Dokumentation zur Einrichtung und Administration von BlueXP

Setup and administration

NetApp
April 26, 2024

Inhalt

Dokumentation zur Einrichtung und Administration von BlueXP

Versionshinweise

Was ist neu

Informieren Sie sich über die Neuerungen bei den BlueXP Administrationsfunktionen: BlueXP Accounts, Connectors, Zugangsdaten für Cloud-Provider und vieles mehr.

Bis 22. April 2024

Anschluss 3.9.39

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Bug Fixes.

Derzeit ist die Version 3.9.39 für den Standardmodus und den eingeschränkten Modus verfügbar.

AWS Berechtigungen zum Erstellen eines Connectors

Zur Erstellung eines Connectors in AWS aus BlueXP sind jetzt zwei zusätzliche Berechtigungen erforderlich:

```
"ec2:DescribeLaunchTemplates",
"ec2:CreateLaunchTemplate",
```

Diese Berechtigungen sind erforderlich, um IMDSv2 auf der EC2-Instanz für den Connector zu aktivieren.

Wir haben diese Berechtigungen in die Richtlinie aufgenommen, die beim Erstellen eines Connectors in der BlueXP Benutzeroberfläche angezeigt wird, und in derselben Richtlinie, die in der Dokumentation enthalten ist.

> Diese Richtlinie enthält nur die Berechtigungen, die zum Starten der Connector-Instanz in AWS von BlueXP erforderlich sind. Es ist nicht dieselbe Richtlinie, die der Connector-Instanz zugewiesen wird.

"Erfahren Sie, wie Sie AWS-Berechtigungen zur Erstellung eines Connectors aus AWS einrichten".

Bis 11. April 2024

Update für die Docker Engine

Wir haben die Anforderungen für die Docker Engine aktualisiert, um die maximal unterstützte Version des Connectors anzugeben. Diese ist 25.0.5. Die unterstützte Mindestversion ist immer noch 19.3.1.

"Host-Anforderungen des Connectors anzeigen".

26 März 2024

Freigabe des privaten Modus (3.9.38)

Für BlueXP ist jetzt eine neue Version des privaten Modus verfügbar. Diese Version umfasst die folgenden Versionen der BlueXP Services, die im Private-Mode unterstützt werden.

Service	Version enthalten
Stecker	3.9.38
Backup und Recovery	12 März 2024
Klassifizierung	4 März 2024
Cloud Volumes ONTAP-Management	8 März 2024
Digitale Brieftasche	30 Juli 2023
Lokales ONTAP-Cluster-Management	30 Juli 2023
Replizierung	18 Sept. 2022

Diese neue Version kann von der NetApp Support-Website heruntergeladen werden.

- "Weitere Informationen zum privaten Modus"
- "Erfahren Sie mehr über die ersten Schritte mit BlueXP im privaten Modus"
- "Erfahren Sie, wie Sie den Connector bei der Verwendung des privaten Modus aktualisieren"

8 März 2024

Anschluss 3.9.38

Derzeit ist die Version 3.9.38 für den Standardmodus und den eingeschränkten Modus verfügbar. Diese Version enthält Unterstützung für IMDSv2 in AWS und ein AWS-Berechtigungs-Update.

Unterstützung für IMDSv2

BlueXP unterstützt jetzt den Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) mit der Connector-Instanz sowie mit Cloud Volumes ONTAP-Instanzen. IMDSv2 bietet einen verbesserten Schutz vor Schwachstellen. Bisher wurde nur IMDSv1 unterstützt.

"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.

"Erfahren Sie, wie Sie IMDSv2 auf vorhandenen Instanzen konfigurieren".

Update zu den AWS-Berechtigungen

Wir haben die Connector-Richtlinie für AWS mit der Berechtigung „ec2:DescribeAvailability Zones“ aktualisiert. Diese Berechtigung ist für eine kommende Version erforderlich. Wir werden die Versionshinweise mit weiteren Details aktualisieren, sobald diese Version verfügbar ist.

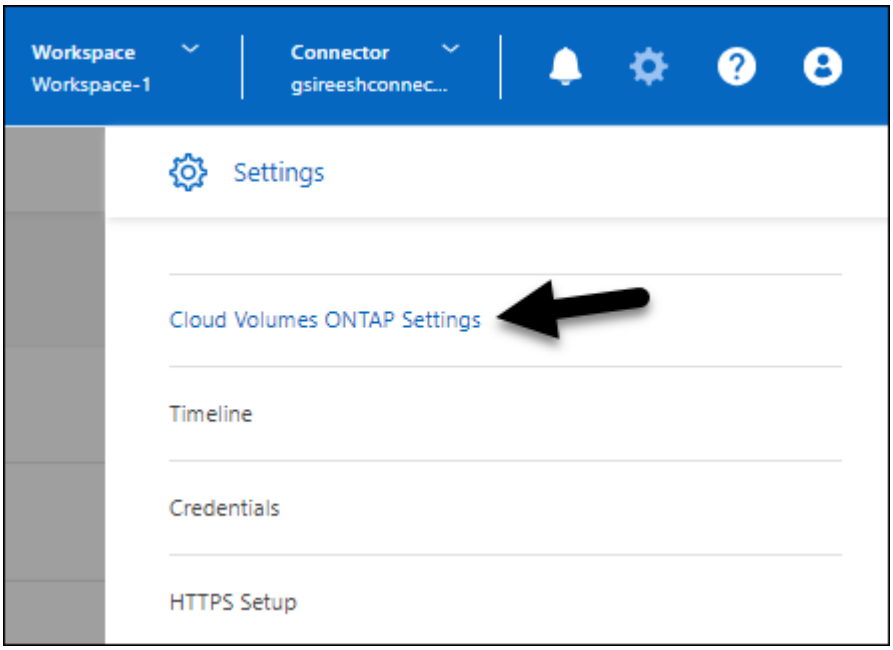
"Anzeigen von AWS-Berechtigungen für den Connector".

Proxy-Einstellungen und Cloud Volumes ONTAP-Einstellungen

Die Proxy-Server-Einstellungen für den Connector sind jetzt auf der Seite **Connectors verwalten** (Standardmodus) oder auf der Seite **Connectors bearbeiten** (eingeschränkter Modus und privater Modus) verfügbar.

"Erfahren Sie, wie Sie den Connector für die Verwendung eines Proxy-Servers konfigurieren".

Außerdem haben wir die Seite **Verbindungseinstellungen** in **Cloud Volumes ONTAP-Einstellungen** umbenannt.



15 Februar 2024

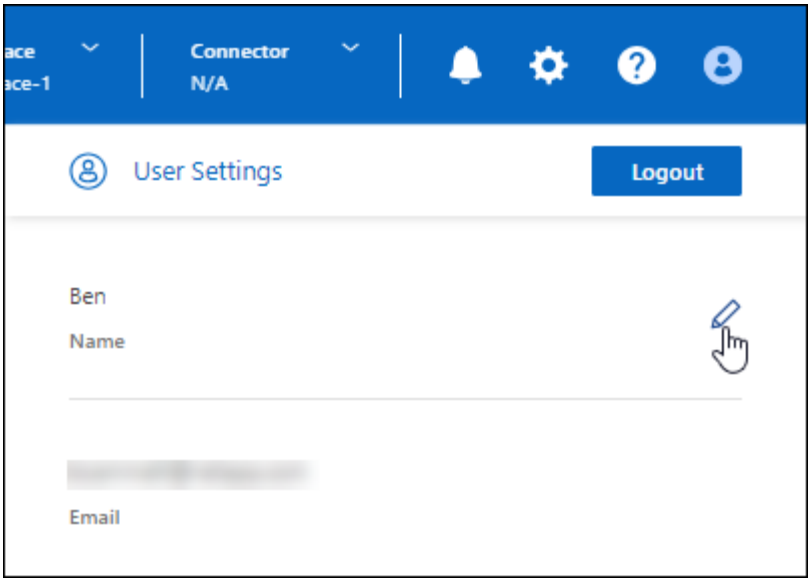
Anschluss 3.9.37

Diese Version des BlueXP Connector enthält kleinere Sicherheitsverbesserungen und Bug Fixes.

Derzeit ist die Version 3.9.37 für den Standardmodus und den eingeschränkten Modus verfügbar.

Namen bearbeiten

Wenn Sie sich mit den NetApp Cloud-Anmeldedaten bei BlueXP anmelden, können Sie jetzt Ihren Namen in **Benutzereinstellungen** bearbeiten.



Die Bearbeitung Ihres Namens wird nicht unterstützt, wenn Sie sich mit einer Verbundverbindung oder mit Ihrem NetApp Support-Website-Konto anmelden.

11 Januar 2024

Anschluss 3.9.36

Diese Version enthält kleinere Verbesserungen, Fehlerbehebungen und Unterstützung für den Connector in den folgenden Cloud-Regionen:

- Der Region Israel (Tel Aviv) in AWS
- Die Region Saudi-Arabien in Google Cloud

Bis 5. Dezember 2023

Freigabe des privaten Modus (3.9.35)

Für BlueXP ist jetzt eine neue Version des privaten Modus verfügbar. Diese Version enthält Version 3.9.35 des Connectors sowie Versionen der BlueXP Services, die ab Oktober 2023 im Privatmodus unterstützt werden.

Diese neue Version kann von der NetApp Support-Website heruntergeladen werden.

- "Informieren Sie sich über die im Private-Mode enthaltenen BlueXP Services"
- "Erfahren Sie mehr über die ersten Schritte mit BlueXP im privaten Modus"
- "Erfahren Sie, wie Sie den Connector bei der Verwendung des privaten Modus aktualisieren"

Bis 8. November 2023

Anschluss 3.9.35

Diese Version enthält kleinere Sicherheitsverbesserungen und Fehlerbehebungen.

6 Oktober 2023

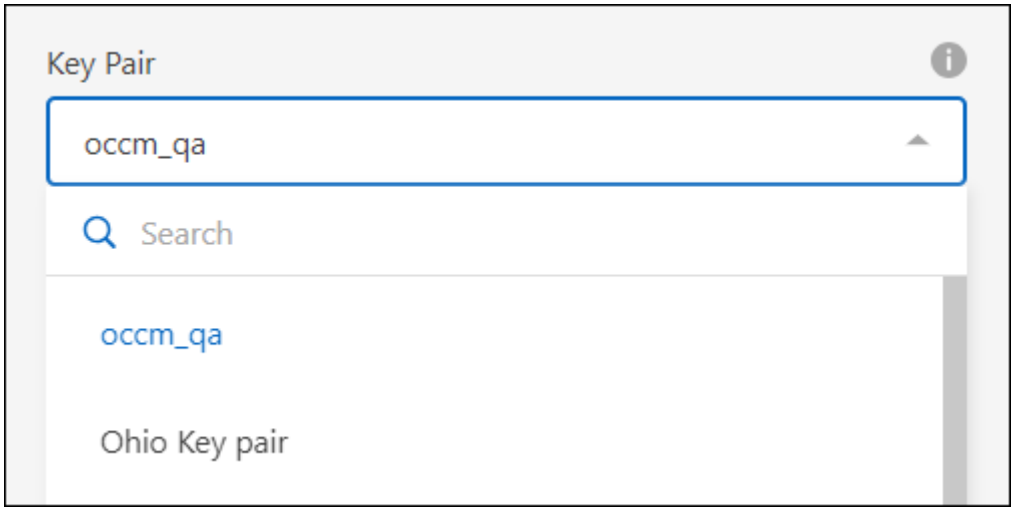
Anschluss 3.9.34

Diese Version enthält kleinere Verbesserungen und Fehlerbehebungen.

10 September 2023

Anschluss 3.9.33

- Wenn Sie einen Connector in AWS von BlueXP erstellen, können Sie nun im Feld Schlüsselpaar suchen, um das Schlüsselpaar, das Sie mit der Connector-Instanz verwenden möchten, einfacher zu finden.



- Dieses Update enthält auch Fehlerbehebungen.

30 Juli 2023

Anschluss 3.9.32

- Sie können jetzt die BlueXP Audit-Service-API für den Export von Audit-Protokollen verwenden.

  Der Audit-Service zeichnet Informationen zu den durch BlueXP Services ausgeführten Vorgängen auf. Dazu gehören Arbeitsbereiche, verwendete Connectors und andere Telemetriedaten. Anhand dieser Daten können Sie bestimmen, welche Aktionen durchgeführt wurden, wer sie ausgeführt hat und wann sie aufgetreten sind.

  "Erfahren Sie mehr über die Verwendung der Audit-Service-API"

  Beachten Sie, dass auf diesen Link auch über die BlueXP Benutzeroberfläche auf der Seite „Zeitleiste“ zugegriffen werden kann.

- Diese Version des Connectors enthält außerdem Cloud Volumes ONTAP-Verbesserungen und On-Premises-ONTAP-Cluster-Verbesserungen.
  - "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"
  - "Die ONTAP-On-Premises-Cluster-Verbesserungen"

2 Juli 2023

Anschluss 3.9.31

- Sie können jetzt On-Premises-ONTAP-Cluster über die Registerkarte **My estate** (vorher **Meine Möglichkeiten**) entdecken.

  "Erfahren Sie auf der Seite My Estate, wie Sie Cluster erkennen".

- Wenn Sie den Connector in einer Azure Government-Region verwenden, sollten Sie sicherstellen, dass der Connector den folgenden Endpunkt erreichen kann:

  https://occmclientinfragov.azurecr.us

  Dieser Endpunkt ist erforderlich, um den Connector manuell zu installieren und den Connector und seine Docker-Komponenten zu aktualisieren.

  Aufgrund dieser Änderung kontaktiert ein Connector in einer Azure-Regierungsregion nicht mehr den folgenden Endpunkt:

  https://cloudmanagerinfraprod.azurecr.io

  Beachten Sie, dass dieser Endpunkt weiterhin für alle anderen Konfigurationen mit eingeschränktem Modus und für den Standardmodus erforderlich ist.

4 Juni 2023

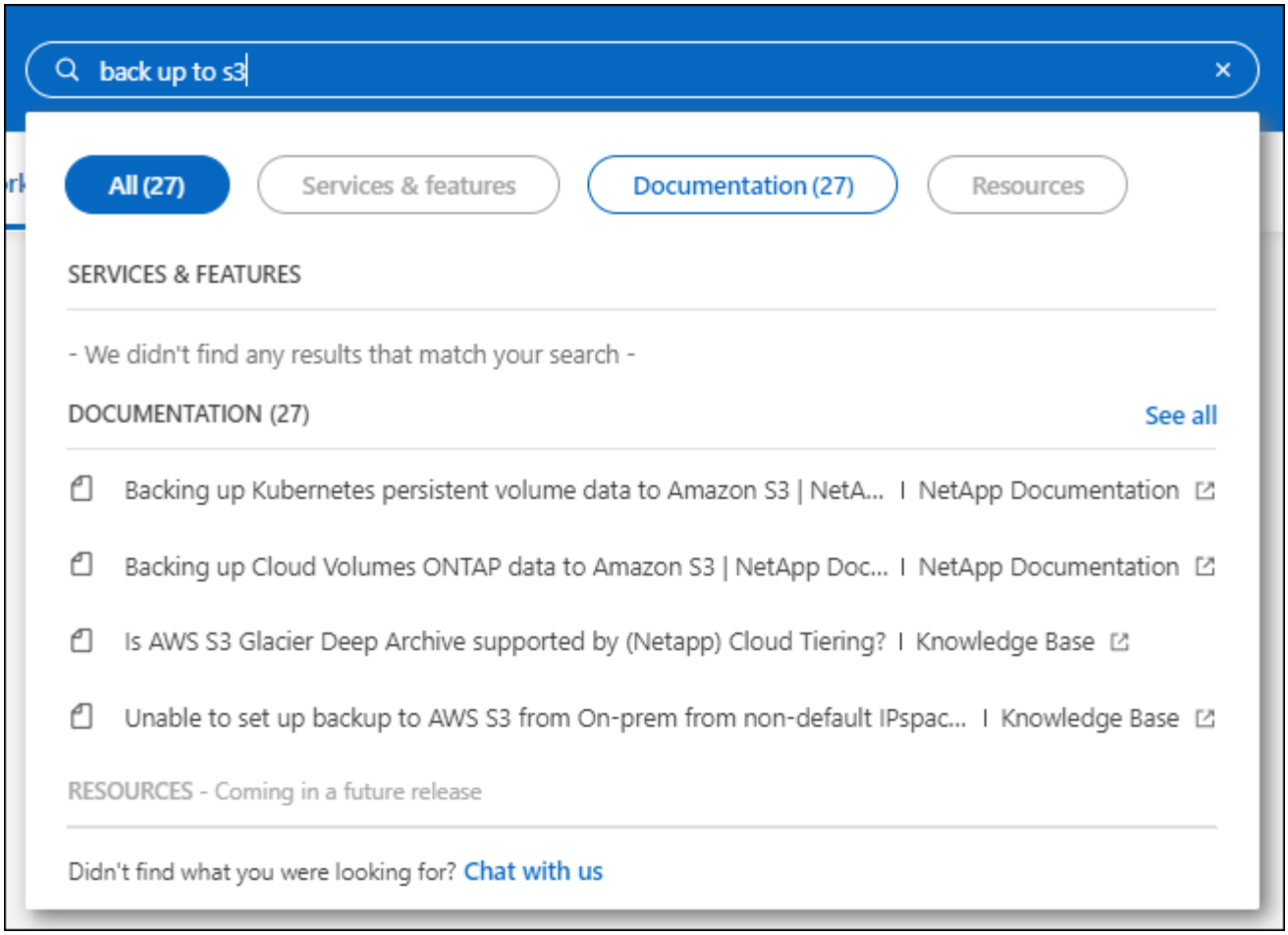
Anschluss 3.9.30

- Wenn Sie einen NetApp Support-Fall über das Support Dashboard öffnen, eröffnet BlueXP nun den Fall über das Konto auf der NetApp Support Website, das mit Ihren BlueXP Anmeldedaten verknüpft ist. BlueXP hat zuvor das NetApp Support Site Konto genutzt, das dem gesamten BlueXP Konto zugeordnet ist.

  Im Rahmen dieser Änderung erfolgt die Support-Registrierung für ein BlueXP Konto jetzt über das NetApp Support Site Konto, das mit den BlueXP Anmeldedaten eines Benutzers verknüpft ist. Zuvor wurde der Support über ein NSS-Konto registriert, das dem gesamten BlueXP Konto zugeordnet ist. Daher werden andere BlueXP Benutzer denselben Support-Registrierungsstatus nicht sehen, wenn sie kein NetApp Support Site Konto mit ihrer BlueXP Anmeldung verknüpft haben. Wenn Sie Ihr BlueXP Konto bereits für Support registriert haben, ist Ihr Registrierungsstatus weiterhin gültig. Sie müssen nur ein NSS-Konto auf Benutzerebene hinzufügen, um den Status anzuzeigen.

  - "Erfahren Sie, wie Sie mit dem NetApp-Support einen Fall erstellen"
  - "Managen Sie Zugangsdaten für Ihre BlueXP Anmeldung"
  - "Erfahren Sie, wie Sie sich für Support registrieren"

- Sie können jetzt in BlueXP nach Dokumentation suchen. Suchergebnisse enthalten nun Links zu Inhalten auf docs.netapp.com und kb.netapp.com, die Ihnen bei der Beantwortung Ihrer Frage helfen könnten.



- Mit Connector können Sie jetzt Azure Storage-Konten von BlueXP hinzufügen und managen.

  "Erfahren Sie, wie Sie neue Azure-Storage-Konten in Ihren Azure-Abonnements von BlueXP hinzufügen".

- Der Connector wird nun in den folgenden AWS Regionen unterstützt:
  - Hyderabad (AP-Süd-2)
  - Melbourne (AP-Südost-4)
  - Spanien (eu-Süd-2)
  - VAE (ME-Central-1)
  - Zürich (eu-Zentral-2)
- Der Connector wird nun in den folgenden Azure-Regionen unterstützt:
  - Brasilien Süd
  - Frankreich Süd
  - Jio India Central
  - Jio Indien Westen
  - Polen, Mitte
  - Qatar Central
- Der Connector wird nun in folgenden Google Cloud Regionen unterstützt:
  - Columbus (USA-öst5)

- Dallas (USA-Süd-1)

"Hier finden Sie die vollständige Liste der unterstützten Regionen"

7 Mai 2023

Anschluss 3.9.29

- Ubuntu 22.04 ist das neue Betriebssystem für den Connector, wenn Sie einen Connector von BlueXP oder vom Marktplatz Ihres Cloud-Providers bereitstellen.

  Sie haben auch die Möglichkeit, den Connector manuell auf Ihrem eigenen Linux-Host zu installieren, auf dem Ubuntu 22.04 ausgeführt wird.

- Red hat Enterprise Linux 8.6 und 8.7 werden bei neuen Connector-Implementierungen nicht mehr unterstützt.

  Diese Versionen werden bei neuen Bereitstellungen nicht unterstützt, da Red hat Docker nicht mehr unterstützt, was für den Connector erforderlich ist. Wenn Sie bereits einen Connector mit RHEL 8.6 oder 8.7 verwenden, unterstützt NetApp Ihre Konfiguration weiterhin.

  Red hat 7.6, 7.7, 7.8 und 7.9 werden weiterhin von neuen und vorhandenen Connectors unterstützt.

- Der Connector wird jetzt in der Region Katar in Google Cloud unterstützt.
- Der Connector wird auch in der Region Sweden Central in Microsoft Azure unterstützt.

  "Hier finden Sie die vollständige Liste der unterstützten Regionen"

- Diese Version des Connectors enthält Cloud Volumes ONTAP-Verbesserungen.

  "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

Bis 4. April 2023

Bereitstellungsmodi

Mit BlueXP *Implementierungsmodi* können Sie BlueXP entsprechend Ihren geschäftlichen und Sicherheitsanforderungen einsetzen. Sie können zwischen drei Modi wählen:

- Standardmodus
- Eingeschränkter Modus
- Privater Modus

"Erfahren Sie mehr über diese Bereitstellungsmodi".

> Die Einführung des eingeschränkten Modus ersetzt die Option zum Aktivieren oder Deaktivieren der SaaS-Plattform. Sie können den eingeschränkten Modus zum Zeitpunkt der Kontoerstellung aktivieren. Sie kann später nicht aktiviert oder deaktiviert werden.

Bis 3. April 2023

Anschluss 3.9.28

- Das Digital Wallet von BlueXP unterstützt jetzt E-Mail-Benachrichtigungen.

  Wenn Sie Ihre Benachrichtigungseinstellungen konfigurieren, können Sie E-Mail-Benachrichtigungen erhalten, wenn Ihre BYOL-Lizenzen ablaufen (eine „Warnung“) oder wenn sie bereits abgelaufen sind (eine „Fehler“-Benachrichtigung).

  "Hier erfahren Sie, wie Sie E-Mail-Benachrichtigungen einrichten".

- Der Connector wird nun in der Region Google Cloud Turin unterstützt.

  "Hier finden Sie die vollständige Liste der unterstützten Regionen"

- Sie können jetzt die Anmeldedaten für den Benutzer managen, die mit Ihrer BlueXP Anmeldung verknüpft sind: ONTAP Zugangsdaten und NSS Zugangsdaten (NetApp Support Site).

  Wenn Sie zu **Einstellungen > Anmeldeinformationen** wechseln, können Sie die Anmeldeinformationen anzeigen, die Anmeldeinformationen aktualisieren und löschen. Wenn Sie beispielsweise das Passwort für diese Anmeldedaten ändern, müssen Sie das Passwort in BlueXP aktualisieren.

  "Erfahren Sie, wie Sie die Anmeldedaten von Benutzern verwalten".

- Anhänge können nun hochgeladen werden, wenn ein Support-Case erstellt oder die Fallhinweise für einen bestehenden Support-Case aktualisiert werden.

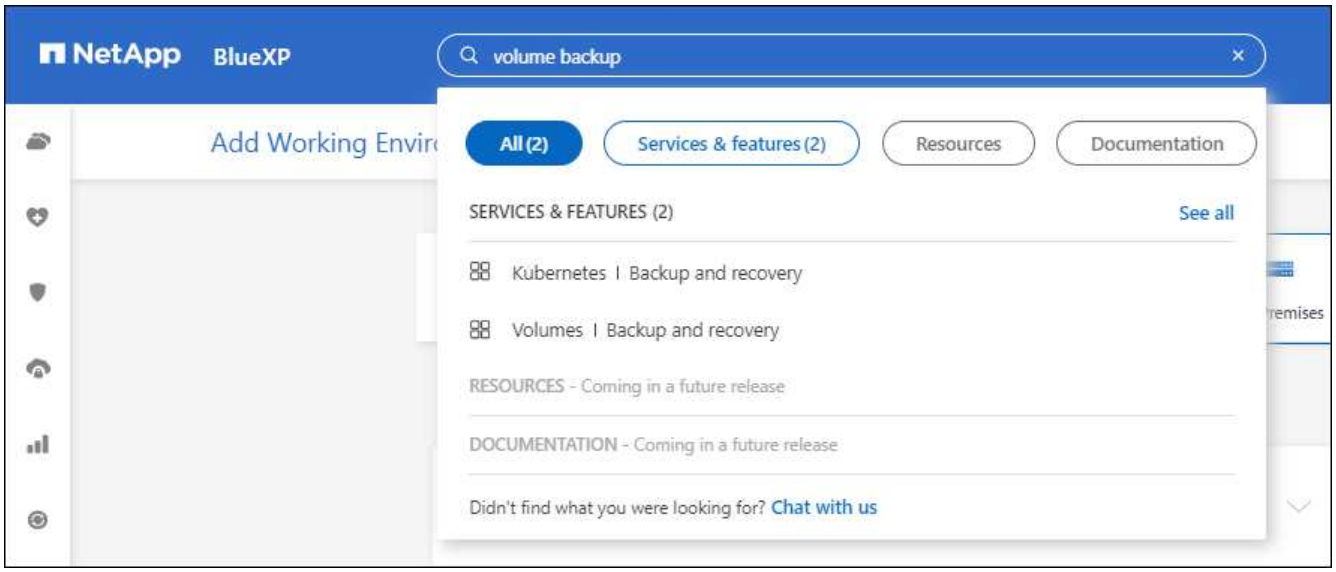
  "Erfahren Sie, wie Sie Support-Fälle erstellen und managen".

- Diese Version des Connectors enthält außerdem Cloud Volumes ONTAP-Verbesserungen und On-Premises-ONTAP-Cluster-Verbesserungen.
  - "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"
  - "Die ONTAP-On-Premises-Cluster-Verbesserungen"

5 März 2023

Anschluss 3.9.27

- Die Suche ist jetzt auch in der BlueXP Konsole verfügbar. Derzeit können Sie über die Suche nach BlueXP Services und Funktionen suchen.



- Sie können aktive und gelöste Support-Cases direkt über BlueXP anzeigen und managen. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Fälle verwalten.

  "Erfahren Sie, wie Sie Ihre Support-Fälle managen".

- Der Connector wird jetzt in jeder Cloud-Umgebung unterstützt, die vollständig vom Internet isoliert ist. Anschließend können Sie die BlueXP Konsole, die auf dem Connector ausgeführt wird, verwenden, um Cloud Volumes ONTAP am selben Standort zu implementieren und lokale ONTAP-Cluster zu erkennen (wenn Sie eine Verbindung von Ihrer Cloud-Umgebung zu Ihrer On-Premises-Umgebung haben). Auch Backup und Recovery mit BlueXP können Sie Cloud Volumes ONTAP Volumes in AWS und Azure kommerziellen Regionen sichern. Andere BlueXP Services werden bei dieser Implementierung nicht unterstützt, außer beim BlueXP Digital Wallet.

  Die Cloud-Region kann eine Region für sichere US-Behörden wie AWS Top Secret Cloud, AWS Secret Cloud, Azure IL6 oder jede kommerzielle Region sein.

  Um zu beginnen, installieren Sie die Connector Software manuell, melden Sie sich bei der BlueXP Konsole an, die auf dem Connector ausgeführt wird, fügen Sie Ihre BYOL-Lizenz zur BlueXP Digital Wallet hinzu und implementieren Sie dann Cloud Volumes ONTAP.

  - "Installieren Sie den Connector an einem Ort ohne Internetzugang"
  - "Greifen Sie über den Connector auf die BlueXP Konsole zu"
  - "Fügen Sie eine nicht zugewiesene Lizenz hinzu"
  - "Legen Sie los – mit Cloud Volumes ONTAP"

- Mit dem Connector können Sie jetzt Amazon S3 Buckets aus BlueXP hinzufügen und managen.

  "So fügen Sie über BlueXP neue Amazon S3 Buckets in Ihrem AWS-Konto hinzu".

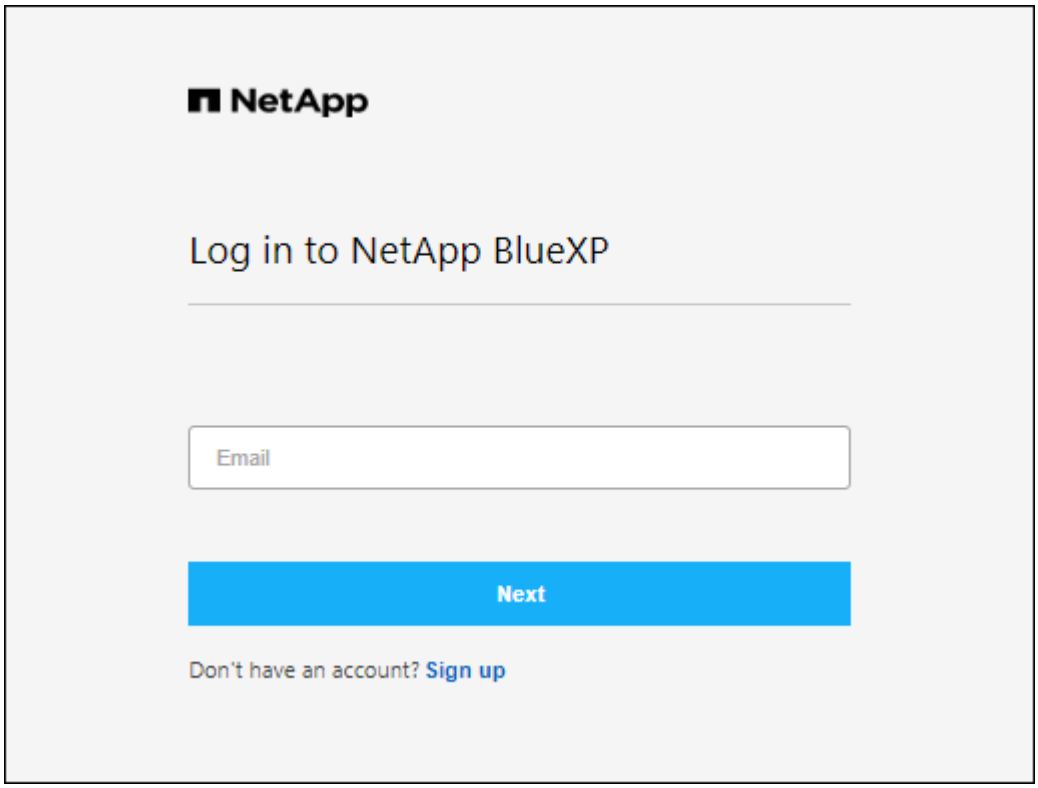
- Diese Version des Connectors enthält Cloud Volumes ONTAP-Verbesserungen.

  "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

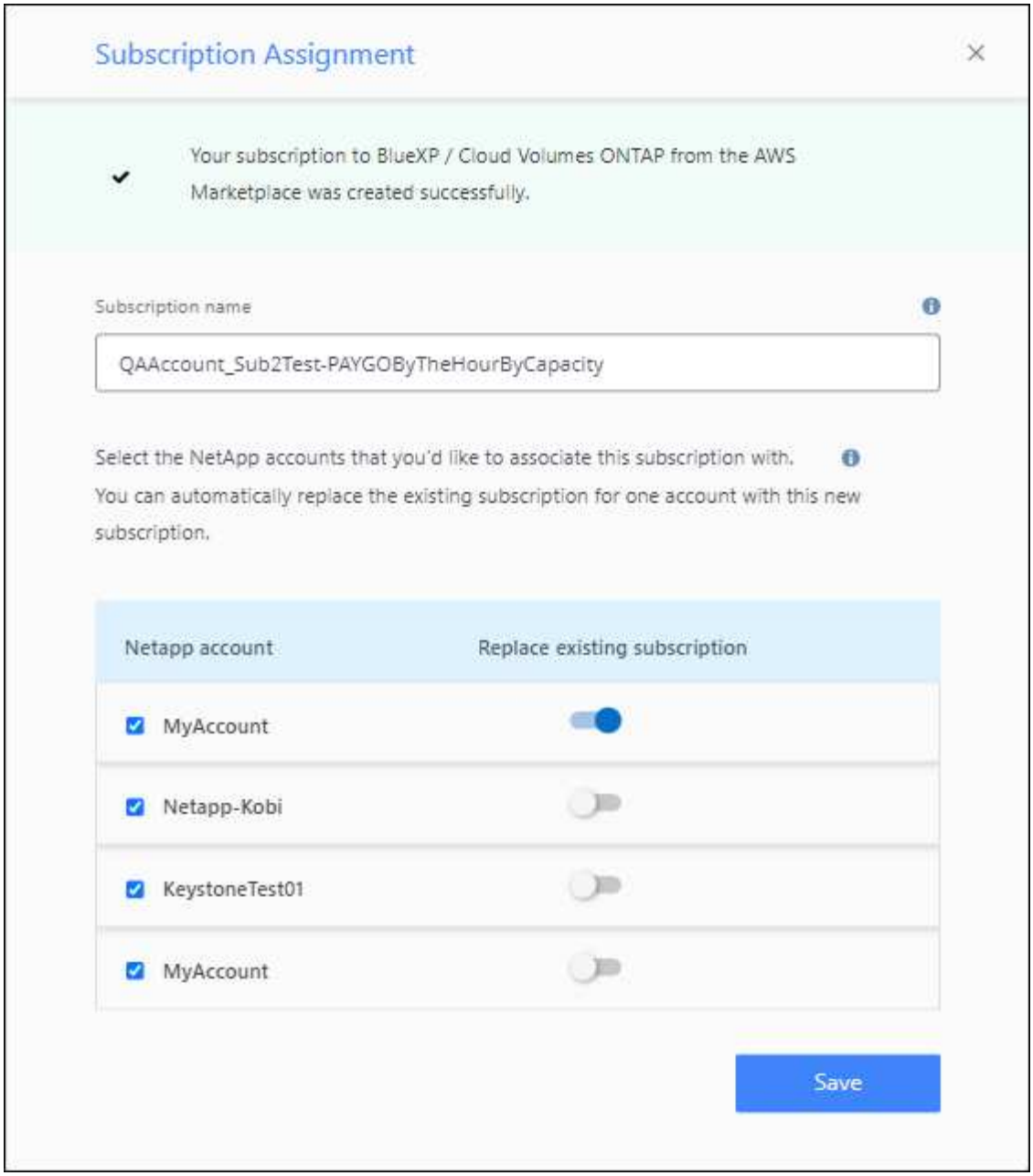
5 Februar 2023

Anschluss 3.9.26

- Auf der Seite **Anmelden** werden Sie jetzt aufgefordert, die mit Ihrem Login verknüpfte E-Mail-Adresse einzugeben. Nachdem Sie **Next** ausgewählt haben, fordert BlueXP Sie auf, sich mit der Authentifizierungsmethode zu authentifizieren, die mit Ihrer Anmeldung verknüpft ist:
  - Das Passwort für Ihre NetApp Cloud-Anmeldedaten
  - Ihre föderierten Identitätsinformationen
  - Ihre Zugangsdaten für die NetApp Support Site



- Wenn Sie neu bei BlueXP sind und über bereits vorhandene Zugangsdaten für die NetApp Support Site (NSS) verfügen, können Sie die Anmeldeseite überspringen und Ihre E-Mail-Adresse direkt auf der Anmeldeseite eingeben. BlueXP meldet Sie im Rahmen dieser ersten Anmeldung an.
- Wenn Sie BlueXP über den Markt Ihres Cloud-Providers abonnieren, haben Sie nun die Möglichkeit, das vorhandene Abonnement für ein Konto durch das neue Abonnement zu ersetzen.



  - "Verbinden Sie ein AWS Abonnement"
  - "Lesen Sie, wie Sie ein Azure-Abonnement zuordnen"
  - "So verknüpfen Sie ein Google Cloud-Abonnement"
- BlueXP benachrichtigt Sie nun, wenn Ihr Connector 14 Tage oder länger ausgeschaltet wurde.
  - "Erfahren Sie mehr über BlueXP-Benachrichtigungen"
  - "Erfahren Sie, warum die Anschlüsse weiterhin ausgeführt werden sollten"
- Wir haben die Connector-Richtlinie für Google Cloud aktualisiert, um eine erforderliche Erlaubnis zum Erstellen und Managen von Storage-VMs auf Cloud Volumes ONTAP HA-Paaren zu enthalten:

  compute.instances.updateNetworkInterface

  "Zeigen Sie Google Cloud-Berechtigungen für den Connector an".

- Diese Version des Connectors enthält Cloud Volumes ONTAP-Verbesserungen.

  "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

Januar 2023

Anschluss 3.9.25

Diese Version des Connectors enthält Cloud Volumes ONTAP-Verbesserungen und Fehlerbehebungen.

"Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

Bis 4. Dezember 2022

Anschluss 3.9.24

- Die URL für die BlueXP-Konsole wurde auf aktualisiert https://console.bluexp.netapp.com
- Der Connector wird nun in der Google Cloud Israel Region unterstützt.
- Diese Version des Connectors enthält außerdem Cloud Volumes ONTAP-Verbesserungen und On-Premises-ONTAP-Cluster-Verbesserungen.
  - "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"
  - "Die ONTAP-On-Premises-Cluster-Verbesserungen"

6. November 2022

Anschluss 3.9.23

- Ihre PAYGO-Abonnements und Jahresverträge für BlueXP können jetzt über das digitale Wallet angezeigt und gemanagt werden.

  "Hier erfahren Sie, wie Sie Ihre Abonnements verwalten"

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

  "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

November 2022

Einführung von BlueXP

NetApp BlueXP erweitert und verbessert die über Cloud Manager bereitgestellten Funktionen. BlueXP ist eine einheitliche Managementplattform, die eine Hybrid-Multi-Cloud-Erfahrung für Storage und Datenservices über On-Premises- und Cloud-Umgebungen hinweg bietet.

Unified Management

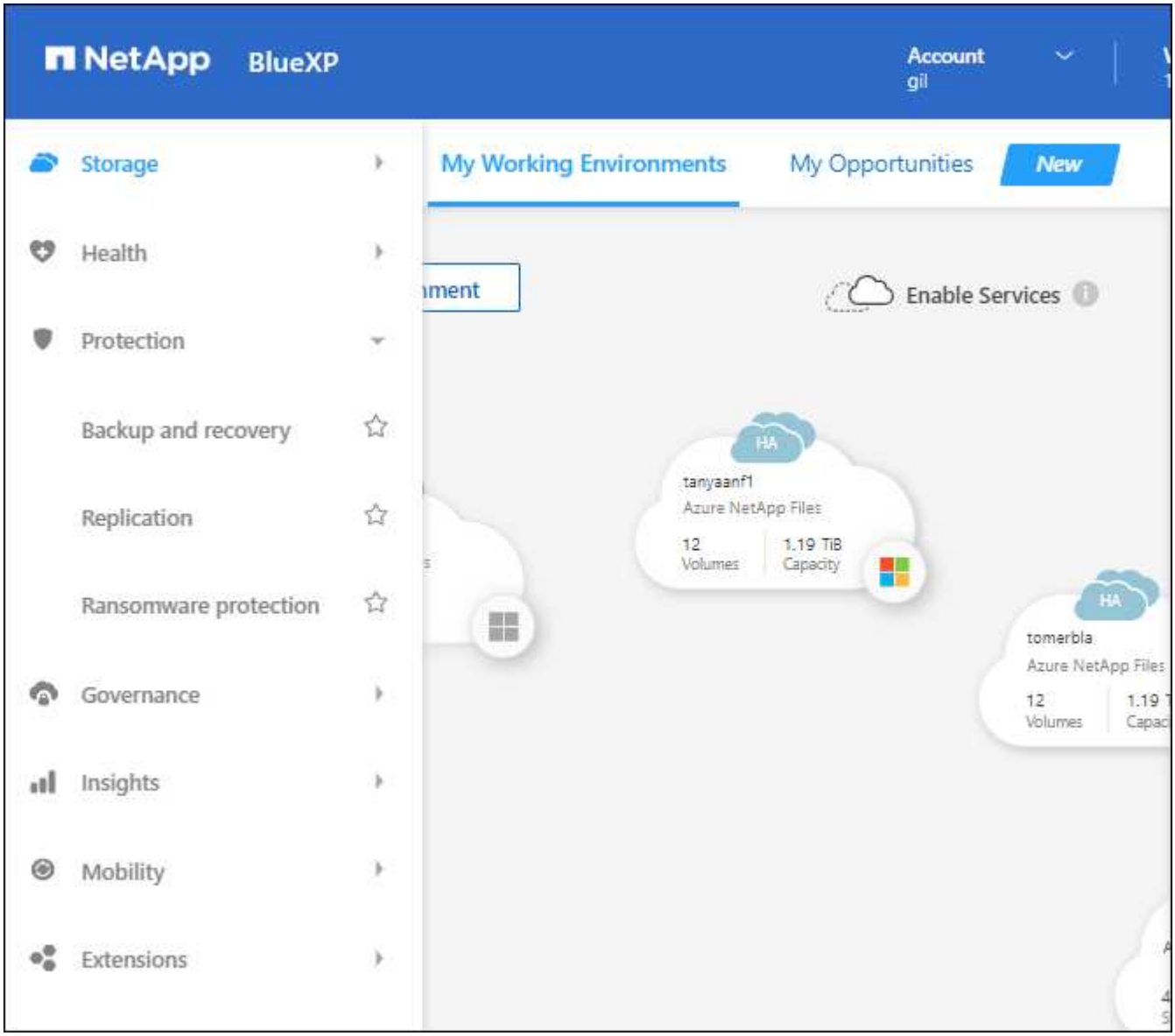
Mit BlueXP können Sie Ihre gesamten Storage- und Daten-Assets über eine einzige Benutzeroberfläche managen.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

"Weitere Informationen finden Sie auf der BlueXP-Website"

Neues Navigationsmenü

Im Navigationsmenü von BlueXP sind die Services nun nach Kategorien sortiert und nach ihrer Funktionalität benannt. Sie können beispielsweise aus der Kategorie **Schutz** auf BlueXP Backup und Recovery zugreifen.



Neue Produktintegrationen

- Sie können jetzt die Amazon S3-Buckets in den AWS-Konten verwalten, in denen der Connector installiert ist.
- Sie können jetzt mehr lokale Storage-Systeme wie E-Series und StorageGRID managen.
- Datenservices, die zuvor nur als Standalone-Service über eine separate UI genutzt werden können, wie etwa der BlueXP Digital Advisor (Active IQ), können jetzt genutzt werden.

Weitere Informationen .

- "Amazon S3 Buckets managen"
- "Management von E-Series Storage-Systemen"

- "Management von StorageGRID Storage-Systemen"
- "Erfahren Sie mehr über die Integration von Digital Advisor"

Aufforderung zum Aktualisieren der NSS-Anmeldeinformationen

Cloud Manager fordert Sie jetzt auf, die mit Ihren Accounts der NetApp Support Website verbundenen Anmeldeinformationen zu aktualisieren, wenn das mit Ihrem Konto verknüpfte Aktualisierungs-Token nach 3 Monaten abläuft. "Erfahren Sie, wie Sie NSS-Konten verwalten"

18. September 2022

Anschluss 3.9.22

- Wir haben den Connector Deployment Wizard erweitert, indem wir eine *in-Product Guide* hinzufügen, die Schritte zur Erfüllung der Mindestanforderungen für die Installation von Konnektor enthält: Berechtigungen, Authentifizierung und Netzwerke.
- Sie können nun einen NetApp Support-Fall direkt über Cloud Manager im **Support Dashboard** erstellen.

  "Erfahren Sie, wie Sie einen Fall erstellen".

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

  "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

31 Juli 2022

Anschluss 3.9.21

- Wir haben eine neue Methode eingeführt, um die vorhandenen Cloud-Ressourcen zu ermitteln, die Sie noch nicht in Cloud Manager verwalten.

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

  In dieser ersten Version können Sie mit My Opportunities vorhandene FSX für ONTAP Dateisysteme in Ihrem AWS-Konto entdecken.

  "Entdecken Sie FSX für ONTAP mithilfe von My Opportunities"

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

  "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

15 Juli 2022

Richtlinienänderungen

Wir haben die Dokumentation aktualisiert und die Cloud Manager Richtlinien direkt in den Dokumenten hinzugefügt. Das bedeutet, dass Sie nun die erforderlichen Berechtigungen für den Konnektor und Cloud Volumes ONTAP direkt neben den Schritten anzeigen können, wie Sie diese einrichten. Auf diese Richtlinien konnte bisher über eine Seite der NetApp Support Site zugegriffen werden.

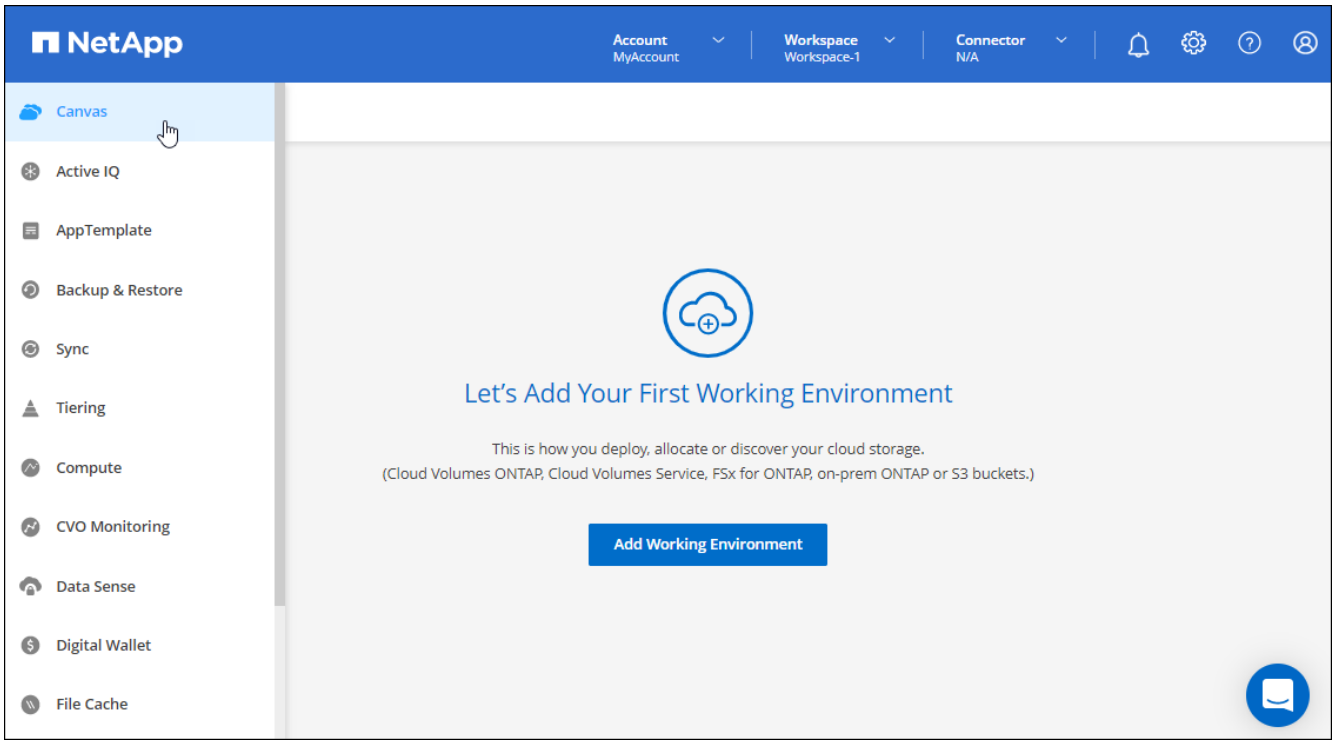
"Das Beispiel zeigt die AWS IAM-Rollenberechtigungen, die zum Erstellen eines Konnektors verwendet werden".

Außerdem haben wir eine Seite erstellt, die Links zu den einzelnen Richtlinien enthält. "Zeigen Sie die Berechtigungsübersicht für Cloud Manager an".

3 Juli 2022

Anschluss 3.9.20

- Jetzt haben wir eine neue Methode eingeführt, um auf die wachsende Liste von Funktionen in der Cloud Manager Benutzeroberfläche zu navigieren. Alle vertrauten Funktionen von Cloud Manager sind jetzt leicht zu finden, indem Sie den Mauszeiger über das linke Feld halten.



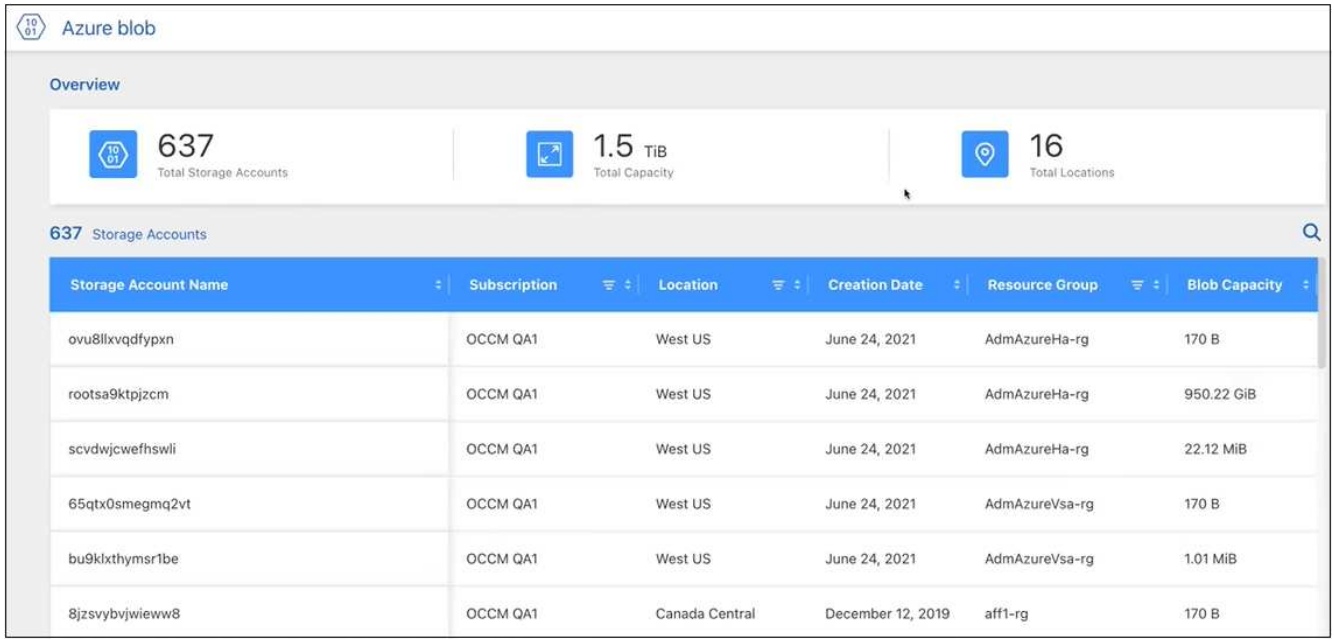
- Sie können Cloud Manager jetzt so konfigurieren, dass Sie Benachrichtigungen per E-Mail versenden, damit Sie über wichtige Systemaktivitäten informiert werden können, auch wenn Sie nicht im System angemeldet sind.

  "Weitere Informationen zu Überwachungsvorgängen in Ihrem Konto".

- Cloud Manager unterstützt jetzt Azure Blob Storage und Google Cloud Storage als Arbeitsumgebungen, ähnlich der Unterstützung von Amazon S3.

  Nach der Installation eines Connectors in Azure oder Google Cloud erkennt Cloud Manager jetzt automatisch Informationen über Azure Blob Storage in Ihrem Azure Abonnement oder Google Cloud Storage in dem Projekt, in dem der Connector installiert wird. Cloud Manager zeigt den Objekt-Storage als Arbeitsumgebung an, in der detailliertere Informationen angezeigt werden können.

  Hier ein Beispiel für eine Azure Blob-Arbeitsumgebung:



- Wir haben die Seite „Ressourcen“ für eine Amazon S3-Arbeitsumgebung neu gestaltet und ausführlichere Informationen zu S3-Buckets wie Kapazität, Verschlüsselungsdetails usw. bereitgestellt.
- Der Connector wird nun in folgenden Google Cloud Regionen unterstützt:
  - Madrid (europa-Südwest1)
  - Paris (europawest9)
  - Warschau (europa-Zentralin2)
- Der Connector wird nun in der Region Azure West US 3 unterstützt.

  "Hier finden Sie die vollständige Liste der unterstützten Regionen"

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

  "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"

28. Juni 2022

Loggen Sie sich mit NetApp Anmeldedaten ein

Wenn sich neue Benutzer bei Cloud Central anmelden, können sie jetzt die Option **mit NetApp** anmelden und sich mit ihren NetApp Support Site Anmeldedaten anmelden. Dies ist eine Alternative zur Eingabe einer E-Mail-Adresse und eines Kennworts.

> Vorhandene Anmeldungen, die eine E-Mail-Adresse und ein Passwort verwenden, müssen diese Anmeldemethode beibehalten. Die Option „mit NetApp anmelden“ ist für neue Benutzer verfügbar, die sich anmelden.

7. Juni 2022

Anschluss 3.9.19

- Der Connector wird nun in der Region AWS Jakarta unterstützt (AP-Südost-3).

- Der Connector wird nun in der Region Azure Brazil Southeast unterstützt.

  "Hier finden Sie die vollständige Liste der unterstützten Regionen"

- Diese Version des Connectors enthält außerdem Cloud Volumes ONTAP-Verbesserungen und On-Premises-ONTAP-Cluster-Verbesserungen.
  - "Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"
  - "Die ONTAP-On-Premises-Cluster-Verbesserungen"

12 Mai 2022

Patch-Anschluss 3.9.18

Wir haben den Connector aktualisiert, um Bug Fixes einzuführen. Die bemerkenswerteste Lösung ist ein Problem, das die Cloud Volumes ONTAP-Implementierung in Google Cloud beeinflusst, wenn der Connector in einer gemeinsamen VPC ausgeführt wird.

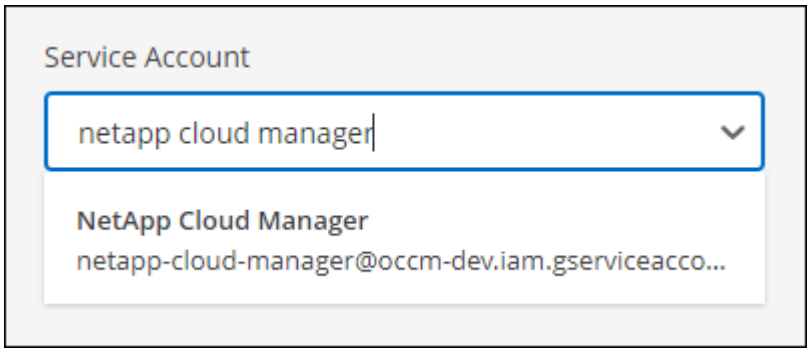
2 Mai 2022

Anschluss 3.9.18

- Der Connector wird nun in folgenden Google Cloud Regionen unterstützt:
  - Delhi (asien-Süd-2)
  - Melbourne (australien-Südheast2)
  - Mailand (europa-West8)
  - Santiago (southamerica-west1)

  "Hier finden Sie die vollständige Liste der unterstützten Regionen"

- Wenn Sie das Google Cloud-Servicekonto auswählen, das mit dem Connector verwendet werden soll, zeigt Cloud Manager jetzt die E-Mail-Adresse an, die mit jedem Dienstkonto verknüpft ist. Durch das Anzeigen der E-Mail-Adresse kann es leichter sein, zwischen Servicekonten, die denselben Namen haben, zu unterscheiden.



- Wir haben den Connector in Google Cloud auf einer VM-Instanz mit einem Betriebssystem zertifiziert, das unterstützt "Geschirmte VM-Funktionen"
- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen. "Erfahren Sie mehr über diese Verbesserungen"
- Für den Connector zur Implementierung von Cloud Volumes ONTAP sind neue AWS Berechtigungen

erforderlich.

Bei der Implementierung eines HA-Paars in einer einzelnen Verfügbarkeitszone (AZ) sind nun die folgenden Berechtigungen erforderlich, um eine AWS Spread-Placement-Gruppe zu erstellen:

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

Diese Berechtigungen sind nun erforderlich, um die Erstellung der Platzierungsgruppe durch Cloud Manager zu optimieren.

Stellen Sie unbedingt diese Berechtigungen für jeden Satz von AWS Zugangsdaten bereit, die Sie Cloud Manager hinzugefügt haben. "Sehen Sie sich die aktuelle IAM-Richtlinie für den Connector an".

3. April 2022

Anschluss 3.9.17

- Sie können jetzt einen Connector erstellen, indem Sie Cloud Manager eine IAM-Rolle übernehmen lassen, die Sie in Ihrer Umgebung eingerichtet haben. Diese Authentifizierungsmethode ist sicherer als die gemeinsame Nutzung eines AWS Zugriffsschlüssels und eines Geheimschlüssels.

  "Erfahren Sie, wie Sie einen Konnektor mithilfe einer IAM-Rolle erstellen".

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen. "Erfahren Sie mehr über diese Verbesserungen"

27 Februar 2022

Anschluss 3.9.16

- Wenn Sie einen neuen Connector in Google Cloud erstellen, zeigt Cloud Manager jetzt alle bestehenden Firewall-Richtlinien an. Zuvor wurden in Cloud Manager keine Richtlinien angezeigt, für die kein Ziel-Tag vorhanden war.
- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen. "Erfahren Sie mehr über diese Verbesserungen"

30 Januar 2022

Anschluss 3.9.15

Diese Version des Connectors enthält Cloud Volumes ONTAP-Verbesserungen. "Erfahren Sie mehr über diese Verbesserungen"

Januar 2022

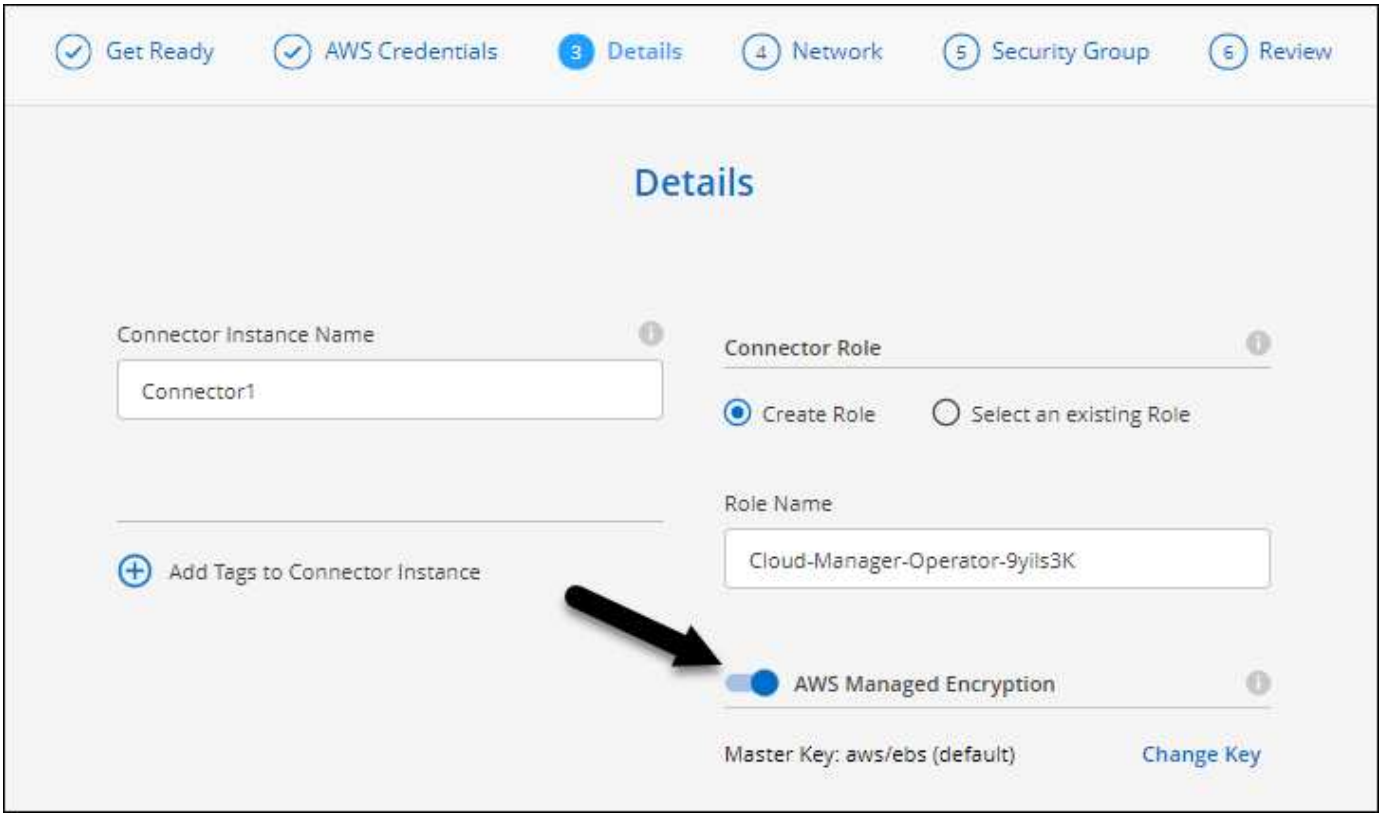
Verringerte Endpunkte für den Konnektor

Wir reduzieren die Anzahl der Endpunkte, die ein Connector kontaktieren muss, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu verwalten.

"Zeigen Sie die Liste der erforderlichen Endpunkte an"

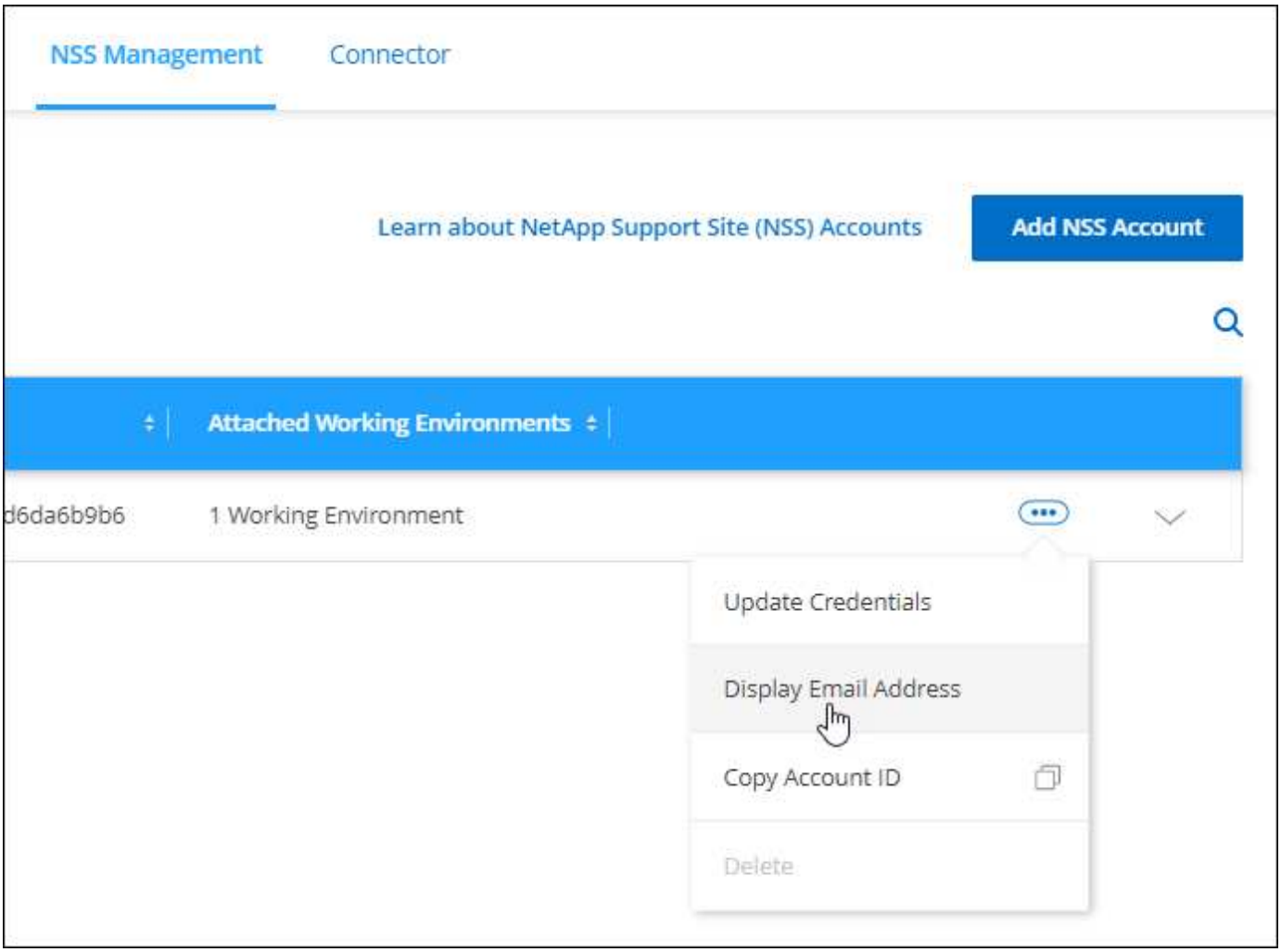
EBS-Festplattenverschlüsselung für den Connector

Wenn Sie einen neuen Connector in AWS über Cloud Manager implementieren, können Sie sich jetzt entscheiden, die EBS-Festplatten des Connectors über den Standard-Master-Schlüssel oder einen gemanagten Schlüssel zu verschlüsseln.



E-Mail-Adresse für NSS-Konten

Cloud Manager kann jetzt die E-Mail-Adresse anzeigen, die mit einem NetApp Support Site Konto verknüpft ist.



28. November 2021

Update für NetApp Support Site Accounts erforderlich

Ab Dezember 2021 verwendet NetApp jetzt Microsoft Azure Active Directory als Identitäts-Provider für speziell auf Support und Lizenzierung spezifische Authentifizierungs-Services. Aufgrund dieses Updates werden Sie von Cloud Manager aufgefordert, die Anmeldedaten für alle bereits hinzugefügten NetApp Support Site Konten zu aktualisieren.

Wenn Sie Ihr NSS-Konto noch nicht zu IDaaS migriert haben, müssen Sie zunächst das Konto migrieren und dann Ihre Zugangsdaten in Cloud Manager aktualisieren.

"Erfahren Sie mehr über die Verwendung von Microsoft Azure Active Directory für das Identitätsmanagement durch NetApp"

NSS-Konten für Cloud Volumes ONTAP ändern

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

"Erfahren Sie, wie Sie eine Arbeitsumgebung an ein anderes NSS-Konto anschließen".

4. November 2021

SOC 2 Typ 2-Zertifizierung

Ein unabhängiger, zertifizierter Wirtschaftsprüfer hat Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense und Cloud Backup (Cloud Manager Plattform) geprüft und bestätigt, dass sie SOC 2 Typ 2 Berichte basierend auf den entsprechenden Kriterien der Trust Services erstellt haben.

"SOC 2-Berichte von NetApp anzeigen".

Connector wird nicht mehr als Proxy unterstützt

Sie können den Cloud-Manageranschluss nicht mehr als Proxyserver verwenden, um AutoSupport-Nachrichten von Cloud Volumes ONTAP zu senden. Diese Funktion wurde entfernt und wird nicht mehr unterstützt. Sie müssen AutoSupport-Konnektivität über eine NAT-Instanz oder Proxy-Services Ihrer Umgebung bereitstellen.

"Erfahren Sie mehr über die Überprüfung von AutoSupport mit Cloud Volumes ONTAP"

31 Oktober 2021

Authentifizierung mit Service-Principal

Wenn Sie einen neuen Connector in Microsoft Azure erstellen, können Sie sich jetzt mit einem Azure-Dienstprincipal authentifizieren, anstatt mit den Azure-Konto-Anmeldedaten.

"Informieren Sie sich, wie Sie sich mit einem Azure-Service-Principal authentifizieren".

Verbesserung der Anmeldeinformationen

Die Credentials-Seite wurde neu gestaltet. Dies ist benutzerfreundlich und passt genau zu dem aktuellen Look and Feel der Cloud Manager-Oberfläche.

September 2021

Ein neuer Benachrichtigungsdienst wurde hinzugefügt

Der Benachrichtigungsservice wurde eingeführt, sodass Sie den Status der Cloud Manager Vorgänge anzeigen können, die Sie während Ihrer aktuellen Anmeldesitzung initiiert haben. Sie können überprüfen, ob der Vorgang erfolgreich war oder ob er fehlgeschlagen ist. "Erfahren Sie, wie Sie die Vorgänge in Ihrem Konto überwachen".

7 Juli 2021

Erweiterungen des Assistenten zum Hinzufügen von Konnektor

Wir haben den Assistenten **Connector** neu gestaltet, um neue Optionen hinzuzufügen und die Bedienung zu vereinfachen. Sie können nun Tags hinzufügen, eine Rolle angeben (für AWS oder Azure), ein Root-Zertifikat für einen Proxy-Server hochladen, Code für die Terraform-Automatisierung anzeigen, Fortschrittsdetails anzeigen und mehr.

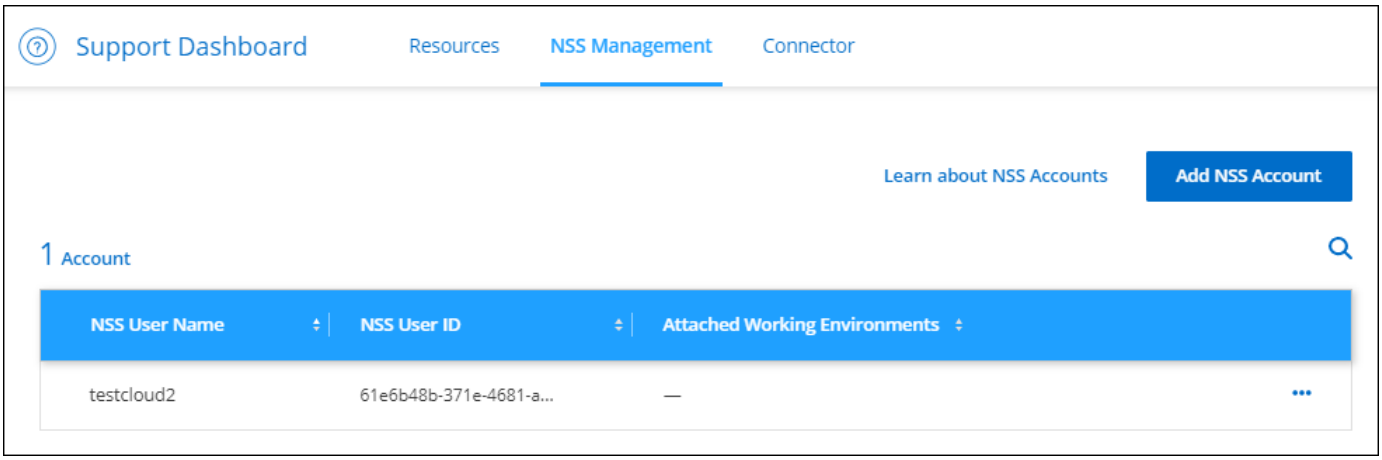
- "Connector in AWS erstellen"
- "Connector in Azure erstellen"

- "Erstellen Sie einen Connector in Google Cloud"

NSS Account-Management über das Support Dashboard

NSS-Konten (NetApp Support Site) werden jetzt über das Support-Dashboard gemanagt anstatt über das Menü „Einstellungen“. Durch diese Änderung finden und managen Sie alle Support-Informationen einfacher über eine zentrale Stelle.

"Erfahren Sie, wie Sie NSS-Konten verwalten".



5 Mai 2021

Konten in der Zeitleiste

In der Zeitleiste in Cloud Manager werden jetzt Aktionen und Ereignisse im Zusammenhang mit der Kontoverwaltung angezeigt. Zu den Aktionen gehören u. a. die Verknüpfung von Benutzern, die Erstellung von Arbeitsbereichen und die Erstellung von Connectors. 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.

"Erfahren Sie, wie Sie den Zeitplan für den Service für die Mandantenfähigkeit filtern".

11. April 2021

API-Aufrufe direkt an Cloud Manager

Wenn Sie einen Proxy-Server konfiguriert haben, können Sie nun eine Option aktivieren, mit der Sie API-Aufrufe direkt an Cloud Manager senden können, ohne über den Proxy zu gehen. Diese Option wird mit Connectors unterstützt, die in AWS oder in Google Cloud ausgeführt werden.

"Erfahren Sie mehr über diese Einstellung".

Benutzer des Servicekontos

Sie können jetzt ein Dienstkonto-Benutzer erstellen.

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

aus der Cloud zu generieren.

"Erfahren Sie mehr über die Verwendung von Servicekonten".

Private Vorschauen

Private Vorschauen in Ihrem Konto können Sie jetzt auf neue NetApp Cloud-Services zugreifen, sobald diese in Cloud Manager als Vorschau verfügbar gemacht werden.

"Weitere Informationen zu dieser Option".

Drittanbieter-Services

Sie haben auch die Möglichkeit, dass Drittanbieterservices in Ihrem Konto Zugriff auf in Cloud Manager verfügbare Drittanbieter-Services erhalten.

"Weitere Informationen zu dieser Option".

8 März 2021

Dieses Update enthält Verbesserungen an verschiedenen Funktionen und Services.

Verbesserungen von Cloud Volumes ONTAP

Diese Version von Cloud Manager enthält Verbesserungen am Management von Cloud Volumes ONTAP.

Erweiterung bei allen Cloud-Providern verfügbar

Cloud Manager kann jetzt Cloud Volumes ONTAP 9.9 implementieren und managen.

"Erfahren Sie mehr über die neuen Funktionen in dieser Version von Cloud Volumes ONTAP".

Verbesserungen in AWS verfügbar

- Die Implementierung von Cloud Volumes ONTAP 9.8 ist nun in der Umgebung der AWS Commercial Cloud Services (C2S) möglich.

  "Erfahren Sie, wie Sie mit C2S beginnen"

- Cloud Manager hat Ihnen immer die Möglichkeit gegeben, Cloud Volumes ONTAP-Daten mit dem AWS Key Management Service (KMS) zu verschlüsseln. Ab Cloud Volumes ONTAP 9.9 werden Daten auf EBS-Festplatten und auf S3 abgestufte Daten verschlüsselt, wenn Sie sich für einen vom Kunden gemanagten CMK entscheiden. Bisher wurden nur EBS-Daten verschlüsselt.

  Beachten Sie, dass Sie für die Cloud Volumes ONTAP IAM-Rolle Zugriff zur Verwendung des CMK bereitstellen müssen.

  "Erfahren Sie mehr über die Einrichtung des AWS KMS mit Cloud Volumes ONTAP"

Erweiterung in Azure verfügbar

Sie können Cloud Volumes ONTAP 9.8 jetzt im Azure Department of Defense (DoD) Impact Level 6 (IL6) implementieren.

Verbesserungen in Google Cloud verfügbar

- In Google Cloud haben wir die Anzahl der für Cloud Volumes ONTAP 9.8 und höher erforderlichen IP-Adressen reduziert. Standardmäßig ist eine niedrigere IP-Adresse erforderlich (wir vereinheitlichen die Intercluster LIF mit der Node-Management-LIF). Darüber hinaus besteht die Möglichkeit, bei Verwendung der API die Erstellung der SVM-Management-LIF zu überspringen, was den Bedarf an einer zusätzlichen IP-Adresse verringert.

  "Informieren Sie sich in Google Cloud über die IP-Adressanforderungen"

- Durch die Implementierung eines Cloud Volumes ONTAP HA-Paars in Google Cloud haben Sie nun die Möglichkeit, gemeinsame VPCs für VPC-1, VPC-2 und VPC-3 auszuwählen. Bisher könnte nur die VPC-0 eine gemeinsame VPC sein. Diese Änderung wird unterstützt durch Cloud Volumes ONTAP 9.8 und höher.

  "Erfahren Sie mehr über die Netzwerkanforderungen von Google Cloud"

Connector-Verbesserungen

- Cloud Manager benachrichtigt jetzt Admin-Benutzer per E-Mail, wenn ein Connector nicht ausgeführt wird.

  Wenn Ihre Connectors stets einsatzbereit sind, können Sie die optimale Verwaltung von Cloud Volumes ONTAP und anderen NetApp Cloud-Diensten sicherstellen.

- Cloud Manager zeigt jetzt eine Benachrichtigung an, wenn Sie den Instanztyp für den Connector ändern müssen.

  Wenn Sie den Instanztyp ändern, können Sie die neuen Funktionen und Funktionen verwenden, die Ihnen derzeit fehlen.

Verbesserungen von Cloud Sync

- Cloud Sync unterstützt jetzt Synchronisierungsbeziehungen zwischen ONTAP S3 Storage und SMB-Servern:
  - Von ONTAP S3 Storage zu einem SMB-Server
  - Ein SMB-Server für ONTAP S3 Storage

    "Anzeigen von unterstützten Synchronisierungsbeziehungen"

- Mit Cloud Sync können Sie die Konfiguration einer Datenbrokergruppe jetzt direkt über die Benutzeroberfläche vereinheitlichen.

  Es wird nicht empfohlen, die Konfiguration selbst zu ändern. Sie sollten sich mit NetApp beraten lassen, um zu erfahren, wann die Konfiguration geändert werden kann und wie Sie sie ändern können.

  "Erfahren Sie mehr über die Definition einer einheitlichen Konfiguration"

Cloud Tiering-Verbesserungen

- Beim Tiering in Google Cloud Storage können Sie eine Lebenszyklusregel anwenden, damit die Tiering-Daten nach 30 Tagen von der Standard-Storage-Klasse in den kostengünstigeren Nearline-, Coldline- oder Archivspeicher überführt werden.
- Es wird jetzt Cloud Tiering angezeigt, wenn Sie noch nicht erkannte On-Premises-ONTAP-Cluster haben, sodass Sie sie Cloud Manager hinzufügen können, um Tiering oder andere Services auf diesen Clustern

zu aktivieren.

"Erfahren Sie, wie Sie diese zusätzlichen Cluster erkennen"

Verbesserungen von Azure NetApp Files

Sie sind nun in der Lage, das Service-Level für ein Volume dynamisch zu ändern, um die Workload-Anforderungen zu erfüllen und die Kosten zu optimieren. Das Volume wird in den anderen Kapazitäts-Pool verschoben, ohne dass sich dies auf das Volume auswirkt. "Weitere Informationen ."

9 Februar 2021

Verbesserungen am Support Dashboard

Wir haben das Support Dashboard aktualisiert, damit Sie Ihre Zugangsdaten für die NetApp Support Website hinzufügen können. Damit registrieren Sie sich für den Support. Sie können auch einen NetApp Support-Fall direkt über das Dashboard initiieren. Klicken Sie einfach auf das Hilfesymbol und dann auf **Support**.

Bekannte Einschränkungen

Bekannte Einschränkungen identifizieren Plattformen, Geräte oder Funktionen, die von dieser Version des Produkts nicht unterstützt werden oder nicht korrekt mit dem Produkt zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Diese Einschränkungen gelten insbesondere für die Einrichtung und Administration von BlueXP: Der Connector, die SaaS-Plattform und vieles mehr.

Einschränkungen an den Anschlüssen

Transparente Proxyserver werden nicht unterstützt

BlueXP unterstützt in Verbindung mit dem Connector keine transparenten Proxyserver.

"Erfahren Sie mehr über die Verwendung eines Proxy-Servers mit dem Connector".

Möglicher Konflikt mit IP-Adressen im Bereich 172

BlueXP implementiert den Connector mit zwei Schnittstellen, die IP-Adressen in den Bereichen 172.17.0.0/16 und 172.18.0.0/16 haben.

Wenn Ihr Netzwerk über ein Subnetz verfügt, das mit einem dieser Bereiche konfiguriert ist, können Verbindungsfehler von BlueXP auftreten. Beispielsweise schlägt die Erkennung von lokalen ONTAP Clustern in BlueXP fehl.

Siehe Knowledge Base-Artikel "BlueXP Connector IP-Konflikt mit vorhandenem Netzwerk" Anweisungen zum Ändern der IP-Adresse der Schnittstellen des Connectors.

SSL-Entschlüsselung wird nicht unterstützt

BlueXP unterstützt keine Firewall-Konfigurationen, bei denen die SSL-Entschlüsselung aktiviert ist. Wenn die SSL-Entschlüsselung aktiviert ist, werden Fehlermeldungen in BlueXP angezeigt, und die Connector-Instanz wird als inaktiv angezeigt.

Um die Sicherheit zu erhöhen, haben Sie die Möglichkeit "Installieren eines von einer Zertifizierungsstelle (CA) signierten HTTPS-Zertifikats".

Leere Seite beim Laden der lokalen Benutzeroberfläche

Wenn Sie die webbasierte Konsole, die auf einem Connector ausgeführt wird, laden, wird die Schnittstelle manchmal nicht angezeigt, und Sie erhalten nur eine leere Seite.

Dieses Problem bezieht sich auf ein Caching-Problem. Die Problemumgehung besteht darin, eine Inkognito- oder private Webbrowser-Sitzung zu verwenden.

Freigegebene Linux-Hosts werden nicht unterstützt

Der Connector wird nicht von einer VM unterstützt, die gemeinsam mit anderen Anwendungen genutzt wird. Die VM muss der Connector-Software zugewiesen sein.

Agenten und Erweiterungen von Drittanbietern

Agenten von Drittanbietern oder VM-Erweiterungen werden auf der Connector-VM nicht unterstützt.

Los geht’s

Lernen Sie die Grundlagen kennen

Erfahren Sie mehr über BlueXP

Mit NetApp BlueXP steht Ihrem Unternehmen eine einzelne Managementplattform zur Verfügung, mit der Sie Ihre Daten über Ihre On-Premises- und Cloud-Umgebungen hinweg erstellen, schützen und regeln können. Die BlueXP SaaS-Plattform umfasst Services für Storage-Management, Datenmobilität, Datensicherung sowie Datenanalyse und -Kontrolle. Managementfunktionen werden über eine webbasierte Konsole und APIs bereitgestellt.

