



# **Azure Zugangsdaten**

## **Set up and administration**

NetApp

January 05, 2023

# Inhaltsverzeichnis

- Azure Zugangsdaten ..... 1
  - Azure Zugangsdaten und Berechtigungen. .... 1
  - Verwalten von Azure-Anmeldeinformationen und -Abonnements für BlueXP ..... 3

# Azure Zugangsdaten

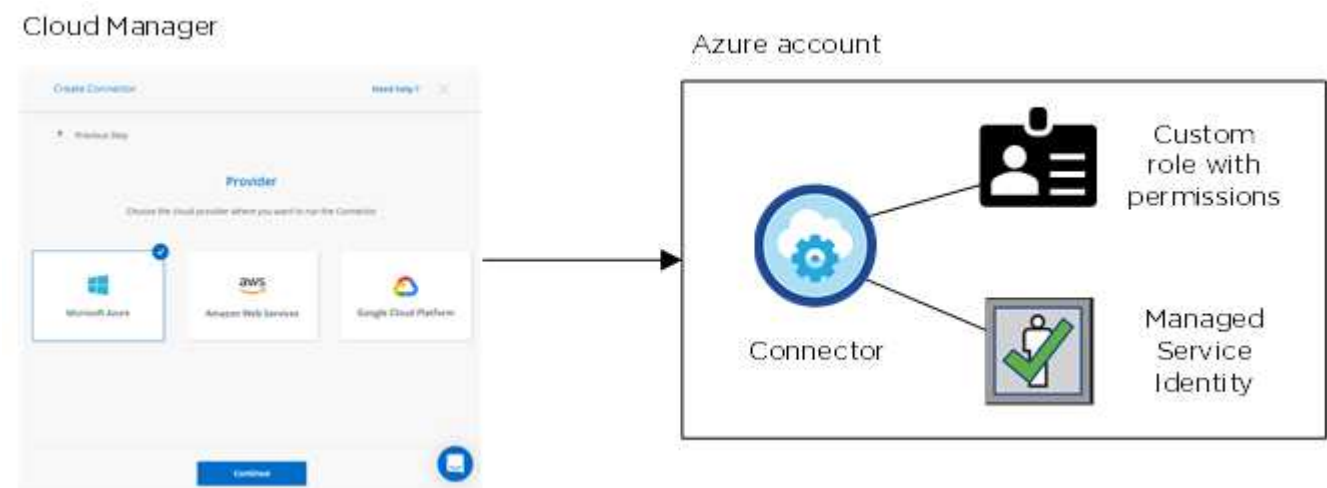
## Azure Zugangsdaten und Berechtigungen

Mit BlueXP können Sie die für die Bereitstellung von Cloud Volumes ONTAP verwendeten Azure Zugangsdaten auswählen. Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

### Erste Azure Zugangsdaten

Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie ein Azure-Konto oder einen Service-Principal verwenden, der über die Berechtigungen zum Bereitstellen der virtuellen Connector-Maschine verfügt. Die erforderlichen Berechtigungen werden im aufgeführt ["Connector-Implementierungsrichtlinie für Azure"](#).

Wenn BlueXP die Connector Virtual Machine in Azure implementiert, wird damit ein aktiviert ["Vom System zugewiesene verwaltete Identität"](#) Erstellt auf einer virtuellen Maschine eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Diese Rolle bietet BlueXP die Berechtigungen, die für das Management von Ressourcen und Prozessen innerhalb des Azure Abonnements erforderlich sind. ["Überprüfen Sie, wie BlueXP die Berechtigungen verwendet"](#).



