



## **Azure**

### **Setup and administration**

NetApp  
April 26, 2024

# Inhalt

- Azure ..... 1
  - Informationen zu Azure Zugangsdaten und Berechtigungen ..... 1
  - Azure Zugangsdaten und Marketplace-Abonnements für BlueXP managen ..... 4

# Azure

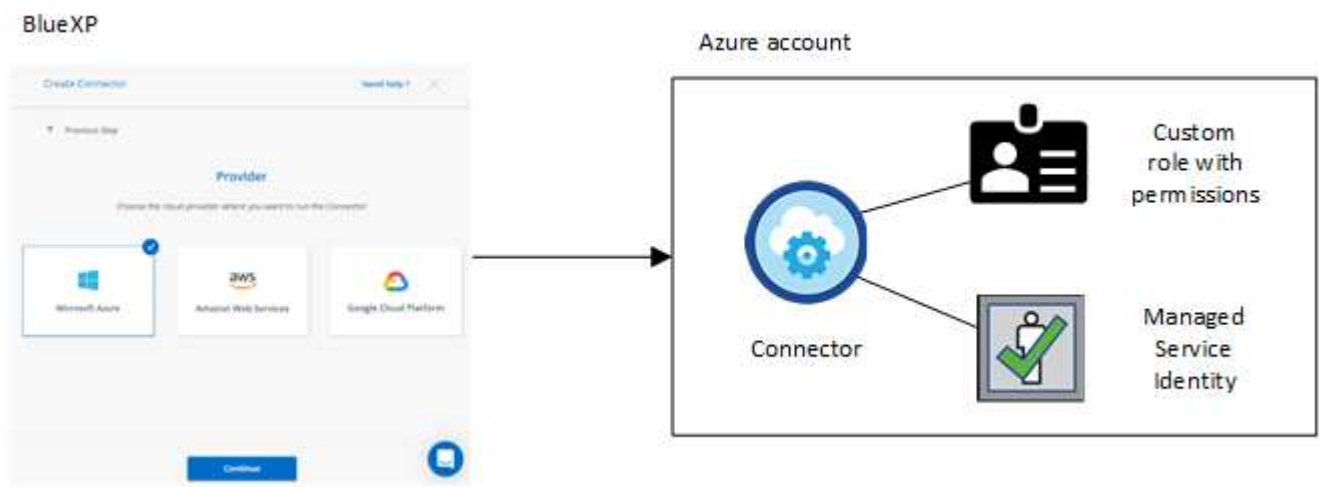
## Informationen zu Azure Zugangsdaten und Berechtigungen

Informieren Sie sich, wie BlueXP für Sie Azure Zugangsdaten verwendet, um Aktionen durchzuführen und wie diese Zugangsdaten mit Marketplace-Abonnements verknüpft sind. Das Verständnis dieser Details kann hilfreich sein, wenn Sie die Anmeldedaten für ein oder mehrere Azure-Abonnements verwalten. Beispielsweise könnte es hilfreich sein, wenn Sie mehr über Azure Zugangsdaten zu BlueXP erfahren möchten.

### 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"](#).



Wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen, wählt BlueXP standardmäßig diese Azure Zugangsdaten 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	

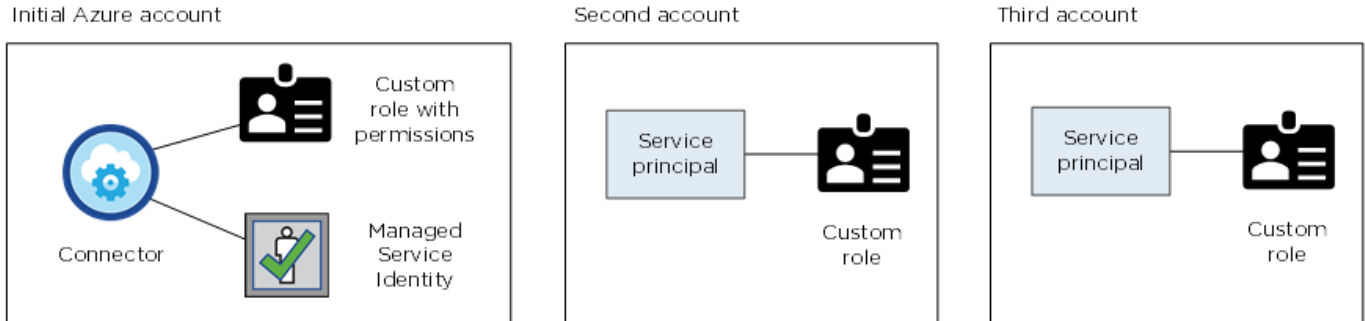
Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