Funktionen

Die BlueXP Plattform umfasst vier Hauptsäulen des Datenmanagements: Storage, Mobilität, Sicherung sowie Analyse und Kontrolle.

Storage

Erkennen, implementieren und managen Sie Storage in AWS, Azure, Google Cloud oder vor Ort.

- Einrichtung und Verwendung "Cloud Volumes ONTAP" Für effizientes, Cloud-übergreifendes Multi-Protokoll-Datenmanagement
- Cloud-File-Storage-Services einrichten und verwenden:
  - "Azure NetApp Dateien"
  - "Amazon FSX für ONTAP"
  - "Cloud Volumes Service für Google Cloud"
- Erkennung und Management "On-Premises-Storage":
  - E-Series Systeme
  - ONTAP Cluster
  - StorageGRID Systeme

Mobilität

Daten werden durch Synchronisierung, Kopieren, Tiering und Caching von Daten dorthin verschoben, wo sie benötigt werden.

- "Kopieren und Synchronisieren"
- "Edge-Caching"
- "Tiering"

Darstellt

Automatisierte Sicherungsmechanismen schützen Daten vor Datenverlust, ungeplanten Ausfällen, Ransomware und anderen Cyberbedrohungen.

- "Backup und Recovery"
- "Replizierung"

- "Datensicherung für Kubernetes-Workloads"

Analyse und Kontrolle

Mit Tools können Sie Ihren Storage und Ihre Infrastruktur überwachen, zuordnen und optimieren. Nützliche Informationen für die Optimierung von Storage-Zustand, Ausfallsicherheit und Wirtschaftlichkeit

- "Klassifizierung"
- "Digitaler Berater"
- "Wirtschaftliche Effizienz"
- "Operative Ausfallsicherheit"

"Erfahren Sie mehr darüber, wie Sie BlueXP für Ihr Unternehmen einsetzen können"

Unterstützte Cloud-Provider

Mit BlueXP können Sie Cloud-Storage managen und Cloud-Services in Amazon Web Services, Microsoft Azure und Google Cloud nutzen.

Kosten

Die Preise für BlueXP hängen von den Leistungen ab, die Sie verwenden möchten. "Weitere Informationen zu den Preisen für BlueXP"

Funktionsweise von BlueXP

BlueXP umfasst eine webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird, Konten für Mandantenfähigkeit und Connectors, die Arbeitsumgebungen managen und BlueXP Cloud-Services aktivieren.

Software-as-a-Service

Auf BlueXP kann über eine zugegriffen werden "Webbasierte Konsole" Und APIs. Dank SaaS-Erfahrung können Sie automatisch auf die neuesten Funktionen zugreifen, sobald sie veröffentlicht wurden, und ganz einfach zwischen Ihren BlueXP Konten und Connectors wechseln.

BlueXP-Konto

Wenn Sie sich zum ersten Mal bei BlueXP anmelden, werden Sie aufgefordert, ein *BlueXP Konto* zu erstellen. Dieses Konto bietet Mandantenfähigkeit und ermöglicht es Ihnen, Benutzer und Ressourcen in isolierten Arbeitsbereichen zu organisieren_.

"Hier erfahren Sie mehr über Accounts".

Anschlüsse

Für den Einstieg in BlueXP benötigen Sie keinen Connector, aber Sie müssen einen Connector erstellen, mit dem Sie alle BlueXP Funktionen und Services nutzen können. Ein Connector ermöglicht Ihnen das Management von Ressourcen und Prozessen in Ihren On-Premises- und Cloud-Umgebungen. Sie ist erforderlich, um Arbeitsumgebungen (z. B. Cloud Volumes ONTAP und lokale ONTAP-Cluster) zu managen und viele BlueXP Datenservices zu nutzen.

"Erfahren Sie mehr über Steckverbinder".

Eingeschränkter Modus und privater Modus

BlueXP wird auch in Umgebungen mit Einschränkungen bei Sicherheit und Konnektivität unterstützt. Sie können den *Restricted Mode* oder *Private Mode* verwenden, um die Outbound-Konnektivität zur BlueXP SaaS-Ebene zu beschränken.

"Weitere Informationen zu den BlueXP Implementierungsmodi".

SOC 2 Typ 2-Zertifizierung

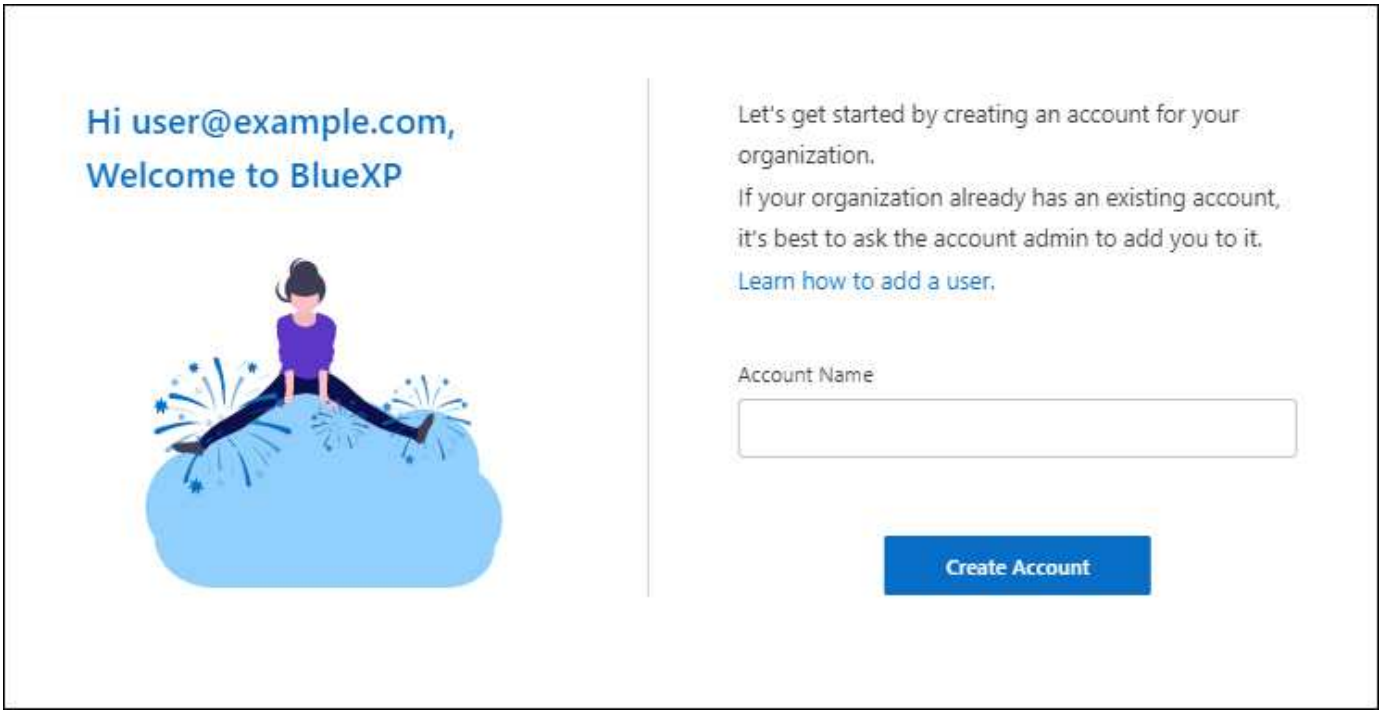
Ein unabhängiger zertifizierter Wirtschaftsprüfer und Wirtschaftsprüfer prüfte BlueXP und bestätigte, dass es SOC 2 Typ 2-Berichte basierend auf den geltenden Trust Services-Kriterien erreichte.

"SOC 2-Berichte von NetApp anzeigen"

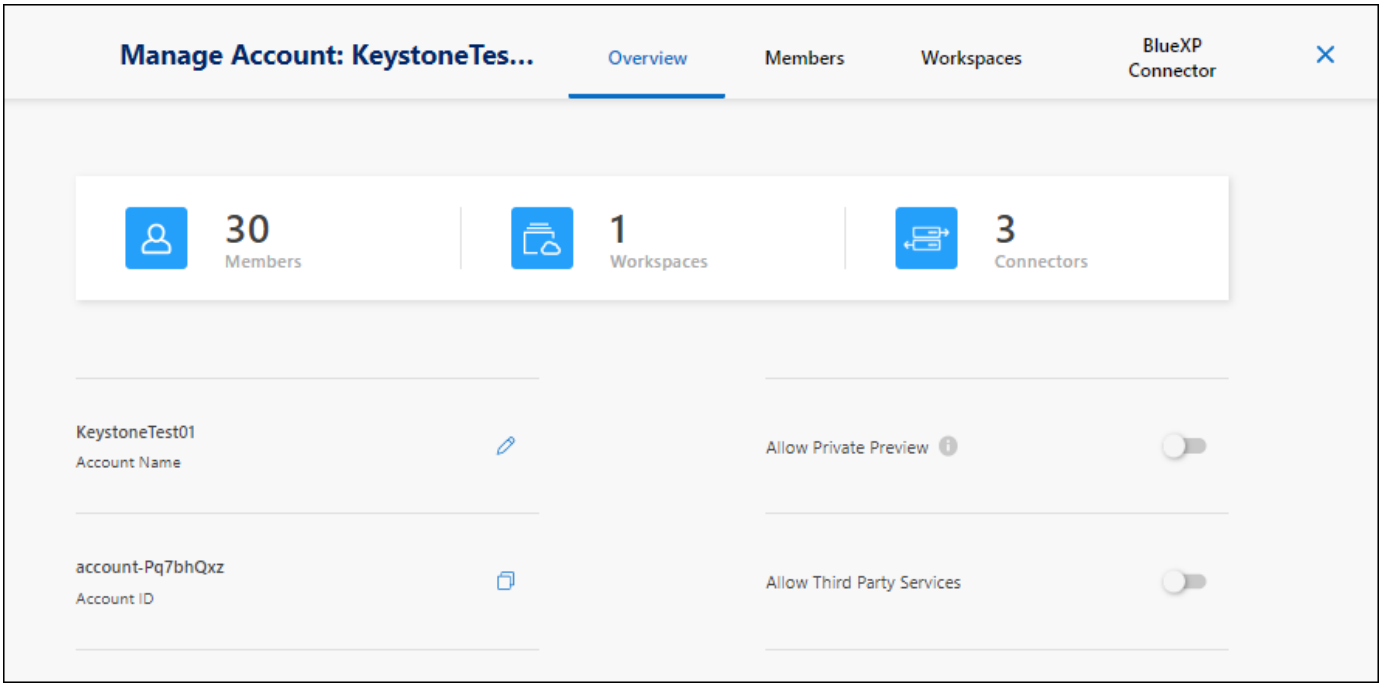
Mehr zu BlueXP Accounts

Ein *BlueXP Konto* bietet Mandantenfähigkeit für Ihr Unternehmen, damit Sie Benutzer und Ressourcen in isolierten *Workspaces* organisieren können. Eine Gruppe von Benutzern kann beispielsweise Cloud Volumes ONTAP-Arbeitsumgebungen in einem Arbeitsbereich bereitstellen und verwalten, der für Benutzer, die Arbeitsumgebungen in einem anderen Arbeitsbereich verwalten, nicht sichtbar ist.

Wenn Sie zum ersten Mal auf BlueXP zugreifen, werden Sie aufgefordert, ein Konto auszuwählen oder zu erstellen. Wenn Sie noch kein Konto haben, wird beispielsweise der folgende Bildschirm angezeigt:



BlueXP-Kontoadministratoren können dann die Einstellungen für dieses Konto ändern, indem sie Benutzer (Mitglieder), Arbeitsbereiche und Connectors verwalten:



"Erfahren Sie, wie Sie Ihr BlueXP Konto verwalten".

Bereitstellungsmodi

BlueXP bietet für Ihr Konto die folgenden Implementierungsmodi: Standardmodus, eingeschränkter Modus und privater Modus. Diese Modi unterstützen Umgebungen mit unterschiedlichen Sicherheits- und Konnektivitätsbeschränkungen.

"Weitere Informationen zu den BlueXP Implementierungsmodi".

Mitglieder

Mitglieder sind BlueXP Benutzer, die Sie mit Ihrem BlueXP Konto verknüpfen. Wenn Sie einen Benutzer mit einem Konto und einem oder mehreren Arbeitsbereichen in diesem Konto verknüpfen, können diese Benutzer Arbeitsumgebungen in BlueXP erstellen und verwalten.

Wenn Sie einen Benutzer zuordnen, weisen Sie ihm eine Rolle zu:

- *Account Admin*: Kann jede Aktion in BlueXP ausführen.
- *Workspace Admin*: Kann Ressourcen im zugewiesenen Arbeitsbereich erstellen und verwalten.
- *Compliance Viewer*: Kann nur Compliance-Informationen für die BlueXP-Klassifizierung anzeigen und Berichte für Arbeitsbereiche generieren, auf die sie zugreifen dürfen.

"Hier erfahren Sie mehr über diese Rollen".

Arbeitsbereiche

In BlueXP isoliert ein Workspace eine beliebige Anzahl von „ Arbeitsumgebungen“ von anderen Benutzern im Konto. Workspace-Administratoren können nicht auf die Arbeitsumgebungen in einem Arbeitsbereich zugreifen, es sei denn, der Kontoadministrator ordnet den Administrator diesem Arbeitsbereich zu.

Eine Arbeitsumgebung ist ein Storage-System. Beispiel:

- Ein Cloud Volumes ONTAP System
- Einem lokalen ONTAP Cluster erhalten
- Einen Kubernetes-Cluster erstellen

"Erfahren Sie, wie Sie einen Arbeitsbereich hinzufügen".

Anschlüsse

Mit einem Connector führen Sie die Aktionen aus, die BlueXP für das Management der Dateninfrastruktur benötigt. Der Connector wird auf einer virtuellen Maschineninstanz ausgeführt, die Sie in Ihrem Cloud-Provider oder auf einem von Ihnen konfigurierten On-Premises-Host bereitstellen.

Sie können einen Connector mit mehr als einem BlueXP Service verwenden. Wenn Sie beispielsweise einen Connector zum Management von Cloud Volumes ONTAP verwenden, können Sie diesen Connector mit einem anderen Service wie BlueXP Tiering verwenden.

"Erfahren Sie mehr über Steckverbinder".

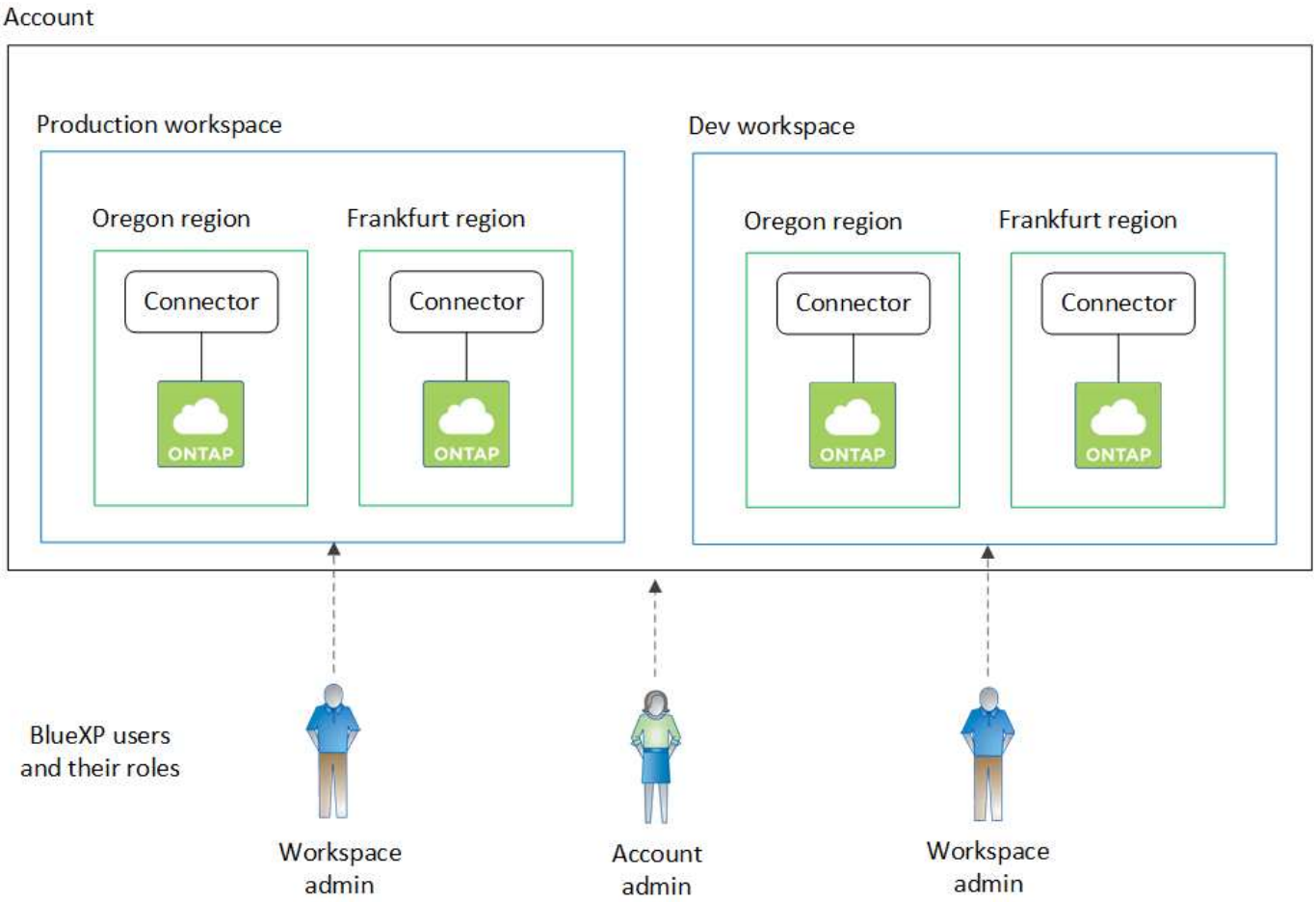
Beispiele

In den folgenden Beispielen wird veranschaulicht, wie Sie Ihre Konten einrichten könnten.

> In beiden nachfolgenden Beispielbildern haben Connector und Cloud Volumes ONTAP Systeme noch nicht wirklich *in* dem BlueXP Konto - sie werden in einem Cloud-Provider ausgeführt. Dies ist eine konzeptionelle Darstellung der Beziehung zwischen den einzelnen Komponenten.

Mehrere Arbeitsbereiche

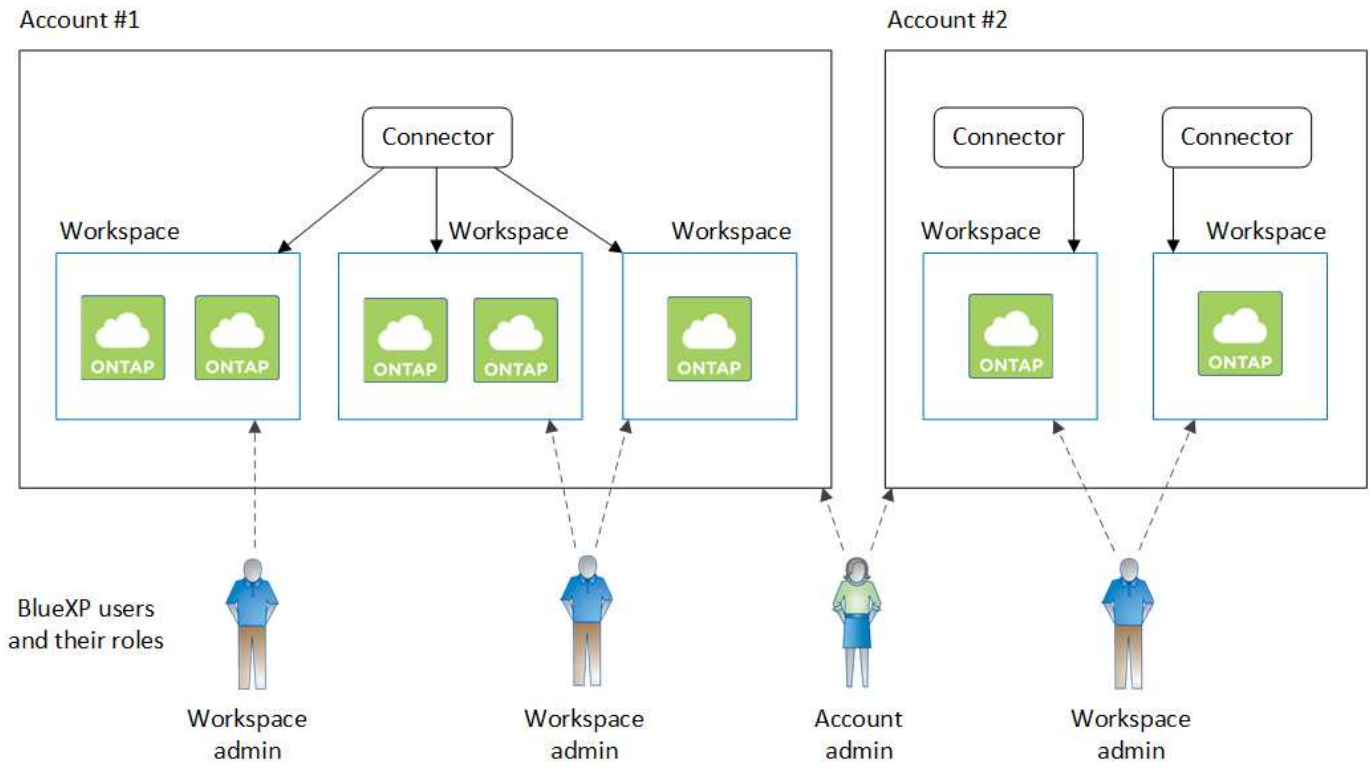
Das folgende Beispiel zeigt ein Konto, das zwei Arbeitsbereiche zum Erstellen isolierter Umgebungen verwendet. Der erste Arbeitsbereich ist für eine Produktionsumgebung und der zweite für eine Entwicklungsumgebung.



Mehrere Konten

Das folgende Beispiel zeigt die höchste Mandantenfähigkeitsstufe durch die Verwendung von zwei separaten BlueXP Konten. So kann ein Service Provider beispielsweise BlueXP in einem Konto für die Bereitstellung von Services für seine Kunden nutzen und gleichzeitig einen anderen Account für die Disaster Recovery einer seiner Geschäftsbereiche verwenden.

Beachten Sie, dass Konto 2 zwei separate Anschlüsse enthält. Dies kann passieren, wenn Systeme in verschiedenen Regionen oder separaten Cloud-Providern vorhanden sind.



Erfahren Sie mehr über Steckverbinder

A *Connector* ist die NetApp Software, die in Ihrem Cloud-Netzwerk oder Ihrem On-Premises-Netzwerk ausgeführt wird. Sie führt die Aktionen aus, die BlueXP für das Management der Dateninfrastruktur benötigt. Der Connector fragt fortlaufend die BlueXP SaaS-Ebene nach möglichen Aktionen ab. Für den Einstieg in BlueXP benötigen Sie keinen Connector, aber Sie müssen einen Connector erstellen, mit dem Sie alle BlueXP Funktionen und Services nutzen können.

Was Sie ohne einen Connector tun können

Für den Einstieg in BlueXP ist kein Connector erforderlich. Sie können mehrere Funktionen und Services in BlueXP nutzen, ohne jemals einen Connector zu erstellen.

Ohne Connector können Sie die folgenden BlueXP Funktionen und Services nutzen:

- Erstellung der Arbeitsumgebung von Amazon FSX for NetApp ONTAP

  Obwohl der Connector nicht zum Erstellen einer Arbeitsumgebung erforderlich ist, ist er für die Erstellung und das Management von Volumes, die Replizierung von Daten und die Integration von FSX für ONTAP mit Services wie der BlueXP Klassifizierung und der BlueXP Kopier- und Synchronisierungsfunktion erforderlich.

- Automatisierungsskatalog
- Azure NetApp Dateien

  Für die Einrichtung und das Management von Azure NetApp Files ist kein Connector erforderlich, aber für die Suche nach Azure NetApp Files Daten ist ein Connector erforderlich.

- Cloud Volumes Service für Google Cloud
- Kopieren und Synchronisieren
- Digitaler Berater
- Digitale Brieftasche

  In fast allen Fällen können Sie der Digital Wallet ohne Connector eine Lizenz hinzufügen.

  Zum Hinzufügen einer Lizenz zur digitalen Brieftasche ist nur ein Connector erforderlich, wenn Cloud Volumes ONTAP *Node-based* Lizenzen verwendet werden. In diesem Fall ist ein Connector erforderlich, da die Daten aus den auf Cloud Volumes ONTAP-Systemen installierten Lizenzen stammen.

- Direkte Erkennung von ONTAP Clustern vor Ort

  Ein Connector ist zwar nicht für die direkte Erkennung eines lokalen ONTAP-Clusters erforderlich, jedoch ist ein Connector erforderlich, wenn Sie zusätzliche BlueXP-Funktionen nutzen möchten.

  "Weitere Informationen zu den Wiederauffindungs- und Managementoptionen für lokale ONTAP Cluster"

- Nachhaltigkeit

Wenn ein Stecker erforderlich ist

Wenn Sie BlueXP im Standardmodus verwenden, ist für die folgenden Funktionen und Services in BlueXP ein Connector erforderlich:

- Managementfunktionen von Amazon FSX für ONTAP
- Amazon S3 Storage
- Azure Blob Storage
- Backup und Recovery
- Klassifizierung
- Cloud Volumes ONTAP
- Disaster Recovery
- E-Series Systeme
- Wirtschaftliche Effizienz [1]
- Edge-Caching
- Google Cloud Storage Buckets
- Kubernetes-Cluster
- Migrationsberichte
- On-Premises-ONTAP-Cluster-Integration in BlueXP-Datenservices
- Ausfallsicherheit der Betriebsabläufe [1]
- Schutz durch Ransomware
- StorageGRID Systeme
- Tiering
- Volume-Caching

[1] während Sie ohne Connector auf diese Dienste zugreifen können, ist ein Connector erforderlich, um Aktionen von den Diensten zu initiieren.

Ein Connector ist erforderlich, um BlueXP im eingeschränkten Modus oder im privaten Modus zu verwenden.

Die Anschlüsse müssen jederzeit betriebsbereit sein

Anschlüsse sind ein grundlegender Bestandteil der Service-Architektur von BlueXP. Es liegt in Ihrer Verantwortung sicherzustellen, dass die entsprechenden Steckverbinder jederzeit betriebsbereit und zugänglich sind. Während der Service darauf ausgelegt ist, kurze Ausfälle der Connector-Verfügbarkeit zu überwinden, müssen Sie bei Bedarf sofort Maßnahmen ergreifen, um Infrastrukturausfälle zu beheben.

Diese Dokumentation unterliegt der EULA. Wenn das Produkt nicht in Übereinstimmung mit der Dokumentation betrieben wird, können die Funktionalität und der Betrieb des Produkts sowie Ihre Rechte im Rahmen der EULA beeinträchtigt werden.

Auswirkungen auf Cloud Volumes ONTAP

Ein Konnektor ist eine wichtige Komponente für den Zustand und Betrieb von Cloud Volumes ONTAP. Wenn ein Connector heruntergefahren wird, werden Cloud Volumes ONTAP PAYGO-Systeme und kapazitätsbasierte BYOL-Systeme heruntergefahren, nachdem die Kommunikation mit einem Connector über einen Zeitraum von mehr als 14 Tagen unterbrochen wurde. Dies geschieht, weil der Connector jeden Tag die Lizenzierung auf dem System aktualisiert.

Wenn Ihr Cloud Volumes ONTAP System über eine Node-basierte BYOL-Lizenz verfügt, wird das System nach 14 Tagen weiter ausgeführt, da die Lizenz auf dem Cloud Volumes ONTAP System installiert wird.

Unterstützte Standorte

Ein Connector wird an folgenden Stellen unterstützt:

- Amazon Web Services
- Microsoft Azure

  Ein Connector in Azure sollte in derselben Azure-Region wie die von ihm gemanagten Cloud Volumes ONTAP-Systeme oder in der bereitgestellt werden "Azure Region Paar" Für die Cloud Volumes ONTAP Systeme. Diese Anforderung stellt sicher, dass eine Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Storage-Konten verwendet wird. "Erfahren Sie, wie Cloud Volumes ONTAP einen privaten Azure Link nutzt"

- Google Cloud

  Wenn Sie BlueXP Services in Verbindung mit Google Cloud nutzen möchten, müssen Sie einen Connector verwenden, der in Google Cloud ausgeführt wird.

- Vor Ort

Eingeschränkter Modus und privater Modus

Um BlueXP im eingeschränkten oder privaten Modus zu verwenden, starten Sie mit BlueXP. Installieren Sie dazu den Connector und greifen dann auf die Benutzeroberfläche zu, die lokal auf dem Connector ausgeführt wird.

"Weitere Informationen zu BlueXP Implementierungsmodi".

So erstellen Sie einen Konnektor

Ein BlueXP Kontoadministrator kann einen Connector direkt aus BlueXP, aus dem Marketplace Ihres Cloud-Providers oder durch manuelle Installation der Software auf Ihrem eigenen Linux-Host erstellen. Der Einstieg hängt davon ab, ob Sie BlueXP im Standardmodus, im eingeschränkten Modus oder im privaten Modus nutzen.

- "Weitere Informationen zu BlueXP Implementierungsmodi"
- "Einstieg in BlueXP im Standardmodus"
- "Einstieg in BlueXP im eingeschränkten Modus"
- "Starten Sie mit BlueXP im privaten Modus"

Berechtigungen

Um den Connector direkt aus BlueXP zu erstellen, sind spezielle Berechtigungen erforderlich, für die Connector-Instanz selbst sind weitere Berechtigungen erforderlich. Wenn Sie den Connector in AWS oder Azure direkt aus BlueXP erstellen, erstellt BlueXP den Connector mit den entsprechenden Berechtigungen.

Wenn Sie BlueXP im Standardmodus verwenden, hängt die Art und Weise, wie Sie Berechtigungen bereitstellen, davon ab, wie Sie den Connector erstellen möchten.

Weitere Informationen zum Einrichten von Berechtigungen finden Sie unter:

- Standardmodus
  - "Installationsoptionen für Konnektoren in AWS"
  - "Optionen für die Connector-Installation in Azure"
  - "Connector-Installationsoptionen in Google Cloud"
  - "Cloud-Berechtigungen für On-Premises-Implementierungen einrichten"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

Auf den folgenden Seiten können Sie die genauen Berechtigungen anzeigen, die der Connector für den täglichen Betrieb benötigt:

- "Erfahren Sie, wie der Connector AWS-Berechtigungen nutzt"
- "Erfahren Sie, wie der Connector Azure-Berechtigungen nutzt"
- "Erfahren Sie, wie der Connector Google Cloud-Berechtigungen nutzt"

Connector-Upgrades

Wir aktualisieren die Connector-Software in der Regel jeden Monat, um neue Funktionen einzuführen und Stabilitätsverbesserungen zu ermöglichen. Während die meisten Services und Funktionen der BlueXP-Plattform über SaaS-basierte Software angeboten werden, sind einige Funktionen von der Version des Connectors abhängig. Dazu gehören Cloud Volumes ONTAP-Management, On-Premises-ONTAP-Cluster-Management, Einstellungen und Hilfe.

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. Wenn Sie BlueXP im privaten Modus nutzen, müssen Sie den Connector manuell aktualisieren.

"Erfahren Sie, wie Sie die Connector-Software manuell aktualisieren".

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.

Mehrere Arbeitsumgebungen

Ein Connector kann mehrere Arbeitsumgebungen in BlueXP verwalten. Die maximale Anzahl von Arbeitsumgebungen, die ein einzelner Connector managen sollte, variiert. Das hängt von der Art der Arbeitsumgebungen, der Anzahl der Volumes, der zu verwaltenden Kapazität und der Anzahl der Benutzer ab.

Nutzen Sie eine umfangreiche Implementierung, arbeiten Sie mit Ihrem NetApp Ansprechpartner zusammen, um die Größe Ihrer Umgebung zu dimensionieren. Sollten Sie während des gesamten Chats Probleme haben, können Sie sich mit uns in Verbindung setzen.

Mehrere Anschlüsse

In einigen Fällen benötigen Sie möglicherweise nur einen Connector, aber Sie benötigen möglicherweise zwei oder mehr Anschlüsse.

Hier nur ein paar Beispiele:

- Sie verfügen über eine Multi-Cloud-Umgebung (z. B. AWS und Azure) und bevorzugen einen Connector in AWS und einen weiteren in Azure. Jedes managt die Cloud Volumes ONTAP Systeme, die in diesen Umgebungen ausgeführt werden.
- Ein Service-Provider nutzt möglicherweise ein BlueXP Konto für die Bereitstellung von Services für seine Kunden und ein weiteres Konto für die Disaster Recovery für einen seiner Geschäftsbereiche. Jedes Konto hätte separate Anschlüsse.

Wann wechseln

Wenn Sie Ihren ersten Connector erstellen, verwendet BlueXP diesen Connector automatisch für jede zusätzliche Arbeitsumgebung, die Sie erstellen. Wenn Sie einen zusätzlichen Connector erstellen, müssen Sie zwischen diesen wechseln, um die für jeden Connector spezifischen Arbeitsumgebungen zu sehen.

"Erfahren Sie, wie Sie zwischen den Anschlüssen wechseln".

Disaster Recovery

Sie können eine Arbeitsumgebung mit mehreren Connectors gleichzeitig für Disaster Recovery-Zwecke verwalten. Wenn ein Anschluss ausfällt, können Sie zum anderen Connector wechseln, um die Arbeitsumgebung sofort zu verwalten.

So richten Sie diese Konfiguration ein:

1. "Wechseln Sie zu einem anderen Anschluss".
2. Erkennung der vorhandenen Arbeitsumgebung
   - "Fügen Sie vorhandene Cloud Volumes ONTAP-Systeme zu BlueXP hinzu"
   - "ONTAP Cluster erkennen"
3. Stellen Sie die ein "Kapazitätsmanagement -Modus"

   Nur der Hauptanschluss sollte auf **Automatikmodus** eingestellt sein. Wenn Sie zu DR-Zwecken auf einen anderen Connector wechseln, können Sie den Kapazitätsverwaltungsmodus bei Bedarf ändern.

Weitere Informationen zu BlueXP Implementierungsmodi

BlueXP bietet mehrere *Implementierungsmodi*, die es Ihnen ermöglichen, BlueXP entsprechend Ihren geschäftlichen und Sicherheitsanforderungen zu nutzen. *Standard Mode* nutzt die BlueXP SaaS-Ebene für die volle Funktionalität. *Restricted Mode* und *Private Mode* stehen Unternehmen mit Konnektivitätsbeschränkungen zur Verfügung.

Während BlueXP den Datenfluss, die Kommunikation und die Datenübertragung im eingeschränkten Modus oder im Private-Modus hemmt, liegt es in Ihrer Verantwortung, dass Ihre Umgebung (lokal und in der Cloud) den erforderlichen Vorschriften entspricht.

Überblick

BlueXP bietet für Ihr Konto folgende Implementierungsmodi. Jeder Modus unterscheidet sich in Bezug auf Anforderungen für ausgehende Verbindungen, Bereitstellungsort, Installationsprozess, Authentifizierungsmethode, verfügbare Daten- und Speicherservices sowie Abrechnungsmethoden.

Standardmodus

BlueXP ist für Benutzer über die webbasierte Konsole als Cloud-Service zugänglich. Abhängig von den geplanten BlueXP Services erstellt ein BlueXP Administrator einen oder mehrere Connectors, um Daten in Ihrer Hybrid-Cloud-Umgebung zu managen.

Dieser Modus verwendet verschlüsselte Datenübertragung über das öffentliche Internet.

Eingeschränkter Modus

Ein BlueXP Connector wird in der Cloud installiert (in einer Regierungsregion, einer souveränen Cloud-Region oder einer kommerziellen Region) und hat eingeschränkte ausgehende Konnektivität zur BlueXP SaaS-Schicht. Benutzer greifen lokal über die webbasierte Konsole auf BlueXP zu, die über den Connector verfügbar ist und nicht über die SaaS-Schicht.

Dieser Modus wird in der Regel von staatlichen und lokalen Behörden und regulierten Unternehmen verwendet.

Erfahren Sie mehr über ausgehende Verbindungen zur SaaS-Ebene.

Privater Modus

Ein BlueXP Connector wird lokal oder in der Cloud (in einer sicheren Region, einer souveränen Cloud-Region oder einer kommerziellen Region) installiert und verfügt über *no* Konnektivität zur BlueXP SaaS-Schicht. Benutzer greifen lokal über die webbasierte Konsole auf BlueXP zu, die über den Connector verfügbar ist und nicht über die SaaS-Schicht.

Eine sichere Region umfasst "AWS Secret Cloud", "Top Secret Cloud von AWS", und "Azure IL6"

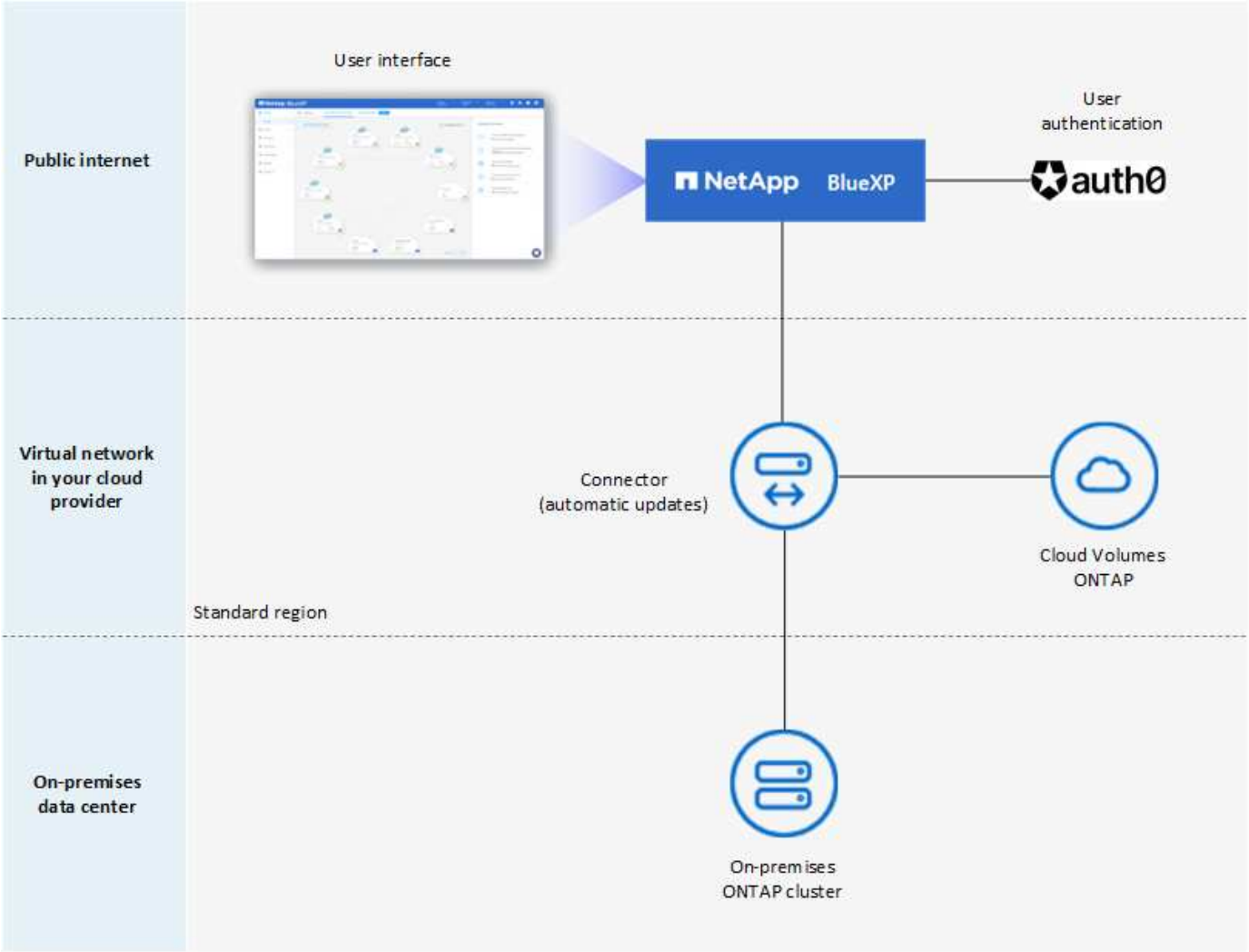
Die folgende Tabelle enthält einen Vergleich dieser Modi.

	Standardmodus	Eingeschränkter Modus	Privater Modus
Verbindung zur BlueXP SaaS-Ebene erforderlich?	Ja.	Nur ausgehend	Nein
Verbindung zu Ihrem Cloud-Provider erforderlich?	Ja.	Ja, innerhalb der Region	Ja, innerhalb der Region (bei Verwendung von Cloud Volumes ONTAP)
Steckverbinder installation	Von BlueXP, Cloud Marketplace oder manuelle Installation	Cloud Marketplace oder manuelle Installation	Manuelle Installation
Connector-Upgrades	Automatische Upgrades der Software NetApp Connector	Automatische Upgrades der Software NetApp Connector	Manuelles Upgrade erforderlich
Zugriff auf die Benutzeroberfläche	Von der BlueXP SaaS-Ebene aus	Lokal von der VM des Connectors aus	Lokal von der VM des Connectors aus
API-Endpunkt	Die BlueXP SaaS-Ebene	Der Anschluss	Der Anschluss
Authentifizierung	Über SaaS mit auth0, NSS-Anmeldung oder Identity Federation	Über SaaS mithilfe von auth0 oder Identity Federation	Lokale Benutzerauthentifizierung
Storage- und Datenservices	Alle werden unterstützt	Viele werden unterstützt	Es werden mehrere unterstützt
Lizenzierungsoptionen	Marketplace-Abonnements und BYOL	Marketplace-Abonnements und BYOL	BYOL

Lesen Sie die folgenden Abschnitte, um mehr über diese Modi zu erfahren, einschließlich der unterstützten BlueXP Funktionen und Services.

Standardmodus

Das folgende Bild zeigt ein Beispiel für eine Standardimplementierung.



BlueXP arbeitet im Standardmodus wie folgt:

Ausgehende Kommunikation

Konnektivität ist erforderlich – vom Connector bis zur SaaS-Schicht von BlueXP, zu den öffentlich verfügbaren Ressourcen Ihres Cloud-Providers und zu anderen wichtigen Komponenten für den täglichen Betrieb.

- "Endpunkte, die der Connector in AWS kontaktiert"
- "Endpunkte, die der Connector in Azure kontaktiert"
- "Endpunkte, die der Connector in Google Cloud kontaktiert"

Unterstützter Speicherort für den Connector

Im Standardmodus wird der Connector in der Cloud oder bei Ihnen vor Ort unterstützt.

Steckverbinderinstallation

Die Connector-Installation ist über einen Setup-Assistenten in BlueXP, über AWS oder Azure Marketplace oder über ein Installationsprogramm möglich, um den Connector manuell auf Ihrem eigenen Linux-Host in Ihrem Datacenter oder in der Cloud zu installieren.

Connector-Upgrades

Automatisierte Upgrades der Connector-Software sind bei BlueXP mit monatlichen Updates erhältlich.

Zugriff auf die Benutzeroberfläche

Der Zugriff auf die Benutzeroberfläche erfolgt über die webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird.

API-Endpunkt

API-Aufrufe werden an den folgenden Endpunkt vorgenommen:
https://cloudmanager.cloud.netapp.com

Authentifizierung

Die Authentifizierung erfolgt über den Cloud-Service von BlueXP mit auth0 oder über die NetApp Support Site (NSS) Anmeldedaten. Identitätsföderation ist verfügbar.

Unterstützte BlueXP Services

Alle BlueXP Services sind für Anwender verfügbar.

Unterstützte Lizenzierungsoptionen

Marketplace-Abonnements und BYOL werden im Standard-Modus unterstützt. Die unterstützten Lizenzierungsoptionen hängen jedoch von dem ab, welchen BlueXP Service Sie verwenden. In der Dokumentation zu den einzelnen Services finden Sie weitere Informationen zu den verfügbaren Lizenzierungsoptionen.

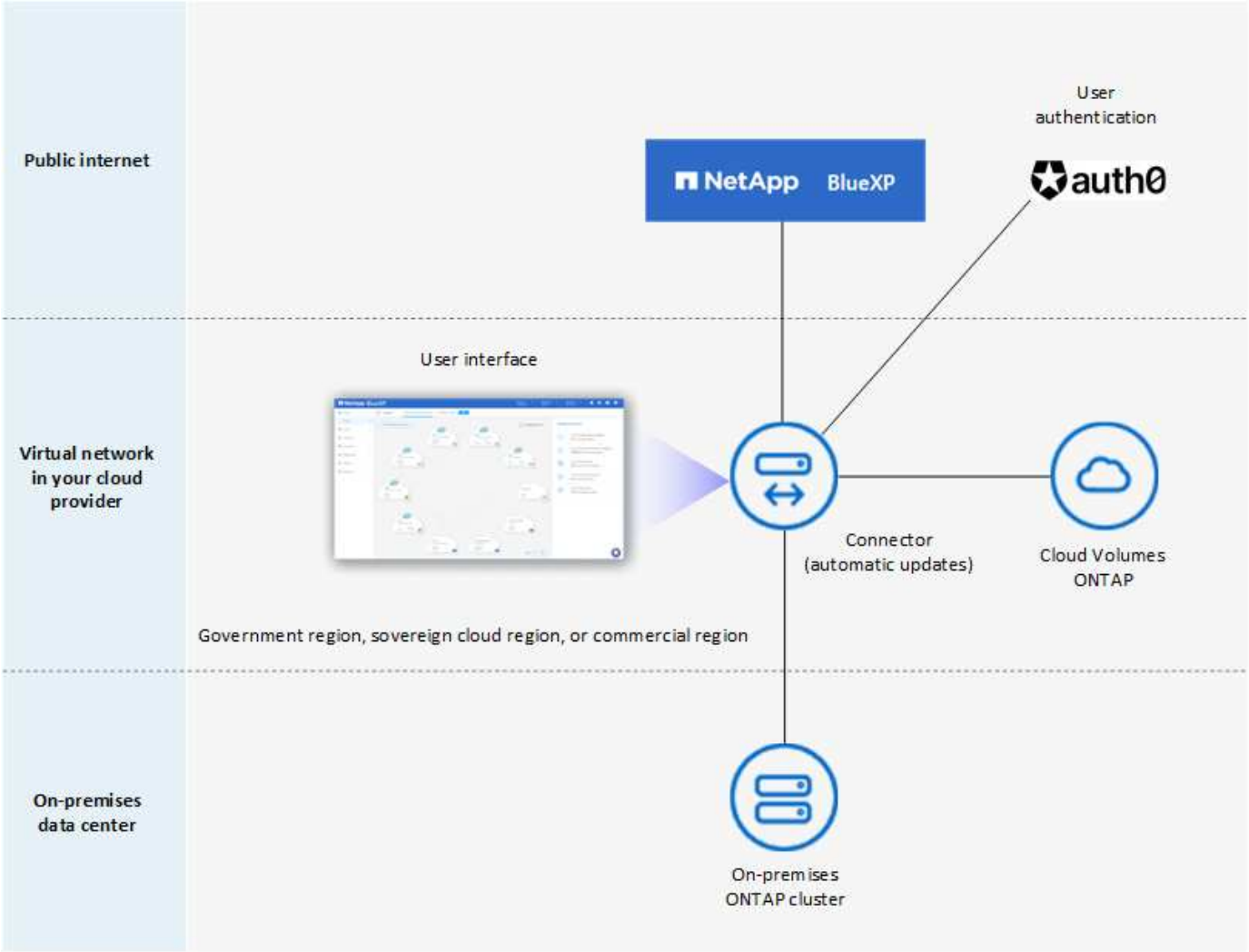
Erste Schritte mit dem Standardmodus

Wechseln Sie zum "BlueXP webbasierte Konsole" Und melden Sie sich an.

"Erste Schritte mit dem Standardmodus".

Eingeschränkter Modus

Das folgende Bild zeigt ein Beispiel für eine Bereitstellung im eingeschränkten Modus.



BlueXP arbeitet im eingeschränkten Modus wie folgt:

Ausgehende Kommunikation

Die ausgehende Konnektivität ist von Connector zur BlueXP SaaS-Ebene erforderlich, um die BlueXP Datenservices zu nutzen, automatische Software-Upgrades des Connector zu aktivieren, auth0-basierte Authentifizierung zu verwenden und Metadaten zu Abrechnungszwecken (Name der Storage-VM, zugewiesene Kapazität, Volume-UUID, Typ und IOPS) zu senden.

Die BlueXP SaaS-Schicht initiiert keine Kommunikation zum Connector. Die gesamte Kommunikation wird vom Connector initiiert, der je nach Bedarf Daten von oder auf die SaaS-Ebene abrufen oder übertragen kann.

Außerdem ist eine Verbindung zu Cloud-Provider-Ressourcen aus der Region erforderlich.

Unterstützter Speicherort für den Connector

Im eingeschränkten Modus wird der Connector in der Cloud unterstützt: In einer Regierungsregion, einer souveränen Region oder einer kommerziellen Region.

Steckverbinderinstallation

Connector-Installation ist über den AWS oder Azure Marketplace möglich oder eine manuelle Installation auf Ihrem eigenen Linux-Host.

Connector-Upgrades

Automatisierte Upgrades der Connector-Software sind bei BlueXP mit monatlichen Updates erhältlich.

Zugriff auf die Benutzeroberfläche

Auf die Benutzeroberfläche kann über die virtuelle Connector-Maschine zugegriffen werden, die in Ihrer Cloud-Region bereitgestellt wird.

API-Endpunkt

API-Aufrufe werden an die virtuelle Connector-Maschine vorgenommen.

Authentifizierung

Die Authentifizierung erfolgt über den Cloud-Service von BlueXP unter Verwendung von auth0. Identitätsföderation ist ebenfalls verfügbar.

Unterstützte BlueXP Services

BlueXP unterstützt folgende Storage- und Datenservices mit eingeschränktem Modus:

Unterstützte Services	Hinweise
Amazon FSX für ONTAP	Volle Unterstützung
Azure NetApp Dateien	Volle Unterstützung
Backup und Recovery	Unterstützt in Regierungsregionen und Geschäftsregionen mit eingeschränkter Betriebsart. Nicht unterstützt in souveränen Regionen mit eingeschränktem Modus. Im eingeschränkten Modus unterstützt BlueXP Backup und Recovery ausschließlich Backup und Wiederherstellung von ONTAP Volume-Daten. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Daten an" Backup und Restore von Applikationsdaten, Virtual Machine Daten und Kubernetes-Daten werden nicht unterstützt.
Klassifizierung	Unterstützt in Regierungsregionen mit eingeschränktem Modus. Nicht unterstützt in kommerziellen Regionen oder in souveränen Regionen mit eingeschränktem Modus. Es gelten die folgenden Einschränkungen: • OneDrive-Konten, SharePoint-Konten und Google-Laufwerk Konten können nicht gescannt werden. • Die Funktionalität der Microsoft Azure Information Protection (AIP)-Etiketten kann nicht integriert werden.
Cloud Volumes ONTAP	Volle Unterstützung

Unterstützte Services	Hinweise
Digitale Brieftasche	Sie können das Digital Wallet mit den unten aufgeführten unterstützten Lizenzierungsoptionen für den eingeschränkten Modus verwenden.
On-Premises ONTAP Cluster	Erkennung mit einem Connector und Ermittlung ohne einen Connector (direkte Erkennung) werden unterstützt. Wenn Sie ein On-Premises-Cluster mit einem Connector ermitteln, wird die erweiterte Ansicht (System Manager) nicht unterstützt.
Replizierung	Unterstützt in Regierungsregionen mit eingeschränktem Modus. Nicht unterstützt in kommerziellen Regionen oder in souveränen Regionen mit eingeschränktem Modus.

Unterstützte Lizenzierungsoptionen

Die folgenden Lizenzierungsoptionen werden im eingeschränkten Modus unterstützt:

- Marketplace-Abonnements (Stunden- und Jahresverträge)

  Beachten Sie Folgendes:

  - Für Cloud Volumes ONTAP wird nur die kapazitätsbasierte Lizenzierung unterstützt.
  - In Azure werden Jahresverträge nicht in Regierungsregionen unterstützt.
- BYOL

  Bei Cloud Volumes ONTAP werden sowohl kapazitätsbasierte Lizenzierung als auch Node-basierte Lizenzierung durch BYOL unterstützt.

Erste Schritte mit eingeschränkter Modus

Wenn Sie Ihr BlueXP Konto erstellen, müssen Sie den eingeschränkten Modus aktivieren.

Wenn Sie noch kein Konto haben, werden Sie aufgefordert, Ihr Konto zu erstellen und den eingeschränkten Modus zu aktivieren, wenn Sie sich zum ersten Mal über einen Connector bei BlueXP anmelden, den Sie manuell installiert haben oder den Sie auf dem Marktplatz Ihres Cloud-Providers erstellt haben.

Wenn Sie bereits ein Konto haben und ein weiteres erstellen möchten, müssen Sie die Mandanten-API verwenden.

Beachten Sie, dass Sie die Einstellung für den eingeschränkten Modus nicht ändern können, 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.

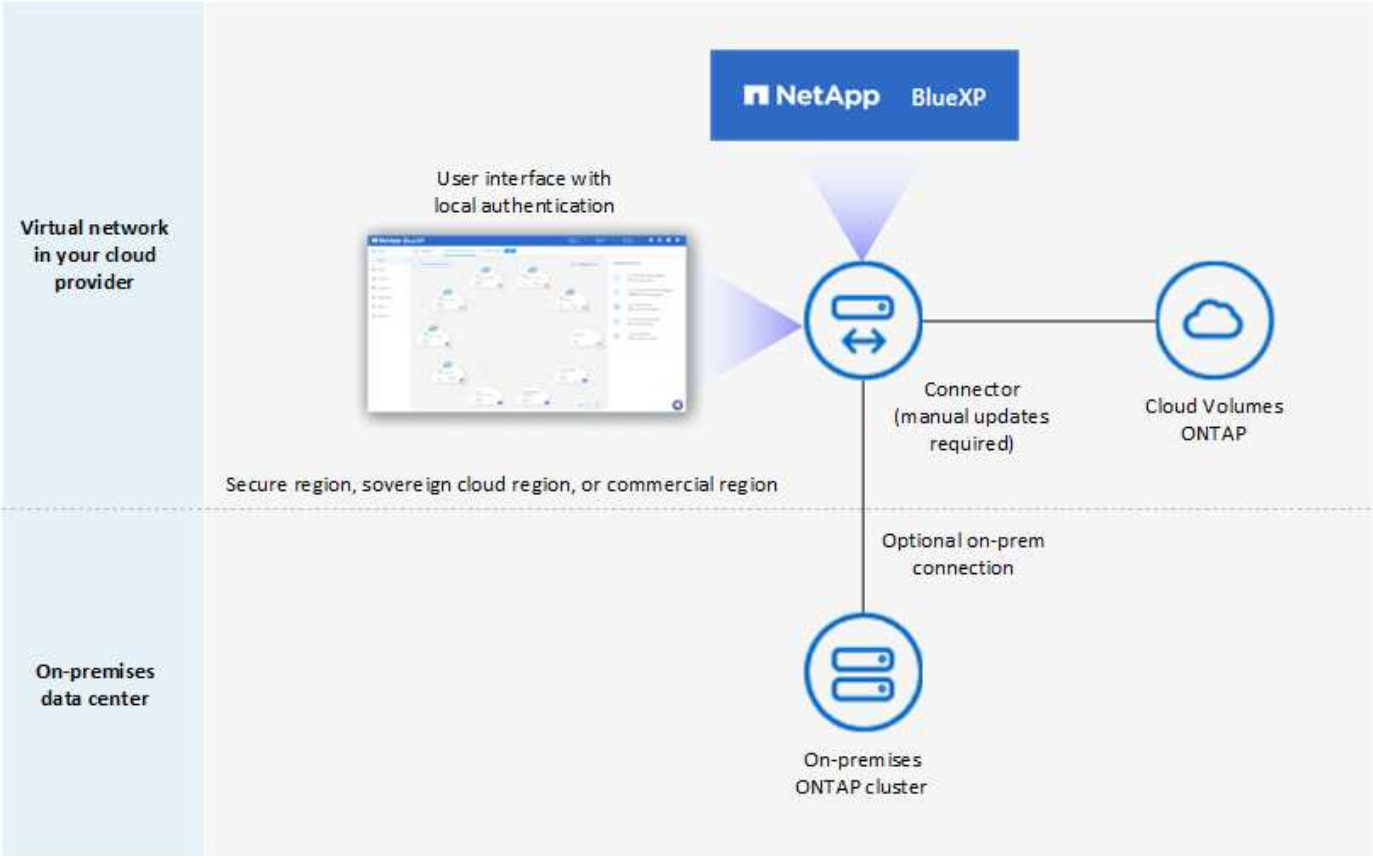
- "Erfahren Sie, wie Sie mit dem eingeschränkten Modus beginnen".
- "Erstellen Sie ein zusätzliches BlueXP Konto".

Privater Modus

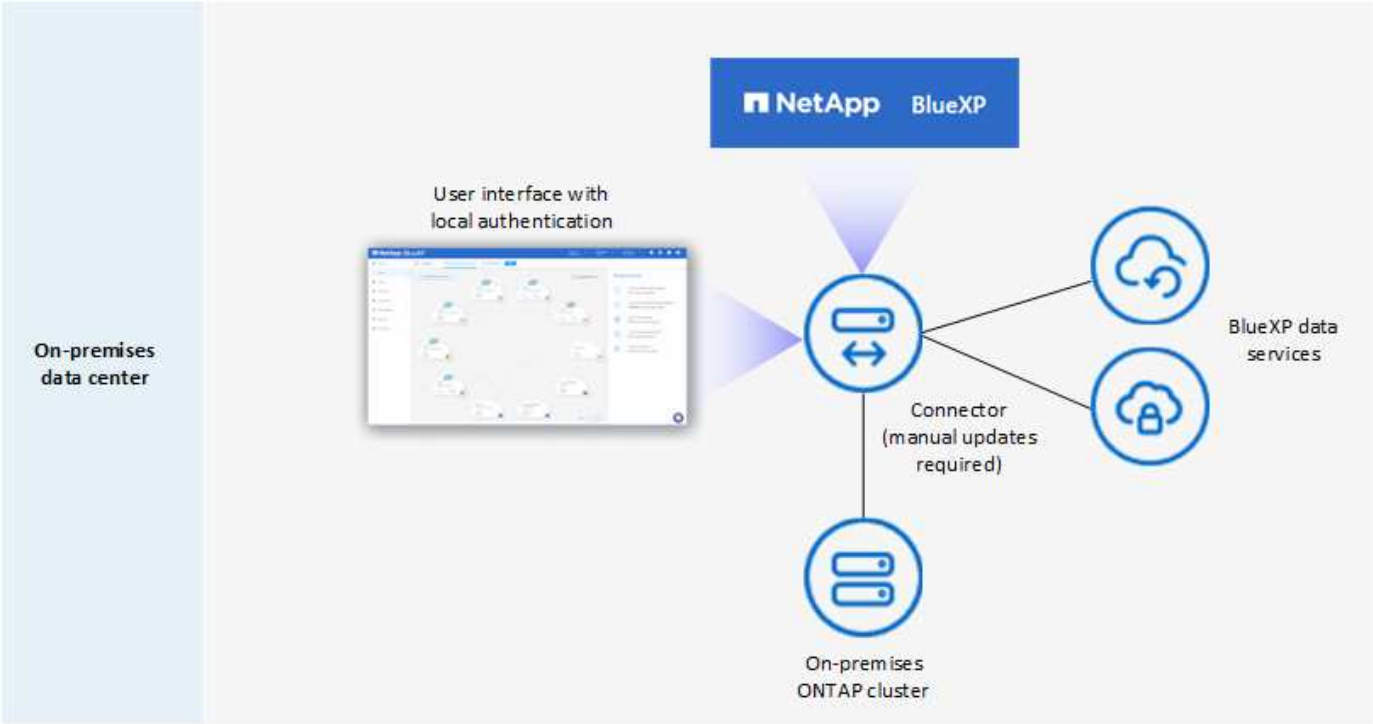
Im privaten Modus können Sie einen Connector entweder vor Ort oder in der Cloud installieren und dann

BlueXP für das Datenmanagement in Ihrer gesamten Hybrid Cloud verwenden. Die SaaS-Ebene von BlueXP wird nicht verbunden.

Die folgende Abbildung zeigt ein Beispiel einer Private-Mode-Implementierung, bei der der Connector in der Cloud installiert ist und sowohl Cloud Volumes ONTAP als auch einen lokalen ONTAP-Cluster managt.



Gleichzeitig zeigt die zweite Abbildung ein Beispiel einer Private-Mode-Implementierung, bei der der Connector vor Ort installiert ist, einen lokalen ONTAP-Cluster managt und Zugriff auf unterstützte BlueXP Datenservices bietet.



BlueXP arbeitet im privaten Modus wie folgt:

Ausgehende Kommunikation

Auf der BlueXP SaaS-Ebene ist keine ausgehende Konnektivität erforderlich. Alle Pakete, Abhängigkeiten und wesentlichen Komponenten werden mit dem Connector verpackt und von der lokalen Maschine bedient. Eine Verbindung zu den öffentlich verfügbaren Ressourcen Ihres Cloud-Providers ist nur erforderlich, wenn Sie Cloud Volumes ONTAP implementieren.

Unterstützter Speicherort für den Connector

Im privaten Modus wird der Connector in der Cloud oder On-Premises unterstützt.

Steckverbinderinstallation

Manuelle Installationen des Connectors werden auf Ihrem eigenen Linux-Host in der Cloud oder vor Ort unterstützt.

Connector-Upgrades

Sie müssen die Connector-Software manuell aktualisieren. Die Connector Software wird in undefinierten Intervallen auf der NetApp Support Website veröffentlicht.

Zugriff auf die Benutzeroberfläche

Auf die Benutzeroberfläche kann über den Connector zugegriffen werden, der in Ihrer Cloud-Region oder vor Ort bereitgestellt wird.

API-Endpunkt

API-Aufrufe werden an die virtuelle Connector-Maschine vorgenommen.

Authentifizierung

Die Authentifizierung erfolgt über lokale Benutzerverwaltung und -Zugriff. Authentifizierung wird nicht über den Cloud-Service von BlueXP bereitgestellt.

Unterstützte BlueXP Services in Cloud-Implementierungen

BlueXP unterstützt bei der Installation des Connector in der Cloud folgende Storage- und Datenservices mit Private Mode:

Unterstützte Services	Hinweise
Backup und Recovery	Unterstützt in kommerziellen Regionen AWS und Azure. Nicht in Google Cloud oder in unterstützt "AWS Secret Cloud", "Top Secret Cloud von AWS", Oder "Azure IL6" Im privaten Modus unterstützt BlueXP Backup und Recovery ausschließlich Backup und Wiederherstellung von ONTAP Volume-Daten. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Daten an" Backup und Restore von Applikationsdaten, Virtual Machine Daten und Kubernetes-Daten werden nicht unterstützt.
Cloud Volumes ONTAP	Da es keinen Internetzugang gibt, sind die folgenden Funktionen nicht verfügbar: Automatisierte Software-Upgrades und AutoSupport.
Digitale Brieftasche	Sie können das Digital Wallet mit den unten aufgeführten unterstützten Lizenzierungsoptionen für den privaten Modus verwenden.
On-Premises ONTAP Cluster	Erfordert Konnektivität aus der Cloud (wo der Connector installiert ist) zur On-Premises-Umgebung. Erkennung ohne Connector (direkte Erkennung) wird nicht unterstützt.

Unterstützte BlueXP Services in On-Premises-Implementierungen

BlueXP unterstützt bei der On-Premises-Installation des Connector folgende Storage- und Datenservices mit Private Mode:

Unterstützte Services	Hinweise
Backup und Recovery	Im privaten Modus unterstützt BlueXP Backup und Recovery ausschließlich Backup und Wiederherstellung von ONTAP Volume-Daten. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Volume-Daten an" Backup und Restore von Applikationsdaten, Virtual Machine Daten und Kubernetes-Daten werden nicht unterstützt.

Unterstützte Services	Hinweise
Klassifizierung	• Die einzigen unterstützten Datenquellen sind die, die Sie lokal ermitteln können. "Zeigen Sie die Quellen an, die Sie lokal ermitteln können" • Funktionen, für die ein abgehender Internetzugang erforderlich ist, werden nicht unterstützt. "Zeigen Sie die Funktionseinschränkungen an"
Digitale Brieftasche	Sie können das Digital Wallet mit den unten aufgeführten unterstützten Lizenzierungsoptionen für den privaten Modus verwenden.
On-Premises ONTAP Cluster	Erkennung ohne Connector (direkte Erkennung) wird nicht unterstützt.
Replizierung	Volle Unterstützung

Unterstützte Lizenzierungsoptionen

Nur BYOL wird im privaten Modus unterstützt.

Bei Cloud Volumes ONTAP BYOL wird nur Node-basierte Lizenzierung unterstützt. Kapazitätsbasierte Lizenzierung wird nicht unterstützt. Da keine ausgehende Internetverbindung verfügbar ist, müssen Sie Ihre Cloud Volumes ONTAP Lizenzdatei manuell in das Digital Wallet von BlueXP hochladen.

"Erweitern Sie Ihr Digital Wallet von BlueXP um Lizenzen"

Erste Schritte mit dem privaten Modus

Der private Modus ist durch Herunterladen des „offline“ Installers von der NetApp Support Site verfügbar.

"Erfahren Sie, wie Sie mit dem privaten Modus beginnen".

> Wenn Sie BlueXP in der verwenden möchten "AWS Secret Cloud" Oder im "Top Secret Cloud von AWS"Dann sollten Sie separate Anweisungen befolgen, um in diesen Umgebungen zu beginnen. "Erste Schritte mit Cloud Volumes ONTAP – in der AWS Secret Cloud oder Top Secret Cloud"

Vergleich von Service und Funktionen

Die folgende Tabelle hilft Ihnen dabei, schnell zu ermitteln, welche BlueXP Services und Funktionen im eingeschränkten Modus und im privaten Modus unterstützt werden.

Beachten Sie, dass einige Dienste möglicherweise eingeschränkt unterstützt werden. Weitere Informationen darüber, wie diese Dienste im eingeschränkten Modus und im privaten Modus unterstützt werden, finden Sie in den obigen Abschnitten.

Produktbereich	BlueXP Service oder Feature	Eingeschränkter Modus	Privater Modus
Arbeitsumgebungen Dieser Teil der Tabelle listet die Unterstützung für das Management der Arbeitsumgebung aus dem BlueXP Arbeitsbereich auf. Die unterstützten Backup-Ziele für BlueXP Backup und Recovery werden nicht angezeigt.	Amazon FSX für ONTAP	Ja.	Nein
	Amazon S3	Nein	Nein
	Azure Blob	Nein	Nein
	Azure NetApp Dateien	Ja.	Nein
	Cloud Volumes ONTAP	Ja.	Ja.
	Cloud Volumes Service für Google Cloud	Nein	Nein
	Google Cloud Storage	Nein	Nein
	Kubernetes-Cluster	Nein	Nein
	ONTAP-Cluster vor Ort	Ja.	Ja.
	E-Series	Nein	Nein
	StorageGRID	Nein	Nein
Services	Backup und Recovery	Ja. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Volume-Daten an"	Ja. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Volume-Daten an"
	Klassifizierung	Ja.	Ja.
	Cloud-Betrieb	Nein	Nein
	Kopieren und Synchronisieren	Nein	Nein
	Digitaler Berater	Nein	Nein
	Digitale Brieftasche	Ja.	Ja.
	Disaster Recovery	Nein	Nein
	Wirtschaftliche Effizienz	Nein	Nein
	Edge-Caching	Nein	Nein
	Migrationsberichte	Nein	Nein
	Operative Ausfallsicherheit	Nein	Nein
	Schutz durch Ransomware	Nein	Nein
	Replizierung	Ja.	Ja.
	Nachhaltigkeit	Nein	Nein
	Tiering	Nein	Nein
	Volume-Caching	Nein	Nein

Produktbereich	BlueXP Service oder Feature	Eingeschränkter Modus	Privater Modus
Eigenschaften	Anmeldedaten	Ja.	Ja.
	NSS-Konten	Ja.	Nein
	Benachrichtigungen	Ja.	Nein
	Suche	Ja.	Nein
	Zeitachse	Ja.	Ja.

Beginnen Sie mit dem Standardmodus

Erste Schritte Workflow (Standardmodus)

Einstieg in BlueXP im Standardmodus: Bereiten Sie Networking für die BlueXP Konsole vor, melden Sie sich an, erstellen Sie ein Konto, erstellen Sie optional einen Connector und abonnieren Sie BlueXP.

Im Standardmodus ist BlueXP über die webbasierte Konsole für Benutzer als Cloud-Service zugänglich. Bevor Sie beginnen, sollten Sie ein Verständnis von haben "BlueXP Accounts", "Anschlüsse", und "Bereitstellungsmodi".

1 **"Networking zur Nutzung der BlueXP Konsole vorbereiten"**

Computer, die auf die BlueXP Konsole zugreifen, sollten über Verbindungen zu bestimmten Endpunkten verfügen, um einige Administrationsaufgaben durchzuführen. Wenn Ihr Netzwerk den ausgehenden Zugriff einschränkt, sollten Sie sicherstellen, dass diese Endpunkte zugelassen sind.

2 **"Registrieren Sie sich und erstellen Sie ein Konto"**

Wechseln Sie zum "BlueXP-Konsole" Und melden Sie sich an. Sie erhalten die Möglichkeit, ein Konto zu erstellen, aber Sie können diesen Schritt überspringen, wenn Sie zu einem bestehenden Konto eingeladen werden.

Jetzt sind Sie angemeldet und können mehrere BlueXP Services wie Digital Advisor, Amazon FSX for ONTAP, Azure NetApp Files und vieles mehr nutzen. "Erfahren Sie, was Sie ohne einen Connector tun können".

3 **Einen Konnektor erstellen**

Für die ersten Schritte mit BlueXP benötigen Sie keinen Connector, aber Sie können einen Connector erstellen, mit dem Sie alle Funktionen und Services von BlueXP ausschöpfen können. Der Connector ist NetApp Software, die BlueXP ermöglicht, Ressourcen und Prozesse innerhalb Ihrer Hybrid-Cloud-Umgebung zu managen.

Ein BlueXP Kontoadministrator kann einen Connector in Ihrem Cloud- oder On-Premises-Netzwerk erstellen.

- "Erfahren Sie mehr darüber, wann Anschlüsse erforderlich sind und wie sie funktionieren"
- "Erfahren Sie, wie Sie in AWS einen Connector erstellen können"

- "Erfahren Sie, wie Sie in Azure einen Connector erstellen"
- "Erfahren Sie, wie Sie einen Connector in Google Cloud erstellen"
- "Erfahren Sie, wie Sie einen Konnektor vor Ort erstellen"

Wenn Sie BlueXP Services für das Management von Storage und Daten in Google Cloud nutzen möchten, muss der Connector in Google Cloud ausgeführt werden.

4 **"Abonnieren Sie BlueXP"**

Abonnieren Sie BlueXP über den Marketplace Ihres Cloud-Providers und zahlen Sie für BlueXP Services zu einem Stundensatz (PAYGO) oder über einen Jahresvertrag.

Networking zur Nutzung der BlueXP Konsole vorbereiten

Bei der Nutzung der webbasierten Konsole von BlueXP, die über die SaaS-Schicht bereitgestellt wird, werden mehrere Endpunkte kontaktiert, wenn einige Administrationsaufgaben durchgeführt werden. Computer, die auf die BlueXP Konsole zugreifen, sollten über Verbindungen zu diesen Endpunkten verfügen.

Diese Endpunkte werden von dem Computer eines Benutzers kontaktiert, wenn bestimmte Aktionen über die BlueXP Konsole durchgeführt werden. Sie sollten auch die Netzwerkanforderungen für den Connector und bestimmte BlueXP Services beachten. Weitere Informationen finden Sie unter den entsprechenden Links am Ende dieser Seite.

Endpunkte	Zweck
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	Wenn Sie die webbasierte Konsole von BlueXP verwenden, kontaktiert Ihr Webbrowser diese URLs.
https://aiq.netapp.com	Voraussetzung für den Zugang zum digitalen Berater von BlueXP.
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Für die Bereitstellung eines Connectors von BlueXP in AWS erforderlich. Der genaue Endpunkt hängt von der Region ab, in der Sie den Connector bereitstellen. "Weitere Informationen finden Sie in der AWS-Dokumentation."
https://management.azure.com https://login.microsoftonline.com	Für die Implementierung eines Connectors von BlueXP in den meisten Azure Regionen erforderlich.
https://management.microsoftazure.de https://login.microsoftonline.de	Für die Implementierung eines Connectors von BlueXP in Azure-Regionen in Deutschland erforderlich.

Endpunkte	Zweck
https://management.usgovcloudapi.net https://login.microsoftonline.com	Erforderlich für die Bereitstellung eines Connectors von BlueXP in Azure US Gov Regionen.
https://www.googleapis.com	Erforderlich, um einen Connector von BlueXP in Google Cloud bereitzustellen.
https://signin.b2c.netapp.com	Erforderlich, um die Zugangsdaten für die NetApp Support Site (NSS) zu aktualisieren oder neue NSS-Zugangsdaten für BlueXP hinzuzufügen
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung über BlueXP zu ermöglicht.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Über diese Endpunkte hinaus müssen Sie auch sicherstellen, dass der Connector über einen ausgehenden Internetzugang zu kontaktspezifischen Endpunkten für den täglichen Betrieb verfügt. Die Liste dieser Endpunkte finden Sie unter den Links im nächsten Abschnitt unten.

Weiterführende Links

- Bereiten Sie die Vernetzung für den Connector vor
  - "AWS-Netzwerk einrichten"
  - "Azure Networking einrichten"
  - "Google Cloud-Netzwerke einrichten"
  - "On-Premises-Netzwerke einrichten"
- Networking für BlueXP Services vorbereiten

  Informationen zu jedem BlueXP Service finden Sie in der Dokumentation.

  "BlueXP-Dokumentation"

Melden Sie sich bei BlueXP an

Der Zugriff auf BlueXP erfolgt über eine webbasierte Konsole. Wenn Sie mit BlueXP starten, müssen Sie sich zunächst mit Ihren vorhandenen Zugangsdaten auf der NetApp Support Website anmelden oder ein NetApp Cloud-Login erstellen.

Über diese Aufgabe

Sie können sich bei BlueXP mithilfe einer der folgenden Optionen anmelden:

- Ihre vorhandenen Zugangsdaten für die NetApp Support Site (NSS
- Geben Sie Ihre E-Mail-Adresse und ein Passwort an, um sich bei einem NetApp Cloud-Login anzumelden

Beide Optionen unterstützen eine föderierte Verbindung, die Single Sign-On mit Anmeldeinformationen aus

Ihrem Unternehmensverzeichnis (föderierte Identität) ermöglicht. Sie können nach der Anmeldung eine Verbündungsverbindung einrichten. "Erfahren Sie mehr über den Einsatz von Identitätsföderation mit BlueXP".

Schritte

1. Öffnen Sie einen Webbrowser, und rufen Sie den auf "BlueXP-Konsole"
2. Wenn Sie über ein NetApp Support Site Konto verfügen, geben Sie die mit Ihrem NSS Konto verknüpfte E-Mail-Adresse direkt auf der **Anmelden** Seite ein.

   Sie können die Anmeldeseite überspringen, wenn Sie ein NSS-Konto haben. BlueXP meldet Sie im Rahmen dieser ersten Anmeldung an.

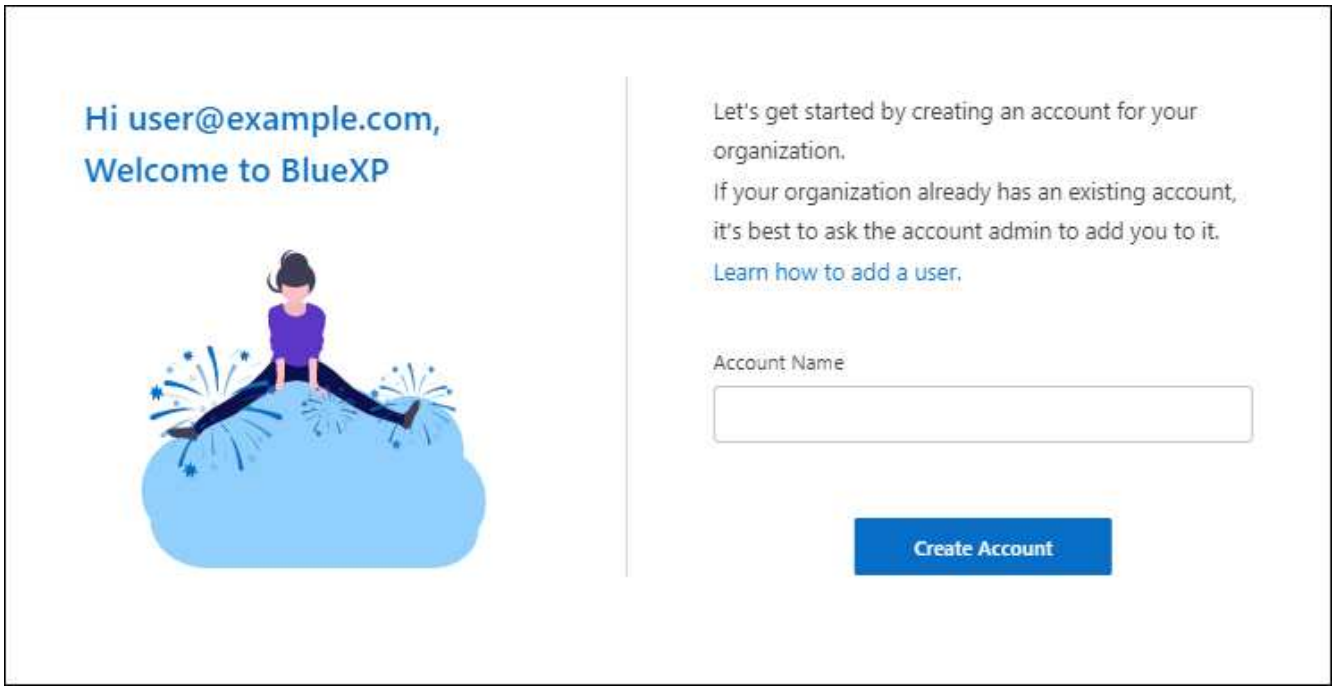
3. Wenn Sie noch keinen NSS-Account haben und sich mit einem NetApp Cloud Login registrieren möchten, wählen Sie **Registrieren**.
4. Geben Sie auf der Seite **Anmelden** die erforderlichen Informationen zur Erstellung eines NetApp Cloud-Logins ein.

   Beachten Sie, dass nur englische Zeichen im Anmeldeformular zulässig sind.

5. Überprüfen Sie, wenn Sie dazu aufgefordert werden, die Endbenutzer-Lizenzvereinbarung und akzeptieren Sie die Bedingungen.
6. Geben Sie auf der Seite **Willkommen** einen Namen für Ihr Konto ein.

   Wenn Ihr Unternehmen bereits über ein Konto verfügt und Sie es beitreten möchten, schließen Sie BlueXP ab und bitten Sie den Eigentümer, Sie mit dem Konto zu verknüpfen. Nachdem der Besitzer Sie hinzugefügt hat, können Sie sich einloggen und haben Zugriff auf das Konto. "Erfahren Sie, wie Sie einem bestehenden Konto Mitglieder hinzufügen".

   Der Account ist das wichtigste Element der Identitätsplattform von NetApp. Sie können Benutzer, Rollen, Berechtigungen und Arbeitsumgebungen hinzufügen und verwalten.



7. Wählen Sie **Konto Erstellen**.

Ergebnis

Sie haben jetzt eine BlueXP-Anmeldung und ein Konto. In den meisten Fällen besteht der nächste Schritt darin, einen Connector zu erstellen, der die Services von BlueXP mit Ihrer Hybrid-Cloud-Umgebung verbindet.

Einen Konnektor erstellen

AWS

Installationsoptionen für Konnektoren in AWS

Es gibt verschiedene Möglichkeiten, einen Connector in AWS zu erstellen. Dies ist die gängigste Methode – direkt von BlueXP.

Folgende Installationsoptionen sind verfügbar:

- "Connector direkt aus BlueXP erstellen" (Dies ist die Standardoption)

  Mit dieser Aktion wird eine EC2-Instanz gestartet, auf der Linux und die Connector-Software in einem VPC Ihrer Wahl ausgeführt werden.

- "Erstellen Sie einen Connector aus dem AWS Marketplace"

  Durch diese Aktion wird auch eine EC2-Instanz gestartet, auf der Linux und die Connector-Software ausgeführt werden. Die Implementierung wird jedoch direkt über AWS Marketplace anstatt über BlueXP gestartet.

- "Laden Sie die Software herunter, und installieren Sie sie manuell auf Ihrem eigenen Linux-Host"

Die von Ihnen gewählte Installationsoption wirkt sich auf die Vorbereitung auf die Installation aus. Dazu gehört auch, wie Sie BlueXP die erforderlichen Berechtigungen bereitstellen, die es zur Authentifizierung und zum Management von Ressourcen in AWS benötigt.

Erstellen Sie einen Connector in AWS von BlueXP

Um einen Connector in AWS von BlueXP zu erstellen, müssen Sie Ihr Netzwerk einrichten, AWS Berechtigungen vorbereiten und anschließend den Connector erstellen.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Connector installieren möchten, die folgenden Anforderungen erfüllt. Durch die Erfüllung dieser Anforderungen kann der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen.

VPC und Subnetz

Wenn Sie den Connector erstellen, müssen Sie die VPC und das Subnetz angeben, in dem sich der Connector befinden soll.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Endpunkte wurden über die BlueXP Konsole kontaktiert

Bei der Nutzung der webbasierten Konsole von BlueXP, die über die SaaS-Schicht bereitgestellt wird, werden mehrere Endpunkte kontaktiert, um Datenmanagement-Aufgaben durchzuführen. Dazu gehören Endpunkte, die kontaktiert werden, um den Connector über die BlueXP Konsole zu implementieren.

"Eine Liste der Endpunkte, die über die BlueXP Konsole kontaktiert wurden, wird angezeigt".

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Sie müssen diese Netzwerkanforderung implementieren, nachdem Sie den Connector erstellt haben.

