



Los geht's

BlueXP setup and administration

NetApp
August 29, 2025

Inhalt

Los geht's	1
Lernen Sie die Grundlagen kennen	1
Erfahren Sie mehr über BlueXP	1
Erfahren Sie mehr über BlueXP -Steckverbinder	5
Weitere Informationen zu BlueXP Implementierungsmodi	9
Beginnen Sie mit dem Standardmodus	21
Erste Schritte Workflow (Standardmodus)	21
Bereiten Sie das Netzwerk für die BlueXP -Konsole vor	22
Melden Sie sich bei BlueXP an oder melden Sie sich an	23
Einen Konnektor erstellen	25
Abonnieren Sie NetApp Intelligent Services (Standardmodus)	148
Nächste Schritte (Standardmodus)	154
Beginnen Sie mit dem eingeschränkten Modus	154
Erste Schritte im Workflow (eingeschränkter Modus)	154
Bereiten Sie die Bereitstellung im eingeschränkten Modus vor	155
Stellen Sie den Connector im eingeschränkten Modus bereit	176
Abonnieren Sie NetApp Intelligent Services (eingeschränkter Modus)	189
Nächste Schritte (eingeschränkter Modus)	196
Starten Sie mit dem privaten Modus	196
Erste Schritte Workflow (privater Modus)	197
Bereiten Sie die Bereitstellung im privaten Modus vor	197
Stellen Sie den Connector im privaten Modus bereit	215
Nächste Schritte (privater Modus)	220

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 Software-as-a-Service-Plattform (SaaS) umfasst Services für Storage-Management, Datenmobilität, Datensicherung sowie Datenanalyse und -Kontrolle. Managementfunktionen werden über eine webbasierte Konsole und APIs bereitgestellt.

Funktionen

BlueXP bietet einheitliche Storage-Kontrolle in Ihrer Hybrid-Multi-Cloud-Umgebung und integrierte Datenservices zum Schutz, zur Sicherung und Optimierung Ihrer Daten.

Einheitliche Storage-Kontrolle über den BlueXP Arbeitsbereich

Mit dem *BlueXP Canvas* können Sie Cloud- und lokalen Speicher entdecken, bereitstellen und verwalten. Die Leinwand zentralisiert die Speicherverwaltung.

Unterstützter Storage in der Cloud und On-Premises

Mit BlueXP können Sie die folgenden Storage-Typen über den BlueXP -Bildschirm managen:

Cloud-Storage-Lösungen

- Amazon FSX für NetApp ONTAP
- Azure NetApp Dateien
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

On-Premises-Flash- und Objekt-Storage

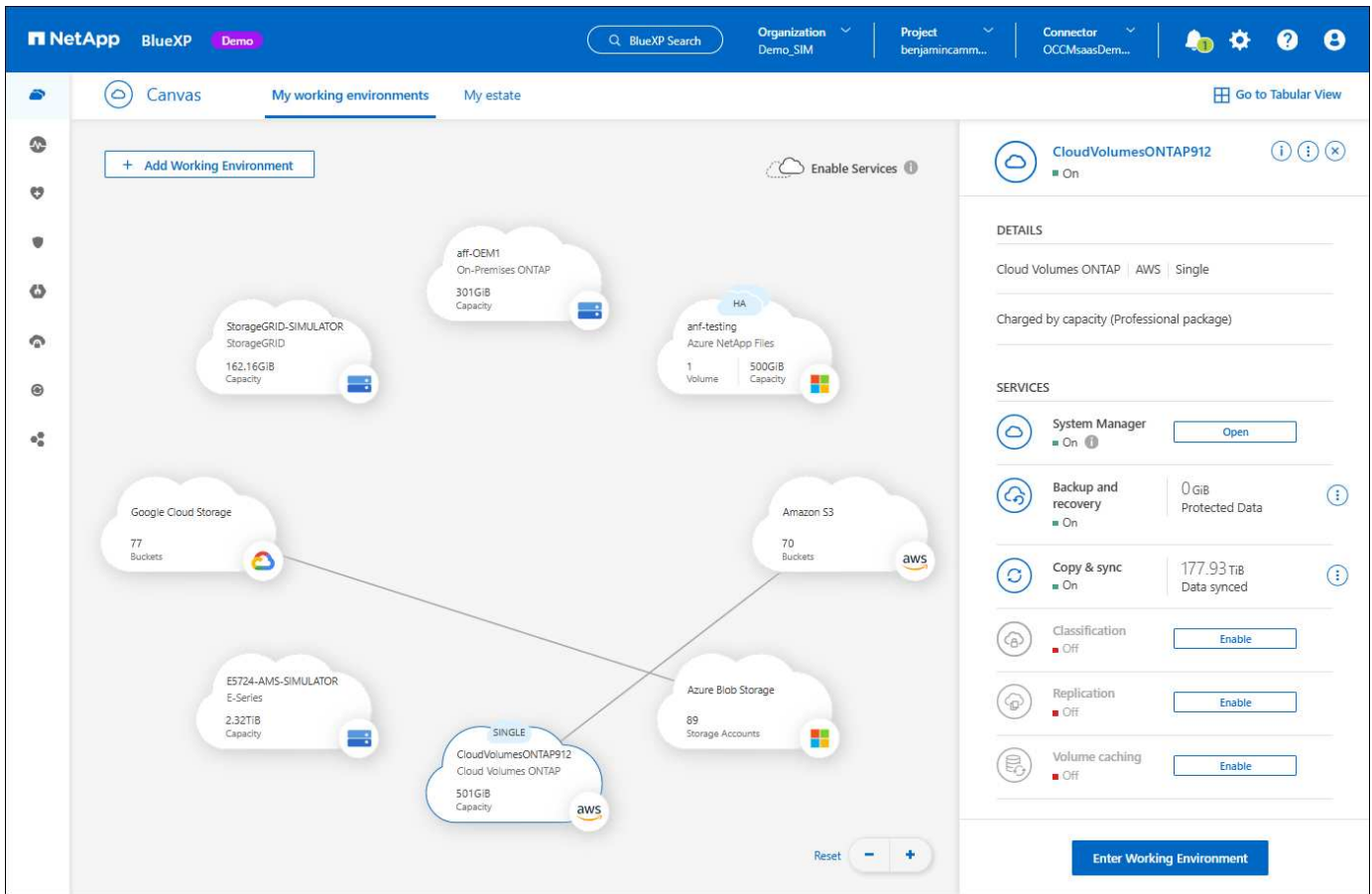
- E-Series Systeme
- ONTAP Cluster
- StorageGRID Systeme

Cloud-Objekt-Storage

- Amazon S3 Storage
- Azure Blob Storage
- Google Cloud Storage

Storage-Management von Arbeitsumgebungen

Auf der BlueXP-Leinwand stellen Arbeitsumgebungen erkannten oder bereitgestellten Speicher dar. Sie können eine Arbeitsumgebung auswählen, um sie in BlueXP-Datendienste zu integrieren oder Speicher zu verwalten, z. B. durch Hinzufügen von Volumes.



Integrierte Services zum Schutz, zur Sicherung und zur Optimierung von Daten

BlueXP umfasst Datendienste zum Sichern und Aufrechterhalten der Datenverfügbarkeit im gesamten Speicher.

BlueXP -Warnmeldungen

Sie erhalten Probleme im Zusammenhang mit Kapazität, Verfügbarkeit, Performance, Sicherung und Sicherheit in Ihrer ONTAP-Umgebung.

BlueXP Automatisierungskatalog

Verwenden Sie skriptbasierte Lösungen, um die Implementierung und Integration von NetApp Produkten und Services zu automatisieren.

BlueXP Backup und Recovery

Sichern und Wiederherstellen von Cloud- und lokalen Daten.

BlueXP Klassifizierung

Sorgen Sie für den Schutz Ihrer Applikationsdaten und Cloud-Umgebungen.

BlueXP Kopier- und Synchronisierungsfunktion

Synchronisieren Sie Daten zwischen lokalen und Cloud-Datenspeichern.

BlueXP Digital Advisor

Prädiktive Analysen und proaktiver Support optimieren die Dateninfrastruktur

Das Digital Wallet von BlueXP

Verwalten und überwachen Sie Ihre Lizenzen und Abonnements.

BlueXP Disaster Recovery

Schützen Sie lokale VMware-Workloads mit VMware Cloud on Amazon FSX for ONTAP als Disaster-Recovery-Standort.

Wirtschaftliche Effizienz von BlueXP

Identifizieren Sie Cluster mit aktueller oder prognostizierter niedriger Kapazität und implementieren Sie Daten-Tiering oder zusätzliche Kapazitätsempfehlungen.

BlueXP vor Ransomware-Schutz

Erkennen Sie Anomalien, die möglicherweise zu Ransomware-Angriffen führen. Schutz und Recovery von Workloads

BlueXP Replizierung

Replizieren Sie Daten zwischen Storage-Systemen, um Backup und Disaster Recovery zu unterstützen.

BlueXP Software-Updates

Automatisierung von Bewertung, Planung und Ausführung von ONTAP Upgrades

BlueXP NachhaltigkeitssDashboard

Analysieren Sie die Nachhaltigkeit Ihrer Storage-Systeme

BlueXP Tiering

Erweitern Sie Ihren lokalen ONTAP -Speicher auf die Cloud.

BlueXP Volume-Caching

Erstellen Sie ein schreibbares Cache-Volume, um den Zugriff auf Daten zu beschleunigen oder den Datenverkehr von Volumes zu reduzieren, auf die sehr viel zugegriffen wird.

BlueXP -Workload ist werkseitig eingestellt

Entwerfen, Einrichten und Betreiben wichtiger Workloads mit Amazon FSX für NetApp ONTAP

["Erfahren Sie mehr über BlueXP und die verfügbaren Datenservices"](#)

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 von Ihnen genutzten Diensten ab. ["Weitere Informationen zu den Preisen für BlueXP"](#)

Funktionsweise von BlueXP

BlueXP umfasst eine webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird, ein Ressourcen- und Zugriffsverwaltungssystem, Connectors, die Arbeitsumgebungen verwalten und BlueXP -Cloud-Services ermöglichen, sowie verschiedene Bereitstellungsmodi, die Ihren Geschäftsanforderungen entsprechen.

Software-as-a-Service

Der Zugriff auf BlueXP ist über ein ["Webbasierte Konsole"](#) und APIs möglich. Mit dieser SaaS-Lösung können Sie automatisch auf die neuesten Funktionen zugreifen, sobald diese veröffentlicht wurden, und problemlos zwischen Ihren BlueXP -Organisationen, -Projekten und -Connectors wechseln.

Identitäts- und Zugriffsmanagement (BlueXP , IAM)

Das Identitäts- und Zugriffsmanagement (BlueXP Identity and Access Management, IAM) ist ein Modell für das Ressourcen- und Zugriffsmanagement, das ein granulares Management von Ressourcen und Berechtigungen bietet:

- Eine übergeordnete *Organisation* ermöglicht Ihnen, den Zugriff über Ihre verschiedenen *Projekte* zu verwalten
- *Ordner* ermöglicht Ihnen, verwandte Projekte zu gruppieren
- Mit der Ressourcenverwaltung können Sie eine Ressource einem oder mehreren Ordnern oder Projekten zuordnen
- Mit der Zugriffsverwaltung können Sie Mitgliedern auf verschiedenen Ebenen der Unternehmenshierarchie eine Rolle zuweisen

BlueXP IAM wird unterstützt, wenn Sie BlueXP im Standard- oder eingeschränkten Modus verwenden. Wenn Sie BlueXP im privaten Modus verwenden, verwalten Sie Arbeitsbereiche, Benutzer und Ressourcen über ein BlueXP-Konto.

- ["Erfahren Sie mehr über BlueXP IAM"](#)

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. Mit einem Connector können Sie Ressourcen und Prozesse in Ihren lokalen und Cloud-Umgebungen verwalten. Sie benötigen ihn für die Verwaltung von Arbeitsumgebungen (z. B. Cloud Volumes ONTAP) und für die Nutzung vieler BlueXP -Dienste.

["Erfahren Sie mehr über Steckverbinder"](#).

Bereitstellungsmodi

BlueXP bietet drei Implementierungsmodi. *Standard Mode* nutzt die BlueXP Software as a Service (SaaS) Ebene, um den vollen Funktionsumfang zu bieten. Wenn in Ihrer Umgebung Einschränkungen hinsichtlich Sicherheit und Konnektivität bestehen, beschränken *eingeschränkter Modus* und *privater Modus* die ausgehende Verbindung zur BlueXP SaaS-Ebene.

["Weitere Informationen zu den BlueXP Implementierungsmodi"](#).

SOC 2 Typ 2-Zertifizierung

Eine unabhängige Wirtschaftsprüfungsgesellschaft und ein Wirtschaftsprüfer haben BlueXP geprüft und bestätigt, dass BlueXP SOC 2 Typ 2-Berichte auf Grundlage der geltenden Trust Services-Kriterien erhalten hat.

["SOC 2-Berichte von NetApp anzeigen"](#)

Erfahren Sie mehr über BlueXP -Steckverbinder

A *Connector* ist die NetApp Software, die in Ihrem Cloud-Netzwerk oder Ihrem On-Premises-Netzwerk ausgeführt wird. Es wird verwendet, um die Dienste von BlueXP mit Ihren Speicherumgebungen zu verbinden.

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:

- Amazon FSX für NetApp ONTAP

Für einige Aktionen ist eine Verknüpfung für den Connector oder die Werkseinstellungen des BlueXP - Workloads erforderlich. ["Erfahren Sie, welche Aktionen einen Konnektor oder eine Verknüpfung erfordern"](#)

- Automatisierungskatalog
- 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
- Digital Wallet (nur Lizenzen, Abonnement-Überwachung erfordert einen Connector)

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.

["Erfahren Sie mehr über Erkennungs- und Verwaltungsoptionen für lokale ONTAP-Cluster"](#)

- Software-Updates
- Nachhaltigkeit
- Arbeitslast Fabrik

Wenn ein Stecker erforderlich ist

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

- Meldungen

- 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
- Google Cloud Storage Buckets
- On-Premises-ONTAP-Cluster-Integration in BlueXP-Datenservices
- 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 gemäß der Dokumentation betrieben wird, können die Funktionalität und der Betrieb des Produkts sowie Ihre Rechte gemäß der EULA beeinträchtigt werden.

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 für die Cloud Volumes ONTAP-Systeme bereitgestellt ["Azure Region Paar"](#) werden. Diese Anforderung sorgt dafür, dass eine Azure Private Link-Verbindung zwischen Cloud Volumes ONTAP und ihren 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

Kommunikation mit Cloud-Providern

Der Connector verwendet TLS 1.3 für die gesamte Kommunikation zu AWS, Azure und Google Cloud.

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 installieren Sie einen Connector

Sie können einen Connector direkt von BlueXP, vom Marktplatz Ihres Cloud-Anbieters oder durch manuelle Installation der Software auf Ihrem eigenen Linux-Host installieren. 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"](#)
 - ["Einrichten von Clouberechtigungen für lokale Bereitstellungen"](#)
- ["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"](#)

Es liegt in Ihrer Verantwortung, die Connector-Richtlinien zu aktualisieren, wenn in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

Connector-Upgrades

Wir aktualisieren die Connector-Software in der Regel jeden Monat, um neue Funktionen einzuführen und Stabilitätsverbesserungen zu ermöglichen. Während die meisten Dienste und Funktionen der BlueXP - Plattform über SaaS-basierte Software angeboten werden, sind einige Funktionen von der Version des Connectors abhängig. Dazu gehören die Verwaltung von Cloud Volumes ONTAP, die Verwaltung von ONTAP-Clustern vor Ort, 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 ausreichenden 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, wenn Sie den privaten Modus verwenden"](#).

Betriebssystem- und VM-Wartung

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

Beachten Sie, dass Sie (Kunde) keine Dienste auf dem Connector-Host anhalten müssen, wenn Sie kleinere Sicherheitsupdates anwenden.

Wenn Sie (Kunde) die Connector VM anhalten und dann starten müssen, sollten Sie dies von der 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 und Steckverbinder

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.

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 Multicloud-Umgebung (z. B. AWS und Azure) und möchten lieber einen Connector in AWS und einen anderen in Azure haben. Jedes managt die Cloud Volumes ONTAP Systeme, die in diesen Umgebungen ausgeführt werden.

- Ein Service-Provider nutzt möglicherweise eine BlueXP Organisation, um ihren Kunden Services bereitzustellen, während ein anderes Unternehmen für Disaster Recovery für einen seiner Geschäftseinheiten einsetzt. Jedes Unternehmen verfügt über separate Connectors.

Weitere Informationen zu BlueXP Implementierungsmodi

BlueXP bietet *Bereitstellungsmodi*, mit denen Sie Ihre Geschäfts- und Sicherheitsanforderungen erfüllen können. Der *Standardmodus* nutzt eine Software-as-a-Service-Schicht (SaaS), um die volle Funktionalität bereitzustellen, während der *eingeschränkte Modus* und der *private Modus* für Organisationen mit Konnektivitätsbeschränkungen verfügbar sind.

Während BlueXP den Verkehrs-, Kommunikations- und Datenfluss bei Verwendung des eingeschränkten oder privaten Modus hemmt, liegt es in Ihrer Verantwortung sicherzustellen, dass Ihre Umgebung (vor Ort und in der Cloud) den erforderlichen Vorschriften für Ihr Unternehmen entspricht.

Überblick

Jeder Bereitstellungsmodus unterscheidet sich hinsichtlich ausgehender Konnektivität, Standort, Installation, Authentifizierung, Datendiensten und Abrechnungsmethoden.

Standardmodus

Sie nutzen einen SaaS-Dienst über die webbasierte Konsole. Abhängig von den Datendiensten und Funktionen, die Sie verwenden möchten, erstellt ein BlueXP-Administrator einen oder mehrere Connectors, um die Daten in Ihrer Hybrid-Cloud-Umgebung zu verwalten.

Dieser Modus verwendet verschlüsselte Datenübertragung über das öffentliche Internet.

Eingeschränkter Modus

Sie installieren einen BlueXP Connector in der Cloud (in einer staatlichen, souveränen oder kommerziellen Region) und dieser verfügt über eine eingeschränkte ausgehende Konnektivität zur BlueXP 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

Sie installieren einen BlueXP Connector vor Ort oder in der Cloud (in einer sicheren Region, einer souveränen Cloud-Region oder einer kommerziellen Region) und haben *keine* Verbindung zur BlueXP SaaS-Schicht. Benutzer greifen lokal auf die vom Connector bereitgestellte BlueXP-Konsole zu, nicht auf die SaaS-Ebene.

Eine sichere Region umfasst ["AWS Secret Cloud"](#), ["Top Secret Cloud von AWS"](#), und ["Azure IL6"](#)

Die folgende Tabelle enthält einen Vergleich dieser Modi.

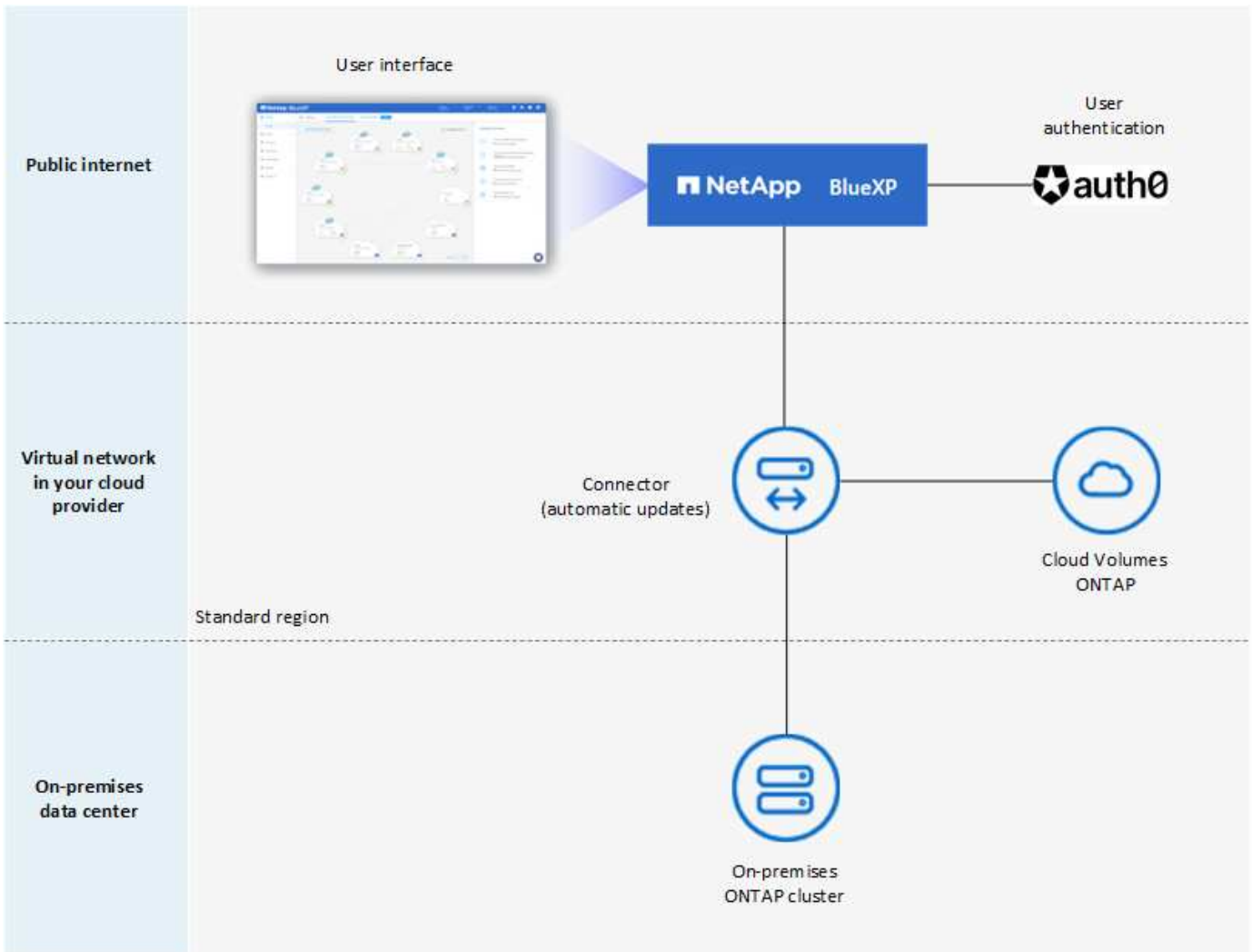
	Standardmodus	Eingeschränkter Modus	Privater Modus
Verbindung zur BlueXP SaaS-Ebene erforderlich?	Ja.	Nur ausgehend	Nein

	Standardmodus	Eingeschränkter Modus	Privater Modus
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
Multi-Faktor-Authentifizierung	Verfügbar für lokale Benutzer	Nicht verfügbar	Nicht verfügbar
Storage- und Datenservices	Alle werden unterstützt	Viele werden unterstützt	Es werden mehrere unterstützt
Lizenzierungsoptionen für Datendienste	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

Sie können den Connector mit dem BlueXP-Setup-Assistenten, AWS oder Azure Marketplace, dem Google Cloud SDK oder einem manuellen Installationsprogramm auf einem Linux-Host in Ihrem Rechenzentrum oder Ihrer Cloud installieren.

Connector-Upgrades

BlueXP bietet automatisierte Upgrades der Connector-Software mit monatlichen Updates.

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

BlueXP bietet Authentifizierung mit Auth0- oder NetApp Support Site (NSS)-Anmeldungen. 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.

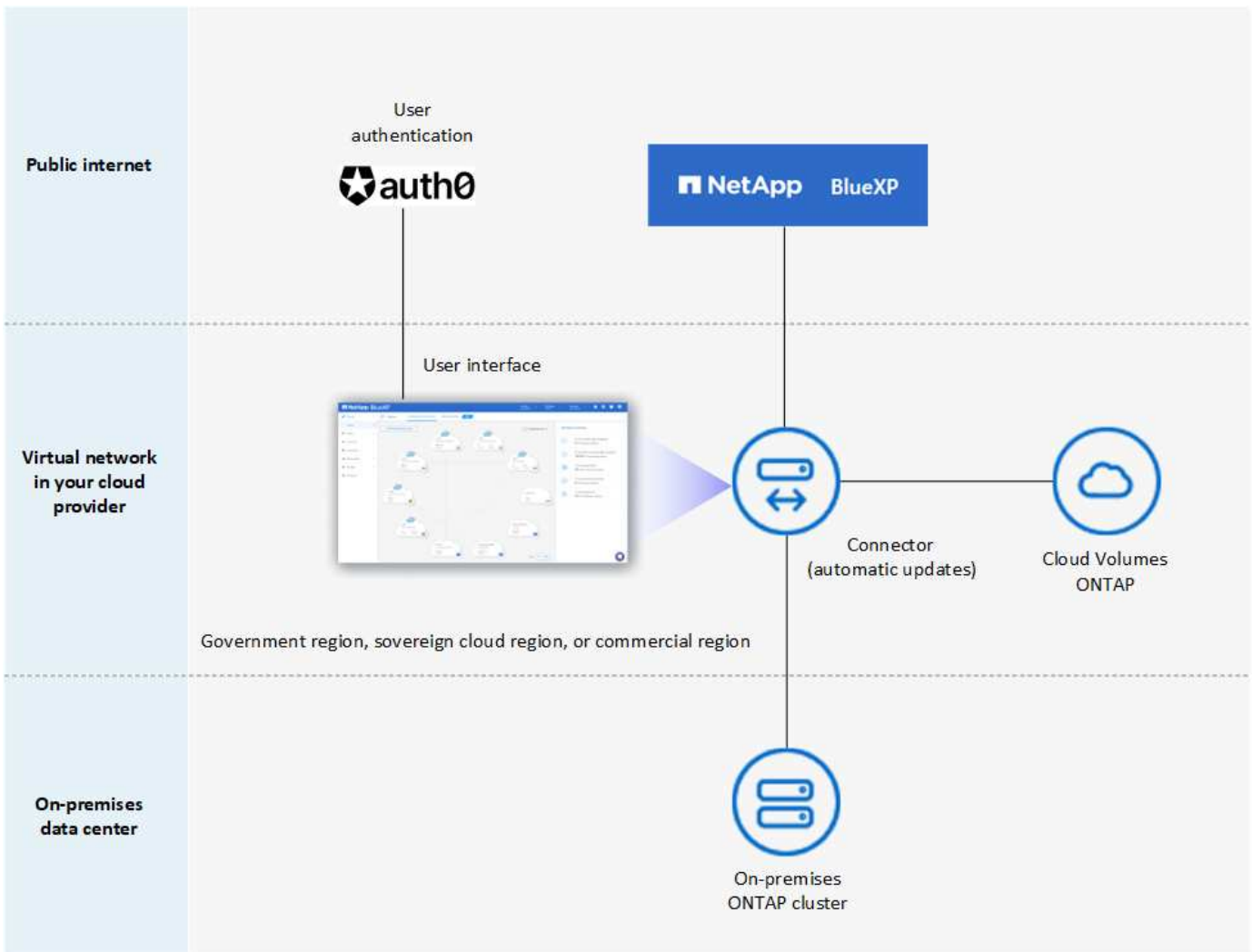
Erste Schritte mit dem Standardmodus

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

Der Connector erfordert eine ausgehende Verbindung zur BlueXP SaaS-Schicht für Datendienste, Software-Upgrades, Authentifizierung und Metadatenübertragung.