Bei der Erstellung einer neuen Arbeitsumgebung für Cloud Volumes ONTAP wählt BlueXP die folgenden Azure-Anmeldedaten standardmäßig aus:

Details & Credentials			
Managed Service Ide...	OCCM QA1	<span>ⓘ</span> No subscription is associated	<a href="#">Edit Credentials</a>
Credential Name	Azure Subscription	Marketplace Subscription	

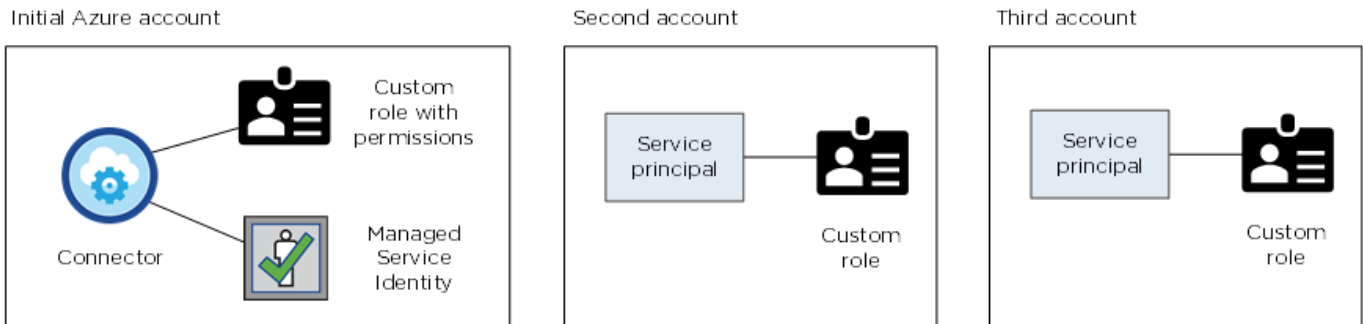
### Zusätzliche Azure-Abonnements für eine gemanagte Identität

Die verwaltete Identität ist mit dem Abonnement verbunden, in dem Sie den Connector gestartet haben. Wenn

Sie ein anderes Azure Abonnement auswählen möchten, müssen Sie es ausführen ["Verknüpfen Sie die verwaltete Identität mit diesen Abonnements"](#).

## Zusätzliche Azure Zugangsdaten

Wenn Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten implementieren möchten, müssen Sie die erforderlichen Berechtigungen von erteilen ["Erstellen und Einrichten eines Service Principal in Azure Active Directory"](#) Für jedes Azure Konto. Das folgende Bild zeigt zwei zusätzliche Konten, die jeweils mit einer Dienstprinzipal- und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



Das würden Sie dann tun ["Fügen Sie die Kontoanmeldeinformationen zu BlueXP hinzu"](#) Durch Angabe von Details zum AD-Dienstprinzipal.

Nachdem Sie einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:

The screenshot shows the 'Edit Account & Add Subscription' form. The 'Credentials' section is highlighted, showing a dropdown menu with the following options:

- cloud-manager-app | Application ID: 57c42424-88a0-480a.
- Managed Service Identity** (selected)
- OCCM QA1 (Default)

## Wie sieht es mit Marketplace-Implementierungen und On-Premises-Implementierungen aus?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Connector beschrieben, der aus BlueXP stammt. Sie können auch einen Connector in Azure über die bereitstellen "[Azure Marketplace](#)", Und Sie können "[Installieren Sie den Steckverbinder vor Ort](#)".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die verwaltete Identität für den Connector manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Für On-Premises-Bereitstellungen können Sie keine verwaltete Identität für den Connector einrichten, aber Sie können Berechtigungen wie bei zusätzlichen Konten mit einem Service-Principal bereitstellen.

## Verwalten von Azure-Anmeldeinformationen und -Abonnements für BlueXP

Wenn Sie ein Cloud Volumes ONTAP-System erstellen, müssen Sie die Azure-Anmeldedaten auswählen, die mit diesem System verwendet werden sollen. Sie müssen auch ein Marketplace-Abonnement wählen, wenn Sie Pay-as-you-go-Lizenzen verwenden. Folgen Sie den Schritten auf dieser Seite, wenn Sie mehrere Azure Zugangsdaten oder mehrere Azure Marketplace Abonnements für Cloud Volumes ONTAP verwenden möchten.

Es gibt zwei Möglichkeiten, in BlueXP zusätzliche Azure-Abonnements und Anmeldedaten hinzuzufügen.

