Los geht's

Setup and administration

NetApp
April 26, 2024

Inhalt

Los geht’s . . . 1
Lernen Sie die Grundlagen kennen . . . 1
Beginnen Sie mit dem Standardmodus . . . 24
Beginnen Sie mit dem eingeschränkten Modus . . . 137
Starten Sie mit dem privaten Modus . . . 172
Melden Sie sich bei BlueXP an . . . 192

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

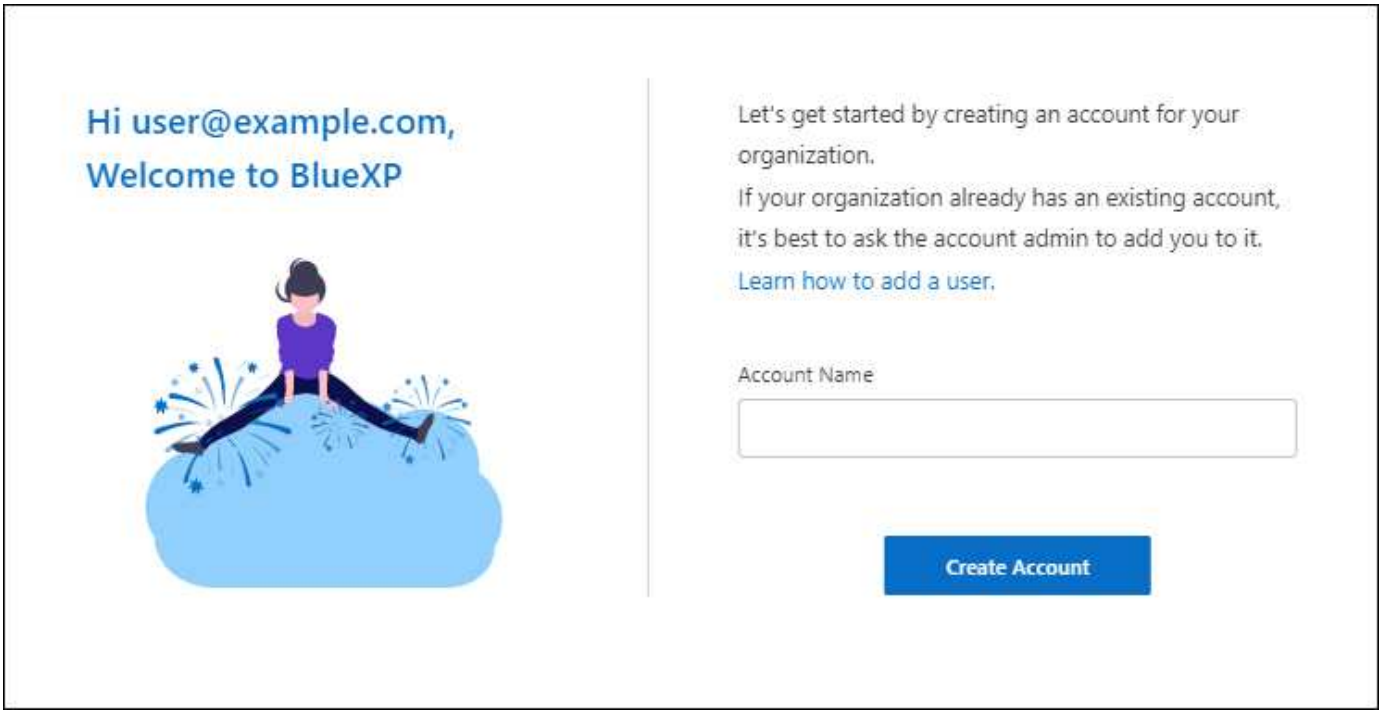
Ein unabhängiger zertifizierter Wirtschaftsprüfer und Wirtschaftsprüfer prüfte BlueXP und bestätigte, dass es SOC 2 Typ 2-Berichte basierend auf den geltenden Trust Services-Kriterien erreichte.

"SOC 2-Berichte von NetApp anzeigen"

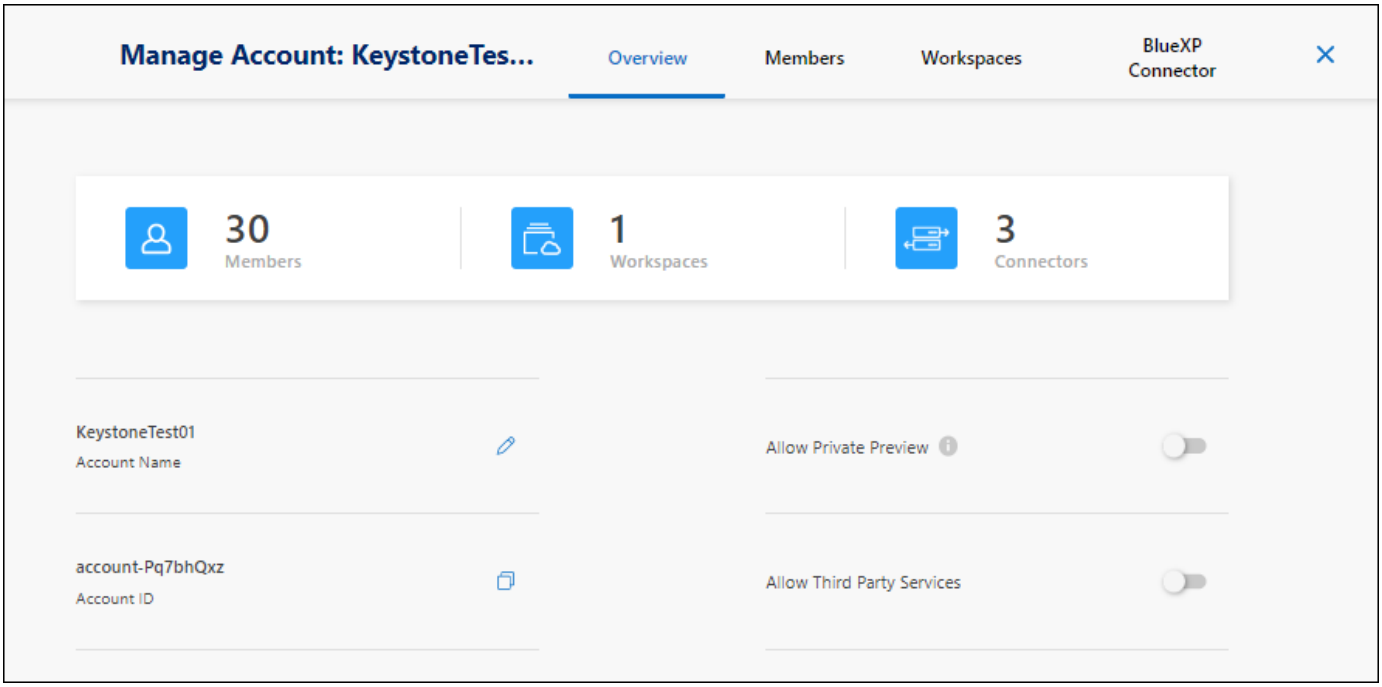
Mehr zu BlueXP Accounts

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".

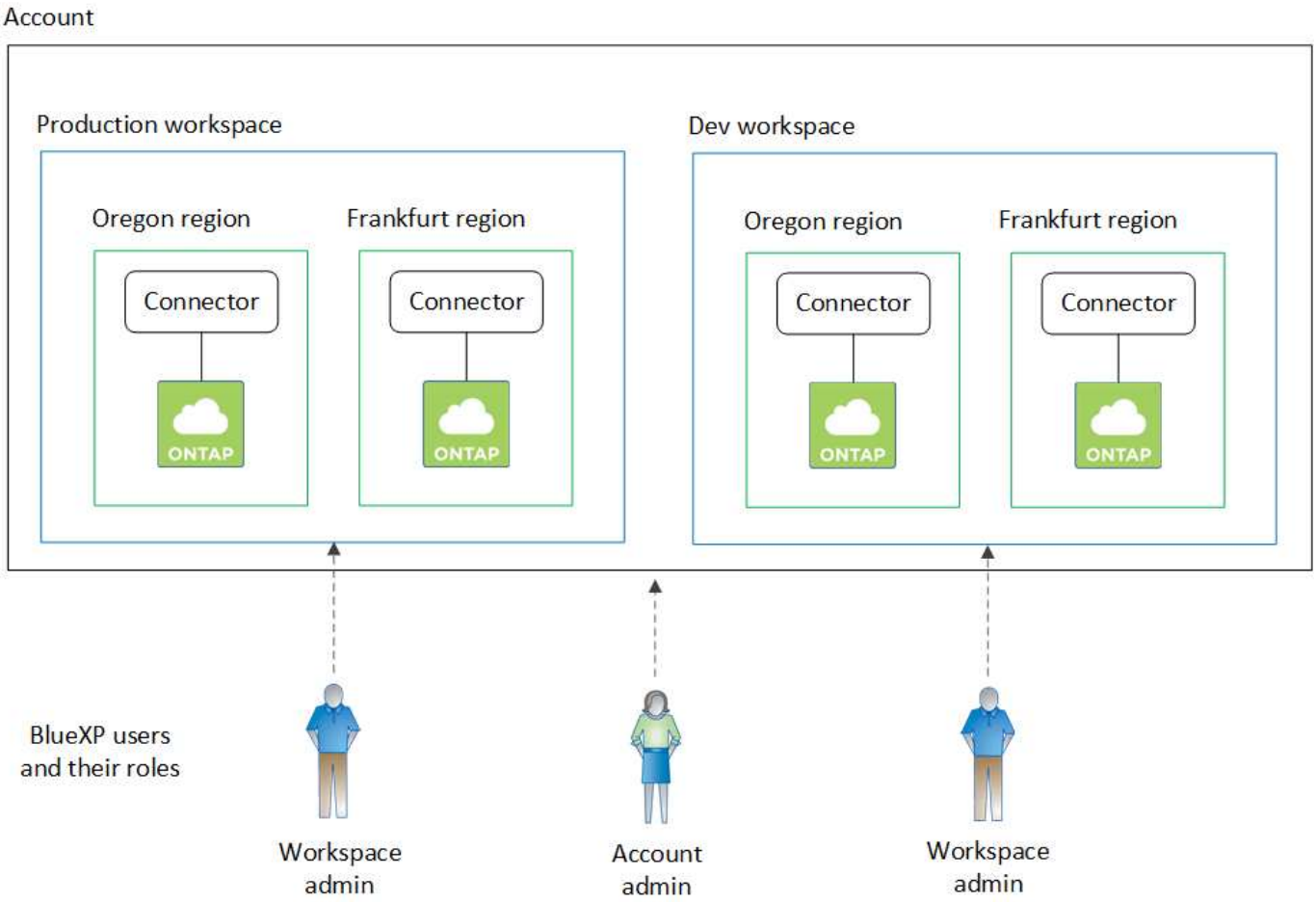
Beispiele

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

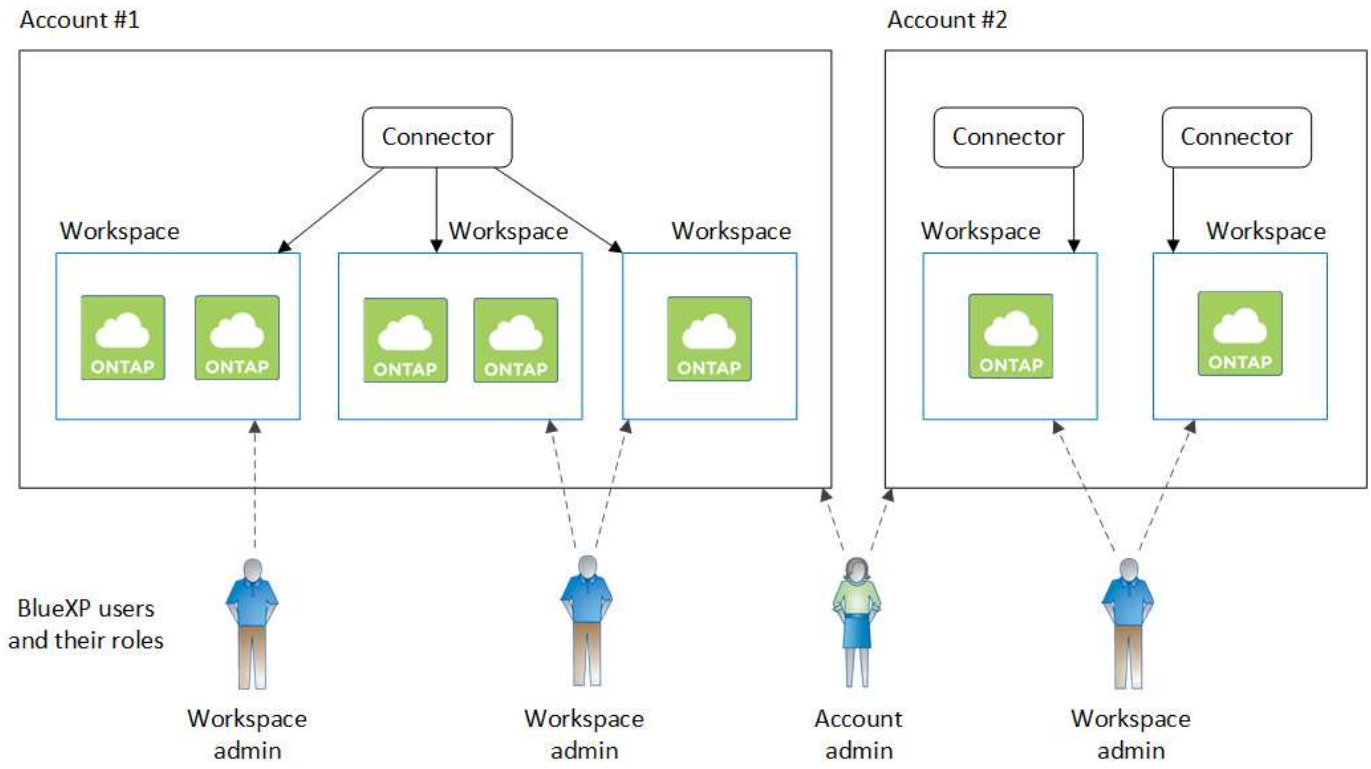
Das folgende Beispiel zeigt ein Konto, das zwei Arbeitsbereiche zum Erstellen isolierter Umgebungen verwendet. Der erste Arbeitsbereich ist für eine Produktionsumgebung und der zweite für eine Entwicklungsumgebung.



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"

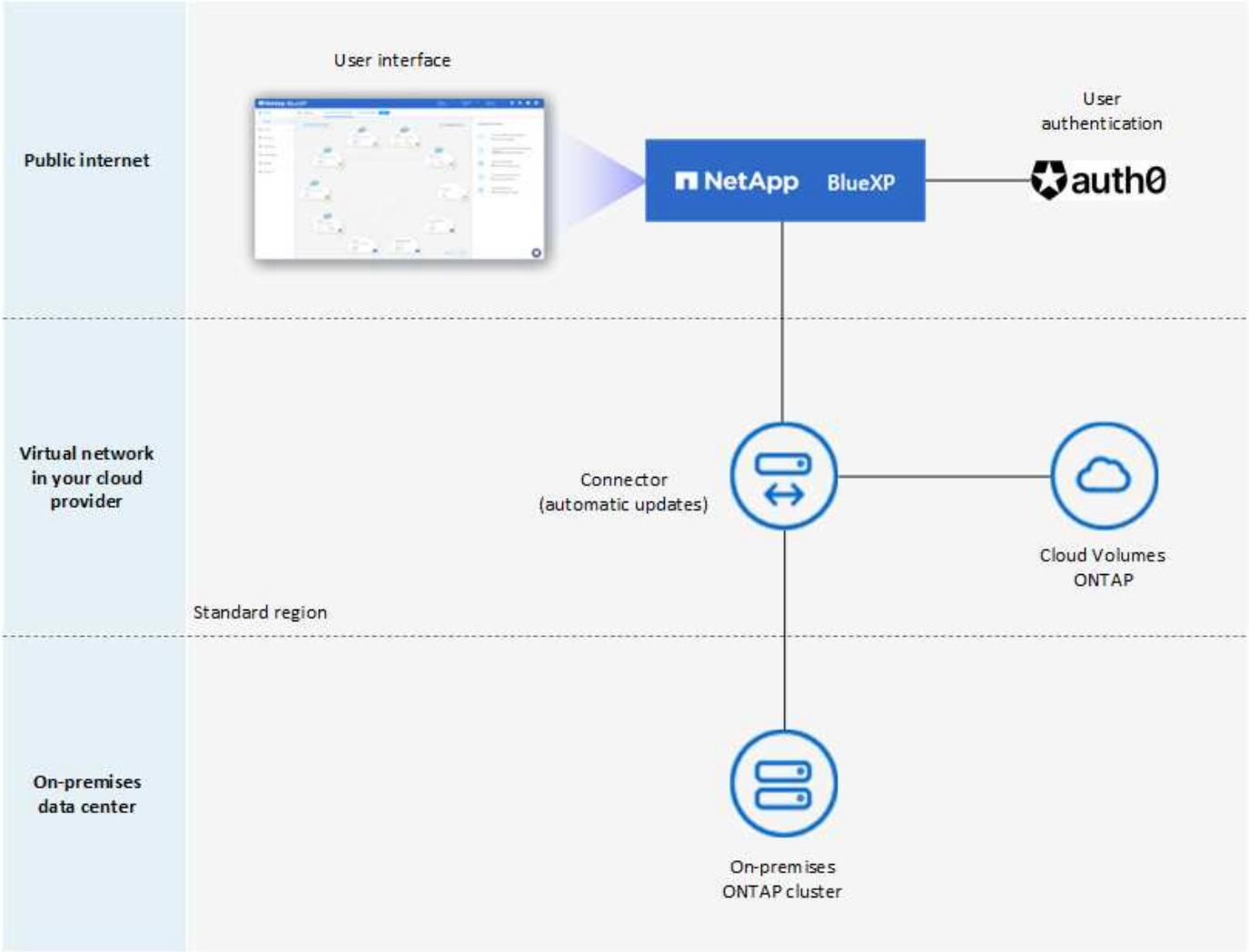
Die folgende Tabelle enthält einen Vergleich dieser Modi.

	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.

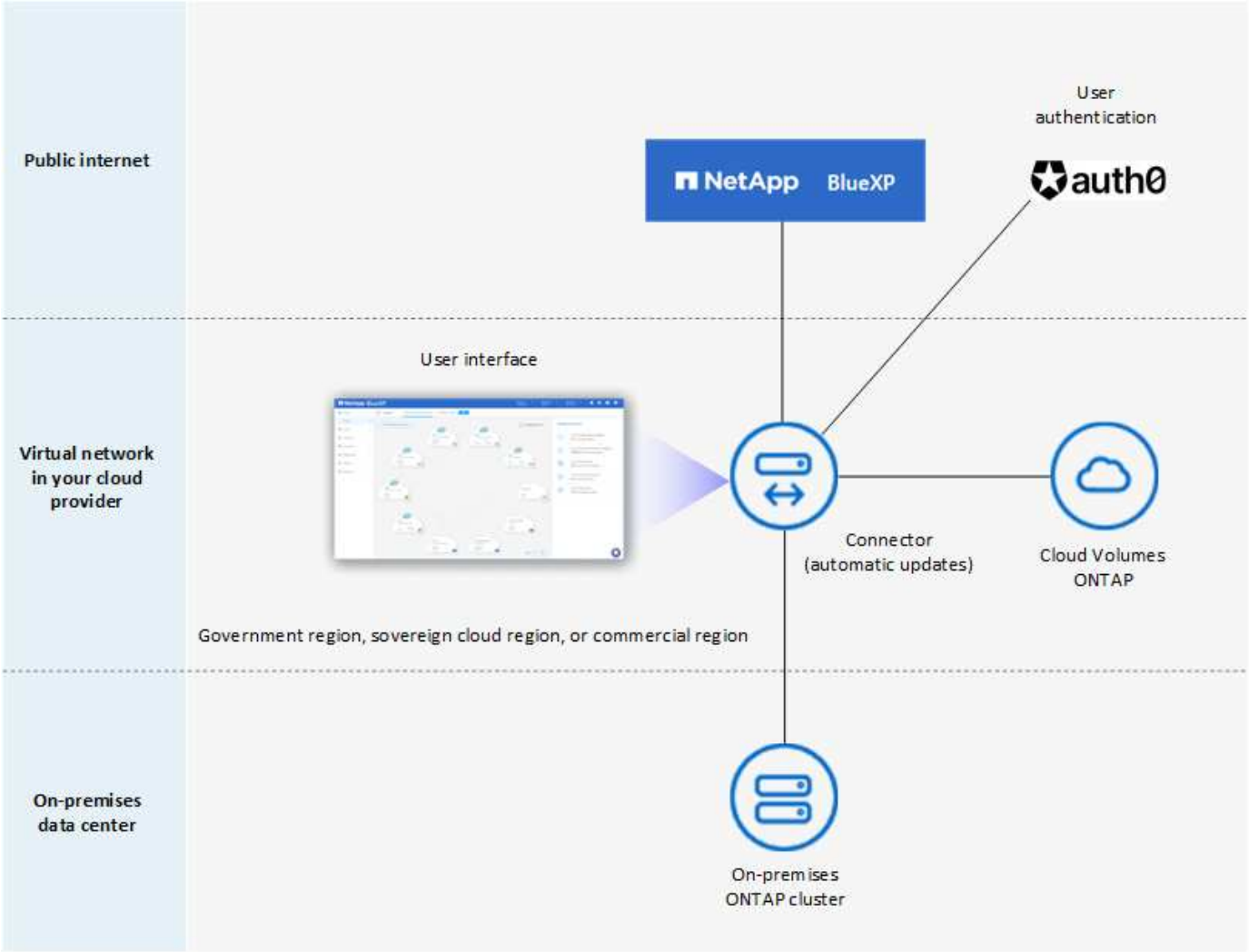
Erste Schritte mit dem Standardmodus

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.