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

BlueXP bietet automatisierte Upgrades der Connector-Software mit monatlichen Updates.

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
Azure NetApp Dateien	Volle Unterstützung
Backup und Recovery	Wird in Regierungsregionen und kommerziellen Regionen mit eingeschränktem Modus unterstützt. Wird in souveränen Regionen mit eingeschränktem Modus nicht unterstützt. Im eingeschränkten Modus unterstützt BlueXP backup and recovery nur die Sicherung und Wiederherstellung von ONTAP Volume-Daten. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Daten an" Im eingeschränkten Modus unterstützt BlueXP backup and recovery nur die Sicherung und Wiederherstellung von ONTAP Volume-Daten. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Daten an" Das Sichern und Wiederherstellen von Anwendungsdaten und Daten virtueller Maschinen wird nicht unterstützt.
Klassifizierung	Unterstützt in Regierungsregionen mit eingeschränktem Modus. Nicht unterstützt in kommerziellen Regionen oder in souveränen Regionen mit eingeschränktem Modus.
Cloud Volumes ONTAP	Volle Unterstützung
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 einen lokalen Cluster mit einem Connector entdecken, 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 keine Organisation haben, werden Sie aufgefordert, Ihre Organisation zu erstellen und den eingeschränkten Modus zu aktivieren, wenn Sie sich zum ersten Mal von einem Connector aus bei BlueXP anmelden, den Sie manuell installiert oder im Marktplatz Ihres Cloud-Anbieters erstellt haben.

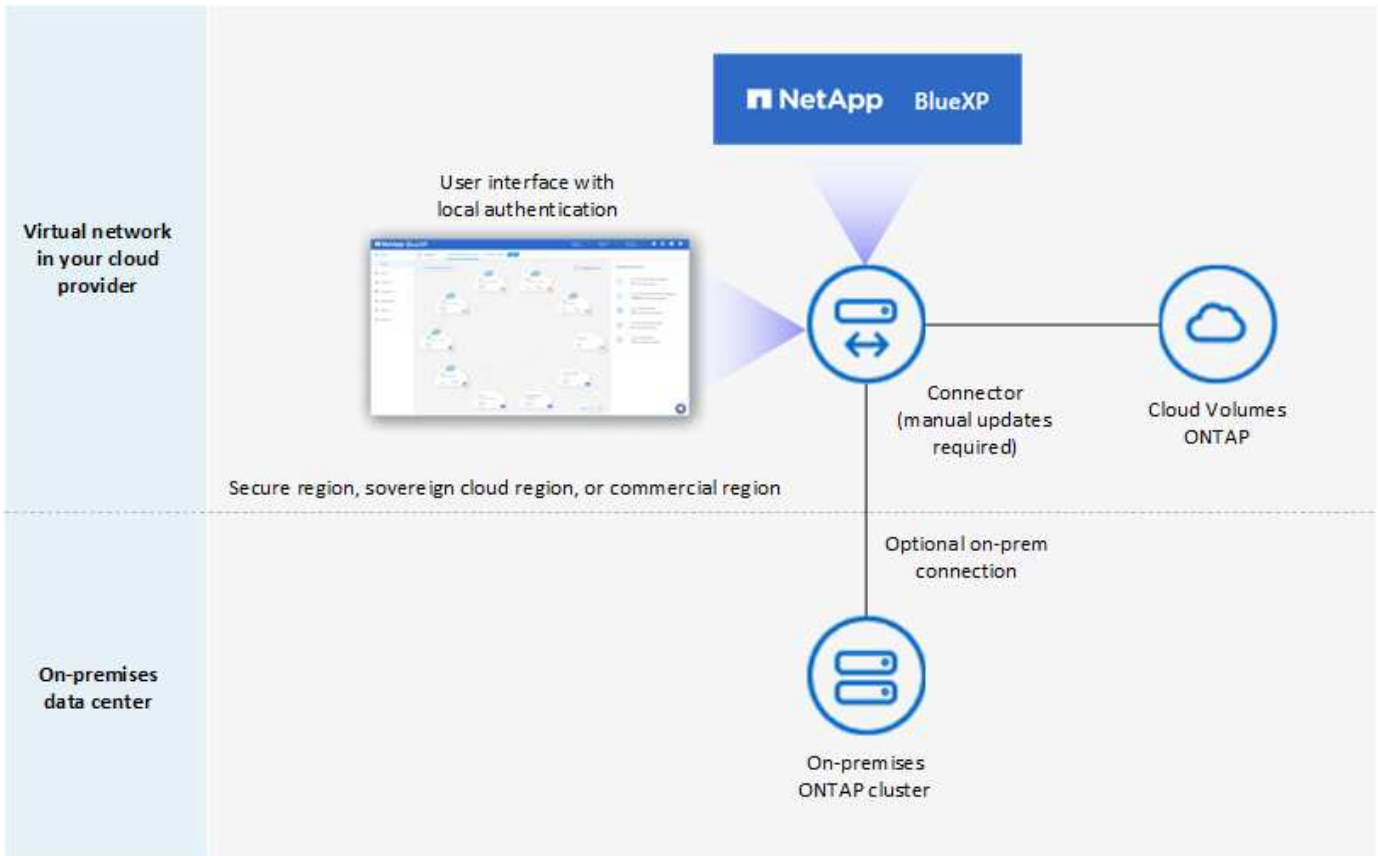
Beachten Sie, dass Sie die Einstellung für den eingeschränkten Modus nicht ändern können, nachdem BlueXP die Organisation erstellt hat. Der eingeschränkte Modus kann später nicht aktiviert werden, und Sie können ihn später nicht mehr deaktivieren.

- ["Erfahren Sie, wie Sie mit dem eingeschränkten Modus beginnen"](#).

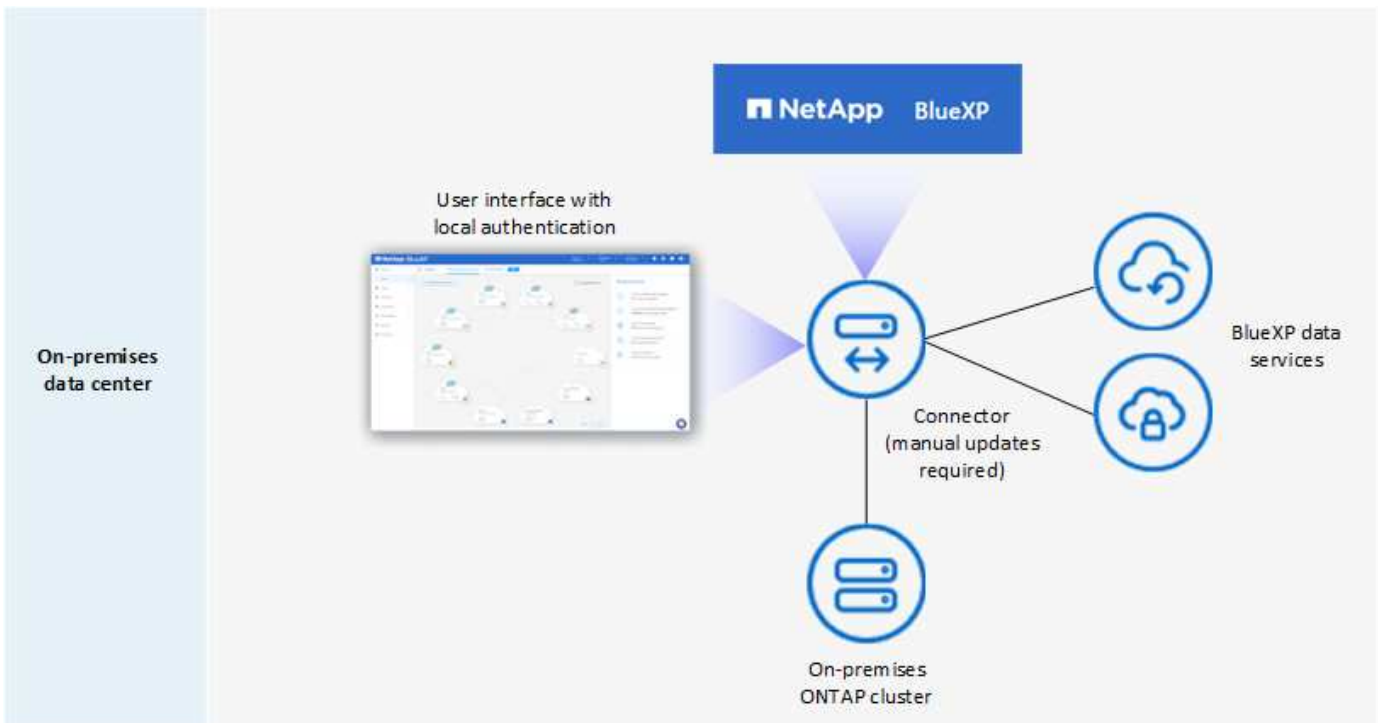
Privater Modus

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.



Die zweite Abbildung zeigt ein Beispiel einer Private-Mode-Implementierung, bei der der Connector vor Ort installiert wird, 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	Wird in kommerziellen AWS- und Azure-Regionen unterstützt. Wird nicht unterstützt in Google Cloud oder in "AWS Secret Cloud" , "Top Secret Cloud von AWS" , oder "Azure IL6" Im privaten Modus unterstützt BlueXP backup and recovery nur die Sicherung und Wiederherstellung von ONTAP Volume-Daten. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Daten an" Das Sichern und Wiederherstellen von Anwendungsdaten und Daten virtueller Maschinen wird nicht unterstützt.
Cloud Volumes ONTAP	Da es keinen Internetzugang gibt, sind die folgenden Funktionen nicht verfügbar: Automatisierte Software-Upgrades und AutoSupport.
Digitale Briefftasche	Sie können das Digital Wallet mit den unten aufgeführten unterstützten Lizenzierungsoptionen für den privaten Modus verwenden.

Unterstützte Services	Hinweise
On-Premises ONTAP Cluster	<p>Erfordert Konnektivität aus der Cloud (wo der Connector installiert ist) zur On-Premises-Umgebung.</p> <p>Erkennung ohne Connector (direkte Erkennung) wird nicht unterstützt.</p>

Unterstützte BlueXP -Dienste in lokalen Bereitstellungen

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

Unterstützte Services	Hinweise
Backup und Recovery	<p>Im privaten Modus unterstützt BlueXP backup and recovery nur die Sicherung und Wiederherstellung von ONTAP Volume-Daten. "Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Volume-Daten an"</p> <p>Backup und Restore von Applikationsdaten und Virtual Machine-Daten werden nicht unterstützt.</p>
Klassifizierung	<ul style="list-style-type: none"> Die einzigen unterstützten Datenquellen sind die, die Sie lokal ermitteln können. <p>"Zeigen Sie die Quellen an, die Sie lokal ermitteln können"</p> <ul style="list-style-type: none"> Funktionen, für die ein abgehender Internetzugang erforderlich ist, werden nicht unterstützt. <p>"Zeigen Sie die Funktionseinschränkungen an"</p>
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 die BlueXP digital wallet 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	Nein	Nein
	Amazon S3	Nein	Nein
	Azure Blob	Nein	Nein
	Azure NetApp Dateien	Ja.	Nein
	Cloud Volumes ONTAP	Ja.	Ja.
	Google Cloud NetApp Volumes	Nein	Nein
	Google Cloud Storage	Nein	Nein
	On-Premises-ONTAP-Cluster	Ja.	Ja.
	E-Series	Nein	Nein
	StorageGRID	Nein	Nein

Produktbereich	BlueXP Service oder Feature	Eingeschränkter Modus	Privater Modus
Services	Meldungen	Nein	Nein
	Backup und Recovery	Ja https://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity ["Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Volume-Daten an"^]	Ja https://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity ["Zeigen Sie die Liste der unterstützten Backup-Ziele für ONTAP-Volume-Daten an"^]
	Klassifizierung	Ja.	Ja.
	Kopieren und Synchronisieren	Nein	Nein
	Digitaler Berater	Nein	Nein
	Digitale Brieftasche	Ja.	Ja.
	Disaster Recovery	Nein	Nein
	Wirtschaftliche Effizienz	Nein	Nein
	Schutz durch Ransomware	Nein	Nein
	Replizierung	Ja.	Ja.
	Software-Updates	Nein	Nein
	Nachhaltigkeit	Nein	Nein
	Tiering	Nein	Nein
	Volume-Caching	Nein	Nein
Arbeitslast Fabrik	Nein	Nein	
Eigenschaften	Identitäts- und Zugriffsmanagement	Ja.	Ja.
	Anmeldedaten	Ja.	Ja.
	Föderation	Ja.	Nein
	Multi-Faktor-Authentifizierung	Ja.	Nein
	NSS-Konten	Ja.	Nein
	Benachrichtigungen	Ja.	Nein
	Suche	Ja.	Nein
	Zeitachse	Ja.	Ja.

Beginnen Sie mit dem Standardmodus

Erste Schritte Workflow (Standardmodus)

Beginnen Sie mit BlueXP im Standardmodus, indem Sie das Netzwerk für die BlueXP-Konsole vorbereiten, sich anmelden und ein Konto erstellen, optional einen Connector erstellen und NetApp Intelligent Services abonnieren.

Im Standardmodus greifen Sie auf eine webbasierte Konsole zu, die als Software-as-a-Service (SaaS)-Produkt von NetApp gehostet wird. Bevor Sie beginnen, sollten Sie ein Verständnis von und haben ["Bereitstellungsmodi"](#) ["Anschlüsse"](#).

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 eine Organisation"](#)

Gehen Sie zu ["BlueXP-Konsole"](#) und melden Sie sich an. Sie haben die Möglichkeit, eine Organisation zu erstellen. Sie können diesen Schritt jedoch überspringen, wenn Sie zu einer bestehenden Organisation 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.

Sie können 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"](#)

Beachten Sie: Wenn Sie NetApp Intelligent Data Services zum Verwalten von Speicher und Daten in Google Cloud verwenden möchten, muss der Connector in Google Cloud ausgeführt werden. Beachten Sie: Wenn Sie NetApps intelligente Datendienste zum Verwalten von Speicher und Daten in Google Cloud verwenden möchten, muss der Connector in Google Cloud ausgeführt werden.

4

"Abonnieren Sie NetApp Intelligent Services (optional)"

Abonnieren Sie NetApp Intelligent Services über den Marktplatz Ihres Cloud-Anbieters und bezahlen Sie Datenservices stundenweise (PAYGO) oder über einen Jahresvertrag. NetApp Intelligent Services umfassen Backup und Recovery, Cloud Volumes ONTAP, Tiering, Ransomware-Schutz und Disaster Recovery. Die Klassifizierung ist in Ihrem Abonnement ohne zusätzliche Kosten enthalten.

Bereiten Sie das Netzwerk für die BlueXP -Konsole vor

Wenn Sie sich anmelden und die webbasierte Konsole verwenden, kontaktiert BlueXP mehrere Endpunkte, um die von Ihnen initiierten Aktionen auszuführen. Computer, die auf die Konsole zugreifen, müssen Verbindungen zu diesen Endpunkten haben.

Diese Endpunkte werden in zwei Szenarien kontaktiert:

- Vom Computer eines Benutzers beim Ausfüllen von Abschnitten aus dem ["BlueXP webbasierte Konsole"](#) die als Software as a Service (SaaS) verfügbar ist.
- Vom Computer eines Benutzers beim Öffnen eines Webbrowsers, Eingabe der IP-Adresse des Connectors und anschließende Anmeldung und Einrichtung des Connectors. Diese Schritte sind erforderlich, wenn Sie den Connector manuell installieren.

Endpunkte	Zweck
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	Dies ist der Endpunkt, den Sie in Ihren Webbrowser eingeben, um die webbasierte Konsole zu verwenden.
https://api.bluexp.netapp.com	Die webbasierte Konsole kontaktiert diesen Endpunkt, um mit der API für Aktionen im Zusammenhang mit Autorisierung, Lizenzierung, Abonnements, Anmeldeinformationen, Benachrichtigungen und mehr zu interagieren.
https://aiq.netapp.com	Erforderlich für den Zugriff auf den digitalen Berater.
AWS-Services (amazonaws.com): <ul style="list-style-type: none"> • 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 Einzelheiten finden Sie in der AWS-Dokumentation." Anregung: "Weitere Einzelheiten 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 ermöglichen.
https://widget.intercom.io	Für den In-Product-Chat, der es Ihnen ermöglicht, mit dem NetApp-Support zu sprechen.

Stellen Sie sicher, dass der Connector ausgehenden Internetzugriff auf die Kontaktendpunkte für den täglichen Betrieb hat. Folgen Sie den Links im nächsten Abschnitt, um die Liste dieser Endpunkte anzuzeigen.

Verwandte Informationen

- Bereiten Sie die Vernetzung für den Connector vor
 - ["AWS-Netzwerk einrichten"](#)
 - ["Azure Networking einrichten"](#)
 - ["Google Cloud-Netzwerke einrichten"](#)
 - ["Einrichten des lokalen Netzwerks"](#)
- Networking für BlueXP Services vorbereiten

Informationen zu jedem BlueXP Service finden Sie in der Dokumentation.

["BlueXP-Dokumentation"](#)

Melden Sie sich bei BlueXP an oder melden Sie sich an

Der Zugriff auf BlueXP erfolgt über eine webbasierte Konsole. Wenn Sie mit BlueXP beginnen, müssen Sie sich als Erstes anmelden oder sich mit Ihren Zugangsdaten für die NetApp Support-Website oder SSO-Anmeldeinformationen aus Ihrem Unternehmensverzeichnis anmelden.

Über diese Aufgabe

Wenn Sie BlueXP zum ersten Mal nutzen, können Sie sich mit einer der folgenden Optionen anmelden oder sich anmelden:

BlueXP Anmeldung

Sie können sich anmelden, indem Sie eine BlueXP Anmeldung erstellen. Für diese Authentifizierungsmethode müssen Sie Ihre E-Mail-Adresse und ein Passwort angeben. Nachdem Sie Ihre

E-Mail-Adresse überprüft haben, können Sie sich anmelden und dann eine BlueXP -Organisation erstellen, sofern Sie nicht bereits einer Organisation angehören.

Zugangsdaten für die NetApp Support-Website (NSS)

Wenn Sie bereits über Anmeldedaten für die NetApp Support-Website verfügen, müssen Sie sich nicht bei BlueXP anmelden. Sie melden sich mit Ihren NSS-Anmeldeinformationen an, und dann fordert BlueXP Sie auf, eine BlueXP -Organisation zu erstellen, falls Sie noch nicht zu einer Organisation gehören.

Beachten Sie, dass es sich bei dem Standardpasswort um eine Einmalkennung zur registrierten E-Mail-Adresse handelt. Bei jedem Anmeldeversuch wird eine neue OTP generiert.

Föderierte Verbindung

Sie können sich mit Single Sign-On über Anmeldedaten aus Ihrem Unternehmensverzeichnis (föderierte Identität) anmelden. Der erste Benutzer im Konto Ihres Unternehmens muss sich bei BlueXP anmelden oder sich über NSS-Anmeldedaten anmelden und dann den Identitätsverbund einrichten. Danach können Sie Mitglieder aus Ihrer Corporate Identity zu Ihrem Unternehmen hinzufügen. Diese Benutzer können sich dann mit ihren SSO-Anmeldeinformationen 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. Wenn Sie über ein NetApp-Support-Website-Konto verfügen oder bereits einen Identitätsverbund eingerichtet haben, geben Sie die mit Ihrem Konto verknüpfte E-Mail-Adresse direkt auf der **Anmelden**-Seite ein.

In beiden Fällen werden Sie von BlueXP im Rahmen dieser ersten Anmeldung registriert.

3. Wenn Sie sich mit einem BlueXP Login registrieren möchten, wählen Sie **Registrieren**.
 - a. Geben Sie auf der Seite **Anmelden** die erforderlichen Informationen ein und wählen Sie **Weiter**.

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

- b. In Ihrem Posteingang finden Sie eine E-Mail von NetApp, die Anweisungen zur Überprüfung Ihrer E-Mail-Adresse enthält.

Dieser Schritt ist erforderlich, bevor Sie sich bei BlueXP anmelden können.

4. Lesen Sie nach der Anmeldung die Endbenutzer-Lizenzvereinbarung durch, und akzeptieren Sie die Bedingungen.


Wenn Ihr Benutzerkonto noch nicht zu einer BlueXP -Organisation gehört, werden Sie aufgefordert, ein Benutzerkonto zu erstellen.

5. Geben Sie auf der Seite **Willkommen** einen Namen für Ihre BlueXP -Organisation ein.

Ein Unternehmen ist das wichtigste Element im BlueXP -Identitäts- und Zugriffsmanagement (IAM). ["Erfahren Sie mehr über BlueXP IAM"](#).

Wenn Ihr Unternehmen bereits über eine BlueXP -Organisation verfügt und Sie ihr beitreten möchten, sollten Sie BlueXP schließen und den Eigentümer bitten, Sie der Organisation zuzuordnen. Nachdem der Besitzer Sie hinzugefügt hat, können Sie sich einloggen und haben Zugriff auf das Konto. ["Erfahren Sie, wie Sie Mitglieder zu einer bestehenden Organisation hinzufügen"](#).

Hi Anand,
Welcome to NetApp BlueXP



Let's get started by creating an organization

If the organization has already been created, it's best to ask the organization admin to add you to it. [Learn how to add user](#)

Connector name

Organization name

Are you running in a secured environment? ^

Use restricted deployment mode to disconnect this account from the BlueXP backend services. Restricted deployments are often required in extremely secure or regulated environments. Note: Use this option only if you're sure you need it as some BlueXP functionality is not available in restricted deployments.

[Learn more about BlueXP deployment modes](#)

Enable restricted mode on this account

Let's Start

6. Wählen Sie **Start**.

Ergebnis

Sie verfügen jetzt über einen BlueXP -Login und ein Unternehmen. 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

Sie können einen Connector in AWS direkt aus BlueXP erstellen. 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 eine haben ["Verständnis von Steckverbindern"](#).
- 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
<p>AWS-Services (amazonaws.com):</p> <ul style="list-style-type: none"> • 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) 	<p>Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"</p>
<p>https://support.netapp.com https://mysupport.netapp.com</p>	<p>Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.</p>
<p>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</p>	<p>Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen.</p>
<p>Wählen Sie zwischen zwei Endpunktsätzen:</p> <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> • Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p> 	<p>Um Bilder für Connector-Upgrades zu erhalten.</p>

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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"](#)

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:

Diese Richtlinie enthält nur die Berechtigungen, die zum Starten der Connector-Instanz in AWS von BlueXP erforderlich sind. Wenn BlueXP den Connector erstellt, wendet es einen neuen Satz an Berechtigungen auf die Connector-Instanz an, sodass der Connector AWS Ressourcen managen kann. ["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](#)".
- Wenn BlueXP den Connector erstellt, werden eine IAM-Rolle und ein Instanzprofil für die Instanz erstellt. Diese Rolle umfasst Berechtigungen, mit denen der Connector AWS Ressourcen managen kann. Sie müssen sicherstellen, dass die Rolle immer auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Versionen hinzugefügt werden. "[Erfahren Sie mehr über die IAM-Richtlinie für den Connector](#)".

Bevor Sie beginnen

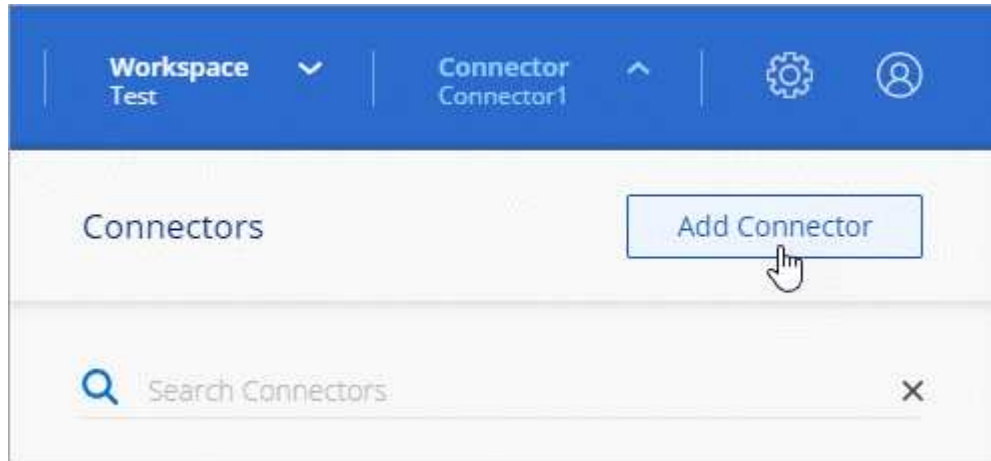
Sie sollten Folgendes haben:

- 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

Sie erstellen einen Connector in AWS direkt über 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 eine haben ["Verständnis von Steckverbindern"](#).
- 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
<p>AWS-Services (amazonaws.com):</p> <ul style="list-style-type: none">• 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)	<p>Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"</p>
<p>https://support.netapp.com https://mysupport.netapp.com</p>	<p>Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.</p>
<p>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</p>	<p>Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen.</p>
<p>Wählen Sie zwischen zwei Endpunktsätzen:</p> <ul style="list-style-type: none">• Option 1 (empfohlen) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io• Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	<p>Um Bilder für Connector-Upgrades zu erhalten.</p>

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

Proxy-Server

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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

8 Kerne oder 8 vCPUs

RAM

32GB

Instanztyp für AWS EC2

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.2xlarge.