1. Verknüpfen Sie zusätzliche Azure-Abonnements mit der von Azure verwalteten Identität.
2. Wenn Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten bereitstellen möchten, erteilen Sie Azure Berechtigungen unter Verwendung eines Service-Principal und fügen dessen Zugangsdaten BlueXP hinzu.

### Verknüpfen weiterer Azure-Abonnements mit einer gemanagten Identität

Mit BlueXP können Sie die Azure Zugangsdaten und das Azure Abonnement auswählen, in dem Sie Cloud Volumes ONTAP bereitstellen möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "[Verwaltete Identität](#)" Mit diesen Abonnements.

#### Über diese Aufgabe

Eine verwaltete Identität ist "[Zunächst das Azure-Konto](#)" Wenn Sie einen Connector von BlueXP bereitstellen. Wenn Sie den Connector bereitgestellt haben, hat BlueXP die Rolle BlueXP Operator erstellt und der virtuellen Connector-Maschine zugewiesen.

#### Schritte

1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Klicken Sie auf **Access Control (IAM)**.

a. Klicken Sie auf **Hinzufügen > Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:

- Wählen Sie die Rolle **BlueXP Operator** aus.



BlueXP Operator ist der Standardname, der in der Connector-Richtlinie angegeben ist. Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einer **virtuellen Maschine** Zugriff zu.
- Wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde.
- Wählen Sie die virtuelle Verbindungsmaschine aus.
- Klicken Sie Auf **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

### Ergebnis

Wenn Sie eine neue Arbeitsumgebung erstellen, sollten Sie nun über mehrere Azure-Abonnements für das verwaltete Identitätsprofil verfügen.

**Edit Account & Add Subscription**

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

*No subscription is associated with this account*

### Hinzufügen zusätzlicher Azure Zugangsdaten zu BlueXP

Wenn Sie einen Connector von BlueXP bereitstellen, aktiviert BlueXP eine vom System zugewiesene verwaltete Identität auf der virtuellen Maschine, die über die erforderlichen Berechtigungen verfügt. BlueXP wählt diese Azure-Anmeldedaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen.



Ein erster Satz von Anmeldeinformationen wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. ["Informationen zu Azure Zugangsdaten und Berechtigungen"](#).

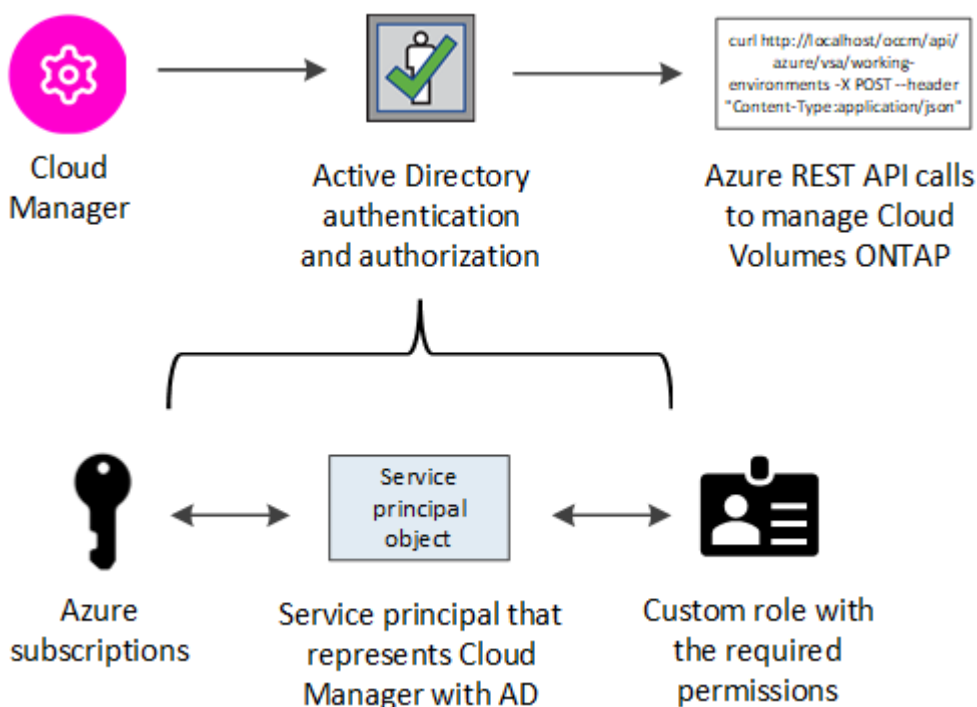
Wenn Sie Cloud Volumes ONTAP mit *different* Azure Zugangsdaten bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure Konto einen Service-Principal in Azure Active Directory erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zu BlueXP hinzufügen.