Schritt 2: AWS-Berechtigungen einrichten

BlueXP muss sich mit AWS authentifizieren, bevor es die Connector-Instanz in der VPC bereitstellen kann. Sie können eine der folgenden Authentifizierungsmethoden wählen:

- Lassen Sie BlueXP eine IAM-Rolle übernehmen, die über die erforderlichen Berechtigungen verfügt
- Geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel für einen IAM-Benutzer an, der über die erforderlichen Berechtigungen verfügt

Bei beiden Optionen besteht der erste Schritt darin, eine IAM-Richtlinie zu erstellen. Diese Richtlinie enthält nur die Berechtigungen, die zum Starten der Connector-Instanz in AWS von BlueXP erforderlich sind.

Bei Bedarf können Sie die IAM-Richtlinie mit Hilfe des IAM einschränken `Condition` Element: "AWS-Dokumentation: Condition Element"

Wenn BlueXP den Connector erstellt, wendet es einen neuen Satz an Berechtigungen auf die Connector-Instanz an, sodass der Connector AWS Ressourcen managen kann.

Schritte

1. Wechseln Sie zur AWS IAM-Konsole.
2. Wählen Sie **Policies > Create Policy** aus.
3. Wählen Sie **JSON**.
4. Kopieren Sie die folgende Richtlinie:

   Zur Erinnerung: Diese Richtlinie enthält nur die Berechtigungen, die zum Starten der Connector-Instanz in AWS aus BlueXP erforderlich sind. "Berechtigungen anzeigen, die für die Connector-Instanz selbst erforderlich sind".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/OCCMInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

5. Wählen Sie **Weiter** und fügen Sie ggf. Tags hinzu.
6. Wählen Sie **Weiter** und geben Sie einen Namen und eine Beschreibung ein.
7. Wählen Sie **Richtlinie erstellen**.
8. Hängen Sie die Richtlinie entweder einer IAM-Rolle an, die BlueXP übernehmen kann, oder einem IAM-Benutzer, damit Sie BlueXP Zugriffsschlüssel bereitstellen können:

- (Option 1) Einrichten einer IAM-Rolle, von der BlueXP ausgehen kann:
  i. Wechseln Sie im Zielkonto zur AWS IAM-Konsole.
  ii. Wählen Sie unter Access Management die Option **Rollen > Rolle erstellen** aus, und befolgen Sie die Schritte zum Erstellen der Rolle.
  iii. Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
  iv. Wählen Sie **ein weiteres AWS-Konto** aus und geben Sie die ID des BlueXP SaaS-Kontos ein: 952013314444
  v. Wählen Sie die Richtlinie aus, die Sie im vorherigen Abschnitt erstellt haben.
  vi. Nachdem Sie die Rolle erstellt haben, kopieren Sie die Rolle ARN, sodass Sie sie bei der Erstellung des Connectors in BlueXP einfügen können.
- (Option 2) Einrichten von Berechtigungen für einen IAM-Benutzer, damit Sie BlueXP Zugriffsschlüssel bereitstellen können:
  i. Wählen Sie in der AWS IAM-Konsole **users** aus und wählen Sie dann den Benutzernamen aus.
  ii. Wählen Sie **Berechtigungen hinzufügen > vorhandene Richtlinien direkt anhängen**.
  iii. Wählen Sie die von Ihnen erstellte Richtlinie aus.
  iv. Wählen Sie **Weiter** und dann **Berechtigungen hinzufügen**.
  v. Stellen Sie sicher, dass Sie über den Zugriffsschlüssel und den geheimen Schlüssel für den IAM-Benutzer verfügen.

Ergebnis

Sie sollten nun über eine IAM-Rolle mit den erforderlichen Berechtigungen verfügen oder über einen IAM-Benutzer mit den erforderlichen Berechtigungen. Wenn Sie den Connector aus BlueXP erstellen, können Sie auch Informationen zur Rolle oder den Zugriffsschlüsseln bereitstellen.

Schritt 3: Erstellen Sie den Konnektor

Erstellen Sie den Connector direkt über die webbasierte Konsole von BlueXP.

Über diese Aufgabe

Bei der Erstellung des Connectors aus BlueXP wird eine EC2-Instanz in AWS mit einer Standardkonfiguration implementiert. Nachdem Sie den Connector erstellt haben, sollten Sie nicht zu einem kleineren EC2-Instanztyp wechseln, der weniger CPU oder RAM hat. "Informieren Sie sich über die Standardkonfiguration des Connectors".

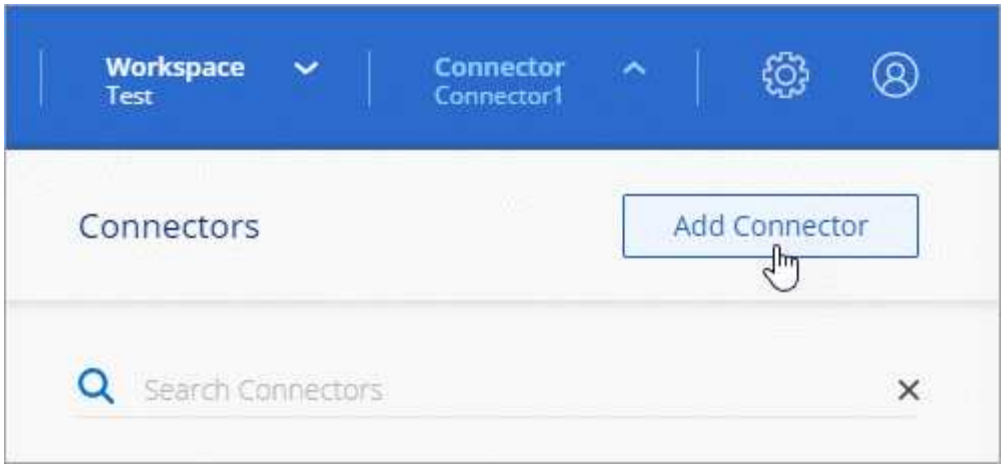
Bevor Sie beginnen

Sie sollten Folgendes haben:

- Eine AWS-Authentifizierungsmethode: Entweder eine IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer mit den erforderlichen Berechtigungen.
- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt
- Ein Schlüsselpaar für die EC2-Instanz.
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

Schritte

1. Wählen Sie die Dropdown-Liste **Connector** aus und wählen Sie **Connector hinzufügen** aus.



2. Wählen Sie **Amazon Web Services** als Ihren Cloud-Provider und wählen Sie **Weiter**.
3. Lesen Sie auf der Seite **Bereitstellen eines Konnektors** die Details dazu, was Sie benötigen. Sie haben zwei Möglichkeiten:
   a. Wählen Sie **Weiter**, um die Bereitstellung mithilfe des Produktleitfadens vorzubereiten. Jeder Schritt im Produktleitfaden enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.
   b. Wählen Sie **Skip to Deployment**, wenn Sie bereits vorbereitet haben, indem Sie die Schritte auf dieser Seite befolgen.
4. Befolgen Sie die Schritte im Assistenten, um den Konnektor zu erstellen:
   - **Get Ready**: Bewerten Sie, was Sie brauchen.
   - **AWS Credentials**: Geben Sie Ihre AWS Region an und wählen Sie dann eine Authentifizierungsmethode aus, die entweder eine IAM-Rolle ist, die BlueXP annehmen kann, oder einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel.

     Wenn Sie die Option **Rolle übernehmen** wählen, können Sie den ersten Satz von Anmeldeinformationen aus dem Assistenten für die Connector-Bereitstellung erstellen. Alle zusätzlichen Anmeldeinformationen müssen auf der Seite Anmeldeinformationen erstellt werden. Sie werden dann über den Assistenten in einer Dropdown-Liste verfügbar sein. "Hier erfahren Sie, wie Sie zusätzliche Anmeldedaten hinzufügen".

   - **Details**: Geben Sie Einzelheiten über den Connector an.
     - Geben Sie einen Namen für die Instanz ein.
     - Fügen Sie der Instanz benutzerdefinierte Tags (Metadaten) hinzu.
     - Wählen Sie aus, ob BlueXP eine neue Rolle mit den erforderlichen Berechtigungen erstellen soll oder ob Sie eine vorhandene Rolle auswählen möchten, die Sie mit eingerichtet haben "Die erforderlichen Berechtigungen".
     - Wählen Sie aus, ob Sie die EBS-Festplatten des Connectors verschlüsseln möchten. Sie haben die Möglichkeit, den Standardverschlüsselungsschlüssel zu verwenden oder einen benutzerdefinierten Schlüssel zu verwenden.
   - **Netzwerk**: Geben Sie ein VPC-, Subnetz- und Schlüsselpaar für die Instanz an, wählen Sie aus, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.

     Stellen Sie sicher, dass Sie über das richtige Schlüsselpaar verfügen, das Sie mit dem Anschluss verwenden können. Ohne ein Schlüsselpaar können Sie nicht auf die virtuelle Connector-Maschine zugreifen.

- **Sicherheitsgruppe**: Wählen Sie, ob Sie eine neue Sicherheitsgruppe erstellen möchten oder ob Sie eine vorhandene Sicherheitsgruppe auswählen möchten, die die erforderlichen ein- und ausgehenden Regeln zulässt.

  "Sicherheitsgruppen-Regeln für AWS ansehen".

- **Review**: Überprüfen Sie Ihre Auswahl, um zu überprüfen, ob Ihre Einrichtung korrekt ist.

5. Wählen Sie **Hinzufügen**.

   Die Instanz sollte in ca. 7 Minuten fertig sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Ergebnis

Nach Abschluss des Prozesses ist der Connector für die Nutzung über BlueXP verfügbar.

Wenn sich in demselben AWS-Konto, bei dem der Connector erstellt wurde, Amazon S3-Buckets befinden, wird automatisch eine Amazon S3-Arbeitsumgebung auf dem BlueXP-Bildschirm angezeigt. "Erfahren Sie, wie Sie S3-Buckets aus BlueXP managen"

Erstellen Sie einen Connector aus dem AWS Marketplace

Um einen Connector über den AWS Marketplace zu erstellen, müssen Sie Ihr Netzwerk einrichten, die AWS-Berechtigungen vorbereiten, die Instanzanforderungen prüfen und dann den Connector erstellen.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Connector installieren möchten, die folgenden Anforderungen erfüllt. Durch die Erfüllung dieser Anforderungen kann der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen.

VPC und Subnetz

Wenn Sie den Connector erstellen, müssen Sie die VPC und das Subnetz angeben, in dem sich der Connector befinden soll.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den

NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Sie müssen diese Netzwerkanforderung implementieren, nachdem Sie den Connector erstellt haben.

Schritt 2: AWS-Berechtigungen einrichten

Zur Vorbereitung auf eine Marktbereitstellung erstellen Sie IAM-Richtlinien in AWS und hängen sie einer IAM-Rolle an. Wenn Sie den Connector über AWS Marketplace erstellen, werden Sie aufgefordert, diese IAM-Rolle auszuwählen.

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:
   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.

      Abhängig von den BlueXP Services, die Sie planen zu verwenden, müssen Sie möglicherweise eine zweite Richtlinie erstellen. Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich. "Erfahren Sie mehr über IAM-Richtlinien für den Connector".
3. Erstellen einer IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Service > EC2** aus.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die soeben erstellte Richtlinie anhängen.
   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

Ergebnis

Sie verfügen jetzt über eine IAM-Rolle, die Sie während der Implementierung über den AWS Marketplace mit

der EC2-Instanz verknüpfen können.

Schritt 3: Überprüfen Sie die Instanzanforderungen

Wenn Sie den Connector erstellen, müssen Sie einen EC2-Instanztyp auswählen, der die folgenden Anforderungen erfüllt.

CPU
: 4 Kerne oder 4 vCPUs

RAM
: 14 GB

Instanztyp für AWS EC2
: Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.xlarge.

Schritt 4: Erstellen Sie den Konnektor

Erstellen Sie den Connector direkt über AWS Marketplace.

Über diese Aufgabe

Beim Erstellen des Connectors aus dem AWS Marketplace wird eine EC2-Instanz in AWS mit einer Standardkonfiguration bereitgestellt. "Informieren Sie sich über die Standardkonfiguration des Connectors".

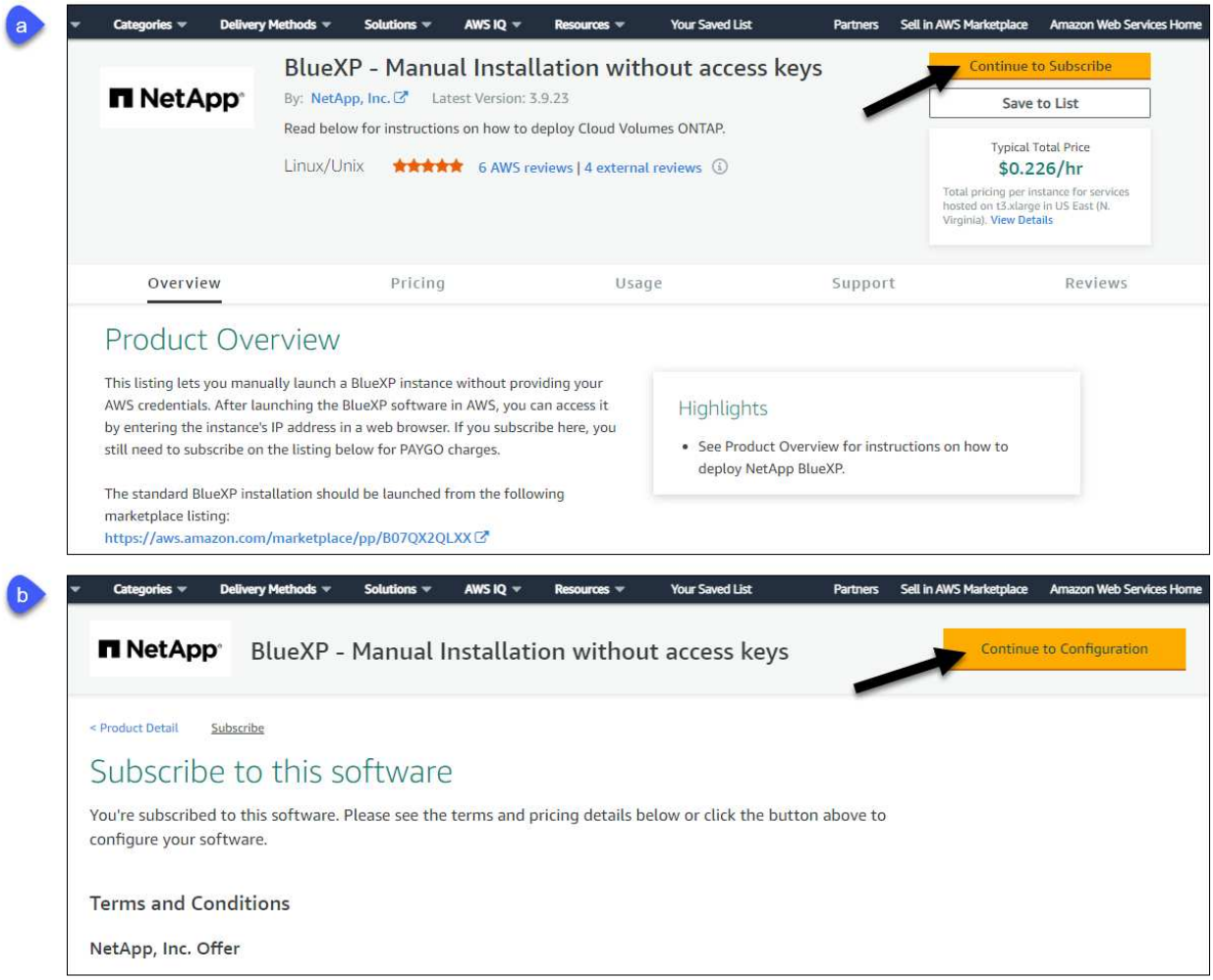
Bevor Sie beginnen

Sie sollten Folgendes haben:

- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt
- Eine IAM-Rolle mit angehängter Richtlinie, die die erforderlichen Berechtigungen für den Connector enthält.
- Berechtigung zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Verständnis der CPU- und RAM-Anforderungen für die Instanz.
- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

1. Wechseln Sie zum "Seite „BlueXP“ im AWS Marketplace"
2. Wählen Sie auf der Marketplace-Seite **Weiter zu Abonnieren** und wählen Sie dann **Weiter zu Konfiguration**.



3. Ändern Sie eine der Standardoptionen, und wählen Sie **Weiter zum Starten**.
4. Wählen Sie unter **Aktion auswählen** die Option **über EC2 starten** aus und wählen Sie dann **Start** aus.

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

5. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:
   - **Name und Tags**: Geben Sie einen Namen und Tags für die Instanz ein.
   - **Anwendung und Betriebssystembild**: Überspringen Sie diesen Abschnitt. Der Stecker AMI ist bereits ausgewählt.
   - **Instanztyp**: Wählen Sie je nach Verfügbarkeit der Region einen Instanztyp aus, der den RAM- und CPU-Anforderungen entspricht (t3.xlarge wird empfohlen).
   - **Schlüsselpaar (Login)**: Wählen Sie das Schlüsselpaar aus, mit dem Sie eine sichere Verbindung zur Instanz herstellen möchten.
   - **Netzwerkeinstellungen**: Bearbeiten Sie die Netzwerkeinstellungen nach Bedarf:
     - Wählen Sie die gewünschte VPC und das Subnetz.
     - Geben Sie an, ob die Instanz eine öffentliche IP-Adresse haben soll.

- Legen Sie Firewall-Einstellungen fest, die die erforderlichen Verbindungsmethoden für die Connector-Instanz SSH, HTTP und HTTPS aktivieren.

  Für spezifische Konfigurationen sind noch einige Regeln erforderlich.

  "Sicherheitsgruppen-Regeln für AWS ansehen".

- **Configure Storage**: Behalten Sie die Standardgröße und den Festplattentyp für das Root-Volume bei.

  Wenn Sie die Amazon EBS-Verschlüsselung auf dem Root-Volume aktivieren möchten, wählen Sie **Erweitert**, erweitern **Volume 1**, wählen **verschlüsselt** und wählen dann einen KMS-Schlüssel aus.

- **Erweiterte Details**: Unter **IAM Instance profile** wählen Sie die IAM-Rolle, die die erforderlichen Berechtigungen für den Connector enthält.
- **Zusammenfassung**: Überprüfen Sie die Zusammenfassung und wählen Sie **Launch Instance**.

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

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

   https://ipaddress

7. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das BlueXP Konto an, das dem Connector zugeordnet werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Unter **laufen Sie in einer gesicherten Umgebung?** Sperrmodus deaktiviert halten.

      Sie sollten den eingeschränkten Modus deaktiviert halten, da nachfolgend beschrieben wird, wie Sie BlueXP im Standardmodus verwenden. Der eingeschränkte Modus sollte nur aktiviert werden, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den BlueXP Backend-Services trennen möchten. Wenn das der Fall ist, "Befolgen Sie die Schritte für den Einstieg in BlueXP im eingeschränkten Modus".

   d. Wählen Sie **Start**.

Ergebnis

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

Öffnen Sie einen Webbrowser, und rufen Sie den auf "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

Wenn sich in demselben AWS-Konto, bei dem der Connector erstellt wurde, Amazon S3-Buckets befinden, wird automatisch eine Amazon S3-Arbeitsumgebung auf dem BlueXP-Bildschirm angezeigt. "Erfahren Sie, wie Sie S3-Buckets aus BlueXP managen"

Installieren Sie den Connector manuell in AWS

Um den Connector manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Host-Anforderungen überprüfen, Ihr Netzwerk einrichten, AWS-Berechtigungen vorbereiten, den Connector installieren und dann die Berechtigungen bereitstellen, die Sie vorbereitet haben.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 und 7.9
- Red hat Enterprise Linux 7.6, 7.7, 7.8 und 7.9

  Der Host muss bei Red hat Subscription Management registriert sein. Wenn er nicht registriert ist, kann der Host während der Connector-Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

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

Hypervisor

Ein Bare-Metal- oder Hosted-Hypervisor, der für Ubuntu, CentOS oder Red hat Enterprise Linux zertifiziert ist, ist erforderlich.

"Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Schlüsselpaar

Wenn Sie den Connector erstellen, müssen Sie ein EC2-Schlüsselpaar auswählen, das mit der Instanz verwendet werden soll.

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine ist auf dem Host erforderlich, bevor Sie den Connector installieren.

- Die unterstützte Version ist mindestens 19.3.1.
- Die maximal unterstützte Version ist 25.0.5.

  "Installationsanweisungen anzeigen"

Schritt 2: Netzwerk einrichten

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Connector installieren möchten, die folgenden Anforderungen erfüllt. Durch die Erfüllung dieser Anforderungen kann der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Endpunkte wurden während der manuellen Installation kontaktiert

Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren, benötigt das Installationsprogramm für den Connector während des Installationsprozesses Zugriff auf die folgenden URLs:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Schritt 3: Berechtigungen einrichten

Sie müssen AWS-Berechtigungen für BlueXP bereitstellen, indem Sie eine der folgenden Optionen verwenden:

- Option 1: Erstellen Sie IAM-Richtlinien und hängen Sie die Richtlinien einer IAM-Rolle an, die Sie der EC2-Instanz zuordnen können.
- Option 2: Bereitstellung von BlueXP mit dem AWS Zugriffsschlüssel für einen IAM-Benutzer mit den erforderlichen Berechtigungen

Führen Sie die Schritte zum Vorbereiten von Berechtigungen für BlueXP durch.

IAM-Rolle

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:
   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.

      Abhängig von den BlueXP Services, die Sie planen zu verwenden, müssen Sie möglicherweise eine zweite Richtlinie erstellen. Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich. "Erfahren Sie mehr über IAM-Richtlinien für den Connector".
3. Erstellen einer IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Service > EC2** aus.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die soeben erstellte Richtlinie anhängen.
   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

Ergebnis

Sie verfügen jetzt über eine IAM-Rolle, die Sie nach der Installation des Connectors mit der EC2-Instanz verknüpfen können.

AWS-Zugriffsschlüssel

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:

   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.

      Abhängig von den BlueXP Services, die Sie planen zu verwenden, müssen Sie möglicherweise eine zweite Richtlinie erstellen.

   Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich. "Erfahren Sie mehr über IAM-Richtlinien für den Connector".
3. Fügen Sie die Richtlinien einem IAM-Benutzer hinzu.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie nach der Installation des Connectors zu BlueXP hinzufügen können.

Ergebnis

Sie verfügen jetzt über einen IAM-Benutzer mit den erforderlichen Berechtigungen und einem Zugriffsschlüssel, den Sie BlueXP bereitstellen können.

Schritt 4: Installieren Sie den Stecker

Nachdem die Voraussetzungen erfüllt sind, können Sie die Software manuell auf Ihrem eigenen Linux-Host installieren.

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Root-Berechtigungen zum Installieren des Connectors.
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, aber dafür muss der Connector neu gestartet werden.

  Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

- Ein CA-signiertes Zertifikat, wenn der Proxy-Server HTTPS verwendet oder wenn der Proxy ein abfangenden Proxy ist.

Über diese Aufgabe

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

Schritte

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

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

2. Wenn die Systemvariablen *http_Proxy* oder *https_Proxy* auf dem Host festgelegt sind, entfernen Sie sie:

   ```
   unset http_proxy
   unset https_proxy
   ```

   Wenn Sie diese Systemvariablen nicht entfernen, schlägt die Installation fehl.

3. Laden Sie die Connector-Software von der herunter "NetApp Support Website", Und dann kopieren Sie es auf den Linux-Host.

   Sie sollten das Installationsprogramm für den „Online“-Connector herunterladen, das für den Einsatz in Ihrem Netzwerk oder in der Cloud gedacht ist. Für den Connector ist ein separater „Offline“-Installer verfügbar, der jedoch nur für Bereitstellungen im privaten Modus unterstützt wird.

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Führen Sie das Installationsskript aus.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

Die Parameter --Proxy und --cacert sind optional. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

Hier sehen Sie ein Beispiel für den Befehl mit beiden optionalen Parametern:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--Proxy konfiguriert den Connector so, dass er einen HTTP- oder HTTPS-Proxy-Server in einem der folgenden Formate verwendet:

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Beachten Sie Folgendes:

  - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
  - Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie oben gezeigt verwenden.
  - BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

6. Warten Sie, bis die Installation abgeschlossen ist.

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

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

https://ipaddress

8. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das BlueXP Konto an, das dem Connector zugeordnet werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Unter **laufen Sie in einer gesicherten Umgebung?** Sperrmodus deaktiviert halten.

      Sie sollten den eingeschränkten Modus deaktiviert halten, da nachfolgend beschrieben wird, wie Sie BlueXP im Standardmodus verwenden. Der eingeschränkte Modus sollte nur aktiviert werden, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den BlueXP Backend-Services trennen möchten. Wenn das der Fall ist, "Befolgen Sie die Schritte für den Einstieg in BlueXP im eingeschränkten Modus".

   d. Wählen Sie **Start**.

Ergebnis

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

Wenn sich in demselben AWS-Konto, bei dem der Connector erstellt wurde, Amazon S3-Buckets befinden, wird automatisch eine Amazon S3-Arbeitsumgebung auf dem BlueXP-Bildschirm angezeigt. "Erfahren Sie, wie Sie S3-Buckets aus BlueXP managen"

Schritt 5: Berechtigungen für BlueXP bereitstellen

Nachdem Sie den Connector installiert haben, müssen Sie BlueXP mit den zuvor festgelegten AWS Berechtigungen versehen. Durch die Berechtigungen kann BlueXP Ihre Daten- und Storage-Infrastruktur in AWS managen.

IAM-Rolle

Fügen Sie die zuvor erstellte IAM-Rolle der Connector EC2-Instanz hinzu.

Schritte

1. Wechseln Sie zur Amazon EC2-Konsole.
2. Wählen Sie **Instanzen**.
3. Wählen Sie die Connector-Instanz aus.
4. Wählen Sie **Actions > Security > Modify IAM Role** aus.
5. Wählen Sie die IAM-Rolle aus und wählen Sie **IAM-Rolle aktualisieren**.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Aktionen in AWS benötigt.

Wechseln Sie zum "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

AWS-Zugriffsschlüssel

Bereitstellen von BlueXP mit dem AWS-Zugriffsschlüssel für einen IAM-Benutzer, der über die erforderlichen Berechtigungen verfügt

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 **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten im Assistenten.
   a. **Anmeldeort**: Wählen Sie **Amazon Web Services > Connector**.
   b. **Zugangsdaten definieren**: 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.
   d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Aktionen in AWS benötigt.

Wechseln Sie zum "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

Azure

Optionen für die Connector-Installation in Azure

Es gibt verschiedene Möglichkeiten, einen Connector in Azure zu erstellen. Dies ist die

gängigste Methode – direkt von BlueXP.

Folgende Installationsoptionen sind verfügbar:

- "Connector direkt aus BlueXP erstellen" (Dies ist die Standardoption)

  Mit dieser Aktion wird eine VM gestartet, auf der Linux und die Connector-Software in einem vnet Ihrer Wahl ausgeführt werden.

- "Erstellen Sie einen Connector aus dem Azure Marketplace"

  Mit dieser Aktion wird auch eine VM gestartet, auf der Linux und die Connector-Software ausgeführt werden. Die Bereitstellung wird jedoch direkt über den Azure Marketplace statt über BlueXP gestartet.

- "Laden Sie die Software herunter, und installieren Sie sie manuell auf Ihrem eigenen Linux-Host"

Die von Ihnen gewählte Installationsoption wirkt sich auf die Vorbereitung auf die Installation aus. Dazu gehört auch, wie Sie BlueXP die erforderlichen Berechtigungen bereitstellen, die es zum Authentifizieren und Managen von Ressourcen in Azure benötigt.

Erstellen Sie einen Connector in Azure von BlueXP

Um einen Connector in Azure aus BlueXP zu erstellen, müssen Sie Ihr Netzwerk einrichten, Azure Berechtigungen vorbereiten und anschließend den Connector erstellen.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Connector installieren möchten, die folgenden Anforderungen erfüllt. Durch die Erfüllung dieser Anforderungen kann der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen.

Azure Region

Wenn Sie Cloud Volumes ONTAP verwenden, sollte der Connector in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP-Systeme oder in der bereitgestellt werden "Azure Region Paar" Für die Cloud Volumes ONTAP Systeme. Diese Anforderung stellt sicher, dass eine Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Storage-Konten verwendet wird.

"Erfahren Sie, wie Cloud Volumes ONTAP einen privaten Azure Link nutzt"

Vnet und Subnetz

Wenn Sie den Connector erstellen, müssen Sie das vnet und das Subnetz angeben, in dem sich der Connector befinden soll.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Endpunkte wurden über die BlueXP Konsole kontaktiert

Bei der Nutzung der webbasierten Konsole von BlueXP, die über die SaaS-Schicht bereitgestellt wird, werden mehrere Endpunkte kontaktiert, um Datenmanagement-Aufgaben durchzuführen. Dazu gehören Endpunkte, die kontaktiert werden, um den Connector über die BlueXP Konsole zu implementieren.

"Eine Liste der Endpunkte, die über die BlueXP Konsole kontaktiert wurden, wird angezeigt".

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Sie müssen diese Netzwerkanforderung implementieren, nachdem Sie den Connector erstellt haben.

Schritt 2: Erstellen Sie eine benutzerdefinierte Rolle

Erstellen Sie eine benutzerdefinierte Azure Rolle, die Sie Ihrem Azure Konto oder einem Microsoft Entra-Dienstprinzipal zuweisen können. BlueXP authentifiziert sich mit Azure und verwendet diese Berechtigungen, um die Connector-Instanz in Ihrem Auftrag zu erstellen.

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"

Schritte

1. Kopieren Sie die erforderlichen Berechtigungen für eine neue benutzerdefinierte Rolle in Azure und speichern Sie sie in einer JSON-Datei.

Diese benutzerdefinierte Rolle enthält nur die Berechtigungen, die zum Starten der Connector-VM in Azure von BlueXP erforderlich sind. Verwenden Sie diese Richtlinie nicht für andere Situationen. Wenn BlueXP den Connector erstellt, wendet er eine neue Gruppe von Berechtigungen auf die Connector-VM an, die es dem Connector ermöglicht, die Ressourcen in Ihrer Public-Cloud-Umgebung zu verwalten.

```
{
    "Name": "Azure SetupAsService",
    "Actions": [
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/locations/operations/read",
        "Microsoft.Compute/operations/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Network/locations/operationResults/read",
        "Microsoft.Network/locations/operations/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",
```

```
"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. Ändern Sie den JSON, indem Sie Ihre Azure Abonnement-ID dem zuweisbaren Umfang hinzufügen.

   Beispiel

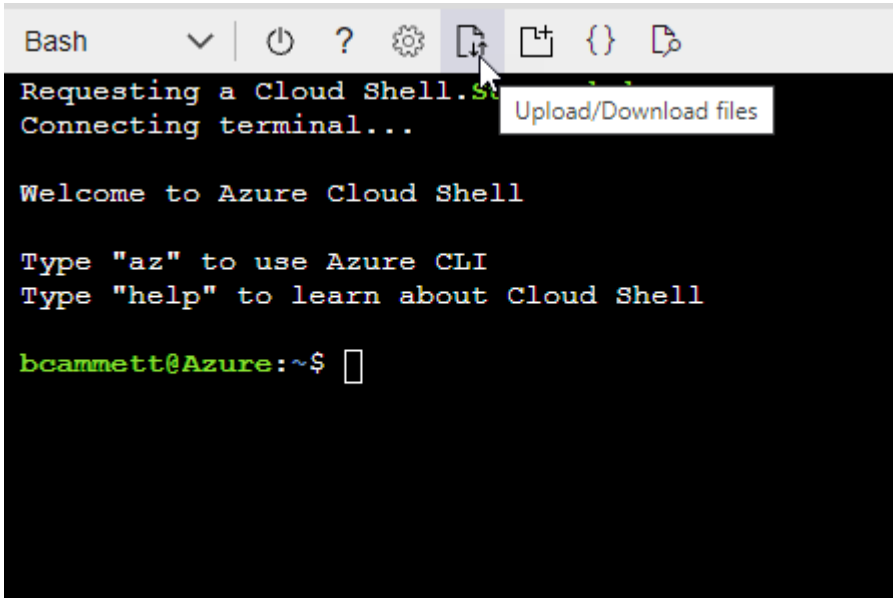
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

3. 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.

a. Starten "Azure Cloud Shell" Und wählen Sie die Bash-Umgebung.

b. Laden Sie die JSON-Datei hoch.



c. Geben Sie den folgenden Befehl der Azure CLI ein:

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

Sie sollten jetzt eine benutzerdefinierte Rolle namens *Azure SetupAsService* haben. Sie können diese benutzerdefinierte Rolle nun auf Ihr Benutzerkonto oder auf einen Dienstprinzipal anwenden.

Schritt 3: Einrichten der Authentifizierung

Beim Erstellen des Connector aus BlueXP müssen Sie eine Anmeldung bereitstellen, mit der BlueXP eine Authentifizierung bei Azure und die Implementierung der VM ermöglichen kann. Sie haben zwei Möglichkeiten:

1. Melden Sie sich bei der entsprechenden Aufforderung mit Ihrem Azure-Konto an. Dieses Konto muss über spezifische Azure Berechtigungen verfügen. Dies ist die Standardoption.
2. Geben Sie Details zu einem Dienstprinzipal von Microsoft Entra an. Dieser Service-Principal erfordert auch spezielle Berechtigungen.

Befolgen Sie die Schritte, um eine dieser Authentifizierungsmethoden für die Verwendung mit BlueXP vorzubereiten.

Azure Konto

Weisen Sie die benutzerdefinierte Rolle dem Benutzer zu, der den Connector aus BlueXP bereitstellen wird.

Schritte

1. Öffnen Sie im Azure-Portal den Dienst **Abonnements** und wählen Sie das Abonnement des Benutzers aus.
2. Klicken Sie auf **Access Control (IAM)**.
3. Klicken Sie auf **Hinzufügen** > **Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
   a. Wählen Sie die Rolle **Azure SetupAsService** aus und klicken Sie auf **Weiter**.

   > Azure SetupAsService ist der Standardname, der in der Connector Deployment Policy für Azure angegeben ist. Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

   b. **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.
   c. Klicken Sie auf **Mitglieder auswählen**, wählen Sie Ihr Benutzerkonto aus und klicken Sie auf **Auswählen**.
   d. Klicken Sie Auf **Weiter**.
   e. Klicken Sie auf **Review + Assign**.

Ergebnis

Der Azure-Benutzer verfügt nun über die erforderlichen Berechtigungen für die Bereitstellung des Connectors von BlueXP.

Service-Principal

Anstatt sich mit Ihrem Azure Konto anzumelden, können Sie BlueXP mit den Zugangsdaten für einen Azure Serviceprinzipal bereitstellen, der über die erforderlichen Berechtigungen verfügt.

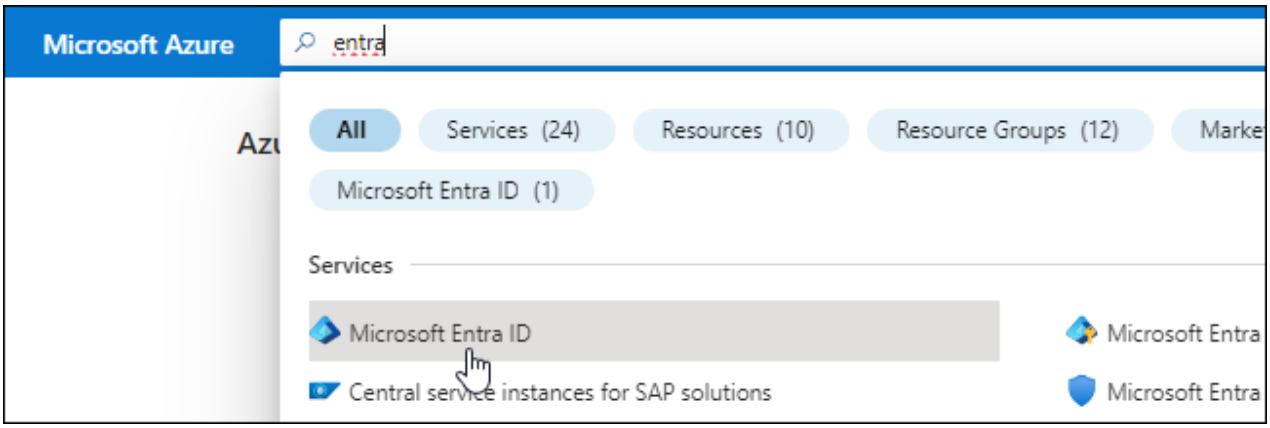
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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**.

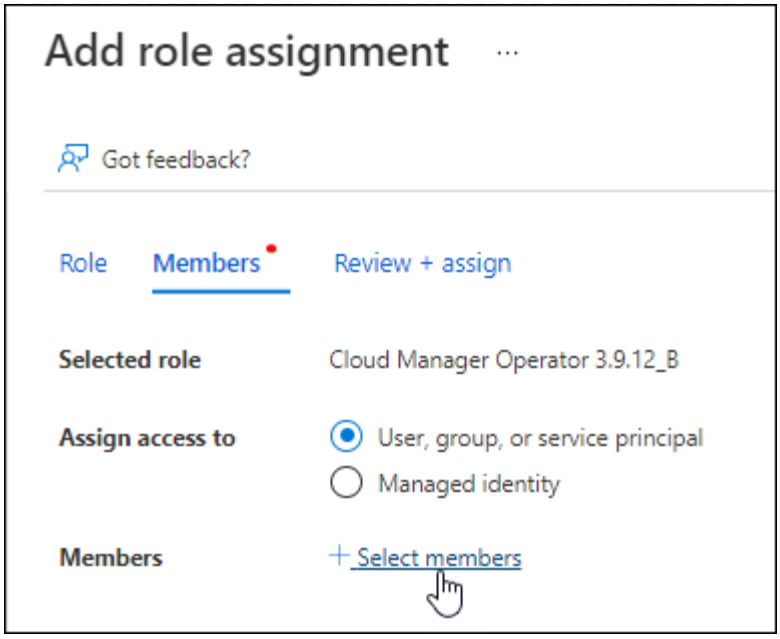
   Sie haben die AD-Anwendung und den Service-Principal erstellt.

Weisen Sie der Anwendung die benutzerdefinierte Rolle zu

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

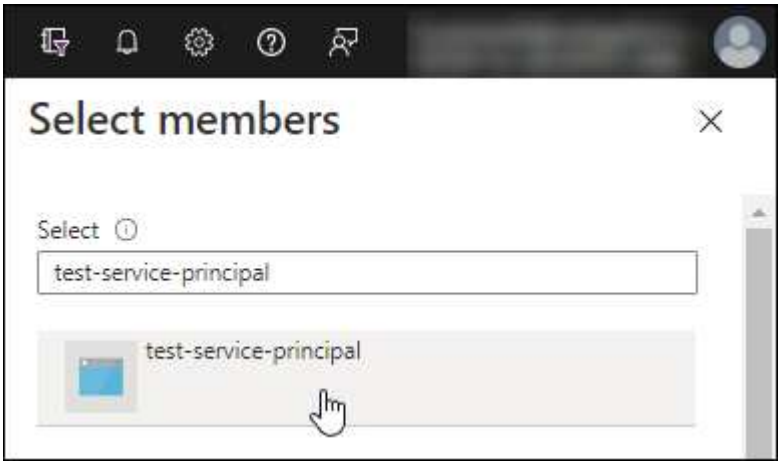
   a. **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.

   b. Klicken Sie auf **Mitglieder auswählen**.



c. Suchen Sie nach dem Namen der Anwendung.

   Hier ein Beispiel:



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

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

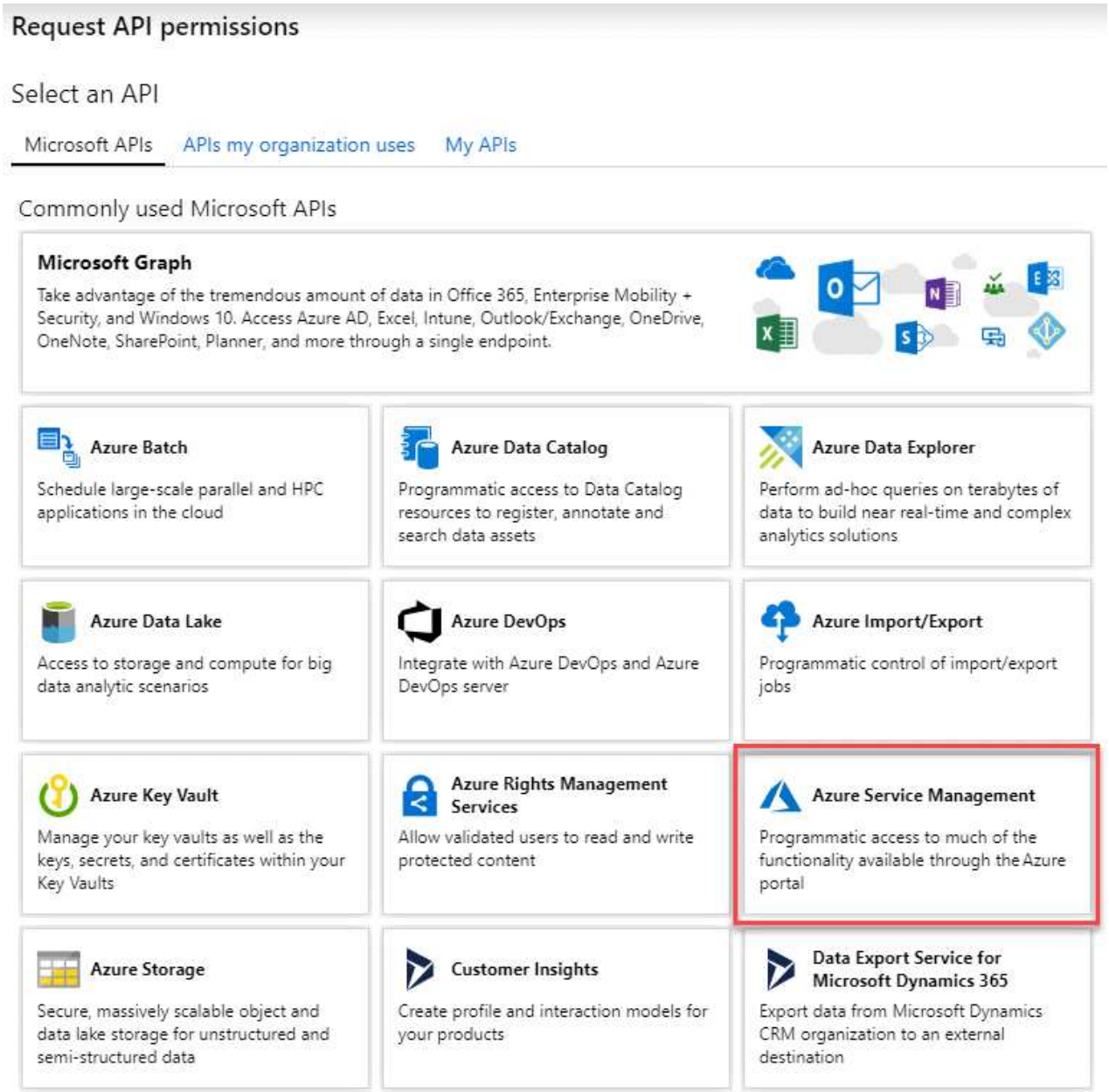
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

   Wenn Sie Ressourcen in mehreren Azure-Abonnements managen möchten, müssen Sie den Service-Prinzipal an jedes dieser Abonnements binden. Mit BlueXP können Sie beispielsweise das Abonnement auswählen, das Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten.

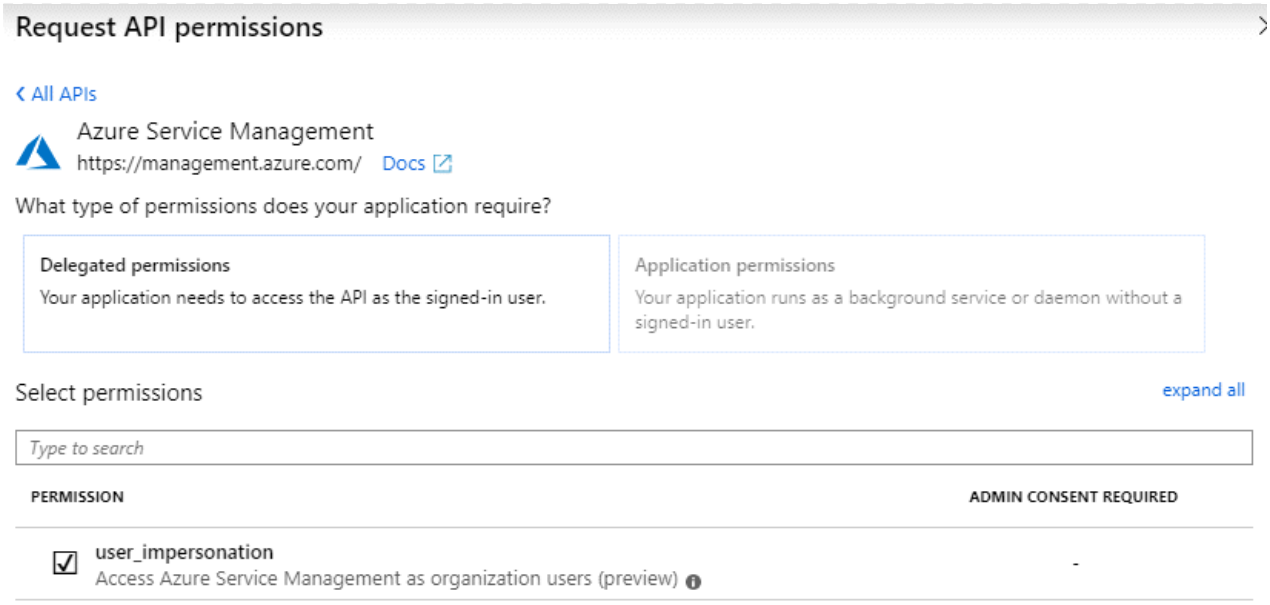
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

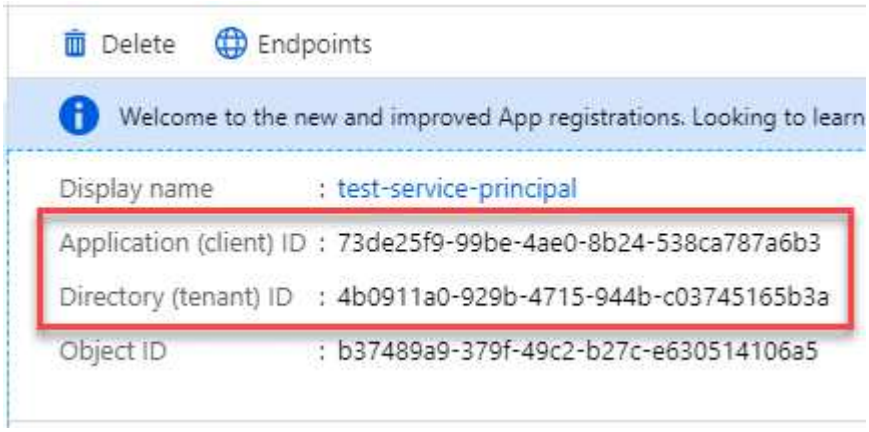


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



Die Anwendungs-ID und die Verzeichnis-ID für die Anwendung abrufen

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

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 den Connector erstellen.

Schritt 4: Erstellen Sie den Konnektor

Erstellen Sie den Connector direkt über die webbasierte Konsole von BlueXP.

Über diese Aufgabe

Beim Erstellen des Connectors aus BlueXP wird eine Virtual Machine in Azure mithilfe einer Standardkonfiguration implementiert. Nachdem Sie den Connector erstellt haben, sollten Sie nicht zu einem kleineren VM-Typ wechseln, der weniger CPU oder RAM hat. "Informieren Sie sich über die Standardkonfiguration des Connectors".

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Ein Azure Abonnement.
- Eine vnet und Subnetz in Ihrer bevorzugten Azure-Region.
- Details zu einem Proxy-Server, wenn Ihr Unternehmen einen Proxy für den gesamten ausgehenden Internet-Datenverkehr benötigt:
  - IP-Adresse
  - Anmeldedaten
  - HTTPS-Zertifikat
- Ein öffentlicher SSH-Schlüssel, wenn Sie diese Authentifizierungsmethode für die virtuelle Connector-Maschine verwenden möchten. Die andere Option für die Authentifizierungsmethode ist die Verwendung eines Passworts.

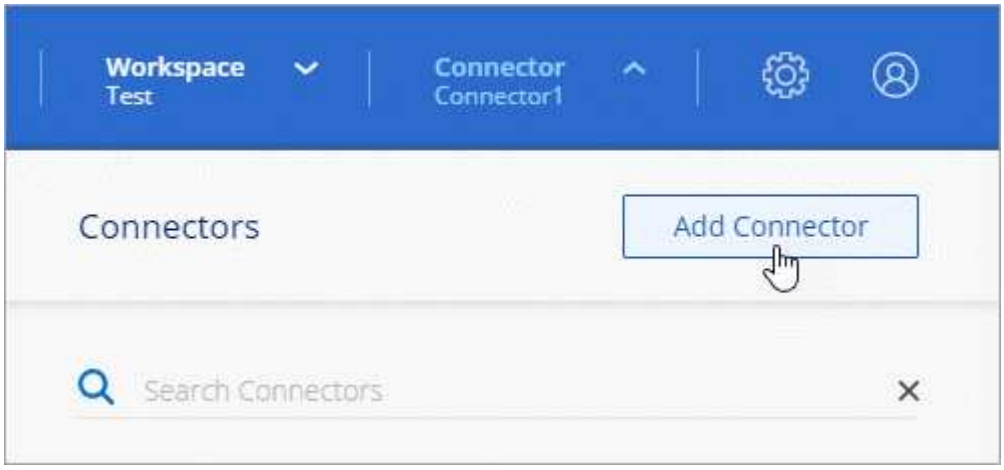
  "Erfahren Sie mehr über die Verbindung mit einer Linux VM in Azure"

- Wenn Sie nicht möchten, dass BlueXP automatisch eine Azure-Rolle für den Connector erstellt, müssen Sie Ihre eigene erstellen "Verwenden der Richtlinie auf dieser Seite".

  Diese Berechtigungen gelten für die Connector-Instanz selbst. Es handelt sich um einen anderen Berechtigungssatz als zuvor für die Bereitstellung der Connector-VM eingerichtet.

Schritte

1. Wählen Sie die Dropdown-Liste **Connector** aus und wählen Sie **Connector hinzufügen** aus.



2. Wählen Sie als Cloud-Provider * Microsoft Azure* aus.
3. Auf der Seite * Ansetzen eines Konnektors*:

   a. Wählen Sie unter **Authentication** die Authentifizierungsoption aus, die der Einrichtung von Azure-Berechtigungen entspricht:

      - Wählen Sie **Azure-Benutzerkonto**, um sich bei Ihrem Microsoft-Konto anzumelden, das die erforderlichen Berechtigungen haben sollte.

        Das Formular ist Eigentum von Microsoft und wird von Microsoft gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.

        > Wenn Sie bereits bei einem Azure-Konto angemeldet sind, nutzt BlueXP das Konto automatisch. Wenn Sie über mehrere Konten verfügen, müssen Sie sich möglicherweise erst abmelden, um sicherzustellen, dass Sie das richtige Konto verwenden.

      - Wählen Sie **Active Directory Service Principal** aus, um Informationen über den Microsoft Entra Service Principal einzugeben, der die erforderlichen Berechtigungen gewährt:
        - Anwendungs-ID (Client)
        - ID des Verzeichnisses (Mandant)
        - Client-Schlüssel

   Erfahren Sie, wie Sie diese Werte für einen Service-Prinzipal erhalten.

4. Befolgen Sie die Schritte im Assistenten, um den Konnektor zu erstellen:

   - **VM-Authentifizierung**: Wählen Sie ein Azure-Abonnement, einen Speicherort, eine neue Ressourcengruppe oder eine vorhandene Ressourcengruppe und wählen Sie dann eine Authentifizierungsmethode für die von Ihnen erstellte virtuelle Connector-Maschine aus.

     Die Authentifizierungsmethode für die virtuelle Maschine kann ein Passwort oder ein öffentlicher SSH-Schlüssel sein.

   "Erfahren Sie mehr über die Verbindung mit einer Linux VM in Azure"

- **Details**: Geben Sie einen Namen für die Instanz ein, geben Sie Tags an und wählen Sie aus, ob BlueXP eine neue Rolle mit den erforderlichen Berechtigungen erstellen soll oder ob Sie eine vorhandene Rolle auswählen möchten, die Sie mit eingerichtet haben "Die erforderlichen Berechtigungen".

  Beachten Sie, dass Sie die mit dieser Rolle verknüpften Azure Abonnements auswählen können. Jedes Abonnement, das Sie auswählen, stellt die Connector-Berechtigungen zum Verwalten von Ressourcen in diesem Abonnement bereit (z. B. Cloud Volumes ONTAP).

- **Netzwerk**: Wählen Sie ein vnet und Subnetz, ob eine öffentliche IP-Adresse aktiviert werden soll, und geben Sie optional eine Proxy-Konfiguration an.
- **Sicherheitsgruppe**: Wählen Sie, ob Sie eine neue Sicherheitsgruppe erstellen möchten oder ob Sie eine vorhandene Sicherheitsgruppe auswählen möchten, die die erforderlichen ein- und ausgehenden Regeln zulässt.

  "Zeigen Sie die Regeln für Sicherheitsgruppen für Azure an".

- **Review**: Überprüfen Sie Ihre Auswahl, um zu überprüfen, ob Ihre Einrichtung korrekt ist.

5. Klicken Sie Auf **Hinzufügen**.

   Die Virtual Machine sollte in ca. 7 Minuten einsatzbereit sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Ergebnis

Nach Abschluss des Prozesses ist der Connector für die Nutzung über BlueXP verfügbar.

Wenn Azure Blob Storage in demselben Azure Abonnement genutzt wird, in dem der Connector erstellt wurde, wird automatisch eine Azure Blob Storage-Arbeitsumgebung auf dem BlueXP Bildschirm angezeigt. "Erfahren Sie, wie Sie Azure Blob Storage aus BlueXP managen"

Erstellen Sie einen Connector aus dem Azure Marketplace

Zum Erstellen eines Connectors aus dem Azure Marketplace müssen Sie das Netzwerk einrichten, die Azure Berechtigungen vorbereiten, die Instanzanforderungen prüfen und dann den Connector erstellen.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Connector installieren möchten, die folgenden Anforderungen erfüllt. Durch die Erfüllung dieser Anforderungen kann der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen.

Azure Region

Wenn Sie Cloud Volumes ONTAP verwenden, sollte der Connector in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP-Systeme oder in der bereitgestellt werden "Azure Region Paar" Für die Cloud Volumes ONTAP Systeme. Diese Anforderung stellt sicher, dass eine Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Storage-Konten verwendet wird.

"Erfahren Sie, wie Cloud Volumes ONTAP einen privaten Azure Link nutzt"

Vnet und Subnetz

Wenn Sie den Connector erstellen, müssen Sie das vnet und das Subnetz angeben, in dem sich der Connector befinden soll.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.

Endpunkte	Zweck
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Sie müssen diese Netzwerkanforderung implementieren, nachdem Sie den Connector erstellt haben.

Schritt 2: Überprüfung der VM-Anforderungen

Wenn Sie den Connector erstellen, müssen Sie einen virtuellen Maschinentyp auswählen, der die folgenden Anforderungen erfüllt.

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Azure VM-Größe

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

Schritt 3: Berechtigungen einrichten

Sie haben folgende Möglichkeiten, Berechtigungen bereitzustellen:

- Option 1: Weisen Sie der Azure VM eine benutzerdefinierte Rolle mit einer vom System zugewiesenen gemanagten Identität zu.
- Option 2: Bereitstellung der Zugangsdaten für einen Azure Serviceprinzipal für BlueXP mit den erforderlichen Berechtigungen

Führen Sie die folgenden Schritte aus, um Berechtigungen für BlueXP einzurichten.

Benutzerdefinierte 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"

Schritte

1. Wenn Sie planen, die Software manuell auf Ihrem eigenen Host zu installieren, aktivieren Sie eine vom System zugewiesene verwaltete Identität auf der VM, sodass Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

   "Microsoft Azure-Dokumentation: Gemanagte Identitäten für Azure-Ressourcen auf einer VM über das Azure-Portal konfigurieren"

2. Kopieren Sie den Inhalt des "Benutzerdefinierte Rollenberechtigungen für den Konnektor" Und speichern Sie sie in einer JSON-Datei.
3. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

   Sie sollten für jedes Azure-Abonnement, das Sie mit BlueXP verwenden möchten, die ID hinzufügen.

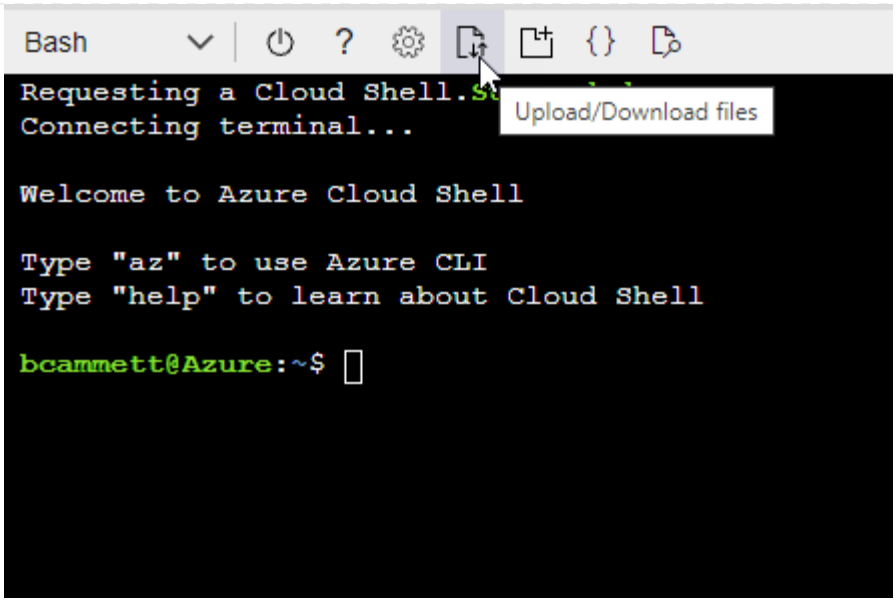
   Beispiel

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

4. 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.

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



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

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

Ergebnis

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

Service-Principal

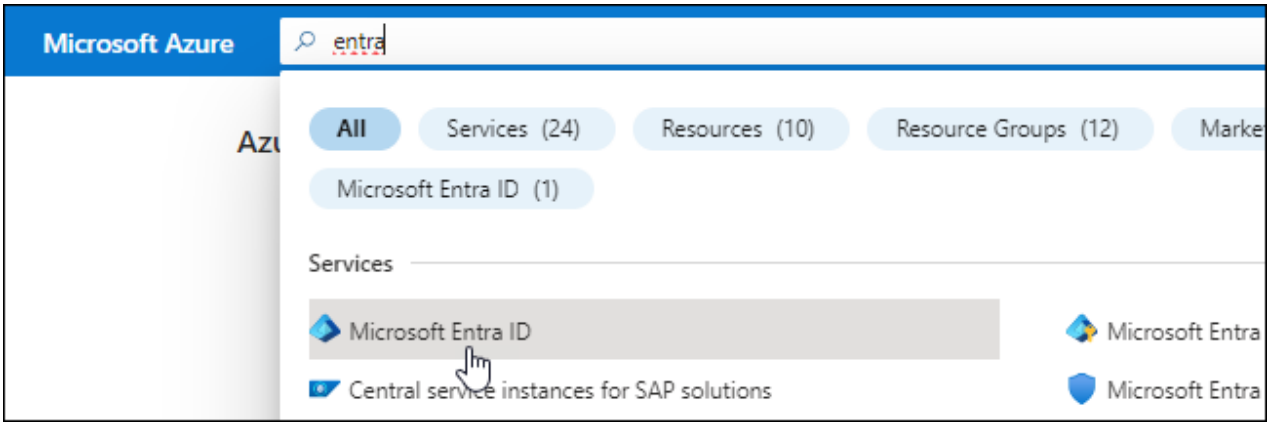
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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.

Anwendung einer Rolle zuweisen

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.

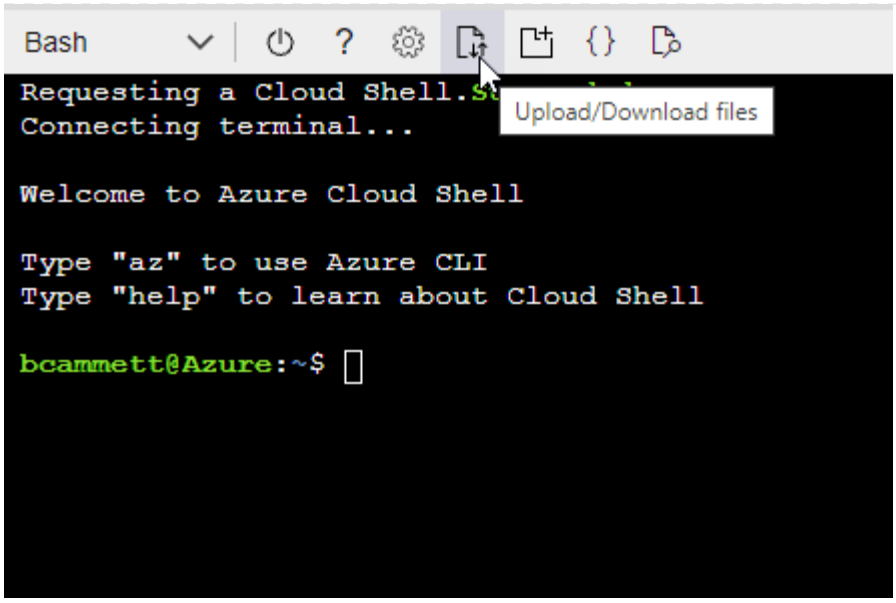
      Beispiel

      ```
      "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:

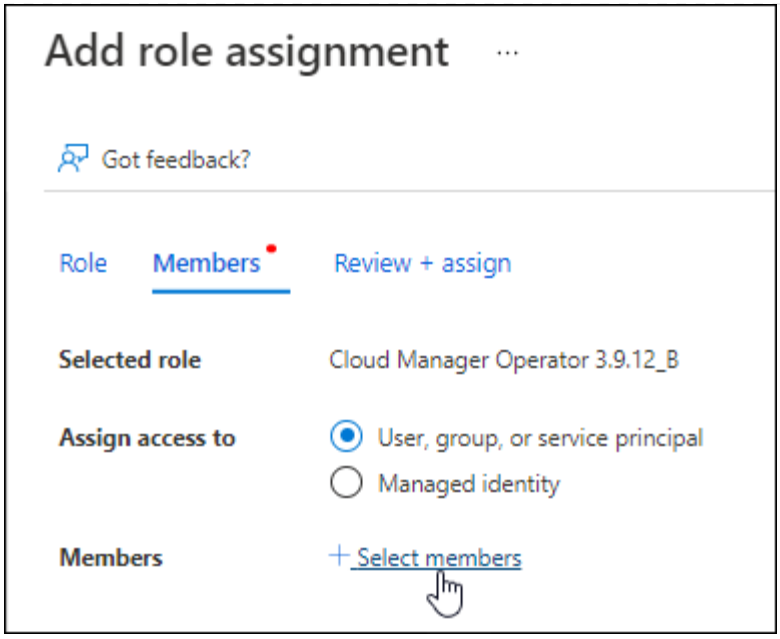
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

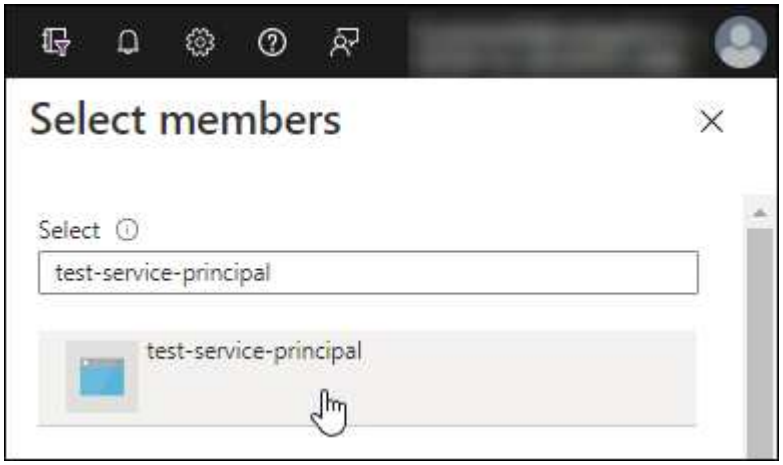
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

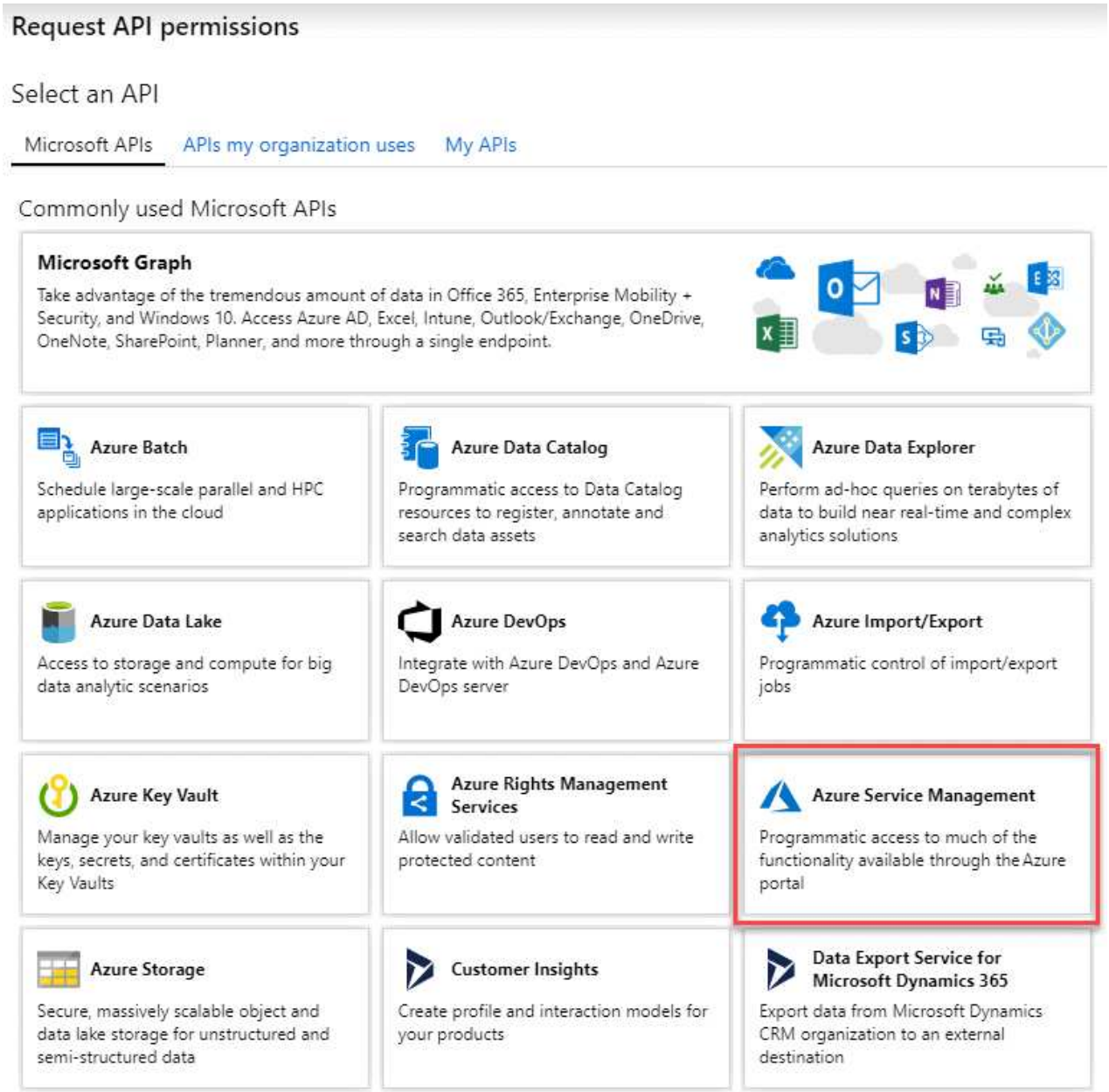
Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

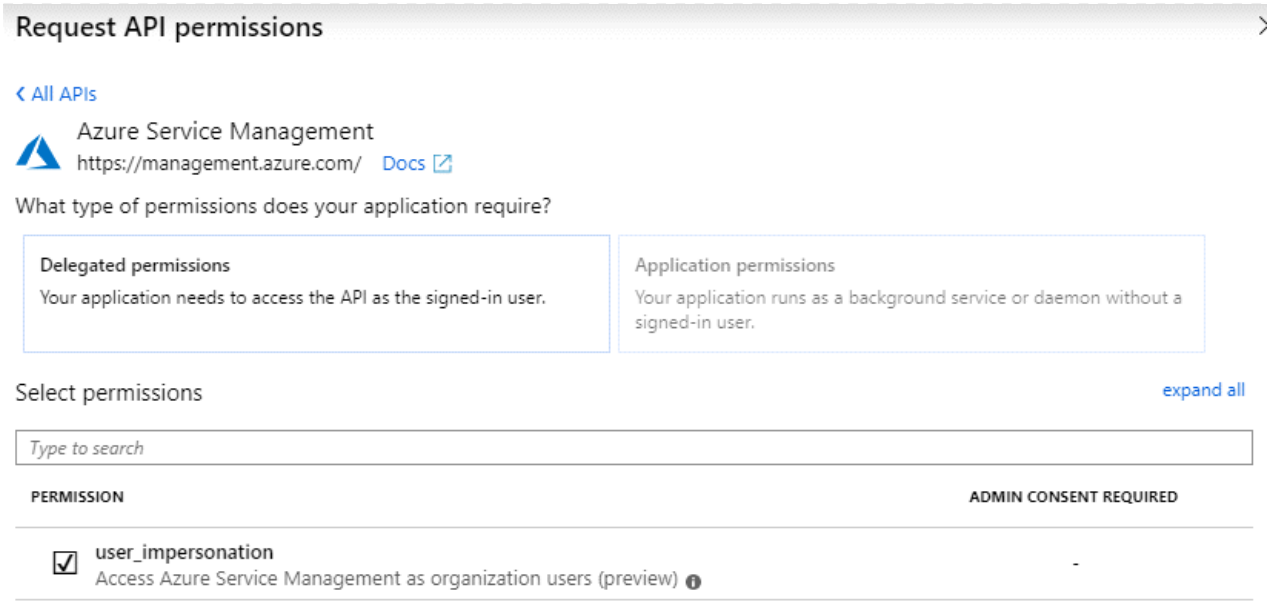
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

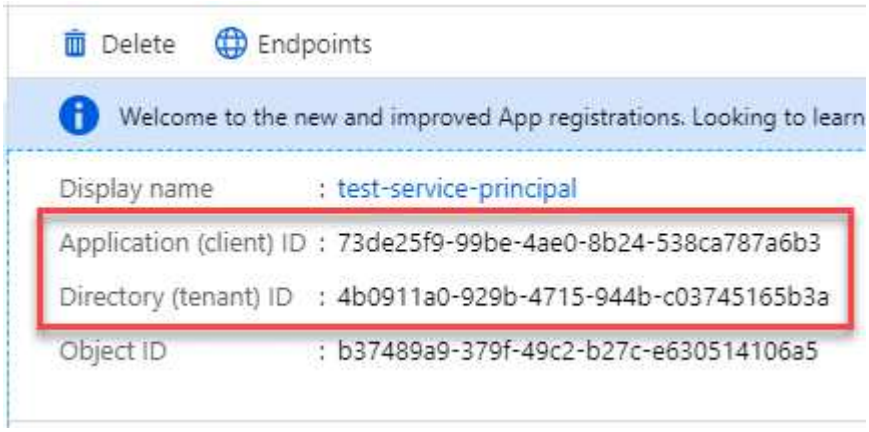


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



Die Anwendungs-ID und die Verzeichnis-ID für die Anwendung abrufen

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

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.

Schritt 4: Erstellen Sie den Konnektor

Starten Sie den Connector direkt über den Azure Marketplace.

Über diese Aufgabe

Beim Erstellen des Connectors aus dem Azure Marketplace wird eine Virtual Machine in Azure mithilfe einer Standardkonfiguration bereitgestellt. "Informieren Sie sich über die Standardkonfiguration des Connectors".

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Ein Azure Abonnement.
- Eine vnet und Subnetz in Ihrer bevorzugten Azure-Region.
- Details zu einem Proxy-Server, wenn Ihr Unternehmen einen Proxy für den gesamten ausgehenden Internet-Datenverkehr benötigt:
  - IP-Adresse
  - Anmeldedaten
  - HTTPS-Zertifikat
- Ein öffentlicher SSH-Schlüssel, wenn Sie diese Authentifizierungsmethode für die virtuelle Connector-Maschine verwenden möchten. Die andere Option für die Authentifizierungsmethode ist die Verwendung eines Passworts.

  "Erfahren Sie mehr über die Verbindung mit einer Linux VM in Azure"

- Wenn Sie nicht möchten, dass BlueXP automatisch eine Azure-Rolle für den Connector erstellt, müssen Sie Ihre eigene erstellen "Verwenden der Richtlinie auf dieser Seite".

  Diese Berechtigungen gelten für die Connector-Instanz selbst. Es handelt sich um einen anderen Berechtigungssatz als zuvor für die Bereitstellung der Connector-VM eingerichtet.

Schritte

1. Wechseln Sie im Azure Marketplace auf die Seite NetApp Connector VM.

"Azure Marketplace-Seite für kommerzielle Regionen"

2. Wählen Sie **Jetzt holen** und wählen Sie dann **Weiter**.
3. Wählen Sie im Azure-Portal **Create** aus und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

   Beachten Sie beim Konfigurieren der VM Folgendes:

   - **VM-Größe**: Wählen Sie eine VM-Größe, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen DS3 v2.
   - **Disks**: Der Connector kann mit HDD- oder SSD-Festplatten optimal funktionieren.
   - **Netzwerksicherheitsgruppe**: Der Connector benötigt eingehende Verbindungen über SSH, HTTP und HTTPS.

     "Zeigen Sie die Regeln für Sicherheitsgruppen für Azure an".

   - **Identität**: Unter **Verwaltung** wählen Sie **System zugewiesene verwaltete Identität aktivieren**.

     Diese Einstellung ist wichtig, da eine verwaltete Identität es der virtuellen Connector-Maschine ermöglicht, sich ohne Angabe von Anmeldeinformationen mit Microsoft Entra ID zu identifizieren. "Erfahren Sie mehr über Managed Identitäten für Azure Ressourcen".

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

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

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

   https://ipaddress

6. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das BlueXP Konto an, das dem Connector zugeordnet werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Unter **laufen Sie in einer gesicherten Umgebung?** Sperrmodus deaktiviert halten.

      Sie sollten den eingeschränkten Modus deaktiviert halten, da nachfolgend beschrieben wird, wie Sie BlueXP im Standardmodus verwenden. Der eingeschränkte Modus sollte nur aktiviert werden, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den BlueXP Backend-Services trennen möchten. Wenn das der Fall ist, "Befolgen Sie die Schritte für den Einstieg in BlueXP im eingeschränkten Modus".

   d. Wählen Sie **Start**.

Ergebnis

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

Wenn Azure Blob Storage in demselben Azure Abonnement genutzt wird, in dem der Connector erstellt wurde, wird automatisch eine Azure Blob Storage-Arbeitsumgebung auf dem BlueXP Bildschirm angezeigt. "Erfahren Sie, wie Sie Azure Blob Storage aus BlueXP managen"

Schritt 5: Berechtigungen für BlueXP bereitstellen

Nachdem Sie den Connector erstellt haben, müssen Sie BlueXP nun die Berechtigungen zuweisen, die Sie zuvor eingerichtet haben. Durch die Berechtigungen kann BlueXP Ihre Daten- und Storage-Infrastruktur in Azure managen.

Benutzerdefinierte Rolle

Wechseln Sie zum Azure-Portal und weisen Sie der virtuellen Connector-Maschine für ein oder mehrere Abonnements die benutzerdefinierte Azure-Rolle zu.

Schritte

1. Öffnen Sie im Azure Portal den Service **Abonnements** und wählen Sie Ihr Abonnement aus.

   Es ist wichtig, die Rolle aus dem Dienst **Subscriptions** zuzuweisen, da hier der Umfang der Rollenzuweisung auf Abonnementebene festgelegt ist. Der *scope* definiert die Ressourcen, für die der Zugriff gilt. Wenn Sie einen Umfang auf einer anderen Ebene angeben (z. B. auf Ebene der Virtual Machines), wirkt es sich darauf aus, dass Sie Aktionen aus BlueXP ausführen können.

   "Microsoft Azure Dokumentation: Umfang für die rollenbasierte Zugriffssteuerung von Azure kennen"

2. Wählen Sie **Zugriffskontrolle (IAM)** > **Hinzufügen** > **Rollenzuweisung hinzufügen**.
3. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.

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

4. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
   a. Weisen Sie einer * verwalteten Identität* Zugriff zu.
   b. Wählen Sie **Mitglieder auswählen**, wählen Sie das Abonnement, in dem die virtuelle Connector-Maschine erstellt wurde, unter **verwaltete Identität**, wählen Sie **virtuelle Maschine** und wählen Sie dann die virtuelle Connector-Maschine aus.
   c. Wählen Sie **Auswählen**.
   d. Wählen Sie **Weiter**.
   e. Wählen Sie **Überprüfen + Zuweisen**.
   f. Wenn Sie Ressourcen in weiteren Azure-Abonnements managen möchten, wechseln Sie zu diesem Abonnement und wiederholen Sie die folgenden Schritte.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Was kommt als Nächstes?

Wechseln Sie zum "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

Service-Principal

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

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Installieren Sie den Connector manuell in Azure

Um den Connector manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Host-Anforderungen überprüfen, Ihr Netzwerk einrichten, Azure-Berechtigungen vorbereiten, den Connector installieren und dann die von Ihnen vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 und 7.9
- Red hat Enterprise Linux 7.6, 7.7, 7.8 und 7.9

  Der Host muss bei Red hat Subscription Management registriert sein. Wenn er nicht registriert ist, kann der Host während der Connector-Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

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

Hypervisor

Ein Bare-Metal- oder Hosted-Hypervisor, der für Ubuntu, CentOS oder Red hat Enterprise Linux zertifiziert ist, ist erforderlich.

"Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Azure VM-Größe

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

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine ist auf dem Host erforderlich, bevor Sie den Connector installieren.

- Die unterstützte Version ist mindestens 19.3.1.
- Die maximal unterstützte Version ist 25.0.5.

"Installationsanweisungen anzeigen"

Schritt 2: Netzwerk einrichten

Stellen Sie sicher, dass der Netzwerkspeicherort, an dem Sie den Connector installieren möchten, die folgenden Anforderungen erfüllt. Durch die Erfüllung dieser Anforderungen kann der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen.

Azure Region

Wenn Sie Cloud Volumes ONTAP verwenden, sollte der Connector in derselben Azure-Region wie die von ihm verwalteten Cloud Volumes ONTAP-Systeme oder in der bereitgestellt werden "Azure Region Paar" Für die Cloud Volumes ONTAP Systeme. Diese Anforderung stellt sicher, dass eine Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und den zugehörigen Storage-Konten verwendet wird.

"Erfahren Sie, wie Cloud Volumes ONTAP einen privaten Azure Link nutzt"

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Endpunkte wurden während der manuellen Installation kontaktiert

Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren, benötigt das Installationsprogramm für den Connector während des Installationsprozesses Zugriff auf die folgenden URLs:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.

Endpunkte	Zweck
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert

wird. "Weitere Informationen zur BlueXP Klassifizierung"

Schritt 3: Berechtigungen einrichten

Sie müssen Azure-Berechtigungen für BlueXP bereitstellen, indem Sie eine der folgenden Optionen verwenden:

- Option 1: Weisen Sie der Azure VM eine benutzerdefinierte Rolle mit einer vom System zugewiesenen gemanagten Identität zu.
- Option 2: Bereitstellung der Zugangsdaten für einen Azure Serviceprinzipal für BlueXP mit den erforderlichen Berechtigungen

Führen Sie die Schritte zum Vorbereiten von Berechtigungen für BlueXP durch.

Benutzerdefinierte 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"

Schritte

1. Wenn Sie planen, die Software manuell auf Ihrem eigenen Host zu installieren, aktivieren Sie eine vom System zugewiesene verwaltete Identität auf der VM, sodass Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

   "Microsoft Azure-Dokumentation: Gemanagte Identitäten für Azure-Ressourcen auf einer VM über das Azure-Portal konfigurieren"

2. Kopieren Sie den Inhalt des "Benutzerdefinierte Rollenberechtigungen für den Konnektor" Und speichern Sie sie in einer JSON-Datei.
3. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

   Sie sollten für jedes Azure-Abonnement, das Sie mit BlueXP verwenden möchten, die ID hinzufügen.

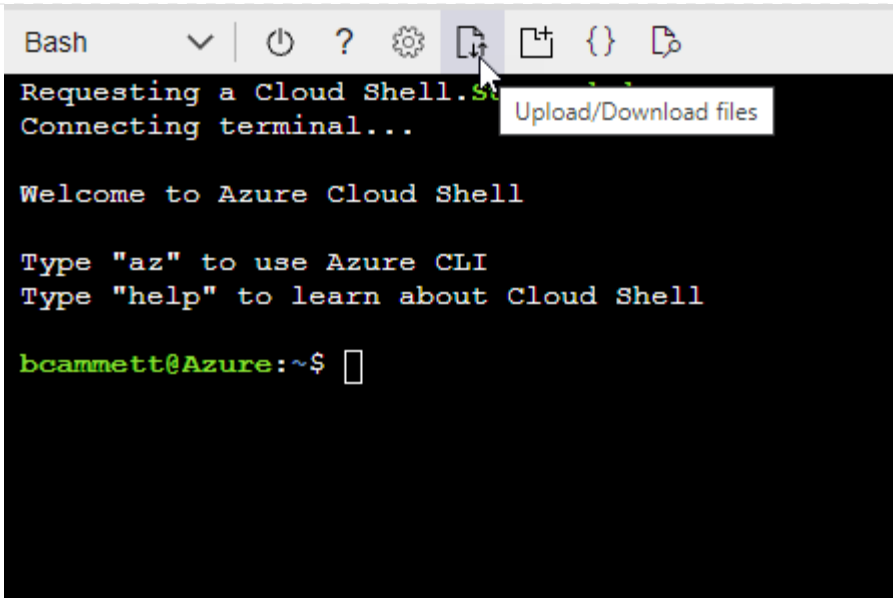
   Beispiel

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

4. 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.

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



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

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

Ergebnis

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

Service-Principal

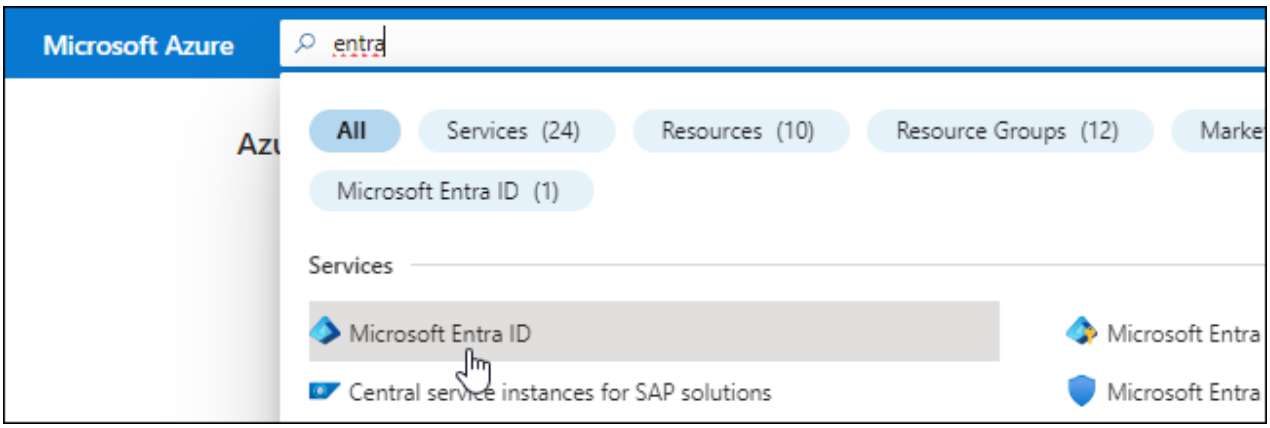
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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.

Anwendung einer Rolle zuweisen

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.

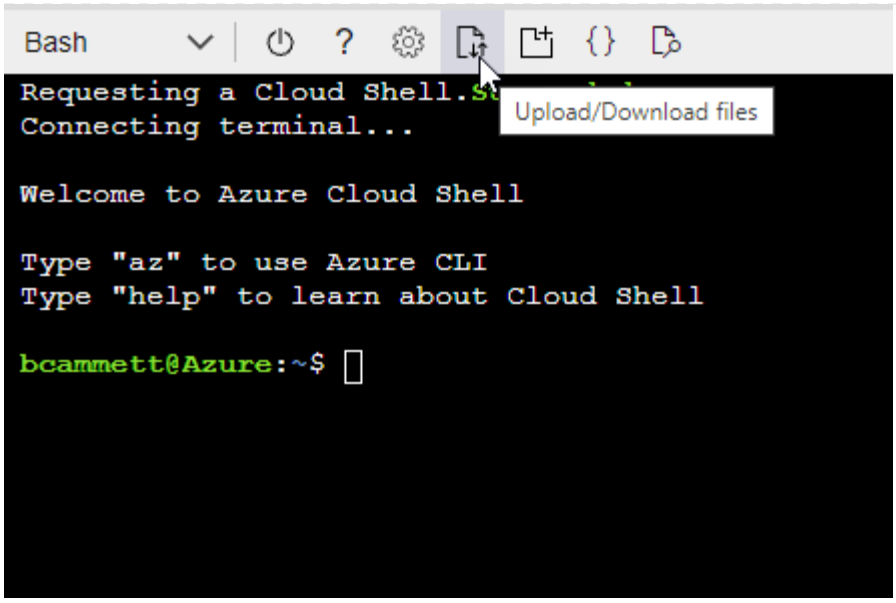
      Beispiel

      ```
      "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**.

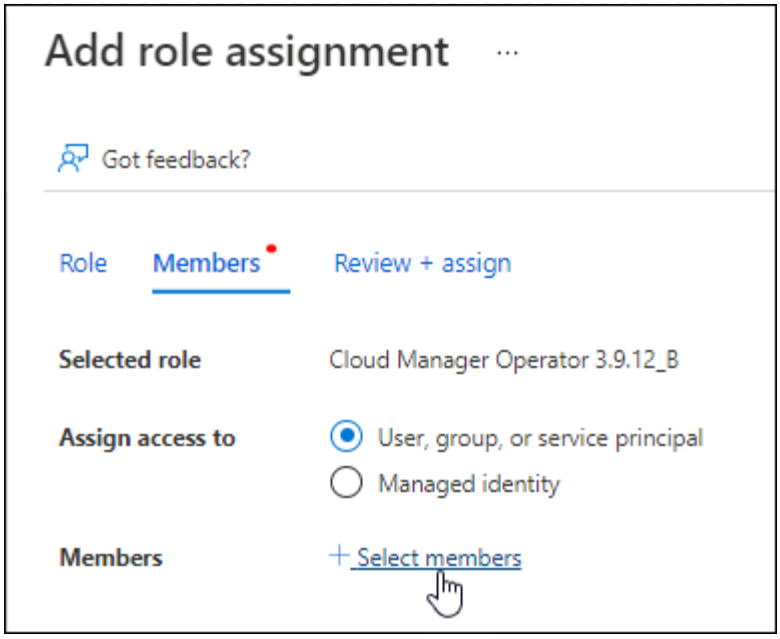
   b. Wählen Sie das Abonnement aus.

   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.

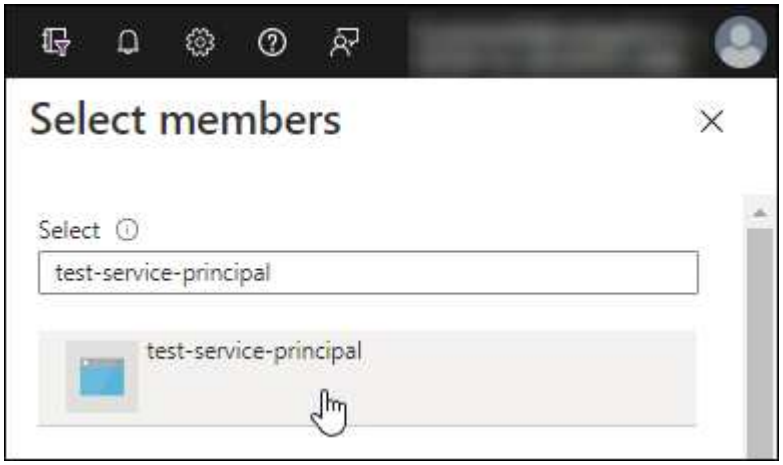
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - **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**.

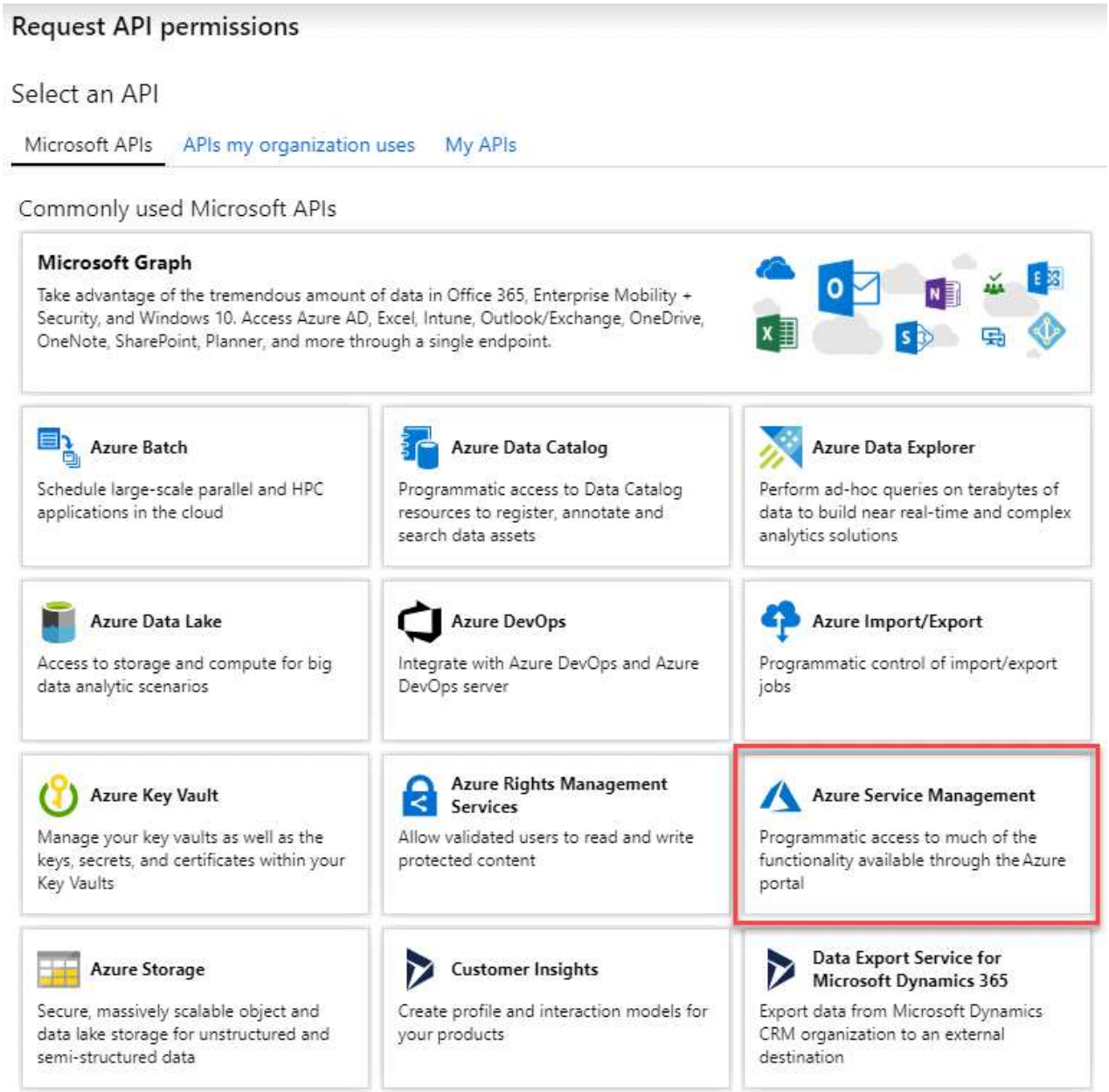
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

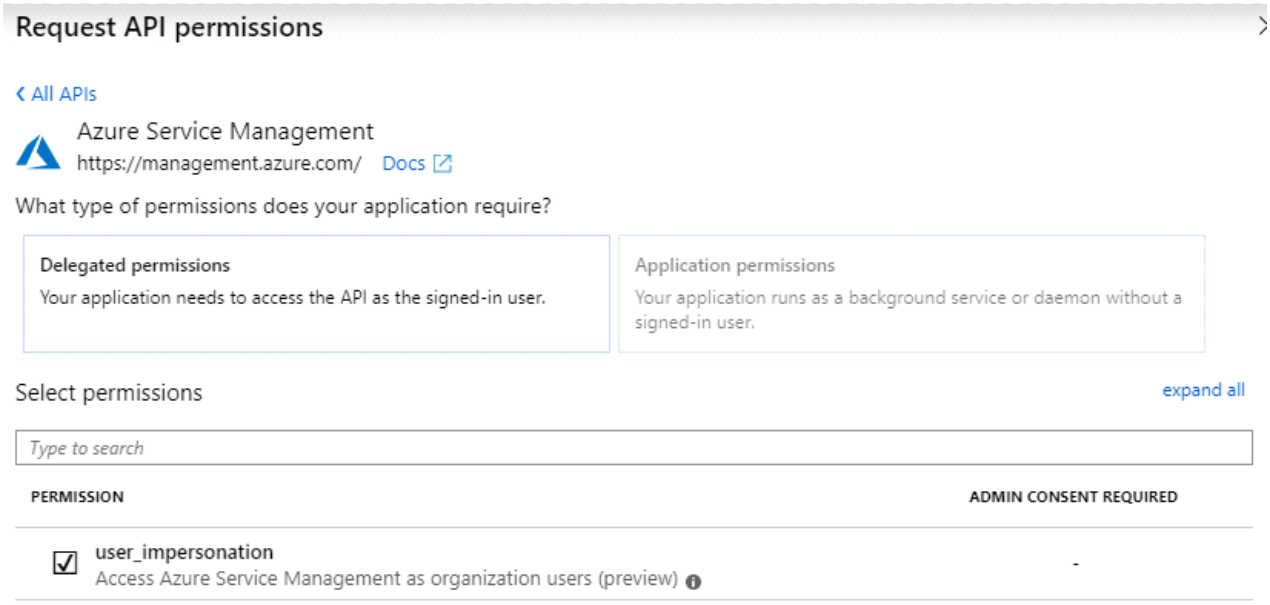
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

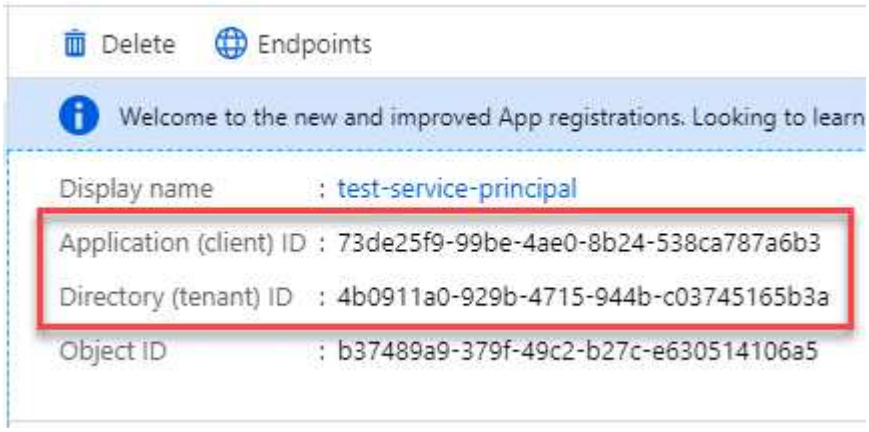


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



Die Anwendungs-ID und die Verzeichnis-ID für die Anwendung abrufen

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

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.

Schritt 4: Installieren Sie den Stecker

Nachdem die Voraussetzungen erfüllt sind, können Sie die Software manuell auf Ihrem eigenen Linux-Host installieren.

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Root-Berechtigungen zum Installieren des Connectors.
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, aber dafür muss der Connector neu gestartet werden.

  Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

- Ein CA-signiertes Zertifikat, wenn der Proxy-Server HTTPS verwendet oder wenn der Proxy ein abfangenden Proxy ist.
- Eine gemanagte Identität, die auf der VM in Azure aktiviert ist, sodass Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

  "Microsoft Azure-Dokumentation: Gemanagte Identitäten für Azure-Ressourcen auf einer VM über das Azure-Portal konfigurieren"

Über diese Aufgabe

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

Schritte

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

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

2. Wenn die Systemvariablen *http_Proxy* oder *https_Proxy* auf dem Host festgelegt sind, entfernen Sie sie:

```
unset http_proxy
unset https_proxy
```

   Wenn Sie diese Systemvariablen nicht entfernen, schlägt die Installation fehl.

3. Laden Sie die Connector-Software von der herunter "NetApp Support Website", Und dann kopieren Sie es auf den Linux-Host.

   Sie sollten das Installationsprogramm für den „Online“-Connector herunterladen, das für den Einsatz in Ihrem Netzwerk oder in der Cloud gedacht ist. Für den Connector ist ein separater „Offline“-Installer verfügbar, der jedoch nur für Bereitstellungen im privaten Modus unterstützt wird.

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Führen Sie das Installationsskript aus.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

   Die Parameter --Proxy und --cacert sind optional. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

   Hier sehen Sie ein Beispiel für den Befehl mit beiden optionalen Parametern:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   --Proxy konfiguriert den Connector so, dass er einen HTTP- oder HTTPS-Proxy-Server in einem der folgenden Formate verwendet:

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port

- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Beachten Sie Folgendes:

  - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
  - Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie oben gezeigt verwenden.
  - BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

6. Warten Sie, bis die Installation abgeschlossen ist.

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

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

   https://ipaddress

8. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das BlueXP Konto an, das dem Connector zugeordnet werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Unter **laufen Sie in einer gesicherten Umgebung?** Sperrmodus deaktiviert halten.

      Sie sollten den eingeschränkten Modus deaktiviert halten, da nachfolgend beschrieben wird, wie Sie BlueXP im Standardmodus verwenden. Der eingeschränkte Modus sollte nur aktiviert werden, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den BlueXP Backend-Services trennen möchten. Wenn das der Fall ist, "Befolgen Sie die Schritte für den Einstieg in BlueXP im eingeschränkten Modus".

   d. Wählen Sie **Start**.

Ergebnis

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

Wenn Azure Blob Storage in demselben Azure Abonnement genutzt wird, in dem der Connector erstellt wurde, wird automatisch eine Azure Blob Storage-Arbeitsumgebung auf dem BlueXP Bildschirm angezeigt. "Erfahren Sie, wie Sie Azure Blob Storage aus BlueXP managen"

Schritt 5: Berechtigungen für BlueXP bereitstellen

Nachdem Sie den Connector jetzt installiert haben, müssen Sie BlueXP die zuvor festgelegten Azure Berechtigungen zuweisen. Durch die Berechtigungen kann BlueXP Ihre Daten- und Storage-Infrastruktur in Azure managen.

Benutzerdefinierte Rolle

Wechseln Sie zum Azure-Portal und weisen Sie der virtuellen Connector-Maschine für ein oder mehrere Abonnements die benutzerdefinierte Azure-Rolle zu.

Schritte

1. Öffnen Sie im Azure Portal den Service **Abonnements** und wählen Sie Ihr Abonnement aus.

   Es ist wichtig, die Rolle aus dem Dienst **Subscriptions** zuzuweisen, da hier der Umfang der Rollenzuweisung auf Abonnementebene festgelegt ist. Der *scope* definiert die Ressourcen, für die der Zugriff gilt. Wenn Sie einen Umfang auf einer anderen Ebene angeben (z. B. auf Ebene der Virtual Machines), wirkt es sich darauf aus, dass Sie Aktionen aus BlueXP ausführen können.

   "Microsoft Azure Dokumentation: Umfang für die rollenbasierte Zugriffssteuerung von Azure kennen"

2. Wählen Sie **Zugriffskontrolle (IAM)** > **Hinzufügen** > **Rollenzuweisung hinzufügen**.
3. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.

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

4. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
   a. Weisen Sie einer * verwalteten Identität* Zugriff zu.
   b. Wählen Sie **Mitglieder auswählen**, wählen Sie das Abonnement, in dem die virtuelle Connector-Maschine erstellt wurde, unter **verwaltete Identität**, wählen Sie **virtuelle Maschine** und wählen Sie dann die virtuelle Connector-Maschine aus.
   c. Wählen Sie **Auswählen**.
   d. Wählen Sie **Weiter**.
   e. Wählen Sie **Überprüfen + Zuweisen**.
   f. Wenn Sie Ressourcen in weiteren Azure-Abonnements managen möchten, wechseln Sie zu diesem Abonnement und wiederholen Sie die folgenden Schritte.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Was kommt als Nächstes?

Wechseln Sie zum "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

Service-Principal

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

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Google Cloud

Connector-Installationsoptionen in Google Cloud

Es gibt verschiedene Möglichkeiten, einen Connector in Google Cloud zu erstellen. Dies ist die gängigste Methode – direkt von BlueXP.

Folgende Installationsoptionen sind verfügbar:

- "Connector direkt aus BlueXP erstellen" (Dies ist die Standardoption)

  Dadurch wird eine VM-Instanz mit Linux und der Connector-Software in einem VPC Ihrer Wahl gestartet.

- "Erstellen Sie den Connector mithilfe von gcloudem"

  Durch diese Aktion wird auch eine VM-Instanz gestartet, auf der Linux und die Connector-Software ausgeführt werden. Die Implementierung wird jedoch direkt aus der Google Cloud anstatt aus BlueXP gestartet.

- "Laden Sie die Software herunter, und installieren Sie sie manuell auf Ihrem eigenen Linux-Host"

Die von Ihnen gewählte Installationsoption wirkt sich auf die Vorbereitung auf die Installation aus. Dazu gehört auch, wie Sie BlueXP die erforderlichen Berechtigungen bereitstellen, die es zum Authentifizieren und Managen von Ressourcen in Google Cloud benötigt.

Connector in Google Cloud von BlueXP oder gcloude erstellen

Um einen Connector in Google Cloud von BlueXP oder mithilfe von gcloude zu erstellen, müssen Sie Ihr Networking einrichten, Google Cloud-Berechtigungen vorbereiten, Google Cloud APIs aktivieren und dann den Connector erstellen.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen kann. Sie müssen beispielsweise sicherstellen, dass Verbindungen für Zielnetzwerke verfügbar sind und dass ein ausgehender Internetzugang verfügbar ist.

VPC und Subnetz

Wenn Sie den Connector erstellen, müssen Sie die VPC und das Subnetz angeben, in dem sich der Connector befinden soll.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.

Endpunkte	Zweck
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Endpunkte wurden über die BlueXP Konsole kontaktiert

Bei der Nutzung der webbasierten Konsole von BlueXP, die über die SaaS-Schicht bereitgestellt wird, werden mehrere Endpunkte kontaktiert, um Datenmanagement-Aufgaben durchzuführen. Dazu gehören Endpunkte, die kontaktiert werden, um den Connector über die BlueXP Konsole zu implementieren.

"Eine Liste der Endpunkte, die über die BlueXP Konsole kontaktiert wurden, wird angezeigt".

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Sie müssen diese Netzwerkanforderung implementieren, nachdem Sie den Connector erstellt haben.

Schritt 2: Richten Sie die Berechtigungen ein, um den Connector zu erstellen

Bevor Sie einen Connector von BlueXP oder mithilfe von gcloude implementieren können, müssen Sie Berechtigungen für den Google Cloud-Benutzer einrichten, der die Connector-VM implementieren wird.

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

   a. Erstellen Sie eine YAML-Datei mit den folgenden Berechtigungen:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
```

```
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Aktivieren Sie in Google Cloud die Cloud Shell.

c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen enthält.

d. Erstellen Sie mithilfe von eine benutzerdefinierte Rolle `gcloud iam roles create` Befehl.

   Im folgenden Beispiel wird auf Projektebene eine Rolle namens „connectorDeployment“ erstellt:

   Gcloud iam-Rollen erstellen connectorDeployment --project=myproject --file=Connector -Deployment.yaml

"Google Cloud docs: Erstellen und Verwalten benutzerdefinierter Rollen"

2. Weisen Sie diese benutzerdefinierte Rolle dem Benutzer zu, der den Connector von BlueXP oder über

gcloude implementieren wird.

"Google Cloud docs: Gewähren Sie eine einzige Rolle"

Ergebnis

Der Google Cloud-Nutzer hat jetzt die erforderlichen Berechtigungen zum Erstellen des Connectors.

Schritt 3: Berechtigungen für den Connector einrichten

Um dem Connector die erforderlichen Berechtigungen für das Ressourcenmanagement in Google Cloud zu geben, ist ein Google Cloud-Servicekonto erforderlich. Wenn Sie den Connector erstellen, müssen Sie dieses Dienstkonto mit der Connector VM verknüpfen.

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

   a. Erstellen Sie eine YAML-Datei, die den Inhalt des enthält "Dienstkontoberechtigungen für den Connector".

   b. Aktivieren Sie in Google Cloud die Cloud Shell.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen enthält.

   d. Erstellen Sie mithilfe von eine benutzerdefinierte Rolle `gcloud iam roles create` Befehl.

      Im folgenden Beispiel wird auf Projektebene eine Rolle namens „Connector“ erstellt:

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Google Cloud docs: Erstellen und Verwalten benutzerdefinierter Rollen"

2. Erstellen Sie ein Service-Konto in Google Cloud und weisen Sie die Rolle dem Service-Konto zu:

   a. Wählen Sie im IAM & Admin-Dienst **Service-Konten > Service-Konto erstellen** aus.

   b. Geben Sie die Details des Servicekontos ein und wählen Sie **Erstellen und Fortfahren**.

   c. Wählen Sie die gerade erstellte Rolle aus.

   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

      "Google Cloud docs: Erstellen eines Dienstkontos"

3. Wenn Sie planen, Cloud Volumes ONTAP-Systeme in verschiedenen Projekten bereitzustellen als das Projekt, in dem sich der Connector befindet, müssen Sie dem Connector-Servicekonto Zugriff auf diese Projekte gewähren.

   Nehmen wir beispielsweise an, dass der Connector in Projekt 1 liegt und Sie Cloud Volumes ONTAP-Systeme in Projekt 2 erstellen möchten. Sie müssen in Projekt 2 Zugriff auf das Servicekonto gewähren.

   a. Wählen Sie aus dem IAM & Admin-Dienst das Google Cloud-Projekt aus, in dem Sie Cloud Volumes ONTAP-Systeme erstellen möchten.

   b. Wählen Sie auf der **IAM**-Seite **Grant Access** und geben Sie die erforderlichen Details ein.

      - Geben Sie die E-Mail des Service-Kontos des Connectors ein.
      - Wählen Sie die benutzerdefinierte Rolle des Connectors aus.
      - Wählen Sie **Speichern**.

Weitere Informationen finden Sie unter "Google Cloud-Dokumentation"

Ergebnis

Das Servicekonto für die Connector-VM wird eingerichtet.

Schritt 4: Einrichtung der gemeinsamen VPC-Berechtigungen

Wenn Sie ein gemeinsam genutztes VPC verwenden, um Ressourcen in einem Serviceprojekt bereitzustellen, müssen Sie Ihre Berechtigungen vorbereiten.

Diese Tabelle dient als Referenz. Ihre Umgebung sollte nach Abschluss der IAM-Konfiguration die Berechtigungstabelle widerspiegeln.

Freigegebene VPC-Berechtigungen anzeigen

Identität	Ersteller	Gehostet in	Berechtigungen für Serviceprojekte	Host-Projektberechtigungen	Zweck
Google-Konto zur Bereitstellung des Connectors	Individuell	Service-Projekt	"Richtlinie für die Connector-Bereitstellung"	compute.networkUser	Bereitstellen des Connectors im Serviceprojekt
Connector-Servicekonto	Individuell	Service-Projekt	"Kontorichtlinie für Connector-Service" Bereitsmanager. Editor	compute.networkUser	Implementierung und Wartung von Cloud Volumes ONTAP und Services im Service-Projekt
Cloud Volumes ONTAP-Servicekonto	Individuell	Service-Projekt	Storage.Administration mitglied: BlueXP Dienstkonto als serviceAccount.user	K. A.	(Optional) für Daten-Tiering sowie Backup und Recovery von BlueXP
Google APIs-Serviceagent	Google Cloud	Service-Projekt	(Standard) Editor	compute.networkUser	Arbeitet im Auftrag der Implementierung mit Google Cloud APIs zusammen. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.
Google Compute Engine Standard-Servicekonto	Google Cloud	Service-Projekt	(Standard) Editor	compute.networkUser	Implementiert Google Cloud-Instanzen und Computing-Infrastrukturen im Auftrag der Implementierung. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.

Hinweise:

1. Wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen, ist encmentmanager.Editor nur beim Host-Projekt erforderlich. BlueXP erstellt eine Bereitstellung im Hostprojekt, die die VPC0-Firewall-Regel enthält, wenn keine Regel angegeben ist.
2. Firewall.create und firewall.delete sind nur erforderlich, wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen. Diese Berechtigungen liegen im BlueXP-Konto .yaml-Datei. Wenn Sie ein HA-Paar mithilfe eines gemeinsam genutzten VPC implementieren, werden diese Berechtigungen verwendet, um die Firewall-Regeln für VPC1, 2 und 3 zu erstellen. Für alle anderen Bereitstellungen werden diese Berechtigungen auch verwendet, um Regeln für VPC0 zu erstellen.
3. Für das Daten-Tiering muss das Tiering-Servicekonto die serviceAccount.user-Rolle auf dem Servicekonto haben, nicht nur auf Projektebene. Derzeit werden serviceAccount.user auf

Projektebene zugewiesen, wenn Sie das Servicekonto mit getIAMPolicy abfragen.

Schritt 5: Google Cloud APIs aktivieren

Bevor Sie den Connector und die Cloud Volumes ONTAP in Google Cloud bereitstellen können, müssen Sie mehrere Google Cloud APIs aktivieren.

Schritt

1. Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt:
   - Cloud Deployment Manager V2-API
   - Cloud-ProtokollierungsAPI
   - Cloud Resource Manager API
   - Compute Engine-API
   - IAM-API (Identitäts- und Zugriffsmanagement
   - KMS-API (Cloud Key Management Service)

     (Nur erforderlich, wenn Sie BlueXP Backup und Recovery mit vom Kunden gemanagten Verschlüsselungsschlüsseln (CMEK) verwenden möchten).

"Google Cloud-Dokumentation: Aktivieren von APIs"

Schritt 6: Erstellen Sie den Konnektor

Erstellen Sie einen Connector direkt über die webbasierte Konsole von BlueXP oder über gcloude.

Über diese Aufgabe

Beim Erstellen des Connectors wird eine Virtual Machine-Instanz in Google Cloud mit einer Standardkonfiguration bereitgestellt. Nachdem Sie den Connector erstellt haben, sollten Sie nicht zu einer kleineren VM-Instanz wechseln, die weniger CPU oder RAM hat. "Informieren Sie sich über die Standardkonfiguration des Connectors".

BlueXP

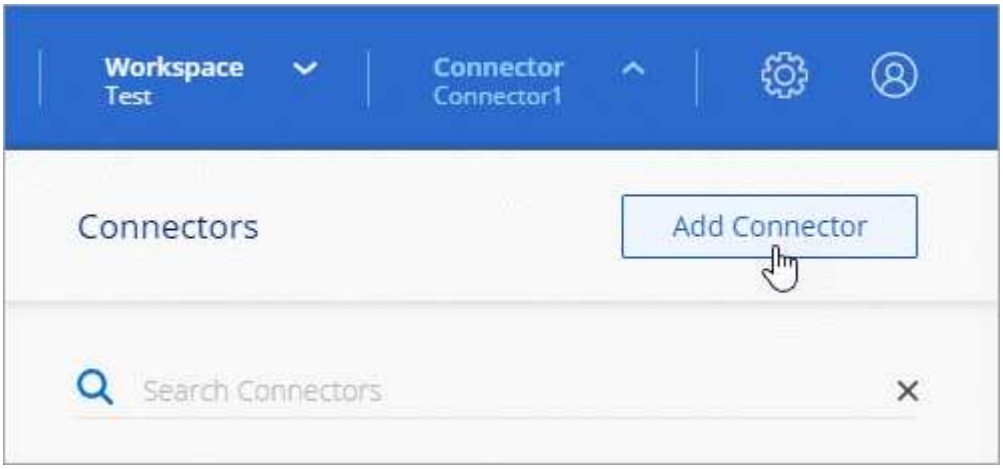
Bevor Sie beginnen

Sie sollten Folgendes haben:

- Die erforderlichen Google Cloud Berechtigungen, um den Connector und ein Servicekonto für die Connector VM zu erstellen.
- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

Schritte

1. Wählen Sie die Dropdown-Liste **Connector** aus und wählen Sie **Connector hinzufügen** aus.



2. Wählen Sie **Google Cloud Platform** als Cloud-Provider.
3. Lesen Sie auf der Seite **Bereitstellen eines Konnektors** die Details dazu, was Sie benötigen. Sie haben zwei Möglichkeiten:
   a. Wählen Sie **Weiter**, um die Bereitstellung mithilfe des Produktleitfadens vorzubereiten. Jeder Schritt im Produktleitfaden enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.
   b. Wählen Sie **Skip to Deployment**, wenn Sie bereits vorbereitet haben, indem Sie die Schritte auf dieser Seite befolgen.
4. Befolgen Sie die Schritte im Assistenten, um den Konnektor zu erstellen:
   - Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der virtuellen Maschineninstanz verfügen sollte.

     Das Formular ist Eigentum und wird von Google gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.
   - **Details**: Geben Sie einen Namen für die virtuelle Maschineninstanz ein, geben Sie Tags an, wählen Sie ein Projekt aus, und wählen Sie dann das Servicekonto aus, das über die erforderlichen Berechtigungen verfügt (Details finden Sie im Abschnitt oben).
   - **Ort**: Geben Sie eine Region, Zone, VPC und Subnetz für die Instanz an.
   - **Netzwerk**: Wählen Sie, ob eine öffentliche IP-Adresse aktiviert werden soll und geben Sie optional eine Proxy-Konfiguration an.

- **Firewallrichtlinie**: Wählen Sie aus, ob eine neue Firewallrichtlinie erstellt werden soll oder ob eine vorhandene Firewallrichtlinie ausgewählt werden soll, die die erforderlichen ein- und ausgehenden Regeln zulässt.

  "Firewall-Regeln in Google Cloud"

- **Review**: Überprüfen Sie Ihre Auswahl, um zu überprüfen, ob Ihre Einrichtung korrekt ist.

5. Wählen Sie **Hinzufügen**.

   Die Instanz sollte in ca. 7 Minuten fertig sein. Sie sollten auf der Seite bleiben, bis der Vorgang abgeschlossen ist.

Ergebnis

Nach Abschluss des Prozesses ist der Connector für die Nutzung über BlueXP verfügbar.

Wenn sich in demselben Google Cloud-Konto, bei dem der Connector erstellt wurde, Google Cloud Storage-Buckets befinden, wird automatisch eine Arbeitsumgebung von Google Cloud Storage auf dem BlueXP-Bildschirm angezeigt. "Erfahren Sie, wie Sie Google Cloud Storage von BlueXP managen"

GCloud

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Die erforderlichen Google Cloud Berechtigungen, um den Connector und ein Servicekonto für die Connector VM zu erstellen.
- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt
- Informationen über die Anforderungen der VM-Instanz.
  - **CPU**: 4 Kerne oder 4 vCPUs
  - **RAM**: 14 GB
  - **Maschinentyp**: Wir empfehlen n2-Standard-4.

    Der Connector wird in Google Cloud auf einer VM-Instanz mit einem Betriebssystem unterstützt, das Shielded VM-Funktionen unterstützt.

Schritte

1. Melden Sie sich am gCloud SDK mit Ihrer bevorzugten Methode an.

   In unseren Beispielen verwenden wir eine lokale Shell mit installiertem gCloud SDK, aber Sie könnten die native Google Cloud Shell in der Google Cloud-Konsole verwenden.

   Weitere Informationen zum Google Cloud SDK finden Sie auf der "Dokumentationsseite für Google Cloud SDK".

2. Stellen Sie sicher, dass Sie als Benutzer angemeldet sind, der über die erforderlichen Berechtigungen verfügt, die im Abschnitt oben definiert sind:

   ```
   gcloud auth list
   ```

   Die Ausgabe sollte Folgendes anzeigen, wobei das * -Benutzerkonto das gewünschte Benutzerkonto

ist, das angemeldet werden soll:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Führen Sie die aus `gcloud compute instances create` Befehl:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

Instanzname
Der gewünschte Instanzname für die VM-Instanz.

Projekt
(Optional) das Projekt, in dem die VM implementiert werden soll.

Service-Konto
Das in der Ausgabe von Schritt 2 angegebene Servicekonto.

Zone
Der Zone, in der die VM implementiert werden soll

Keine Adresse
(Optional) Es wird keine externe IP-Adresse verwendet (Sie benötigen eine Cloud NAT oder einen Proxy, um den Datenverkehr zum öffentlichen Internet zu leiten).

Network-Tag

(Optional) Fügen Sie das Netzwerk-Tagging hinzu, um eine Firewall-Regel mithilfe von Tags zur Connector-Instanz zu verknüpfen

Netzwerkpfad

(Optional) Fügen Sie den Namen des Netzwerks hinzu, in dem der Connector bereitgestellt werden soll (für eine gemeinsame VPC benötigen Sie den vollständigen Pfad).

Subnetz-Pfad

(Optional) Fügen Sie den Namen des Subnetzes hinzu, in dem der Connector bereitgestellt werden soll (für eine freigegebene VPC benötigen Sie den vollständigen Pfad)

Km-Schlüsselpfad

(Optional) Hinzufügen eines KMS-Schlüssels zur Verschlüsselung der Festplatten des Connectors (IAM-Berechtigungen müssen auch angewendet werden)

Weitere Informationen zu diesen Flaggen finden Sie im "Dokumentation des Google Cloud Compute SDK".

+
Wenn der Befehl ausgeführt wird, wird der Connector mit dem Golden Image von NetApp implementiert. Die Connector-Instanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

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

   https://ipaddress

2. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das BlueXP Konto an, das dem Connector zugeordnet werden soll.

      "Mehr zu BlueXP Accounts".

   b. Geben Sie einen Namen für das System ein.

Ergebnis

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

Öffnen Sie einen Webbrowser, und rufen Sie den auf "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

Installieren Sie den Connector manuell in Google Cloud

Um den Connector manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Host-Anforderungen überprüfen, Ihr Netzwerk einrichten, Google Cloud-Berechtigungen vorbereiten, Google Cloud-APIs aktivieren, den Connector installieren und dann die von Ihnen vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 und 7.9
- Red hat Enterprise Linux 7.6, 7.7, 7.8 und 7.9

  Der Host muss bei Red hat Subscription Management registriert sein. Wenn er nicht registriert ist, kann der Host während der Connector-Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

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

Hypervisor

Ein Bare-Metal- oder Hosted-Hypervisor, der für Ubuntu, CentOS oder Red hat Enterprise Linux zertifiziert ist, ist erforderlich.

"Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Google Cloud-Maschinentyp

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

Der Connector wird in Google Cloud auf einer VM-Instanz mit einem unterstützten Betriebssystem unterstützt "Geschirmte VM-Funktionen"

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine ist auf dem Host erforderlich, bevor Sie den Connector installieren.

- Die unterstützte Version ist mindestens 19.3.1.
- Die maximal unterstützte Version ist 25.0.5.

  "Installationsanweisungen anzeigen"

Schritt 2: Netzwerk einrichten

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen kann. Sie müssen beispielsweise sicherstellen, dass Verbindungen für Zielnetzwerke verfügbar sind und dass ein ausgehender Internetzugang verfügbar ist.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Endpunkte wurden während der manuellen Installation kontaktiert

Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren, benötigt das Installationsprogramm für den Connector während des Installationsprozesses Zugriff auf die folgenden URLs:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.

Endpunkte	Zweck
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Schritt 3: Berechtigungen für den Connector einrichten

Um dem Connector die erforderlichen Berechtigungen für das Ressourcenmanagement in Google Cloud zu geben, ist ein Google Cloud-Servicekonto erforderlich. Wenn Sie den Connector erstellen, müssen Sie dieses Dienstkonto mit der Connector VM verknüpfen.

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

   a. Erstellen Sie eine YAML-Datei, die den Inhalt des enthält "Dienstkontoberechtigungen für den Connector".

   b. Aktivieren Sie in Google Cloud die Cloud Shell.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen enthält.

   d. Erstellen Sie mithilfe von eine benutzerdefinierte Rolle `gcloud iam roles create` Befehl.

      Im folgenden Beispiel wird auf Projektebene eine Rolle namens „Connector“ erstellt:

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Google Cloud docs: Erstellen und Verwalten benutzerdefinierter Rollen"

2. Erstellen Sie ein Service-Konto in Google Cloud und weisen Sie die Rolle dem Service-Konto zu:

   a. Wählen Sie im IAM & Admin-Dienst **Service-Konten > Service-Konto erstellen** aus.

   b. Geben Sie die Details des Servicekontos ein und wählen Sie **Erstellen und Fortfahren**.

   c. Wählen Sie die gerade erstellte Rolle aus.

   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

      "Google Cloud docs: Erstellen eines Dienstkontos"

3. Wenn Sie planen, Cloud Volumes ONTAP-Systeme in verschiedenen Projekten bereitzustellen als das Projekt, in dem sich der Connector befindet, müssen Sie dem Connector-Servicekonto Zugriff auf diese Projekte gewähren.

   Nehmen wir beispielsweise an, dass der Connector in Projekt 1 liegt und Sie Cloud Volumes ONTAP-Systeme in Projekt 2 erstellen möchten. Sie müssen in Projekt 2 Zugriff auf das Servicekonto gewähren.

   a. Wählen Sie aus dem IAM & Admin-Dienst das Google Cloud-Projekt aus, in dem Sie Cloud Volumes ONTAP-Systeme erstellen möchten.

   b. Wählen Sie auf der **IAM**-Seite **Grant Access** und geben Sie die erforderlichen Details ein.

      - Geben Sie die E-Mail des Service-Kontos des Connectors ein.
      - Wählen Sie die benutzerdefinierte Rolle des Connectors aus.
      - Wählen Sie **Speichern**.

   Weitere Informationen finden Sie unter "Google Cloud-Dokumentation"

Ergebnis

Das Servicekonto für die Connector-VM wird eingerichtet.

Schritt 4: Einrichtung der gemeinsamen VPC-Berechtigungen

Wenn Sie ein gemeinsam genutztes VPC verwenden, um Ressourcen in einem Serviceprojekt bereitzustellen, müssen Sie Ihre Berechtigungen vorbereiten.

Diese Tabelle dient als Referenz. Ihre Umgebung sollte nach Abschluss der IAM-Konfiguration die Berechtigungstabelle widerspiegeln.

Freigegebene VPC-Berechtigungen anzeigen

Identität	Ersteller	Gehostet in	Berechtigungen für Serviceprojekte	Host-Projektberechtigungen	Zweck
Google-Konto zur Bereitstellung des Connectors	Individuell	Service-Projekt	"Richtlinie für die Connector-Bereitstellung"	compute.networkUser	Bereitstellen des Connectors im Serviceprojekt
Connector-Servicekonto	Individuell	Service-Projekt	"Kontorichtlinie für Connector-Service" Bereitsmanager. Editor	compute.networkUser	Implementierung und Wartung von Cloud Volumes ONTAP und Services im Service-Projekt
Cloud Volumes ONTAP-Servicekonto	Individuell	Service-Projekt	Storage.Administration mitglied: BlueXP Dienstkonto als serviceAccount.user	K. A.	(Optional) für Daten-Tiering sowie Backup und Recovery von BlueXP
Google APIs-Serviceagent	Google Cloud	Service-Projekt	(Standard) Editor	compute.networkUser	Arbeitet im Auftrag der Implementierung mit Google Cloud APIs zusammen. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.
Google Compute Engine Standard-Servicekonto	Google Cloud	Service-Projekt	(Standard) Editor	compute.networkUser	Implementiert Google Cloud-Instanzen und Computing-Infrastrukturen im Auftrag der Implementierung. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.

Hinweise:

1. Wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen, ist encmentmanager.Editor nur beim Host-Projekt erforderlich. BlueXP erstellt eine Bereitstellung im Hostprojekt, die die VPC0-Firewall-Regel enthält, wenn keine Regel angegeben ist.
2. Firewall.create und firewall.delete sind nur erforderlich, wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen. Diese Berechtigungen liegen im BlueXP-Konto .yaml-Datei. Wenn Sie ein HA-Paar mithilfe eines gemeinsam genutzten VPC implementieren, werden diese Berechtigungen verwendet, um die Firewall-Regeln für VPC1, 2 und 3 zu erstellen. Für alle anderen Bereitstellungen werden diese Berechtigungen auch verwendet, um Regeln für VPC0 zu erstellen.
3. Für das Daten-Tiering muss das Tiering-Servicekonto die serviceAccount.user-Rolle auf dem Servicekonto haben, nicht nur auf Projektebene. Derzeit werden serviceAccount.user auf

Projektebene zugewiesen, wenn Sie das Servicekonto mit getIAMPolicy abfragen.

Schritt 5: Google Cloud APIs aktivieren

Bevor Sie Cloud Volumes ONTAP Systeme in Google Cloud bereitstellen können, müssen mehrere Google Cloud APIs aktiviert sein.

Schritt

1. Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt:
    - Cloud Deployment Manager V2-API
    - Cloud-ProtokollierungsAPI
    - Cloud Resource Manager API
    - Compute Engine-API
    - IAM-API (Identitäts- und Zugriffsmanagement
    - KMS-API (Cloud Key Management Service)

      (Nur erforderlich, wenn Sie BlueXP Backup und Recovery mit vom Kunden gemanagten Verschlüsselungsschlüsseln (CMEK) verwenden möchten).

"Google Cloud-Dokumentation: Aktivieren von APIs"

Schritt 6: Installieren Sie den Stecker

Nachdem die Voraussetzungen erfüllt sind, können Sie die Software manuell auf Ihrem eigenen Linux-Host installieren.

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Root-Berechtigungen zum Installieren des Connectors.
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, aber dafür muss der Connector neu gestartet werden.

  Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

- Ein CA-signiertes Zertifikat, wenn der Proxy-Server HTTPS verwendet oder wenn der Proxy ein abfangenden Proxy ist.

Über diese Aufgabe

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

Schritte

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

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

2. Wenn die Systemvariablen *http_Proxy* oder *https_Proxy* auf dem Host festgelegt sind, entfernen Sie sie:

```
unset http_proxy
unset https_proxy
```

   Wenn Sie diese Systemvariablen nicht entfernen, schlägt die Installation fehl.

3. Laden Sie die Connector-Software von der herunter "NetApp Support Website", Und dann kopieren Sie es auf den Linux-Host.

   Sie sollten das Installationsprogramm für den „Online“-Connector herunterladen, das für den Einsatz in Ihrem Netzwerk oder in der Cloud gedacht ist. Für den Connector ist ein separater „Offline“-Installer verfügbar, der jedoch nur für Bereitstellungen im privaten Modus unterstützt wird.

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Führen Sie das Installationsskript aus.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

   Die Parameter --Proxy und --cacert sind optional. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

   Hier sehen Sie ein Beispiel für den Befehl mit beiden optionalen Parametern:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   --Proxy konfiguriert den Connector so, dass er einen HTTP- oder HTTPS-Proxy-Server in einem der folgenden Formate verwendet:

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port

- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Beachten Sie Folgendes:

  - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
  - Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie oben gezeigt verwenden.
  - BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

6. Warten Sie, bis die Installation abgeschlossen ist.

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

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

   https://ipaddress

8. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das BlueXP Konto an, das dem Connector zugeordnet werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Unter **laufen Sie in einer gesicherten Umgebung?** Sperrmodus deaktiviert halten.

      Sie sollten den eingeschränkten Modus deaktiviert halten, da nachfolgend beschrieben wird, wie Sie BlueXP im Standardmodus verwenden. Der eingeschränkte Modus sollte nur aktiviert werden, wenn Sie über eine sichere Umgebung verfügen und dieses Konto von den BlueXP Backend-Services trennen möchten. Wenn das der Fall ist, "Befolgen Sie die Schritte für den Einstieg in BlueXP im eingeschränkten Modus".

   d. Wählen Sie **Start**.

Ergebnis

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

Wenn sich in demselben Google Cloud-Konto, bei dem der Connector erstellt wurde, Google Cloud Storage-Buckets befinden, wird automatisch eine Arbeitsumgebung von Google Cloud Storage auf dem BlueXP-Bildschirm angezeigt. "Erfahren Sie, wie Sie Google Cloud Storage von BlueXP managen"

Schritt 7: Berechtigungen für BlueXP bereitstellen

Sie müssen für BlueXP die zuvor festgelegten Google Cloud-Berechtigungen bereitstellen. Durch die Berechtigungen kann BlueXP Ihre Daten- und Storage-Infrastruktur in Google Cloud managen.

Schritte

1. Wechseln Sie zum Google Cloud Portal und weisen Sie das Servicekonto der VM-Instanz des Connectors zu.

"Google Cloud-Dokumentation: Ändern des Dienstkontos und des Zugriffsumfangs für eine Instanz"

2. Wenn Sie Ressourcen in anderen Google Cloud-Projekten managen möchten, gewähren Sie Zugriff, indem Sie das Servicekonto mit der BlueXP Rolle zu diesem Projekt hinzufügen. Sie müssen diesen Schritt für jedes Projekt wiederholen.

Ergebnis

BlueXP verfügt jetzt über die nötigen Berechtigungen, um Aktionen in Google Cloud für Sie durchzuführen.

Installieren und Einrichten eines Connectors auf dem Gelände

Installieren Sie einen Connector vor Ort, melden Sie sich anschließend an und richten Sie ihn für die Nutzung mit Ihrem BlueXP Konto ein.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

Die Connector-Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Port-Anforderungen usw. erfüllt. Stellen Sie sicher, dass Ihr Host diese Anforderungen erfüllt, bevor Sie den Connector installieren.

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 und 7.9
- Red hat Enterprise Linux 7.6, 7.7, 7.8 und 7.9

  Der Host muss bei Red hat Subscription Management registriert sein. Wenn er nicht registriert ist, kann der Host während der Connector-Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

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

Hypervisor

Ein Bare-Metal- oder Hosted-Hypervisor, der für Ubuntu, CentOS oder Red hat Enterprise Linux zertifiziert ist, ist erforderlich.

"Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine ist auf dem Host erforderlich, bevor Sie den Connector installieren.

- Die unterstützte Version ist mindestens 19.3.1.
- Die maximal unterstützte Version ist 25.0.5.

  "Installationsanweisungen anzeigen"

Schritt 2: Netzwerk einrichten

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Hybrid-Cloud-Umgebung managen kann. Sie müssen beispielsweise sicherstellen, dass Verbindungen für Zielnetzwerke verfügbar sind und dass ein ausgehender Internetzugang verfügbar ist.

Verbindungen zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu dem Standort, an dem Sie Arbeitsumgebungen erstellen und verwalten möchten. Ein Beispiel ist ein Netzwerk, in dem Sie Cloud Volumes ONTAP Systeme oder ein Storage-System in Ihrer lokalen Umgebung erstellen möchten.

Outbound-Internetzugang

Der Netzwerkstandort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen, um bestimmte Endpunkte zu kontaktieren.

Endpunkte wurden während der manuellen Installation kontaktiert

Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren, benötigt das Installationsprogramm für den Connector während des Installationsprozesses Zugriff auf die folgenden URLs:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

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

Vom Connector kontaktierte Endpunkte

Für den Connector ist ein ausgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung für den täglichen Betrieb zu managen.

Beachten Sie, dass es sich bei den unten aufgeführten Endpunkten um alle CNAME-Einträge handelt.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.

Endpunkte	Zweck
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert

wird. "Weitere Informationen zur BlueXP Klassifizierung"

Schritt 3: Cloud-Berechtigungen einrichten

Wenn Sie BlueXP Services in AWS oder Azure mit einem On-Premises Connector nutzen möchten, müssen Sie Berechtigungen bei Ihrem Cloud-Provider einrichten, damit Sie nach der Installation die Zugangsdaten zum Connector hinzufügen können.

> Warum nicht Google Cloud? Der Connector kann vor Ort installiert werden und nicht Ihre Ressourcen in Google Cloud managen. Der Connector muss in Google Cloud installiert sein, um alle dort residieren zu managen.

AWS

Wenn der Connector vor Ort installiert ist, müssen Sie BlueXP mit AWS Berechtigungen versehen, indem Sie Zugriffsschlüssel für einen IAM-Benutzer mit den erforderlichen Berechtigungen hinzufügen.

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

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:

   a. Wählen Sie **Policies > Create Policy** aus.

   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".

   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.

      Abhängig von den BlueXP Services, die Sie planen zu verwenden, müssen Sie möglicherweise eine zweite Richtlinie erstellen.

   Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich. "Erfahren Sie mehr über IAM-Richtlinien für den Connector".

3. Fügen Sie die Richtlinien einem IAM-Benutzer hinzu.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie nach der Installation des Connectors zu BlueXP hinzufügen können.

Ergebnis

Sie sollten nun über Zugriffsschlüssel für einen IAM-Benutzer verfügen, der über die erforderlichen Berechtigungen verfügt. Nach der Installation des Connectors müssen Sie diese Anmeldeinformationen mit dem Connector von BlueXP verknüpfen.

Azure

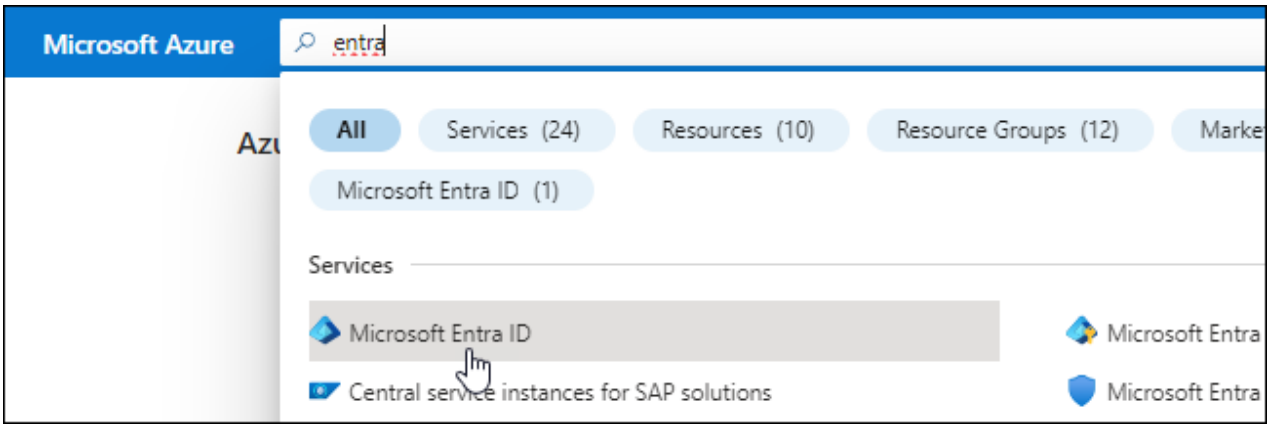
Wenn der Connector vor Ort installiert ist, müssen Sie BlueXP mit Azure-Berechtigungen versehen, indem Sie einen Service-Prinzipal in der Microsoft Entra-ID einrichten und die für BlueXP erforderlichen Azure-Berechtigungen erhalten.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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.

Anwendung einer Rolle zuweisen

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.

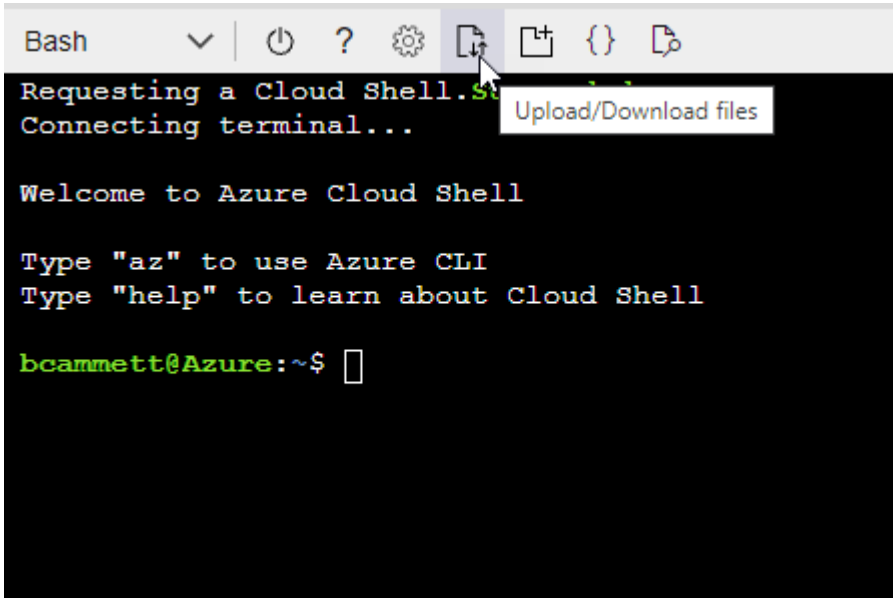
      Beispiel

      ```
      "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:

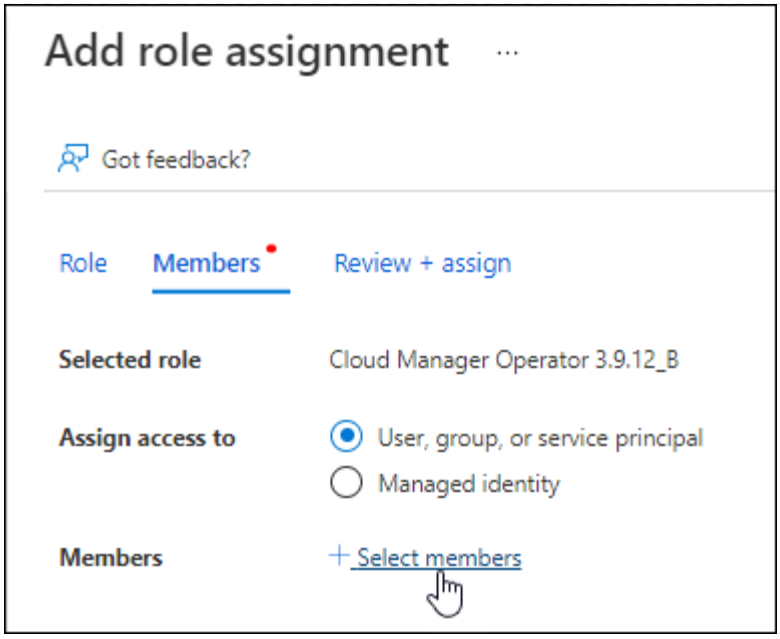
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

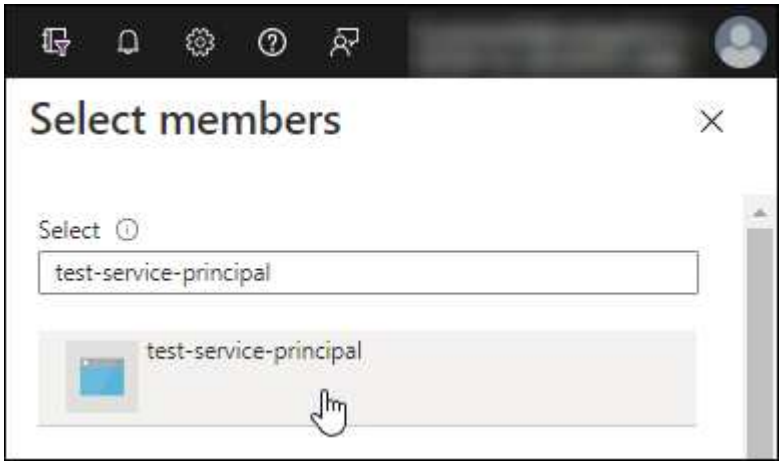
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

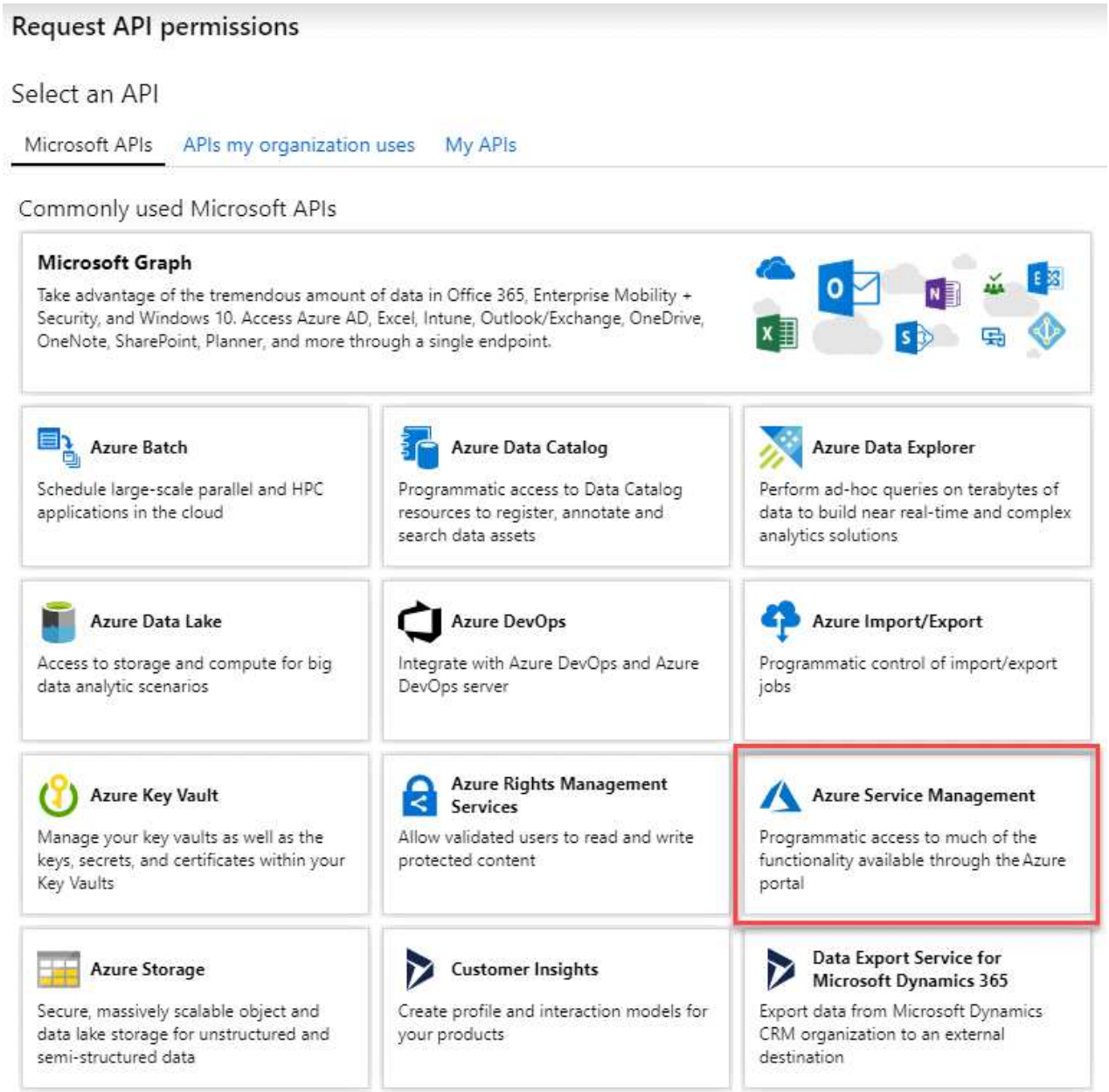
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

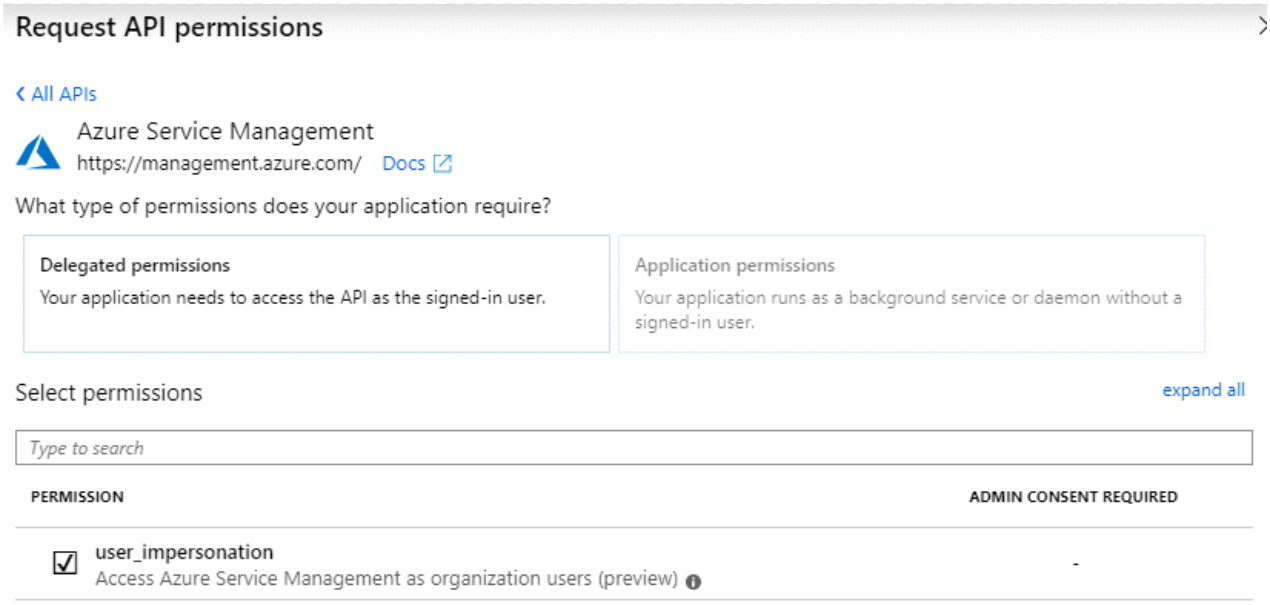
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

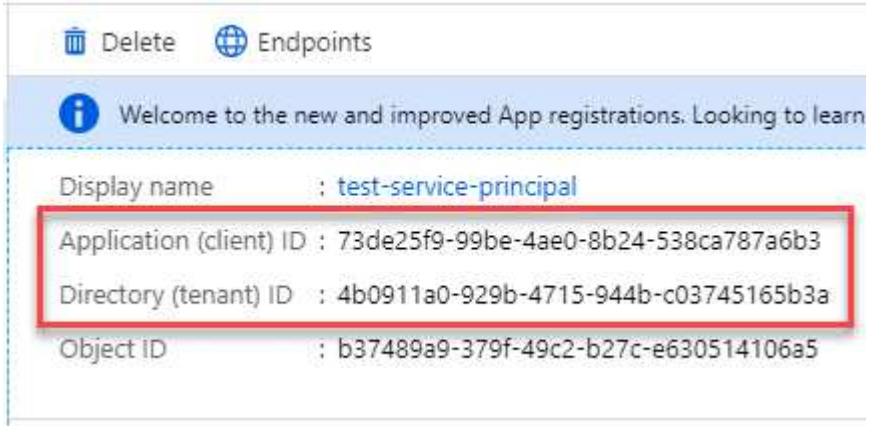


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



Die Anwendungs-ID und die Verzeichnis-ID für die Anwendung abrufen

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

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. Nach der Installation des Connectors müssen Sie diese Anmeldeinformationen mit dem Connector von BlueXP verknüpfen.

Schritt 4: Installieren Sie den Stecker

Laden Sie die Connector-Software herunter, und installieren Sie sie auf einem vorhandenen Linux-Host vor Ort.

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Root-Berechtigungen zum Installieren des Connectors.
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, aber dafür muss der Connector neu gestartet werden.

  Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

- Ein CA-signiertes Zertifikat, wenn der Proxy-Server HTTPS verwendet oder wenn der Proxy ein abfangenden Proxy ist.

Über diese Aufgabe

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

Schritte

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

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

2. Wenn die Systemvariablen *http_Proxy* oder *https_Proxy* auf dem Host festgelegt sind, entfernen Sie sie:

```
unset http_proxy
unset https_proxy
```

Wenn Sie diese Systemvariablen nicht entfernen, schlägt die Installation fehl.

3. Laden Sie die Connector-Software von der herunter "NetApp Support Website", Und dann kopieren Sie es auf den Linux-Host.

   Sie sollten das Installationsprogramm für den „Online“-Connector herunterladen, das für den Einsatz in Ihrem Netzwerk oder in der Cloud gedacht ist. Für den Connector ist ein separater „Offline“-Installer verfügbar, der jedoch nur für Bereitstellungen im privaten Modus unterstützt wird.

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Führen Sie das Installationsskript aus.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

   Die Parameter --Proxy und --cacert sind optional. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

   Hier sehen Sie ein Beispiel für den Befehl mit beiden optionalen Parametern:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   --Proxy konfiguriert den Connector so, dass er einen HTTP- oder HTTPS-Proxy-Server in einem der folgenden Formate verwendet:

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Beachten Sie Folgendes:

- Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
- Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie oben gezeigt verwenden.
- BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

Ergebnis

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

Schritt 5: Richten Sie den Connector ein

Melden Sie sich an, oder melden Sie sich an, und richten Sie den Connector dann für die Arbeit mit Ihrem BlueXP Konto ein.

Schritte

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

   https://ipaddress

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

2. Anmelden oder anmelden.
3. Richten Sie nach der Anmeldung BlueXP ein:
   a. Geben Sie das BlueXP Konto an, das dem Connector zugeordnet werden soll.
   b. Geben Sie einen Namen für das System ein.
   c. Unter **laufen Sie in einer gesicherten Umgebung?** Sperrmodus deaktiviert halten.

      Sie sollten den eingeschränkten Modus deaktiviert halten, da nachfolgend beschrieben wird, wie Sie BlueXP im Standardmodus verwenden. (Außerdem wird der eingeschränkte Modus nicht unterstützt, wenn der Connector vor Ort installiert ist.)

   d. Wählen Sie **Start**.

Ergebnis

BlueXP ist jetzt mit dem Connector eingerichtet, den Sie gerade installiert haben.

Schritt 6: Berechtigungen für BlueXP bereitstellen

Fügen Sie nach der Installation und Einrichtung des Connector Ihre Cloud-Anmeldedaten hinzu, damit BlueXP über die erforderlichen Berechtigungen zum Ausführen von Aktionen in AWS oder Azure verfügt.

AWS

Bevor Sie beginnen

Wenn Sie diese Anmeldedaten gerade in AWS 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. 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 **Amazon Web Services > Connector**.
   b. **Zugangsdaten definieren**: 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.
   d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Aktionen in AWS benötigt.

Sie können jetzt die öffnen "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

Azure

Bevor Sie beginnen

Wenn Sie diese Anmeldedaten gerade in Azure 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 **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

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt. Sie können jetzt die öffnen "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

BlueXP abonnieren (Standardmodus)

Abonnieren Sie BlueXP über den Marketplace Ihres Cloud-Providers und zahlen Sie für BlueXP Services zu einem Stundensatz (PAYGO) oder über einen Jahresvertrag. Wenn Sie eine Lizenz von NetApp (BYOL) erworben haben, müssen Sie auch das Marketplace-Angebot abonnieren. Ihre Lizenz wird immer zuerst berechnet, aber Sie werden mit dem Stundensatz belastet, wenn Sie Ihre lizenzierte Kapazität überschreiten oder wenn die Laufzeit der Lizenz abläuft.

Über ein Marketplace Abonnement können die folgenden BlueXP Services berechnet werden:

- Backup und Recovery
- Klassifizierung
- Cloud Volumes ONTAP
- Tiering

Bevor Sie beginnen

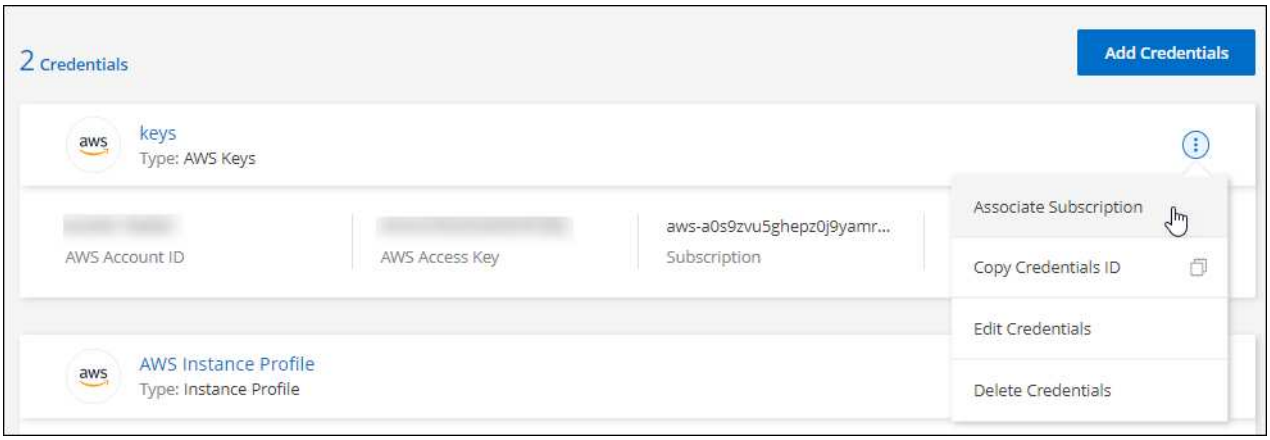
Für das Abonnement von BlueXP wird ein Marketplace-Abonnement mit den Cloud-Zugangsdaten verknüpft, die einem Connector zugeordnet sind. Wenn Sie den Workflow „erste Schritte mit Standardmodus“ befolgt haben, sollten Sie bereits über einen Connector verfügen. Weitere Informationen finden Sie im "Schneller Einstieg für BlueXP im Standard-Modus".

AWS

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:

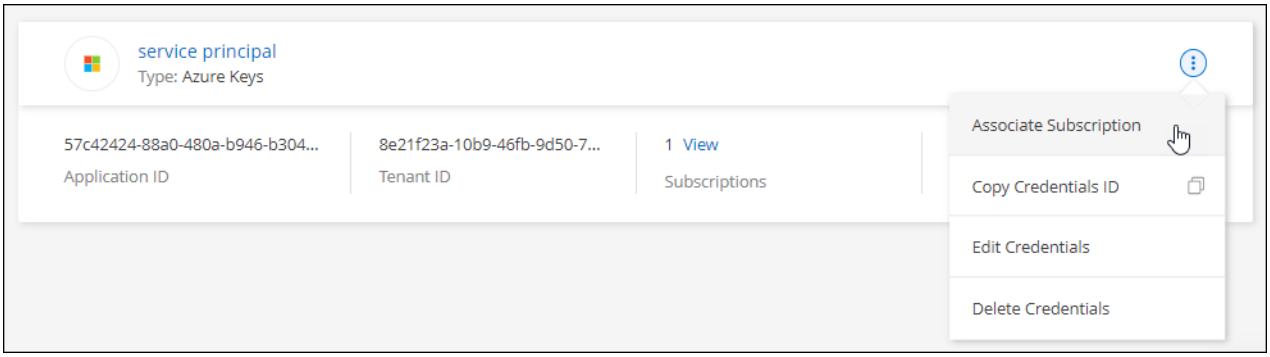
Abonnieren Sie BlueXP über den AWS Marketplace

Azure

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**.

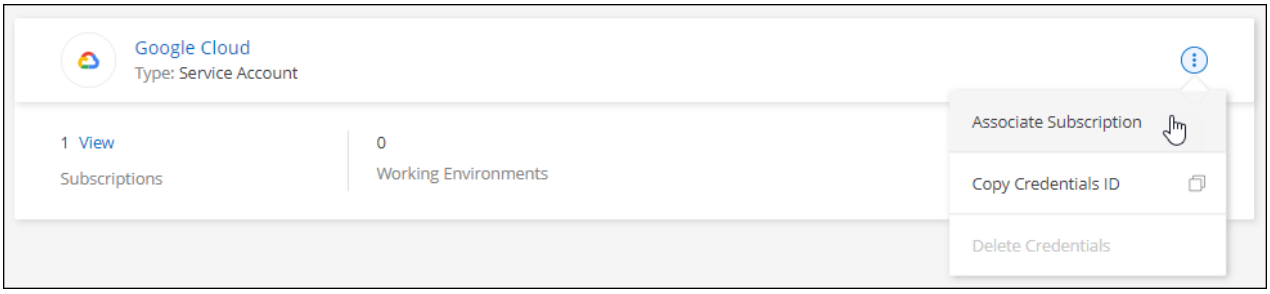
Im folgenden Video sehen Sie, wie Sie im Azure Marketplace abonnieren:

Abonnieren Sie BlueXP über den Azure Marketplace

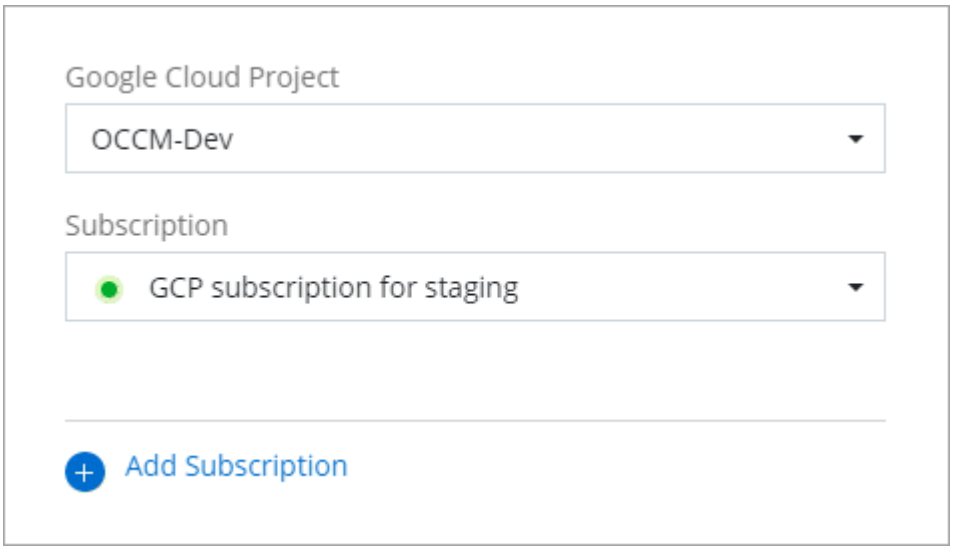
Google Cloud

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**.



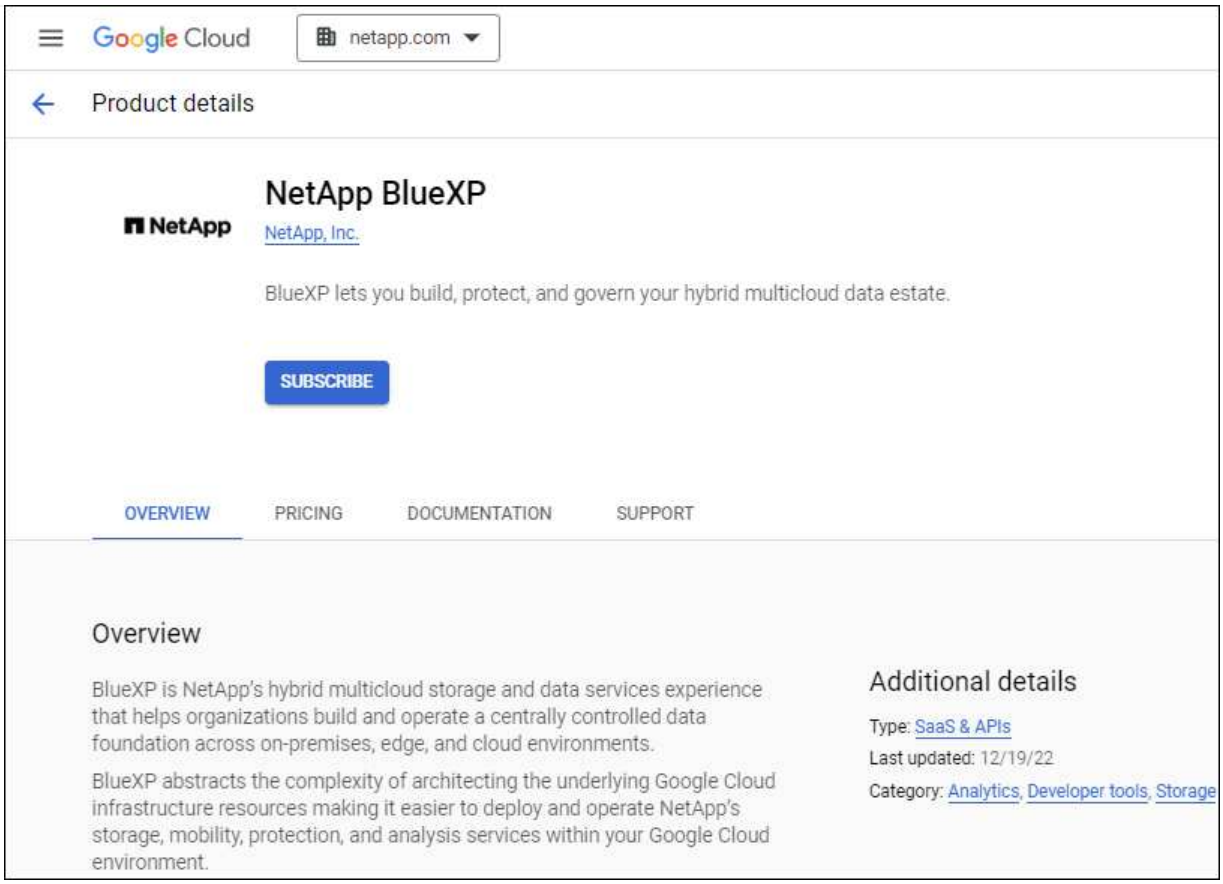
3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, und wählen Sie dann **Associate** aus.



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**.

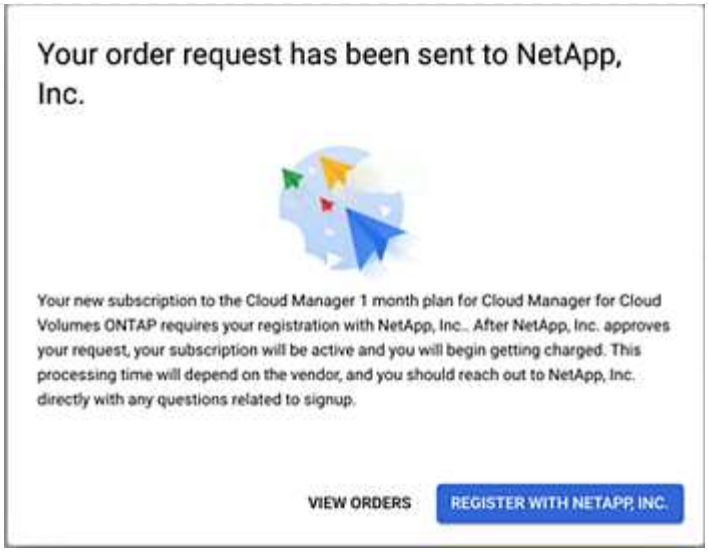
c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

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.

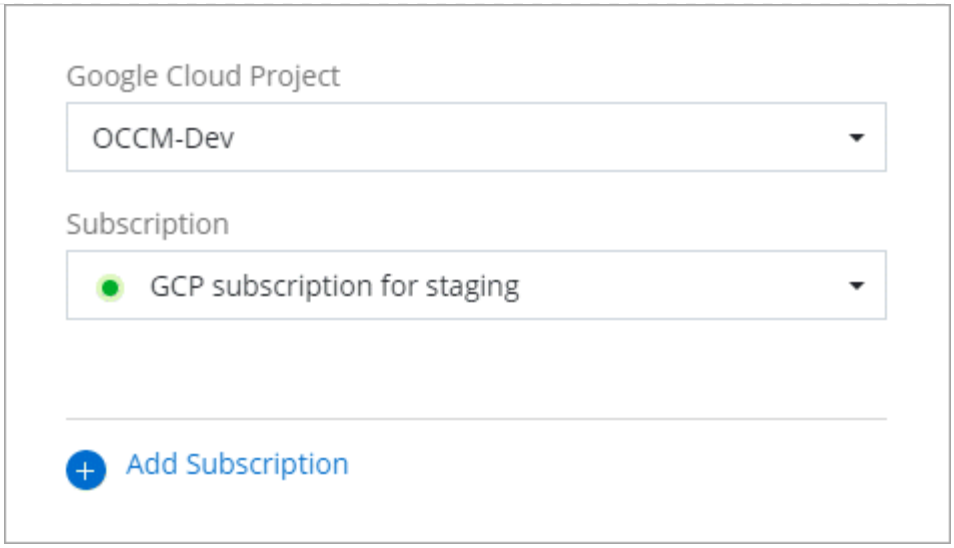
Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden Schritte wiederholen.

- 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.



Weiterführende Links

- "Managen Sie kapazitätsbasierte BYOL-Lizenzen für Cloud Volumes ONTAP"
- "Managen von BYOL-Lizenzen für BlueXP Datenservices"
- "Managen Sie AWS Anmeldeinformationen und Abonnements für BlueXP"
- "Managen Sie Azure Anmeldedaten und Abonnements für BlueXP"
- "Managen Sie Google Cloud-Anmeldedaten und -Abonnements für BlueXP"

Nächste Schritte (Standardmodus)

Nachdem Sie sich jetzt angemeldet und BlueXP im Standardmodus eingerichtet haben, können Benutzer Arbeitsumgebungen erstellen und erkennen und BlueXP Datenservices nutzen.

> Wenn Sie einen Connector in AWS, Microsoft Azure oder Google Cloud installiert haben, erkennt BlueXP automatisch Informationen zu Amazon S3 Buckets, Azure Blob Storage oder Google Cloud Storage an dem Ort, an dem der Connector installiert ist. Eine Arbeitsumgebung wird automatisch dem BlueXP Arbeitsbereich hinzugefügt.

Hilfe erhalten Sie im "Startseite für die BlueXP Dokumentation" Um die Dokumente zu allen BlueXP Services einzusehen.

Verwandter Link

"BlueXP Implementierungsmodi"

Beginnen Sie mit dem eingeschränkten Modus

Erste Schritte im Workflow (eingeschränkter Modus)

Der Einstieg in BlueXP ist eingeschränkt, indem Sie Ihre Umgebung vorbereiten, Connector implementieren und BlueXP abonnieren.

Der eingeschränkte Modus wird in der Regel von staatlichen und lokalen Behörden sowie von Unternehmen genutzt, die Auflagen unterliegen, einschließlich Implementierungen in AWS GovCloud und Azure Government Regionen. Bevor Sie beginnen, sollten Sie ein Verständnis von haben "BlueXP Accounts", "Anschlüsse", und "Bereitstellungsmodi".

1 **"Vorbereitungen für die Implementierung"**

1. Bereiten Sie einen dedizierten Linux-Host vor, der die Anforderungen für CPU, RAM, Festplattenspeicher, Docker Engine und mehr erfüllt.
2. Richten Sie ein Netzwerk ein, das den Zugriff auf die Zielnetzwerke, den ausgehenden Internetzugang für manuelle Installationen und das ausgehende Internet für den täglichen Zugriff bietet.
3. Richten Sie Berechtigungen in Ihrem Cloud-Provider ein, damit Sie diese Berechtigungen nach der Bereitstellung mit der Connector-Instanz verknüpfen können.

2 **"Implementieren Sie den Connector"**

1. Installieren Sie den Connector auf dem Marktplatz Ihres Cloud-Anbieters oder installieren Sie die Software manuell auf Ihrem eigenen Linux-Host.
2. Richten Sie BlueXP ein, indem Sie einen Webbrowser öffnen und die IP-Adresse des Linux-Hosts eingeben.
3. Bereitstellen von BlueXP mit den Berechtigungen, die Sie bereits eingerichtet haben.

3 **"Abonnieren Sie BlueXP"**

Abonnieren Sie BlueXP über den Marketplace Ihres Cloud-Providers und zahlen Sie für BlueXP Services zu einem Stundensatz (PAYGO) oder über einen Jahresvertrag.

Bereiten Sie die Bereitstellung im eingeschränkten Modus vor

Bereiten Sie Ihre Umgebung vor der Implementierung von BlueXP im eingeschränkten Modus vor. Sie müssen beispielsweise die Hostanforderungen prüfen, das Netzwerk vorbereiten, Berechtigungen einrichten und vieles mehr.

Schritt 1: Verstehen, wie eingeschränkter Modus funktioniert

Bevor Sie beginnen, sollten Sie wissen, wie BlueXP im eingeschränkten Modus funktioniert.

Sie sollten beispielsweise verstehen, dass Sie die browserbasierte Oberfläche verwenden müssen, die lokal über den BlueXP Connector verfügbar ist, die Sie installieren müssen. Der Zugriff auf BlueXP erfolgt nicht über die webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird.

Außerdem sind nicht alle BlueXP Services verfügbar.

"Erfahren Sie, wie eingeschränkter Modus funktioniert".

Schritt 2: Überprüfen Sie die Installationsoptionen

Im eingeschränkten Modus können Sie den Connector nur in der Cloud installieren. Folgende Installationsoptionen sind verfügbar:

- Über AWS Marketplace
- Über den Azure Marketplace
- Manuelles Installieren des Connectors auf Ihrem eigenen Linux-Host, der in AWS, Azure oder Google Cloud ausgeführt wird

Schritt 3: Überprüfen Sie die Host-Anforderungen

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

Wenn Sie den Connector über AWS oder Azure Marketplace implementieren, enthält das Image die erforderlichen Betriebssystem- und Softwarekomponenten. Sie müssen lediglich einen Instanztyp auswählen, der die CPU- und RAM-Anforderungen erfüllt.

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 und 7.9
- Red hat Enterprise Linux 7.6, 7.7, 7.8 und 7.9

  Der Host muss bei Red hat Subscription Management registriert sein. Wenn er nicht registriert ist, kann der Host während der Connector-Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

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

Hypervisor

Ein Bare-Metal- oder Hosted-Hypervisor, der für Ubuntu, CentOS oder Red hat Enterprise Linux zertifiziert ist, ist erforderlich.

"Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Azure VM-Größe

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

Google Cloud-Maschinentyp

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

Der Connector wird in Google Cloud auf einer VM-Instanz mit einem unterstützten Betriebssystem unterstützt "Geschirmte VM-Funktionen"

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine ist auf dem Host erforderlich, bevor Sie den Connector installieren.

- Die unterstützte Version ist mindestens 19.3.1.
- Die maximal unterstützte Version ist 25.0.5.

"Installationsanweisungen anzeigen"

Schritt 4: Vorbereitung der Vernetzung

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung managen kann. Abgesehen von einem virtuellen Netzwerk und einem Subnetz für den Connector müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind.

Verbindungen zu Zielnetzwerken

Der Connector muss über eine Netzwerkverbindung zu dem Speicherort verfügen, an dem Sie Speicher verwalten möchten. Beispielsweise die VPC oder vnet, bei der Sie Cloud Volumes ONTAP implementieren möchten, oder das Datacenter, in dem sich Ihre ONTAP-Cluster vor Ort befinden.

Networking für Benutzerzugriff auf die BlueXP Konsole vorbereiten

Im eingeschränkten Modus ist der Zugriff auf die BlueXP Benutzeroberfläche über den Connector möglich. Bei der Nutzung der BlueXP Benutzeroberfläche wendet sich das IT-Programm an einige Endpunkte, um Datenmanagementaufgaben durchzuführen. Diese Endpunkte werden von dem Computer eines Benutzers kontaktiert, wenn bestimmte Aktionen über die BlueXP Konsole durchgeführt werden.

Endpunkte	Zweck
https://signin.b2c.netapp.com	Erforderlich, um die Zugangsdaten für die NetApp Support Site (NSS) zu aktualisieren oder neue NSS-Zugangsdaten für BlueXP hinzuzufügen
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung über BlueXP zu ermöglicht.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Endpunkte wurden während der manuellen Installation kontaktiert

Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren, benötigt das Installationsprogramm für den Connector während des Installationsprozesses Zugriff auf die folgenden URLs:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Dieser Endpunkt ist in Regionen der Azure-Regierung nicht erforderlich.

- https://occmclientinfragov.azurecr.us

  Dieser Endpunkt ist nur in Regionen der Azure-Regierung erforderlich.

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

Outbound-Internetzugang für den täglichen Betrieb

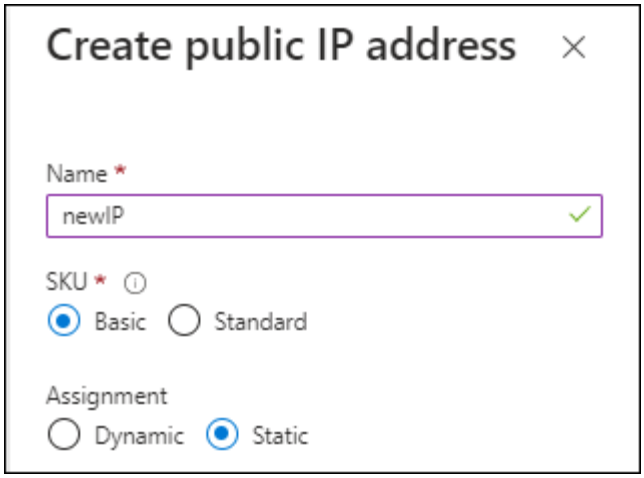
Der Netzwerkspeicherort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen. Für den Konnektor ist ein abgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu verwalten.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Managen von Ressourcen in Azure Government Regionen.

Endpunkte	Zweck
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Dieser Endpunkt ist in Regionen der Azure-Regierung nicht erforderlich. https://occmclientinfragov.azurecr.us Dieser Endpunkt ist nur in Regionen der Azure-Regierung erforderlich.	Aktualisierung des Connectors und seiner Docker Komponenten.

Öffentliche IP-Adresse in Azure

Wenn Sie eine öffentliche IP-Adresse mit der Connector-VM in Azure verwenden möchten, muss die IP-Adresse eine Basis-SKU verwenden, um sicherzustellen, dass BlueXP diese öffentliche IP-Adresse verwendet.



Wenn Sie stattdessen eine Standard-SKU-IP-Adresse verwenden, verwendet BlueXP anstelle der öffentlichen IP die *private* IP-Adresse des Connectors. Wenn die Maschine, die Sie für den Zugriff auf die BlueXP-Konsole nutzen, keinen Zugriff auf diese private IP-Adresse hat, dann schlagen Aktionen aus der BlueXP-Konsole fehl.

"Azure-Dokumentation: Öffentliche IP-SKU"

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy. Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

Ports

Es erfolgt kein eingehender Datenverkehr zum Connector, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy verwendet wird, um AutoSupport-Nachrichten von Cloud Volumes ONTAP an den NetApp-Support zu senden.

- HTTP (80) und HTTPS (443) bieten Zugriff auf die lokale Benutzeroberfläche, die Sie in seltenen Fällen verwenden werden.
- SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.
- Eingehende Verbindungen über Port 3128 sind erforderlich, wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen, in dem keine ausgehende Internetverbindung verfügbar ist.

  Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport Meldungen haben, konfiguriert BlueXP diese 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.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Wenn Sie den Connector aus dem Marktplatz Ihres Cloud-Anbieters erstellen möchten, müssen Sie diese Netzwerkanforderung implementieren, nachdem Sie den Connector erstellt haben.

Schritt: 5 Cloud-Berechtigungen vorbereiten

BlueXP erfordert Berechtigungen Ihres Cloud-Providers zur Implementierung von Cloud Volumes ONTAP in einem virtuellen Netzwerk und zur Nutzung von BlueXP Datenservices. Sie müssen Berechtigungen in Ihrem Cloud-Provider einrichten und diese dann dem Connector zuordnen.

Um die erforderlichen Schritte anzuzeigen, wählen Sie die Authentifizierungsoption aus, die Sie für Ihren Cloud-Provider verwenden möchten.

AWS IAM-Rolle

Verwenden Sie eine IAM-Rolle, um dem Connector Berechtigungen zu gewähren.

Wenn Sie den Connector über AWS Marketplace erstellen, werden Sie beim Start der EC2-Instanz aufgefordert, diese IAM-Rolle auszuwählen.

Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren, müssen Sie die Rolle an die EC2-Instanz anhängen.

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:
   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.
3. Erstellen einer IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Service > EC2** aus.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die soeben erstellte Richtlinie anhängen.
   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

Ergebnis

Sie haben jetzt eine IAM-Rolle für die EC2-Instanz des Connectors.

AWS-Zugriffsschlüssel

Richten Sie Berechtigungen und einen Zugriffsschlüssel für einen IAM-Benutzer ein. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP mit dem AWS-Zugriffsschlüssel bereitstellen.

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:

   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.

      Abhängig von den BlueXP Services, die Sie planen zu verwenden, müssen Sie möglicherweise eine zweite Richtlinie erstellen.

   Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich. "Erfahren Sie mehr über IAM-Richtlinien für den Connector".

3. Fügen Sie die Richtlinien einem IAM-Benutzer hinzu.
   - "AWS Documentation: Erstellung von IAM-Rollen"

- "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie nach der Installation des Connectors zu BlueXP hinzufügen können.

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen.

Azure Rolle

Erstellen einer benutzerdefinierten Azure-Rolle mit den erforderlichen Berechtigungen. Sie werden diese Rolle der Connector-VM zuweisen.

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"

Schritte

1. Wenn Sie planen, die Software manuell auf Ihrem eigenen Host zu installieren, aktivieren Sie eine vom System zugewiesene verwaltete Identität auf der VM, sodass Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

   "Microsoft Azure-Dokumentation: Gemanagte Identitäten für Azure-Ressourcen auf einer VM über das Azure-Portal konfigurieren"

2. Kopieren Sie den Inhalt des "Benutzerdefinierte Rollenberechtigungen für den Konnektor" Und speichern Sie sie in einer JSON-Datei.
3. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

   Sie sollten für jedes Azure-Abonnement, das Sie mit BlueXP verwenden möchten, die ID hinzufügen.

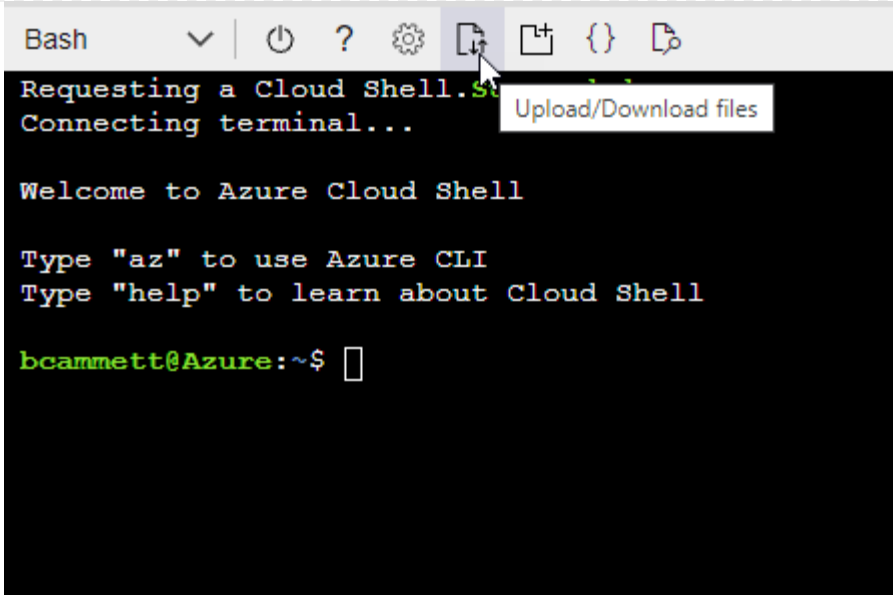
   Beispiel

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

4. 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.

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



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

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

Ergebnis

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

Azure Service Principal

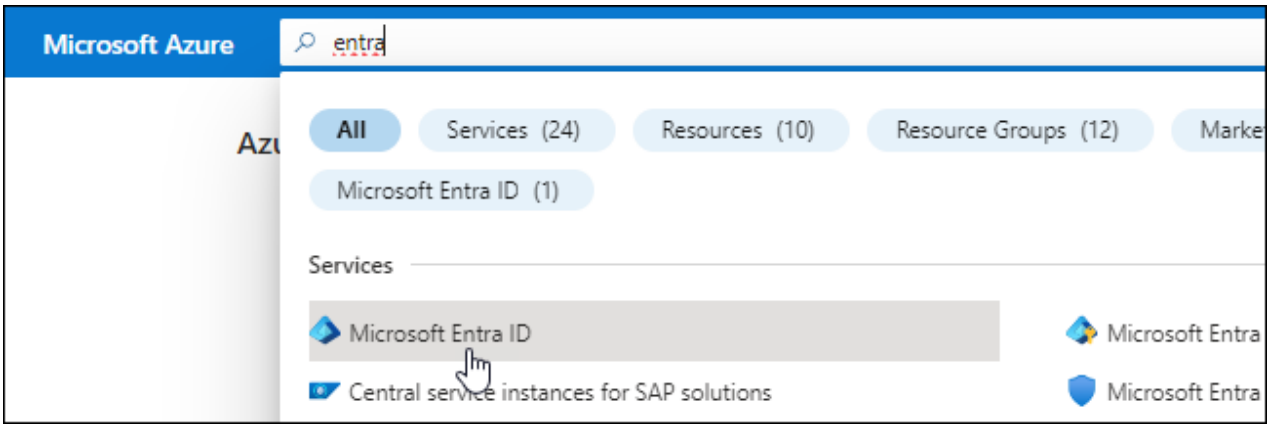
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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.

Anwendung einer Rolle zuweisen

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.

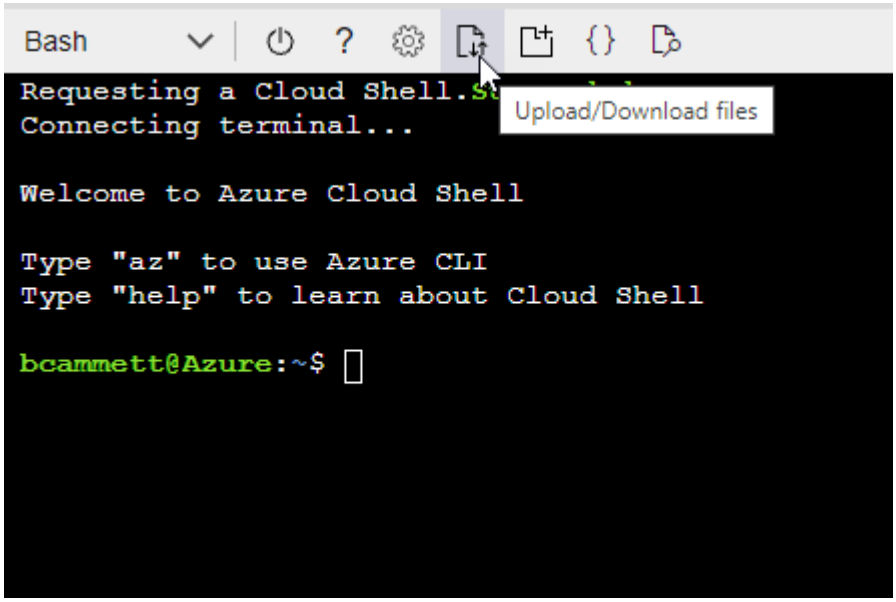
      Beispiel

      ```
      "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:

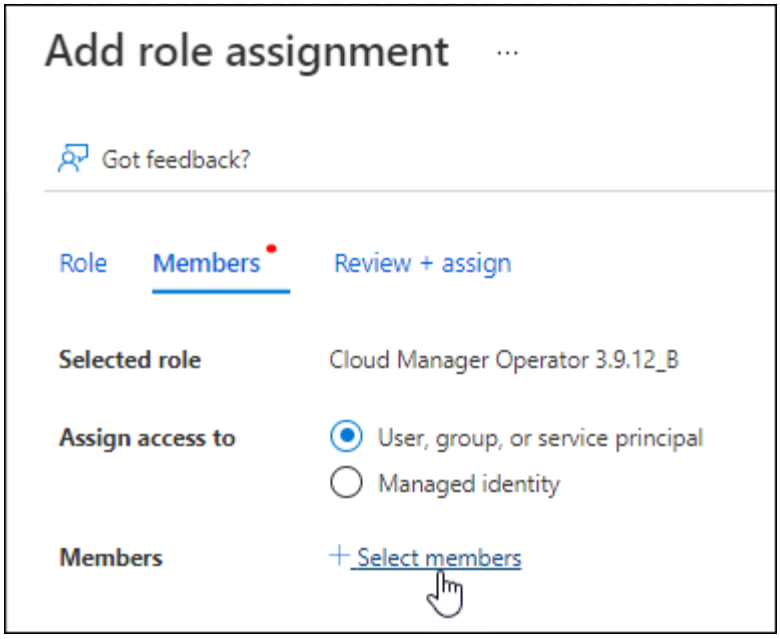
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

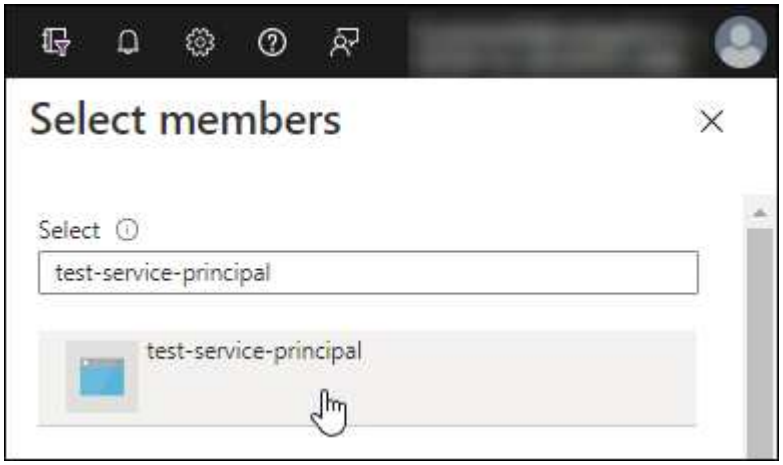
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

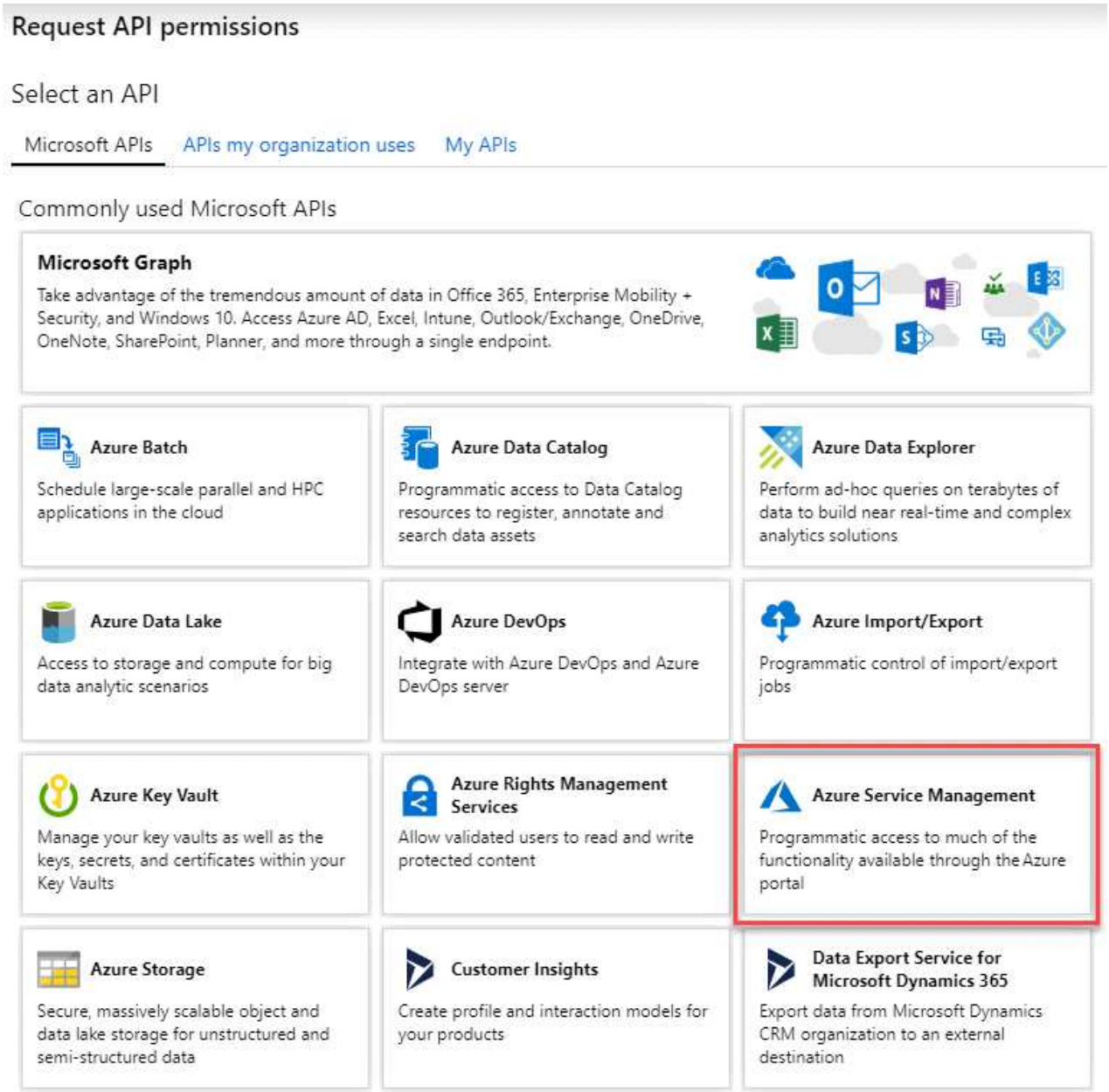
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

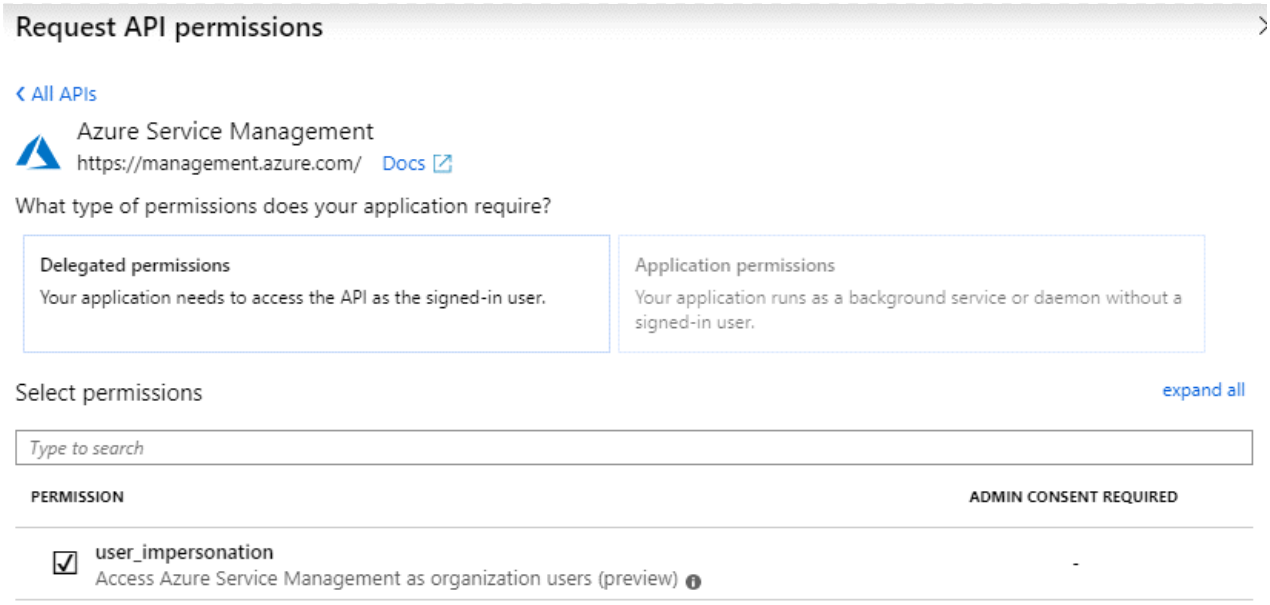
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

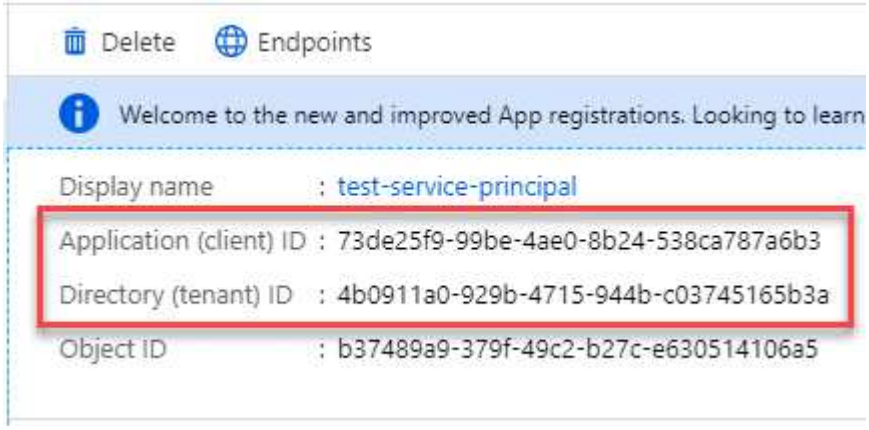


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



Die Anwendungs-ID und die Verzeichnis-ID für die Anwendung abrufen

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

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.

Google Cloud Service-Konto

Erstellen Sie eine Rolle und wenden Sie sie auf ein Servicekonto an, das Sie für die VM-Instanz des Connectors verwenden werden.

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

   a. Erstellen Sie eine YAML-Datei, die die in definierten Berechtigungen enthält "Connector-Richtlinie für Google Cloud".

   b. Aktivieren Sie in Google Cloud die Cloud Shell.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen für den Connector enthält.

   d. Erstellen Sie mithilfe von eine benutzerdefinierte Rolle `gcloud iam roles create` Befehl.

      Im folgenden Beispiel wird auf Projektebene eine Rolle namens „Connector“ erstellt:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Google Cloud docs: Erstellen und Verwalten benutzerdefinierter Rollen"

2. Erstellen Sie ein Servicekonto in Google Cloud:

   a. Wählen Sie im IAM & Admin-Dienst **Service-Konten > Service-Konto erstellen** aus.

   b. Geben Sie die Details des Servicekontos ein und wählen Sie **Erstellen und Fortfahren**.

   c. Wählen Sie die gerade erstellte Rolle aus.

   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

      "Google Cloud docs: Erstellen eines Dienstkontos"

Ergebnis

Sie verfügen jetzt über ein Servicekonto, das Sie der VM-Instanz des Connectors zuweisen können.

Schritt 6: Google Cloud APIs aktivieren

Für die Implementierung von Cloud Volumes ONTAP in Google Cloud sind mehrere APIs erforderlich.

Schritt

1. "Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt"
    - Cloud Deployment Manager V2-API
    - Cloud-ProtokollierungsAPI
    - Cloud Resource Manager API
    - Compute Engine-API
    - IAM-API (Identitäts- und Zugriffsmanagement
    - KMS-API (Cloud Key Management Service)

      (Nur erforderlich, wenn Sie BlueXP Backup und Recovery mit vom Kunden gemanagten Verschlüsselungsschlüsseln (CMEK) verwenden möchten).

Stellen Sie den Connector im eingeschränkten Modus bereit

Implementieren Sie den Connector im eingeschränkten Modus, sodass Sie BlueXP mit eingeschränkter Outbound-Konnektivität zur BlueXP SaaS-Ebene nutzen können. Installieren Sie den Connector, richten Sie BlueXP über die Benutzeroberfläche ein, die auf dem Connector ausgeführt wird, und stellen Sie dann die zuvor festgelegten Cloud-Berechtigungen bereit.

Schritt 1: Installieren Sie den Stecker

Installieren Sie den Connector auf dem Marktplatz Ihres Cloud-Anbieters oder installieren Sie die Software manuell auf Ihrem eigenen Linux-Host.

AWS Commercial Marketplace

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt

  "Hier erhalten Sie Informationen zu den Netzwerkanforderungen"

- Eine IAM-Rolle mit angehängter Richtlinie, die die erforderlichen Berechtigungen für den Connector enthält.

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

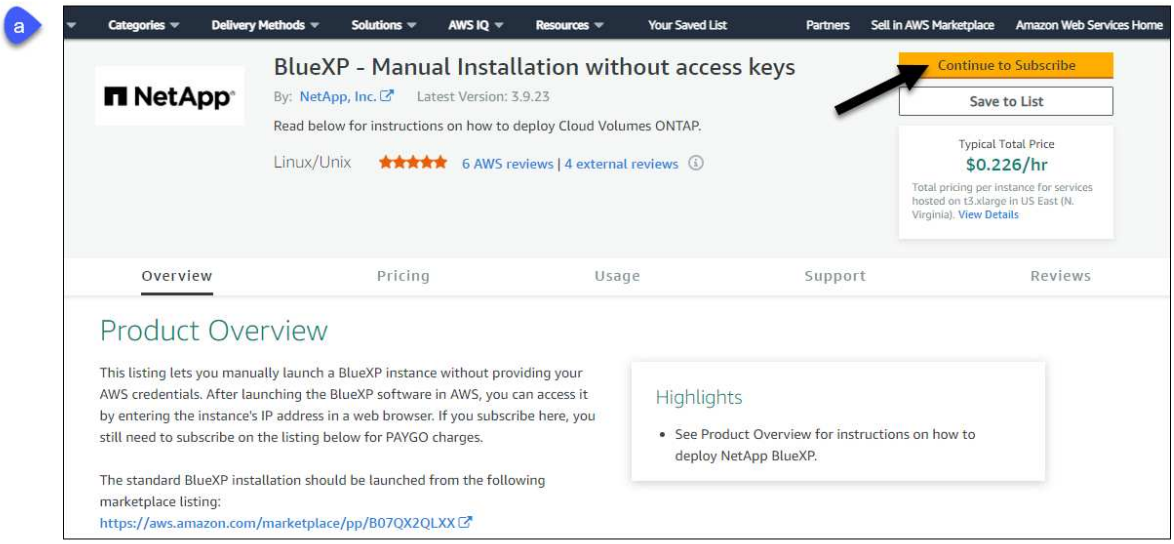
- Berechtigung zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Verständnis der CPU- und RAM-Anforderungen für die Instanz.

  "Prüfen Sie die Instanzanforderungen".

- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

1. Wechseln Sie zum "Seite „BlueXP“ im AWS Marketplace"
2. Wählen Sie auf der Marketplace-Seite **Weiter zu Abonnieren** und wählen Sie dann **Weiter zu Konfiguration**.



3. Ändern Sie eine der Standardoptionen, und wählen Sie **Weiter zum Starten**.
4. Wählen Sie unter **Aktion auswählen** die Option **über EC2 starten** aus und wählen Sie dann **Start** aus.

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

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

   - **Name und Tags**: Geben Sie einen Namen und Tags für die Instanz ein.
   - **Anwendung und Betriebssystembild**: Überspringen Sie diesen Abschnitt. Der Stecker AMI ist bereits ausgewählt.
   - **Instanztyp**: Wählen Sie je nach Verfügbarkeit der Region einen Instanztyp aus, der den RAM- und CPU-Anforderungen entspricht (t3.xlarge wird empfohlen).
   - **Schlüsselpaar (Login)**: Wählen Sie das Schlüsselpaar aus, mit dem Sie eine sichere Verbindung zur Instanz herstellen möchten.
   - **Netzwerkeinstellungen**: Bearbeiten Sie die Netzwerkeinstellungen nach Bedarf:
     - Wählen Sie die gewünschte VPC und das Subnetz.
     - Geben Sie an, ob die Instanz eine öffentliche IP-Adresse haben soll.
     - Legen Sie Firewall-Einstellungen fest, die die erforderlichen Verbindungsmethoden für die

Connector-Instanz SSH, HTTP und HTTPS aktivieren.

Für spezifische Konfigurationen sind noch einige Regeln erforderlich.

"Sicherheitsgruppen-Regeln für AWS ansehen".

- **Configure Storage**: Behalten Sie die Standardgröße und den Festplattentyp für das Root-Volume bei.

  Wenn Sie die Amazon EBS-Verschlüsselung auf dem Root-Volume aktivieren möchten, wählen Sie **Erweitert**, erweitern **Volume 1**, wählen **verschlüsselt** und wählen dann einen KMS-Schlüssel aus.

- **Erweiterte Details**: Unter **IAM Instance profile** wählen Sie die IAM-Rolle, die die erforderlichen Berechtigungen für den Connector enthält.
- **Zusammenfassung**: Überprüfen Sie die Zusammenfassung und wählen Sie **Launch Instance**.

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

AWS Gov Marketplace

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt

  "Hier erhalten Sie Informationen zu den Netzwerkanforderungen"

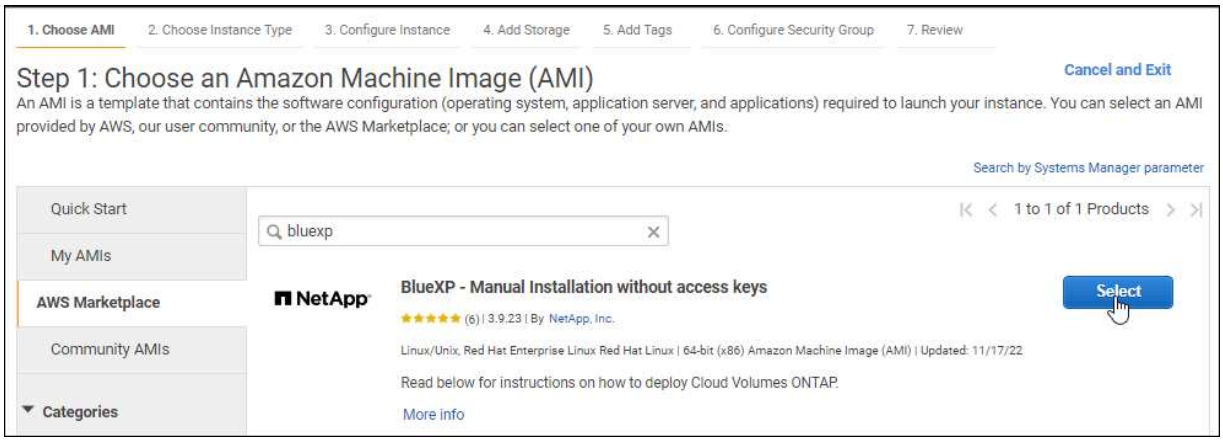
- Eine IAM-Rolle mit angehängter Richtlinie, die die erforderlichen Berechtigungen für den Connector enthält.

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

- Berechtigung zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

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

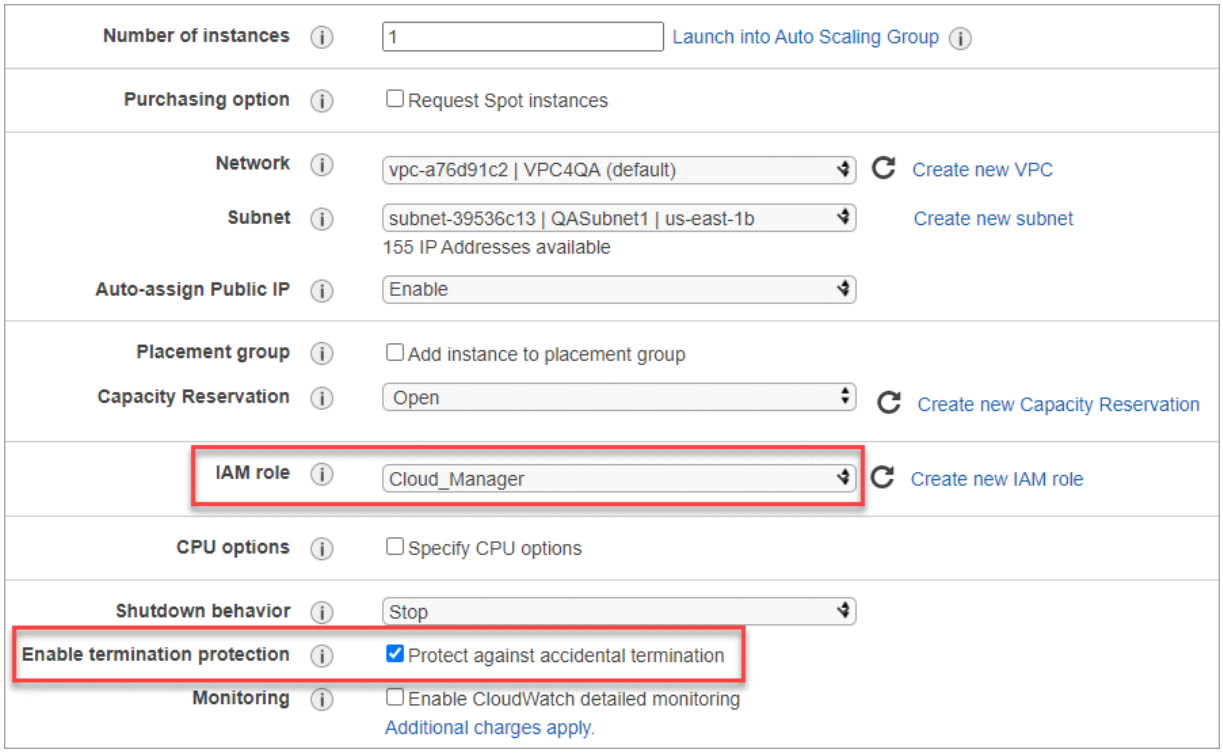


d. Wählen Sie **Weiter**.

2. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:
   - **Wählen Sie einen Instanztyp**: Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.xlarge wird empfohlen).

     "Prüfen Sie die Anforderungen an die Instanz".

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



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

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

Azure Marketplace

Bevor Sie beginnen

Sie sollten Folgendes haben:

- V-net und Subnetz, die die Netzwerkanforderungen erfüllen

  "Hier erhalten Sie Informationen zu den Netzwerkanforderungen"

- Eine benutzerdefinierte Azure-Rolle, die die erforderlichen Berechtigungen für den Connector enthält.

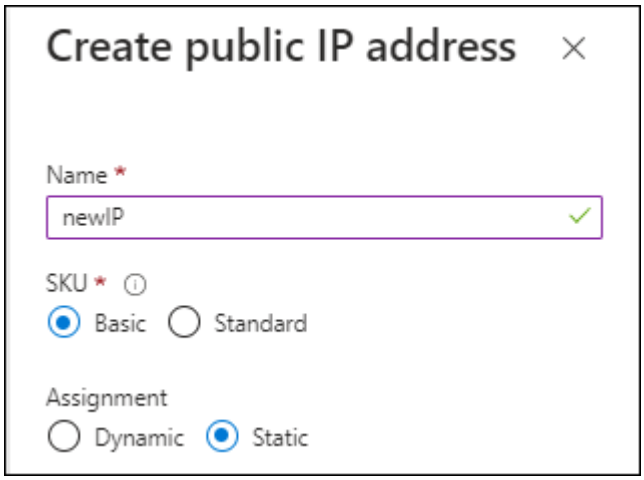
  "Erfahren Sie, wie Sie Azure-Berechtigungen einrichten"

Schritte

1. Wechseln Sie im Azure Marketplace auf die Seite NetApp Connector VM.
   - "Azure Marketplace-Seite für kommerzielle Regionen"
   - "Azure Marketplace-Seite für Azure Government Regions"
2. Wählen Sie **Jetzt holen** und wählen Sie dann **Weiter**.
3. Wählen Sie im Azure-Portal **Create** aus und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

   Beachten Sie beim Konfigurieren der VM Folgendes:

   - **VM-Größe**: Wählen Sie eine VM-Größe, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen DS3 v2.
   - **Disks**: Der Connector kann mit HDD- oder SSD-Festplatten optimal funktionieren.
   - **Öffentliche IP**: Wenn Sie eine öffentliche IP-Adresse mit der Connector VM verwenden möchten, muss die IP-Adresse eine Basis-SKU verwenden, um sicherzustellen, dass BlueXP diese öffentliche IP-Adresse verwendet.



Wenn Sie stattdessen eine Standard-SKU-IP-Adresse verwenden, verwendet BlueXP anstelle der öffentlichen IP die *private* IP-Adresse des Connectors. Wenn die Maschine, die Sie für den Zugriff auf die BlueXP-Konsole nutzen, keinen Zugriff auf diese private IP-Adresse hat, dann schlagen Aktionen aus der BlueXP-Konsole fehl.

"Azure-Dokumentation: Öffentliche IP-SKU"

- **Netzwerksicherheitsgruppe**: Der Connector benötigt eingehende Verbindungen über SSH, HTTP und HTTPS.

  "Zeigen Sie die Regeln für Sicherheitsgruppen für Azure an".

- **Identität**: Unter **Verwaltung** wählen Sie **System zugewiesene verwaltete Identität aktivieren**.

  Diese Einstellung ist wichtig, da eine verwaltete Identität es der virtuellen Connector-Maschine ermöglicht, sich ohne Angabe von Anmeldeinformationen mit Microsoft Entra ID zu identifizieren. "Erfahren Sie mehr über Managed Identitäten für Azure Ressourcen".

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

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

Manuelle Installation

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Root-Berechtigungen zum Installieren des Connectors.
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, aber dafür muss der Connector neu gestartet werden.

  Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

- Ein CA-signiertes Zertifikat, wenn der Proxy-Server HTTPS verwendet oder wenn der Proxy ein abfangenden Proxy ist.

Über diese Aufgabe

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

Schritte

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

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

2. Wenn die Systemvariablen *http_Proxy* oder *https_Proxy* auf dem Host festgelegt sind, entfernen Sie sie:

```
unset http_proxy
unset https_proxy
```

   Wenn Sie diese Systemvariablen nicht entfernen, schlägt die Installation fehl.

3. Laden Sie die Connector-Software von der herunter "NetApp Support Website", Und dann kopieren Sie es auf den Linux-Host.

   Sie sollten das Installationsprogramm für den „Online“-Connector herunterladen, das für den Einsatz in Ihrem Netzwerk oder in der Cloud gedacht ist. Für den Connector ist ein separater „Offline“-Installer verfügbar, der jedoch nur für Bereitstellungen im privaten Modus unterstützt wird.

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Führen Sie das Installationsskript aus.

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

   Die Parameter --Proxy und --cacert sind optional. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

   Hier sehen Sie ein Beispiel für den Befehl mit beiden optionalen Parametern:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   --Proxy konfiguriert den Connector so, dass er einen HTTP- oder HTTPS-Proxy-Server in einem der folgenden Formate verwendet:

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port

- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Beachten Sie Folgendes:

  - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
  - Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie oben gezeigt verwenden.
  - BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

Schritt 2: BlueXP einrichten

Wenn Sie zum ersten Mal auf die BlueXP Konsole zugreifen, werden Sie aufgefordert, ein Konto auszuwählen, mit dem der Connector verknüpft werden soll, und den eingeschränkten Modus zu aktivieren.

> Wenn Sie bereits ein Konto haben und ein weiteres erstellen möchten, müssen Sie die Mandanten-API verwenden. "Erstellen Sie ein zusätzliches BlueXP Konto".

Schritte

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

   https://ipaddress

2. Melden Sie sich bei BlueXP an oder melden Sie sich an.
3. Nachdem Sie angemeldet sind, richten Sie BlueXP ein:

   a. Geben Sie einen Namen für den Connector ein.

   b. Geben Sie einen Namen für ein neues BlueXP Konto ein, oder wählen Sie ein bestehendes Konto aus.

      Sie können ein bestehendes Konto auswählen, wenn Ihr Login bereits einem BlueXP Konto zugeordnet ist.

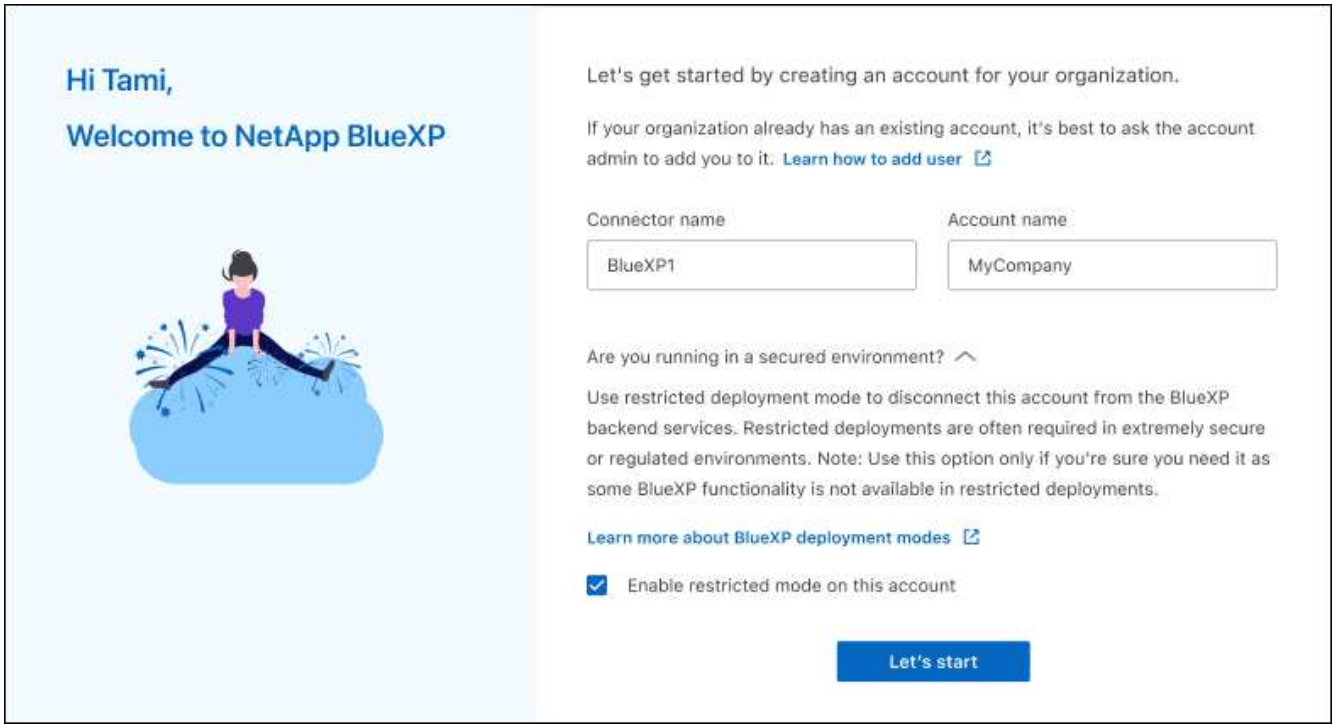
   c. Wählen Sie **laufen Sie in einer sicheren Umgebung?**

   d. Wählen Sie **eingeschränkten Modus für dieses Konto aktivieren**.

      Beachten Sie, dass Sie diese Einstellung nicht ändern können, nachdem BlueXP das Konto erstellt hat. Der eingeschränkte Modus kann später nicht aktiviert werden, und Sie können ihn später nicht

mehr deaktivieren.

Wenn Sie den Connector in einer Regierungsregion bereitgestellt haben, ist das Kontrollkästchen bereits aktiviert und kann nicht geändert werden. Dies liegt daran, dass der eingeschränkte Modus der einzige Modus ist, der in Regierungsregionen unterstützt wird.



a. Wählen Sie **Start**.

Ergebnis

Der Connector ist jetzt mit Ihrem BlueXP Konto installiert und eingerichtet. Alle Benutzer müssen über die IP-Adresse der Connector-Instanz auf BlueXP zugreifen.

Was kommt als Nächstes?

Bereitstellen von BlueXP mit den Berechtigungen, die Sie bereits eingerichtet haben.

Schritt 3: Berechtigungen für BlueXP bereitstellen

Wenn Sie den Connector über den Azure Marketplace bereitgestellt oder die Connector-Software manuell installiert haben, müssen Sie die zuvor festgelegten Berechtigungen zur Nutzung der BlueXP Services angeben.

Diese Schritte gelten nicht, wenn Sie den Connector über AWS Marketplace bereitgestellt haben, da Sie während der Bereitstellung die erforderliche IAM-Rolle ausgewählt haben.

"Erfahren Sie, wie Sie Cloud-Berechtigungen vorbereiten".

AWS IAM-Rolle

Hängen Sie die zuvor erstellte IAM-Rolle an die EC2-Instanz an, in der Sie den Connector installiert haben.

Diese Schritte gelten nur, wenn Sie den Connector manuell in AWS installiert haben. Bei AWS Marketplace-Implementierungen haben Sie die Connector-Instanz bereits einer IAM-Rolle zugeordnet, die die erforderlichen Berechtigungen enthält.

Schritte

1. Wechseln Sie zur Amazon EC2-Konsole.
2. Wählen Sie **Instanzen**.
3. Wählen Sie die Connector-Instanz aus.
4. Wählen Sie **Actions > Security > Modify IAM Role** aus.
5. Wählen Sie die IAM-Rolle aus und wählen Sie **IAM-Rolle aktualisieren**.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Aktionen in AWS benötigt.

AWS-Zugriffsschlüssel

Bereitstellen von BlueXP mit dem AWS-Zugriffsschlüssel für einen IAM-Benutzer, der über die erforderlichen Berechtigungen verfügt

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 **Amazon Web Services > Connector**.
   b. **Zugangsdaten definieren**: 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.
   d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Aktionen in AWS benötigt.

Azure Rolle

Wechseln Sie zum Azure-Portal und weisen Sie der virtuellen Connector-Maschine für ein oder mehrere Abonnements die benutzerdefinierte Azure-Rolle zu.

Schritte

1. Öffnen Sie im Azure Portal den Service **Abonnements** und wählen Sie Ihr Abonnement aus.

Es ist wichtig, die Rolle aus dem Dienst **Subscriptions** zuzuweisen, da hier der Umfang der Rollenzuweisung auf Abonnementebene festgelegt ist. Der *scope* definiert die Ressourcen, für die der Zugriff gilt. Wenn Sie einen Umfang auf einer anderen Ebene angeben (z. B. auf Ebene der Virtual Machines), wirkt es sich darauf aus, dass Sie Aktionen aus BlueXP ausführen können.

"Microsoft Azure Dokumentation: Umfang für die rollenbasierte Zugriffssteuerung von Azure kennen"

2. Wählen Sie **Zugriffskontrolle (IAM)** > **Hinzufügen** > **Rollenzuweisung hinzufügen**.
3. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.

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

4. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
   a. Weisen Sie einer * verwalteten Identität* Zugriff zu.
   b. Wählen Sie **Mitglieder auswählen**, wählen Sie das Abonnement, in dem die virtuelle Connector-Maschine erstellt wurde, unter **verwaltete Identität**, wählen Sie **virtuelle Maschine** und wählen Sie dann die virtuelle Connector-Maschine aus.
   c. Wählen Sie **Auswählen**.
   d. Wählen Sie **Weiter**.
   e. Wählen Sie **Überprüfen + Zuweisen**.
   f. Wenn Sie Ressourcen in weiteren Azure-Abonnements managen möchten, wechseln Sie zu diesem Abonnement und wiederholen Sie die folgenden Schritte.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Azure Service Principal

Stellen Sie BlueXP die Zugangsdaten für das zuvor von Ihnen Setup für den Azure Service Principal zur Verfügung.

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

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Google Cloud Service-Konto

Verknüpfen Sie das Servicekonto mit der Konnektor-VM.

Schritte

1. Wechseln Sie zum Google Cloud Portal und weisen Sie das Servicekonto der VM-Instanz des Connectors zu.

   "Google Cloud-Dokumentation: Ändern des Dienstkontos und des Zugriffsumfangs für eine Instanz"

2. Wenn Sie Ressourcen in anderen Projekten managen möchten, gewähren Sie Zugriff, indem Sie das Servicekonto mit der BlueXP Rolle zu diesem Projekt hinzufügen. Sie müssen diesen Schritt für jedes Projekt wiederholen.

Ergebnis

BlueXP verfügt jetzt über die nötigen Berechtigungen, um Aktionen in Google Cloud für Sie durchzuführen.

BlueXP abonnieren (eingeschränkter Modus)

Abonnieren Sie BlueXP über den Marketplace Ihres Cloud-Providers und zahlen Sie für BlueXP Services zu einem Stundensatz (PAYGO) oder über einen Jahresvertrag. Wenn Sie eine Lizenz von NetApp (BYOL) erworben haben, müssen Sie auch das Marketplace-Angebot abonnieren. Ihre Lizenz wird immer zuerst berechnet, aber Sie werden mit dem Stundensatz belastet, wenn Sie Ihre lizenzierte Kapazität überschreiten oder wenn die Laufzeit der Lizenz abläuft.

Ein Marketplace Abonnement ermöglicht die Abrechnung der folgenden BlueXP Services mit eingeschränktem Modus:

- Backup und Recovery
- Klassifizierung
- Cloud Volumes ONTAP

Bevor Sie beginnen

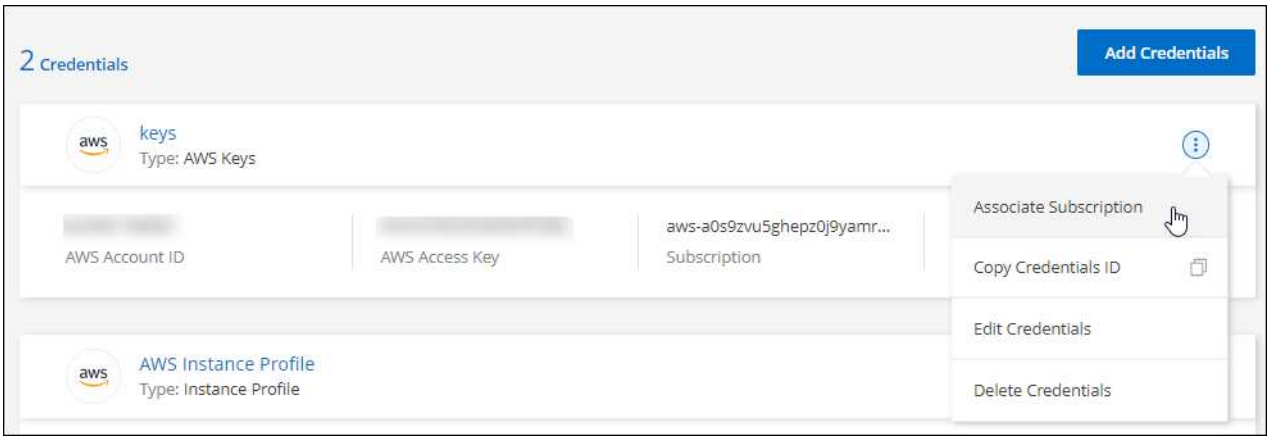
Für das Abonnement von BlueXP wird ein Marketplace-Abonnement mit den Cloud-Zugangsdaten verknüpft, die einem Connector zugeordnet sind. Wenn Sie den Workflow „erste Schritte mit eingeschränktem Modus“ befolgt haben, sollten Sie bereits über einen Connector verfügen. Weitere Informationen finden Sie im "Schnellstart für BlueXP im eingeschränkten Modus".

AWS

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:

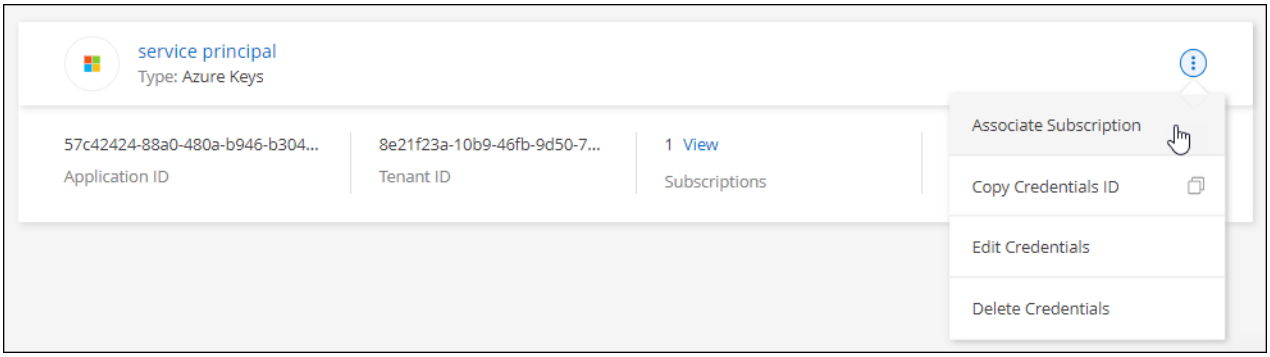
Abonnieren Sie BlueXP über den AWS Marketplace

Azure

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**.

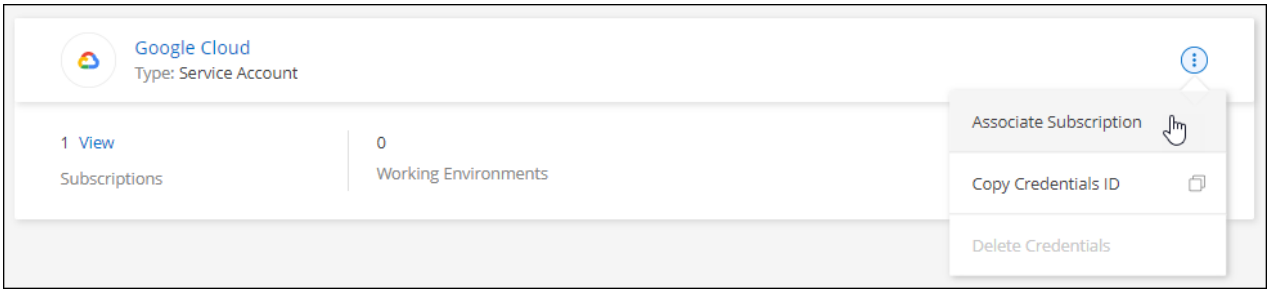
Im folgenden Video sehen Sie, wie Sie im Azure Marketplace abonnieren:

Abonnieren Sie BlueXP über den Azure Marketplace

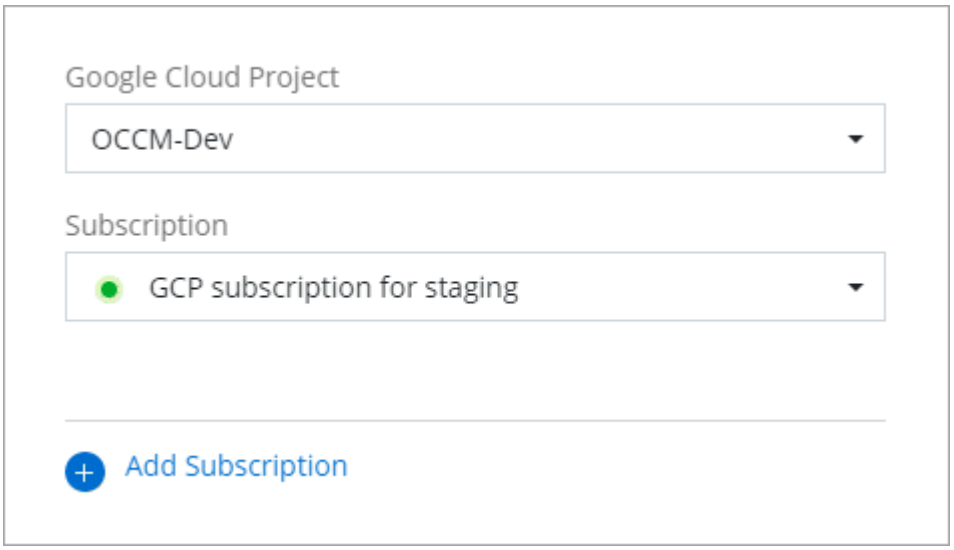
Google Cloud

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**.



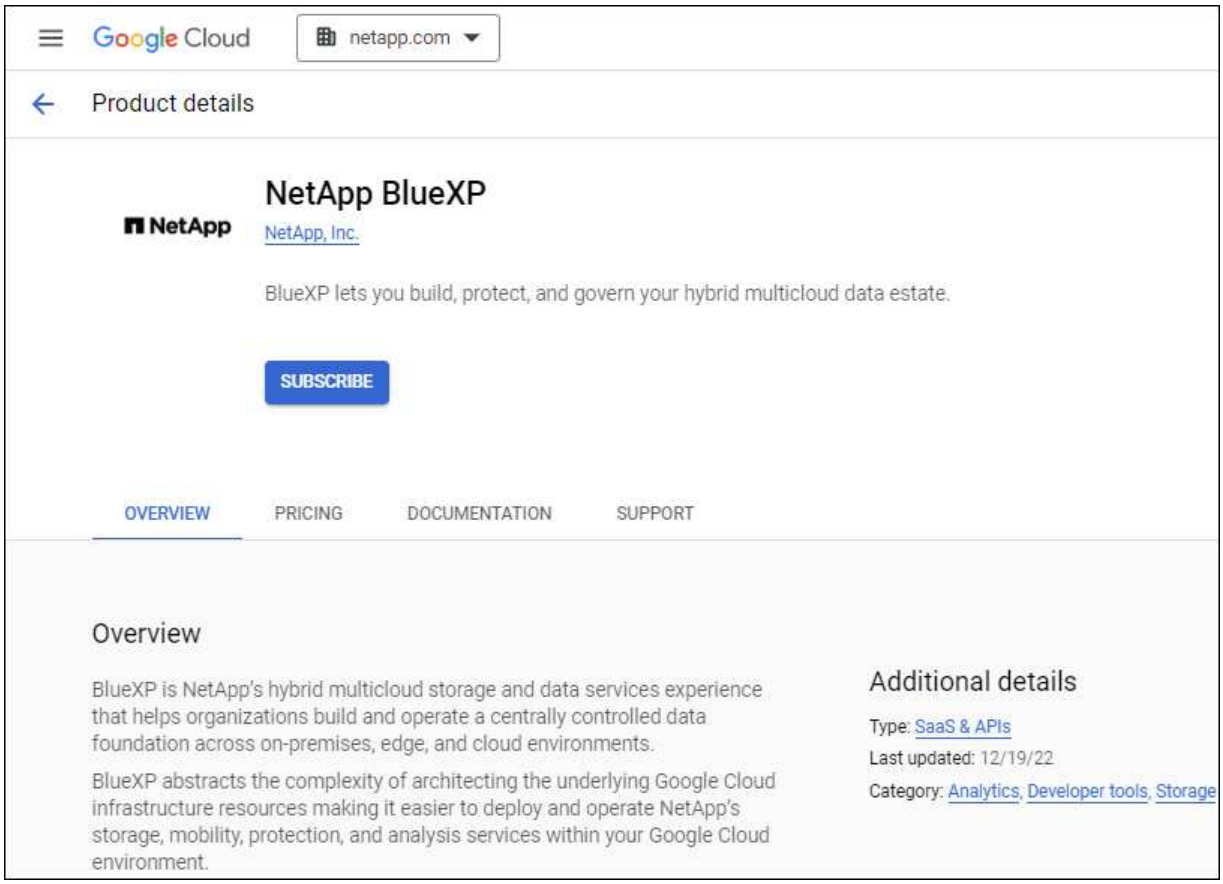
3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, und wählen Sie dann **Associate** aus.



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**.

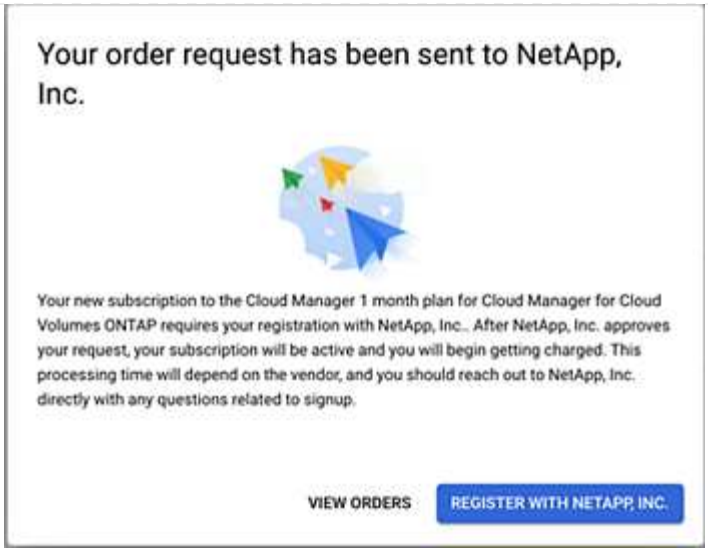
c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

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.

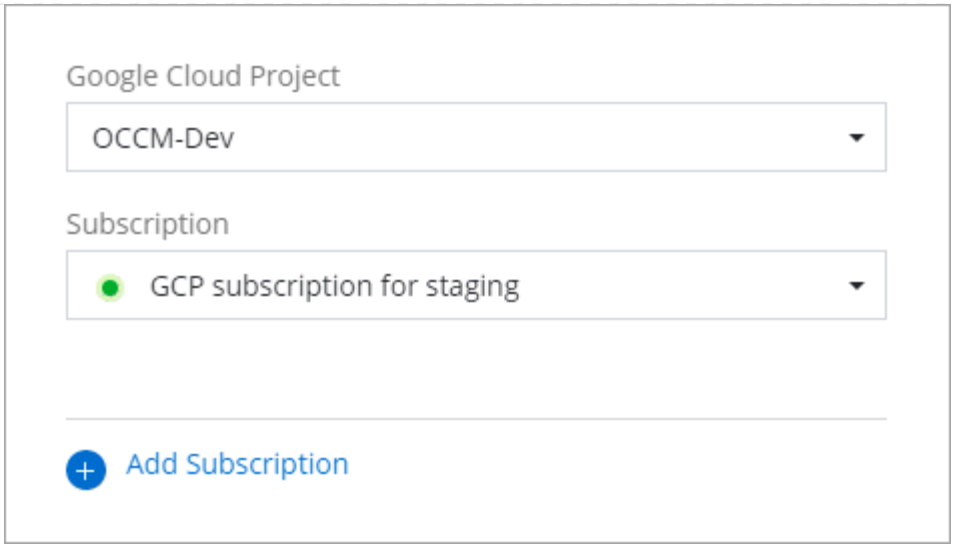
Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden Schritte wiederholen.

- 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.



Weiterführende Links

- "Managen Sie kapazitätsbasierte BYOL-Lizenzen für Cloud Volumes ONTAP"
- "Managen von BYOL-Lizenzen für BlueXP Datenservices"
- "Managen Sie AWS Anmeldeinformationen und Abonnements für BlueXP"
- "Managen Sie Azure Anmeldedaten und Abonnements für BlueXP"
- "Managen Sie Google Cloud-Anmeldedaten und -Abonnements für BlueXP"

Nächste Schritte (eingeschränkter Modus)

Nachdem Sie BlueXP im eingeschränkten Modus eingerichtet haben, können Sie die BlueXP Services, die mit eingeschränktem Modus unterstützt werden, nutzen.

Hilfe finden Sie in der Dokumentation zu diesen Services:

- "Amazon FSX für ONTAP Dokumentation"
- "Azure NetApp Files Dokumentation"
- "Dokumentation zu Backup und Recovery"
- "Dokumente zur Klassifizierung"
- "Cloud Volumes ONTAP Dokumentation"
- "ONTAP-Cluster-Dokumentation vor Ort"
- "Replizierungsdokumente"

Verwandter Link

"BlueXP Implementierungsmodi"

Starten Sie mit dem privaten Modus

Erste Schritte Workflow (privater Modus)

Erste Schritte mit BlueXP im privaten Modus: Bereiten Sie Ihre Umgebung vor und implementieren Sie den Connector.

Der private Modus wird in der Regel mit On-Premises-Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, einschließlich "AWS Secret Cloud", "Top Secret Cloud von AWS", und "Azure IL6"

Bevor Sie beginnen, sollten Sie ein Verständnis von haben "BlueXP Accounts", "Anschlüsse", und "Bereitstellungsmodi".

1 **"Vorbereitungen für die Implementierung"**

1. Bereiten Sie einen dedizierten Linux-Host vor, der die Anforderungen für CPU, RAM, Festplattenspeicher, Docker Engine und mehr erfüllt.
2. Richten Sie ein Netzwerk ein, das Zugriff auf die Zielnetzwerke bietet.
3. Richten Sie bei Cloud-Bereitstellungen Berechtigungen in Ihrem Cloud-Provider ein, damit Sie diese Berechtigungen nach der Installation der Software mit dem Connector verknüpfen können.

2 **"Implementieren Sie den Connector"**

1. Installieren Sie die Connector-Software auf Ihrem eigenen Linux-Host.
2. Richten Sie BlueXP ein, indem Sie einen Webbrowser öffnen und die IP-Adresse des Linux-Hosts eingeben.
3. Stellen Sie für Cloud-Implementierungen BlueXP die Berechtigungen bereit, die Sie zuvor eingerichtet haben.

Bereiten Sie die Bereitstellung im privaten Modus vor

Bereiten Sie Ihre Umgebung vor der Implementierung von BlueXP im privaten Modus vor. Sie müssen beispielsweise die Hostanforderungen prüfen, das Netzwerk vorbereiten, Berechtigungen einrichten und vieles mehr.

> Wenn Sie BlueXP in der verwenden möchten "AWS Secret Cloud" Oder im "Top Secret Cloud von AWS"Dann sollten Sie separate Anweisungen befolgen, um in diesen Umgebungen zu beginnen. "Erste Schritte mit Cloud Volumes ONTAP – in der AWS Secret Cloud oder Top Secret Cloud"

Schritt 1: Verstehen, wie der private Modus funktioniert

Bevor Sie beginnen, sollten Sie sich ein Bild davon machen, wie BlueXP im privaten Modus funktioniert.

Sie sollten beispielsweise verstehen, dass Sie die browserbasierte Oberfläche verwenden müssen, die lokal über den BlueXP Connector verfügbar ist, die Sie installieren müssen. Der Zugriff auf BlueXP erfolgt nicht über die webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird.

Außerdem sind nicht alle BlueXP Services verfügbar.

"Erfahren Sie, wie der private Modus funktioniert".

Schritt 2: Überprüfen Sie die Installationsoptionen

Im privaten Modus können Sie den Connector vor Ort oder in der Cloud installieren, indem Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren.

Bei der Installation des Connectors wird festgelegt, welche BlueXP Services und Funktionen beim Einsatz des privaten Modus verfügbar sind. Beispielsweise muss der Connector in der Cloud installiert sein, wenn Sie Cloud Volumes ONTAP bereitstellen und verwalten möchten. "Weitere Informationen zum privaten Modus".

Schritt 3: Überprüfen Sie die Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 und 7.9
- Red hat Enterprise Linux 7.6, 7.7, 7.8 und 7.9

  Der Host muss bei Red hat Subscription Management registriert sein. Wenn er nicht registriert ist, kann der Host während der Connector-Installation nicht auf Repositorys zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

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

Hypervisor

Ein Bare-Metal- oder Hosted-Hypervisor, der für Ubuntu, CentOS oder Red hat Enterprise Linux zertifiziert ist, ist erforderlich.

"Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Azure VM-Größe

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

Google Cloud-Maschinentyp

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

Der Connector wird in Google Cloud auf einer VM-Instanz mit einem unterstützten Betriebssystem

unterstützt "Geschirmte VM-Funktionen"

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine ist auf dem Host erforderlich, bevor Sie den Connector installieren.

- Die unterstützte Version ist mindestens 19.3.1.
- Die maximal unterstützte Version ist 25.0.5.

"Installationsanweisungen anzeigen"

Schritt 4: Vernetzung für den Connector vorbereiten

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung managen kann. Abgesehen von einem virtuellen Netzwerk und einem Subnetz für den Connector müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind.

Verbindungen zu Zielnetzwerken

Der Connector muss über eine Netzwerkverbindung zu dem Speicherort verfügen, an dem Sie Speicher verwalten möchten. Beispielsweise die VPC oder vnet, bei der Sie Cloud Volumes ONTAP implementieren möchten, oder das Datacenter, in dem sich Ihre ONTAP-Cluster vor Ort befinden.

Endpunkte für den täglichen Betrieb

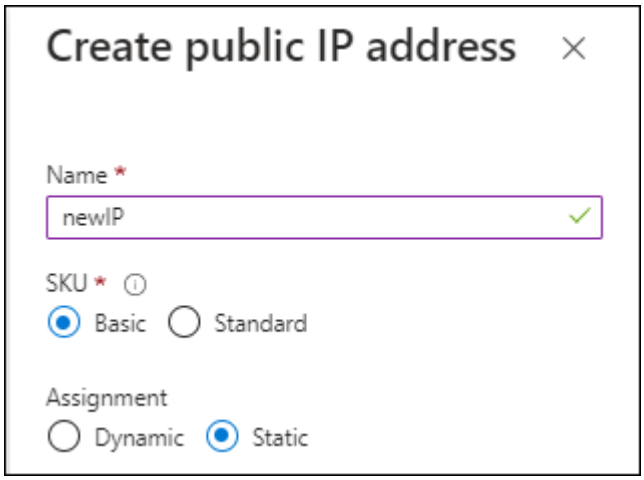
Der Connector kontaktiert die folgenden Endpunkte, um Ressourcen und Prozesse in der Public Cloud-Umgebung zu managen.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.

Endpunkte	Zweck
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Zum Managen von Ressourcen in der Region Azure-IL6.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.

Öffentliche IP-Adresse in Azure

Wenn Sie eine öffentliche IP-Adresse mit der Connector-VM in Azure verwenden möchten, muss die IP-Adresse eine Basis-SKU verwenden, um sicherzustellen, dass BlueXP diese öffentliche IP-Adresse verwendet.



Wenn Sie stattdessen eine Standard-SKU-IP-Adresse verwenden, verwendet BlueXP anstelle der öffentlichen IP die *private* IP-Adresse des Connectors. Wenn die Maschine, die Sie für den Zugriff auf die BlueXP-Konsole nutzen, keinen Zugriff auf diese private IP-Adresse hat, dann schlagen Aktionen aus der BlueXP-Konsole fehl.

"Azure-Dokumentation: Öffentliche IP-SKU"

Proxy-Server

Wenn Ihr Unternehmen die Bereitstellung eines Proxy-Servers für den gesamten ausgehenden Internet-Datenverkehr erfordert, erhalten Sie die folgenden Informationen zu Ihrem HTTP- oder HTTPS-Proxy.

Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

Beachten Sie, dass BlueXP keine transparenten Proxy-Server unterstützt.

+
Im privaten Modus sendet BlueXP lediglich Outbound-Datenverkehr zu Ihrem Cloud-Provider, um ein Cloud Volumes ONTAP System zu erstellen.

Ports

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn.

HTTP (80) und HTTPS (443) bieten den Zugriff auf die BlueXP Konsole. SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

Aktivieren Sie NTP

Wenn Sie Vorhaben, die BlueXP Klassifizierung zum Scannen von Unternehmensdatenquellen zu nutzen, sollten Sie sowohl auf dem BlueXP Connector-System als auch dem BlueXP Klassifizierungssystem einen Network Time Protocol (NTP)-Service aktivieren, damit die Zeit zwischen den Systemen synchronisiert wird. "Weitere Informationen zur BlueXP Klassifizierung"

Schritt 5: Cloud-Berechtigungen vorbereiten

Wenn der Connector in der Cloud installiert ist und Sie planen, Cloud Volumes ONTAP-Systeme zu erstellen, erfordert BlueXP Berechtigungen von Ihrem Cloud-Provider. Sie müssen Berechtigungen in Ihrem Cloud-Provider einrichten und diese Berechtigungen dann der Connector-Instanz zuordnen, nachdem Sie sie installiert haben.

Um die erforderlichen Schritte anzuzeigen, wählen Sie die Authentifizierungsoption aus, die Sie für Ihren Cloud-Provider verwenden möchten.

AWS IAM-Rolle

Verwenden Sie eine IAM-Rolle, um dem Connector Berechtigungen zu gewähren. Sie müssen die Rolle manuell an die EC2-Instanz für den Connector anhängen.

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:
   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.
3. Erstellen einer IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Service > EC2** aus.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die soeben erstellte Richtlinie anhängen.
   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

Ergebnis

Sie haben jetzt eine IAM-Rolle für die EC2-Instanz des Connectors.

AWS-Zugriffsschlüssel

Richten Sie Berechtigungen und einen Zugriffsschlüssel für einen IAM-Benutzer ein. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP mit dem AWS-Zugriffsschlüssel bereitstellen.

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:
   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.

      Abhängig von den BlueXP Services, die Sie planen zu verwenden, müssen Sie möglicherweise eine zweite Richtlinie erstellen.

   Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich. "Erfahren Sie mehr über IAM-Richtlinien für den Connector".
3. Fügen Sie die Richtlinien einem IAM-Benutzer hinzu.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie nach der Installation des Connectors zu BlueXP hinzufügen können.

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen.

Azure Rolle

Erstellen einer benutzerdefinierten Azure-Rolle mit den erforderlichen Berechtigungen. Sie werden diese Rolle der Connector-VM zuweisen.

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"

Schritte

1. Aktivieren Sie eine vom System zugewiesene gemanagte Identität auf der VM, bei der Sie den Connector installieren möchten, damit Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

   "Microsoft Azure-Dokumentation: Gemanagte Identitäten für Azure-Ressourcen auf einer VM über das Azure-Portal konfigurieren"

2. Kopieren Sie den Inhalt des "Benutzerdefinierte Rollenberechtigungen für den Konnektor" Und speichern Sie sie in einer JSON-Datei.
3. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

   Sie sollten für jedes Azure-Abonnement, das Sie mit BlueXP verwenden möchten, die ID hinzufügen.

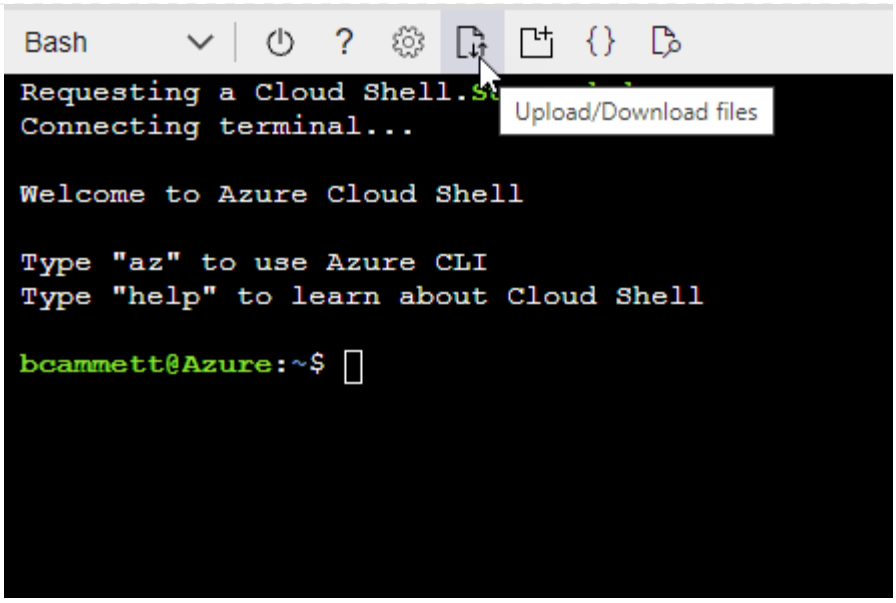
   Beispiel

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

4. 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.

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



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

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

Ergebnis

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

Azure Service Principal

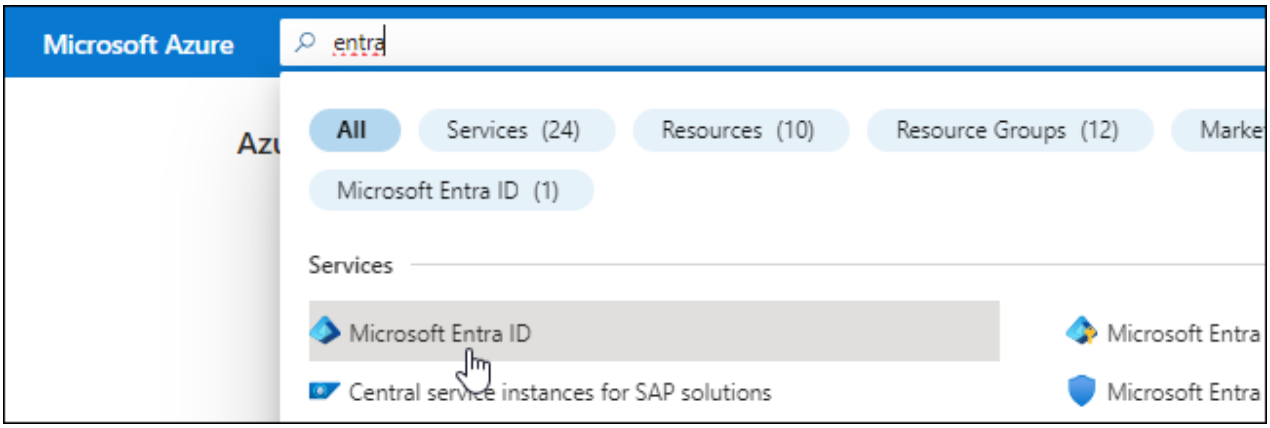
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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.

Anwendung einer Rolle zuweisen

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.

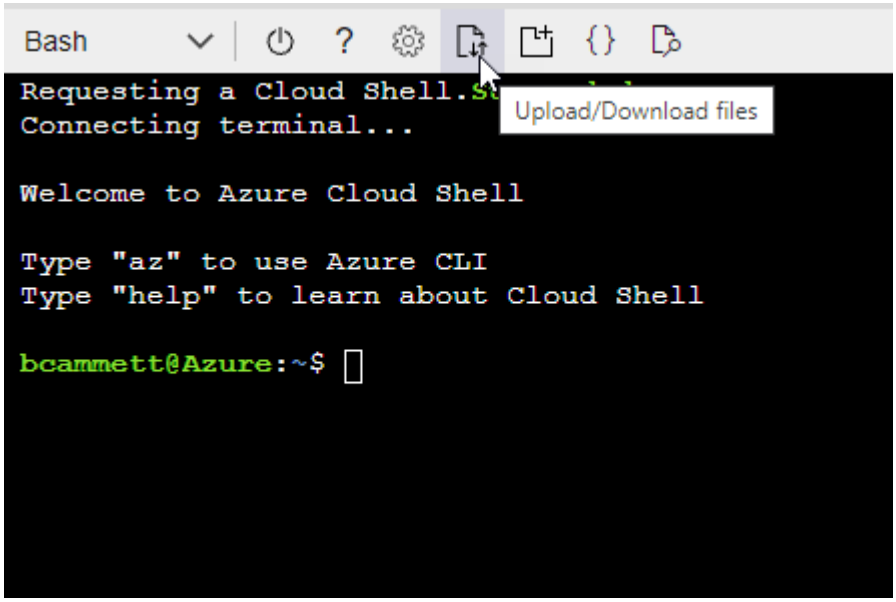
      Beispiel

      ```
      "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:

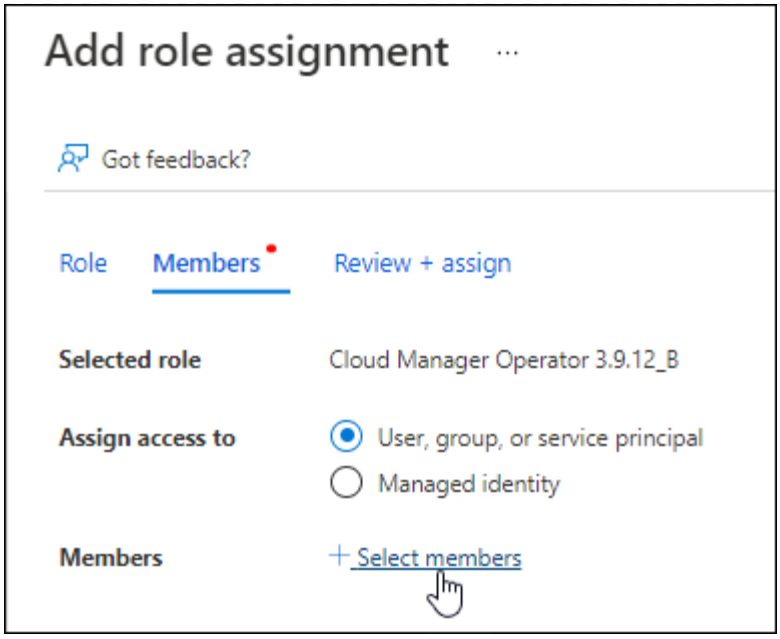
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

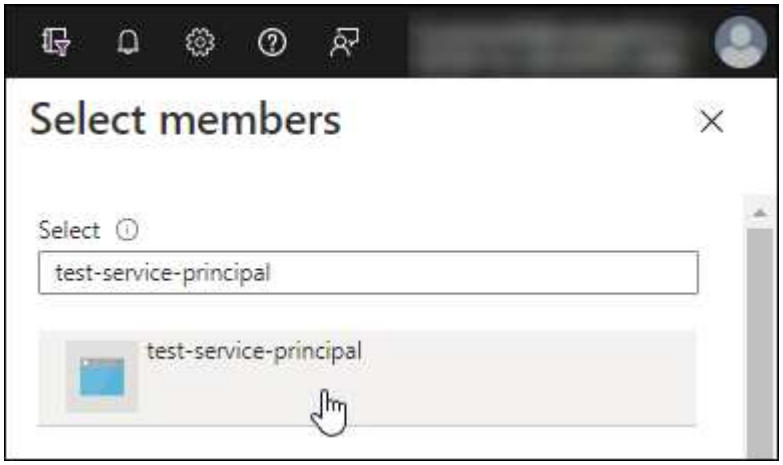
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

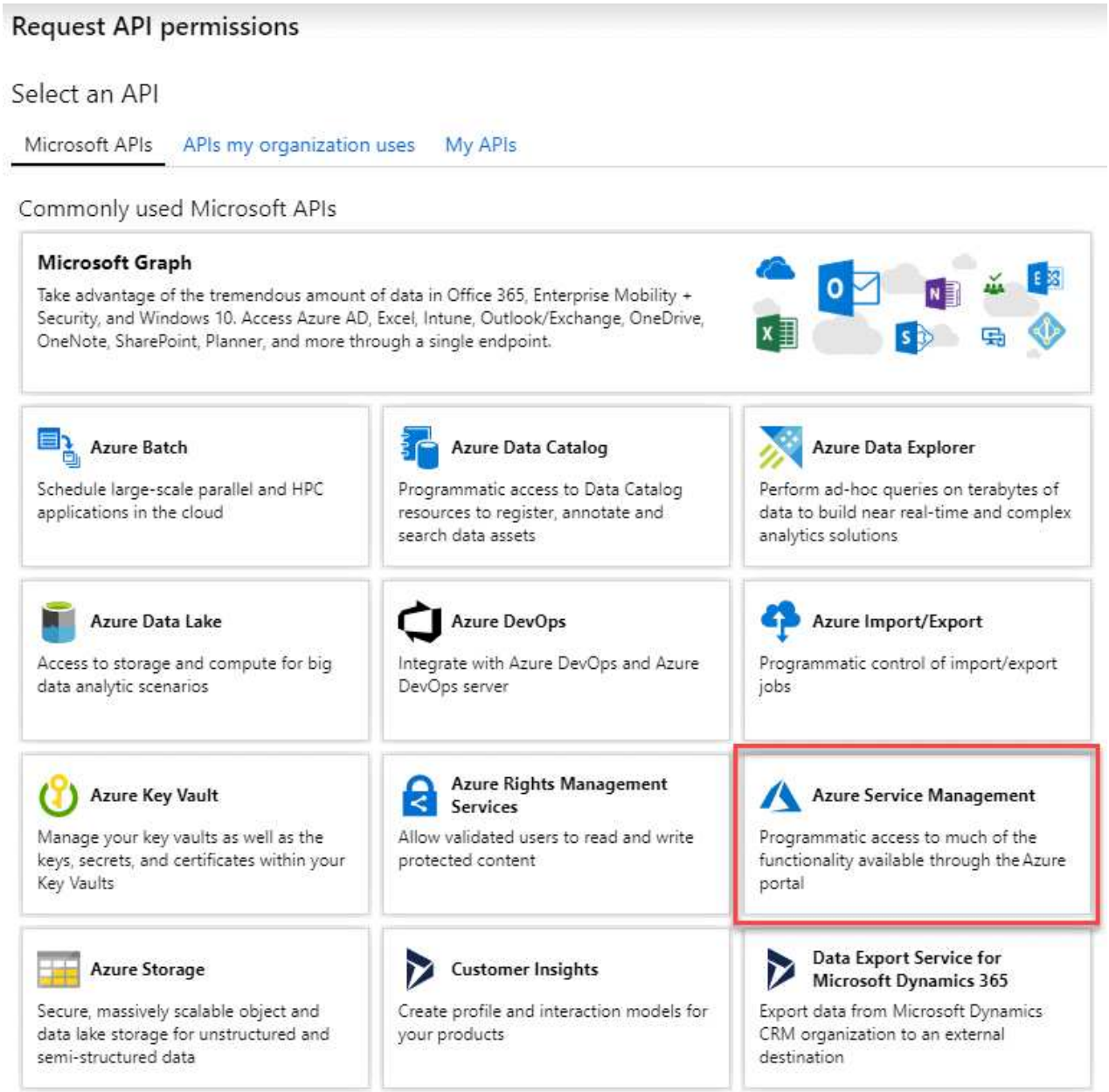
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

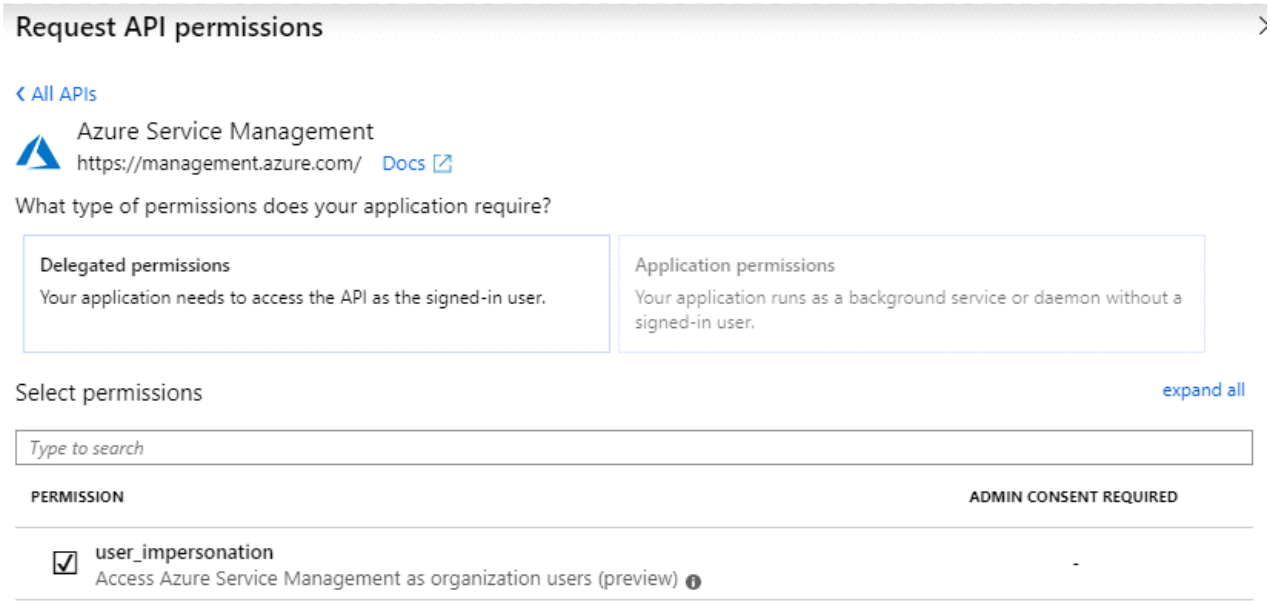
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

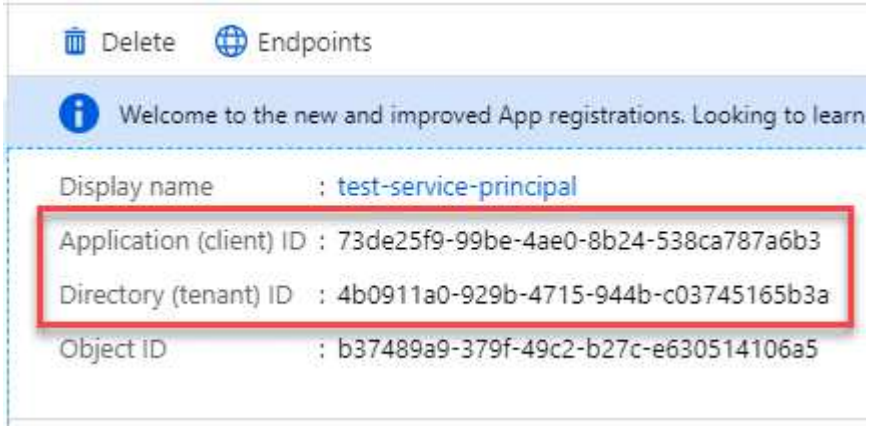


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



Die Anwendungs-ID und die Verzeichnis-ID für die Anwendung abrufen

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

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.

Google Cloud Service-Konto

Erstellen Sie eine Rolle und wenden Sie sie auf ein Servicekonto an, das Sie für die VM-Instanz des Connectors verwenden werden.

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

   a. Erstellen Sie eine YAML-Datei, die die in definierten Berechtigungen enthält "Connector-Richtlinie für Google Cloud".

   b. Aktivieren Sie in Google Cloud die Cloud Shell.

   c. Laden Sie die YAML-Datei hoch, die die erforderlichen Berechtigungen für den Connector enthält.

   d. Erstellen Sie mithilfe von eine benutzerdefinierte Rolle `gcloud iam roles create` Befehl.

      Im folgenden Beispiel wird auf Projektebene eine Rolle namens „Connector“ erstellt:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Google Cloud docs: Erstellen und Verwalten benutzerdefinierter Rollen"

2. Erstellen Sie ein Servicekonto in Google Cloud:

   a. Wählen Sie im IAM & Admin-Dienst **Service-Konten > Service-Konto erstellen** aus.

   b. Geben Sie die Details des Servicekontos ein und wählen Sie **Erstellen und Fortfahren**.

   c. Wählen Sie die gerade erstellte Rolle aus.

   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

      "Google Cloud docs: Erstellen eines Dienstkontos"

Ergebnis

Sie verfügen jetzt über ein Servicekonto, das Sie der VM-Instanz des Connectors zuweisen können.

Schritt 6: Google Cloud APIs aktivieren

Für die Implementierung von Cloud Volumes ONTAP in Google Cloud sind mehrere APIs erforderlich.

Schritt

1. "Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt"
   - Cloud Deployment Manager V2-API
   - Cloud-ProtokollierungsAPI
   - Cloud Resource Manager API
   - Compute Engine-API
   - IAM-API (Identitäts- und Zugriffsmanagement
   - KMS-API (Cloud Key Management Service)

     (Nur erforderlich, wenn Sie BlueXP Backup und Recovery mit vom Kunden gemanagten Verschlüsselungsschlüsseln (CMEK) verwenden möchten).

Stellen Sie den Connector im privaten Modus bereit

Implementieren Sie den Connector im privaten Modus, sodass Sie BlueXP ohne Outbound-Konnektivität zur BlueXP SaaS-Ebene nutzen können. Installieren Sie den Connector, richten Sie BlueXP über die Benutzeroberfläche ein, die auf dem Connector ausgeführt wird, und stellen Sie dann die zuvor festgelegten Cloud-Berechtigungen bereit.

Schritt 1: Installieren Sie den Stecker

Laden Sie das Produkt-Installationsprogramm von der NetApp Support Site herunter und installieren Sie den Connector dann manuell auf Ihrem eigenen Linux Host.

Wenn Sie BlueXP in der verwenden möchten "AWS Secret Cloud" Oder im "Top Secret Cloud von AWS"Dann sollten Sie separate Anweisungen befolgen, um in diesen Umgebungen zu beginnen. "Erste Schritte mit Cloud Volumes ONTAP – in der AWS Secret Cloud oder Top Secret Cloud"

Bevor Sie beginnen

Zur Installation des Connectors sind Root-Berechtigungen erforderlich.

Schritte

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

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

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

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

3. Kopieren Sie das Installationsprogramm auf den Linux-Host.
4. 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.

5. Führen Sie das Installationsskript aus:

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

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

Ergebnis

Die Connector-Software ist installiert. Sie können jetzt BlueXP einrichten.

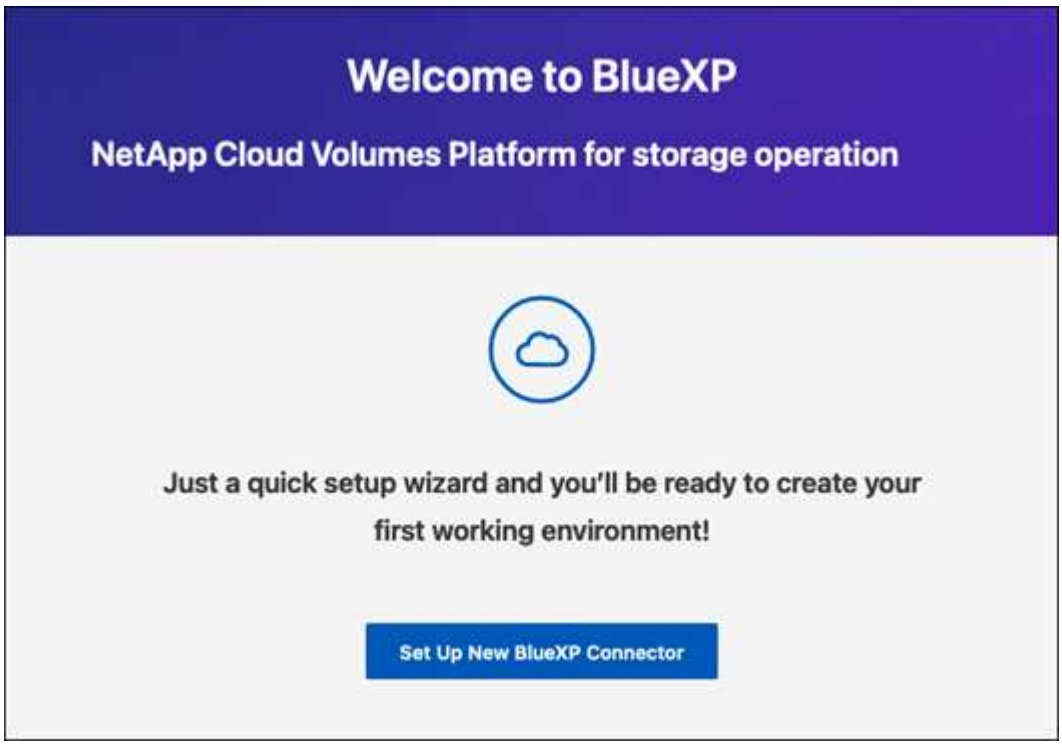
Schritt 2: BlueXP einrichten

Wenn Sie zum ersten Mal die BlueXP Konsole aufrufen, werden Sie aufgefordert, BlueXP einzurichten.

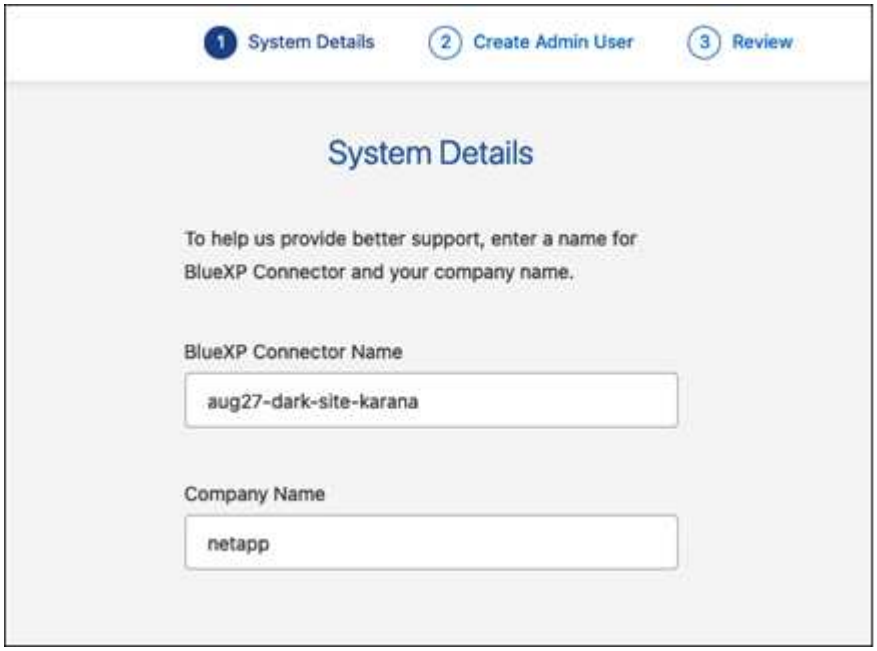
Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie ein https://ipaddress Wobei ipaddress die IP-Adresse des Linux-Hosts ist, auf dem Sie den Connector installiert haben.

   Der folgende Bildschirm sollte angezeigt werden.



2. Wählen Sie **Set up New BlueXP Connector** und folgen Sie den Anweisungen, um das System einzurichten.
    - **Systemdetails**: Geben Sie einen Namen für den Connector und Ihren Firmennamen ein.



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

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

    - **Review**: Überprüfen Sie die Details, akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Setup**.
3. Melden Sie sich mit dem gerade erstellten Admin-Benutzer bei BlueXP an.

Ergebnis

Der Connector ist jetzt installiert und eingerichtet.

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

Was kommt als Nächstes?

Bereitstellen von BlueXP mit den Berechtigungen, die Sie bereits eingerichtet haben.

Schritt 3: Berechtigungen für BlueXP bereitstellen

Wenn Sie Cloud Volumes ONTAP-Arbeitsumgebungen erstellen möchten, müssen Sie BlueXP mit den zuvor festgelegten Cloud-Berechtigungen versehen.

"Erfahren Sie, wie Sie Cloud-Berechtigungen vorbereiten".

AWS IAM-Rolle

Fügen Sie die zuvor erstellte IAM-Rolle der Connector EC2-Instanz hinzu.

Schritte

1. Wechseln Sie zur Amazon EC2-Konsole.
2. Wählen Sie **Instanzen**.
3. Wählen Sie die Connector-Instanz aus.
4. Wählen Sie **Actions > Security > Modify IAM Role** aus.
5. Wählen Sie die IAM-Rolle aus und wählen Sie **IAM-Rolle aktualisieren**.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Aktionen in AWS benötigt.

AWS-Zugriffsschlüssel

Bereitstellen von BlueXP mit dem AWS-Zugriffsschlüssel für einen IAM-Benutzer, der über die erforderlichen Berechtigungen verfügt

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 **Amazon Web Services > Connector**.
   b. **Zugangsdaten definieren**: 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.
   d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Aktionen in AWS benötigt.

Azure Rolle

Wechseln Sie zum Azure-Portal und weisen Sie der virtuellen Connector-Maschine für ein oder mehrere Abonnements die benutzerdefinierte Azure-Rolle zu.

Schritte

1. Öffnen Sie im Azure Portal den Service **Abonnements** und wählen Sie Ihr Abonnement aus.

   Es ist wichtig, die Rolle aus dem Dienst **Subscriptions** zuzuweisen, da hier der Umfang der Rollenzuweisung auf Abonnementebene festgelegt ist. Der *scope* definiert die Ressourcen, für die der Zugriff gilt. Wenn Sie einen Umfang auf einer anderen Ebene angeben (z. B. auf Ebene der Virtual Machines), wirkt es sich darauf aus, dass Sie Aktionen aus BlueXP ausführen können.

"Microsoft Azure Dokumentation: Umfang für die rollenbasierte Zugriffssteuerung von Azure kennen"

2. Wählen Sie **Zugriffskontrolle (IAM)** > **Hinzufügen** > **Rollenzuweisung hinzufügen**.
3. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.

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

4. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
   a. Weisen Sie einer * verwalteten Identität* Zugriff zu.
   b. Wählen Sie **Mitglieder auswählen**, wählen Sie das Abonnement, in dem die virtuelle Connector-Maschine erstellt wurde, unter **verwaltete Identität**, wählen Sie **virtuelle Maschine** und wählen Sie dann die virtuelle Connector-Maschine aus.
   c. Wählen Sie **Auswählen**.
   d. Wählen Sie **Weiter**.
   e. Wählen Sie **Überprüfen + Zuweisen**.
   f. Wenn Sie Ressourcen in weiteren Azure-Abonnements managen möchten, wechseln Sie zu diesem Abonnement und wiederholen Sie die folgenden Schritte.

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Azure Service Principal

Stellen Sie BlueXP die Zugangsdaten für das zuvor von Ihnen Setup für den Azure Service Principal zur Verfügung.

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

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt.

Google Cloud Service-Konto

Verknüpfen Sie das Servicekonto mit der Konnektor-VM.

Schritte

1. Wechseln Sie zum Google Cloud Portal und weisen Sie das Servicekonto der VM-Instanz des Connectors zu.

   "Google Cloud-Dokumentation: Ändern des Dienstkontos und des Zugriffsumfangs für eine Instanz"

2. Wenn Sie Ressourcen in anderen Projekten managen möchten, gewähren Sie Zugriff, indem Sie das Servicekonto mit der BlueXP Rolle zu diesem Projekt hinzufügen. Sie müssen diesen Schritt für jedes Projekt wiederholen.

Ergebnis

BlueXP verfügt jetzt über die nötigen Berechtigungen, um Aktionen in Google Cloud für Sie durchzuführen.

Nächste Schritte (privater Modus)

Nachdem Sie BlueXP im privaten Modus eingerichtet haben, können Sie die BlueXP Services, die vom privaten Modus unterstützt werden, sofort nutzen.

Hilfe finden Sie in der folgenden Dokumentation:

- "Erstellen von Cloud Volumes ONTAP Systemen"
- "Erkennen von ONTAP Clustern vor Ort"
- "Datenreplizierung"
- "Scannen Sie On-Premises-ONTAP-Volume-Daten mithilfe der BlueXP Klassifizierung"
- "Sichern Sie lokale ONTAP Volume-Daten mithilfe von BlueXP Backup- und Recovery-Funktionen in StorageGRID"

Verwandter Link

"BlueXP Implementierungsmodi"

Melden Sie sich bei BlueXP an

Die Anmeldung bei BlueXP hängt vom BlueXP Implementierungsmodus ab, den Sie für Ihr Konto verwenden.

Standardmodus

Nachdem Sie sich bei BlueXP angemeldet haben, können Sie sich über die webbasierte Konsole anmelden, um mit dem Management Ihrer Daten und Storage-Infrastruktur zu beginnen.

Über diese Aufgabe

Sie können sich über eine der folgenden Optionen bei der webbasierten Konsole von BlueXP anmelden:

- Ihre vorhandenen Zugangsdaten für die NetApp Support Site (NSS
- Nutzen Sie Ihre E-Mail-Adresse und ein Passwort, um sich bei einem NetApp Cloud-Login anzumelden
- Eine Verbundverbindung

  Sie können sich mit Single Sign-On über Anmeldedaten aus Ihrem Unternehmensverzeichnis (föderierte Identität) anmelden. "Erfahren Sie mehr über den Einsatz von Identitätsföderation mit BlueXP".

Schritte

1. Öffnen Sie einen Webbrowser, und rufen Sie den auf "BlueXP-Konsole"
2. Geben Sie auf der Seite **Anmelden** die E-Mail-Adresse ein, die mit Ihrem Login verknüpft ist.
3. Abhängig von der Authentifizierungsmethode, die mit Ihrer Anmeldung verknüpft ist, werden Sie aufgefordert, Ihre Anmeldedaten einzugeben:
   - NetApp Cloud-Anmeldedaten: Geben Sie Ihr Passwort ein
   - Föderierte Benutzer: Geben Sie Ihre föderierten Identitätsinformationen ein
   - NetApp Support Site Konto: Geben Sie Ihre Zugangsdaten für die NetApp Support Site ein

Ergebnis

Sie sind jetzt angemeldet und können mit BlueXP Ihre Hybrid-Multi-Cloud-Infrastruktur managen.

Eingeschränkter Modus

Wenn Sie BlueXP im eingeschränkten Modus nutzen, müssen Sie sich über die lokale Benutzeroberfläche des Connector bei der BlueXP Konsole anmelden.

Über diese Aufgabe

BlueXP unterstützt die Anmeldung über eine der folgenden Optionen, wenn Ihr Konto im eingeschränkten Modus eingerichtet wird:

- Nutzen Sie Ihre E-Mail-Adresse und ein Passwort, um sich bei einem NetApp Cloud-Login anzumelden
- Eine Verbundverbindung

  Sie können sich mit Single Sign-On über Anmeldedaten aus Ihrem Unternehmensverzeichnis (föderierte Identität) anmelden. "Erfahren Sie mehr über den Einsatz von Identitätsföderation mit BlueXP".

Schritte

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

   https://ipaddress

Ipaddress kann localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein, abhängig von der Konfiguration des Hosts, auf dem Sie den Connector installiert haben. Sie müssen beispielsweise eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-Host hat.

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

Ergebnis

Sie sind jetzt angemeldet und können mit BlueXP Ihre Hybrid-Multi-Cloud-Infrastruktur managen.

Privater Modus

Wenn Sie BlueXP im privaten Modus nutzen, müssen Sie sich über die lokale Benutzeroberfläche des Connector bei der BlueXP Konsole anmelden.

Über diese Aufgabe

Der private Modus unterstützt lokale Benutzerverwaltung und -Zugriff. Authentifizierung wird nicht über den Cloud-Service von BlueXP bereitgestellt.

Schritte

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

   https://ipaddress

   Ipaddress kann localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein, abhängig von der Konfiguration des Hosts, auf dem Sie den Connector installiert haben. Sie müssen beispielsweise eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-Host hat.

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

Ergebnis

Sie sind jetzt angemeldet und können mit BlueXP Ihre Hybrid-Multi-Cloud-Infrastruktur managen.

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:

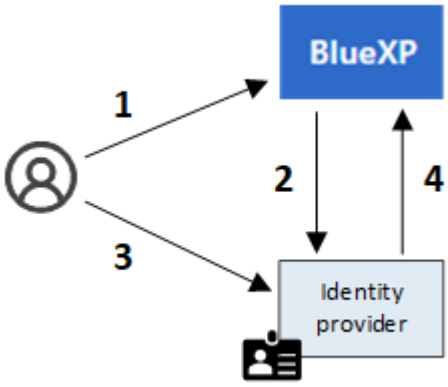
- Laden Sie die herunter, und füllen Sie die aus "Antragsformular für die NetApp Föderation"
- Senden Sie das Formular an die im Formular angegebene E-Mail-Adresse

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

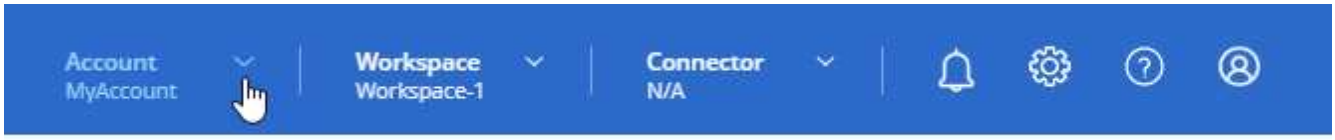
Der Benutzer in Ihrem Konto kann auf die Ressourcen in bestimmten Arbeitsbereichen zugreifen und diese verwalten.

Benutzer hinzufügen

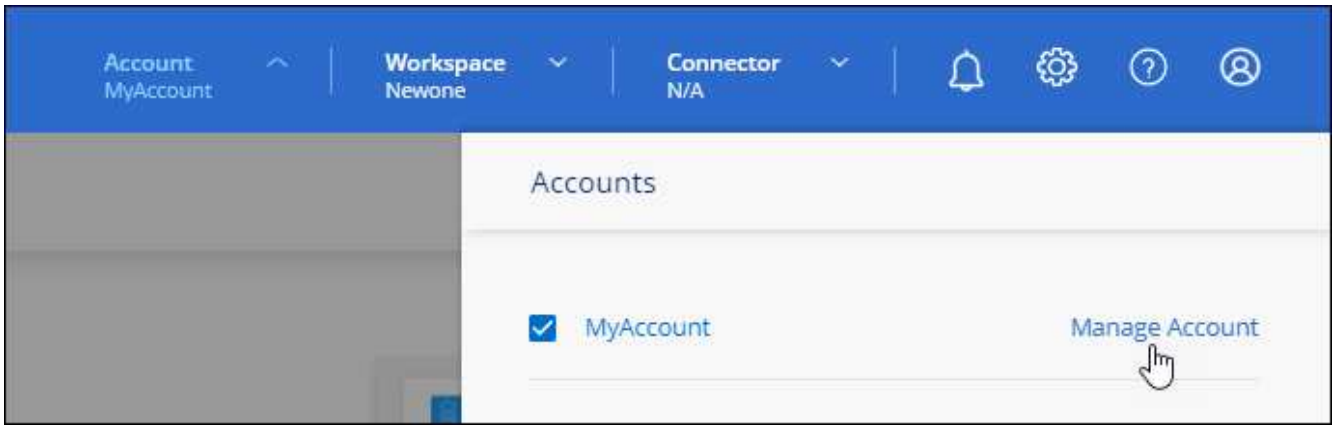
Ordnen Sie Benutzer Ihrem BlueXP Konto zu, damit diese Benutzer Arbeitsumgebungen in BlueXP erstellen und managen können.

Schritte

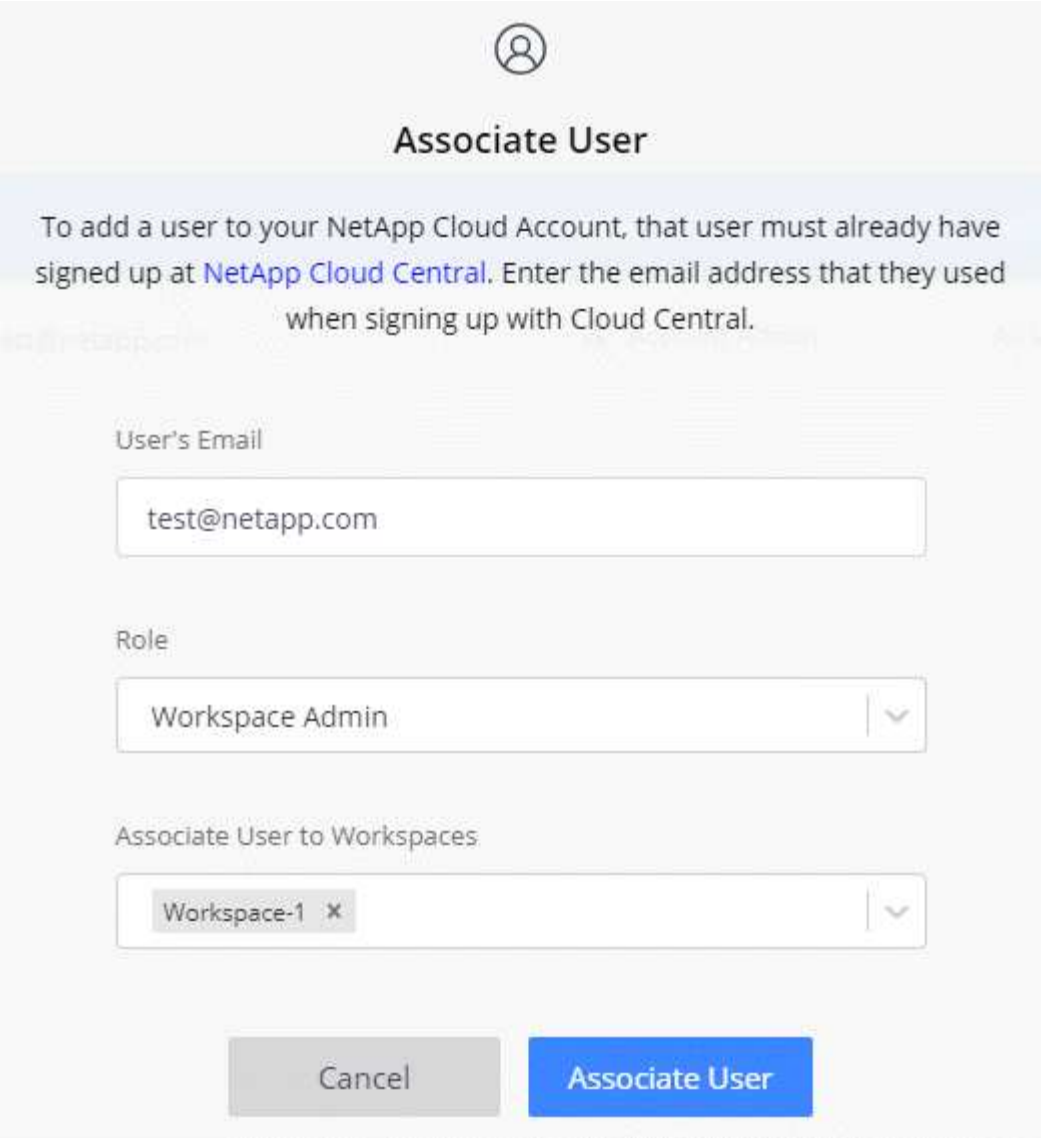
1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "NetApp BlueXP Website" Und melden Sie sich an.
2. Wählen Sie oben in BlueXP das Dropdown-Menü **Account** aus.



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

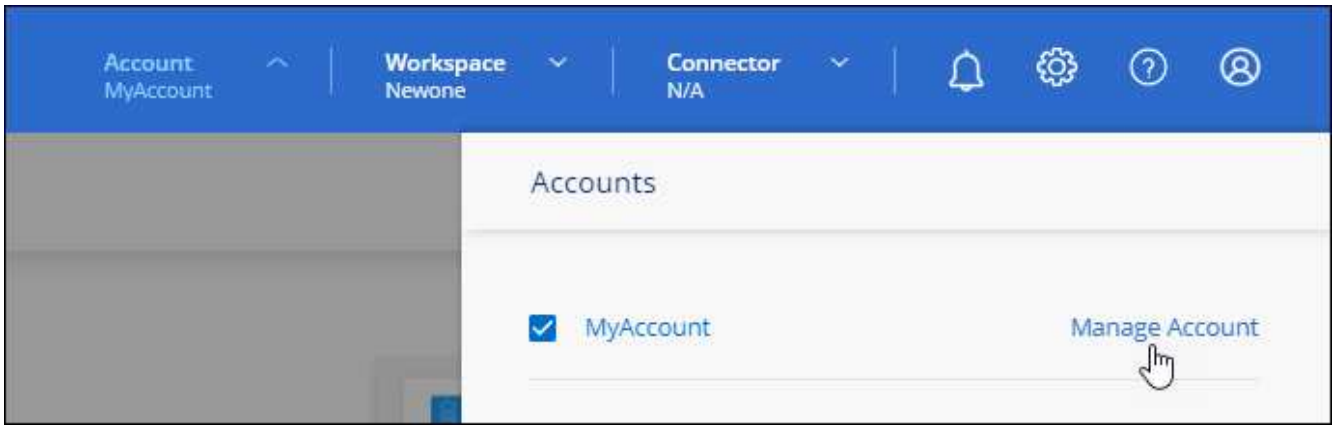
Der Benutzer sollte eine E-Mail von NetApp BlueXP mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die Informationen, die für den Zugriff auf BlueXP erforderlich sind.

Benutzer entfernen

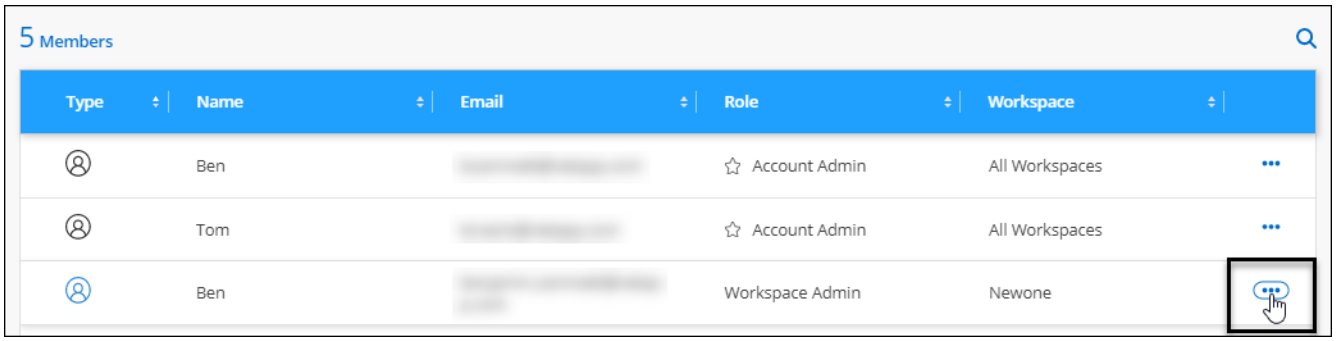
Durch das Auflösen der Zuordnung eines Benutzers wird kein Zugriff mehr auf die Ressourcen in einem BlueXP Konto möglich.

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.

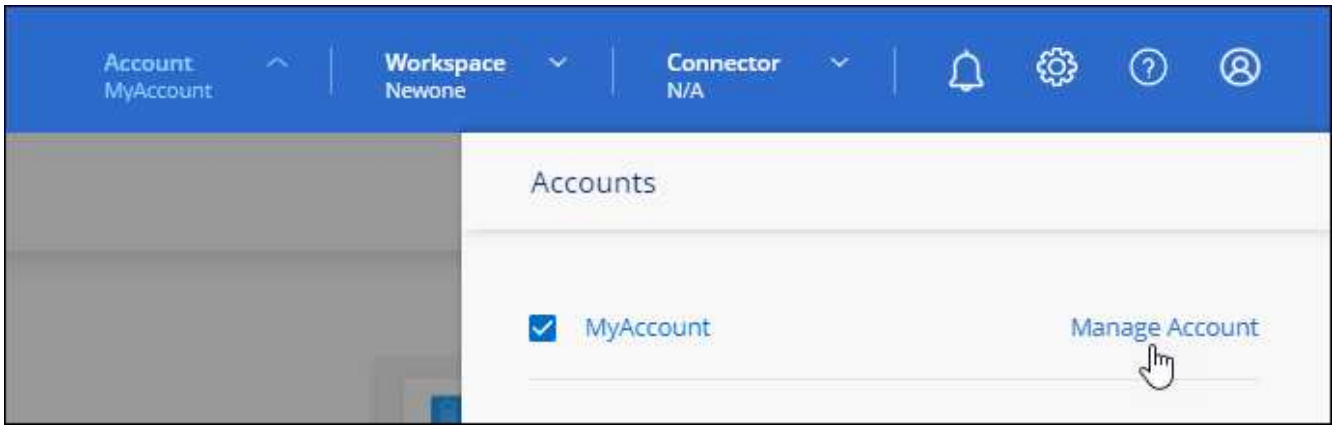
Verwalten der Arbeitsbereiche eines Arbeitsbereichsadministrators

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.

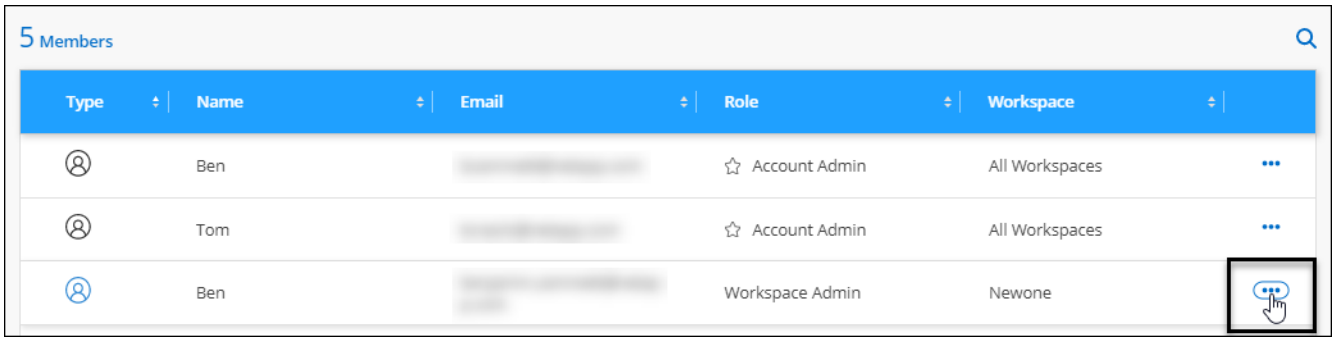
> Sie müssen den Connector auch mit Workspaces verknüpfen, damit Workspace-Administratoren auf die Workspaces von BlueXP zugreifen können. "Erfahren Sie, wie Sie die Arbeitsbereiche eines Connectors verwalten".

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.

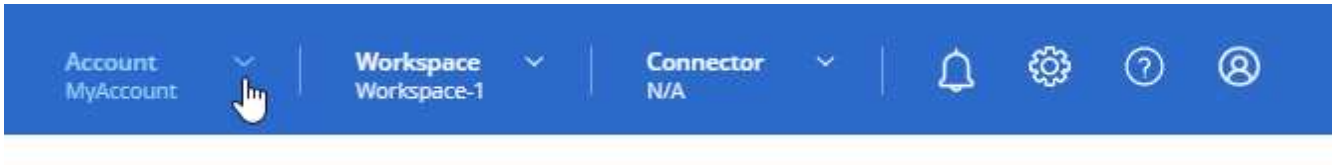
Beachten Sie, dass ein Aktualisierungs-Token für API-Vorgänge nicht erforderlich ist, wenn ein Servicekonto verwendet wird. "Erfahren Sie mehr über das Aktualisieren von Token"

Erstellen eines Dienstkontos

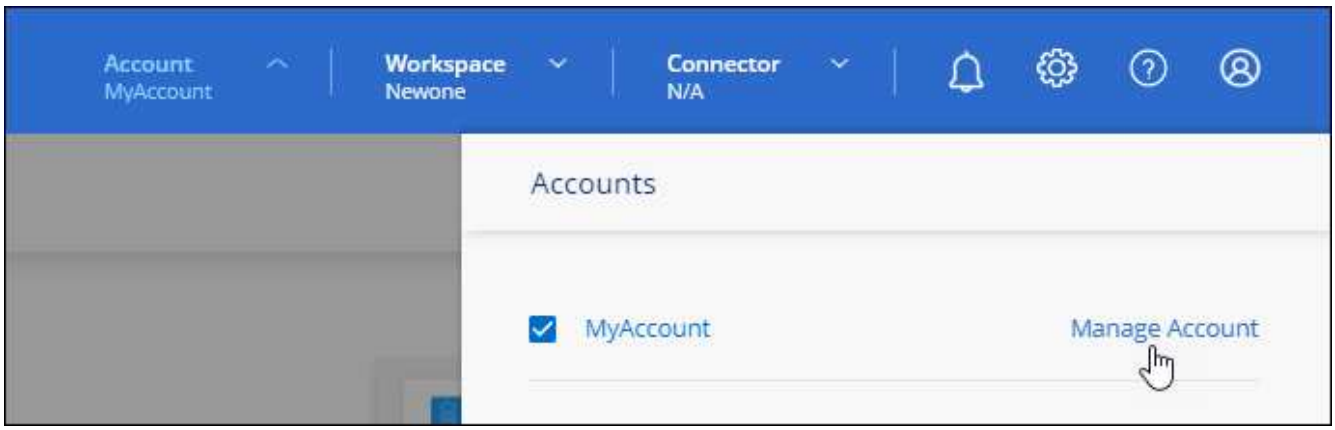
Erstellen Sie so viele Service-Konten wie für das Management der Ressourcen in Ihren Arbeitsumgebungen erforderlich.

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.

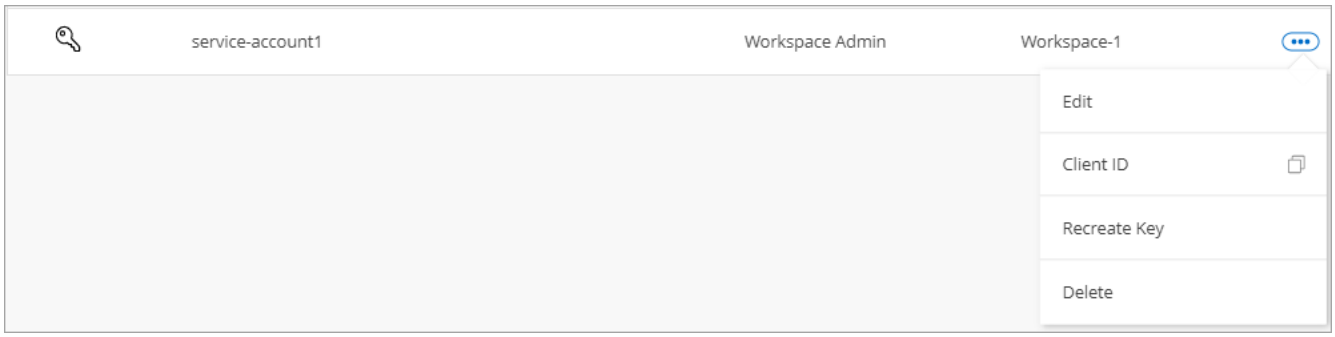
"Erfahren Sie, wie Sie ein Service-Konto-Token erstellen"

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.



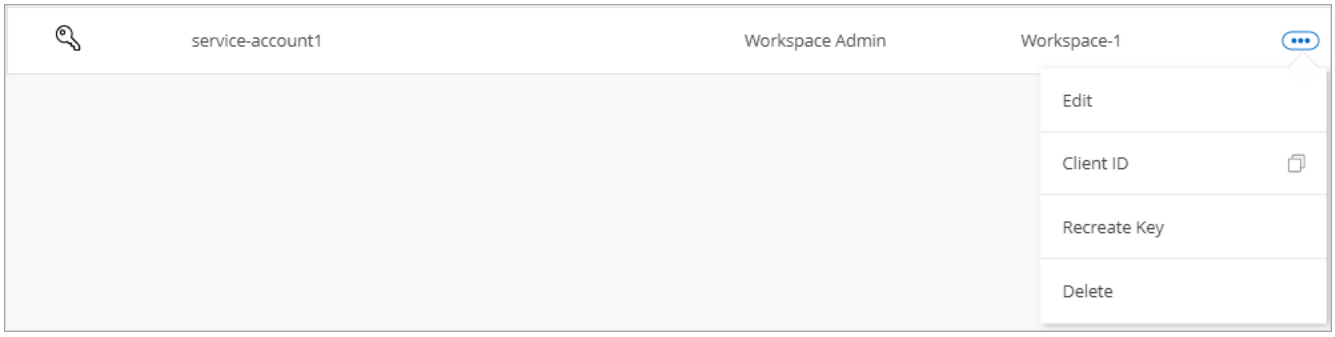
2. Wählen Sie **Client-ID**.
3. Die ID wird in die Zwischenablage kopiert.

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.

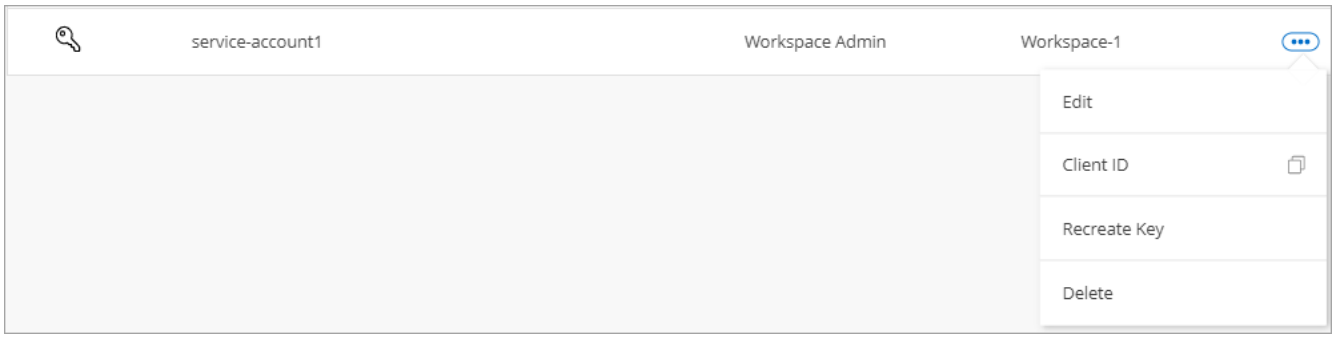
5. Wählen Sie **Schließen**.

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.

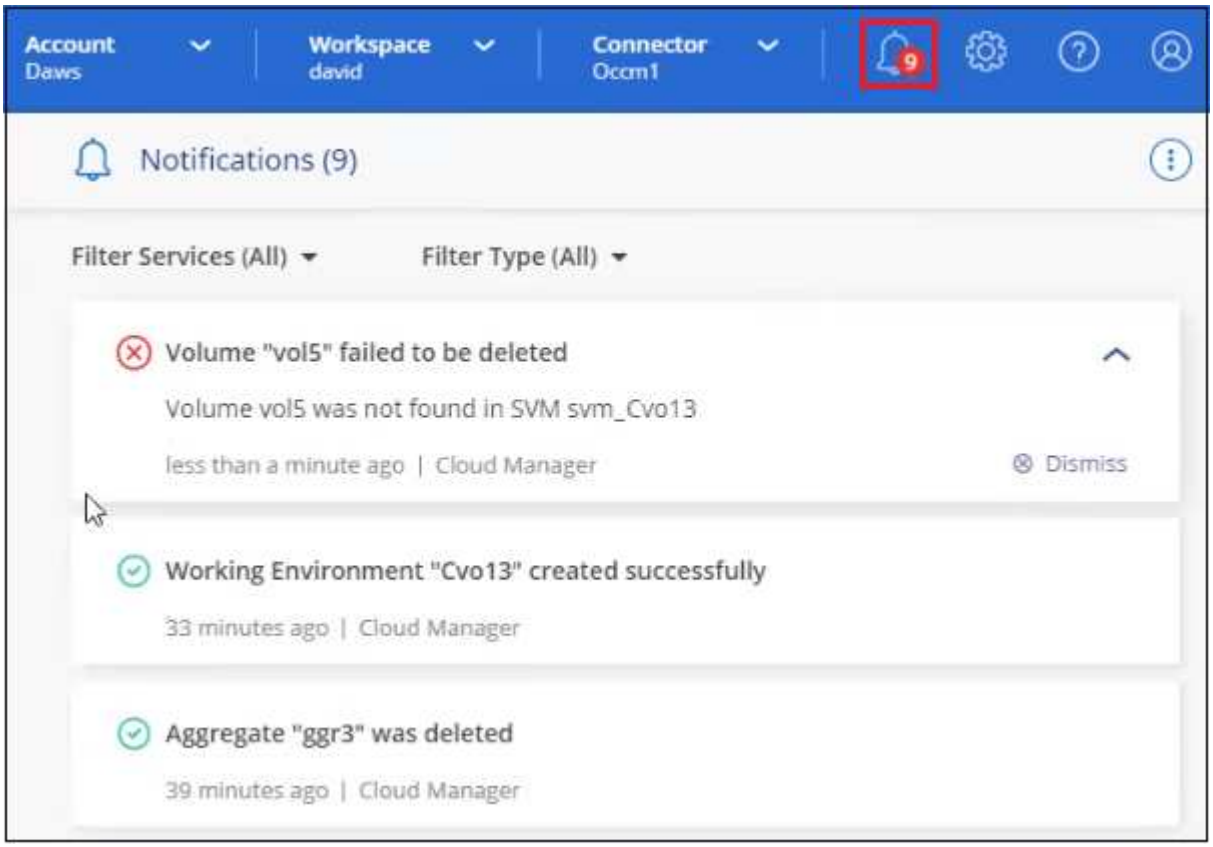
Notification Center	Zeitachse
Zeigt den allgemeinen Status von Ereignissen und Aktionen an	Enthält Details zu jedem Ereignis oder jeder Aktion zur weiteren Untersuchung
Zeigt den Status der aktuellen Anmeldesitzung an (die Informationen werden nach dem Abmelden nicht im Benachrichtigungscenter angezeigt)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

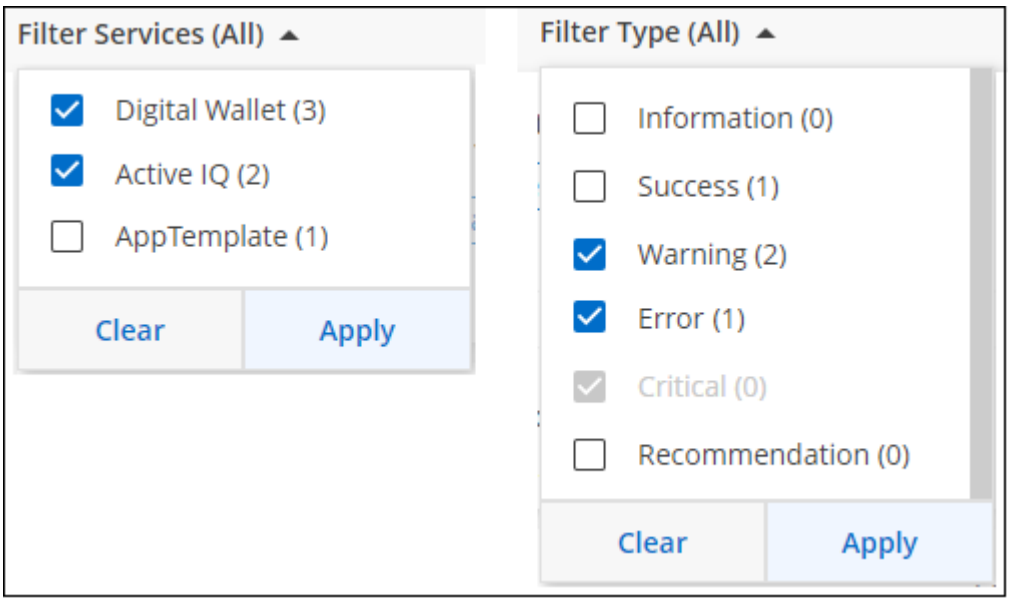
Benachrichtigungstypen

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.

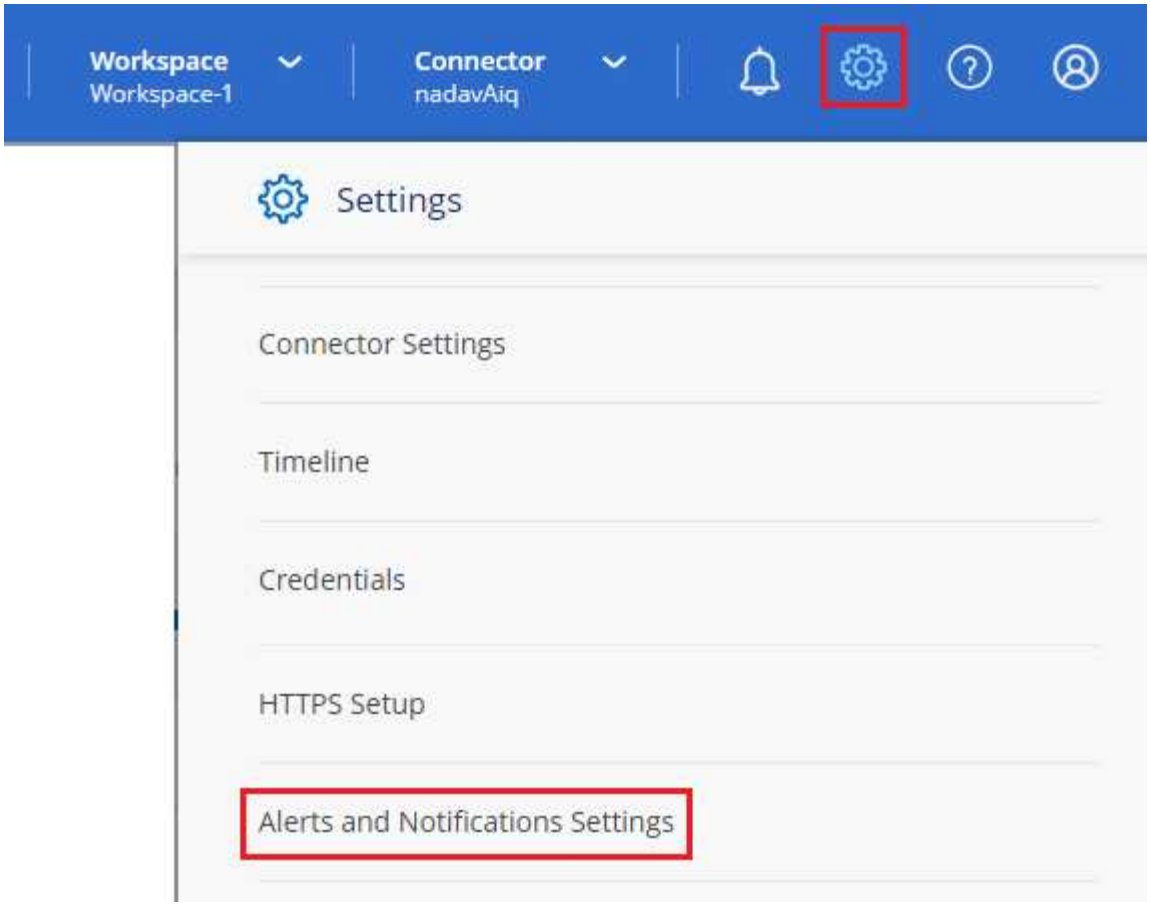
Die Filter, die Sie im Benachrichtigungscenter festlegen, bestimmen nicht, welche Arten von Benachrichtigungen Sie per E-Mail erhalten. Standardmäßig erhalten BlueXP-Kontoadministratoren E-Mails für alle „kritischen“ und „Empfehlungsbenachrichtigungen“. Diese Benachrichtigungen gelten für alle Services. 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.

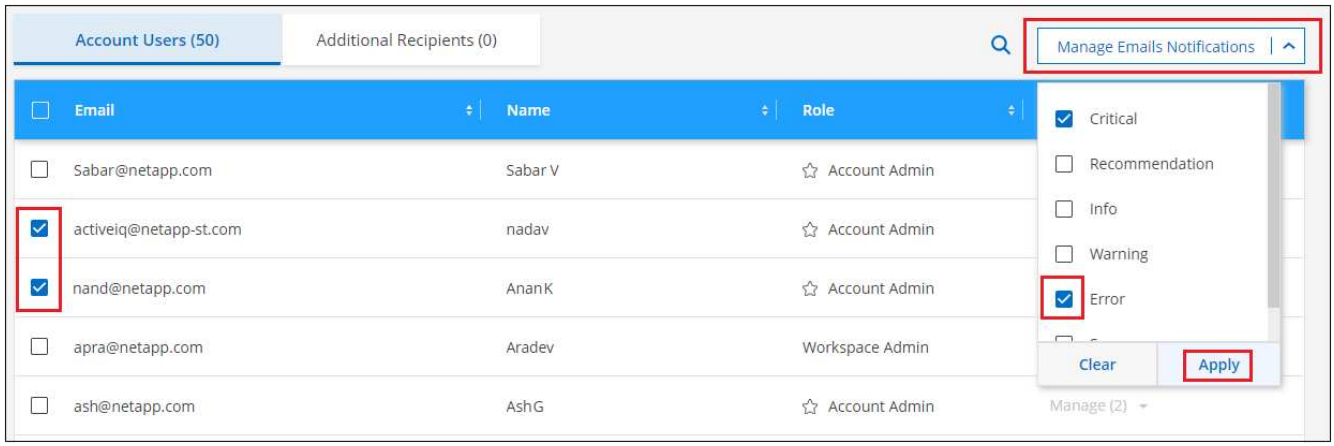
Schritte

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.

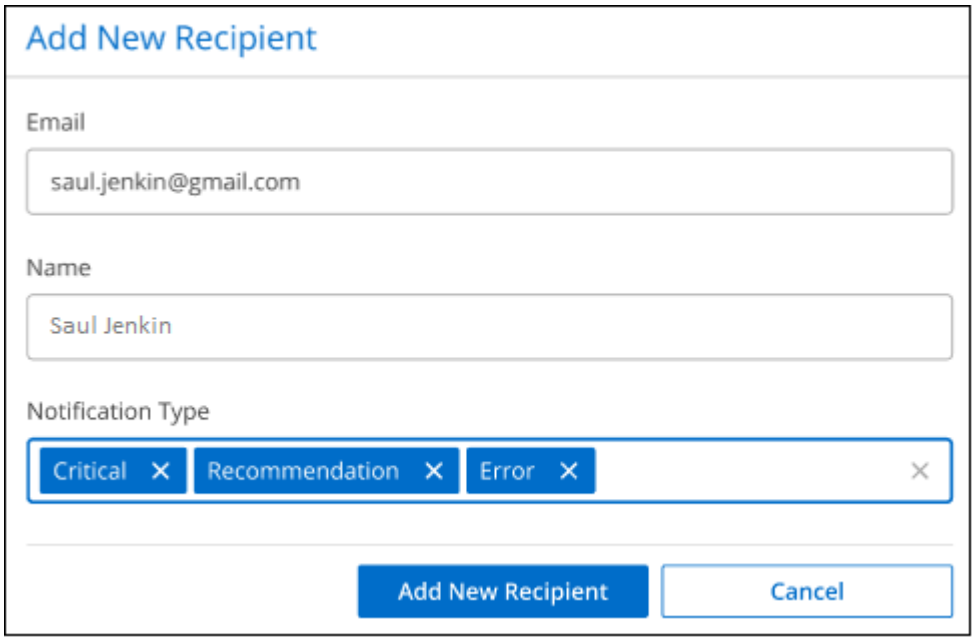


Fügen Sie weitere E-Mail-Empfänger hinzu

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

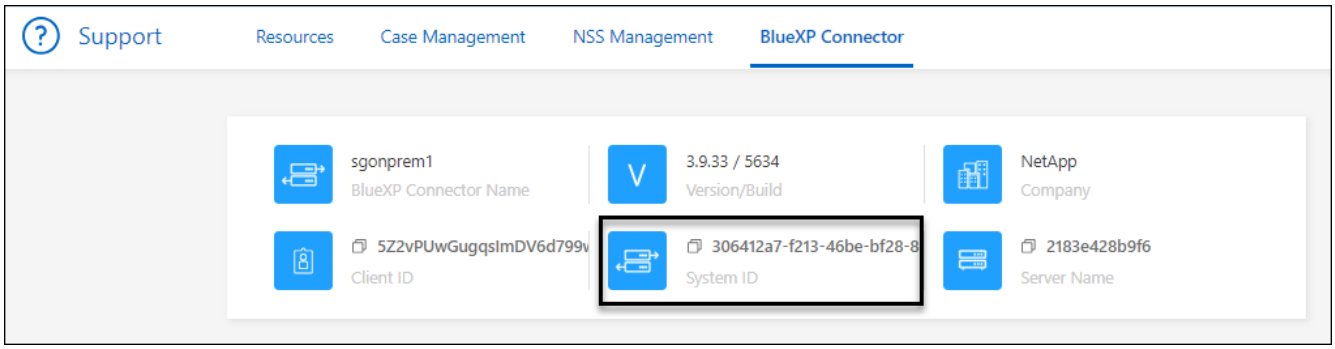
Um Ihnen bei den ersten Schritten zu helfen, fragen Sie möglicherweise Ihr NetApp Ansprechpartner nach der System-ID Ihres Connectors. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

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".

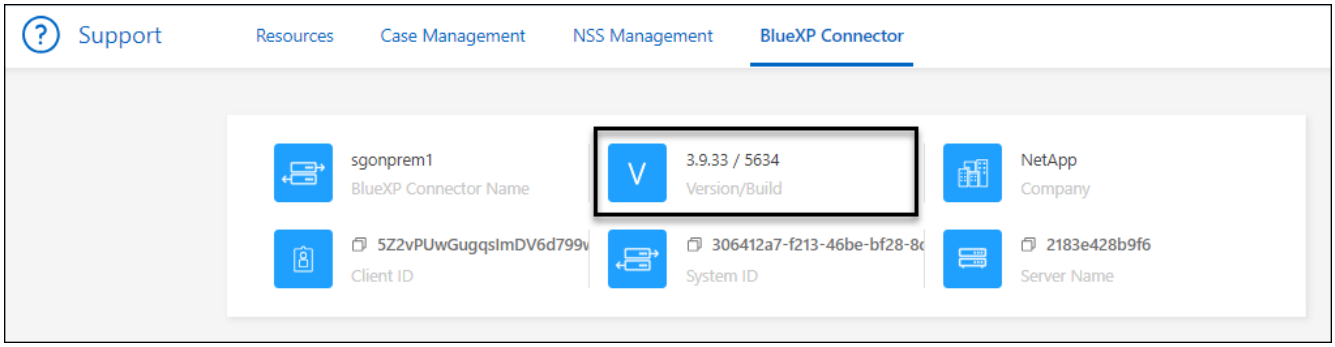
Anzeigen der Version eines Connectors

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.



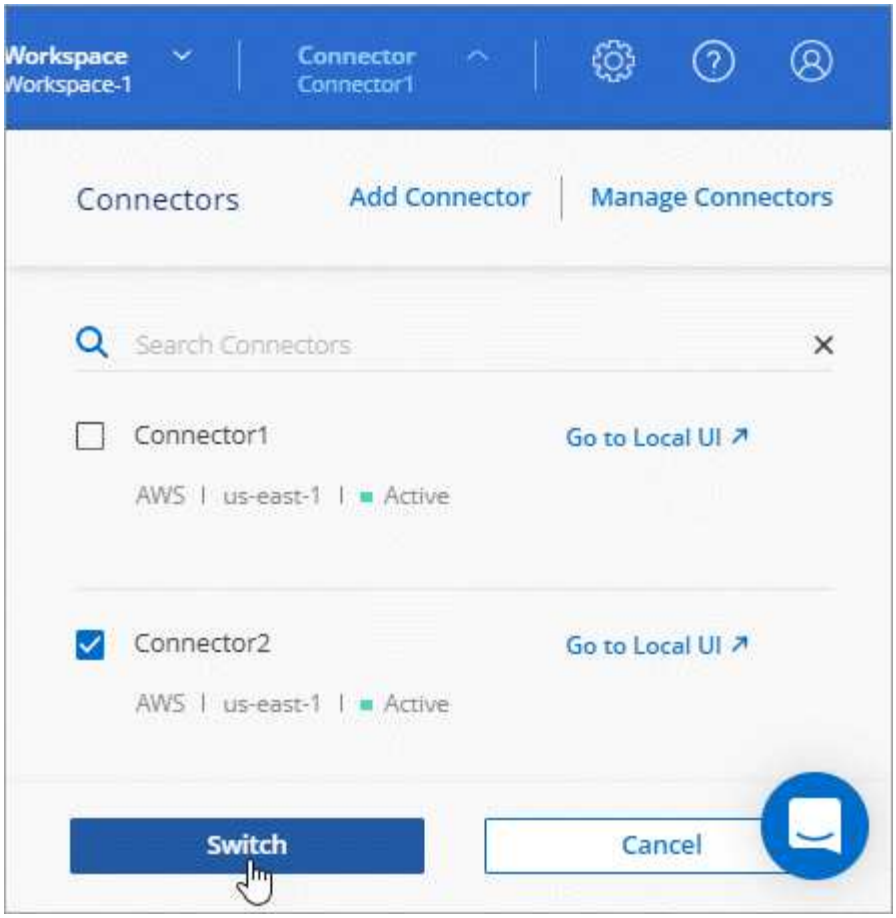
Zwischen den Anschlüssen wechseln

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

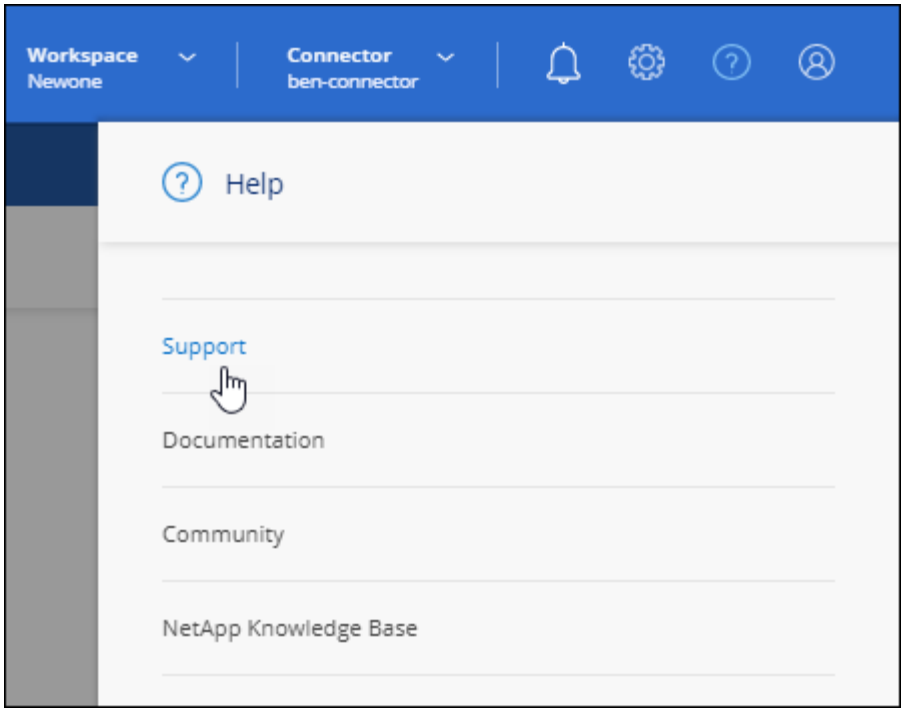
BlueXP aktualisiert und zeigt die Arbeitsumgebungen, die mit dem ausgewählten Connector verknüpft sind.

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

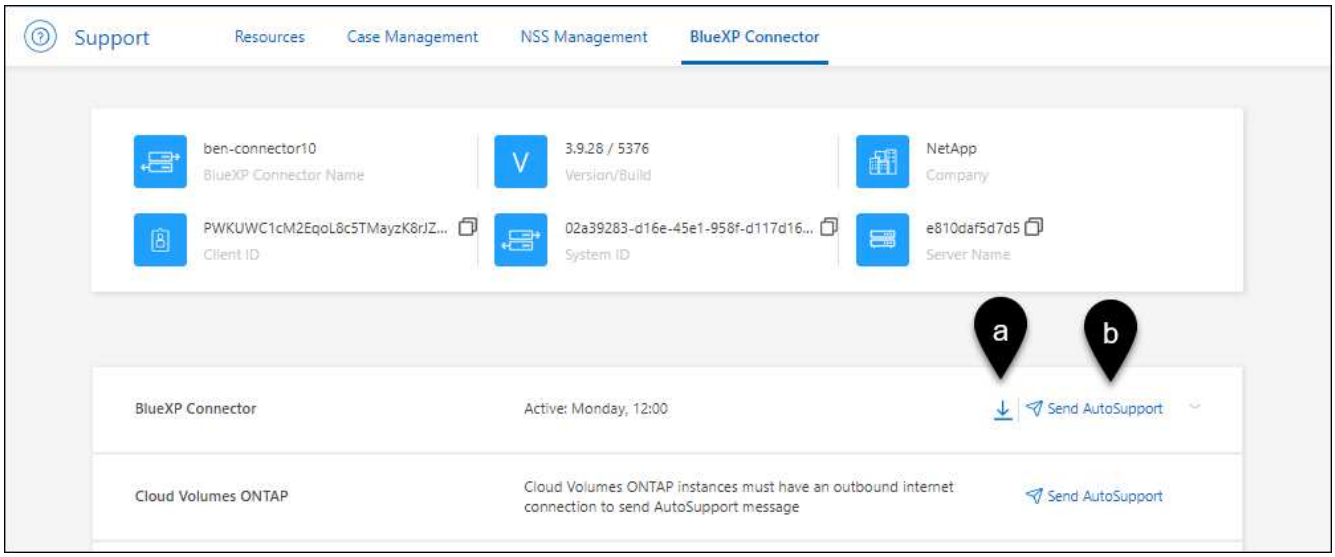
1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



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

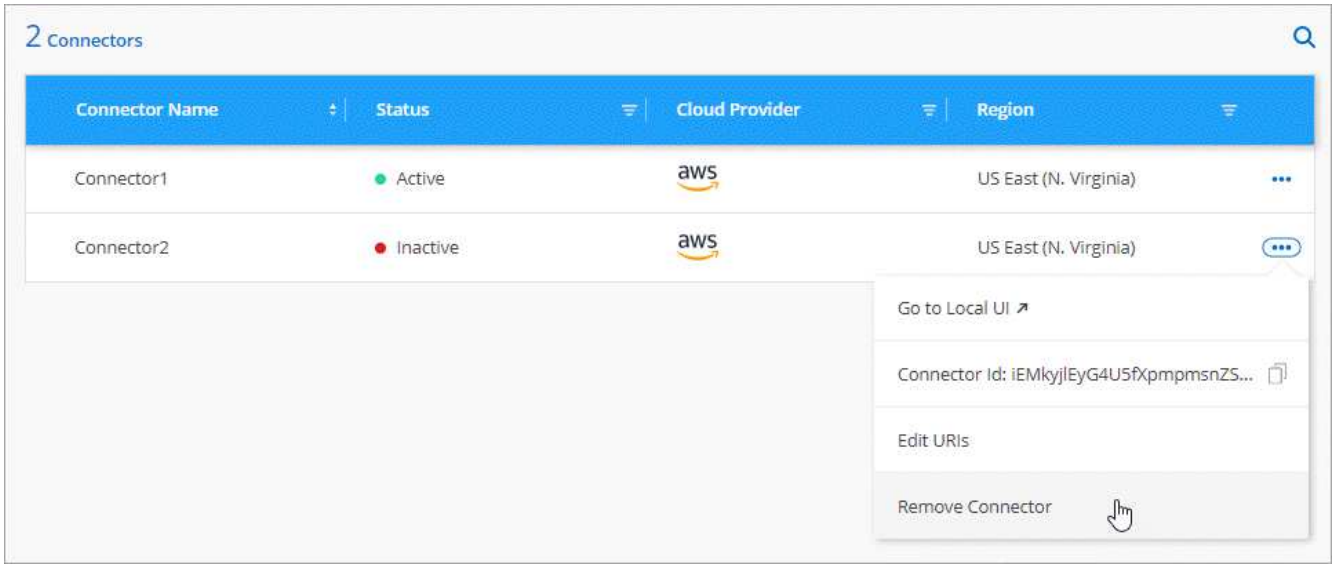
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in BlueXP entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

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.

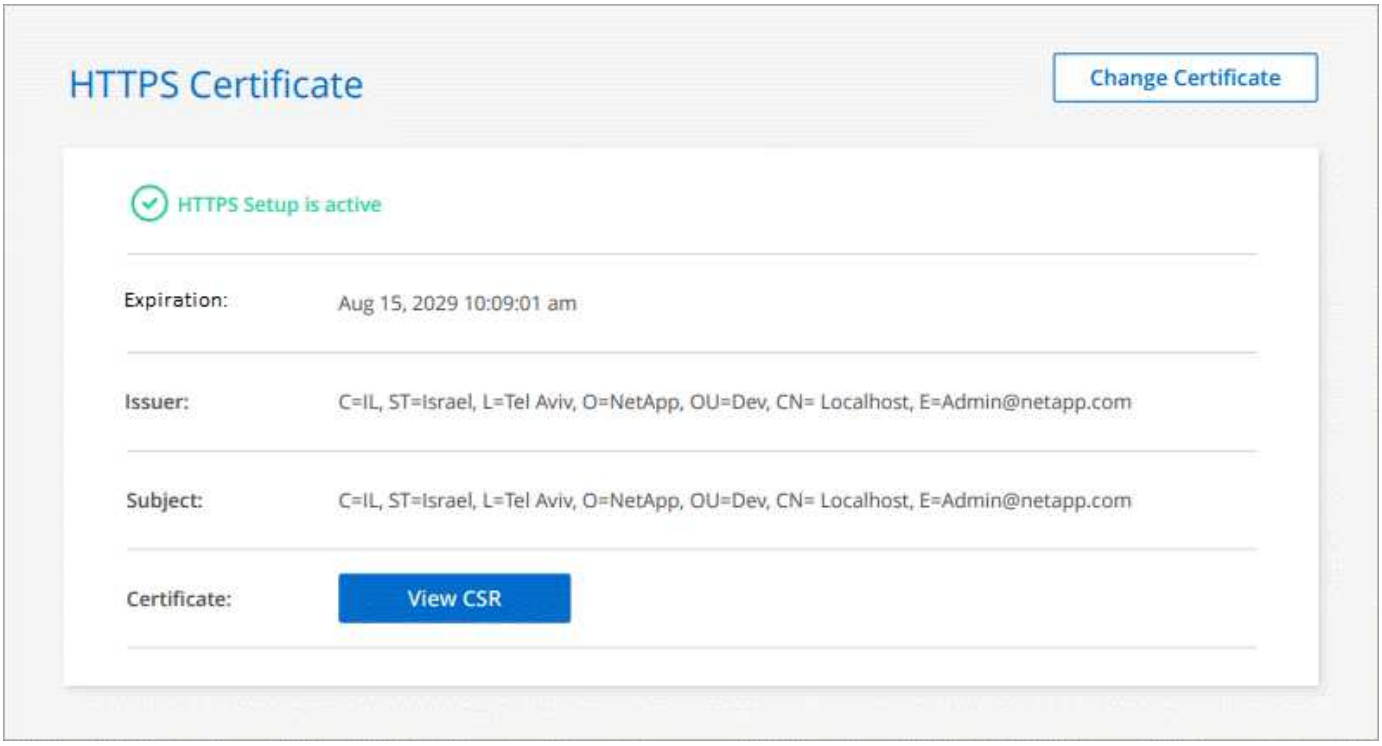
2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung

(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

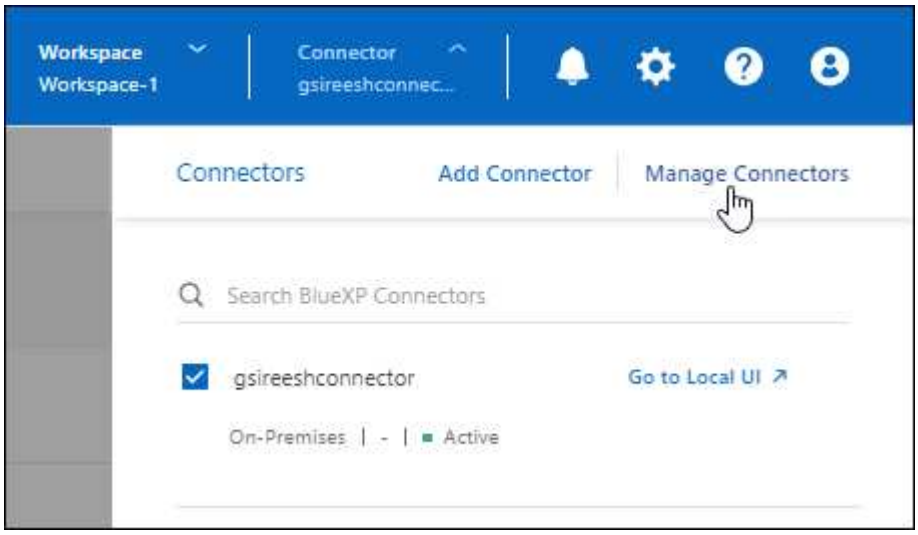
1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**.

   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).

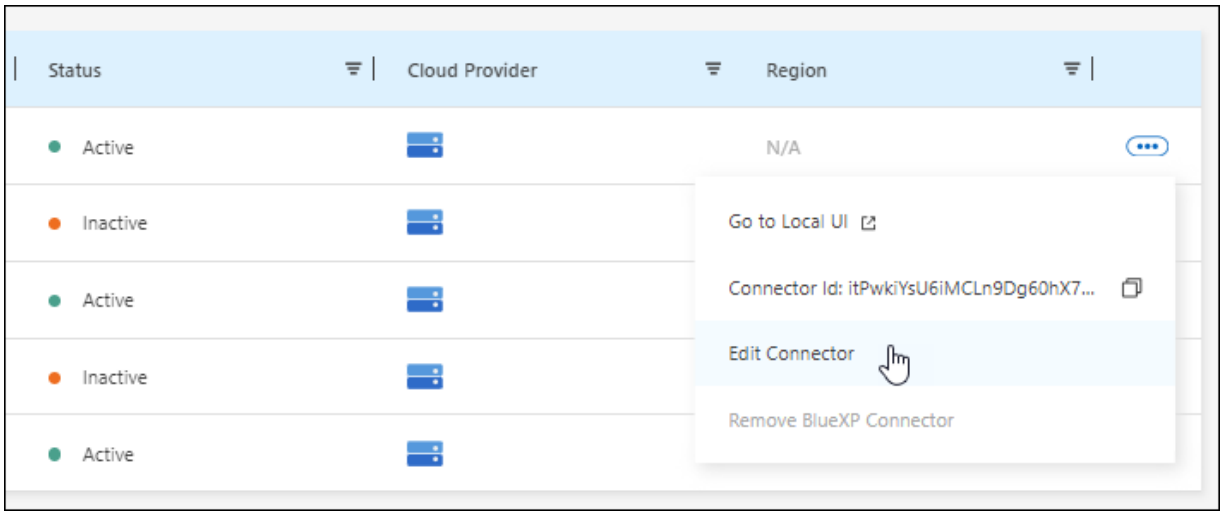
Standardmodus

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

b. Wählen Sie **Connectors Verwalten**.



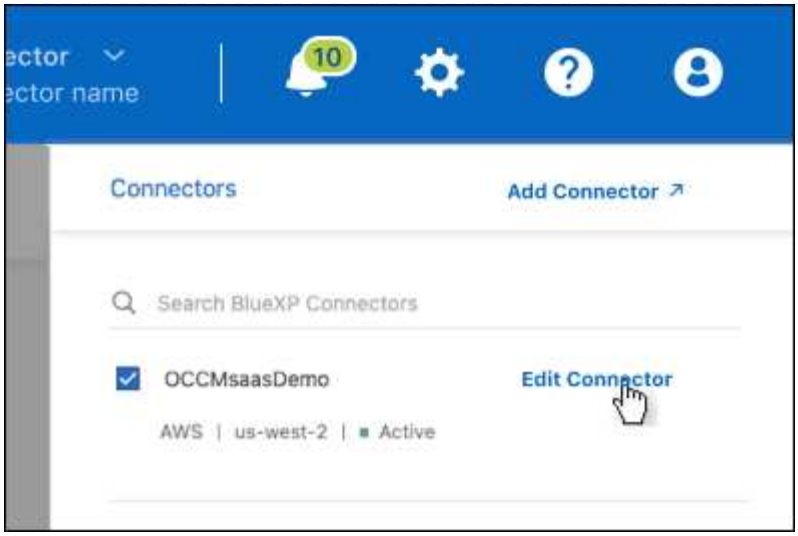
c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.



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

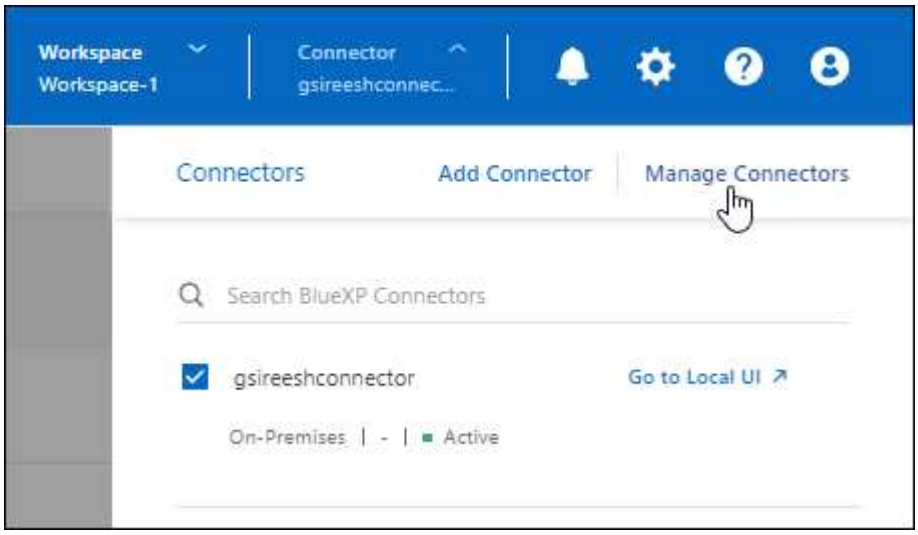
1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**:

   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).

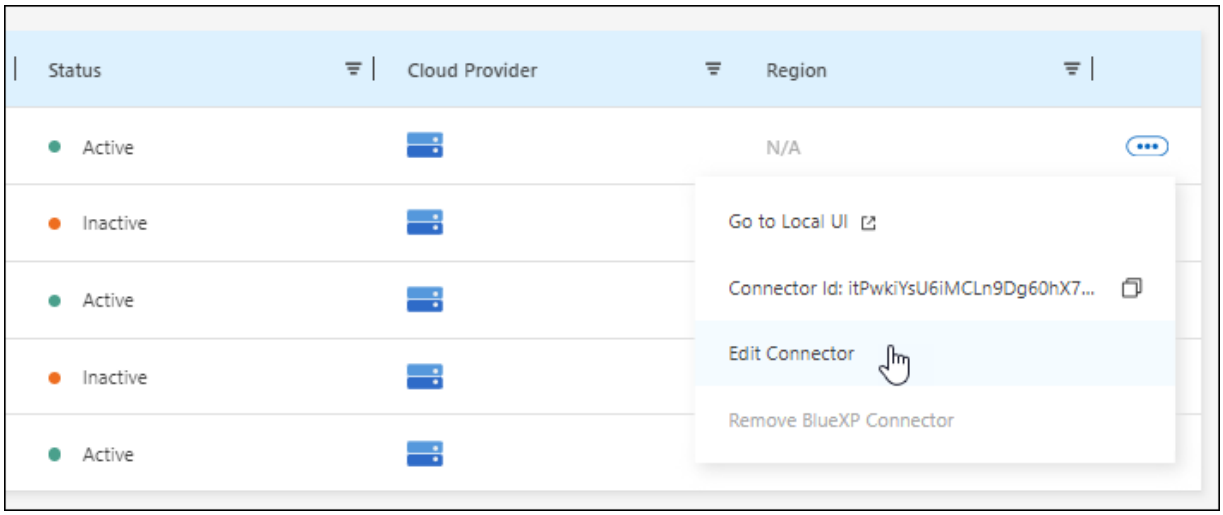
Standardmodus

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

b. Wählen Sie **Connectors Verwalten**.



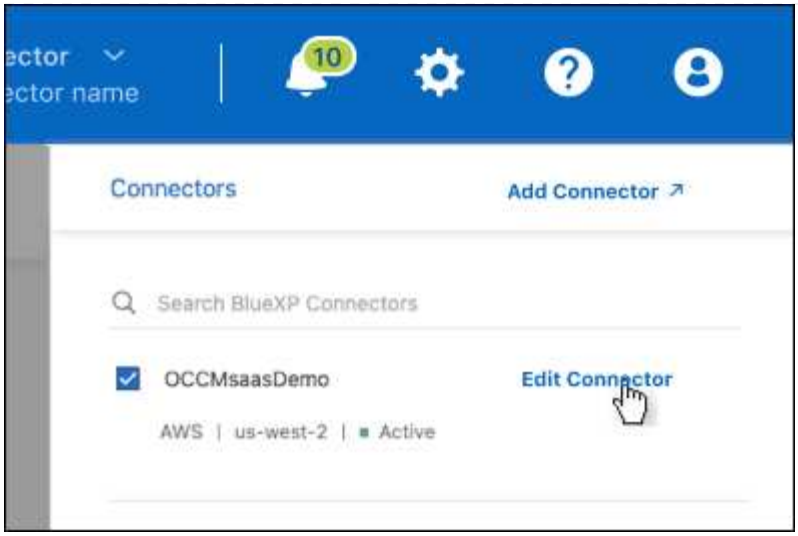
c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.



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

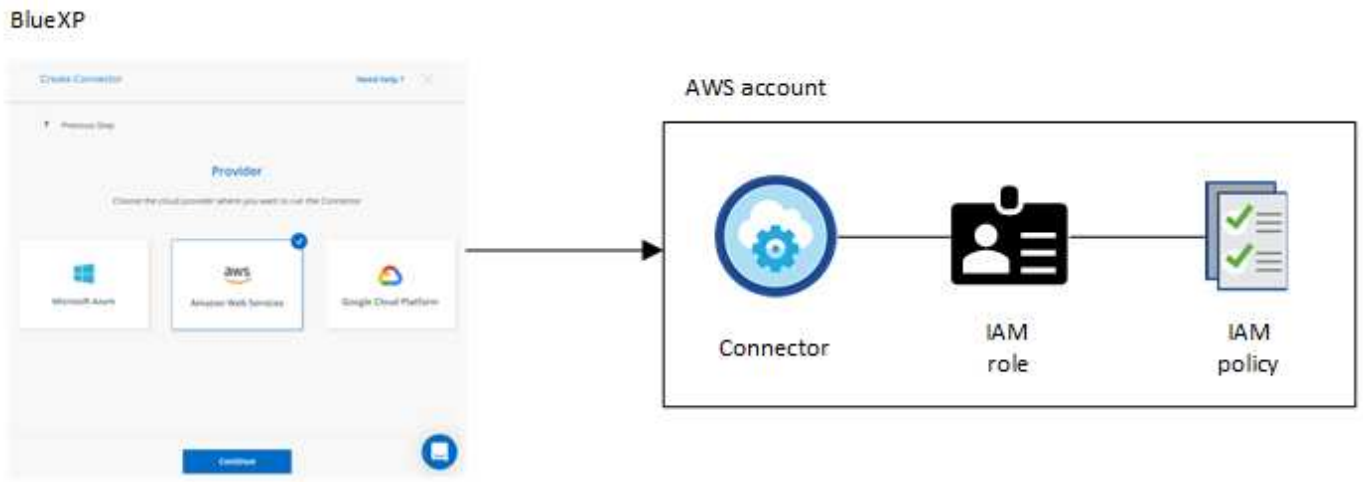
Weitere Informationen zu AWS Zugangsdaten und Berechtigungen

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.

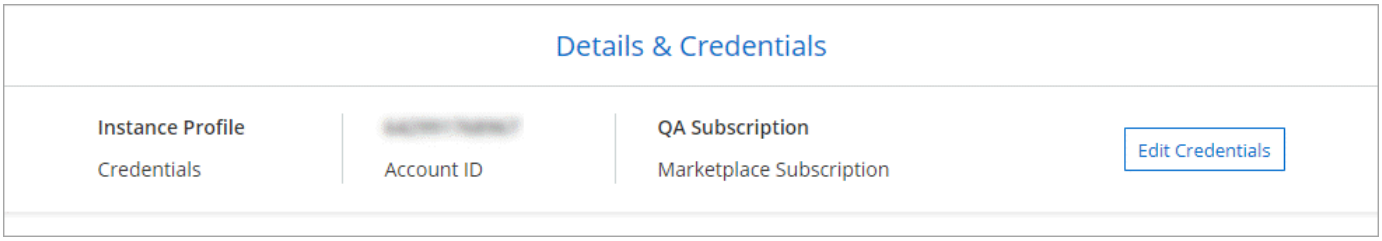
Erste AWS Zugangsdaten

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

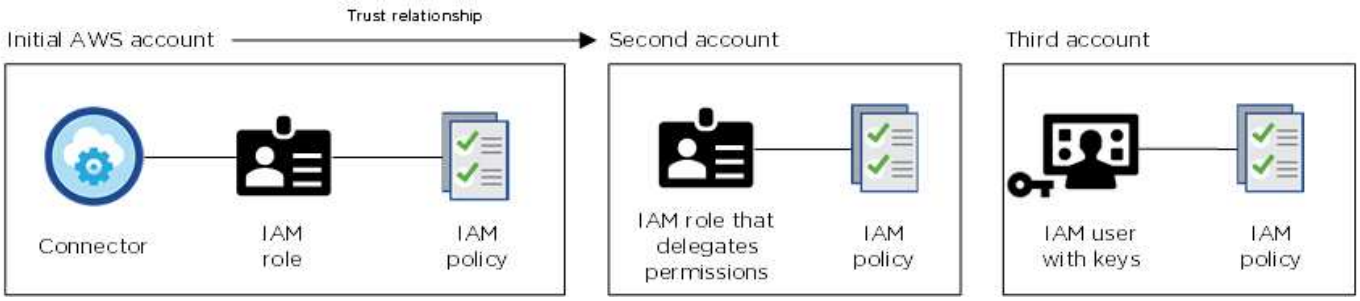
Es gibt zwei Möglichkeiten, zusätzliche AWS-Anmeldedaten hinzuzufügen:

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

Weitere Informationen finden Sie in den folgenden Abschnitten.

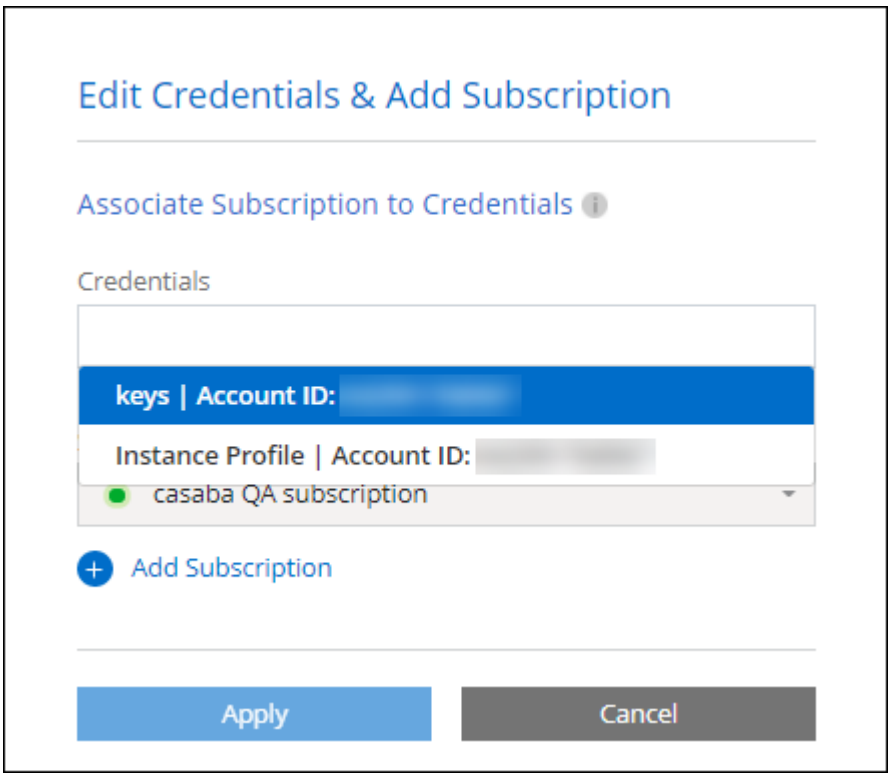
Fügen Sie AWS Zugangsdaten zu einem vorhandenen Connector hinzu

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.

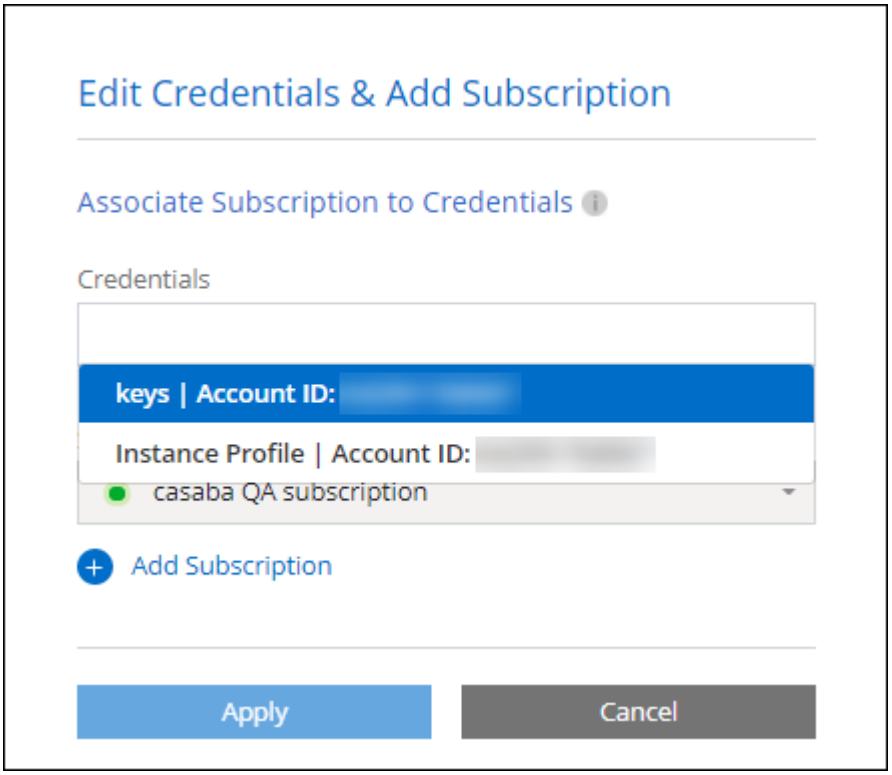
c. **Marketplace-Abonnement**: Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

   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.

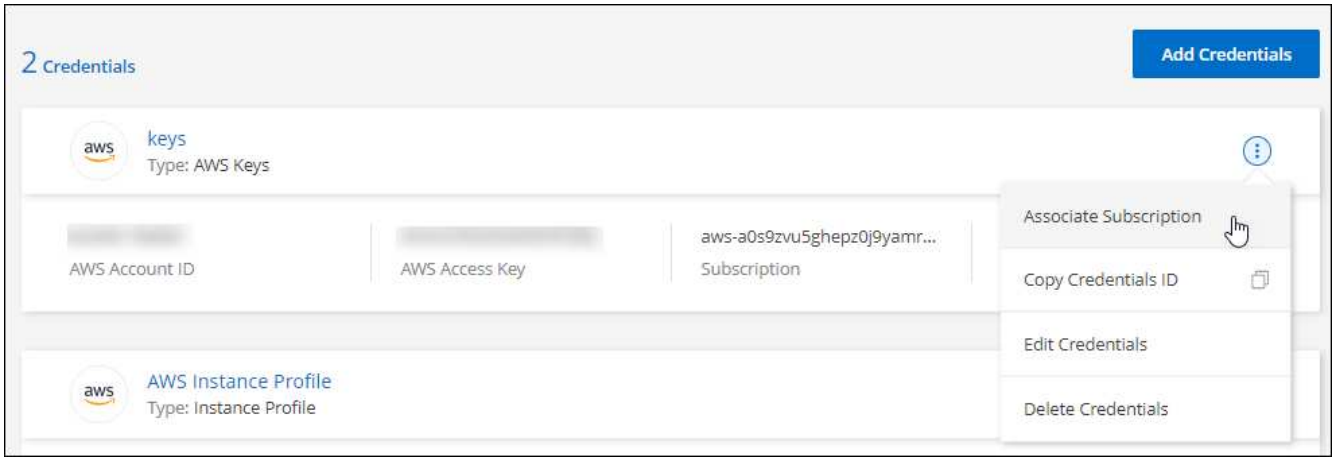
Bevor Sie beginnen

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

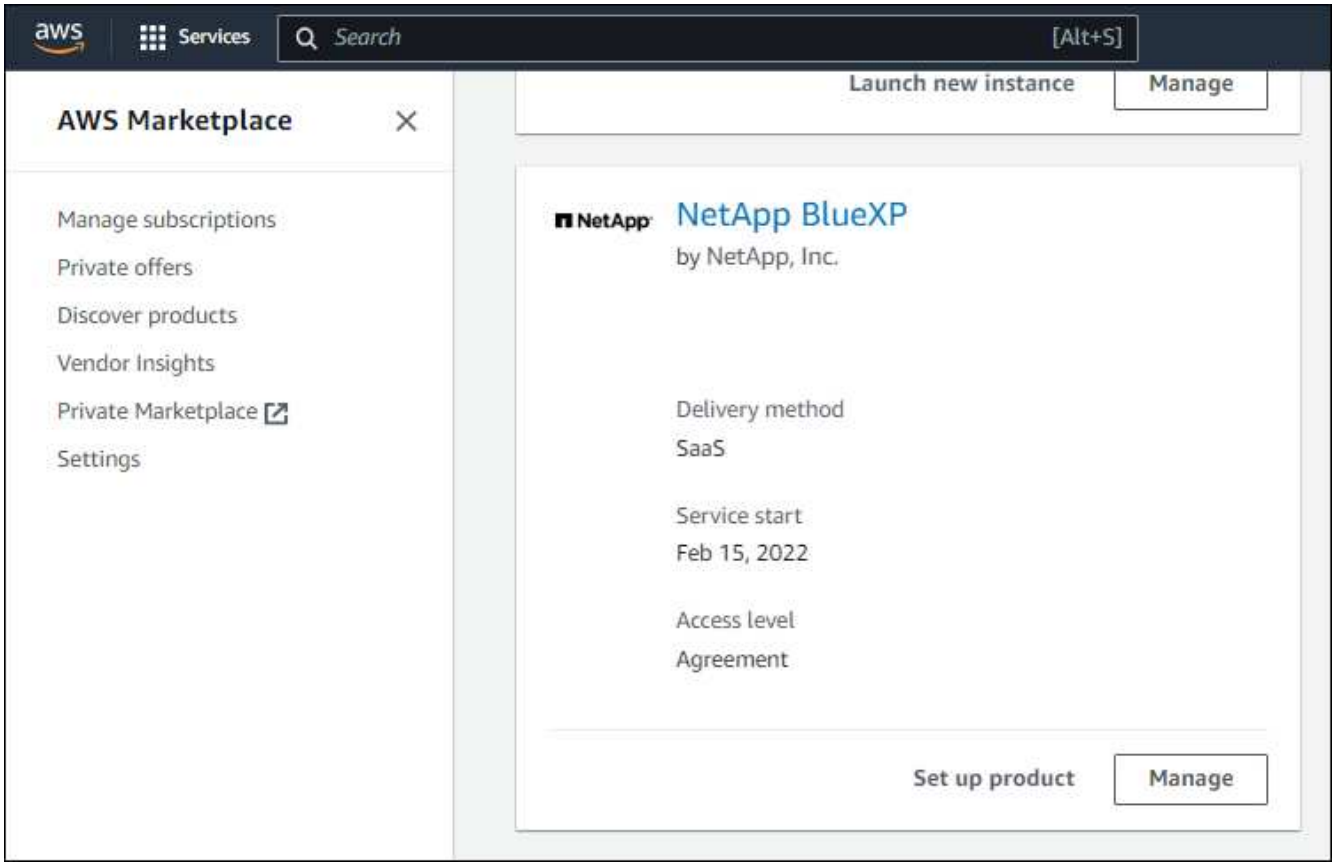
Wenn Sie BlueXP über den AWS Marketplace abonnieren, besteht der letzte Schritt darin, das Abonnement mit Ihren BlueXP Konten auf der BlueXP Website zu verknüpfen. Wenn Sie diesen Schritt nicht abgeschlossen haben, können Sie das Abonnement nicht mit Ihrem BlueXP Konto verwenden.

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.

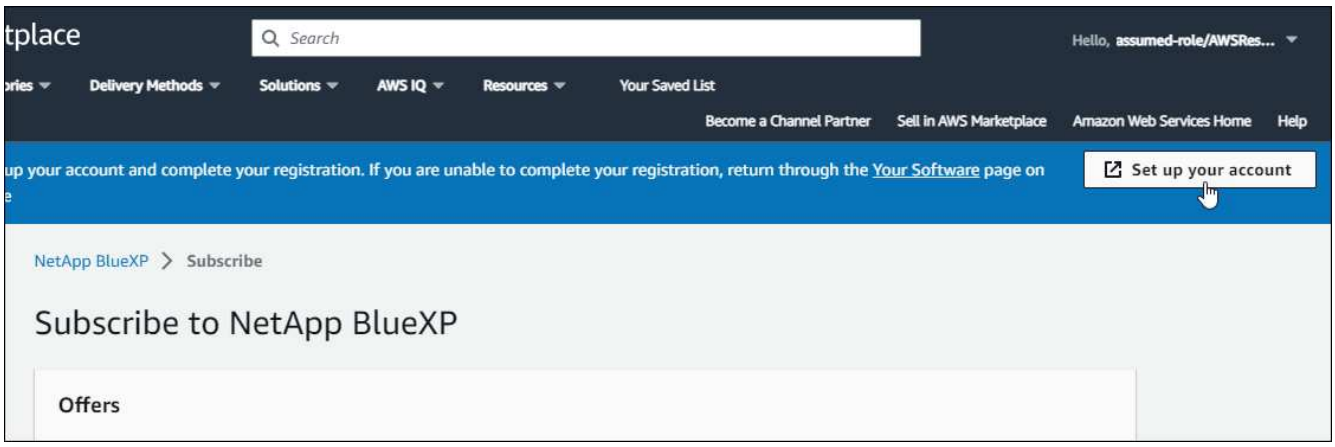
      Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen. Wenn Ihr Abonnement nicht angezeigt wird, fahren Sie mit den folgenden Schritten fort.
2. Melden Sie sich an der AWS-Konsole an, und navigieren Sie zu **AWS Marketplace Subscriptions**.
3. Zum NetApp BlueXP Abonnement



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.

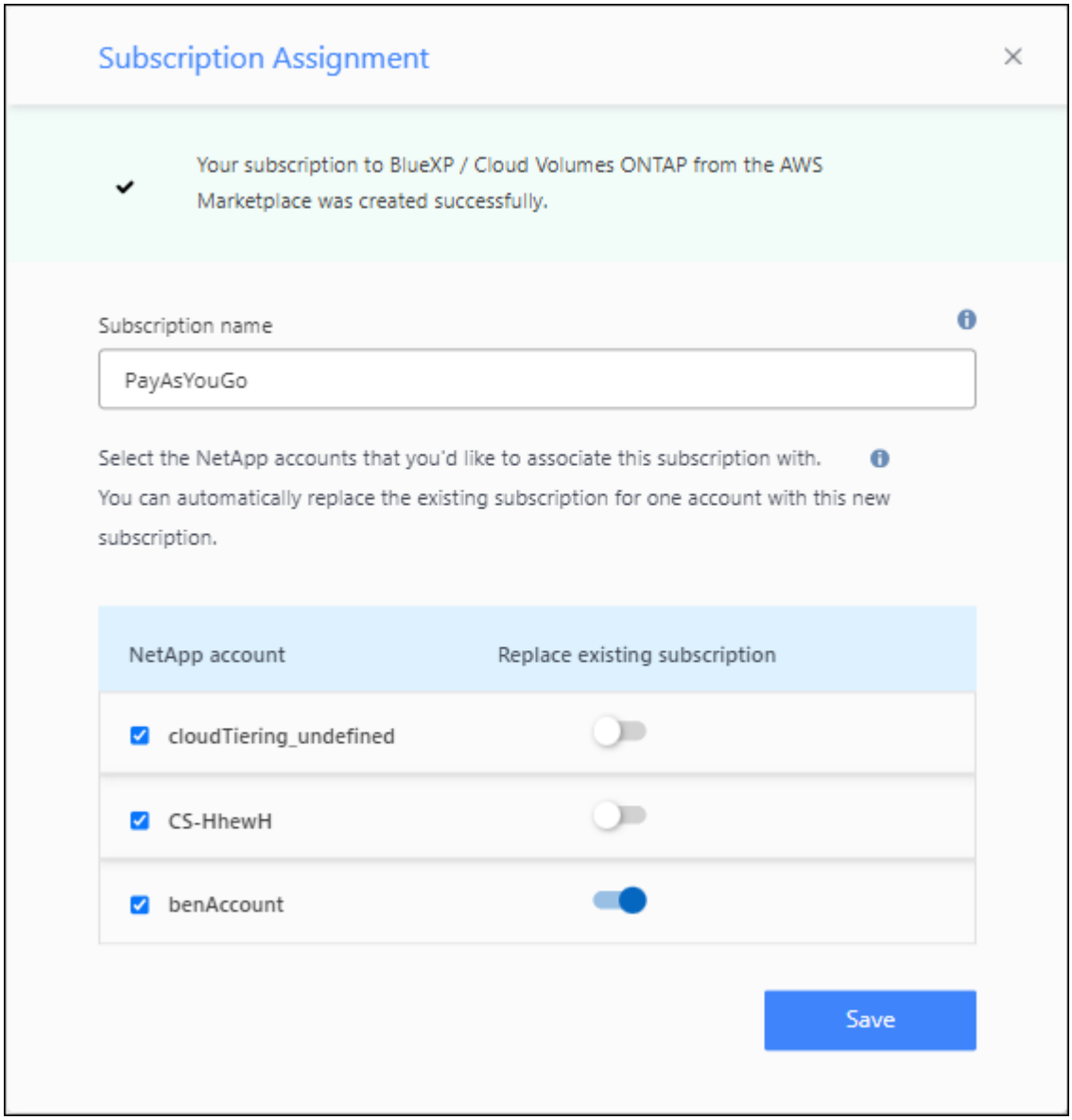
6. Auf der Seite **Subscription Assignment**:

   - 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.

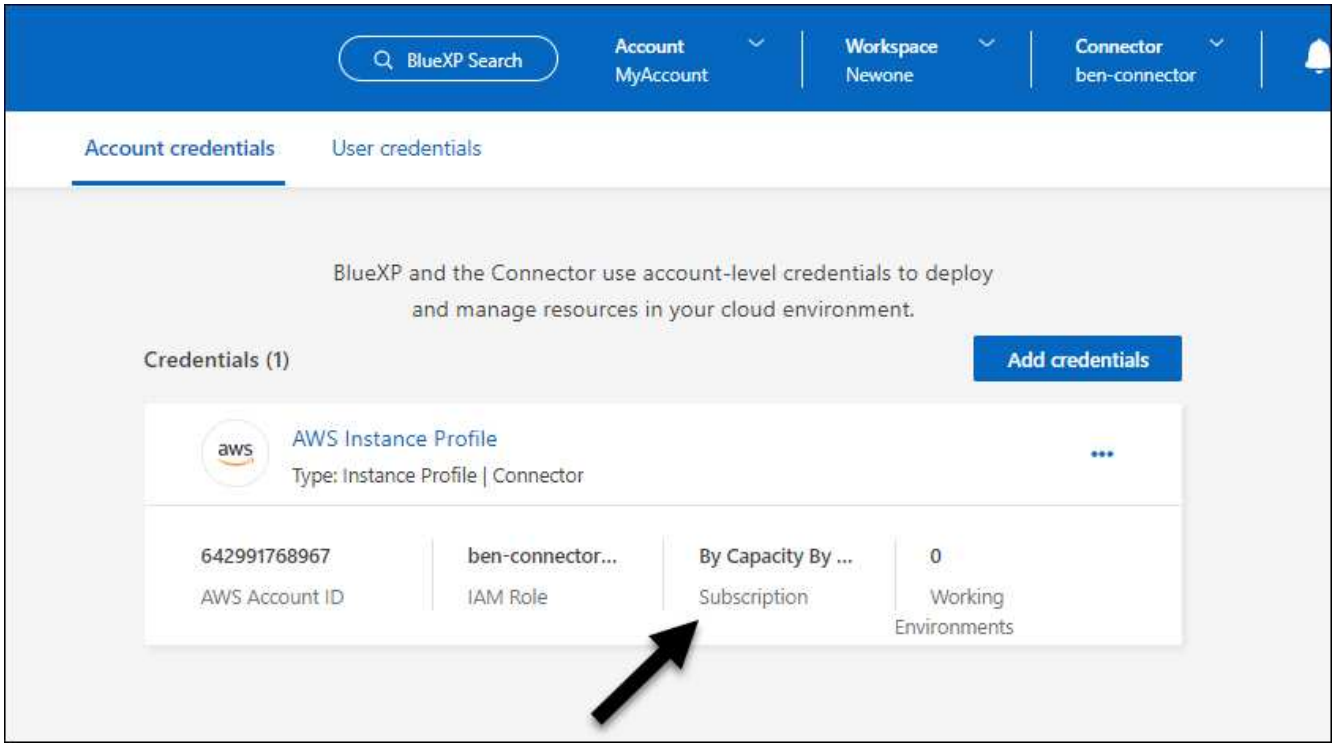


7. Über das Digital Wallet von BlueXP können Sie sich bestätigen, dass das Abonnement mit Ihrem BlueXP Konto verknüpft ist.
   a. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
   b. Wählen Sie **Abonnements**.
   c. Vergewissern Sie sich, dass Ihr BlueXP Abonnement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

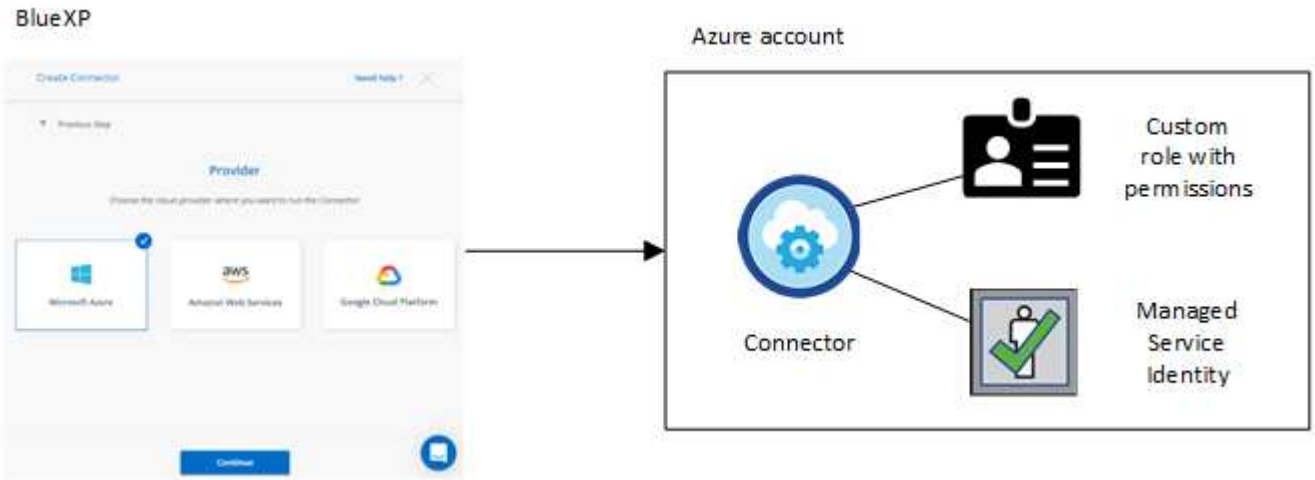
Informationen zu Azure Zugangsdaten und Berechtigungen

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.

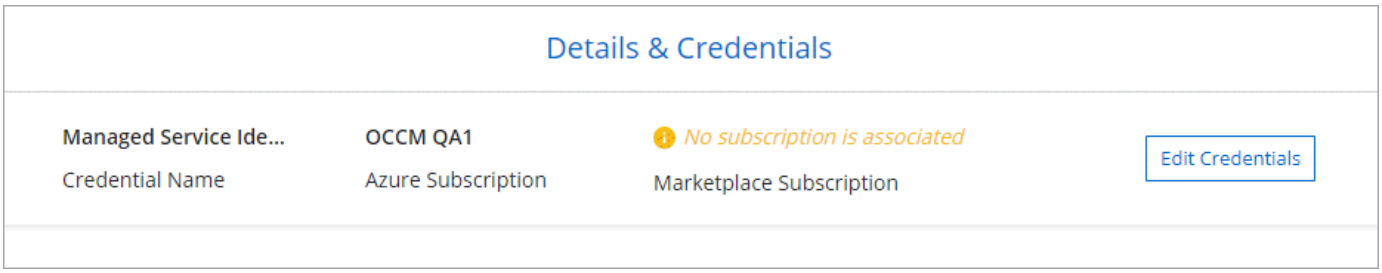
Erste Azure Zugangsdaten

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:



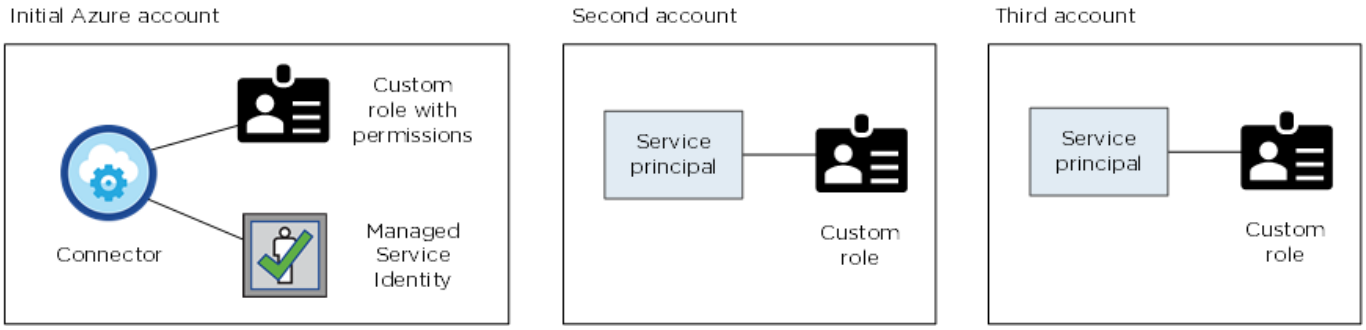
Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

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".

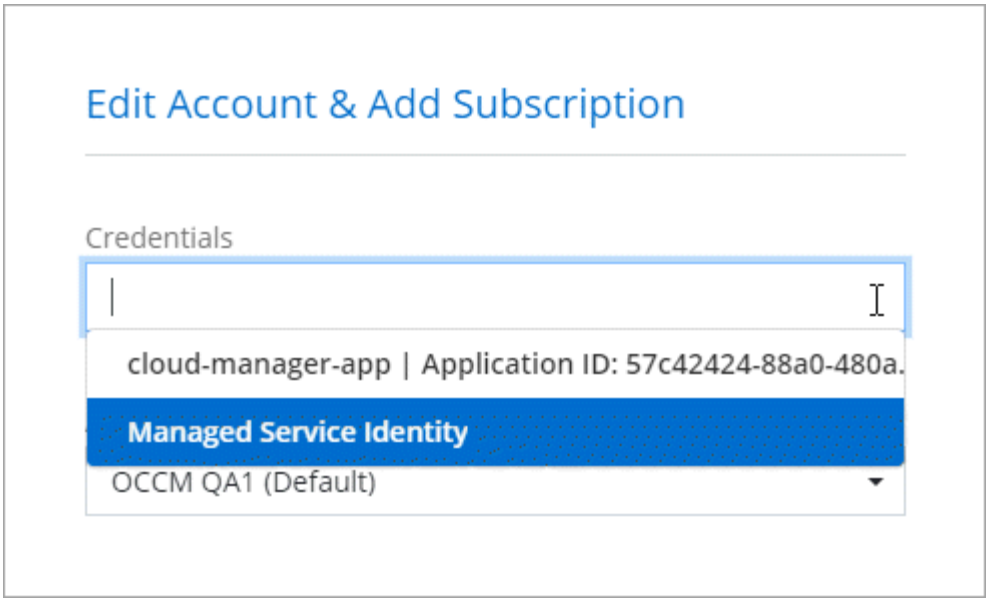
Zusätzliche Azure Zugangsdaten

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

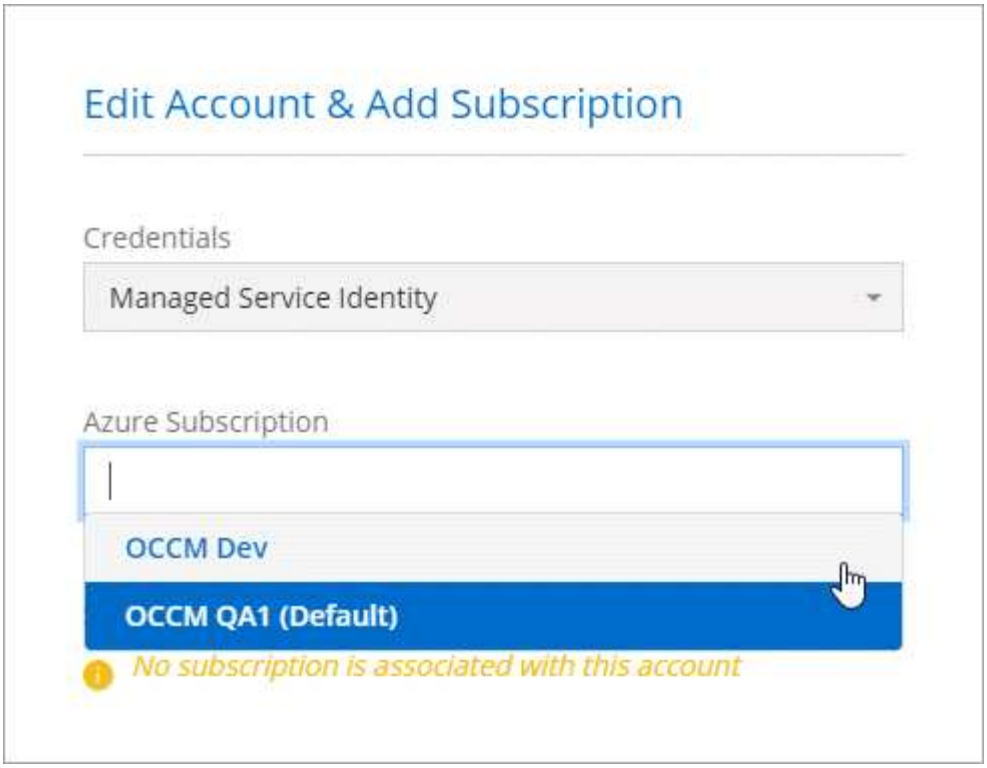
1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Wählen Sie **Access Control (IAM)**.
   a. Wählen Sie **Hinzufügen** > **Rollenzuweisung hinzufügen** und fügen Sie dann die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

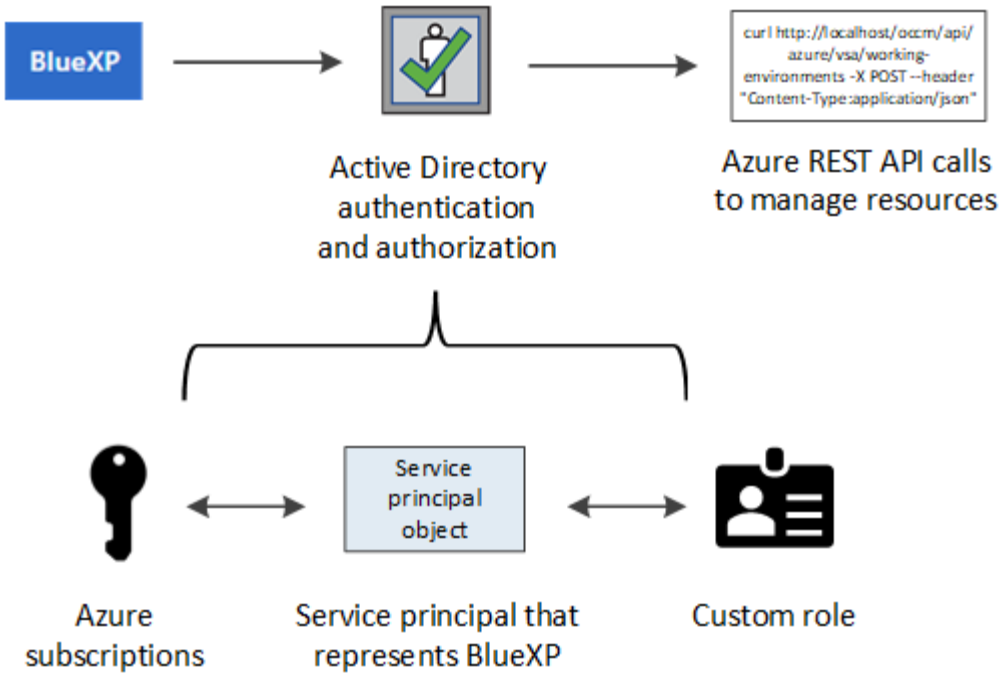
Wenn Sie Cloud Volumes ONTAP mit *different* Azure-Anmeldeinformationen bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure-Konto einen Dienstprinzipal in der Microsoft Entra-ID erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen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

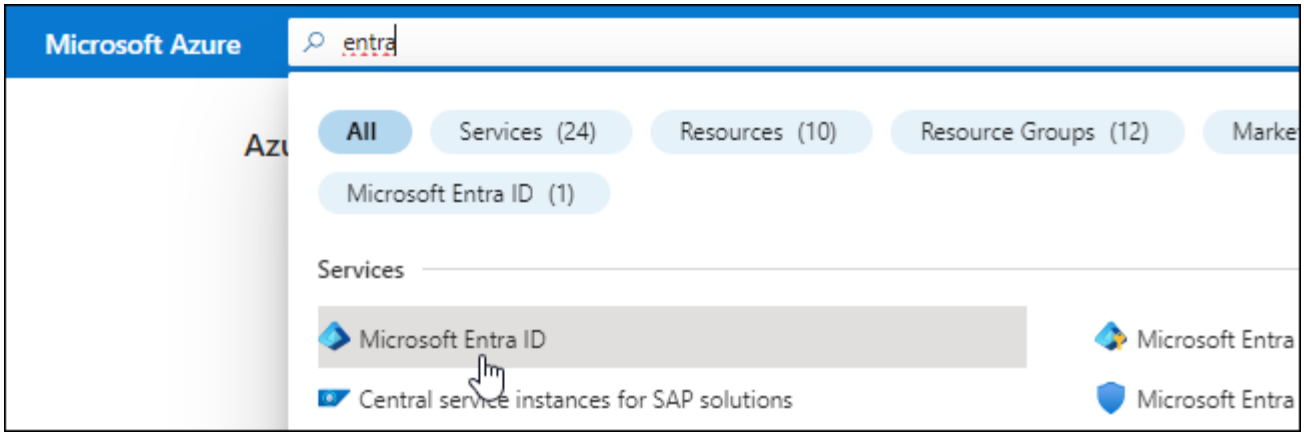
Erstellen Sie ein Microsoft Entra-Applikations- und Serviceprinzip, das BlueXP für die rollenbasierte Zugriffssteuerung verwenden kann.

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.

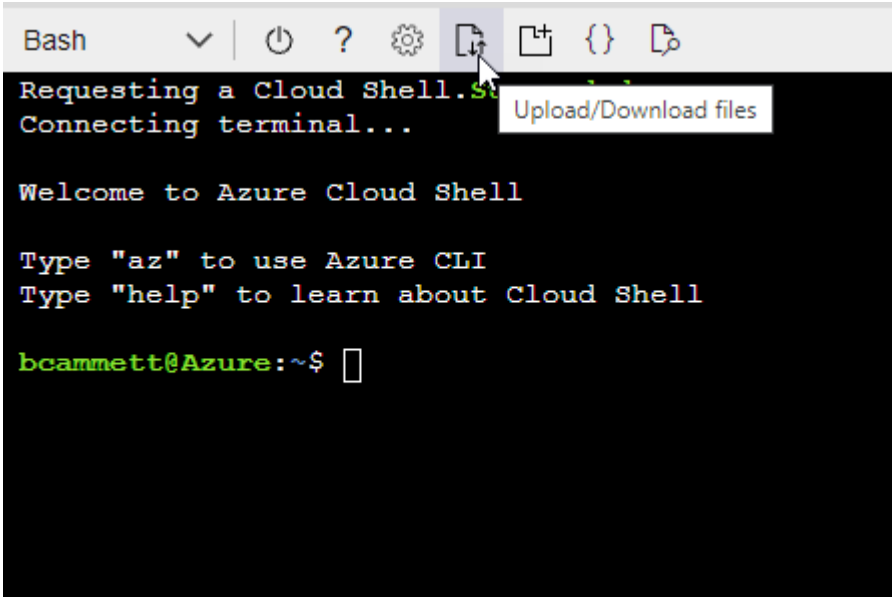
      Beispiel