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:

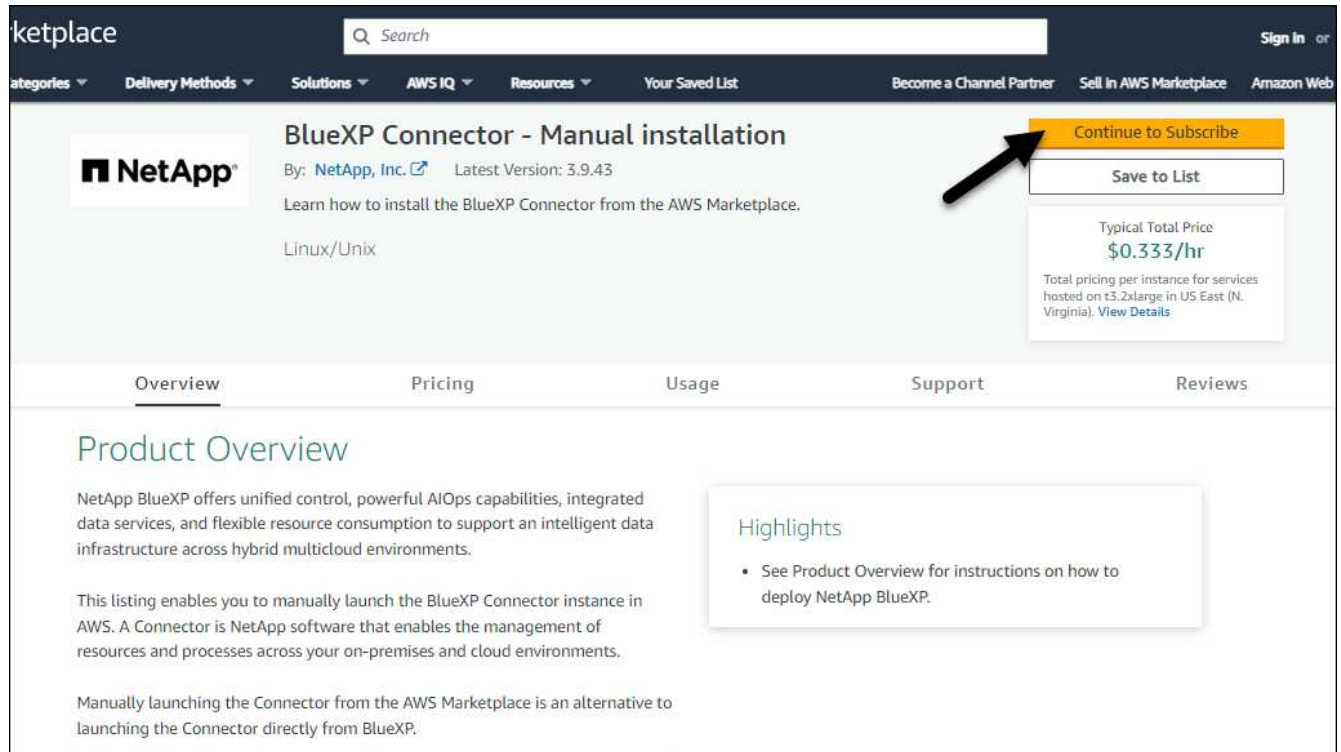
- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt
- Eine IAM-Rolle mit angehängter Richtlinie, die die erforderlichen Berechtigungen für den Connector

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. Go to the "[BlueXP Connector listing on the AWS Marketplace](#)"
2. Wählen Sie auf der Marketplace-Seite **Weiter zum Abonnieren**.



NetApp

BlueXP Connector - Manual installation

By: [NetApp, Inc.](#) Latest Version: 3.9.43

Learn how to install the BlueXP Connector from the AWS Marketplace.

Linux/Unix

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price
\$0.333/hr

Total pricing per instance for services hosted on t3.2xlarge in US East (N. Virginia). [View Details](#)

[Overview](#) [Pricing](#) [Usage](#) [Support](#) [Reviews](#)

Product Overview

NetApp BlueXP offers unified control, powerful AIOps capabilities, integrated data services, and flexible resource consumption to support an intelligent data infrastructure across hybrid multicloud environments.

This listing enables you to manually launch the BlueXP Connector instance in AWS. A Connector is NetApp software that enables the management of resources and processes across your on-premises and cloud environments.

Manually launching the Connector from the AWS Marketplace is an alternative to launching the Connector directly from BlueXP.

Highlights

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

3. Um die Software zu abonnieren, wählen Sie **Bedingungen akzeptieren**.

Das Abonnement kann einige Minuten dauern.

4. Wählen Sie nach Abschluss des Abonnements **Weiter zur Konfiguration** aus.

NetApp BlueXP Connector - Manual installation

[Continue to Configuration](#)

< Product Detail [Subscribe](#)

Subscribe to this software

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

Terms and Conditions

NetApp, Inc. Offer

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

Product	Effective date	Expiration date	Action
BlueXP Connector - Manual installation	N/A	N/A	Show Details

5. Stellen Sie auf der Seite **Configure this Software** sicher, dass Sie die richtige Region ausgewählt haben, und wählen Sie dann **Continue to Launch** aus.
6. Wählen Sie auf der Seite **Diese Software starten** unter **Aktion auswählen 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.

7. 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 Betriebssystem-Images:** 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 (t3.2xlarge ist vorausgewählt und 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.
 - Geben Sie die Einstellungen für Sicherheitsgruppen an, die die erforderlichen Verbindungsmethoden für die Connector-Instanz aktivieren: SSH, HTTP und HTTPS.

["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.

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

`https://ipaddress`

9. Richten Sie nach der Anmeldung den Konnektor ein:

- a. Geben Sie die BlueXP -Organisation an, die 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 Ihrer BlueXP -Organisation 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

Sie können einen Connector manuell auf einem Linux-Host installieren, der in AWS ausgeführt wird. 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 eine haben "[Verständnis von Steckverbindern](#)".
- 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.



Der Connector reserviert den UID- und GID-Bereich von 19000 bis 19200. Dieser Bereich ist fest und kann nicht geändert werden. Wenn Drittanbietersoftware auf Ihrem Host UIDs oder GIDs innerhalb dieses Bereichs verwendet, schlägt die Connector-Installation fehl. NetApp empfiehlt die Verwendung eines Hosts ohne Drittanbietersoftware, um Konflikte zu vermeiden.

Dedizierter Host

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

Der Host kann eine beliebige Architektur aufweisen, die die folgenden Größenanforderungen erfüllt:

- CPU: 8 Cores oder 8 vCPUs
- RAM: 32 GB

Hypervisor

Ein Bare-Metal- oder gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

Anforderungen an das Betriebssystem und den Container

BlueXP unterstützt den Connector mit den folgenden Betriebssystemen, wenn BlueXP im Standardmodus oder im eingeschränkten Modus verwendet wird. Vor der Installation des Connectors ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte OS-Versionen	Unterstützte Connector-Versionen	Benötigter Container-Tool	SELinux
Red Hat Enterprise Linux	9.1 bis 9.4 8.6 bis 8.10 7,9	3.9.40 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Podman Version 4.6.1 oder 4.9.4 Zeigen Sie die Konfigurationsanforderungen für Podman an.	Unterstützt im Enforcing-Modus oder im permissiven Modus ¹
Ubuntu	24,04 LTS	3.9.45 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Docker Engine 23.06 bis 28.0.0.	Nicht unterstützt

Hinweise:

1. Die Verwaltung von Cloud Volumes ONTAP-Systemen wird von Connectors, auf denen SELinux auf dem Betriebssystem aktiviert ist, nicht unterstützt.
2. Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.

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

Instanztyp für AWS EC2

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.2xlarge.

Schlüsselpaar

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

SETZEN SIE bei der Verwendung von IMDSv2 das Limit für den Response Hop

Wenn IMDSv2 auf der EC2-Instanz aktiviert ist (dies ist die Standardeinstellung für neue EC2-Instanzen), müssen Sie das PUT Response Hop Limit auf der Instanz auf 3 ändern. Wenn Sie die Begrenzung der EC2-Instanz nicht ändern, erhalten Sie beim Einrichten des Connectors einen Initialisierungsfehler in der Benutzeroberfläche.

- ["Erfordern die Verwendung von IMDSv2 auf Amazon EC2 Instanzen"](#)
- ["AWS-Dokumentation: Ändern Sie das PUT-Response-Hop-Limit"](#)

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

BlueXP verwendet /opt, um das Verzeichnis und seinen Inhalt zu installieren
/opt/application/netapp.

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

BlueXP erfordert diesen Platz /var Da Docker oder Podman so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Insbesondere werden Container in der erstellt
/var/lib/containers/storage Verzeichnis. Externe Mounts oder Symlinks funktionieren nicht für diesen Raum.

Schritt 2: Installieren Sie Podman oder Docker Engine

Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

- Podman ist für Red hat Enterprise Linux 8 und 9 erforderlich.

[Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

- Docker Engine ist für Ubuntu erforderlich.

[Zeigen Sie die von BlueXP unterstützten Versionen der Docker Engine an.](#)

Beispiel 1. Schritte

Podman

Führen Sie die folgenden Schritte aus, um Podman zu installieren und zu konfigurieren, um die folgenden Anforderungen zu erfüllen:

- Aktivieren und starten Sie den Dienst podman.socket
- python3 einbauen
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu



Passen Sie bei Verwendung von Podman den aardvark-dns-Dienstport (Standard: 53) nach der Installation des Connectors an, um Konflikte mit dem DNS-Port auf dem Host zu vermeiden. Folgen Sie den Anweisungen zur Portkonfiguration.

Schritte

1. Entfernen Sie das Paket podman-Docker, wenn es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

Podman ist über die offiziellen Red hat Enterprise Linux-Repositorys erhältlich.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

3. Aktivieren und starten Sie den podman.Socket-Dienst.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie Python3.

```
sudo dnf install python3
```

5. Installieren Sie das EPEL Repository-Paket, wenn es nicht bereits auf Ihrem System verfügbar ist.

Dieser Schritt ist erforderlich, da podman-compose im Repository Extra Packages for Enterprise Linux (EPEL) verfügbar ist.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Für Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Installieren Sie das Paket „podman-compose“ 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Verwenden der `dnf install` Befehl erfüllt die Anforderung zum Hinzufügen von podman-compose zur Umgebungsvariable PATH. Der Installationsbefehl fügt podman-compose zu `/usr/bin` hinzu, das bereits im enthalten ist `secure_path` Option auf dem Host.

Docker Engine

Folgen Sie der Dokumentation von Docker, um die Docker Engine zu installieren.

Schritte

1. ["Installationsanweisungen von Docker anzeigen"](#)

Befolgen Sie die Schritte, um eine bestimmte Version der Docker Engine zu installieren. Durch die Installation der neuesten Version wird eine Docker Version installiert, die BlueXP nicht unterstützt.

2. Docker muss aktiviert und ausgeführt werden.

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

Schritt 3: 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, die von Computern kontaktiert werden, wenn die webbasierte Konsole von BlueXP verwendet wird

Computer, die über einen Webbrowser auf die BlueXP -Konsole zugreifen, müssen in der Lage sein, mehrere Endpunkte zu kontaktieren. Sie müssen die BlueXP -Konsole verwenden, um den Connector einzurichten und für die tägliche Verwendung von BlueXP .

["Bereiten Sie das Netzwerk für die BlueXP -Konsole vor"](#).

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://mysupport.netapp.com>
- <https://signin.b2c.NetApp.com> (dieser Endpunkt ist die CNAME-URL für <https://mysupport.NetApp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- Um Bilder zu erhalten, benötigt das Installationsprogramm Zugriff auf einen der beiden folgenden Endpunkte:
 - Option 1 (empfohlen):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

Die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.

- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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): <ul style="list-style-type: none"> • 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.
Wählen Sie zwischen zwei Endpunktsätzen: <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> • Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p> 	Um Bilder für Connector-Upgrades zu erhalten.

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie

Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

Proxy-Server

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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 4: 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 Dokumentation: 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 5: 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.
- Ein CA-signiertes Zertifikat, wenn der Proxy-Server HTTPS verwendet oder wenn der Proxy ein abfangenden Proxy ist.



Bei der manuellen Installation des Connectors können Sie kein Zertifikat für einen transparenten Proxyserver festlegen. Wenn Sie ein Zertifikat für einen transparenten Proxyserver festlegen müssen, müssen Sie nach der Installation die Wartungskonsole verwenden. Erfahren Sie mehr über die "[Connector-Wartungskonsole](#)".

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. 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.

2. 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.

3. 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.

4. Führen Sie das Installationskript aus.

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

Sie müssen Proxy-Informationen hinzufügen, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter `--proxy` und `--cacert` sind optional und werden nicht dazu aufgefordert. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben.

Hier ist ein Beispiel für die Konfiguration eines expliziten Proxyservers mit einem von einer Zertifizierungsstelle signierten Zertifikat:

```
./BlueXP-Connector-Cloud-v3.9.40--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 ein \ wie oben gezeigt verwenden.
- BlueXP unterstützt keine Benutzernamen oder Passwörter, die das @ Zeichen enthalten.
- Wenn das Passwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen umgehen, indem Sie es mit einem Backslash: & Oder !

Beispiel:

```
http://bxpproxyuser:netapp1!@address:3128
```

`--cacert` gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und

transparente Proxyserver erforderlich.

Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyservers. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Fügen Sie Ihrem Connector-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Wenn Sie Podman verwendet haben, müssen Sie den Aardvark-DNS-Port anpassen.
 - a. Stellen Sie per SSH eine Verbindung zur virtuellen Maschine des BlueXP Connector her.
 - b. Öffnen Sie die Datei `podman_/usr/share/containers/containers.conf_` und ändern Sie den gewählten Port für den Aardvark DNS-Dienst. Ändern Sie ihn beispielsweise in 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

- c. Starten Sie die virtuelle Connector-Maschine neu.
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 die BlueXP -Organisation an, die 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**.

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 6: 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

Sie können einen Connector in Azure direkt von BlueXP installieren. Um einen Connector in Azure von BlueXP zu erstellen, müssen Sie Ihr Netzwerk einrichten, eine Azure-Rolle für die Bereitstellung des Connectors vorbereiten und dann den Connector implementieren.

Bevor Sie beginnen

- Sie sollten eine haben ["Verständnis von Steckverbindern"](#).
- 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.
Wählen Sie zwischen zwei Endpunktsätzen: <ul style="list-style-type: none">Option 1 (empfohlen) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.ioOption 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Um Bilder für Connector-Upgrades zu erhalten.

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.

- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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 einer Connector-Bereitstellungsrichtlinie (benutzerdefinierte Rolle)

Sie müssen eine benutzerdefinierte Rolle erstellen, die über Berechtigungen zum Bereitstellen des Connectors in Azure verfügt.

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.

Nachdem BlueXP die virtuelle Connector-Maschine in Azure bereitgestellt hat, wird ein auf der virtuellen Maschine aktiviert "[Vom System zugewiesene verwaltete Identität](#)", erstellt automatisch die Rolle, die sie benötigt, und weist sie der virtuellen Maschine zu. Die automatisch erstellte Rolle erteilt BlueXP die erforderlichen Berechtigungen zum Managen der Ressourcen und Prozesse in diesem Azure-Abonnement. "[Überprüfen Sie, wie BlueXP die Berechtigungen verwendet](#)".

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 es einen neuen Satz an Berechtigungen auf die Connector-VM an, sodass der Connector Azure Ressourcen managen kann.

```
{
  "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/read",
"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/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/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

```

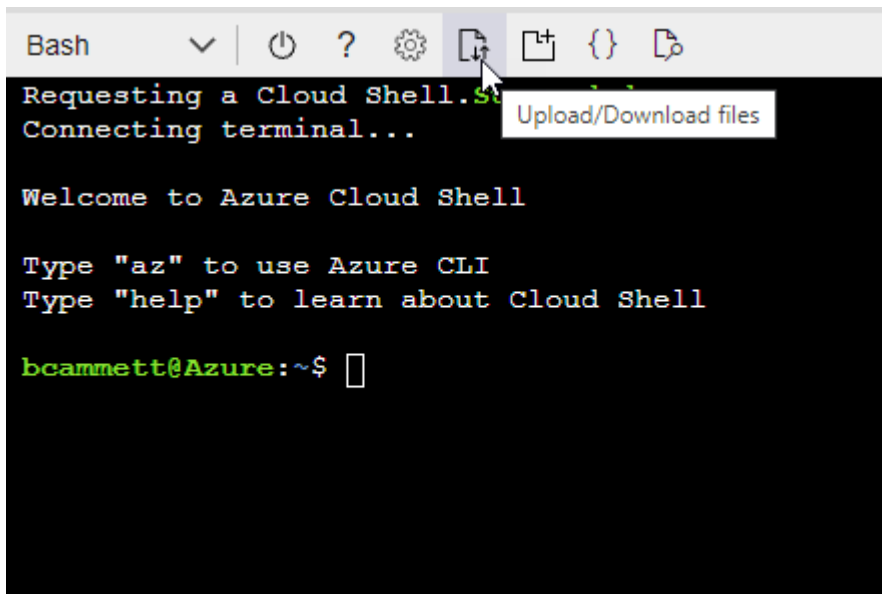
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

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.

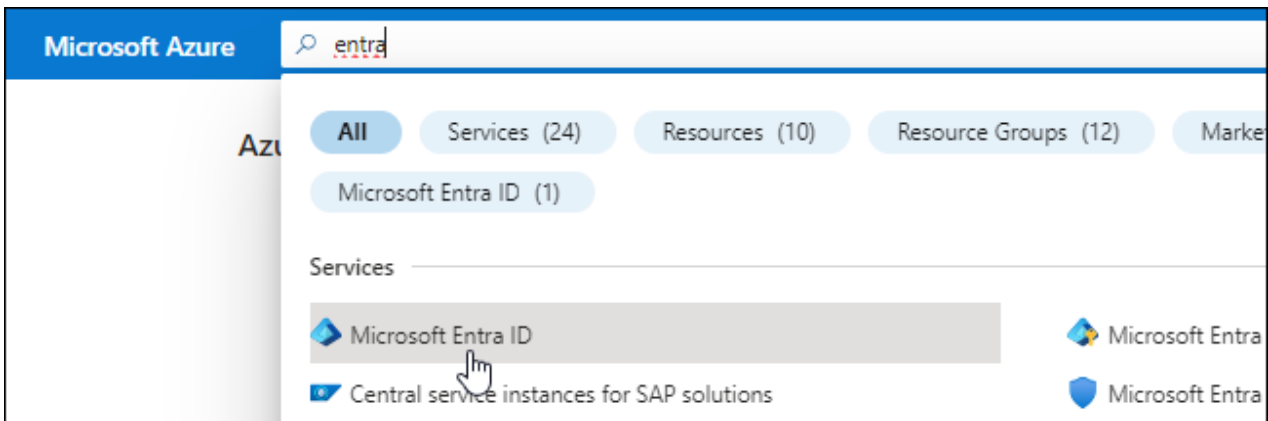
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

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**.

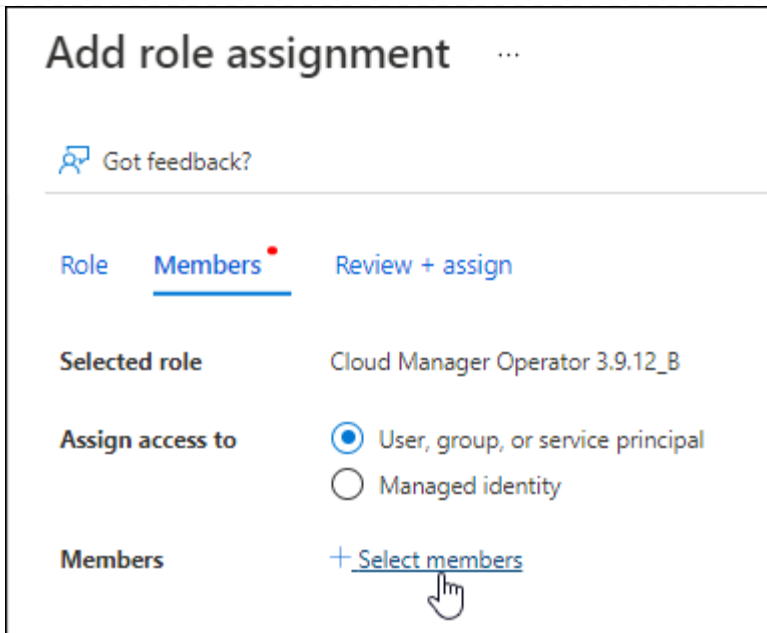


3. Wählen Sie im Menü **App-Registrierungen**.
4. Wählen Sie **Neue Registrierung**.
5. Geben Sie Details zur Anwendung an:
 - **Name**: Geben Sie einen Namen für die Anwendung ein.
 - **Kontotyp**: Wählen Sie einen Kontotyp aus (jeder kann mit BlueXP verwendet werden).
 - **Redirect URI**: Sie können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

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

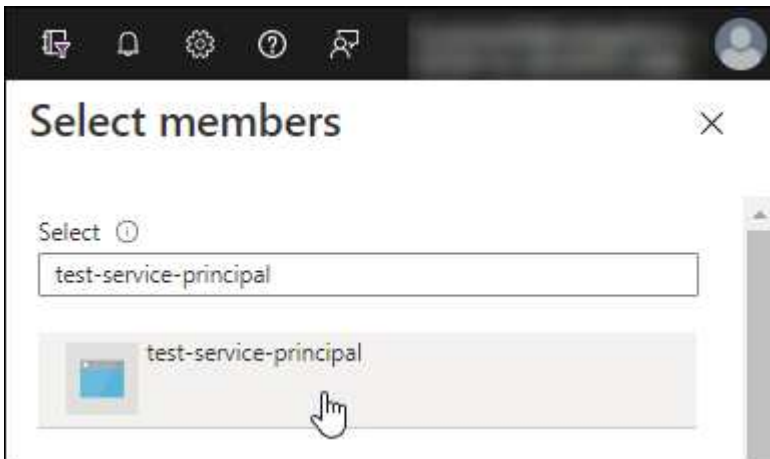
Weisen Sie der Anwendung die benutzerdefinierte Rolle zu

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.


Request API permissions













Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.




 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)

 Azure Service Management
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

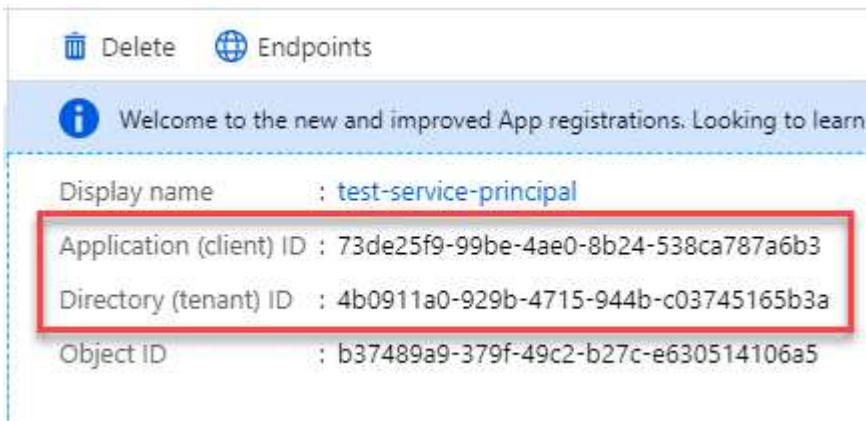
PERMISSION

ADMIN CONSENT REQUIRED

user_impersonation
Access Azure Service Management as organization users (preview)

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**.



Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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"](#).
- Wenn BlueXP den Connector bereitstellt, wird eine benutzerdefinierte Rolle erstellt und dieser der Connector-VM zugewiesen. Diese Rolle umfasst Berechtigungen, mit denen der Connector Azure Ressourcen managen kann. Sie müssen sicherstellen, dass die Rolle immer auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Versionen hinzugefügt werden. ["Erfahren Sie mehr über die benutzerdefinierte Rolle für den Connector"](#).

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"](#)

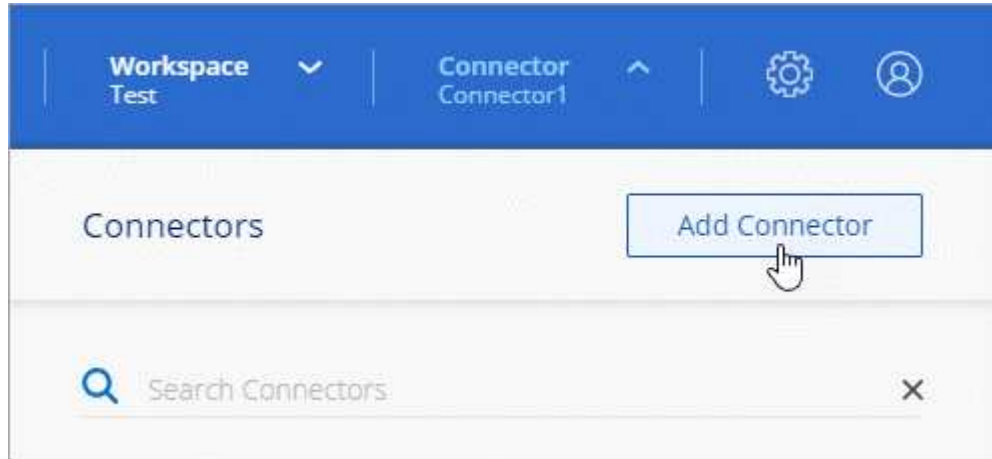
- Wenn Sie nicht möchten, dass BlueXP automatisch eine Azure-Rolle für den Connector erstellt, müssen

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

Ein Connector kann direkt aus dem Azure Marketplace in Azure erstellt werden. 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 eine haben "[Verständnis von Steckverbindern](#)".
- Rezension "[Einschränkungen an den Anschlüssen](#)".

Schritt 1: Netzwerk einrichten

Stellen Sie sicher, dass der Netzwerkstandort, an dem Sie den Connector installieren möchten, die folgenden Anforderungen unterstützt. Diese Anforderungen ermöglichen dem Connector die Verwaltung von Ressourcen in Ihrer Hybrid Cloud.

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.

Endpunkte	Zweck
<p>Wählen Sie zwischen zwei Endpunktsätzen:</p> <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> <ul style="list-style-type: none"> • Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p>	<p>Um Bilder für Connector-Upgrades zu erhalten.</p>

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

Proxy-Server

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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](#)"

Implementieren Sie die Netzwerkanforderungen, nachdem Sie den Connector erstellt haben.

Schritt 2: Überprüfung der VM-Anforderungen

Wählen Sie beim Erstellen des Connectors einen virtuellen Maschinentyp aus, der die folgenden Anforderungen erfüllt.

CPU

8 Kerne oder 8 vCPUs

RAM

32GB

Azure VM-Größe

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen Standard_D8s_v3.

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.

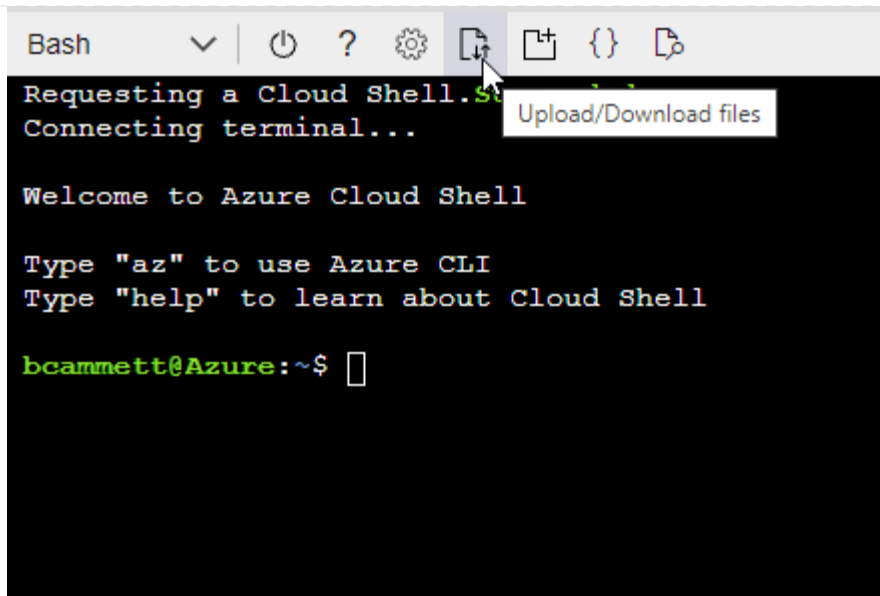
Beispiel

```
"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

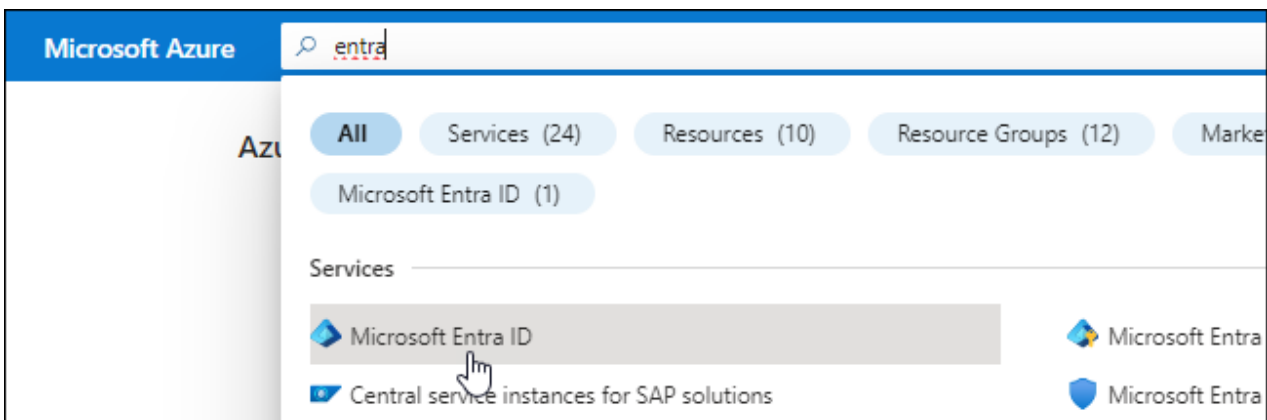
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

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.

