



# **Verwalten von BlueXP**

## **Set up and administration**

NetApp

November 23, 2022

# Inhaltsverzeichnis

- Verwalten von BlueXP ..... 1
  - NetApp Accounts ..... 1
  - Anschlüsse ..... 16
  - PAYGO-Abonnements und -Verträge verwalten ..... 48
  - Cloud Storage erkannt ..... 50
  - AWS Zugangsdaten ..... 55
  - Azure Zugangsdaten ..... 64
  - Google Cloud-Anmeldedaten ..... 77
  - Fügen Sie Konten der NetApp Support Site in BlueXP hinzu und managen Sie sie ..... 85
  - Meine Opportunitys ..... 92

# Verwalten von BlueXP

## NetApp Accounts

### Managen Ihres NetApp Kontos

"[Nach der ersten Einrichtung](#)", Sie können Ihre Kontoeinstellungen später verwalten, indem Sie Benutzer, Servicekonten, Arbeitsbereiche, Anschlüsse und Abonnements verwalten.

"[Erfahren Sie mehr über die Funktionsweise von NetApp Accounts](#)".

### Managen Ihres Kontos mit der Tenancy API

Wenn Sie Ihre Kontoeinstellungen durch Senden von API-Anfragen verwalten möchten, müssen Sie die API *Tenancy* verwenden. Diese API unterscheidet sich von der BlueXP API, die Sie zum Erstellen und Verwalten von Cloud Volumes ONTAP-Arbeitsumgebungen verwenden.

"[Anzeige von Endpunkten für die Mandanten-API](#)"

### Erstellen und Verwalten von Benutzern

Die Benutzer in Ihrem Konto können auf die Ressourcen in den Arbeitsbereichen Ihres Kontos verwalten zugreifen.

#### Benutzer hinzufügen

Verknüpfen Sie Benutzer mit Ihrem NetApp Konto, damit diese Benutzer Arbeitsumgebungen in BlueXP erstellen und verwalten können.

#### Schritte

1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "[NetApp BlueXP Website](#)" Und melden Sie sich an.
2. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto**.



3. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



4. Klicken Sie auf der Registerkarte Mitglieder auf **Benutzer verknüpfen**.
5. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
  - **Account Admin:** Kann jede Aktion in BlueXP ausführen.
  - **Workspace Admin:** Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
  - **Compliance Viewer:** Kann nur Informationen zur Compliance von Cloud Data Sense anzeigen und Berichte für Arbeitsbereiche erstellen, auf die sie zugreifen können.
  - **SnapCenter Admin:** Kann den SnapCenter Service verwenden, um mit diesen Backups anwendungskonsistente Backups zu erstellen und Daten wiederherzustellen. *Dieser Dienst befindet sich derzeit in der Beta.*
6. Wenn Sie Workspace Admin oder Compliance Viewer ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



The image shows a web-based dialog box titled "Associate User". At the top, there is a user icon. Below the title, a light blue banner contains the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." The main form area has three sections: "User's Email" with a text input field containing "test@netapp.com"; "Role" with a dropdown menu showing "Workspace Admin"; and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom, there are two buttons: a grey "Cancel" button and a blue "Associate User" button.



### Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 X

Cancel Associate User

7. Klicken Sie Auf **Mitarbeiter**.

Der Benutzer sollte eine E-Mail von NetApp BlueXP mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die Informationen, die für den Zugriff auf BlueXP erforderlich sind.

#### Benutzer werden entfernt

Die Trennung der Verknüpfung eines Benutzers wird dadurch ermöglicht, dass er nicht mehr auf die Ressourcen eines NetApp Kontos zugreifen kann.

#### Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie zur Bestätigung auf **Benutzer entzuordnen** und klicken Sie zur Bestätigung auf **Mitarbeiter nicht zuordnen**.

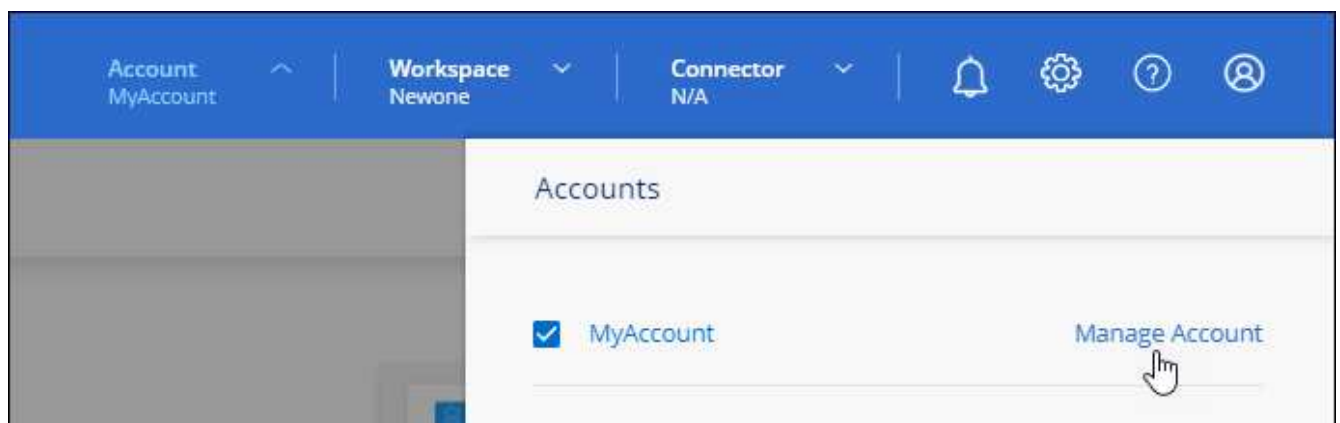
Der Anwender kann nicht mehr auf die Ressourcen in diesem NetApp Konto zugreifen.

#### Arbeitsbereiche eines Arbeitsbereichs-Administrators verwalten

Sie können Workspace-Administratoren jederzeit mit Arbeitsbereichen verknüpfen und sie ablösen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.

#### Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.

5 Members						
Type	Name	Email	Role	Workspace		
	Ben		☆ Account Admin	All Workspaces	...	
	Tom		☆ Account Admin	All Workspaces	...	
	Ben		Workspace Admin	Newone		

3. Klicken Sie Auf **Arbeitsbereiche Verwalten**.

4. Wählen Sie die Arbeitsbereiche aus, die dem Benutzer zugeordnet werden sollen, und klicken Sie auf **Anwenden**.

Der Benutzer kann jetzt von BlueXP auf diese Arbeitsbereiche zugreifen, solange der Connector auch mit den Arbeitsbereichen verknüpft war.

## Erstellen und Verwalten von Servicekonten

Ein Servicekonto fungiert als „Benutzer“, der autorisierte API-Aufrufe zu Automatisierungszwecken an BlueXP vornehmen kann. So ist das Management der Automatisierung einfacher, da keine Automatisierungsskripts auf Basis des Benutzerkontos eines echten Mitarbeiters erstellt werden müssen, der das Unternehmen jederzeit verlassen kann. Und bei Verwendung von Federation können Sie ein Token erstellen, ohne ein Update-Token aus der Cloud zu generieren.

Sie erteilen einem Servicekonto Berechtigungen, indem Sie ihm eine Rolle zuweisen, genau wie jeder andere BlueXP-Benutzer. Sie können das Servicekonto auch mit bestimmten Arbeitsbereichen verknüpfen, um die Arbeitsumgebungen (Ressourcen) zu kontrollieren, auf die der Service zugreifen kann.

Wenn Sie das Dienstkonto erstellen, können Sie mit BlueXP eine Client-ID und einen Clientschlüssel für das Dienstkonto kopieren oder herunterladen. Dieses Schlüsselpaar wird für die Authentifizierung mit BlueXP verwendet.

### Erstellen eines Dienstkontos

Erstellen Sie so viele Service-Konten wie für das Management der Ressourcen in Ihren Arbeitsumgebungen erforderlich.

### Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto**.



2. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



3. Klicken Sie auf der Registerkarte Mitglieder auf **Dienstkonto erstellen**.
4. Geben Sie einen Namen ein, und wählen Sie eine Rolle aus. Wenn Sie eine andere Rolle als Kontoadministrator auswählen, wählen Sie den Arbeitsbereich aus, der mit diesem Dienstkonto verknüpft werden soll.
5. Klicken Sie Auf **Erstellen**.
6. Kopieren Sie die Client-ID und den Clientschlüssel, oder laden Sie sie herunter.

Das Clientgeheimnis ist nur einmal sichtbar und wird von BlueXP nirgendwo gespeichert. Kopieren oder laden Sie das Geheimnis herunter und speichern Sie es sicher.

7. Klicken Sie Auf **Schließen**.

#### Abrufen eines Inhabertoken für ein Dienstkonto

Um API-Aufrufe an das zu tätigen "**Mandanten-API**", Sie müssen ein Inhaberzeichen für ein Service-Konto zu erhalten.

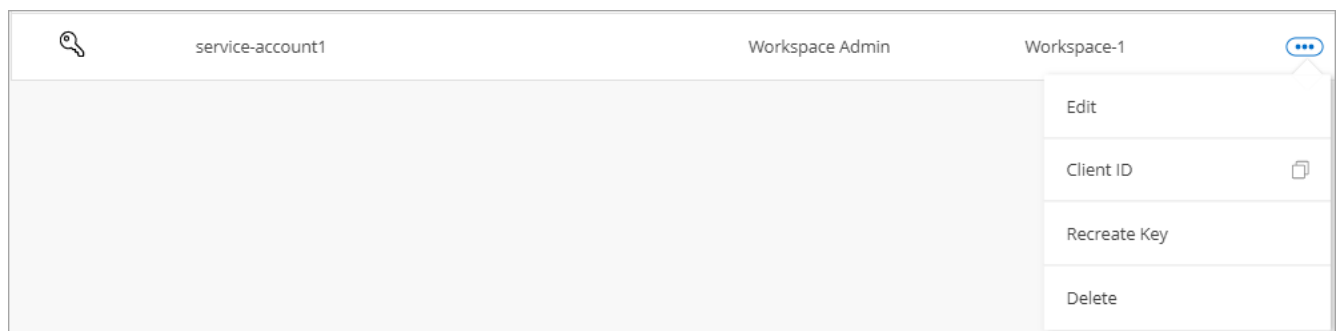
"Erfahren Sie, wie Sie ein Service-Konto-Token erstellen"

#### Kopieren der Client-ID

Sie können die Client-ID eines Dienstkontos jederzeit kopieren.

#### Schritte

1. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Dienstkonto entspricht.



2. Klicken Sie auf **Client-ID**.
3. Die ID wird in die Zwischenablage kopiert.

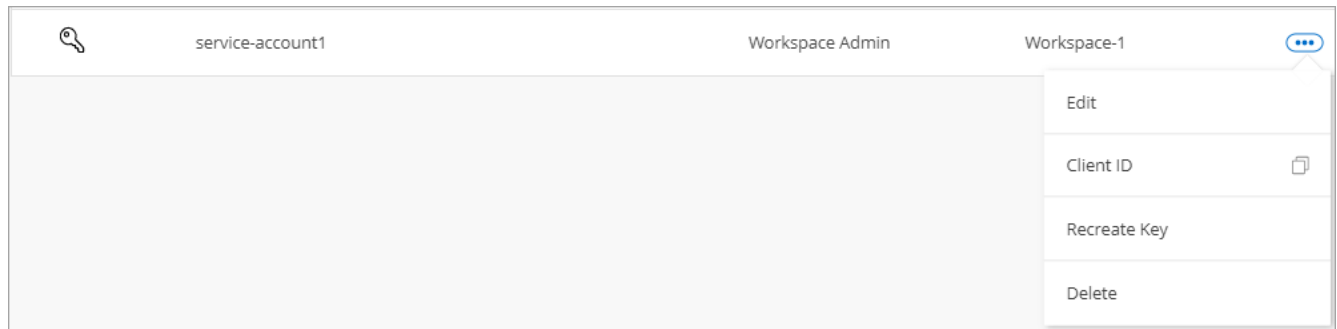


## Schlüssel werden neu erstellt

Durch Neuerstellen des Schlüssels wird der vorhandene Schlüssel für dieses Servicekonto gelöscht und anschließend ein neuer Schlüssel erstellt. Sie können den vorherigen Schlüssel nicht verwenden.

### Schritte

1. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Dienstkonto entspricht.



2. Klicken Sie Auf **Reproduzieren Schlüssel**.
3. Klicken Sie zur Bestätigung auf **reproduzieren**.
4. Kopieren Sie die Client-ID und den Clientschlüssel, oder laden Sie sie herunter.

Das Clientgeheimnis ist nur einmal sichtbar und wird von BlueXP nirgendwo gespeichert. Kopieren oder laden Sie das Geheimnis herunter und speichern Sie es sicher.

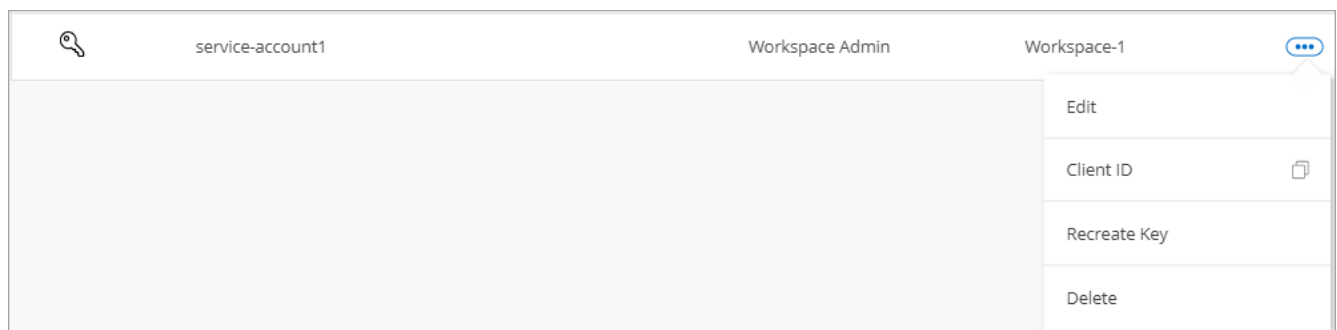
5. Klicken Sie Auf **Schließen**.

## Löschen eines Dienstkontos

Löschen Sie ein Dienstkonto, wenn Sie es nicht mehr verwenden müssen.

### Schritte

1. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Dienstkonto entspricht.



2. Klicken Sie Auf **Löschen**.
3. Klicken Sie zur Bestätigung erneut auf **Löschen**.

## Arbeitsbereiche verwalten

Verwalten Sie Ihre Arbeitsbereiche, indem Sie sie erstellen, umbenennen und löschen. Beachten Sie, dass Sie

einen Arbeitsbereich nicht löschen können, wenn er Ressourcen enthält. Er muss leer sein.

### Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Arbeitsbereiche**.
3. Wählen Sie eine der folgenden Optionen:
  - Klicken Sie auf **Neuen Arbeitsbereich hinzufügen**, um einen neuen Arbeitsbereich zu erstellen.
  - Klicken Sie auf **Umbenennen**, um den Arbeitsbereich umzubenennen.
  - Klicken Sie auf **Löschen**, um den Arbeitsbereich zu löschen.

### Verwalten der Arbeitsbereiche eines Connectors

Sie müssen den Connector mit Arbeitsbereichen verknüpfen, damit Workspace-Administratoren von BlueXP auf diese Arbeitsbereiche zugreifen können.

Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Kontoadministratoren haben standardmäßig die Möglichkeit, auf alle Arbeitsbereiche in BlueXP zuzugreifen.

["Erfahren Sie mehr über Benutzer, Arbeitsbereiche und Connectors"](#).

### Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Connector**.
3. Klicken Sie auf **Arbeitsbereiche verwalten** für den Konnektor, den Sie verknüpfen möchten.
4. Wählen Sie die Arbeitsbereiche aus, die mit dem Connector verknüpft werden sollen, und klicken Sie auf **Anwenden**.

### Verwalten von Abonnements

Nachdem Sie den Marketplace eines Cloud-Providers abonniert haben, steht jedes Abonnement über das Widget „Account Settings“ (Kontoeinstellungen) zur Verfügung. Sie haben die Möglichkeit, ein Abonnement umzubenennen und das Abonnement von einem oder mehreren Konten zu entfernen.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

["Weitere Informationen zu Abonnements"](#).

### Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Abonnements**.

Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

3. Klicken Sie in der Zeile auf das Aktionsmenü, das dem Abonnement entspricht, das Sie verwalten möchten.

2 Subscriptions

Name	Service	Cloud Provider	Status
QA Subscription	test-service	aws	Unsubscribed
metering service subscription QA !!!!	cloud-volumes-ontap	aws	Subscribed

Rename Subscription  
Manage Accounts

- Wählen Sie diese Option, um das Abonnement umzubenennen oder um die Konten zu verwalten, die mit dem Abonnement verbunden sind.

## Ihren Kontonamen ändern

Ändern Sie Ihren Kontonamen jederzeit, um ihn in etwas Sinnvolles für Sie zu ändern.

### Schritte

- Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
- Klicken Sie auf der Registerkarte **Übersicht** neben dem Kontonamen auf das Bearbeiten-Symbol.
- Geben Sie einen neuen Kontonamen ein und klicken Sie auf **Speichern**.

## Private Vorschauen zulassen

Ermöglichen Sie privaten Vorschau in Ihrem Konto, um Zugriff auf die neuen NetApp Cloud-Services zu erhalten, die in BlueXP als Vorschau zur Verfügung gestellt werden.

Services in der privaten Vorschau sind nicht garantiert, dass sich wie erwartet verhalten und können Ausfälle aufrecht erhalten und fehlende Funktionen sein.

### Schritte

- Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
- Aktivieren Sie auf der Registerkarte **Übersicht** die Einstellung **Private Vorschau zulassen**.

## Durch die Nutzung von Services anderer Anbieter

Lassen Sie Drittanbieter-Services in Ihrem Konto zu, um Zugriff auf Dienste von Drittanbietern zu erhalten, die in BlueXP verfügbar sind. Drittanbieter-Services sind ähnlich wie die Services von NetApp, werden aber von Drittanbieter gemanagt und unterstützt.

### Schritte

- Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
- Aktivieren Sie auf der Registerkarte **Übersicht** die Option **Drittanbieter-Services zulassen**.

## Deaktivieren der SaaS-Plattform

Wir empfehlen nicht, die SaaS-Plattform zu deaktivieren, es sei denn, Sie müssen, um die Sicherheitsrichtlinien Ihres Unternehmens zu erfüllen. Durch die Deaktivierung der SaaS-Plattform ist Ihre Fähigkeit zur Nutzung von integrierten NetApp Cloud-Services begrenzt.

Die folgenden Dienste stehen bei BlueXP nicht zur Verfügung, wenn Sie die SaaS-Plattform deaktivieren:

- Cloud-Daten Sinnvoll
- Kubernetes
- Cloud Tiering
- Globaler Datei-Cache

Wenn Sie die SaaS-Plattform deaktivieren, müssen Sie alle Aufgaben von ausführen ["Die lokale Benutzeroberfläche, die auf einem Connector verfügbar ist"](#).



Dies ist eine irreversible Aktion, die Sie daran hindert, die BlueXP SaaS-Plattform zu verwenden. Sie müssen Aktionen über den lokalen Konnektor durchführen. Sie können nicht viele integrierte Cloud-Services von NetApp nutzen und die erneute Aktivierung der SaaS-Plattform erfordert die Unterstützung durch NetApp.

### Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Schalten Sie auf der Registerkarte Übersicht die Option ein, um die Nutzung der SaaS-Plattform zu deaktivieren.

## Überwachen von Vorgängen in Ihrem Konto


Sie können den Status der Operationen überwachen, die BlueXP durchführt, um zu sehen, ob Probleme auftreten, die Sie beheben müssen. Sie können den Status im Benachrichtigungscenter, in der Zeitleiste anzeigen oder Benachrichtigungen an Ihre E-Mail senden.

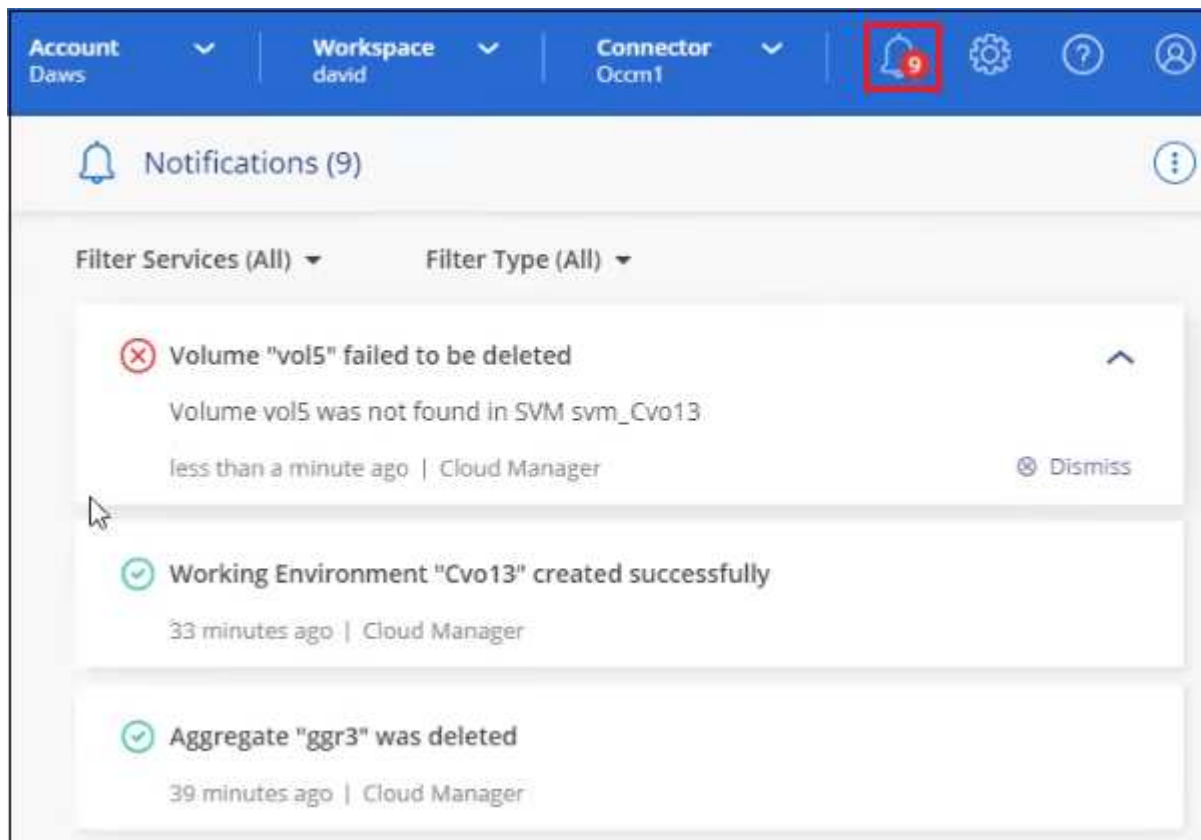
In dieser Tabelle werden das Benachrichtigungscenter und die Zeitleiste verglichen, damit Sie verstehen können, was die einzelnen Angebote zu bieten haben.