### Azure-Berechtigungen über einen Service-Principal gewähren

Für Aktionen in Azure benötigt BlueXP Berechtigungen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Service-Principal in Azure Active Directory erstellen und einrichten, sowie die für BlueXP erforderlichen Azure Zugangsdaten erhalten.

#### Über diese Aufgabe

Die folgende Abbildung zeigt, wie BlueXP Berechtigungen zur Durchführung von Operationen in Azure erhält. Ein Service-Principal-Objekt, das an ein oder mehrere Azure-Abonnements gebunden ist, repräsentiert BlueXP in Azure Active Directory und wird einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen zulässt.



#### Schritte

1. Erstellen Sie eine Azure Active Directory-Anwendung.
2. Anwendung einer Rolle zuweisen.
3. Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.
4. Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.
5. Erstellen Sie einen Clientschlüssel.

## Erstellen einer Azure Active Directory-Anwendung

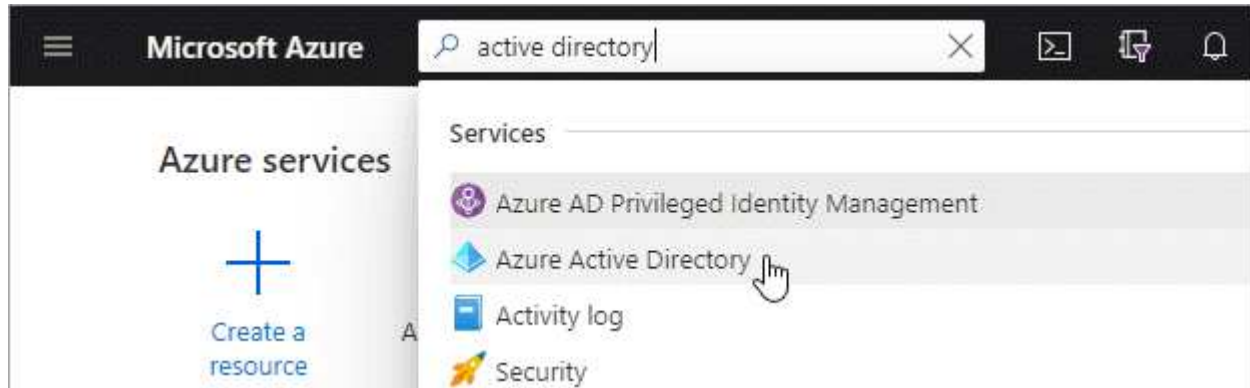
Erstellen Sie eine Applikation und einen Service-Principal für Azure Active Directory (AD), die BlueXP für die rollenbasierte Zugriffssteuerung verwenden kann.

### Bevor Sie beginnen

Sie müssen über die richtigen Berechtigungen in Azure verfügen, um eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen. Weitere Informationen finden Sie unter "[Microsoft Azure-Dokumentation: Erforderliche Berechtigungen](#)".

### Schritte

1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



2. Klicken Sie im Menü auf **App-Registrierungen**.
3. Klicken Sie auf **Neue Registrierung**.
4. Geben Sie Details zur Anwendung an:
  - **Name:** Geben Sie einen Namen für die Anwendung ein.
  - **Kontotyp:** Wählen Sie einen Kontotyp aus (jeder kann mit BlueXP verwendet werden).
  - **Redirect URI:** Sie können dieses Feld leer lassen.
5. Klicken Sie Auf **Registrieren**.