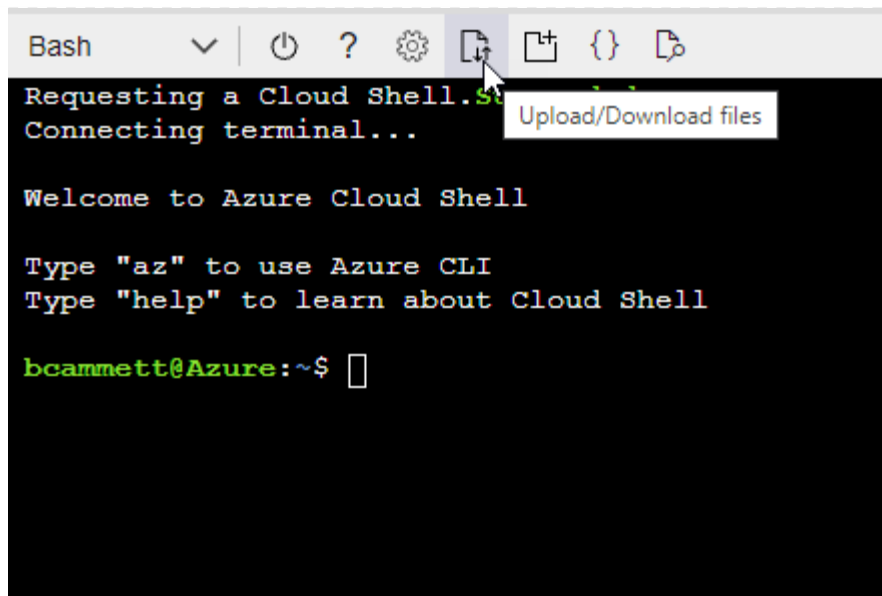
Beispiel

```
"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.



```
Bash
Requesting a Cloud Shell.
Connecting terminal...
Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

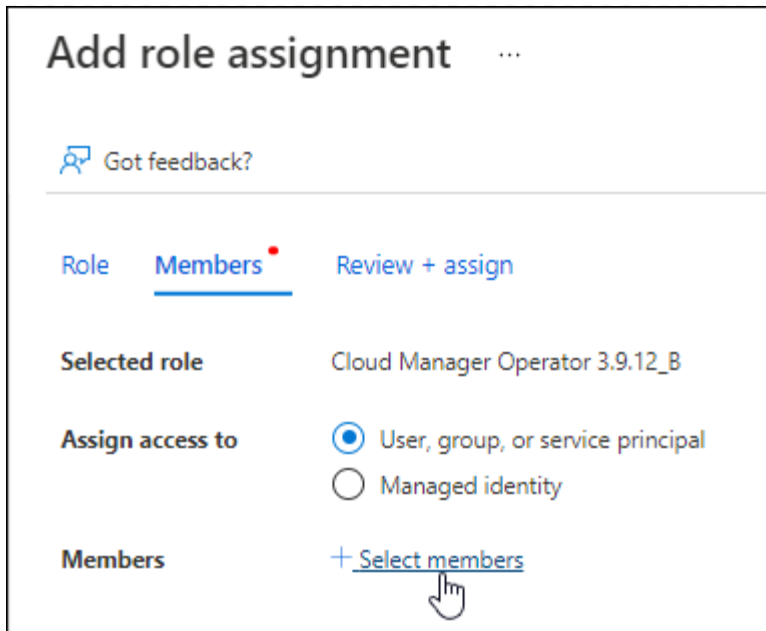
- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

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

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

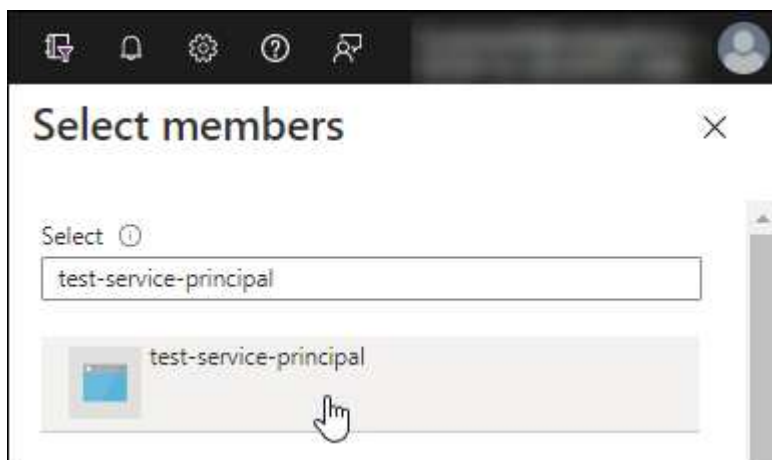
2. Applikation der Rolle zuweisen:

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



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



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

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

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

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Principal 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.

Request API permissions


Select an API













Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Batch</p> <p>Schedule large-scale parallel and HPC applications in the cloud</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Data Catalog</p> <p>Programmatic access to Data Catalog resources to register, annotate and search data assets</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Data Explorer</p> <p>Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p> </div>
<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Data Lake</p> <p>Access to storage and compute for big data analytic scenarios</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure DevOps</p> <p>Integrate with Azure DevOps and Azure DevOps server</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Import/Export</p> <p>Programmatic control of import/export jobs</p> </div>
<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Key Vault</p> <p>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Rights Management Services</p> <p>Allow validated users to read and write protected content</p> </div>	<div style="border: 2px solid red; padding: 5px;">  <p>Azure Service Management</p> <p>Programmatic access to much of the functionality available through the Azure portal</p> </div>
<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Storage</p> <p>Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Customer Insights</p> <p>Create profile and interaction models for your products</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Data Export Service for Microsoft Dynamics 365</p> <p>Export data from Microsoft Dynamics CRM organization to an external destination</p> </div>

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview)

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**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

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

Schritt 4: Erstellen Sie den Konnektor

Starten Sie den Connector direkt über den Azure Marketplace.

Über diese Aufgabe

Durch Erstellen des Connectors aus dem Azure Marketplace wird eine virtuelle Maschine mit einer Standardkonfiguration eingerichtet. ["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 Standard_D8s_v3.
- **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. Sie sollten sehen, dass die virtuelle Maschine und die Connector-Software 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:

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

6. Richten Sie nach der Anmeldung den Konnektor ein:
 - a. Geben Sie die BlueXP -Organisation an, die 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.

Lassen Sie den eingeschränkten Modus deaktiviert, um BlueXP im Standardmodus zu 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

Sie haben jetzt den Connector installiert und mit Ihrer BlueXP-Organisation 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

Ein Connector ist eine NetApp Software, die in Ihrem Cloud-Netzwerk oder Ihrem On-Premises-Netzwerk ausgeführt wird. Mit ihr können Sie alle Funktionen und Services von BlueXP nutzen. Eine der verfügbaren Installationsoptionen ist die manuelle Installation der Connector-Software auf einem Linux-Host, der in Azure ausgeführt wird. 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 eine haben "[Verständnis von Steckverbindern](#)".
- 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.



Der Connector reserviert den UID- und GID-Bereich von 19000 bis 19200. Dieser Bereich ist fest und kann nicht geändert werden. Wenn Drittanbietersoftware auf Ihrem Host UIDs oder GIDs innerhalb dieses Bereichs verwendet, schlägt die Connector-Installation fehl. NetApp empfiehlt die Verwendung eines Hosts ohne Drittanbietersoftware, um Konflikte zu vermeiden.

Dedizierter Host

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

Der Host kann eine beliebige Architektur aufweisen, die die folgenden Größenanforderungen erfüllt:

- CPU: 8 Cores oder 8 vCPUs

- RAM: 32 GB

Hypervisor

Ein Bare-Metal- oder gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

Anforderungen an das Betriebssystem und den Container

BlueXP unterstützt den Connector mit den folgenden Betriebssystemen, wenn BlueXP im Standardmodus oder im eingeschränkten Modus verwendet wird. Vor der Installation des Connectors ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte OS-Versionen	Unterstützte Connector-Versionen	Benötigter Container-Tool	SELinux
Red Hat Enterprise Linux	9.1 bis 9.4 8.6 bis 8.10 7,9	3.9.40 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Podman Version 4.6.1 oder 4.9.4 Zeigen Sie die Konfigurationsanforderungen für Podman an.	Unterstützt im Enforcing-Modus oder im permissiven Modus ¹
Ubuntu	24,04 LTS	3.9.45 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Docker Engine 23.06 bis 28.0.0.	Nicht unterstützt

Hinweise:

1. Die Verwaltung von Cloud Volumes ONTAP-Systemen wird von Connectors, auf denen SELinux auf dem Betriebssystem aktiviert ist, nicht unterstützt.
2. Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.
3. Für RHEL muss der Host 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.

Azure VM-Größe

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen Standard_D8s_v3.

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

BlueXP verwendet /opt, um das Verzeichnis und seinen Inhalt zu installieren
/opt/application/netapp.

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

BlueXP erfordert diesen Platz `/var` Da Docker oder Podman so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Insbesondere werden Container in der erstellt `/var/lib/containers/storage` Verzeichnis. Externe Mounts oder Symlinks funktionieren nicht für diesen Raum.

Schritt 2: Installieren Sie Podman oder Docker Engine

Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

- Podman ist für Red hat Enterprise Linux 8 und 9 erforderlich.

[Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

- Docker Engine ist für Ubuntu erforderlich.

[Zeigen Sie die von BlueXP unterstützten Versionen der Docker Engine an.](#)

Beispiel 2. Schritte

Podman

Führen Sie die folgenden Schritte aus, um Podman zu installieren und zu konfigurieren, um die folgenden Anforderungen zu erfüllen:

- Aktivieren und starten Sie den Dienst podman.socket
- python3 einbauen
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu



Passen Sie bei Verwendung von Podman den aardvark-dns-Dienstport (Standard: 53) nach der Installation des Connectors an, um Konflikte mit dem DNS-Port auf dem Host zu vermeiden. Folgen Sie den Anweisungen zur Portkonfiguration.

Schritte

1. Entfernen Sie das Paket podman-Docker, wenn es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

Podman ist über die offiziellen Red hat Enterprise Linux-Repositorys erhältlich.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

3. Aktivieren und starten Sie den podman.Socket-Dienst.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie Python3.

```
sudo dnf install python3
```

5. Installieren Sie das EPEL Repository-Paket, wenn es nicht bereits auf Ihrem System verfügbar ist.

Dieser Schritt ist erforderlich, da podman-compose im Repository Extra Packages for Enterprise Linux (EPEL) verfügbar ist.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Für Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Installieren Sie das Paket „podman-compose“ 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Verwenden der `dnf install` Befehl erfüllt die Anforderung zum Hinzufügen von podman-compose zur Umgebungsvariable PATH. Der Installationsbefehl fügt podman-compose zu `/usr/bin` hinzu, das bereits im enthalten ist `secure_path` Option auf dem Host.

Docker Engine

Folgen Sie der Dokumentation von Docker, um die Docker Engine zu installieren.

Schritte

1. ["Installationsanweisungen von Docker anzeigen"](#)

Befolgen Sie die Schritte, um eine bestimmte Version der Docker Engine zu installieren. Durch die Installation der neuesten Version wird eine Docker Version installiert, die BlueXP nicht unterstützt.

2. Docker muss aktiviert und ausgeführt werden.

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

Schritt 3: 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, die von Computern kontaktiert werden, wenn die webbasierte Konsole von BlueXP verwendet wird

Computer, die über einen Webbrowser auf die BlueXP -Konsole zugreifen, müssen in der Lage sein, mehrere Endpunkte zu kontaktieren. Sie müssen die BlueXP -Konsole verwenden, um den Connector einzurichten und für die tägliche Verwendung von BlueXP .

["Bereiten Sie das Netzwerk für die BlueXP -Konsole vor"](#).

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://mysupport.netapp.com>
- <https://signin.b2c.NetApp.com> (dieser Endpunkt ist die CNAME-URL für <https://mysupport.NetApp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- Um Bilder zu erhalten, benötigt das Installationsprogramm Zugriff auf einen der beiden folgenden Endpunkte:
 - Option 1 (empfohlen):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

Die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen

werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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.
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.

Endpunkte	Zweck
<p>Wählen Sie zwischen zwei Endpunktsätzen:</p> <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> <ul style="list-style-type: none"> • Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p>	<p>Um Bilder für Connector-Updates zu erhalten.</p>

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

Proxy-Server

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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 4: Einrichten von Berechtigungen für die Connector-Bereitstellung

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.

Erstellen Sie eine benutzerdefinierte Rolle für die Connector-Bereitstellung

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.

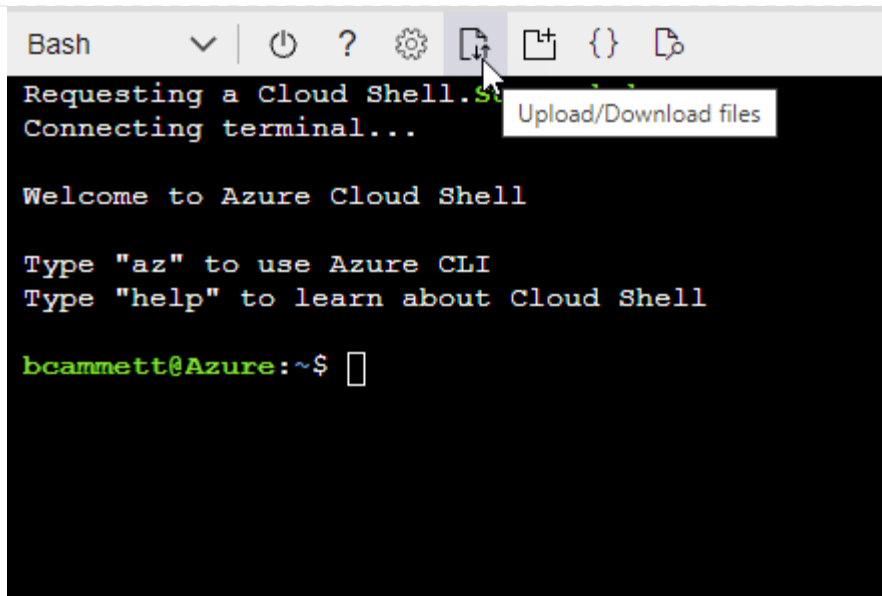
Beispiel

```
"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

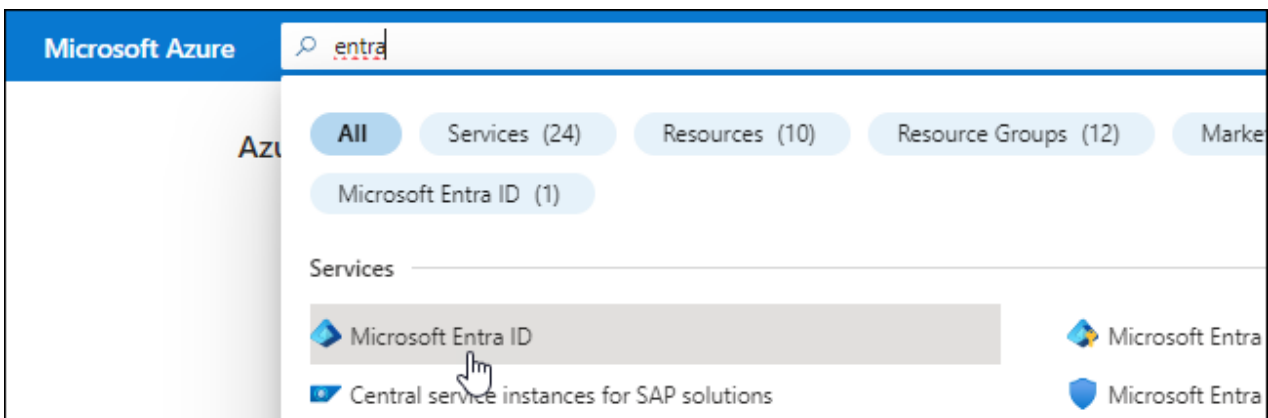
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

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.

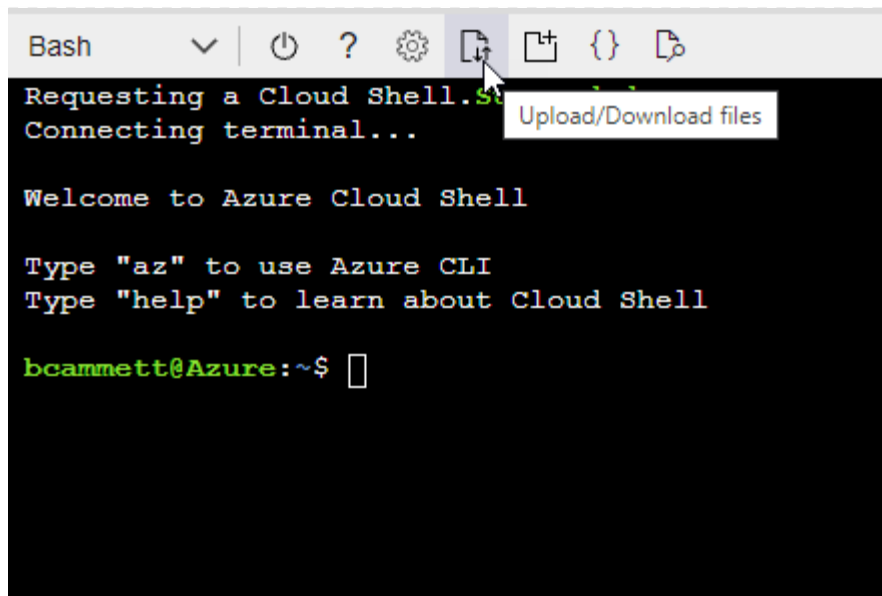
Beispiel

```
"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.



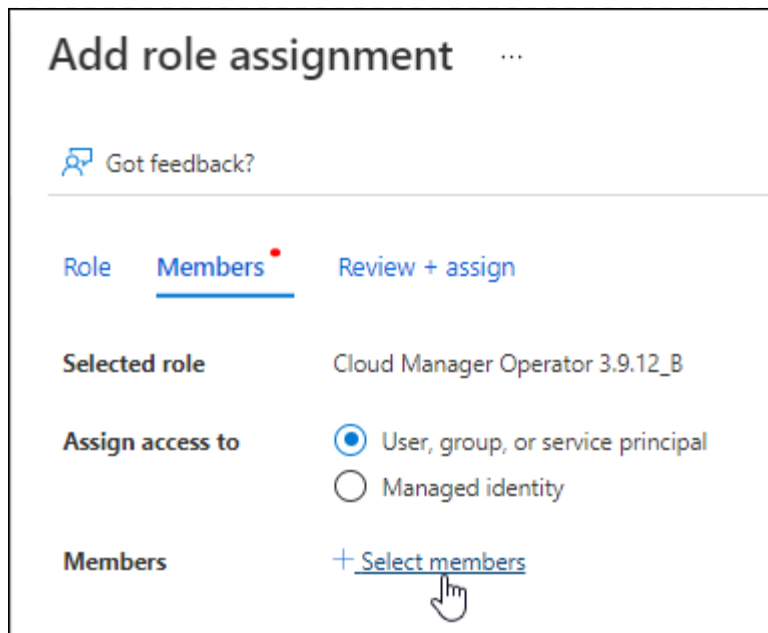
- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
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.

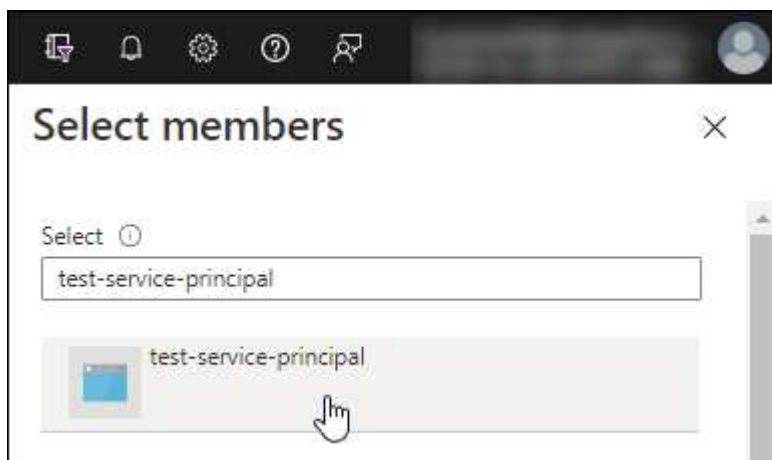
2. Applikation der Rolle zuweisen:

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



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



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

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

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

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Principal 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.

Request API permissions


Select an API













Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.




 <p>Azure Batch</p> <p>Schedule large-scale parallel and HPC applications in the cloud</p>	 <p>Azure Data Catalog</p> <p>Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	 <p>Azure Data Explorer</p> <p>Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>
 <p>Azure Data Lake</p> <p>Access to storage and compute for big data analytic scenarios</p>	 <p>Azure DevOps</p> <p>Integrate with Azure DevOps and Azure DevOps server</p>	 <p>Azure Import/Export</p> <p>Programmatic control of import/export jobs</p>
 <p>Azure Key Vault</p> <p>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>	 <p>Azure Rights Management Services</p> <p>Allow validated users to read and write protected content</p>	 <p>Azure Service Management</p> <p>Programmatic access to much of the functionality available through the Azure portal</p>
 <p>Azure Storage</p> <p>Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p>	 <p>Customer Insights</p> <p>Create profile and interaction models for your products</p>	 <p>Data Export Service for Microsoft Dynamics 365</p> <p>Export data from Microsoft Dynamics CRM organization to an external destination</p>

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

Request API permissions

[< All APIs](#)

 Azure Service Management
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

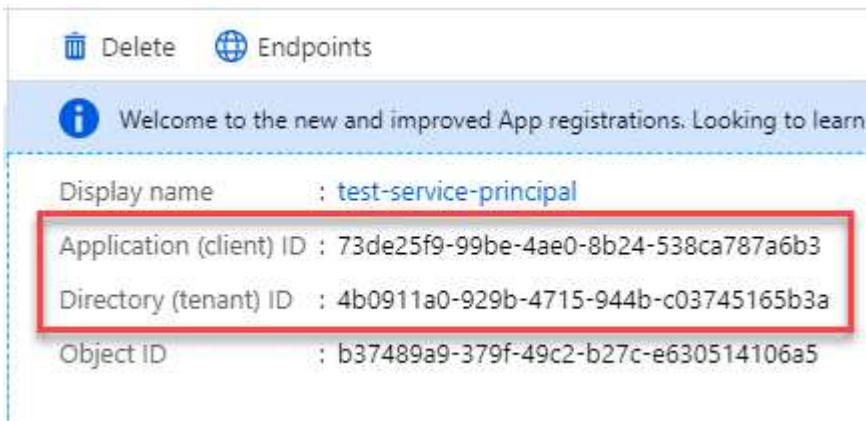
PERMISSION

ADMIN CONSENT REQUIRED

user_impersonation
Access Azure Service Management as organization users (preview)

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**.



Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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 5: 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.

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



Bei der manuellen Installation des Connectors können Sie kein Zertifikat für einen transparenten Proxyserver festlegen. Wenn Sie ein Zertifikat für einen transparenten Proxyserver festlegen müssen, müssen Sie nach der Installation die Wartungskonsole verwenden. Erfahren Sie mehr über die "[Connector-Wartungskonsole](#)".

- 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. 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.

2. 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.

3. 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.

4. Führen Sie das Installationskript aus.

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

Sie müssen Proxy-Informationen hinzufügen, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter `--proxy` und `--cacert` sind optional und werden nicht dazu aufgefordert. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben.

