



Get started

Azure NetApp Files

NetApp
February 11, 2024

This PDF was generated from <https://docs.netapp.com/us-en/blurxp-azure-netapp-files/concept-azure-netapp-files.html> on February 11, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Get started 1
 - Learn about Azure NetApp Files 1
 - Getting started workflow 2
 - Set up a Microsoft Entra application 2
 - Create an Azure NetApp Files working environment 6

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 BlueXP

- Migrate NFS or SMB data to Azure NetApp Files directly from BlueXP. Data migrations are powered by BlueXP copy and sync.

[Learn more about BlueXP copy and sync](#)

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

[Learn more about BlueXP classification](#)

Cost

[View Azure NetApp Files pricing](#)

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

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 BlueXP website: Azure NetApp Files](#)
- [Azure NetApp Files documentation](#)
- [BlueXP copy and sync documentation](#)

Getting started workflow

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

1

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.

2

Create an Azure NetApp Files working environment

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

Set up a Microsoft Entra application

BlueXP 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 BlueXP needs.

Step 1: Create the application

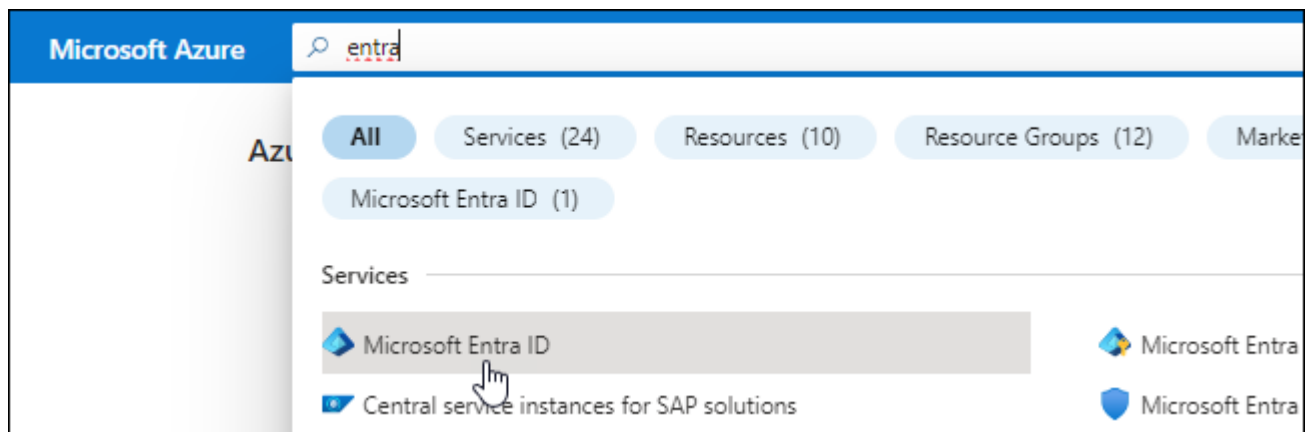
Create a Microsoft Entra application and service principal that BlueXP can use for role-based access control.

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.



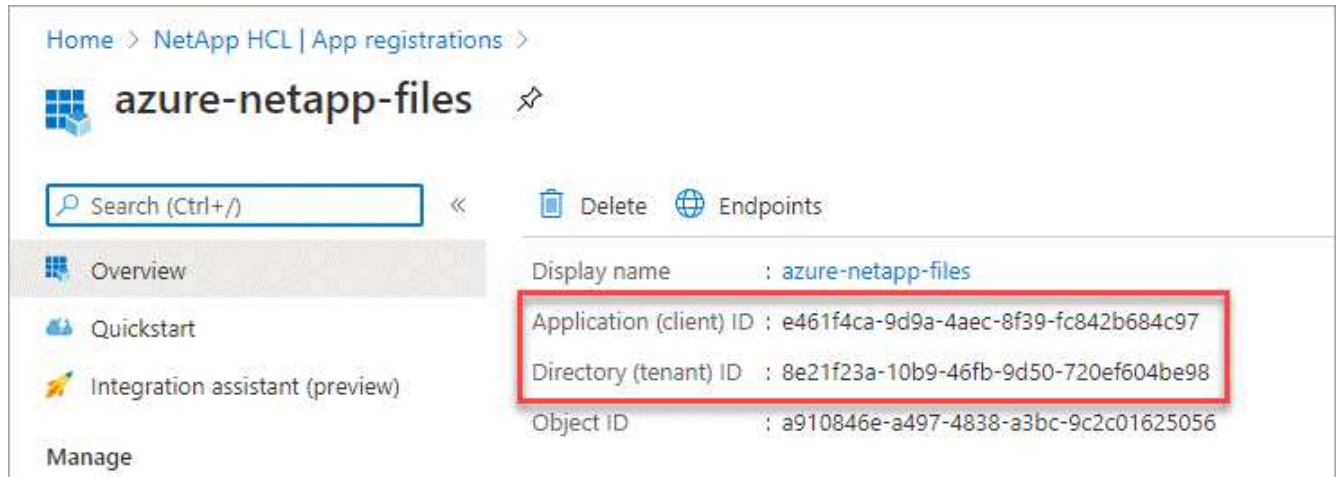
2. In the menu, click **App registrations**.
3. Create the application:
 - a. Click **New registration**.

b. Specify details about the application:

- **Name:** Enter a name for the application.
- **Account type:** Select an account type (any will work with BlueXP).
- **Redirect URI:** You can leave this blank.

c. Click **Register**.

