Verwalten von BlueXP

Setup and administration

NetApp
April 26, 2024

Inhalt

Verwalten von BlueXP

Nutzung von Identitätsföderation mit BlueXP

Identity Federation ermöglicht Single Sign On mit BlueXP, sodass Benutzer sich mithilfe von Anmeldedaten Ihrer Unternehmensidentität anmelden können. Erste Schritte sind die Zusammenarbeit von Identity Federation mit BlueXP und ein Überblick über den Setup-Prozess möglich.

Identitätsföderation mit NSS-Anmeldedaten

Wenn Sie sich mit Ihren NSS-Zugangsdaten (NetApp Support Site) bei BlueXP anmelden, sollten Sie die Anweisungen auf dieser Seite nicht befolgen, um die Identity Federation einzurichten. Sie sollten stattdessen Folgendes tun:

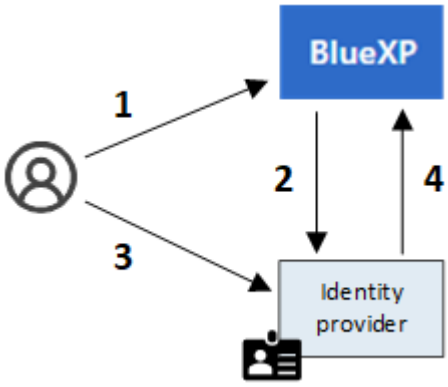
- Laden Sie die herunter, und füllen Sie die aus "Antragsformular für die NetApp Föderation"
- Senden Sie das Formular an die im Formular angegebene E-Mail-Adresse

Das Identitäts- und Zugriffsmanagement durch NetApp wird Ihren Antrag prüfen.

Funktionsweise der Identitätsföderation

Durch die Einrichtung des Identity Federation wird eine Vertrauensverbindung zwischen dem BlueXP Authentifizierungsservice-Provider (auth0) und Ihrem eigenen Identitätsmanagement-Anbieter hergestellt.

Die folgende Abbildung zeigt die Zusammenarbeit von Identity Federation mit BlueXP:



1. Ein Benutzer gibt seine E-Mail-Adresse auf der BlueXP Anmeldeseite ein.
2. BlueXP erkennt, dass die E-Mail-Domäne Teil einer Verbundverbindung ist, und sendet die Authentifizierungsanforderung über die vertrauenswürdige Verbindung an den Identitätsanbieter.

   Wenn Sie eine föderierte Verbindung einrichten, verwendet BlueXP immer diese föderierte Verbindung für die Authentifizierung.

3. Der Benutzer authentifiziert sich mit Anmeldeinformationen aus Ihrem Firmenverzeichnis.
4. Ihr Identitätsanbieter authentifiziert die Identität des Benutzers, und der Benutzer ist bei BlueXP angemeldet.

Identity Federation verwendet offene Standards wie Security Assertion Markup Language 2.0 (SAML) und OpenID Connect (OIDC).

Unterstützte Identitätsanbieter

BlueXP unterstützt folgende Identitätsanbieter:

- Security Assertion Markup Language (SAML)-Identitätsanbieter
- Microsoft Entra-ID
- Active Directory Federation Services (ADFS)
- PingFederate

BlueXP unterstützt nur von Service-Providern initiiertes (von SP-initiiertes) SSO. Von Identitätsanbietern initiiertes SSO (von IdP initiiert) wird nicht unterstützt.

Überblick über den Setup-Prozess

Bevor Sie eine Verbindung zwischen BlueXP und Ihrem Identitätsmanagement-Anbieter herstellen, sollten Sie die erforderlichen Schritte kennen, damit Sie sich entsprechend vorbereiten können.

Diese Schritte sind speziell für Benutzer bestimmt, die sich über ein NetApp Cloud-Login bei BlueXP anmelden. Wenn Sie Ihre NSS-Anmeldedaten für die Anmeldung bei BlueXP verwenden, Erfahren Sie, wie Sie Identitätsföderation mit NSS-Anmeldeinformationen einrichten.

SAML-Identitätsanbieter

Das Einrichten einer föderierten Verbindung zwischen BlueXP und einem SAML-Identitätsanbieter umfasst im allgemeinen folgende Schritte:

Schritt	Abgeschlossen von	Beschreibung
1	Active Directory (AD) Admin	Konfigurieren Sie Ihren SAML-Identitätsanbieter zur Aktivierung der Identitätsföderation mit BlueXP. Anweisungen für Ihren SAML-Identitätsanbieter anzeigen: • "ADFS" • "Okta" • "OneLogin" • "PingFederate" • "Salesforce" • "SiteMinder" • "SSOCircle" Wenn Ihr Identitätsanbieter nicht in der Liste oben angezeigt wird, "Befolgen Sie diese allgemeinen Anweisungen" Führen Sie *Not* die Schritte aus, die beschreiben, wie eine Verbindung in auth0 erstellt wird. Im nächsten Schritt erstellen Sie diese Verbindung.
2	BlueXP Admin	Wechseln Sie zum "NetApp Federation Setup-Seite" Stellen Sie die Verbindung zu BlueXP her. Um diesen Schritt abzuschließen, müssen Sie Folgendes von Ihrem AD-Administrator über den Identitätsanbieter beziehen: • Anmelde-URL • Ein X509-Signaturzertifikat (PEM- oder CER-Format) • Abmelden-URL (optional) Nachdem Sie die Verbindung mithilfe dieser Informationen erstellt haben, werden auf der Seite Verbindungseinrichtung die Parameter aufgeführt, die Sie an Ihren AD-Administrator senden können, um die Konfiguration im nächsten Schritt abzuschließen. Beachten Sie das Ablaufdatum des Zertifikats. Sie müssen zur Seite „Föderationseinrichtung“ zurückkehren und das Zertifikat *vor* aktualisieren. Das liegt in Ihrer Verantwortung. Das Ablaufdatum wird von BlueXP nicht aufgezeichnet. Am besten arbeiten Sie mit Ihrem AD-Team zusammen, um rechtzeitig benachrichtigt zu werden.
3	AD Admin	Führen Sie die Konfiguration auf dem Identitätsanbieter mit den Parametern aus, die nach Abschluss von Schritt 2 auf der Seite „Einrichtung der Föderation“ angezeigt werden.

Schritt	Abgeschlossen von	Beschreibung
4	BlueXP Admin	Testen und aktivieren Sie die Verbindung vom "NetApp Federation Setup-Seite" Beachten Sie, dass die Seite zwischen dem Testen der Verbindung und dem Aktivieren der Verbindung aktualisiert wird.

Microsoft Entra-ID

Das Einrichten einer föderierten Verbindung zwischen BlueXP und der Microsoft Entra ID umfasst im allgemeinen die folgenden Schritte:

Schritt	Abgeschlossen von	Beschreibung
1	AD Admin	Konfigurieren Sie die Microsoft Entra ID zur Aktivierung der Identitätsföderation mit BlueXP. "Anweisungen zur Registrierung der Anwendung mit Microsoft Entra ID anzeigen" Führen Sie *Not* die Schritte aus, die beschreiben, wie eine Verbindung in auth0 erstellt wird. Im nächsten Schritt erstellen Sie diese Verbindung.
2	BlueXP Admin	Wechseln Sie zum "NetApp Federation Setup-Seite" Stellen Sie die Verbindung zu BlueXP her. Um diesen Schritt abzuschließen, müssen Sie Folgendes von Ihrem AD-Administrator erhalten: • Client-ID • Geheimer Client-Wert • Microsoft Entra ID-Domäne Nachdem Sie die Verbindung mithilfe dieser Informationen erstellt haben, werden auf der Seite Verbindungseinrichtung die Parameter aufgeführt, die Sie an Ihren AD-Administrator senden können, um die Konfiguration im nächsten Schritt abzuschließen. Beachten Sie das Ablaufdatum des geheimen Schlüssels. Sie müssen zur Seite „Föderationseinrichtung“ zurückkehren und das Zertifikat *vor* aktualisieren. Das liegt in Ihrer Verantwortung. Das Ablaufdatum wird von BlueXP nicht aufgezeichnet. Am besten arbeiten Sie mit Ihrem AD-Team zusammen, um rechtzeitig benachrichtigt zu werden.
3	AD Admin	Schließen Sie die Konfiguration in Microsoft Entra ID mit den Parametern ab, die auf der Seite Federation Setup angezeigt werden, nachdem Sie Schritt 2 abgeschlossen haben.

Schritt	Abgeschlossen von	Beschreibung
4	BlueXP Admin	Testen und aktivieren Sie die Verbindung vom "NetApp Federation Setup-Seite" Beachten Sie, dass die Seite zwischen dem Testen der Verbindung und dem Aktivieren der Verbindung aktualisiert wird.

ADFS

Das Einrichten einer verbundenen Verbindung zwischen BlueXP und ADFS umfasst im Allgemeinen die folgenden Schritte:

Schritt	Abgeschlossen von	Beschreibung
1	AD Admin	Konfigurieren Sie den ADFS-Server so, dass die Identity Federation mit BlueXP aktiviert wird. "Anweisungen zur Konfiguration des ADFS-Servers mit auth0 anzeigen"
2	BlueXP Admin	Wechseln Sie zum "NetApp Federation Setup-Seite" Stellen Sie die Verbindung zu BlueXP her. Um diesen Schritt abzuschließen, müssen Sie Folgendes von Ihrem AD-Administrator erhalten: Die URL für den ADFS-Server oder die Verbundmetadaten-Datei. Nachdem Sie die Verbindung mithilfe dieser Informationen erstellt haben, werden auf der Seite Verbindungseinrichtung die Parameter aufgeführt, die Sie an Ihren AD-Administrator senden können, um die Konfiguration im nächsten Schritt abzuschließen. Beachten Sie das Ablaufdatum des Zertifikats. Sie müssen zur Seite „Föderationseinrichtung“ zurückkehren und das Zertifikat *vor* aktualisieren. Das liegt in Ihrer Verantwortung. Das Ablaufdatum wird von BlueXP nicht aufgezeichnet. Am besten arbeiten Sie mit Ihrem AD-Team zusammen, um rechtzeitig benachrichtigt zu werden.
3	AD Admin	Schließen Sie die Konfiguration auf dem ADFS-Server mit den Parametern ab, die auf der Seite Federation Setup angezeigt werden, nachdem Sie Schritt 2 abgeschlossen haben.
4	BlueXP Admin	Testen und aktivieren Sie die Verbindung vom "NetApp Federation Setup-Seite" Beachten Sie, dass die Seite zwischen dem Testen der Verbindung und dem Aktivieren der Verbindung aktualisiert wird.

PingFederate

Das Einrichten einer föderierten Verbindung zwischen BlueXP und einem PingFederate Server umfasst im allgemeinen die folgenden Schritte:

Schritt	Abgeschlossen von	Beschreibung
1	AD Admin	Konfigurieren Sie den PingFederate Server zur Aktivierung der Identity Federation mit BlueXP. "Anweisungen zum Erstellen einer Verbindung anzeigen" Führen Sie *Not* die Schritte aus, die beschreiben, wie eine Verbindung in auth0 erstellt wird. Im nächsten Schritt erstellen Sie diese Verbindung.
2	BlueXP Admin	Wechseln Sie zum "NetApp Federation Setup-Seite" Stellen Sie die Verbindung zu BlueXP her. Um diesen Schritt abzuschließen, müssen Sie Folgendes von Ihrem AD-Administrator erhalten: • Die URL für den PingFederate-Server • Ein X509-Signaturzertifikat (PEM- oder CER-Format) Nachdem Sie die Verbindung mithilfe dieser Informationen erstellt haben, werden auf der Seite Verbindungseinrichtung die Parameter aufgeführt, die Sie an Ihren AD-Administrator senden können, um die Konfiguration im nächsten Schritt abzuschließen. Beachten Sie das Ablaufdatum des Zertifikats. Sie müssen zur Seite „Föderationseinrichtung“ zurückkehren und das Zertifikat *vor* aktualisieren. Das liegt in Ihrer Verantwortung. Das Ablaufdatum wird von BlueXP nicht aufgezeichnet. Am besten arbeiten Sie mit Ihrem AD-Team zusammen, um rechtzeitig benachrichtigt zu werden.
3	AD Admin	Schließen Sie die Konfiguration auf dem PingFederate-Server mit den Parametern ab, die auf der Seite Federation Setup angezeigt werden, nachdem Sie Schritt 2 abgeschlossen haben.
4	BlueXP Admin	Testen und aktivieren Sie die Verbindung vom "NetApp Federation Setup-Seite" Beachten Sie, dass die Seite zwischen dem Testen der Verbindung und dem Aktivieren der Verbindung aktualisiert wird.

Aktualisieren einer föderierten Verbindung

Nachdem der BlueXP Admin eine Verbindung ermöglicht hat, kann der Admin die Verbindung jederzeit über das aktualisieren "NetApp Federation Setup-Seite"

Sie müssen beispielsweise die Verbindung aktualisieren, indem Sie ein neues Zertifikat hochladen.

Der BlueXP Administrator, der die Verbindung erstellt hat, ist der einzige autorisierte Benutzer, der die Verbindung aktualisieren kann. Wenn Sie weitere Administratoren hinzufügen möchten, wenden Sie sich an den NetApp Support.

BlueXP Accounts

Managen Sie Ihr BlueXP Konto

Wenn Sie ein BlueXP Konto erstellen, wird nur ein einziger Admin-Benutzer und eine Arbeitsumgebung eingeschlossen. Sie können das Konto so verwalten, dass es den Anforderungen Ihres Unternehmens entspricht, indem Sie Benutzer hinzufügen, Servicekonten für Automatisierungszwecke erstellen, Arbeitsbereiche hinzufügen und vieles mehr.

"Mehr zur Funktionsweise von BlueXP Accounts".

Account-Management mit der Mandanten-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

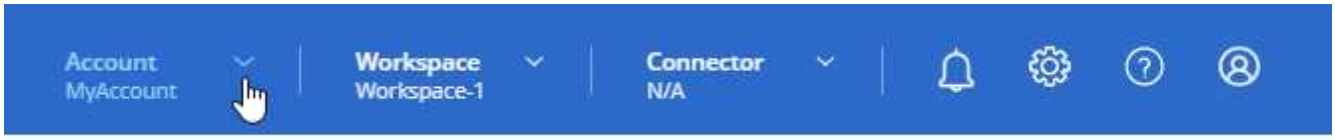
Der Benutzer in Ihrem Konto kann auf die Ressourcen in bestimmten Arbeitsbereichen zugreifen und diese verwalten.

Benutzer hinzufügen

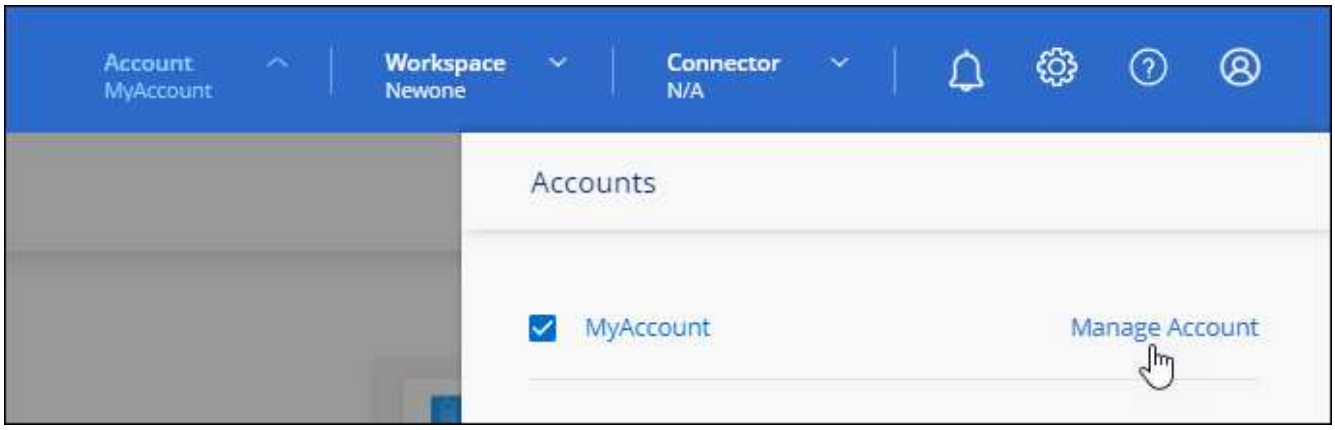
Ordnen Sie Benutzer Ihrem BlueXP Konto zu, damit diese Benutzer Arbeitsumgebungen in BlueXP erstellen und managen können.

Schritte

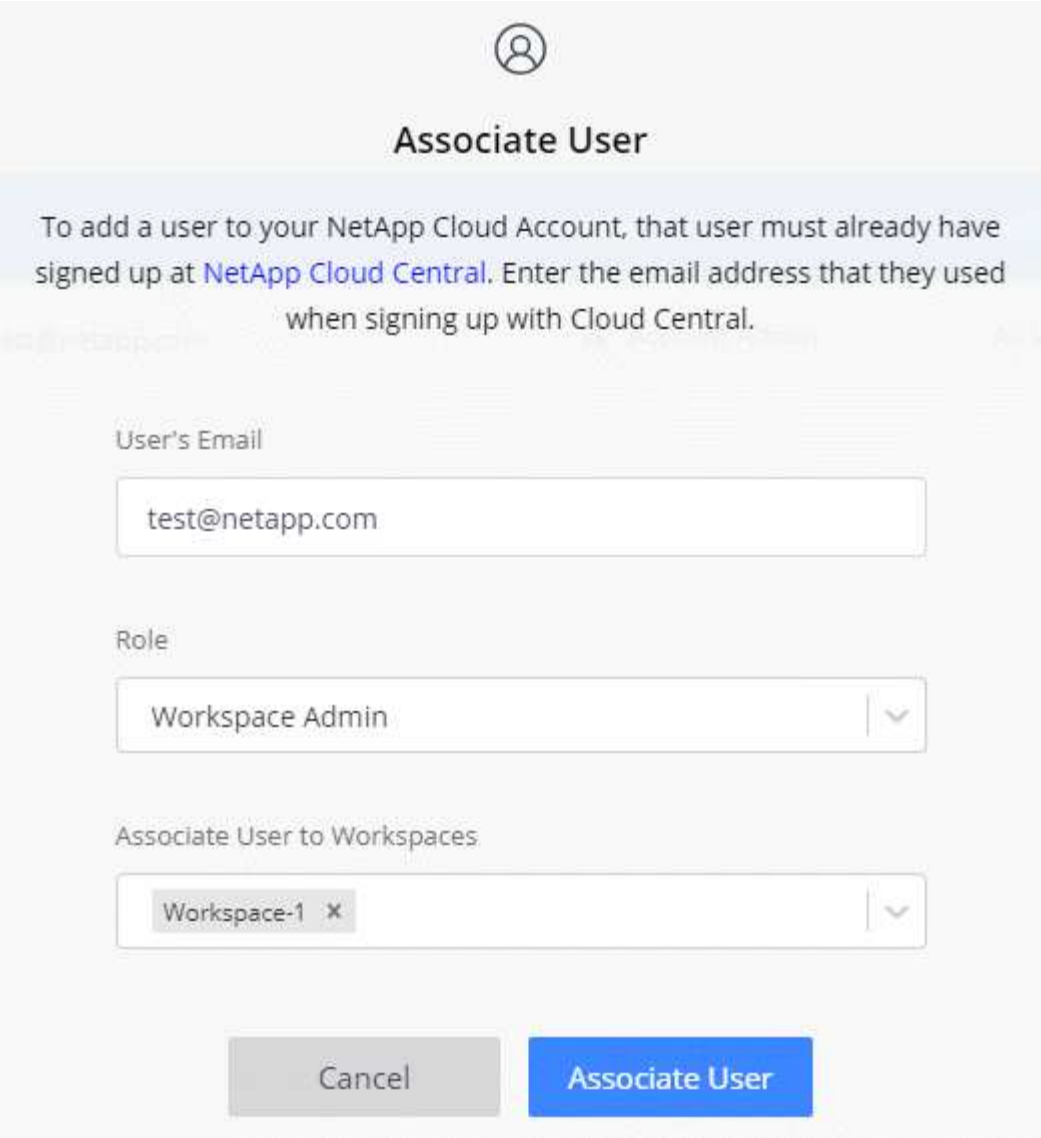
1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "NetApp BlueXP Website" Und melden Sie sich an.
2. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus.



3. Wählen Sie **Konto verwalten** neben dem aktuell ausgewählten Konto.



4. Wählen Sie auf der Registerkarte Mitglieder die Option * Associate User*.
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 Compliance-Informationen für die BlueXP-Klassifizierung anzeigen und Berichte für Arbeitsbereiche generieren, auf die sie zugreifen dürfen.
6. Wenn Sie Workspace Admin oder Compliance Viewer ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



7. Wählen Sie **Mitarbeiter**.

Ergebnis

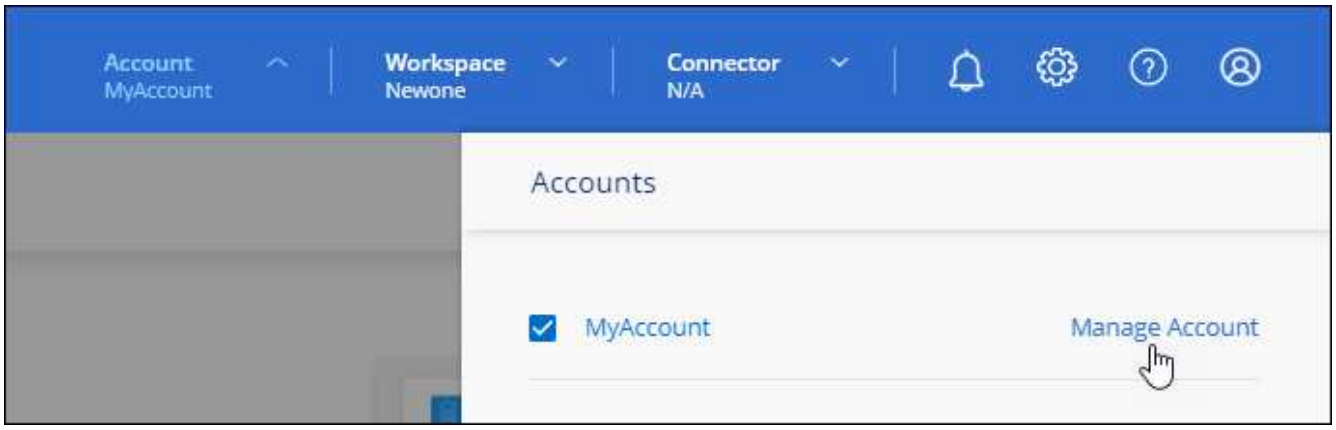
Der Benutzer sollte eine E-Mail von NetApp BlueXP mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die Informationen, die für den Zugriff auf BlueXP erforderlich sind.

Benutzer entfernen

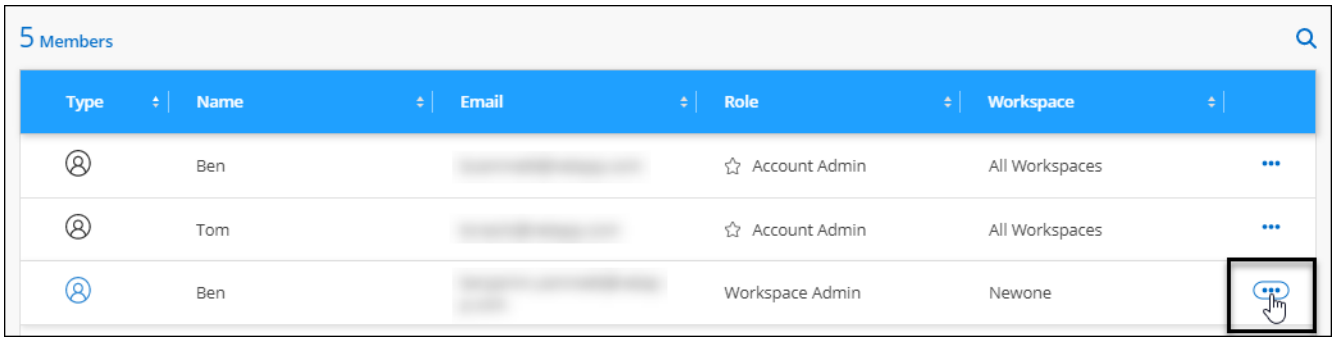
Durch das Auflösen der Zuordnung eines Benutzers wird kein Zugriff mehr auf die Ressourcen in einem BlueXP Konto möglich.

Schritte

1. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus und wählen Sie **Konto verwalten** aus.



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



3. Wählen Sie **Benutzer aufheben**, und wählen Sie zur Bestätigung **Zuordnung aufheben**.

Ergebnis

Der Benutzer kann nicht mehr auf die Ressourcen in diesem BlueXP Konto zugreifen.

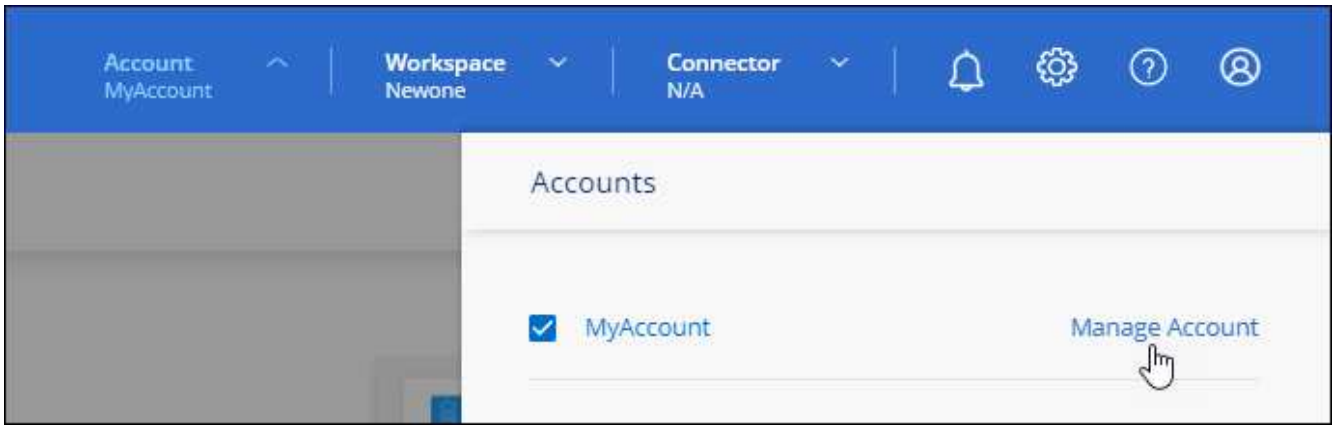
Verwalten der Arbeitsbereiche eines Arbeitsbereichsadministrators

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.

