Azure NetApp Files

Cloud Manager

NetApp
October 11, 2021

Table of Contents

Azure NetApp Files

Learn about Azure NetApp Files

Azure NetApp Files enables enterprises to migrate and run their performance-intensive and latency-sensitive core, business-critical applications in Azure with no need to refactor for the cloud.

Features

- Support for multiple protocols enables "lift & shift" of both Linux & Windows applications to run seamlessly in Azure.
- Multiple performance tiers allow for close alignment with workload performance requirements.
- Leading certifications including SAP HANA, GDPR, and HIPAA enables migration of the most demanding workloads to Azure.

Additional features in Cloud Manager

- Migrate NFS or SMB data to Azure NetApp Files directly from Cloud Manager. Data migrations are powered by NetApp's Cloud Sync service. Learn more.
- Using Artificial Intelligence (AI) driven technology, Cloud Data Sense can help you understand data context and identify sensitive data that resides in your Azure NetApp Files accounts. Learn more.

Cost

View Azure NetApp Files pricing.

Note that your subscription and charging are maintained by the Azure NetApp Files service and not by Cloud Manager.

Supported regions

View supported Azure regions.

Requesting access

You need to be granted access to Azure NetApp Files by submitting an online request. You'll need to wait for approval from the Azure NetApp Files team before you can proceed.

Getting help

For technical support issues associated with Azure NetApp Files, use the Azure portal to log a support request to Microsoft. Select your associated Microsoft subscription and select the **Azure NetApp Files** service name under **Storage**. Provide the remaining information required to create your Microsoft support request.

For issues related to Cloud Sync and Azure NetApp Files, you can start with NetApp using your Cloud Sync serial number directly from the Cloud Sync service. You will need to access the Cloud Sync service through the link in Cloud Manager. View the process to enable Cloud Sync support.

Related links

- NetApp Cloud Central: Azure NetApp Files
- Azure NetApp Files documentation
- Cloud Sync documentation

Setting up and discovering Azure NetApp Files

Create an Azure NetApp Files working environment in Cloud Manager to create and manage NetApp accounts, capacity pools, volumes, and snapshots.

If you haven't set up Azure NetApp Files yet, you'll need to complete all of the steps on this page.

If you already set up Azure NetApp Files from outside of Cloud Manager, then you simply need to set up an Azure AD application and then create the Azure NetApp Files working environment.

Quick start

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

Request access

Submit an online request to be granted access to Azure NetApp Files.

Set up an Azure AD application

From Azure, grant permissions to an Azure AD application and copy the application (client) ID, the directory (tenant) ID, and the value of a client secret.

Create an Azure NetApp Files working environment

In Cloud Manager, click **Add Working Environment** > **Microsoft Azure** > **Azure NetApp Files** and then provide details about the AD application.

Requesting access

You need to be granted access to Azure NetApp Files by submitting an online request. You'll need to wait for approval from the Azure NetApp Files team before you can proceed.

Setting up an Azure AD application

Cloud Manager needs permissions to set up and manage Azure NetApp Files. You can grant the required permissions to an Azure account by creating and setting up an Azure AD application and by obtaining the Azure credentials that Cloud Manager needs.

Creating the AD application

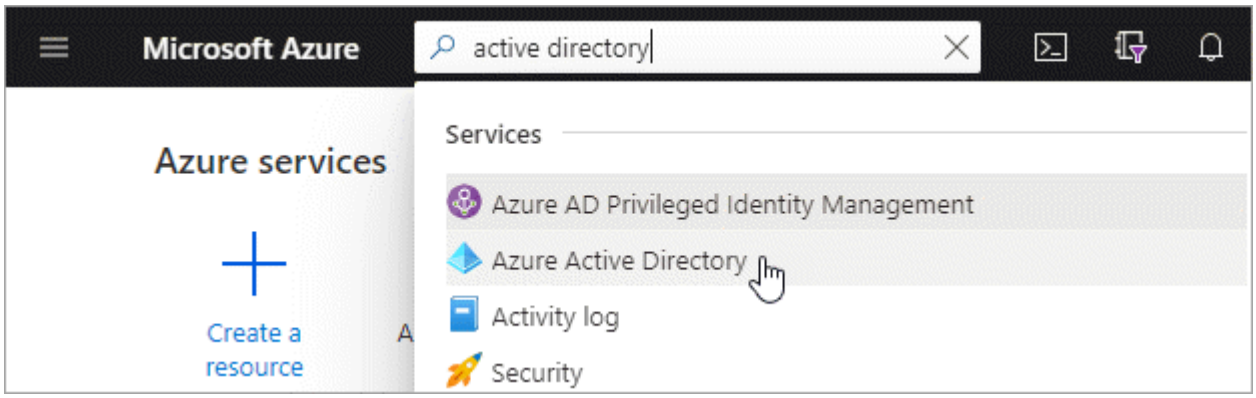
Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