## Zusätzliche Azure-Abonnements für eine gemanagte Identität

Die der Konnektor-VM zugewiesene, vom System zugewiesene verwaltete Identität ist mit dem Abonnement verknüpft, 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 unterschiedliche Azure-Anmeldedaten für BlueXP verwenden möchten, müssen Sie die erforderlichen Berechtigungen bis erteilen ["Erstellen und Einrichten eines Dienstprincipals in Microsoft Entra ID"](#) 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.

Sie können beispielsweise beim Erstellen einer neuen Cloud Volumes ONTAP-Arbeitsumgebung zwischen den Anmeldedaten wechseln:

The screenshot shows the 'Edit Account & Add Subscription' dialog. Under the 'Credentials' section, there is a dropdown menu. The first option is 'cloud-manager-app | Application ID: 57c42424-88a0-480a...'. The second option, 'Managed Service Identity', is highlighted in blue. Below it, 'OCCM QA1 (Default)' is visible with a downward arrow.

## Anmeldedaten und Abonnements für den Marktplatz

Die Zugangsdaten, die Sie zu einem Connector hinzufügen, müssen mit einem Azure Marketplace Abonnement verbunden sein, sodass Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO) oder über einen Jahresvertrag zahlen und andere BlueXP Services nutzen können.

["Lesen Sie, wie Sie ein Azure-Abonnement zuordnen"](#).

Beachten Sie Folgendes zu Azure Zugangsdaten und Marketplace-Abonnements:

- Sie können nur ein Azure Marketplace Abonnement mit einem Satz von Azure Zugangsdaten verknüpfen
- Sie können ein bestehendes Marketplace-Abonnement durch ein neues Abonnement ersetzen

## Häufig gestellte Fragen

Die folgende Frage bezieht sich auf Anmeldeinformationen und Abonnements.

### **Kann ich das Azure Marketplace Abonnement für Cloud Volumes ONTAP-Arbeitsumgebungen ändern?**

Ja, können Sie. Mit Änderung des Abonnements für Azure Marketplace für bestimmte Azure Zugangsdaten werden alle bestehenden und neuen Cloud Volumes ONTAP-Arbeitsumgebungen mit dem neuen Abonnement abgerechnet.

["Lesen Sie, wie Sie ein Azure-Abonnement zuordnen"](#).

### **Kann ich mehrere Azure Zugangsdaten mit jeweils unterschiedlichen Marketplace-Abonnements hinzufügen?**

Alle Azure Zugangsdaten, die zum selben Azure Abonnement gehören, werden mit demselben Azure Marketplace Abonnement verknüpft.

Wenn Sie mehrere Azure-Anmeldeinformationen haben, die zu verschiedenen Azure-Abonnements gehören, können diese Anmeldeinformationen demselben Azure Marketplace Abonnement oder verschiedenen Marketplace-Abonnements zugeordnet werden.

### **Kann ich vorhandene Cloud Volumes ONTAP-Arbeitsumgebungen auf ein anderes Azure Abonnement verschieben?**

Nein, es ist nicht möglich, die Azure Ressourcen, die Ihrer Cloud Volumes ONTAP-Arbeitsumgebung zugeordnet sind, in ein anderes Azure Abonnement zu verschieben.

### **Wie funktionieren Anmeldedaten für Marketplace-Implementierungen und On-Premises-Implementierungen?**

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Connector beschrieben, der aus BlueXP stammt. Sie können einen Connector auch in Azure über den Azure Marketplace implementieren und die Connector-Software auf Ihrem eigenen Linux-Host installieren.

Wenn Sie den Marketplace verwenden, können Sie Berechtigungen bereitstellen, indem Sie der Connector-VM und einer vom System zugewiesenen verwalteten Identität eine benutzerdefinierte Rolle zuweisen oder ein Microsoft Entra-Dienstprincipal verwenden.

Für On-Premises-Bereitstellungen können Sie keine verwaltete Identität für den Connector einrichten, aber Sie können Berechtigungen mithilfe eines Dienstprincipals bereitstellen.