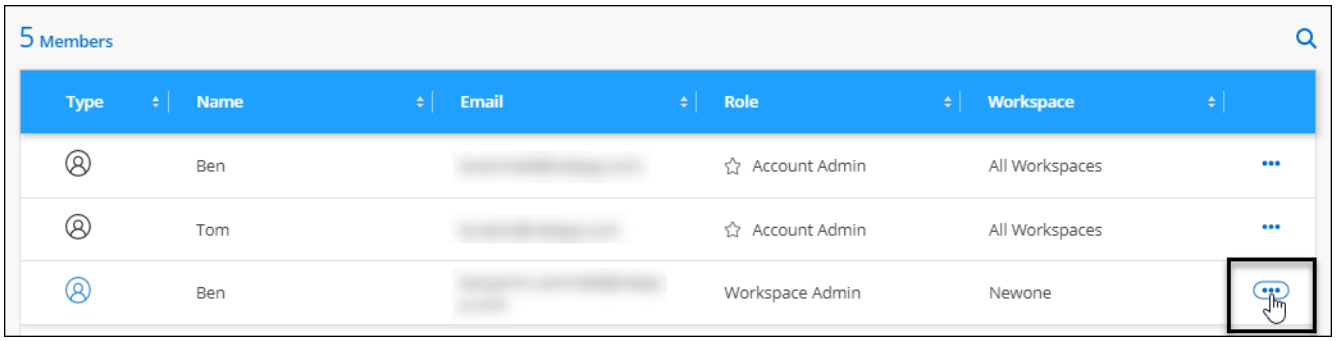
> Sie müssen den Connector auch mit Workspaces verknüpfen, damit Workspace-Administratoren auf die Workspaces von BlueXP zugreifen können. "Erfahren Sie, wie Sie die Arbeitsbereiche eines Connectors verwalten".

Schritte

1. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus und wählen Sie **Konto verwalten** aus.



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



3. Wählen Sie **Arbeitsbereiche Verwalten**.
4. Wählen Sie die Arbeitsbereiche aus, die dem Benutzer zugeordnet werden sollen, und wählen Sie **Anwenden**.

Ergebnis

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.

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.

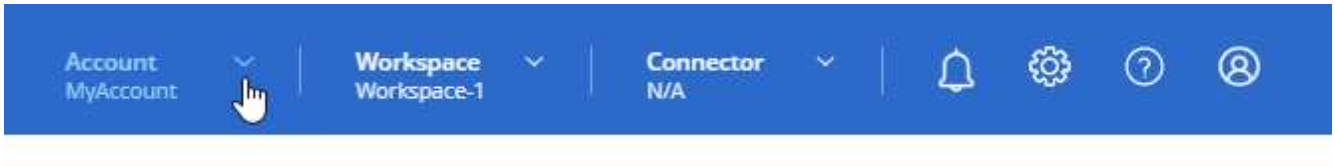
Beachten Sie, dass ein Aktualisierungs-Token für API-Vorgänge nicht erforderlich ist, wenn ein Servicekonto verwendet wird. "Erfahren Sie mehr über das Aktualisieren von Token"

Erstellen eines Dienstkontos

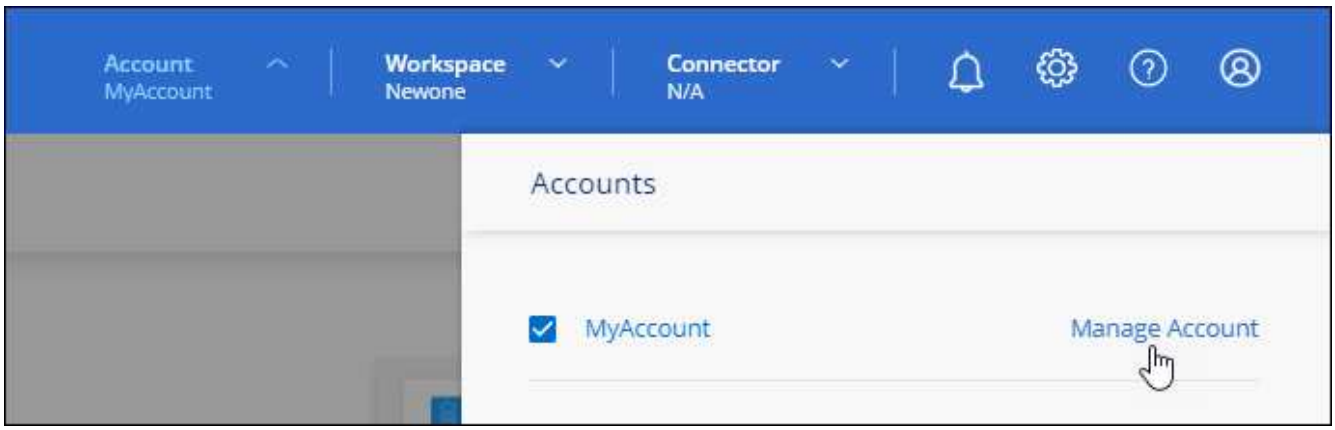
Erstellen Sie so viele Service-Konten wie für das Management der Ressourcen in Ihren Arbeitsumgebungen erforderlich.

Schritte

1. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus.



2. Wählen Sie **Konto verwalten** neben dem aktuell ausgewählten Konto.



3. Wählen Sie auf der Registerkarte Mitglieder die Option **Service-Konto 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. Wählen Sie **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. Wählen Sie **Schließen**.

Holen Sie sich ein Token für den Inhaber eines Dienstkontos ein

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

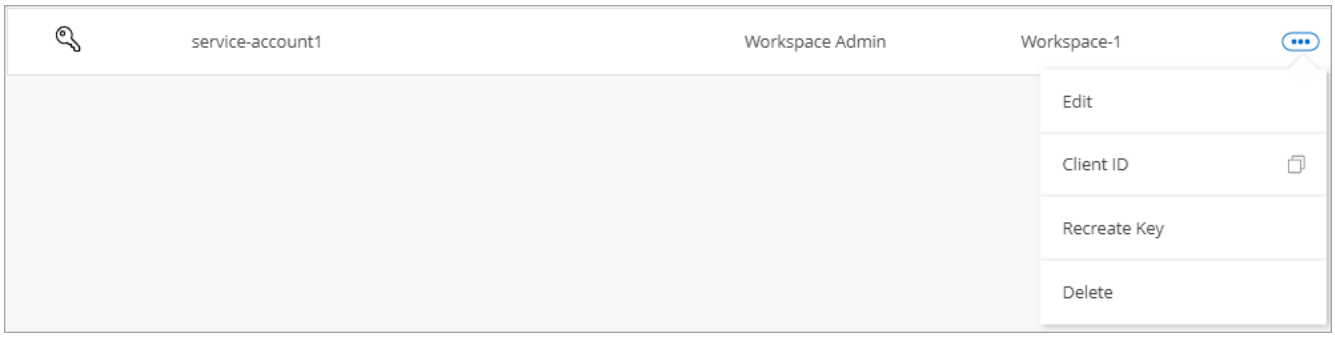
"Erfahren Sie, wie Sie ein Service-Konto-Token erstellen"

Kopieren Sie die Client-ID

Sie können die Client-ID eines Dienstkontos jederzeit kopieren.

Schritte

1. Wählen Sie auf der Registerkarte Mitglieder das Aktionsmenü in der Zeile aus, die dem Servicekonto entspricht.



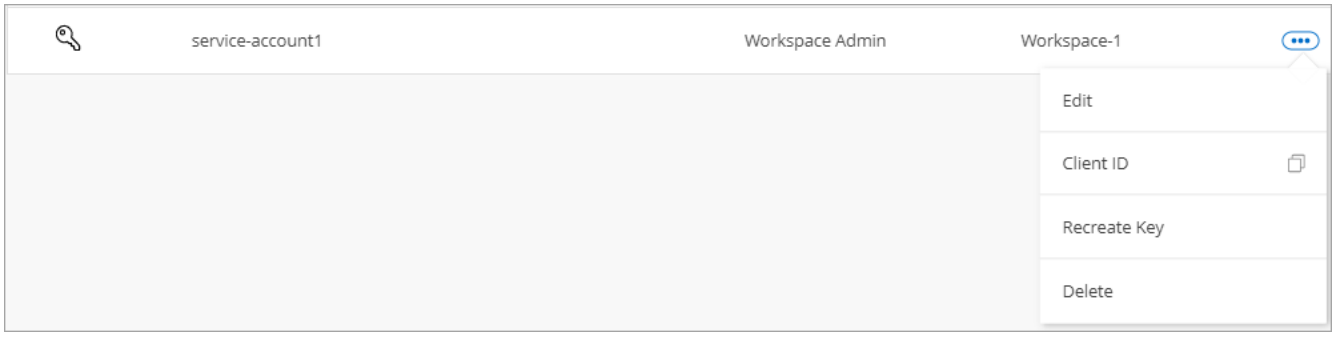
2. Wählen Sie **Client-ID**.
3. Die ID wird in die Zwischenablage kopiert.

Schlüssel neu erstellen

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

Schritte

1. Wählen Sie auf der Registerkarte Mitglieder das Aktionsmenü in der Zeile aus, die dem Servicekonto entspricht.



2. Wählen Sie **Recreate Key**.
3. Wählen Sie zur Bestätigung **recreate**.
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.

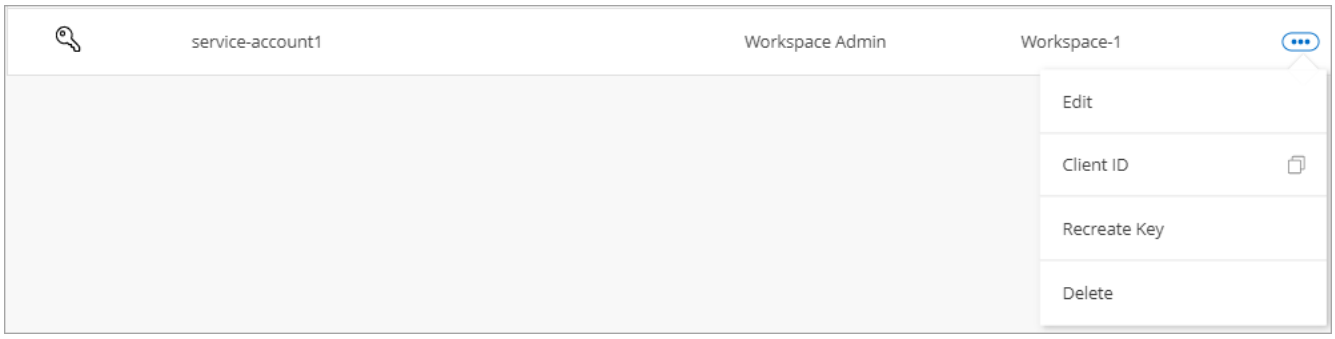
5. Wählen Sie **Schließen**.

Löschen Sie ein Dienstkonto

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

Schritte

1. Wählen Sie auf der Registerkarte Mitglieder das Aktionsmenü in der Zeile aus, die dem Servicekonto entspricht.



2. Wählen Sie **Löschen**.
3. Wählen Sie zur Bestätigung noch einmal **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. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus und wählen Sie **Konto verwalten** aus.
2. Wählen Sie **Workspaces**.
3. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie **Neuen Arbeitsbereich hinzufügen**, um einen neuen Arbeitsbereich zu erstellen.
   - Wählen Sie **Umbenennen**, um den Arbeitsbereich umzubenennen.
   - Wählen Sie **Löschen**, um den Arbeitsbereich zu löschen.

   Wenn Sie einen neuen Arbeitsbereich erstellt haben, müssen Sie den Connector auch zu diesem Arbeitsbereich hinzufügen. Wenn Sie den Connector nicht hinzufügen, können Workspace-Administratoren auf keine der Ressourcen im Arbeitsbereich zugreifen. Weitere Informationen finden Sie im folgenden Abschnitt.

Die Arbeitsbereiche eines Connectors verwalten

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. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus und wählen Sie **Konto verwalten** aus.
2. Wählen Sie **Connector**.
3. Wählen Sie **Arbeitsbereiche verwalten** für den Konnektor, den Sie verknüpfen möchten.
4. Wählen Sie die Arbeitsbereiche aus, die dem Connector zugeordnet werden sollen, und wählen Sie **Apply**.

Ändern Sie Ihren Kontonamen

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

Schritte

1. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus und wählen Sie **Konto verwalten** aus.
2. Wählen Sie auf der Registerkarte **Übersicht** das Bearbeiten-Symbol neben dem Kontonamen.
3. Geben Sie einen neuen Kontonamen ein und wählen Sie **Speichern**.

Private Vorschauen zulassen

Erlauben Sie privaten Vorschauen in Ihrem Konto, auf neue Services zuzugreifen, die als Vorschau in BlueXP 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

1. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus und wählen Sie **Konto verwalten** aus.
2. Aktivieren Sie auf der Registerkarte **Übersicht** die Einstellung **Private Vorschau zulassen**.

Drittanbieter-Services zulassen

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

1. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus und wählen Sie **Konto verwalten** aus.
2. Aktivieren Sie auf der Registerkarte **Übersicht** die Option **Drittanbieter-Services zulassen**.

Überwachen Sie den Betrieb Ihres Kontos

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.

Die folgende Tabelle enthält einen Vergleich zwischen dem Benachrichtigungscenter und der Zeitleiste, damit Sie verstehen können, was jedes einzelne zu bieten hat.

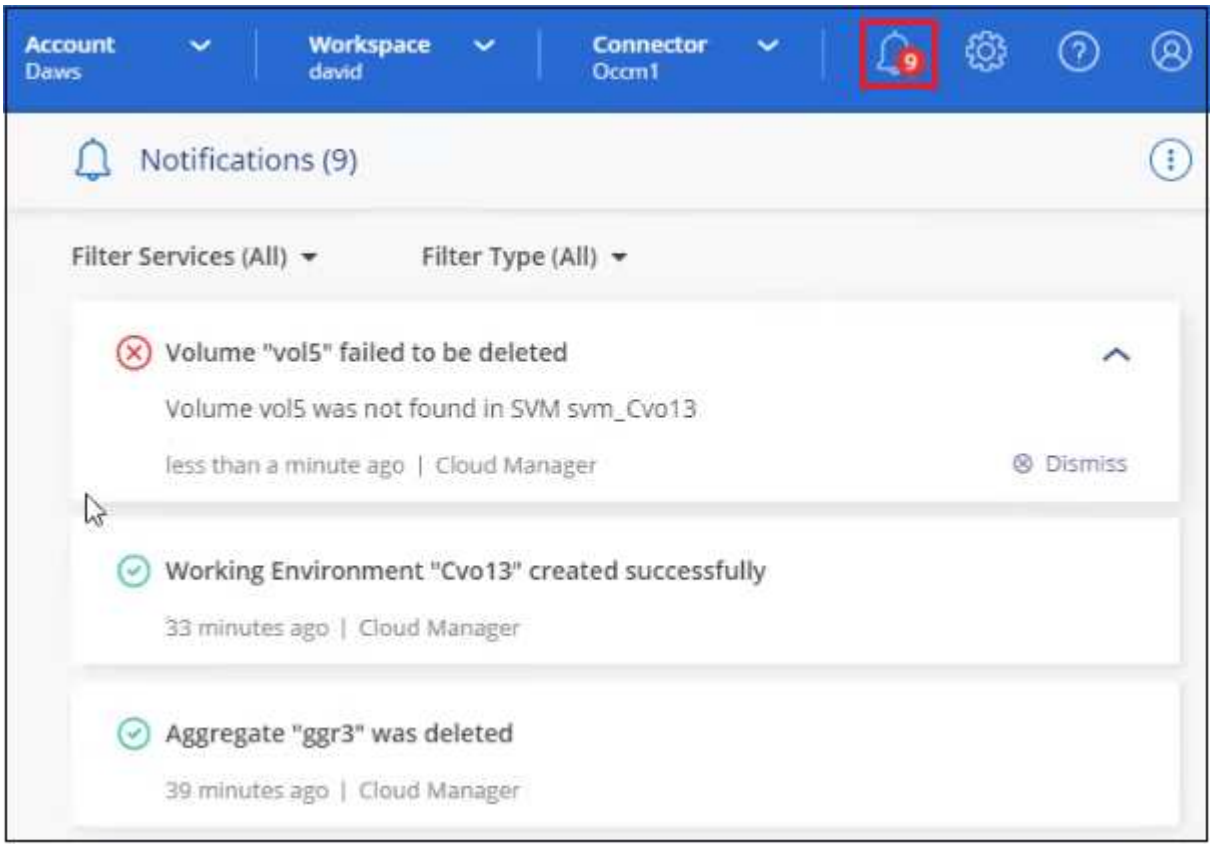
Notification Center	Zeitachse
Zeigt den allgemeinen Status von Ereignissen und Aktionen an	Enthält Details zu jedem Ereignis oder jeder Aktion zur weiteren Untersuchung
Zeigt den Status der aktuellen Anmeldesitzung an (die Informationen werden nach dem Abmelden nicht im Benachrichtigungscenter angezeigt)	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

Notification Center	Zeitachse
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 Sie Aktivitäten mit dem Benachrichtigungscenter

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. Derzeit werden nicht alle BlueXP Services dem Benachrichtigungs-Center gemeldet.

Sie können die Benachrichtigungen anzeigen, indem Sie die Benachrichtigungsanzeige ( ) 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.



Sie können BlueXP auch so konfigurieren, dass bestimmte Arten von Benachrichtigungen per E-Mail gesendet werden, sodass Sie über wichtige Systemaktivitäten informiert werden können, selbst wenn Sie nicht beim System angemeldet sind. Außerdem können E-Mails an alle Benutzer Ihres BlueXP Kontos oder an alle Empfänger gesendet werden, die bestimmte Arten von Systemaktivitäten kennen müssen. Informieren Sie sich darüber Einstellungen für E-Mail-Benachrichtigungen festlegen.

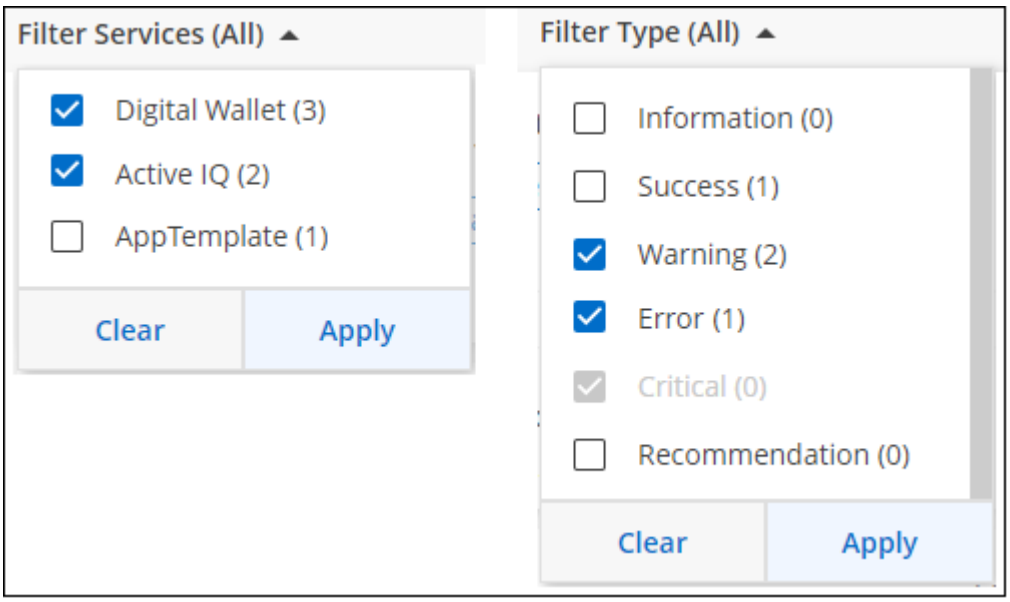
Benachrichtigungstypen

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.
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.

Benachrichtigungen filtern

Standardmäßig werden alle aktiven Benachrichtigungen im Benachrichtigungscenter angezeigt. Sie können die Benachrichtigungen filtern, die Sie sehen, 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.

Benachrichtigungen schließen

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 zu schließen, wählen Sie im Benachrichtigungscenter aus ⋮ Und wählen Sie **Alle verwerfen**.

Um einzelne Benachrichtigungen zu schließen, bewegen Sie den Mauszeiger über die Benachrichtigung und wählen **Abweisen**.

Einstellungen für E-Mail-Benachrichtigungen festlegen

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. Außerdem können E-Mails an alle Benutzer Ihres BlueXP Kontos oder an alle Empfänger gesendet werden, die bestimmte Arten von Systemaktivitäten kennen müssen.

- Derzeit werden Benachrichtigungen zu folgenden BlueXP Funktionen und Services per E-Mail gesendet: Connector, BlueXP Digital Wallet, BlueXP Kopier- und Synchronisierungsfunktion, BlueXP Backup und Recovery, BlueXP Tiering und BlueXP Migrationsberichte. 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.

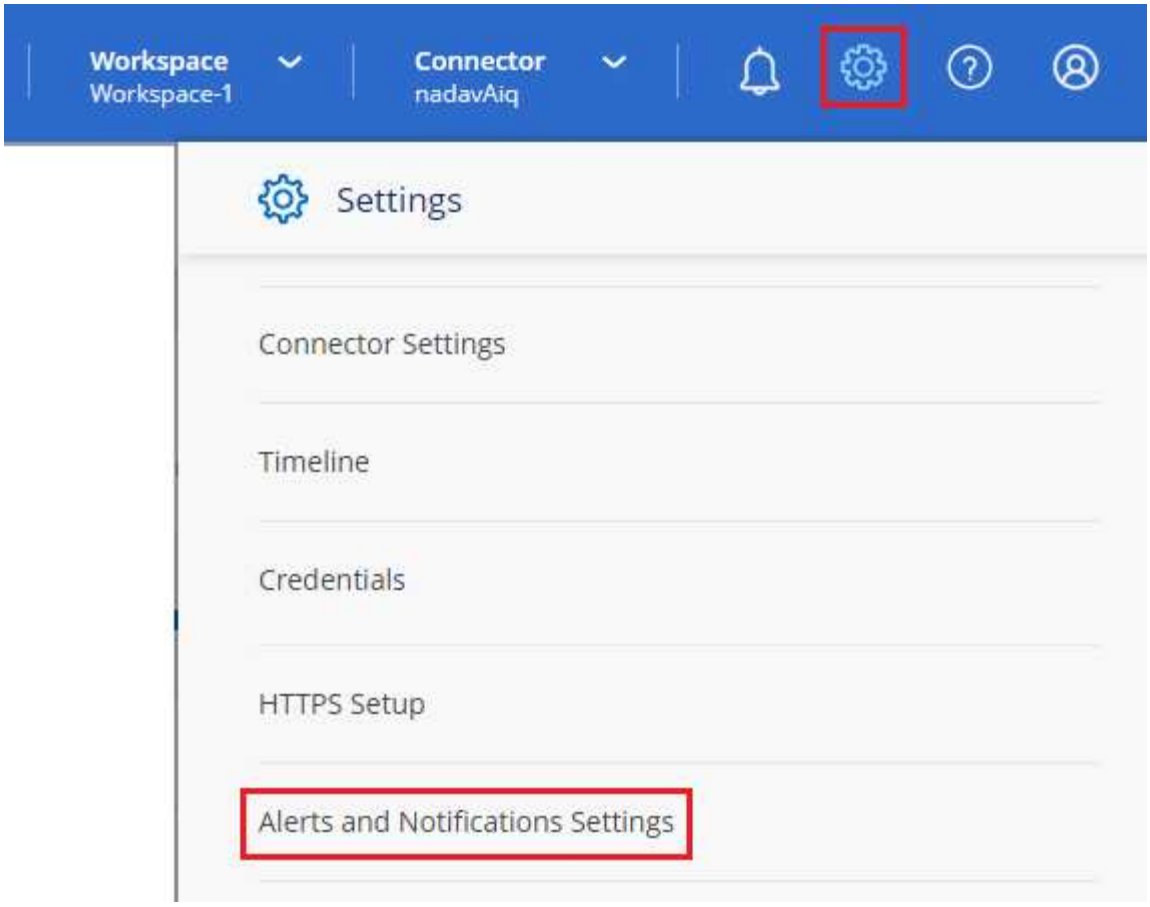
Die Filter, die Sie im Benachrichtigungscenter festlegen, bestimmen nicht, welche Arten von Benachrichtigungen Sie per E-Mail erhalten. Standardmäßig erhalten BlueXP-Kontoadministratoren E-Mails für alle „kritischen“ und „Empfehlungsbenachrichtigungen“. Diese Benachrichtigungen gelten für alle Services. Sie können keine Benachrichtigungen nur für bestimmte Services erhalten, z. B. Connectors oder BlueXP Backup und Recovery.

Alle anderen Benutzer und Empfänger sind so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten. Sie müssen daher die Benachrichtigungseinstellungen für weitere Benutzer konfigurieren.

Sie müssen ein Kontoadministrator sein, um die Benachrichtigungseinstellungen anzupassen.

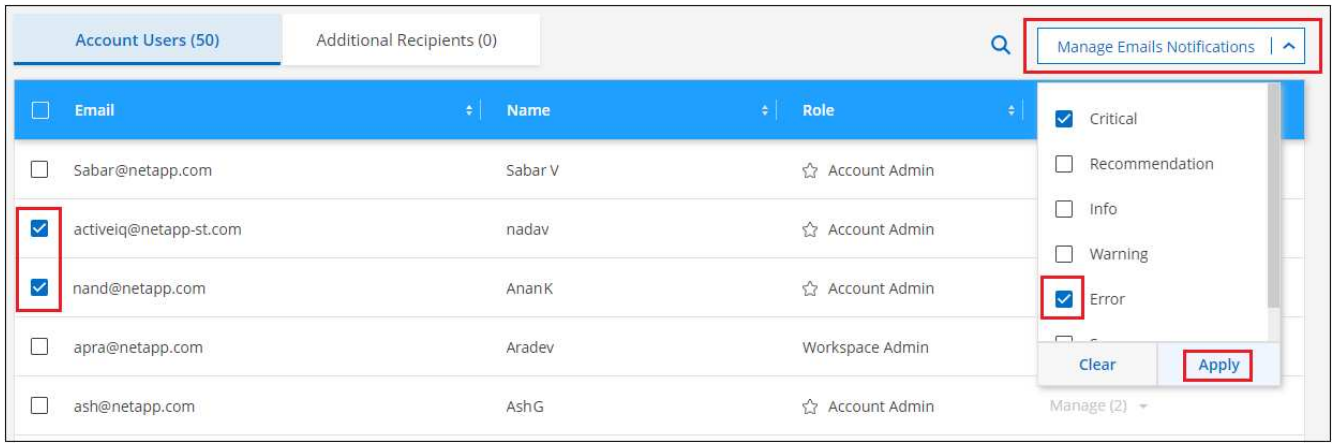
Schritte

1. Wählen Sie in der BlueXP Menüleiste **Einstellungen > Einstellungen für Warnmeldungen und Benachrichtigungen** aus.



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 für einen einzelnen Benutzer vorzunehmen, wählen Sie das Menü in der Spalte Benachrichtigungen für diesen Benutzer aus, überprüfen Sie die zu sendenden Benachrichtigungstypen und wählen Sie **Anwenden** aus.
   - Um Änderungen für mehrere Benutzer vorzunehmen, aktivieren Sie das Kontrollkästchen für jeden Benutzer, wählen Sie **E-Mail-Benachrichtigungen verwalten**, aktivieren Sie die zu sendenden Benachrichtigungstypen und wählen Sie **Anwenden** aus.