Before you begin

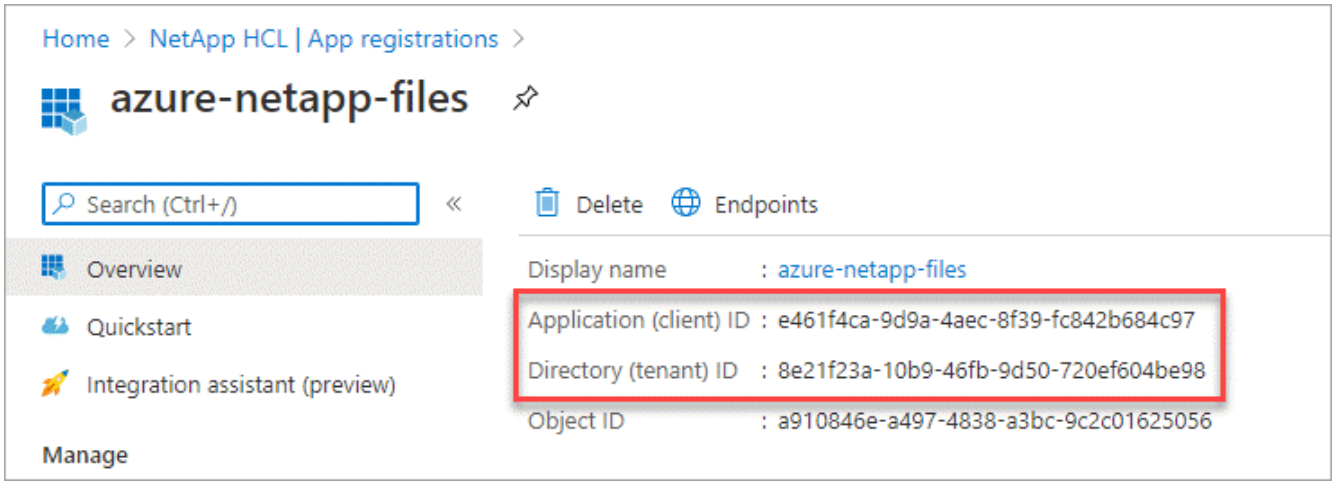
You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Required permissions.

Steps

1. From the Azure portal, open the **Azure Active Directory** service.



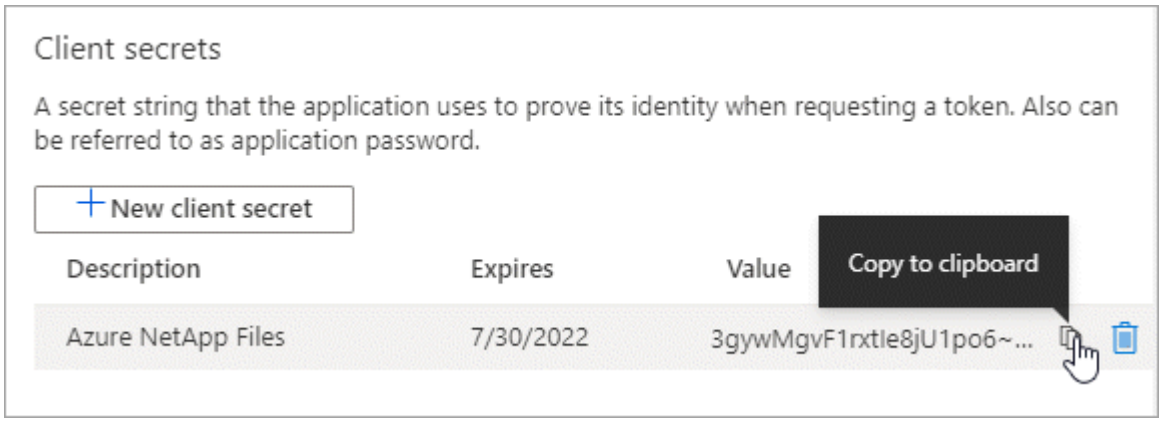
2. In the menu, click **App registrations**.
3. Create the application:
   a. Click **New registration**.
   b. Specify details about the application:
      - **Name**: Enter a name for the application.
      - **Account type**: Select an account type (any will work with Cloud Manager).
      - **Redirect URI**: You can leave this blank.
   c. Click **Register**.
4. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



When you create the Azure NetApp Files working environment in Cloud Manager, you need to provide the

application (client) ID and the directory (tenant) ID for the application. Cloud Manager uses the IDs to programmatically sign in.