Hier ist ein Beispiel für die Konfiguration eines expliziten Proxyserver mit einem von einer Zertifizierungsstelle signierten Zertifikat:

```
./BlueXP-Connector-Cloud-v3.9.40--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 ein \ wie oben gezeigt verwenden.
- BlueXP unterstützt keine Benutzernamen oder Passwörter, die das @ Zeichen enthalten.
- Wenn das Passwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen umgehen, indem Sie es mit einem Backslash: & Oder !

Beispiel:

`http://bxpproxyuser:netapp1!\@address:3128`

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyserver. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Fügen Sie Ihrem Connector-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Wenn Sie Podman verwendet haben, müssen Sie den Aardvark-DNS-Port anpassen.

- a. Stellen Sie per SSH eine Verbindung zur virtuellen Maschine des BlueXP Connector her.
- b. Öffnen Sie die Datei `podman_/usr/share/containers/containers.conf_` und ändern Sie den gewählten Port für den Aardvark DNS-Dienst. Ändern Sie ihn beispielsweise in 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

c. Starten Sie die virtuelle Connector-Maschine neu.

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:

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

8. Richten Sie nach der Anmeldung den Konnektor ein:
- Geben Sie die BlueXP -Organisation an, die dem Connector zugeordnet werden soll.
 - Geben Sie einen Namen für das System ein.
 - 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"](#).

- Wählen Sie **Start**.

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 6: 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 gcloud erstellen

Sie können einen Connector in Google Cloud von BlueXP oder mithilfe von Google Cloud erstellen. Sie müssen Ihr Netzwerk einrichten, Google Cloud-Berechtigungen vorbereiten, Google Cloud APIs aktivieren und anschließend den Connector erstellen.

Bevor Sie beginnen

- Sie sollten eine haben ["Verständnis von Steckverbindern"](#).

- Sie sollten es überprüfen "[Einschränkungen an den Anschlüssen](#)".

Schritt 1: Netzwerk einrichten

Richten Sie das Netzwerk ein, um sicherzustellen, dass der Connector Ressourcen mit Verbindungen zu Zielnetzwerken und ausgehendem Internetzugriff verwalten kann.

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.
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.

Endpunkte	Zweck
<p>Wählen Sie zwischen zwei Endpunktsätzen:</p> <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> <ul style="list-style-type: none"> • Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p>	<p>Um Bilder für Connector-Upgrades zu erhalten.</p>

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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"](#)

Implementieren Sie diese Netzwerkanforderung, 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 gcloud 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 gcloud implementieren wird.

["Google Cloud docs: Gewähren Sie eine einzige Rolle"](#)

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.

Es liegt in Ihrer Verantwortung, die benutzerdefinierte Rolle zu aktualisieren, wenn in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

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.network User	Bereitstellen des Connectors im Serviceprojekt
Connector-Servicekonto	Individuell	Service-Projekt	" Kontorichtlinie für Connector-Service "	compute.network User Bereitsmanager. Editor	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.network User	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.network User	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 encrementmanager.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

Sie müssen mehrere Google Cloud-APIs aktivieren, bevor Sie den Connector und Cloud Volumes ONTAP bereitstellen.

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 gcloud.

Über diese Aufgabe

Beim Erstellen des Connectors wird eine Virtual Machine-Instanz in Google Cloud mit einer Standardkonfiguration bereitgestellt. Ändern Sie den Connector nach der Erstellung nicht in eine kleinere VM-Instanz mit weniger CPU oder RAM. ["Informieren Sie sich über die Standardkonfiguration des Connectors"](#).

BlueXP

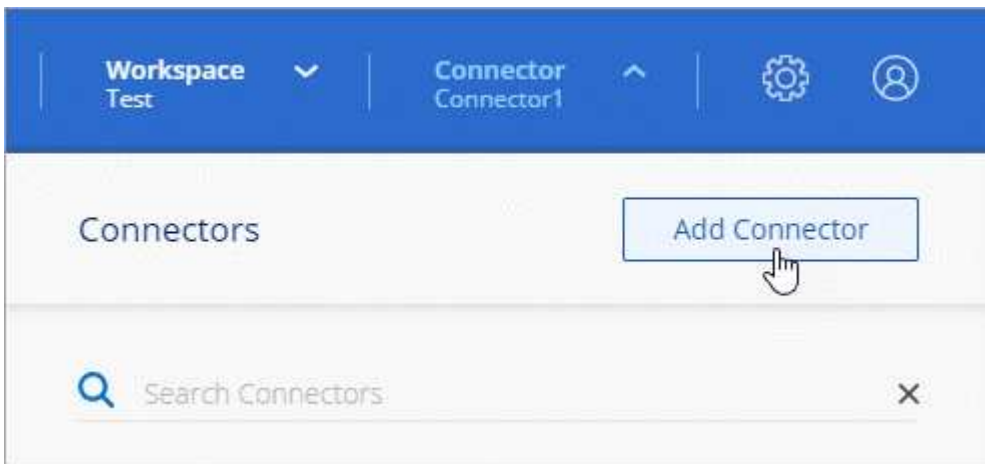
Bevor Sie beginnen

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.

- **Netzwerk-Tags:** Fügen Sie der Connector-Instanz ein Netzwerk-Tag hinzu, wenn Sie einen transparenten Proxy verwenden. Netzwerk-Tags müssen mit einem Kleinbuchstaben beginnen und können Kleinbuchstaben, Zahlen und Bindestriche enthalten. Tags müssen mit einem Kleinbuchstaben oder einer Zahl enden. Sie können beispielsweise das Tag „connector-proxy“ verwenden.
- **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 ist in etwa 7 Minuten bereit. Bleiben Sie auf der Seite, bis der Vorgang abgeschlossen ist.

Ergebnis

Nachdem der Vorgang abgeschlossen ist, steht der Connector von BlueXP zur Verwendung bereit.

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:** 8 Kerne oder 8 vCPUs
 - **RAM:** 32 GB
 - **Maschinentyp:** Wir empfehlen n2-Standard-8.

Der Connector wird in Google Cloud auf einer VM-Instanz mit einem Betriebssystem unterstützt, das Shielded VM-Funktionen unterstützt.

Schritte

1. Melden Sie sich mit Ihrer bevorzugten Methode beim gcloud SDK 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-8
  --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:

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

2. Richten Sie nach der Anmeldung den Konnektor ein:
 - a. Geben Sie die BlueXP -Organisation an, die dem Connector zugeordnet werden soll.

["Erfahren Sie mehr über das Identitäts- und Zugriffsmanagement von BlueXP "](#).

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

Ergebnis

Der Connector ist jetzt installiert und mit Ihrer BlueXP -Organisation 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

Sie können q Connector manuell auf einem Linux-Host installieren, der in Google Cloud ausgeführt wird. Um den Connector manuell auf Ihrem eigenen Linux-Host zu installieren, müssen Sie die Host-Anforderungen überprüfen, Ihr Netzwerk einrichten, Google Cloud-Berechtigungen vorbereiten, APIs aktivieren, den Connector installieren und dann die von

Ihnen vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

- Sie sollten eine haben "[Verständnis von Steckverbindern](#)".
- 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.



Der Connector reserviert den UID- und GID-Bereich von 19000 bis 19200. Dieser Bereich ist fest und kann nicht geändert werden. Wenn Drittanbietersoftware auf Ihrem Host UIDs oder GIDs innerhalb dieses Bereichs verwendet, schlägt die Connector-Installation fehl. NetApp empfiehlt die Verwendung eines Hosts ohne Drittanbietersoftware, um Konflikte zu vermeiden.

Dedizierter Host

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

Der Host kann eine beliebige Architektur aufweisen, die die folgenden Größenanforderungen erfüllt:

- CPU: 8 Cores oder 8 vCPUs
- RAM: 32 GB

Hypervisor

Ein Bare-Metal- oder gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

Anforderungen an das Betriebssystem und den Container

BlueXP unterstützt den Connector mit den folgenden Betriebssystemen, wenn BlueXP im Standardmodus oder im eingeschränkten Modus verwendet wird. Vor der Installation des Connectors ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte OS-Versionen	Unterstützte Connector-Versionen	Benötigter Container-Tool	SELinux
Red Hat Enterprise Linux	9.1 bis 9.4 8.6 bis 8.10 7,9	3.9.40 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Podman Version 4.6.1 oder 4.9.4 Zeigen Sie die Konfigurationsanforderungen für Podman an.	Unterstützt im Enforcing-Modus oder im permissiven Modus ¹
Ubuntu	24,04 LTS	3.9.45 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Docker Engine 23.06 bis 28.0.0.	Nicht unterstützt

Hinweise:

1. Die Verwaltung von Cloud Volumes ONTAP-Systemen wird von Connectors, auf denen SELinux auf dem Betriebssystem aktiviert ist, nicht unterstützt.
2. Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.
3. Für RHEL muss der Host 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.

Google Cloud-Maschinentyp

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n2-Standard-8.

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

BlueXP verwendet /opt, um das Verzeichnis und seinen Inhalt zu installieren
/opt/application/netapp.

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

BlueXP erfordert diesen Platz /var Da Docker oder Podman so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Insbesondere werden Container in der erstellt /var/lib/containers/storage Verzeichnis. Externe Mounts oder Symlinks funktionieren nicht für diesen Raum.

Schritt 2: Installieren Sie Podman oder Docker Engine

Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

- Podman ist für Red hat Enterprise Linux 8 und 9 erforderlich.

[Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

- Docker Engine ist für Ubuntu erforderlich.

[Zeigen Sie die von BlueXP unterstützten Versionen der Docker Engine an.](#)

Beispiel 3. Schritte

Podman

Führen Sie die folgenden Schritte aus, um Podman zu installieren und zu konfigurieren, um die folgenden Anforderungen zu erfüllen:

- Aktivieren und starten Sie den Dienst podman.socket
- python3 einbauen
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu



Passen Sie bei Verwendung von Podman den aardvark-dns-Dienstport (Standard: 53) nach der Installation des Connectors an, um Konflikte mit dem DNS-Port auf dem Host zu vermeiden. Folgen Sie den Anweisungen zur Portkonfiguration.

Schritte

1. Entfernen Sie das Paket podman-Docker, wenn es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

Podman ist über die offiziellen Red hat Enterprise Linux-Repositorys erhältlich.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

3. Aktivieren und starten Sie den podman.Socket-Dienst.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie Python3.


```
sudo dnf install python3
```

5. Installieren Sie das EPEL Repository-Paket, wenn es nicht bereits auf Ihrem System verfügbar ist.

Dieser Schritt ist erforderlich, da podman-compose im Repository Extra Packages for Enterprise Linux (EPEL) verfügbar ist.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Für Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Installieren Sie das Paket „podman-compose“ 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Verwenden der `dnf install` Befehl erfüllt die Anforderung zum Hinzufügen von podman-compose zur Umgebungsvariable PATH. Der Installationsbefehl fügt podman-compose zu `/usr/bin` hinzu, das bereits im enthalten ist `secure_path` Option auf dem Host.

Docker Engine

Folgen Sie der Dokumentation von Docker, um die Docker Engine zu installieren.

Schritte

1. ["Installationsanweisungen von Docker anzeigen"](#)

Befolgen Sie die Schritte, um eine bestimmte Version der Docker Engine zu installieren. Durch die Installation der neuesten Version wird eine Docker Version installiert, die BlueXP nicht unterstützt.

2. Docker muss aktiviert und ausgeführt werden.

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

Schritt 3: 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, die von Computern kontaktiert werden, wenn die webbasierte Konsole von BlueXP verwendet wird

Computer, die über einen Webbrowser auf die BlueXP -Konsole zugreifen, müssen in der Lage sein, mehrere Endpunkte zu kontaktieren. Sie müssen die BlueXP -Konsole verwenden, um den Connector einzurichten und für die tägliche Verwendung von BlueXP .

["Bereiten Sie das Netzwerk für die BlueXP -Konsole vor"](#).

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://mysupport.netapp.com>
- <https://signin.b2c.NetApp.com> (dieser Endpunkt ist die CNAME-URL für <https://mysupport.NetApp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- Um Bilder zu erhalten, benötigt das Installationsprogramm Zugriff auf einen der beiden folgenden Endpunkte:
 - Option 1 (empfohlen):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

Die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.

- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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.
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.
<p>Wählen Sie zwischen zwei Endpunktsätzen:</p> <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> • Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p> 	Um Bilder für Connector-Upgrades zu erhalten.

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

Proxy-Server

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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 4: 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.

Es liegt in Ihrer Verantwortung, die benutzerdefinierte Rolle zu aktualisieren, wenn in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

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 5: 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.network User	Bereitstellen des Connectors im Serviceprojekt
Connector-Servicekonto	Individuell	Service-Projekt	" Kontorichtlinie für Connector-Service "	compute.network User Bereitsmanager. Editor	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.network User	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.network User	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 encrementmanager.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 6: 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 7: 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.

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



Bei der manuellen Installation des Connectors können Sie kein Zertifikat für einen transparenten Proxyserver festlegen. Wenn Sie ein Zertifikat für einen transparenten Proxyserver festlegen müssen, müssen Sie nach der Installation die Wartungskonsole verwenden. Erfahren Sie mehr über die ["Connector-Wartungskonsole"](#).

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. 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.

2. 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.

3. 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.

4. Führen Sie das Installationskript aus.

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

Sie müssen Proxy-Informationen hinzufügen, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter `--proxy` und `--cacert` sind optional und werden nicht dazu aufgefordert. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben.

Hier ist ein Beispiel für die Konfiguration eines expliziten Proxyservers mit einem von einer Zertifizierungsstelle signierten Zertifikat:

```
./BlueXP-Connector-Cloud-v3.9.40--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 ein \ wie oben gezeigt verwenden.
- BlueXP unterstützt keine Benutzernamen oder Passwörter, die das @ Zeichen enthalten.
- Wenn das Passwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen umgehen, indem Sie es mit einem Backslash: & Oder !

Beispiel:

`http://bxpproxyuser:netapp1!\@address:3128`

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyserver. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Fügen Sie Ihrem Connector-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Wenn Sie Podman verwendet haben, müssen Sie den Aardvark-DNS-Port anpassen.

- a. Stellen Sie per SSH eine Verbindung zur virtuellen Maschine des BlueXP Connector her.
- b. Öffnen Sie die Datei `podman_/usr/share/containers/containers.conf_` und ändern Sie den gewählten Port für den Aardvark DNS-Dienst. Ändern Sie ihn beispielsweise in 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

c. Starten Sie die virtuelle Connector-Maschine neu.

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 die BlueXP -Organisation an, die 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**.

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 8: 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 vor Ort

Sie können einen Connector auf einem Ihrer Maschinen vor Ort installieren. Um den Connector vor Ort auszuführen, müssen Sie die Host-Anforderungen überprüfen, Ihr Netzwerk einrichten, Cloud-Berechtigungen vorbereiten, den Connector installieren, den Connector einrichten und dann die von Ihnen vorbereiteten Berechtigungen bereitstellen.

Bevor Sie beginnen

- Überprüfen Sie Informationen zu ["Anschlüsse"](#).
- Sie sollten es überprüfen ["Einschränkungen an den Anschlüssen"](#).

Schritt: Überprüfung der Host-Anforderungen

Führen Sie die Connector-Software auf einem Host aus, der die Anforderungen an Betriebssystem, RAM und Port erfüllt. Stellen Sie sicher, dass Ihr Host diese Anforderungen erfüllt, bevor Sie den Connector installieren.



Der Connector reserviert den UID- und GID-Bereich von 19000 bis 19200. Dieser Bereich ist fest und kann nicht geändert werden. Wenn Drittanbietersoftware auf Ihrem Host UIDs oder GIDs innerhalb dieses Bereichs verwendet, schlägt die Connector-Installation fehl. NetApp empfiehlt die Verwendung eines Hosts ohne Drittanbietersoftware, um Konflikte zu vermeiden.

Dedizierter Host

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

Der Host kann eine beliebige Architektur aufweisen, die die folgenden Größenanforderungen erfüllt:

- CPU: 8 Cores oder 8 vCPUs
- RAM: 32 GB

Hypervisor

Ein Bare-Metal- oder gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

Anforderungen an das Betriebssystem und den Container

BlueXP unterstützt den Connector mit den folgenden Betriebssystemen, wenn BlueXP im Standardmodus oder im eingeschränkten Modus verwendet wird. Vor der Installation des Connectors ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte OS-Versionen	Unterstützte Connector-Versionen	Benötigter Container-Tool	SELinux
Red Hat Enterprise Linux	9.1 bis 9.4 8.6 bis 8.10 7,9	3.9.40 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Podman Version 4.6.1 oder 4.9.4 Zeigen Sie die Konfigurationsanforderungen für Podman an.	Unterstützt im Enforcing-Modus oder im permissiven Modus ¹
Ubuntu	24,04 LTS	3.9.45 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Docker Engine 23.06 bis 28.0.0.	Nicht unterstützt

Hinweise:

1. Die Verwaltung von Cloud Volumes ONTAP-Systemen wird von Connectors, auf denen SELinux auf dem Betriebssystem aktiviert ist, nicht unterstützt.
2. Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.

3. Für RHEL muss der Host 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.

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

BlueXP verwendet /opt, um das Verzeichnis und seinen Inhalt zu installieren
/opt/application/netapp.

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

BlueXP erfordert diesen Platz /var Da Docker oder Podman so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Insbesondere werden Container in der erstellt /var/lib/containers/storage Verzeichnis. Externe Mounts oder Symlinks funktionieren nicht für diesen Raum.

Schritt 2: Installieren Sie Podman oder Docker Engine

Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

- Podman ist für Red hat Enterprise Linux 8 und 9 erforderlich.

[Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

- Docker Engine ist für Ubuntu erforderlich.

[Zeigen Sie die von BlueXP unterstützten Versionen der Docker Engine an.](#)

Beispiel 4. Schritte

Podman

Führen Sie die folgenden Schritte aus, um Podman zu installieren und zu konfigurieren, um die folgenden Anforderungen zu erfüllen:

- Aktivieren und starten Sie den Dienst podman.socket
- python3 einbauen
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu



Passen Sie bei Verwendung von Podman den aardvark-dns-Dienstport (Standard: 53) nach der Installation des Connectors an, um Konflikte mit dem DNS-Port auf dem Host zu vermeiden. Folgen Sie den Anweisungen zur Portkonfiguration.

Schritte

1. Entfernen Sie das Paket podman-Docker, wenn es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

Podman ist über die offiziellen Red hat Enterprise Linux-Repositorys erhältlich.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

3. Aktivieren und starten Sie den podman.Socket-Dienst.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie Python3.

```
sudo dnf install python3
```

5. Installieren Sie das EPEL Repository-Paket, wenn es nicht bereits auf Ihrem System verfügbar ist.

Dieser Schritt ist erforderlich, da podman-compose im Repository Extra Packages for Enterprise Linux (EPEL) verfügbar ist.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Für Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Installieren Sie das Paket „podman-compose“ 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Verwenden der `dnf install` Befehl erfüllt die Anforderung zum Hinzufügen von podman-compose zur Umgebungsvariable PATH. Der Installationsbefehl fügt podman-compose zu `/usr/bin` hinzu, das bereits im enthalten ist `secure_path` Option auf dem Host.

Docker Engine

Folgen Sie der Dokumentation von Docker, um die Docker Engine zu installieren.

Schritte

1. ["Installationsanweisungen von Docker anzeigen"](#)

Befolgen Sie die Schritte, um eine bestimmte Version der Docker Engine zu installieren. Durch die Installation der neuesten Version wird eine Docker Version installiert, die BlueXP nicht unterstützt.

2. Docker muss aktiviert und ausgeführt werden.

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

Schritt 3: Netzwerk einrichten

Richten Sie das Netzwerk ein, um sicherzustellen, dass der Connector Ressourcen mit Verbindungen zu Zielnetzwerken und ausgehendem Internetzugriff verwalten kann.

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, die von Computern kontaktiert werden, wenn die webbasierte Konsole von BlueXP verwendet wird

Computer, die über einen Webbrowser auf die BlueXP -Konsole zugreifen, müssen in der Lage sein, mehrere Endpunkte zu kontaktieren. Sie müssen die BlueXP -Konsole verwenden, um den Connector einzurichten und für die tägliche Verwendung von BlueXP .

"Bereiten Sie das Netzwerk für die BlueXP -Konsole vor".

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://mysupport.netapp.com>
- <https://signin.b2c.NetApp.com> (dieser Endpunkt ist die CNAME-URL für <https://mysupport.NetApp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- Um Bilder zu erhalten, benötigt das Installationsprogramm Zugriff auf einen der beiden folgenden Endpunkte:
 - Option 1 (empfohlen):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

Die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in

Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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
<p>AWS-Services (amazonaws.com):</p> <ul style="list-style-type: none"> • 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) 	<p>Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"</p>
<p>https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net</p>	<p>Für das Managen von Ressourcen in Azure Public Regionen.</p>
<p>https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn</p>	<p>Für das Management von Ressourcen in Azure China Regionen.</p>
<p>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</p>	<p>Zum Managen von Ressourcen in Google Cloud.</p>
<p>https://support.netapp.com https://mysupport.netapp.com</p>	<p>Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.</p>

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.
Wählen Sie zwischen zwei Endpunktsätzen: <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <ul style="list-style-type: none"> https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 <ul style="list-style-type: none"> https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io 	Um Bilder für Connector-Upgrades zu erhalten.

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

Proxy-Server

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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 4: 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. Sie müssen den Connector in Google Cloud installieren, um alle dort vorhandenen Ressourcen zu verwalten.

AWS

Wenn der Connector On-Premises installiert ist, müssen Sie BlueXP über AWS-Berechtigungen verfügen, 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 Dokumentation: 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. Nachdem Sie den Connector installiert haben, verknüpfen Sie diese Anmeldeinformationen mit dem Connector von BlueXP.

Azure

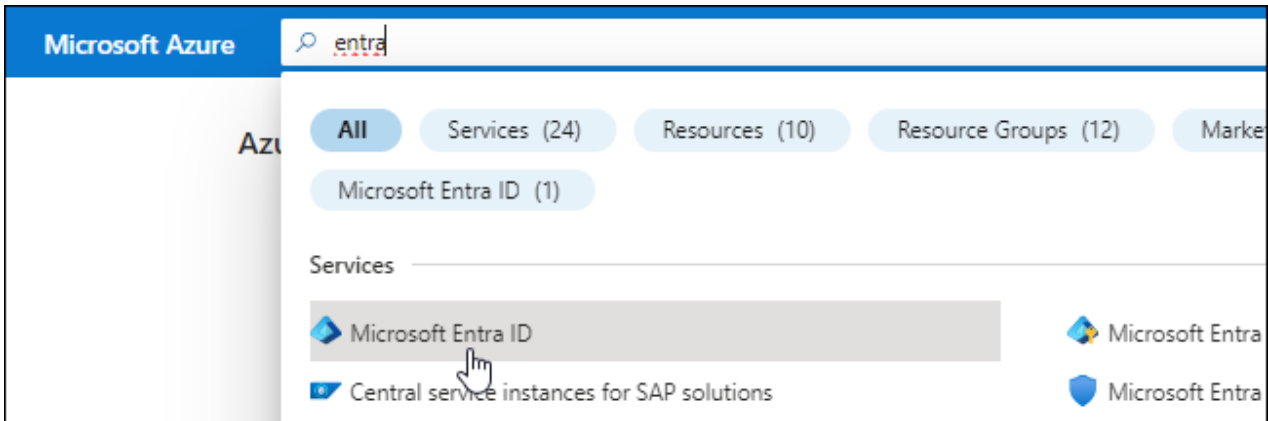
Wenn der Connector On-Premises installiert ist, müssen Sie BlueXP Azure-Berechtigungen erteilen, indem Sie einen Service-Principal in der Microsoft Entra-ID einrichten und die für BlueXP erforderlichen Azure-Berechtigungen erhalten.

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.

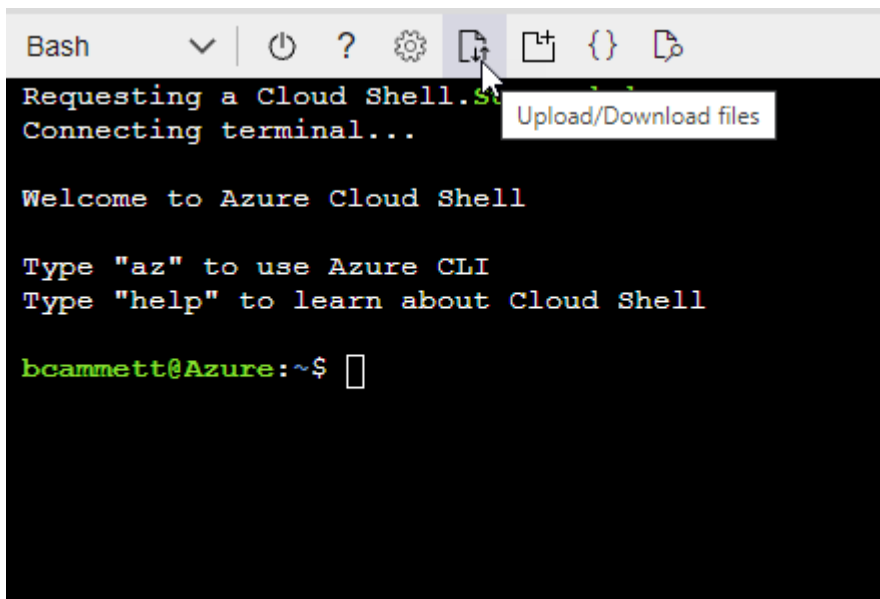
Beispiel

```
"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.



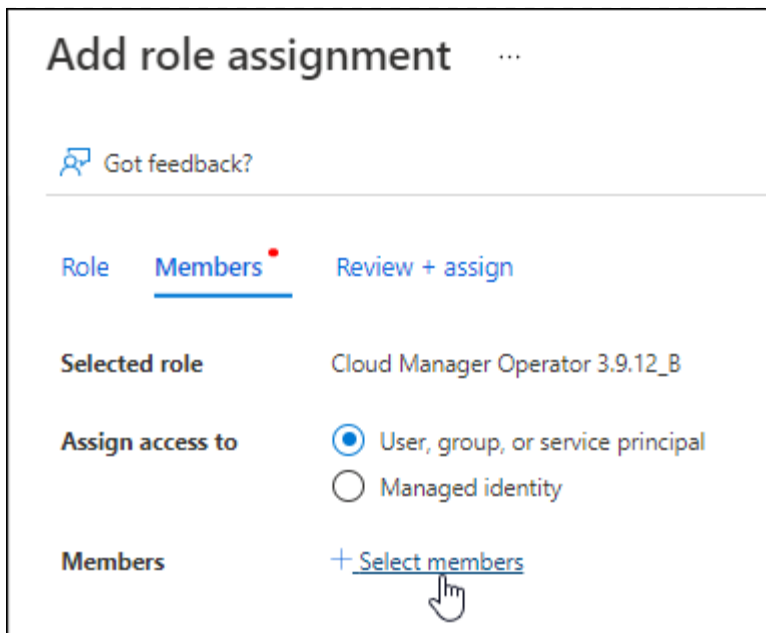
- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
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.

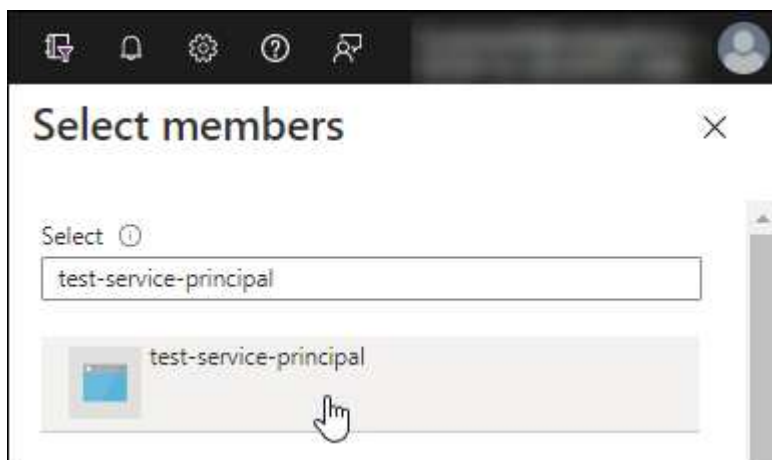
2. Applikation der Rolle zuweisen:

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



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



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

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

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

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Principal 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.


Request API permissions













Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview)

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**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA	

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

Schritt 5: 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.

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



Bei der manuellen Installation des Connectors können Sie kein Zertifikat für einen transparenten Proxyserver festlegen. Wenn Sie ein Zertifikat für einen transparenten Proxyserver festlegen müssen, müssen Sie nach der Installation die Wartungskonsole verwenden. Erfahren Sie mehr über die "[Connector-Wartungskonsole](#)".

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. 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.

2. 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.

3. 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.

4. Führen Sie das Installationskript aus.

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

Sie müssen Proxy-Informationen hinzufügen, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter `--proxy` und `--cacert` sind optional und werden nicht dazu aufgefordert. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben.

Hier ist ein Beispiel für die Konfiguration eines expliziten Proxyservers mit einem von einer Zertifizierungsstelle signierten Zertifikat:

```
./BlueXP-Connector-Cloud-v3.9.40--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 ein \ wie oben gezeigt verwenden.
- BlueXP unterstützt keine Benutzernamen oder Passwörter, die das @ Zeichen enthalten.
- Wenn das Passwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen umgehen, indem Sie es mit einem Backslash: & Oder !