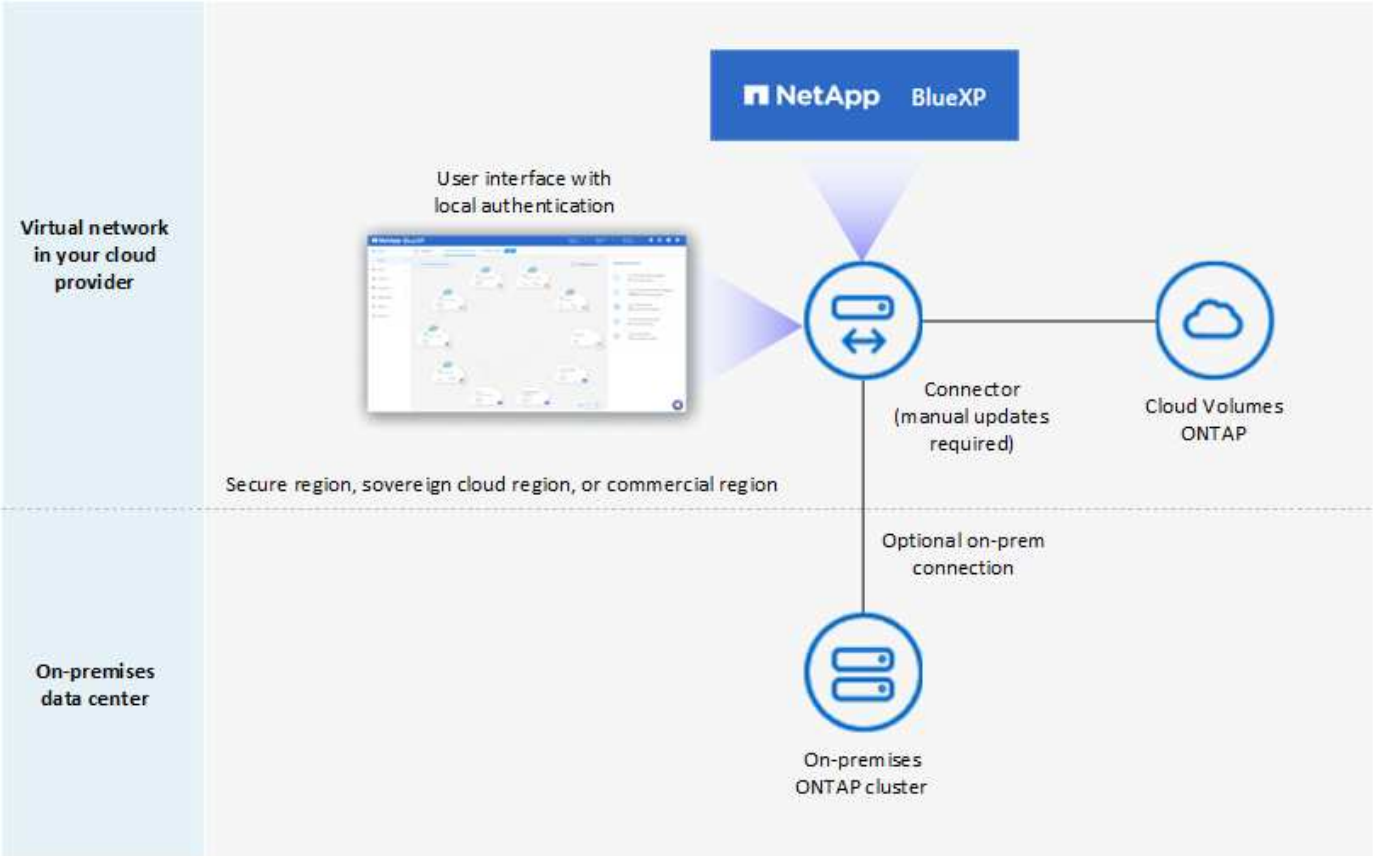
- "Erfahren Sie, wie Sie mit dem eingeschränkten Modus beginnen".
- "Erstellen Sie ein zusätzliches BlueXP Konto".

Privater Modus

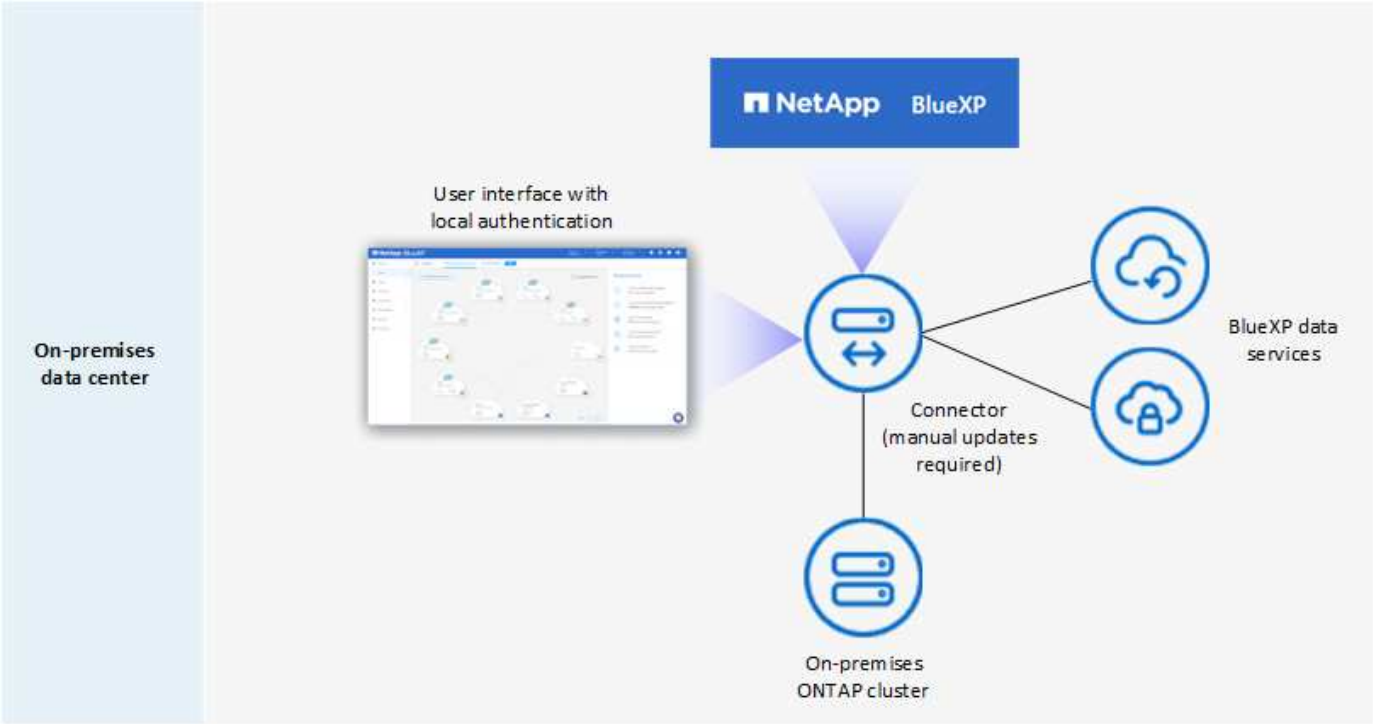
Im privaten Modus können Sie einen Connector entweder vor Ort oder in der Cloud installieren und dann

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.

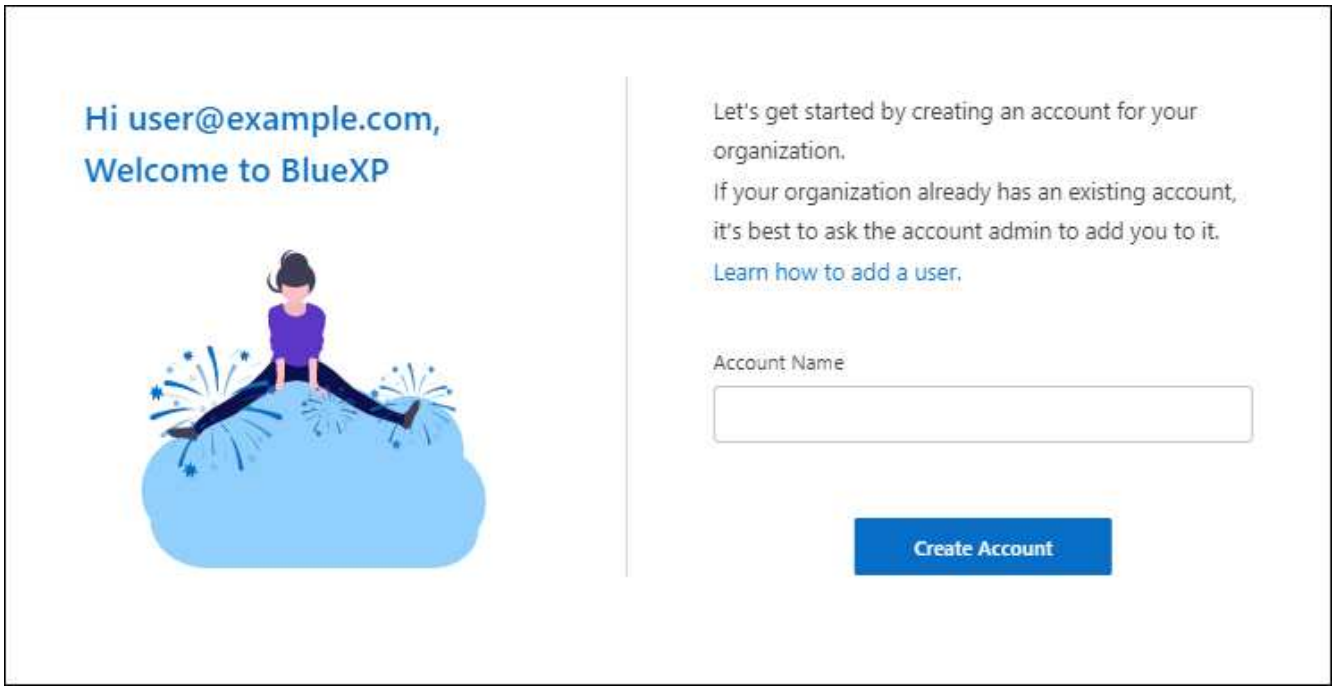
3. Wenn Sie noch keinen NSS-Account haben und sich mit einem NetApp Cloud Login registrieren möchten, wählen Sie **Registrieren**.
4. Geben Sie auf der Seite **Anmelden** die erforderlichen Informationen zur Erstellung eines NetApp Cloud-Logins ein.

   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".

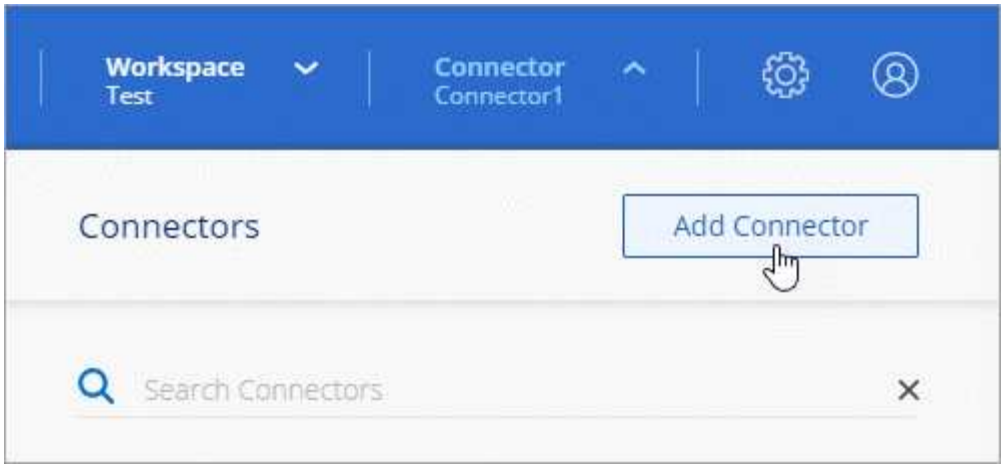
Bevor Sie beginnen

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".

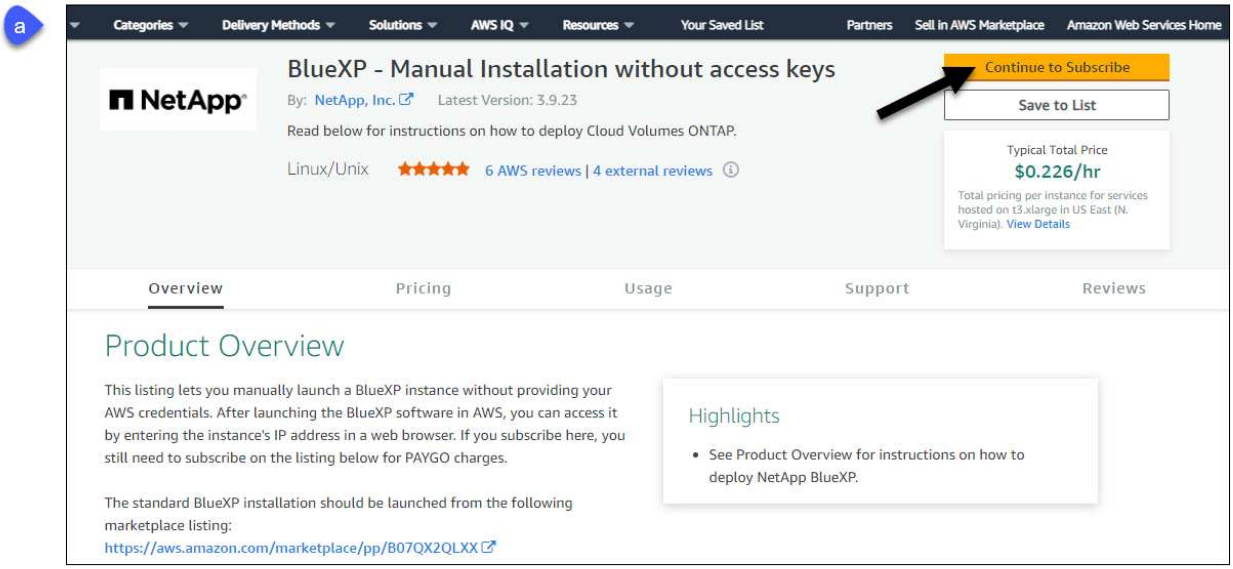
Bevor Sie beginnen

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

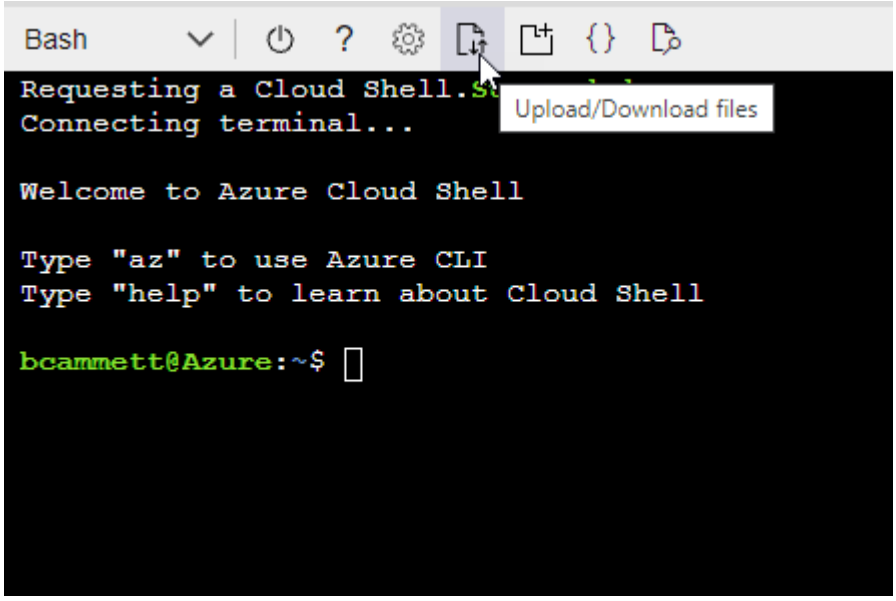
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

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.

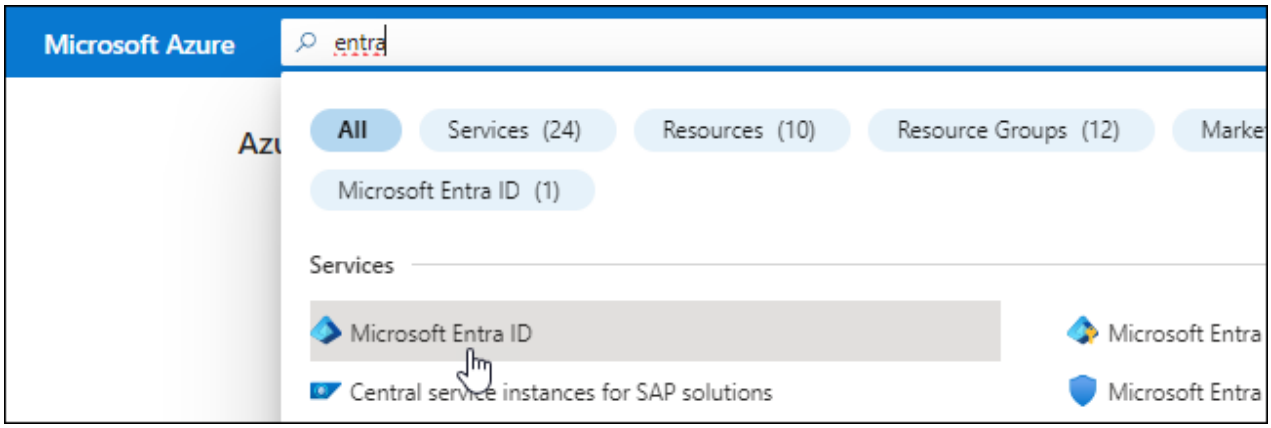
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

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**.

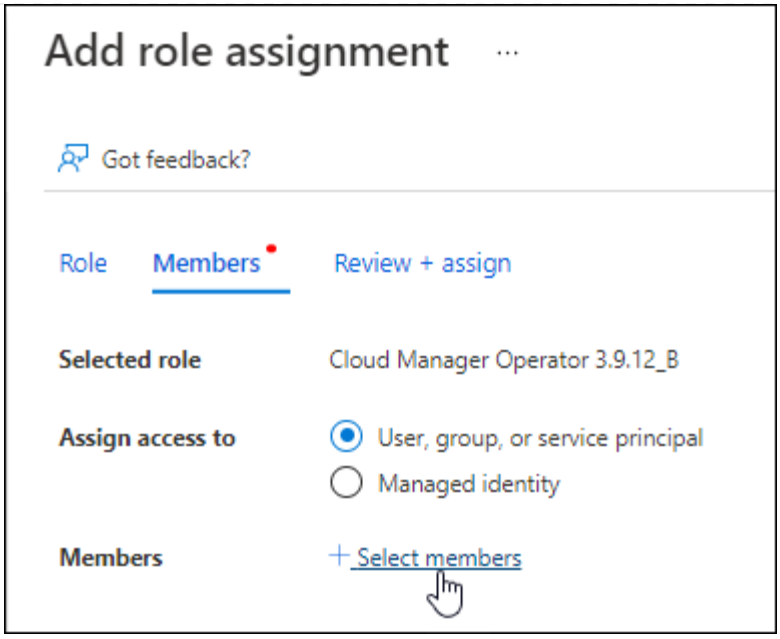
   Sie haben die AD-Anwendung und den Service-Principal erstellt.

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:

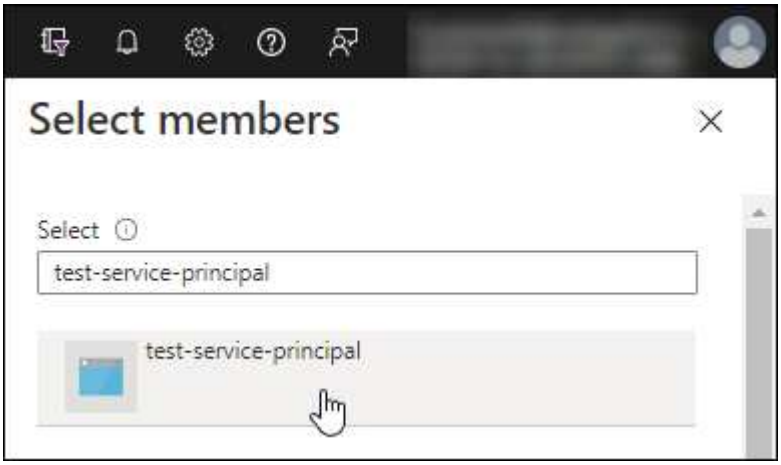
   a. **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.

   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**.

