



## **Erste Schritte**

### Azure NetApp Files

NetApp  
November 06, 2025

# Inhalt

Erste Schritte . . . . .	1
Informationen zu Azure NetApp Files . . . . .	1
Features . . . . .	1
NetApp Console . . . . .	1
Kosten . . . . .	1
Unterstützte Regionen . . . . .	2
Hilfe bekommen . . . . .	2
Weiterführende Links . . . . .	2
Workflow „Erste Schritte“ . . . . .	2
Einrichten einer Microsoft Entra-Anwendung . . . . .	2
Schritt 1: Erstellen der Anwendung . . . . .	2
Schritt 2: Weisen Sie der App eine Rolle zu . . . . .	4
Schritt 3: Fügen Sie die Anmeldeinformationen zur Konsole hinzu . . . . .	6
Erstellen eines Azure NetApp Files Systems in der NetApp Console . . . . .	7

# Erste Schritte

## Informationen zu Azure NetApp Files

Azure NetApp Files ermöglicht es Unternehmen, ihre leistungsintensiven und latenzempfindlichen geschäftskritischen Kernanwendungen in Azure zu migrieren und dort auszuführen, ohne dass eine Umgestaltung für die Cloud erforderlich ist.

### Features

- Die Unterstützung mehrerer Protokolle ermöglicht die nahtlose Ausführung von Linux- und Windows-Anwendungen per „Lift & Shift“ in Azure.
- Mehrere Leistungsstufen ermöglichen eine genaue Abstimmung auf die Leistungsanforderungen der Arbeitslast.
- Führende Zertifizierungen, darunter SAP HANA, DSGVO und HIPAA, ermöglichen die Migration der anspruchsvollsten Workloads zu Azure.

### Zusätzliche Funktionen in der NetApp Console

- Migrieren Sie NFS- oder SMB-Daten direkt von der NetApp Console zu Azure NetApp Files . Datenmigrationen werden durch NetApp Copy and Sync unterstützt.

["Erfahren Sie mehr über Kopieren und Synchronisieren"](#)

- Mithilfe künstlicher Intelligenz (KI) kann Ihnen die NetApp Data Classification dabei helfen, den Datenkontext zu verstehen und vertrauliche Daten zu identifizieren, die sich in Ihren Azure NetApp Files -Konten befinden.

["Erfahren Sie mehr über die Datenklassifizierung"](#)

### NetApp Console

Auf Azure NetApp Files kann über die NetApp Console zugegriffen werden.

Die NetApp Console ermöglicht eine zentrale Verwaltung von NetApp -Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene. Die Konsole ist für den Zugriff auf und die Nutzung der NetApp -Datendienste erforderlich. Als Verwaltungsschnittstelle ermöglicht es Ihnen, viele Speicherressourcen über eine Schnittstelle zu verwalten. Konsolenadministratoren können den Zugriff auf Speicher und Dienste für alle Systeme innerhalb des Unternehmens steuern.

Sie benötigen weder eine Lizenz noch ein Abonnement, um die NetApp Console zu verwenden. Es fallen nur dann Kosten an, wenn Sie Konsolenagenten in Ihrer Cloud bereitstellen müssen, um die Konnektivität zu Ihren Speichersystemen oder NetApp -Datendiensten sicherzustellen. Einige NetApp -Datendienste, auf die über die Konsole zugegriffen werden kann, sind jedoch lizenzierte oder abonnementbasiert.

Erfahren Sie mehr über die["NetApp Console"](#) .

### Kosten

["Preise für Azure NetApp Files anzeigen"](#)

Abonnement und Abrechnung werden vom Azure NetApp Files Dienst verwaltet, nicht von der Konsole.

## Unterstützte Regionen

["Anzeigen der unterstützten Azure-Regionen"](#)

## Hilfe bekommen

Verwenden Sie bei technischen Supportproblemen im Zusammenhang mit Azure NetApp Files das Azure-Portal, um eine Supportanfrage an Microsoft zu senden. Wählen Sie Ihr zugehöriges Microsoft-Abonnement aus und wählen Sie unter **Speicher** den Dienstnamen \* Azure NetApp Files\* aus. Geben Sie die restlichen Informationen ein, die zum Erstellen Ihrer Microsoft-Supportanfrage erforderlich sind.

## Weiterführende Links

- ["NetApp Console -Konsolenwebsite: Azure NetApp Files"](#)
- ["Azure NetApp Files Dokumentation"](#)
- ["Dokumentation zum Kopieren und Synchronisieren"](#)

## Workflow „Erste Schritte“

Beginnen Sie mit Azure NetApp Files , indem Sie eine Microsoft Entra-Anwendung einrichten und ein System erstellen.

