Get started

Azure NetApp Files

NetApp
July 19, 2022

Table of Contents

Get started

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 about Cloud Sync

- 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 about Cloud Data Sense

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

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.

Related links

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

- Cloud Sync documentation

Quick start for Azure NetApp Files

Get started quickly by following these steps or follow the links for full details.

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.

Learn how to set up an Azure AD application.

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.

Learn how to create a working environment.

Set 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 Active Directory (AD) application and by obtaining the Azure credentials that Cloud Manager needs.

Create the AD application

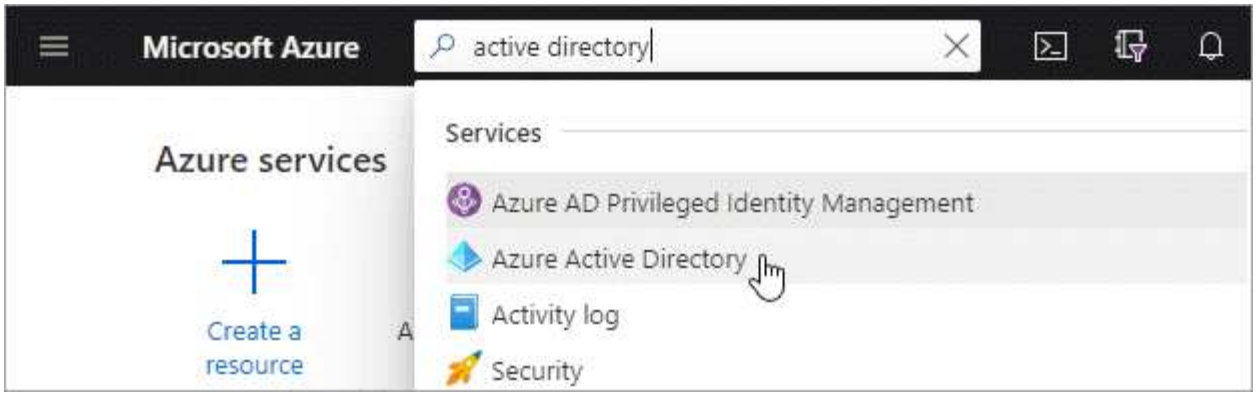
Create an Azure AD application and service principal that Cloud Manager can use for role-based access control.

Before you begin

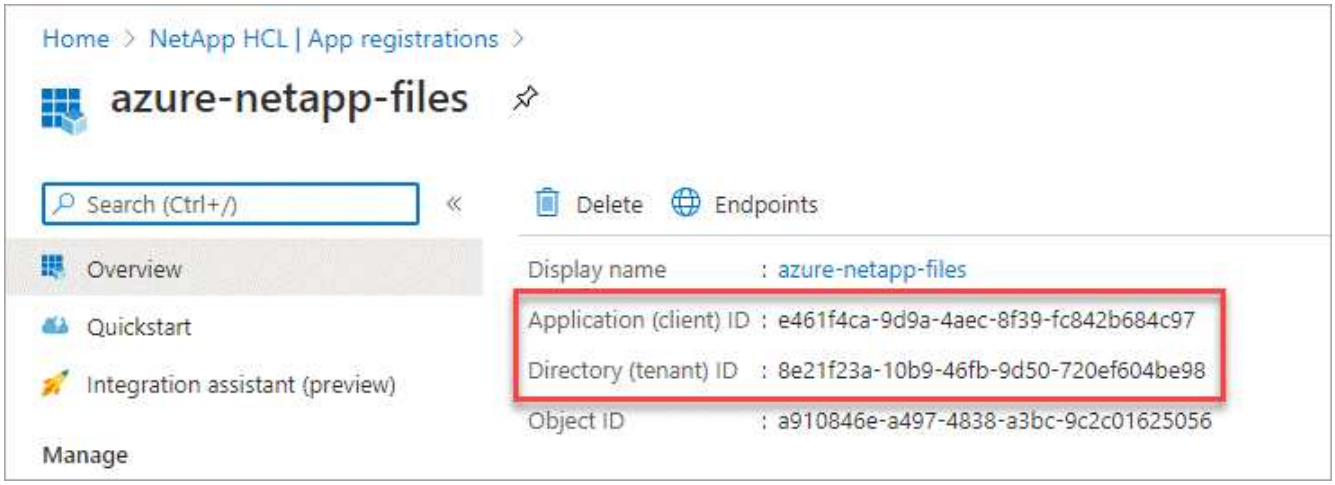
You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Required permissions.

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.

Assign 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.