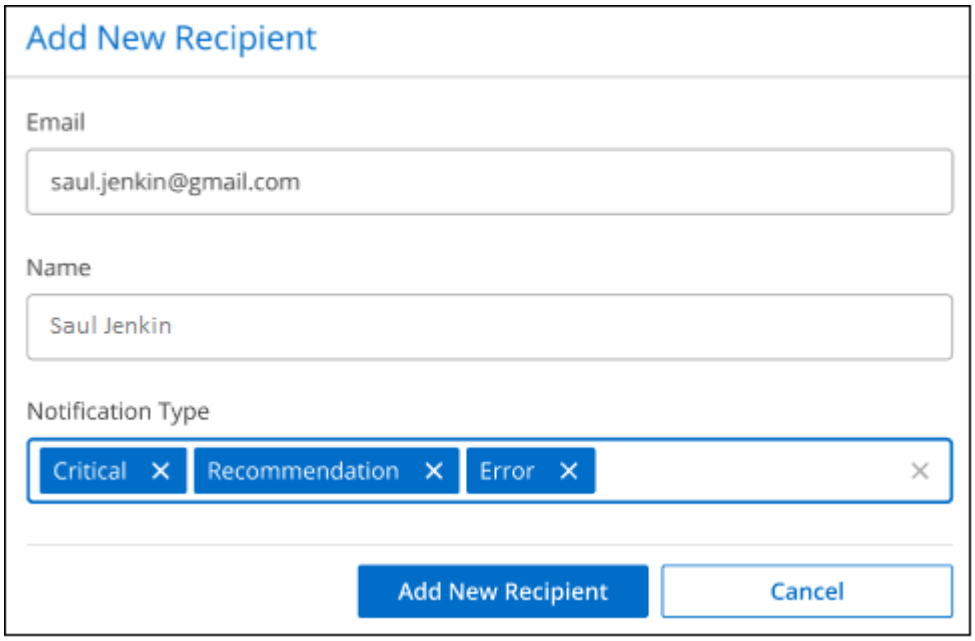


Fügen Sie weitere E-Mail-Empfänger hinzu

Die Benutzer, die auf der Registerkarte „*Account users*“ angezeigt werden, werden automatisch von den Benutzern in Ihrem BlueXP Konto (über die) ausgefüllt "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. Wählen Sie auf der Seite Einstellungen für Warnmeldungen und Benachrichtigungen die Option **Neue Empfänger hinzufügen** aus.



2. Geben Sie den Namen und die E-Mail-Adresse ein, und wählen Sie die Benachrichtigungstypen aus, die der Empfänger erhalten soll, und wählen Sie **Neuen Empfänger hinzufügen**.

Überwachen Sie die Benutzeraktivität in Ihrem Konto

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. Wählen Sie in der BlueXP Menüleiste **Einstellungen > Zeitleiste**.
2. Wählen Sie unter den Filtern **Service**, Enable **Tenancy** und wählen Sie **Apply**.

Ergebnis

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

Ein weiteres BlueXP Konto erstellen

Wenn Sie sich bei BlueXP anmelden, werden Sie aufgefordert, ein Konto für Ihr

Unternehmen zu erstellen. Dieser Account könnte alles sein, was Sie benötigen. Wenn Ihr Unternehmen jedoch mehrere Accounts benötigt, müssen Sie mithilfe der Mandanten-API zusätzliche Konten erstellen.

Erstellen Sie mithilfe des folgenden API-Anrufs ein zusätzliches BlueXP Konto:

POST `/tenancy/account/{accountName}`

Wenn Sie den eingeschränkten Modus aktivieren möchten, müssen Sie Folgendes in den Anforderungstext aufnehmen:

```
{
  "isSaasDisabled": true
}
```

> Die Einstellung für den eingeschränkten Modus kann nicht geändert werden, nachdem BlueXP das Konto erstellt hat. Der eingeschränkte Modus kann später nicht aktiviert werden, und Sie können ihn später nicht mehr deaktivieren. Sie muss zum Zeitpunkt der Kontoerstellung festgelegt werden.

"Erfahren Sie, wie Sie diesen API-Aufruf verwenden"

Weiterführende Links

- "Mehr zu BlueXP Accounts"
- "Weitere Informationen zu BlueXP Implementierungsmodi"

Benutzerrollen

Die Rollen Kontoverwaltung, Arbeitsbereichsverwaltung, Compliance Viewer und SnapCenter-Admin bieten Benutzern spezifische Berechtigungen. Sie können eine dieser Rollen zuweisen, wenn Sie einen neuen Benutzer mit Ihrem BlueXP Konto verknüpfen.

Die Compliance Viewer-Rolle dient dem schreibgeschützten BlueXP Klassifizierungszugriff.

Aufgabe	Kontoadministrator	Workspace-Verwaltung	Compliance Viewer	SnapCenter Admin
Verwalten von Arbeitsumgebungen	Ja.	Ja.	Nein	Nein
Services in Arbeitsumgebungen ermöglichen	Ja.	Ja.	Nein	Nein
Entfernen von Arbeitsumgebungen aus einem Arbeitsbereich	Ja.	Ja.	Nein	Nein
Arbeitsumgebungen löschen	Ja.	Ja.	Nein	Nein

Aufgabe	Kontoadministrator	Workspace-Verwaltung	Compliance Viewer	SnapCenter Admin
Anzeigen des Status der Datenreplizierung	Ja.	Ja.	Nein	Nein
Zeitachse anzeigen	Ja.	Ja.	Nein	Nein
Wechseln Sie zwischen Arbeitsbereichen	Ja.	Ja.	Ja.	Nein
Sehen Sie sich die Ergebnisse des BlueXP Klassifizierungs-Scans an	Ja.	Ja.	Ja.	Nein
Cloud Volumes ONTAP Bericht erhalten	Ja.	Nein	Nein	Nein
Anschlüsse Erstellen	Ja.	Nein	Nein	Nein
BlueXP Konten 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
Installieren Sie ein HTTPS-Zertifikat	Ja.	Nein	Nein	Nein

Weiterführende Links

- "Einrichten von Workspaces und Benutzern im BlueXP Konto"
- "Managen von Workspaces und Benutzern im BlueXP Konto"

Anschlüsse

Suchen Sie die System-ID für einen Anschluss

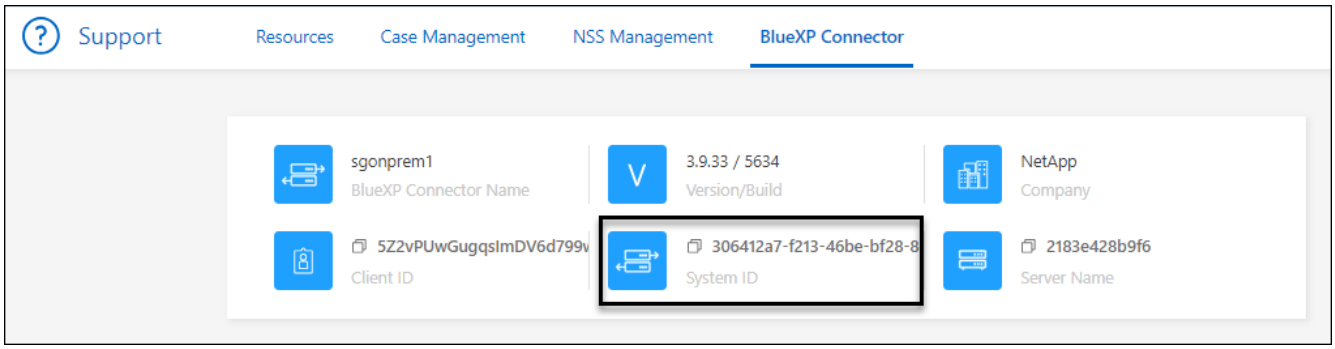
Um Ihnen bei den ersten Schritten zu helfen, fragen Sie möglicherweise Ihr NetApp Ansprechpartner nach der System-ID Ihres Connectors. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol aus.
2. Wählen Sie **Support > BlueXP Connector**.

   Die System-ID wird oben auf der Seite angezeigt.

   Beispiel



Verwalten Sie vorhandene Anschlüsse

Nachdem Sie einen Connector erstellt haben, müssen Sie ihn möglicherweise ab und zu verwalten. Sie können beispielsweise zwischen den Anschlüssen wechseln, wenn Sie über mehrere verfügen. Oder Sie müssen den Connector möglicherweise manuell aktualisieren, wenn Sie BlueXP im privaten Modus verwenden.

"Erfahren Sie, wie Anschlüsse funktionieren".

> Der Connector enthält eine lokale Benutzeroberfläche, auf die über den Connector-Host zugegriffen werden kann. Diese UI steht Kunden zur Verfügung, die BlueXP im eingeschränkten Modus oder im privaten Modus verwenden. Wenn Sie BlueXP im Standardmodus verwenden, sollten Sie über die auf die Benutzeroberfläche zugreifen "BlueXP SaaS-Konsole"
>
> "Weitere Informationen zu BlueXP Implementierungsmodi".

Betriebssystem- und VM-Wartung

Die Wartung des Betriebssystems auf dem Connector-Host liegt in Ihrer Verantwortung. Sie sollten beispielsweise Sicherheitsupdates auf dem Betriebssystem auf dem Connector-Host anwenden, indem Sie die Standardverfahren Ihres Unternehmens für die Betriebssystemverteilung befolgen.

Beachten Sie, dass Sie keine Dienste auf dem Connector-Host anhalten müssen, wenn Sie ein Betriebssystem-Update ausführen.

Wenn Sie die Connector VM anhalten und dann starten müssen, sollten Sie dies über die Konsole Ihres Cloud-Providers oder mithilfe der Standardverfahren für das On-Premises-Management tun.

"Beachten Sie, dass der Connector jederzeit betriebsbereit sein muss".

VM oder Instanztyp

Wenn Sie einen Connector direkt aus BlueXP erstellt haben, hat BlueXP eine Virtual Machine-Instanz in Ihrem Cloud-Provider implementiert, die eine Standardkonfiguration verwendet. Nachdem Sie den Connector erstellt haben, sollten Sie nicht zu einer kleineren VM-Instanz wechseln, die weniger CPU oder RAM hat.

Die CPU- und RAM-Anforderungen lauten wie folgt:

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

"Informieren Sie sich über die Standardkonfiguration des Connectors".

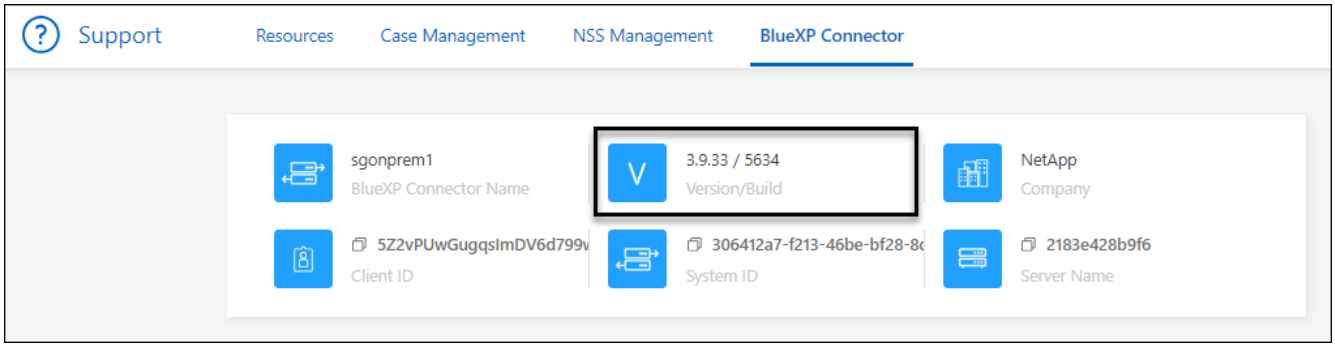
Anzeigen der Version eines Connectors

Sie können die Version Ihres Connectors anzeigen, um zu überprüfen, ob der Connector automatisch auf die neueste Version aktualisiert wurde, oder weil Sie ihn mit Ihrem NetApp-Vertreter teilen müssen.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol aus.
2. Wählen Sie **Support > BlueXP Connector**.

   Die Version wird oben auf der Seite angezeigt.



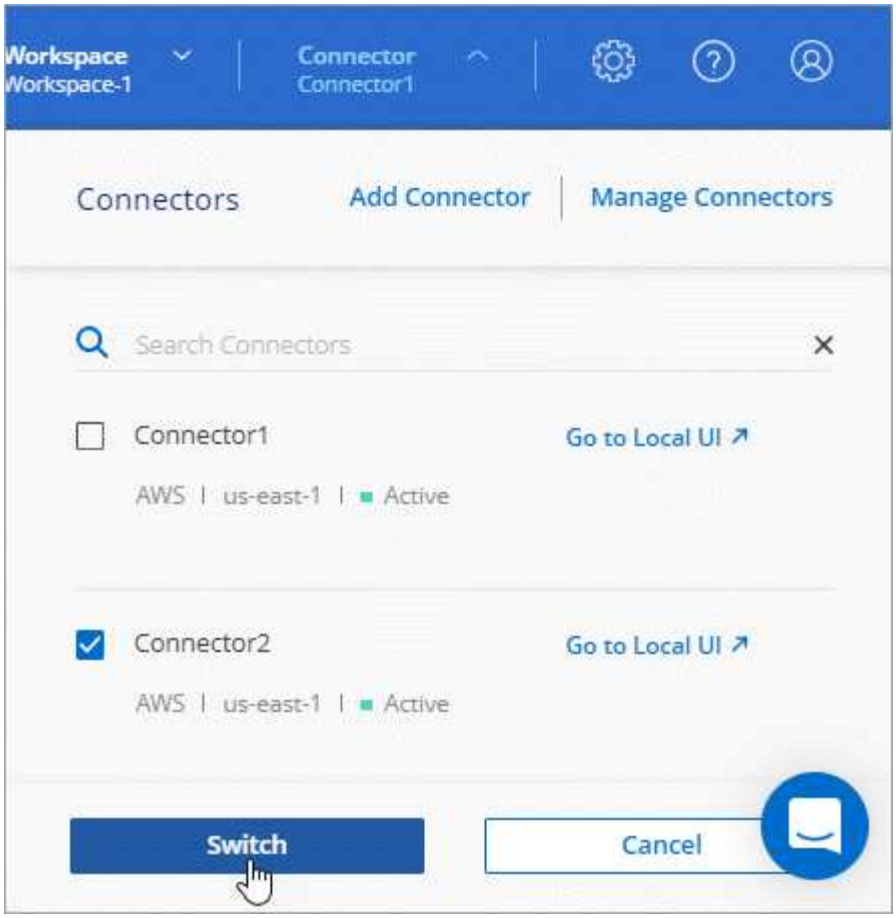
Zwischen den Anschlüssen wechseln

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. Wählen Sie die Dropdown-Liste **Connector** aus, wählen Sie einen anderen Konnektor aus und wählen Sie dann **Switch** aus.



Ergebnis

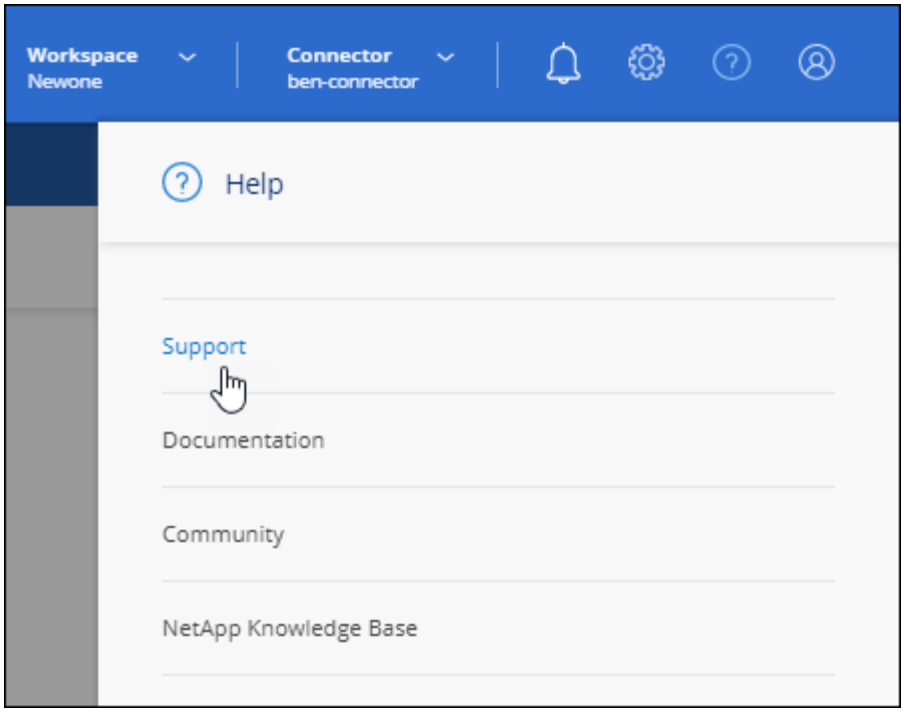
BlueXP aktualisiert und zeigt die Arbeitsumgebungen, die mit dem ausgewählten Connector verknüpft sind.

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

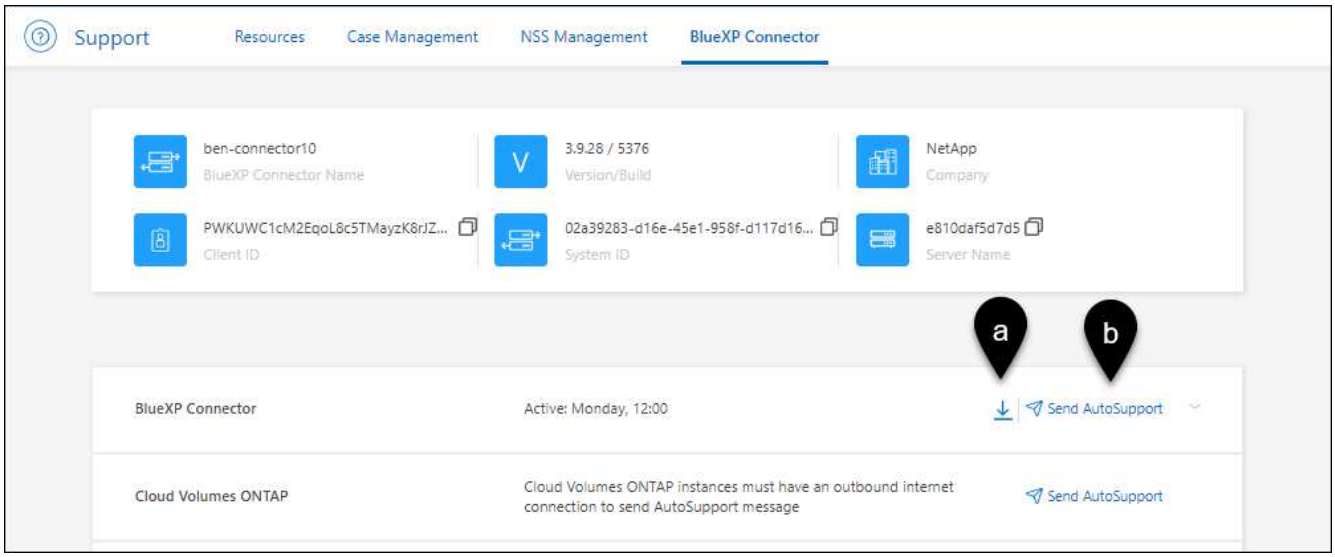
1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



2. Wählen Sie **BlueXP Connector** aus.
3. 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. Wählen Sie **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. Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).

"AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"

Azure

Beim Erstellen der Connector-VM in Azure haben Sie einen Benutzernamen angegeben und sich für die Authentifizierung mit einem Kennwort oder einem öffentlichen SSH-Schlüssel entschieden. 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 (gcloudd) herstellen.

"Google Cloud Docs: Verbindung zu Linux-VMs herstellen"

Erfordern die Verwendung von IMDSv2 auf Amazon EC2 Instanzen

Ab März 2024 unterstützt BlueXP jetzt den Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) mit dem Connector und Cloud Volumes ONTAP (einschließlich des Mediators für HA-Implementierungen). In den meisten Fällen wird IMDSv2 automatisch auf neuen EC2-Instanzen konfiguriert. IMDSv1 wurde vor März 2024 aktiviert. Falls dies durch Ihre Sicherheitsrichtlinien erforderlich ist, müssen Sie IMDSv2 möglicherweise manuell auf Ihren EC2-Instanzen konfigurieren.

Über diese Aufgabe

IMDSv2 bietet einen verbesserten Schutz vor Schwachstellen. "Weitere Informationen zu IMDSv2 finden Sie im AWS Security Blog"

Der Instance Metadata Service (IMDS) wird in EC2-Instanzen wie folgt aktiviert:

- Für neue Connector-Implementierungen von BlueXP oder durch die Nutzung von "Terraform-Skripte", IMDSv2 ist standardmäßig auf der EC2-Instanz aktiviert.
- Wenn Sie eine neue EC2-Instanz in AWS starten und dann die Connector-Software manuell installieren, ist IMDSv2 standardmäßig ebenfalls aktiviert.
- Wenn Sie den Connector vom AWS Marketplace starten, ist IMDSv1 standardmäßig aktiviert. Sie können IMDSv2 auf der EC2-Instanz manuell konfigurieren.
- Für bestehende Connectors wird IMDSv1 weiterhin unterstützt, Sie können IMDSv2 jedoch manuell auf der EC2-Instanz konfigurieren, wenn Sie dies wünschen.
- Für Cloud Volumes ONTAP ist IMDSv1 standardmäßig auf neuen und bestehenden Instanzen aktiviert. Sie können IMDSv2 auf den EC2-Instanzen manuell konfigurieren, wenn Sie möchten.

Bevor Sie beginnen

- Die Connector-Version muss 3.9.38 oder höher sein.
- Cloud Volumes ONTAP muss eine der folgenden Versionen ausführen:
  - 9.12.1 P2 (oder jedes weitere Patch)

- 9.13.0 P4 (oder jedes weitere Patch)
- 9.13.1 oder eine beliebige Version nach dieser Version

- Diese Änderung erfordert einen Neustart der Cloud Volumes ONTAP-Instanzen.

Über diese Aufgabe

Für diese Schritte ist die Verwendung der AWS CLI erforderlich, da Sie das Limit für den Response-Hop auf 3 ändern müssen.

Schritte

1. Erfordern die Verwendung von IMDSv2 auf der Connector-Instanz:

   a. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.

      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. Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).

      "AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"

   b. Installieren Sie die AWS CLI.

      "AWS Docs: Installieren oder aktualisieren Sie auf die neueste Version der AWS CLI"

   c. Verwenden Sie die `aws ec2 modify-instance-metadata-options` Befehl, um die Verwendung von IMDSv2 zu erfordern und das PUT Response Hop Limit auf 3 zu ändern.

      Beispiel

      ```
      aws ec2 modify-instance-metadata-options \
          --instance-id <instance-id> \
          --http-put-response-hop-limit 3 \
          --http-tokens required \
          --http-endpoint enabled
      ```

      Der `http-tokens` Parameter setzt IMDSv2 auf erforderlich. Wenn `http-tokens` Ist erforderlich, müssen Sie auch festlegen `http-endpoint` Auf aktiviert.

2. Erfordern die Verwendung von IMDSv2 auf Cloud Volumes ONTAP Instanzen:

   a. Wechseln Sie zum "Amazon EC2 Konsole"

   b. Wählen Sie im Navigationsbereich **instances** aus.

   c. Wählen Sie eine Cloud Volumes ONTAP-Instanz aus.

   d. Wählen Sie **Aktionen > Instanzeinstellungen > Optionen für Instanzmetadaten ändern**.

   e. Wählen Sie im Dialogfeld **Modify Instance Metadata options** Folgendes aus:

      - Wählen Sie für **Instance Metadata Service enable** aus.
      - Wählen Sie für **IMDSv2 required** aus.

    - Wählen Sie **Speichern**.

f. Wiederholen Sie diese Schritte für andere Cloud Volumes ONTAP Instanzen, einschließlich des HA Mediators.

g. "Stoppen und starten Sie die Cloud Volumes ONTAP-Instanzen"

Ergebnis

Die Connector-Instanz und die Cloud Volumes ONTAP-Instanzen sind jetzt so konfiguriert, dass sie IMDSv2 verwenden.

Aktualisieren Sie den Connector, wenn Sie den privaten Modus verwenden

Wenn Sie BlueXP im privaten Modus nutzen, können Sie den Connector aktualisieren, wenn eine neuere Version von der NetApp Support Site verfügbar ist.

Der Connector muss während des Upgrade-Vorgangs neu gestartet werden, damit die webbasierte Konsole während des Upgrades nicht verfügbar ist.

> Wenn Sie BlueXP im Standardmodus oder im eingeschränkten Modus verwenden, aktualisiert der Connector seine Software automatisch auf die neueste Version, sofern er über ausgehenden Internetzugang verfügt, um das Softwareupdate zu erhalten.

Schritte

1. Laden Sie die Connector-Software von der herunter "NetApp Support Website".

   Stellen Sie sicher, dass Sie das Offline-Installationsprogramm für private Netzwerke ohne Internetzugang herunterladen.