```
"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
```

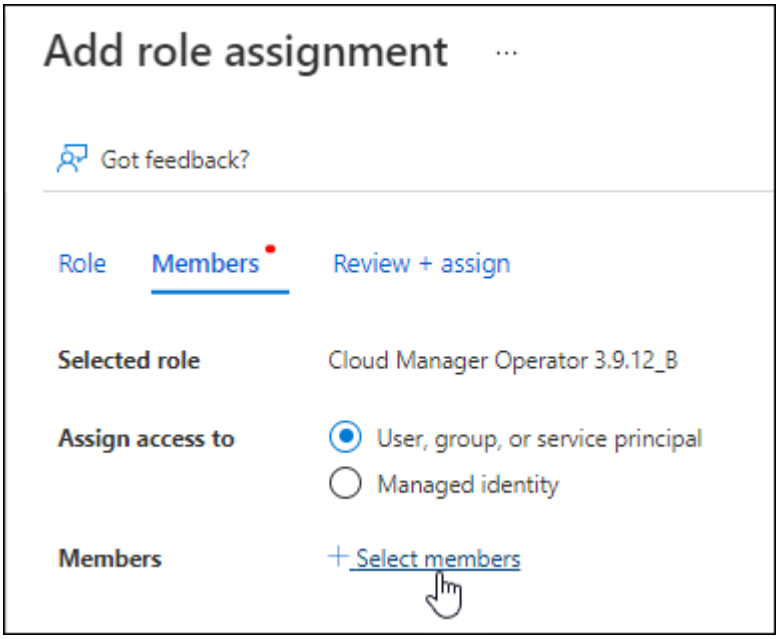
   Sie sollten nun eine benutzerdefinierte Rolle namens BlueXP Operator haben, die Sie der virtuellen Connector-Maschine zuweisen können.

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:

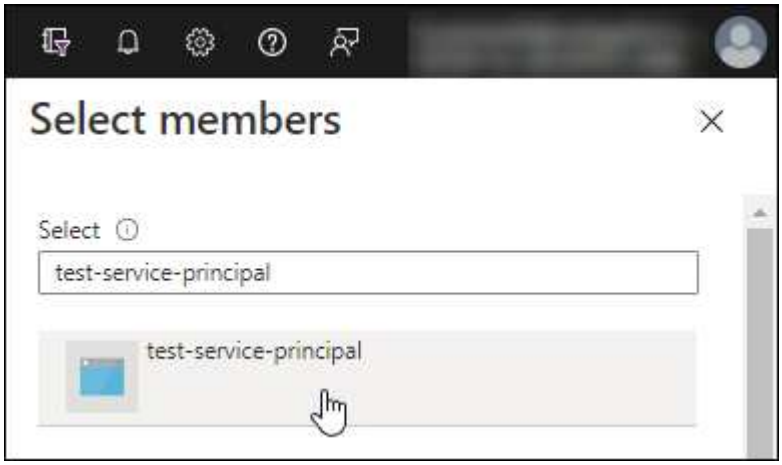
      - **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.

- 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.

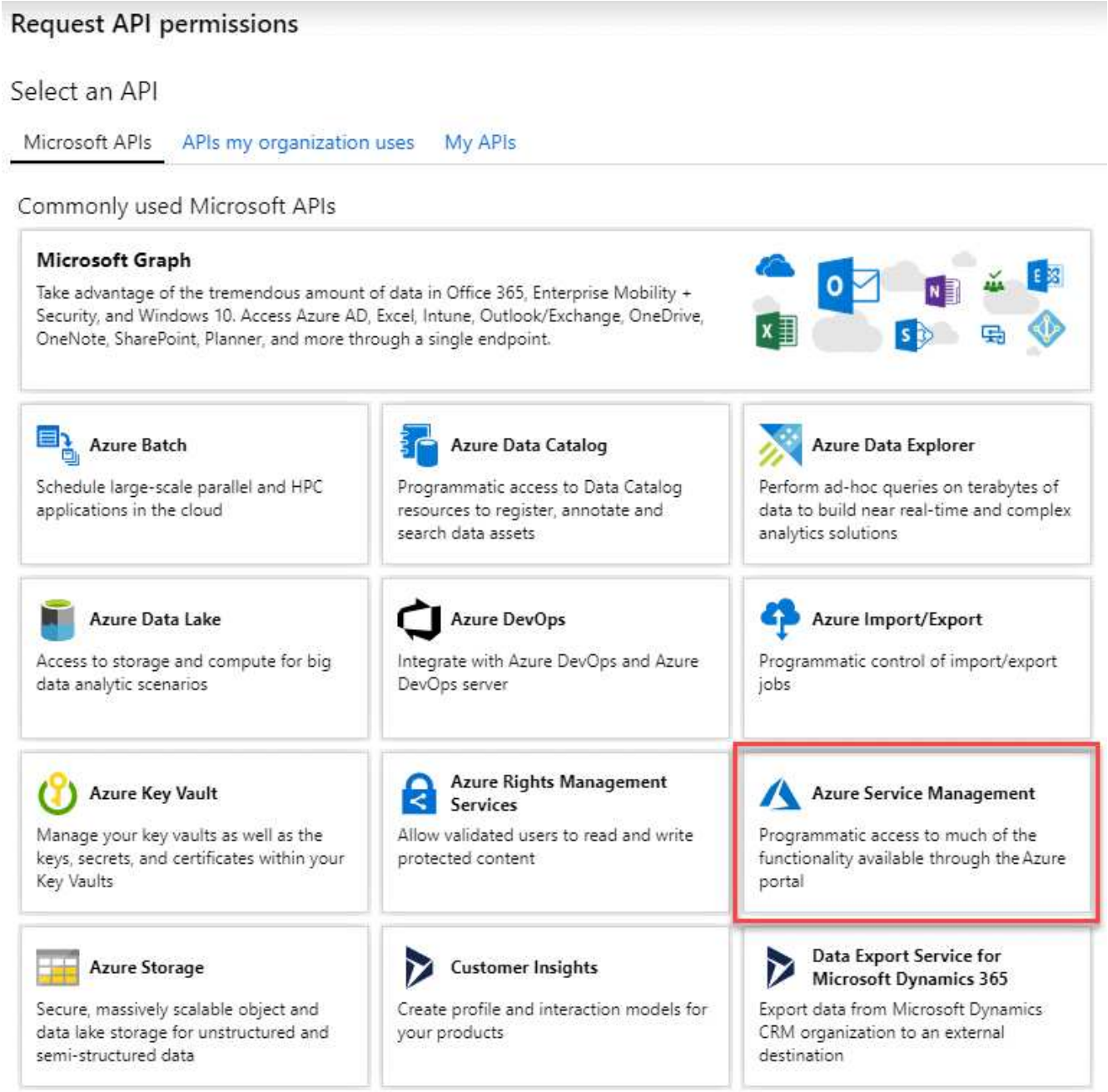
Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Prinzipal an jedes dieser Subscriptions binden. Mit BlueXP können Sie das Abonnement auswählen, das Sie bei der Bereitstellung von Cloud Volumes ONTAP verwenden möchten.

Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

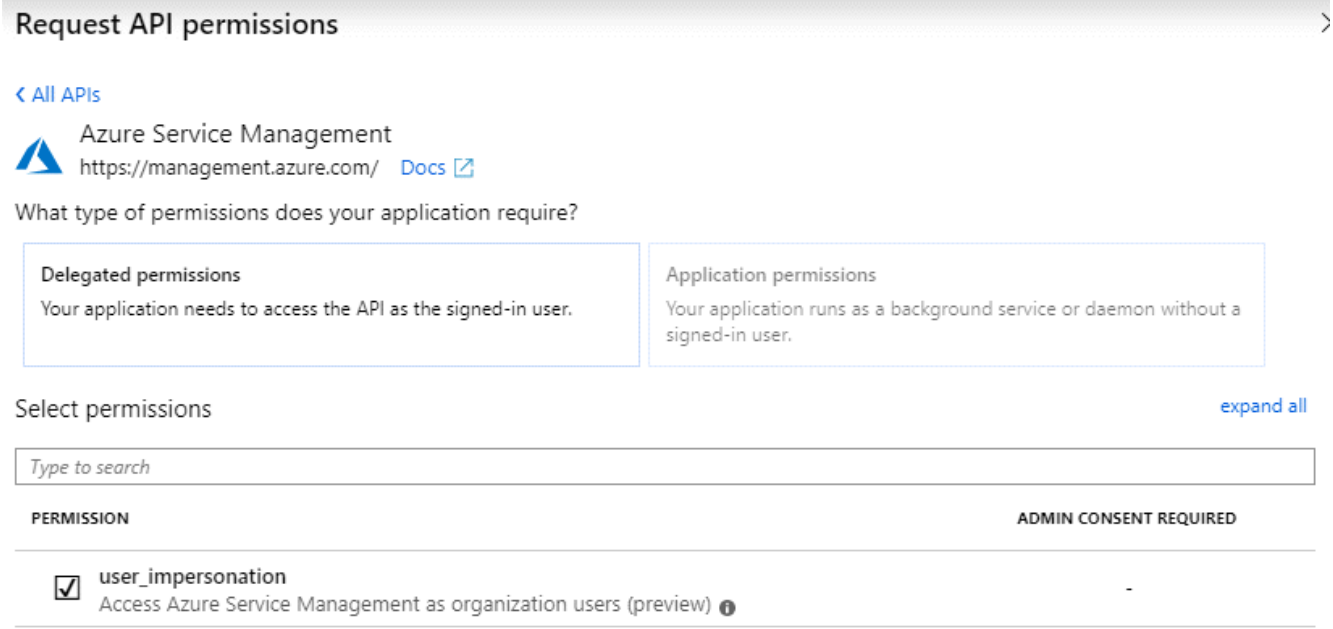
Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

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**.

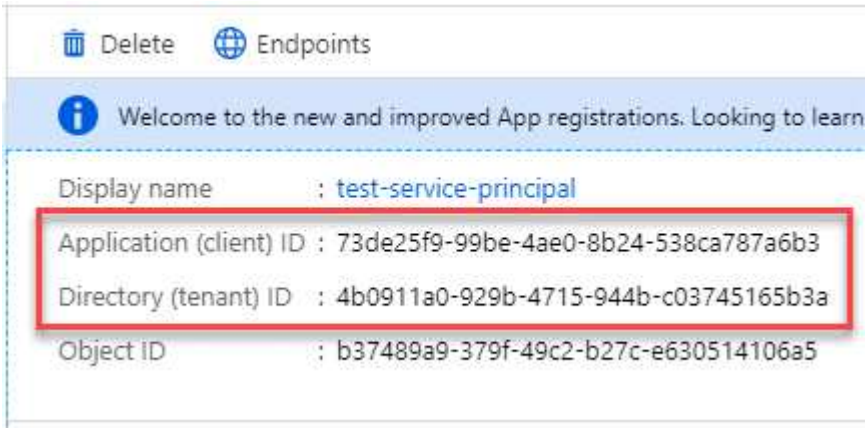


Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab

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:

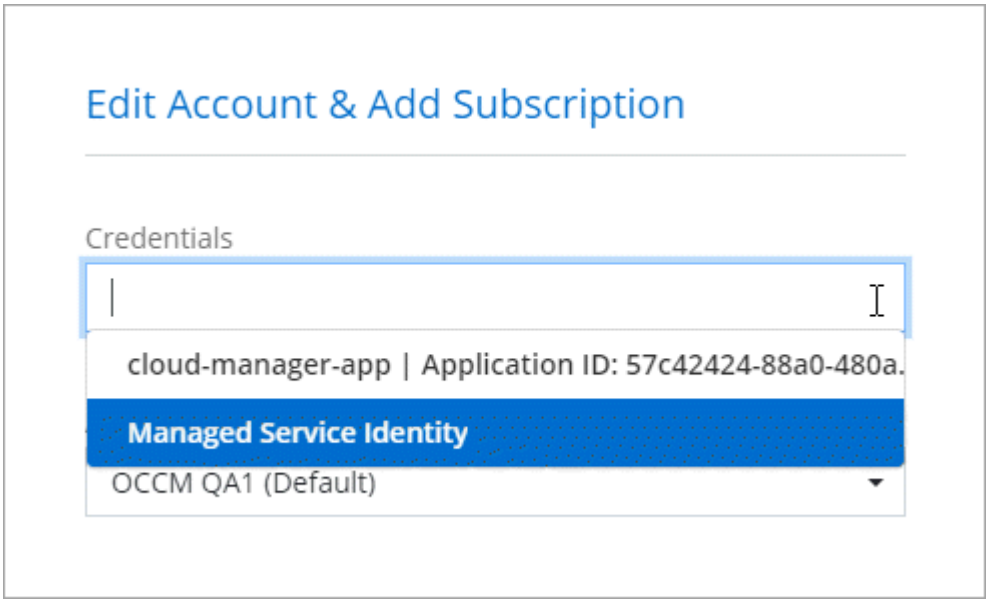
   - Anwendungs-ID (Client)
   - ID des Verzeichnisses (Mandant)
   - Client-Schlüssel

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.

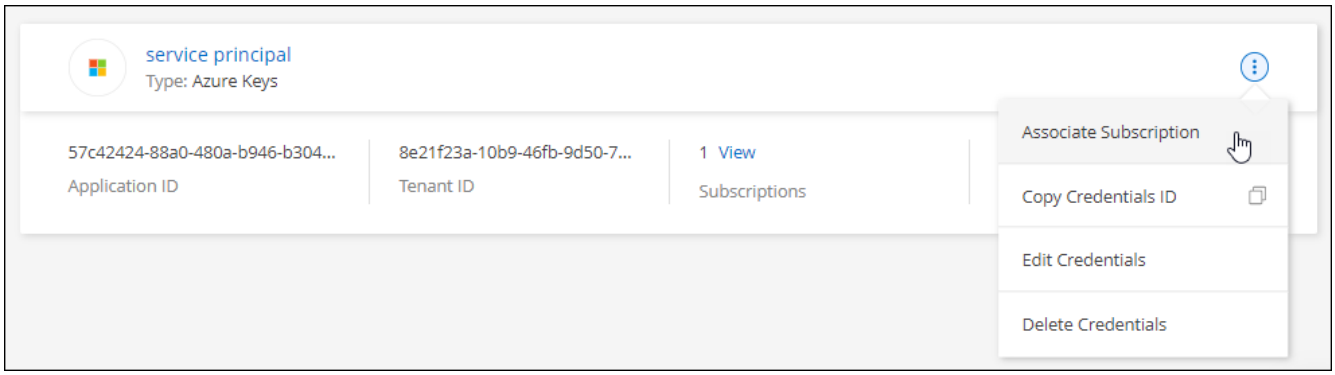
Bevor Sie beginnen

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.

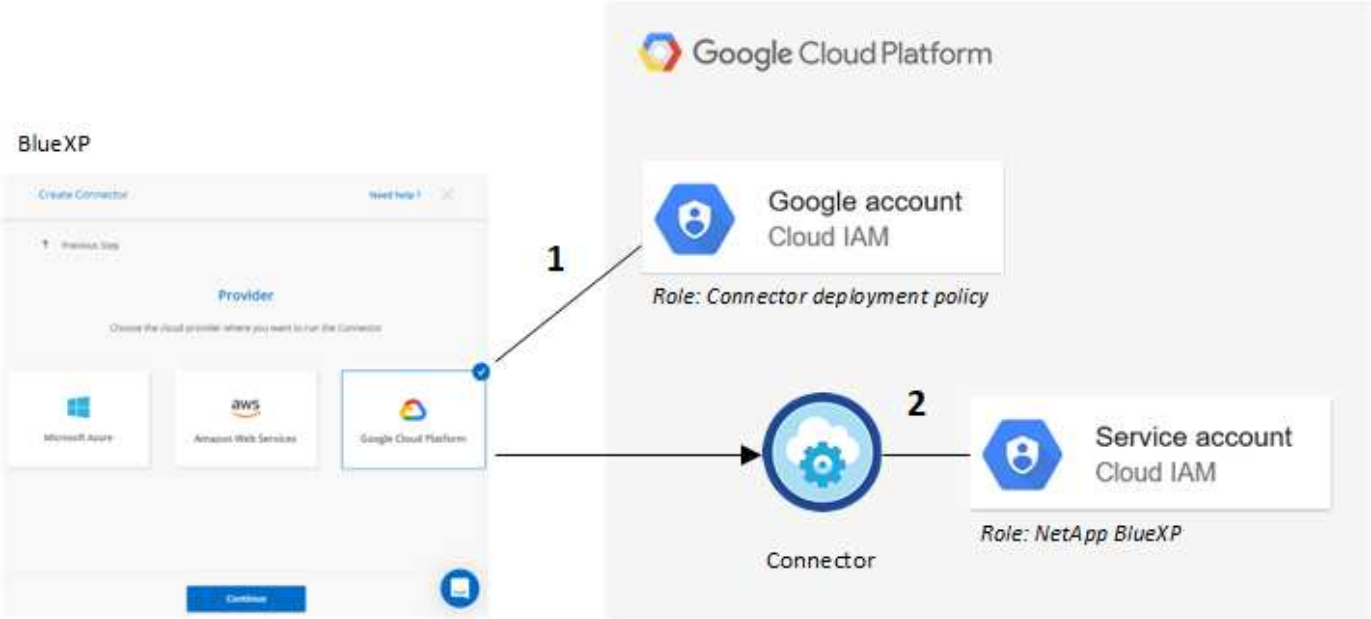
Projekt und Berechtigungen für BlueXP

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.

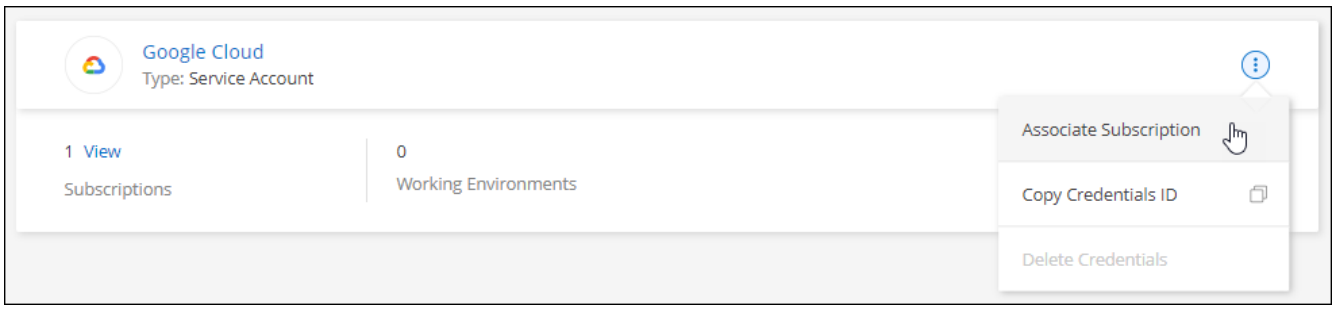
Verbinden Sie ein Marketplace-Abonnement mit Google Cloud-Anmeldedaten

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.

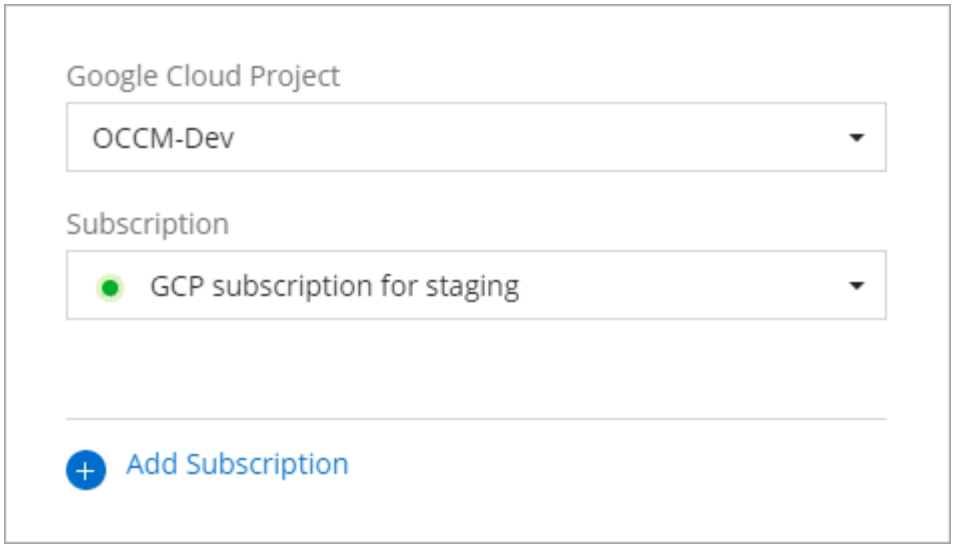
Durch den Austausch des aktuellen Marketplace-Abonnements durch ein neues Abonnement wird das Marketplace-Abonnement für alle bestehenden Cloud Volumes ONTAP Arbeitsumgebungen und alle neuen Arbeitsumgebungen geändert.

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**.



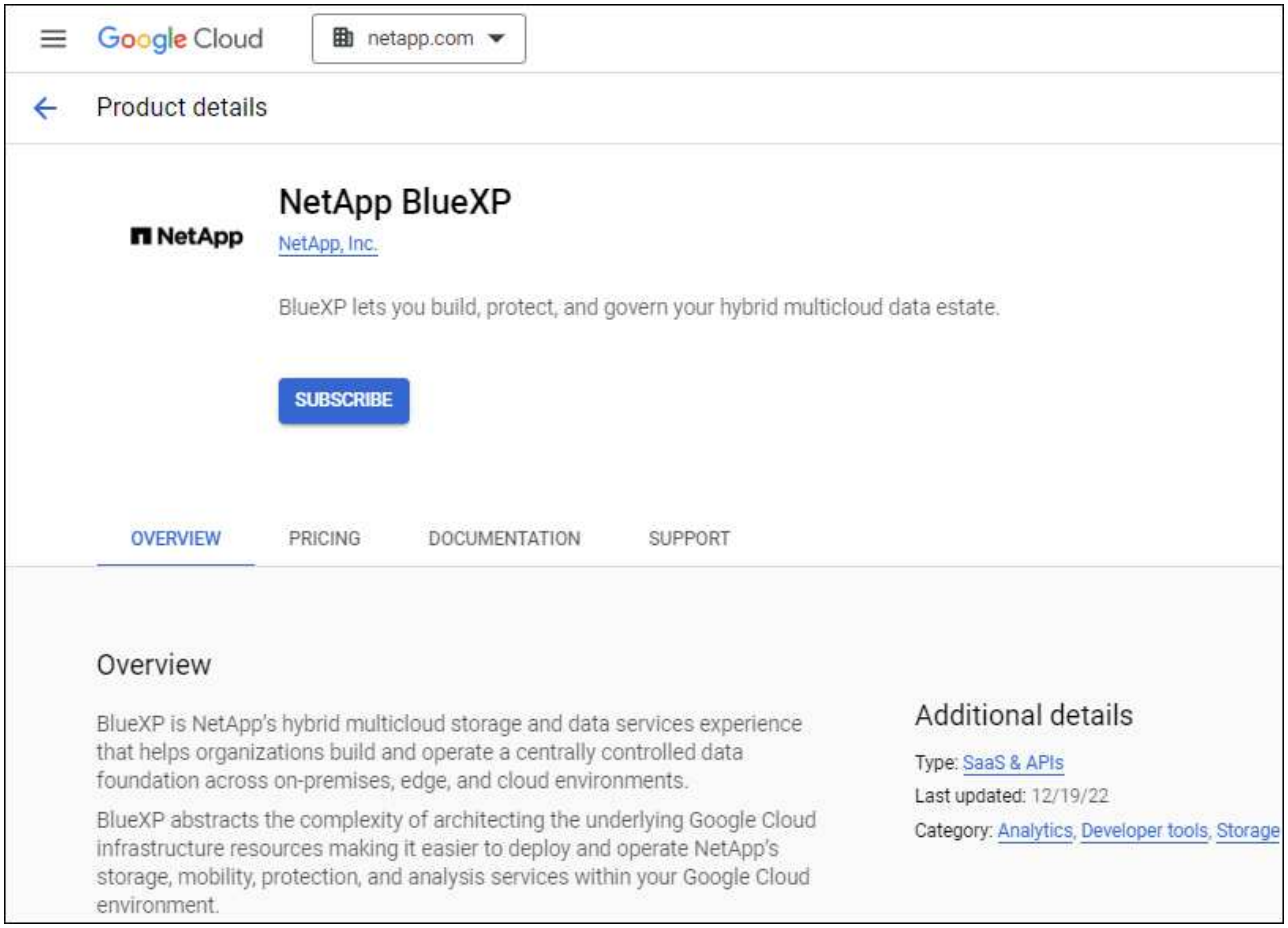
3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, und wählen Sie dann **Associate** aus.



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**.

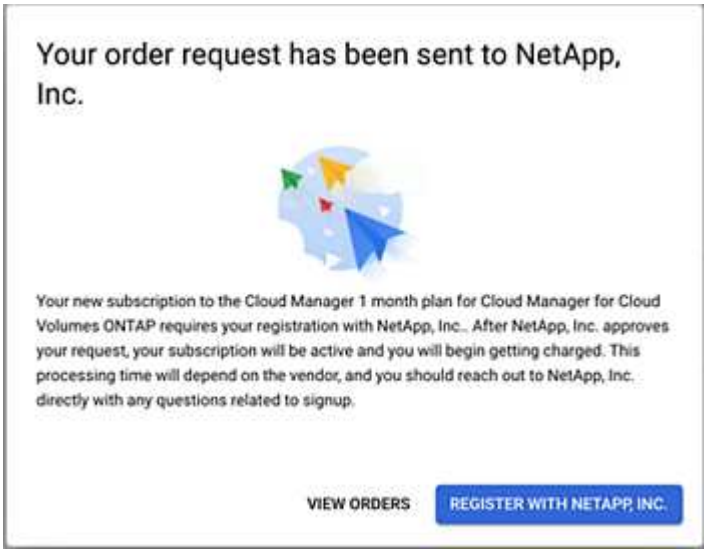
c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

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.

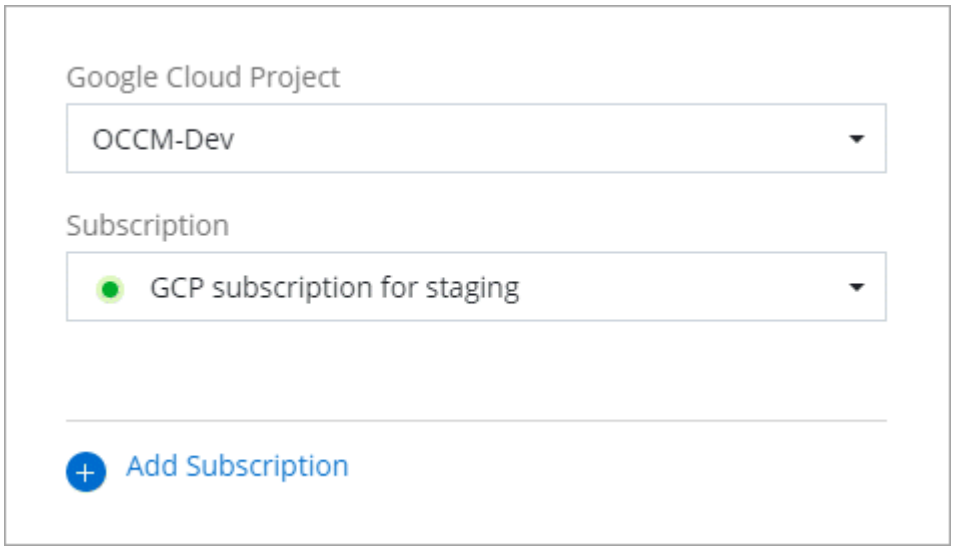
   Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden Schritte wiederholen.

   - 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.

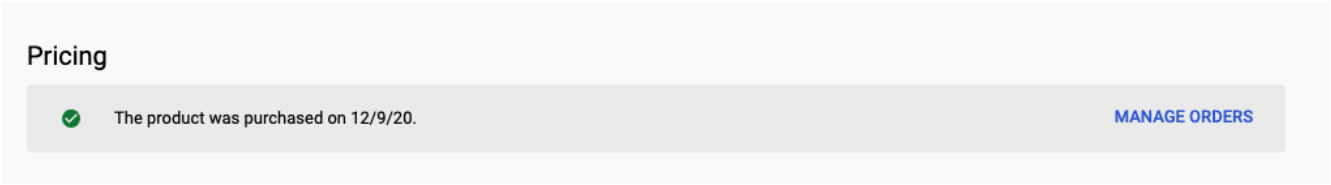


Fehlerbehebung bei der Marketplace-Subscription

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.

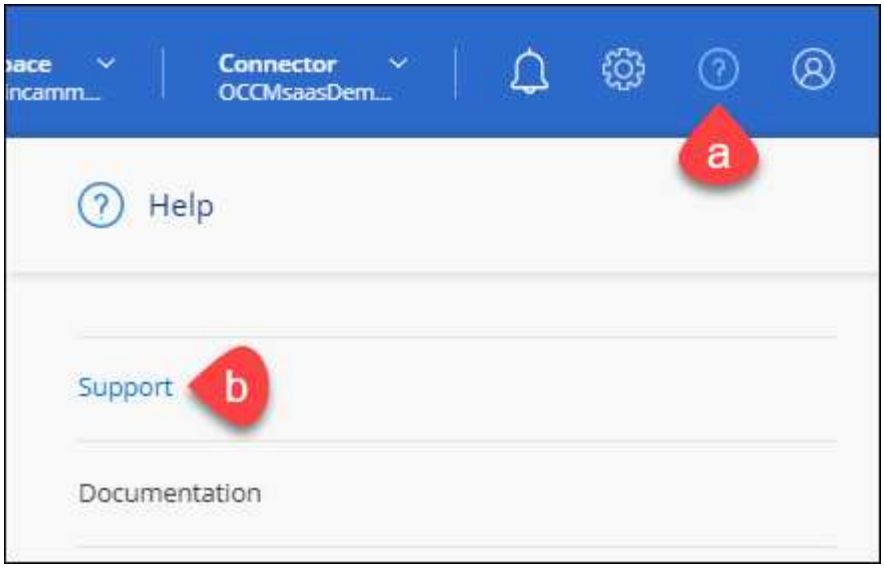
Fügen Sie ein NSS-Konto hinzu

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"

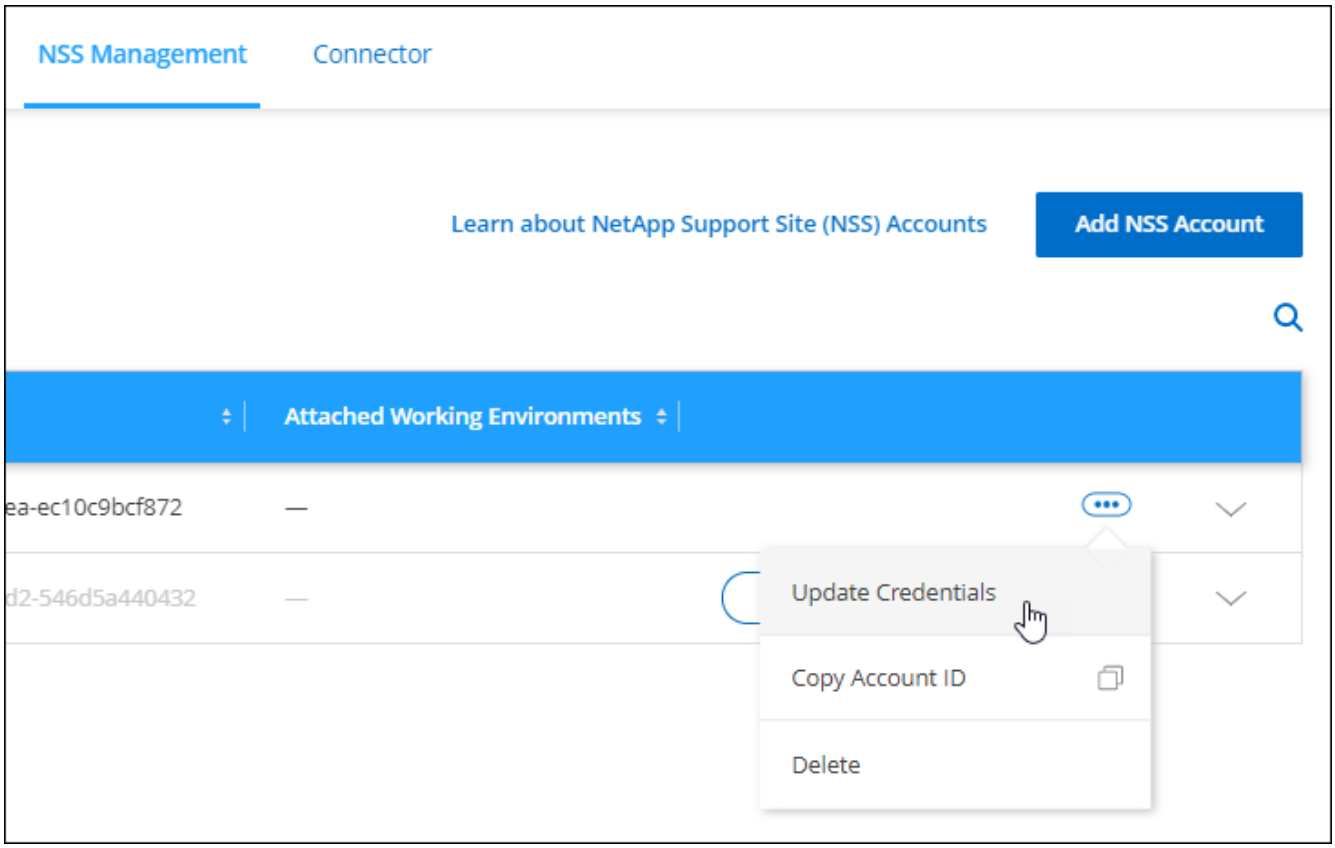
NSS-Anmeldeinformationen aktualisieren

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.

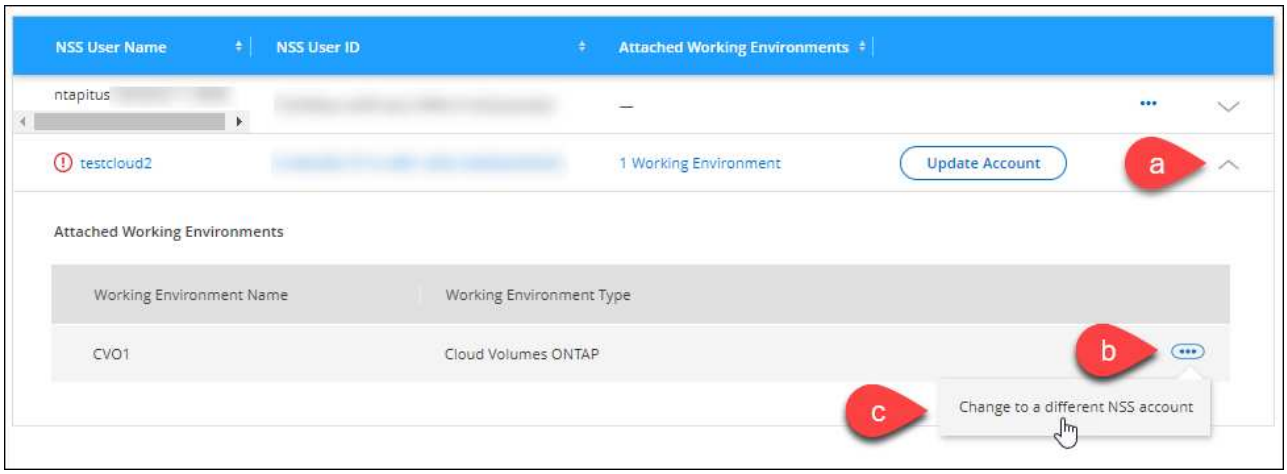
Verbinden Sie eine Arbeitsumgebung mit einem anderen NSS-Konto

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**.

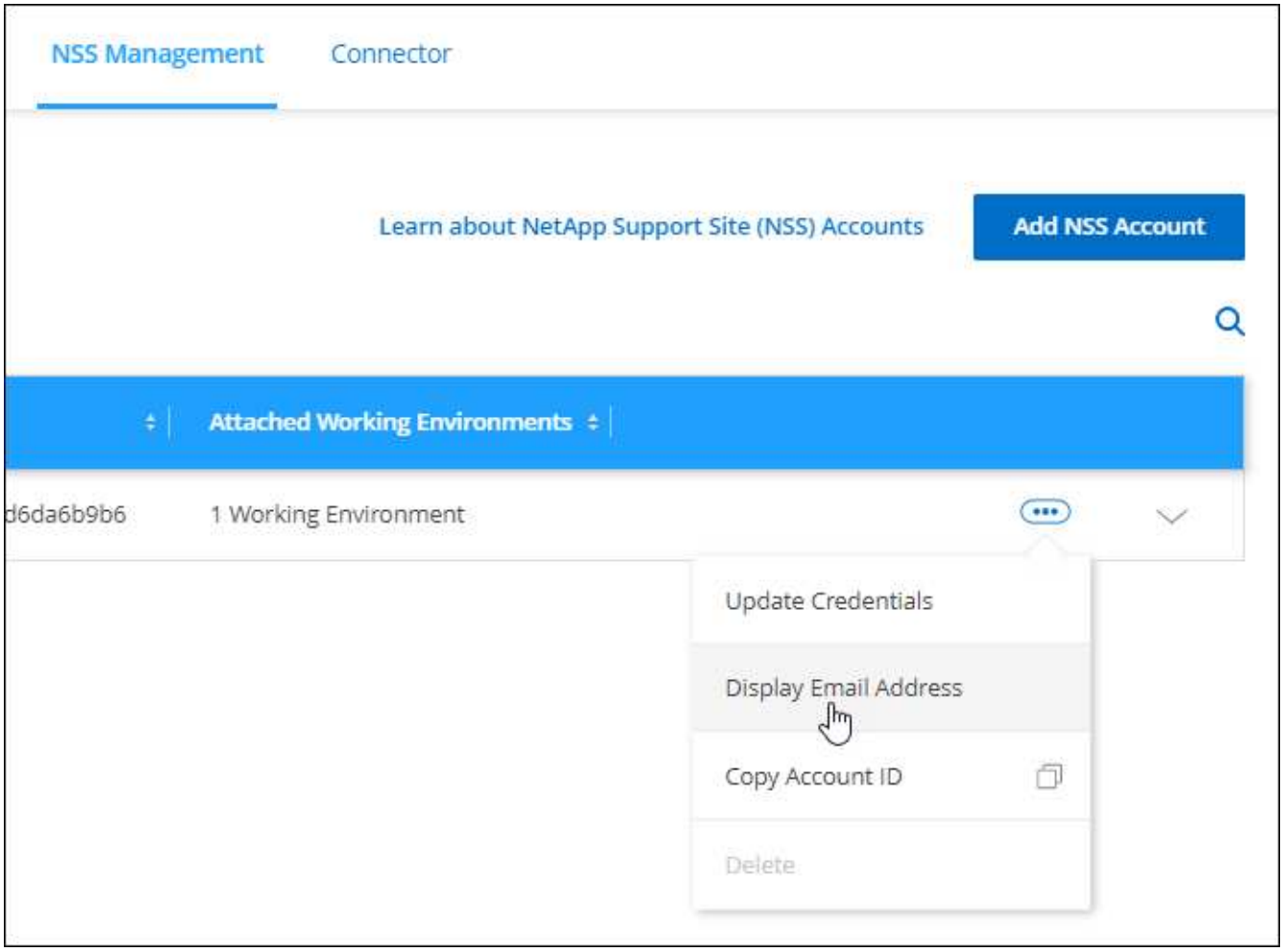
Zeigen Sie die E-Mail-Adresse für ein NSS-Konto an

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.

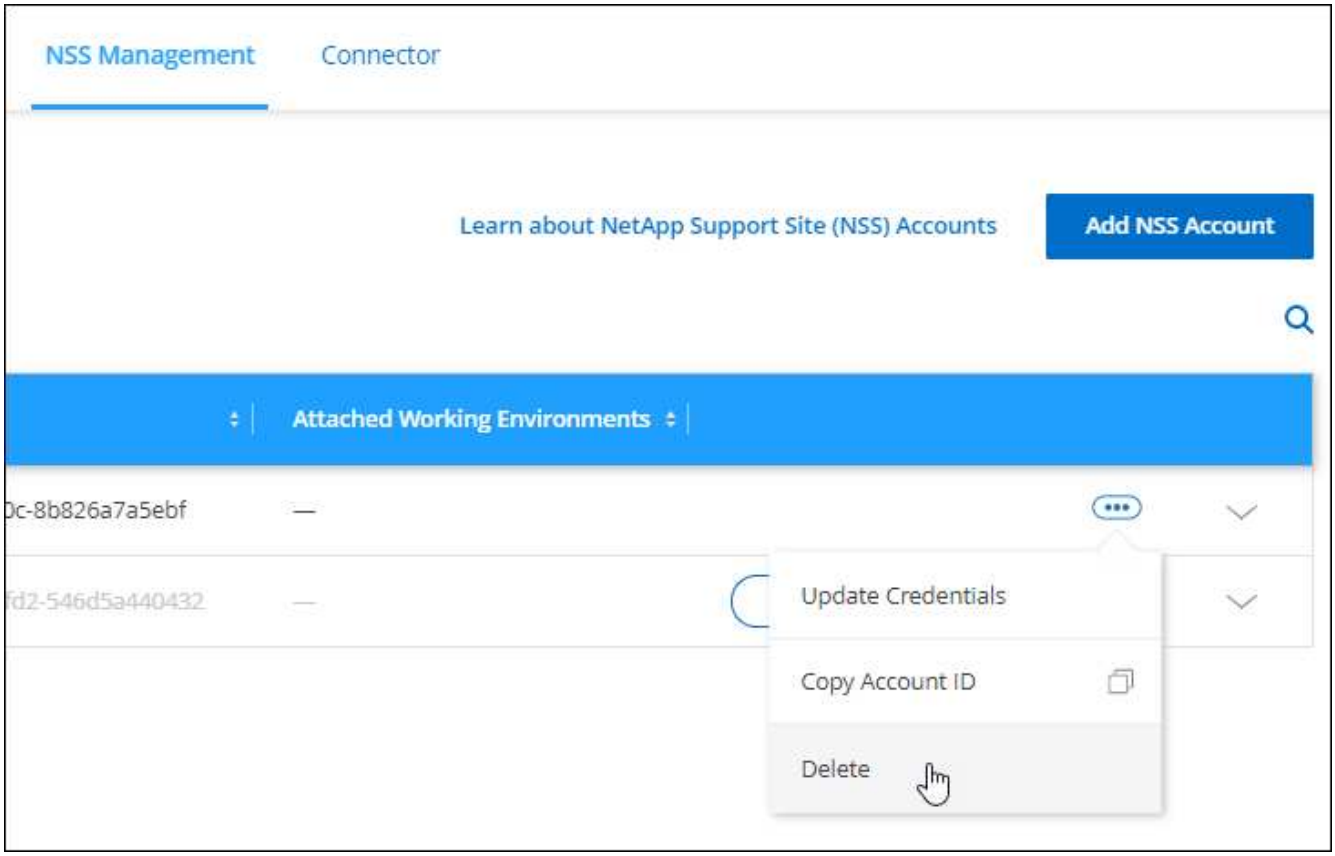
Entfernen Sie ein NSS-Konto

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.

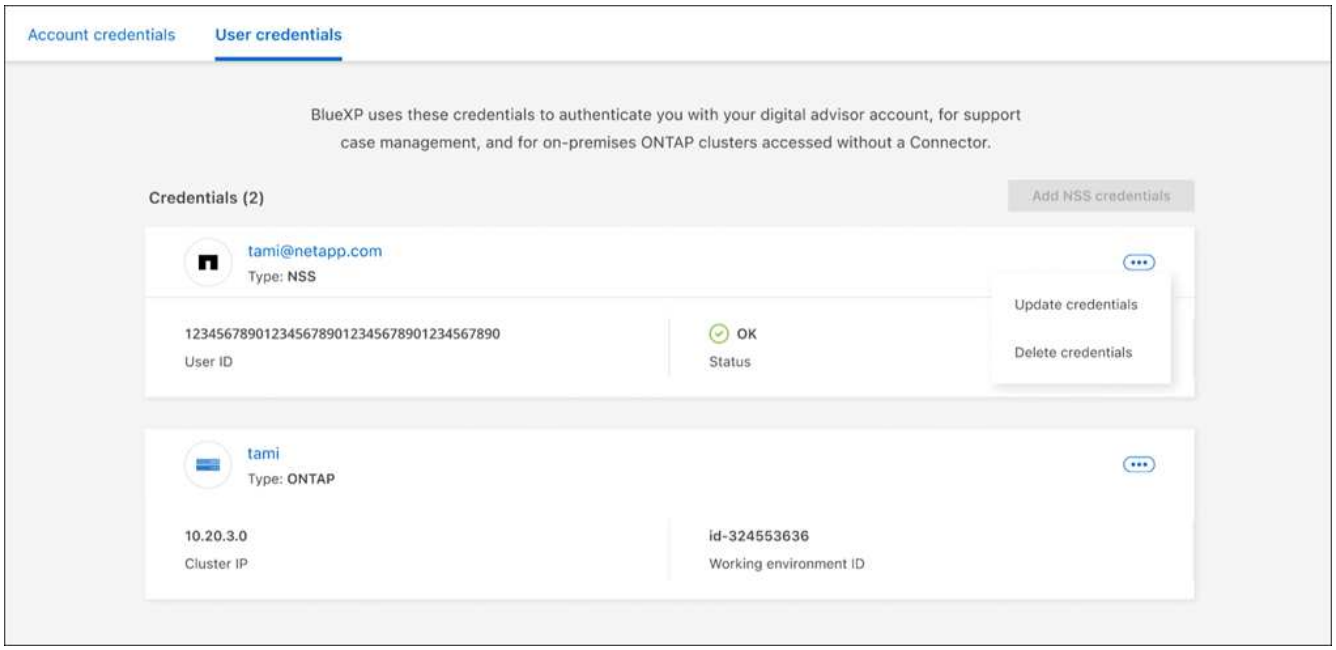
  "Erfahren Sie mehr über die Verwendung von NSS Credentials mit Ihrem BlueXP Konto".

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.

Referenz

Berechtigungen

Zusammenfassung der Berechtigungen für BlueXP

Um Funktionen und Services von BlueXP nutzen zu können, müssen Sie Berechtigungen bereitstellen, damit BlueXP Vorgänge in Ihrer Cloud-Umgebung ausführen kann. Über die Links auf dieser Seite können Sie schnell auf die Berechtigungen zugreifen, die Sie basierend auf Ihrem Ziel benötigen.

AWS Berechtigungen

BlueXP erfordert AWS Berechtigungen für den Connector und für einzelne Services.

Anschlüsse

Ziel	Beschreibung	Verlinken
Implementieren Sie den Connector von BlueXP	Der Benutzer, der einen Connector von BlueXP erstellt, benötigt spezielle Berechtigungen, um die Instanz in AWS bereitzustellen.	"AWS-Berechtigungen einrichten"
Geben Sie Berechtigungen für den Connector an	Beim Start des Connectors durch BlueXP wird eine Richtlinie an die Instanz angehängt, die die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen in Ihrem AWS-Konto bereitstellt. Sie müssen die Richtlinie selbst einrichten, wenn Sie einen Connector vom AWS Marketplace starten, den Connector manuell installieren oder wenn Sie ihn starten "Fügen Sie weitere AWS Zugangsdaten zu einem Connector hinzu". Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.	"AWS-Berechtigungen für den Connector"

Backup und Recovery

Ziel	Beschreibung	Verlinken
Sichern Sie On-Premises-ONTAP-Cluster in Amazon S3	Bei der Aktivierung von Backups auf Ihren ONTAP Volumes werden Sie von BlueXP Backup und Recovery aufgefordert, einen Zugriffsschlüssel und einen Schlüssel für einen IAM-Benutzer mit spezifischen Berechtigungen einzugeben.	"Richten Sie S3-Berechtigungen für Backups ein"

Cloud Volumes ONTAP

Ziel	Beschreibung	Verlinken
Stellen Sie Berechtigungen für Cloud Volumes ONTAP-Knoten bereit	Eine IAM-Rolle muss mit jedem Cloud Volumes ONTAP-Node in AWS verbunden sein. Das gleiche gilt für den HA Mediator. Die Standardeinstellung ist, dass BlueXP die IAM-Rollen für Sie erstellen lässt. Sie können jedoch Ihre eigenen beim Erstellen der Arbeitsumgebung verwenden.	"Erfahren Sie, wie Sie die IAM-Rollen selbst einrichten"

Kopieren und Synchronisieren

Ziel	Beschreibung	Verlinken
Implementieren Sie den Daten-Broker in AWS	Das AWS-Benutzerkonto, mit dem Sie den Daten-Broker bereitstellen, muss über spezielle Berechtigungen verfügen.	"Erforderliche Berechtigungen für die Bereitstellung des Data Brokers in AWS"
Geben Sie Berechtigungen für den Daten-Broker an	Wenn der Daten-Broker durch BlueXP Kopier- und Synchronisierungsfunktion implementiert wird, wird eine IAM-Rolle für die Daten-Broker-Instanz erstellt. Sie können den Data Broker auf Wunsch mit Ihrer eigenen IAM-Rolle bereitstellen.	"Anforderungen für die Nutzung Ihrer eigenen IAM-Rolle mit dem AWS Data Broker"
Aktivieren Sie AWS Zugriff für einen manuell installierten Daten-Broker	Wenn Sie den Daten-Broker mit einer Synchronisierungsbeziehung nutzen, die einen S3-Bucket umfasst, sollten Sie den Linux Host auf AWS-Zugriff vorbereiten. Wenn Sie den Daten-Broker installieren, müssen Sie AWS-Schlüssel für einen IAM-Benutzer bereitstellen, der programmatischen Zugriff und bestimmte Berechtigungen hat.	"Zugriff auf AWS wird ermöglicht"

FSX für ONTAP

Ziel	Beschreibung	Verlinken
FSX für ONTAP erstellen und managen	Zum Erstellen oder Managen einer Arbeitsumgebung von Amazon FSX for NetApp ONTAP müssen Sie AWS-Zugangsdaten zu BlueXP hinzufügen. Hierfür stellen Sie den ARN einer IAM-Rolle bereit, die BlueXP die Berechtigungen gibt, die zum Erstellen der Arbeitsumgebung erforderlich sind.	"Erfahren Sie, wie Sie AWS Zugangsdaten für FSX einrichten"

Tiering

Ziel	Beschreibung	Verlinken
Das Tiering lokaler ONTAP Cluster zu Amazon S3	Wenn Sie BlueXP Tiering zu AWS aktivieren, werden Sie vom Assistenten aufgefordert, einen Zugriffsschlüssel und einen geheimen Schlüssel einzugeben. Diese Anmeldedaten werden an den ONTAP Cluster weitergeleitet, sodass ONTAP Daten-Tiering in den S3-Bucket durchführen kann.	"S3-Berechtigungen für Tiering einrichten"

Azure-Berechtigungen

BlueXP erfordert für den Connector und einzelne Services Azure Berechtigungen.

Anschlüsse

Ziel	Beschreibung	Verlinken
Implementieren Sie den Connector von BlueXP	Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie ein Azure-Konto oder einen Service-Principal verwenden, der über die Berechtigungen zum Bereitstellen der Connector-VM in Azure verfügt.	"Azure-Berechtigungen einrichten"
Geben Sie Berechtigungen für den Connector an	Wenn BlueXP die Connector VM in Azure implementiert, wird eine benutzerdefinierte Rolle erstellt, die die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen im Azure Abonnement bietet. Sie müssen die benutzerdefinierte Rolle selbst einrichten, wenn Sie einen Connector vom Marktplatz starten, wenn Sie den Connector manuell installieren oder wenn Sie dies tun "Fügen Sie weitere Azure Credentials zu einem Connector hinzu". Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.	"Azure-Berechtigungen für den Connector"

Kopieren und Synchronisieren

Ziel	Beschreibung	Verlinken
Implementieren Sie den Daten-Broker in Azure	Das Azure-Benutzerkonto, mit dem Sie den Daten-Broker bereitstellen, muss über die erforderlichen Berechtigungen verfügen.	"Erforderliche Berechtigungen für die Bereitstellung des Daten-Brokers in Azure"

Google Cloud-Berechtigungen

BlueXP erfordert für den Connector und einzelne Services Google Cloud-Berechtigungen.

Anschlüsse

Ziel	Beschreibung	Verlinken
Implementieren Sie den Connector von BlueXP	Der Google Cloud-Benutzer, der einen Connector von BlueXP bereitstellt, benötigt spezielle Berechtigungen, um den Connector in Google Cloud bereitzustellen.	"Richten Sie Berechtigungen zum Erstellen des Connectors ein"
Geben Sie Berechtigungen für den Connector an	Das Servicekonto für die Connector-VM-Instanz muss über spezielle Berechtigungen für den täglichen Betrieb verfügen. Sie müssen das Dienstkonto während der Bereitstellung dem Connector zuordnen. Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.	"Richten Sie die Berechtigungen für den Connector ein"

Backup und Recovery

Ziel	Beschreibung	Verlinken
Backup von Cloud Volumes ONTAP in der Google Cloud	Wenn Sie BlueXP Backup und Recovery für ein Backup von Cloud Volumes ONTAP verwenden, müssen Sie in den folgenden Szenarien Berechtigungen zum Connector hinzufügen: • Sie möchten die Funktion „Suchen & Wiederherstellen“ verwenden • Sie möchten vom Kunden gemanagte Verschlüsselungsschlüssel (CMEK) verwenden.	• "Berechtigungen für die Funktion Suchen Wiederherstellen " • "Berechtigungen für CMEKs"
Backup von lokalen ONTAP Clustern in Google Cloud	Wenn Sie Backup und Recovery von lokalen ONTAP-Clustern mit BlueXP nutzen, müssen Sie Berechtigungen zum Connector hinzufügen, um die Funktion „Suchen und Wiederherstellen“ nutzen zu können.	"Berechtigungen für die Funktion Suchen Wiederherstellen"

Cloud Volumes Service für Google Cloud

Ziel	Beschreibung	Verlinken
Cloud Volumes Service für Google Cloud entdecken	BlueXP benötigt Zugriff auf die Cloud Volumes Service API und die richtigen Berechtigungen über ein Google Cloud-Dienstkonto.	"Erstellen eines Servicekontos"

Kopieren und Synchronisieren

Ziel	Beschreibung	Verlinken
Implementieren Sie den Daten-Broker in Google Cloud	Stellen Sie sicher, dass der Google Cloud-Benutzer, der den Daten-Broker bereitstellt, über die erforderlichen Berechtigungen verfügt.	"Erforderliche Berechtigungen für die Bereitstellung des Daten-Brokers in Google Cloud"
Aktivieren Sie Google Cloud-Zugriff für einen manuell installierten Daten-Broker	Wenn Sie den Daten-Broker mit einer Synchronisierungsbeziehung verwenden möchten, die einen Google Cloud Storage Bucket enthält, sollten Sie den Linux-Host für Google Cloud-Zugriff vorbereiten. Nach der Installation des Daten-Brokers müssen Sie einen Schlüssel für ein Servicekonto mit spezifischen Berechtigungen bereitstellen.	"Zugriff auf Google Cloud wird ermöglicht"

StorageGRID-Berechtigungen

BlueXP erfordert StorageGRID Berechtigungen für zwei Services.

Backup und Recovery

Ziel	Beschreibung	Verlinken
Sichern Sie On-Premises-ONTAP-Cluster in StorageGRID	Wenn Sie StorageGRID als Backup-Ziel für ONTAP Cluster vorbereiten, werden Sie beim BlueXP Backup und Recovery aufgefordert, einen Zugriffsschlüssel und einen Schlüssel für einen IAM-Benutzer mit spezifischen Berechtigungen einzugeben.	"StorageGRID als Backup-Ziel vorbereiten"

Tiering

Ziel	Beschreibung	Verlinken
Tiering von lokalen ONTAP Clustern zu StorageGRID	Wenn Sie BlueXP Tiering auf StorageGRID einrichten, müssen Sie für BlueXP Tiering einen S3 Zugriffsschlüssel und einen geheimen Schlüssel bereitstellen. BlueXP Tiering verwendet die Schlüssel für den Zugriff auf Ihre Buckets.	"Tiering in StorageGRID vorbereiten"

AWS-Berechtigungen für den Connector

Beim Start der Connector-Instanz in AWS hängt BlueXP eine Richtlinie an die Instanz an, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. Der Connector verwendet die Berechtigungen, um API-Aufrufe an verschiedene AWS Services wie EC2, S3, CloudFormation, IAM, Der Key Management Service (KMS) und vieles mehr.

IAM-Richtlinien

Die unten verfügbaren IAM-Richtlinien bieten die Berechtigungen, die ein Connector zur Verwaltung von Ressourcen und Prozessen innerhalb Ihrer Public-Cloud-Umgebung basierend auf Ihrer AWS-Region benötigt.

Beachten Sie Folgendes:

- Wenn Sie einen Connector in einer standardmäßigen AWS-Region direkt aus BlueXP erstellen, wendet BlueXP automatisch Richtlinien auf den Connector an. Sie müssen in diesem Fall nichts tun.
- Sie müssen die Richtlinien selbst einrichten, wenn Sie den Connector über AWS Marketplace implementieren, den Connector manuell auf einem Linux-Host installieren oder zusätzliche AWS-Anmeldedaten zu BlueXP hinzufügen möchten.
- Außerdem müssen Sie sicherstellen, dass die Richtlinien immer auf dem neuesten Stand sind, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.
- Bei Bedarf können Sie die IAM-Richtlinien mit Hilfe des IAM einschränken `Condition` Element: "AWS-Dokumentation: Condition Element"
- Informationen zur schrittweisen Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:
  - "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"

Wählen Sie Ihre Region aus, um die erforderlichen Richtlinien anzuzeigen:

Standardregionen

Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich.

Die erste Richtlinie bietet Berechtigungen für folgende Dienste:

- Amazon S3 Bucket-Erkennung
- Backup und Recovery
- Klassifizierung
- Cloud Volumes ONTAP
- FSX für ONTAP
- Tiering

Die zweite Richtlinie bietet Berechtigungen für die folgenden Dienste:

- Edge-Caching
- Kubernetes

Richtlinie #1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
```

```
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
                "s3:GetObject",
```

```
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
```

```
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
    ]
```

```
}
```