Notification Center	Zeitachse
Zeigt den allgemeinen Status von Ereignissen und Aktionen an	Enthält Details zu jedem Ereignis oder jeder Aktion zur weiteren Untersuchung
Zeigt den Status der aktuellen Anmeldesitzung an. Die Informationen werden nach der Abmeldung nicht im Benachrichtigungscenter angezeigt	Behält den Status des letzten Monats bei
Zeigt nur Aktionen an, die in der Benutzeroberfläche initiiert wurden	Zeigt alle Aktionen der UI oder der APIs an
Zeigt benutzerinitiierte Aktionen an	Zeigt alle Aktionen an, ob vom Benutzer initiiert oder vom System initiiert
Ergebnisse nach Bedeutung filtern	Filtern nach Dienst, Aktion, Benutzer, Status und mehr
Ermöglicht das E-Mail-Versenden von Benachrichtigungen an Benutzer von Konten und an andere Benutzer	Keine E-Mail-Funktion

## Überwachen von Aktivitäten mithilfe des Benachrichtigungszentrums

Benachrichtigungen verfolgen den Fortschritt der Vorgänge, die Sie in BlueXP initiiert haben, damit Sie überprüfen können, ob der Vorgang erfolgreich war oder nicht. Mit diesen können Sie den Status vieler BlueXP-Aktionen anzeigen, die Sie während Ihrer aktuellen Anmeldesitzung initiiert haben. Nicht alle Dienste berichten zu diesem Zeitpunkt Informationen in das Benachrichtigungszentrum.

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Benachrichtigungs-Bell (klicken ) In der Menüleiste. Die Farbe der kleinen Blase in der Glocke zeigt die Meldung mit dem höchsten Schweregrad an, die aktiv ist. Wenn Sie also eine rote Blase sehen, bedeutet dies, dass eine wichtige Benachrichtigung angezeigt wird, die Sie sich ansehen sollten.



Außerdem können Sie BlueXP so konfigurieren, dass Benachrichtigungen per E-Mail versendet werden, damit Sie auch dann über wichtige Systemaktivitäten informiert werden können, wenn Sie nicht am System angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihres NetApp Cloud Kontos sind, oder an andere Empfänger, die bestimmte Arten von Systemaktivitäten kennen müssen. Siehe [email notification settings](#), Einstellen der Einstellungen für E-Mail-Benachrichtigungen Unten.

### Benachrichtigungstypen

Benachrichtigungen werden in die folgenden Kategorien eingeteilt:

Benachrichtigungstyp	Beschreibung
Kritisch	Ein Problem, das zu einer Serviceunterbrechung führen kann, wenn keine Korrekturmaßnahmen sofort ergriffen werden.
Fehler	Eine Aktion oder ein Prozess wurde mit einem Fehler beendet oder könnte zu einem Fehler führen, wenn keine Korrekturmaßnahmen ergriffen werden.

Benachrichtigungstyp	Beschreibung
Warnung	Ein Problem, das Sie beachten sollten, um sicherzustellen, dass es den kritischen Schweregrad nicht erreicht. Benachrichtigungen dieses Schweregrades verursachen keine Serviceunterbrechungen und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich.
Empfehlung	Eine Systemempfehlung für Sie, Maßnahmen zur Verbesserung des Systems oder eines bestimmten Dienstes zu ergreifen, zum Beispiel: Kostenersparnis, Vorschlag für neue Dienste, empfohlene Sicherheitskonfiguration, etc
Informationsdaten	Eine Meldung, die zusätzliche Informationen zu einer Aktion oder einem Prozess enthält.
Erfolg	Eine Aktion oder ein Prozess erfolgreich abgeschlossen.

### Filtern von Benachrichtigungen

Standardmäßig werden alle Benachrichtigungen angezeigt. Sie können die Benachrichtigungen filtern, die im Benachrichtigungscenter angezeigt werden, um nur die Benachrichtigungen anzuzeigen, die für Sie wichtig sind. Sie können nach BlueXP „Service“ und nach Benachrichtigung „Typ“ filtern.

Wenn Sie beispielsweise nur „Fehler“ und „Warnung“ für BlueXP-Vorgänge sehen möchten, wählen Sie diese Einträge aus, und Sie werden nur die Arten von Benachrichtigungen sehen.

### Einstellen der Einstellungen für E-Mail-Benachrichtigungen

Sie können bestimmte Arten von Benachrichtigungen per E-Mail versenden, damit Sie über wichtige Systemaktivitäten informiert werden können, auch wenn Sie nicht bei BlueXP angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihres NetApp Kontos sind, oder an andere Empfänger, die bestimmte Arten von Systemaktivitäten kennen müssen.



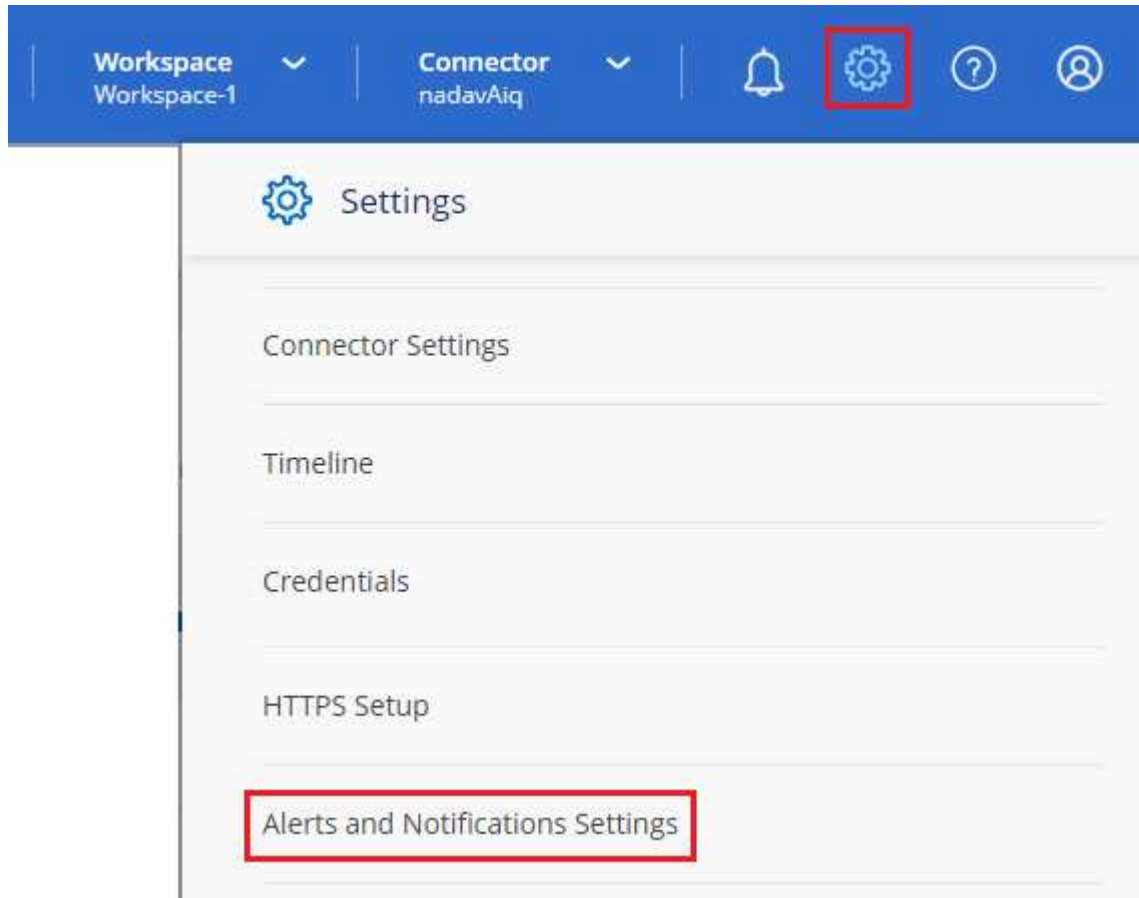
- Derzeit senden nur Cloud Sync und Cloud Backup Benachrichtigungen per E-Mail. Weitere Services werden in zukünftigen Versionen hinzugefügt.
- Das Senden von E-Mail-Benachrichtigungen wird nicht unterstützt, wenn der Connector auf einer Website ohne Internetzugang installiert ist.

Standardmäßig erhalten BlueXP-Kontoadministratoren E-Mails für alle „kritischen“ und „Empfehlungsbenachrichtigungen“. Alle anderen Benutzer und Empfänger sind standardmäßig so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten.

Sie müssen ein Kontoadministrator sein, um die Benachrichtigungseinstellungen anzupassen.

### Schritte

1. Klicken Sie in der Menüleiste von BlueXP auf **Einstellungen > Einstellungen für Warnungen und Benachrichtigungen**.



2. Wählen Sie einen Benutzer oder mehrere Benutzer entweder auf der Registerkarte *Account Users* oder auf der Registerkarte *Additional Recipients* aus, und wählen Sie den Typ der zu sendenden Benachrichtigungen aus:
  - Um Änderungen an einem einzelnen Benutzer vorzunehmen, klicken Sie in der Spalte Benachrichtigungen für diesen Benutzer auf das Menü, überprüfen Sie die zu sendenden Benachrichtigungsarten und klicken Sie auf **Anwenden**.
  - Um Änderungen für mehrere Benutzer vorzunehmen, aktivieren Sie das Kontrollkästchen für jeden Benutzer, klicken Sie auf **E-Mail-Benachrichtigungen verwalten**, markieren Sie die zu sendenden Benachrichtigungsarten und klicken Sie auf **Anwenden**.

Email	Name	Role
<input type="checkbox"/> Sabar@netapp.com	Sabar V	Account Admin
<input checked="" type="checkbox"/> activeiq@netapp-st.com	nadav	Account Admin
<input checked="" type="checkbox"/> nand@netapp.com	AnanK	Account Admin
<input type="checkbox"/> apra@netapp.com	Aradev	Workspace Admin
<input type="checkbox"/> ash@netapp.com	AshG	Account Admin

### Hinzufügen von zusätzlichen E-Mail-Empfängern

Die Benutzer, die auf der Registerkarte „Account Users“ angezeigt werden, werden automatisch von den Benutzern Ihres NetApp Kontos ausgefüllt (von der [Seite „Konto verwalten“](#)). Sie können E-Mail-Adressen auf der Registerkarte „Additional Recipients“ für andere Personen oder Gruppen hinzufügen, die keinen Zugriff auf BlueXP haben, aber über bestimmte Arten von Warnungen und Benachrichtigungen benachrichtigt werden müssen.

#### Schritte

1. Klicken Sie auf der Seite Einstellungen für Warnungen und Benachrichtigungen auf **Neue Empfänger hinzufügen**.

2. Geben Sie den Namen, die E-Mail-Adresse ein, und wählen Sie die Art der Benachrichtigungen aus, die der Empfänger empfangen wird, und klicken Sie auf **Neuen Empfänger hinzufügen**.

### Benachrichtigungen nicht vorhanden

Sie können Benachrichtigungen von der Seite entfernen, wenn Sie sie nicht mehr sehen müssen. Sie können alle Benachrichtigungen auf einmal verwerfen oder einzelne Benachrichtigungen verwerfen.

Um alle Benachrichtigungen auszublenden, klicken Sie im Benachrichtigungscenter auf Und wählen Sie **Alle**





verwerfen.

Um einzelne Benachrichtigungen zu verwerfen, bewegen Sie den Cursor über die Benachrichtigung und



klicken auf **abweisen**.

**Benutzeraktivitäten in Ihrem Konto prüfen**

In der Zeitleiste in BlueXP werden die Aktionen angezeigt, die Benutzer zur Verwaltung Ihres Kontos abgeschlossen haben. Dazu gehören Verwaltungsaktionen wie das Verknüpfen von Benutzern, das Erstellen von Arbeitsbereichen, das Erstellen von Connectors und vieles mehr.

Das Prüfen der Zeitleiste kann hilfreich sein, wenn Sie feststellen müssen, wer eine bestimmte Aktion durchgeführt hat oder ob Sie den Status einer Aktion identifizieren müssen.

**Schritte**

- 1. Klicken Sie in der Menüleiste von BlueXP auf **Einstellungen > Timeline**.
- 2. Klicken Sie unter Filter auf **Service**, aktivieren Sie **Tenancy** und klicken Sie auf **Apply**.

Die Zeitleiste wird aktualisiert, um Ihnen Aktionen zur Kontoverwaltung anzuzeigen.

**Rollen**

Die Rollen Kontoverwaltung, Arbeitsbereichsverwaltung, Compliance Viewer und SnapCenter-Admin bieten Benutzern spezifische Berechtigungen.

Die Compliance Viewer-Rolle dient dem schreibgeschützten Cloud Data Sense Zugriff.

Aufgabe	Kontoadministrat or	Workspace- Verwaltung	Compliance Viewer	SnapCenter Admin
Verwalten von Arbeitsumgebungen	Ja.	Ja.	Nein	Nein
Services in Arbeitsumgebungen ermöglichen	Ja.	Ja.	Nein	Nein
Anzeigen des Status der Datenreplizierung	Ja.	Ja.	Nein	Nein
Zeitachse anzeigen	Ja.	Ja.	Nein	Nein
Wechseln Sie zwischen Arbeitsbereichen	Ja.	Ja.	Ja.	Nein

Aufgabe	Kontoadministrator	Workspace-Verwaltung	Compliance Viewer	SnapCenter Admin
Zeigen Sie die Ergebnisse des Data Sense-Scans an	Ja.	Ja.	Ja.	Nein
Arbeitsumgebungen löschen	Ja.	Nein	Nein	Nein
Kubernetes-Cluster mit Arbeitsumgebungen verbinden	Ja.	Nein	Nein	Nein
Cloud Volumes ONTAP Bericht erhalten	Ja.	Nein	Nein	Nein
Anschlüsse Erstellen	Ja.	Nein	Nein	Nein
NetApp Accounts managen	Ja.	Nein	Nein	Nein
Anmeldeinformationen verwalten	Ja.	Nein	Nein	Nein
Ändern Sie die Einstellungen von BlueXP	Ja.	Nein	Nein	Nein
Anzeigen und Verwalten des Support-Dashboards	Ja.	Nein	Nein	Nein
Entfernen Sie Arbeitsumgebungen aus BlueXP	Ja.	Nein	Nein	Nein
Installieren Sie ein HTTPS-Zertifikat	Ja.	Nein	Nein	Nein
Verwenden Sie den SnapCenter-Dienst	Ja.	Ja.	Nein	Ja.

#### Weiterführende Links

- ["Einrichtung von Workspaces und Benutzern im NetApp Konto"](#)
- ["Managen von Workspaces und Benutzern im NetApp Account"](#)

## Anschlüsse

### Erweiterte Implementierung

#### Erstellen Sie einen Connector aus dem AWS Marketplace

Für eine kommerzielle AWS Region empfiehlt es sich, einen Connector direkt aus BlueXP zu erstellen, aber Sie können einen Connector auf dem AWS Marketplace starten, falls Sie es bevorzugen. Für Regionen der AWS Regierung kann der Connector nicht über die BlueXP SaaS-Website in einer Regierungsregion bereitgestellt werden. Die nächste

Option ist daher der AWS Marketplace.



Sie können die Connector-Software auch auf einem bestehenden Linux-Host in Ihrem Netzwerk oder in der Cloud herunterladen und installieren. ["Erfahren Sie, wie Sie den Connector auf einem vorhandenen Linux-Host installieren"](#).

#### Connector in einer kommerziellen AWS-Region erstellen

Sie können die Connector-Instanz direkt aus dem AWS Marketplace-Angebot für BlueXP in einer kommerziellen AWS-Region starten.

Der IAM-Benutzer, der den Connector erstellt, muss über AWS Marketplace-Berechtigungen zum Abonnieren und Abbestellen verfügen.

#### Schritte

1. Einrichten von Berechtigungen in AWS:
  - a. Erstellen Sie über die IAM-Konsole die erforderlichen Richtlinien, indem Sie die Inhalte von kopieren und einfügen ["Die IAM-Richtlinien für den Connector"](#).
  - b. Erstellen Sie eine IAM-Rolle mit dem Rollentyp Amazon EC2 und hängen Sie die Richtlinien an, die Sie im vorherigen Schritt erstellt haben.
2. Wechseln Sie zum ["Seite „BlueXP“ im AWS Marketplace"](#) So stellen Sie den Stecker über eine AMI bereit:
3. Klicken Sie auf der Marketplace-Seite auf **Weiter zur Anmeldung** und dann auf **Weiter zur Konfiguration**.

## Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price  
**\$0.226/hr**

Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Overview

Pricing

Usage

Support

Reviews

### Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

#### Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

## Cloud Manager - Manual Installation without access keys

[Continue to Configuration](#)

[< Product Detail](#) [Subscribe](#)

### Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

#### Terms and Conditions

NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

- Ändern Sie eine der Standardoptionen, und klicken Sie auf **Weiter zum Starten**.
- Wählen Sie unter **Aktion auswählen über EC2 starten** und klicken Sie dann auf **Start**.

In diesen Schritten wird beschrieben, wie Sie die Instanz von der EC2-Konsole aus starten, da Sie über die Konsole eine IAM-Rolle an die Connector-Instanz anhängen können. Dies ist mit der Aktion \* von Website starten\* nicht möglich.

- Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:
  - Name und Tags:** Geben Sie einen Namen und Tags für die Instanz ein.
  - Anwendung und Betriebssystembild:** Überspringen Sie diesen Abschnitt. Der Stecker AMI ist bereits ausgewählt.

- **Instanztyp:** Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.xlarge wird empfohlen).

["Prüfen Sie die Anforderungen an die Instanz".](#)

- **Schlüsselpaar (Login):** Wählen Sie das Schlüsselpaar aus, mit dem Sie eine sichere Verbindung zur Instanz herstellen möchten.
- **Netzwerkeinstellungen:** Bearbeiten Sie die Netzwerkeinstellungen nach Bedarf:
  - Wählen Sie die gewünschte VPC und das Subnetz.
  - Geben Sie an, ob die Instanz eine öffentliche IP-Adresse haben soll.
  - Legen Sie Firewall-Einstellungen fest, die die erforderlichen Verbindungsmethoden für die Connector-Instanz SSH, HTTP und HTTPS aktivieren.
- **Storage konfigurieren:** Behalten Sie die standardmäßigen Speicheroptionen bei.
- **Erweiterte Details:** Wählen Sie unter **IAM-Instanzprofil** die IAM-Rolle aus, die Sie in Schritt 1 erstellt haben.
- **Zusammenfassung:** Lesen Sie die Zusammenfassung durch und klicken Sie auf **Instanz starten**.

AWS startet die Software mit den angegebenen Einstellungen. Die Connector-Instanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

7. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung zur Verbindungsinstanz hat, und geben Sie die folgende URL ein:

`https://ipaddress[]`

8. Richten Sie nach der Anmeldung den Konnektor ein:

- a. Geben Sie den NetApp Account an, der mit dem Connector verknüpft werden soll.

["Informationen zu NetApp Accounts".](#)

- b. Geben Sie einen Namen für das System ein.



9. Öffnen Sie einen Webbrowser, und gehen Sie zu <https://cloudmanager.netapp.com> Um den Connector mit BlueXP zu verwenden.

Der Connector ist jetzt mit Ihrem NetApp Konto installiert und eingerichtet. BlueXP verwendet diesen Connector automatisch, wenn Sie neue Arbeitsumgebungen erstellen. Aber wenn Sie mehr als einen Connector haben, müssen Sie dies tun "[Wechseln Sie zwischen ihnen](#)".

Wenn Sie Amazon S3 Buckets im gleichen AWS-Konto haben, in dem Sie den Connector erstellt haben, wird automatisch eine Amazon S3-Arbeitsumgebung auf dem Canvas angezeigt. "[Erfahren Sie mehr darüber, was Sie mit dieser Arbeitsumgebung tun können](#)".

#### **Connector in einer AWS-Regierungsregion erstellen**

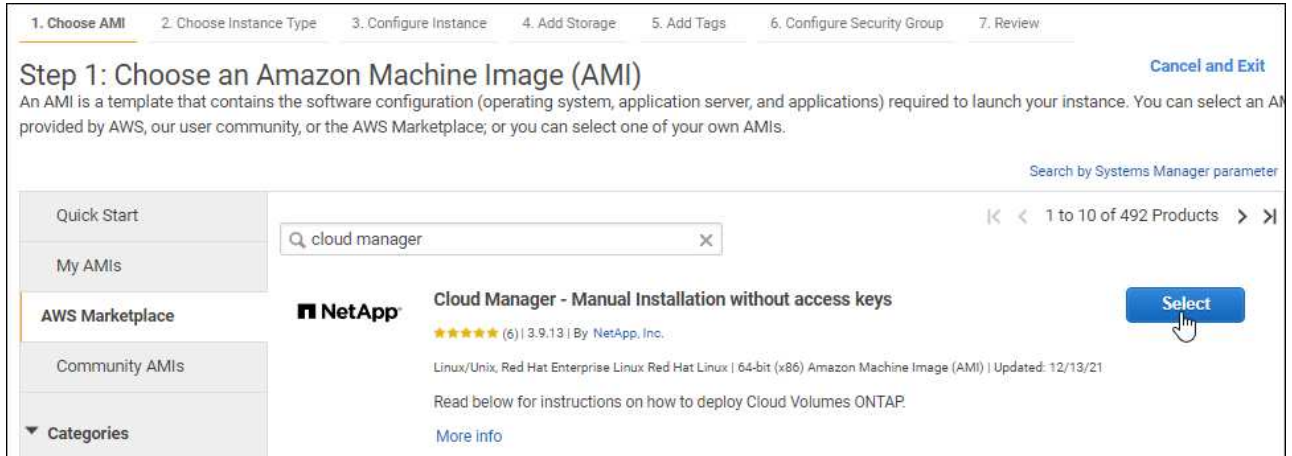
Für die Implementierung des Connectors in einer AWS Government-Region müssen Sie den EC2 Service besuchen und das BlueXP-Angebot im AWS Marketplace auswählen.

#### **Schritte**

1. Einrichten von Berechtigungen in AWS:
  - a. Erstellen Sie von der IAM-Konsole aus Ihre eigene Richtlinie, indem Sie die Inhalte von kopieren und einfügen "[Die IAM-Richtlinie für den Connector](#)".
  - b. Erstellen Sie eine IAM-Rolle mit dem Rollentyp Amazon EC2, und hängen Sie die im vorherigen Schritt erstellte Richtlinie an die Rolle an.
2. Gehen Sie zum BlueXP Angebot im AWS Marketplace.

Der IAM-Benutzer muss über AWS Marketplace-Berechtigungen zum Abonnieren und Abbestellen verfügen.

- a. Öffnen Sie den EC2-Dienst und wählen Sie **Launch Instance** aus.
- b. Wählen Sie **AWS Marketplace** aus.
- c. Suchen Sie nach BlueXP, und wählen Sie das Angebot aus.



- d. Klicken Sie Auf **Weiter**.

3. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:

- **Wählen Sie einen Instanztyp:** Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.xlarge wird empfohlen).

"Prüfen Sie die Anforderungen an die Instanz".

- **Instanzdetails konfigurieren:** Wählen Sie eine VPC und ein Subnetz aus, wählen Sie die IAM-Rolle aus, die Sie in Schritt 1 erstellt haben, aktivieren Sie den Terminierungsschutz (empfohlen) und wählen Sie andere Konfigurationsoptionen aus, die Ihren Anforderungen entsprechen.

Number of instances	1	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2   VPC4QA (default)	<a href="#">Create new VPC</a>
Subnet	subnet-39536c13   QASubnet1   us-east-1b 155 IP Addresses available	<a href="#">Create new subnet</a>
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<a href="#">Create new Capacity Reservation</a>
IAM role	Cloud_Manager	<a href="#">Create new IAM role</a>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	

- **Speicher hinzufügen:** Behalten Sie die Standard-Speicheroptionen.
- **Tags hinzufügen:** Geben Sie bei Bedarf Tags für die Instanz ein.
- **Sicherheitsgruppe konfigurieren:** Geben Sie die erforderlichen Verbindungsmethoden für die Connector-Instanz an: SSH, HTTP und HTTPS.
- **Review:** Überprüfen Sie Ihre Auswahl und klicken Sie auf **Start**.

AWS startet die Software mit den angegebenen Einstellungen. Die Connector-Instanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

- Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung zur Verbindungsinstanz hat, und geben Sie die folgende URL ein:

`https://ipaddress[]`

- Richten Sie nach der Anmeldung den Konnektor ein:
  - Geben Sie den NetApp Account an, der mit dem Connector verknüpft werden soll.  
["Informationen zu NetApp Accounts"](#).
  - Geben Sie einen Namen für das System ein.