Weitere Informationen zum Einrichten von Berechtigungen finden Sie auf den folgenden Seiten:

- Standardmodus
  - ["Richten Sie Berechtigungen für eine Azure Marketplace-Implementierung ein"](#)

- "Richten Sie Berechtigungen für On-Premises-Implementierungen ein"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

## Azure Zugangsdaten und Marketplace-Abonnements für BlueXP managen

Hinzufügen und Managen von Azure-Anmeldeinformationen, um zu ermöglichen, dass BlueXP über die erforderlichen Berechtigungen zum Implementieren und Managen von Cloud-Ressourcen in Ihren Azure Abonnements verfügt. Wenn Sie mehrere Azure Marketplace-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen Azure Zugangsdaten zuweisen.

Folgen Sie den Schritten auf dieser Seite, wenn Sie mehrere Azure Zugangsdaten oder mehrere Azure Marketplace Abonnements für Cloud Volumes ONTAP verwenden möchten.

### Überblick

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.

### Zuordnen zusätzlicher Azure-Abonnements zu 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. Wählen Sie **Access Control (IAM)**.
  - a. Wählen Sie **Hinzufügen > Rollenzuweisung 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.
- Wählen Sie **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*

## Zusätzliche Azure Zugangsdaten zu BlueXP hinzufügen

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-Anmeldeinformationen 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-Anmeldeinformationen bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure-Konto einen Dienstprinzipal in der Microsoft Entra-ID erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zu

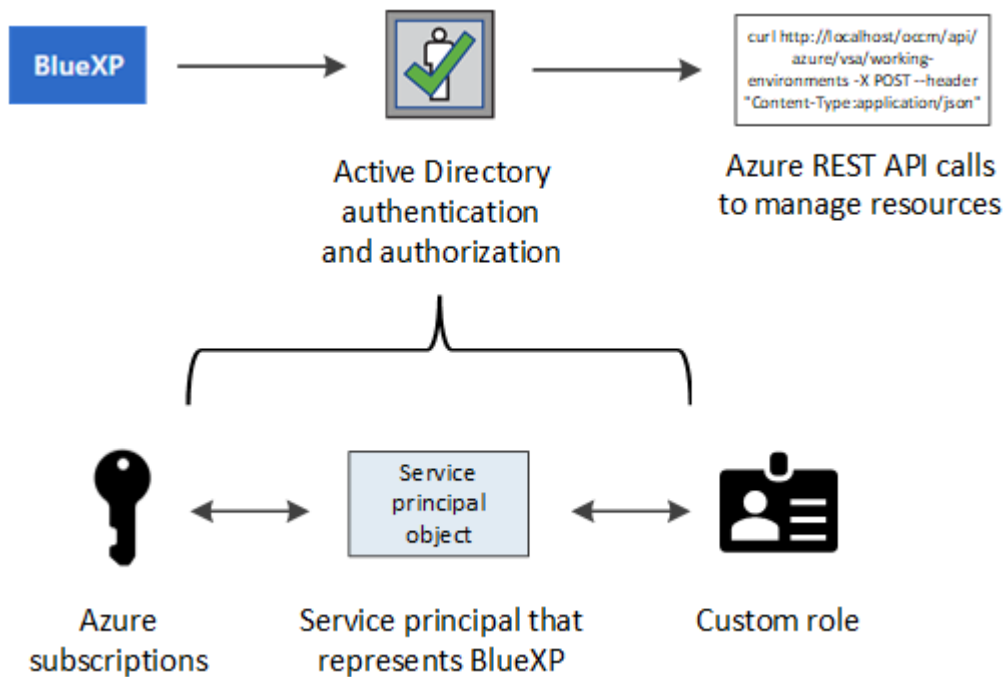
BlueXP hinzufügen.

## Erteilen Sie Azure Berechtigungen mithilfe eines Service-Prinzips

Für Aktionen in Azure benötigt BlueXP Berechtigungen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie in der Microsoft Entra-ID einen Service-Principal erstellen und einrichten und 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 der Microsoft Entra ID und wird einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen erlaubt.



### Schritte

1. Erstellen Sie eine Microsoft Entra-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 Sie eine Microsoft Entra-Anwendung

Erstellen Sie ein Microsoft Entra-Applikations- und Serviceprinzip, das BlueXP für die rollenbasierte Zugriffssteuerung verwenden kann.