2. Kopieren Sie das Installationsprogramm auf den Linux-Host.
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   ```
   chmod +x /path/BlueXP-Connector-offline-<version>
   ```

   Wobei <version> die Version des Connectors ist, den Sie heruntergeladen haben.

4. Führen Sie das Installationsskript aus:

   ```
   sudo /path/BlueXP-Connector-offline-<version>
   ```

   Wobei <version> die Version des Connectors ist, den Sie heruntergeladen haben.

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

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.

   Sie müssen den Backup-Speicherort für jedes Cloud Volumes ONTAP-System aktualisieren.

   a. Führen Sie den folgenden Befehl über die Cloud Volumes ONTAP-CLI aus, um das aktuelle Backup-Ziel anzuzeigen:

   ```
   system configuration backup show
   ```

   b. Führen Sie den folgenden Befehl aus, um die IP-Adresse für das Backup-Ziel zu aktualisieren:

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

Bearbeiten Sie die URIs eines Connectors

Fügen Sie den Uniform Resource Identifier (URI) für einen Connector hinzu und entfernen Sie ihn.

Schritte

1. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.
2. Wählen Sie **Connectors Verwalten**.
3. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **URIs bearbeiten**.
4. Fügen Sie URIs hinzu und entfernen Sie sie, und wählen Sie dann **Apply**.

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"

Entfernen Sie die Anschlüsse von BlueXP

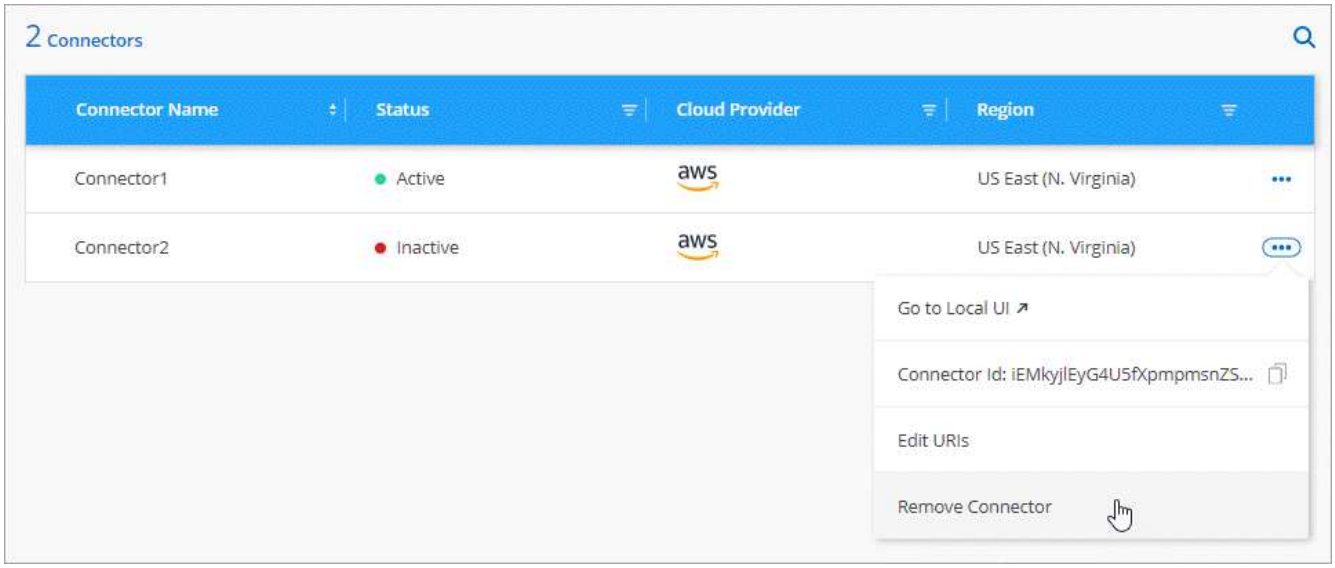
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in BlueXP entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

Beachten Sie Folgendes zum Entfernen eines Konnektors:

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

Schritte

1. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.
2. Wählen Sie **Connectors Verwalten**.
3. Wählen Sie das Aktionsmenü für einen inaktiven Konnektor aus und wählen Sie **Connector entfernen**.



4. Geben Sie den Namen des zu bestätigten Connectors ein, und wählen Sie dann **Entfernen**.

Ergebnis

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 (Standardmodus oder eingeschränkter Modus) oder auf einem Host in einem Netzwerk ohne Internetzugang (privater Modus) installiert haben.

Deinstallieren, wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden

Mit den folgenden Schritten können Sie die Connector-Software deinstallieren, wenn Sie BlueXP im Standardmodus oder im eingeschränkten Modus verwenden.

Schritte

1. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.
2. Führen Sie auf dem Linux-Host das Deinstallationsskript aus:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

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

Deinstallieren Sie die Software, wenn Sie den privaten Modus verwenden

Mit den folgenden Schritten können Sie die Connector-Software deinstallieren, wenn Sie BlueXP im privaten Modus verwenden, auf den kein Internetzugang verfügbar ist.

Schritte

1. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.
2. Führen Sie auf dem Linux-Host die folgenden Befehle aus:

   ```
   ./opt/application/netapp/ds/cleanup.sh
   rm -rf /opt/application/netapp/ds
   ```

Installieren Sie ein HTTPS-Zertifikat für sicheren Zugriff

Standardmäßig verwendet BlueXP ein selbstsigniertes Zertifikat für HTTPS-Zugriff auf die Webkonsole. Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle signiertes Zertifikat installieren, das einen besseren Schutz bietet als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie".

Installieren Sie ein HTTPS-Zertifikat

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

Schritte

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

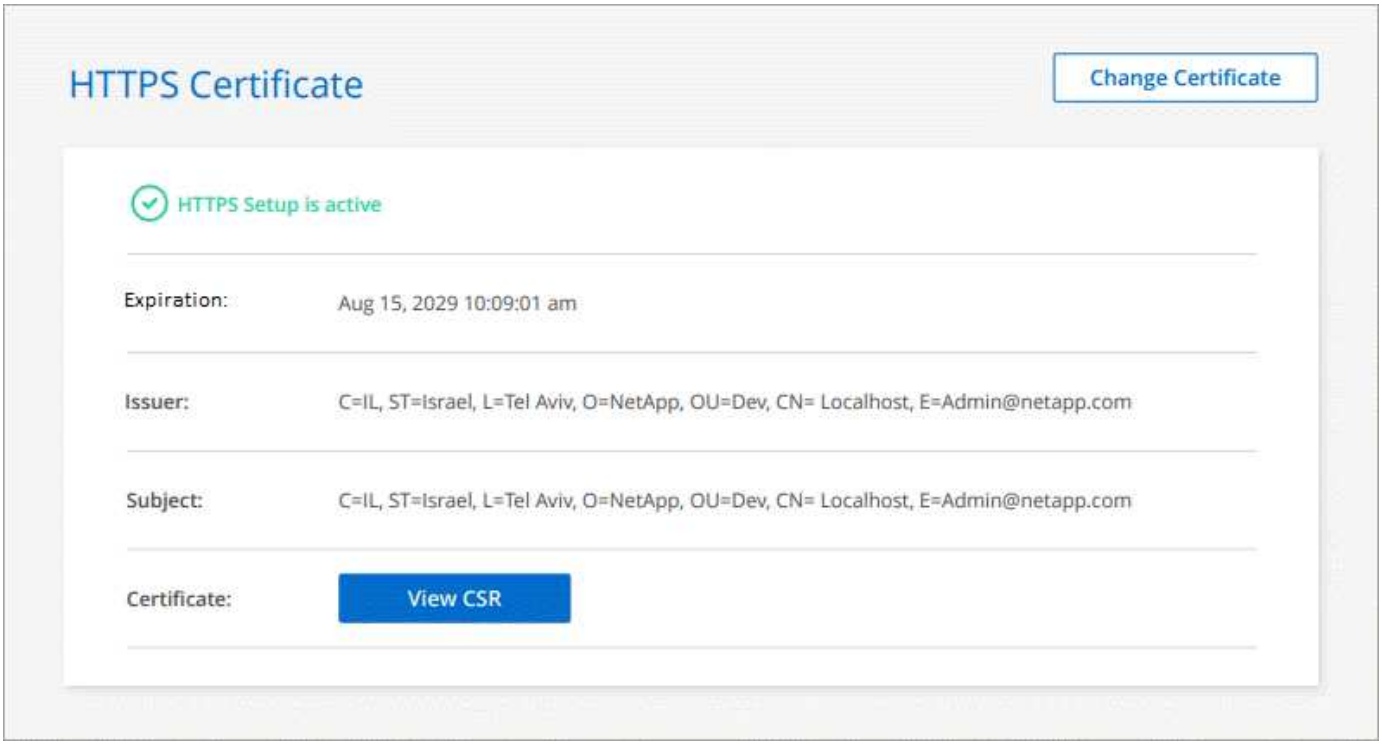
2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung

(CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

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

Ergebnis

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 Sie das BlueXP HTTPS-Zertifikat

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 auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS Setup** aus.

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

2. Wählen Sie **Zertifikat ändern** und folgen Sie den Schritten, um eine CSR zu generieren oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

Ergebnis

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

Konfigurieren Sie einen Konnektor für die Verwendung eines Proxy-Servers

Wenn Sie in Ihren Unternehmensrichtlinien einen Proxyserver für die gesamte Kommunikation mit dem Internet verwenden müssen, müssen Sie Ihre Connectors so konfigurieren, dass sie diesen Proxy-Server verwenden. Wenn Sie während der Installation keinen Connector so konfiguriert haben, dass er einen Proxyserver verwendet, können Sie den Connector so konfigurieren, dass er diesen Proxyserver verwendet.

Wenn der Connector für die Verwendung eines Proxy-Servers konfiguriert wird, erhält der ausgehende Internetzugriff, wenn eine öffentliche IP-Adresse oder ein NAT-Gateway nicht 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. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Unterstützte Konfigurationen

- BlueXP unterstützt HTTP und HTTPS.
- Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.
- BlueXP unterstützt keine transparenten Proxyserver.

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 Vorgänge ausführt, bevor Sie fortfahren.

Schritte

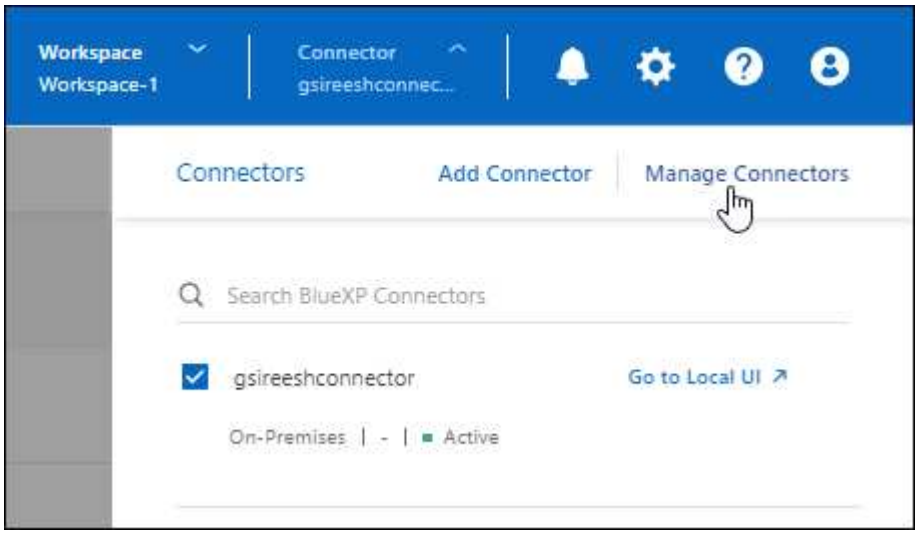
1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**.

   Die Navigation hängt davon ab, ob Sie BlueXP im Standardmodus (Zugriff auf die BlueXP Schnittstelle über die SaaS-Website) oder BlueXP im eingeschränkten Modus oder privaten Modus nutzen (lokaler Zugriff auf die BlueXP Schnittstelle vom Connector-Host aus).

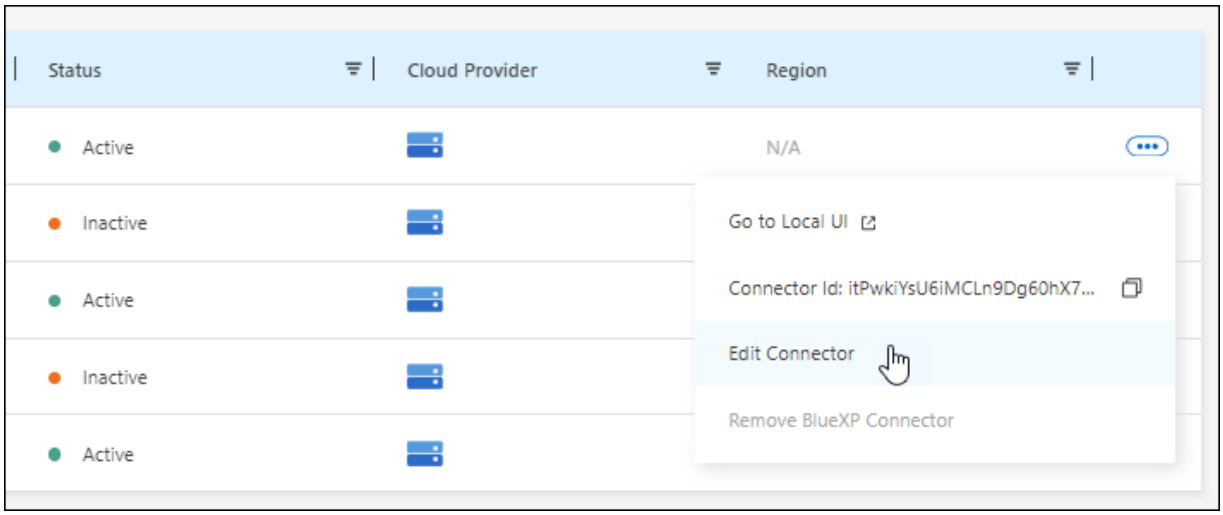
Standardmodus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connectors Verwalten**.



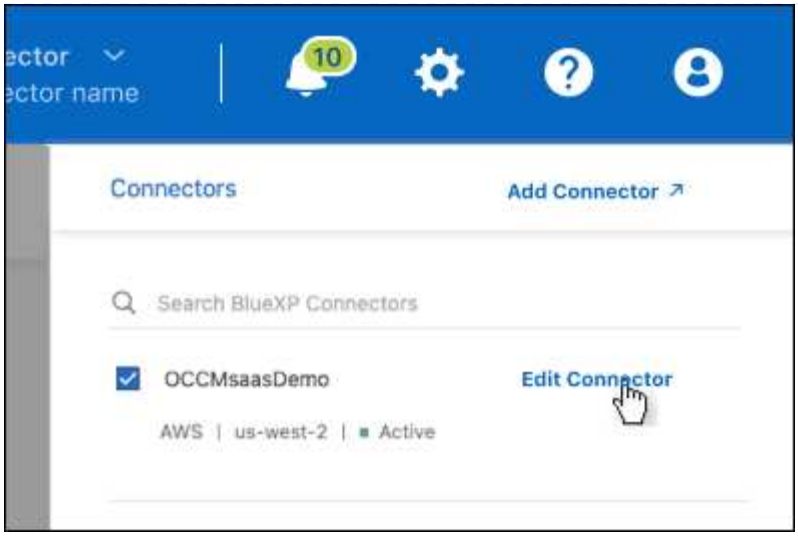
c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.



Eingeschränkter oder privater Modus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connector Bearbeiten**.



2. Wählen Sie **HTTP Proxy Configuration** aus.
3. Richten Sie den Proxy ein:
   a. Wählen Sie **Proxy Aktivieren**.
   b. Geben Sie den Server mithilfe der Syntax an http://address:port Oder https://address:port
   c. Geben Sie einen Benutzernamen und ein Kennwort an, wenn eine grundlegende Authentifizierung für den Server erforderlich ist.

      Beachten Sie Folgendes:

      - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
      - Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie folgt eingeben: Domain-Name%92user-Name

        Beispiel: netapp%92Proxy

      - BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.
   d. Wählen Sie **Speichern**.

Aktivieren Sie direkten API-Verkehr

Wenn Sie einen Connector für die Verwendung eines Proxy-Servers konfiguriert haben, können Sie direkten API-Datenverkehr auf dem Connector aktivieren, um API-Aufrufe direkt an Cloud-Provider-Dienste zu senden, ohne über den Proxy zu gehen. Diese Option wird mit Connectors unterstützt, die in AWS, in Azure oder in Google Cloud ausgeführt werden.

Wenn Sie die Verwendung von privaten Azure-Links mit Cloud Volumes ONTAP deaktiviert und stattdessen Service-Endpunkte verwenden, müssen Sie direkten API-Datenverkehr aktivieren. Andernfalls wird der Datenverkehr nicht korrekt geleitet.

"Weitere Informationen zur Verwendung eines Azure Private Links oder von Service-Endpunkten mit Cloud Volumes ONTAP"

Schritte

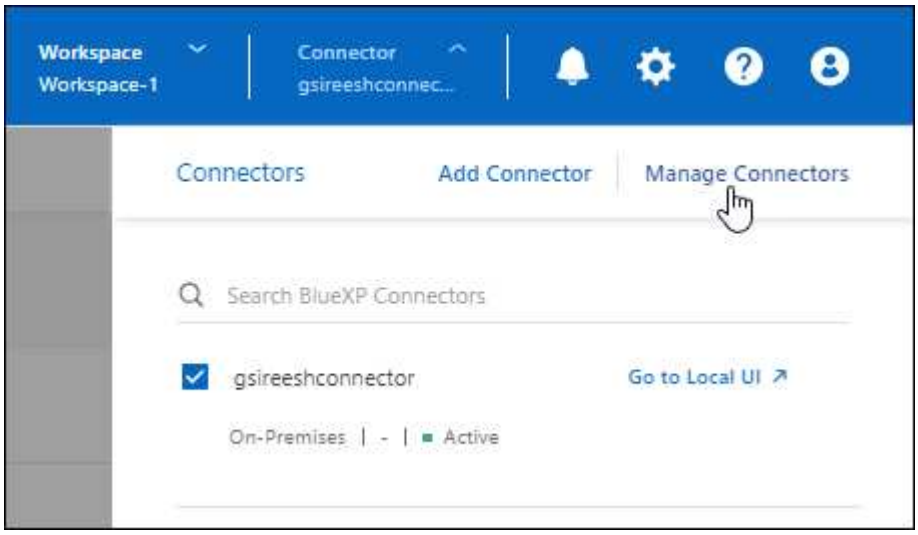
1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**:

   Die Navigation hängt davon ab, ob Sie BlueXP im Standardmodus (Zugriff auf die BlueXP Schnittstelle über die SaaS-Website) oder BlueXP im eingeschränkten Modus oder privaten Modus nutzen (lokaler Zugriff auf die BlueXP Schnittstelle vom Connector-Host aus).

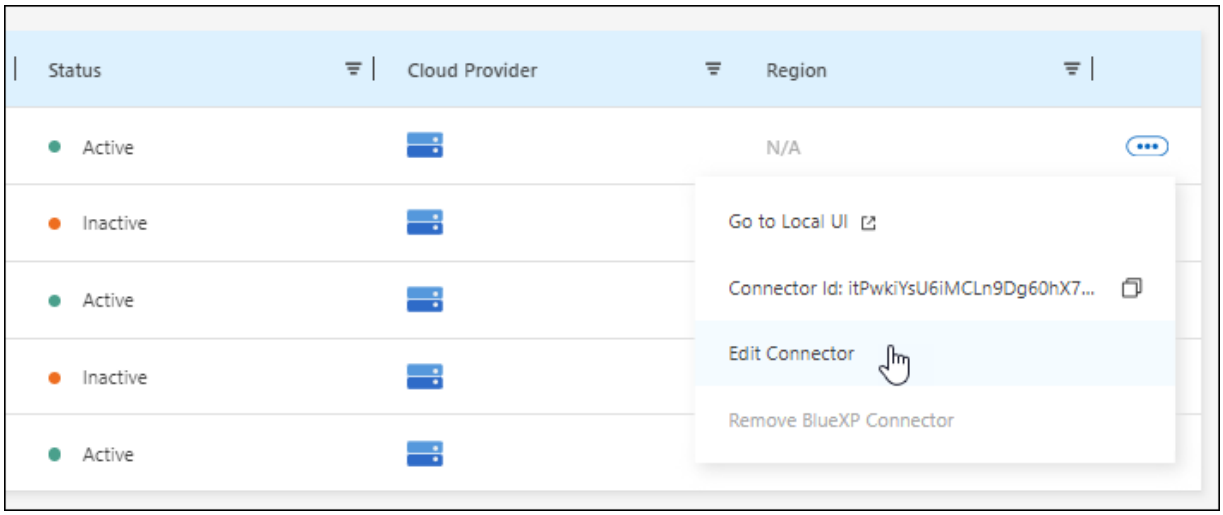
Standardmodus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connectors Verwalten**.



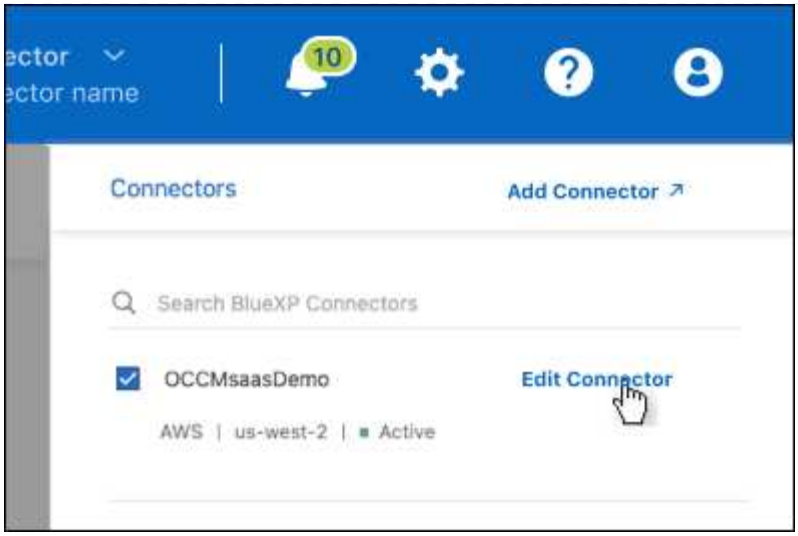
c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.



Eingeschränkter oder privater Modus

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connector Bearbeiten**.



2. Wählen Sie **Support Direct API Traffic**.
3. Aktivieren Sie das Kontrollkästchen, um die Option zu aktivieren, und wählen Sie dann **Speichern**.

Standardkonfiguration für den Konnektor

Möglicherweise möchten Sie mehr über die Konfiguration des Connectors 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 Ubuntu 22.04 LTS.

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

- Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername 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 Ubuntu 22.04 LTS.

  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 implementiert haben, beachten Sie Folgendes:

- Die VM-Instanz ist n2-Standard-4.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  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
  Oder
- /Opt/Application/netapp/Service-Manager-2/logs (beginnend mit den neuen 3.9.23 Installationen)

  Die Protokolle in diesen Ordnern 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.

Ports

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

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

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

Anmeldedaten und Abonnements

AWS