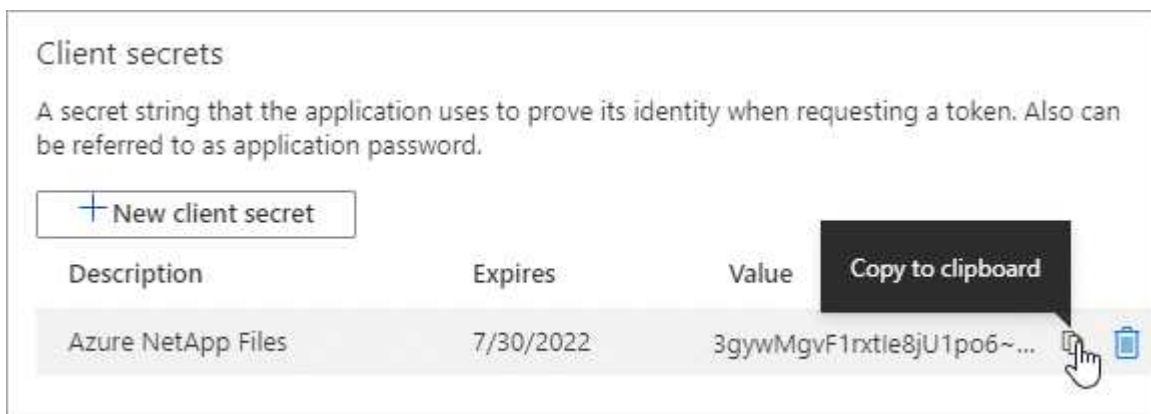
4. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



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

5. Create a client secret for the application so BlueXP can use it to authenticate with Microsoft Entra ID:

- Click **Certificates & secrets > New client secret**.
- Provide a description of the secret and a duration.
- Click **Add**.
- 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 BlueXP when you add an Azure NetApp Files working environment.

Step 2: Assign the app to a role

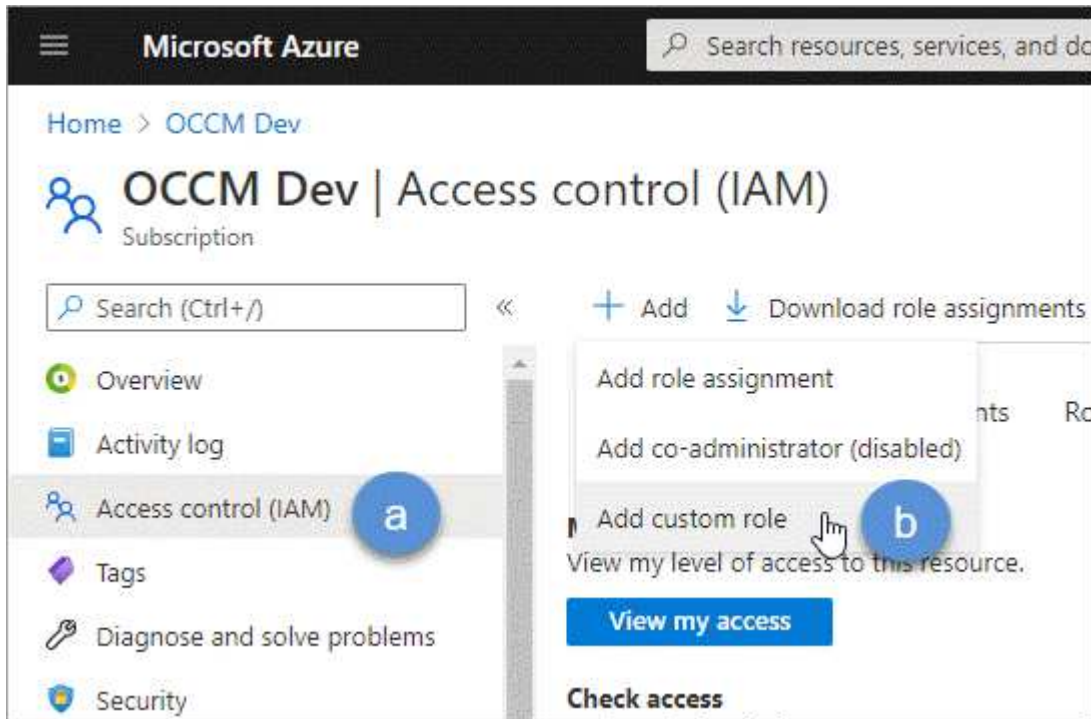
You must bind the service principal to your Azure subscription and assign it a custom role that has the required permissions.