Der Connector ist jetzt mit Ihrem NetApp Konto installiert und eingerichtet.

Wenn Sie BlueXP verwenden möchten, öffnen Sie Ihren Webbrowser und stellen Sie eine Verbindung zur IP-Adresse der Connector-Instanz her: [https://ipaddress\[\]](https://ipaddress[])

Da der Connector in einer Regierungsregion eingesetzt wurde, ist er von nicht zugänglich <https://cloudmanager.netapp.com>.

#### **Offener Port 3128 für AutoSupport-Meldungen**

Wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen möchten, in dem keine ausgehende Internetverbindung verfügbar ist, konfiguriert BlueXP Cloud Volumes ONTAP automatisch für die Verwendung des Connectors als Proxyserver.

Die einzige Anforderung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors *eingehende* -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie die Standardsicherheitsgruppe für Cloud Volumes ONTAP verwenden, sind keine Änderungen an der Sicherheitsgruppe erforderlich. Wenn Sie aber strenge ausgehende Regeln für Cloud Volumes ONTAP definieren möchten, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

## Erstellen Sie einen Connector aus dem Azure Marketplace

Für eine kommerzielle Azure-Region ist es am besten, einen Connector direkt aus BlueXP zu erstellen, aber Sie können einen Connector im Azure Marketplace starten, falls Sie es bevorzugen. Für Azure-Regierungsregionen kann der Connector nicht über die BlueXP SaaS-Website in einer Regierungsregion bereitgestellt werden. Die nächste Option ist daher der Azure Marketplace.



Sie können die Connector-Software auch auf einem bestehenden Linux-Host in Ihrem Netzwerk oder in der Cloud herunterladen und installieren. ["Erfahren Sie, wie Sie den Connector auf einem vorhandenen Linux-Host installieren"](#).

### Erstellen eines Connectors in Azure

Implementieren Sie den Connector in Azure mithilfe des Images im Azure Marketplace. Melden Sie sich dann bei Connector an, um Ihren NetApp Account anzugeben.

#### Schritte

1. Wechseln Sie im Azure Marketplace auf die Seite NetApp Connector VM.
  - ["Azure Marketplace-Seite für kommerzielle Regionen"](#)
  - ["Azure Marketplace-Seite für Azure Government Regions"](#)
2. Klicken Sie auf **Jetzt holen** und klicken Sie dann auf **Weiter**.
3. Klicken Sie im Azure-Portal auf **Erstellen** und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

Beachten Sie beim Konfigurieren der VM Folgendes:

- Der Connector kann mit Festplatten der Festplatte oder der SSD optimal arbeiten.
- Wählen Sie eine VM-Größe aus, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen DS3 v2.

["VM-Anforderungen prüfen"](#).

- Für die Netzwerksicherheitsgruppe benötigt der Connector eingehende Verbindungen unter Verwendung von SSH, HTTP und HTTPS.

["Erfahren Sie mehr über die Regeln für Sicherheitsgruppen für den Connector"](#).

- Aktivieren Sie unter **Management** \* \* die vom System zugewiesene verwaltete Identität\* für den Connector, indem Sie **ein** wählen.

Diese Einstellung ist wichtig, da sich die Virtual Machine Connector mit Azure Active Directory identifizieren kann, ohne dass Anmeldedaten vorhanden sind. ["Erfahren Sie mehr über Managed Identitäten für Azure Ressourcen"](#).

4. Überprüfen Sie auf der Seite **Überprüfen + erstellen** Ihre Auswahl und klicken Sie auf **Erstellen**, um die Bereitstellung zu starten.

Azure stellt die virtuelle Maschine mit den angegebenen Einstellungen bereit. Die virtuelle Maschine und die Connector-Software sollten in etwa fünf Minuten ausgeführt werden.

5. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung mit der virtuellen Verbindungsmaschine hat, und geben Sie die folgende URL ein:

[https://ipaddress\[\]](https://ipaddress[])

6. Richten Sie nach der Anmeldung den Konnektor ein:
- Geben Sie den NetApp Account an, der mit dem Connector verknüpft werden soll.

["Informationen zu NetApp Accounts"](#).

- Geben Sie einen Namen für das System ein.



Der Connector ist jetzt mit Ihrem NetApp Konto installiert und eingerichtet.

Wenn sich der Connector in einer kommerziellen Azure-Region befindet, öffnen Sie einen Webbrowser, und gehen Sie zu <https://cloudmanager.netapp.com> Um den Connector mit BlueXP zu verwenden.

Wenn sich der Connector in einer Region der Azure-Regierung befindet, können Sie BlueXP verwenden, indem Sie Ihren Webbrowser öffnen und eine Verbindung zur IP-Adresse der Connector-Instanz herstellen: [https://ipaddress\[\]](https://ipaddress[])

Da der Connector in einer Regierungsregion eingesetzt wurde, ist er von nicht zugänglich <https://cloudmanager.netapp.com>.

## Azure-Berechtigungen werden gewährt

Bei der Implementierung des Connectors in Azure sollten Sie a aktiviert haben "[Vom System zugewiesene verwaltete Identität](#)". Sie müssen nun die erforderlichen Azure-Berechtigungen erteilen, indem Sie eine benutzerdefinierte Rolle erstellen und dann die Rolle der virtuellen Connector-Maschine für ein oder mehrere Abonnements zuweisen.

### 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.

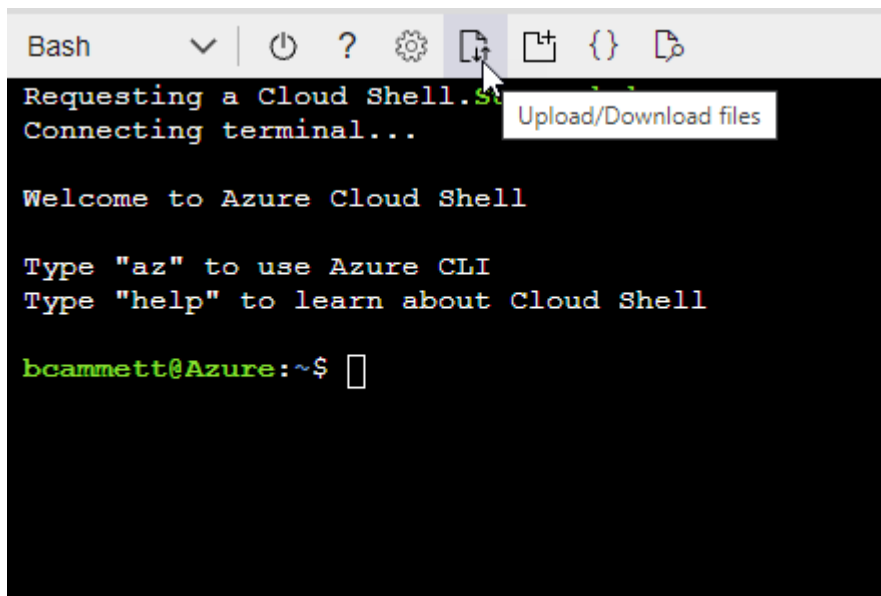
### Beispiel

```
"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. Weisen Sie der virtuellen Verbindungsmaschine die Rolle für eine oder mehrere Abonnements zu:
  - a. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP-Systeme bereitstellen möchten.
  - b. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
  - c. Wählen Sie auf der Registerkarte \* Role\* die Rolle **BlueXP Operator** aus und klicken Sie auf **Next**.



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

- d. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
  - Weisen Sie einer \* verwalteten Identität\* Zugriff zu.
  - Klicken Sie auf **Mitglieder auswählen**, wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde, wählen Sie **Virtuelle Maschine** und wählen Sie dann die virtuelle Connector-Maschine aus.
  - Klicken Sie Auf **Auswählen**.
  - Klicken Sie Auf **Weiter**.
- e. Klicken Sie auf **Review + Assign**.
- f. Wenn Sie Cloud Volumes ONTAP von zusätzlichen Abonnements aus implementieren möchten, wechseln Sie zu diesem Abonnement, und wiederholen Sie diese Schritte.

Der Connector verfügt nun über die Berechtigungen, die die IT für das Management von Ressourcen und Prozessen in Ihrer Public Cloud-Umgebung benötigt. BlueXP verwendet diesen Connector automatisch, wenn Sie neue Arbeitsumgebungen erstellen. Aber wenn Sie mehr als einen Connector haben, müssen Sie dies tun ["Wechseln Sie zwischen ihnen"](#).

Wenn Sie Azure Blob Storage in demselben Azure Konto haben, in dem Sie den Connector erstellt haben, wird automatisch eine Azure Blob Arbeitsumgebung auf dem Canvas angezeigt. ["Erfahren Sie mehr darüber, was Sie mit dieser Arbeitsumgebung tun können"](#).

### Offener Port 3128 für AutoSupport-Meldungen

Wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen möchten, in dem keine ausgehende Internetverbindung verfügbar ist, konfiguriert BlueXP Cloud Volumes ONTAP automatisch für die Verwendung des Connectors als Proxyserver.

Die einzige Anforderung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors **eingehende** -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie die Standardsicherheitsgruppe für Cloud Volumes ONTAP verwenden, sind keine Änderungen an der Sicherheitsgruppe erforderlich. Wenn Sie aber strenge ausgehende Regeln für Cloud Volumes ONTAP

definieren möchten, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

## Installieren Sie den Connector auf einem vorhandenen Linux-Host mit Internetzugang

Die häufigste Möglichkeit zur Erstellung eines Connectors liegt direkt über BlueXP oder über den Markt eines Cloud-Providers. Sie haben jedoch die Möglichkeit, die Connector-Software auf einem bestehenden Linux-Host in Ihrem Netzwerk oder in der Cloud herunterzuladen und zu installieren. Diese Schritte sind spezifisch für Hosts mit Internetzugang.

["Erfahren Sie mehr über andere Möglichkeiten zur Bereitstellung eines Connectors"](#).



Wenn Sie ein Cloud Volumes ONTAP-System in Google Cloud erstellen möchten, dann müssen Sie über einen Connector verfügen, der auch in Google Cloud läuft. Es kann kein Connector verwendet werden, der in AWS, Azure oder lokal ausgeführt wird.

### Host-Anforderungen prüfen

Die Connector-Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Port-Anforderungen usw. erfüllt.

### Ein dedizierter Host ist erforderlich

Der Connector wird nicht auf einem Host unterstützt, der für andere Anwendungen freigegeben ist. Der Host muss ein dedizierter Host sein.

### CPU

4 Kerne oder 4 vCPUs

### RAM

14 GB

### Instanztyp für AWS EC2

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.xlarge.

### Azure VM-Größe

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen DS3 v2.

### GCP-Maschinentyp

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n2-Standard-4.

Der Connector wird in Google Cloud auf einer VM-Instanz mit einem unterstützten Betriebssystem unterstützt ["Geschirmte VM-Funktionen"](#)

### Unterstützte Betriebssysteme

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9

- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Das Red Hat Enterprise Linux System muss beim Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Connector-Installation nicht auf Repositories zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.

## Hypervisor

Ein Bare Metal- oder gehosteter Hypervisor, der für die Ausführung von CentOS oder Red hat Enterprise Linux zertifiziert ist <https://access.redhat.com/certified-hypervisors>["Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"^]

## Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

## Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

## Outbound-Internetzugang

Das Installationsprogramm für den Connector muss während der Installation auf die folgenden URLs zugreifen:

- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) oder <https://hub.docker.com>

Der Host versucht möglicherweise, während der Installation Betriebssystempakete zu aktualisieren. Der Host kann verschiedene Spiegelungsstandorte für diese Betriebssystempakete kontaktieren.

## Den Stecker einbauen

Nachdem Sie sich vergewissern, dass Sie über einen unterstützten Linux-Host verfügen, können Sie die Connector-Software erwerben und dann installieren.

Zur Installation des Connectors sind Root-Berechtigungen erforderlich.

## Über diese Aufgabe

- Die Installation installiert die AWS Befehlszeilen-Tools (awscli), um Recovery-Verfahren durch den NetApp Support zu ermöglichen.

Wenn Sie eine Meldung erhalten, dass die Installation des awscli fehlgeschlagen ist, können Sie die Meldung ignorieren. Der Steckverbinder kann ohne Werkzeuge erfolgreich betrieben werden.

- Das Installationsprogramm, das auf der NetApp Support-Website verfügbar ist, kann möglicherweise eine frühere Version sein. Nach der Installation aktualisiert sich der Connector automatisch, wenn eine neue Version verfügbar ist.

## Schritte

1. Laden Sie die Connector-Software von der herunter ["NetApp Support Website"](#), Und dann kopieren Sie es auf den Linux-Host.

Informationen zum Verbinden und Kopieren der Datei auf eine EC2-Instanz in AWS finden Sie unter ["AWS Documentation: Herstellen einer Verbindung zu Ihrer Linux-Instanz mithilfe von SSH"](#).

2. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x OnCommandCloudManager-V3.9.19.sh
```

3. Führen Sie das Installationsskript aus.

Wenn Sie über einen Proxy-Server verfügen, müssen Sie die unten aufgeführten Befehlsparameter eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

```
./OnCommandCloudManager-V3.9.19.sh [silent] [proxy=ipaddress]  
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

*Silent* führt die Installation aus, ohne dass Sie zur Information aufgefordert werden.

*Proxy* ist erforderlich, wenn sich der Host hinter einem Proxy-Server befindet.

*proxyport* ist der Port für den Proxy-Server.

*Proxyuser* ist der Benutzername für den Proxy-Server, wenn eine grundlegende Authentifizierung erforderlich ist.

*Proxypwd* ist das Passwort für den von Ihnen angegebenen Benutzernamen.

4. Wenn Sie nicht den Silent-Parameter angegeben haben, geben Sie **Y** ein, um mit der Installation fortzufahren.

Der Connector ist jetzt installiert. Am Ende der Installation wird der Connector-Dienst (occm) zweimal neu gestartet, wenn Sie einen Proxy-Server angegeben haben.

5. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

`https://ipaddress[]`

*Ipaddress* kann abhängig von der Konfiguration des Hosts localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Connector beispielsweise ohne öffentliche IP-Adresse in der Public Cloud befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-Host hat.

6. Anmelden oder anmelden.

7. Wenn Sie den Connector in Google Cloud installiert haben, richten Sie ein Servicekonto ein, das über die Berechtigungen verfügt, die BlueXP zum Erstellen und Verwalten von Cloud Volumes ONTAP-Systemen in Projekten benötigt.

- a. ["Rolle in GCP anlegen"](#) Dazu gehören die im definierten Berechtigungen ["Connector-Richtlinie für GCP"](#).



- b. "Erstellen Sie ein GCP-Service-Konto und wenden Sie die benutzerdefinierte Rolle an, die Sie gerade erstellt haben".
  - c. "Verknüpfen Sie dieses Servicekonto mit der Connector-VM".
  - d. Wenn Sie Cloud Volumes ONTAP in anderen Projekten implementieren möchten, "Gewähren Sie Zugriff, indem Sie dem Projekt das Servicekonto mit der Rolle BlueXP hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.
8. Richten Sie nach der Anmeldung BlueXP ein:
- a. Geben Sie den NetApp Account an, der mit dem Connector verknüpft werden soll.  
"Informationen zu NetApp Accounts".
  - b. Geben Sie einen Namen für das System ein.



Der Connector ist jetzt mit Ihrem NetApp Konto installiert und eingerichtet. BlueXP verwendet diesen Connector automatisch, wenn Sie neue Arbeitsumgebungen erstellen.

Richten Sie Berechtigungen ein, damit BlueXP Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung verwalten kann:

- AWS, "Richten Sie ein AWS-Konto ein und fügen Sie es dann BlueXP hinzu"
- Azure: "Richten Sie ein Azure-Konto ein und fügen Sie es dann BlueXP hinzu"
- Google Cloud: Siehe Schritt 7 oben

## Installieren Sie den Connector On-Prem ohne Internetzugang

Sie können den Connector auf einem lokalen Linux-Host installieren, der keinen Internetzugang hat. Anschließend können Sie ONTAP-Cluster vor Ort erkennen, Daten zwischen ihnen replizieren, Volumes mit Cloud Backup sichern und mithilfe von Cloud Data Sense scannen.

Diese Installationsanweisungen richten sich speziell an den oben beschriebenen Anwendungsfall. ["Erfahren Sie mehr über andere Möglichkeiten zur Bereitstellung eines Connectors"](#).

### Host-Anforderungen prüfen

Die Connector-Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Port-Anforderungen usw. erfüllt.

### Ein dedizierter Host ist erforderlich

Der Connector wird nicht auf einem Host unterstützt, der für andere Anwendungen freigegeben ist. Der Host muss ein dedizierter Host sein.

### CPU

4 Kerne oder 4 vCPUs

### RAM

14 GB

### Unterstützte Betriebssysteme

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Das Red Hat Enterprise Linux System muss beim Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Connector-Installation nicht auf Repositories zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.

### Hypervisor

Ein Bare Metal- oder gehosteter Hypervisor, der für die Ausführung von CentOS oder Red hat Enterprise Linux zertifiziert ist <https://access.redhat.com/certified-hypervisors>["Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"^]

### Festplattentyp

Eine SSD ist erforderlich

## Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

## Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

## Docker Engine

Docker Engine Version 19 oder höher ist auf dem Host erforderlich, bevor Sie den Connector installieren.  
["Installationsanweisungen anzeigen"](#).

## Den Stecker einbauen

Nachdem Sie sich vergewissern, dass Sie über einen unterstützten Linux-Host verfügen, können Sie die Connector-Software erwerben und dann installieren.

Zur Installation des Connectors sind Root-Berechtigungen erforderlich.

## Schritte

1. Vergewissern Sie sich, dass der Docker aktiviert ist und ausgeführt wird.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. Laden Sie die BlueXP-Software von der herunter ["NetApp Support Website"](#).
3. Kopieren Sie das Installationsprogramm auf den Linux-Host.
4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.19
```

5. Führen Sie das Installationsskript aus:

```
sudo /path/cloud-manager-connector-offline-v3.9.19
```

6. Öffnen Sie einen Webbrowser, und geben Sie ein `https://ipaddress[]` Wobei *ipaddress* die IP-Adresse des Linux-Hosts ist.

Der folgende Bildschirm sollte angezeigt werden.



7. Klicken Sie auf **Neues BlueXP** einrichten und befolgen Sie die Anweisungen zur Einrichtung des Systems.
  - **Systemdetails:** Geben Sie einen Namen für den Connector und Ihren Firmennamen ein.

- **Admin-Benutzer erstellen:** Erstellen Sie den Admin-Benutzer für das System.

Dieses Benutzerkonto wird lokal auf dem System ausgeführt. Über BlueXP ist keine Verbindung zum aut0-Service verfügbar.

- **Review:** Lesen Sie die Details durch, akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Einrichten**.

8. Melden Sie sich mit dem gerade erstellten Admin-Benutzer bei BlueXP an.

Der Connector ist jetzt installiert und Sie können die BlueXP-Funktionen nutzen, die bei der Installation an dunklen Standorten verfügbar sind.

#### Was und#8217;s als Nächstes?

- ["Erkennen von On-Premises-ONTAP-Clustern"](#)

- "Replizieren von Daten zwischen lokalen ONTAP Clustern"
- "On-Premises-ONTAP-Volume-Daten werden mit Cloud-Backup in StorageGRID gesichert"
- "Scannen Sie ONTAP-Volume-Daten vor Ort mit Cloud-Data Sense"

Sobald neue Versionen der Connector-Software verfügbar sind, werden diese auf der NetApp Support Site veröffentlicht. ["Erfahren Sie, wie Sie den Connector aktualisieren können"](#).

## Suchen der System-ID für einen Konnektor

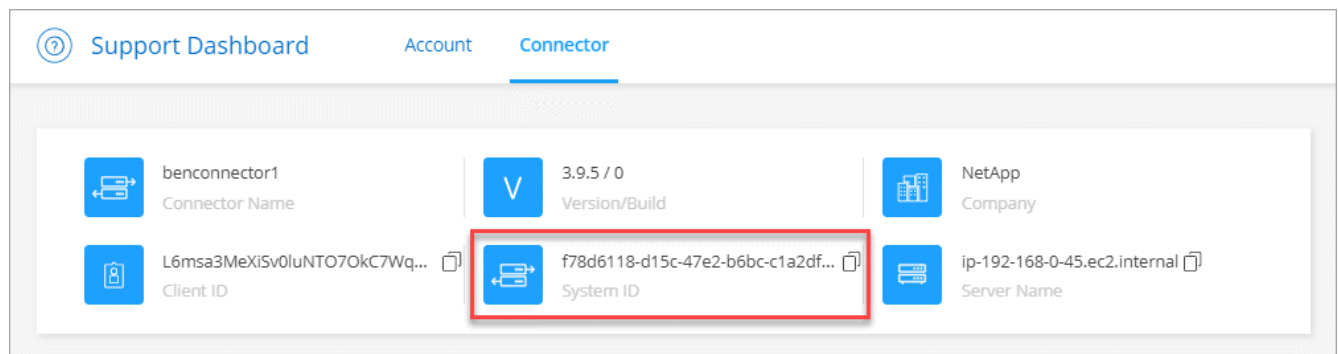
Um Ihnen bei den ersten Schritten zu helfen, bittet Ihr NetApp Mitarbeiter Sie möglicherweise um die System-ID für einen Connector. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungs Zwecke verwendet.

### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol.
2. Klicken Sie Auf **Support > Connector**.

Die System-ID wird oben angezeigt.

### Beispiel



## Verwalten vorhandener Anschlüsse

Nachdem Sie einen oder mehrere Anschlüsse erstellt haben, können Sie diese verwalten, indem Sie zwischen den Anschlüssen wechseln, eine Verbindung zur lokalen Benutzeroberfläche herstellen, die auf einem Connector ausgeführt wird, und mehr.

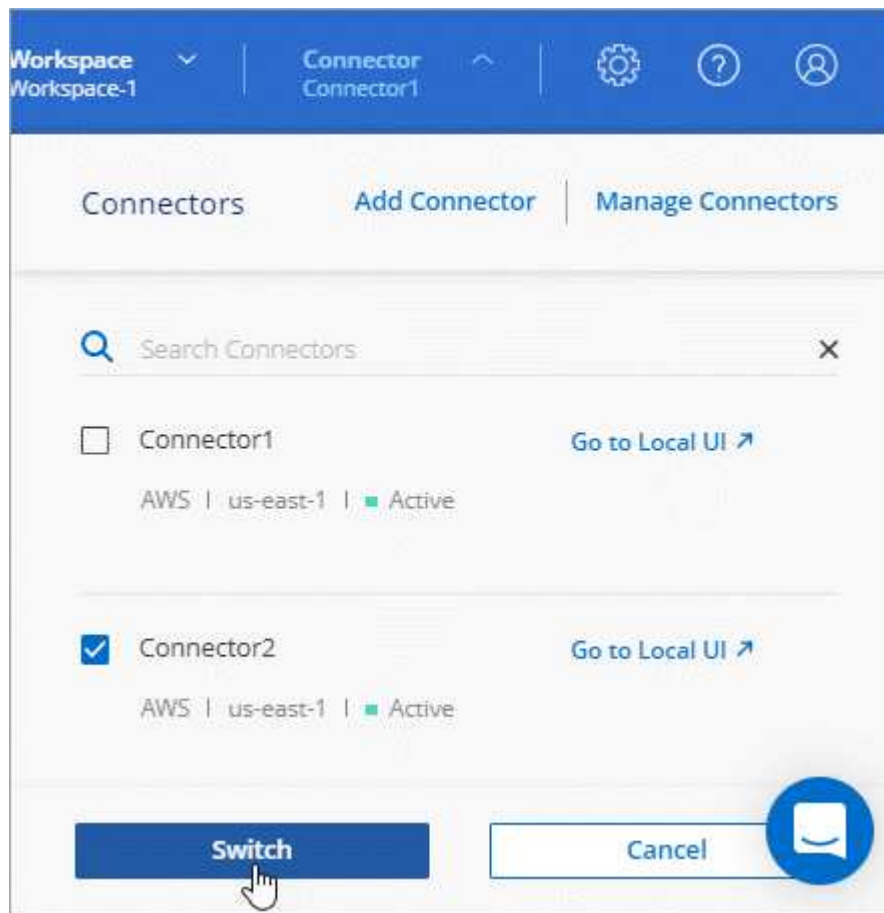
### Zwischen den Anschlüssen wechseln

Wenn Sie über mehrere Anschlüsse verfügen, können Sie zwischen diesen wechseln, um die Arbeitsumgebungen zu sehen, die mit einem bestimmten Konnektor verknüpft sind.