5. Create a client secret for the application so Cloud Manager can use it to authenticate with Azure AD:
   a. Click **Certificates & secrets > New client secret**.
   b. Provide a description of the secret and a duration.
   c. Click **Add**.
   d. Copy the value of the client secret.



Result

Your AD application is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in Cloud Manager when you add an Azure NetApp Files working environment.

Assigning the app to a role

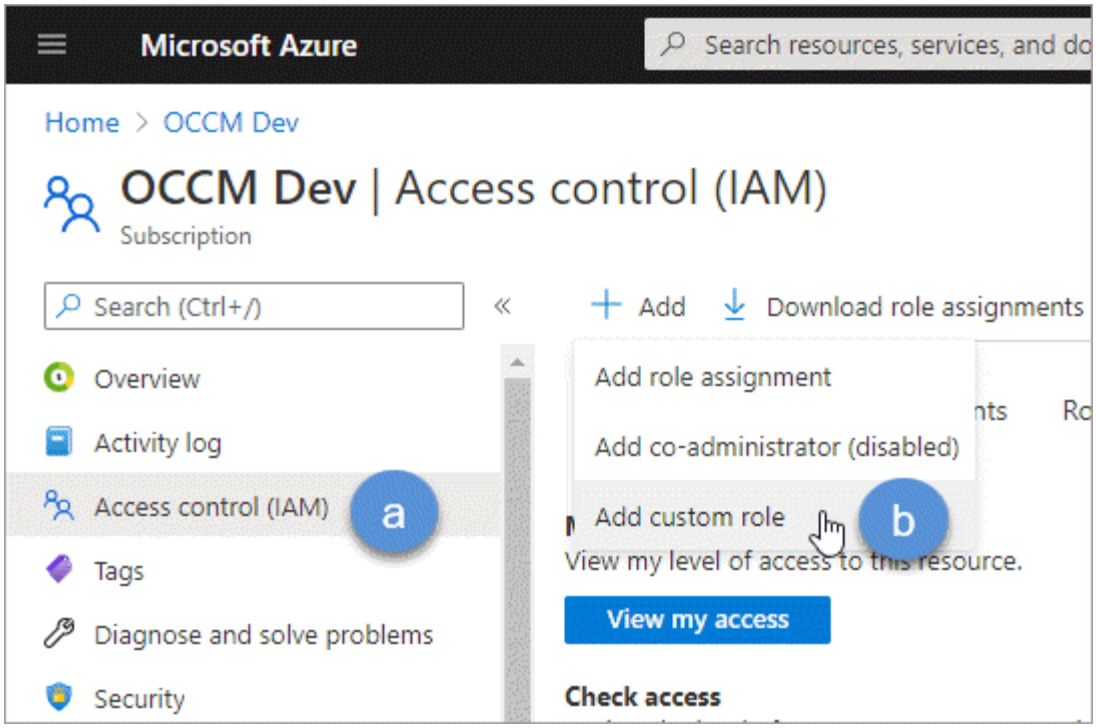
You must bind the service principal to your Azure subscription and assign it a custom role that has the required permissions.

Steps

1. Create a custom role in Azure.

   The following steps describe how to create the role from the Azure portal.

   a. Open the subscription and click **Access control (IAM)**.
   b. Click **Add > Add custom role**.



c. In the **Basics** tab, enter a name and description for the role.

d. Click **JSON** and click **Edit** which appears at the top right of the JSON format.

e. Add the following permissions under *actions*:

```
"actions": [
    "Microsoft.NetApp/*",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Insights/Metrics/Read"
    ],
```

f. Click **Save**, click **Next**, and then click **Create**.

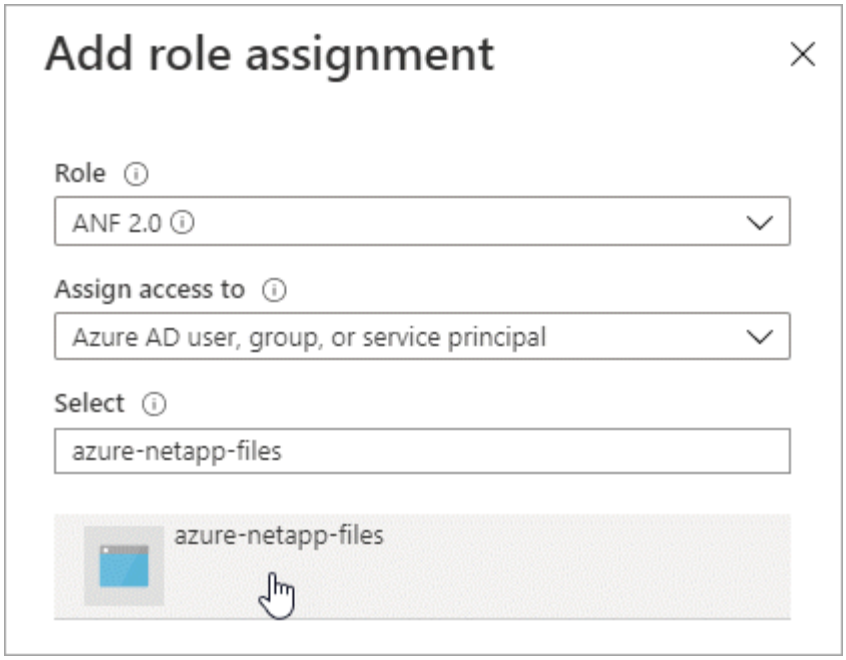
2. Now assign the application to the role that you just created:

a. From the Azure portal, open the subscription and click **Access control (IAM) > Add > Add role assignment**.

b. Select the custom role that you created.

c. Keep **Azure AD user, group, or service principal** selected.

d. Search for the name of the application (you can't find it in the list by scrolling).



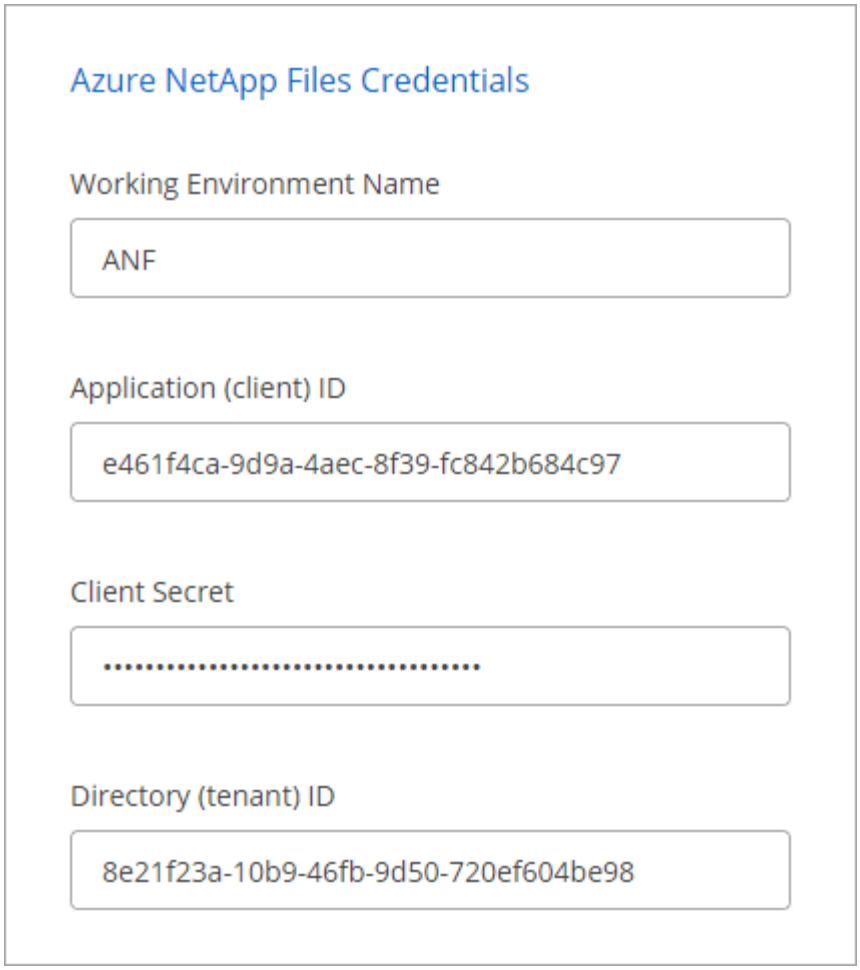
e. Select the application and click **Save**.

The service principal for Cloud Manager now has the required Azure permissions for that subscription.

Creating an Azure NetApp Files working environment

Set up an Azure NetApp Files working environment in Cloud Manager so you can start creating volumes.

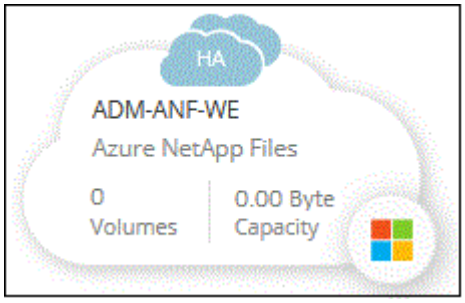
1. From the Canvas page, click **Add Working Environment**.
2. Select **Microsoft Azure** and then **Azure NetApp Files**.
3. Provide details about the AD application that you previously set up.



4. Click **Add**.

Result

You should now have an Azure NetApp Files working environment.



What's next?

