the networking details and click **Next**.
 - a. The IPspace in the ONTAP cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
 - b. Optionally, choose whether you will configure an Azure Private Endpoint. [See details about using a Private Endpoint](#).

 A screenshot of the 'Networking' form. It contains four main sections:

- IPspace:** A dropdown menu with 'IP_Space_1' selected.
- Private Endpoint Configuration:** A toggle switch that is currently turned off.
- VNet:** A dropdown menu with 'Select VNet' as the placeholder text.
- Subnet:** A dropdown menu with 'Select Subnet' as the placeholder text.

6. In the *Define Policy* page, select an existing backup schedule and retention value, or define a new backup policy, and click **Next**.

Define Policy

Policy - Retention & Schedule

☐ Create a New Policy

☒ Select an Existing Policy

Select Policy

Default Policy (30 Daily)

DP Volumes

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

See [the list of existing policies](#).

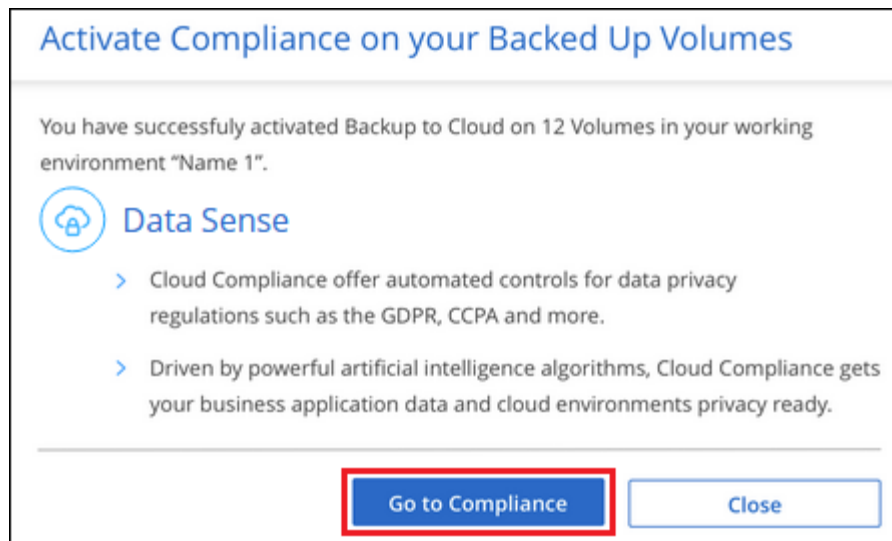
7. Select the volumes that you want to back up.
- To back up all volumes, check the box in the title row (☒ Volume Name).

To back up individual volumes, check the box for each volume (☒ Volume_1).

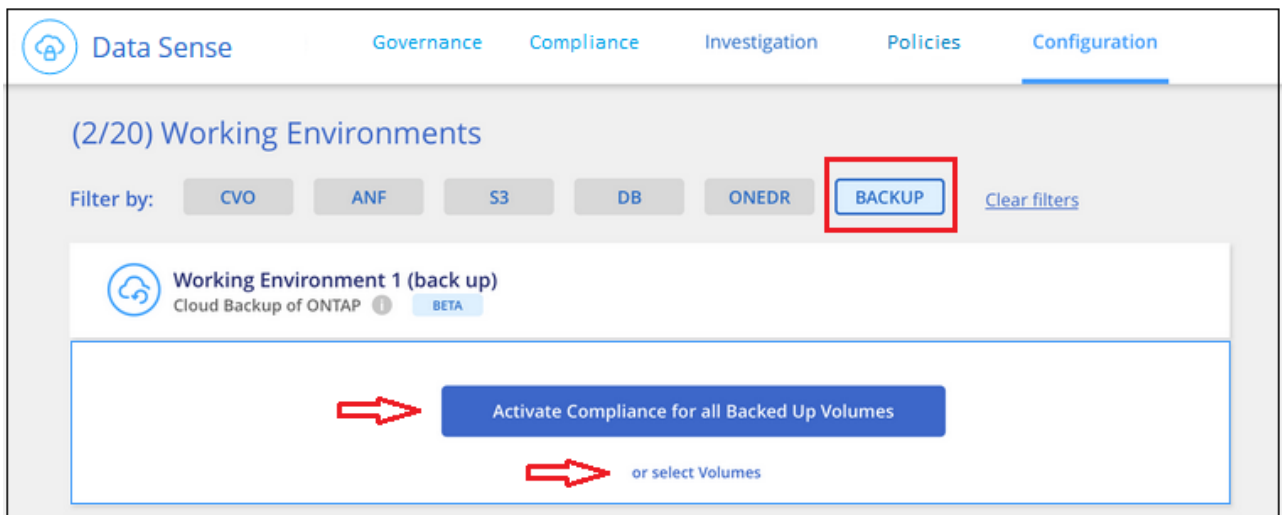
Select Volumes							
57 Volumes							
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status	
<input checked="" type="checkbox"/>	Volume_Name_1	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active	
<input checked="" type="checkbox"/>	Volume_Name_2	RW	SVM_Name_2	0.25 TB	10 TB	<input type="radio"/> Not Active	
<input checked="" type="checkbox"/>	Volume_Name_3	RW	SVM_Name_3	0.25 TB	10 TB	<input type="radio"/> Not Active	
<input checked="" type="checkbox"/>	Volume_Name_4	DP	SVM_Name_4	0.25 TB	10 TB	<input type="radio"/> Not Active	
<input checked="" type="checkbox"/>	Volume_Name_5	RW	SVM_Name_5	0.25 TB	10 TB	<input type="radio"/> Not Active	