Nehmen wir zum Beispiel an, dass Sie in einer Multi-Cloud-Umgebung arbeiten. Möglicherweise verfügen Sie über einen Connector in AWS und einen anderen in Google Cloud. Zum Managen der Cloud Volumes ONTAP Systeme, die in diesen Clouds ausgeführt werden, müsste zwischen diesen Anschlüssen gewechselt werden.

### Schritt

1. Klicken Sie auf das Dropdown-Menü **Connector**, wählen Sie einen anderen Anschluss aus und klicken Sie dann auf **Switch**.



BlueXP aktualisiert und zeigt die Arbeitsumgebungen, die mit dem ausgewählten Connector verknüpft sind.

### Greifen Sie auf die lokale UI zu

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Wenn Sie über eine Regierungsregion oder eine Website ohne Outbound-Internetzugang auf BlueXP zugreifen, müssen Sie die lokale Benutzeroberfläche verwenden, die auf dem Connector ausgeführt wird.

### Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

`https://ipaddress[]`

*Ipaddress* kann abhängig von der Konfiguration des Hosts localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Connector beispielsweise ohne öffentliche IP-Adresse in der Public Cloud befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-Host hat.

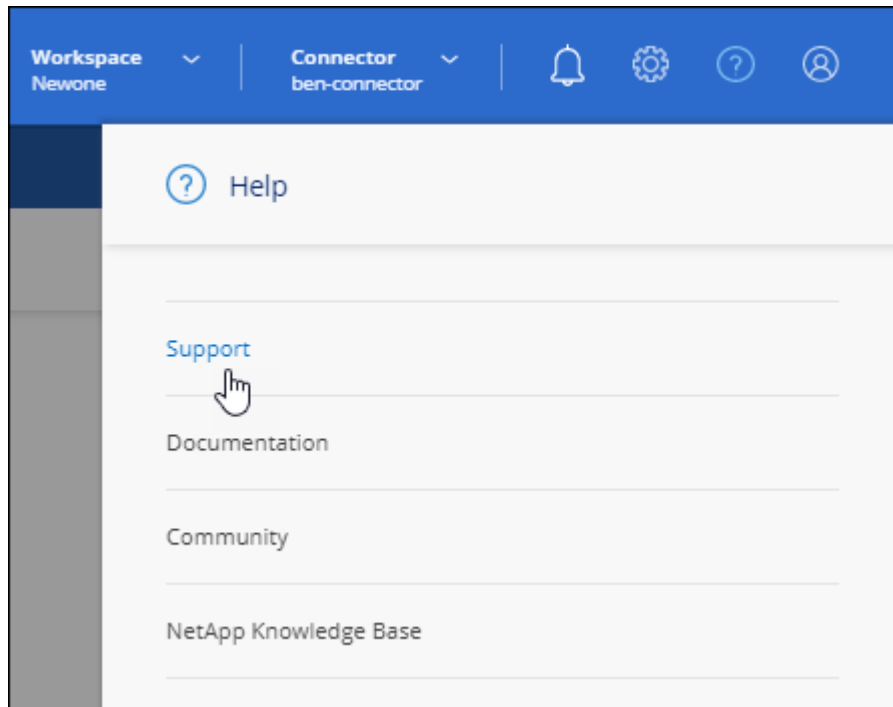
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um sich anzumelden.

### Laden Sie eine AutoSupport Nachricht herunter oder senden Sie sie

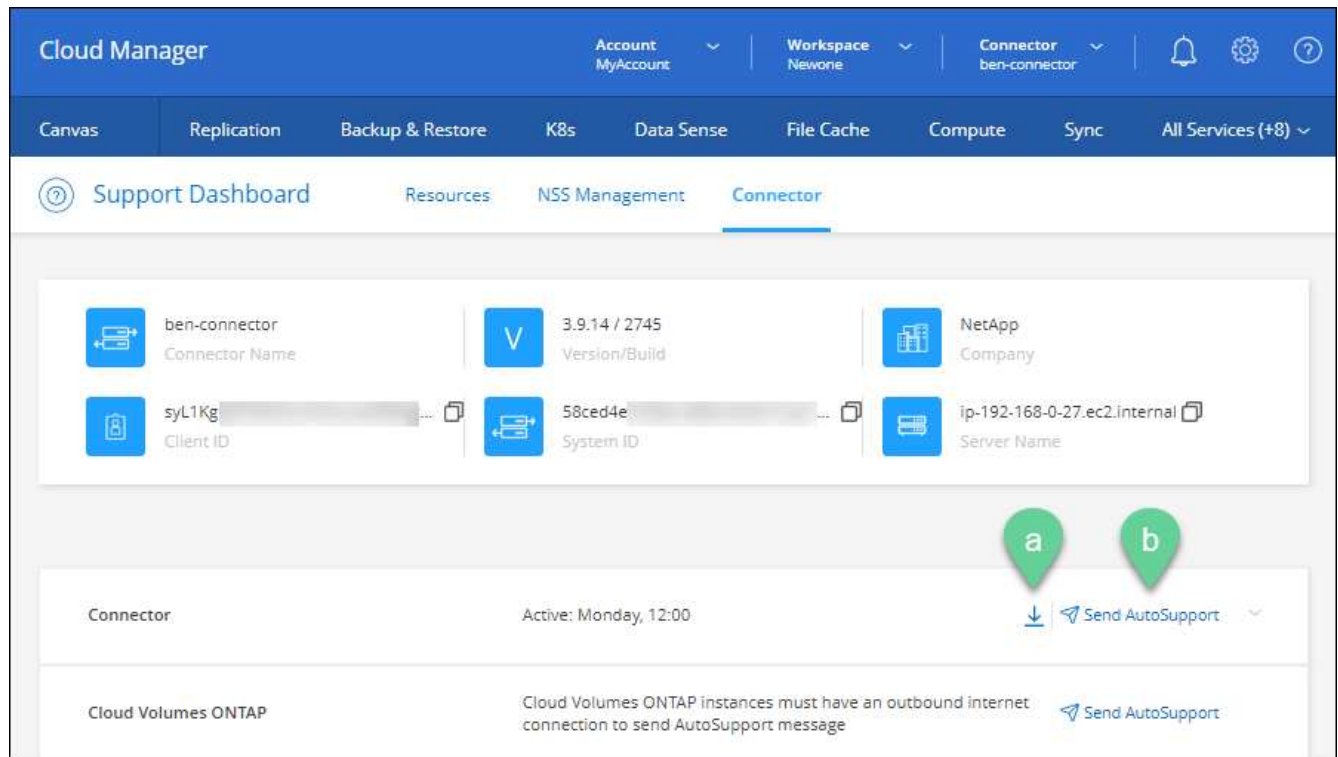
Wenn Sie Probleme haben, werden Sie möglicherweise von den Mitarbeitern von NetApp gebeten, zur Fehlerbehebung eine AutoSupport Nachricht an den NetApp Support zu senden.

## Schritte

1. Stellen Sie eine Verbindung zur lokalen Benutzeroberfläche des Connectors her, wie im Abschnitt oben beschrieben.
2. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



3. Klicken Sie Auf **Connector**.
4. Je nachdem, wie Sie die Informationen an den NetApp Support senden, wählen Sie eine der folgenden Optionen:
  - a. Wählen Sie die Option, um die AutoSupport-Nachricht auf Ihren lokalen Computer herunterzuladen. Sie können es dann auf bevorzugte Art und Weise an den NetApp Support senden.
  - b. Klicken Sie auf **AutoSupport senden**, um die Nachricht direkt an den NetApp Support zu senden.



## Stellen Sie eine Verbindung zur Linux VM her

Wenn Sie eine Verbindung zur Linux-VM herstellen möchten, auf der der Connector ausgeführt wird, können Sie dies über die Verbindungsoptionen Ihres Cloud-Providers tun.

### AWS

Als Sie die Connector-Instanz in AWS erstellt haben, haben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel angegeben. Sie können dieses Schlüsselpaar für SSH zur Instanz verwenden.

["AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"](#)

### Azure

Bei der Erstellung der Connector-VM in Azure wählen Sie die Authentifizierung mit einem Passwort oder einem öffentlichen SSH-Schlüssel aus. Verwenden Sie die Authentifizierungsmethode, die Sie für die Verbindung zur VM ausgewählt haben.

["Azure Docs: SSH in Ihre VM"](#)

### Google Cloud

Sie können keine Authentifizierungsmethode angeben, wenn Sie einen Connector in Google Cloud erstellen. Sie können eine Verbindung zur Linux VM-Instanz jedoch über die Google Cloud Console oder Google Cloud CLI (gcloud) herstellen.

["Google Cloud Docs: Verbindung zu Linux-VMs herstellen"](#)

## Sicherheitsupdates anwenden

Aktualisieren Sie das Betriebssystem auf dem Konnektor, um sicherzustellen, dass es mit den neuesten



Sicherheitsupdates gepatcht wird.

### Schritte

1. Greifen Sie auf die CLI-Shell auf dem Connector-Host zu.
2. Führen Sie folgende Befehle mit erhöhten Berechtigungen aus:

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

### Ändern Sie die IP-Adresse für einen Konnektor

Wenn es für Ihr Unternehmen erforderlich ist, können Sie die interne IP-Adresse und die öffentliche IP-Adresse der Connector-Instanz ändern, die automatisch von Ihrem Cloud-Provider zugewiesen wird.

### Schritte

1. Befolgen Sie die Anweisungen Ihres Cloud-Providers, um die lokale IP-Adresse oder die öffentliche IP-Adresse (oder beide) für die Connector-Instanz zu ändern.
2. Wenn Sie die öffentliche IP-Adresse geändert haben und eine Verbindung zur lokalen Benutzeroberfläche auf dem Connector herstellen müssen, starten Sie die Connector-Instanz neu, um die neue IP-Adresse bei BlueXP zu registrieren.
3. Wenn Sie die private IP-Adresse geändert haben, aktualisieren Sie den Backup-Speicherort für Cloud Volumes ONTAP-Konfigurationsdateien, so dass die Backups an die neue private IP-Adresse des Connectors gesendet werden.
  - a. Führen Sie den folgenden Befehl aus der Cloud Volumes ONTAP-CLI aus, um das aktuelle Backup-Ziel zu entfernen:

```
system configuration backup settings modify -destination ""
```

- b. Gehen Sie zu BlueXP, und öffnen Sie die Arbeitsumgebung.
- c. Klicken Sie auf das Menü und wählen Sie **Erweitert > Konfigurations-Backups**.
- d. Klicken Sie Auf **Backup-Ziel Festlegen**.

### Bearbeiten Sie die URIs eines Connectors

Fügen Sie die URIs für einen Konnektor hinzu und entfernen Sie sie.

### Schritte

1. Klicken Sie in der BlueXP-Kopfzeile auf das Dropdown-Menü **Connector**.
2. Klicken Sie Auf **Connectors Verwalten**.
3. Klicken Sie auf das Aktionsmenü für einen Konnektor und klicken Sie auf **URIs bearbeiten**.
4. Fügen Sie URIs hinzu und entfernen Sie sie, und klicken Sie dann auf **Anwenden**.

## Beheben Sie Download-Fehler bei Verwendung eines Google Cloud NAT-Gateways

Der Connector lädt automatisch Software-Updates für Cloud Volumes ONTAP herunter. Der Download kann fehlschlagen, wenn Ihre Konfiguration ein Google Cloud NAT Gateway verwendet. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt muss mithilfe der BlueXP API abgeschlossen werden.

### Schritt

1. SENDEN SIE EINE PUT-Anforderung an `/occm/config` mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

Der Wert für `maxDownloadSessions` kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert, den Sie verwenden sollten, hängt von Ihrer NAT-Konfiguration und der Anzahl der Sitzungen ab, die Sie gleichzeitig haben können.

["Erfahren Sie mehr über den Aufruf der `/occm/config` API"](#).

## Upgrade des Connectors On-Prem ohne Internetzugang

Wenn Sie ["Der Connector wurde auf einem lokalen Host installiert, der keinen Internetzugang hat"](#), Sie können den Connector aktualisieren, wenn eine neuere Version von der NetApp Support-Website verfügbar ist.

Der Connector muss während des Aktualisierungsvorgangs neu gestartet werden, damit die Benutzeroberfläche während des Upgrades nicht verfügbar ist.

### Schritte

1. Laden Sie die Connector-Software von der herunter ["NetApp Support Website"](#).
2. Kopieren Sie das Installationsprogramm auf den Linux-Host.
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. Führen Sie das Installationsskript aus:

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. Nachdem die Aktualisierung abgeschlossen ist, können Sie die Version des Connectors überprüfen, indem Sie **Hilfe > Support > Connector** aufrufen.

## Wie sieht es mit Software-Upgrades auf Hosts mit Internetzugang aus?

Der Connector aktualisiert seine Software automatisch auf die neueste Version, solange er ausgehenden Internetzugriff hat, um das Softwareupdate zu erhalten.

### Entfernen Sie die Anschlüsse von BlueXP

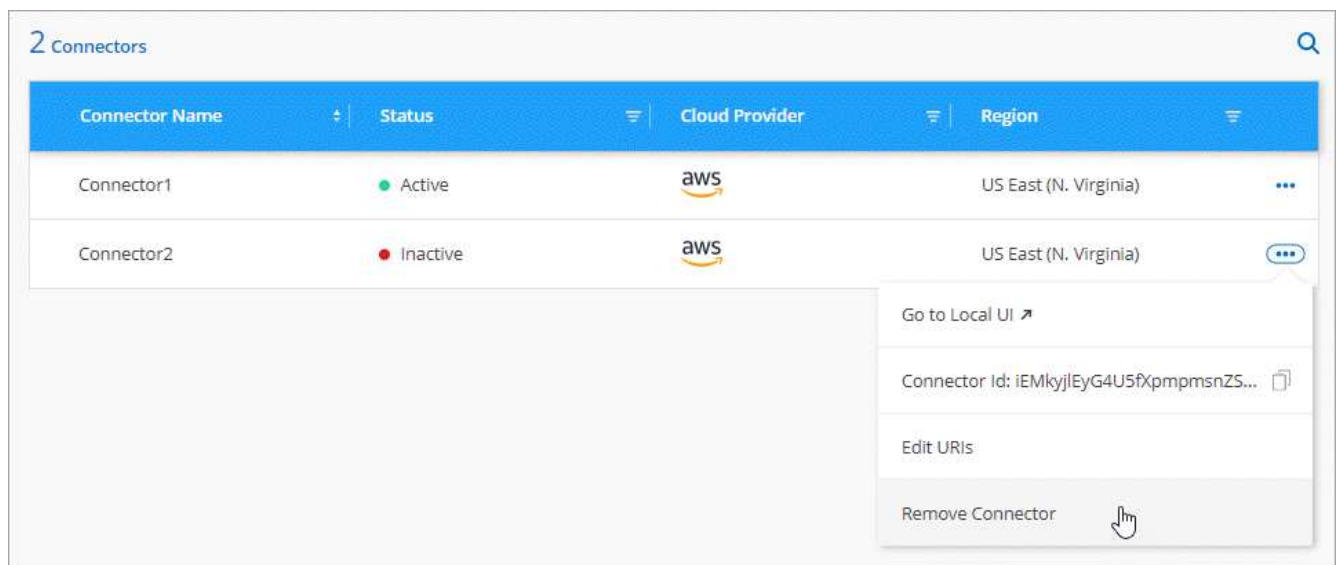
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in BlueXP entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

Beachten Sie Folgendes zum Entfernen eines Konnektors:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden. Wenn Sie einen Connector aus BlueXP entfernen, können Sie ihn nicht wieder hinzufügen

### Schritte

1. Klicken Sie in der BlueXP-Kopfzeile auf das Dropdown-Menü **Connector**.
2. Klicken Sie Auf **Connectors Verwalten**.
3. Klicken Sie auf das Aktionsmenü für einen inaktiven Konnektor und klicken Sie auf **Connector entfernen**.



4. Geben Sie den Namen des zu bestätigenden Connectors ein, und klicken Sie anschließend auf Entfernen.

BlueXP entfernt den Connector aus seinen Datensätzen.

### Deinstallieren Sie die Connector-Software

Deinstallieren Sie die Connector-Software, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Die Schritte, die Sie verwenden müssen, hängen davon ab, ob Sie den Connector auf einem Host mit Internetzugang oder einem Host in einem eingeschränkten Netzwerk installiert haben, das keinen Internetzugang hat.

## Deinstallieren Sie von einem Host mit Internetzugang

Der Online Connector enthält ein Deinstallationsskript, mit dem Sie die Software deinstallieren können.

### Schritt

1. Führen Sie auf dem Linux-Host das Deinstallationsskript aus:

```
/opt/Application/netapp/cloudmanager/bin/uninstall.sh [Silent]
```

*Silent* führt das Skript aus, ohne dass Sie zur Bestätigung aufgefordert werden.

## Deinstallieren Sie von einem Host ohne Internetzugang

Verwenden Sie diese Befehle, wenn Sie die Connector Software von der NetApp Support Site heruntergeladen und in einem Netzwerk mit beschränktem Zugriff installiert haben.

### Schritt

1. Führen Sie auf dem Linux-Host die folgenden Befehle aus:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

## Verwalten eines HTTPS-Zertifikats für sicheren Zugriff

Standardmäßig verwendet BlueXP ein selbstsigniertes Zertifikat für HTTPS-Zugriff auf die Webkonsole. Sie können ein Zertifikat installieren, das von einer Zertifizierungsstelle (CA) signiert wurde. Dies bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

### Bevor Sie beginnen

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

### Installieren eines HTTPS-Zertifikats

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat, um den sicheren Zugriff zu gewährleisten.

### Schritte

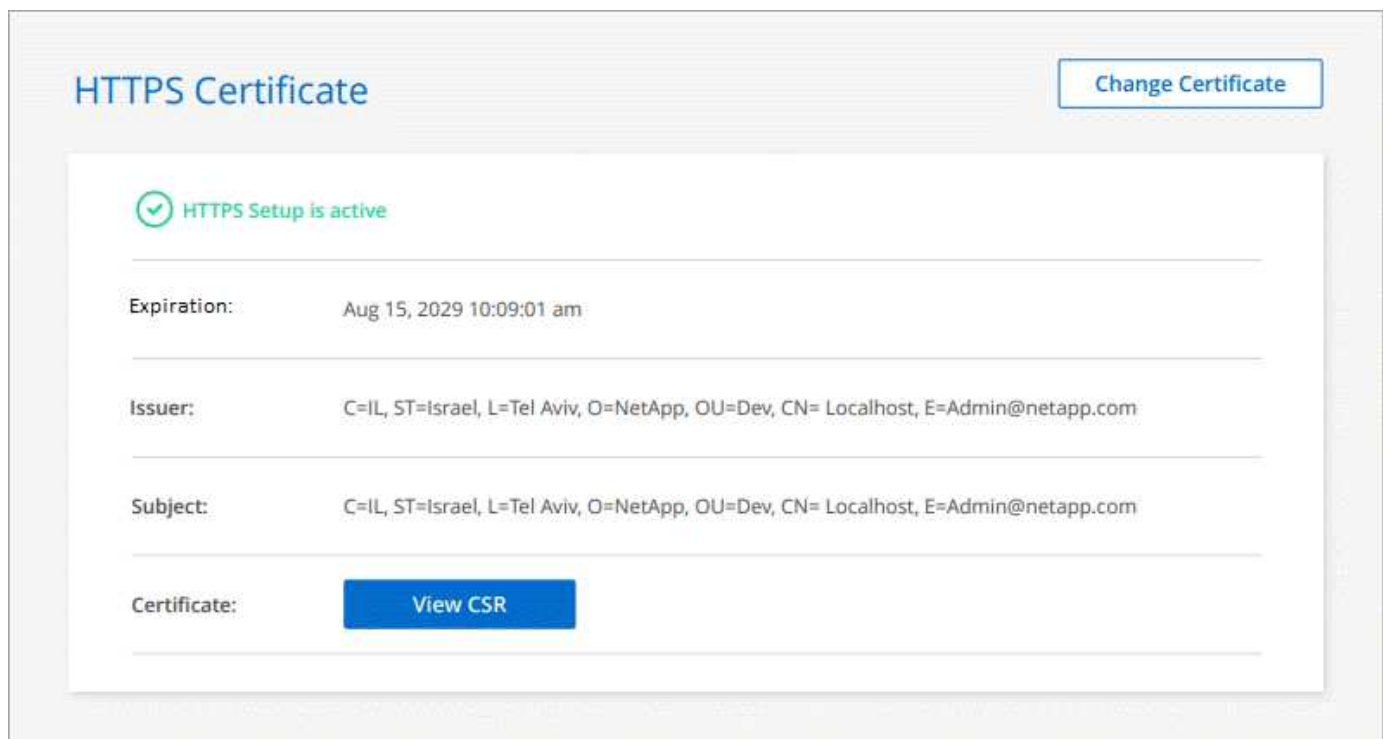
1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS-Setup**.



2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung (CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	<p>a. Geben Sie den Hostnamen oder den DNS des Connector-Hosts (dessen allgemeiner Name) ein, und klicken Sie dann auf <b>CSR erstellen</b>.</p> <p>BlueXP zeigt eine Anfrage zum Signieren des Zertifikats an.</p> <p>b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden.</p> <p>Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.</p> <p>c. Laden Sie die Zertifikatsdatei hoch und klicken Sie dann auf <b>Installieren</b>.</p>
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	<p>a. Wählen Sie <b>CA-signiertes Zertifikat installieren</b>.</p> <p>b. Laden Sie sowohl die Zertifikatsdatei als auch den privaten Schlüssel und klicken Sie dann auf <b>Installieren</b>.</p> <p>Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.</p>

BlueXP verwendet jetzt das von der Zertifizierungsstelle signierte Zertifikat, um einen sicheren HTTPS-Zugriff zu ermöglichen. Die folgende Abbildung zeigt ein BlueXP-Konto, das für den sicheren Zugriff konfiguriert ist:



### Erneuern des HTTPS-Zertifikats von BlueXP

Sie sollten das BlueXP HTTPS-Zertifikat erneuern, bevor es abläuft, um einen sicheren Zugriff auf die BlueXP-Konsole zu gewährleisten. Wenn Sie das Zertifikat nicht erneuern, bevor es abläuft, wird eine Warnung

angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

### Schritte

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

Es werden Details zum BlueXP-Zertifikat angezeigt, einschließlich des Ablaufdatums.

2. Klicken Sie auf **Zertifikat ändern** und befolgen Sie die Schritte, um eine CSR zu erstellen oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

BlueXP verwendet das neue CA-signierte Zertifikat, um sicheren HTTPS-Zugriff bereitzustellen.

## Konfigurieren eines Connectors für die Verwendung eines HTTP-Proxyservers

Wenn Sie in Ihren Unternehmensrichtlinien einen Proxyserver für die gesamte HTTP-Kommunikation mit dem Internet verwenden müssen, müssen Sie Ihre Connectors so konfigurieren, dass sie einen HTTP-Proxyserver verwenden. Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.



BlueXP unterstützt die Verwendung eines HTTPS-Proxys mit dem Connector nicht.