### Ergebnis

Sie haben die AD-Anwendung und den Service-Principal erstellt.

### Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „BlueXP Operator“ zuweisen, damit BlueXP über Berechtigungen in Azure verfügt.

### Schritte

1. Erstellen einer benutzerdefinierten Rolle:
  - a. Kopieren Sie den Inhalt des "[Benutzerdefinierte Rollenberechtigungen für den Konnektor](#)" Und speichern Sie sie in einer JSON-Datei.
  - b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.



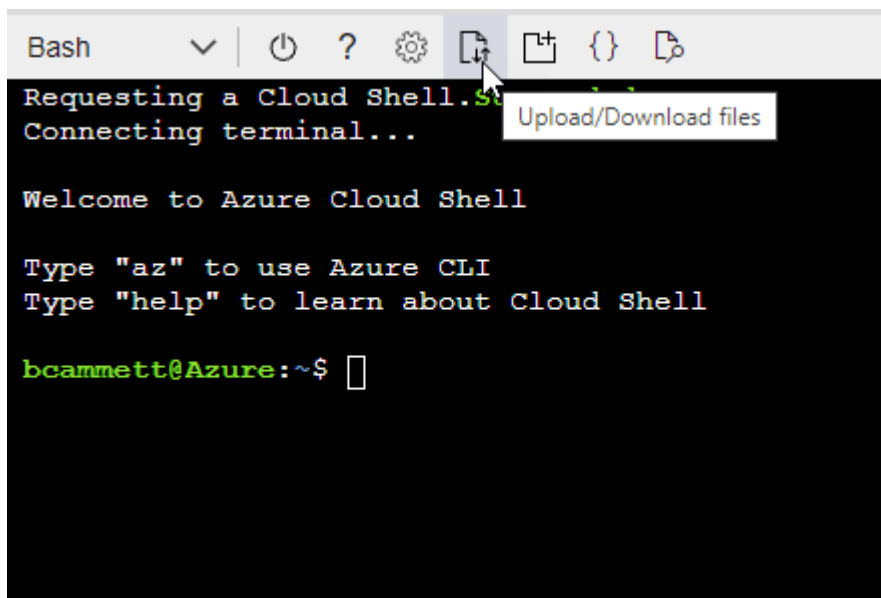
## Beispiel

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

In den folgenden Schritten wird beschrieben, wie die Rolle mithilfe von Bash in Azure Cloud Shell erstellt wird.

- Starten "Azure Cloud Shell" Und wählen Sie die Bash-Umgebung.
- Laden Sie die JSON-Datei hoch.



- Geben Sie den folgenden Befehl der Azure CLI ein:

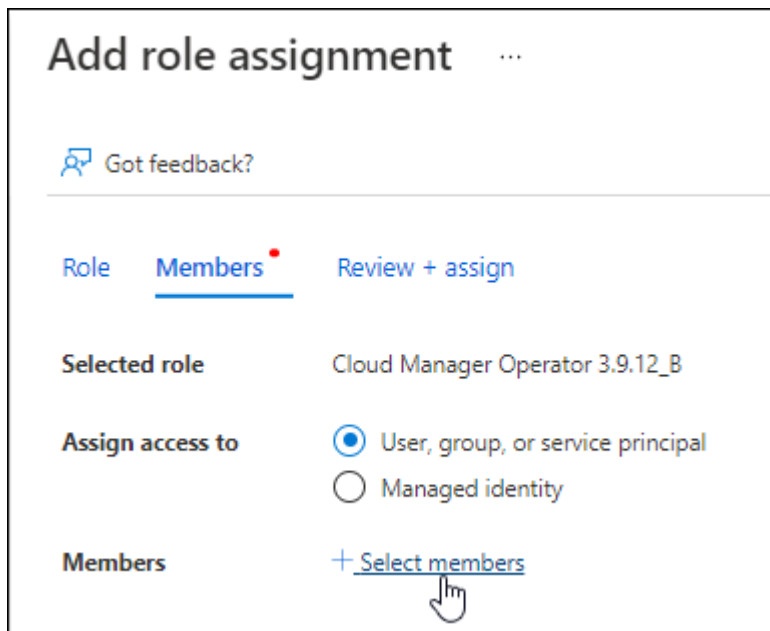
```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

Sie sollten nun eine benutzerdefinierte Rolle namens BlueXP Operator haben, die Sie der virtuellen Connector-Maschine zuweisen können.

## 2. Applikation der Rolle zuweisen:

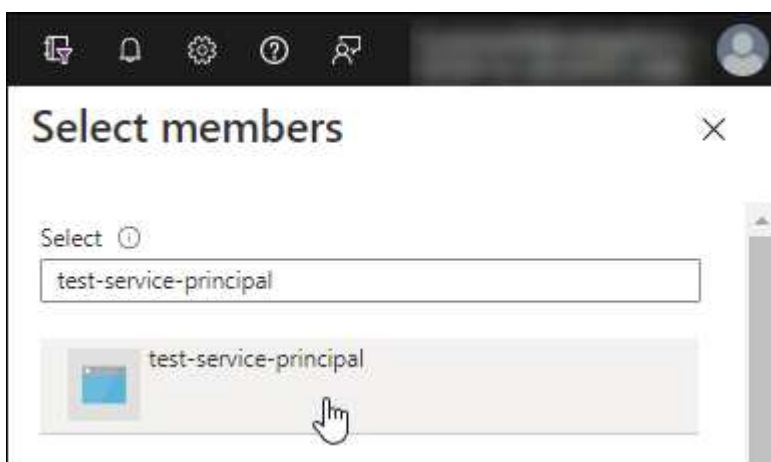
- Öffnen Sie im Azure-Portal den Service **Abonnements**.
- Wählen Sie das Abonnement aus.
- Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte \* Role\* die Rolle **BlueXP Operator** aus und klicken Sie auf **Next**.
- Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

- **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.
- Klicken Sie auf **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



- Wählen Sie die Anwendung aus und klicken Sie auf **Auswählen**.
- Klicken Sie Auf **Weiter**.

f. Klicken Sie auf **Review + Assign**.

Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Prinzipal an jedes dieser Subscriptions binden. Mit BlueXP können Sie das Abonnement auswählen, das Sie bei der Bereitstellung von Cloud Volumes ONTAP verwenden möchten.

## Windows Azure Service Management-API-Berechtigungen werden hinzugefügt

Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

### Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Klicken Sie auf **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.













### Request API permissions

Select an API

Microsoft APIs   **APIs my organization uses**   My APIs

#### Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 <b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	 <b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	 <b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 <b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios	 <b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server	 <b>Azure Import/Export</b> Programmatic control of import/export jobs
 <b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
 <b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 <b>Customer Insights</b> Create profile and interaction models for your products	 <b>Data Export Service for Microsoft Dynamics 365</b> Export data from Microsoft Dynamics CRM organization to an external destination

4. Klicken Sie auf **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann auf **Berechtigungen hinzufügen**.

## Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

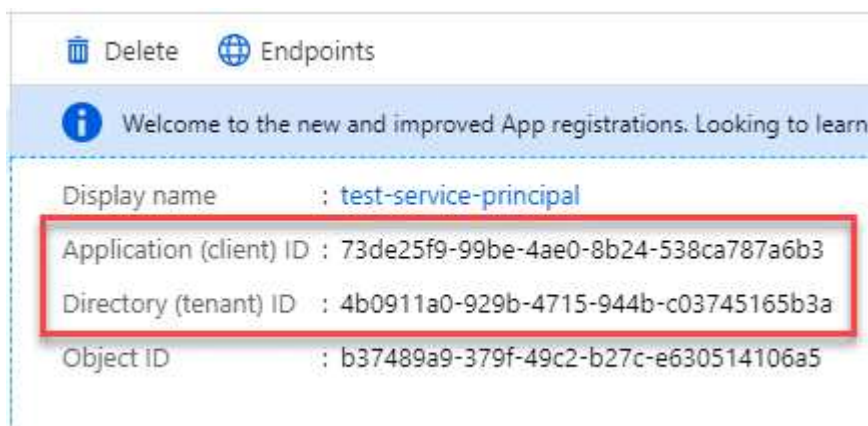
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

## Abrufen der Anwendungs-ID und der Verzeichnis-ID

Wenn Sie das Azure-Konto zu BlueXP hinzufügen, müssen Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) für die Anwendung angeben. BlueXP verwendet die IDs, um sich programmatisch anzumelden.

### Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) ID**.



