Beginnen Sie mit dem eingeschränkten Modus

Setup and administration

NetApp
April 26, 2024

Inhalt

Beginnen Sie mit dem eingeschränkten Modus

Erste Schritte im Workflow (eingeschränkter Modus)

Der Einstieg in BlueXP ist eingeschränkt, indem Sie Ihre Umgebung vorbereiten, Connector implementieren und BlueXP abonnieren.

Der eingeschränkte Modus wird in der Regel von staatlichen und lokalen Behörden sowie von Unternehmen genutzt, die Auflagen unterliegen, einschließlich Implementierungen in AWS GovCloud und Azure Government Regionen. Bevor Sie beginnen, sollten Sie ein Verständnis von haben "BlueXP Accounts", "Anschlüsse", und "Bereitstellungsmodi".

1 **"Vorbereitungen für die Implementierung"**

1. Bereiten Sie einen dedizierten Linux-Host vor, der die Anforderungen für CPU, RAM, Festplattenspeicher, Docker Engine und mehr erfüllt.
2. Richten Sie ein Netzwerk ein, das den Zugriff auf die Zielnetzwerke, den ausgehenden Internetzugang für manuelle Installationen und das ausgehende Internet für den täglichen Zugriff bietet.
3. Richten Sie Berechtigungen in Ihrem Cloud-Provider ein, damit Sie diese Berechtigungen nach der Bereitstellung mit der Connector-Instanz verknüpfen können.

2 **"Implementieren Sie den Connector"**

1. Installieren Sie den Connector auf dem Marktplatz Ihres Cloud-Anbieters oder installieren Sie die Software manuell auf Ihrem eigenen Linux-Host.
2. Richten Sie BlueXP ein, indem Sie einen Webbrowser öffnen und die IP-Adresse des Linux-Hosts eingeben.
3. Bereitstellen von BlueXP mit den Berechtigungen, die Sie bereits eingerichtet haben.

3 **"Abonnieren Sie BlueXP"**

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

Bereiten Sie die Bereitstellung im eingeschränkten Modus vor

Bereiten Sie Ihre Umgebung vor der Implementierung von BlueXP im eingeschränkten Modus vor. Sie müssen beispielsweise die Hostanforderungen prüfen, das Netzwerk vorbereiten, Berechtigungen einrichten und vieles mehr.

Schritt 1: Verstehen, wie eingeschränkter Modus funktioniert

Bevor Sie beginnen, sollten Sie wissen, wie BlueXP im eingeschränkten Modus funktioniert.

Sie sollten beispielsweise verstehen, dass Sie die browserbasierte Oberfläche verwenden müssen, die lokal

über den BlueXP Connector verfügbar ist, die Sie installieren müssen. Der Zugriff auf BlueXP erfolgt nicht über die webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird.

Außerdem sind nicht alle BlueXP Services verfügbar.

"Erfahren Sie, wie eingeschränkter Modus funktioniert".

Schritt 2: Überprüfen Sie die Installationsoptionen

Im eingeschränkten Modus können Sie den Connector nur in der Cloud installieren. Folgende Installationsoptionen sind verfügbar:

- Über AWS Marketplace
- Über den Azure Marketplace
- Manuelles Installieren des Connectors auf Ihrem eigenen Linux-Host, der in AWS, Azure oder Google Cloud ausgeführt wird

Schritt 3: Überprüfen Sie die Host-Anforderungen

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

Wenn Sie den Connector über AWS oder Azure Marketplace implementieren, enthält das Image die erforderlichen Betriebssystem- und Softwarekomponenten. Sie müssen lediglich einen Instanztyp auswählen, der die CPU- und RAM-Anforderungen erfüllt.

Dedizierter Host

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

Unterstützte Betriebssysteme

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

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

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

Hypervisor

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

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

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Azure VM-Größe

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

Google Cloud-Maschinentyp

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

Der Connector wird in Google Cloud auf einer VM-Instanz mit einem unterstützten Betriebssystem unterstützt "Geschirmte VM-Funktionen"

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

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

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

"Installationsanweisungen anzeigen"

Schritt 4: Vorbereitung der Vernetzung

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung managen kann. Abgesehen von einem virtuellen Netzwerk und einem Subnetz für den Connector müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind.

Verbindungen zu Zielnetzwerken

Der Connector muss über eine Netzwerkverbindung zu dem Speicherort verfügen, an dem Sie Speicher verwalten möchten. Beispielsweise die VPC oder vnet, bei der Sie Cloud Volumes ONTAP implementieren möchten, oder das Datacenter, in dem sich Ihre ONTAP-Cluster vor Ort befinden.

Networking für Benutzerzugriff auf die BlueXP Konsole vorbereiten

Im eingeschränkten Modus ist der Zugriff auf die BlueXP Benutzeroberfläche über den Connector möglich. Bei der Nutzung der BlueXP Benutzeroberfläche wendet sich das IT-Programm an einige Endpunkte, um Datenmanagementaufgaben durchzuführen. Diese Endpunkte werden von dem Computer eines Benutzers kontaktiert, wenn bestimmte Aktionen über die BlueXP Konsole durchgeführt werden.

Endpunkte	Zweck
https://signin.b2c.netapp.com	Erforderlich, um die Zugangsdaten für die NetApp Support Site (NSS) zu aktualisieren oder neue NSS-Zugangsdaten für BlueXP hinzuzufügen

Endpunkte	Zweck
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung über BlueXP zu ermöglicht.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Endpunkte wurden während der manuellen Installation kontaktiert

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

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

  Dieser Endpunkt ist in Regionen der Azure-Regierung nicht erforderlich.

- https://occmclientinfragov.azurecr.us

  Dieser Endpunkt ist nur in Regionen der Azure-Regierung erforderlich.

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

Outbound-Internetzugang für den täglichen Betrieb

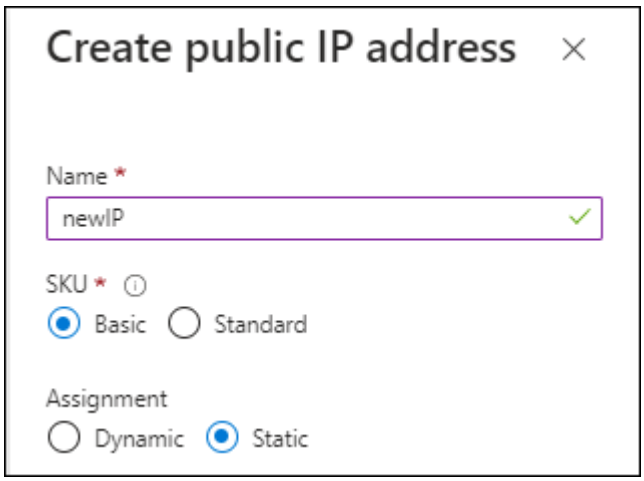
Der Netzwerkspeicherort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen. Für den Konnektor ist ein abgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu verwalten.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Managen von Ressourcen in Azure Government Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.

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

Öffentliche IP-Adresse in Azure

Wenn Sie eine öffentliche IP-Adresse mit der Connector-VM in Azure verwenden möchten, muss die IP-Adresse eine Basis-SKU verwenden, um sicherzustellen, dass BlueXP diese öffentliche IP-Adresse verwendet.



Wenn Sie stattdessen eine Standard-SKU-IP-Adresse verwenden, verwendet BlueXP anstelle der öffentlichen IP die *private* IP-Adresse des Connectors. Wenn die Maschine, die Sie für den Zugriff auf die BlueXP-Konsole nutzen, keinen Zugriff auf diese private IP-Adresse hat, dann schlagen Aktionen aus der BlueXP-Konsole fehl.

"Azure-Dokumentation: Öffentliche IP-SKU"

Proxy-Server

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

Diese Informationen müssen Sie bei der Installation angeben.

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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

Ports

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

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

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

Aktivieren Sie NTP

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

Wenn Sie den Connector aus dem Marktplatz Ihres Cloud-Anbieters erstellen möchten, müssen Sie diese Netzwerkanforderung implementieren, nachdem Sie den Connector erstellt haben.

