Starten Sie mit dem privaten Modus

Setup and administration

NetApp
April 26, 2024

Inhalt

Starten Sie mit dem privaten Modus

Erste Schritte Workflow (privater Modus)

Erste Schritte mit BlueXP im privaten Modus: Bereiten Sie Ihre Umgebung vor und implementieren Sie den Connector.

Der private Modus wird in der Regel mit On-Premises-Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, einschließlich "AWS Secret Cloud", "Top Secret Cloud von AWS", und "Azure IL6"

Bevor Sie beginnen, sollten Sie ein Verständnis von haben "BlueXP Accounts", "Anschlüsse", und "Bereitstellungsmodi".

1 **"Vorbereitungen für die Implementierung"**

1. Bereiten Sie einen dedizierten Linux-Host vor, der die Anforderungen für CPU, RAM, Festplattenspeicher, Docker Engine und mehr erfüllt.
2. Richten Sie ein Netzwerk ein, das Zugriff auf die Zielnetzwerke bietet.
3. Richten Sie bei Cloud-Bereitstellungen Berechtigungen in Ihrem Cloud-Provider ein, damit Sie diese Berechtigungen nach der Installation der Software mit dem Connector verknüpfen können.

2 **"Implementieren Sie den Connector"**

1. Installieren Sie die Connector-Software auf Ihrem eigenen Linux-Host.
2. Richten Sie BlueXP ein, indem Sie einen Webbrowser öffnen und die IP-Adresse des Linux-Hosts eingeben.
3. Stellen Sie für Cloud-Implementierungen BlueXP die Berechtigungen bereit, die Sie zuvor eingerichtet haben.

Bereiten Sie die Bereitstellung im privaten Modus vor

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

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

Schritt 1: Verstehen, wie der private Modus funktioniert

Bevor Sie beginnen, sollten Sie sich ein Bild davon machen, wie BlueXP im privaten Modus funktioniert.

Sie sollten beispielsweise verstehen, dass Sie die browserbasierte Oberfläche verwenden müssen, die lokal über den BlueXP Connector verfügbar ist, die Sie installieren müssen. Der Zugriff auf BlueXP erfolgt nicht über die webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird.

Außerdem sind nicht alle BlueXP Services verfügbar.

"Erfahren Sie, wie der private Modus funktioniert".

Schritt 2: Überprüfen Sie die Installationsoptionen

Im privaten Modus können Sie den Connector vor Ort oder in der Cloud installieren, indem Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren.

Bei der Installation des Connectors wird festgelegt, welche BlueXP Services und Funktionen beim Einsatz des privaten Modus verfügbar sind. Beispielsweise muss der Connector in der Cloud installiert sein, wenn Sie Cloud Volumes ONTAP bereitstellen und verwalten möchten. "Weitere Informationen zum privaten Modus".

Schritt 3: Überprüfen Sie die Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

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

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

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

Hypervisor

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

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

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Azure VM-Größe

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

Google Cloud-Maschinentyp

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

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

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

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

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

  "Installationsanweisungen anzeigen"

Schritt 4: Vernetzung für den Connector vorbereiten

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

Verbindungen zu Zielnetzwerken

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

Endpunkte für den täglichen Betrieb

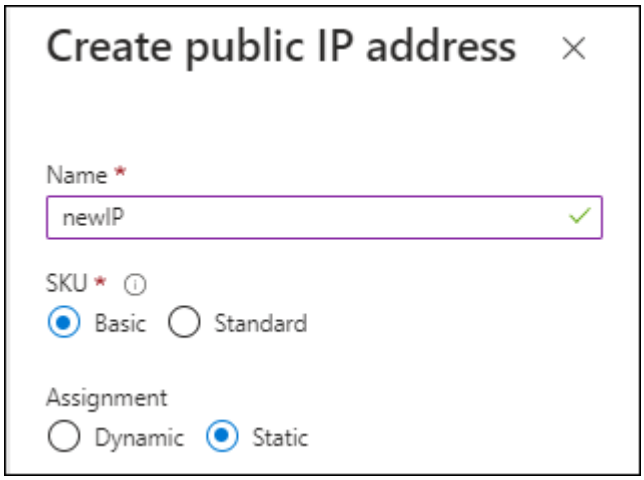
Der Connector kontaktiert die folgenden Endpunkte, um Ressourcen und Prozesse in der Public Cloud-Umgebung zu managen.