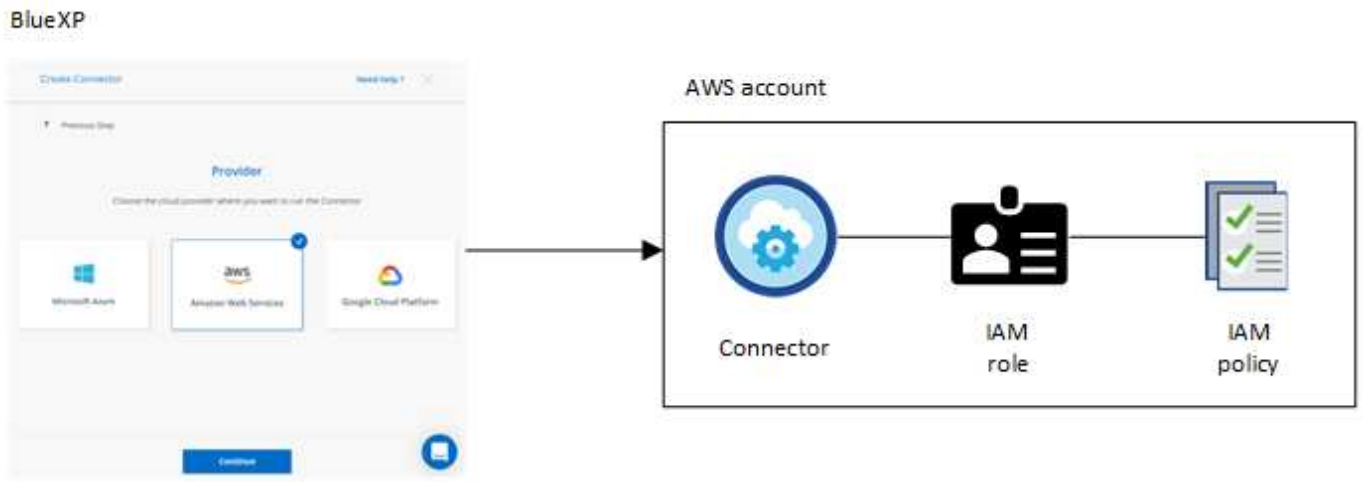
Weitere Informationen zu AWS Zugangsdaten und Berechtigungen

Informieren Sie sich, wie BlueXP für Sie AWS Zugangsdaten verwendet, um Aktionen durchzuführen und wie diese Zugangsdaten mit Marketplace-Abonnements verknüpft sind. Diese Details zu verstehen, ist hilfreich, wenn Sie die Anmeldedaten für einen oder mehrere AWS-Konten in BlueXP managen. So könnte es beispielsweise interessant sein, wann Sie BlueXP um zusätzliche AWS Zugangsdaten erweitern können.

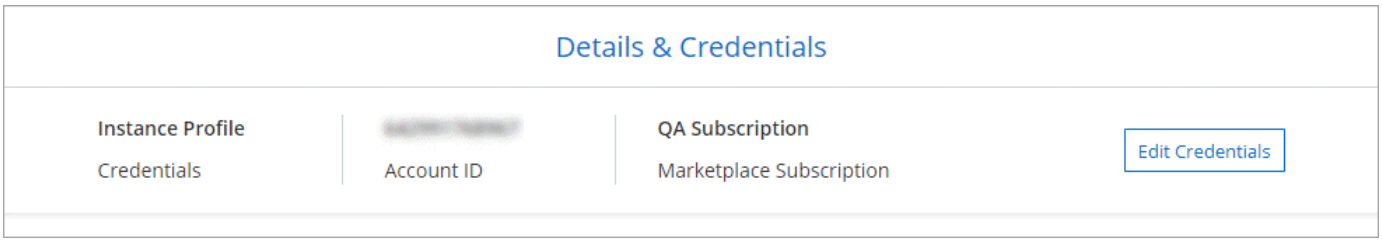
Erste AWS Zugangsdaten

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".



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



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

Zusätzliche AWS Zugangsdaten

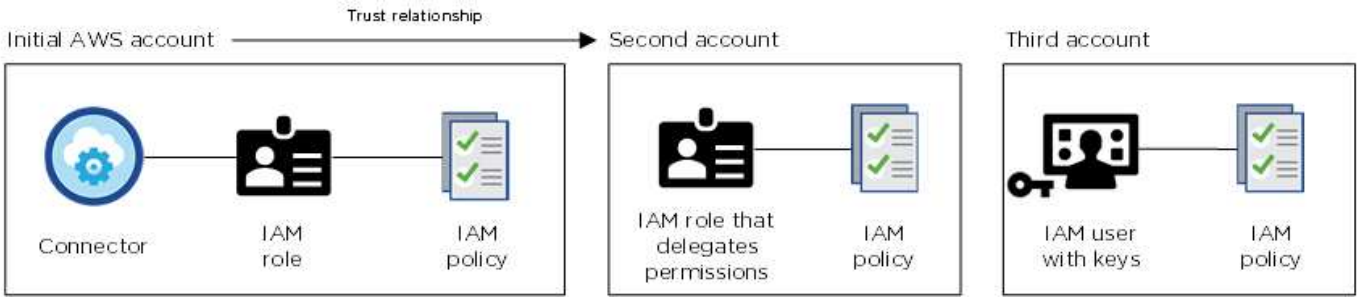
Es gibt zwei Möglichkeiten, zusätzliche AWS-Anmeldedaten hinzuzufügen:

- Sie können einem vorhandenen Connector AWS-Anmeldedaten hinzufügen
- Sie können AWS Zugangsdaten direkt in BlueXP hinzufügen

Weitere Informationen finden Sie in den folgenden Abschnitten.

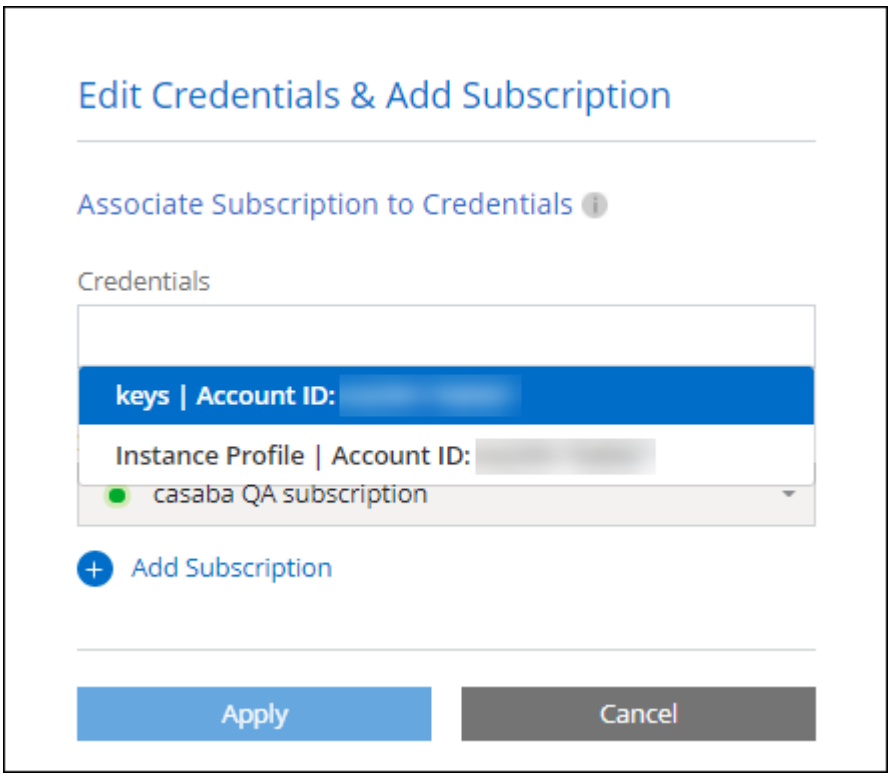
Fügen Sie AWS Zugangsdaten zu einem vorhandenen Connector hinzu

Wenn Sie BlueXP mit zusätzlichen AWS-Konten nutzen möchten, können Sie entweder 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:



Sie würden dann die Account-Anmeldedaten zu BlueXP hinzufügen, indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

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



"Informieren Sie sich, wie Sie einem vorhandenen Connector AWS-Anmeldedaten hinzufügen."

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.

- "Informieren Sie sich, wie Sie BlueXP für Amazon FSX for ONTAP mit AWS Zugangsdaten ergänzen"
- "Erfahren Sie, wie Sie zur Erstellung eines Connectors AWS Zugangsdaten zu BlueXP hinzufügen"

Anmeldedaten und Abonnements für den Marktplatz

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

"Verbinden Sie ein AWS Abonnement".

Beachten Sie Folgendes zu AWS Zugangsdaten und Marketplace-Abonnements:

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

Häufig gestellte Fragen

Die folgenden Fragen beziehen sich auf Anmeldeinformationen und Abonnements.

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Wie oben in den Abschnitten beschrieben, können Sie mit BlueXP Ihre AWS Zugangsdaten auf verschiedene Weise bereitstellen: Eine mit der Connector-Instanz verbundene IAM-Rolle, indem Sie eine IAM-Rolle in einem vertrauenswürdigen Konto übernehmen oder AWS Zugriffsschlüssel bereitstellen.

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.

Kann ich das AWS Marketplace Abonnement für Cloud Volumes ONTAP Arbeitsumgebungen ändern?

Ja, können Sie. Wenn Sie das AWS Marketplace Abonnement ändern, das mit einer Reihe von Zugangsdaten verknüpft ist, wird das neue Abonnement für alle vorhandenen und neuen Cloud Volumes ONTAP Arbeitsumgebungen in Rechnung gestellt.

"Verbinden Sie ein AWS Abonnement".

Kann ich mehrere AWS Zugangsdaten mit jeweils unterschiedlichen Marketplace-Abonnements hinzufügen?

Alle AWS Zugangsdaten, die demselben AWS Konto angehören, werden demselben AWS Marketplace Abonnement zugeordnet.

Wenn Sie mehrere AWS-Anmeldeinformationen haben, die zu verschiedenen AWS-Konten gehören, können diese Anmeldeinformationen mit demselben AWS Marketplace Abonnement oder verschiedenen Abonnements verknüpft werden.

Kann ich vorhandene Cloud Volumes ONTAP Arbeitsumgebungen auf ein anderes AWS Konto verschieben?

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

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

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

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.

Sie können bei lokalen Implementierungen keine IAM-Rolle für das BlueXP System einrichten, aber mithilfe von AWS Zugriffsschlüsseln bieten Sie Berechtigungen.

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

- Standardmodus
  - "Richten Sie Berechtigungen für eine AWS Marketplace-Implementierung ein"
  - "Richten Sie Berechtigungen für On-Premises-Implementierungen ein"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

Management von AWS Zugangsdaten und Marketplace-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 Marketplace-Abonnements managen, können Sie jede davon auf der Seite Anmeldedaten verschiedenen AWS-Anmeldedaten 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. 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. 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.

Fügen Sie zusätzliche Anmeldedaten zu einem Connector hinzu

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

Wenn Sie gerade erst mit BlueXP starten, "So nutzt BlueXP AWS Zugangsdaten und Berechtigungen".

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

- indem Sie eine IAM-Rolle in einem anderen Konto übernehmen
- Erteilen Sie Berechtigungen durch die Bereitstellung von AWS Schlüsseln

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.

Wenn der Connector vor Ort installiert ist, können Sie diese Authentifizierungsmethode nicht verwenden. AWS-Schlüssel müssen verwendet werden.

Schritte

1. Rufen Sie die IAM-Konsole im Zielkonto auf, in dem Sie dem Connector Berechtigungen erteilen möchten.
2. Wählen Sie unter Access Management die Option **Rollen > Rolle erstellen** aus, 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.

Ergebnis

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.

Sie müssen diese Authentifizierungsmethode verwenden, wenn der Connector vor Ort installiert ist. Sie können keine IAM-Rolle verwenden.

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"

Ergebnis

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.

Bevor Sie beginnen

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

Schritte

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

3. Wählen Sie auf der Seite **Account Credentials** die Option **Add Credentials** aus 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.

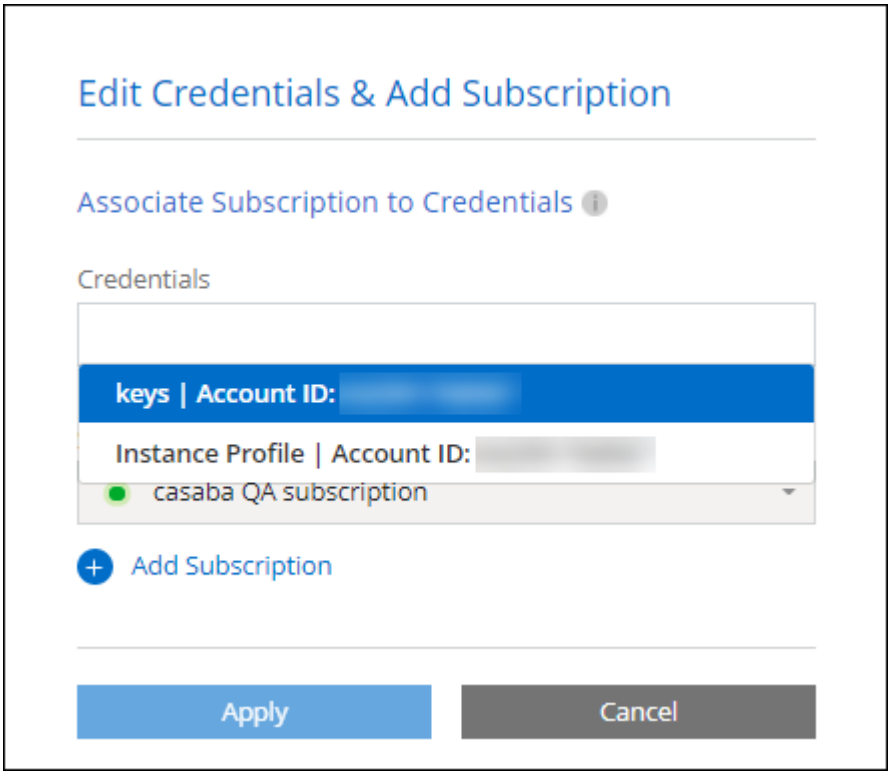
c. **Marketplace-Abonnement**: Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

   Damit die BlueXP Services zu einem Stundensatz (PAYGO) oder mit einem Jahresvertrag bezahlt werden können, müssen die AWS Zugangsdaten mit einem AWS Marketplace Abonnement verbunden sein.

d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

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, damit die BlueXP SaaS-Schicht die Rolle übernimmt.

Schritte

1. Wechseln Sie im Zielkonto zur IAM-Konsole.
2. Wählen Sie unter Access Management die Option **Rollen > Rolle erstellen** aus, 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.

Ergebnis

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.

Bevor Sie beginnen

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 auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.

2. Wählen Sie auf der Seite **Account Credentials** die Option **Add Credentials** aus 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 Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

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

Zugangsdaten zu BlueXP für Amazon FSX for ONTAP hinzufügen

Weitere Informationen finden Sie im "BlueXP Dokumentation für Amazon FSX for ONTAP"

AWS Abonnement zuordnen

Nachdem Sie Ihre AWS Zugangsdaten zu BlueXP hinzugefügt haben, können Sie ein AWS Marketplace Abonnement mit diesen Anmeldedaten verknüpfen. Dank des Abonnements können Sie für Cloud Volumes ONTAP zu einem Stundensatz (PAYGO) bezahlen oder einen Jahresvertrag nutzen und andere BlueXP 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 das AWS Marketplace-Abonnement ändern, das mit den AWS Zugangsdaten verknüpft ist.

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

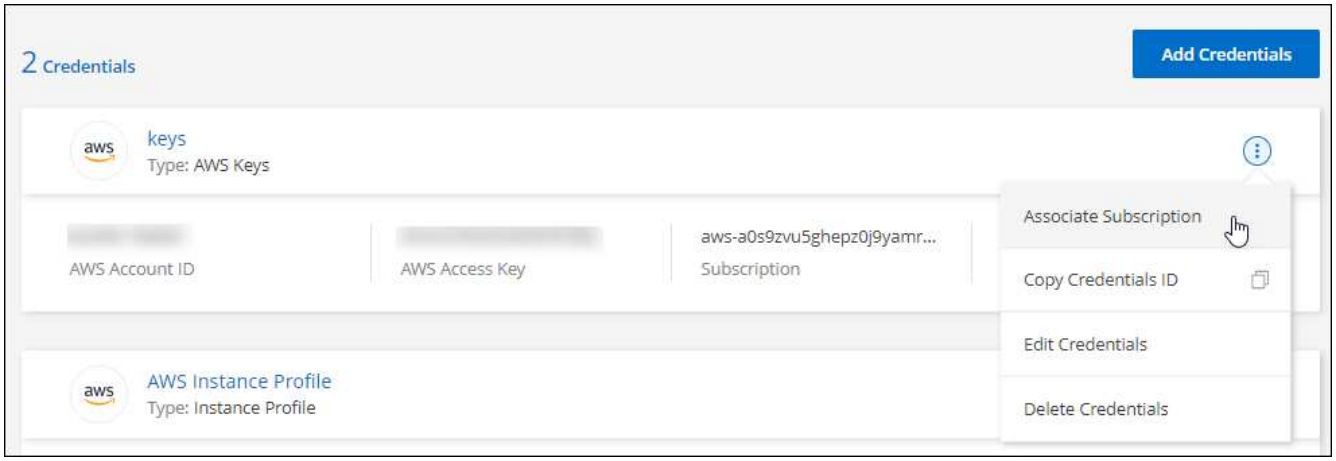
Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie Sie einen Konnektor erstellen".

Schritte

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

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



3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie das Abonnement aus der Down-Liste aus und wählen **Associate** aus.
4. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Weiter** und befolgen Sie die Schritte im AWS Marketplace:

   a. Wählen Sie **Kaufoptionen anzeigen**.

   b. Wählen Sie **Abonnieren**.

   c. Wählen Sie **Konto einrichten**.

      Sie werden auf die BlueXP-Website umgeleitet.

   d. Auf der Seite **Subscription Assignment**:

      - Wählen Sie die BlueXP Konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.

- Wählen Sie im Feld **vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

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

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

- Wählen Sie **Speichern**.

  Im folgenden Video werden die Schritte zum Abonnieren über AWS Marketplace gezeigt:

Abonnieren Sie BlueXP über den AWS Marketplace

Verknüpfen Sie ein bestehendes Abonnement mit Ihrem Konto

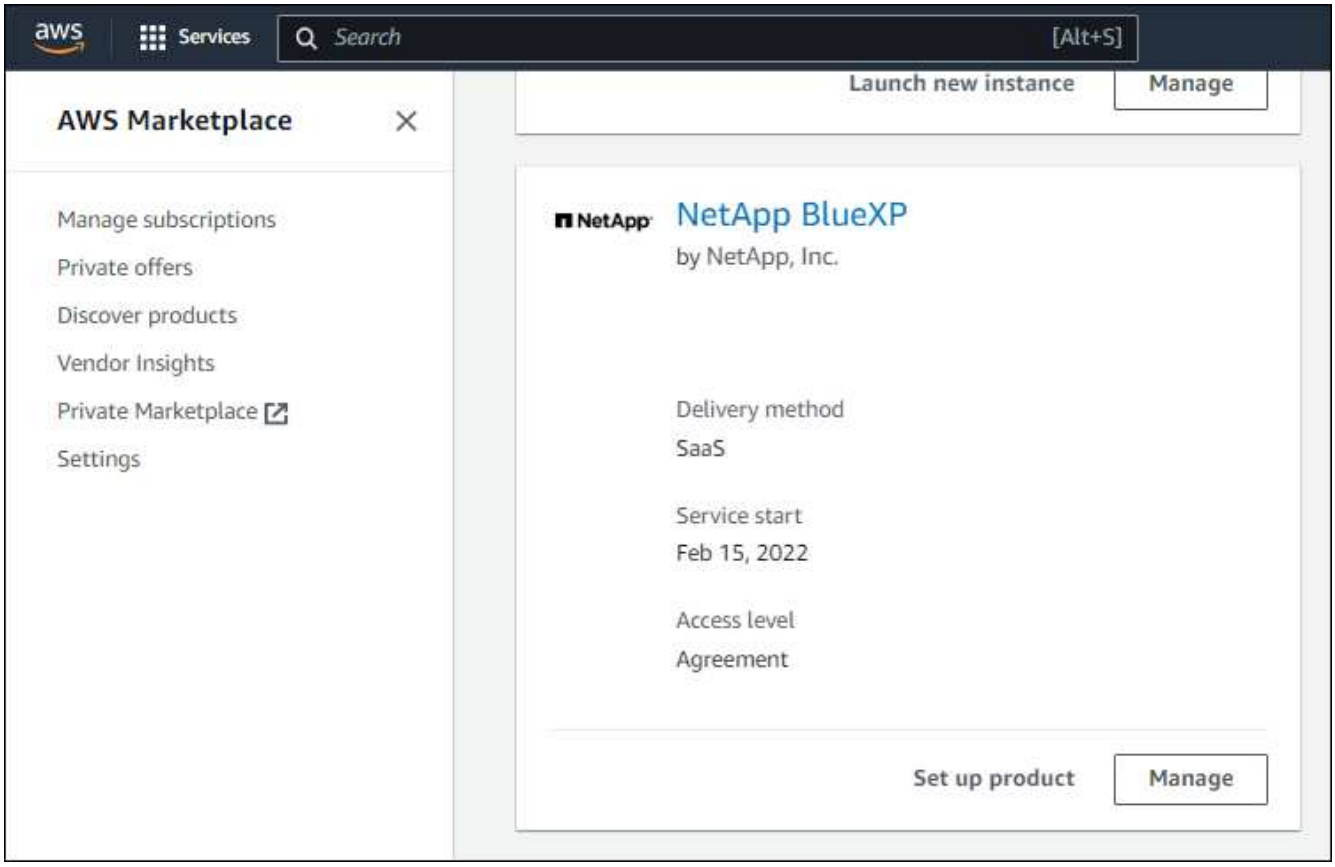
Wenn Sie BlueXP über den AWS Marketplace abonnieren, besteht der letzte Schritt darin, das Abonnement mit Ihren BlueXP Konten auf der BlueXP Website zu verknüpfen. Wenn Sie diesen Schritt nicht abgeschlossen haben, können Sie das Abonnement nicht mit Ihrem BlueXP Konto verwenden.

Befolgen Sie die nachstehenden Schritte, wenn Sie BlueXP über AWS Marketplace abonniert haben, aber Sie haben den Schritt verpasst, das Abonnement mit Ihrem Konto zu verknüpfen.

Schritte