Schritt: 5 Cloud-Berechtigungen vorbereiten

BlueXP erfordert Berechtigungen Ihres Cloud-Providers zur Implementierung von Cloud Volumes ONTAP in einem virtuellen Netzwerk und zur Nutzung von BlueXP Datenservices. Sie müssen Berechtigungen in Ihrem Cloud-Provider einrichten und diese dann dem Connector zuordnen.

Um die erforderlichen Schritte anzuzeigen, wählen Sie die Authentifizierungsoption aus, die Sie für Ihren Cloud-Provider verwenden möchten.

AWS IAM-Rolle

Verwenden Sie eine IAM-Rolle, um dem Connector Berechtigungen zu gewähren.

Wenn Sie den Connector über AWS Marketplace erstellen, werden Sie beim Start der EC2-Instanz aufgefordert, diese IAM-Rolle auszuwählen.

Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren, müssen Sie die Rolle an die EC2-Instanz anhängen.

Schritte

1. Melden Sie sich bei der AWS-Konsole an, und navigieren Sie zum IAM-Service.
2. Erstellen einer Richtlinie:
   a. Wählen Sie **Policies > Create Policy** aus.
   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".
   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.
3. Erstellen einer IAM-Rolle:
   a. Wählen Sie **Rollen > Rolle erstellen**.
   b. Wählen Sie **AWS-Service > EC2** aus.
   c. Fügen Sie Berechtigungen hinzu, indem Sie die soeben erstellte Richtlinie anhängen.
   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

Ergebnis

Sie haben jetzt eine IAM-Rolle für die EC2-Instanz des Connectors.

AWS-Zugriffsschlüssel

Richten Sie Berechtigungen und einen Zugriffsschlüssel für einen IAM-Benutzer ein. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP mit dem AWS-Zugriffsschlüssel bereitstellen.

Schritte

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

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

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

   Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich. "Erfahren Sie mehr über IAM-Richtlinien für den Connector".

3. Fügen Sie die Richtlinien einem IAM-Benutzer hinzu.
   - "AWS Documentation: Erstellung von IAM-Rollen"

- "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie nach der Installation des Connectors zu BlueXP hinzufügen können.

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen.

Azure Rolle

Erstellen einer benutzerdefinierten Azure-Rolle mit den erforderlichen Berechtigungen. Sie werden diese Rolle der Connector-VM zuweisen.

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

Schritte

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

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

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

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

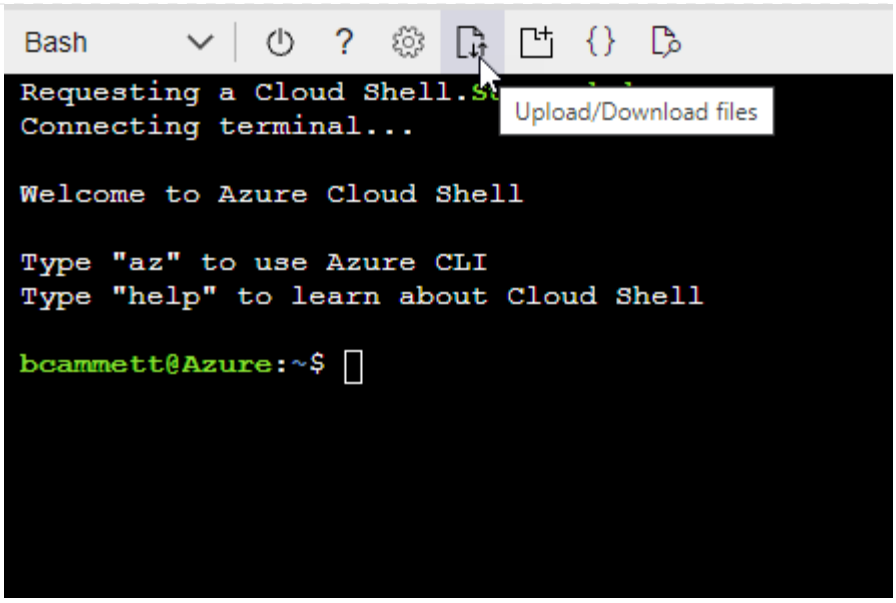
   Beispiel

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

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

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

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



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

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

Ergebnis

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

Azure Service Principal

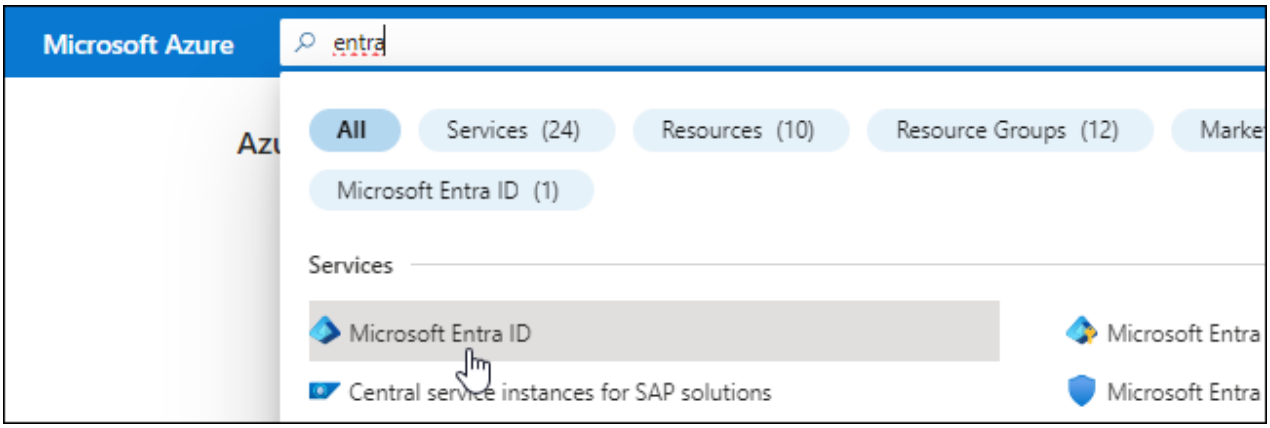
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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

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

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



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

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

Anwendung einer Rolle zuweisen

1. Erstellen einer benutzerdefinierten Rolle:

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

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

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

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

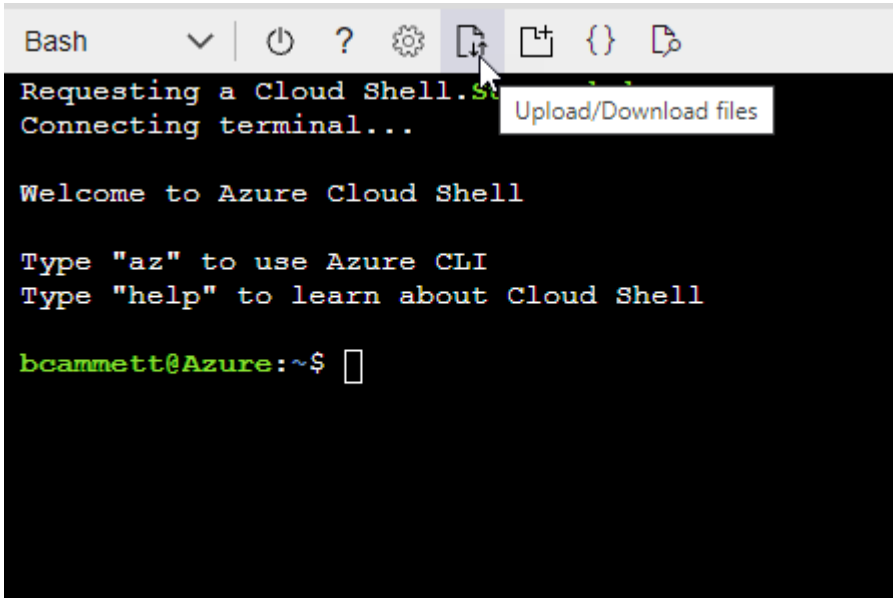
      Beispiel

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

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

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

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



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

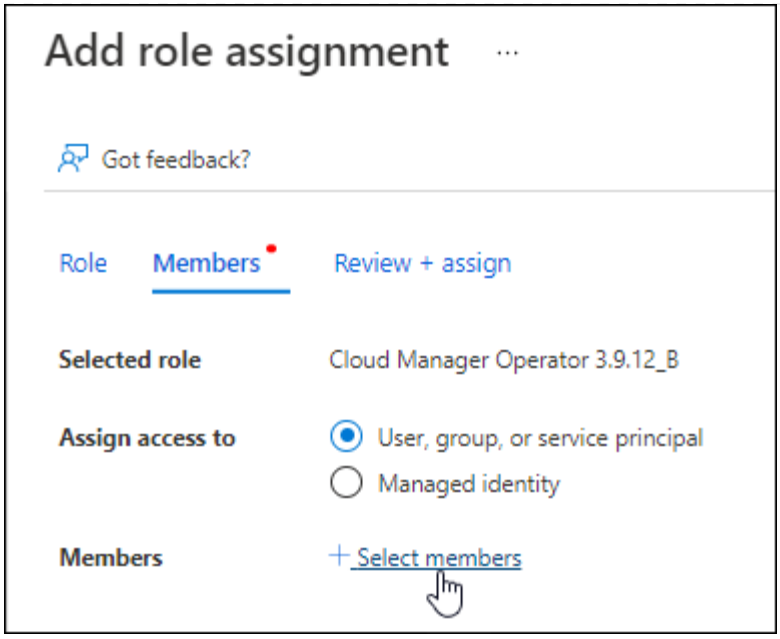
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