Die Konfiguration des Connectors zur Verwendung eines HTTP-Proxyservers bietet ausgehenden Internetzugriff, wenn keine öffentliche IP-Adresse oder ein NAT-Gateway verfügbar ist. Dieser Proxy-Server stellt nur den Connector mit einer ausgehenden Verbindung bereit. Es bietet keine Konnektivität für Cloud Volumes ONTAP Systeme.

Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten haben, konfiguriert BlueXP diese Cloud Volumes ONTAP-Systeme automatisch so, dass sie einen Proxyserver verwenden, der im Connector enthalten ist. Die einzige Anforderung besteht darin, sicherzustellen, dass die Sicherheitsgruppe des Connectors eingehende Verbindungen über Port 3128 zulässt. Sie müssen diesen Port öffnen, nachdem Sie den Connector bereitgestellt haben.

### Aktivieren Sie einen Proxy auf einem Konnektor

Wenn Sie einen Connector so konfigurieren, dass er einen Proxy-Server verwendet, verwenden dieser Connector und die von ihm verwalteten Cloud Volumes ONTAP-Systeme (einschließlich aller HA-Mediatoren) den Proxy-Server.

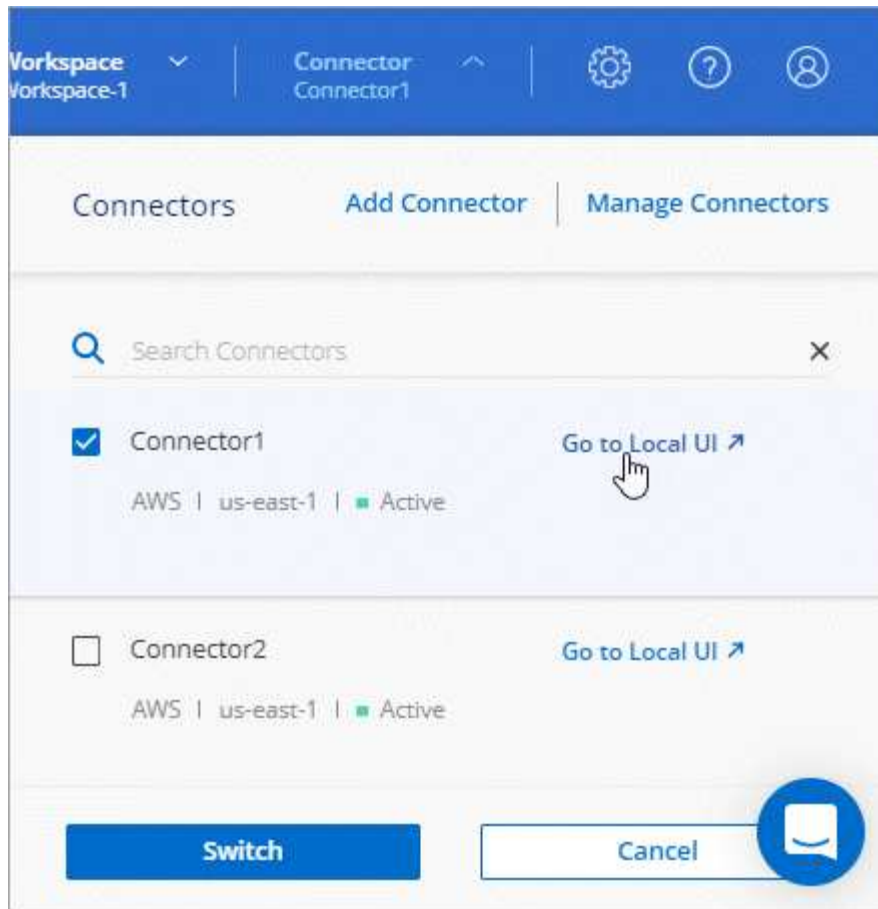
Beachten Sie, dass mit diesem Vorgang der Anschluss neu gestartet wird. Stellen Sie sicher, dass der Connector keine Operationen durchführt, bevor Sie fortfahren.

### Schritte

1. "[Melden Sie sich bei der BlueXP SaaS-Schnittstelle an](#)" Von einem Computer mit einer Netzwerkverbindung zur Instanz des Connectors.

Wenn der Connector keine öffentliche IP-Adresse hat, benötigen Sie eine VPN-Verbindung oder Sie müssen eine Verbindung von einem Jump-Host herstellen, der sich im gleichen Netzwerk wie der Connector befindet.

2. Klicken Sie auf das Dropdown-Menü **Connector** und dann auf **zur lokalen Benutzeroberfläche** für einen bestimmten Konnektor.



Die BlueXP-Schnittstelle, die auf dem Connector ausgeführt wird, wird in einem neuen Browser-Tab geladen.

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



4. Klicken Sie unter **Allgemein** auf **HTTP Proxy Configuration**.
5. Richten Sie den Proxy ein:
  - a. Klicken Sie Auf **Proxy Aktivieren**.
  - b. Geben Sie den Server mithilfe der Syntax an `http://address:port[]`
  - c. Geben Sie einen Benutzernamen und ein Kennwort an, wenn eine grundlegende Authentifizierung für den Server erforderlich ist
  - d. Klicken Sie Auf **Speichern**.



BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.

## Aktivieren Sie direkten API-Verkehr

Wenn Sie einen Proxyserver konfiguriert haben, können Sie API-Anrufe direkt an BlueXP senden, ohne über den Proxy zu gehen. Diese Option wird mit Connectors unterstützt, die in AWS, in Azure oder in Google Cloud ausgeführt werden.

### Schritte

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



2. Klicken Sie unter **Allgemein** auf **direkte API-Traffic unterstützen**.
3. Klicken Sie auf das Kontrollkästchen, um die Option zu aktivieren, und klicken Sie dann auf **Speichern**.

## Standardkonfiguration für den Konnektor

Möglicherweise möchten Sie mehr über den Connector erfahren, bevor Sie ihn bereitstellen, oder wenn Sie Probleme beheben müssen.

### Standardkonfiguration mit Internetzugang

Die folgenden Konfigurationsdetails gelten, wenn Sie den Connector von BlueXP, vom Markt Ihres Cloud-Providers oder manuell auf einem lokalen Linux-Host mit Internetzugang installiert haben.

#### AWS – Details

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Der EC2-Instanztyp ist t3.xlarge.
- Das Betriebssystem für das Image ist Red hat Enterprise Linux 7.6 (HVM).

Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Der Benutzername für die EC2 Linux Instanz ist ec2-user.
- Die Standardfestplatte des Systems ist eine 100 gib gp2-Festplatte.

#### Azure – Details

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Der VM-Typ ist DS3 v2.
- Das Betriebssystem für das Image ist CentOS 7.6.

Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.



- Die Standardfestplatte des Systems beträgt 100 gib Premium-SSD-Festplatte.

### **Google Cloud-Details**

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Die VM-Instanz ist n2-Standard-4.
- Das Betriebssystem für das Image ist Red hat Enterprise Linux 8.6.

Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Standardfestplatte des Systems beträgt eine persistente SSD-Festplatte mit 100 gib.

### **Installationsordner**

Der Installationsordner des Connectors befindet sich an folgender Stelle:

`/opt/application/netapp/cloudmanager`

### **Log-Dateien**

Protokolldateien sind in den folgenden Ordnern enthalten:

- `/opt/application/netapp/cloudmanager/log`

Die Protokolle in diesem Ordner enthalten Details zu den Konnektor- und Docker-Images.

- `/Opt/Application/netapp/CloudManager/docker_occm/Data/log`

Die Protokolle in diesem Ordner enthalten Details zu Cloud-Diensten und zum BlueXP-Dienst, der auf dem Connector ausgeführt wird.

### **Verbindungsdienst**

- Der BlueXP-Dienst heißt occm.
- Der occm-Dienst ist vom MySQL-Dienst abhängig.

Wenn der MySQL-Dienst nicht verfügbar ist, ist auch der occm-Dienst nicht verfügbar.

### **Pakete**

BlueXP installiert die folgenden Pakete auf dem Linux-Host, falls diese noch nicht installiert sind:

- 7-Zip
- AWSCLI
- Docker
- Java
- Kubectl
- MySQL

- Tridentctl
- Ziehen
- Wget

## Ports

Der Connector verwendet die folgenden Ports auf dem Linux-Host:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff
- 3306 für die BlueXP-Datenbank
- 8080 für den BlueXP API Proxy
- 8666 für die Service Manager API
- 8777 für die Health-Checker Container Service API

## Standardkonfiguration ohne Internetzugang

Die folgende Konfiguration gilt, wenn Sie den Connector manuell auf einem lokalen Linux-Host installiert haben, der keinen Internetzugang hat. ["Erfahren Sie mehr über diese Installationsoption"](#).

- Der Installationsordner des Connectors befindet sich an folgender Stelle:

`/Opt/Application/netapp/ds`

- Protokolldateien sind in den folgenden Ordnern enthalten:

`/Var/lib/docker/Volumes/ds_occmdata/data-data/log`

Die Protokolle in diesem Ordner enthalten Details zu den Konnektor- und Docker-Images.

- Alle Services werden in Docker Containern ausgeführt

Die Dienste sind abhängig vom laufenden Docker Runtime Service

- Der Connector verwendet die folgenden Ports auf dem Linux-Host:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff

## PAYGO-Abonnements und -Verträge verwalten

Wenn Sie BlueXP über den Marktplatz eines Cloud-Providers abonnieren, werden Sie auf die BlueXP-Website weitergeleitet, auf der Sie Ihr Abonnement speichern und mit bestimmten Konten verknüpfen müssen. Nach dem Abonnement können Sie jedes Abonnement über Digital Wallet verwalten.

## Ihre Abonnements anzeigen

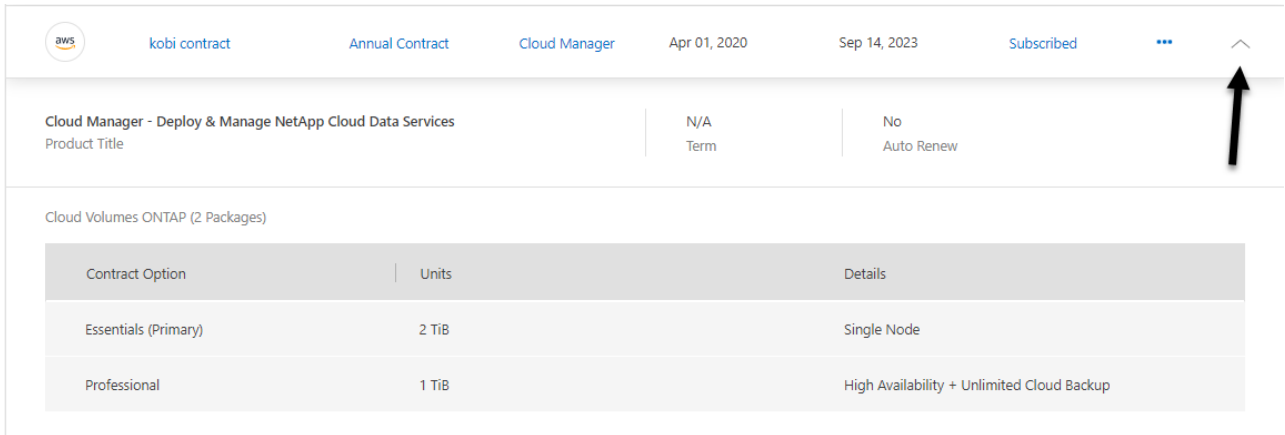
Das Digital Wallet enthält Details zu jedem PAYGO-Abonnement und einem Jahresvertrag, der mit Ihrem BlueXP-Konto und mit Astra verbunden ist (Astra nutzt den BlueXP-Gebührendienst).

## Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie **Abonnements**.

Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

3. Wenn Sie die Informationen zu Ihren Abonnements anzeigen, können Sie wie folgt mit den Details in der Tabelle interagieren:
  - Erweitern Sie eine Zeile, um weitere Details anzuzeigen.



The screenshot shows the AWS Digital Wallet interface. At the top, there's a header with the AWS logo, account name 'kobi contract', contract type 'Annual Contract', service 'Cloud Manager', start date 'Apr 01, 2020', end date 'Sep 14, 2023', and status 'Subscribed'. Below this, a table lists subscription details. The first row shows 'Cloud Manager - Deploy & Manage NetApp Cloud Data Services' with 'N/A' for the term and 'No Auto Renew' for renewal. Below this, a section titled 'Cloud Volumes ONTAP (2 Packages)' contains a table with two rows: 'Essentials (Primary)' with '2 TiB' units and 'Single Node' details, and 'Professional' with '1 TiB' units and 'High Availability + Unlimited Cloud Backup' details. A black arrow points to the expand icon (three dots) in the top right of the subscription row.

Contract Option	Units	Details
Essentials (Primary)	2 TiB	Single Node
Professional	1 TiB	High Availability + Unlimited Cloud Backup

- Klicken Sie Auf  So legen Sie fest, welche Spalten in der Tabelle angezeigt werden sollen.

Beachten Sie, dass die Spalten „Begriff“ und „Automatische Verlängerung“ standardmäßig nicht angezeigt werden. In der Spalte „Automatische Erneuerung“ werden nur Informationen zur Verlängerung von Azure-Verträgen angezeigt.

Beachten Sie Folgendes zu den in der Tabelle aufgeführten Informationen:

### Startdatum

Das Startdatum ist, wenn Sie das Abonnement erfolgreich mit Ihrem Konto verknüpft haben und der Ladevorgang gestartet wurde.

### K. A.

Wenn in der Tabelle „N/A“ angezeigt wird, sind die Informationen derzeit nicht über die API des Cloud-Providers verfügbar.

### Verträge

- Wenn Sie die Details für einen Vertrag erweitern, zeigt das Digital Wallet an, was für Ihren aktuellen Plan zur Verfügung steht: Die Vertragsoptionen und Einheiten (Kapazität oder Anzahl der Knoten).
- Das Digital Wallet identifiziert das Enddatum und gibt an, ob der Vertrag bald verlängert, bald beendet wird oder ob er bereits beendet ist.
- Wenn Sie über einen AWS-Vertrag verfügen und nach dem Startdatum eine der Optionen des Vertrags geändert haben, sollten Sie Ihre Vertragsoptionen von AWS validieren.







## Verwalten Sie Ihre Abonnements

Sie können Ihre Abonnements über das Digital Wallet verwalten, indem Sie ein Abonnement umbenennen und die Konten auswählen, die mit dem Abonnement verknüpft sind.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

### Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie **Abonnements**.
3. Klicken Sie in der Zeile auf das Aktionsmenü, das dem Abonnement entspricht, das Sie verwalten möchten.

Provider	Name	Type	Service	Start Date	End Date	Status	
	aws-sub-a2	PAYGO	Cloud Manager	Apr 02, 2020	N/A	Subscribed	
	Aleksey_aws_marketplace	Annual Contract	Astra	Oct 18, 2022	Oct 18, 2023		
	By Capacity By Node 3	PAYGO	Cloud Manager	Mar 31, 2020	N/A	Subscribed	

Associate Subscription

Rename Subscription

4. Sie können das Abonnement umbenennen oder die NetApp Konten, die dem Abonnement zugeordnet sind, verwalten.

## Cloud Storage erkannt

### Anzeigen Ihrer Amazon S3 Buckets

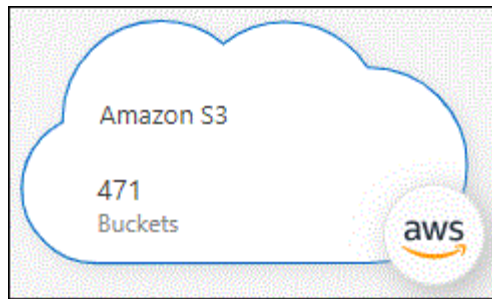
Nach der Installation eines Connectors in AWS erkennt BlueXP automatisch Informationen zu den Amazon S3 Buckets, die sich im AWS Konto befinden, in dem der Connector installiert ist. Eine Amazon S3-Arbeitsumgebung wird dem Canvas hinzugefügt, damit Sie diese Informationen anzeigen können.

Sie erhalten Details zu Ihren S3 Buckets, einschließlich Region, Zugriffsrichtlinien, Konto, Gesamt- und genutzter Kapazität, und mehr. Diese Buckets können als Ziele für Cloud-Backup, Cloud-Tiering oder Cloud Sync-Vorgänge verwendet werden. Zudem können Sie mit Cloud Data Sense diese Buckets scannen.

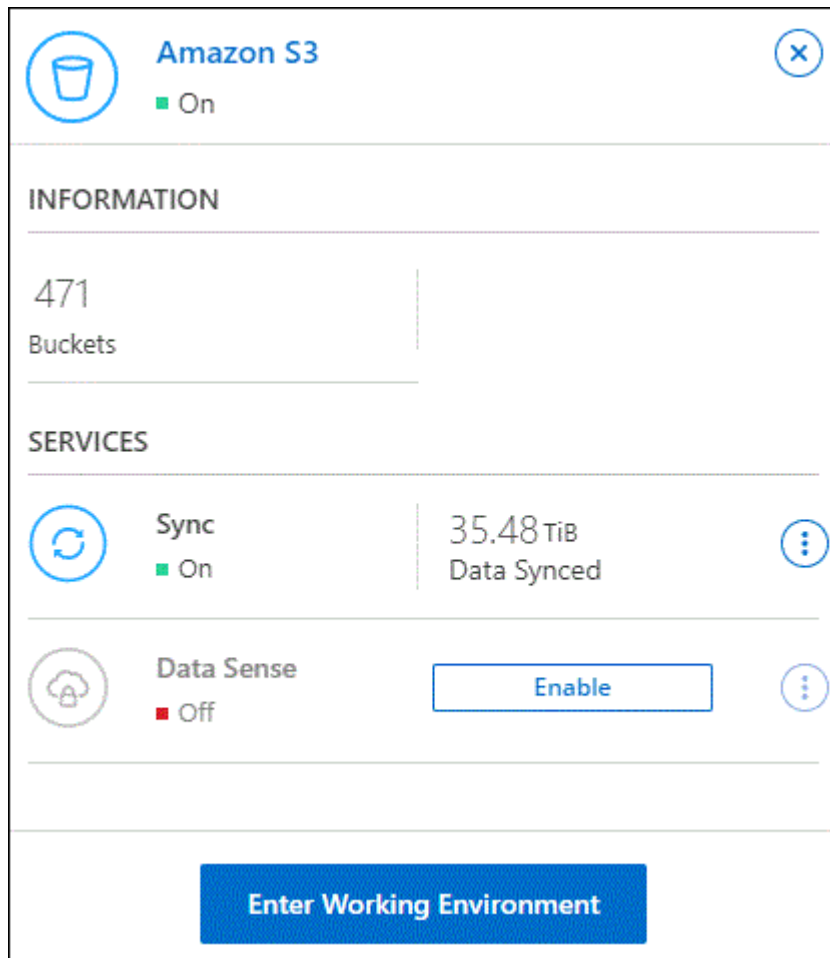
### Schritte

1. **"Installieren Sie einen Anschluss"** In dem AWS Konto, wo Sie Ihre Amazon S3 Buckets anzeigen möchten.
2. Wählen Sie im Navigationsmenü die Option **Storage > Canvas** aus.

Sie sollten bald automatisch eine Amazon S3-Arbeitsumgebung sehen.



3. Klicken Sie auf die Arbeitsumgebung, und wählen Sie eine Aktion im rechten Fensterbereich aus.



4. Klicken Sie auf **Daten synchronisieren**, um Daten mit oder von S3 Buckets zu synchronisieren.

Weitere Informationen finden Sie unter ["Überblick über den Cloud Sync Service"](#).

5. Klicken Sie auf **Aktivieren**, wenn Cloud Data Sense die S3 Buckets nach persönlichen und sensiblen Daten scannen soll.

Weitere Informationen finden Sie unter ["Erste Schritte mit Cloud Data Sense für Amazon S3"](#).

6. Klicken Sie auf **Arbeitsumgebung eingeben**, um Details zu den S3-Buckets in Ihrem AWS-Konto anzuzeigen.

Amazon S3

Overview

471 Total Buckets | 6,94 TiB Total Capacity | 23 Total Regions

471 Buckets

Bucket Name	AWS Account	Region	Creation Date	Encryption	Is Public	Size	Total Objects
athena-query-results-us-east-1	4642620614	US East (N. Virginia)	September 27, 2021	Disabled	Bucket and objects not public	35.27 GiB	3,01K
catalog-sg	4642620614	US East (N. Virginia)	October 1, 2021	Disabled	Bucket and objects not public	1.35 GiB	1,44K
cbsqa	4642620614	US East (N. Virginia)	August 9, 2021	Disabled	Public	33.95 GiB	185
template-19-ap-southeast-3	4642620614	ap-southeast-3	March 10, 2022	Enabled ⓘ	Objects can be public	21.38 KiB	3
template-7dxc-ca-central-1	4642620614	Canada (Central)	November 2, 2020	Enabled ⓘ	Objects can be public	24.01 KiB	2

## Anzeigen Ihrer Azure Blob Konten

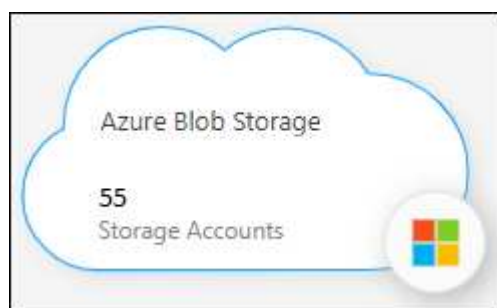
Nach der Installation eines Connectors in Azure erkennt BlueXP automatisch Informationen zu den Azure Storage-Konten, die sich in den Azure-Abonnements befinden, in denen der Connector installiert ist. Eine Azure Blob Arbeitsumgebung wird dem Canvas hinzugefügt, damit Sie diese Informationen anzeigen können.

Sie sehen Details zu Ihren Azure Storage-Konten, einschließlich Standort, Ressourcengruppe, Gesamt- und genutzter Kapazität und mehr. Diese Konten können als Ziele für Cloud-Backup, Cloud-Tiering oder Cloud Sync-Vorgänge verwendet werden.

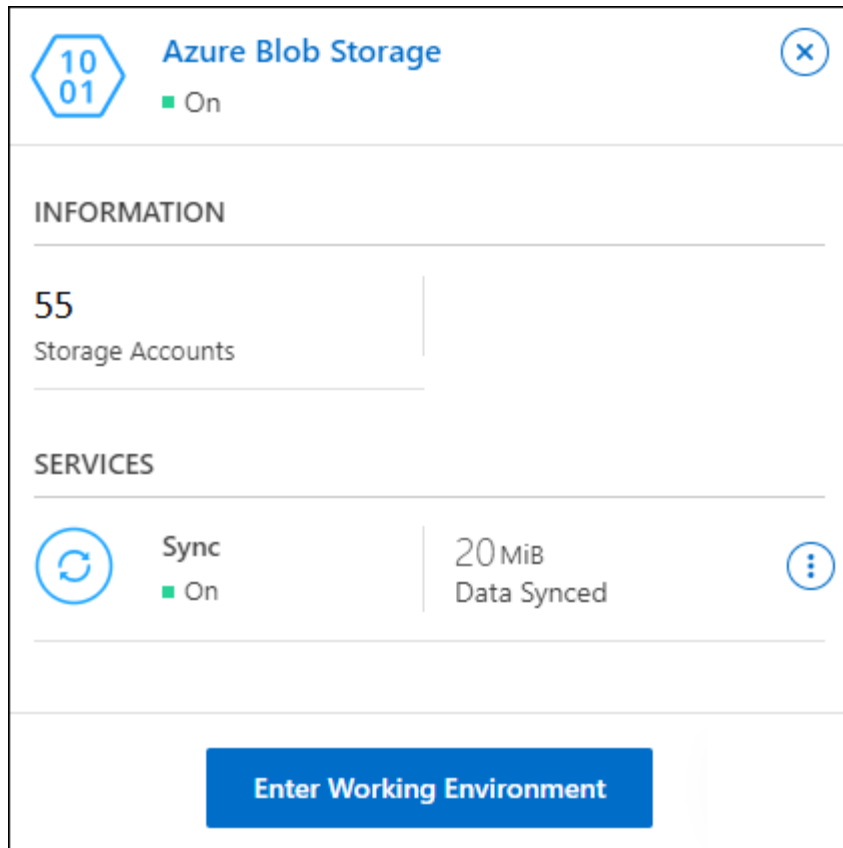
### Schritte

1. "Installieren Sie einen Anschluss" Geben Sie im Azure-Konto Ihre Azure-Storage-Konten an.
2. Wählen Sie im Navigationsmenü die Option **Storage > Canvas** aus.