Beispiel:

http://bxpproxyuser:netapp1!@address:3128

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyserver. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Fügen Sie Ihrem Connector-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Wenn Sie Podman verwendet haben, müssen Sie den Aardvark-DNS-Port anpassen.

- a. Stellen Sie per SSH eine Verbindung zur virtuellen Maschine des BlueXP Connector her.
- b. Öffnen Sie die Datei `podman_/usr/share/containers/containers.conf_` und ändern Sie den gewählten Port für den Aardvark DNS-Dienst. Ändern Sie ihn beispielsweise in 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

- c. Starten Sie die virtuelle Connector-Maschine neu.

Ergebnis

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

Schritt 6: Registrieren Sie den Connector bei BlueXP

Melden Sie sich bei BlueXP an und verknüpfen Sie den Connector mit Ihrer Organisation. Die Anmeldung hängt vom Modus ab, in dem Sie BlueXP verwenden. Wenn Sie BlueXP im Standardmodus verwenden, melden Sie sich über die SaaS-Website an. Wenn Sie BlueXP im eingeschränkten oder privaten Modus verwenden, melden Sie sich lokal vom Connector-Host aus an.

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 die BlueXP -Organisation an, die 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.

Lassen Sie den eingeschränkten Modus deaktiviert, da diese Schritte BlueXP im Standardmodus verwenden. (Außerdem wird der eingeschränkte Modus nicht unterstützt, wenn der Connector vor Ort installiert ist.)

- d. Wählen Sie **Start**.

Schritt 7: 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 AWS-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie 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 Azure-Anmeldeinformationen gerade erstellt haben, kann es einige Minuten dauern, bis sie 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.

Abonnieren Sie NetApp Intelligent Services (Standardmodus)

Abonnieren Sie NetApp Intelligent Services über den Marktplatz Ihres Cloud-Anbieters, um Datendienste stundenweise (PAYGO) oder über einen Jahresvertrag zu bezahlen. 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.

Mit einem Marktplatz-Abonnement können Sie die folgenden NetApp-Datendienste in Rechnung stellen:

- Backup und Recovery
- Cloud Volumes ONTAP
- Tiering
- Schutz durch Ransomware
- Disaster Recovery

Die Klassifizierung wird durch Ihr Abonnement aktiviert, für die Verwendung der Klassifizierung fallen jedoch keine Gebühren an.

Bevor Sie beginnen

Das Abonnieren von Datendiensten umfasst die Verknüpfung eines Marktplatzabonnements mit den Cloud-Anmeldeinformationen, 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

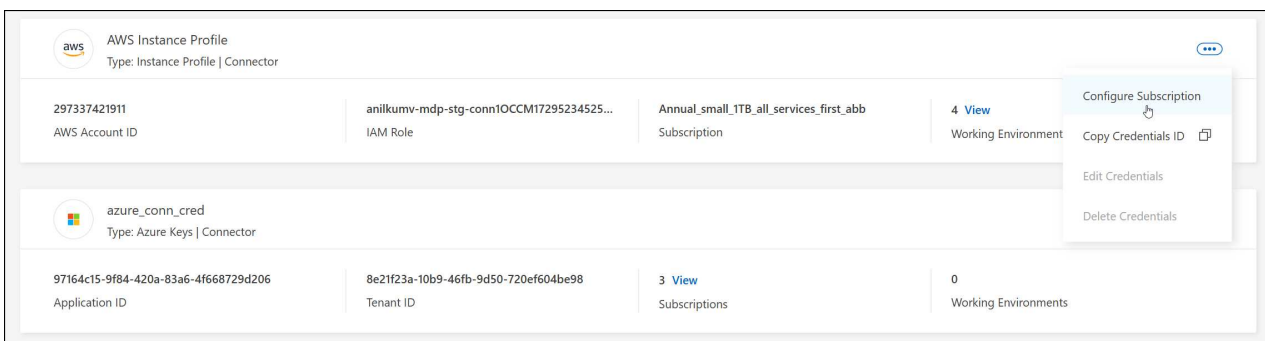
Das folgende Video zeigt die Schritte zum Abonnieren von NetApp Intelligent Services vom AWS Marketplace:

Abonnieren Sie NetApp Intelligent Services vom AWS Marketplace

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 **Abonnement konfigurieren**.

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 Sie **Konfigurieren**.
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 -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
- Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

Azure

Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Abonnement konfigurieren**.

Sie müssen Anmeldeinformationen auswählen, die einem Connector zugeordnet sind. Sie können kein Marketplace-Abonnement mit Anmeldeinformationen 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 Sie **Konfigurieren**.
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 zu BlueXP weitergeleitet.

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

- Wählen Sie die BlueXP -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
- Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldeinformationen verknüpft.

Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

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

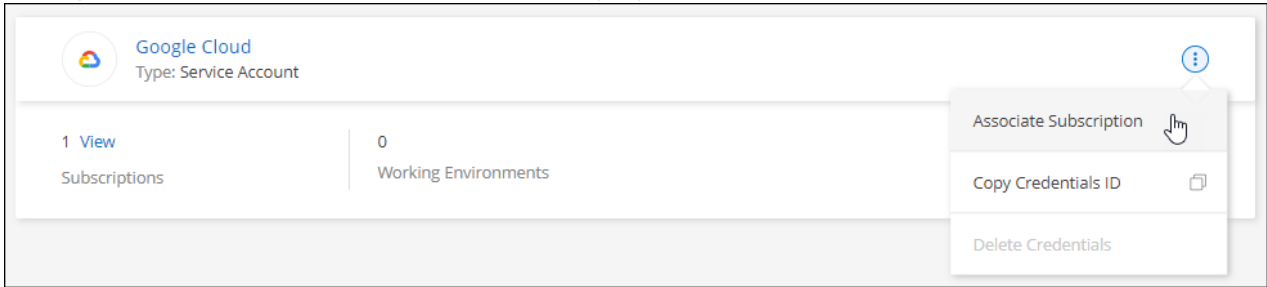
[Abonnieren Sie NetApp Intelligent Services vom Azure Marketplace](#)

Google Cloud

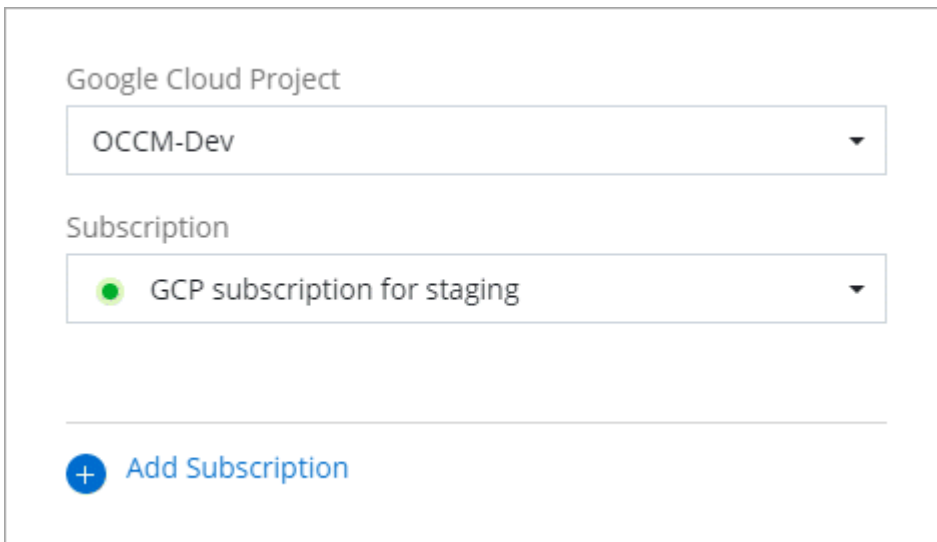
Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.

2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Abonnement konfigurieren**. +neuer Screenshot erforderlich (TS)



3. Um ein bestehendes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus, und wählen Sie dann **Konfigurieren** aus.

A screenshot of a configuration form. It has two dropdown menus. The first is labeled 'Google Cloud Project' and has 'OCCM-Dev' selected. The second is labeled 'Subscription' and has 'GCP subscription for staging' selected. Below the dropdowns, there is a blue button with a plus sign and the text '+ Add Subscription'.

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 weitergeleitet wurden auf die "[NetApp Intelligent Services-Seite im Google Cloud Marketplace](#)", stellen Sie sicher, dass im oberen Navigationsmenü das richtige Projekt ausgewählt ist.

Google Cloud netapp.com

Product details

NetApp BlueXP

NetApp, Inc.

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

SUBSCRIBE

OVERVIEW PRICING DOCUMENTATION SUPPORT

Overview

BlueXP is NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp's storage, mobility, protection, and analysis services within your Google Cloud environment.

Additional details

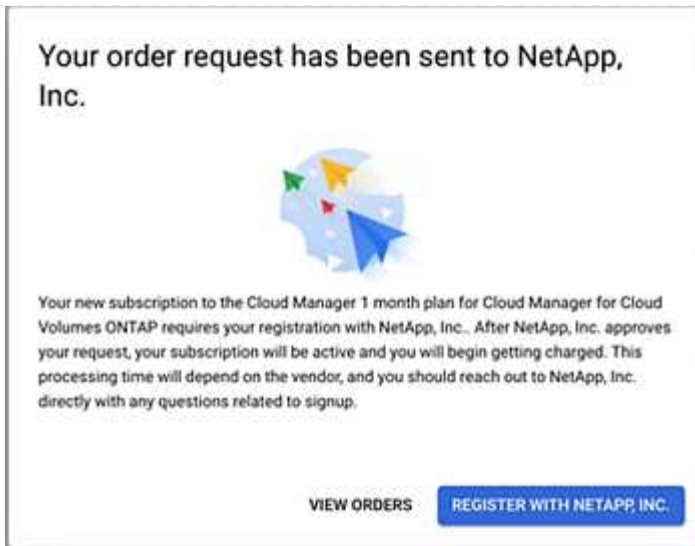
Type: [SaaS & APIs](#)
Last updated: 12/19/22
Category: [Analytics](#), [Developer tools](#), [Storage](#)

- 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 Ihrer Organisation oder 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 -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
- Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

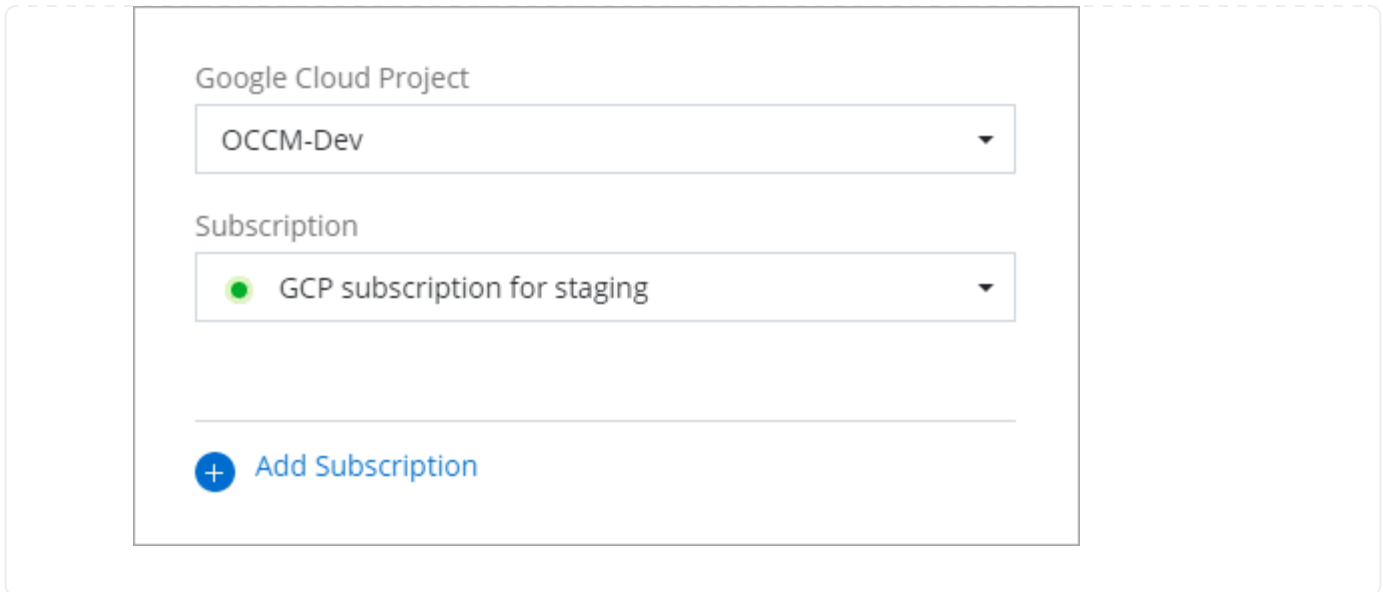
Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

- 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.



Verwandte Informationen

- ["Managen Sie kapazitätsbasierte BYOL-Lizenzen für Cloud Volumes ONTAP"](#)
- ["Verwalten Sie BYOL-Lizenzen für Datendienste"](#)
- ["Verwalten von AWS-Anmeldeinformationen und Abonnements"](#)
- ["Verwalten von Azure-Anmeldeinformationen und Abonnements"](#)
- ["Verwalten Sie Google Cloud-Anmeldeinformationen und -Abonnements"](#)

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.

Verwandte Informationen

["BlueXP Implementierungsmodi"](#)

Beginnen Sie mit dem eingeschränkten Modus

Erste Schritte im Workflow (eingeschränkter Modus)

Beginnen Sie mit BlueXP im eingeschränkten Modus, indem Sie Ihre Umgebung vorbereiten und den Connector bereitstellen.

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, stellen Sie sicher, dass Sie Folgendes verstehen: ["Anschlüsse"](#) Und ["Bereitstellungsmodi"](#) .

1

"Vorbereitungen für die Implementierung"

1. Bereiten Sie einen dedizierten Linux-Host vor, der die Anforderungen für CPU, RAM, Festplattenspeicher, Container-Orchestrierungstool und vieles 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 NetApp Intelligent Services (optional)"

Optional: Abonnieren Sie NetApp Intelligent Services über den Marktplatz Ihres Cloud-Anbieters und bezahlen Sie Datenservices stundenweise (PAYGO) oder über einen Jahresvertrag. NetApp Intelligent Services umfassen Backup und Recovery, Cloud Volumes ONTAP, Tiering, Ransomware-Schutz und Disaster Recovery. Die Klassifizierung ist in Ihrem Abonnement ohne zusätzliche Kosten enthalten.

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.

Der Host kann eine beliebige Architektur aufweisen, die die folgenden Größenanforderungen erfüllt:

- CPU: 8 Cores oder 8 vCPUs
- RAM: 32 GB

Hypervisor

Ein Bare-Metal- oder gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

Anforderungen an das Betriebssystem und den Container

BlueXP unterstützt den Connector mit den folgenden Betriebssystemen, wenn BlueXP im Standardmodus oder im eingeschränkten Modus verwendet wird. Vor der Installation des Connectors ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte OS-Versionen	Unterstützte Connector-Versionen	Benötigter Container-Tool	SELinux
Red Hat Enterprise Linux	9.1 bis 9.4 8.6 bis 8.10 7,9	3.9.40 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Podman Version 4.6.1 oder 4.9.4 Zeigen Sie die Konfigurationsanforderungen für Podman an.	Unterstützt im Enforcing-Modus oder im permissiven Modus ¹

Betriebssystem	Unterstützte OS-Versionen	Unterstützte Connector-Versionen	Benötigter Container-Tool	SELinux
Ubuntu	24,04 LTS	3.9.45 oder höher mit BlueXP im Standard- oder eingeschränkter Modus	Docker Engine 23.06 bis 28.0.0.	Nicht unterstützt

Hinweise:

1. Die Verwaltung von Cloud Volumes ONTAP-Systemen wird von Connectors, auf denen SELinux auf dem Betriebssystem aktiviert ist, nicht unterstützt.
2. Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.
3. Für RHEL muss der Host 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.

Instanztyp für AWS EC2

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.2xlarge.

Azure VM-Größe

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen Standard_D8s_v3.

Google Cloud-Maschinentyp

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n2-Standard-8.

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

BlueXP verwendet /opt, um das Verzeichnis und seinen Inhalt zu installieren /opt/application/netapp.

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

BlueXP erfordert diesen Platz /var Da Docker oder Podman so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Insbesondere werden Container in der erstellt /var/lib/containers/storage Verzeichnis. Externe Mounts oder Symlinks funktionieren nicht für diesen Raum.

Schritt 4: Installieren Sie Podman oder Docker Engine

Wenn Sie planen, die Connector-Software manuell zu installieren, müssen Sie den Host vorbereiten, indem Sie Podman oder die Docker Engine installieren.

Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

- Podman ist für Red hat Enterprise Linux 8 und 9 erforderlich.

[Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

- Docker Engine ist für Ubuntu erforderlich.

[Zeigen Sie die von BlueXP unterstützten Versionen der Docker Engine an.](#)

Beispiel 5. Schritte

Podman

Führen Sie die folgenden Schritte aus, um Podman zu installieren und zu konfigurieren, um die folgenden Anforderungen zu erfüllen:

- Aktivieren und starten Sie den Dienst podman.socket
- python3 einbauen
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu



Passen Sie bei Verwendung von Podman den aardvark-dns-Dienstport (Standard: 53) nach der Installation des Connectors an, um Konflikte mit dem DNS-Port auf dem Host zu vermeiden. Folgen Sie den Anweisungen zur Portkonfiguration.

Schritte

1. Entfernen Sie das Paket podman-Docker, wenn es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

Podman ist über die offiziellen Red hat Enterprise Linux-Repositorys erhältlich.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

3. Aktivieren und starten Sie den podman.Socket-Dienst.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie Python3.

```
sudo dnf install python3
```

5. Installieren Sie das EPEL Repository-Paket, wenn es nicht bereits auf Ihrem System verfügbar ist.

Dieser Schritt ist erforderlich, da podman-compose im Repository Extra Packages for Enterprise Linux (EPEL) verfügbar ist.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Für Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Installieren Sie das Paket „podman-compose“ 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Verwenden der `dnf install` Befehl erfüllt die Anforderung zum Hinzufügen von podman-compose zur Umgebungsvariable PATH. Der Installationsbefehl fügt podman-compose zu `/usr/bin` hinzu, das bereits im enthalten ist `secure_path` Option auf dem Host.

Docker Engine

Folgen Sie der Dokumentation von Docker, um die Docker Engine zu installieren.

Schritte

1. ["Installationsanweisungen von Docker anzeigen"](#)

Befolgen Sie die Schritte, um eine bestimmte Version der Docker Engine zu installieren. Durch die Installation der neuesten Version wird eine Docker Version installiert, die BlueXP nicht unterstützt.

2. Docker muss aktiviert und ausgeführt werden.

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

Schritt 5: 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://api.bluexp.netapp.com	Die webbasierte BlueXP -Konsole kontaktiert diesen Endpunkt, um mit der BlueXP -API für Aktionen in Bezug auf Autorisierung, Lizenzierung, Abonnements, Anmeldeinformationen, Benachrichtigungen und vieles mehr zu interagieren.
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 ermöglichen.
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 mehrere URLs.

- Die folgenden Endpunkte werden immer kontaktiert, unabhängig davon, wo Sie den Connector installieren:
 - <https://mysupport.netapp.com>
 - <https://signin.b2c.NetApp.com> (dieser Endpunkt ist die CNAME-URL für <https://mysupport.NetApp.com>)
 - <https://cloudmanager.cloud.netapp.com/tenancy>
 - <https://stream.cloudmanager.cloud.netapp.com>
 - <https://production-artifacts.cloudmanager.cloud.netapp.com>
- Wenn Sie den Connector in einer AWS Government-Region installieren, benötigt das Installationsprogramm auch Zugriff auf die folgenden Endpunkte:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraproduct.azurecr.io>

- Wenn Sie den Connector in einer Azure Government-Region installieren, benötigt das Installationsprogramm auch Zugriff auf die folgenden Endpunkte:
 - https://*.blob.core.windows.net
 - <https://occmclientinfragov.azurecr.us>
- Wenn Sie den Connector in einer kommerziellen Region oder einer souveränen Region installieren, können Sie zwischen zwei Endpunktsätzen wählen:
 - Option 1 (empfohlen):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

Die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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
<p>AWS-Services (amazonaws.com):</p> <ul style="list-style-type: none"> • 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) 	<p>Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"</p>
<p>https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net</p>	<p>Für das Managen von Ressourcen in Azure Public Regionen.</p>
<p>https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net</p>	<p>Managen von Ressourcen in Azure Government Regionen.</p>
<p>https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn</p>	<p>Für das Management von Ressourcen in Azure China Regionen.</p>
<p>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</p>	<p>Zum Managen von Ressourcen in Google Cloud.</p>
<p>https://support.netapp.com https://mysupport.netapp.com</p>	<p>Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.</p>
<p>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</p>	<p>Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen.</p>

Endpunkte	Zweck
Wenn sich der Connector in einer AWS Regierungsregion befindet: https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Um Images für Connector-Upgrades abzurufen, wenn der Connector in einer AWS-Regierungsregion installiert ist.
Wenn sich der Connector in einer Azure Government-Region befindet: https://*.blob.core.windows.net https://occmclientinfragov.azurecr.us	So erhalten Sie Bilder für Connector-Upgrades, wenn der Connector in einer Azure Government-Region installiert ist.
Wenn sich der Connector in einer kommerziellen Region oder einer souveränen Region befindet, können Sie zwischen zwei Endpunktsätzen wählen: <ul style="list-style-type: none"> • Option 1 (empfohlen) ¹ <ul style="list-style-type: none"> https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 <ul style="list-style-type: none"> https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io 	Um Bilder für Connector-Upgrades zu erhalten, wenn der Connector in einer kommerziellen Region oder souveränen Region installiert ist.

¹ die in Option 1 aufgeführten Endpunkte werden empfohlen, da sie sicherer sind. Wir empfehlen, dass Sie Ihre Firewall so einrichten, dass die in Option 1 aufgeführten Endpunkte zugelassen werden, während Sie die in Option 2 aufgeführten Endpunkte nicht zulassen. Zu diesen Endpunkten ist Folgendes zu beachten:

- Die in Option 1 aufgeführten Endpunkte werden ab Version 3.9.47 des Connectors unterstützt. Es besteht keine Abwärtskompatibilität mit früheren Versionen des Connectors.
- Der Connector kontaktiert zuerst die unter Option 2 aufgeführten Endpunkte. Wenn auf diese Endpunkte nicht zugegriffen werden kann, kontaktiert der Connector automatisch die in Option 1 aufgeführten Endpunkte.
- Die Endpunkte in Option 1 werden nicht unterstützt, wenn Sie den Connector mit BlueXP Backup und Recovery oder BlueXP Ransomware-Schutz verwenden. In diesem Fall können Sie die in Option 1 aufgeführten Endpunkte nicht zulassen, während Sie die in Option 2 aufgeführten Endpunkte zulassen.

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.

Create public IP address ×

Name * ✓

SKU * ⓘ

Basic Standard

Assignment

Dynamic Static

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

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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 6: 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.