## Erstellen eines Clientgeheimnisses

Sie müssen ein Clientgeheimnis erstellen und dann BlueXP den Wert des Geheimnisses zur Verfügung stellen, damit BlueXP es zur Authentifizierung mit Azure AD nutzen kann.

### Schritte

1. Öffnen Sie den Dienst **Azure Active Directory**.
2. Klicken Sie auf **App-Registrierungen** und wählen Sie Ihre Anwendung aus.

3. Klicken Sie auf **Zertifikate & Geheimnisse > Neuer Client Secret**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Klicken Sie Auf **Hinzufügen**.
6. Kopieren Sie den Wert des Clientgeheimnisses.

#### 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.

<a href="#">+ New client secret</a>			
DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	<a href="#">Copy to clipboard</a>

### Ergebnis

Ihr Service-Principal ist jetzt eingerichtet und Sie sollten die Anwendungs- (Client-)ID, die Verzeichnis- (Mandanten-)ID und den Wert des Clientgeheimnisses kopiert haben. Sie müssen diese Informationen in BlueXP eingeben, wenn Sie ein Azure-Konto hinzufügen.

### Hinzufügen der Anmeldeinformationen zu BlueXP

Nachdem Sie ein Azure-Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie die Anmeldedaten für dieses Konto bei BlueXP hinzufügen. Durch diesen Schritt können Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten starten.

#### Bevor Sie beginnen

Falls Sie diese Zugangsdaten gerade bei Ihrem Cloud-Provider erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

#### Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. ["Erfahren Sie, wie"](#).

#### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und befolgen Sie die Schritte im Assistenten.
  - a. **Anmeldeort:** Wählen Sie **Microsoft Azure > Connector**.
  - b. **Anmeldedaten definieren:** Geben Sie Informationen über den Azure Active Directory Service Principal ein, der die erforderlichen Berechtigungen erteilt:
    - Anwendungs-ID (Client): Siehe [Abrufen der Anwendungs-ID und der Verzeichnis-ID](#).
    - Verzeichnis-ID (Mandant): Siehe [Abrufen der Anwendungs-ID und der Verzeichnis-ID](#).

- Client Secret: Siehe [Erstellen eines Clientgeheimnisses](#).
- c. **Marketplace-Abonnement:** Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

Damit Sie für Cloud Volumes ONTAP mit einem stündlichen Tarif (PAYGO) bezahlen können, müssen diese Azure Zugangsdaten einem Abonnement im Azure Marketplace zugeordnet sein.

- d. **Review:** Bestätigen Sie die Angaben zu den neuen Anmeldedaten und klicken Sie auf **Hinzufügen**.

## Ergebnis

Auf der Seite Details und Anmeldeinformationen können Sie nun zu verschiedenen Anmeldeinformationen wechseln "[Beim Erstellen einer neuen Arbeitsumgebung](#)"

The screenshot shows a web interface titled "Edit Account & Add Subscription". Below the title is a section labeled "Credentials". Inside this section is a dropdown menu. The dropdown is open, showing several options. The top option is "cloud-manager-app | Application ID: 57c42424-88a0-480a...". Below it, the option "Managed Service Identity" is highlighted in blue. At the bottom of the dropdown, the selected option "OCCM QA1 (Default)" is visible with a downward arrow icon.