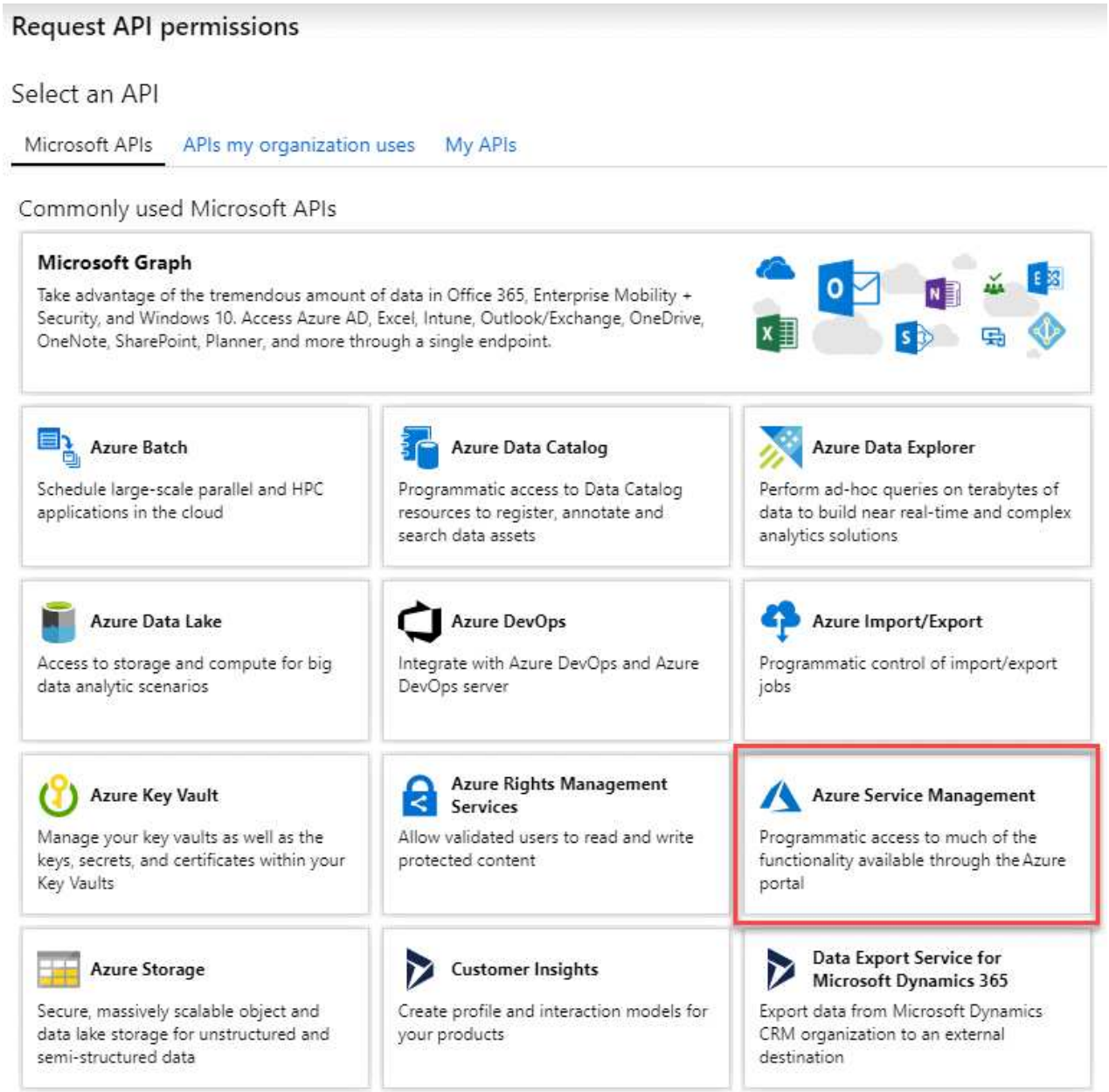
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

   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.

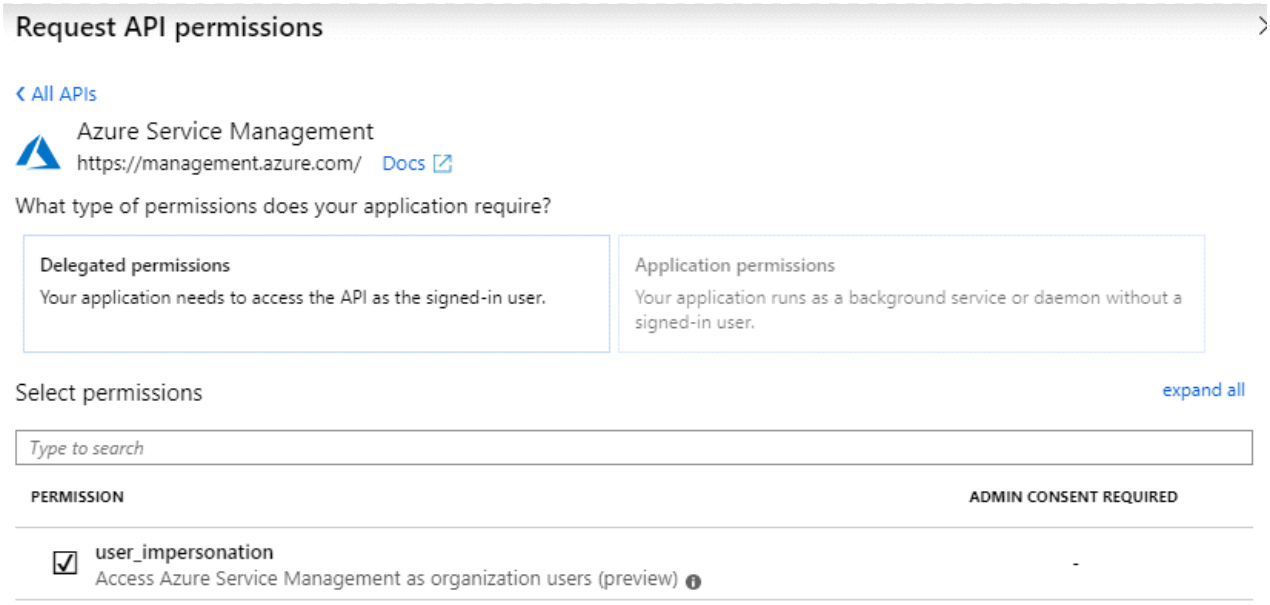
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

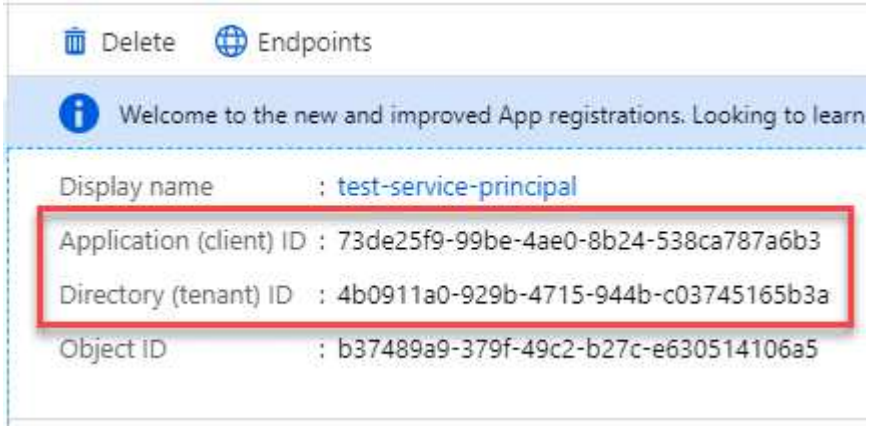


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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.

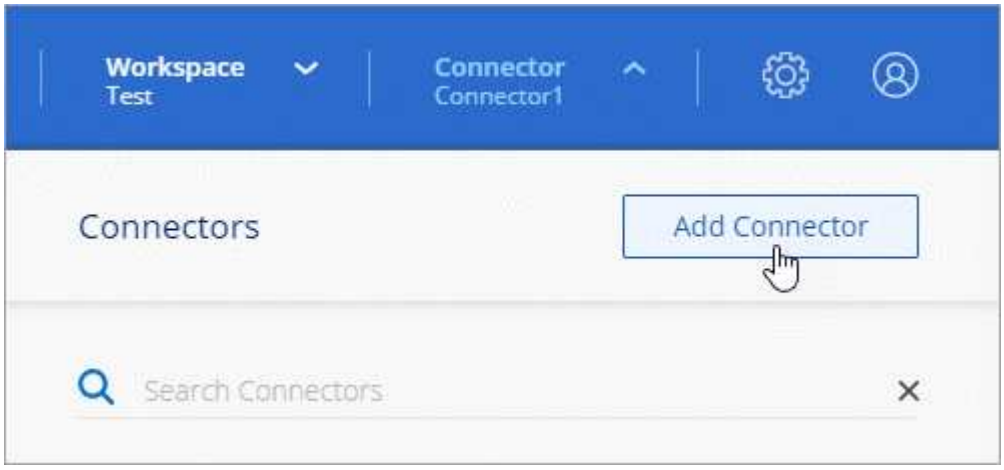
  "Erfahren Sie mehr über die Verbindung mit einer Linux VM in Azure"

- 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.

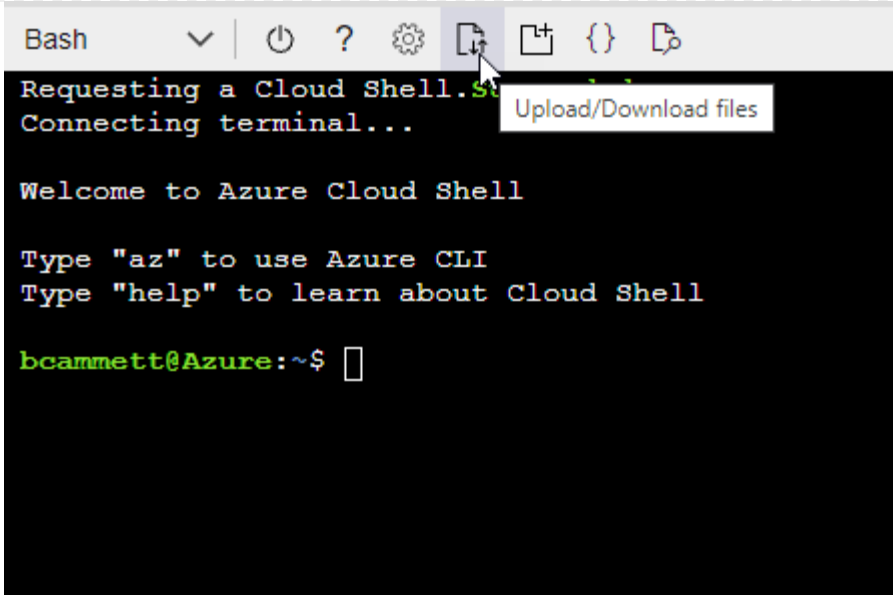
   Beispiel

   ```
   "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

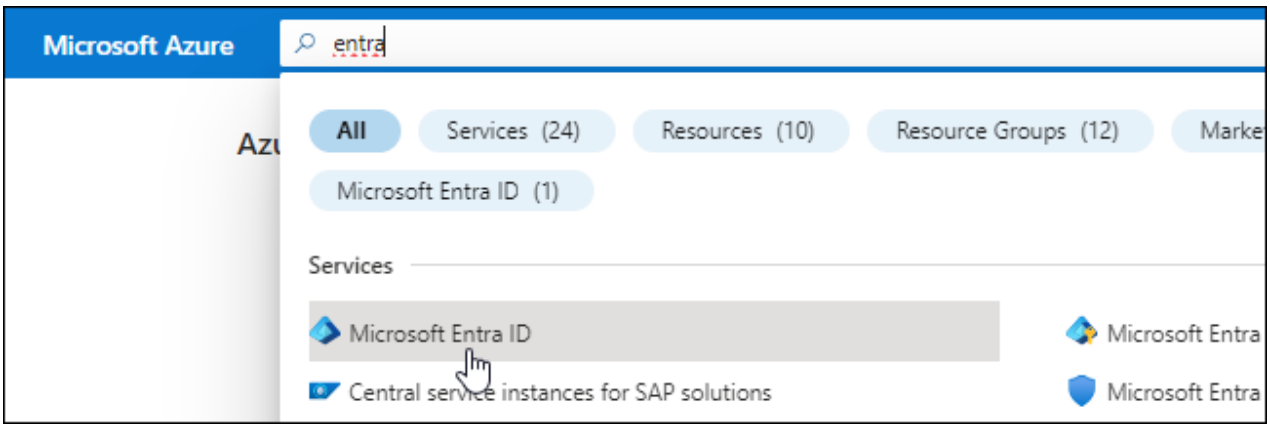
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

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.

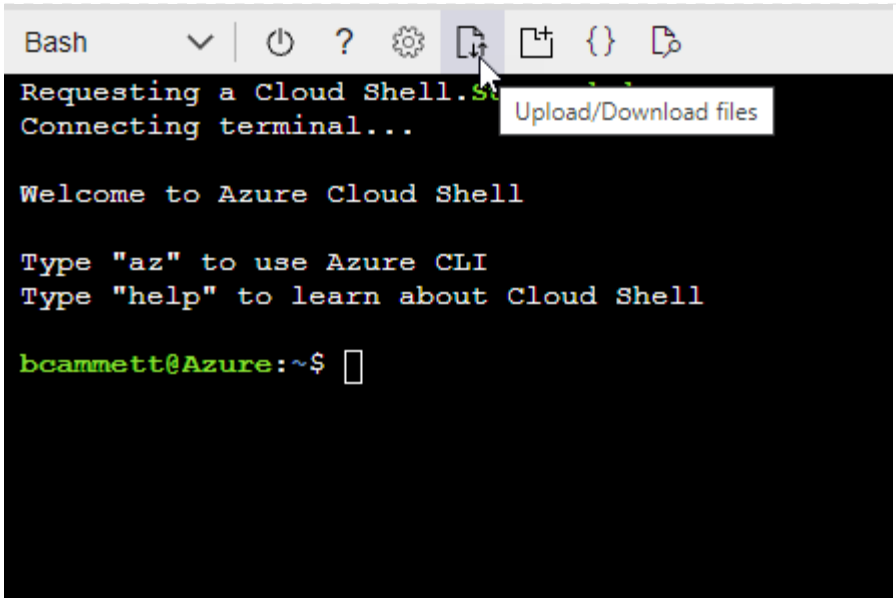
      Beispiel

      ```
      "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**.

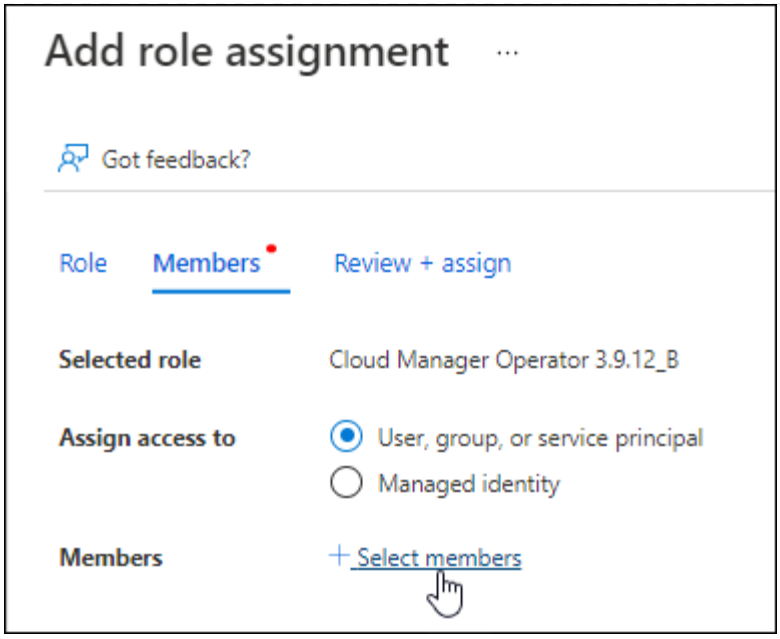
   b. Wählen Sie das Abonnement aus.

   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.

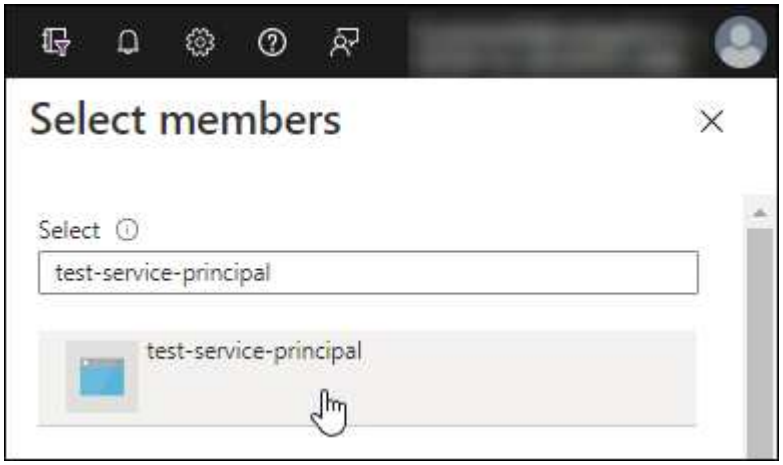
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - **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**.

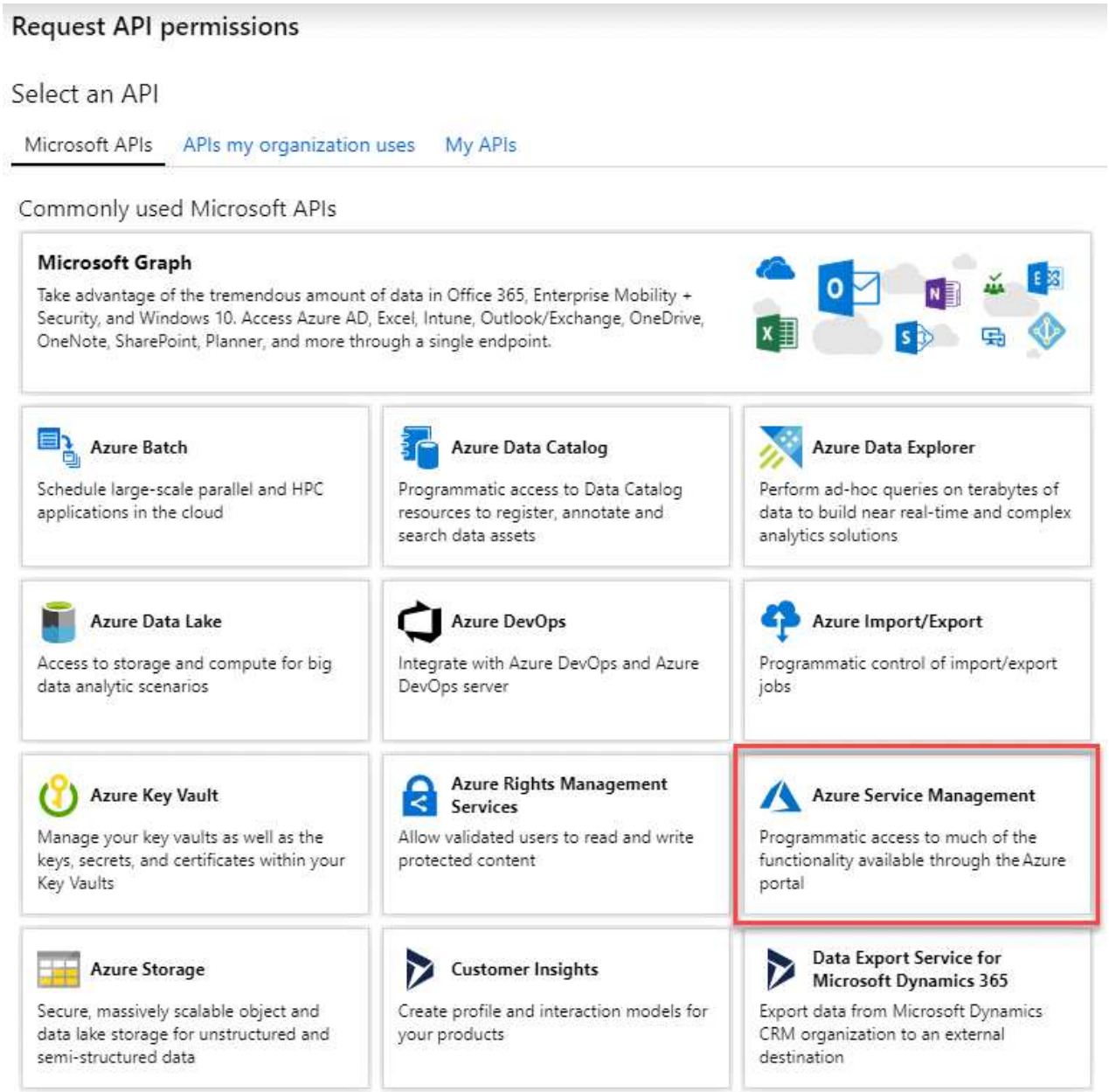
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

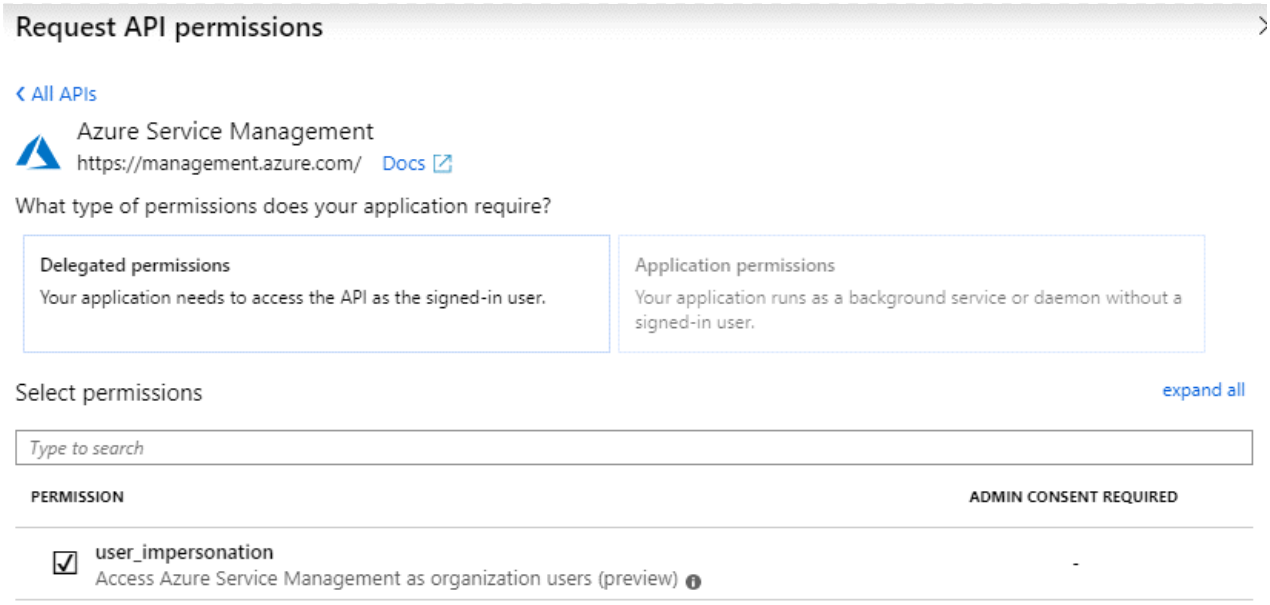
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

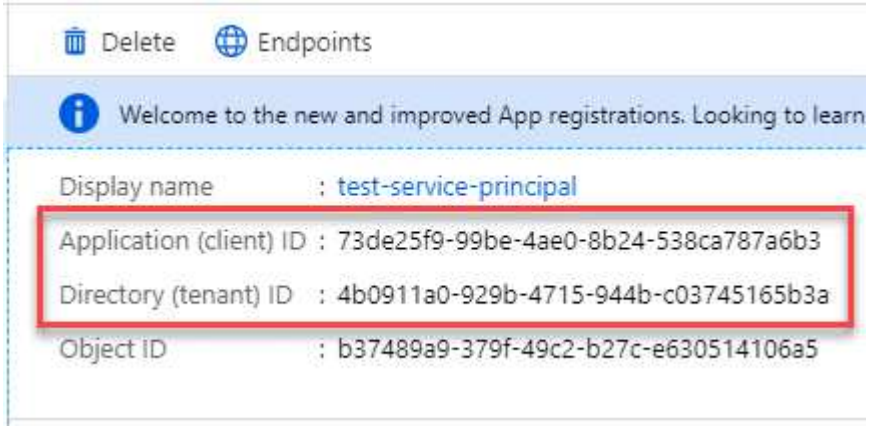


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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.

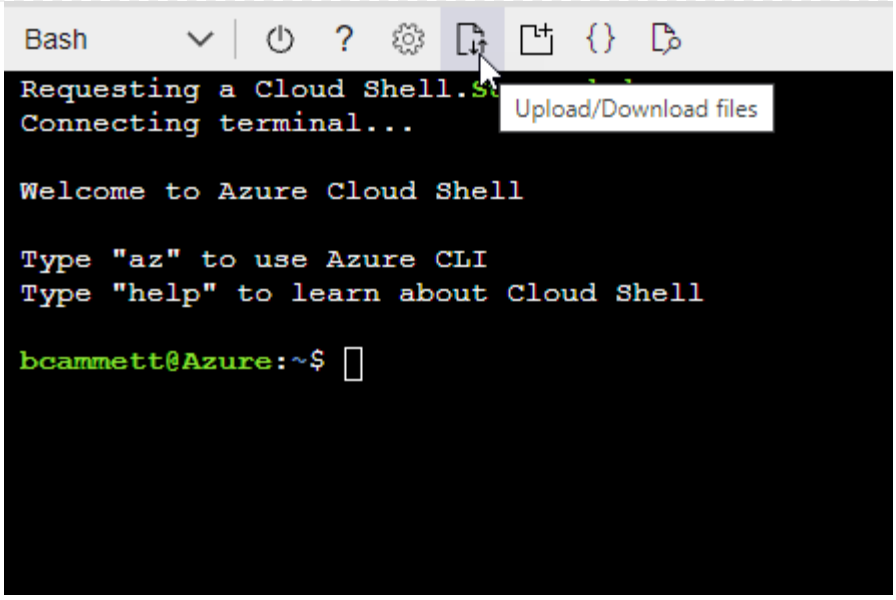
   Beispiel

   ```
   "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