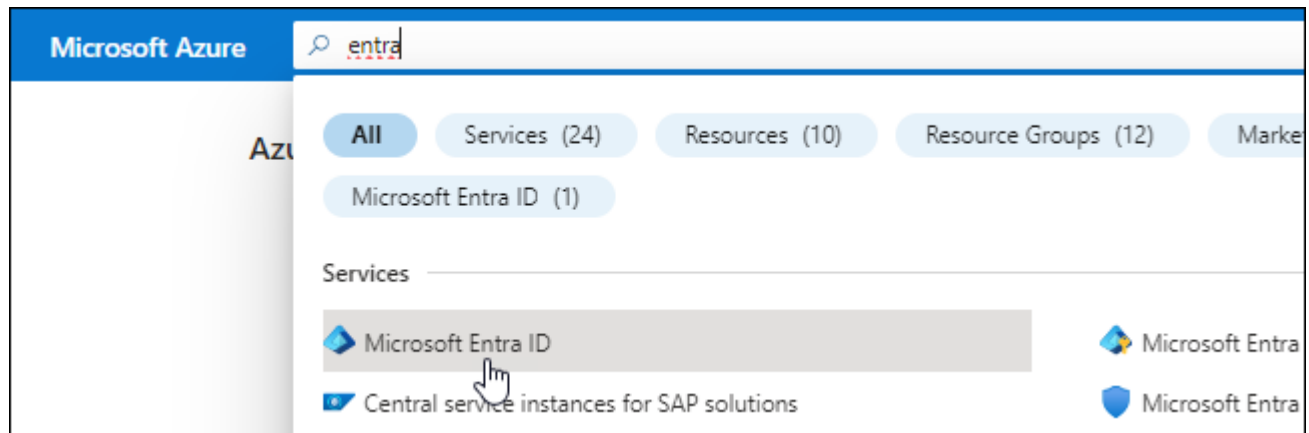
### Schritte

1. Stellen Sie sicher, dass Sie in Azure über die Berechtigungen zum Erstellen einer Active Directory-Anwendung und zum Zuweisen der Anwendung zu einer Rolle verfügen.

Weitere Informationen finden Sie unter "[Microsoft Azure-Dokumentation: Erforderliche Berechtigungen](#)"



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



3. Wählen Sie im Menü **App-Registrierungen**.

4. Wählen Sie **Neue Registrierung**.

5. 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.

6. Wählen Sie **Registrieren**.

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

## 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:

Beachten Sie, dass Sie eine benutzerdefinierte Azure-Rolle über das Azure-Portal, Azure PowerShell, Azure CLI oder REST-API erstellen können. Die folgenden Schritte zeigen, wie Sie die Rolle mithilfe der Azure-CLI erstellen. Wenn Sie eine andere Methode verwenden möchten, finden Sie weitere Informationen unter "[Azure-Dokumentation](#)"

- 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.