1. Bestätigen Sie über das Digital Wallet von BlueXP, dass Sie Ihr Abonnement nicht mit Ihrem BlueXP Konto verknüpft haben.
   a. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
   b. Wählen Sie **Abonnements**.
   c. Vergewissern Sie sich, dass Ihr BlueXP Abonnement nicht angezeigt wird.

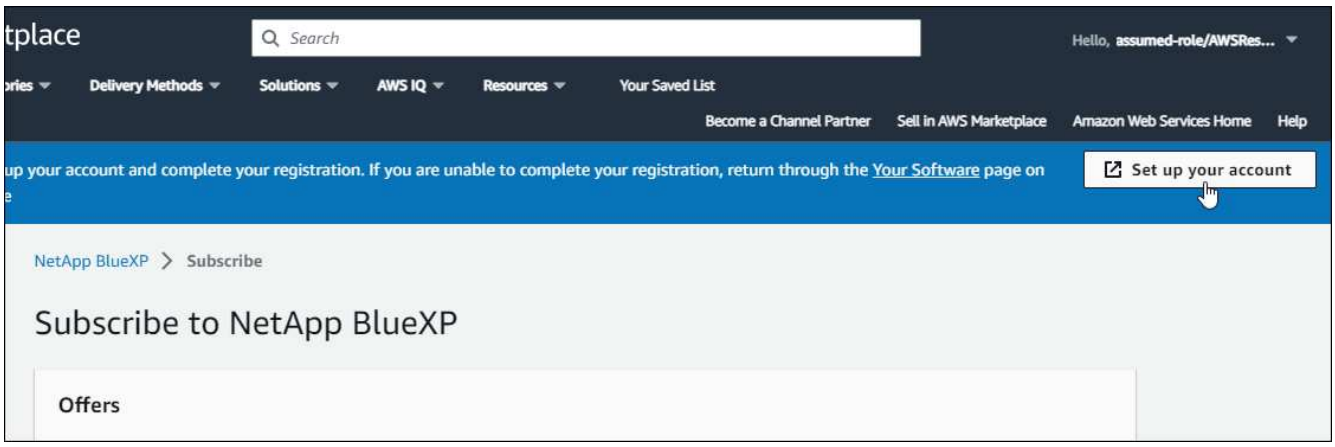
      Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen. Wenn Ihr Abonnement nicht angezeigt wird, fahren Sie mit den folgenden Schritten fort.
2. Melden Sie sich an der AWS-Konsole an, und navigieren Sie zu **AWS Marketplace Subscriptions**.
3. Zum NetApp BlueXP Abonnement



4. Wählen Sie **Produkt einrichten**.

   Die Abonnementseite sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

5. Wählen Sie **Konto einrichten**.



   Die Seite **Subscription Assignment** auf netapp.com sollte in einem neuen Browser-Tab oder -Fenster geladen werden.

   Beachten Sie, dass Sie möglicherweise zuerst zur Anmeldung bei BlueXP aufgefordert werden.

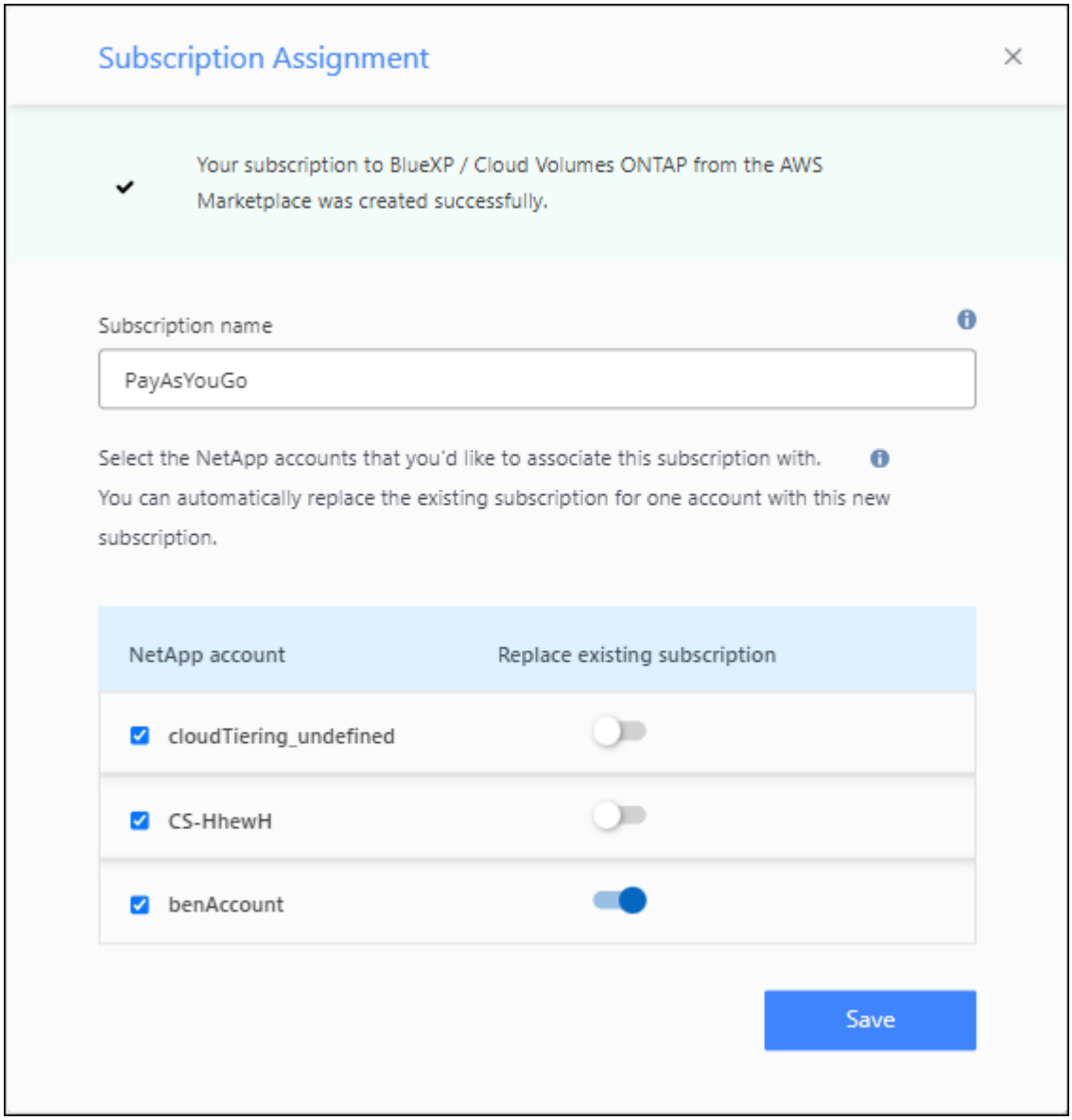
6. Auf der Seite **Subscription Assignment**:

   - Wählen Sie die BlueXP Konten aus, mit denen Sie dieses Abonnement verknüpfen möchten.

- Wählen Sie im Feld **vorhandenes Abonnement ersetzen** aus, ob Sie das vorhandene Abonnement für ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

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

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

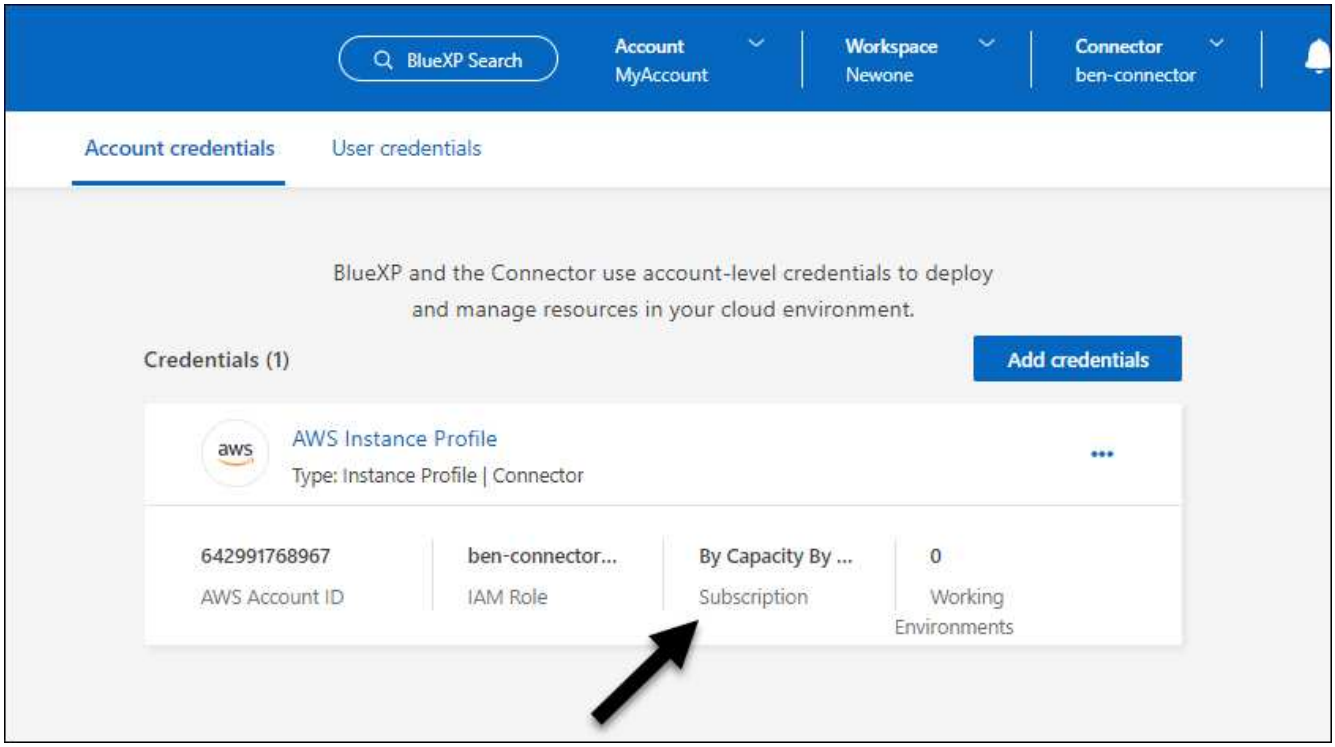


7. Über das Digital Wallet von BlueXP können Sie sich bestätigen, dass das Abonnement mit Ihrem BlueXP Konto verknüpft ist.
   a. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
   b. Wählen Sie **Abonnements**.
   c. Vergewissern Sie sich, dass Ihr BlueXP Abonnement angezeigt wird.
8. Vergewissern Sie sich, dass das Abonnement mit Ihren AWS-Anmeldedaten verknüpft ist.

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

b. Überprüfen Sie auf der Seite **Account Credentials**, ob das Abonnement mit Ihren AWS-Anmeldedaten verknüpft ist.

   Hier ein Beispiel



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

Anmeldeinformationen löschen

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

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

Schritte

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

Azure

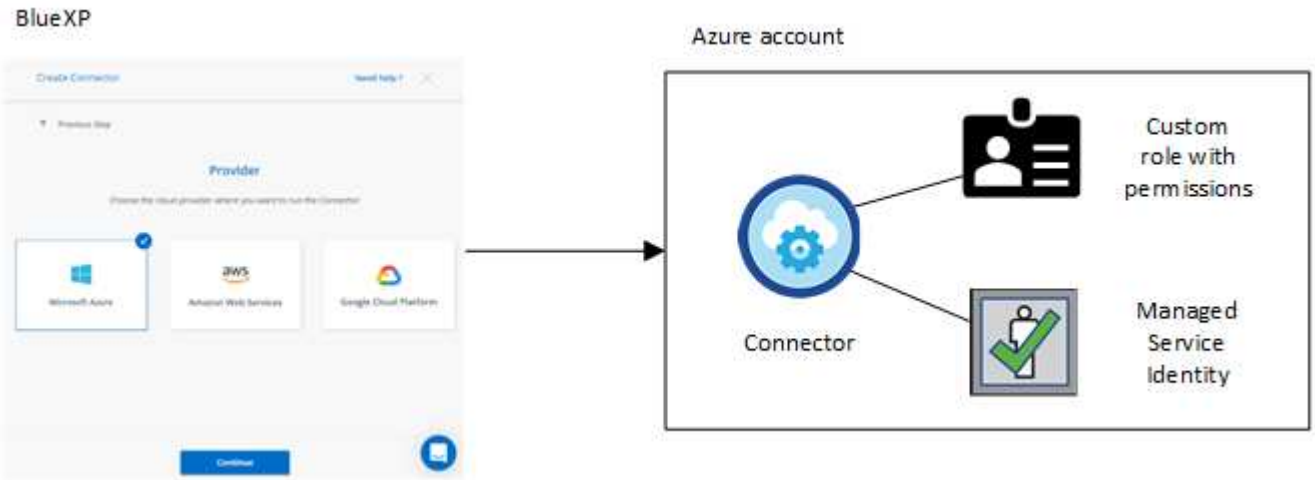
Informationen zu Azure Zugangsdaten und Berechtigungen

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

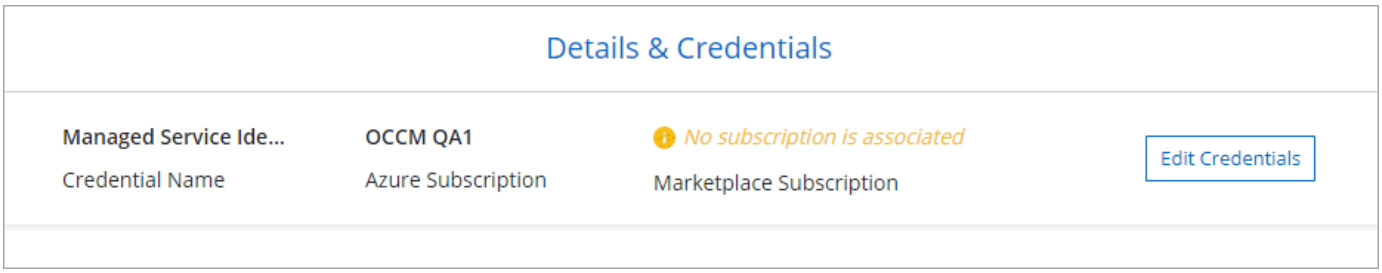
Erste Azure Zugangsdaten

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

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



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



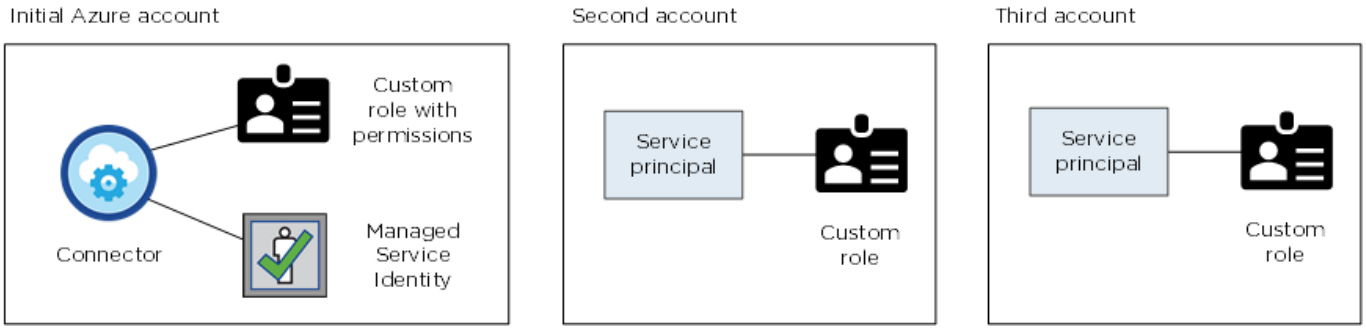
Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

Zusätzliche Azure-Abonnements für eine gemanagte Identität

Die der Konnektor-VM zugewiesene, vom System zugewiesene verwaltete Identität ist mit dem Abonnement verknüpft, in dem Sie den Connector gestartet haben. Wenn Sie ein anderes Azure Abonnement auswählen möchten, müssen Sie es ausführen "Verknüpfen Sie die verwaltete Identität mit diesen Abonnements".

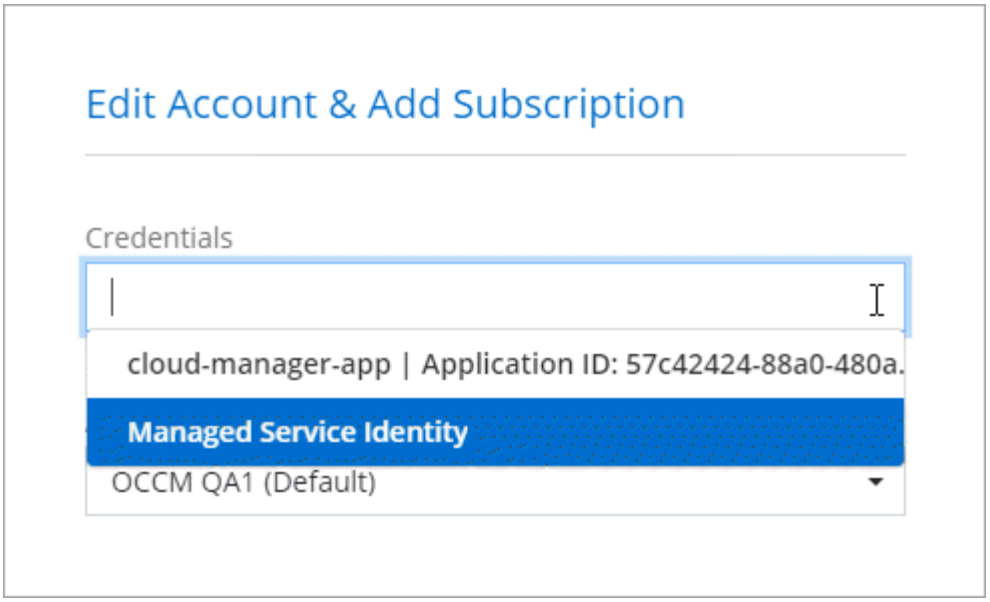
Zusätzliche Azure Zugangsdaten

Wenn Sie unterschiedliche Azure-Anmeldedaten für BlueXP verwenden möchten, müssen Sie die erforderlichen Berechtigungen bis erteilen "Erstellen und Einrichten eines Dienstprincipals in Microsoft Entra ID" Für jedes Azure Konto. Das folgende Bild zeigt zwei zusätzliche Konten, die jeweils mit einer Dienstprinzipal- und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



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

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



Anmeldedaten und Abonnements für den Marktplatz

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

"Lesen Sie, wie Sie ein Azure-Abonnement zuordnen".

Beachten Sie Folgendes zu Azure Zugangsdaten und Marketplace-Abonnements:

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

Häufig gestellte Fragen

Die folgende Frage bezieht sich auf Anmeldeinformationen und Abonnements.

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

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

"Lesen Sie, wie Sie ein Azure-Abonnement zuordnen".

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

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

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

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

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

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

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

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

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

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

- Standardmodus
  - "Richten Sie Berechtigungen für eine Azure Marketplace-Implementierung ein"
  - "Richten Sie Berechtigungen für On-Premises-Implementierungen ein"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

Azure Zugangsdaten und Marketplace-Abonnements für BlueXP managen

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

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

Überblick

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

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

Zuordnen zusätzlicher Azure-Abonnements zu einer gemanagten Identität

Mit BlueXP können Sie die Azure Zugangsdaten und das Azure Abonnement auswählen, in dem Sie Cloud Volumes ONTAP bereitstellen möchten. Sie können kein anderes Azure-Abonnement für das verwaltete

Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" Mit diesen Abonnements.

Über diese Aufgabe

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

Schritte

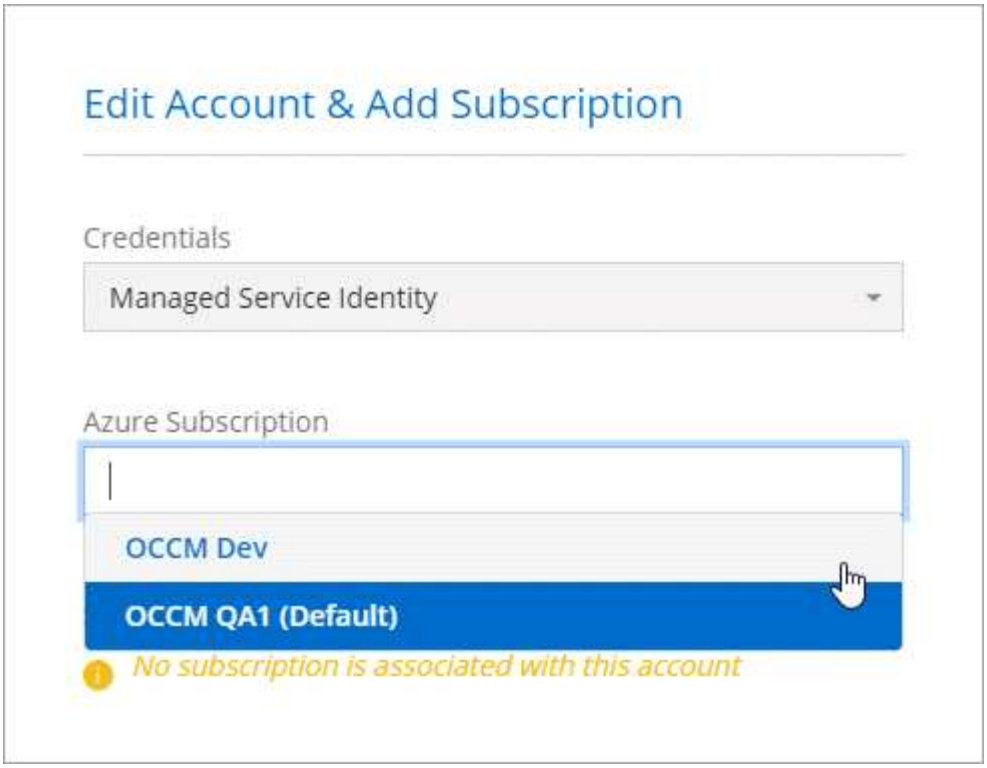
1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Wählen Sie **Access Control (IAM)**.
   a. Wählen Sie **Hinzufügen** > **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **BlueXP Operator** aus.

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

      - Weisen Sie einer **virtuellen Maschine** Zugriff zu.
      - Wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde.
      - Wählen Sie die virtuelle Verbindungsmaschine aus.
      - Wählen Sie **Speichern**.
4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

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



Zusätzliche Azure Zugangsdaten zu BlueXP hinzufügen

Wenn Sie einen Connector von BlueXP bereitstellen, aktiviert BlueXP eine vom System zugewiesene verwaltete Identität auf der virtuellen Maschine, die über die erforderlichen Berechtigungen verfügt. BlueXP wählt diese Azure-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".

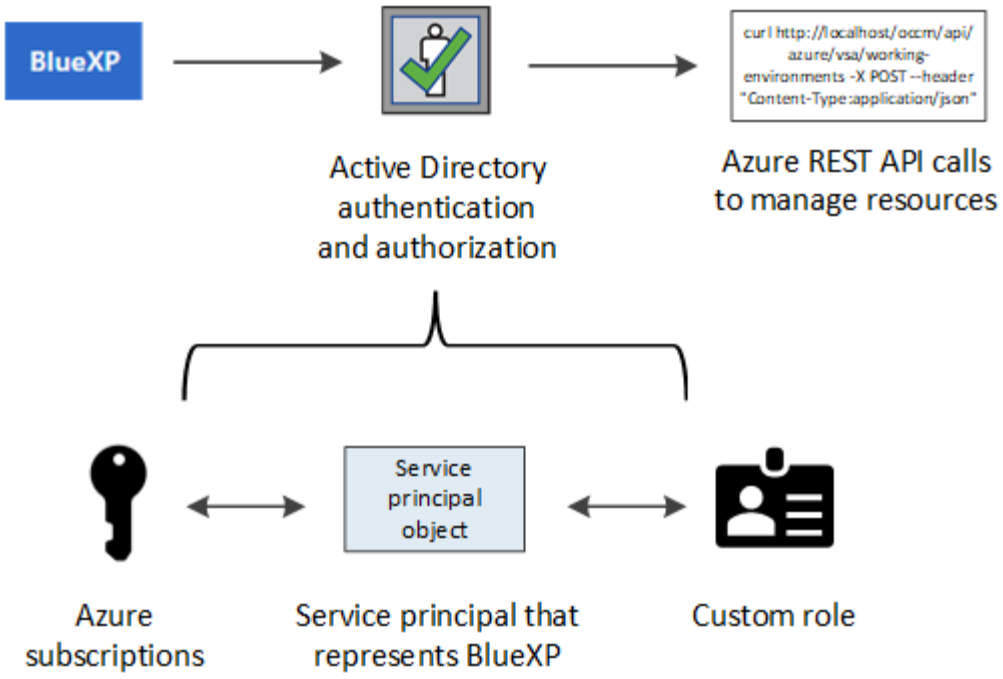
Wenn Sie Cloud Volumes ONTAP mit *different* Azure-Anmeldeinformationen bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure-Konto einen Dienstprinzipal in der Microsoft Entra-ID erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zu BlueXP hinzufügen.

Erteilen Sie Azure Berechtigungen mithilfe eines Service-Prinzipals

Für Aktionen in Azure benötigt BlueXP Berechtigungen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie in der Microsoft Entra-ID einen Service-Principal erstellen und einrichten und die für BlueXP erforderlichen Azure-Zugangsdaten erhalten.

Über diese Aufgabe

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



Schritte

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

Erstellen Sie eine Microsoft Entra-Anwendung

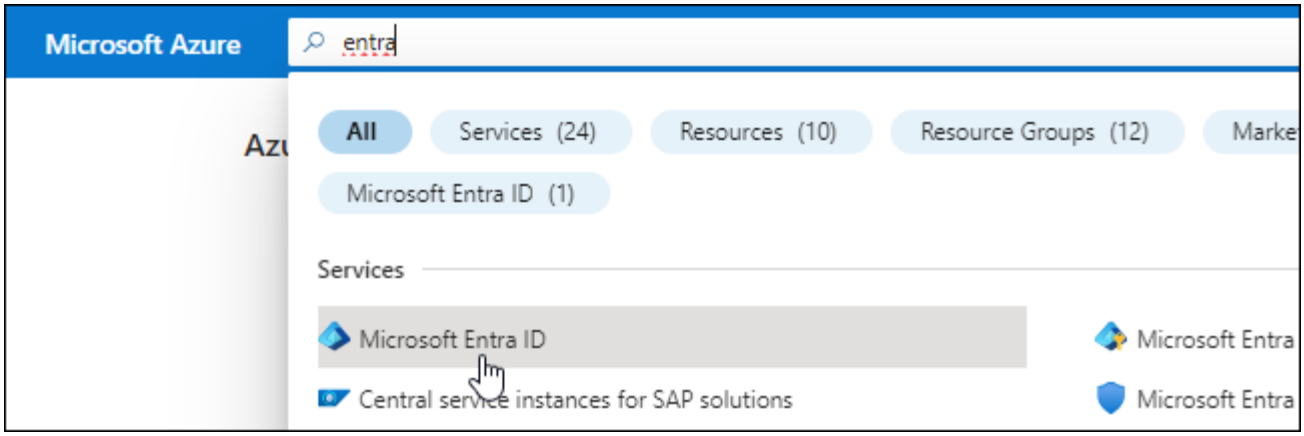
Erstellen Sie ein Microsoft Entra-Applikations- und Serviceprinzip, das BlueXP für die rollenbasierte Zugriffssteuerung verwenden kann.

Schritte

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

   Weitere Informationen finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen"

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



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

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

Ergebnis

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

Anwendung einer Rolle zuweisen

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

Schritte

1. Erstellen einer benutzerdefinierten Rolle:

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

   a. Kopieren Sie den Inhalt des "Benutzerdefinierte Rollenberechtigungen für den Konnektor" Und speichern Sie sie in einer JSON-Datei.

   b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

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

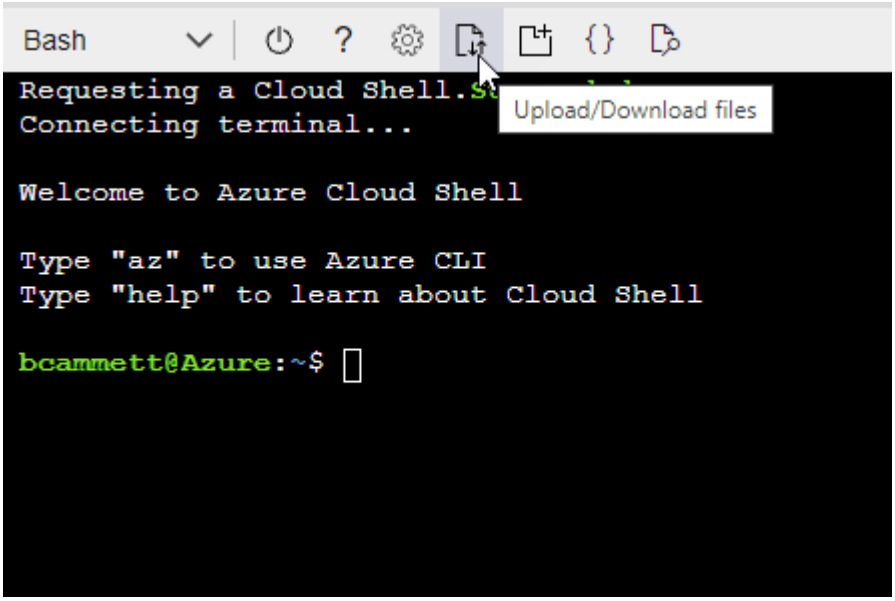
      Beispiel

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

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

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

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



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

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

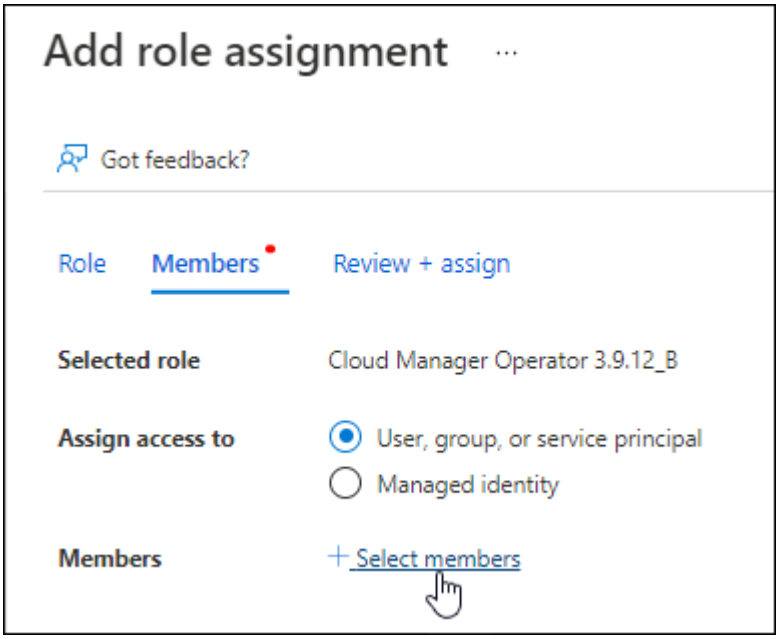
   Sie sollten nun eine benutzerdefinierte Rolle namens BlueXP Operator haben, die Sie der virtuellen Connector-Maschine zuweisen können.

2. Applikation der Rolle zuweisen:

   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

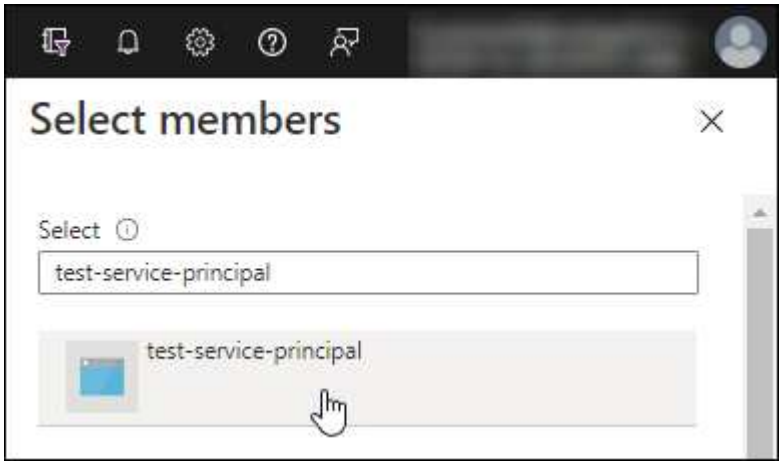
      - **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.

- Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ein Beispiel:



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