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"

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.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Zum Managen von Ressourcen in der Region Azure-IL6.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.

Öffentliche IP-Adresse in Azure

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



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

"Azure-Dokumentation: Öffentliche IP-SKU"

Proxy-Server

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

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

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

+
Im privaten Modus sendet BlueXP lediglich Outbound-Datenverkehr zu Ihrem Cloud-Provider, um ein Cloud Volumes ONTAP System zu erstellen.

Ports

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn.

HTTP (80) und HTTPS (443) bieten den Zugriff auf die BlueXP Konsole. SSH (22) ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

Aktivieren Sie NTP

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

Schritt 5: Cloud-Berechtigungen vorbereiten

Wenn der Connector in der Cloud installiert ist und Sie planen, Cloud Volumes ONTAP-Systeme zu erstellen, erfordert BlueXP Berechtigungen von Ihrem Cloud-Provider. Sie müssen Berechtigungen in Ihrem Cloud-Provider einrichten und diese Berechtigungen dann der Connector-Instanz zuordnen, nachdem Sie sie installiert haben.

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

AWS IAM-Rolle

Verwenden Sie eine IAM-Rolle, um dem Connector Berechtigungen zu gewähren. Sie müssen die Rolle manuell an die EC2-Instanz für den Connector anhängen.

Schritte

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

Ergebnis

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

AWS-Zugriffsschlüssel

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

Schritte

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

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

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

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen.

Azure Rolle

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

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

Schritte

1. Aktivieren Sie eine vom System zugewiesene gemanagte Identität auf der VM, bei der Sie den Connector installieren möchten, damit Sie die erforderlichen Azure-Berechtigungen über eine benutzerdefinierte Rolle bereitstellen können.