Steps

1. [Create a custom role in Azure](#).

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

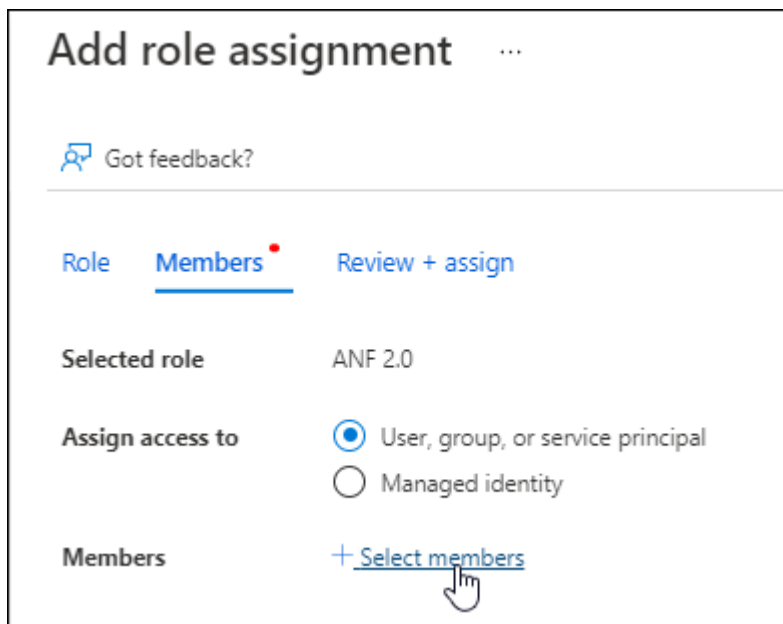
- a. Open the subscription and click **Access control (IAM)**.
- b. Click **Add > Add custom role**.



- 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*:

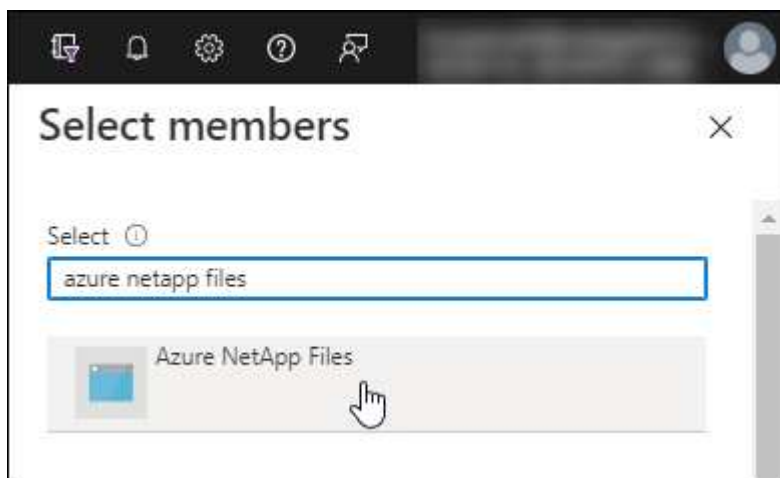
```
"actions": [  
  "Microsoft.NetApp/*",  
  "Microsoft.Resources/resources/read",  
  "Microsoft.Resources/subscriptions/resourceGroups/read",  
  
  "Microsoft.Resources/subscriptions/resourcegroups/resources/read",  
  "Microsoft.Resources/subscriptions/resourceGroups/write",  
  "Microsoft.Network/virtualNetworks/read",  
  "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 BlueXP now has the required Azure permissions for that subscription.

Step 3: Add the credentials to BlueXP

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

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.



2. Click **Add Credentials** and follow the steps in the wizard.
 - a. **Credentials Location:** Select **Microsoft Azure > BlueXP**.
 - 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 and click **Add**.

Create an Azure NetApp Files working environment

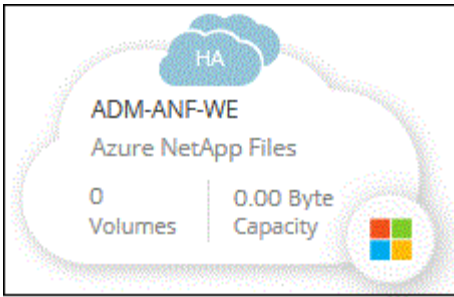
After you set up a Microsoft Entra application and add the credentials to BlueXP, create an Azure NetApp Files working environment so that you can start creating the volumes that you need.

Steps

1. From the Canvas page, click **Add Working Environment**.
2. Select **Microsoft Azure**.
3. Next to Azure NetApp Files, select **Discover**.
4. On the Details page, enter a working environment name and select the credentials that you previously set up.
5. Click **Continue**.

Result

You should now have an Azure NetApp Files working environment.



What's next?

[Start creating and managing volumes.](#)

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.