Kurz danach wird eine Azure Blob Arbeitsumgebung bereitgestellt.



3. Klicken Sie auf die Arbeitsumgebung, und wählen Sie eine Aktion im rechten Fensterbereich aus.



4. Klicken Sie auf **Synchronisierungsdaten**, um Daten mit oder von Azure Blob Storage zu synchronisieren.  
Weitere Informationen finden Sie unter "[Überblick über den Cloud Sync Service](#)".
5. Klicken Sie auf **Enter Working Environment**, um Details zu den Azure Storage-Konten in Ihren Azure Blobs anzuzeigen.

Azure blob

Overview

637

Total Storage Accounts

1.5

TiB

Total Capacity

16

Total Locations

637

Storage Accounts

Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
ovu8llxvdfypxn	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	170 B
rootsa9ktpjzcm	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	950.22 GiB
scvdwjcwehswli	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	22.12 MiB
65qtx0smegmq2vt	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	170 B
bu9klxthymr1be	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	1.01 MiB
8jzsvybvjiwieww8	OCCM QA1	Canada Central	December 12, 2019	aff1-rg	170 B

## Anzeigen Ihrer Google Cloud Storage Buckets

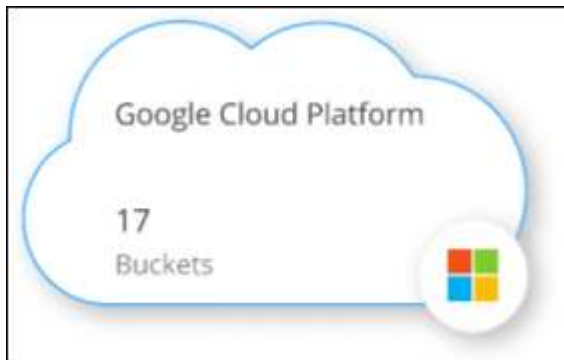
Nach der Installation eines Connectors in Google Cloud kann BlueXP automatisch Informationen über die Google Cloud Storage Buckets finden, die sich im Google-Konto befinden, in dem der Connector installiert ist. Eine Google Cloud Storage Arbeitsumgebung wird dem Canvas hinzugefügt, damit Sie diese Informationen anzeigen können.

Sie erhalten Details zu Ihren Google Cloud Storage Buckets, einschließlich Standort, Zugriffsstatus, Storage-Klasse, Gesamt- und genutzter Kapazität und mehr. Diese Buckets können als Ziele für Cloud-Backup, Cloud-Tiering oder Cloud Sync-Vorgänge verwendet werden.

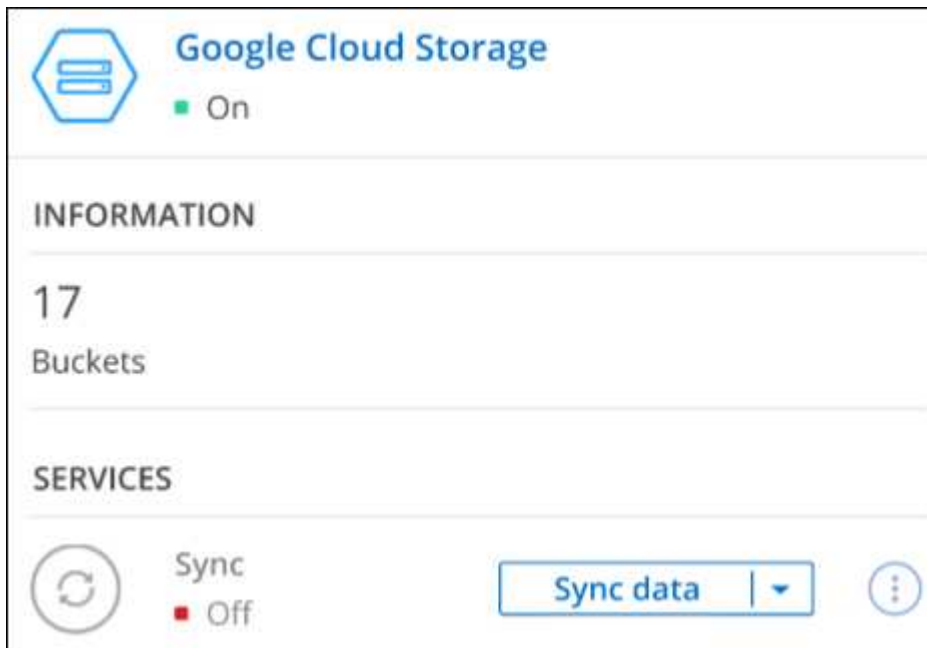
### Schritte

1. ["Installieren Sie einen Anschluss"](#) In dem Google-Konto, in dem Sie Ihre Google Cloud Storage Buckets anzeigen möchten.
2. Wählen Sie im Navigationsmenü die Option **Storage > Canvas** aus.

Kurz darauf sollten Sie automatisch eine Google Cloud Storage Arbeitsumgebung sehen.



3. Klicken Sie auf die Arbeitsumgebung, und wählen Sie eine Aktion im rechten Fensterbereich aus.

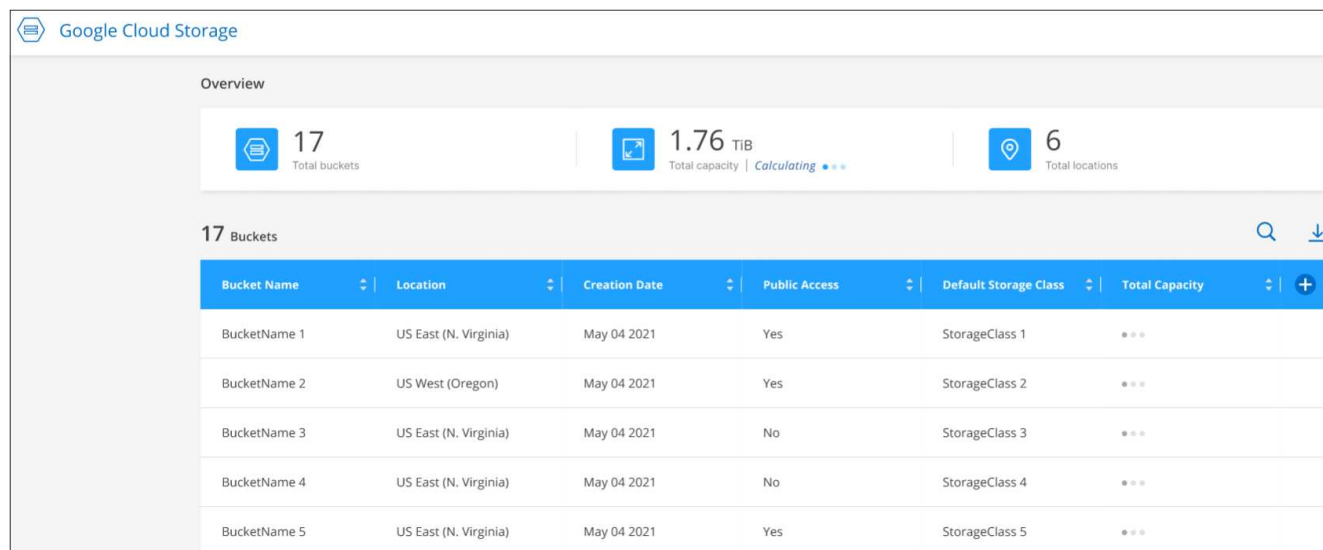




4. Klicken Sie auf **Daten synchronisieren**, um Daten mit oder von Google Cloud Storage Buckets zu synchronisieren.

Weitere Informationen finden Sie unter ["Überblick über den Cloud Sync Service"](#).

5. Klicken Sie auf **Arbeitsumgebung eingeben**, um Details zu den Buckets in Ihrem Google-Konto anzuzeigen.



Bucket Name	Location	Creation Date	Public Access	Default Storage Class	Total Capacity
BucketName 1	US East (N. Virginia)	May 04 2021	Yes	StorageClass 1	***
BucketName 2	US West (Oregon)	May 04 2021	Yes	StorageClass 2	***
BucketName 3	US East (N. Virginia)	May 04 2021	No	StorageClass 3	***
BucketName 4	US East (N. Virginia)	May 04 2021	No	StorageClass 4	***
BucketName 5	US East (N. Virginia)	May 04 2021	Yes	StorageClass 5	***

## AWS Zugangsdaten

### AWS Zugangsdaten und Berechtigungen

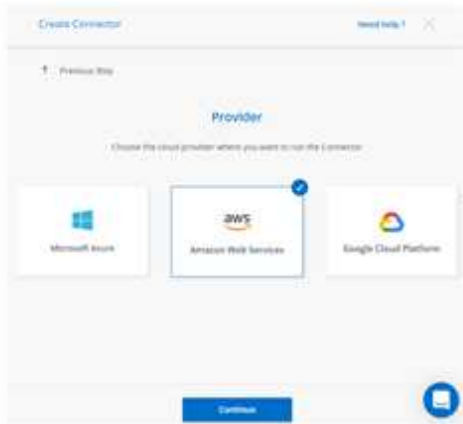
Mit BlueXP können Sie die AWS Zugangsdaten für die Bereitstellung von Cloud Volumes ONTAP auswählen. Alle Cloud Volumes ONTAP Systeme können über die ersten AWS Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

#### Erste AWS Zugangsdaten

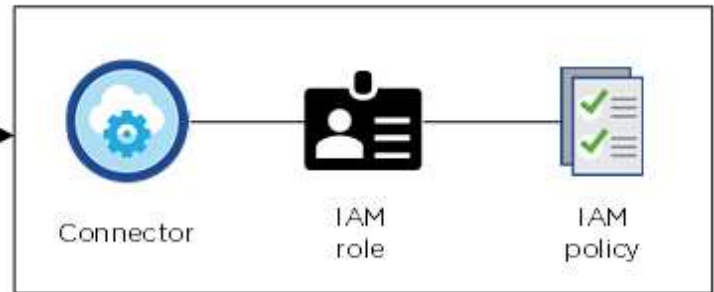
Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie das ARN einer IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer bereitstellen. Die verwendete Authentifizierungsmethode muss über die erforderlichen Berechtigungen für die Bereitstellung der Connector-Instanz in AWS verfügen. Die erforderlichen Berechtigungen werden im aufgeführt ["Connector-Implementierungsrichtlinie für AWS"](#).

Wenn BlueXP die Connector-Instanz in AWS startet, erstellt sie eine IAM-Rolle und ein Instanzprofil für die Instanz. Zudem wird eine Richtlinie angehängt, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. ["Überprüfen Sie, wie BlueXP die Berechtigungen verwendet"](#).

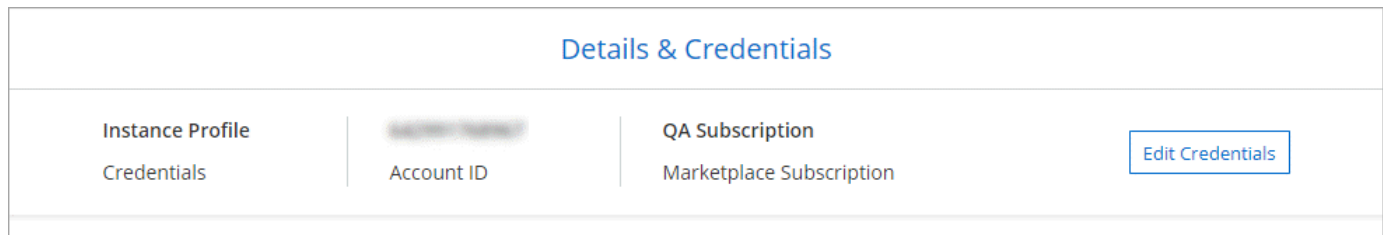
## Cloud Manager



## AWS account



BlueXP wählt die AWS Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:

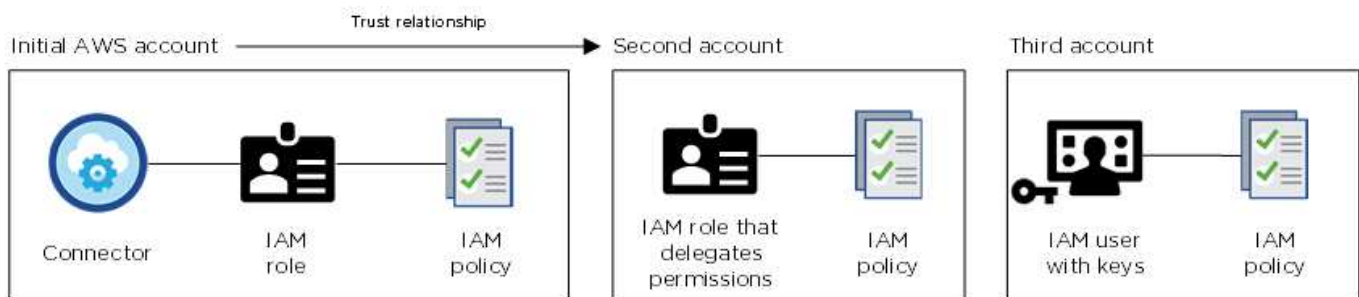


## Zusätzliche AWS Zugangsdaten

Es gibt zwei Möglichkeiten, zusätzliche AWS Zugangsdaten hinzuzufügen.

### Fügen Sie AWS Zugangsdaten zu einem vorhandenen Connector hinzu

Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Accounts starten möchten, haben Sie eine der Möglichkeiten ["AWS Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen"](#). Die folgende Abbildung zeigt zwei zusätzliche Konten: Eines mit Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto und ein weiteres über die AWS Schlüssel eines IAM-Benutzers:



Das würden Sie dann tun ["Fügen Sie die Kontoanmeldeinformationen zu BlueXP hinzu"](#) Indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

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

**Fügen Sie AWS Zugangsdaten direkt in BlueXP hinzu**

Beim Hinzufügen neuer AWS Zugangsdaten zu BlueXP stehen die erforderlichen Berechtigungen zum Erstellen und Managen einer FSX für ONTAP Arbeitsumgebung oder zum Erstellen eines Connectors zur Verfügung.

### **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 AWS von der bereitstellen ["AWS Marketplace"](#) Und das können Sie auch ["Installieren Sie den Steckverbinder vor Ort"](#).

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

Bei On-Premises-Implementierungen können Sie keine IAM-Rolle für das BlueXP-System einrichten, Sie können aber auch Berechtigungen wie bei zusätzlichen AWS-Konten bereitstellen.

### **Wie kann ich meine AWS Zugangsdaten sicher drehen?**

Wie oben beschrieben, können Sie mit BlueXP auf verschiedene Weise AWS Zugangsdaten bereitstellen: Eine mit der Konnektor-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel.

Bei den ersten beiden Optionen verwendet BlueXP den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dies ist die Best Practice, also automatisch und sicher.

Wenn Sie BlueXP mit AWS-Zugriffsschlüsseln zur Verfügung stellen, sollten Sie die Schlüssel durch Aktualisierung in BlueXP in einem regelmäßigen Intervall drehen. Es handelt sich hierbei um einen vollständig manuellen Prozess.

## Managen Sie AWS Anmeldeinformationen und Abonnements für BlueXP

Fügen Sie AWS Anmeldedaten hinzu und managen Sie diese, damit BlueXP über die erforderlichen Berechtigungen verfügt, um Cloud-Ressourcen in Ihren AWS-Konten bereitzustellen und zu managen. Wenn Sie mehrere AWS-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen AWS Zugangsdaten zuweisen.

### Überblick

AWS Zugangsdaten können zu einem vorhandenen Connector oder direkt zu BlueXP hinzugefügt werden:

- Fügen Sie einem vorhandenen Connector zusätzliche AWS Zugangsdaten hinzu

Wenn Sie einem vorhandenen Connector AWS Zugangsdaten hinzufügen, erhalten Sie die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen in Ihrer Public-Cloud-Umgebung. [credentials to a Connector](#), Erfahren Sie, wie Sie AWS Zugangsdaten zu einem Connector hinzufügen.

- Fügen Sie zur Erstellung eines Connectors AWS Credentials zu BlueXP hinzu

Wenn Sie BlueXP neue AWS-Anmeldeinformationen hinzufügen, erhalten Sie mit BlueXP die erforderlichen Berechtigungen zum Erstellen eines Connectors. [credentials to BlueXP for creating a Connector](#), Erfahren Sie, wie Sie AWS Zugangsdaten zu BlueXP hinzufügen.

- Fügen Sie AWS Credentials zu BlueXP für FSX für ONTAP hinzu

Wenn Sie BlueXP neue AWS Zugangsdaten hinzufügen, erhalten Sie unter BlueXP die erforderlichen Berechtigungen zum Erstellen und Managen von FSX für ONTAP. ["Erfahren Sie, wie Sie Berechtigungen für FSX für ONTAP einrichten"](#)

### So drehen Sie die Anmeldeinformationen

Mit BlueXP können Sie AWS Zugangsdaten auf verschiedene Arten bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel. ["Weitere Informationen zu AWS Zugangsdaten und Berechtigungen"](#).

Bei den ersten beiden Optionen verwendet BlueXP den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dieser Prozess ist die Best Practice, da er automatisch und sicher ist.

Wenn Sie BlueXP mit AWS-Zugriffsschlüsseln zur Verfügung stellen, sollten Sie die Schlüssel durch Aktualisierung in BlueXP in einem regelmäßigen Intervall drehen. Es handelt sich hierbei um einen vollständig manuellen Prozess.

### Anmeldedaten zu einem Konnektor hinzufügen

Fügen Sie AWS Zugangsdaten zu einem Connector hinzu, damit die IT auch über die erforderlichen Berechtigungen zum Management von Ressourcen und Prozessen in Ihrer Public Cloud-Umgebung verfügt. Sie können entweder den ARN einer IAM-Rolle in einem anderen Konto bereitstellen oder AWS-Zugriffsschlüssel bereitstellen.

## Berechtigungen erteilen

Bevor Sie AWS Zugangsdaten zu einem Connector hinzufügen, müssen Sie die erforderlichen Berechtigungen bereitstellen. Mithilfe der Berechtigungen kann BlueXP Ressourcen und Prozesse innerhalb dieses AWS Kontos verwalten. Wie Sie die Berechtigungen bereitstellen, hängt davon ab, ob Sie BlueXP mit dem ARN einer Rolle in einem vertrauenswürdigen Konto oder AWS Schlüsseln bereitstellen möchten.



Wenn Sie einen Connector von BlueXP bereitgestellt haben, hat BlueXP automatisch AWS-Anmeldeinformationen für das Konto hinzugefügt, in dem Sie den Connector bereitgestellt haben. Dieses Erstkonto wird nicht hinzugefügt, wenn Sie den Connector über den AWS Marketplace bereitgestellt haben oder wenn Sie die Connector-Software manuell auf einem vorhandenen System installieren. "[Weitere Informationen zu AWS Zugangsdaten und Berechtigungen](#)".

## Auswahl

- permissions by assuming an IAM role in another account
- permissions by providing AWS keys

## Erteilen Sie Berechtigungen, indem Sie eine IAM-Rolle in einem anderen Konto übernehmen

Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Connector-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie BlueXP über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

### Schritte

1. Rufen Sie die IAM-Konsole im Zielkonto auf, in dem Sie dem Connector Berechtigungen erteilen möchten.
2. Klicken Sie unter Zugriffsverwaltung auf **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

Gehen Sie wie folgt vor:

- Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
  - Wählen Sie **ein weiteres AWS-Konto** aus, und geben Sie die ID des Kontos ein, auf dem sich die Connector-Instanz befindet.
  - Erstellen Sie die erforderlichen Richtlinien, indem Sie den Inhalt von kopieren und einfügen "[Die IAM-Richtlinien für den Connector](#)".
3. Kopieren Sie die Rolle ARN der IAM-Rolle, damit Sie sie später in BlueXP einfügen können.

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können die Anmeldeinformationen jetzt einem Connector hinzufügen.

## Erteilen Sie Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Wenn Sie BlueXP für einen IAM-Benutzer AWS-Schlüssel bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die BlueXP IAM-Richtlinie definiert die AWS Aktionen und Ressourcen, die BlueXP verwenden darf.

### Schritte

1. Erstellen Sie Richtlinien von der IAM-Konsole aus, indem Sie die Inhalte von kopieren und einfügen "[Die IAM-Richtlinien für den Connector](#)".

## "AWS Dokumentation: Erstellung von IAM-Richtlinien"

2. Hängen Sie die Richtlinien an eine IAM-Rolle oder einen IAM-Benutzer an.

- ["AWS Documentation: Erstellung von IAM-Rollen"](#)
- ["AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"](#)

Das Konto verfügt nun über die erforderlichen Berechtigungen. ,Sie können die Anmeldeinformationen jetzt einem Connector hinzufügen.

### Fügen Sie die Anmeldeinformationen hinzu

Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie die Anmeldedaten für dieses Konto einem bestehenden Connector hinzufügen. Damit können Sie Cloud Volumes ONTAP-Systeme in diesem Konto mit demselben Connector starten.

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.

### Schritte

1. Stellen Sie sicher, dass derzeit in BlueXP der richtige Connector ausgewählt ist.
2. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



3. Klicken Sie auf **Anmeldeinformationen hinzufügen** und befolgen Sie die Schritte im Assistenten.
  - a. **Anmeldeort:** Wählen Sie **Amazon Web Services > Connector**.
  - b. **Identifizierungsdaten definieren:** Geben Sie den ARN (Amazon Resource Name) einer vertrauenswürdigen IAM-Rolle an, oder geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
  - c. **Marketplace-Abonnement:** Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

Damit Cloud Volumes ONTAP mit stündlichem Tarif (PAYGO) oder mit einem Jahresvertrag bezahlt werden kann, müssen AWS Zugangsdaten über den AWS Marketplace mit einem Abonnement für Cloud Volumes ONTAP verknüpft werden.

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

Sie können jetzt bei der Erstellung einer neuen Arbeitsumgebung auf eine andere Gruppe von Anmeldeinformationen von der Seite Details und Anmeldeinformationen wechseln:

### Fügen Sie für die Erstellung eines Connectors Anmeldeinformationen zu BlueXP hinzu

Fügen Sie BlueXP die AWS Zugangsdaten hinzu, indem Sie das ARN einer IAM-Rolle bereitstellen, die BlueXP die zur Erstellung eines Connectors erforderlichen Berechtigungen erteilt. Sie können diese Anmeldeinformationen beim Erstellen eines neuen Connectors auswählen.

#### Einrichten der IAM-Rolle

Richten Sie eine IAM-Rolle ein, mit der BlueXP SaaS die Rolle übernehmen kann.

#### Schritte

1. Wechseln Sie im Zielkonto zur IAM-Konsole.
2. Klicken Sie unter Zugriffsverwaltung auf **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

Gehen Sie wie folgt vor:

- Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
- Wählen Sie **ein weiteres AWS-Konto** und geben Sie die ID des BlueXP SaaS: 952013314444 ein
- Erstellen Sie eine Richtlinie, die die zum Erstellen eines Connectors erforderlichen Berechtigungen enthält.
  - ["Zeigen Sie die für FSX für ONTAP erforderlichen Berechtigungen an"](#)
  - ["Sehen Sie sich die Richtlinie zur Bereitstellung von Konnektor an"](#)

3. Kopieren Sie die Rolle ARN der IAM-Rolle, sodass Sie sie im nächsten Schritt in BlueXP einfügen können.

Die IAM-Rolle verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu BlueXP hinzufügen.