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

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

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

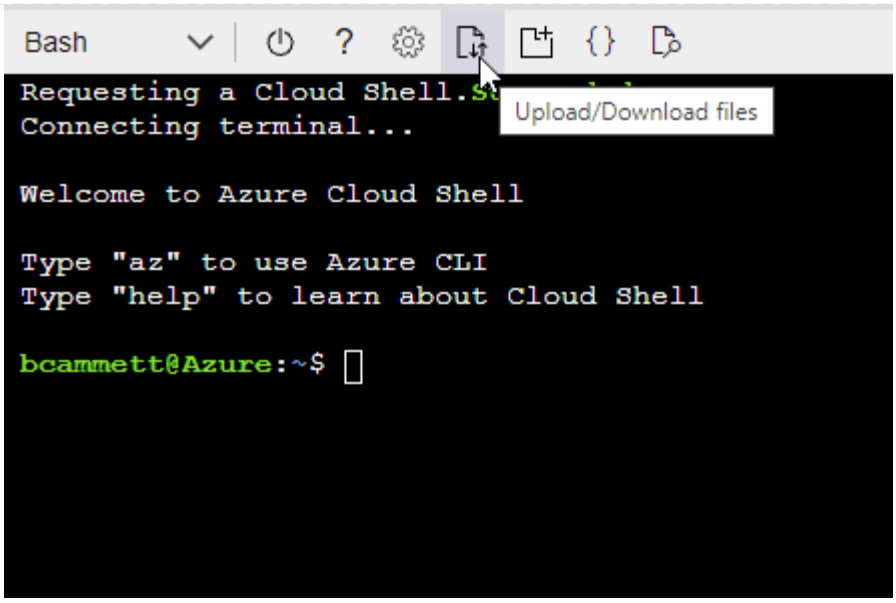
   Beispiel

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

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

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

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



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

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

Ergebnis

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

Azure Service Principal

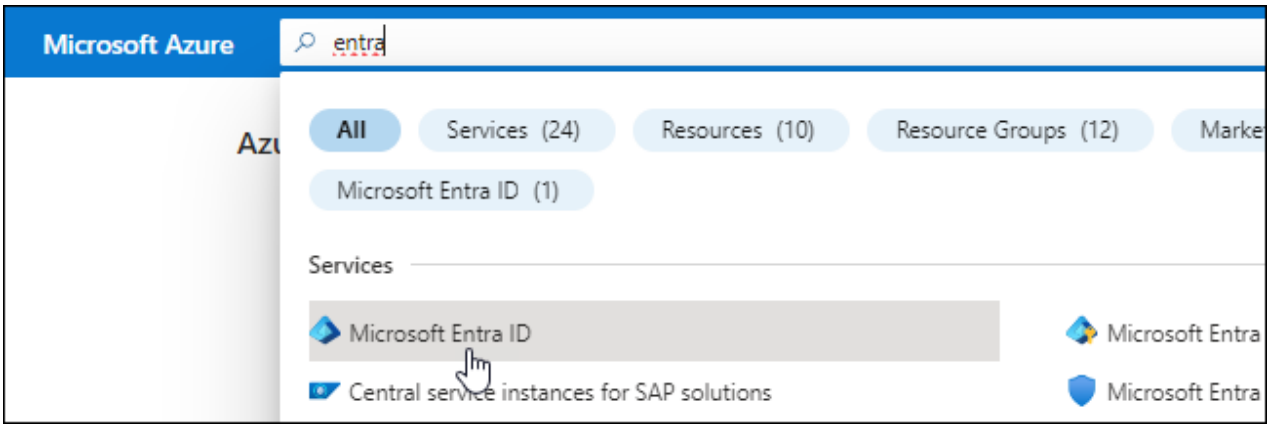
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten. Sie müssen BlueXP nach der Installation des Connectors und der Einrichtung von BlueXP über diese Zugangsdaten informieren.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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