8. Click **Activate Backup** and Cloud Backup starts taking the initial backups of your volumes.

You are prompted whether you want to run compliance scans on the backed up volumes. Cloud Data Sense scans are free when you run them on the backed up volumes (except for the [cost of the deployed Cloud Data Sense instance](#)).



9. Click **Go to Compliance** to activate compliance scans on the volumes. (If you choose **Close** and not to scan these backed up volumes, you can always [enable this functionality](#) later from Cloud Data Sense.)
 - If an instance of Cloud Data Sense is already deployed in your environment, you are directed to the Configuration page to select the volumes you want to scan in each on-premises working environment that has backups. See [how to choose the volumes](#).



- If Cloud Data Sense has not been deployed, you are directed to the Compliance page where you can choose to deploy Compliance in the cloud or in your premises. We strongly recommend deploying it in the cloud. Go [here](#) for installation requirements and instructions.

The screenshot shows the Data Sense web interface. At the top left is the 'Data Sense' logo. Below it is a link 'How does it work?'. The main heading is 'Always-on Privacy & Compliance Controls'. Below this is a paragraph: 'Automated controls for data privacy regulations - GDPR, CCPA, HIPAA and more. Driven by powerful artificial intelligence algorithms, Data Sense gets your business application data and cloud environments privacy ready.' There are two buttons: 'Deploy Data Sense in the Cloud' (highlighted with a red border) and 'Deploy Data Sense On-Premises'. Below the buttons is a link: 'Learn about the differences between cloud deployment and on-premises deployment'. On the right side, there is a 'Compliance Status' dashboard. It features a 'Data Distribution' chart showing 75% Non-Sensitive, 20% Personal, and 5% Sensitive Personal data. Below this, it shows '28,000 Personal Files' and '7,000 Sensitive Personal Files'. There are also lists of sensitive data types: 'Email Address' (2,700 Files), 'Credit Card' (2,700 Files), 'Health' (2,700 Files), and 'Ethnicity' (2,700 Files).

Data Sense

How does it work?

Always-on Privacy & Compliance Controls

Automated controls for data privacy regulations - GDPR, CCPA, HIPAA and more.
Driven by powerful artificial intelligence algorithms, Data Sense gets your business application data and cloud environments privacy ready.

[Deploy Data Sense in the Cloud](#) [Deploy Data Sense On-Premises](#)

[Learn about the differences between cloud deployment and on-premises deployment](#)

Compliance Status

Data Distribution

- 75% Non-Sensitive
- 20% Personal
- 5% Sensitive Personal

28,000 Personal Files [View All](#)

- Email Address 2,700 Files
- Credit Card 2,700 Files

7,000 Sensitive Personal Files [View All](#)

- Health 2,700 Files
- Ethnicity 2,700 Files

After you have deployed Compliance you can choose the volumes you want to scan as described above.

Result

Cloud Backup backs up your volumes from the on-premises ONTAP system, and optionally, Cloud Data Sense runs compliance scans on the backed up volumes.

What's next?

You can [start and stop backups for volumes or change the backup schedule](#) and you can [restore entire volumes or individual files from a backup file](#).

You can also [view the results of the compliance scans](#) and review other features of Cloud Data Sense that can help you understand data context and identify sensitive data in your organization.



The scan results are not available immediately because Cloud Backup has to finish creating the backups before Cloud Data Sense can start compliance scans.

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.