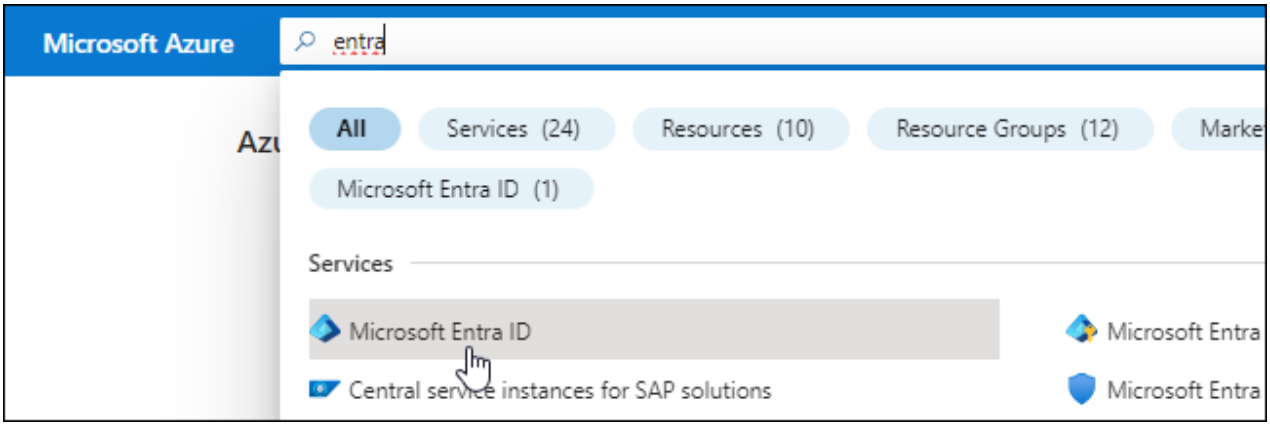
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

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.

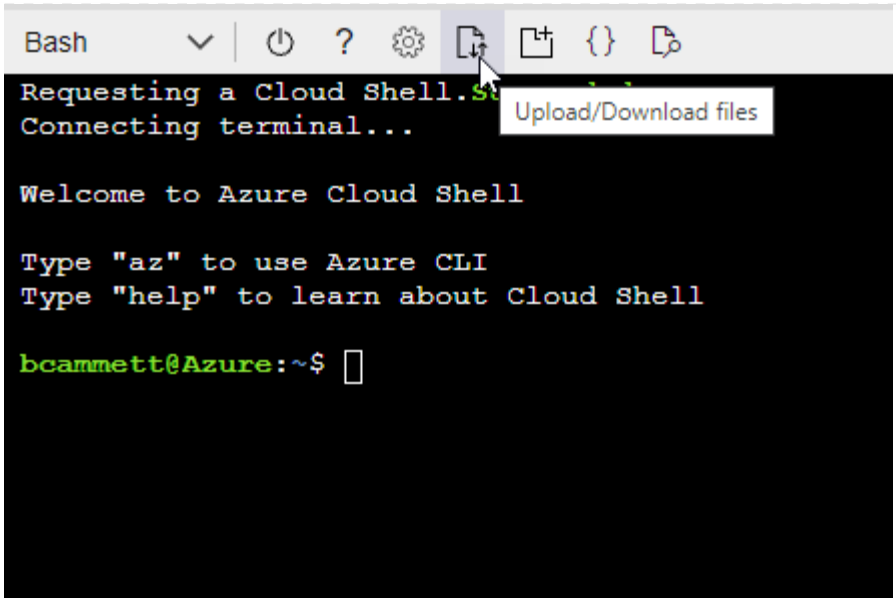
      Beispiel

      ```
      "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**.

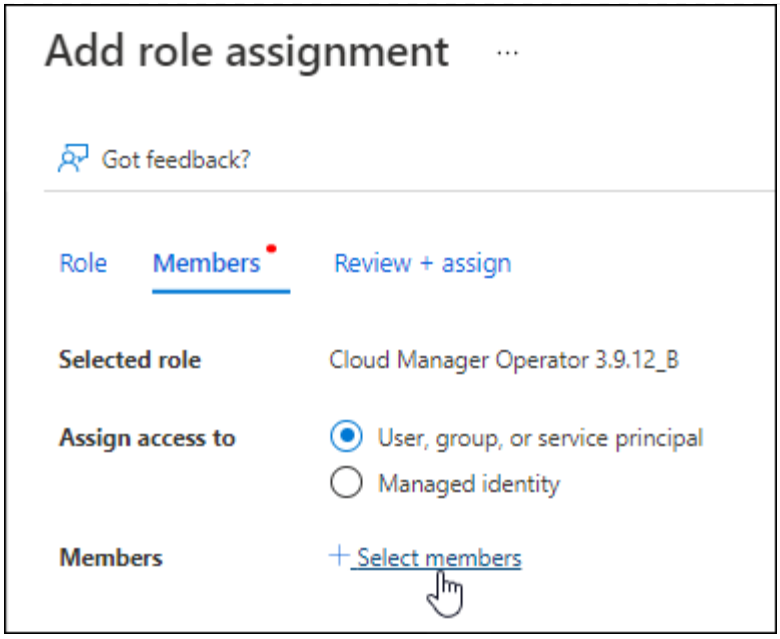
   b. Wählen Sie das Abonnement aus.

   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.

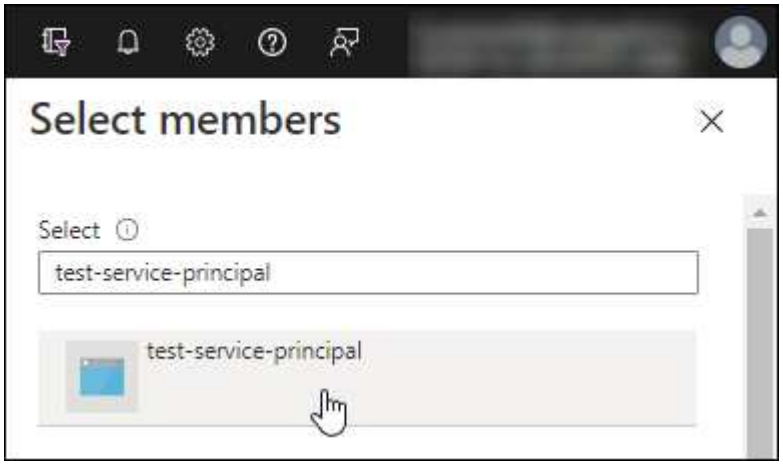
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

      - **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**.

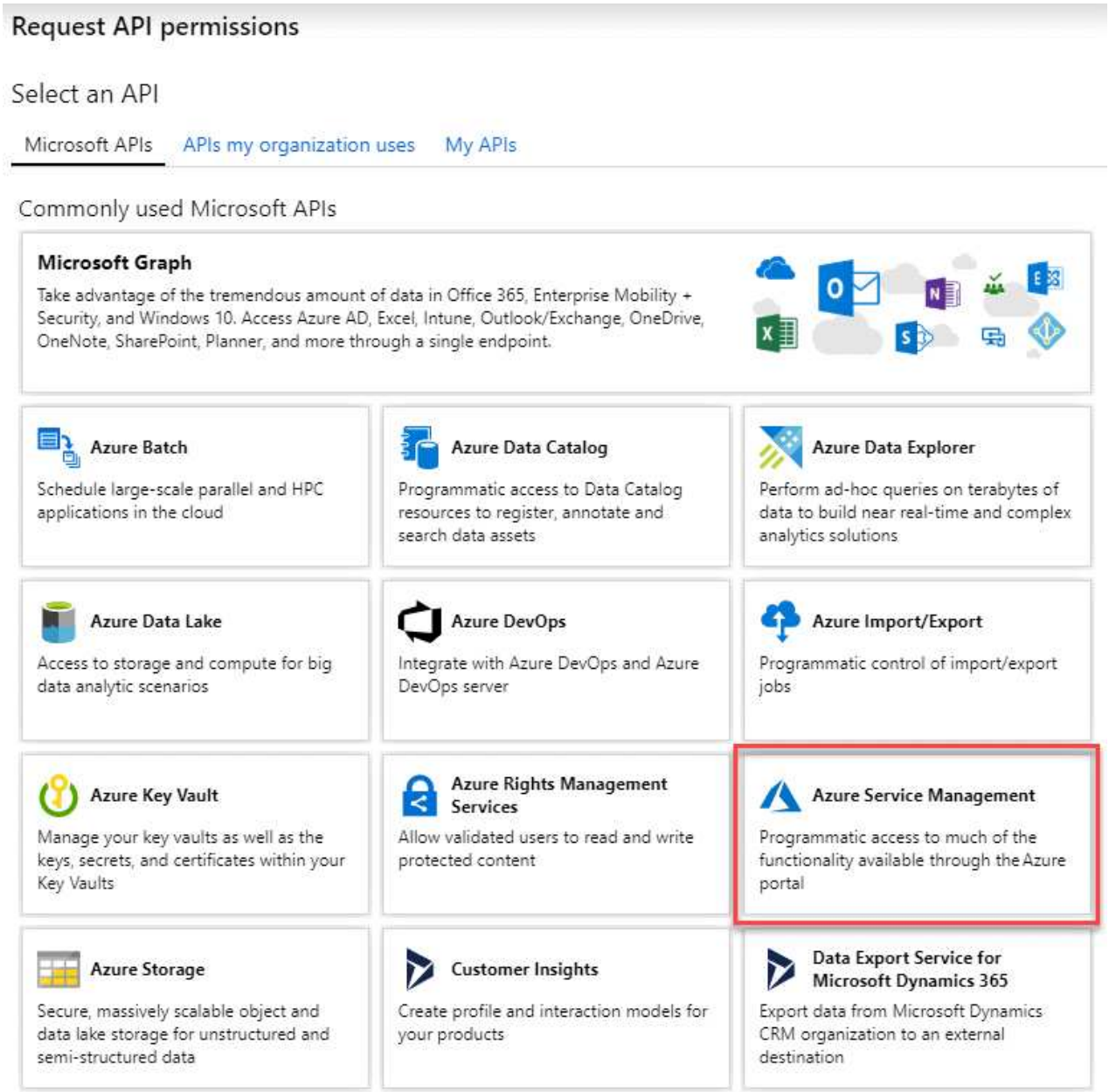
Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

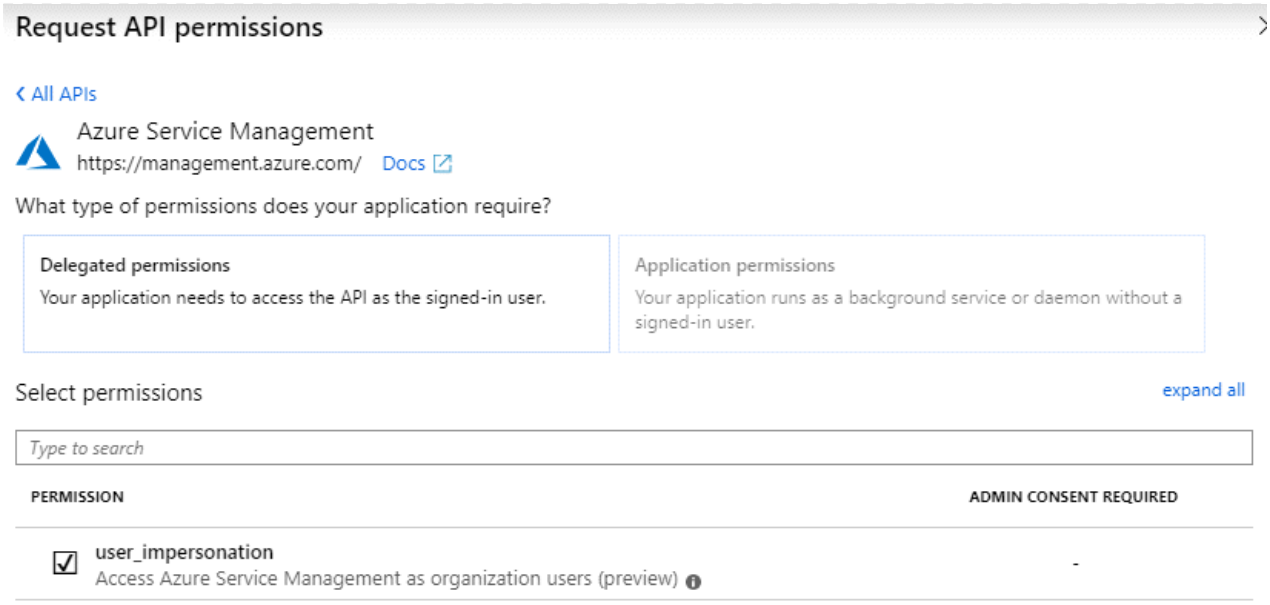
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

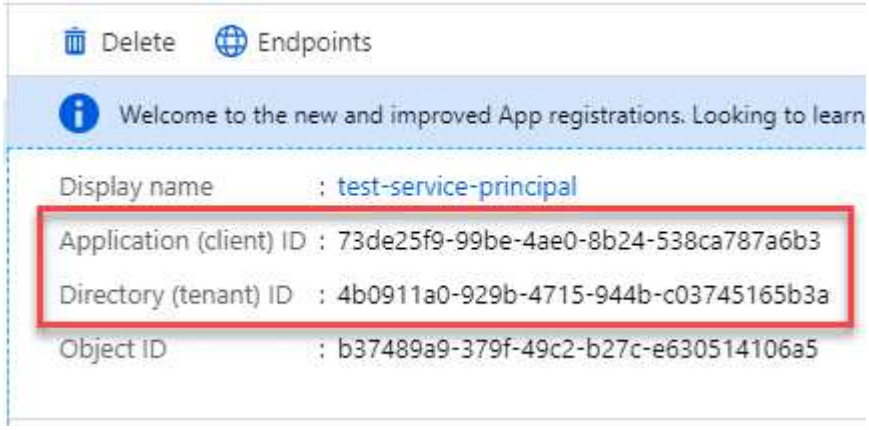


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

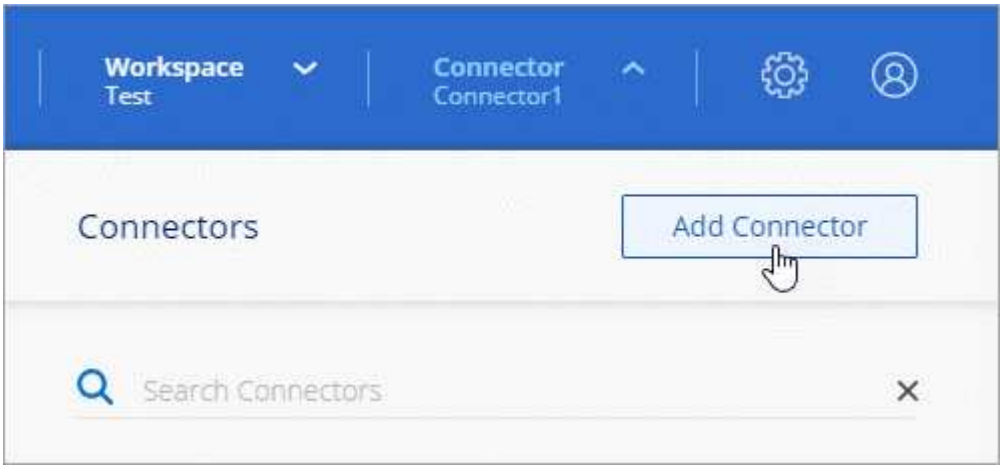
Bevor Sie beginnen

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

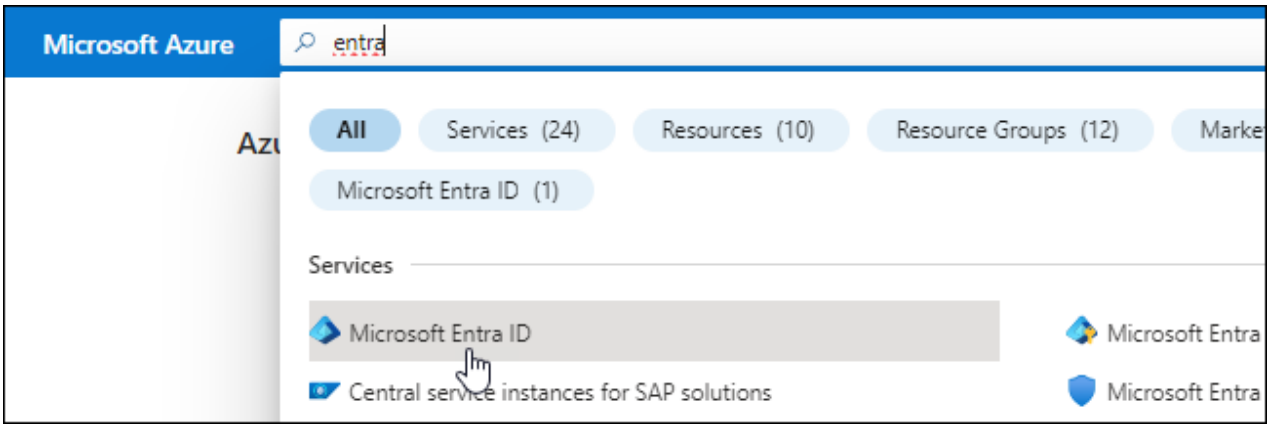
Wenn der Connector vor Ort installiert ist, müssen Sie BlueXP mit Azure-Berechtigungen versehen, indem Sie einen Service-Prinzipal in der Microsoft Entra-ID einrichten und die für BlueXP erforderlichen Azure-Berechtigungen erhalten.

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.