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

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



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

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

Anwendung einer Rolle zuweisen

1. Erstellen einer benutzerdefinierten Rolle:

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

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

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

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

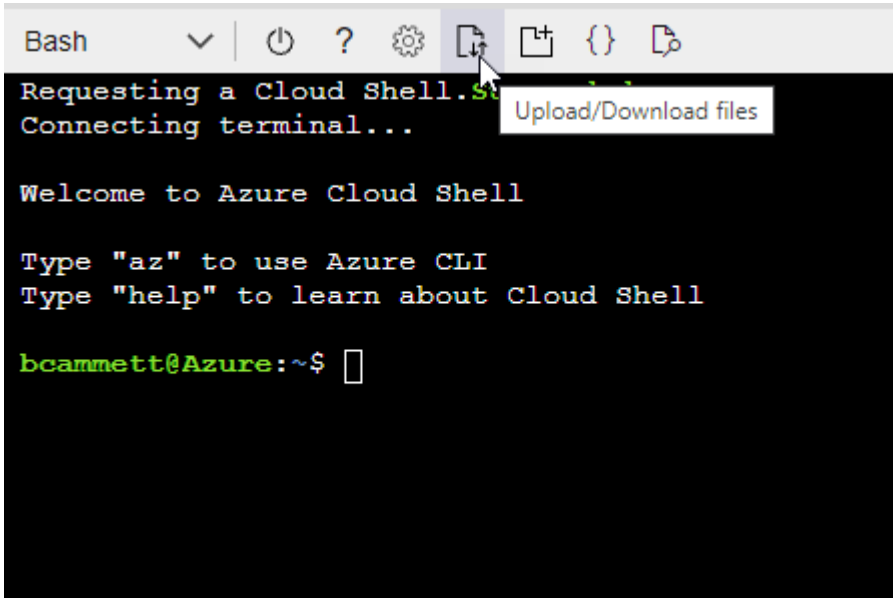
      Beispiel

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

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

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

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



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

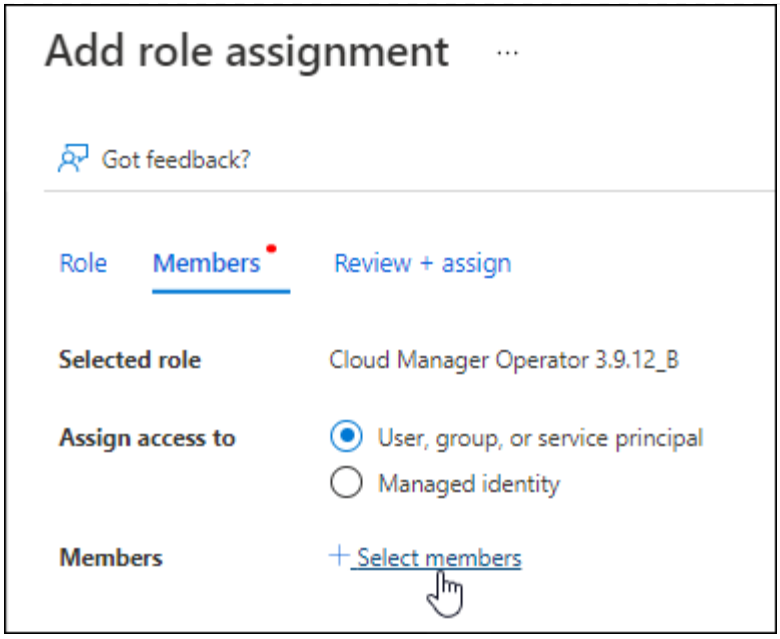
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

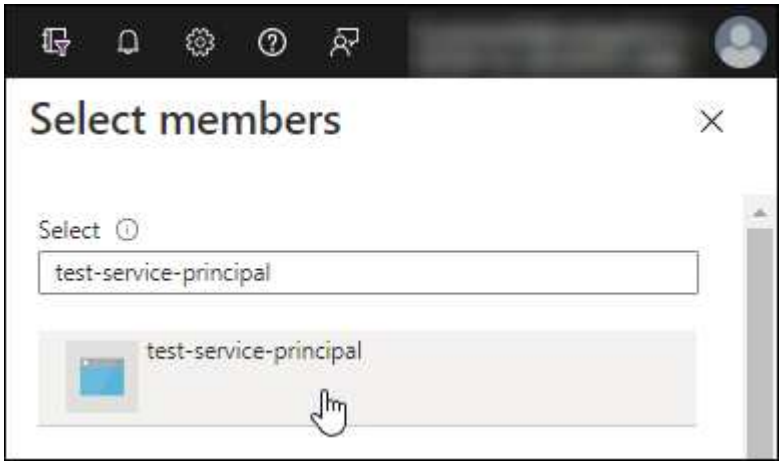
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ein Beispiel:



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

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

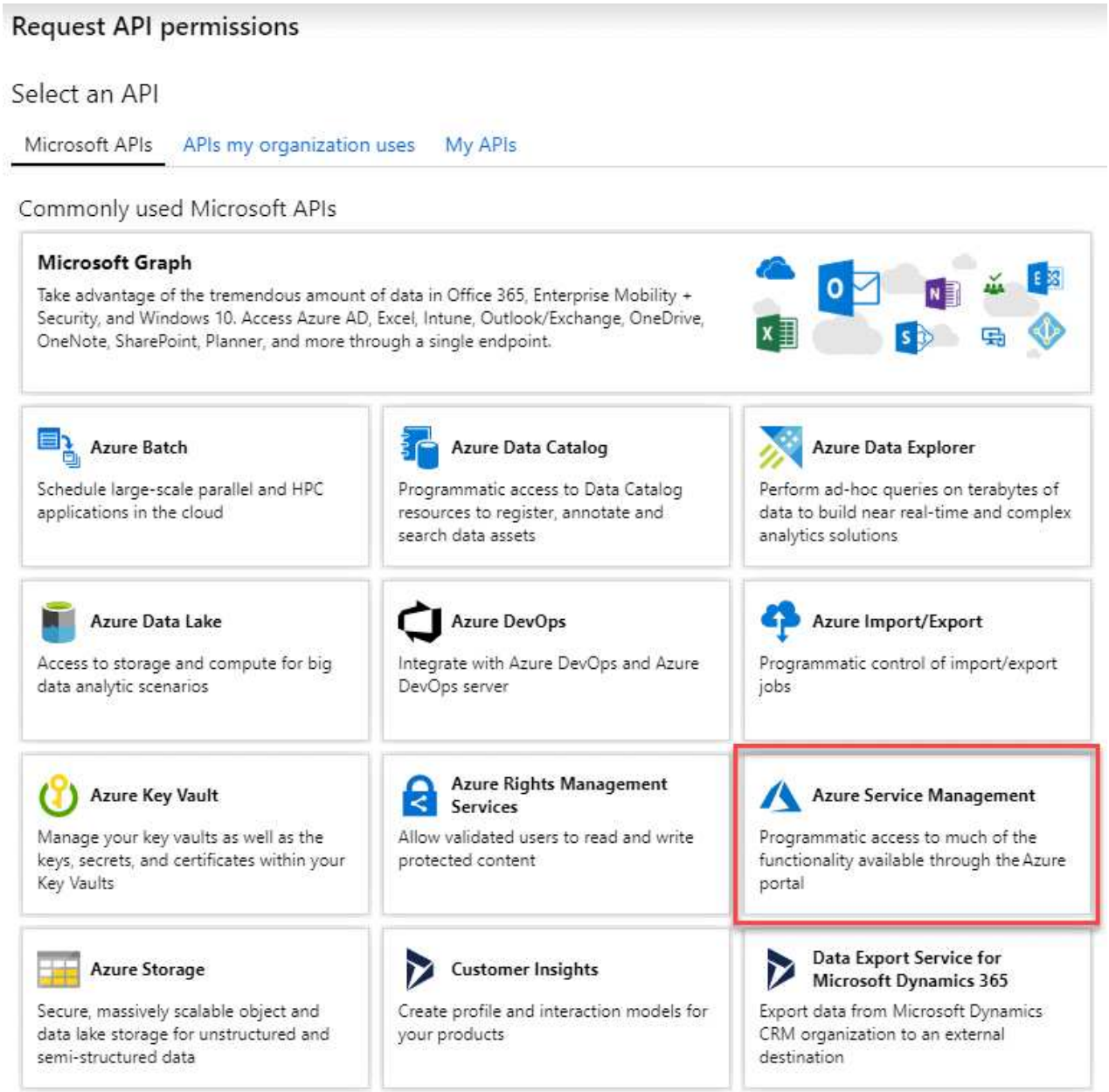
   Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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