## Fügen Sie die Anmeldeinformationen hinzu

Nachdem Sie die IAM-Rolle mit den erforderlichen Berechtigungen angegeben haben, fügen Sie die Rolle ARN zu BlueXP hinzu.

Wenn Sie gerade die IAM-Rolle erstellt haben, kann es ein paar Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

### 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 **Amazon Web Services > BlueXP**.
  - b. **Anmeldedaten definieren:** Geben Sie den ARN (Amazon Resource Name) der IAM-Rolle an.
  - c. **Review:** Bestätigen Sie die Angaben zu den neuen Anmeldedaten und klicken Sie auf **Hinzufügen**.

Sie können die Anmeldeinformationen jetzt beim Erstellen eines neuen Connectors verwenden.

## AWS Abonnement zuordnen

Nachdem Sie Ihre AWS Zugangsdaten zu BlueXP hinzugefügt haben, können Sie ein AWS Marketplace Abonnement mit diesen Anmeldedaten verknüpfen. Mit dem Abonnement können Sie Cloud Volumes ONTAP auf Stundenbasis (PAYGO) oder bei Nutzung eines Jahresvertrags bezahlen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein AWS 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 AWS Marketplace Abonnement durch ein neues Abonnement ersetzen.

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

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

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

## Anmeldedaten bearbeiten

Bearbeiten Sie Ihre AWS Zugangsdaten in BlueXP, indem Sie den Kontotyp (AWS Schlüssel oder ANGEEN Rolle) ändern, indem Sie den Namen bearbeiten oder die Anmeldeinformationen selbst aktualisieren (die Schlüssel oder die Rolle ARN).



Sie können die Anmeldeinformationen für ein Instanzprofil, das einer Connector-Instanz zugeordnet ist, nicht bearbeiten.

## 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.



Sie können die Anmeldeinformationen für ein Instanzprofil nicht löschen, das einer Konnektor-Instanz zugeordnet ist.

## 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**.

# Azure Zugangsdaten

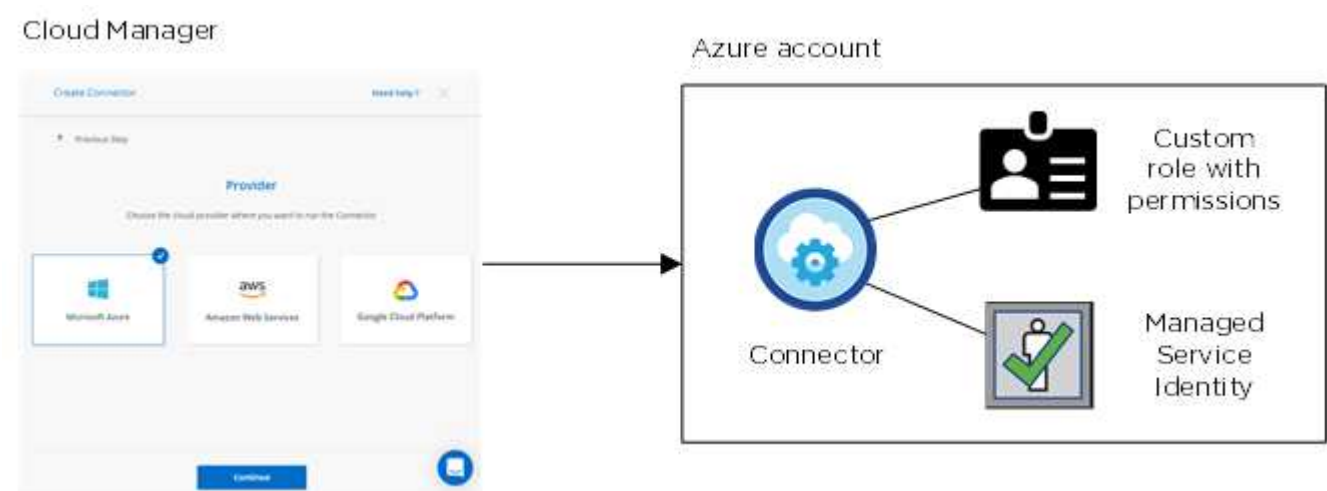
## Azure Zugangsdaten und Berechtigungen

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	

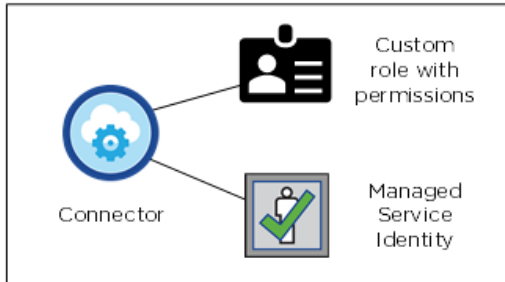
### Zusätzliche Azure-Abonnements für eine gemanagte Identität

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"](#).

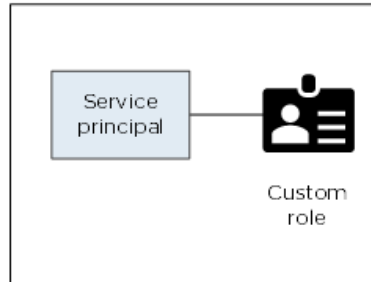
## Zusätzliche Azure Zugangsdaten

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:

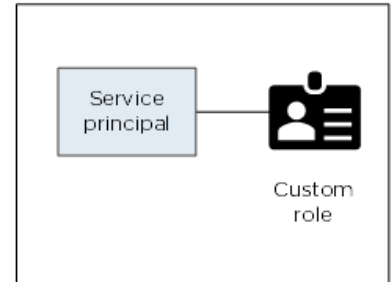
Initial Azure account



Second account



Third account



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 a dialog titled 'Edit Account & Add Subscription'. Under the 'Credentials' section, there is a text input field with a dropdown menu. The dropdown menu is open, showing three options: 'cloud-manager-app | Application ID: 57c42424-88a0-480a.', 'Managed Service Identity' (which is highlighted in blue), and '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.

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.

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.



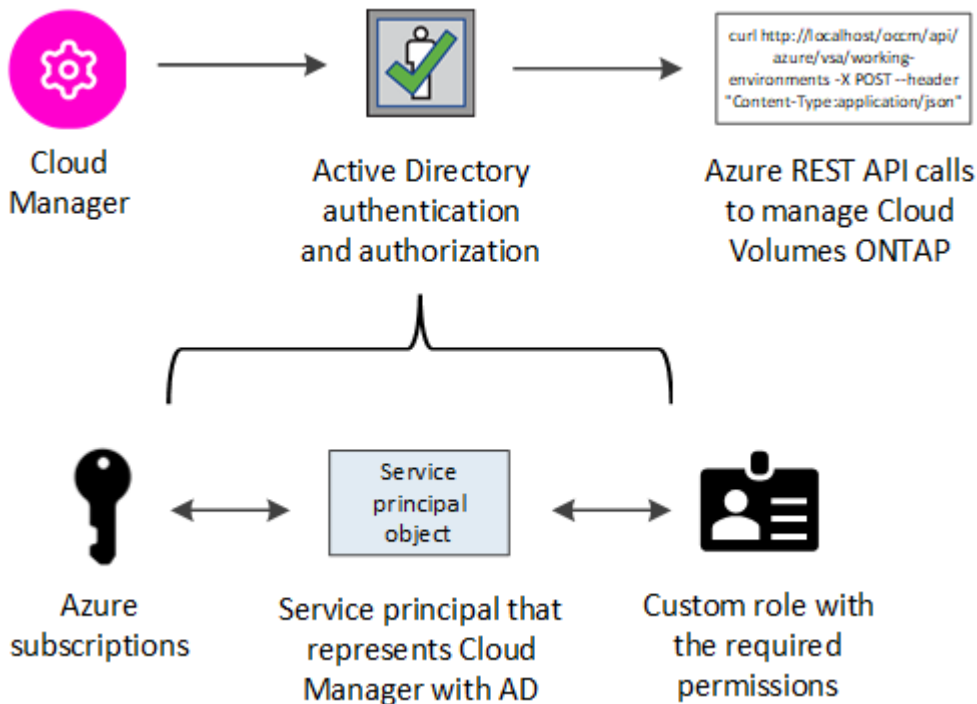
Ein erster Satz von Anmeldeinformationen wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. ["Informationen zu Azure Zugangsdaten und Berechtigungen"](#).

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.

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. an Azure Active Directory application, Erstellen Sie eine Azure Active Directory-Anwendung.
2. the application to a role, Anwendung einer Rolle zuweisen.
3. Windows Azure Service Management API permissions, Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.
4. the application ID and directory ID, Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.
5. a client secret, Erstellen Sie einen Clientschlüssel.

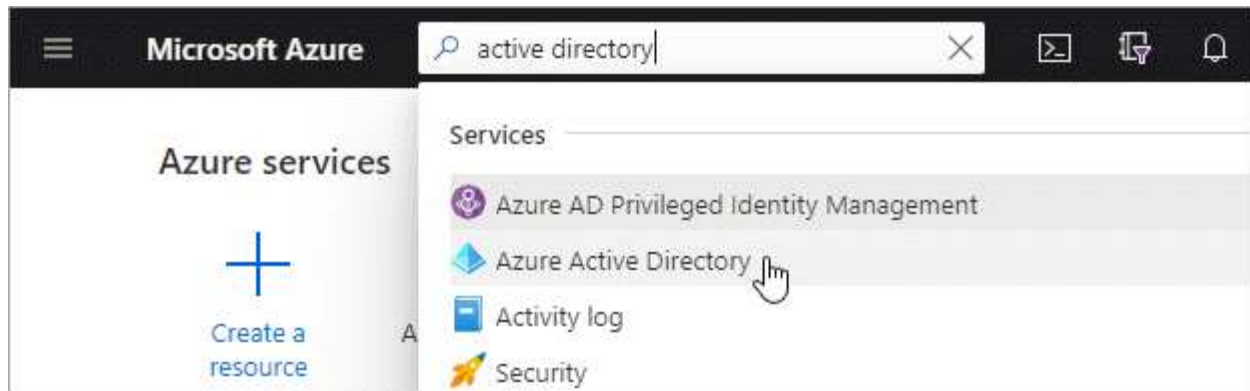
### Erstellen einer Azure Active Directory-Anwendung

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

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**.

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.