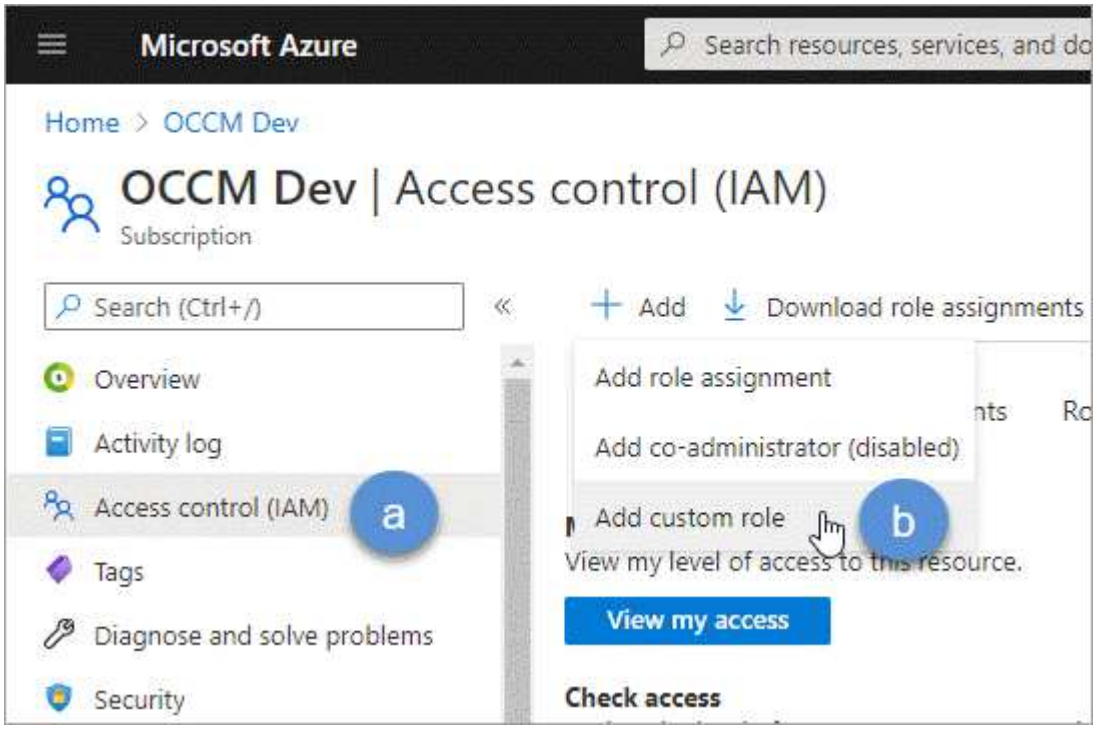
Steps

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 **Subscriptions** service.

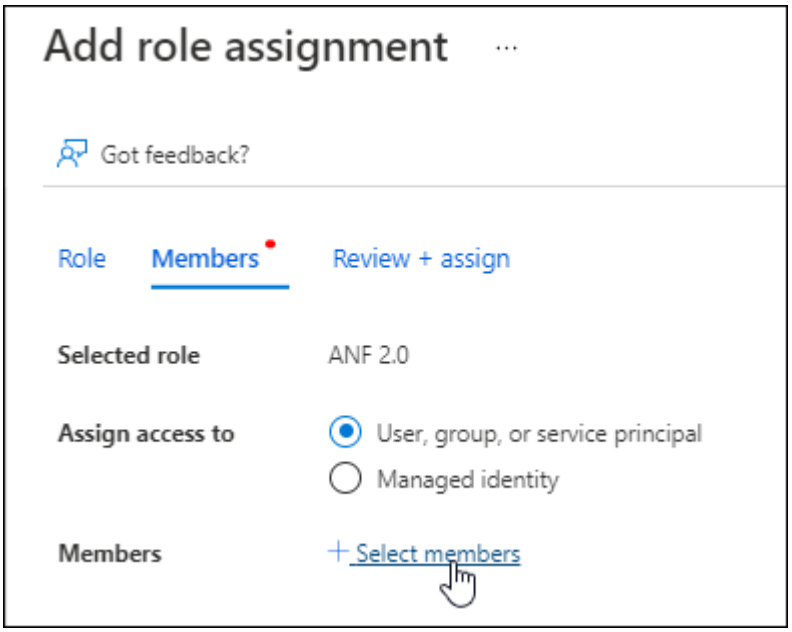
b. Select the subscription.

c. Click **Access control (IAM) > Add > Add role assignment**.

d. In the **Role** tab, select the custom role that you created and click **Next**.