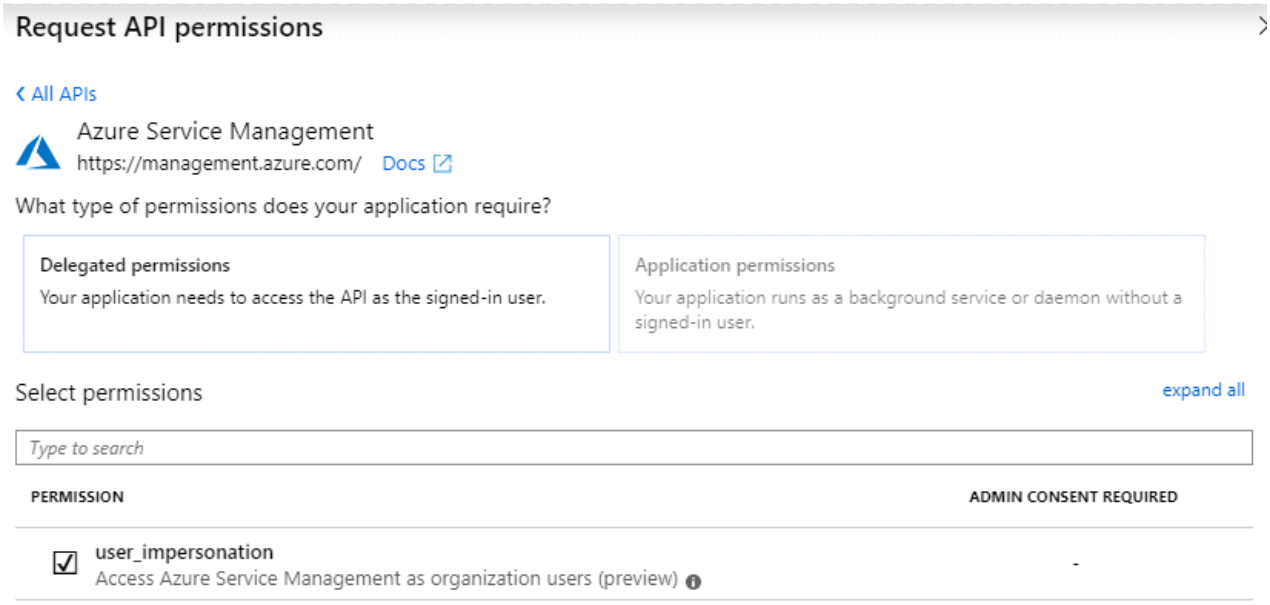
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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

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

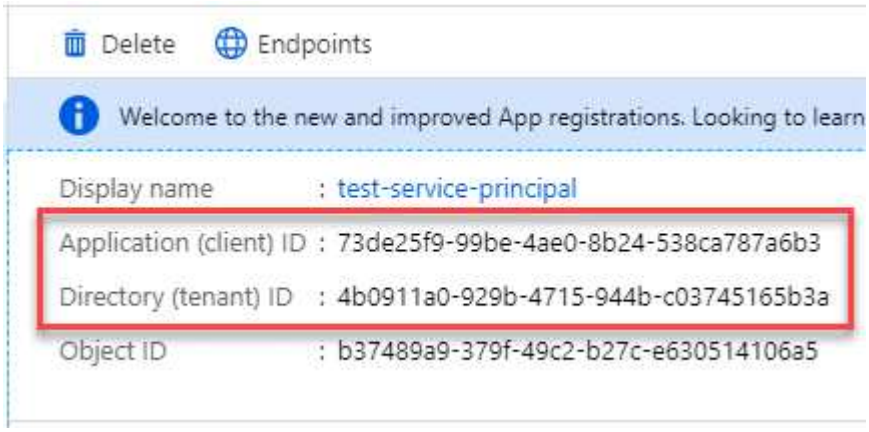


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen Sie einen Clientschlüssel

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

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

Ergebnis

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

Google Cloud Service-Konto

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

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

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

   b. Aktivieren Sie in Google Cloud die Cloud Shell.

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

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

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

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

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

2. Erstellen Sie ein Servicekonto in Google Cloud:

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

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

   c. Wählen Sie die gerade erstellte Rolle aus.

