



Setting up and discovering Azure NetApp Files

Cloud Manager

Ben Cammett
June 30, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/task_manage_anf.html on July 20, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Setting up and discovering Azure NetApp Files 1
 - Quick start 1
 - Requesting access 1
 - Setting up an Azure AD application 1
 - Creating an Azure NetApp Files working environment 5

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.

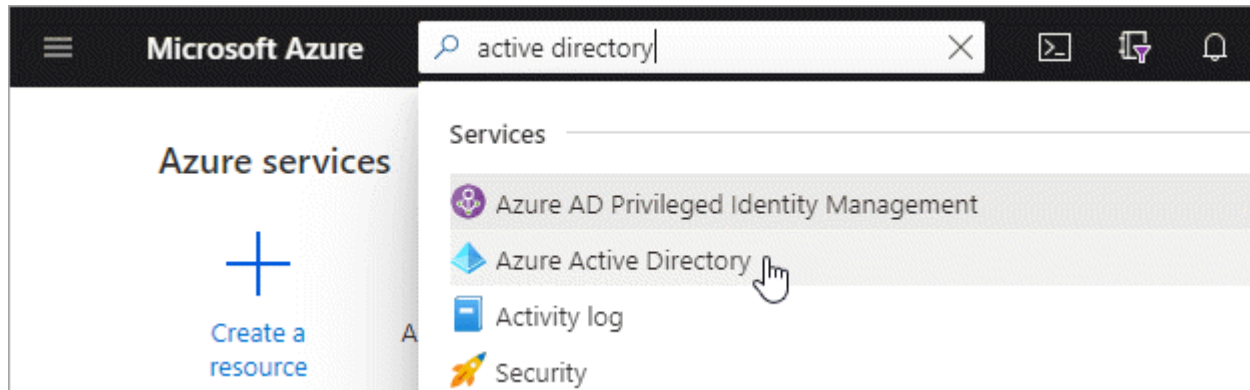
Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the

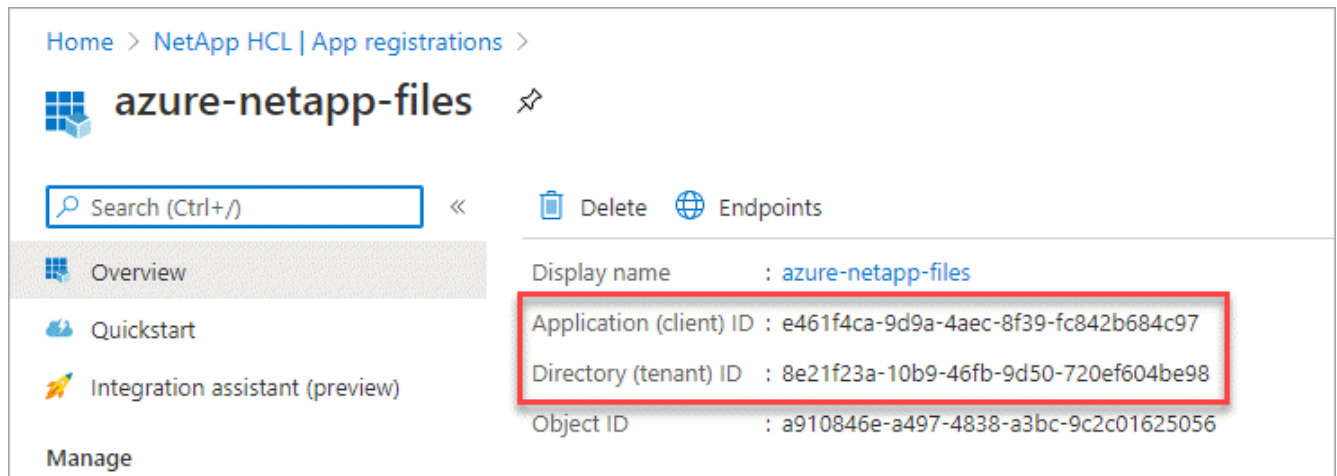
application to a role. For details, refer to [Microsoft Azure Documentation: Required permissions](#).