1

### ["Einrichten einer Microsoft Entra-Anwendung"](#)

Erteilen Sie von Azure aus Berechtigungen für eine Microsoft Entra-Anwendung und kopieren Sie die Anwendungs-ID (Client), die Verzeichnis-ID (Mandant) und den Wert eines Client-Geheimnisses.

2

### ["Erstellen eines Azure NetApp Files Systems"](#)

Wählen Sie auf der Seite „Systeme“ in der NetApp Console\*System hinzufügen\* > **Microsoft Azure** > \* Azure NetApp Files\* aus und geben Sie dann Details zur Active Directory-Anwendung ein.

## Einrichten einer Microsoft Entra-Anwendung

Die NetApp Console benötigt Berechtigungen zum Einrichten und Verwalten von Azure NetApp Files. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie eine Microsoft Entra-Anwendung erstellen und einrichten und die Azure-Anmeldeinformationen abrufen, die die Konsole benötigt.

### Schritt 1: Erstellen der Anwendung

Erstellen Sie eine Microsoft Entra-Anwendung und einen Dienstprinzipal, den die Konsole für die rollenbasierte Zugriffskontrolle verwenden kann.

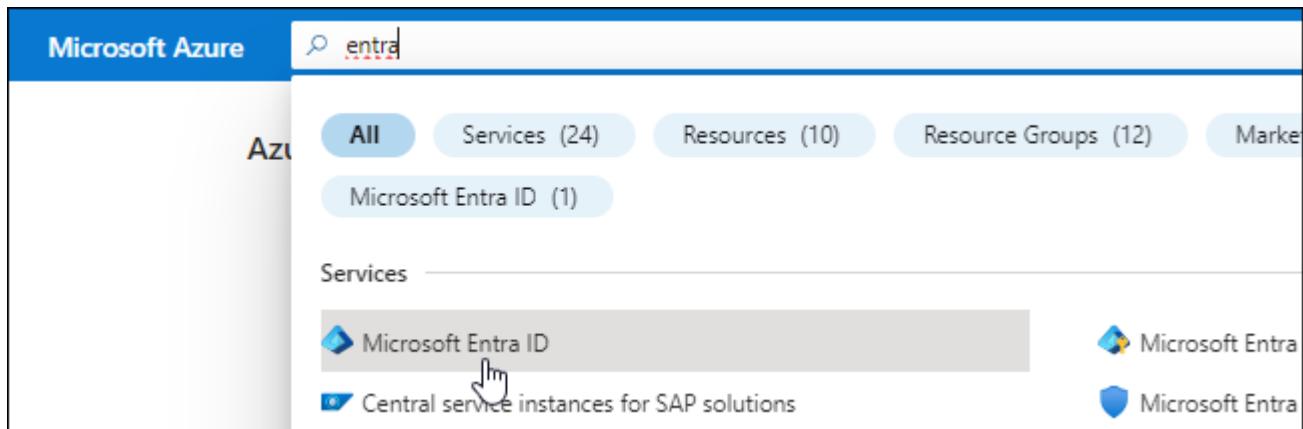
#### Bevor Sie beginnen

Sie müssen in Azure über die richtigen Berechtigungen verfügen, um eine Active Directory-Anwendung zu

erstellen und die Anwendung einer Rolle zuzuweisen. Weitere Einzelheiten finden Sie unter "["Microsoft Azure-Dokumentation: Erforderliche Berechtigungen"](#)" .

## Schritte

1. Öffnen Sie im Azure-Portal den Dienst **Microsoft Entra ID**.



The screenshot shows the Microsoft Azure portal interface. In the top navigation bar, the search bar contains the text "entra". Below the search bar, there are several filter buttons: "All", "Services (24)", "Resources (10)", "Resource Groups (12)", and "Marketplace". A single result, "Microsoft Entra ID (1)", is listed under the "Services" category. The result card for "Microsoft Entra ID" includes a blue icon, the service name, and a link to "Central service instances for SAP solutions". To the right of the main search area, there are two other service cards: "Microsoft Entra" and "Microsoft Entra".