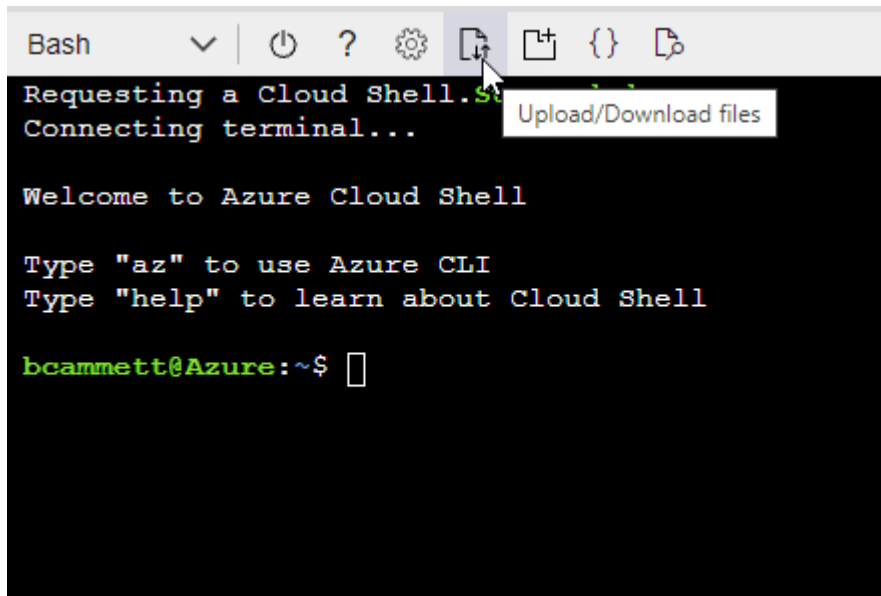
## Beispiel

```
"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.



- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

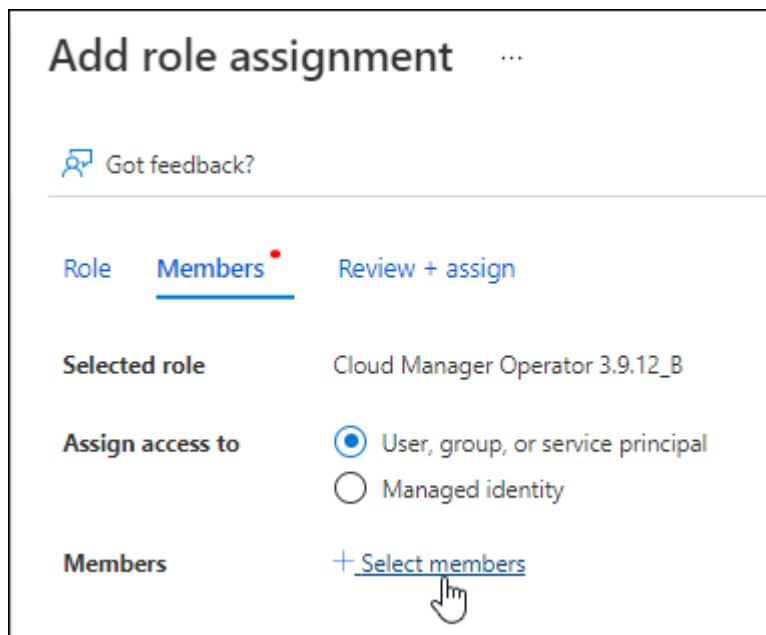
```
az role definition create --role-definition Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

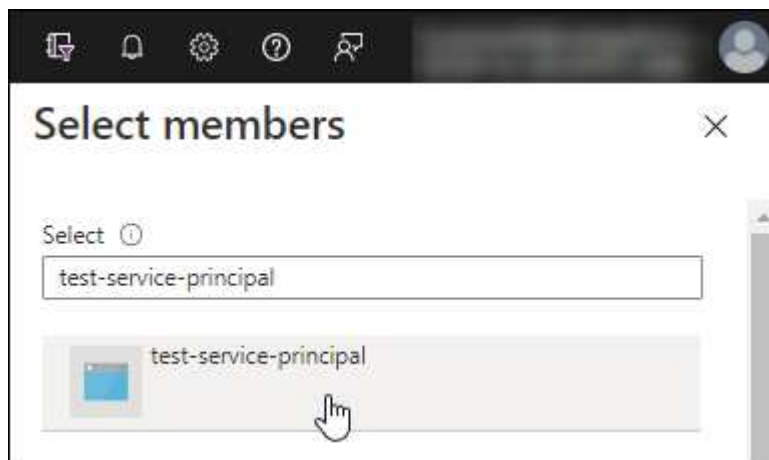
- Öffnen Sie im Azure-Portal den Service **Abonnements**.
- Wählen Sie das Abonnement aus.
- Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
- Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
  - **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.

- Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



- Wählen Sie die Anwendung aus und wählen Sie **Select**.
- Wählen Sie **Weiter**.

f. Wählen Sie **Überprüfen + Zuweisen**.

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.

## Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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

### Schritte

1. Wählen Sie im **Microsoft Entra ID-Dienst App-Registrierungen** aus und wählen Sie die Anwendung aus.
2. Wählen Sie **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. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **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](#)