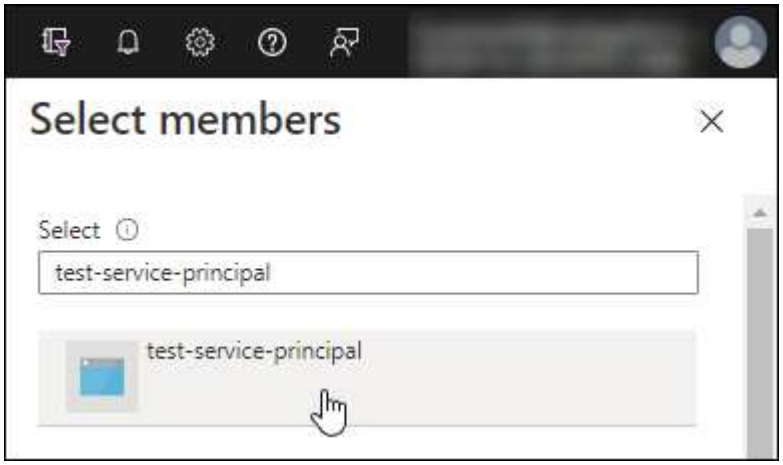
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

      - **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.
      - Wählen Sie **Mitglieder auswählen**.



- Suchen Sie nach dem Namen der Anwendung.

  Hier ein Beispiel:



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

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

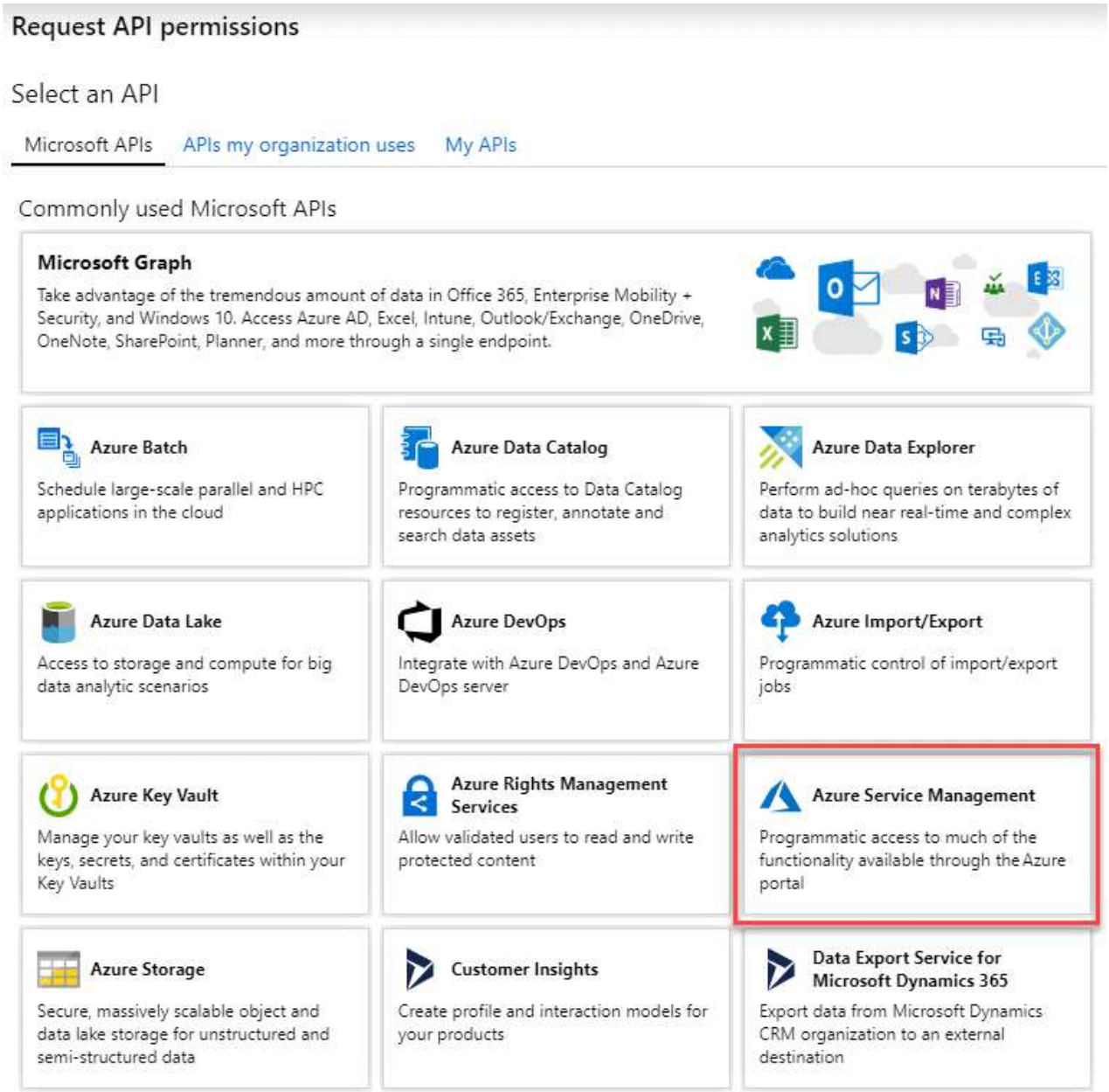
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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

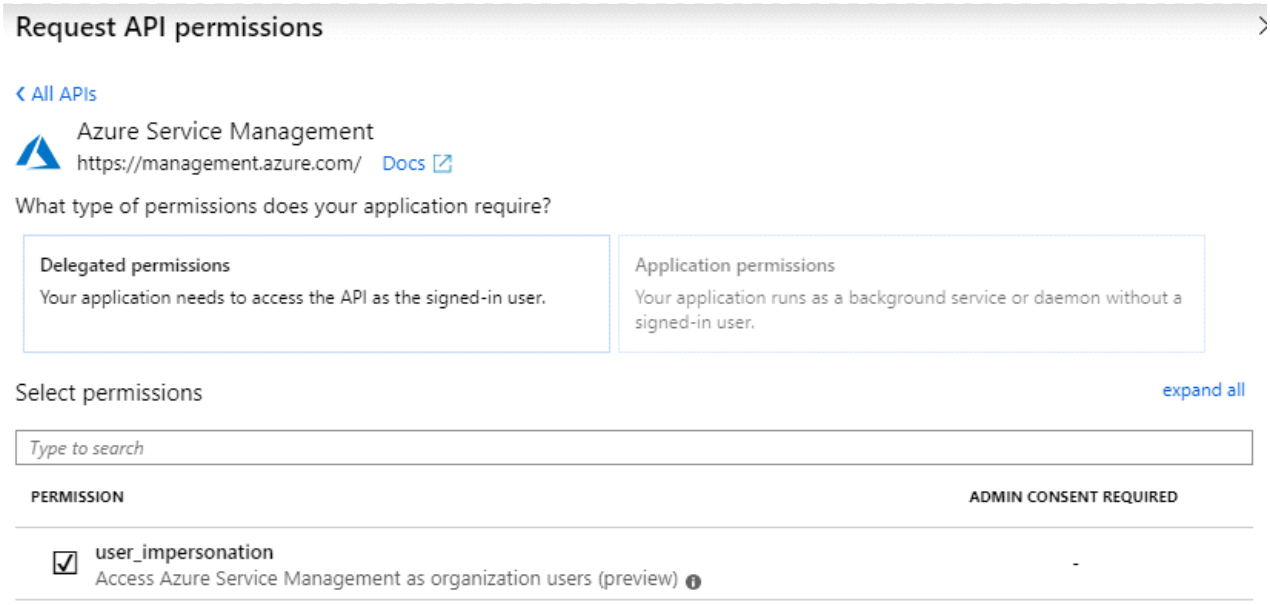
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