2. Wählen Sie im Menü **App-Registrierungen** aus.

3. Erstellen Sie die Anwendung:

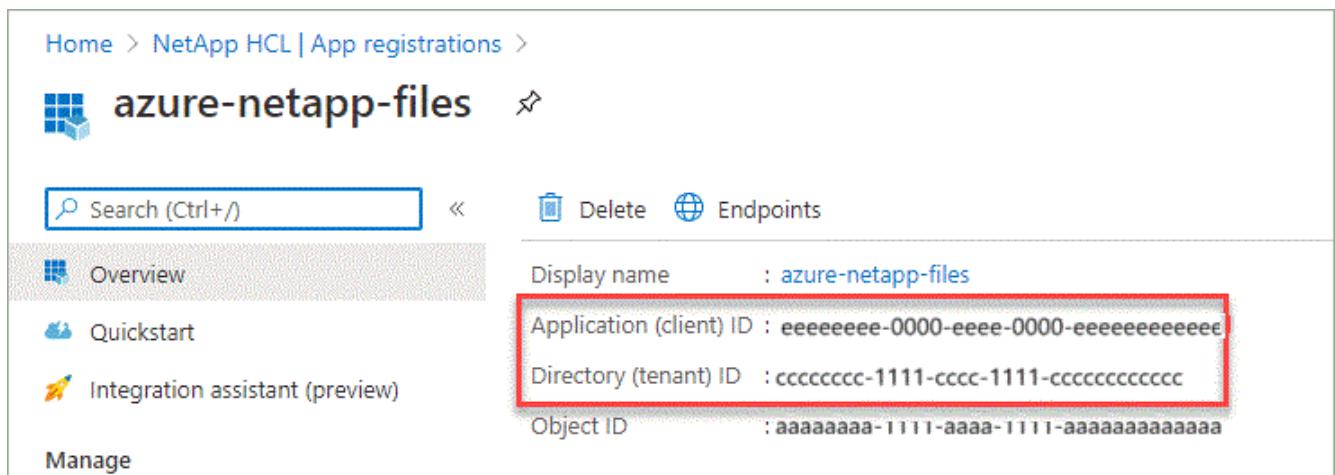
- a. Wählen Sie **Neuregistrierung**.

- b. Geben Sie Details zur Anwendung an:

- **Name:** Geben Sie einen Namen für die Anwendung ein.
- **Kontotyp:** Wählen Sie einen Kontotyp aus (alle funktionieren mit der Konsole).
- **Umleitungs-URI:** Sie können dieses Feld leer lassen.

- c. Wählen Sie **Registrieren**.

4. Kopieren Sie die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandant-ID)**.



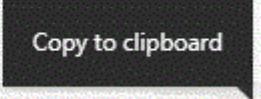
The screenshot shows the "App registrations" section of the Azure portal. The URL in the address bar is "Home > NetApp HCL | App registrations >". There is a search bar with the placeholder "Search (Ctrl+ /)". On the left, there is a sidebar with links: "Overview" (which is highlighted), "Quickstart", and "Integration assistant (preview)". On the right, there is a "Delete" button and an "Endpoints" link. Below these, there is a table with the following data:

Display name	:	azure-netapp-files
Application (client) ID	:	eeeeeeee-0000-e000-0000-eeeeeeeeeeee
Directory (tenant) ID	:	ccccccc-1111-cccc-1111-ccccccccccc
Object ID	:	aaaaaaaa-1111-aaaa-1111aaaaaaaaaa

The "Application (client) ID" and "Directory (tenant) ID" rows are highlighted with a red box.

Wenn Sie das Azure NetApp Files -System in der Konsole erstellen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. Die Konsole verwendet die IDs zur programmgesteuerten Anmeldung.

5. Erstellen Sie ein Client-Geheimnis für die Anwendung, damit die Konsole es zur Authentifizierung mit der Microsoft Entra-ID verwenden kann:
  - a. Wählen Sie **Zertifikate und Geheimnisse > Neues Clientgeheimnis**.
  - b. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
  - c. Wählen Sie **Hinzufügen**.
  - d. Kopieren Sie den Wert des Client-Geheimnisses.

Description	Expires	Value
Azure NetApp Files	7/30/2022	1aaaAaaA1aaaaa1aA1aaA...  

## Ergebnis

Ihre AD-Anwendung ist jetzt eingerichtet und Sie sollten die Anwendungs-ID (Client-ID), die Verzeichnis-ID (Mandanten-ID) und den Wert des Client-Geheimnisses kopiert haben. Sie müssen diese Informationen in der Konsole eingeben, wenn Sie ein Azure NetApp Files -System hinzufügen.

## Schritt 2: Weisen Sie der App eine Rolle zu

Sie müssen den Dienstprinzipal an Ihr Azure-Abonnement binden und ihm eine benutzerdefinierte Rolle mit den erforderlichen Berechtigungen zuweisen.

### Schritte

1. ["Erstellen einer benutzerdefinierten Rolle in Azure"](#) .

Die folgenden Schritte beschreiben, wie Sie die Rolle über das Azure-Portal erstellen.

- a. Öffnen Sie das Abonnement und wählen Sie **Zugriffskontrolle (IAM)**.
- b. Wählen Sie **Hinzufügen > Benutzerdefinierte Rolle hinzufügen**.