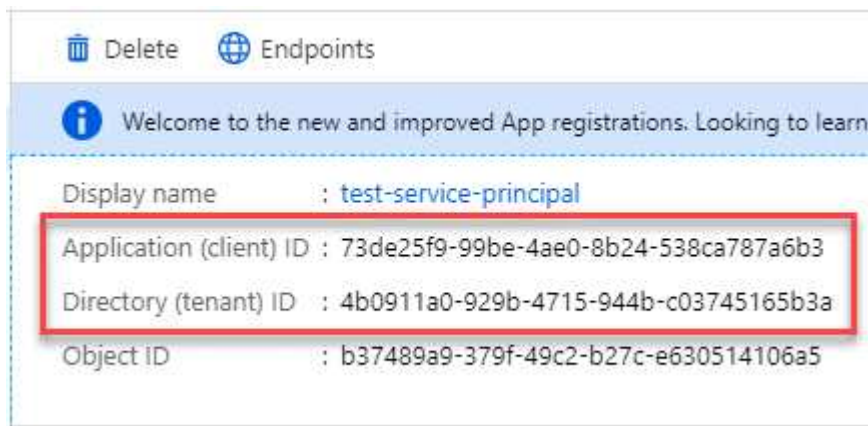
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview)	-

### Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab

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. Wählen Sie im **Microsoft Entra ID**-Dienst **App-Registrierungen** aus und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) 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.

### Erstellen Sie einen Clientschlüssel

Sie müssen einen Client Secret erstellen und BlueXP dann den Wert des Geheimnisses bereitstellen, damit BlueXP ihn zur Authentifizierung mit Microsoft Entra ID verwenden kann.

#### Schritte

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate & Geheimnisse > Neues Kundegeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **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*-ZR0v4NLfdAcY7:+0vA	<a href="#">Copy to clipboard</a>

Jetzt haben Sie einen Client-Schlüssel, den BlueXP zur Authentifizierung mit Microsoft Entra ID verwenden kann.

### 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.

### Zugangsdaten zu BlueXP hinzufügen

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.

### Bevor Sie beginnen

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

### Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.

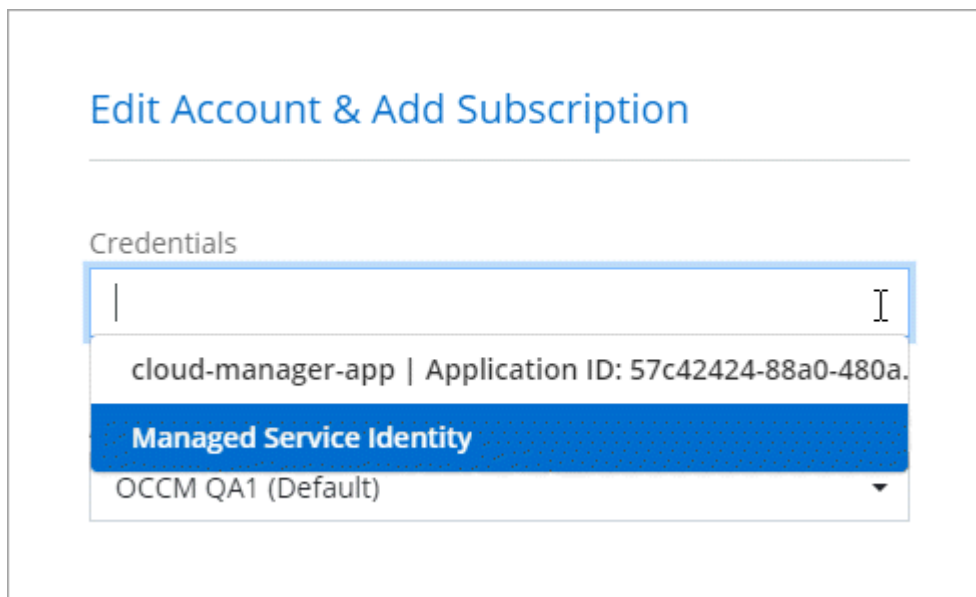


2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten im Assistenten.

- a. **Anmeldeort:** Wählen Sie **Microsoft Azure > Connector**.
- b. **Credentials definieren:** Geben Sie Informationen über den Microsoft Entra-Dienst-Prinzipal ein, der die erforderlichen Berechtigungen gewährt:
  - Anwendungs-ID (Client)
  - ID des Verzeichnisses (Mandant)
  - Client-Schlüssel
- c. **Marketplace-Abonnement:** Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.
- d. **Review:** Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

## 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". A dropdown menu is open, displaying the text "cloud-manager-app | Application ID: 57c42424-88a0-480a.". Below this, there is a blue bar with the text "Managed Service Identity". At the bottom of the dropdown, the text "OCCM QA1 (Default)" is visible with a small downward arrow.

