Get started

Azure NetApp Files

NetApp
November 06, 2025

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 the NetApp Console

- Migrate NFS or SMB data to Azure NetApp Files directly from the NetApp Console. Data migrations are powered by NetApp Copy and Sync.

  Learn more about Copy and Sync

- Using Artificial Intelligence (AI) driven technology, NetApp Data Classification can help you understand data context and identify sensitive data that resides in your Azure NetApp Files accounts.

  Learn more about Data Classification

NetApp Console

Azure NetApp Files is accessible through the NetApp Console.

The NetApp Console provides centralized management of NetApp storage and data services across on-premises and cloud environments at enterprise grade. The Console is required to access and use NetApp data services. As a management interface, it enables you to manage many storage resources from one interface. Console administrators can control access to storage and services for all systems within the enterprise.

You don’t need a license or subscription to start using NetApp Console and you only incur charges when you need to deploy Console agents in your cloud to ensure connectivity to your storage systems or NetApp data services. However, some NetApp data services accessible from the Console are licensed or subscription-based.

Learn more about the NetApp Console.

Cost

View Azure NetApp Files pricing

Subscription and billing are maintained by the Azure NetApp Files service, not by the Console.

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 Console website: Azure NetApp Files
- Azure NetApp Files documentation
- Copy and Sync documentation

Getting started workflow

Get started with Azure NetApp Files by setting up a Microsoft Entra application and by creating a system.

Set up a Microsoft Entra application

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

Create an Azure NetApp Files system

From the Systems page in the NetApp Console, select **Add system** > **Microsoft Azure** > **Azure NetApp Files** then provide details about the Active Directory application.

Set up a Microsoft Entra application

The NetApp Console 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 a Microsoft Entra application and by obtaining the Azure credentials that the Console needs.

Step 1: Create the application

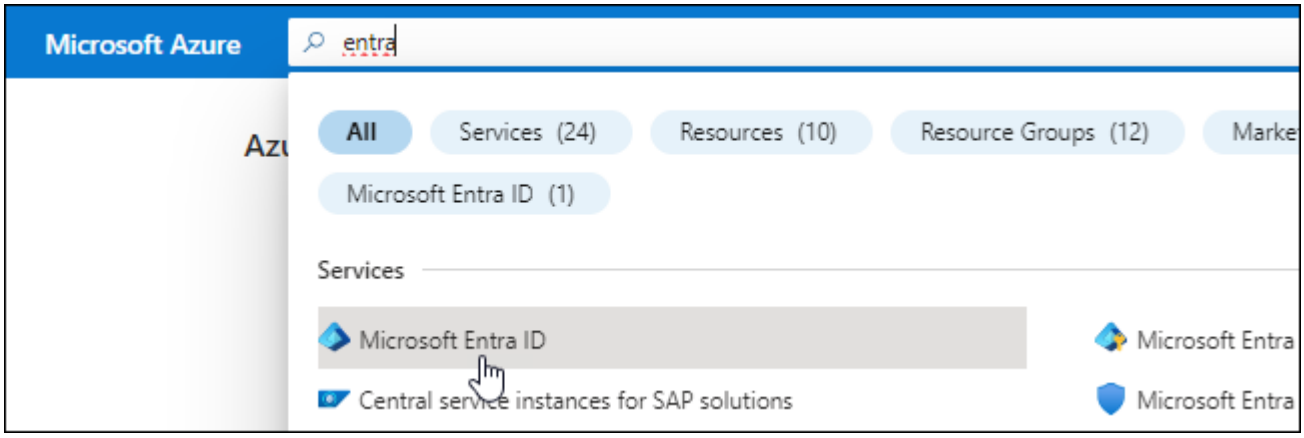
Create a Microsoft Entra application and service principal that the Console can use for role-based access control.