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

      "Google Cloud docs: Erstellen eines Dienstkontos"

Ergebnis

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

Schritt 6: Google Cloud APIs aktivieren

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

Schritt

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

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

Stellen Sie den Connector im privaten Modus bereit

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

Schritt 1: Installieren Sie den Stecker

Laden Sie das Produkt-Installationsprogramm von der NetApp Support Site herunter und installieren Sie den Connector dann manuell auf Ihrem eigenen Linux Host.

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

Bevor Sie beginnen

Zur Installation des Connectors sind Root-Berechtigungen erforderlich.

Schritte

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

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

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

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

herunterladen.

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

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

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

5. Führen Sie das Installationsskript aus:

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

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

Ergebnis

Die Connector-Software ist installiert. Sie können jetzt BlueXP einrichten.

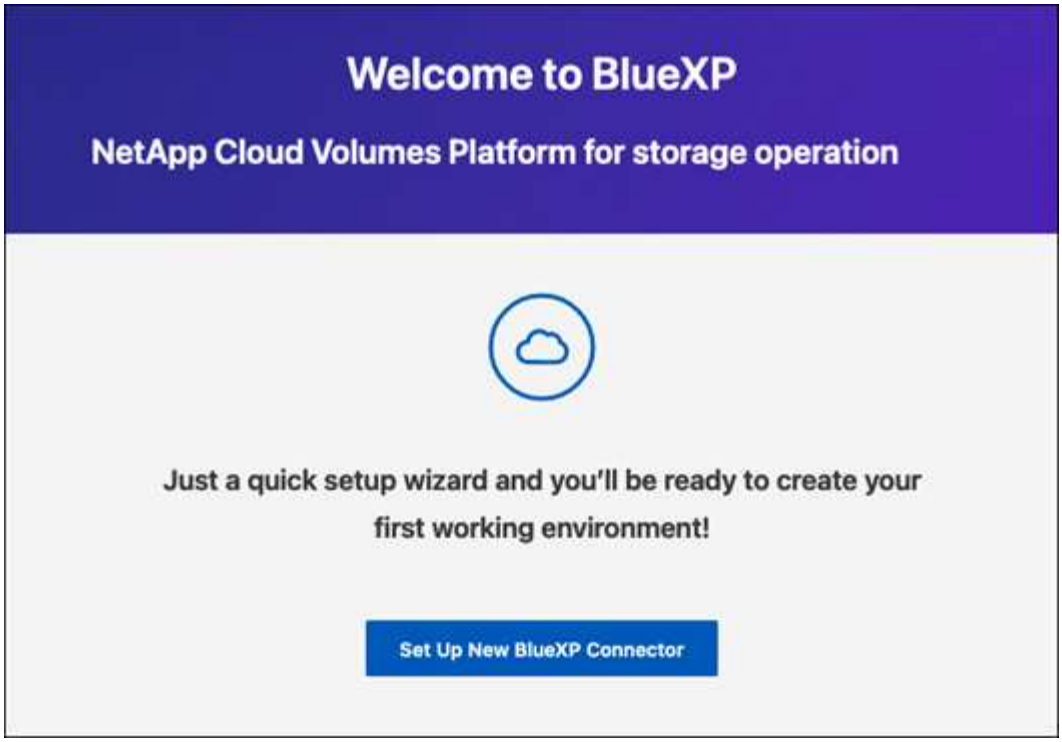
Schritt 2: BlueXP einrichten

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

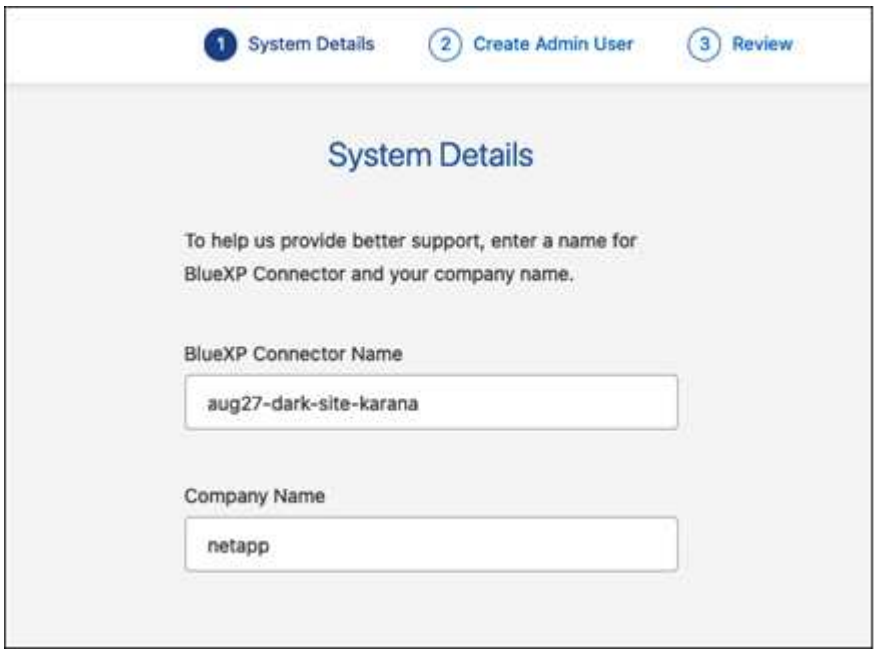
Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie ein https://ipaddress Wobei ipaddress die IP-Adresse des Linux-Hosts ist, auf dem Sie den Connector installiert haben.

   Der folgende Bildschirm sollte angezeigt werden.



2. Wählen Sie **Set up New BlueXP Connector** und folgen Sie den Anweisungen, um das System einzurichten.
   - **Systemdetails**: Geben Sie einen Namen für den Connector und Ihren Firmennamen ein.



   - **Admin-Benutzer erstellen**: Erstellen Sie den Admin-Benutzer für das System.

     Dieses Benutzerkonto wird lokal auf dem System ausgeführt. Über BlueXP ist keine Verbindung zum aut0-Service verfügbar.

   - **Review**: Überprüfen Sie die Details, akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Setup**.

3. Melden Sie sich mit dem gerade erstellten Admin-Benutzer bei BlueXP an.

Ergebnis

Der Connector ist jetzt installiert und eingerichtet.