Start creating and managing volumes.

Creating and managing volumes for Azure NetApp Files

After you set up your working environment, you can create and manage Azure NetApp Files accounts, capacity pools, volumes, and snapshots.

Creating volumes

You can create NFS or SMB volumes in a new or existing Azure NetApp Files account.

A Cloud Manager feature called "templates" enables you to create volumes that are optimized for the workload requirements for certain applications; such as databases or streaming services. If your organization has created volume templates that you should use, follow these steps.

Before you begin

- If you want to use SMB, you must have set up DNS and Active Directory.
- When planning to create an SMB volume, you must have a Windows Active Directory server available to which you can connect. You will enter this information when creating the volume.

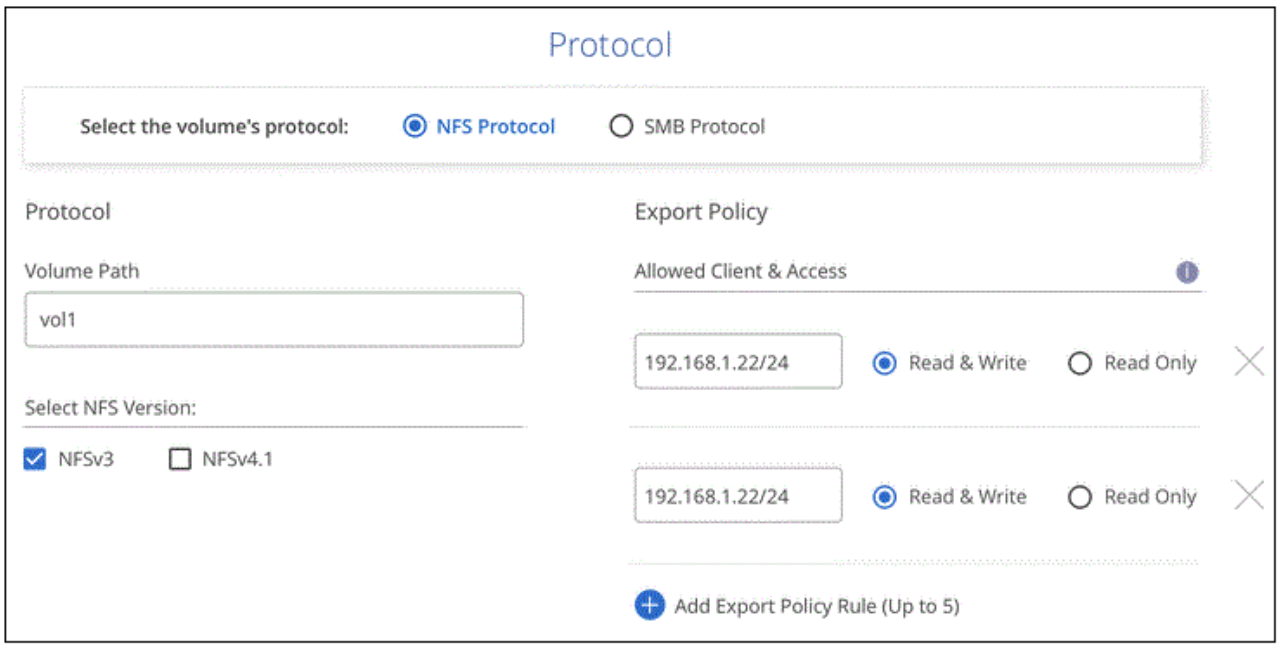
Steps

1. Open the Azure NetApp Files working environment.
2. Click **Add New Volume**.
3. Provide the required information on each page:
    - **Azure NetApp Files Account**: Choose an existing Azure NetApp Files account or create a new account. When creating a new account you can also choose the Resource Group that you want to use.
    - **Capacity Pool**: Select an existing capacity pool or create a new capacity pool.

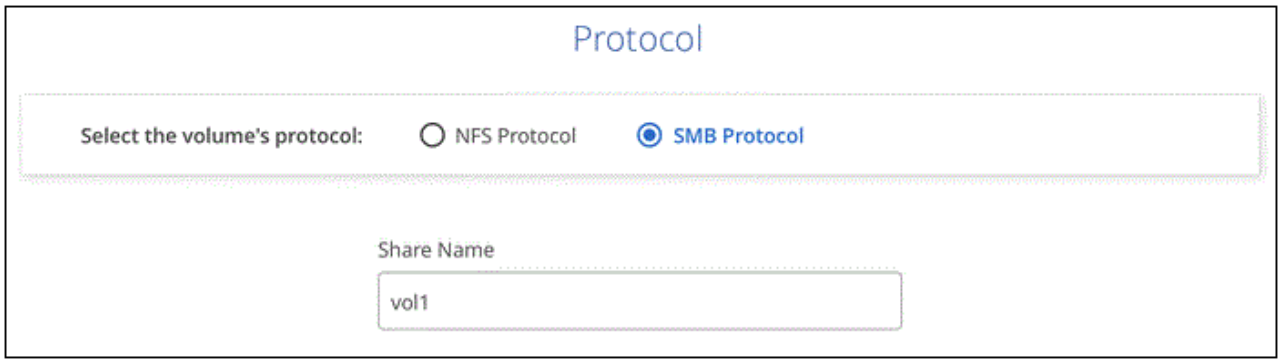
      If you create a new capacity pool, you need to specify a size and select a service level.