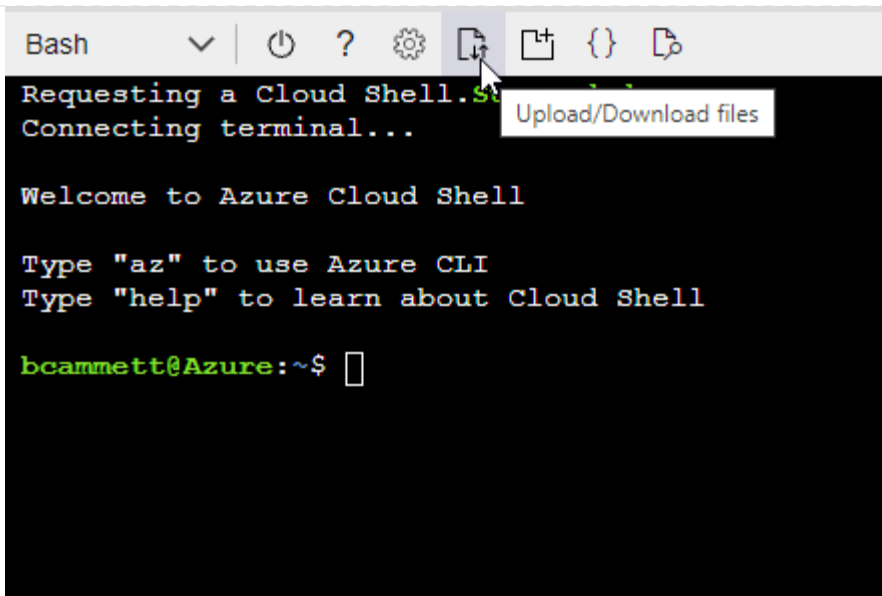
Beispiel

```
"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

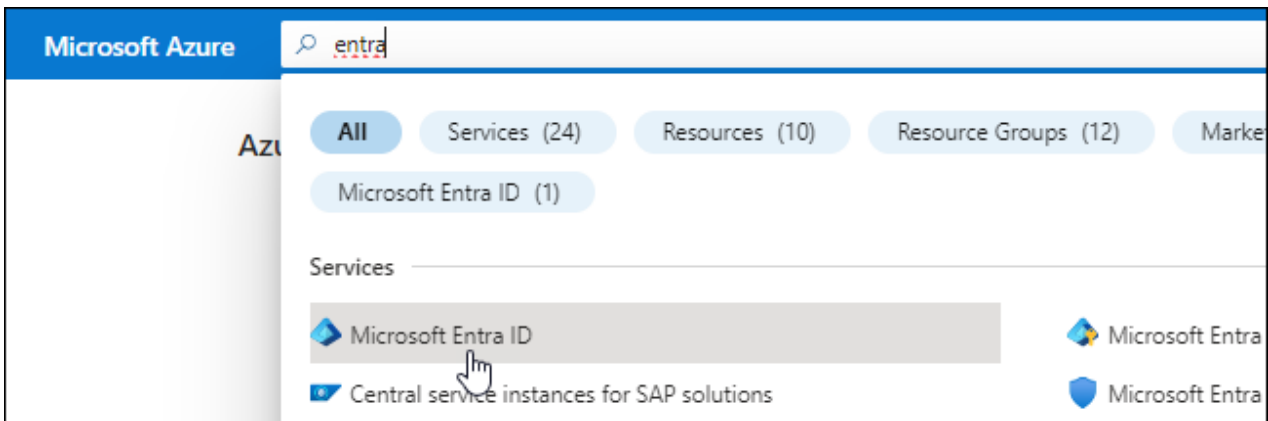
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

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.

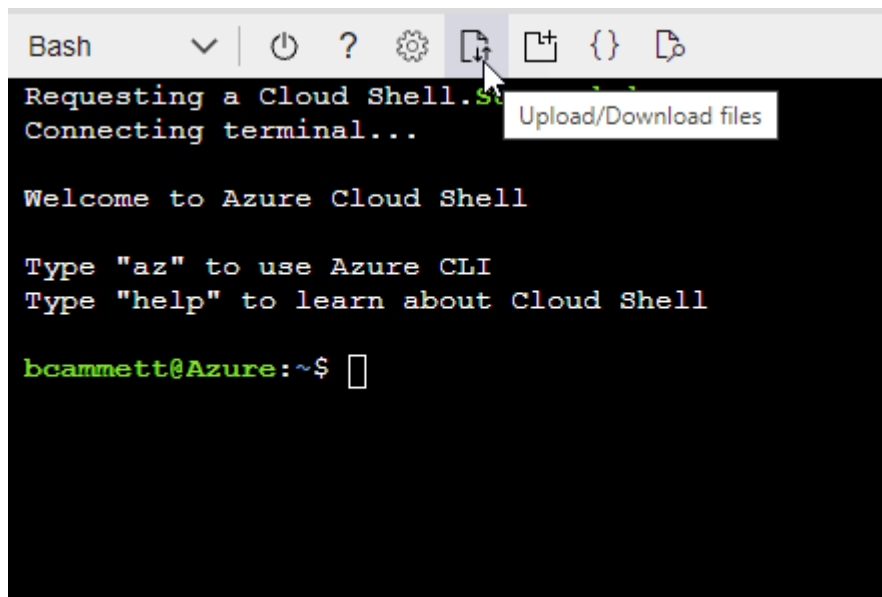
Beispiel

```
"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.



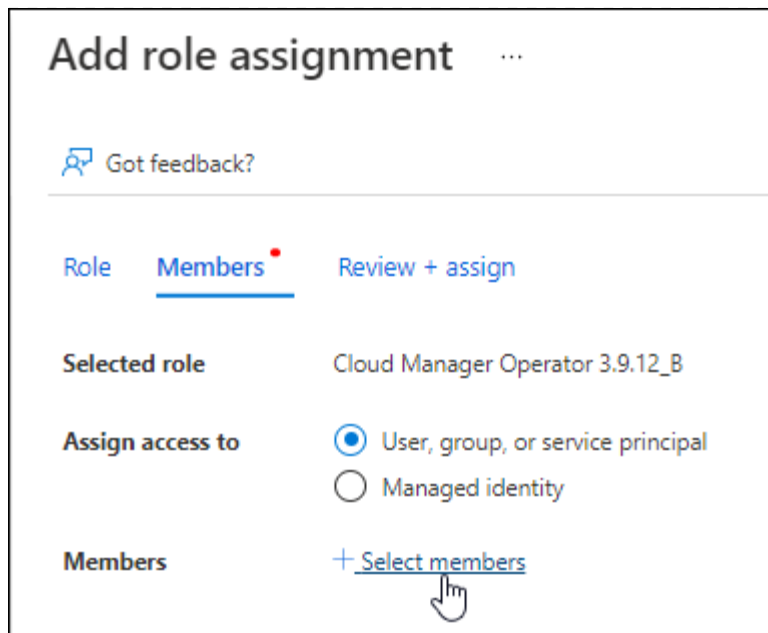
- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
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.

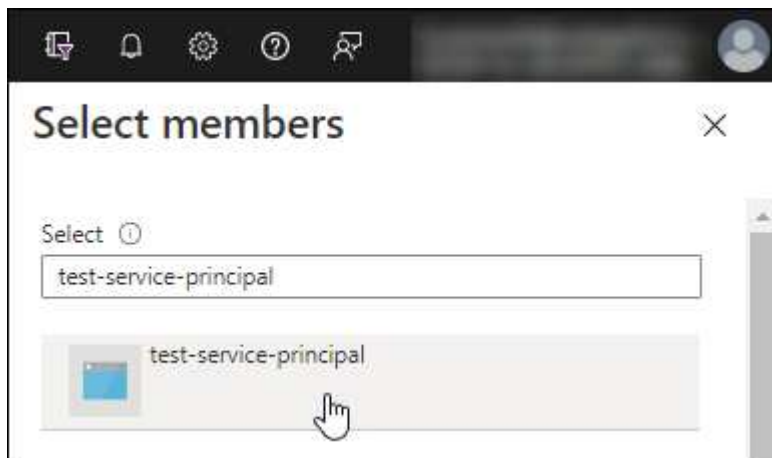
2. Applikation der Rolle zuweisen:

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



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



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

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

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

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Principal 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.

Request API permissions


Select an API













Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Batch</p> <p>Schedule large-scale parallel and HPC applications in the cloud</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Data Catalog</p> <p>Programmatic access to Data Catalog resources to register, annotate and search data assets</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Data Explorer</p> <p>Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p> </div>
<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Data Lake</p> <p>Access to storage and compute for big data analytic scenarios</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure DevOps</p> <p>Integrate with Azure DevOps and Azure DevOps server</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Import/Export</p> <p>Programmatic control of import/export jobs</p> </div>
<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Key Vault</p> <p>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Rights Management Services</p> <p>Allow validated users to read and write protected content</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Service Management</p> <p>Programmatic access to much of the functionality available through the Azure portal</p> </div>
<div style="border: 1px solid #ccc; padding: 5px;">  <p>Azure Storage</p> <p>Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Customer Insights</p> <p>Create profile and interaction models for your products</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;">  <p>Data Export Service for Microsoft Dynamics 365</p> <p>Export data from Microsoft Dynamics CRM organization to an external destination</p> </div>

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

Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview)

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**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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 7: 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

Stellen Sie den Connector im eingeschränkten Modus bereit, damit Sie BlueXP mit eingeschränkter ausgehender Konnektivität verwenden 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"](#)

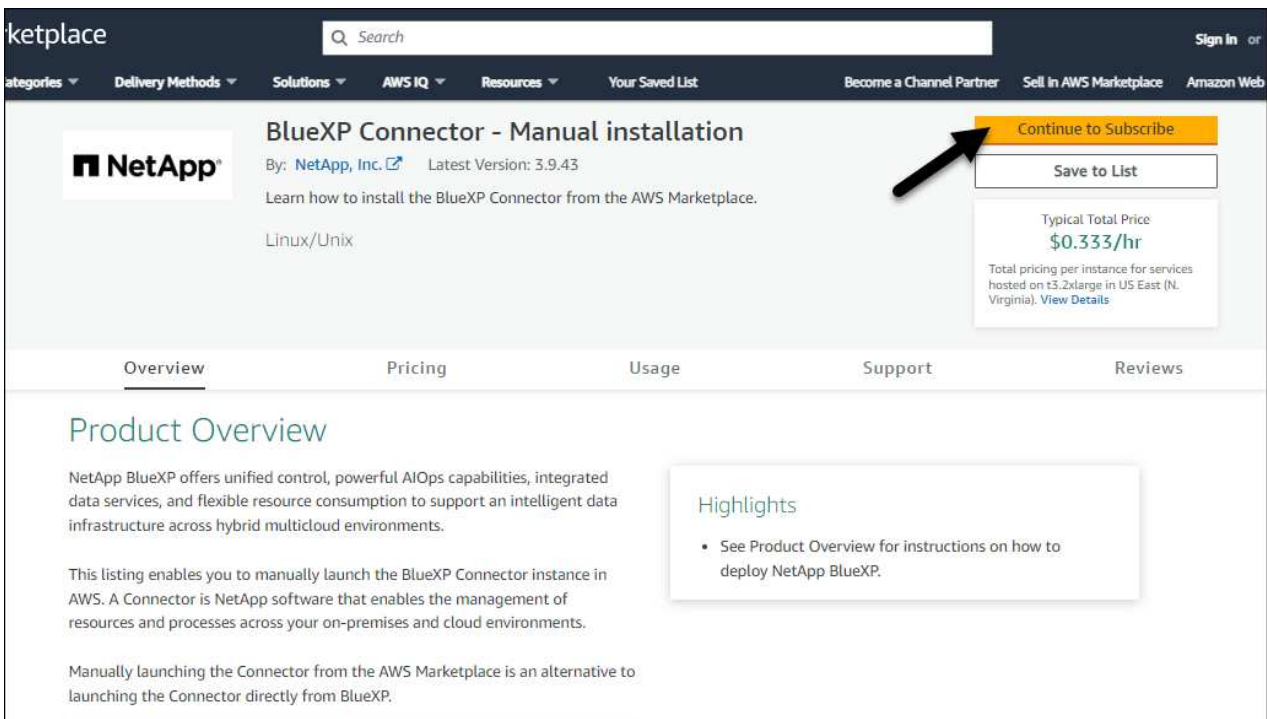
- Berechtigung zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Verständnis der CPU- und RAM-Anforderungen für die Instanz.

["Prüfen Sie die Instanzanforderungen"](#).

- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

1. Go to the ["BlueXP Connector listing on the AWS Marketplace"](#)
2. Wählen Sie auf der Marketplace-Seite **Weiter zum Abonnieren**.



The screenshot shows the AWS Marketplace listing for NetApp BlueXP Connector - Manual installation. The page features a dark navigation bar with the 'marketplace' logo and a search bar. Below the navigation bar, the product title 'BlueXP Connector - Manual installation' is displayed, along with the NetApp logo and the text 'By: NetApp, Inc. Latest Version: 3.9.43'. A prominent orange button labeled 'Continue to Subscribe' is highlighted with a black arrow. Below this button are two white buttons: 'Save to List' and a pricing box showing 'Typical Total Price \$0.333/hr'. The pricing box also includes the text 'Total pricing per instance for services hosted on t3.2xlarge in US East (N. Virginia). View Details'. The page is divided into sections: 'Overview', 'Pricing', 'Usage', 'Support', and 'Reviews'. The 'Product Overview' section contains text about NetApp BlueXP capabilities and a 'Highlights' box with a bullet point: 'See Product Overview for instructions on how to deploy NetApp BlueXP.'

3. Um die Software zu abonnieren, wählen Sie **Bedingungen akzeptieren**.

Das Abonnement kann einige Minuten dauern.

4. Wählen Sie nach Abschluss des Abonnements **Weiter zur Konfiguration** aus.

ketplace Hello,

categories ▾ Delivery Methods ▾ Solutions ▾ AWS IQ ▾ Resources ▾ Your Saved List Become a Channel Partner Sell In AWS Marketplace Amazon Web Se

NetApp BlueXP Connector - Manual installation [Continue to Configuration](#)

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

Subscribe to this software

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

Terms and Conditions

NetApp, Inc. Offer

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

Product	Effective date	Expiration date	Action
BlueXP Connector - Manual installation	N/A	N/A	Show Details

5. Stellen Sie auf der Seite **Configure this Software** sicher, dass Sie die richtige Region ausgewählt haben, und wählen Sie dann **Continue to Launch** aus.

6. Wählen Sie auf der Seite **Diese Software starten** unter **Aktion auswählen 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.

7. 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 Betriebssystem-Images:** 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 (t3.2xlarge ist vorausgewählt und 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.
 - Geben Sie die Einstellungen für Sicherheitsgruppen an, die die erforderlichen Verbindungsmethoden für die Connector-Instanz aktivieren: SSH, HTTP und HTTPS.

["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"](#)

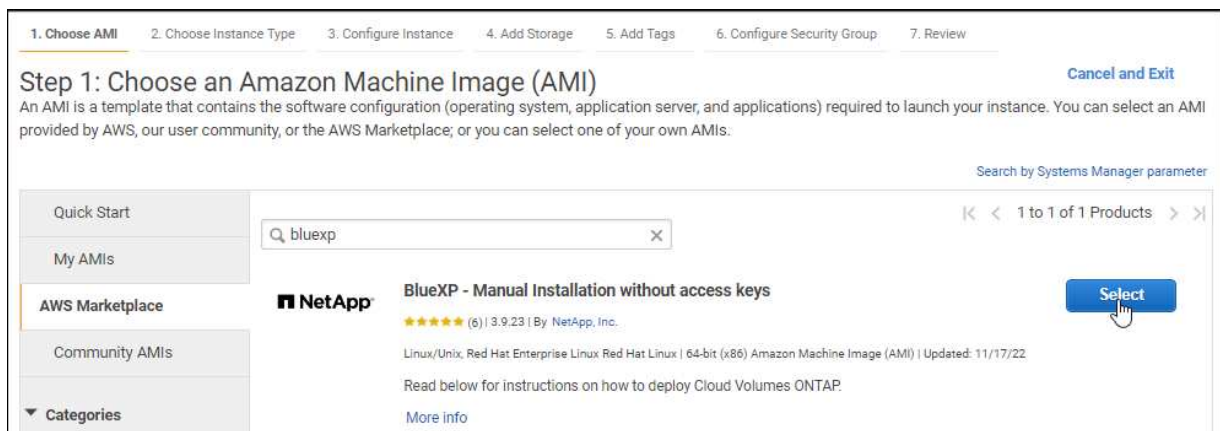
- Eine IAM-Rolle mit angehängter Richtlinie, die die erforderlichen Berechtigungen für den Connector enthält.

["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 (t3.2xlarge wird empfohlen).

"Prüfen Sie die Anforderungen an die Instanz".

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

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

- **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.

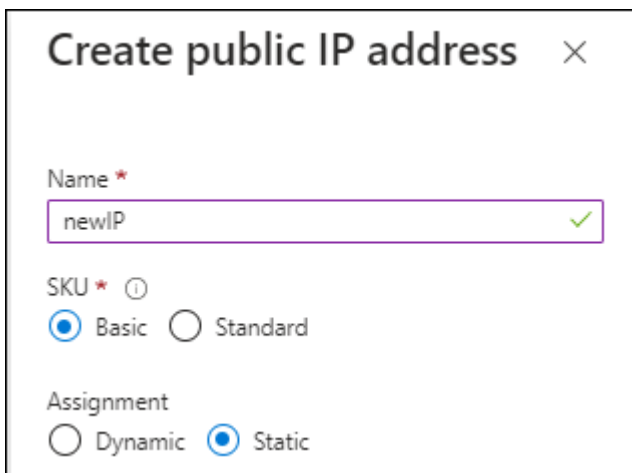
"Erfahren Sie, wie Sie Azure-Berechtigungen einrichten"

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 Standard_D8s_v3.
- **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.



The screenshot shows a dialog box titled "Create public IP address" with a close button (X) in the top right corner. Below the title, there are three sections of form controls:

- Name ***: A text input field containing "newIP" with a green checkmark on the right side, indicating it is valid.
- SKU * ⓘ**: Two radio button options: "Basic" (which is selected) and "Standard".
- Assignment**: Two radio button options: "Dynamic" and "Static" (which is selected).

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"](#).

- 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.

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



Bei der manuellen Installation des Connectors können Sie kein Zertifikat für einen transparenten Proxyserver festlegen. Wenn Sie ein Zertifikat für einen transparenten Proxyserver festlegen müssen, müssen Sie nach der Installation die Wartungskonsole verwenden. Erfahren Sie mehr über die ["Connector-Wartungskonsole"](#).

- Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

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. 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.

2. 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.

3. 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.

4. Führen Sie das Installationskript aus.

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

Sie müssen Proxy-Informationen hinzufügen, wenn Ihr Netzwerk einen Proxy für den Internetzugang benötigt. Sie können entweder einen transparenten oder einen expliziten Proxy hinzufügen. Die Parameter `--proxy` und `--cacert` sind optional und werden nicht dazu aufgefordert. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben.

Hier ist ein Beispiel für die Konfiguration eines expliziten Proxyservers mit einem von einer Zertifizierungsstelle signierten Zertifikat:

```
./BlueXP-Connector-Cloud-v3.9.40--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 ein \ wie oben gezeigt verwenden.
- BlueXP unterstützt keine Benutzernamen oder Passwörter, die das @ Zeichen enthalten.

- Wenn das Passwort eines der folgenden Sonderzeichen enthält, müssen Sie dieses Sonderzeichen umgehen, indem Sie es mit einem Backslash: & Oder !

Beispiel:

```
http://bxpproxyuser:netapp1!\@address:3128
```

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist für HTTPS-Proxyserver, abfangende Proxyserver und transparente Proxyserver erforderlich.

Hier ist ein Beispiel für die Konfiguration eines transparenten Proxyserver. Wenn Sie einen transparenten Proxy konfigurieren, müssen Sie den Proxyserver nicht definieren. Fügen Sie Ihrem Connector-Host lediglich ein von einer Zertifizierungsstelle signiertes Zertifikat hinzu:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert  
/tmp/cacert/certificate.cer
```

5. Wenn Sie Podman verwendet haben, müssen Sie den Aardvark-DNS-Port anpassen.
 - a. Stellen Sie per SSH eine Verbindung zur virtuellen Maschine des BlueXP Connector her.
 - b. Öffnen Sie die Datei `podman_/usr/share/containers/containers.conf_` und ändern Sie den gewählten Port für den Aardvark DNS-Dienst. Ändern Sie ihn beispielsweise in 54.

```
vi /usr/share/containers/containers.conf  
...  
# Port to use for dns forwarding daemon with netavark in rootful  
bridge  
# mode and dns enabled.  
# Using an alternate port might be useful if other DNS services  
should  
# run on the machine.  
#  
dns_bind_port = 54  
...  
Esc:wq
```

- c. Starten Sie die virtuelle Connector-Maschine neu.

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.

Bevor Sie beginnen

Die Person, die den BlueXP -Connector eingerichtet hat, muss sich mit einem Login bei BlueXP anmelden, das nicht zu einem BlueXP -Konto oder einer Organisation gehört.

Wenn Ihr BlueXP -Login mit einem anderen Konto oder einer anderen Organisation verknüpft ist, müssen Sie sich mit einem neuen BlueXP -Login registrieren. Andernfalls wird die Option zum Aktivieren des eingeschränkten Modus auf dem Setup-Bildschirm nicht angezeigt.

Schritte

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

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

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.
 - 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.

Hi Tami,
Welcome to NetApp BlueXP

Let's get started by creating an account for your organization.

If your organization already has an existing account, it's best to ask the account admin to add you to it. [Learn how to add user](#)

Connector name: BlueXP1 Account name: MyCompany

Are you running in a secured environment? ^

Use restricted deployment mode to disconnect this account from the BlueXP backend services. Restricted deployments are often required in extremely secure or regulated environments. Note: Use this option only if you're sure you need it as some BlueXP functionality is not available in restricted deployments.

[Learn more about BlueXP deployment modes](#)

Enable restricted mode on this account

Let's start

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.

Abonnieren Sie NetApp Intelligent Services (eingeschränkter Modus)

Abonnieren Sie NetApp Intelligent Services über den Marktplatz Ihres Cloud-Anbieters, um Datendienste stundenweise (PAYGO) oder über einen Jahresvertrag zu bezahlen. 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 Marktplatz-Abonnement ermöglicht die Abrechnung der folgenden Datendienste im eingeschränkten Modus:

- Backup und Recovery
- Cloud Volumes ONTAP
- Tiering
- Schutz durch Ransomware
- Disaster Recovery

Die Klassifizierung wird durch Ihr Abonnement aktiviert, für die Verwendung der Klassifizierung fallen jedoch keine Gebühren an.

Bevor Sie beginnen

Das Abonnieren von Datendiensten umfasst die Verknüpfung eines Marktplatzabonnements mit den Cloud-Anmeldeinformationen, 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

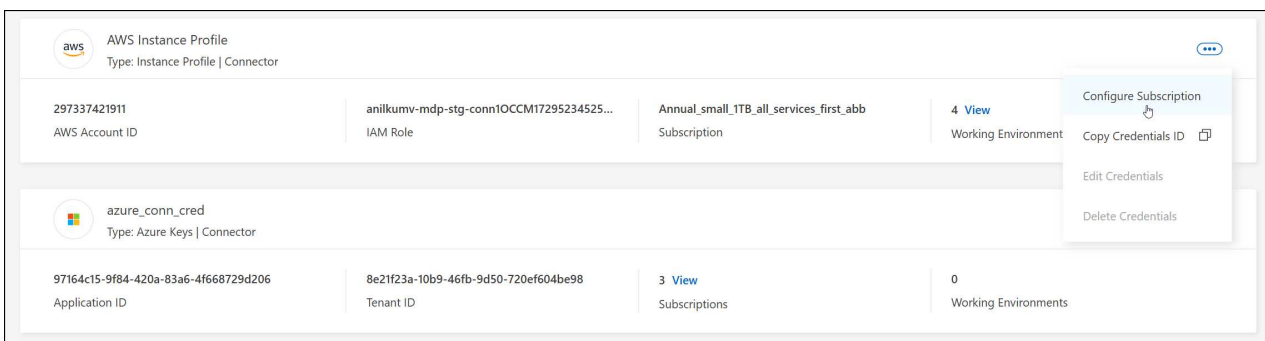
Das folgende Video zeigt die Schritte zum Abonnieren von NetApp Intelligent Services vom AWS Marketplace:

Abonnieren Sie NetApp Intelligent Services vom AWS Marketplace

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 **Abonnement konfigurieren**.

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 Sie **Konfigurieren**.
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 -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
- Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

Azure

Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Abonnement konfigurieren**.

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 Sie **Konfigurieren**.
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 zu BlueXP weitergeleitet.

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

- Wählen Sie die BlueXP -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
- Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

- Wählen Sie **Speichern**.

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

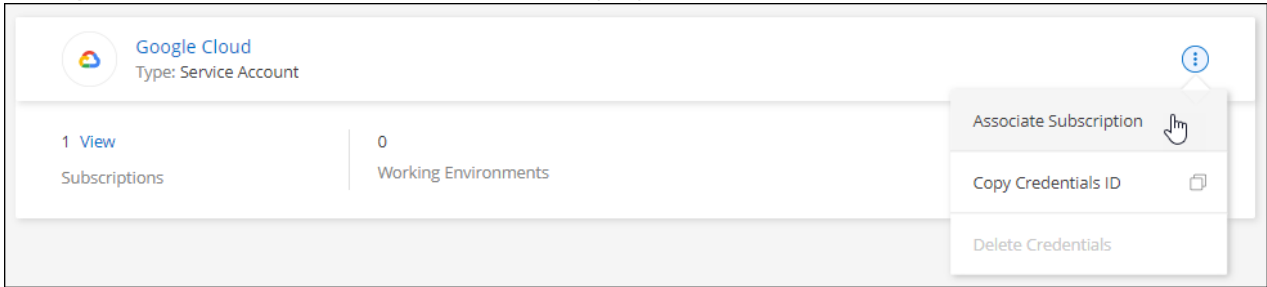
[Abonnieren Sie NetApp Intelligent Services vom Azure Marketplace](#)

Google Cloud

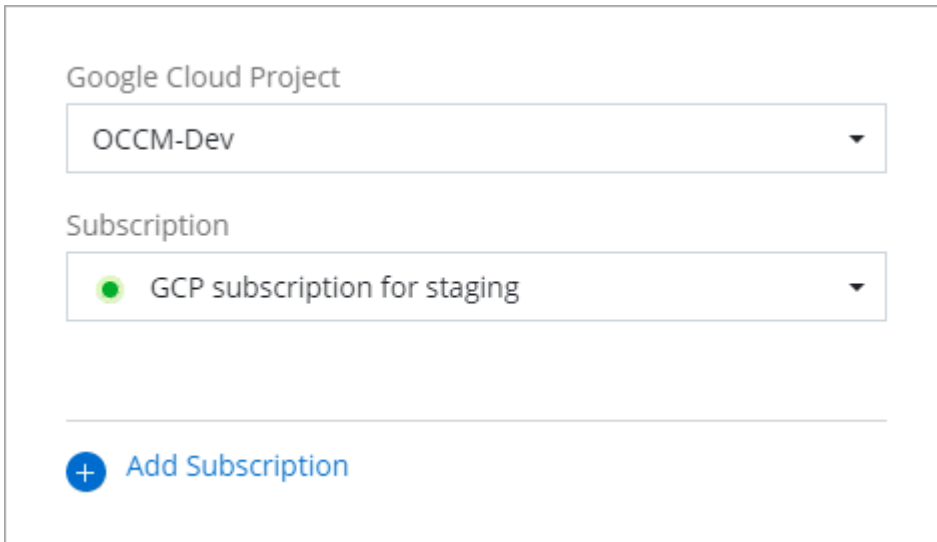
Schritte

1. Wählen Sie oben rechts in der Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.

2. Wählen Sie das Aktionsmenü für einen Satz von Anmeldeinformationen und dann **Abonnement konfigurieren**. +neuer Screenshot erforderlich (TS)



3. Um ein bestehendes Abonnement mit den ausgewählten Anmeldeinformationen zu konfigurieren, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Dropdown-Liste aus, und wählen Sie dann **Konfigurieren** aus.

A screenshot of a configuration form. It has two dropdown menus. The first is labeled 'Google Cloud Project' and has 'OCCM-Dev' selected. The second is labeled 'Subscription' and has 'GCP subscription for staging' selected. Below the dropdowns is a blue button with a plus sign and the text 'Add Subscription'.

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 weitergeleitet wurden auf die "[NetApp Intelligent Services-Seite im Google Cloud Marketplace](#)", stellen Sie sicher, dass im oberen Navigationsmenü das richtige Projekt ausgewählt ist.

Google Cloud netapp.com

Product details

NetApp BlueXP

NetApp, Inc.

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

SUBSCRIBE

OVERVIEW PRICING DOCUMENTATION SUPPORT

Overview

BlueXP is NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp's storage, mobility, protection, and analysis services within your Google Cloud environment.