Before you begin

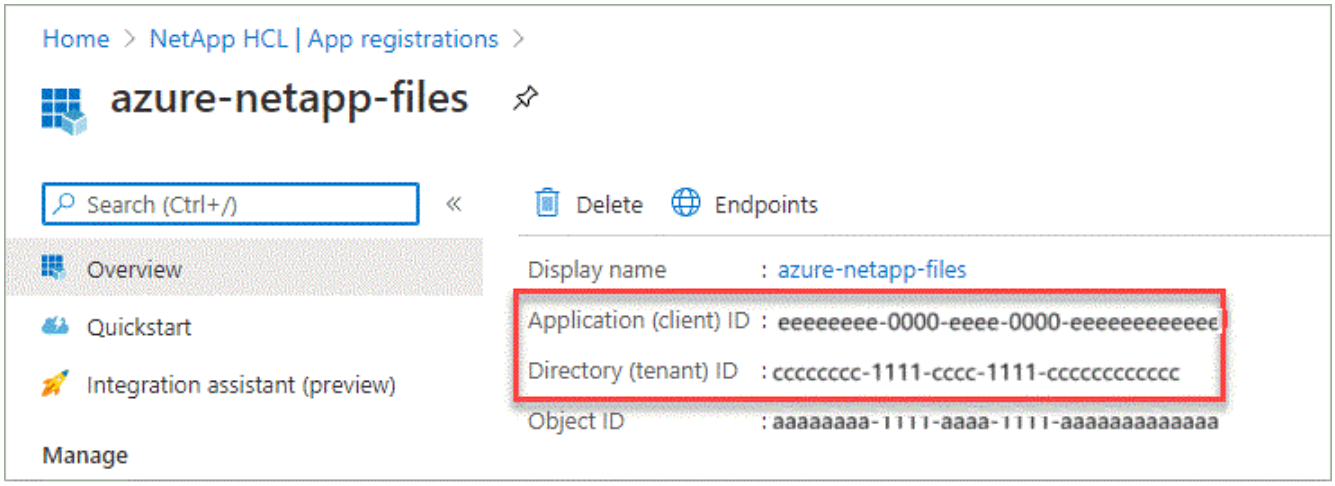
You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Required permissions.

Steps

1. From the Azure portal, open the **Microsoft Entra ID** service.

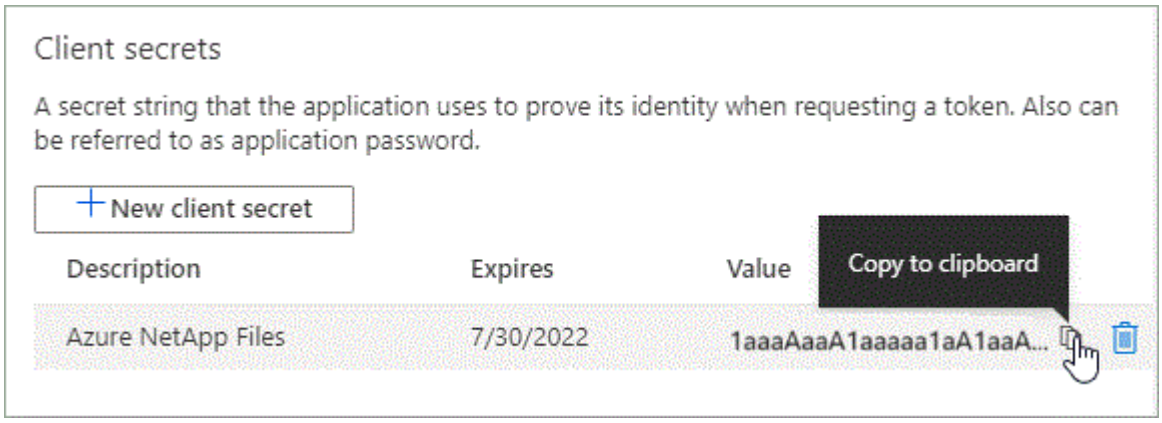


2. In the menu, select **App registrations**.
3. Create the application:
   a. Select **New registration**.
   b. Specify details about the application:
      - **Name**: Enter a name for the application.
      - **Account type**: Select an account type (any will work with the Console).
      - **Redirect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



When you create the Azure NetApp Files system in the Console, you need to provide the application (client) ID and the directory (tenant) ID for the application. The Console uses the IDs to programmatically sign in.

5. Create a client secret for the application so the Console can use it to authenticate with Microsoft Entra ID:
    a. Select **Certificates & secrets > New client secret**.
    b. Provide a description of the secret and a duration.
    c. Select **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 the Console when you add an Azure NetApp Files system.