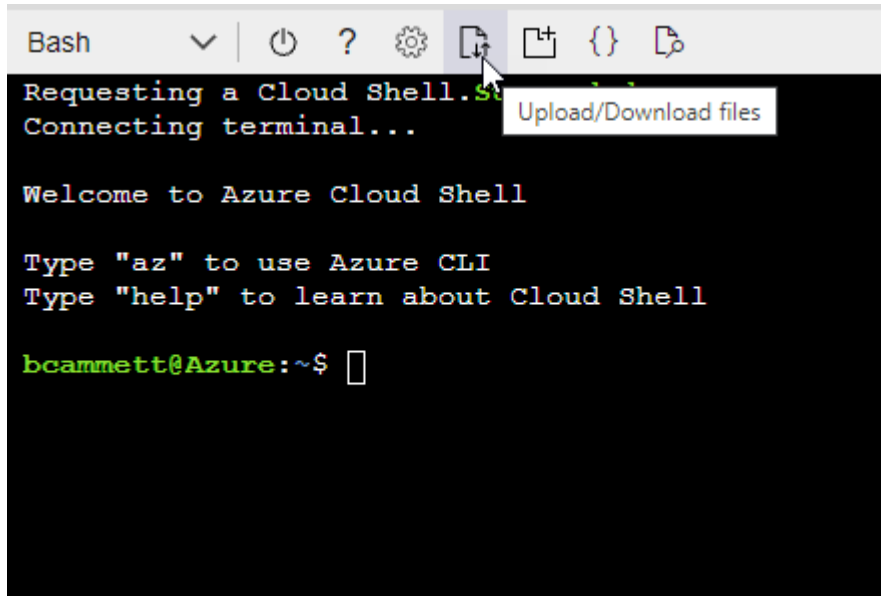
### Beispiel

```
"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:

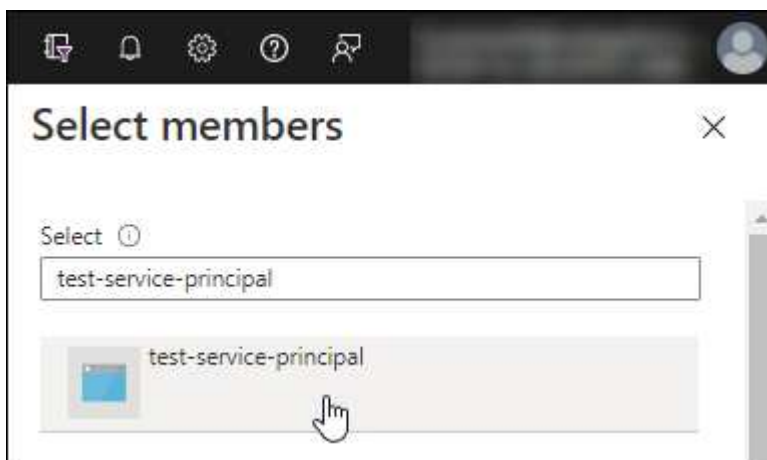
- Öffnen Sie im Azure-Portal den Service **Abonnements**.
- Wählen Sie das Abonnement aus.
- Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte \* Role\* die Rolle **BlueXP Operator** aus und klicken Sie auf **Next**.
- Führen Sie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





**Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud


**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets


**Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions


**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios


**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server


**Azure Import/Export**  
Programmatic control of import/export jobs


**Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**  
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**  
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](#)

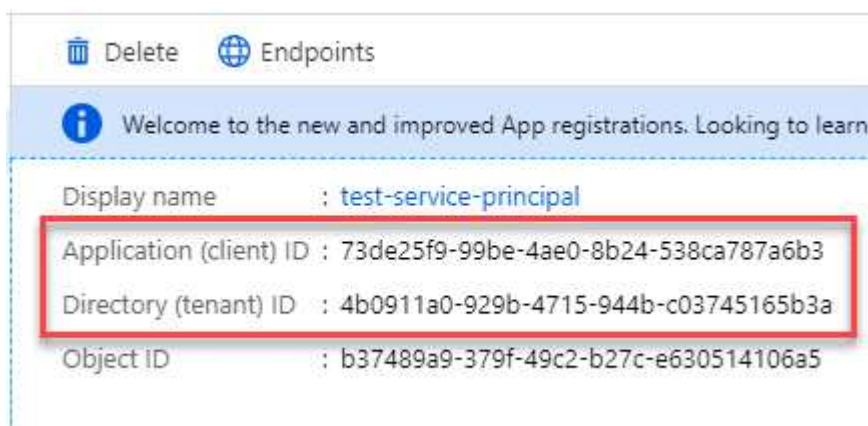
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview)	-

## 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	Copy to clipboard

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.

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.

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**.

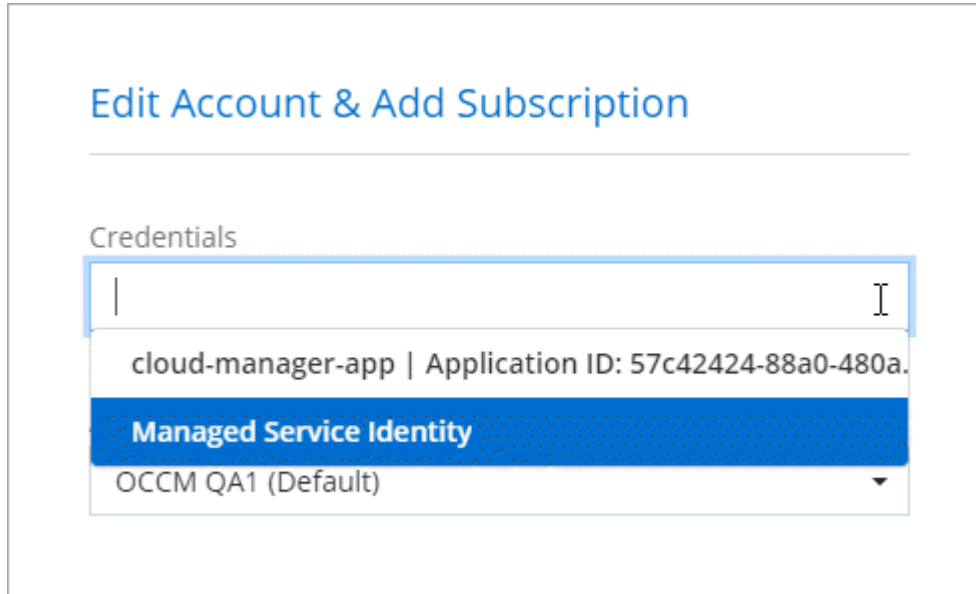


2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und befolgen Sie die Schritte im Assistenten.
  - a. **Anmeldeort:** Wählen Sie **Microsoft Azure > Connector**.
  - b. **Anmeldedaten definieren:** Geben Sie Informationen über den Azure Active Directory Service Principal ein, der die erforderlichen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

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



**Edit Account & Add Subscription**

Credentials

cloud-manager-app | Application ID: 57c42424-88a0-480a.

**Managed Service Identity**

OCCM QA1 (Default)

### 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.

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**.

## Google Cloud-Anmeldedaten

### Google Cloud Projekte, Berechtigungen und Konten

Ein Servicekonto bietet BlueXP Berechtigungen zum Bereitstellen und Verwalten von Cloud Volumes ONTAP-Systemen, die sich im selben Projekt wie der Connector befinden, oder in verschiedenen Projekten.

#### Projekt und Berechtigungen für BlueXP

Bevor Sie Cloud Volumes ONTAP in Google Cloud bereitstellen können, müssen Sie zunächst einen Connector in einem Google Cloud-Projekt bereitstellen. Der Connector kann nicht vor Ort oder bei einem anderen Cloud-Provider ausgeführt werden.

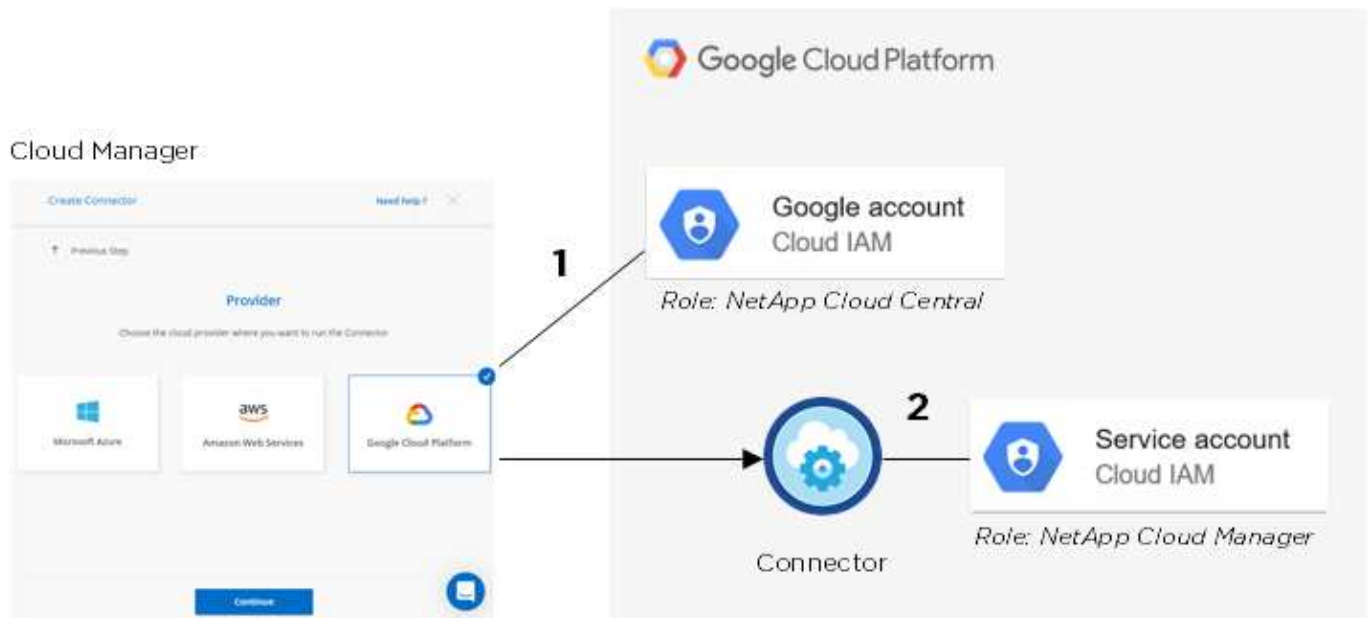
Zwei Berechtigungsgruppen müssen vorhanden sein, bevor Sie einen Connector direkt von BlueXP bereitstellen:

1. Sie müssen einen Connector mit einem Google-Konto bereitstellen, das über Berechtigungen zum Starten der Connector VM-Instanz von BlueXP verfügt.
2. Bei der Bereitstellung des Connectors werden Sie aufgefordert, ein auszuwählen **"Servicekonto"** Für die VM-Instanz. BlueXP erhält über das Servicekonto Berechtigungen zum Erstellen und Verwalten von Cloud Volumes ONTAP-Systemen in Ihrem Auftrag. Berechtigungen werden durch Hinzufügen einer benutzerdefinierten Rolle an das Servicekonto bereitgestellt.



Wir haben zwei YAML-Dateien eingerichtet, die die erforderlichen Berechtigungen für den Benutzer und das Dienstkonto enthalten. ["Erfahren Sie, wie Sie mit den YAML-Dateien Berechtigungen einrichten"](#).

Das folgende Bild zeigt die in den Nummern 1 und 2 oben beschriebenen Berechtigungsanforderungen:



## Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann im selben Projekt wie der Connector oder in einem anderen Projekt residieren. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zunächst das Connector-Servicekonto und die Rolle zu diesem Projekt hinzufügen.

- ["Erfahren Sie, wie Sie ein Servicekonto einrichten"](#)
- ["Erfahren Sie, wie Cloud Volumes ONTAP in GCP implementiert und ein Projekt ausgewählt wird"](#)

## Verwalten von Google Cloud-Anmeldeinformationen und -Abonnements für BlueXP

Sie können die Anmeldeinformationen verwalten, die der Connector-VM-Instanz zugeordnet sind.

### Verknüpfen eines Marketplace-Abonnements mit GCP-Zugangsdaten

Wenn Sie einen Connector in GCP bereitstellen, erstellt BlueXP einen Standardsatz von Anmeldeinformationen, die der Connector-VM-Instanz zugeordnet sind. Dies sind die Anmeldeinformationen, die BlueXP zur Bereitstellung von Cloud Volumes ONTAP verwendet.

Sie können das Marketplace-Abonnement jederzeit ändern, das mit diesen Anmeldedaten verknüpft ist. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

### 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 Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus.


Google Cloud Project

OCCM-Dev ▼

Subscription

● GCP subscription for staging ▼

---

 [Add Subscription](#)

4. Klicken Sie Auf **Mitarbeiter**.

5. Wenn Sie noch kein Abonnement haben, klicken Sie auf **Abonnement hinzufügen** und führen Sie die folgenden Schritte aus, um ein neues Abonnement zu erstellen.



Bevor Sie die folgenden Schritte durchführen, stellen Sie sicher, dass Sie sowohl Billing Admin-Berechtigungen in Ihrem Google Cloud-Konto als auch BlueXP-Login haben.

6. Führen Sie die Schritte des Abonnements durch und klicken Sie auf **Weiter**.

## Add Subscription


### Subscription Steps:


- 1 **Cloud Manager**  
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
  - 2 **Google Cloud Marketplace**  
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
  - 3 **Cloud Central**  
Save your subscription.
  - 4 **Cloud Manager**  
Associate the Marketplace subscription with your Google Cloud project.
-  View video instructions

Continue

Cancel

7. Nachdem Sie auf die umgeleitet wurden "[Seite zu NetApp BlueXP im Google Cloud Marketplace](#)", Stellen Sie sicher, dass das richtige Projekt im oberen Navigationsmenü ausgewählt ist.


Google Cloud Platform
My First Project



## Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

SUBSCRIBE

OVERVIEW
PRICING
SUPPORT

### Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

### Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. Klicken Sie Auf **Abonnieren**.

9. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

## 2. Purchase details

Select a billing account \*

Secondary\_Billing\_Account

## 3. Terms

### Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

### Additional terms

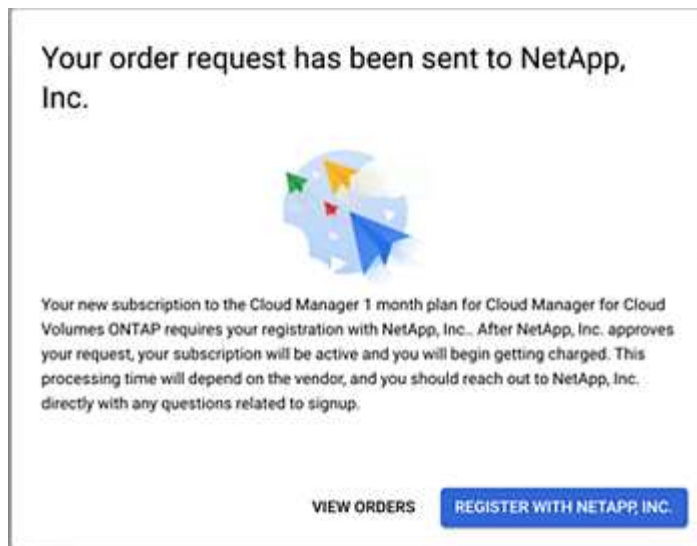
- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ⓘ
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. Klicken Sie Auf **Abonnieren**.

Dieser Schritt sendet Ihre Transferanfrage an NetApp.

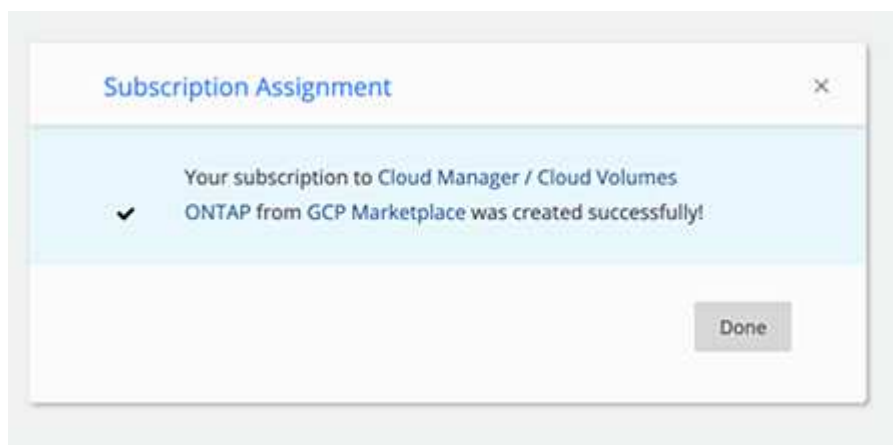
11. Klicken Sie im Popup-Dialogfeld auf **mit NetApp registrieren, Inc.**, um zur NetApp BlueXP Website umgeleitet zu werden.



Mit diesem Schritt müssen Sie das GCP-Abonnement mit Ihrem NetApp Konto verknüpfen. Der Vorgang der Verknüpfung eines Abonnements ist erst abgeschlossen, wenn Sie von dieser Seite umgeleitet und dann bei BlueXP angemeldet sind.

12. Nachdem Sie zu BlueXP umgeleitet wurden, melden Sie sich an oder registrieren Sie sich, und klicken Sie dann auf **Fertig**, um fortzufahren.

Das GCP-Abonnement ist mit allen NetApp Konten verknüpft, mit denen Ihre Benutzeranmeldung verknüpft ist.




Wenn ein Mitarbeiter Ihres Unternehmens bereits über Ihr Rechnungskonto das NetApp BlueXP Abonnement abonniert hat, werden Sie weitergeleitet "[Die Cloud Volumes ONTAP-Seite auf der BlueXP-Website](#)" Stattdessen. Sollte dies nicht unerwartet sein, wenden Sie sich an Ihr NetApp Vertriebsteam. Google ermöglicht nur ein Abonnement pro Google-Abrechnungskonto.


13. Navigieren Sie nach Abschluss dieses Vorgangs zur Seite Anmeldeinformationen in BlueXP, und wählen Sie dieses neue Abonnement aus.

Google Cloud Project

OCCM-Dev

Subscription

 GCP subscription for staging




## Fehlerbehebung beim Marketplace-Abonnementprozess

Manchmal kann das Abonnieren von Cloud Volumes ONTAP über den Google Cloud Marketplace fragmentiert werden aufgrund falscher Berechtigungen oder versehentlich nicht nach der Umleitung zur BlueXP-Website. Wenn dies geschieht, führen Sie die folgenden Schritte aus, um den Abonnementprozess abzuschließen.

### Schritte

1. Navigieren Sie zum ["Seite zu NetApp BlueXP im Google Cloud Marketplace"](#) Um den Status der Bestellung zu überprüfen. Wenn auf der Seite **auf Anbieter verwalten** steht, scrollen Sie nach unten und klicken Sie auf **Bestellungen verwalten**.

Pricing

 The product was purchased on 12/9/20.

MANAGE ORDERS

- a. Wenn der Auftrag ein grünes Häkchen anzeigt und dies unerwartet ist, kann bereits ein anderer Mitarbeiter des Unternehmens, der dasselbe Rechnungskonto verwendet, abonniert werden. Wenn das unerwartete vorbereitet ist oder wenn Sie die Details zu diesem Abonnement benötigen, wenden Sie sich an Ihr NetApp Vertriebsteam.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc... 	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	

- b. Wenn der Auftrag einen Clock- und **Ausstehend**-Status anzeigt, gehen Sie zurück zur Marktplatzseite und wählen Sie **auf Anbieter verwalten**, um den Prozess wie oben beschrieben abzuschließen.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	d56c66... 	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	

# Fügen Sie Konten der NetApp Support Site in BlueXP hinzu und managen Sie sie

Bereitstellen von Zugangsdaten für Ihre NetApp Support Site (NSS) Accounts zur Registrierung für Support, zum Aktivieren wichtiger Workflows für Cloud Volumes ONTAP usw.

## Überblick

Wenn Sie Ihr Konto auf der NetApp Support Site zu BlueXP hinzufügen, müssen Sie die folgenden Aufgaben aktivieren:

- Um sich für den Support zu registrieren
- Cloud Volumes ONTAP bei Nutzung einer eigenen Lizenz (BYOL)

Die Bereitstellung Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für den von Ihnen erworbenen Zeitraum aktivieren kann. Dies schließt automatische Updates für Vertragsverlängerungen ein.

- Um Pay-as-you-go Cloud Volumes ONTAP Systeme zu registrieren

Die Bereitstellung Ihres NSS Kontos ist erforderlich, um Support für Ihr System zu aktivieren und Zugang zu den technischen Support-Ressourcen von NetApp zu erhalten.

- Um ein Upgrade der Cloud Volumes ONTAP Software auf die neueste Version durchzuführen

Sie müssen außerdem Ihre NSS-Zugangsdaten eingeben, um Digital Advisor (ehemals Active IQ) aus BlueXP zu verwenden. Diese Anmeldedaten sind direkt mit Ihrem Benutzerkonto verknüpft und dürfen nur mit Digital Advisor verwendet werden. Lesen Sie im folgenden Abschnitt weitere Einzelheiten.

## Verwalten eines NSS-Kontos im Zusammenhang mit Digital Advisor

Wenn Sie in BlueXP auf Digital Advisor zugreifen, werden Sie aufgefordert, sich bei Digital Advisor anzumelden, indem Sie Ihre NSS-Anmeldedaten eingeben. Nachdem Sie Ihre NSS-Anmeldedaten eingegeben haben, wird das NSS-Konto oben auf der NSS-Verwaltungsseite angezeigt. Diese Anmeldedaten können nach Bedarf gemanagt werden.

Beachten Sie Folgendes über dieses NSS-Konto:

- Das Konto wird auf Benutzerebene verwaltet, was bedeutet, dass es von anderen Benutzern, die sich anmelden, nicht angezeigt wird.
- Das Konto kann nicht mit anderen BlueXP Funktionen verwendet werden, nicht mit der Erstellung, Lizenzierung oder dem Support von Cloud Volumes ONTAP.
- Es kann nur ein NSS-Konto für Digital Advisor pro Benutzer vorhanden sein.

## Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Klicken Sie auf **NSS Management**.
3. Klicken Sie unter **Ihre NSS-Anmeldeinformationen** auf **Aktion** und wählen Sie eine der folgenden Optionen:
  - **Associate NSS User:** Anmeldedaten für ein NetApp Support Site Konto hinzufügen, damit Sie in BlueXP auf Digital Advisor zugreifen können.
  - **Vorhandene Anmeldedaten aktualisieren:** Die Zugangsdaten für Ihr NetApp Support Site Konto aktualisieren.
  - **Löschen:** Entfernen Sie das Konto, das mit Digital Advisor verknüpft ist.

BlueXP aktualisiert das NSS-Konto im Zusammenhang mit Digital Advisor.

## Fügen Sie ein NSS-Konto hinzu

Über das Support-Dashboard können Sie Ihre NetApp Support Site Konten zur Verwendung mit BlueXP auf der NetApp Kontoebene hinzufügen und managen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie ein Partner- oder Reseller-Konto haben, können Sie ein oder mehrere NSS-Konten hinzufügen, aber sie können nicht neben Kunden-Level-Accounts hinzugefügt werden.

### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.





2. Klicken Sie auf **NSS Management > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

Beachten Sie Folgendes:

- Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
- Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern. Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet wird. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen **...** Menü.
- Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option **...** Menü. Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden.

Sie können das Konto jetzt beim Erstellen neuer Cloud Volumes ONTAP Systeme auswählen, wenn Sie bestehende Cloud Volumes ONTAP Systeme registrieren und sich für Support registrieren.

- ["Starten von Cloud Volumes ONTAP in AWS"](#)
- ["Starten von Cloud Volumes ONTAP in Azure"](#)
- ["Einführung von Cloud Volumes ONTAP in GCP"](#)
- ["Registrieren von Pay-as-you-go-Systemen"](#)

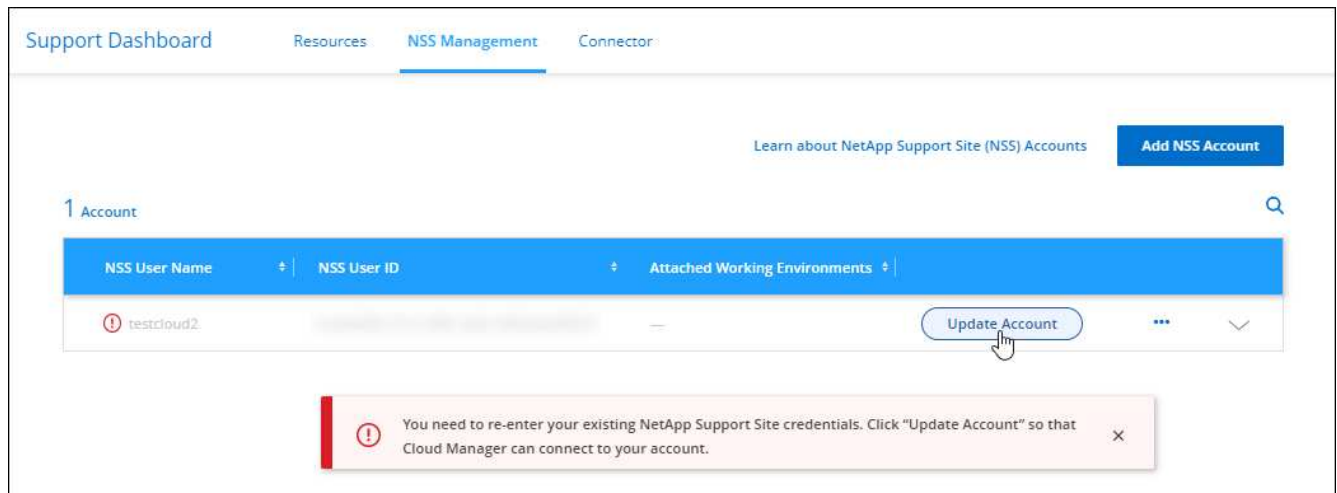
## Aktualisieren Sie ein NSS-Konto für die neue Authentifizierungsmethode

Im November 2021 verwendet NetApp jetzt Microsoft Azure Active Directory als Identitäts-Provider für speziell auf Support und Lizenzierung applikationsspezifische Authentifizierungs-Services. Als Ergebnis dieses

Updates werden Sie von BlueXP aufgefordert, die Anmeldeinformationen für alle vorhandenen Konten, die Sie zuvor hinzugefügt haben, zu aktualisieren.

### Schritte

1. Falls noch nicht geschehen, "[Erstellen Sie ein Microsoft Azure Active Directory B2C-Konto, das mit Ihrem aktuellen NetApp Konto verknüpft wird](#)".
2. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
3. Klicken Sie auf **NSS Management**.
4. Klicken Sie für das NSS-Konto, das Sie aktualisieren möchten, auf **Konto aktualisieren**.



5. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

6. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

Nach Abschluss des Vorgangs sollte das Konto, das Sie aktualisiert haben, nun als *New* Konto in der Tabelle aufgeführt werden. Die *ältere* Version des Kontos ist weiterhin in der Tabelle aufgeführt, zusammen mit allen vorhandenen Arbeitsumgebungsverknüpfungen.

7. Wenn vorhandene Cloud Volumes ONTAP-Arbeitsumgebungen an die ältere Version des Kontos angeschlossen sind, befolgen Sie die nachstehenden Schritte a working environment to a different NSS account, Verbinden Sie die Arbeitsumgebungen mit einem anderen NSS-Konto.
8. Wechseln Sie zur älteren Version des NSS-Kontos, klicken Sie auf **...** Und wählen Sie dann **Löschen**.

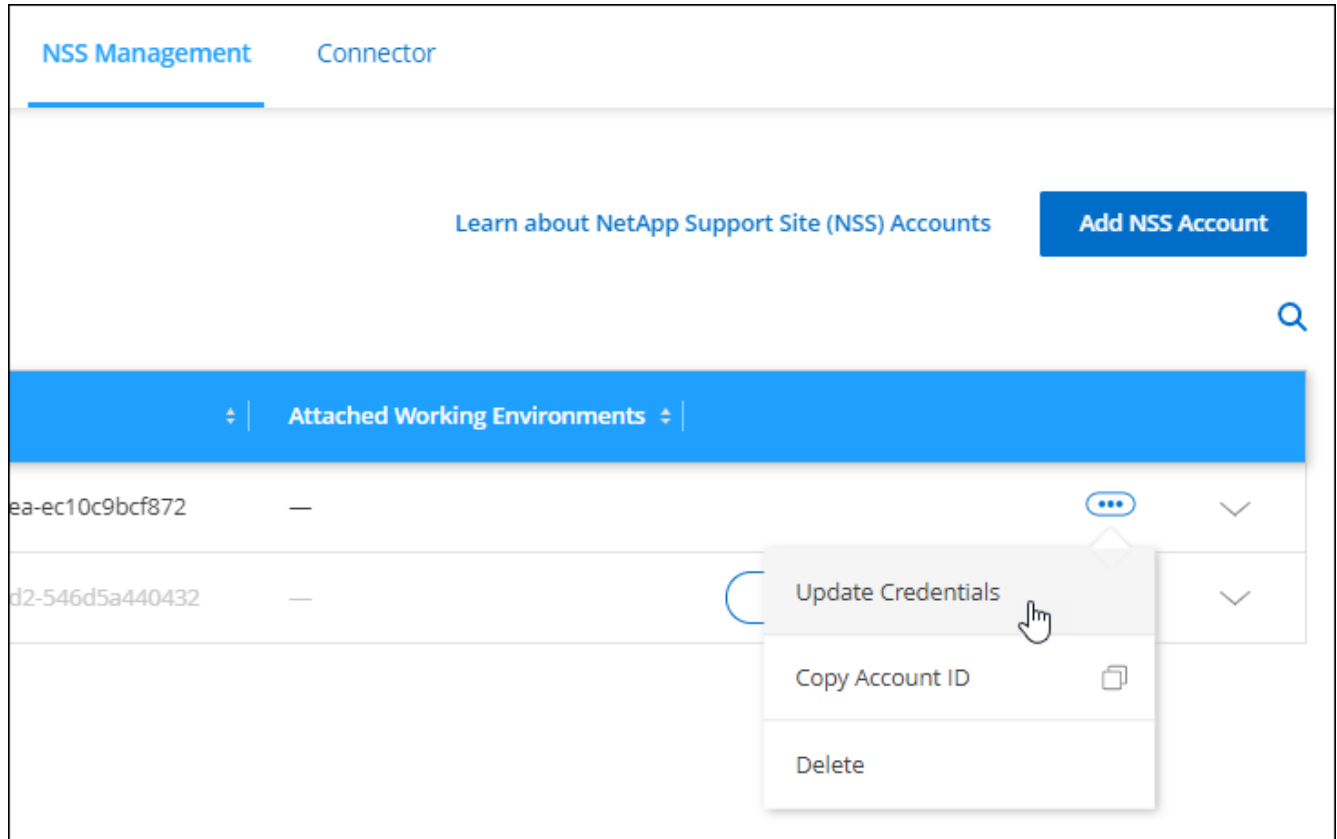
## NSS-Anmeldeinformationen aktualisieren

Sie müssen die Anmeldeinformationen für Ihre NSS-Konten in BlueXP aktualisieren, wenn eine der folgenden Ereignisse eintritt:

- Sie ändern die Anmeldeinformationen für das Konto
- Das Aktualisieren-Token für Ihr Konto läuft nach 3 Monaten ab

### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
2. Klicken Sie auf **NSS Management**.
3. Klicken Sie für das NSS-Konto, das Sie aktualisieren möchten, auf **...** Und wählen Sie dann **Anmeldeinformationen aktualisieren**.



4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

5. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

## Verbinden Sie eine Arbeitsumgebung mit einem anderen NSS-Konto

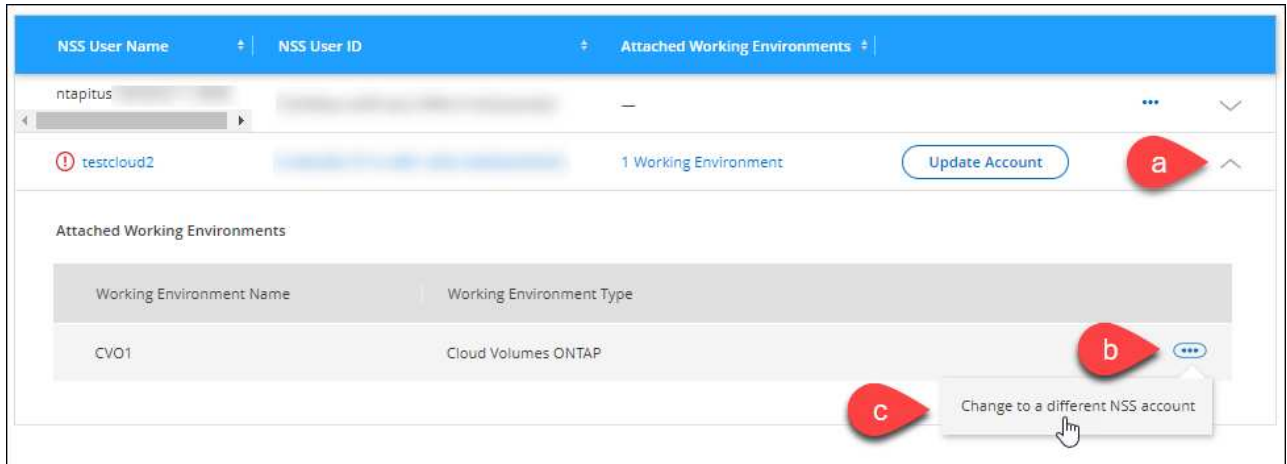
Wenn Ihr Unternehmen über mehrere NetApp Support Site Accounts verfügt, können Sie ändern, welches Konto einem Cloud Volumes ONTAP System zugeordnet ist.

Diese Funktion wird nur bei NSS-Konten unterstützt, die für die Verwendung von Microsoft Azure AD konfiguriert sind, das von NetApp zum Identitätsmanagement eingeführt wurde. Bevor Sie diese Funktion nutzen können, klicken Sie auf **NSS-Konto hinzufügen** oder **Konto aktualisieren**.

### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
2. Klicken Sie auf **NSS Management**.
3. Führen Sie die folgenden Schritte aus, um das NSS-Konto zu ändern:

- Erweitern Sie die Zeile für den NetApp Support Site Account, dem die Arbeitsumgebung derzeit zugeordnet ist.
- Klicken Sie für die Arbeitsumgebung, für die Sie die Zuordnung ändern möchten, auf ...
- Wählen Sie **Ändern Sie auf ein anderes NSS-Konto**.



- Wählen Sie das Konto aus und klicken Sie dann auf **Speichern**.

## Zeigen Sie die E-Mail-Adresse für ein NSS-Konto an

Da für die Authentifizierungsdienste von NetApp Support-Site jetzt Microsoft Azure Active Directory verwendet wird, ist der NSS-Benutzername in BlueXP in der Regel eine vom Azure AD generierte Kennung. Als Ergebnis können Sie möglicherweise nicht sofort die E-Mail-Adresse kennen, die mit diesem Konto verknüpft ist. Aber BlueXP hat die Möglichkeit, Ihnen die zugehörige E-Mail-Adresse anzuzeigen.



Wenn Sie die NSS-Verwaltungsseite aufrufen, generiert BlueXP für jedes Konto in der Tabelle ein Token. Dieses Token enthält Informationen zur zugehörigen E-Mail-Adresse. Das Token wird dann entfernt, wenn Sie die Seite verlassen. Die Informationen werden niemals zwischengespeichert, wodurch Ihre Privatsphäre geschützt wird.

### Schritte

- Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
- Klicken Sie auf **NSS Management**.
- Klicken Sie für das NSS-Konto, das Sie aktualisieren möchten, auf ... Und wählen Sie dann **E-Mail-Adresse anzeigen**.



BlueXP zeigt den Benutzernamen und die zugehörige E-Mail-Adresse der NetApp Support Website an. Sie können die Schaltfläche Kopieren verwenden, um die E-Mail-Adresse zu kopieren.

## Entfernen Sie ein NSS-Konto

Löschen Sie alle NSS-Konten, die Sie nicht mehr mit BlueXP verwenden möchten.

Sie können kein Konto löschen, das derzeit einer Cloud Volumes ONTAP Arbeitsumgebung zugeordnet ist. Das müssen Sie zuerst a working environment to a different NSS account, Verbinden Sie die Arbeitsumgebungen mit einem anderen NSS-Konto.

### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
2. Klicken Sie auf **NSS Management**.
3. Klicken Sie für das NSS-Konto, das Sie löschen möchten, auf **...** Und wählen Sie dann **Löschen**.



4. Klicken Sie zur Bestätigung auf **Löschen**.

## Meine Opportunitys

Auf dem Canvas bietet die Registerkarte \* My Opportunities\* einen zentralen Ort, um vorhandene Ressourcen zu entdecken, die Sie BlueXP hinzufügen können, um konsistente Datenservices und Abläufe in Ihrer gesamten hybriden Multi-Cloud zu erhalten.

Mithilfe von My Opportunities können Sie derzeit bestehende FSX für ONTAP-Dateisysteme in Ihrem AWS-Konto erkennen.

["Entdecken Sie FSX für ONTAP mithilfe von My Opportunities"](#)

## 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.