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

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

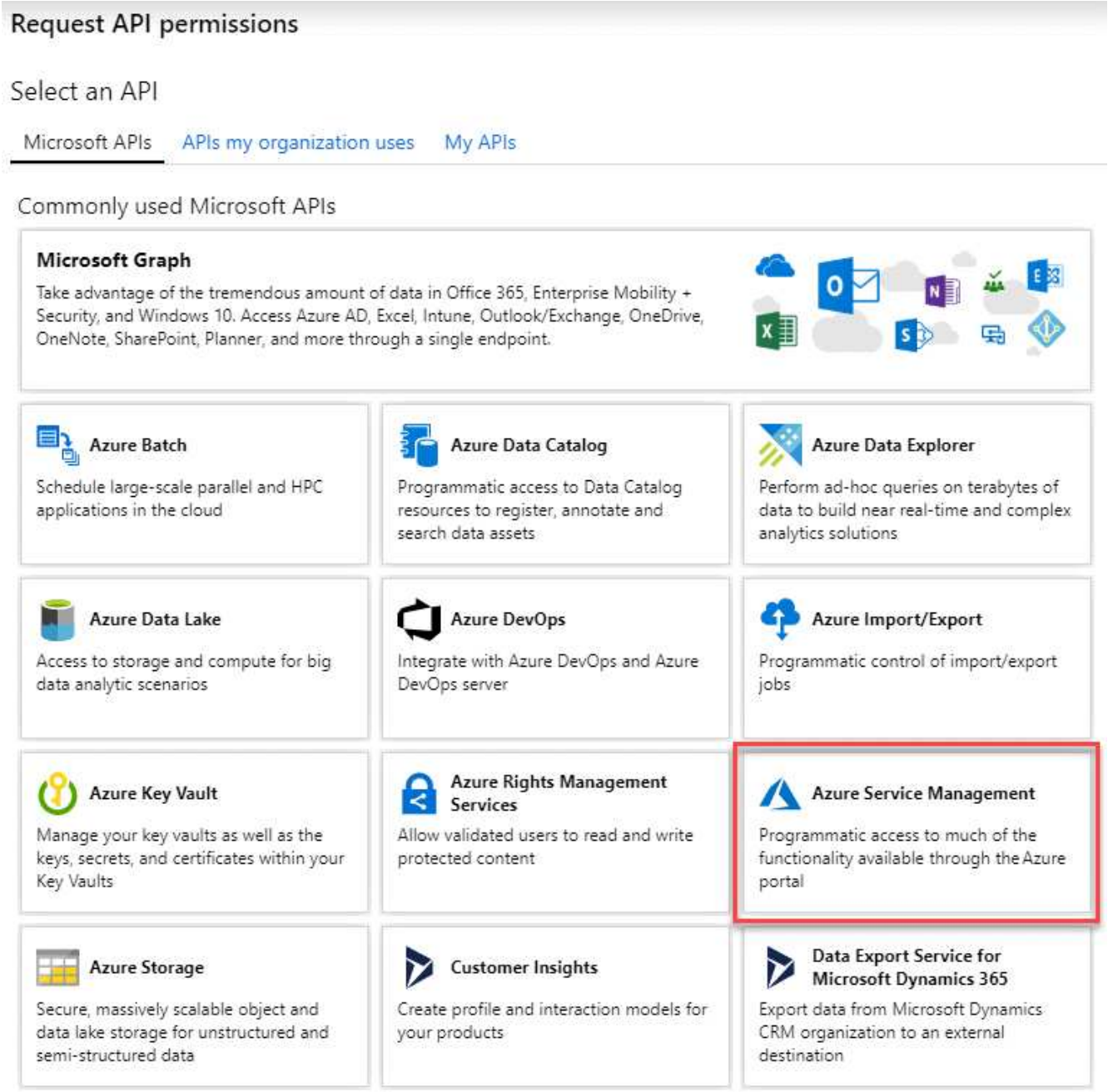
Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Prinzipal an jedes dieser Subscriptions binden. Mit BlueXP können Sie das Abonnement auswählen, das Sie bei der Bereitstellung von Cloud Volumes ONTAP verwenden möchten.

Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

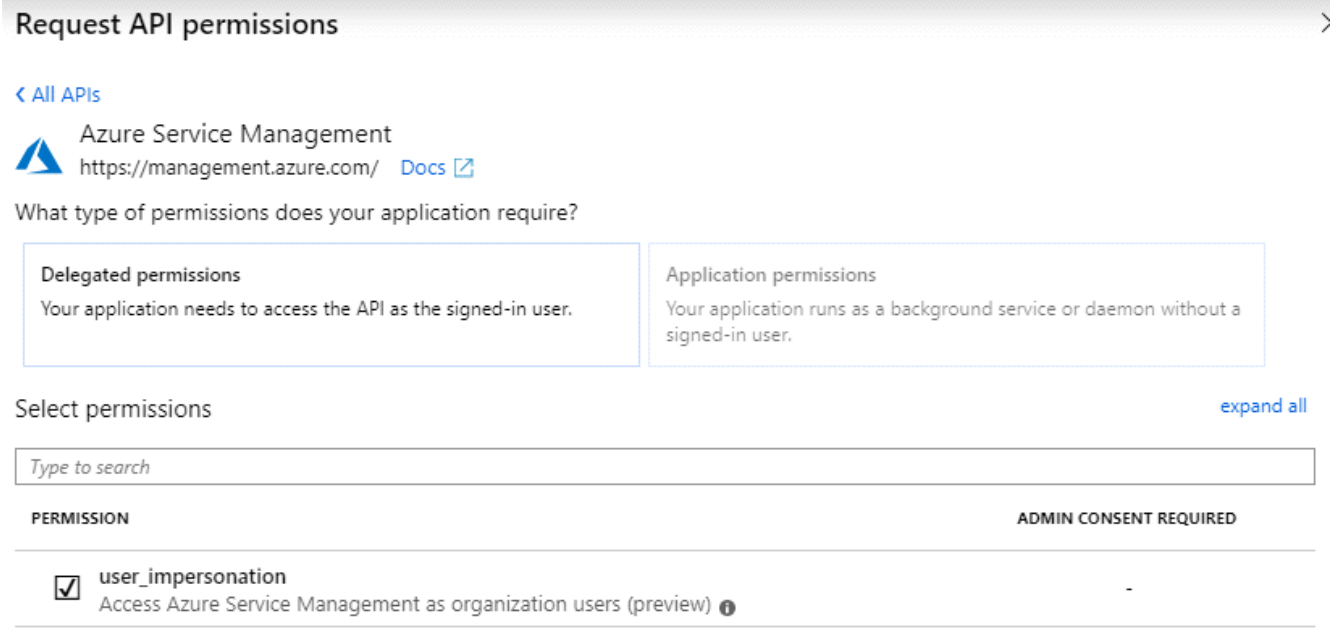
Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

Schritte

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



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

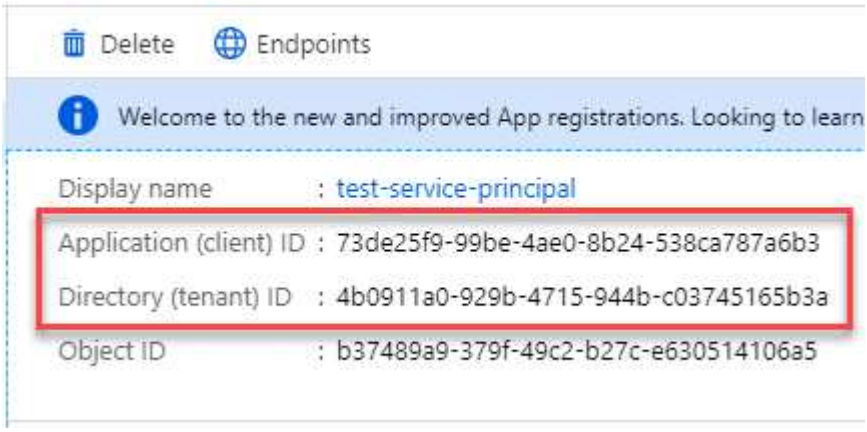


Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab

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

Schritte

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



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

Erstellen Sie einen Clientschlüssel

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

Schritte

1. Öffnen Sie den Dienst **Microsoft Entra ID**.
2. Wählen Sie **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Wählen Sie **Zertifikate & Geheimnisse > Neues Kundengeheimnis**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Wählen Sie **Hinzufügen**.
6. Kopieren Sie den Wert des Clientgeheimnisses.

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

Ergebnis

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

Zugangsdaten zu BlueXP hinzufügen

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

Bevor Sie beginnen

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

Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie Sie einen Konnektor erstellen".

Schritte

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

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

a. **Anmeldeort**: Wählen Sie **Microsoft Azure > Connector**.

b. **Credentials definieren**: Geben Sie Informationen über den Microsoft Entra-Dienst-Prinzipal ein, der die erforderlichen Berechtigungen gewährt:

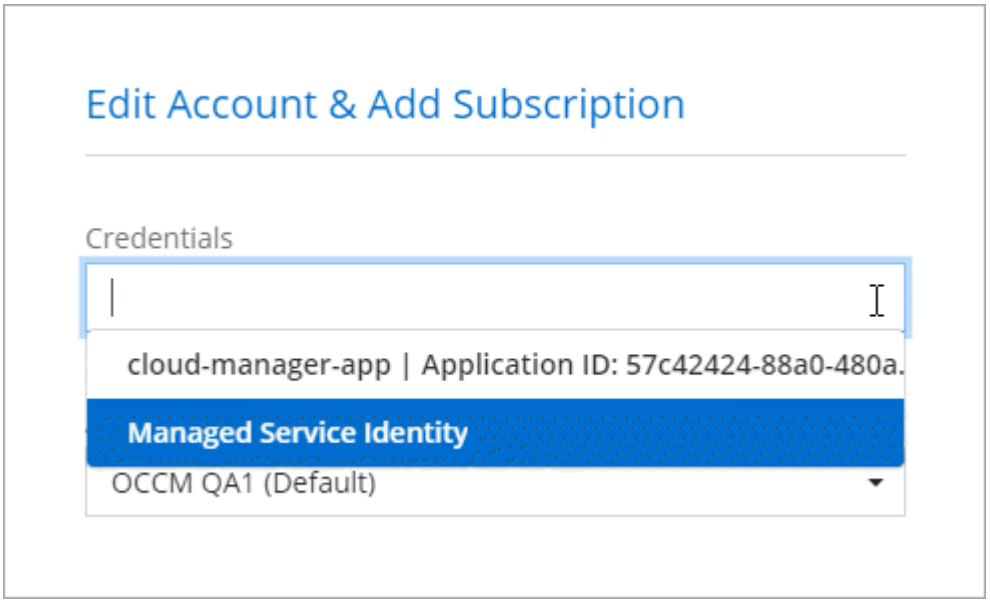
   - Anwendungs-ID (Client)
   - ID des Verzeichnisses (Mandant)
   - Client-Schlüssel

c. **Marketplace-Abonnement**: Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

Auf der Seite Details und Anmeldeinformationen können Sie nun zu verschiedenen Anmeldeinformationen wechseln "Beim Erstellen einer neuen Arbeitsumgebung"



Vorhandene Anmeldedaten verwalten

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

Azure Marketplace Abonnement mit Anmeldedaten verknüpfen

Nachdem Sie Ihre Azure Zugangsdaten zu BlueXP hinzugefügt haben, können Sie diesen Anmeldedaten ein Azure Marketplace Abonnement zuordnen. Mit dem Abonnement können Sie ein Pay-as-you-go Cloud Volumes ONTAP System erstellen und andere BlueXP Services nutzen.

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

- Sie haben ein Abonnement nicht zugeordnet, wenn Sie die Anmeldeinformationen zu BlueXP hinzugefügt haben.
- Sie möchten das Abonnement für Azure Marketplace ändern, das mit den Azure-Anmeldedaten verknüpft ist.

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

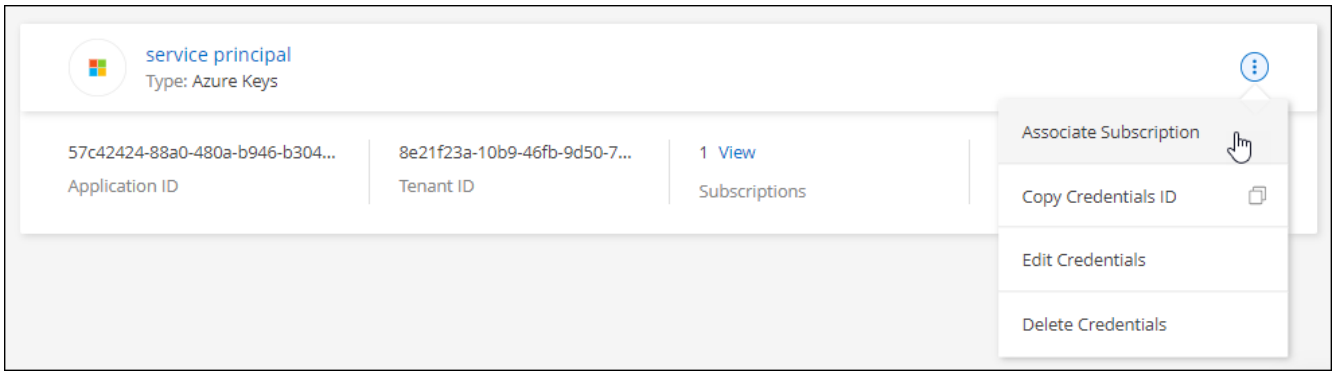
Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

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

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



3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie das Abonnement aus der Down-Liste aus und wählen **Associate** aus.
4. Um die Anmeldeinformationen einem neuen Abonnement zuzuordnen, wählen Sie **Abonnement hinzufügen > Weiter** und befolgen Sie die Schritte im Azure Marketplace:

   a. Melden Sie sich bei Ihrem Azure-Konto an, wenn Sie dazu aufgefordert werden.

   b. Wählen Sie **Abonnieren**.

   c. Füllen Sie das Formular aus und wählen Sie **Abonnieren**.

   d. Wählen Sie nach Abschluss des Abonnements **Konto jetzt konfigurieren** aus.

      Sie werden auf die BlueXP-Website umgeleitet.

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

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

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

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

Schritte wiederholen.

- Wählen Sie **Speichern**.

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

Abonnieren Sie BlueXP über den Azure Marketplace

Anmeldedaten bearbeiten

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

Schritte

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

Anmeldeinformationen löschen

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

Schritte

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

Google Cloud

Mehr über Google Cloud-Projekte und -Berechtigungen erfahren

Erfahren Sie, wie BlueXP für Sie Aktionen mit Google Cloud Credentials durchführt und diese Zugangsdaten mit Marketplace-Abonnements verknüpft. Diese Details zu verstehen, kann hilfreich sein, wenn Sie die Anmeldeinformationen für ein oder mehrere Google Cloud-Projekte verwalten. Vielleicht möchten Sie mehr über das Servicekonto erfahren, das mit der Connector-VM verbunden ist.

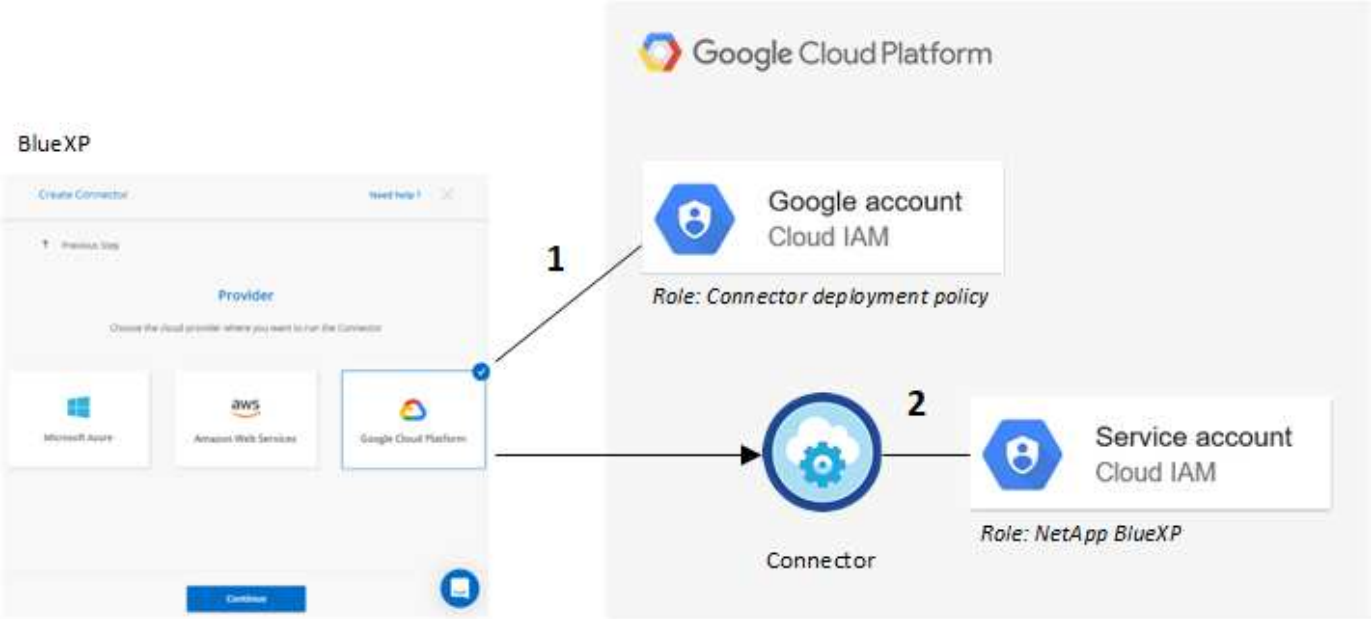
Projekt und Berechtigungen für BlueXP

Bevor Sie BlueXP zum Managen von Ressourcen in Ihrem Google Cloud-Projekt verwenden können, müssen Sie zunächst einen Connector implementieren. 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 Berechtigungen über das Servicekonto, um Cloud Volumes ONTAP Systeme zu erstellen und zu managen, Backups mit BlueXP Backup und Recovery zu managen usw. Berechtigungen werden durch Hinzufügen einer benutzerdefinierten Rolle an das Servicekonto bereitgestellt.

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



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

- "Richten Sie Google Cloud-Berechtigungen für den Standardmodus ein"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

Anmeldedaten und Abonnements für den Marktplatz

Wenn Sie einen Connector in Google Cloud implementieren, erstellt BlueXP im Projekt, in dem sich der Connector befindet, einen StandardSatz an Anmeldeinformationen für das Google Cloud Servicekonto. Diese Anmeldedaten müssen mit einem Google Cloud Marketplace Abonnement verbunden sein, sodass Sie für Cloud Volumes ONTAP einen Stundensatz (PAYGO) zahlen und andere BlueXP Services nutzen können.

"Erfahren Sie, wie Sie ein Google Cloud Marketplace Abonnement verknüpfen".

Beachten Sie Folgendes über Google Cloud-Anmeldedaten und Marketplace-Abonnements:

- Einem Connector kann nur ein Satz Google Cloud-Anmeldedaten zugeordnet werden
- Sie können den Anmeldedaten nur ein Google Cloud Marketplace-Abonnement zuweisen
- Sie können ein bestehendes Marketplace-Abonnement durch ein neues Abonnement ersetzen

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 das Service-Konto einrichten"
- "Erfahren Sie, wie Sie Cloud Volumes ONTAP in Google Cloud implementieren und ein Projekt auswählen"

Managen Sie Google Cloud-Anmeldedaten und -Abonnements für BlueXP

Sie können die Google Cloud-Anmeldedaten verwalten, die mit der VM-Instanz Connector verknüpft sind, indem Sie ein Marketplace-Abonnement zuordnen und den Abonnementprozess beheben. Mit beiden Aufgaben stellen Sie sicher, dass Sie Ihr Marketplace-Abonnement verwenden können, um BlueXP Services zu bezahlen.

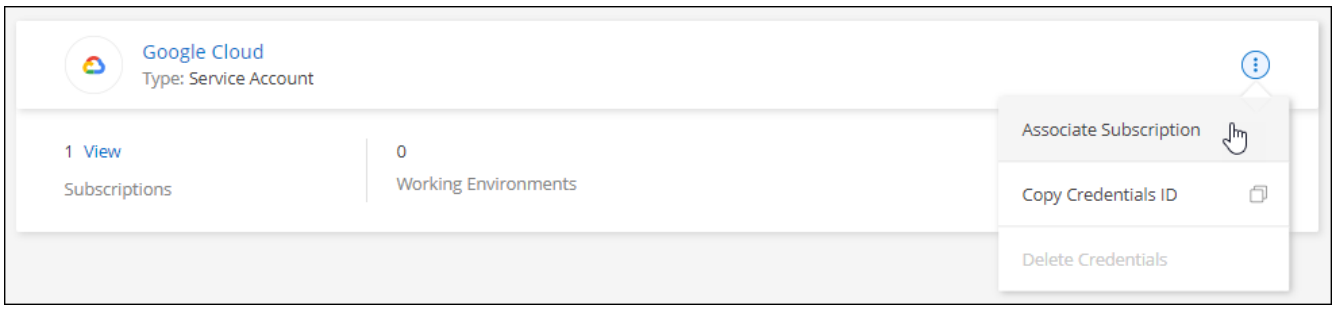
Verbinden Sie ein Marketplace-Abonnement mit Google Cloud-Anmeldedaten

Wenn Sie einen Connector in Google Cloud bereitstellen, erstellt BlueXP einen Standardsatz von Anmeldeinformationen, die der Connector-VM-Instanz zugeordnet sind. Sie können jederzeit das mit diesen Anmeldedaten verbundene Abonnement von Google Cloud Marketplace ändern. Mit dem Abonnement können Sie ein Pay-as-you-go Cloud Volumes ONTAP System erstellen und andere BlueXP Services nutzen.

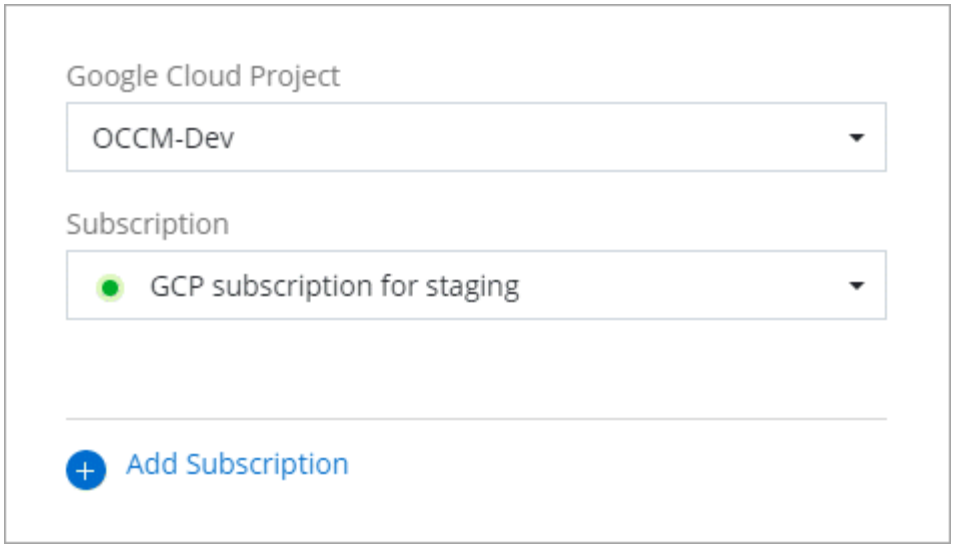
Durch den Austausch des aktuellen Marketplace-Abonnements durch ein neues Abonnement wird das Marketplace-Abonnement für alle bestehenden Cloud Volumes ONTAP Arbeitsumgebungen und alle neuen Arbeitsumgebungen geändert.

Schritte

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



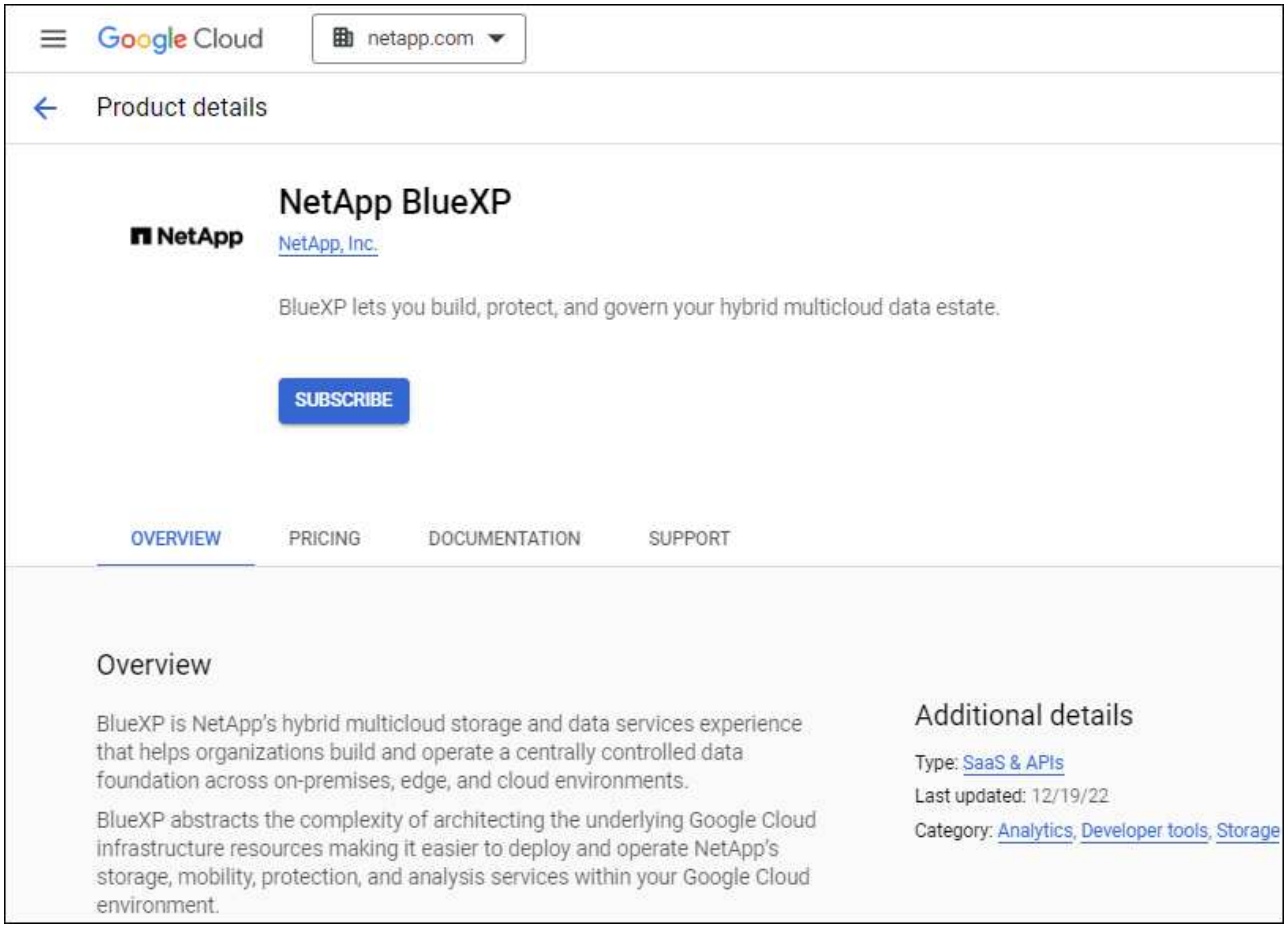
3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, und wählen Sie dann **Associate** aus.



4. Wenn Sie noch kein Abonnement besitzen, wählen Sie **Abonnement hinzufügen > Weiter** und folgen Sie den Schritten im Google Cloud Marketplace.

> 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.

a. 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.



b. Wählen Sie **Abonnieren**.

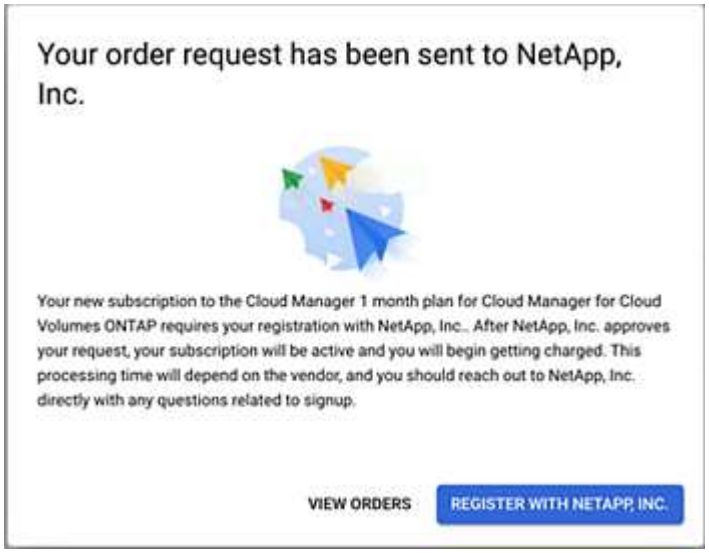
c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

d. Wählen Sie **Abonnieren**.

   Dieser Schritt sendet Ihre Transferanfrage an NetApp.

e. Wählen Sie im Popup-Dialogfeld **Registrierung bei NetApp, Inc.** aus

   Dieser Schritt muss abgeschlossen sein, um das Google Cloud Abonnement mit Ihrem BlueXP Konto zu verknüpfen. Der Vorgang der Verknüpfung eines Abonnements ist erst abgeschlossen, wenn Sie von dieser Seite umgeleitet und dann bei BlueXP angemeldet sind.



f. Führen Sie die Schritte auf der Seite **Subscription Assignment** aus:

   > 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.

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

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

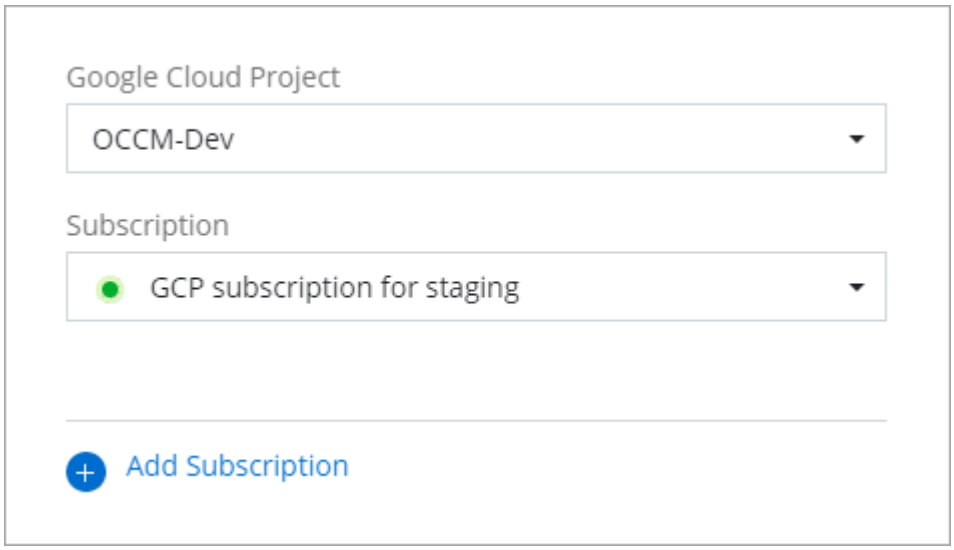
   Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden Schritte wiederholen.

   - Wählen Sie **Speichern**.