Step 2: Assign the app to a role

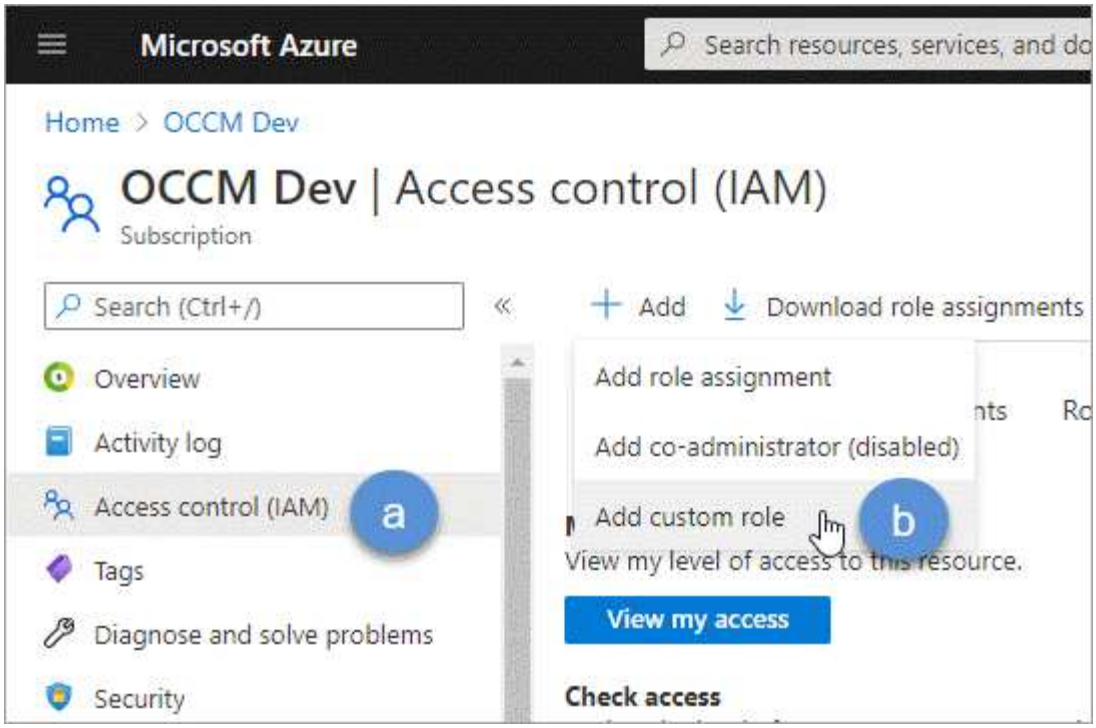
You must bind the service principal to your Azure subscription and assign it a custom role that has the required permissions.

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 select **Access control (IAM)**.
    b. Select **Add > Add custom role**.