1. Wählen Sie im **Microsoft Entra ID**-Dienst **App-Registrierungen** aus und wählen Sie die Anwendung aus.

2. Wählen Sie **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.

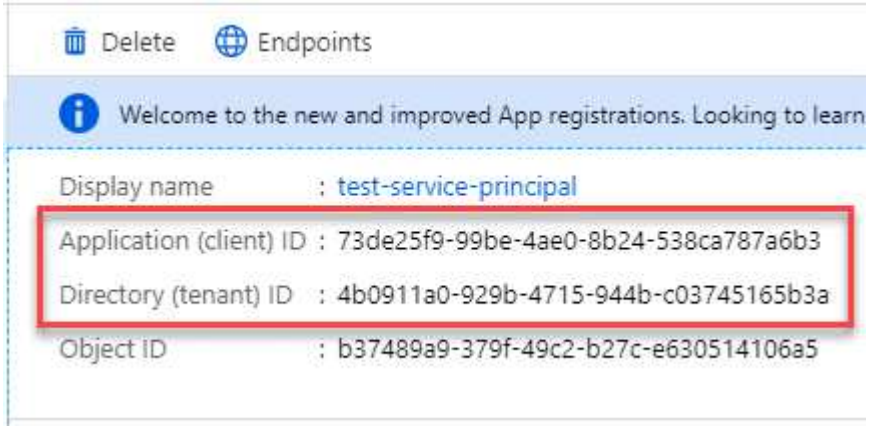


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen Sie einen Clientschlüssel

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

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

Ergebnis

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

Google Cloud Service-Konto

Erstellen Sie eine Rolle und wenden Sie sie auf ein Servicekonto an, das Sie für die VM-Instanz des Connectors verwenden werden.

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

   a. Erstellen Sie eine YAML-Datei, die die in definierten Berechtigungen enthält "Connector-Richtlinie für Google Cloud".

   b. Aktivieren Sie in Google Cloud die Cloud Shell.

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

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

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

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

   +
   "Google Cloud docs: Erstellen und Verwalten benutzerdefinierter Rollen"

2. Erstellen Sie ein Servicekonto in Google Cloud:

   a. Wählen Sie im IAM & Admin-Dienst **Service-Konten > Service-Konto erstellen** aus.

   b. Geben Sie die Details des Servicekontos ein und wählen Sie **Erstellen und Fortfahren**.

   c. Wählen Sie die gerade erstellte Rolle aus.

   d. Beenden Sie die verbleibenden Schritte, um die Rolle zu erstellen.

      "Google Cloud docs: Erstellen eines Dienstkontos"

Ergebnis

Sie verfügen jetzt über ein Servicekonto, das Sie der VM-Instanz des Connectors zuweisen können.

Schritt 6: Google Cloud APIs aktivieren

Für die Implementierung von Cloud Volumes ONTAP in Google Cloud sind mehrere APIs erforderlich.

Schritt

1. "Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt"
    - Cloud Deployment Manager V2-API
    - Cloud-ProtokollierungsAPI
    - Cloud Resource Manager API
    - Compute Engine-API
    - IAM-API (Identitäts- und Zugriffsmanagement
    - KMS-API (Cloud Key Management Service)

      (Nur erforderlich, wenn Sie BlueXP Backup und Recovery mit vom Kunden gemanagten Verschlüsselungsschlüsseln (CMEK) verwenden möchten).

Stellen Sie den Connector im eingeschränkten Modus bereit

Implementieren Sie den Connector im eingeschränkten Modus, sodass Sie BlueXP mit eingeschränkter Outbound-Konnektivität zur BlueXP SaaS-Ebene nutzen können. Installieren Sie den Connector, richten Sie BlueXP über die Benutzeroberfläche ein, die auf dem Connector ausgeführt wird, und stellen Sie dann die zuvor festgelegten Cloud-Berechtigungen bereit.

Schritt 1: Installieren Sie den Stecker

Installieren Sie den Connector auf dem Marktplatz Ihres Cloud-Anbieters oder installieren Sie die Software manuell auf Ihrem eigenen Linux-Host.

AWS Commercial Marketplace

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt

  "Hier erhalten Sie Informationen zu den Netzwerkanforderungen"

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

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

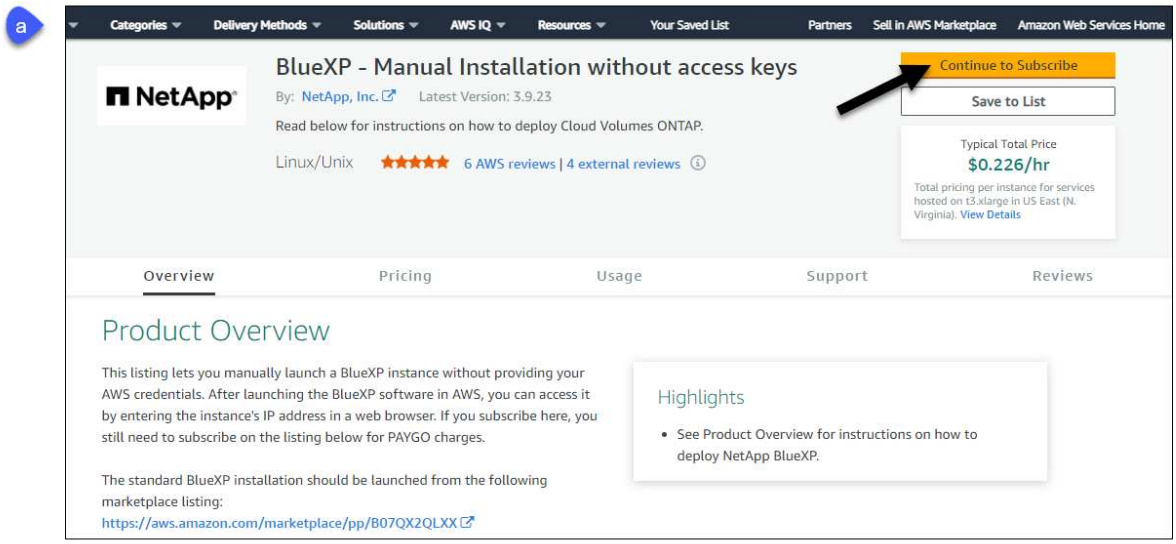
- Berechtigung zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Verständnis der CPU- und RAM-Anforderungen für die Instanz.

  "Prüfen Sie die Instanzanforderungen".

- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

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



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

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

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

Connector-Instanz SSH, HTTP und HTTPS aktivieren.

Für spezifische Konfigurationen sind noch einige Regeln erforderlich.

"Sicherheitsgruppen-Regeln für AWS ansehen".

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

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

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

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

AWS Gov Marketplace

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt

  "Hier erhalten Sie Informationen zu den Netzwerkanforderungen"

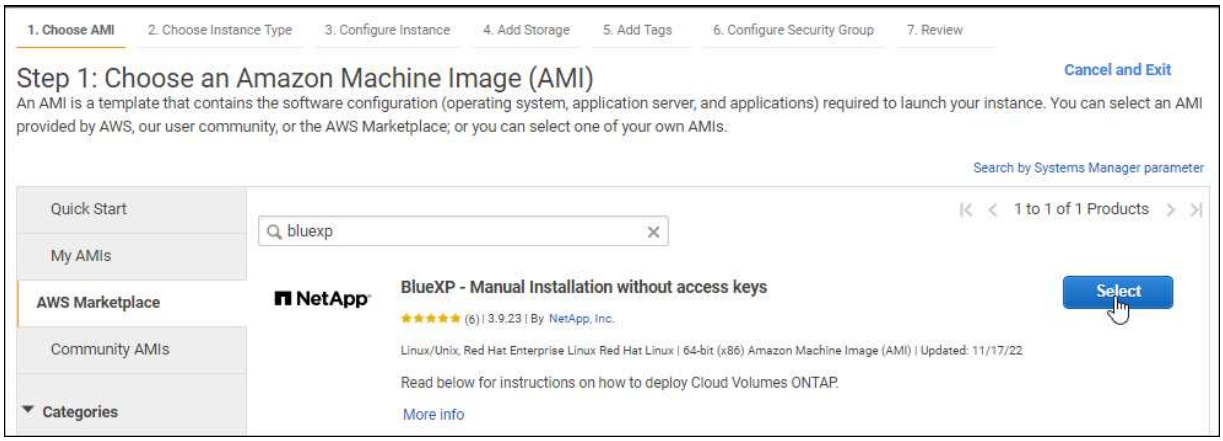
- Eine IAM-Rolle mit angehängter Richtlinie, die die erforderlichen Berechtigungen für den Connector enthält.

