Get started with Cloud Data Sense for Amazon FSx for ONTAP

Cloud Manager

Julia
September 30, 2021

Table of Contents

Get started with Cloud Data Sense for Amazon FSx for ONTAP

Complete a few steps to get started with Cloud Data Sense for FSx for ONTAP.

Before you begin

- You need an active Connector in AWS to deploy and manage Data Sense.
- The security group you selected when creating the working environment must allow traffic from the Cloud Data Sense instance. You can find the associated security group using the ENI connected to the FSx for ONTAP file system and edit it using the AWS Management Console.

  AWS security groups for Linux instances

  AWS security groups for Windows instances

  AWS elastic network interfaces (ENI)

Quick start

Get started quickly by following these steps or scroll down for full details.

Discover the data sources that contain the data you want to scan

Before you can scan FSx for ONTAP volumes, you must have an FSx working environment with volumes configured.

Deploy the Cloud Data Sense instance

Deploy Cloud Data Sense in Cloud Manager if there isn't already an instance deployed.

Enable Cloud Data Sense and select the volumes to scan

Click **Data Sense**, select the **Configuration** tab, and activate compliance scans for volumes in specific working environments.

Ensure access to volumes

Now that Cloud Data Sense is enabled, ensure that it can access all volumes.

- The Cloud Data Sense instance needs a network connection to each FSx for ONTAP subnet.
- Make sure the following ports are open to the Data Sense instance.
  - For NFS – ports 111 and 2049.

- For CIFS – ports 139 and 445.

- NFS volume export policies must allow access from the Data Sense instance.
- Data Sense needs Active Directory credentials to scan CIFS volumes.

  Click **Compliance** > **Configuration** > **Edit CIFS Credentials** and provide the credentials.

5 **Manage the volumes you want to scan**

Select or deselect the volumes you want to scan and Cloud Data Sense will start or stop scanning them.

Discovering the data sources that you want to scan

If the data sources you want to scan are not already in your Cloud Manager environment, you can add them to the canvas at this time.

For FSx for ONTAP, Cloud Manager must be set up to discover the configuration.

Deploying the Cloud Data Sense instance

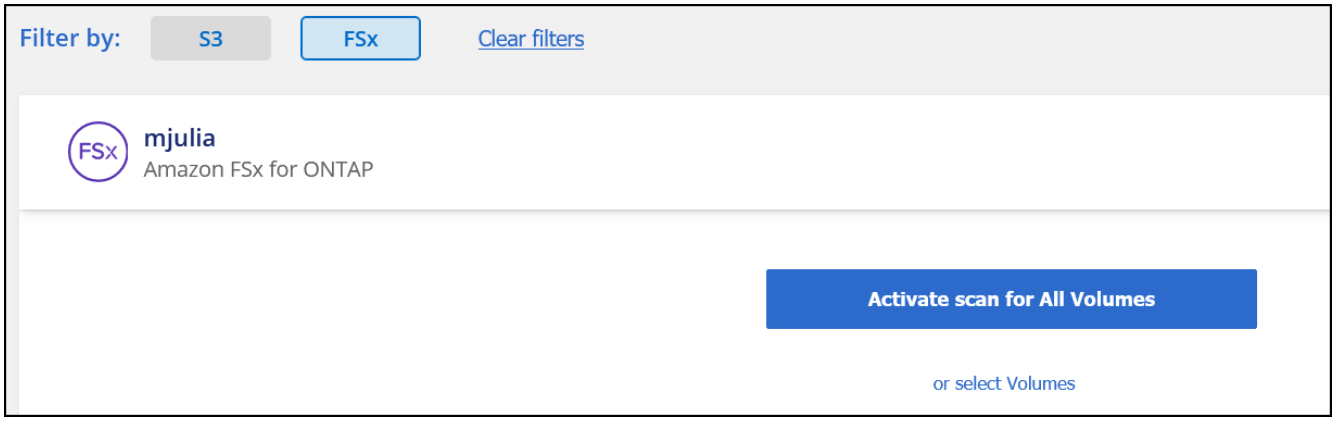
Deploy Cloud Data Sense if there isn't already an instance deployed.

Data Sense should be deployed in the same AWS network as the Connector for AWS and the FSx volumes you wish to scan.

Enabling Cloud Data Sense in your working environments

You can enable Cloud Data Sense for FSx for ONTAP volumes.

1. At the top of Cloud Manager, click **Data Sense** and then select the **Configuration** tab.



2. To scan all volumes in a working environment, click **Activate Scanning for All Volumes**.

   When enabled in this manner, full "mapping and classification" scanning is performed on all volumes.

   If you want to enable scanning only for certain volumes, or if you only want to perform "mapping-only" scanning, click **or select Volumes** and then choose the volumes you want to scan.

See Enabling and disabling compliance scans on volumes for details.