- Geben Sie auf der Registerkarte **Grundlagen** einen Namen und eine Beschreibung für die Rolle ein.
- Wählen Sie **JSON** und dann **Bearbeiten**, das oben rechts im JSON-Format angezeigt wird.
- Fügen Sie unter **Aktionen** die folgenden Berechtigungen hinzu:

```

"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"
],
  
```

- Wählen Sie **Speichern > Weiter** und dann **Erstellen**.
- Weisen Sie der Anwendung die Rolle zu, die Sie gerade erstellt haben:
    - Öffnen Sie im Azure-Portal **Abonnements**.
    - Wählen Sie das Abonnement aus.
    - Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
    - Wählen Sie auf der Registerkarte **Rolle** die benutzerdefinierte Rolle aus, die Sie erstellt haben, und klicken Sie dann auf **Weiter**.
    - Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

- Behalten Sie die Auswahl von **Benutzer, Gruppe oder Dienstprinzipal** bei.
- Wählen Sie **Mitglieder auswählen**.

Add role assignment ...

Role Members \* Review + assign

Selected role ANF 2.0

Assign access to  User, group, or service principal  Managed identity

Members [+ Select members](#)

- Suchen Sie nach dem Namen der Anwendung.

Hier ist ein Beispiel:

Select members

Select ⓘ

azure netapp files

Azure NetApp Files

- Wählen Sie die Anwendung aus und klicken Sie dann auf **Auswählen**.
- Wählen Sie **Weiter**.
  - a. Wählen Sie **Überprüfen + zuweisen**.

Der Dienstprinzipal für die Konsole verfügt jetzt über die erforderlichen Azure-Berechtigungen für dieses Abonnement.

### Schritt 3: Fügen Sie die Anmeldeinformationen zur Konsole hinzu

Wenn Sie das Azure NetApp Files -System erstellen, werden Sie aufgefordert, die mit dem Dienstprinzipal verknüpften Anmeldeinformationen auszuwählen. Sie müssen diese Anmeldeinformationen zur Konsole

hinzufügen, bevor Sie das System erstellen.

#### Schritte

1. Wählen Sie in der linken Navigationsleiste der Konsole **Administration > Anmeldeinformationen** aus.
2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten des Assistenten.
  - a. **Speicherort der Anmeldeinformationen:** Wählen Sie **Microsoft Azure > NetApp Console**.
  - b. **Anmeldeinformationen definieren:** Geben Sie Informationen zum Microsoft Entra-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:
    - Client-Geheimnis
    - Anwendungs-ID (Client-ID)
    - Verzeichnis-ID (Mandant)
  - c. **Überprüfen:** Bestätigen Sie die Details zu den neuen Anmeldeinformationen und wählen Sie dann **Hinzufügen**.

Sie sollten diese Informationen erfasst haben, als Sie [die AD-Anwendung erstellt](#).

## Erstellen eines Azure NetApp Files Systems in der NetApp Console

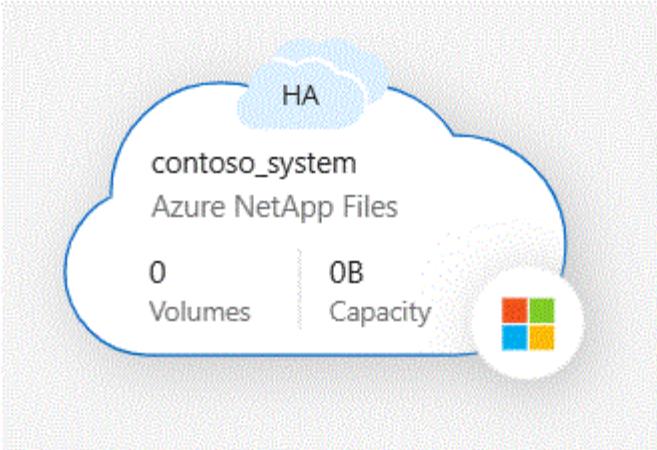
Nachdem Sie eine Microsoft Entra-Anwendung eingerichtet und die Anmeldeinformationen zur NetApp Console hinzugefügt haben, erstellen Sie ein Azure NetApp Files -System, damit Sie mit der Erstellung der benötigten Volumes beginnen können.

#### Schritte

1. Wählen Sie auf der Seite „Systeme“ die Option „System hinzufügen“ aus.
2. Wählen Sie **Microsoft Azure** aus.
3. Wählen Sie neben Azure NetApp Files die Option **Discover** aus.
4. Geben Sie auf der Seite „Details“ einen Systemnamen ein und wählen Sie die Anmeldeinformationen aus, die Sie zuvor eingerichtet haben.
5. Wählen Sie **Weiter**.

#### Ergebnis

Sie verfügen jetzt über ein Azure NetApp Files System.



### Wie geht es weiter?

"Beginnen Sie mit der Erstellung und Verwaltung von Volumes" .

## **Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

**ERLÄUTERUNG ZU „RESTRICTED RIGHTS“:** Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## **Markeninformationen**

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.