  "Erfahren Sie, wie Sie AWS-Berechtigungen einrichten"

- Berechtigung zum Abonnieren und Abbestellen des AWS Marketplace für Ihren IAM-Benutzer.
- Ein Schlüsselpaar für die EC2-Instanz.

Schritte

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

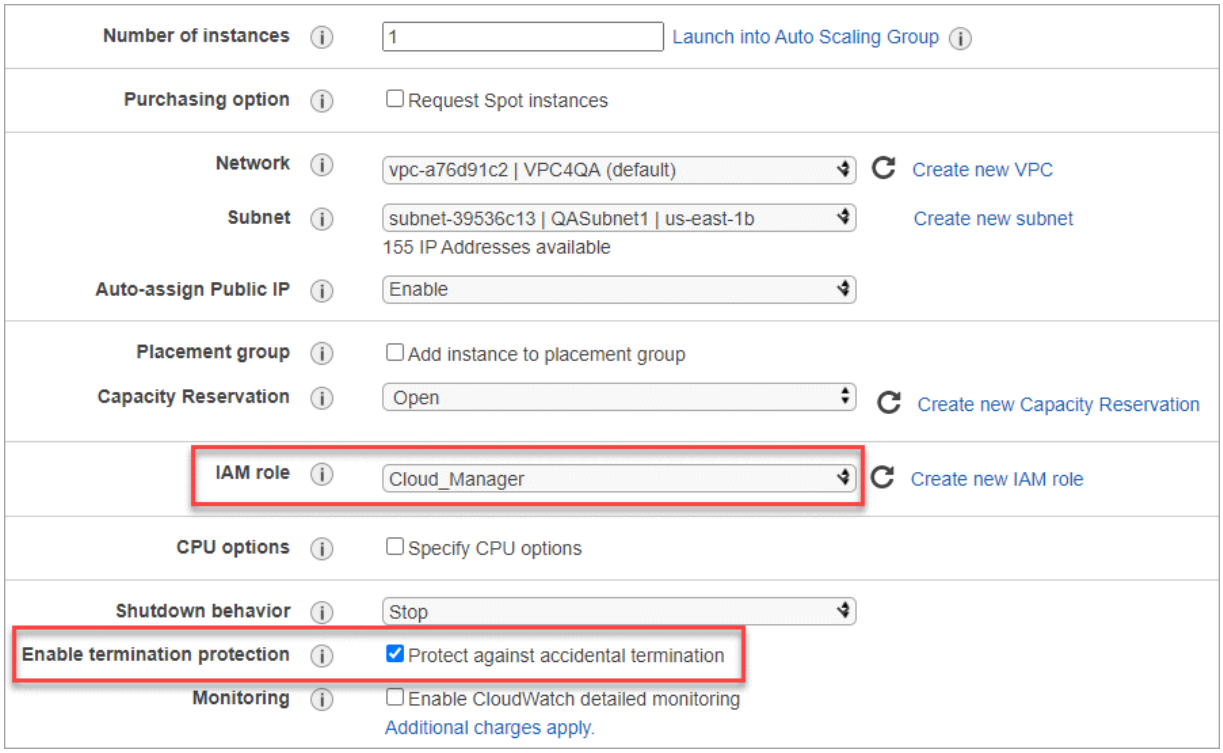


d. Wählen Sie **Weiter**.

2. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:
   - **Wählen Sie einen Instanztyp**: Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.xlarge wird empfohlen).

     "Prüfen Sie die Anforderungen an die Instanz".

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



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

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

Azure Marketplace

Bevor Sie beginnen

Sie sollten Folgendes haben:

- V-net und Subnetz, die die Netzwerkanforderungen erfüllen

  "Hier erhalten Sie Informationen zu den Netzwerkanforderungen"

- Eine benutzerdefinierte Azure-Rolle, die die erforderlichen Berechtigungen für den Connector enthält.

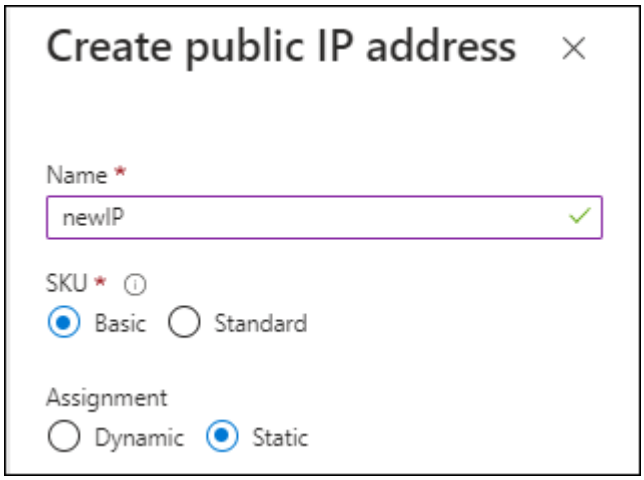
  "Erfahren Sie, wie Sie Azure-Berechtigungen einrichten"

Schritte

1. Wechseln Sie im Azure Marketplace auf die Seite NetApp Connector VM.
   - "Azure Marketplace-Seite für kommerzielle Regionen"
   - "Azure Marketplace-Seite für Azure Government Regions"
2. Wählen Sie **Jetzt holen** und wählen Sie dann **Weiter**.
3. Wählen Sie im Azure-Portal **Create** aus und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

   Beachten Sie beim Konfigurieren der VM Folgendes:

   - **VM-Größe**: Wählen Sie eine VM-Größe, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen DS3 v2.
   - **Disks**: Der Connector kann mit HDD- oder SSD-Festplatten optimal funktionieren.
   - **Öffentliche IP**: Wenn Sie eine öffentliche IP-Adresse mit der Connector VM verwenden möchten, muss die IP-Adresse eine Basis-SKU verwenden, um sicherzustellen, dass BlueXP diese öffentliche IP-Adresse verwendet.



Wenn Sie stattdessen eine Standard-SKU-IP-Adresse verwenden, verwendet BlueXP anstelle der öffentlichen IP die *private* IP-Adresse des Connectors. Wenn die Maschine, die Sie für den Zugriff auf die BlueXP-Konsole nutzen, keinen Zugriff auf diese private IP-Adresse hat, dann schlagen Aktionen aus der BlueXP-Konsole fehl.

"Azure-Dokumentation: Öffentliche IP-SKU"

- **Netzwerksicherheitsgruppe**: Der Connector benötigt eingehende Verbindungen über SSH, HTTP und HTTPS.

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

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

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

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

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

Manuelle Installation

Bevor Sie beginnen

Sie sollten Folgendes haben:

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

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

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

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

Über diese Aufgabe

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

Schritte

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

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

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

```
unset http_proxy
unset https_proxy
```

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

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

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

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

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

5. Führen Sie das Installationsskript aus.

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

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

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

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

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

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

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

  Beachten Sie Folgendes:

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

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

Ergebnis

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

Was kommt als Nächstes?

BlueXP einrichten:

Schritt 2: BlueXP einrichten

Wenn Sie zum ersten Mal auf die BlueXP Konsole zugreifen, werden Sie aufgefordert, ein Konto auszuwählen, mit dem der Connector verknüpft werden soll, und den eingeschränkten Modus zu aktivieren.