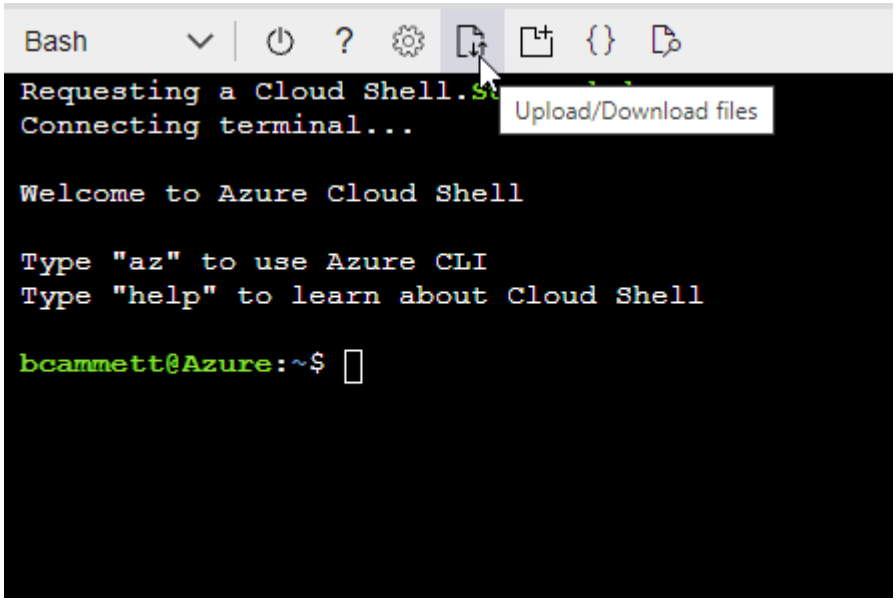
      Beispiel

      ```
      "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:

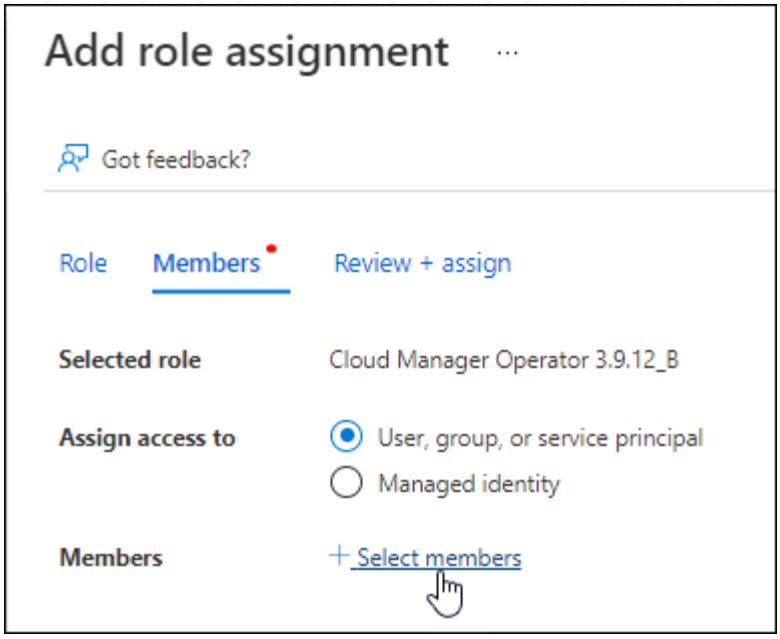
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

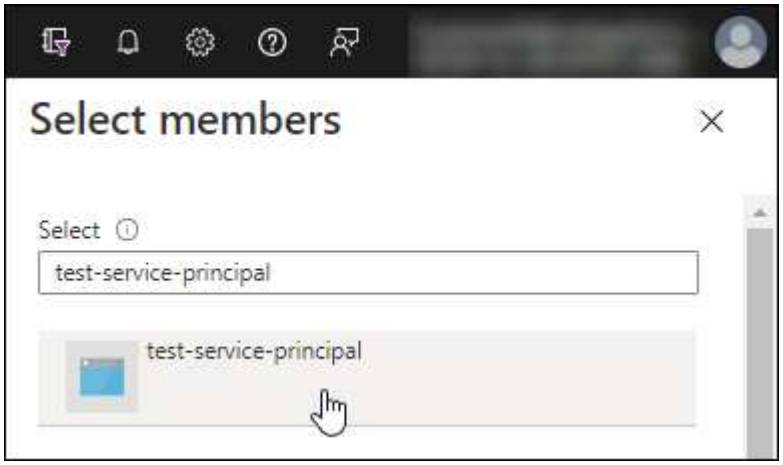
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

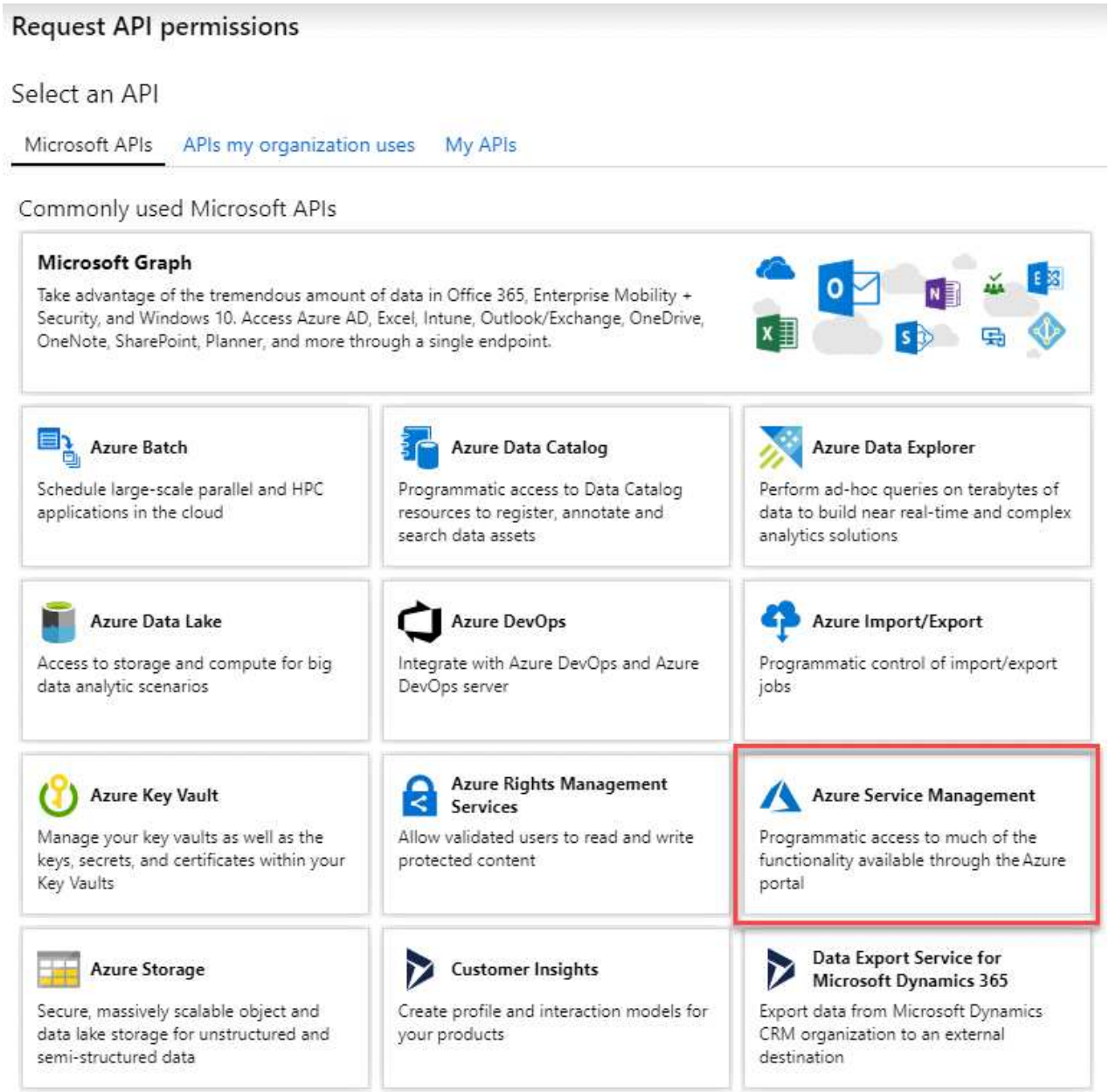
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

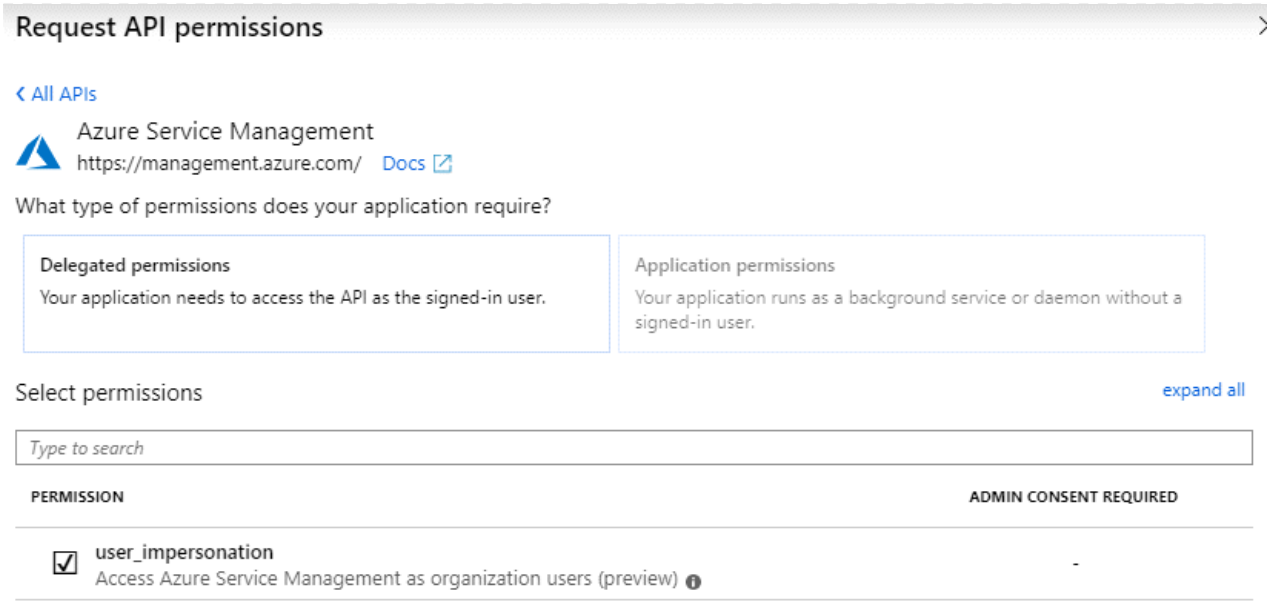
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

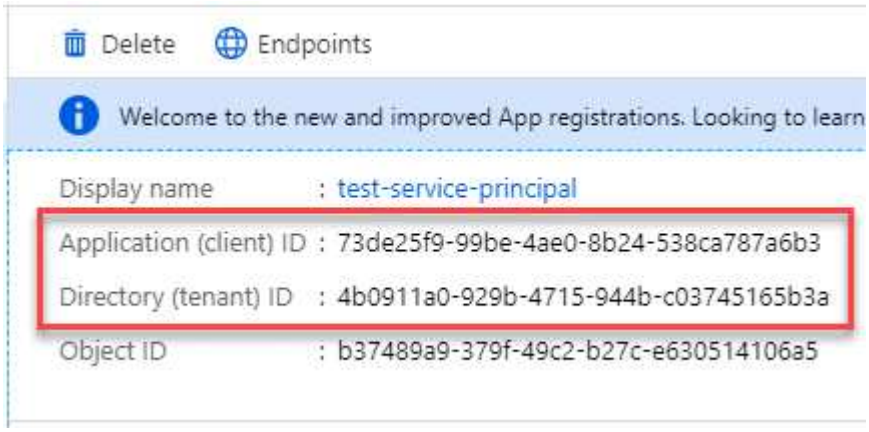


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

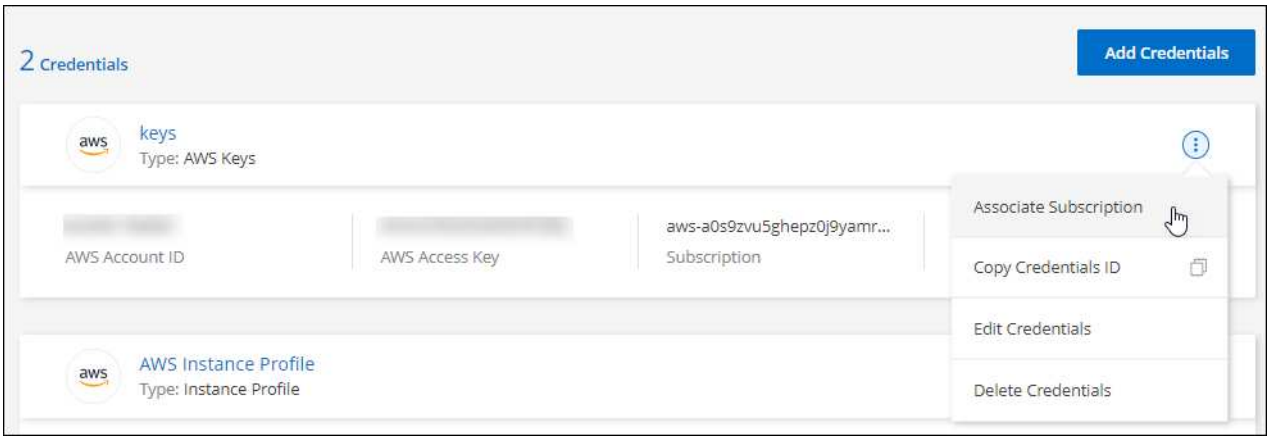
Für das Abonnement von BlueXP wird ein Marketplace-Abonnement mit den Cloud-Zugangsdaten verknüpft, die einem Connector zugeordnet sind. Wenn Sie den Workflow „erste Schritte mit Standardmodus“ befolgt haben, sollten Sie bereits über einen Connector verfügen. Weitere Informationen finden Sie im "Schneller 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:

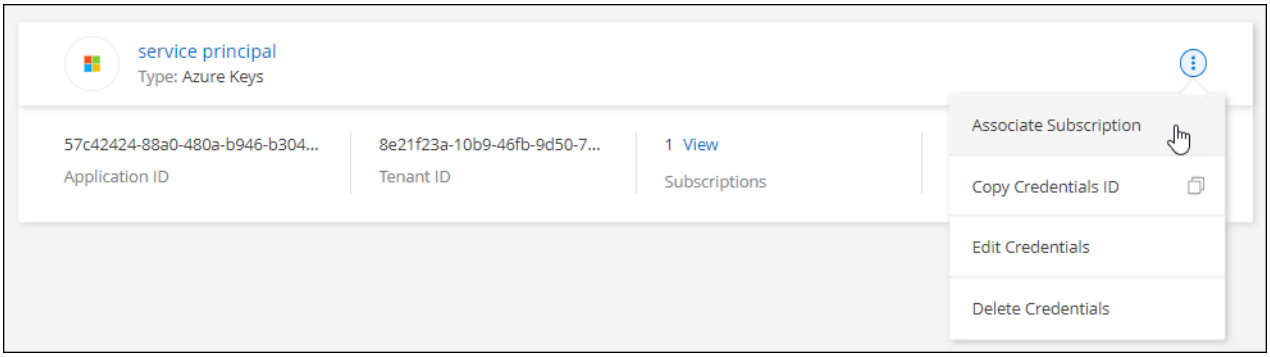
Abonnieren Sie BlueXP über den AWS Marketplace

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**.

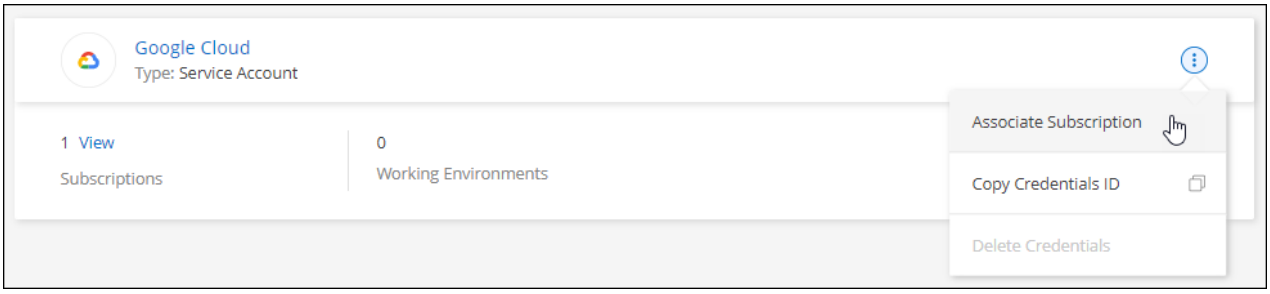
Im folgenden Video sehen Sie, wie Sie im Azure Marketplace abonnieren:

Abonnieren Sie BlueXP über den Azure Marketplace

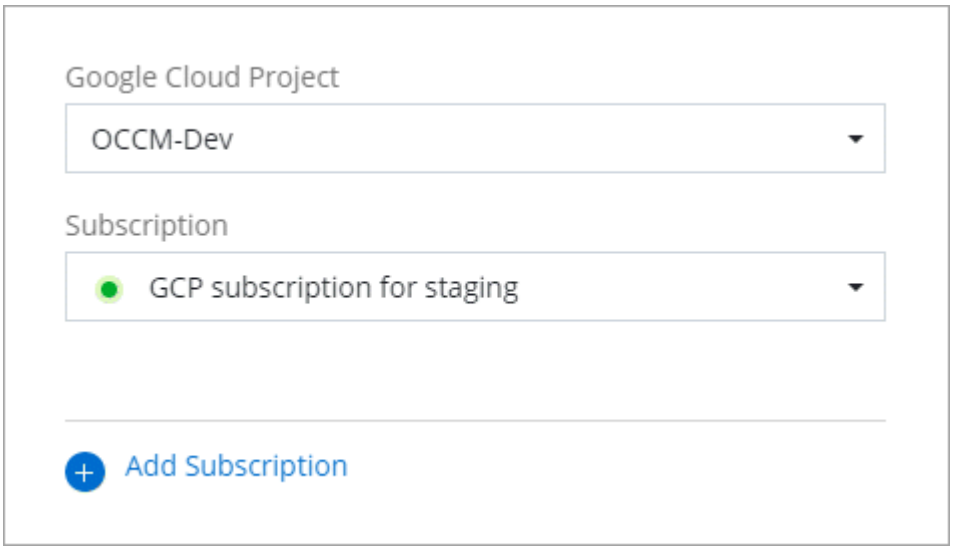
Google Cloud

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**.



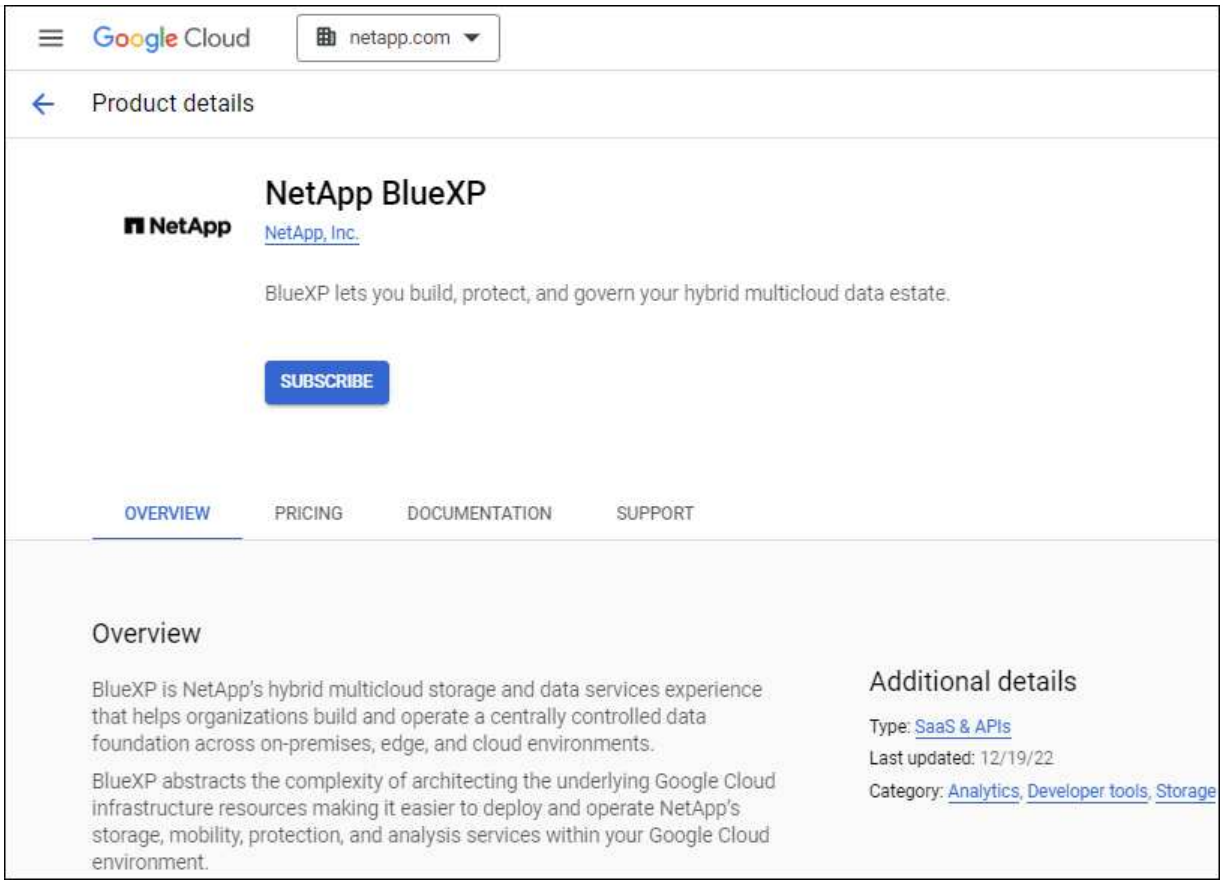
3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, und wählen Sie dann **Associate** aus.



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**.

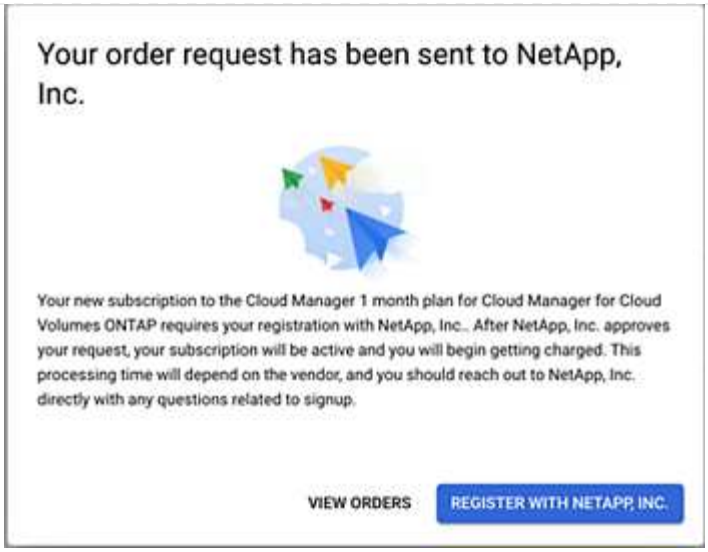
c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

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.