     Im folgenden Video sehen Sie, wie Sie sich für den Google Cloud Marketplace anmelden können:

Abonnieren Sie BlueXP über den Google Cloud Marketplace

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

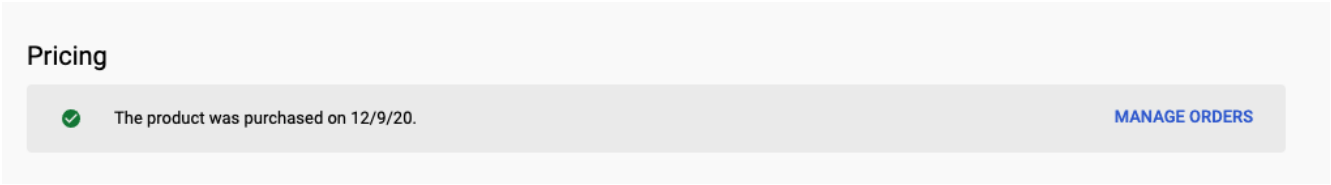


Fehlerbehebung bei der Marketplace-Subscription

Wenn Sie BlueXP über den Google Cloud Marketplace abonnieren, kann es manchmal zu einer Fragmentierung kommen, weil Sie falsche Berechtigungen haben oder versehentlich die Umleitung zur BlueXP Website nicht folgen. 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 wählen Sie **Bestellungen verwalten**.



   - 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.

   - 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

NSS-Anmeldedaten managen, die mit einem BlueXP Konto verknüpft sind

Ordnen Sie Ihrem BlueXP Konto ein NetApp Support Site Konto zu, um wichtige Workflows für Cloud Volumes ONTAP zu ermöglichen. Diese NSS-Zugangsdaten sind dem gesamten BlueXP Konto zugeordnet.

BlueXP unterstützt zudem die Zuordnung eines NSS-Kontos pro BlueXP Benutzer. "Erfahren Sie, wie Sie Anmeldedaten auf Benutzerebene verwalten".

Überblick

Um die folgenden Aufgaben in BlueXP zu ermöglichen, ist es erforderlich, die NetApp Support Site Anmeldedaten mit Ihrer spezifischen BlueXP Account-ID zu verknüpfen:

- Implementierung von Cloud Volumes ONTAP unter Verwendung von BYOL (Bring-Your-Own-License)

  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.

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen

  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.

- Aktualisieren der Cloud Volumes ONTAP Software auf die neueste Version

Diese Zugangsdaten sind mit Ihrer spezifischen BlueXP Konto-ID verknüpft. Benutzer, die zum BlueXP Konto gehören, können über **Support > NSS Management** auf diese Anmeldedaten zugreifen.

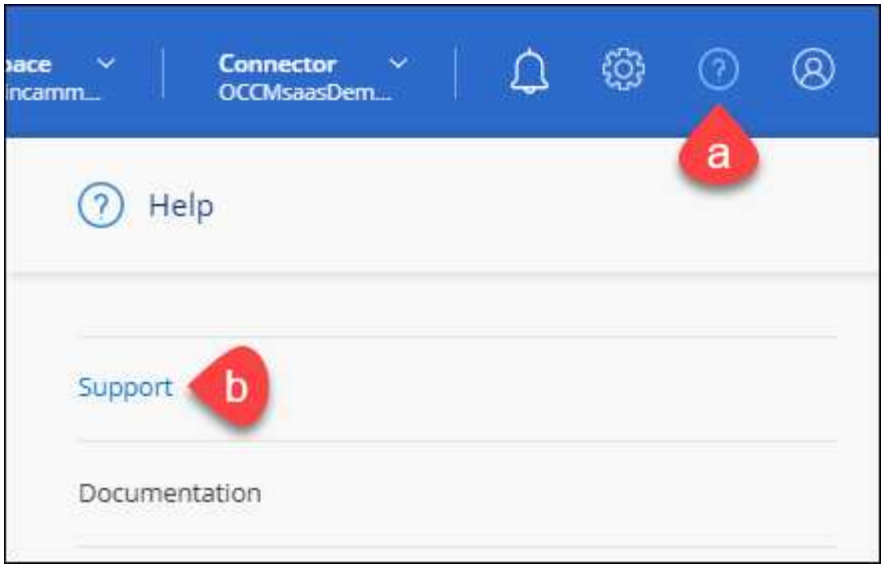
Fügen Sie ein NSS-Konto hinzu

Mit dem Support Dashboard können Sie Ihre NetApp Support Site Konten zur Verwendung mit BlueXP auf BlueXP Kontoebene hinzufügen und managen.

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

Schritte

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



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite umgeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices, die speziell auf Support und Lizenzierung zugeschnitten sind.

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 NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder Temporärkonto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto vorhanden sein, wenn es sich bei diesem Konto um ein Partner-Level-Konto handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da es bereits NSS-Benutzer unterschiedlichen Typs gibt.“

   Dasselbe gilt, wenn Sie bereits NSS-Konten auf Kundenebene haben und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet ist. 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. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird gesendet, um Sie

darüber zu informieren.

Was kommt als Nächstes?

Benutzer können jetzt das Konto beim Erstellen neuer Cloud Volumes ONTAP-Systeme und bei der Registrierung vorhandener Cloud Volumes ONTAP-Systeme auswählen.

- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Cloud Volumes ONTAP in Google Cloud wird gestartet"
- "Registrieren von Pay-as-you-go-Systemen"

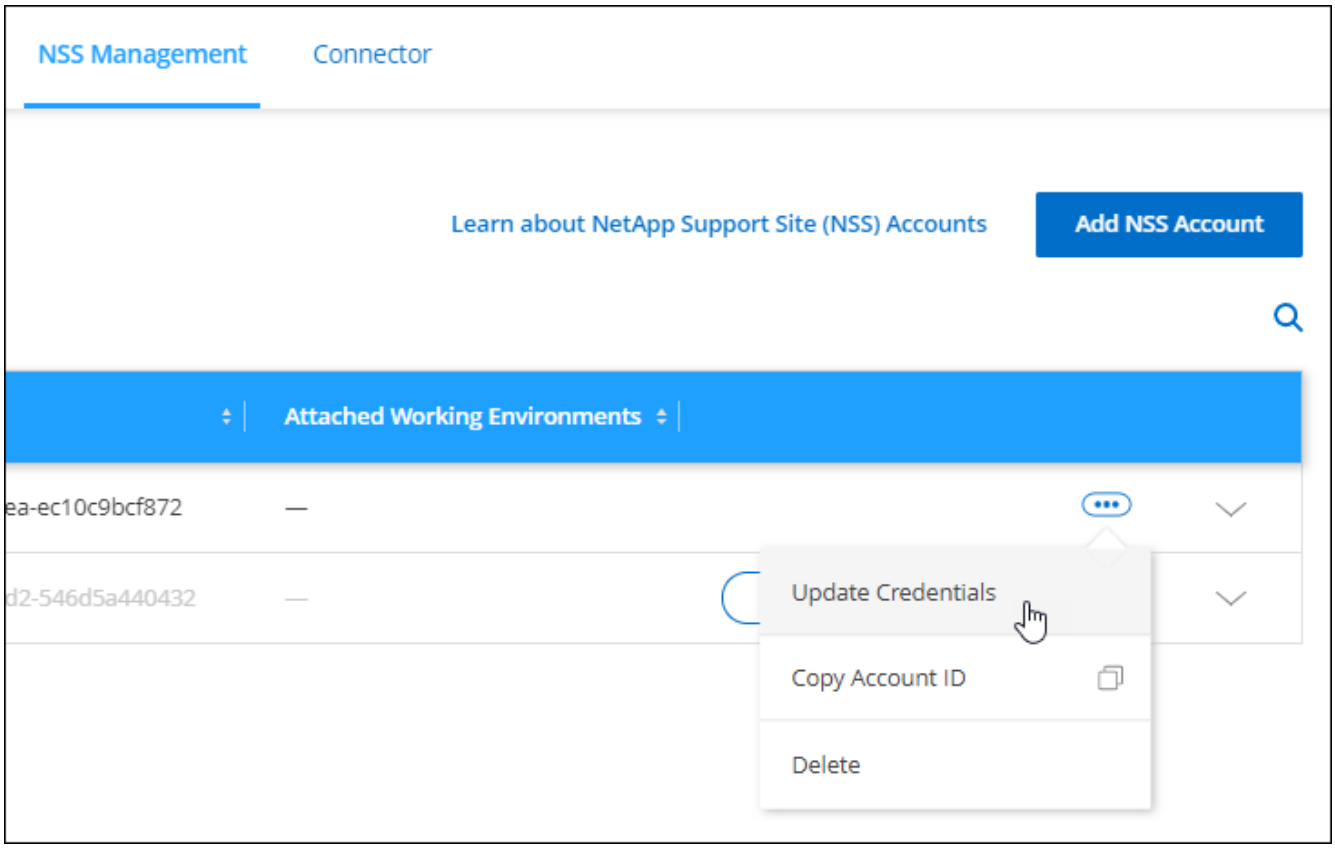
NSS-Anmeldeinformationen aktualisieren

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 auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.
2. Wählen Sie **NSS Management**.
3. Wählen Sie für das NSS-Konto, das Sie aktualisieren möchten, aus ••• Und wählen Sie dann **Anmeldeinformationen aktualisieren**.



4. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite umgeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices, die speziell auf Support und Lizenzierung zugeschnitten sind.

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

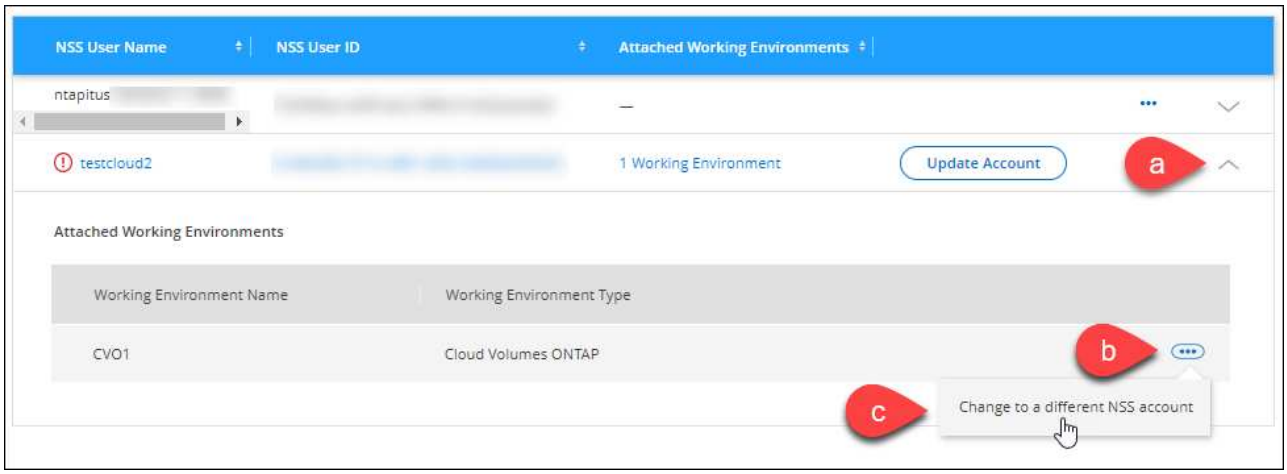
Verbinden Sie eine Arbeitsumgebung mit einem anderen NSS-Konto

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 der von NetApp für die Identitätsverwaltung übernommenen Microsoft-Entra-ID konfiguriert sind. Bevor Sie diese Funktion verwenden können, müssen Sie **NSS-Konto hinzufügen** oder **Konto aktualisieren** auswählen.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.
2. Wählen Sie **NSS Management**.
3. Führen Sie die folgenden Schritte aus, um das NSS-Konto zu ändern:
   a. Erweitern Sie die Zeile für den NetApp Support Site Account, dem die Arbeitsumgebung derzeit zugeordnet ist.
   b. Wählen Sie für die Arbeitsumgebung, für die Sie die Zuordnung ändern möchten, aus •••
   c. Wählen Sie **Ändern Sie auf ein anderes NSS-Konto**.



   d. Wählen Sie das Konto aus und wählen Sie dann **Speichern**.

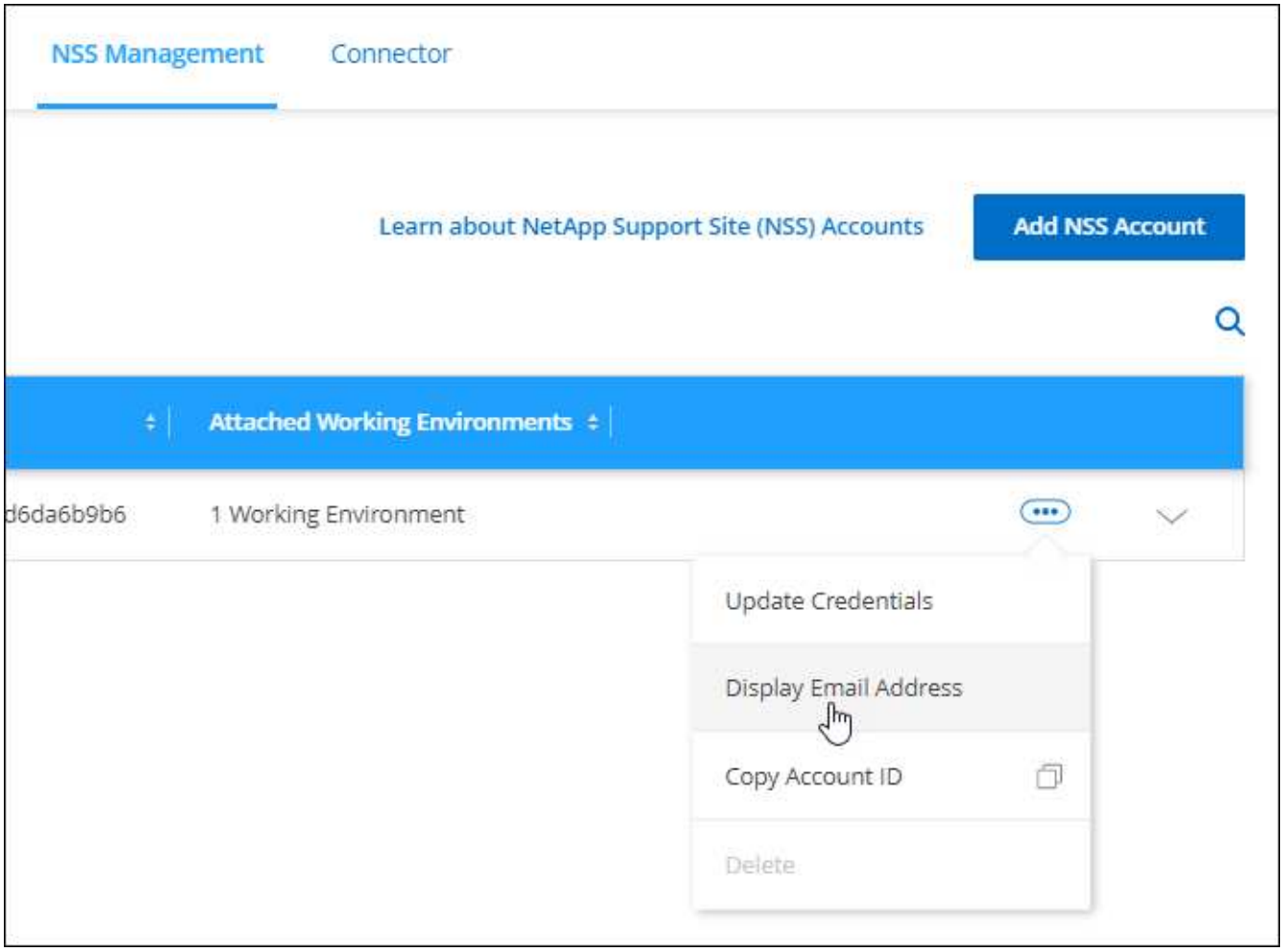
Zeigen Sie die E-Mail-Adresse für ein NSS-Konto an

Da nun Konten der NetApp-Support-Website Microsoft Entra ID für Authentifizierungsdienste verwenden, ist der in BlueXP angezeigte NSS-Benutzername in der Regel eine von Microsoft Entra 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

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



Ergebnis

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.

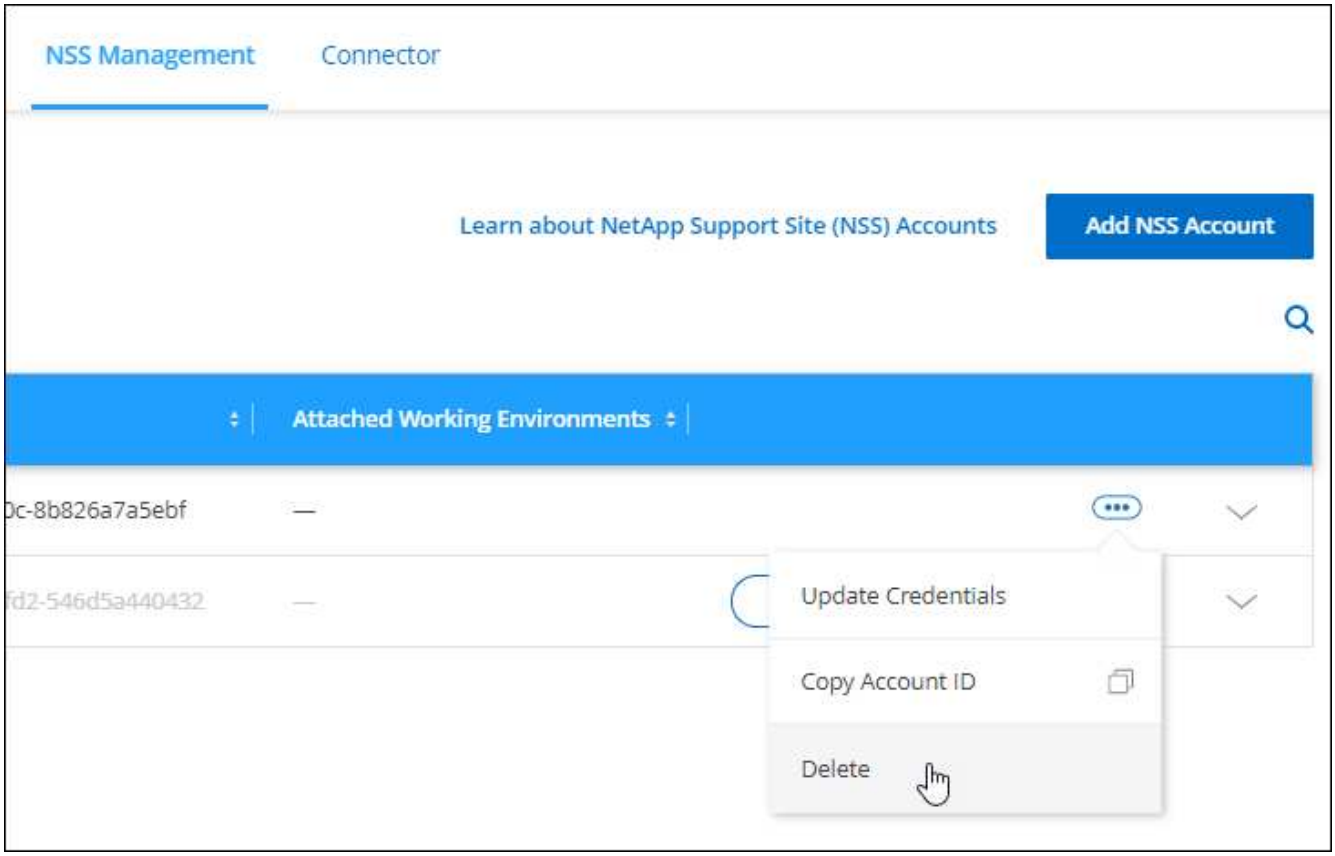
Entfernen Sie ein NSS-Konto

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 Verbinden Sie die Arbeitsumgebungen mit einem anderen NSS-Konto.

Schritte

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



4. Wählen Sie **Löschen**, um zu bestätigen.

Managen Sie die mit Ihren BlueXP Anmeldedaten verbundenen Zugangsdaten

Je nach den Aktionen, die Sie in BlueXP durchgeführt haben, können Sie Ihren BlueXP Benutzeranmeldeinformationen zur ONTAP und zur NetApp Support Website (NSS) zugeordnet haben. Sie können diese Anmeldedaten in BlueXP anzeigen und managen, nachdem Sie sie verknüpft haben. Wenn Sie beispielsweise das Passwort für diese Anmeldedaten ändern, müssen Sie das Passwort in BlueXP aktualisieren.

ONTAP Referenzen

Wenn Sie ein lokales ONTAP-Cluster direkt ohne einen Connector erkennen, werden Sie aufgefordert, die ONTAP-Anmeldedaten für das Cluster einzugeben. Diese Anmeldeinformationen werden auf Benutzerebene verwaltet, was bedeutet, dass sie von anderen Benutzern, die sich anmelden, nicht angezeigt werden können.

NSS-Anmeldeinformationen

Die NSS-Zugangsdaten für Ihre BlueXP Anmeldung ermöglichen die Support-Registrierung, das Fallmanagement und den Zugriff auf Digital Advisor.

- Wenn Sie **Support > Ressourcen** aufrufen und sich für den Support registrieren, werden Sie aufgefordert, Ihre NSS-Anmeldedaten mit Ihrem BlueXP Login zu verknüpfen.

  Durch diese Aktion wird das BlueXP Konto für den Support registriert und die Support-Berechtigung aktiviert. Nur ein Benutzer in Ihrem BlueXP Konto muss ein NetApp Support Site Konto mit seinen BlueXP Anmeldedaten verknüpfen, um sich für den Support zu registrieren und die Support-Berechtigung zu aktivieren. Nachdem dies abgeschlossen ist, zeigt die Seite **Ressourcen** an, dass Ihr Konto für Support registriert ist.

  "Erfahren Sie, wie Sie sich für Support registrieren"

- Wenn Sie auf **Support > Case Management** zugreifen, werden Sie aufgefordert, Ihre NSS-Anmeldedaten einzugeben, sofern Sie dies noch nicht getan haben. Auf dieser Seite können Sie die Support-Fälle erstellen und verwalten, die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpft sind.
- Wenn Sie in BlueXP auf Digital Advisor zugreifen, werden Sie aufgefordert, sich bei Digital Advisor anzumelden, indem Sie Ihre NSS-Anmeldedaten eingeben.

Beachten Sie Folgendes zu dem NSS-Konto bei Ihrer BlueXP Anmeldung:

- Das Konto wird auf Benutzerebene verwaltet, was bedeutet, dass es von anderen Benutzern, die sich anmelden, nicht angezeigt wird.
- Digital Advisor und Support-Case-Management können nur ein NSS-Konto pro Benutzer zugeordnet werden.
- Wenn Sie ein NetApp Support Site Konto mit einer Cloud Volumes ONTAP Arbeitsumgebung verknüpfen möchten, können Sie nur aus den NSS-Konten wählen, die dem BlueXP Konto hinzugefügt wurden, dem Sie angehören.

  Die Zugangsdaten für NSS Konten unterscheiden sich von dem NSS-Konto, das mit Ihrer BlueXP Anmeldung verknüpft ist. Mit den Zugangsdaten für NSS Konten können Sie Cloud Volumes ONTAP implementieren, wenn Sie Ihre eigene Lizenz (BYOL) verwenden, PAYGO-Systeme registrieren und die Cloud Volumes ONTAP Software aktualisieren.

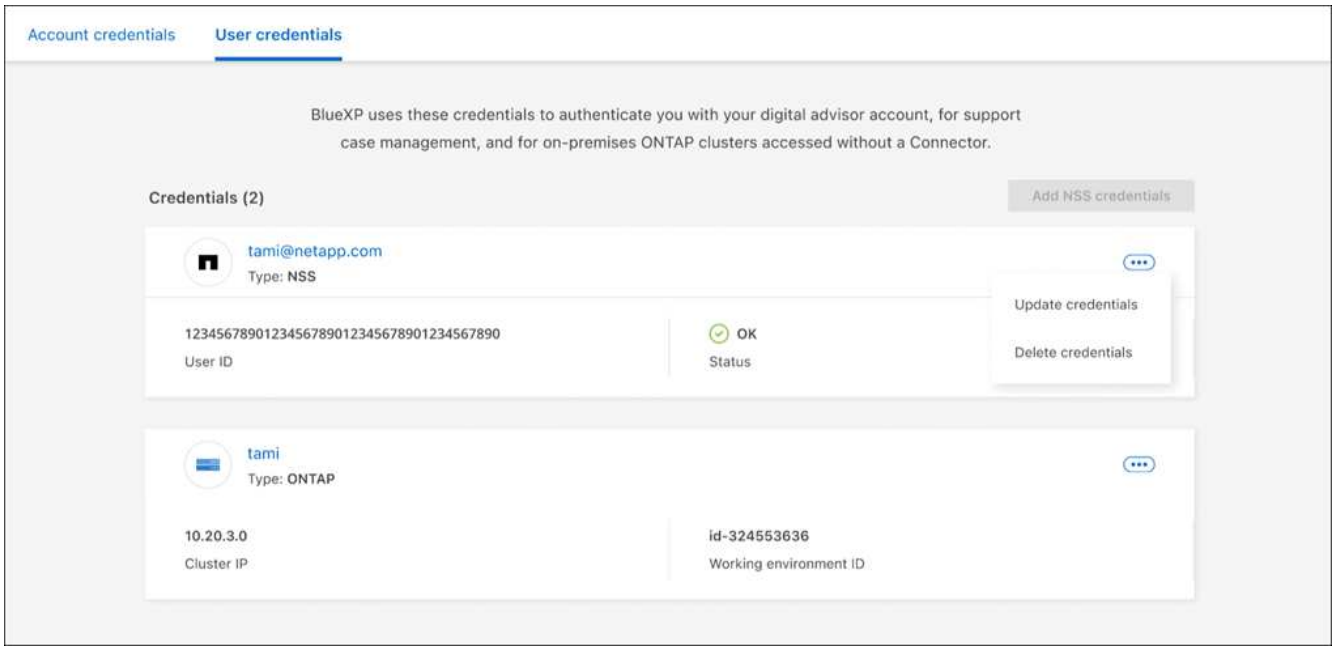
  "Erfahren Sie mehr über die Verwendung von NSS Credentials mit Ihrem BlueXP Konto".

Verwalten Sie Ihre Benutzeranmeldeinformationen

Verwalten Sie Ihre Benutzeranmeldeinformationen, indem Sie den Benutzernamen und das Kennwort aktualisieren oder die Anmeldeinformationen löschen.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wenn Sie noch keine Anmeldedaten für den Benutzer haben, können Sie **Add NSS Credentials** auswählen, um Ihr NetApp Support Site Konto hinzuzufügen.
4. Verwalten Sie vorhandene Anmeldeinformationen, indem Sie folgende Optionen auswählen:
   - **Zugangsdaten aktualisieren**: Aktualisieren Sie den Benutzernamen und das Passwort für das Konto.
   - **Zugangsdaten löschen**: Entfernen Sie das Konto, das Ihrem BlueXP Benutzerkonto zugeordnet ist.



Ergebnis

BlueXP aktualisiert Ihre Zugangsdaten. Die Änderungen werden angezeigt, wenn Sie auf den ONTAP-Cluster, den Digital Advisor oder die Seite Case-Management zugreifen.