> Wenn Sie bereits ein Konto haben und ein weiteres erstellen möchten, müssen Sie die Mandanten-API verwenden. "Erstellen Sie ein zusätzliches BlueXP Konto".

Schritte

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

   https://ipaddress

2. Melden Sie sich bei BlueXP an oder melden Sie sich an.
3. Nachdem Sie angemeldet sind, richten Sie BlueXP ein:

   a. Geben Sie einen Namen für den Connector ein.

   b. Geben Sie einen Namen für ein neues BlueXP Konto ein, oder wählen Sie ein bestehendes Konto aus.

      Sie können ein bestehendes Konto auswählen, wenn Ihr Login bereits einem BlueXP Konto zugeordnet ist.

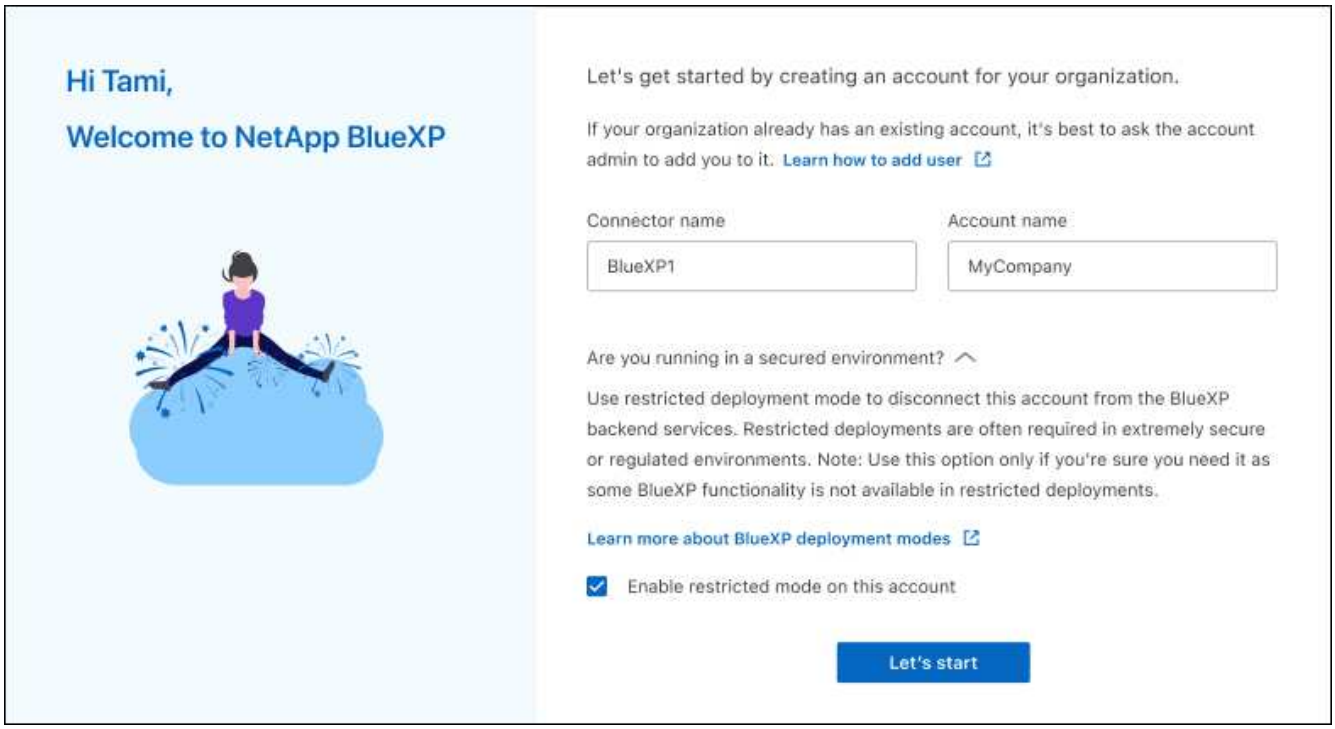
   c. Wählen Sie **laufen Sie in einer sicheren Umgebung?**

   d. Wählen Sie **eingeschränkten Modus für dieses Konto aktivieren**.

      Beachten Sie, dass Sie diese Einstellung nicht ändern können, nachdem BlueXP das Konto erstellt

hat. Der eingeschränkte Modus kann später nicht aktiviert werden, und Sie können ihn später nicht mehr deaktivieren.

Wenn Sie den Connector in einer Regierungsregion bereitgestellt haben, ist das Kontrollkästchen bereits aktiviert und kann nicht geändert werden. Dies liegt daran, dass der eingeschränkte Modus der einzige Modus ist, der in Regierungsregionen unterstützt wird.



a. Wählen Sie **Start**.

Ergebnis

Der Connector ist jetzt mit Ihrem BlueXP Konto installiert und eingerichtet. Alle Benutzer müssen über die IP-Adresse der Connector-Instanz auf BlueXP zugreifen.

Was kommt als Nächstes?

Bereitstellen von BlueXP mit den Berechtigungen, die Sie bereits eingerichtet haben.

Schritt 3: Berechtigungen für BlueXP bereitstellen

Wenn Sie den Connector über den Azure Marketplace bereitgestellt oder die Connector-Software manuell installiert haben, müssen Sie die zuvor festgelegten Berechtigungen zur Nutzung der BlueXP Services angeben.

Diese Schritte gelten nicht, wenn Sie den Connector über AWS Marketplace bereitgestellt haben, da Sie während der Bereitstellung die erforderliche IAM-Rolle ausgewählt haben.

"Erfahren Sie, wie Sie Cloud-Berechtigungen vorbereiten".

AWS IAM-Rolle

Hängen Sie die zuvor erstellte IAM-Rolle an die EC2-Instanz an, in der Sie den Connector installiert haben.

Diese Schritte gelten nur, wenn Sie den Connector manuell in AWS installiert haben. Bei AWS Marketplace-Implementierungen haben Sie die Connector-Instanz bereits einer IAM-Rolle zugeordnet, die die erforderlichen Berechtigungen enthält.

Schritte

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

Ergebnis

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

AWS-Zugriffsschlüssel

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

Schritte

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

2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten im Assistenten.
   a. **Anmeldeort**: Wählen Sie **Amazon Web Services > Connector**.
   b. **Zugangsdaten definieren**: Geben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel ein.
   c. **Marketplace-Abonnement**: Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.
   d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

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

Azure Rolle

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

Schritte

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

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

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

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

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

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

Ergebnis

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

Azure Service Principal

Stellen Sie BlueXP die Zugangsdaten für das zuvor von Ihnen Setup für den Azure Service Principal zur Verfügung.

Schritte

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

2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten im Assistenten.
   a. **Anmeldeort**: Wählen Sie **Microsoft Azure > Connector**.
   b. **Credentials definieren**: Geben Sie Informationen über den Microsoft Entra-Dienst-Prinzipal ein, der die erforderlichen Berechtigungen gewährt:
      - Anwendungs-ID (Client)
      - ID des Verzeichnisses (Mandant)

    - Client-Schlüssel

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

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

Ergebnis

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

Google Cloud Service-Konto

Verknüpfen Sie das Servicekonto mit der Konnektor-VM.

Schritte

1. Wechseln Sie zum Google Cloud Portal und weisen Sie das Servicekonto der VM-Instanz des Connectors zu.

   "Google Cloud-Dokumentation: Ändern des Dienstkontos und des Zugriffsumfangs für eine Instanz"

2. Wenn Sie Ressourcen in anderen Projekten managen möchten, gewähren Sie Zugriff, indem Sie das Servicekonto mit der BlueXP Rolle zu diesem Projekt hinzufügen. Sie müssen diesen Schritt für jedes Projekt wiederholen.

Ergebnis

BlueXP verfügt jetzt über die nötigen Berechtigungen, um Aktionen in Google Cloud für Sie durchzuführen.

BlueXP abonnieren (eingeschränkter Modus)

Abonnieren Sie BlueXP über den Marketplace Ihres Cloud-Providers und zahlen Sie für BlueXP Services zu einem Stundensatz (PAYGO) oder über einen Jahresvertrag. Wenn Sie eine Lizenz von NetApp (BYOL) erworben haben, müssen Sie auch das Marketplace-Angebot abonnieren. Ihre Lizenz wird immer zuerst berechnet, aber Sie werden mit dem Stundensatz belastet, wenn Sie Ihre lizenzierte Kapazität überschreiten oder wenn die Laufzeit der Lizenz abläuft.