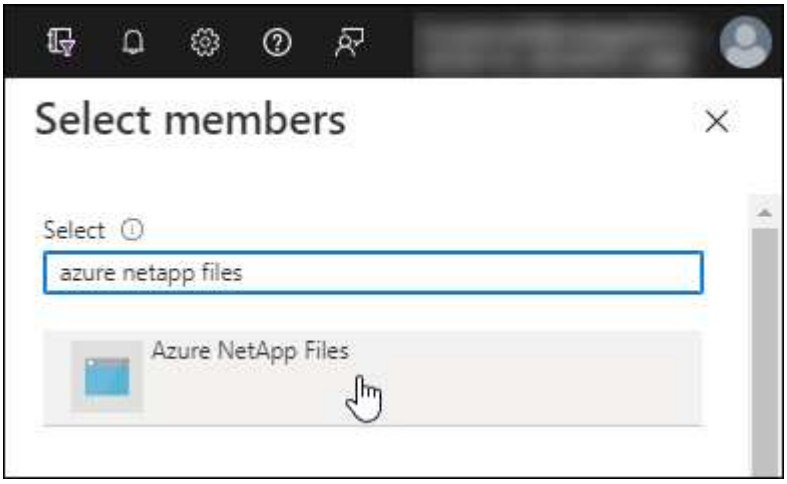
e. In the **Members** tab, complete the following steps:

- Keep **User, group, or service principal** selected.
- Click **Select members**.



- Search for the name of the application.

Here's an example:



- Select the application and click **Select**.
- Click **Next**.

f. Click **Review + assign**.

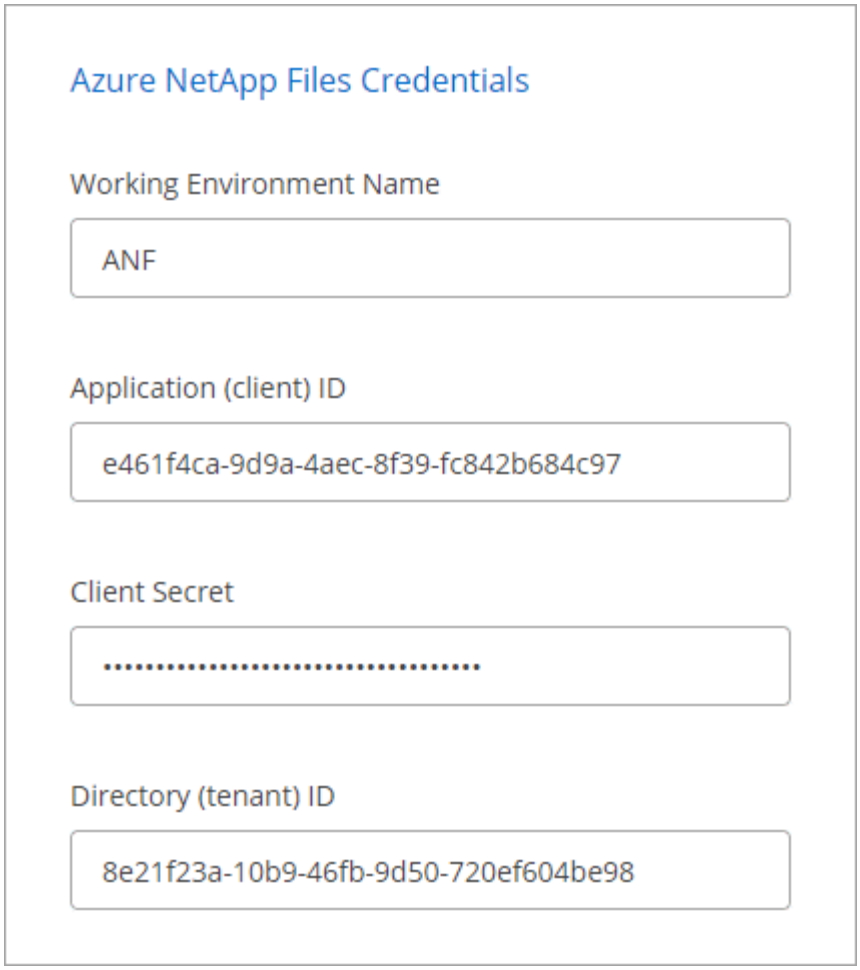
The service principal for Cloud Manager now has the required Azure permissions for that subscription.

Create an Azure NetApp Files working environment

After you set up an Azure Active Directory application, create an Azure NetApp Files working environment in Cloud Manager so that you can start creating the volumes that you need.

Steps

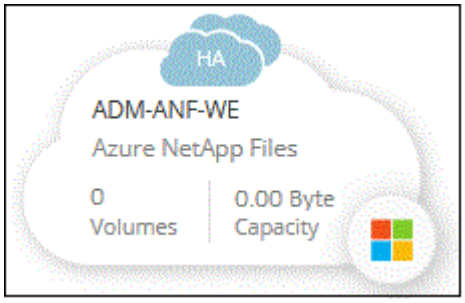
1. From the Canvas page, click **Add Working Environment**.
2. Select **Microsoft Azure** and then **Azure NetApp Files**.
3. Provide details about the AD application that you previously set up.



4. Click **Add**.

Result

You should now have an Azure NetApp Files working environment.



What's next?

Start creating and managing volumes.