Additional details

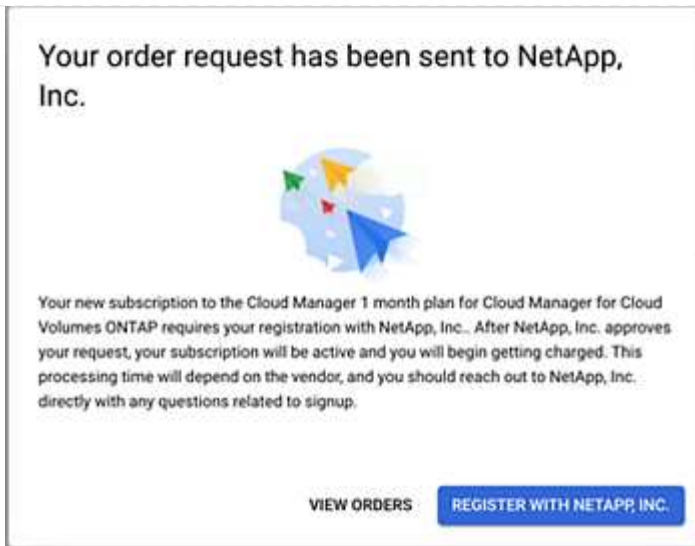
Type: [SaaS & APIs](#)
Last updated: 12/19/22
Category: [Analytics](#), [Developer tools](#), [Storage](#)

- 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 Ihrer Organisation oder 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 -Organisationen oder -Konten aus, denen Sie dieses Abonnement zuordnen möchten.
- Wählen Sie im Feld **bestehendes Abonnement ersetzen** aus, ob Sie das bestehende Abonnement für eine Organisation oder ein Konto automatisch durch dieses neue Abonnement ersetzen möchten.

BlueXP ersetzt mit diesem neuen Abonnement das bestehende Abonnement für alle Anmeldeinformationen im Unternehmen oder Konto. Wenn eine Gruppe von Anmeldeinformationen noch nicht mit einem Abonnement verknüpft wurde, wird dieses neue Abonnement nicht mit diesen Anmeldedaten verknüpft.

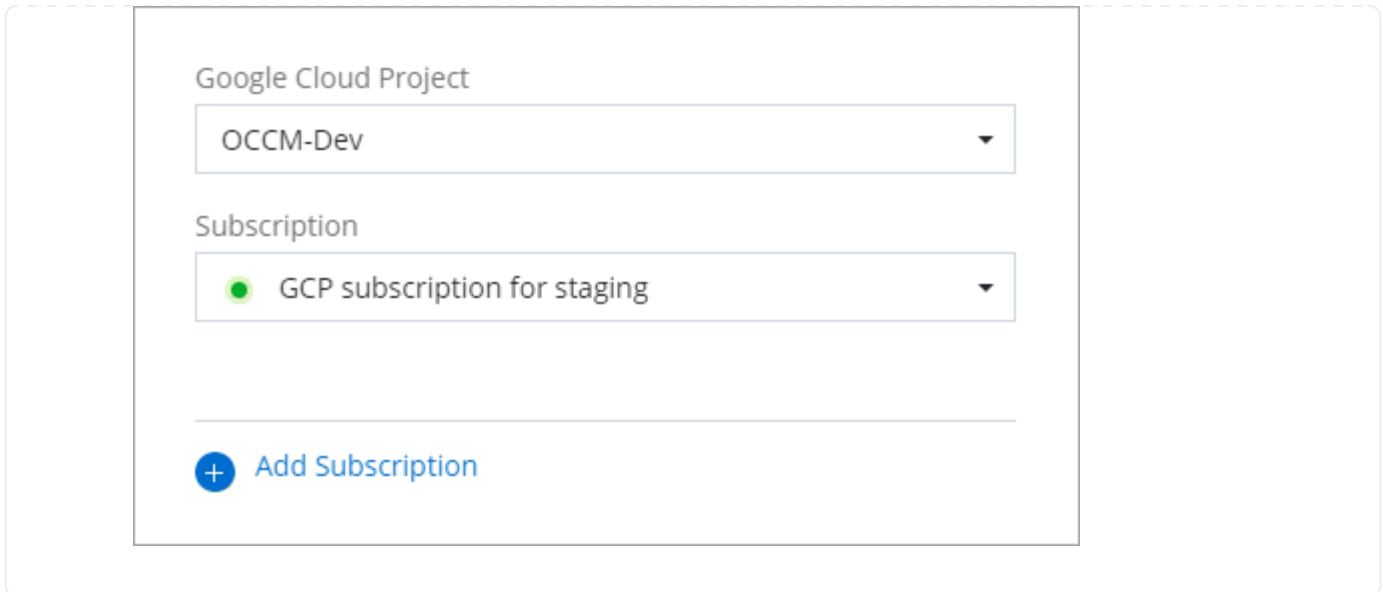
Bei allen anderen Organisationen oder Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie diese Schritte wiederholen.

- 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.



Verwandte Informationen

- ["Managen Sie kapazitätsbasierte BYOL-Lizenzen für Cloud Volumes ONTAP"](#)
- ["Verwalten Sie BYOL-Lizenzen für Datendienste"](#)
- ["Verwalten von AWS-Anmeldeinformationen und Abonnements"](#)
- ["Verwalten von Azure-Anmeldeinformationen und Abonnements"](#)
- ["Verwalten Sie Google Cloud-Anmeldeinformationen und -Abonnements"](#)

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:

- ["Azure NetApp Files Dokumentation"](#)
- ["Dokumentation zu Backup und Recovery"](#)
- ["Dokumente zur Klassifizierung"](#)
- ["Cloud Volumes ONTAP Dokumentation"](#)
- ["Dokumente zur digitalen Brieftasche"](#)
- ["ONTAP-Cluster-Dokumentation vor Ort"](#)
- ["Replizierungsdokumente"](#)

Verwandte Informationen

["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 und haben ["Anschlüsse"](#) ["Bereitstellungsmodi"](#).

1

"Vorbereitungen für die Implementierung"

1. Bereiten Sie einen dedizierten Linux-Host vor, der die Anforderungen für CPU, RAM, Festplattenspeicher, Container-Orchestrierungstool und vieles 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.



Um BlueXP in der ["AWS Secret Cloud"](#) oder die ["Top Secret Cloud von AWS"](#), befolgen Sie die spezifischen Anweisungen für diese Umgebungen. ["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 den privaten Modus verstehen.

Sie müssen beispielsweise die browserbasierte Schnittstelle verwenden, die lokal über den von Ihnen installierten Connector verfügbar ist. Der Zugriff auf BlueXP erfolgt nicht über die webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird.

Darüber hinaus sind nicht alle Funktionen und Dienste 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

Der Host muss bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Portanforderungen usw. erfüllen, um die Connector-Software ausführen zu können.

Dedizierter Host

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

Der Host kann eine beliebige Architektur aufweisen, die die folgenden Größenanforderungen erfüllt:

- CPU: 8 Cores oder 8 vCPUs
- RAM: 32 GB

Anforderungen an das Betriebssystem und den Container

BlueXP unterstützt den Connector mit den folgenden Betriebssystemen, wenn BlueXP im privaten Modus verwendet wird. Vor der Installation des Connectors ist ein Container-Orchestrierungstool erforderlich.

Betriebssystem	Unterstützte OS-Versionen	Unterstützte Connector-Versionen	Benötigter Container-Tool	SELinux
Red Hat Enterprise Linux	9.1 bis 9.4 8.6 bis 8.10	3.9.42 oder höher mit BlueXP im privaten Modus	Podman Version 4.6.1 oder 4.9.4 Zeigen Sie die Konfigurationsanforderungen für Podman an.	Unterstützt im Enforcing-Modus oder im permissiven Modus ¹
Ubuntu	22,04 LTS	3.9.29 oder höher	Docker Engine 23.0.6 bis 26.0.0 26.0.0 wird mit <i>New Connector</i> 3.9.44 oder neueren Installationen unterstützt	Nicht unterstützt

Hinweise:

1. Die Verwaltung von Cloud Volumes ONTAP-Systemen wird von Connectors, auf denen SELinux auf dem Betriebssystem aktiviert ist, nicht unterstützt.

2. Der Connector wird auf Englisch-sprachigen Versionen dieser Betriebssysteme unterstützt.
3. Für RHEL muss der Host bei Red hat Subscription Management registriert sein. Wenn er nicht registriert ist, kann der Host während der Connector-Installation nicht auf Repositories zugreifen, um erforderliche Drittanbietersoftware zu aktualisieren.

Hypervisor

Ein Bare-Metal- oder gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

CPU

8 Kerne oder 8 vCPUs

RAM

32GB

Instanztyp für AWS EC2

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen t3.2xlarge.

Azure VM-Größe

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen Standard_D8s_v3.

Google Cloud-Maschinentyp

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n2-Standard-8.

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

BlueXP verwendet /opt, um das Verzeichnis und seinen Inhalt zu installieren
/opt/application/netapp.

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

BlueXP erfordert diesen Platz /var Da Docker oder Podman so konzipiert sind, dass die Container in diesem Verzeichnis erstellt werden. Insbesondere werden Container in der erstellt /var/lib/containers/storage Verzeichnis. Externe Mounts oder Symlinks funktionieren nicht für diesen Raum.

Schritt 4: Installieren Sie Podman oder Docker Engine

Sie müssen den Host für den Connector vorbereiten, indem Sie Podman oder die Docker Engine installieren.

Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

- Podman ist für Red hat Enterprise Linux 8 und 9 erforderlich.

Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.

- Docker Engine ist für Ubuntu erforderlich.

Zeigen Sie die von BlueXP unterstützten Versionen der Docker Engine an.

Beispiel 6. Schritte

Podman

Führen Sie die folgenden Schritte aus, um Podman zu installieren und zu konfigurieren, um die folgenden Anforderungen zu erfüllen:

- Aktivieren und starten Sie den Dienst podman.socket
- python3 einbauen
- Installieren Sie das Podman-Compose-Paket Version 1.0.6
- Fügen Sie podman-compose zur Umgebungsvariablen PATH hinzu



Passen Sie bei Verwendung von Podman den aardvark-dns-Dienstport (Standard: 53) nach der Installation des Connectors an, um Konflikte mit dem DNS-Port auf dem Host zu vermeiden. Folgen Sie den Anweisungen zur Portkonfiguration.

Schritte

1. Entfernen Sie das Paket podman-Docker, wenn es auf dem Host installiert ist.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installieren Sie Podman.

Podman ist über die offiziellen Red hat Enterprise Linux-Repositorys erhältlich.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Wobei <version> die unterstützte Version von Podman ist, die Sie installieren. [Zeigen Sie die Podman-Versionen an, die von BlueXP unterstützt werden.](#)

3. Aktivieren und starten Sie den podman.Socket-Dienst.

```
sudo systemctl enable --now podman.socket
```

4. Installieren Sie Python3.

```
sudo dnf install python3
```

5. Installieren Sie das EPEL Repository-Paket, wenn es nicht bereits auf Ihrem System verfügbar ist.

Dieser Schritt ist erforderlich, da podman-compose im Repository Extra Packages for Enterprise Linux (EPEL) verfügbar ist.

Für Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

Für Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Installieren Sie das Paket „podman-compose“ 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Verwenden der `dnf install` Befehl erfüllt die Anforderung zum Hinzufügen von podman-compose zur Umgebungsvariable PATH. Der Installationsbefehl fügt podman-compose zu `/usr/bin` hinzu, das bereits im enthalten ist `secure_path` Option auf dem Host.

Docker Engine

Folgen Sie der Dokumentation von Docker, um die Docker Engine zu installieren.

Schritte

1. ["Installationsanweisungen von Docker anzeigen"](#)

Befolgen Sie die Schritte, um eine bestimmte Version der Docker Engine zu installieren. Durch die Installation der neuesten Version wird eine Docker Version installiert, die BlueXP nicht unterstützt.

2. Docker muss aktiviert und ausgeführt werden.

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

Schritt 5: Vorbereitung der Vernetzung

Richten Sie das Netzwerk für den Connector ein, um Ressourcen in Ihrer öffentlichen Cloud zu verwalten.

Stellen Sie neben einem virtuellen Netzwerk und einem Subnetz für den Connector sicher, dass die folgenden Anforderungen erfüllt sind. Verbindungen zu Zielnetzwerken: Der Connector benötigt eine Netzwerkverbindung zum Standort, an dem Sie den 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.

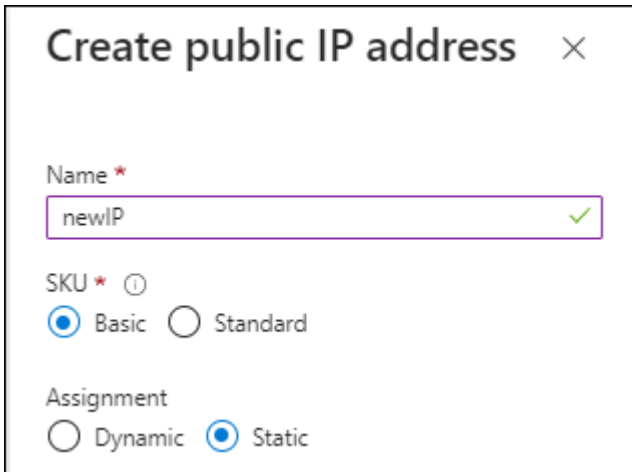
Endpunkte für den täglichen Betrieb

Wenn Sie planen, Cloud Volumes ONTAP-Systeme zu erstellen, benötigt der Connector Verbindungen zu Endpunkten in den öffentlich verfügbaren Ressourcen Ihres Cloud-Providers.

Endpunkte	Zweck
<p>AWS-Services (amazonaws.com):</p> <ul style="list-style-type: none"> • 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) 	<p>Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"</p>
<p>https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net</p>	<p>Für das Managen von Ressourcen in Azure Public Regionen.</p>
<p>https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud</p>	<p>Zum Managen von Ressourcen in der Region Azure-IL6.</p>
<p>https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn</p>	<p>Für das Management von Ressourcen in Azure China Regionen.</p>
<p>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</p>	<p>Zum Managen von Ressourcen in Google Cloud.</p>

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.



The screenshot shows a dialog box titled "Create public IP address" with a close button (X) in the top right corner. Below the title, there are three sections:

- Name ***: A text input field containing "newIP" with a green checkmark on the right.
- SKU ***: Two radio buttons, "Basic" (selected) and "Standard".
- Assignment**: Two radio buttons, "Dynamic" and "Static" (selected).

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

NetApp unterstützt sowohl explizite als auch transparente Proxy-Konfigurationen. Bei Verwendung eines transparenten Proxys müssen Sie lediglich das Zertifikat für den Proxyserver angeben. Bei Verwendung eines expliziten Proxys benötigen Sie zusätzlich die IP-Adresse und die Anmeldeinformationen.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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 6: Cloud-Berechtigungen vorbereiten

Wenn der Connector in der Cloud installiert ist und Sie Cloud Volumes ONTAP-Systeme erstellen möchten, benötigt BlueXP die Berechtigungen des Cloud-Anbieters. 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. Geben Sie BlueXP den AWS-Zugriffsschlüssel, nachdem Sie den Connector installiert und BlueXP eingerichtet haben.

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. Weisen Sie diese Rolle der Connector-VM zu.

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.

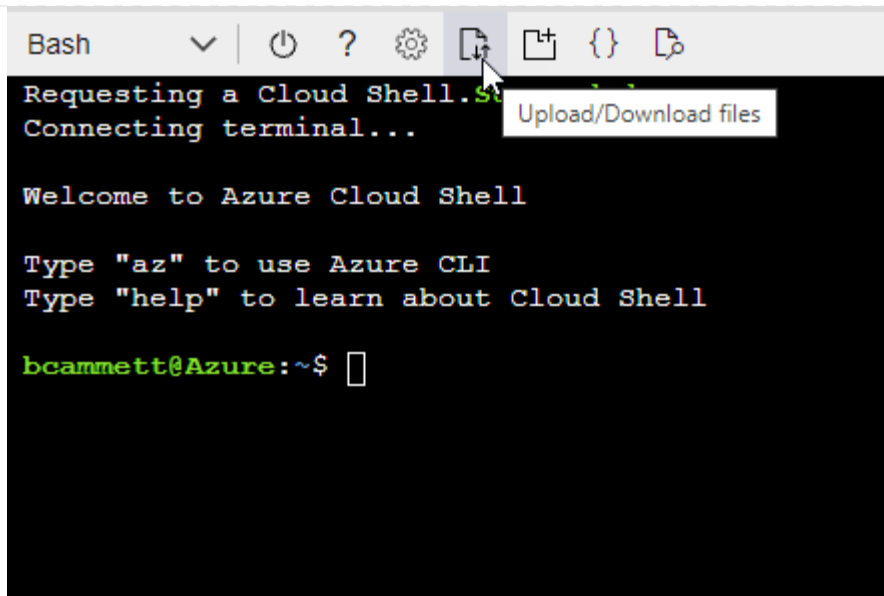
Beispiel

```
"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

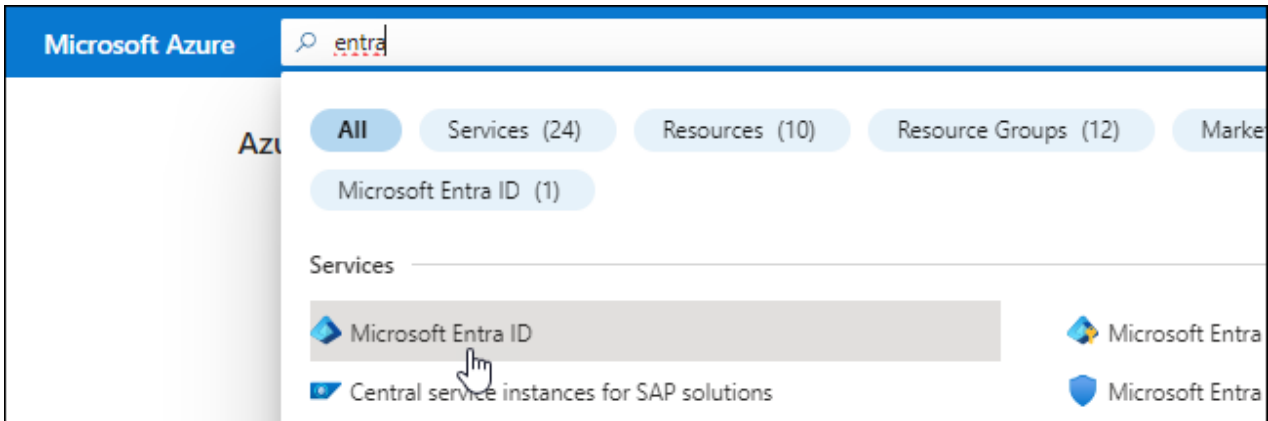
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

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.

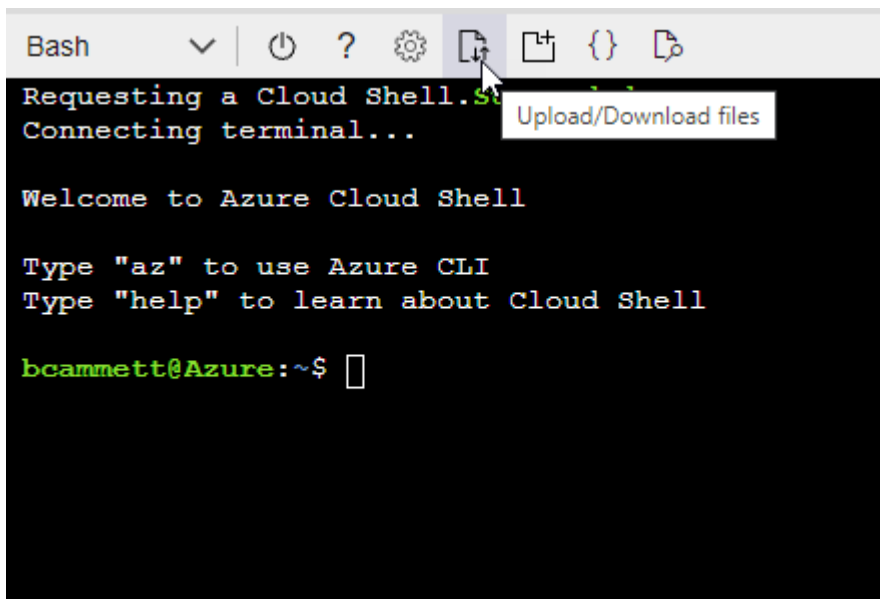
Beispiel

```
"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.



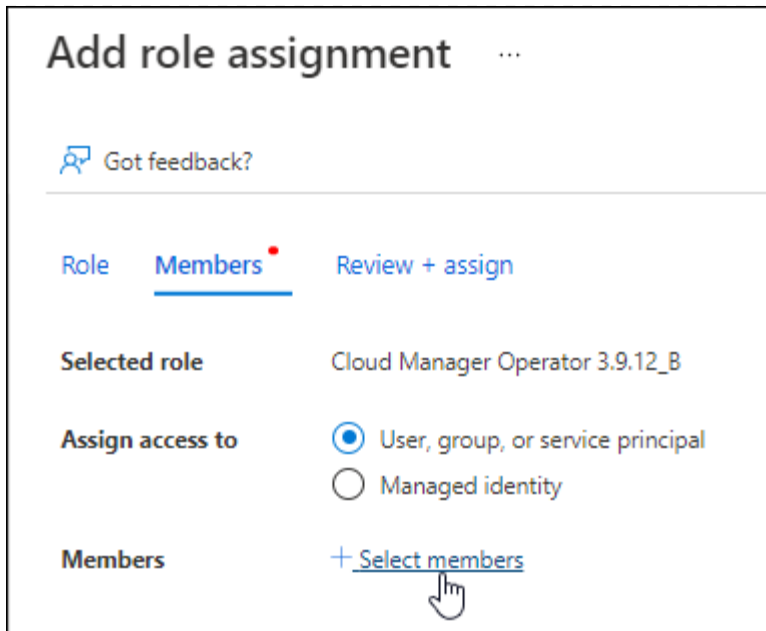
- Verwenden Sie die Azure CLI, um die benutzerdefinierte Rolle zu erstellen:

```
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.

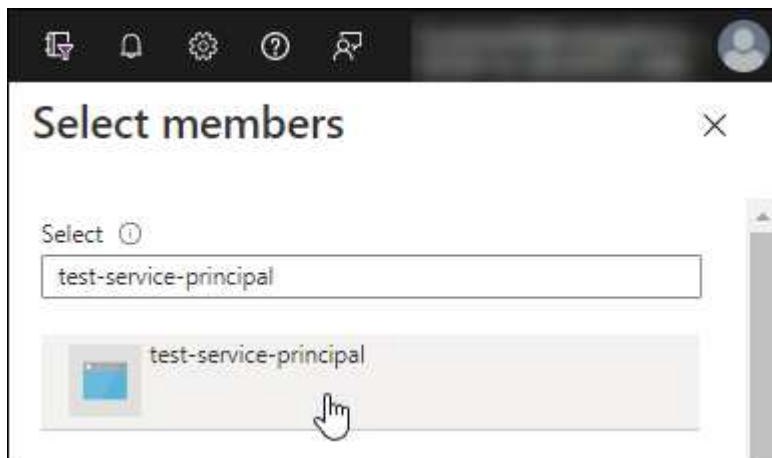
2. Applikation der Rolle zuweisen:

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



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



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

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

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

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Principal 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.


Request API permissions













Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview)

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**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA	

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. Geben Sie diese Informationen in BlueXP ein, 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 7: Google Cloud APIs aktivieren

Sie müssen mehrere APIs aktivieren, um Cloud Volumes ONTAP in Google Cloud bereitzustellen.

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

Stellen Sie den Connector im privaten Modus bereit, sodass Sie BlueXP ohne ausgehende Verbindung zur SaaS-Ebene (Software as a Service) von BlueXP verwenden 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.
- Je nach Betriebssystem ist entweder Podman oder Docker Engine erforderlich, bevor Sie den Connector installieren.

Schritte

1. Laden Sie die Connector-Software von der herunter "[NetApp Support Website](#)"

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

2. Kopieren Sie das Installationsprogramm auf den Linux-Host.

3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

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

4. Führen Sie das Installationskript 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.

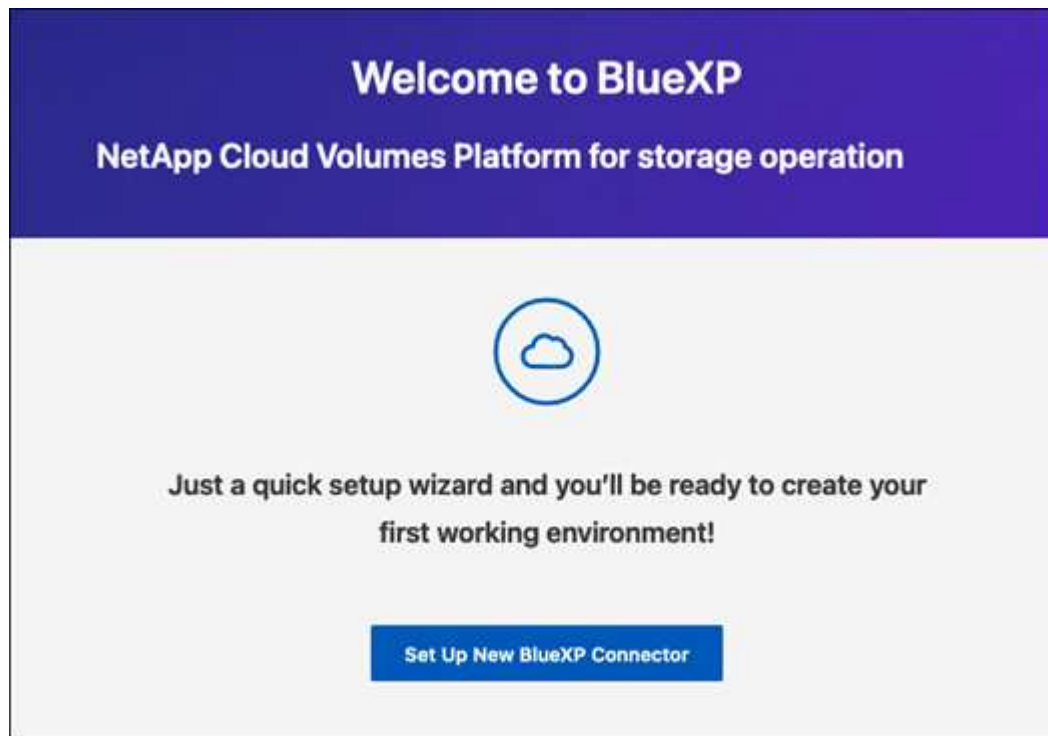
Schritt 2: BlueXP einrichten

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

Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie ein

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.

1 System Details 2 Create Admin User 3 Review

System Details

To help us provide better support, enter a name for BlueXP Connector and your company name.

BlueXP Connector Name
aug27-dark-site-karana

Company Name
netapp

- **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:

- ["Erkennen von ONTAP Clustern vor Ort"](#)
- ["Verwalten von Softwareupdates"](#)
- ["Scannen Sie lokale ONTAP-Volumedaten mithilfe der BlueXP-Klassifizierung"](#)
- ["Überwachen Sie die Lizenznutzung mit Digital Wallet"](#)
- ["Mit dem digitalen Berater Informationen zum Storage-Zustand anzeigen"](#)

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.