Result

Cloud Data Sense starts scanning the volumes you selected in the working environment. Results will be available in the Compliance dashboard as soon as Cloud Data Sense finishes the initial scans. The time that it takes depends on the amount of data—it could be a few minutes or hours.

Verifying that Cloud Data Sense has access to volumes

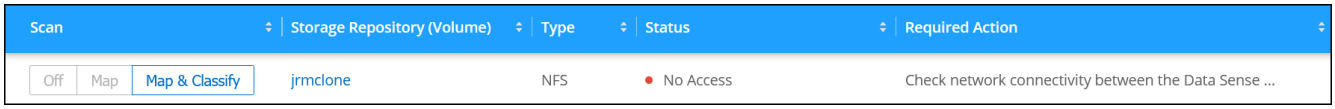
Make sure Cloud Data Sense can access volumes by checking your networking, security groups, and export policies.

You'll need to provide Data Sense with CIFS credentials so it can access CIFS volumes.

Steps

1. On the *Configuration* page, click **View Details** to review the status and correct any errors.

   For example, the following image shows a volume Cloud Data Sense can't scan due to network connectivity issues between the Data Sense instance and the volume.



2. Make sure there's a network connection between the Cloud Data Sense instance and each network that includes volumes for FSx for ONTAP.

   For FSx for ONTAP, Cloud Data Sense can scan volumes only in the same region as Cloud Manager.

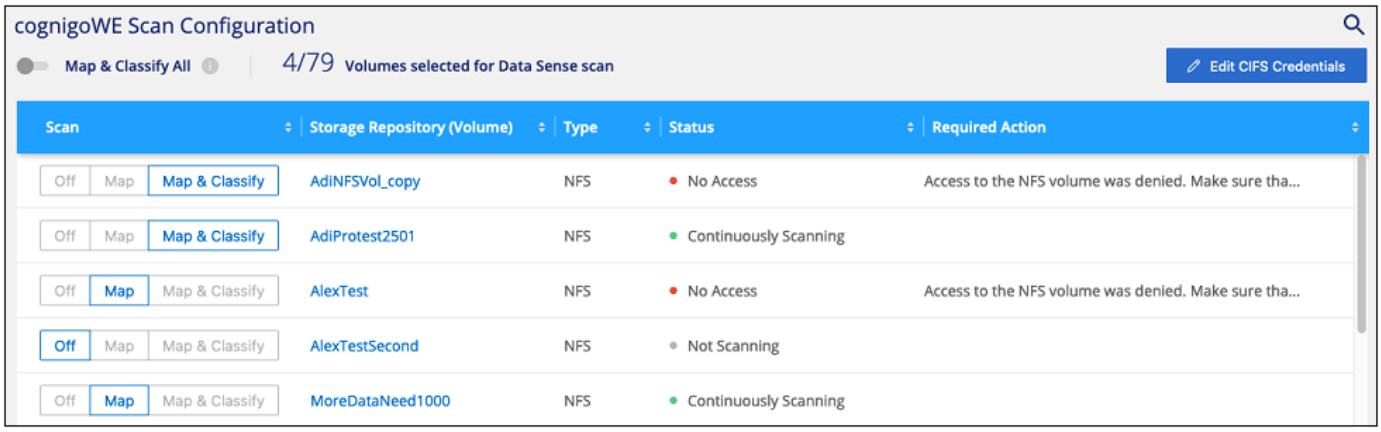
3. Ensure the following ports are open to the Data Sense instance.
   - For NFS – ports 111 and 2049.
   - For CIFS – ports 139 and 445.
4. Ensure NFS volume export policies include the IP address of the Data Sense instance so it can access the data on each volume.
5. If you use CIFS, provide Data Sense with Active Directory credentials so it can scan CIFS volumes.
   a. At the top of Cloud Manager, click **Data Sense**.
   b. Click the **Configuration** tab.
   c. For each working environment, click **Edit CIFS Credentials** and enter the user name and password that Data Sense needs to access CIFS volumes on the system.

      The credentials can be read-only, but providing admin credentials ensures that Data Sense can read any data that requires elevated permissions. The credentials are stored on the Cloud Data Sense instance.

      After you enter the credentials, you should see a message that all CIFS volumes were authenticated successfully.

Enabling and disabling compliance scans on volumes

You can stop or start mapping scans, or mapping and classification scans, in a working environment at any time from the Configuration page. We recommend that you scan all volumes.



To:	Do this:
Enable mapping-only scans on a volume	Click **Map**
Enable full scanning on a volume	Click **Map & Classify**
Enable full scanning on all volumes	Move the **Map & Classify All** slider to the right
Disable scanning on a volume	Click **Off**
Disable scanning on all volumes	Move the **Map & Classify All** slider to the left

New volumes added to the working environment are automatically scanned only when the **Activate Compliance for all Volumes** setting is enabled. When this setting is disabled, you'll need to activate scanning on each new volume you create in the working environment.