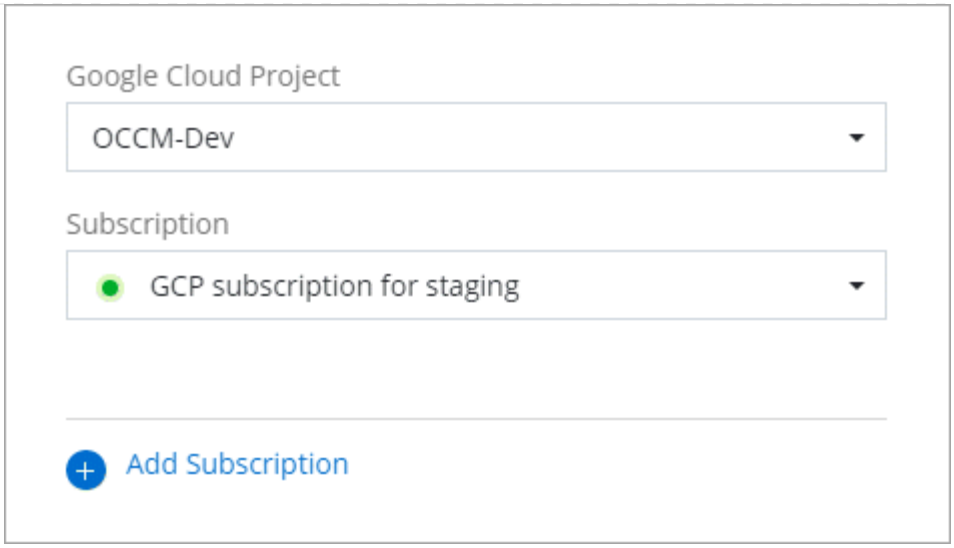
Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden Schritte wiederholen.

- 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

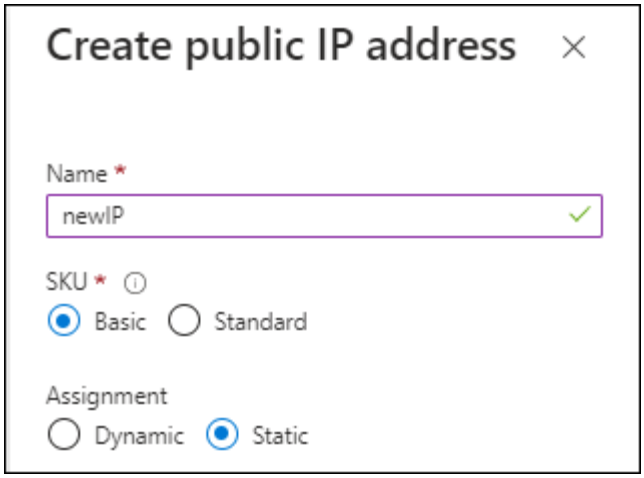
Der Netzwerkspeicherort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen. Für den Konnektor ist ein abgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu verwalten.

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.