      The minimum size for the capacity pool is 4 TB. You can specify a size in multiples of 4 TB.
    - **Details & Tags**: Enter a volume name and size, the VNet and subnet where the volume should reside, and optionally specify tags for the volume.
    - **Protocol**: Choose the NFS or SMB protocol and enter the required information.

      Here's an example of details for NFS.



Here's an example of details for SMB. You'll need to provide Active Directory information on the next page when you set up your first SMB volume.



4. If you want this volume to be created based on a snapshot of an existing volume, select the snapshot from the Snapshot Name drop-down list.
5. Click **Add Volume**.

Result

The new volume is added to the working environment.

Continue with mounting the cloud volume.

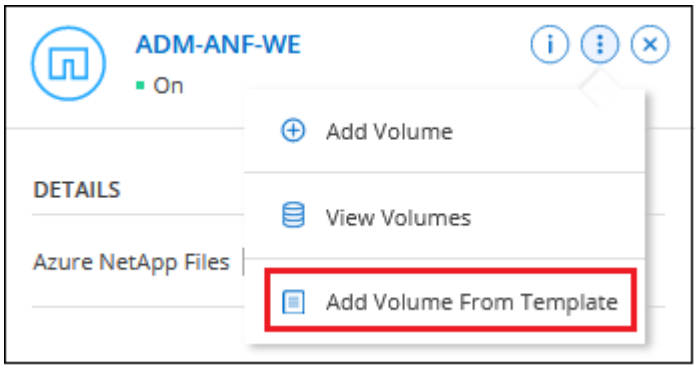
Creating volumes from templates

If your organization has created ANF volume templates so you can deploy volumes that are optimized for the workload requirements for certain applications, follow the steps in this section.

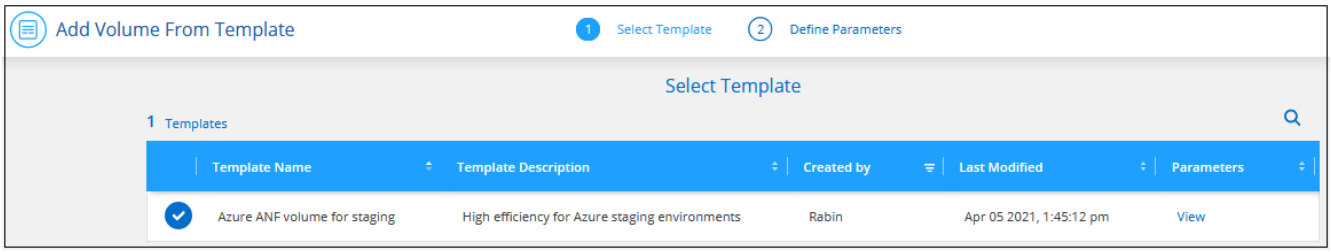
The template should make your job easier because certain volume parameters will already be defined in the template, such as capacity pool, size, protocol, VNet and subnet where the volume should reside, and more. When a parameter is already predefined, you can just skip to the next volume parameter.