## Vorhandene Anmeldedaten verwalten

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

### Azure Marketplace Abonnement mit Anmeldedaten verknüpfen

Nachdem Sie Ihre Azure Zugangsdaten zu BlueXP hinzugefügt haben, können Sie diesen Anmeldedaten ein Azure Marketplace Abonnement zuordnen. Mit dem Abonnement können Sie ein Pay-as-you-go Cloud Volumes ONTAP System erstellen und andere BlueXP 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 das Abonnement für Azure Marketplace ändern, das mit den Azure-Anmeldedaten verknüpft ist.



Durch den Austausch des aktuellen Marketplace-Abonnements durch ein neues Abonnement wird das Marketplace-Abonnement für alle bestehenden Cloud Volumes ONTAP Arbeitsumgebungen und alle neuen Arbeitsumgebungen geändert.

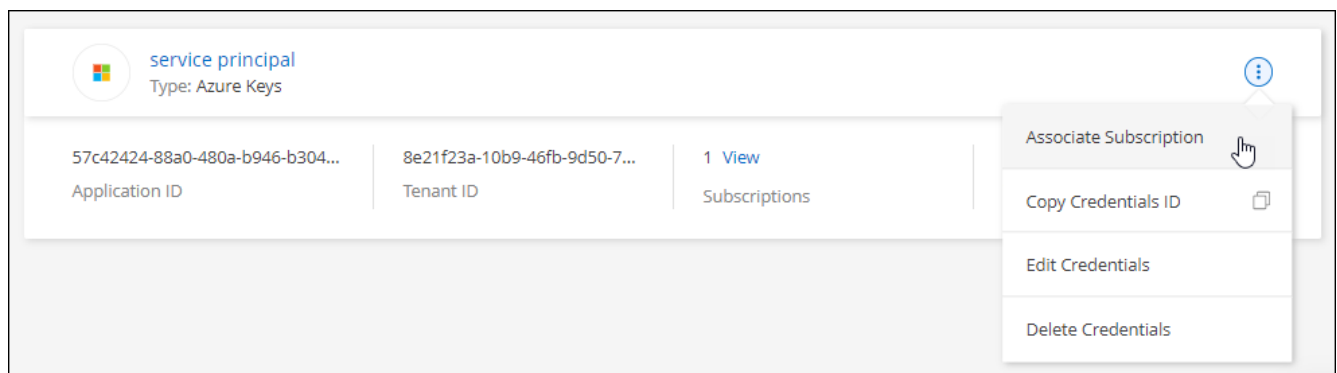
## Bevor Sie beginnen

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

## Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Associate Subscription**.

Sie müssen Anmeldeinformationen auswählen, die einem Connector zugeordnet sind. Sie können kein Marketplace-Abonnement mit Anmeldedaten verknüpfen, die mit BlueXP verknüpft sind.



3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie das Abonnement aus der Down-Liste aus und wählen **Associate** aus.
4. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Weiter** und befolgen Sie die Schritte im Azure Marketplace:
  - a. Melden Sie sich bei Ihrem Azure-Konto an, wenn Sie dazu aufgefordert werden.
  - b. Wählen Sie **Abonnieren**.
  - c. Füllen Sie das Formular aus und wählen Sie **Abonnieren**.
  - d. Wählen Sie nach Abschluss des Abonnements **Konto jetzt konfigurieren** aus.

Sie werden auf die BlueXP-Website umgeleitet.

- e. Auf der Seite **Subscription Assignment**:

- Wählen Sie die BlueXP Konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.
- Wählen Sie im Feld **vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

BlueXP ersetzt das vorhandene Abonnement für alle Anmeldeinformationen im Konto durch dieses neue Abonnement. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden



Schritte wiederholen.

- Wählen Sie **Speichern**.

Im folgenden Video sehen Sie, wie Sie im Azure Marketplace abonnieren:

[Abonnieren Sie BlueXP über den Azure Marketplace](#)

## Anmeldedaten bearbeiten

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 auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie auf der Seite **Account Credentials** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Credentials bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann **Anwenden**.

## Anmeldeinformationen löschen

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 auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie auf der Seite **Account Credentials** das Aktionsmenü für einen Satz von Anmeldeinformationen aus und wählen Sie dann **Credentials löschen**.
3. Wählen Sie **Löschen**, um zu bestätigen.

## Copyright-Informationen

Copyright © 2024 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.