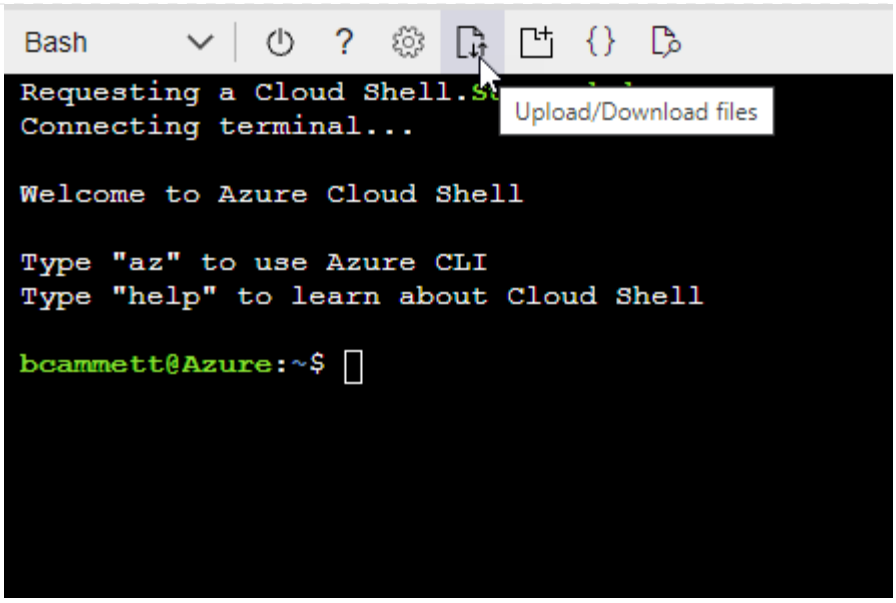
   Beispiel

   ```
   "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

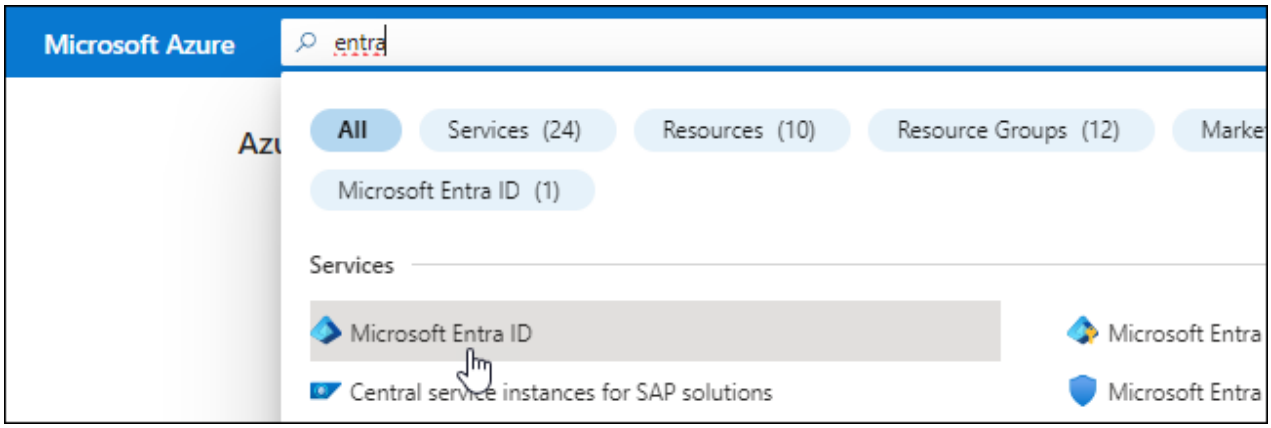
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

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.

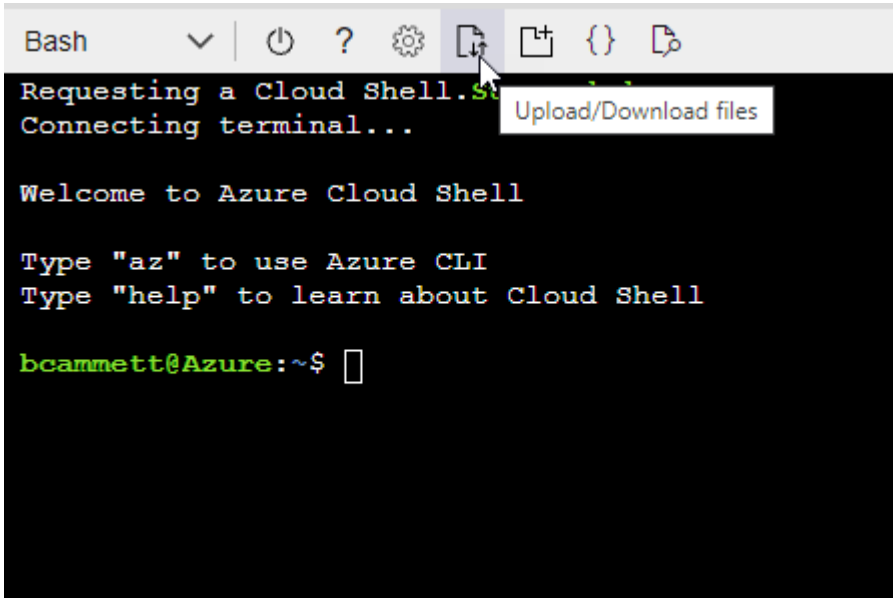
      Beispiel

      ```
      "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:

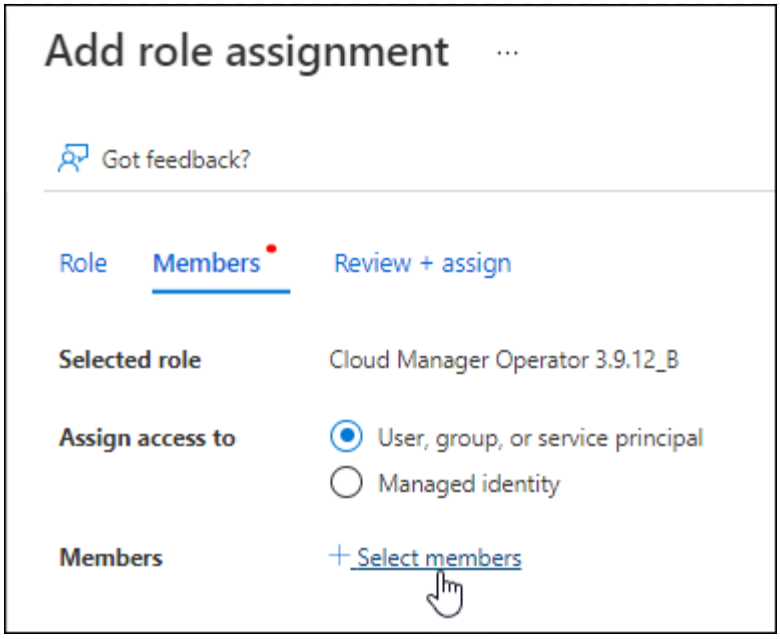
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

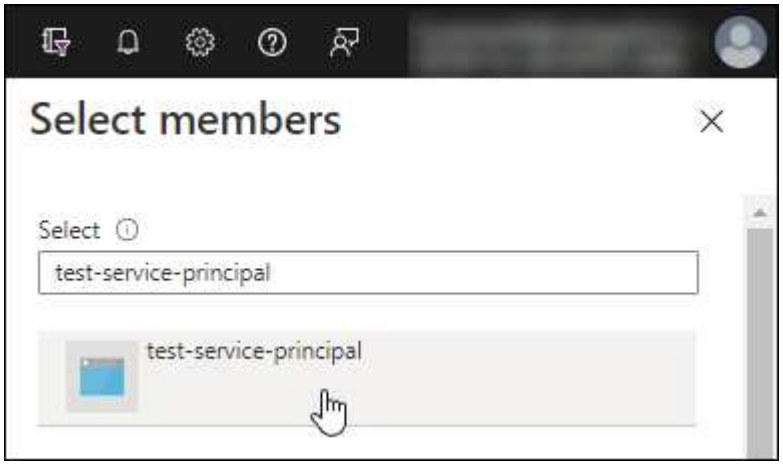
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

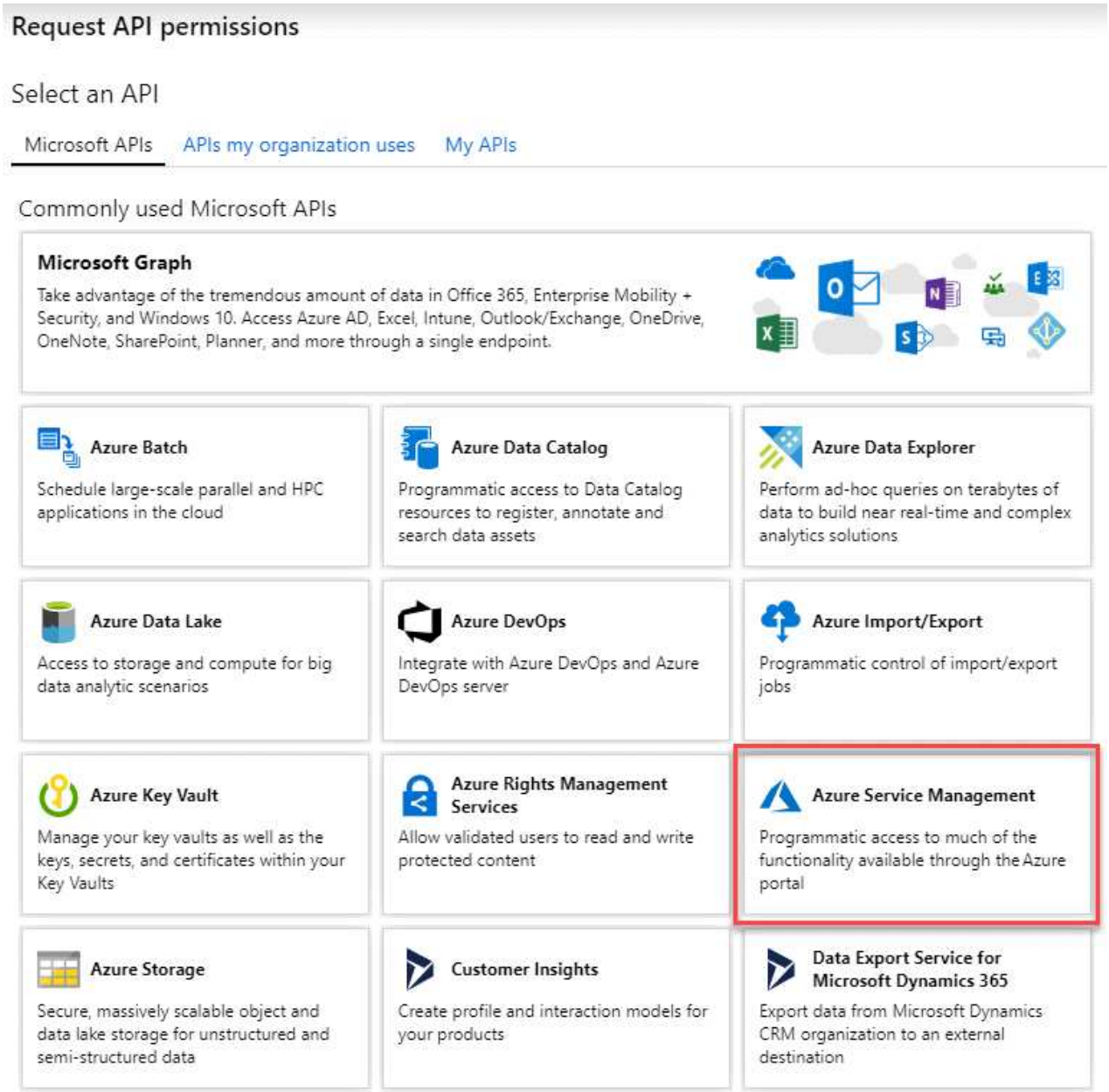
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

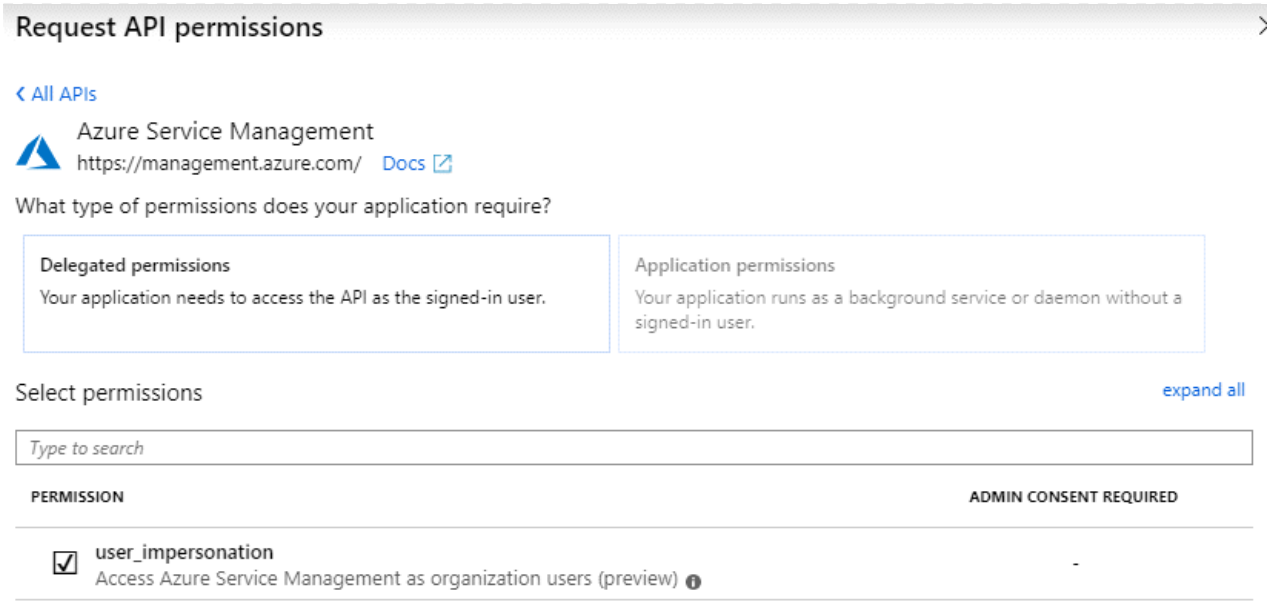
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

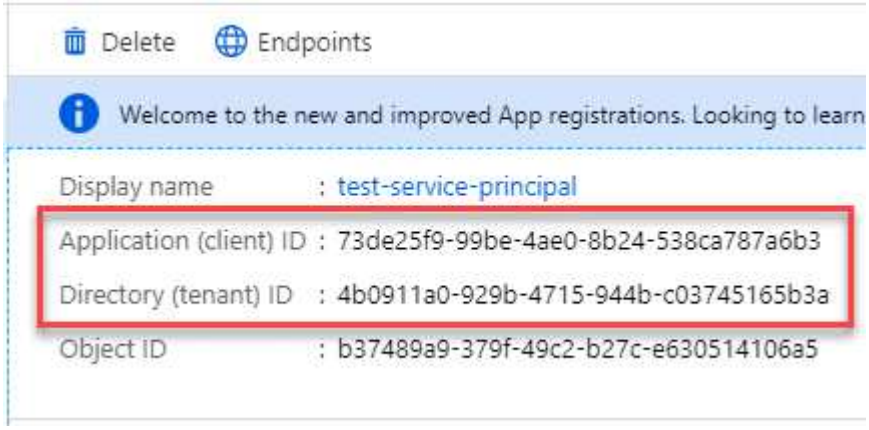


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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"

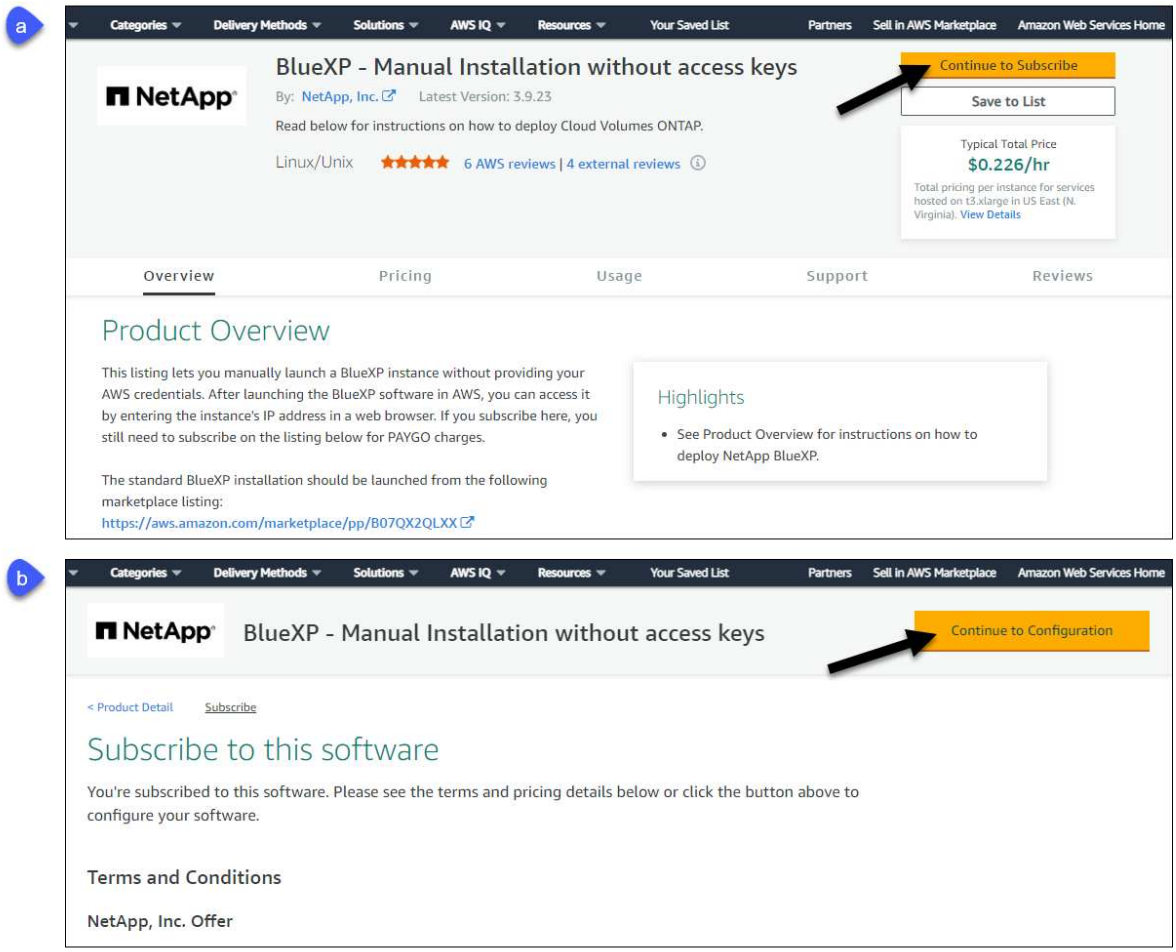
- Berechtigung zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Verständnis der CPU- und RAM-Anforderungen für die Instanz.

  "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"

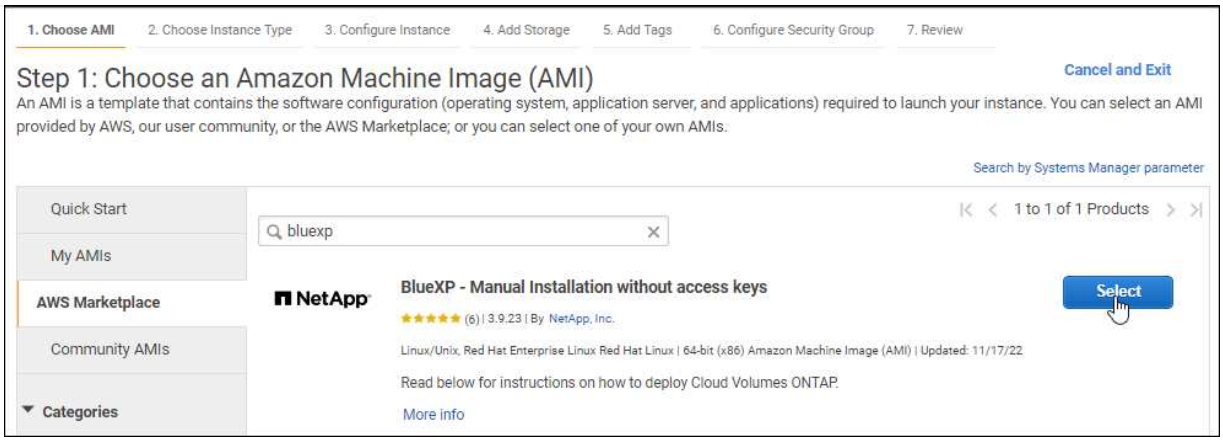
- Eine IAM-Rolle mit angehängter Richtlinie, die die erforderlichen Berechtigungen für den Connector enthält.

  "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.

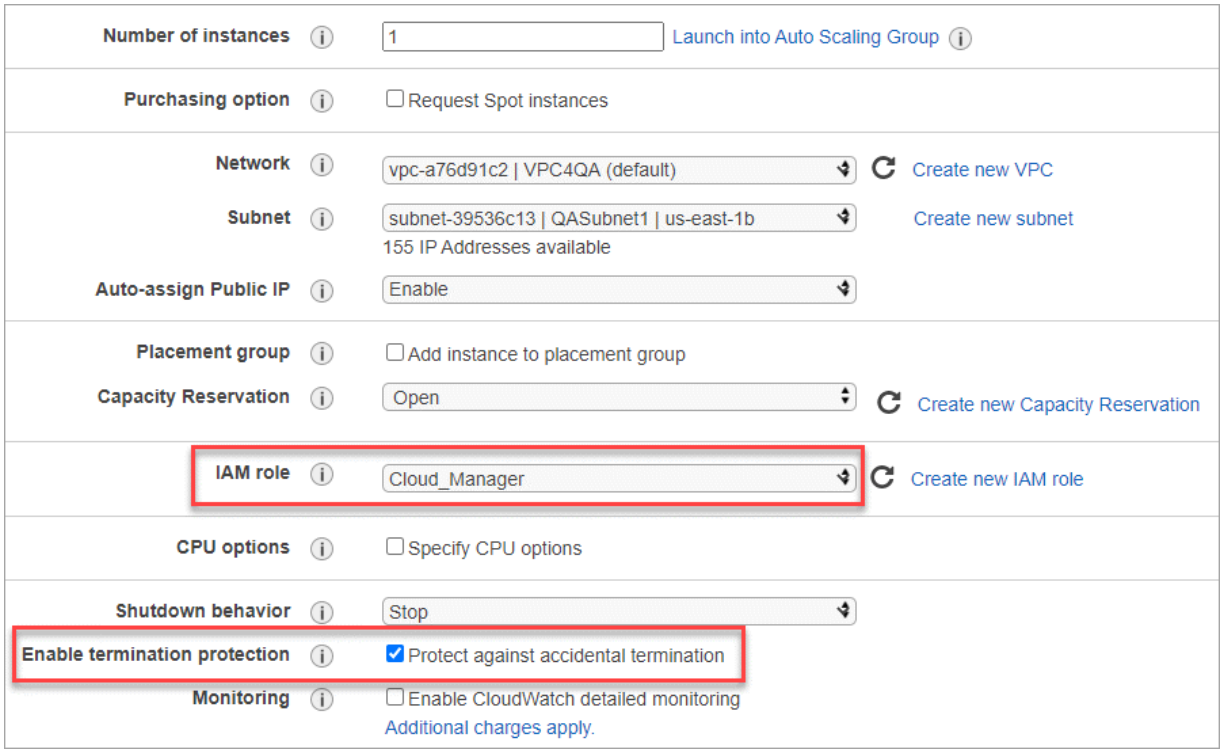


d. Wählen Sie **Weiter**.

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.

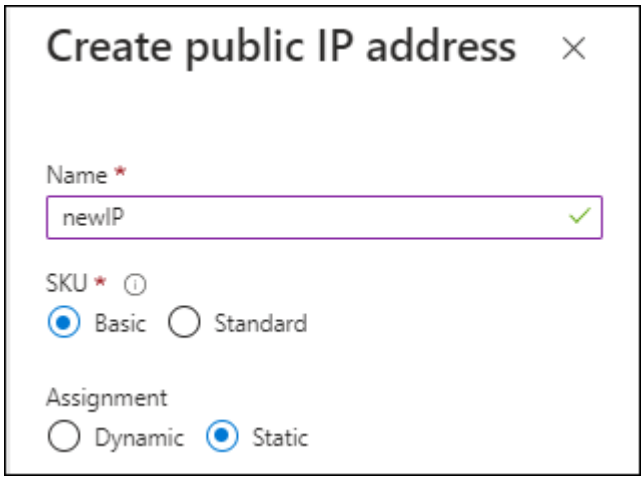
  "Erfahren Sie, wie Sie Azure-Berechtigungen einrichten"

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.

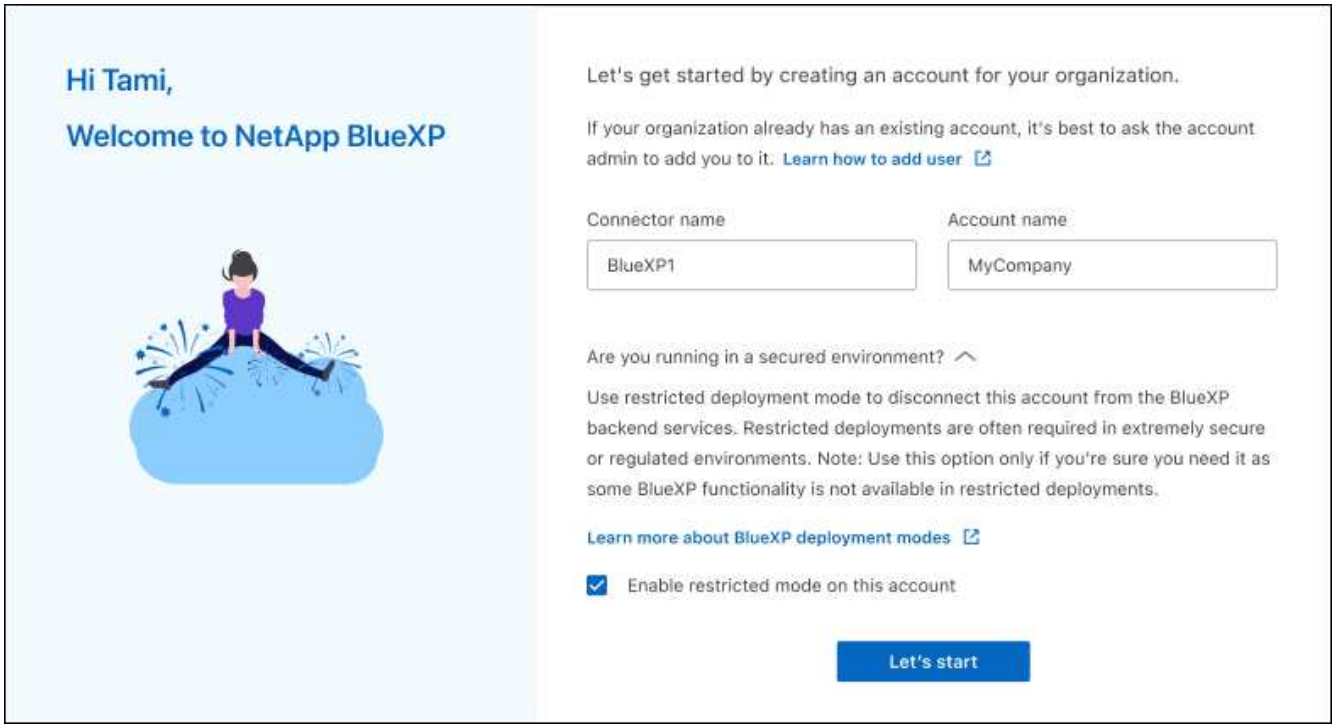
   c. Wählen Sie **laufen Sie in einer sicheren Umgebung?**

   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

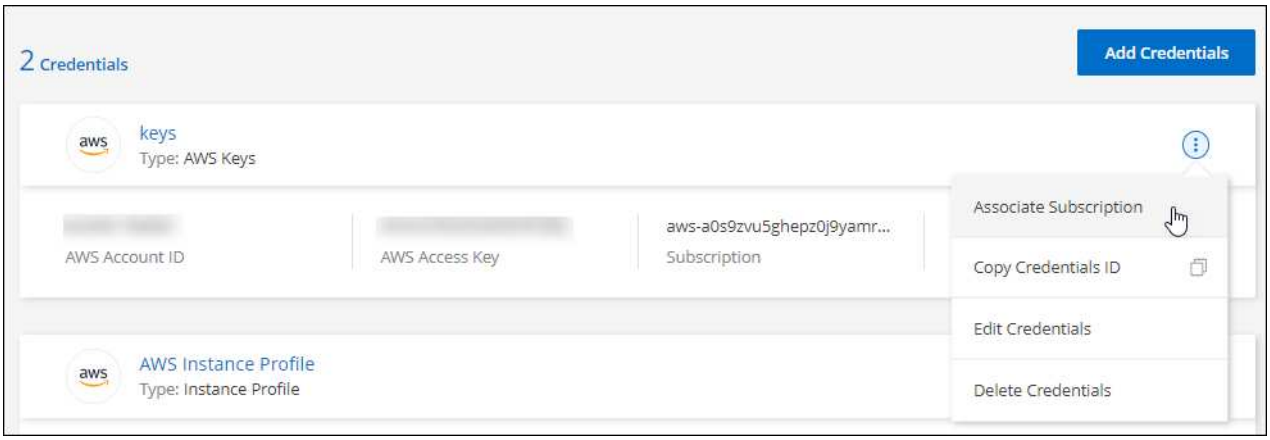
Für das Abonnement von BlueXP wird ein Marketplace-Abonnement mit den Cloud-Zugangsdaten verknüpft, die einem Connector zugeordnet sind. Wenn Sie den Workflow „erste Schritte mit eingeschränktem Modus“ befolgt haben, sollten Sie bereits über einen Connector verfügen. Weitere Informationen finden Sie 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:

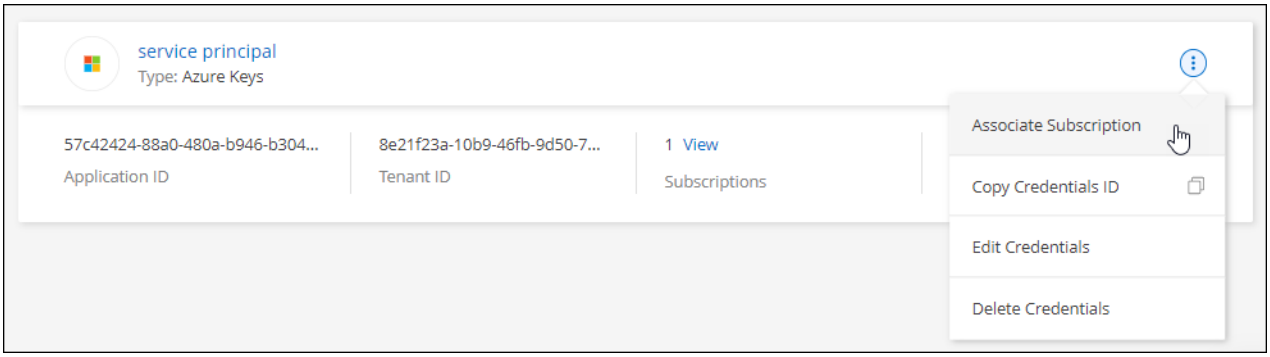
Abonnieren Sie BlueXP über den AWS Marketplace

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**.

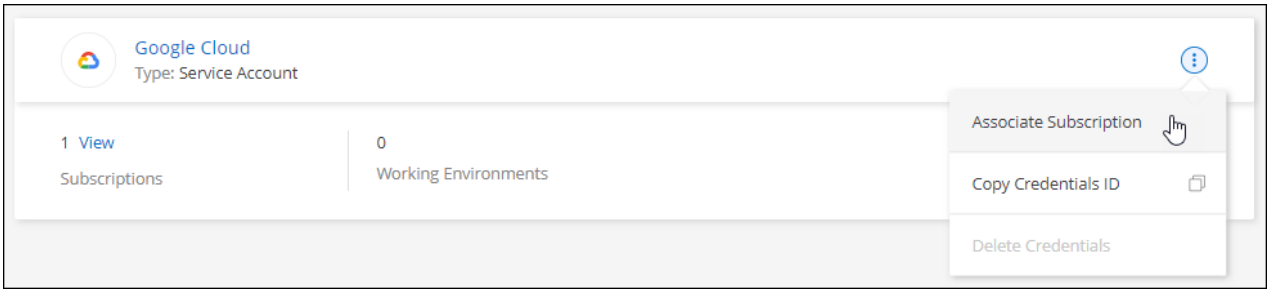
Im folgenden Video sehen Sie, wie Sie im Azure Marketplace abonnieren:

Abonnieren Sie BlueXP über den Azure Marketplace

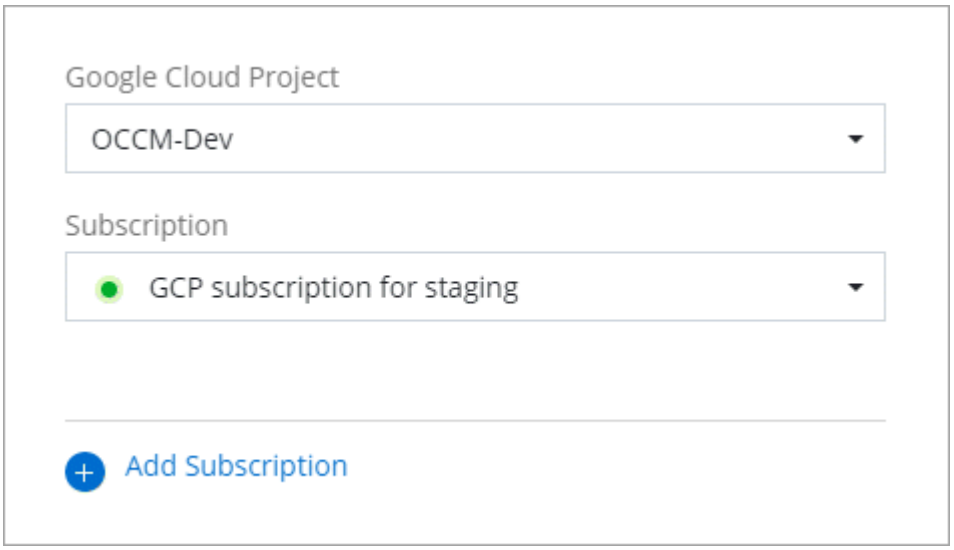
Google Cloud

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**.



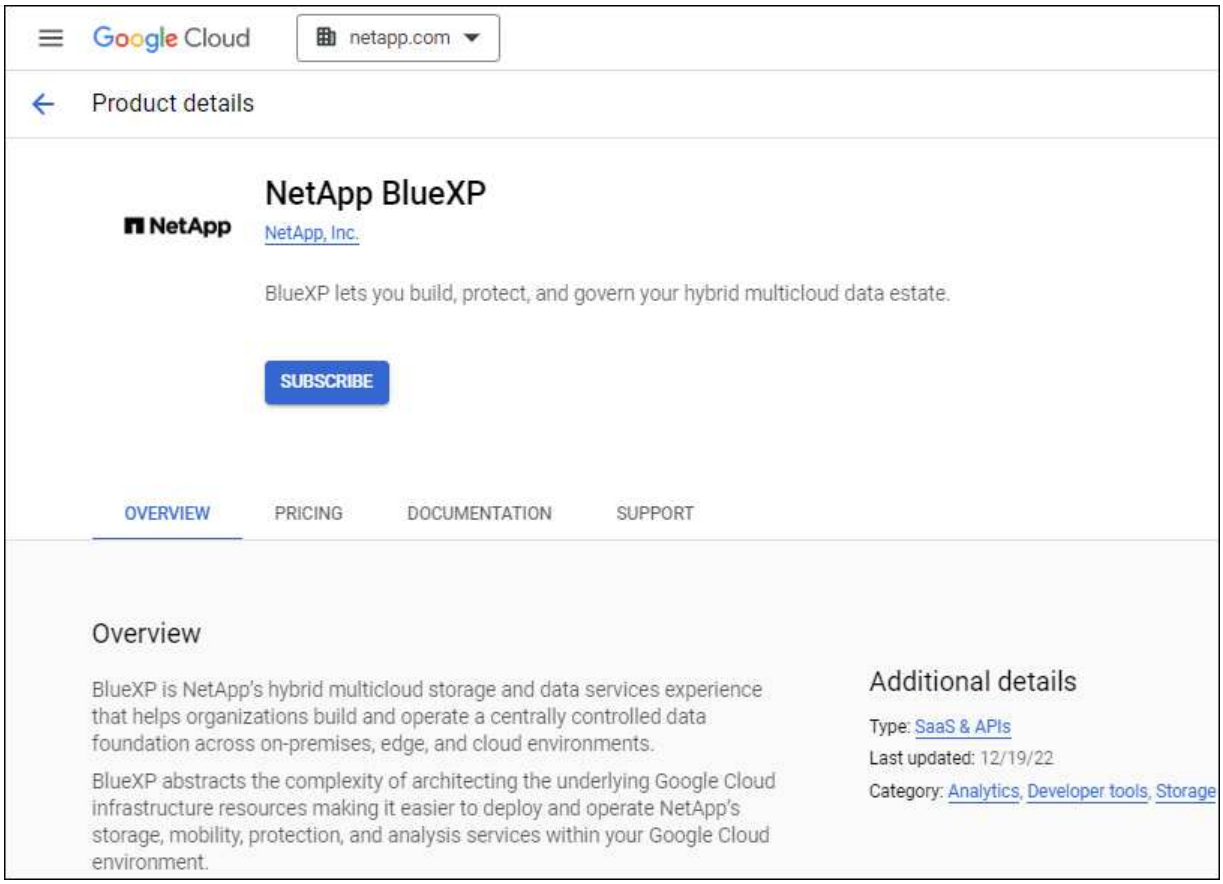
3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, und wählen Sie dann **Associate** aus.



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**.

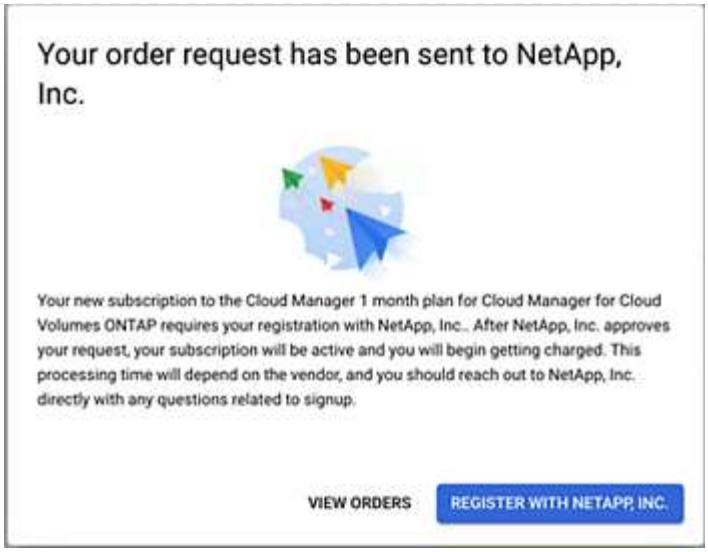
c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

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.

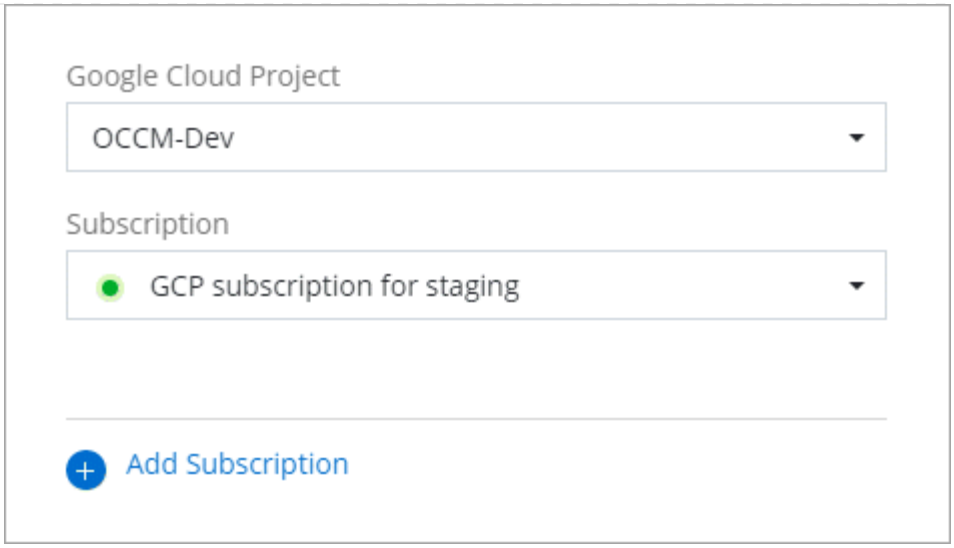
Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden Schritte wiederholen.

- 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

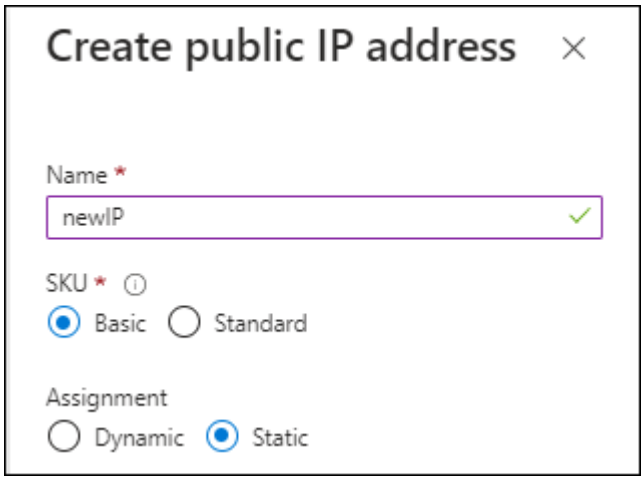
Der Connector kontaktiert die folgenden Endpunkte, um Ressourcen und Prozesse in der Public Cloud-Umgebung zu managen.

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.

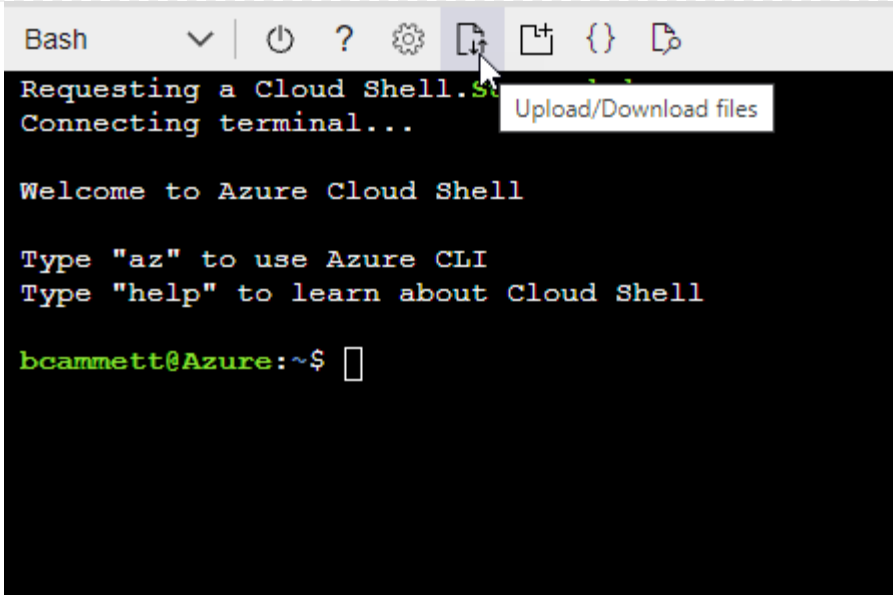
   Beispiel

   ```
   "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