## Vorhandene Anmeldedaten verwalten

Verwalten Sie die Azure-Anmeldedaten, die Sie BlueXP bereits hinzugefügt haben, indem Sie ein Marketplace-Abonnement zuordnen, Anmeldedaten bearbeiten und löschen.

## Verknüpfen eines Azure Marketplace Abonnements mit den Zugangsdaten

Nachdem Sie Ihre Azure Zugangsdaten zu BlueXP hinzugefügt haben, können Sie diesen Anmeldedaten ein Azure Marketplace Abonnement zuordnen. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement verknüpfen können, nachdem Sie BlueXP bereits die Zugangsdaten hinzugefügt haben:

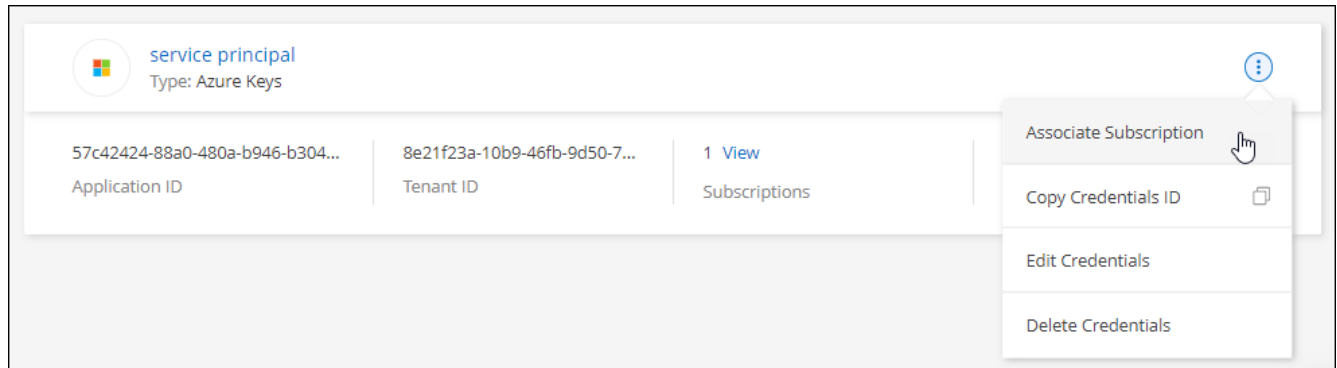
- Sie haben ein Abonnement nicht zugeordnet, wenn Sie die Anmeldeinformationen zu BlueXP hinzugefügt haben.
- Sie möchten ein vorhandenes Azure Marketplace Abonnement durch ein neues Abonnement ersetzen.

## Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "[Erfahren Sie, wie](#)".

## Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für eine Reihe von Anmeldeinformationen und wählen Sie dann **Abonnement verknüpfen**.



3. Wählen Sie ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

Das folgende Video beginnt im Kontext des Assistenten zur Arbeitsumgebung, zeigt Ihnen aber den gleichen Workflow, nachdem Sie auf **Abonnement hinzufügen** geklickt haben:

► [https://docs.netapp.com/de-de/cloud-manager-setup-admin//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/de-de/cloud-manager-setup-admin//media/video_subscribing_azure.mp4)

(video)

## Anmeldedaten werden bearbeitet

Bearbeiten Sie Ihre Azure-Anmeldedaten in BlueXP, indem Sie die Details zu Ihren Azure-Serviceanmeldeinformationen ändern. Sie müssen beispielsweise den Clientschlüssel aktualisieren, wenn ein neues Geheimnis für die Service-Hauptanwendung erstellt wurde.

### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für eine Reihe von Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die gewünschten Änderungen vor und klicken Sie dann auf **Anwenden**.

## Anmeldedaten werden gelöscht

Wenn Sie keine Anmeldedaten mehr benötigen, können Sie diese aus BlueXP löschen. Sie können nur Anmeldeinformationen löschen, die nicht mit einer Arbeitsumgebung verknüpft sind.

### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für einen Satz von Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen löschen**.
3. Klicken Sie zur Bestätigung auf **Löschen**.



## Copyright-Informationen

Copyright © 2022 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 BESCHRÄNKT 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, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT 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 IRGEND EINER 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.