Steps

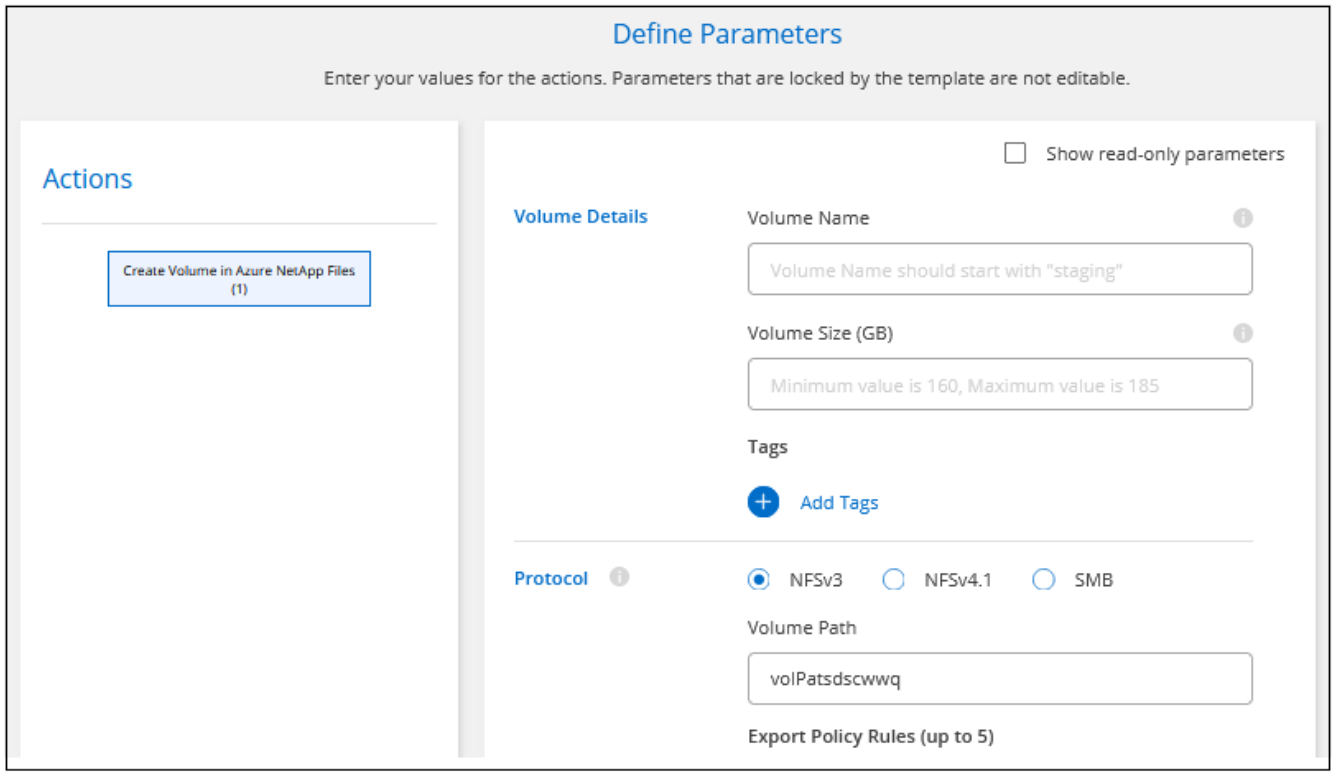
1. On the Canvas page, click the Azure NetApp Files working environment on which you want to provision a volume.
2. Click > **Add Volume From Template**.



3. In the *Select Template* page, select the template that you want to use to create the volume and click **Next**.



The *Define Parameters* page is displayed.



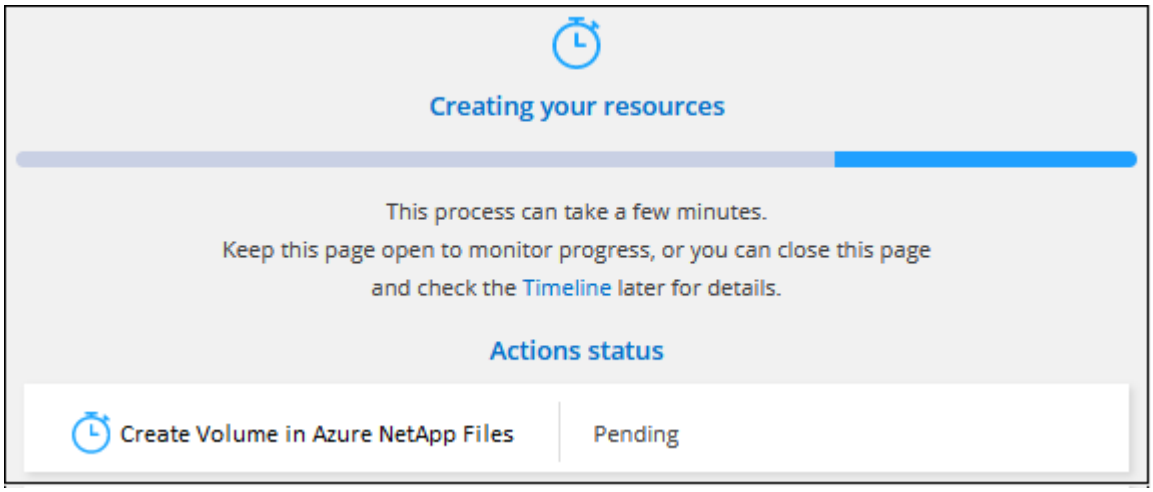
Note: You can click the checkbox **Show read-only parameters** to show all the fields that have been locked by the template if you want to see the values for those parameters. By default these predefined

fields are hidden and only the fields you need to complete are shown.