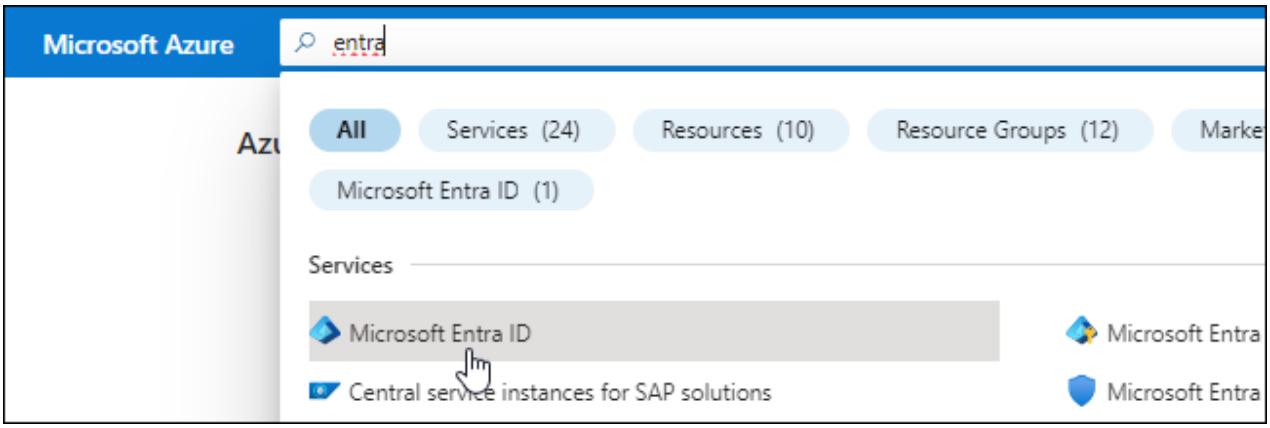
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

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.

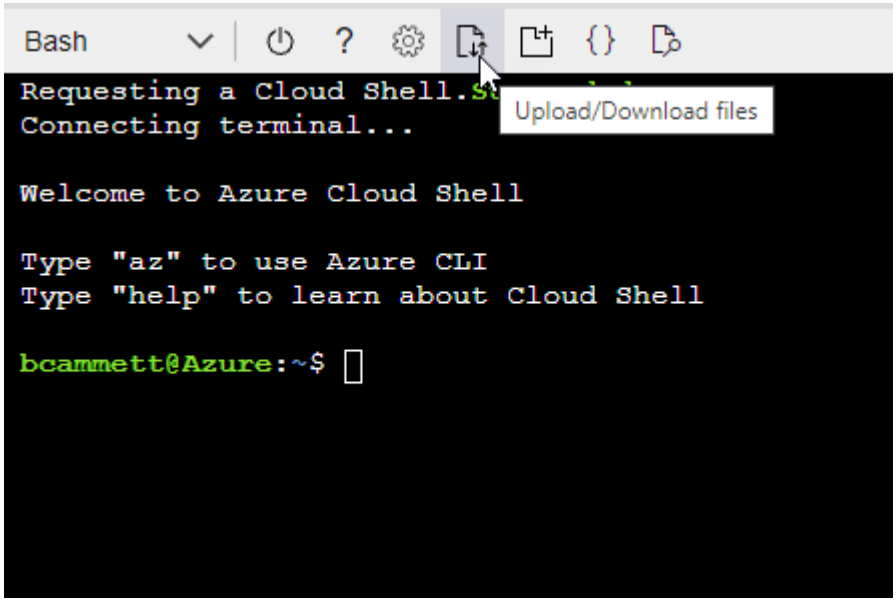
      Beispiel

      ```
      "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:

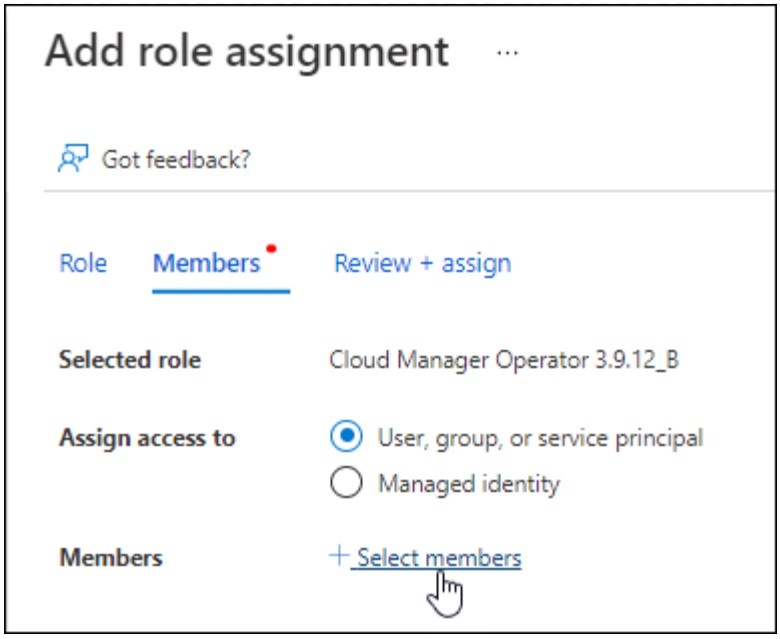
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

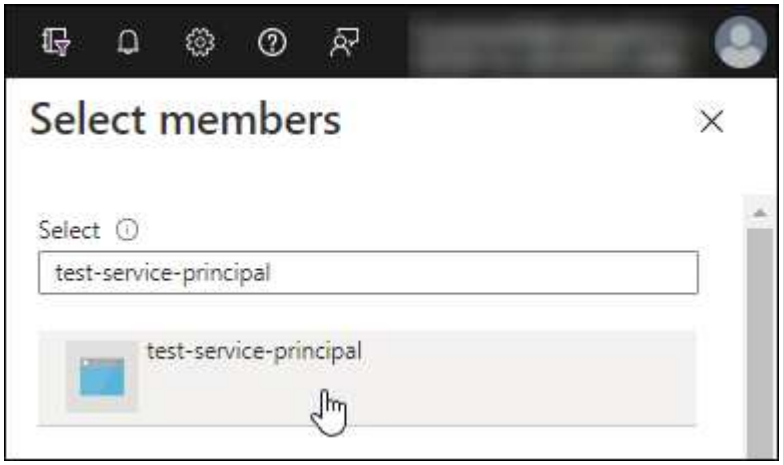
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

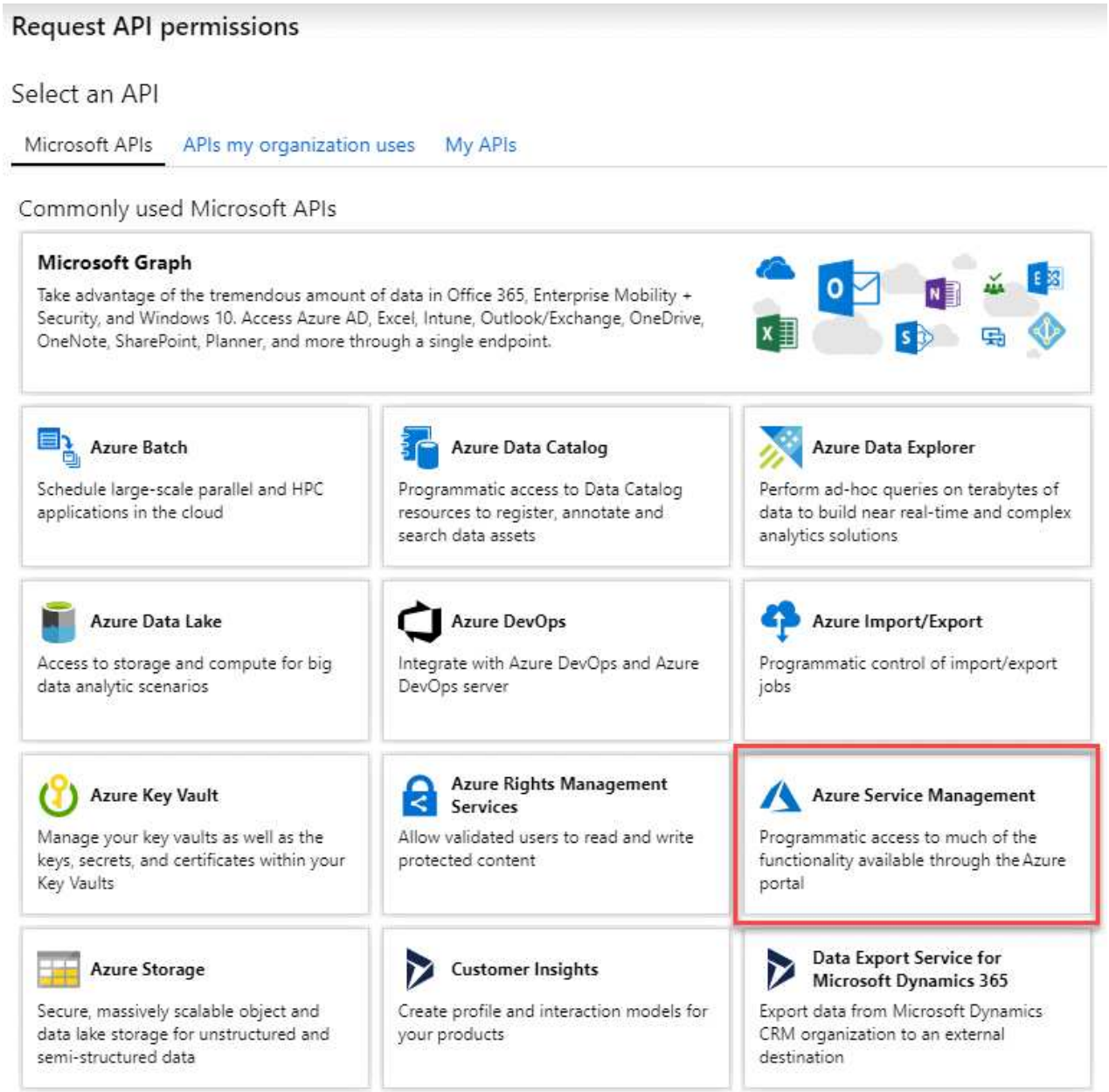
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

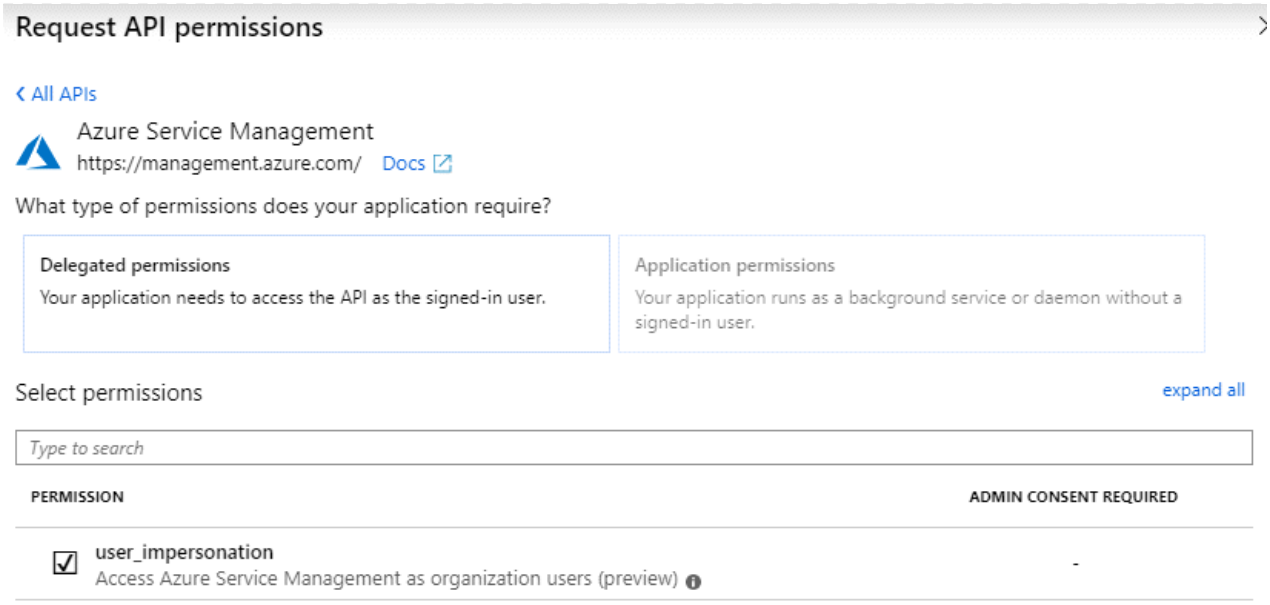
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

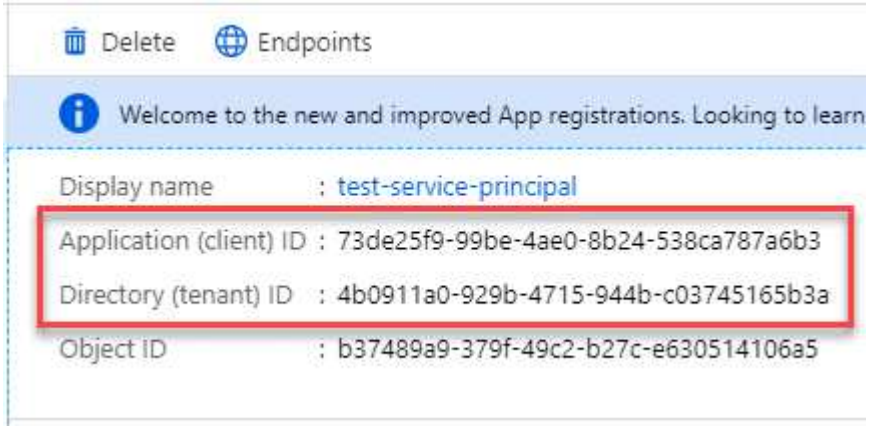


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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.

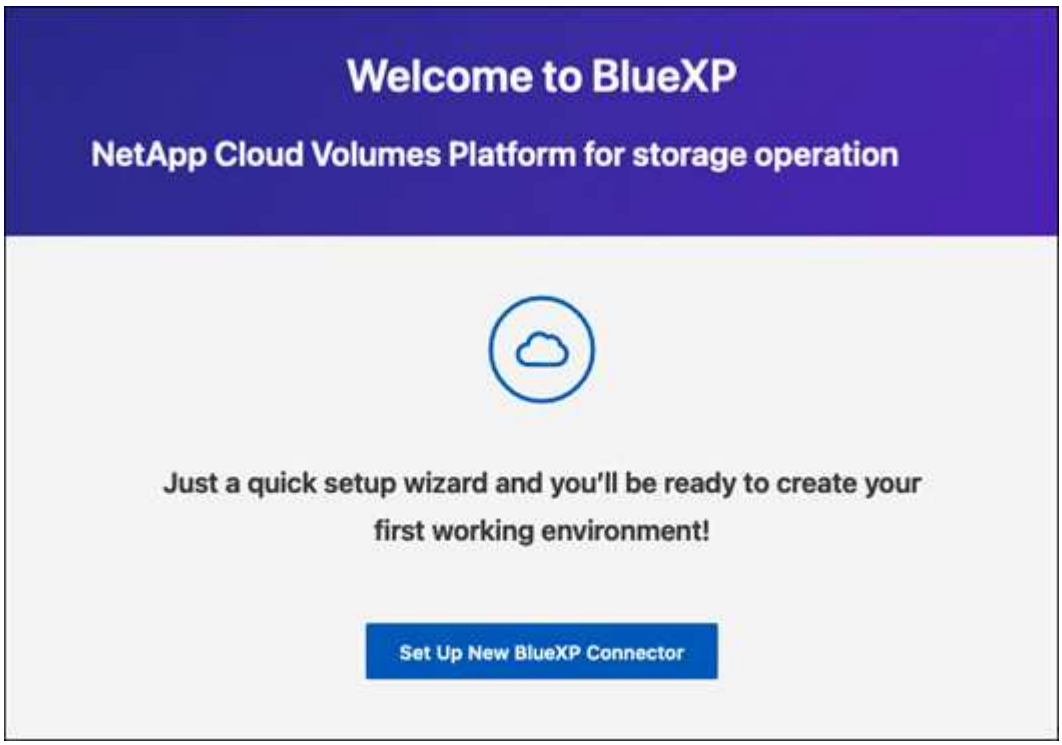
Schritt 2: BlueXP einrichten

Wenn Sie zum ersten Mal die BlueXP Konsole aufrufen, werden Sie aufgefordert, BlueXP einzurichten.

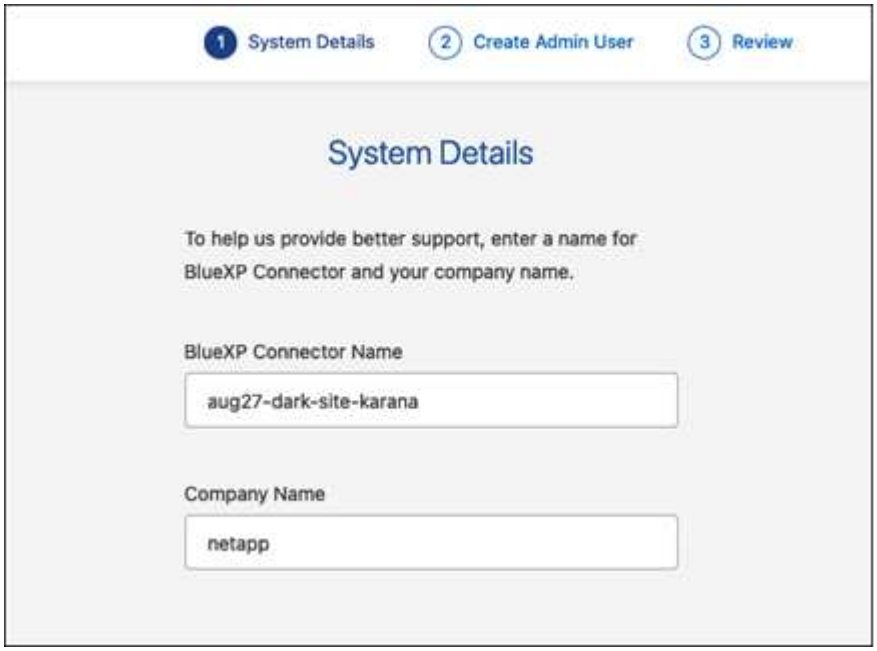
Schritte

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.