Richtlinie #2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

GovCloud (USA) Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
```

```
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
```

```
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Geheime Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Top Secret Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Wie werden die AWS Berechtigungen verwendet

In den folgenden Abschnitten wird die Nutzung der Berechtigungen für jeden BlueXP Service beschrieben. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf bereitgestellt werden.

Amazon FSX für ONTAP

Der Connector stellt die folgenden API-Anforderungen für das Management von Amazon FSX für ONTAP bereit:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribut
- ec2:DescribeRouteTables
- ec2:DescribeBilder
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces

- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeypairs
- ec2:DescribeRegionen
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfilVerbände
- ec2:DescribeReserviertInstanceAngebote
- ec2:DescribeVpcEndpunkte
- ec2:DescribeVpcs
- ec2:DescribeVolumiesModified
- ec2:DescribePlacementGroups
- Km:Liste*
- Km:Beschreiben*
- Km:CreateGrant
- Km:ListAliase
- fsx:Beschreiben*
- fsx:Liste*

Amazon S3 Bucket-Erkennung

Der Connector stellt folgende API-Anforderung vor, Amazon S3 Buckets zu erkennen:

s3:GetVerschlüsselungKonfiguration

Backup und Recovery

Der Connector stellt folgende API-Anforderungen zum Management von Backups in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuchs
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleKonfiguration
- s3:PutLifecycleKonfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Km:Liste*

- Km:Beschreiben*
- s3:GetObject
- ec2:DescribeVpcEndpunkte
- Km:ListAliase
- s3:PutVerschlüsselungKonfiguration

Der Connector stellt folgende API-Anforderungen vor, wenn Sie die Methode Suchen und Wiederherstellen verwenden, um Volumes und Dateien wiederherzustellen:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleKonfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMehrteilaUpload
- s3:ListeMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StoppQueryExecution
- Kleber:CreateDatabase
- Kleber:CreateTable
- Kleber:BatchDeletePartition

Der Connector macht die folgenden API-Anforderungen, wenn Sie DataLock und Ransomware-Schutz für Ihre Volume-Backups verwenden:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAkl
- s3:PuttObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention

- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleKonfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersionierung
- s3:PuttObjectVersionTagging
- s3:GetBucketVersionierung
- s3:GetBucketAcl
- s3:BypassGovernanceAufbewahrung
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Der Connector macht die folgenden API-Anforderungen, wenn Sie ein anderes AWS-Konto für Ihre Cloud Volumes ONTAP-Backups verwenden, als Sie für die Quell-Volumes verwenden:

- s3:PutBucketPolicy
- s3:PutBucketEigentümerControls

Klassifizierung

Der Connector macht die folgenden API-Anfragen zur Implementierung der BlueXP Klassifizierungsinstanz:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:DescribeSecurityGroups

- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:DescribeRegionen
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- Wolkenbildung:DescribeStacks
- Molkenbildung:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfil
- ec2:DescribeIamInstanceProfilVerbände

Der Connector macht die folgenden API-Anfragen zum Scannen von S3-Buckets, wenn Sie die BlueXP-Klassifizierung verwenden:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfil
- ec2:DescribeIamInstanceProfilVerbände
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuchs
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:PutObject
- STS:AssumeRole

Cloud Volumes ONTAP

Der Connector stellt die folgenden API-Anforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in AWS.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellung und Management von IAM-Rollen und Instanzprofilen für Cloud Volumes ONTAP Instanzen	iam:ListInstanceProfiles	Ja.	Ja.	Nein
	iam:CreateRollenole	Ja.	Nein	Nein
	iam:DeleteRole	Nein	Ja.	Ja.
	iam:PuttePolicy	Ja.	Nein	Nein
	iam:CreateInstanceProfil	Ja.	Nein	Nein
	iam:DeleteRolePolicy	Nein	Ja.	Ja.
	iam:AddRoleToInstanceProfile	Ja.	Nein	Nein
	iam:RemoveRoleFromInstanceProfile	Nein	Ja.	Ja.
	iam:DeleteInstanceProfil	Nein	Ja.	Ja.
	iam:PassRole	Ja.	Nein	Nein
	ec2:AssociateIamInstanceProfil	Ja.	Ja.	Nein
	ec2:DescribeIamInstanceProfilVerbände	Ja.	Ja.	Nein
	ec2:DisassociateIamInstanceProfil	Nein	Ja.	Nein
Dekodieren von Autorisierungsstatusmeldungen	STS:DekodeAuthorisationNachricht	Ja.	Ja.	Nein
Beschreiben Sie die angegebenen Bilder (Amis), die dem Konto zur Verfügung stehen	ec2:DescribeBilder	Ja.	Ja.	Nein
Routingtabellen in einer VPC beschreiben (nur für HA-Paare erforderlich)	ec2:DescribeRouteTables	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Beenden, starten und überwachen Sie Instanzen	ec2:StartInstances	Ja.	Ja.	Nein
	ec2:StopInstances	Ja.	Ja.	Nein
	ec2:DescribeInstances	Ja.	Ja.	Nein
	ec2:DescribeInstanceStatus	Ja.	Ja.	Nein
	ec2:RunInstances	Ja.	Nein	Nein
	ec2:TerminateInstances	Nein	Nein	Ja.
	ec2:ModifyInstanceAttribut	Nein	Ja.	Nein
Vergewissern Sie sich, dass erweitertes Networking für unterstützte Instanztypen aktiviert ist	ec2:DescribeInstanceAttribut	Nein	Ja.	Nein
Markieren Sie Ressourcen mit den Tags „WorkingEnvironment“ und „WorkingEnvironment ID“, die zur Wartung und Kostenverteilung verwendet werden	ec2:CreateTags	Ja.	Ja.	Nein
Management von EBS Volumes, die Cloud Volumes ONTAP als Back-End Storage verwendet	ec2:CreateVolume	Ja.	Ja.	Nein
	ec2:DescribeVolumes	Ja.	Ja.	Ja.
	ec2:ModifyVolumeAttribute	Nein	Ja.	Ja.
	ec2:AttachVolume	Ja.	Ja.	Nein
	ec2:DeleteVolume	Nein	Ja.	Ja.
	ec2:DetachVolume	Nein	Ja.	Ja.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Managen von Sicherheitsgruppen für Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Ja.	Nein	Nein
	ec2:DeleteSecurityGroup	Nein	Ja.	Ja.
	ec2:DescribeSecurityGroups	Ja.	Ja.	Ja.
	ec2:RevokeSecurityGroupEgress	Ja.	Nein	Nein
	ec2:AuthoriseSecurityGroupEgress	Ja.	Nein	Nein
	ec2:AuthoriseSecurityGroupIngress	Ja.	Nein	Nein
	ec2:RevokeSecurityGroupIngress	Ja.	Ja.	Nein
Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz erstellen und verwalten	ec2:CreateNetworkInterface	Ja.	Nein	Nein
	ec2:DescribeNetworkInterfaces	Ja.	Ja.	Nein
	ec2:DeleteNetworkInterface	Nein	Ja.	Ja.
	ec2:ModifyNetworkInterface Attribute	Nein	Ja.	Nein
Abrufen der Liste der Zielnetze und -Sicherheitsgruppen	ec2:DescribeSubnets	Ja.	Ja.	Nein
	ec2:DescribeVpcs	Ja.	Ja.	Nein
Abrufen der DNS-Server und des Standard-Domain-Namens für Cloud Volumes ONTAP-Instanzen	ec2:DescribeDhcpOptions	Ja.	Nein	Nein
Erstellen von Snapshots von EBS Volumes für Cloud Volumes ONTAP	ec2:CreateSnapshot	Ja.	Ja.	Nein
	ec2:DeleteSnapshot	Nein	Ja.	Ja.
	ec2:DescribeSnapshots	Nein	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erfassen Sie die Cloud Volumes ONTAP Konsole, die an AutoSupport Meldungen angeschlossen ist	ec2:GetConsoleOutput	Ja.	Ja.	Nein
Erhalten Sie die Liste der verfügbaren Schlüsselpaare	ec2:DescribeKeypairs	Ja.	Nein	Nein
Hier erhalten Sie eine Liste der verfügbaren AWS Regionen	ec2:DescribeRegionen	Ja.	Ja.	Nein
Verwalten von Tags für Ressourcen, die Cloud Volumes ONTAP Instanzen zugeordnet sind	ec2:DeleteTags	Nein	Ja.	Ja.
	ec2:DescribeTags	Nein	Ja.	Nein
Stacks für AWS CloudFormation-Vorlagen erstellen und managen	CloudFormation:CreateStack	Ja.	Nein	Nein
	CloudFormation:DeleteStack	Ja.	Nein	Nein
	Wolkenbildung:DescribeStacks	Ja.	Ja.	Nein
	Molkenbildung:DescribeStackEvents	Ja.	Nein	Nein
	Cloudformation:ValidierteVorlage	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Es wird ein S3-Bucket erstellt und gemanagt, den ein Cloud Volumes ONTAP System als Kapazitäts-Tier für Daten-Tiering verwendet	s3:CreateBucket	Ja.	Ja.	Nein
	s3:DeleteBucket	Nein	Ja.	Ja.
	s3:GetLifecycleKonfiguration	Nein	Ja.	Nein
	s3:PutLifecycleKonfiguration	Nein	Ja.	Nein
	s3:PutBucketTagging	Nein	Ja.	Nein
	s3:ListBucketVersions	Nein	Ja.	Nein
	s3:GetBucketPolicyStatus	Nein	Ja.	Nein
	s3:GetBucketPublicAccessBlock	Nein	Ja.	Nein
	s3:GetBucketAcl	Nein	Ja.	Nein
	s3:GetBucketPolicy	Nein	Ja.	Nein
	s3:PutBucketPublicAccessBlock	Nein	Ja.	Nein
	s3:GetBucketTagging	Nein	Ja.	Nein
	s3:GetBucketLocation	Nein	Ja.	Nein
	s3:ListAllMyBuchs	Nein	Nein	Nein
	s3:ListBucket	Nein	Ja.	Nein
Datenverschlüsselung von Cloud Volumes ONTAP mithilfe des AWS KMS (Key Management Service)	Km:Liste*	Ja.	Ja.	Nein
	Km:ReVerschlüsseln*	Ja.	Nein	Nein
	Km:Beschreiben*	Ja.	Ja.	Nein
	Km:CreateGrant	Ja.	Ja.	Nein
	Kms:GenerateDataKeyWithoutPlaintext	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und managen Sie eine AWS Spread-Platzierungsgruppe für zwei HA-Nodes und den Mediator in einer einzigen AWS Availability Zone	ec2:CreatePlacementGroup	Ja.	Nein	Nein
	ec2:DeletePlacementGroup	Nein	Ja.	Ja.
Erstellen von Berichten	fsx:Beschreiben*	Nein	Ja.	Nein
	fsx:Liste*	Nein	Ja.	Nein
Aggregate erstellen und managen, die die Amazon EBS Elastic Volumes Funktion unterstützen	ec2:DescribeVolumiesModified	Nein	Ja.	Nein
	ec2:ModifyVolume	Nein	Ja.	Nein

Edge-Caching

Der Connector macht die folgenden API-Anfragen zur Implementierung von BlueXP Edge-Caching-Instanzen während der Implementierung:

- Wolkenbildung:DescribeStacks
- cloudwatch:GetMetricStatistics
- CloudFormation:ListenStacks

Kubernetes

Der Connector stellt folgende API-Anforderungen zur Erkennung und Verwaltung von Amazon EKS-Clustern vor:

- ec2:DescribeRegionen
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

8 März 2024

Die folgende Berechtigung ist jetzt in der Connector-Richtlinie enthalten:

ec2:DescribeAvailability Zones

Diese Berechtigung ist für eine kommende Version erforderlich. Wir werden die Versionshinweise mit weiteren Details aktualisieren, sobald diese Version verfügbar ist.

6 Juni 2023

Für Cloud Volumes ONTAP ist nun die folgende Berechtigung erforderlich:

Kms:GenerateDataKeyWithoutPlaintext

14 Februar 2023

Für BlueXP Tiering ist jetzt die folgende Berechtigung erforderlich:

ec2:DescribeVpcEndpunkte

Azure-Berechtigungen für den Connector

Beim Start der Connector-VM in Azure wird von BlueXP eine benutzerdefinierte Rolle an die VM angehängt, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb des Azure-Abonnements bietet. Der Connector nutzt die Berechtigungen, um API-Aufrufe an mehrere Azure-Services durchzuführen.

Berechtigungen für benutzerdefinierte Rollen

Die unten aufgeführte benutzerdefinierte Rolle stellt die Berechtigungen bereit, die ein Connector zur Verwaltung von Ressourcen und Prozessen in Ihrem Azure-Netzwerk benötigt.

Wenn Sie einen Connector direkt aus BlueXP erstellen, wendet BlueXP diese benutzerdefinierte Rolle automatisch auf den Connector an.

Wenn Sie den Connector über den Azure Marketplace bereitstellen oder den Connector manuell auf einem Linux-Host installieren, müssen Sie die benutzerdefinierte Rolle selbst einrichten.

Informationen zur schrittweisen Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:

- "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"

Außerdem müssen Sie sicherstellen, dass die Rolle auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

```
{
    "Name": "BlueXP Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
```

```
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Storage/checknameavailability/read",
```

```
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
```

```
"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",
```

```
"Microsoft.ContainerService/managedClusters/listClusterUserCredential/acti
on",
                    "Microsoft.ContainerService/managedClusters/read",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

Verwendung von Azure Berechtigungen

In den folgenden Abschnitten wird die Nutzung der Berechtigungen für jeden BlueXP Service beschrieben. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf bereitgestellt werden.

Azure NetApp Dateien

Wenn Sie die BlueXP Klassifizierung zum Scannen von Azure NetApp Files-Daten verwenden, stellt der Connector die folgenden API-Anforderungen:

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

Backup und Recovery

Der Connector macht die folgenden API-Anfragen für das Backup und Recovery von BlueXP:

- Microsoft.Storage/StorageAccounts/Listkeys/Action
- Microsoft.Storage/StorageAccounts/Lesevorgang
- Microsoft.Storage/StorageAccounts/write
- Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang
- Microsoft.Storage/storageAccounts/listeAccountActionSas/Action
- Microsoft.KeyVault/Vaults/read
- Microsoft.KeyVault/Vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen
- Microsoft.Resources/Subskriptionen/resourceGroups/write
- Microsoft.Authorization/Locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressourcen/Bereitstellungen/löschen
- Microsoft.ManagedIdentity/userAssignetIdentities/assign/Action

Der Konnektor stellt folgende API-Anforderungen zur Verfügung, wenn Sie die Funktion Suchen & Wiederherstellen verwenden:

- Microsoft.Synapse/Workspaces/schreiben
- Microsoft.Synapse/Workspaces/Lesen
- Microsoft.Synapse/Workspaces/delete
- Microsoft.Synapse/Register/Aktion
- Microsoft.Synapse/CheckNameVerfügbarkeit/Aktion
- Microsoft.Synapse/Workspaces/OperationStatus/Lesen

- Microsoft.Synapse/Workspaces/Firewall Regeln/lesen
- Microsoft.Synapse/Workspaces/ersetzenAllIpFirewallRegeln/Aktion
- Microsoft.Synapse/Workspaces/OperationResults/read
- Microsoft.Synapse/Workspaces/private EndpointConnectionsGenehmigung/Aktion

Klassifizierung

Bei der Verwendung der BlueXP Klassifizierung macht der Connector die folgenden API-Anfragen.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Compute/locations/operations/read	Ja.	Ja.
Microsoft.Compute/locations/vmSizes/read	Ja.	Ja.
Microsoft.Compute/operations/read	Ja.	Ja.
Microsoft.Compute/virtualMachines/instanceView/read	Ja.	Ja.
Microsoft.Compute/virtualMachines/powerOff/action	Ja.	Nein
Microsoft.Compute/virtualMachines/read	Ja.	Ja.
Microsoft.Compute/virtualMachines/restart/action	Ja.	Nein
Microsoft.Compute/virtualMachines/start/action	Ja.	Nein
Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja.
Microsoft.Compute/virtualMachines/write	Ja.	Nein
Microsoft.Compute/images/read	Ja.	Ja.
Microsoft.Compute/disks/delete	Ja.	Nein
Microsoft.Compute/disks/read	Ja.	Ja.
Microsoft.Compute/disks/write	Ja.	Nein
Microsoft.Storage/ChecknameVerfügbarkeit/Lesevorgang	Ja.	Ja.
Microsoft.Storage/Operations/Lesevorgang	Ja.	Ja.
Microsoft.Storage/StorageAccounts/Listkeys/Action	Ja.	Nein
Microsoft.Storage/StorageAccounts/Lesevorgang	Ja.	Ja.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Storage/StorageAccounts/write	Ja.	Nein
Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang	Ja.	Ja.
Microsoft.Network/networkInterfaces/read	Ja.	Ja.
Microsoft.Network/networkInterfaces/write	Ja.	Nein
Microsoft.Network/networkInterfaces/join/action	Ja.	Nein
Microsoft.Network/networkSecurityGroups/read	Ja.	Ja.
Microsoft.Network/networkSecurityGroups/write	Ja.	Nein
Microsoft.Ressourcen/Abonnements/Standorte/gelesen	Ja.	Ja.
Microsoft.Network/locations/operationResults/read	Ja.	Ja.
Microsoft.Network/locations/operations/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/subnets/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/virtualMachines/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/subnets/join/action	Ja.	Nein
Microsoft.Network/virtualNetworks/subnets/write	Ja.	Nein
Microsoft.Network/routeTables/join/action	Ja.	Nein
Microsoft.Ressourcen/Implementierungen/Betrieb/Lesevorgang	Ja.	Ja.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Ressourcen/Implementierungen/lesen	Ja.	Ja.
Microsoft.Ressourcen/Implementierungen/schreiben	Ja.	Nein
Microsoft.Ressourcen/Ressourcen/Lesen	Ja.	Ja.
Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen	Ja.	Ja.
Microsoft.Resources/Subskriptionen/resourceGroups/delete	Ja.	Nein
Microsoft.Resources/Subskriptionen/resourceGroups/read	Ja.	Ja.
Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen	Ja.	Ja.
Microsoft.Resources/Subskriptionen/resourceGroups/write	Ja.	Nein

Cloud Volumes ONTAP

Der Connector stellt folgende API-Anforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in Azure.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Managen von VMs	Microsoft.Compute/locations/operations/read	Ja.	Ja.	Nein
	Microsoft.Compute/locations/vmSizes/read	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Abonnements/Standorte/gelesen	Ja.	Nein	Nein
	Microsoft.Compute/operations/read	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/instanceView/read	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/powerOff/action	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/read	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/restart/action	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/start/action	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/deallocate/action	Nein	Ja.	Ja.
	Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja.	Nein
	Microsoft.Compute/virtualMachines/write	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/delete	Ja.	Ja.	Ja.
	Microsoft.Ressourcen/Bereitstellungen/löschen	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Implementierung über eine VHD ermöglichen	Microsoft.Compute/images/read	Ja.	Nein	Nein
	Microsoft.Compute/images/write	Ja.	Nein	Nein
Netzwerkschnittstellen im Ziel-Subnetz erstellen und verwalten	Microsoft.Network/networkInterfaces/read	Ja.	Ja.	Nein
	Microsoft.Network/networkInterfaces/write	Ja.	Ja.	Nein
	Microsoft.Network/networkInterfaces/join/action	Ja.	Ja.	Nein
	Microsoft.Network/networkInterfaces/delete	Ja.	Ja.	Nein
Erstellen und Verwalten von Netzwerksicherheitsgruppen	Microsoft.Network/networkSecurityGroups/read	Ja.	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/write	Ja.	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/join/action	Ja.	Nein	Nein
	Microsoft.Network/networkSecurityGroups/delete	Nein	Ja.	Ja.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Abrufen der Netzwerkinformationen zu Regionen, Ziel-vnet und Subnetz, und Hinzufügen der VMs zu VNets	Microsoft.Network/locations/operationResults/read	Ja.	Ja.	Nein
	Microsoft.Network/locations/operations/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/read	Ja.	Nein	Nein
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja.	Nein	Nein
	Microsoft.Network/virtualNetworks/subnets/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/virtualMachines/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/subnets/join/action	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Ressourcengruppen	Microsoft.Ressourcen/Implementierungen/Betrieb/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Implementierungen/lesen	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Implementierungen/schreiben	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Ressourcen/Lesen	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen	Ja.	Ja.	Nein
	Microsoft.Resources/Subskriptionen/resourceGroups/delete	Ja.	Ja.	Ja.
	Microsoft.Resources/Subskriptionen/resourceGroups/read	Nein	Ja.	Nein
	Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen	Ja.	Ja.	Nein
	Microsoft.Resources/Subskriptionen/resourceGroups/write	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Azure-Storage-Konten und -Festplatten managen	Microsoft.Compute/disks/read	Ja.	Ja.	Ja.
	Microsoft.Compute/disks/write	Ja.	Ja.	Nein
	Microsoft.Compute/disks/delete	Ja.	Ja.	Ja.
	Microsoft.Storage/CheckknameVerfügbarkeit/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Storage/Operations/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Storage/StorageAccounts/Listkeys/Action	Ja.	Ja.	Nein
	Microsoft.Storage/StorageAccounts/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Storage/StorageAccounts/delete	Nein	Ja.	Ja.
	Microsoft.Storage/StorageAccounts/write	Ja.	Ja.	Nein
	Microsoft.Speicherung/Verwendung/Lesen	Nein	Ja.	Nein
Ermöglichen von Backups auf Blob Storage und Verschlüsselung von Storage-Konten	Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.KeyVault/Vaults/read	Ja.	Ja.	Nein
	Microsoft.KeyVault/Vaults/accessPolicies/write	Ja.	Ja.	Nein
Vnet-Service-Endpunkte für Daten-Tiering aktivieren	Microsoft.Network/virtualNetworks/subnets/write	Ja.	Ja.	Nein
	Microsoft.Network/routeTables/join/action	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und managen Sie über Azure gemanagte Snapshots	Microsoft.Compute/snapshots/write	Ja.	Ja.	Nein
	Microsoft.Compute/snapshots/read	Ja.	Ja.	Nein
	Microsoft.Compute/snapshots/delete	Nein	Ja.	Ja.
	Microsoft.Compute/disks/beginGetAccess/action	Nein	Ja.	Nein
Erstellung und Management von Verfügbarkeitsgruppen	Microsoft.Compute/availabilitySets/write	Ja.	Nein	Nein
	Microsoft.Compute/availabilitySets/read	Ja.	Nein	Nein
Programmatische Implementierungen über den Markt ermöglichen	Microsoft.MarketplaceOrdering/offertypes/Publisher/Offers/Plans/Agreements/read	Ja.	Nein	Nein
	Microsoft.MarketplaceOrdering/offertypes/Publisher/Offers/Plans/Agreements/write	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Managen Sie einen Load Balancer für HA-Paare	Microsoft.Network/loadBalancers/read	Ja.	Ja.	Nein
	Microsoft.Network/loadBalancers/write	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/delete	Nein	Ja.	Ja.
	Microsoft.Network/loadBalancers/backendAddressPools/read	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Ja.	Ja.	Nein
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/probes/read	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/probes/join/action	Ja.	Nein	Nein
Verwaltung von Sperren auf Azure Festplatten aktivieren	Microsoft.Authorization/Locks/*	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren Sie private Endpunkte für HA-Paare, wenn sich keine Verbindung außerhalb des Subnetzes befindet	Microsoft.Network/privateEndpoints/write	Ja.	Ja.	Nein
	Microsoft.Speicherung/Speicherkonten/PrivateEndpointConnectionsGenehmigung/Aktion	Ja.	Nein	Nein
	Microsoft.Storage/StorageAccounts/private EndpointConnections/Lesevorgang	Ja.	Ja.	Ja.
	Microsoft.Network/privateEndpoints/read	Ja.	Ja.	Ja.
	Microsoft.Network/privateDnsZones/write	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/join/action	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/A/write	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/read	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Ja.	Ja.	Nein
Erforderlich für einige VM-Bereitstellungen, abhängig von der zugrunde liegenden physischen Hardware	Microsoft.Ressourcen/Implementierungen/OperationStatuses/read	Ja.	Ja.	Nein
Entfernen von Ressourcen aus einer Ressourcengruppe bei Ausfall oder Löschen der Bereitstellung	Microsoft.Network/privateEndpoints/delete	Ja.	Ja.	Nein
	Microsoft.Compute/availabilitySets/delete	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Nutzen Sie die API, wenn Sie die vom Kunden gemanagten Schlüssel verwenden	Microsoft.Compute/diskEncryptionSets/read	Ja.	Ja.	Ja.
	Microsoft.Compute/diskEncryptionSets/write	Ja.	Ja.	Nein
	Microsoft.KeyVault/Vaults/Deploy/Action	Ja.	Nein	Nein
	Microsoft.Compute/diskEncryptionSets/delete	Ja.	Ja.	Ja.
Konfigurieren Sie eine Applikationssicherheitsgruppe für ein HA-Paar, um die HA Interconnect- und Cluster-Netzwerk-NICs zu isolieren	Microsoft.Network/applicationSecurityGroups/write	Nein	Ja.	Nein
	Microsoft.Network/applicationSecurityGroups/read	Nein	Ja.	Nein
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Nein	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/securityRules/write	Ja.	Ja.	Nein
	Microsoft.Network/applicationSecurityGroups/delete	Nein	Ja.	Ja.
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Nein	Ja.	Ja.
Lesen, Schreiben und Löschen von Tags im Zusammenhang mit Cloud Volumes ONTAP Ressourcen	Microsoft.Ressourcen/Tags/lesen	Nein	Ja.	Nein
	Microsoft.Ressourcen/Tags/schreiben	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Tags/delete	Ja.	Nein	Nein
Verschlüsselung von Speicherkonten bei der Erstellung	Microsoft.ManagedIdentity/userAssignetIdentities/assign/Action	Ja.	Ja.	Nein

Edge-Caching

Der Connector macht die folgenden API-Anfragen, wenn Sie BlueXP Edge Caching verwenden:

- Microsoft.Insights/Metriken/Lesevorgang
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressourcen/Bereitstellungen/löschen

Kubernetes

Der Connector stellt folgende API-Anforderungen zur Erkennung und Verwaltung von Clustern in Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen
- Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen
- Microsoft.ContainerService/manageCluster/lesen
- Microsoft.ContainerService/verwaltungCluster/listClusterUserCredential/Action

Tiering

Der Connector macht die folgenden API-Anfragen, wenn Sie BlueXP Tiering einrichten.

- Microsoft.Storage/StorageAccounts/Listkeys/Action
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen

Der Connector stellt folgende API-Anforderungen für den täglichen Betrieb.

- Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang
- Microsoft.Storage/StorageAccounts/Management Policies/read
- Microsoft.Storage/StorageAccounts/Management Richtlinien/schreiben
- Microsoft.Storage/StorageAccounts/Lesevorgang

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

5 Dezember 2023

Die folgenden Berechtigungen für das BlueXP Backup und Recovery beim Backup von Volume-Daten auf Azure Blob Storage sind nicht mehr erforderlich:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Diese Berechtigungen sind für andere BlueXP Storage-Services erforderlich, sodass sie weiterhin für den Connector relevant sind, wenn Sie diese anderen Storage-Services nutzen.

12 Mai 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für das Cloud Volumes ONTAP-Management erforderlich sind:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da sie nicht mehr erforderlich sind:

- Microsoft.Storage/StorageAccounts/blobServices/Container/write
- Microsoft.Network/publicIPAddresses/delete

23 März 2023

Die Berechtigung „Microsoft.Storage/storageAccounts/delete“ wird für die BlueXP Klassifizierung nicht mehr benötigt.

Diese Genehmigung ist für Cloud Volumes ONTAP weiterhin erforderlich.

5. Januar 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt:

- Microsoft.Storage/storageAccounts/listeAccountActionSas/Action
- Microsoft.Synapse/Workspaces/private EndpointConnectionsGenehmigung/Aktion

  Diese Berechtigungen sind für das Backup und Recovery von BlueXP erforderlich.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Diese Berechtigung ist für die Cloud Volumes ONTAP-Bereitstellung erforderlich.

Google Cloud-Berechtigungen für den Connector

Für Aktionen in Google Cloud sind für BlueXP Berechtigungen erforderlich. Diese Berechtigungen sind Bestandteil einer benutzerdefinierten Rolle, die NetApp zur

Verfügung stellt. Vielleicht möchten Sie wissen, was BlueXP mit diesen Berechtigungen macht.

Berechtigungen für Dienstkonto

Die unten abgebildete benutzerdefinierte Rolle bietet die Berechtigungen, die ein Connector zur Verwaltung von Ressourcen und Prozessen in Ihrem Google Cloud-Netzwerk benötigt.

Sie müssen diese benutzerdefinierte Rolle auf ein Servicekonto anwenden, das mit der Connector-VM verbunden ist.

- "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"

Außerdem müssen Sie sicherstellen, dass die Rolle auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
```

```
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
```

```
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Verwendung von Google Cloud-Berechtigungen

Aktionen	Zweck
- Compute.Disks.create - Compute.Disks.createSnapshot - compute.disks.delete - Compute.Disks.get - Compute.Disks.list - compute.disks.setLabels - compute.disks.use	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.
- Compute.Firewalls.create - compute.firewalls.delete - Compute.Firewalls.get - Compute.Firewalls.list	Um Firewall-Regeln für Cloud Volumes ONTAP zu erstellen.
- Compute.globalOperations.get	Um den Status von Vorgängen anzuzeigen.

Aktionen	Zweck
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Um Images für VM-Instanzen zu erhalten.
- compute.instances.attachDisk - compute.instances.detachDisk	Zum Verbinden und Trennen von Festplatten mit Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Um Cloud Volumes ONTAP VM-Instanzen zu erstellen und zu löschen.
- compute.instances.get	Um VM-Instanzen aufzulisten.
- compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.
- compute.instances.list	Um die Liste der Instanzen in einer Zone abzurufen.
- compute.instances.setDeletionProtection	So legen Sie den Löschschutz für die Instanz fest:
- compute.instances.setLabels	So fügen Sie Etiketten hinzu:
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.
- compute.instances.setMetadata	Um Metadaten hinzuzufügen.
- compute.instances.setTags	Um Tags für Firewall-Regeln hinzuzufügen.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Um Cloud Volumes ONTAP zu starten und anzuhalten.
- Compute.machineTypes.get	Um die Anzahl der Kerne zu erhalten, um qouten zu überprüfen.
- compute.projects.get	Zur Unterstützung mehrerer Projekte.
- Compute.Snapshots.create - compute.snapshots.delete - Compute.Snapshots.get - Compute.Snapshots.list - compute.snapshots.setLabels	Um persistente Festplatten-Snapshots zu erstellen und zu managen.
- compute.networks.get - compute.networks.list - Compute.Regions.get - Compute.Regions.list - Compute.subnetworks.get - Compute.subnetworks.list - Compute.zoneOperations.get - Compute.Zones.get - Compute.Zones.list	Um die Netzwerkinformationen zu erhalten, die für die Erstellung einer neuen Instanz einer Cloud Volumes ONTAP Virtual Machine erforderlich sind.

Aktionen	Zweck
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - Deploymentmanager.Manifeste.get - Deplomentmanager.Manifeste.list - Deploymentmanager.Operations.get - Deplomentmanager.Operations.list - Deploymentmanager.Resources.get - Deploymentmanager.Resources.list - Deploymentmanager.typProviders.get - Deplomentmanager.typProviders.list - Deplomentmanager.types.get - Deplomentmanager.types.list	Um die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereitzustellen.
- Logging.logEinträge.list - Logging.privateLogEinträge.list	Zum Abrufen von Stack-Protokolllaufwerken.
- resourcemanager.projects.get	Zur Unterstützung mehrerer Projekte.
- Storage.Buckets.create - storage.buckets.delete - Storage.Buckets.get - Storage.Buckets.list - Storage.Buckets.Update	Zur Erstellung und Verwaltung eines Google Cloud Storage Buckets für Daten-Tiering
- cloudkms.cryptoKeyVersions.useToEncrypt - Cloudkms.cryptkeys.get - Cloudkms.cryptkeys.list - Cloudkms.Keyrings.list	Verwenden von vom Kunden gemanagten Verschlüsselungen aus dem Cloud-Verschlüsselungsmanagement-Service mit Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - Storage.objects.get - Storage.objects.list	So legen Sie ein Servicekonto für die Cloud Volumes ONTAP-Instanz fest: Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket.
- Compute.Addresses.list	So rufen Sie die Adressen in einer Region ab, wenn Sie ein HA-Paar bereitstellen.
- Compute.backendServices.create - Compute.regionBackendServices.create - Compute.regionBackendServices.get - Compute.regionBackendServices.list	Um einen Backend-Service für die Verteilung von Datenverkehr in einem HA-Paar zu konfigurieren
- compute.networks.updatePolicy	So wenden Sie Firewall-Regeln auf die VPCs und Subnetze für ein HA-Paar an.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Um die BlueXP Klassifizierung zu aktivieren.

Aktionen	Zweck
- Container.Clusters.get - Container.Clusters.list	Um Kubernetes Cluster zu erkennen, die in der Google Kubernetes Engine ausgeführt werden.
- compute.instanceGroups.get - Compute.addresses.get - compute.instances.updateNetworkInterface	Um Storage VMs auf Cloud Volumes ONTAP HA-Paaren zu erstellen und zu managen.
- Monitoring.timeseries.list - Storage.Buckets.getIamPolicy	Um Informationen zu Google Cloud Storage Buckets zu erhalten.
- Cloudkms.cryptkeys.get - Cloudkms.cryptkeys.getIamPolicy - Cloudkms.cryptkeys.list - cloudkms.cryptoKeys.setIamPolicy - Cloudkms.Schlüsselanhänger.get - Cloudkms.Keyrings.getIamPolicy - Cloudkms.Keyrings.list - cloudkms.keyRings.setIamPolicy	So wählen Sie im BlueXP Aktivierungsassistenten für Backup und Recovery eigene vom Kunden gemanagte Schlüssel aus, statt die standardmäßigen, von Google gemanagten Schlüssel zu verwenden.

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

6 Februar 2023

Die folgende Berechtigung wurde dieser Richtlinie hinzugefügt:

- compute.instances.updateNetworkInterface

Diese Erlaubnis ist für Cloud Volumes ONTAP erforderlich.

27 Januar 2023

Die Richtlinie hat folgende Berechtigungen hinzugefügt:

- Cloudkms.KryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- Cloudkms.Schlüsselanhänger.get
- Cloudkms.Keyrings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Diese Berechtigungen sind für das Backup und Recovery von BlueXP erforderlich.

Ports

Regeln für die Connector-Sicherheitsgruppe in AWS

Für die AWS Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen

Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der BlueXP Klassifizierungsinstanz
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"
TCP	9060, 9061	BlueXP Klassifizierung und BlueXP Backup und Recovery in Regierungsregionen lassen sich aktivieren und nutzen.

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS, ONTAP, BlueXP Klassifizierung und das Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP HA Mediator	Kommunikation mit dem ONTAP HA Mediator
	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Regeln für die Connector-Sicherheitsgruppe in Azure

Für die Azure-Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der BlueXP Klassifizierungsinstanz

Protokoll	Port	Zweck
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"
TCP	9060, 9061	BlueXP Klassifizierung und BlueXP Backup und Recovery in Regierungsregionen lassen sich aktivieren und nutzen.

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe zu Azure, zu ONTAP, zur BlueXP Klassifizierung und zum Senden von AutoSupport Nachrichten an NetApp

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Connector-Firewall-Regeln in Google Cloud

Die Google Cloud Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"

Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector öffnen den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector enthalten die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an Google Cloud, an ONTAP, an BlueXP Klassifizierung und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Anschlüsse für den On-Prem Connector

Der Connector verwendet *Inbound*-Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird. Möglicherweise müssen Sie diese Ports zu Planungszwecken verwenden.

Diese Inbound Regeln gelten für alle BlueXP Implementierungsmodelle.

Protokoll	Port	Zweck
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Wissen und Support

Für den Support anmelden

Für den Support von BlueXP und seinen Storage-Lösungen und Services ist eine Support-Registrierung erforderlich. Um wichtige Workflows für Cloud Volumes ONTAP Systeme zu ermöglichen, ist außerdem eine Support-Registrierung erforderlich.

Durch die Registrierung für den Support wird die NetApp-Unterstützung für einen Fileservice eines Cloud-Providers nicht aktiviert. Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren Ihres BlueXP-Konto-ID-Support-Abonnements (Ihre 20-stellige Seriennummer 960xxxxxxxxx auf der Seite Support-Ressourcen in BlueXP).

  Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

  Diese Seriennummern werden als *PAYGO Seriennummern* bezeichnet und werden zum Zeitpunkt der Cloud Volumes ONTAP Implementierung von BlueXP generiert.

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen. Die Registrierung ist abgeschlossen, indem wie unten beschrieben Konten der NetApp Support Website (NSS) zu BlueXP hinzugefügt werden.

Registrieren Sie Ihr BlueXP Konto für NetApp Support

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer in Ihrem BlueXP Konto ein NetApp Support Site Konto mit seinen BlueXP Anmeldedaten verknüpfen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

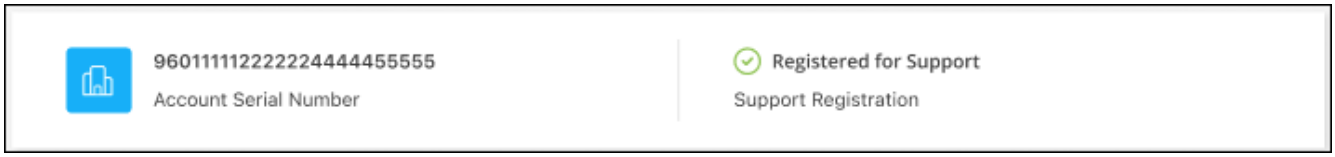
Bestandskunde mit NSS-Konto

Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Eingabeaufforderung für die NetApp-Support-Website (NSS)-Authentifizierung.
4. Um zu bestätigen, dass die Registrierung erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihr Konto für Support registriert ist.

   Beachten Sie, dass andere BlueXP Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie ihrem BlueXP Login kein NetApp Support Site Konto zugeordnet haben. Das bedeutet jedoch nicht, dass Ihr BlueXP Konto nicht für den Support registriert ist. Solange ein Benutzer im Konto diese Schritte befolgt hat, wurde Ihr Konto registriert.

Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über vorhandene Lizenzen und Seriennummern sowie *No* NSS Konto verfügen, müssen Sie ein NSS Konto erstellen und es Ihren BlueXP Anmeldedaten zuordnen.

Schritte

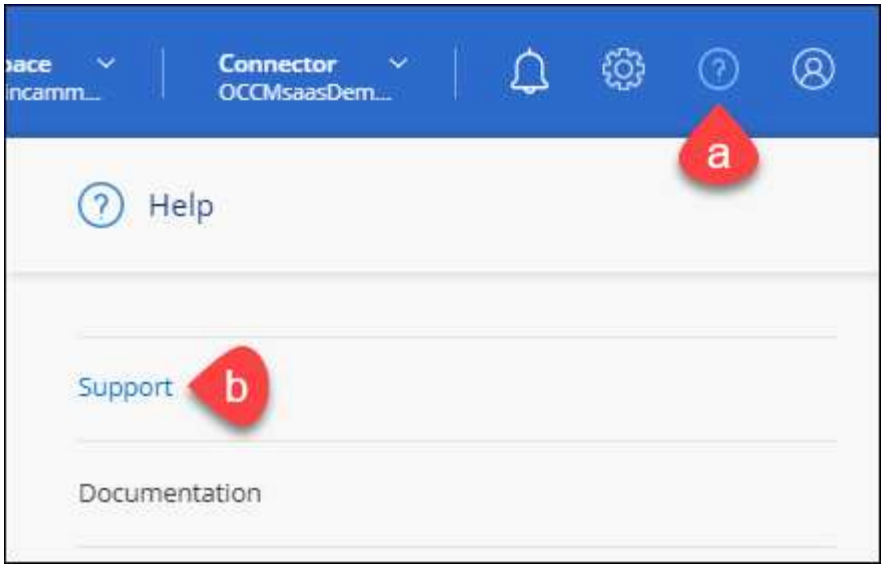
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.
2. Ordnen Sie Ihr neues NSS-Konto Ihrer BlueXP Anmeldung zu, indem Sie die unter aufgeführten Schritte durchführen Bestandskunde mit NSS-Konto.

Neu bei NetApp

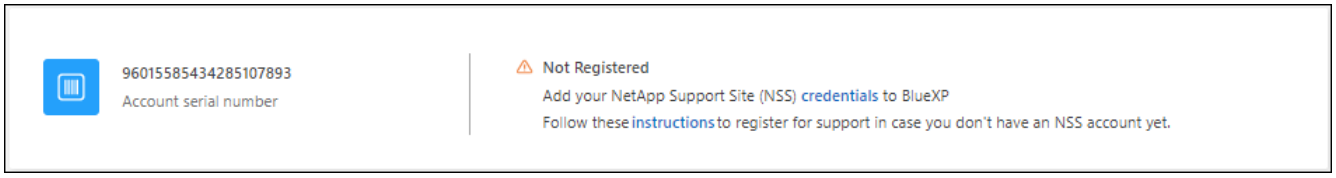
Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

Schritte

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



2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.



3. Navigieren Sie zu "Die Support-Registrierungs-Website von NetApp" Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

   Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

7. Bestätigen Sie die Aktion in der E-Mail.

   Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch wird die Kontobearbeitung beschleunigt.

Nachdem Sie fertig sind

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Wenn Sie über Ihren NetApp Support Site Account verfügen, ordnen Sie das Konto Ihrer BlueXP Anmeldung zu, indem Sie die Schritte unter ausführen Bestandskunde mit NSS-Konto.

Verknüpfen von NSS-Anmeldeinformationen für den Cloud Volumes ONTAP-Support

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu ermöglichen, müssen die Zugangsdaten für die NetApp Support Website mit Ihrem BlueXP Konto verknüpft werden:

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

  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.

- 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.

- Aktualisieren der Cloud Volumes ONTAP Software auf die neueste Version

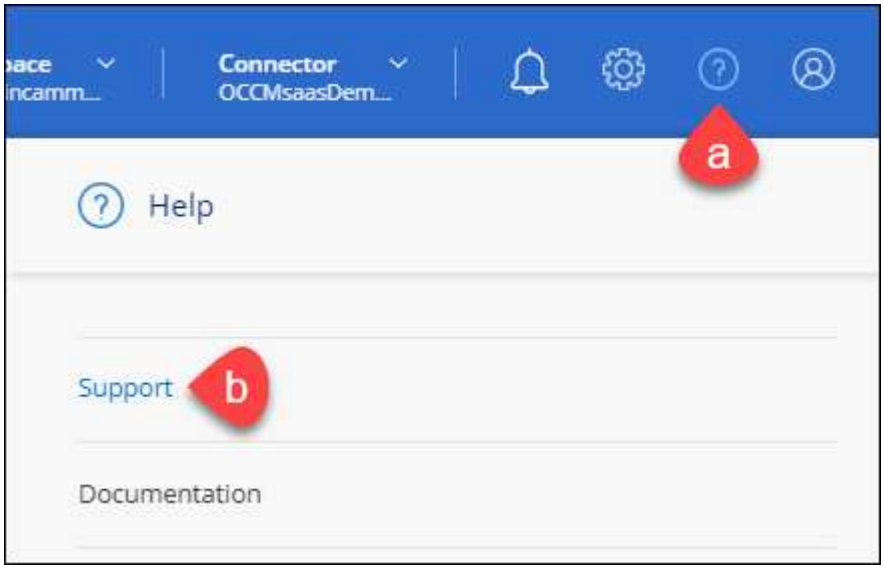
Das Zuordnen der NSS-Anmeldedaten zu Ihrem BlueXP Konto unterscheidet sich von dem NSS-Konto, das mit einer BlueXP Benutzeranmeldung verknüpft ist.

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

- 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.

Holen Sie sich Hilfe

NetApp bietet Unterstützung für BlueXP und seine Cloud-Services auf unterschiedliche Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Unterstützung für Fileservices von Cloud-Providern

Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Cloud Volumes Service für Google Cloud"

Wenn Sie technischen Support für BlueXP und seine Storage-Lösungen und -Services erhalten möchten, nutzen Sie die unten beschriebenen Support-Optionen.

Nutzen Sie Self-Support-Optionen

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- Dokumentation

  Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- "Communitys"

  Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** nutzen zu können, müssen Sie zunächst Ihre Anmeldedaten für die NetApp Support-Website mit Ihren BlueXP Anmeldedaten verknüpfen. "Managen Sie Zugangsdaten für Ihre BlueXP Anmeldung".
- Wenn Sie einen Fall für ein ONTAP System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer des Systems verknüpft sein.

Schritte

1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie auf der Seite **Ressourcen** eine der verfügbaren Optionen unter Technischer Support:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket mit einem NetApp-Supportspezialisten zu öffnen:

      - **Service**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
      - **Arbeitsumgebung**: Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

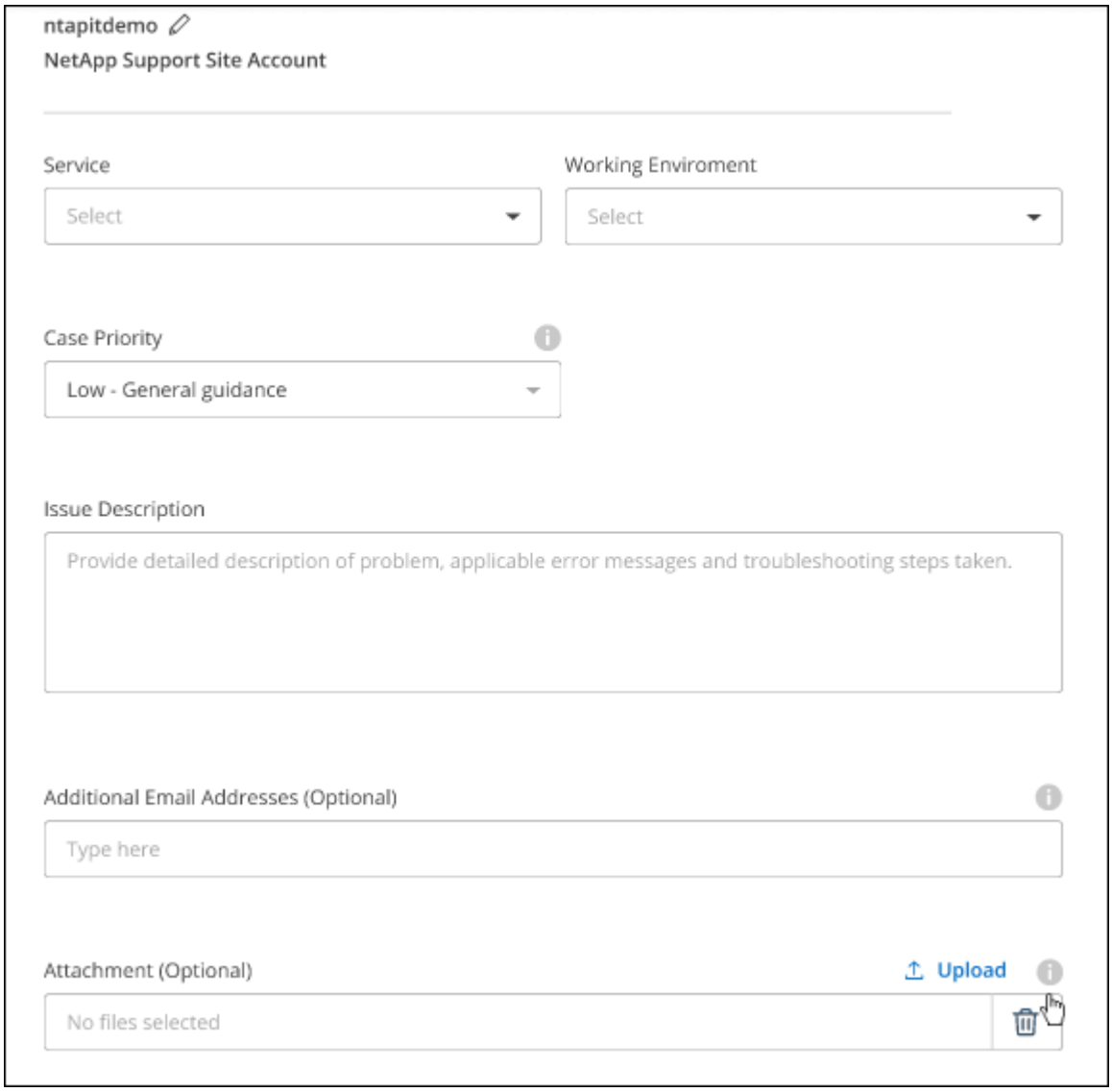
        Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Case Priority**: Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

  Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.
- **Anhang (optional)**: Laden Sie bis zu fünf Anhänge nacheinander hoch.

  Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nachdem Sie fertig sind

Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall und macht Sie umgehend mit.

Um eine Historie deiner Support-Fälle anzuzeigen, kannst du **Einstellungen > Chronik** auswählen und nach Aktionen mit dem Namen „Support-Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Service zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh 960xxxx) oder Seriennummer der Arbeitsumgebung. Sie können Hilfe mit einer der folgenden Optionen anfordern:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter https://mysupport.netapp.com/site/help

Managen Ihrer Support-Cases (Vorschau)

Sie können aktive und gelöste Support-Cases direkt über BlueXP anzeigen und managen. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Fälle verwalten.

Case Management ist als Vorschau verfügbar. Wir planen, diese Erfahrungen weiter zu verbessern und in zukünftigen Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Ihr Feedback über den Product-Chat.

Beachten Sie Folgendes:

- Das Case-Management-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der Fälle, die in den letzten 3 Monaten durch das von Ihnen angegebene NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto an.

  Die Ergebnisse in der Tabelle geben die Fälle in Bezug auf die ausgewählte Ansicht wieder.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten nur Sortierfunktionen.

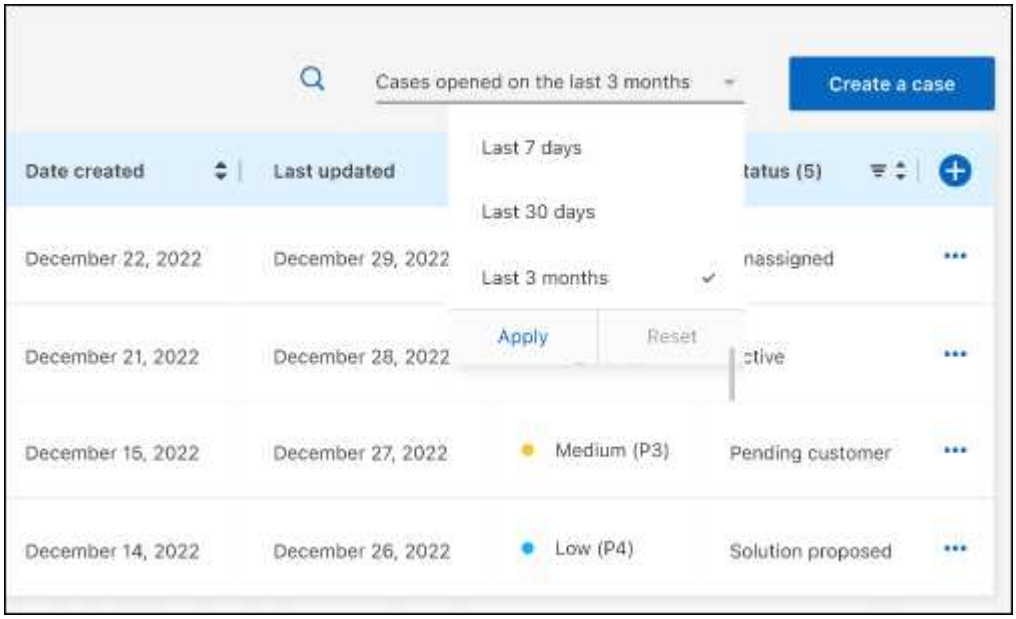
  Weitere Informationen erhalten Sie in den Schritten unten.
- Auf Fallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Geschlossen“ oder „Geschlossen“ befindet.

Schritte

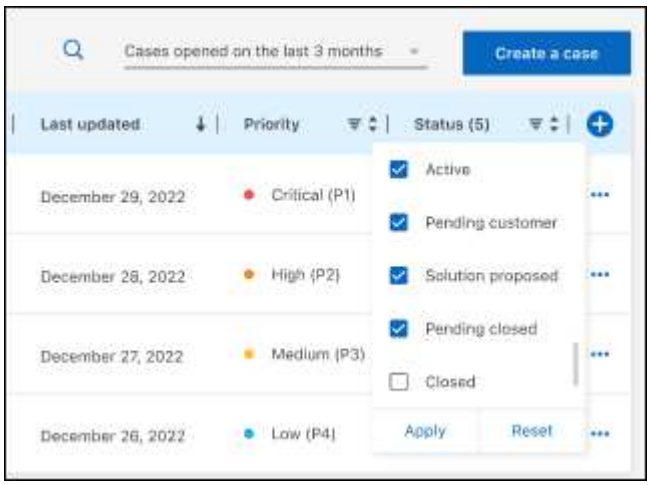
1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie **Case Management** aus und fügen Sie bei Aufforderung Ihr NSS-Konto zu BlueXP hinzu.

   Auf der Seite **Case Management** werden offene Fälle im Zusammenhang mit dem NSS-Konto angezeigt, das mit Ihrem BlueXP Benutzerkonto verknüpft ist. Dies ist das gleiche NSS-Konto, das oben auf der Seite **NSS Management** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:

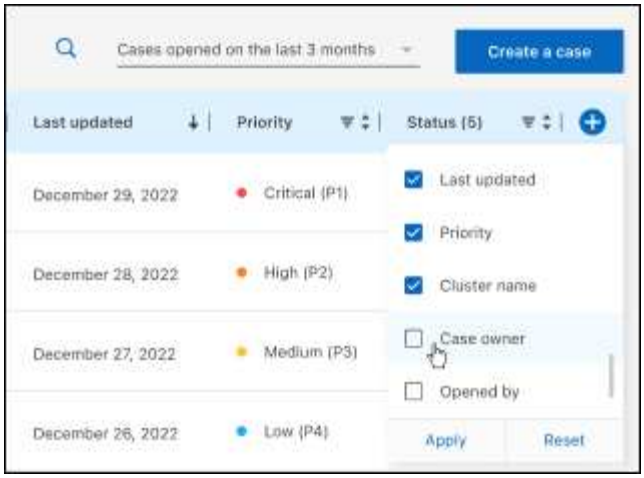
- Wählen Sie unter **Vorgänge der Organisation Ansicht** aus, um alle mit Ihrem Unternehmen verbundenen Fälle anzuzeigen.
- Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.



- Filtern Sie den Inhalt der Spalten.



- Ändern Sie die Spalten, die in der Tabelle angezeigt werden, indem Sie auswählen Und wählen Sie dann die Spalten, die Sie anzeigen möchten.

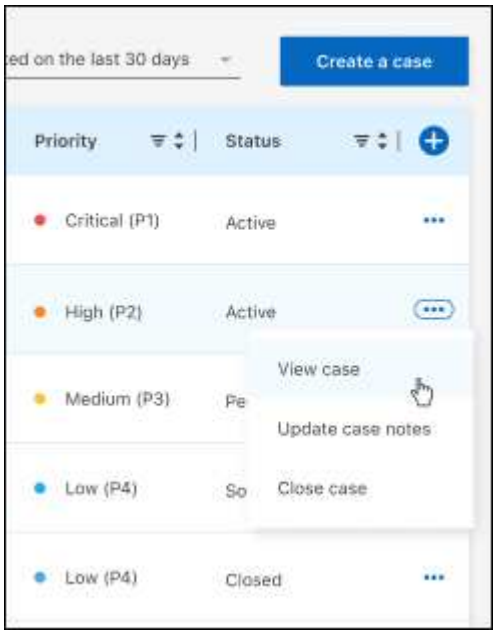


4. Managen Sie einen bestehenden Fall, indem Sie auswählen ••• Und eine der verfügbaren Optionen auswählen:

   - **Fall anzeigen**: Vollständige Details zu einem bestimmten Fall anzeigen.
   - **Aktennotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um maximal fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Folgende Dateierweiterungen werden unterstützt: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

   - **Fall schließen**: Geben Sie Einzelheiten darüber an, warum Sie den Fall schließen und wählen Sie **Fall schließen**.



Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis für BlueXP"