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

d. Select **JSON** then **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.Network/virtualNetworks/subnets/read",
    "Microsoft.Insights/Metrics/Read"
    ],
```

f. Select **Save** > **Next** then **Create**.

2. Assign the application to the role that you just created:

a. From the Azure portal, open **Subscriptions**.

b. Select the subscription.

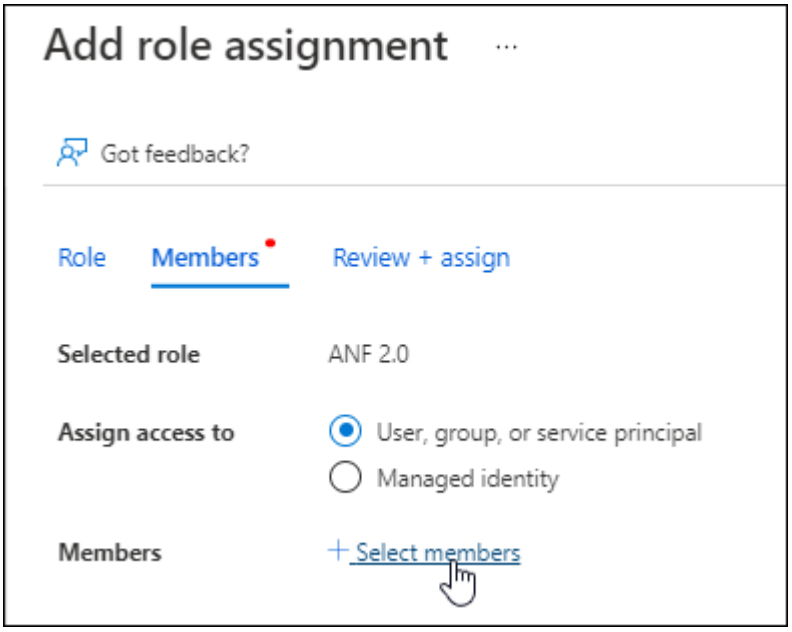
c. Select **Access control (IAM) > Add > Add role assignment**.

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

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

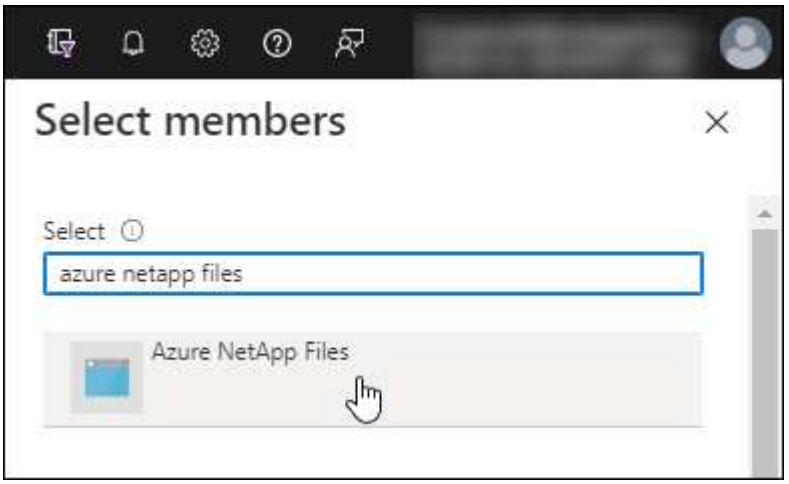
- Keep **User, group, or service principal** selected.

- Select **Select members**.



- Search for the name of the application.

  Here's an example:



- Select the application then **Select**.
- Select **Next**.

f. Select **Review + assign**.

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

Step 3: Add the credentials to the Console

When you create the Azure NetApp Files system, you're prompted to select the credentials associated with the service principal. You need to add these credentials to the Console before you create the system.

Steps

1. In the left navigation of the Console, select **Administration** > **Credentials**.
2. Select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Microsoft Azure > NetApp Console**.
   b. **Define Credentials**: Enter information about the Microsoft Entra service principal that grants the required permissions:
      - Client Secret
      - Application (client) ID
      - Directory (tenant) ID

      You should have captured this information when you created the AD application.
   c. **Review**: Confirm the details about the new credentials then select **Add**.

Create an Azure NetApp Files system in the NetApp Console

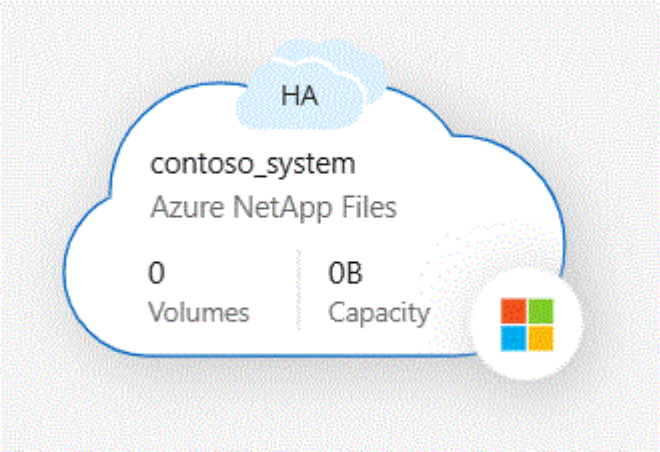
After you set up a Microsoft Entra application and add the credentials to the NetApp Console, create an Azure NetApp Files system so that you can start creating the volumes that you need.

Steps

1. From the Systems page, select **Add system**.
2. Select **Microsoft Azure**.
3. Next to Azure NetApp Files, select **Discover**.
4. On the Details page, enter a system name and select the credentials that you previously set up.
5. Select **Continue**.

Result

You now have an Azure NetApp Files system.



What's next?

Start creating and managing volumes.

Copyright information

Trademark information