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Copy to clipboard
Azure NetApp Files	7/30/2022	3gywMgvF1rxtle8jU1po6~...	

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

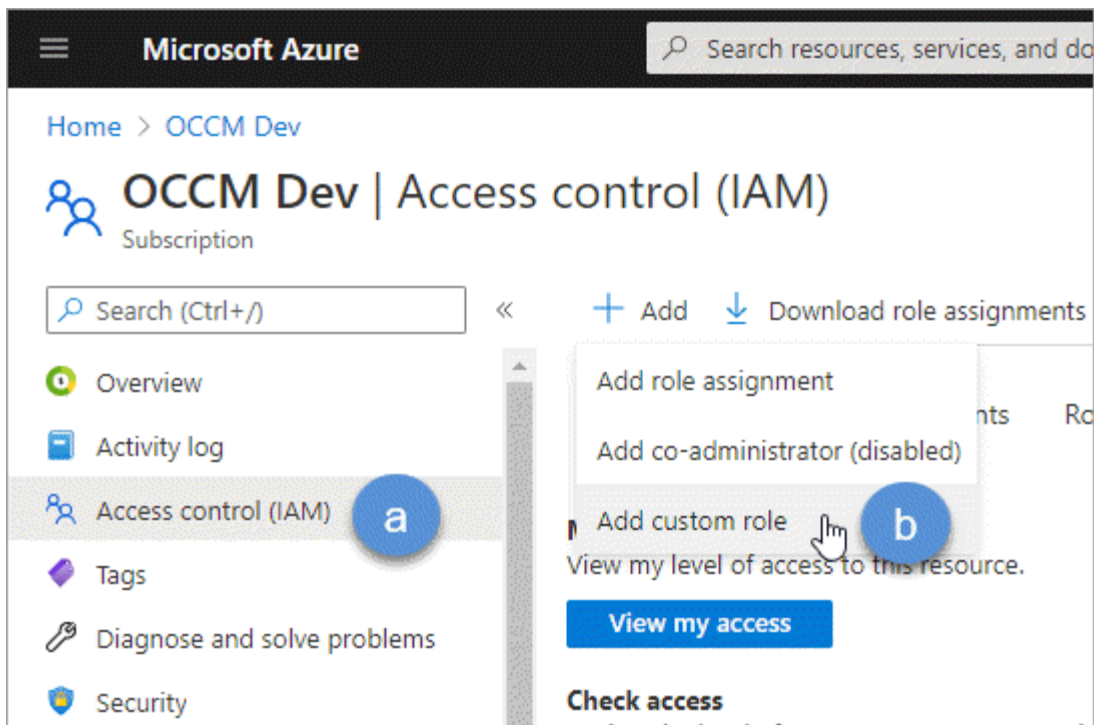
You must bind the service principal to your Azure subscription and assign it a custom role that has the required permissions.

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).

Add role assignment ×

Role ⓘ
ANF 2.0 ⓘ

Assign access to ⓘ
Azure AD user, group, or service principal

Select ⓘ
azure-netapp-files

azure-netapp-files

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.

Azure NetApp Files Credentials

Working Environment Name

ANF

Application (client) ID

e461f4ca-9d9a-4aec-8f39-fc842b684c97

Client Secret

.....

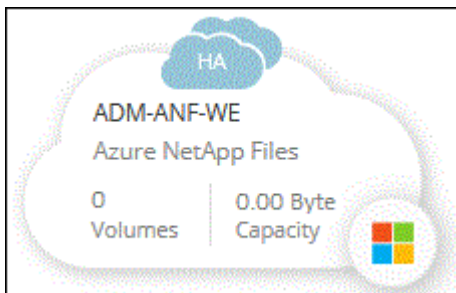
Directory (tenant) ID

8e21f23a-10b9-46fb-9d50-720ef604be98

4. Click **Add**.

Result

You should now have an Azure NetApp Files working environment.



What's next?

[Start creating and managing volumes.](#)

Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.