4. Add values for all of the parameters that are not hard-coded from the template. See creating volumes for details about all the parameters you need to complete to deploy an ANF volume.
5. Click **Run Template** after you have defined all the parameters needed for this volume.

Result

Cloud Manager provisions the volume and displays a page so that you can see the progress.



Then the new volume is added to the working environment.

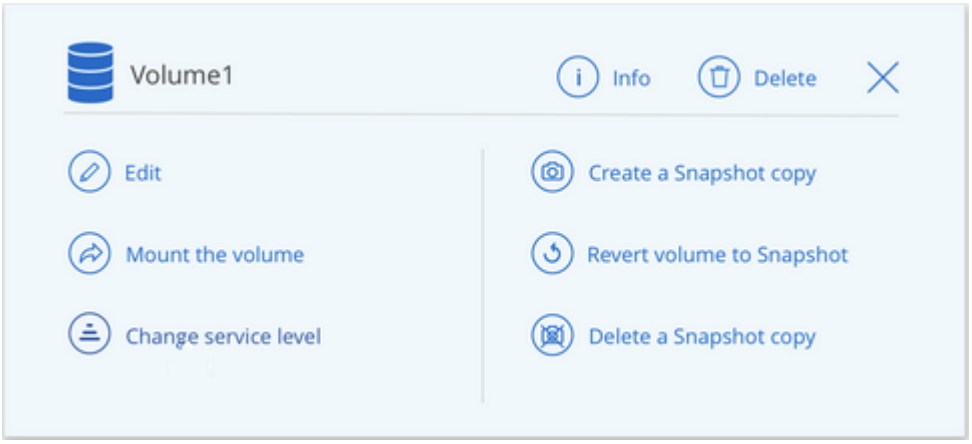
Continue with mounting the cloud volume.

Mounting volumes

Access mounting instructions from within Cloud Manager so you can mount the volume to a host.

Steps

1. Open the working environment.
2. Hover over the volume and select **Mount the volume**.



3. Follow the instructions to mount the volume.

Editing a volume's size and tags

After you create a volume, you can modify its size and tags at any time.

Steps

1. Open the working environment.
2. Hover over the volume and select **Edit**.
3. Modify the size and tags as needed.
4. Click **Apply**.

Changing the volume's service level

After you create a volume, you can change the service level at any time as long as the destination capacity pool already exists.

Steps

1. Open the working environment.
2. Hover over the volume and select **Change service level**.
3. Select the capacity pool that provides the service level that you want.
4. Click **Change**.

Result

The volume is moved to the other capacity pool with no impact to the volume.

Managing Snapshot copies

Snapshot copies provide a point-in-time copy of your volume. Create Snapshot copies, restore the data to a new volume, and delete Snapshot copies.

Steps

1. Open the working environment.
2. Hover over the volume and choose one of the available options to manage Snapshot copies:
   - **Create a Snapshot copy**
   - **Revert volume to Snapshot**
   - **Delete a Snapshot copy**
3. Follow the prompts to complete the selected action.

Deleting volumes

Delete the volumes that you no longer need.

Steps

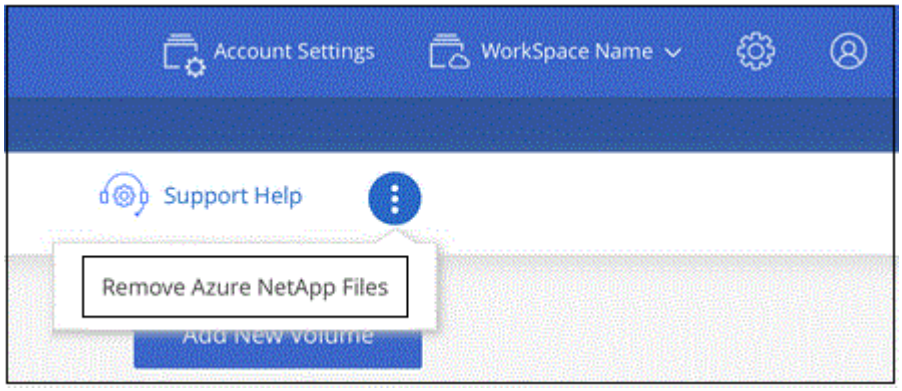
1. Open the working environment.
2. Hover over the volume and click **Delete**.
3. Confirm that you want to delete the volume.

Removing Azure NetApp Files

This action removes Azure NetApp Files from Cloud Manager. It doesn't delete your Azure NetApp Files account or volumes. You can add Azure NetApp Files back to Cloud Manager at any time.

Steps

1. Open the Azure NetApp Files working environment.
2. At the top right of the page, select the actions menu and click **Remove Azure NetApp Files**.



3. Click **Remove** to confirm.