Ein Marketplace Abonnement ermöglicht die Abrechnung der folgenden BlueXP Services mit eingeschränktem Modus:

- Backup und Recovery
- Klassifizierung
- Cloud Volumes ONTAP

Bevor Sie beginnen

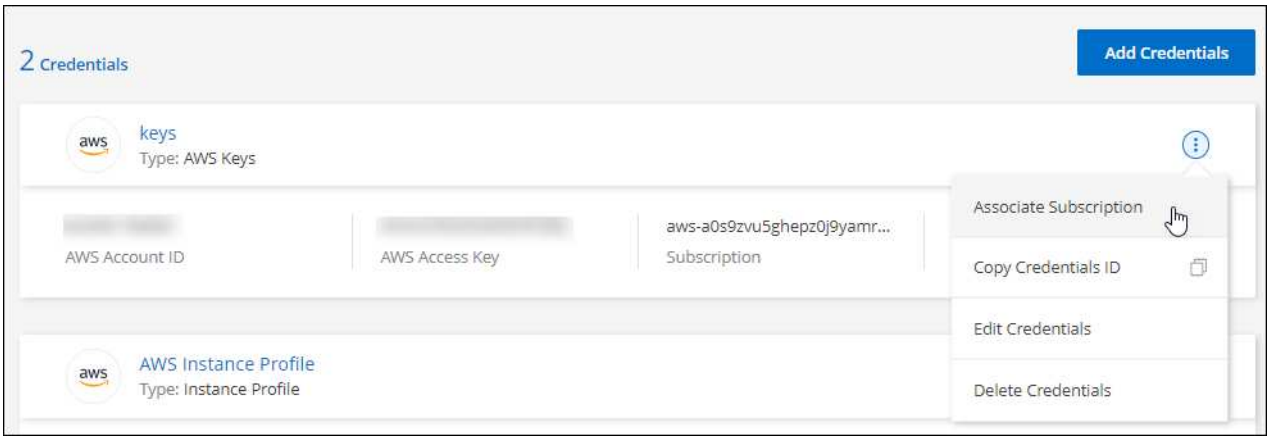
Für das Abonnement von BlueXP wird ein Marketplace-Abonnement mit den Cloud-Zugangsdaten verknüpft, die einem Connector zugeordnet sind. Wenn Sie den Workflow „erste Schritte mit eingeschränktem Modus“ befolgt haben, sollten Sie bereits über einen Connector verfügen. Weitere Informationen finden Sie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

AWS

Schritte

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

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



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

   a. Wählen Sie **Kaufoptionen anzeigen**.

   b. Wählen Sie **Abonnieren**.

   c. Wählen Sie **Konto einrichten**.

      Sie werden auf die BlueXP-Website umgeleitet.

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

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

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

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

      - Wählen Sie **Speichern**.

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

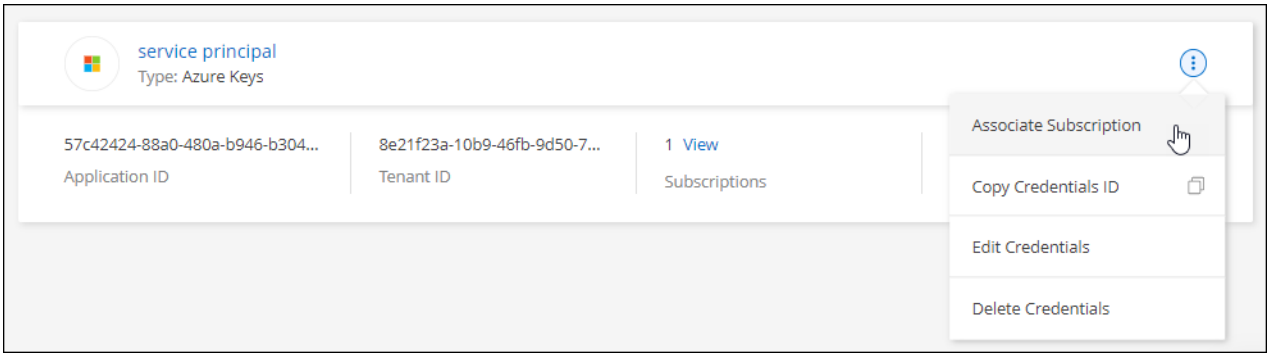
Abonnieren Sie BlueXP über den AWS Marketplace

Azure

Schritte

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

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



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

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

   b. Wählen Sie **Abonnieren**.

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

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

      Sie werden auf die BlueXP-Website umgeleitet.

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

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

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

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

      - Wählen Sie **Speichern**.

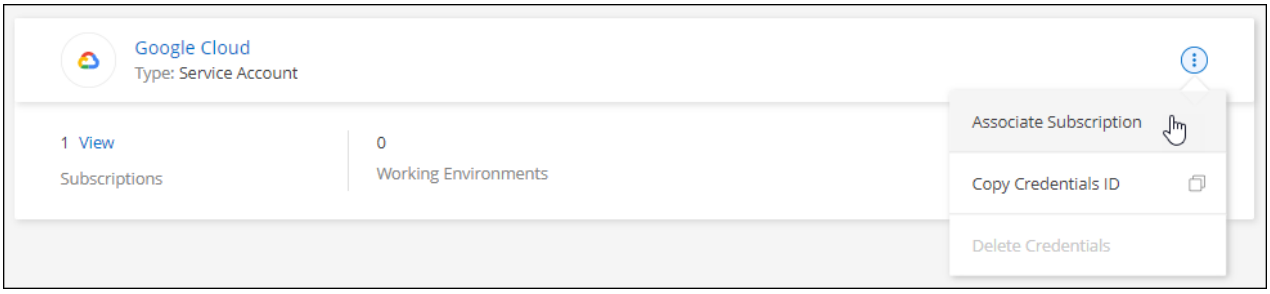
Im folgenden Video sehen Sie, wie Sie im Azure Marketplace abonnieren:

Abonnieren Sie BlueXP über den Azure Marketplace

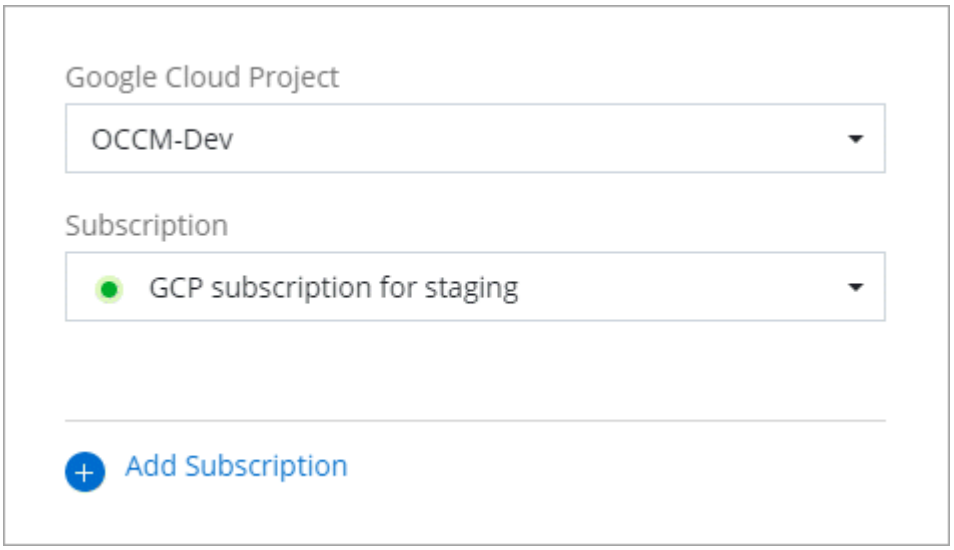
Google Cloud

Schritte

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



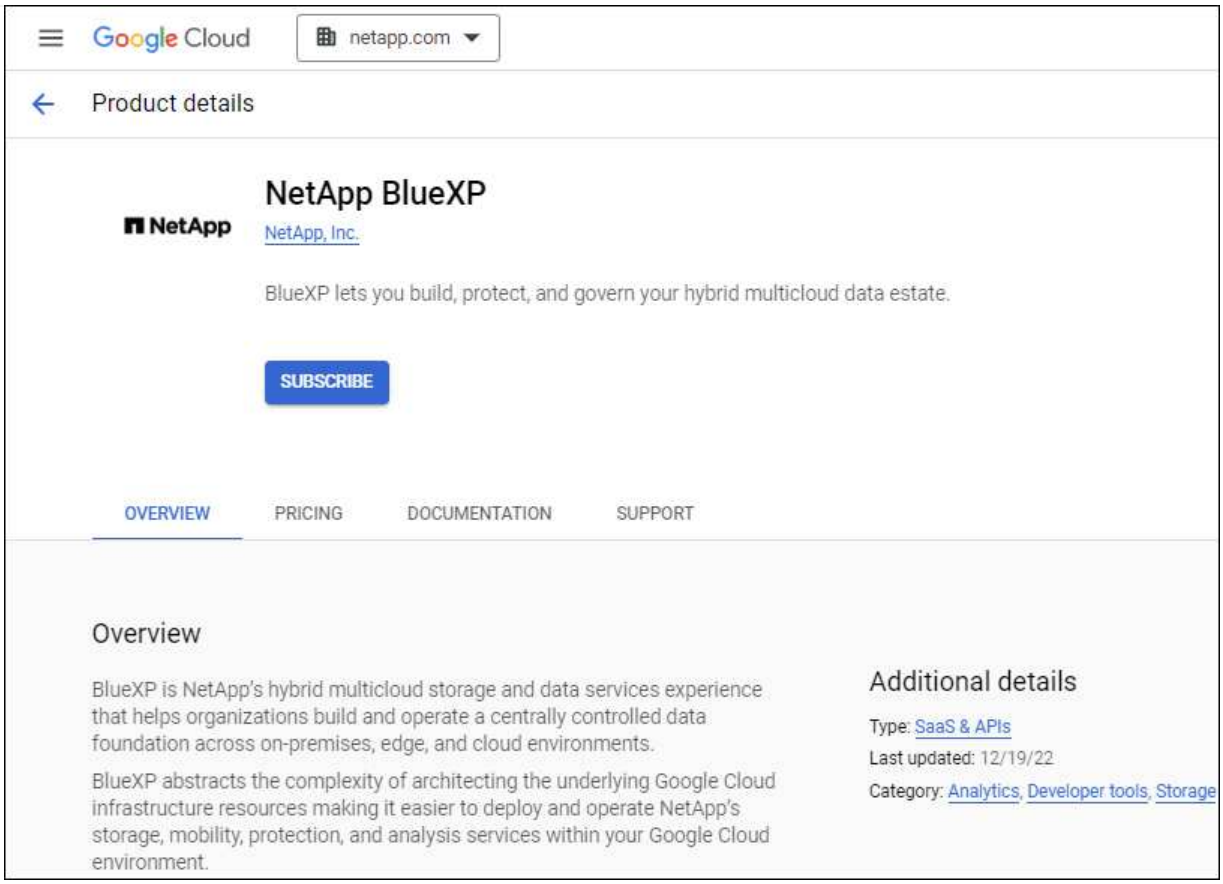
3. Um die Anmeldeinformationen einem bestehenden Abonnement zuzuordnen, wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, und wählen Sie dann **Associate** aus.



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

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

   a. Nachdem Sie auf die umgeleitet wurden "Seite zu NetApp BlueXP im Google Cloud Marketplace", Stellen Sie sicher, dass das richtige Projekt im oberen Navigationsmenü ausgewählt ist.



b. Wählen Sie **Abonnieren**.

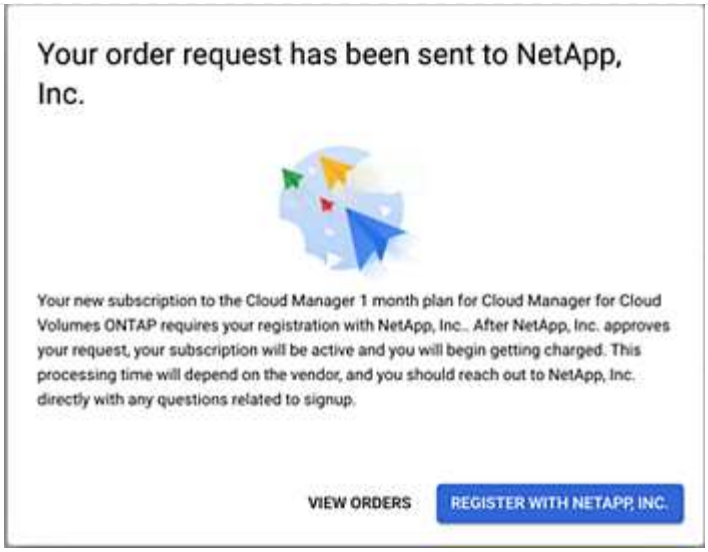
c. Wählen Sie das entsprechende Rechnungskonto aus und stimmen Sie den allgemeinen Geschäftsbedingungen zu.

d. Wählen Sie **Abonnieren**.

   Dieser Schritt sendet Ihre Transferanfrage an NetApp.

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

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



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

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

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

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

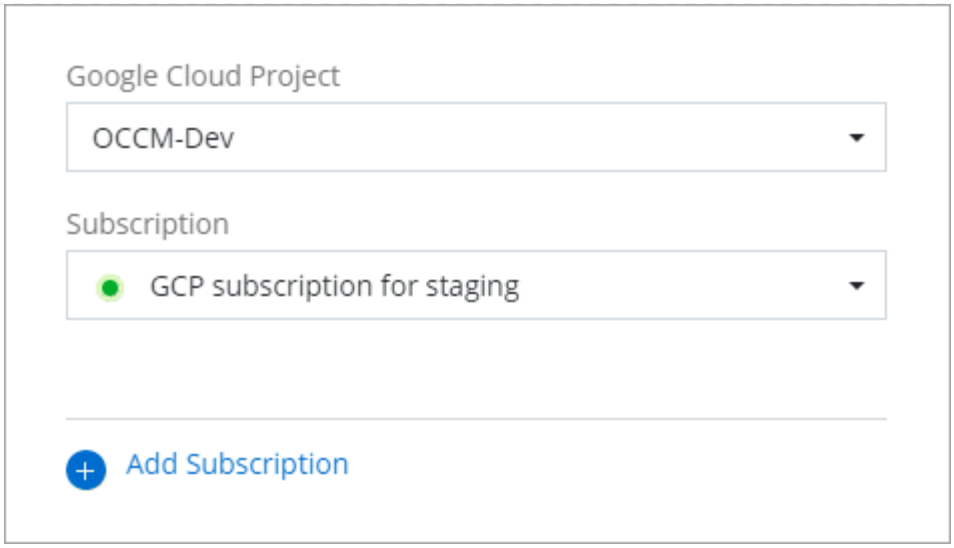
Bei allen anderen Konten müssen Sie das Abonnement manuell verknüpfen, indem Sie die folgenden Schritte wiederholen.

- Wählen Sie **Speichern**.

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

Abonnieren Sie BlueXP über den Google Cloud Marketplace

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



Weiterführende Links

- "Managen Sie kapazitätsbasierte BYOL-Lizenzen für Cloud Volumes ONTAP"
- "Managen von BYOL-Lizenzen für BlueXP Datenservices"
- "Managen Sie AWS Anmeldeinformationen und Abonnements für BlueXP"
- "Managen Sie Azure Anmeldedaten und Abonnements für BlueXP"
- "Managen Sie Google Cloud-Anmeldedaten und -Abonnements für BlueXP"

Nächste Schritte (eingeschränkter Modus)

Nachdem Sie BlueXP im eingeschränkten Modus eingerichtet haben, können Sie die BlueXP Services, die mit eingeschränktem Modus unterstützt werden, nutzen.

Hilfe finden Sie in der Dokumentation zu diesen Services:

- "Amazon FSX für ONTAP Dokumentation"
- "Azure NetApp Files Dokumentation"
- "Dokumentation zu Backup und Recovery"
- "Dokumente zur Klassifizierung"
- "Cloud Volumes ONTAP Dokumentation"
- "ONTAP-Cluster-Dokumentation vor Ort"
- "Replizierungsdokumente"

Verwandter Link

"BlueXP Implementierungsmodi"