Sobald neue Versionen der Connector-Software verfügbar sind, werden diese auf der NetApp Support Site veröffentlicht. "Erfahren Sie, wie Sie den Connector aktualisieren können".

Was kommt als Nächstes?

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

Schritt 3: Berechtigungen für BlueXP bereitstellen

Wenn Sie Cloud Volumes ONTAP-Arbeitsumgebungen erstellen möchten, müssen Sie BlueXP mit den zuvor festgelegten Cloud-Berechtigungen versehen.

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

AWS IAM-Rolle

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

Schritte

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

Ergebnis

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

AWS-Zugriffsschlüssel

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

Schritte

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

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

Ergebnis

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

Azure Rolle

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

Schritte

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

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

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

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

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

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

Ergebnis

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

Azure Service Principal

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

Schritte

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

2. Wählen Sie **Anmeldeinformationen hinzufügen** und folgen Sie den Schritten im Assistenten.
   a. **Anmeldeort**: Wählen Sie **Microsoft Azure > Connector**.
   b. **Credentials definieren**: Geben Sie Informationen über den Microsoft Entra-Dienst-Prinzipal ein, der die erforderlichen Berechtigungen gewährt:
      - Anwendungs-ID (Client)
      - ID des Verzeichnisses (Mandant)
      - Client-Schlüssel
   c. **Marketplace-Abonnement**: Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.
   d. **Review**: Bestätigen Sie die Details zu den neuen Zugangsdaten und wählen Sie **Add**.

Ergebnis

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

Google Cloud Service-Konto

Verknüpfen Sie das Servicekonto mit der Konnektor-VM.

Schritte

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

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

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

Ergebnis

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

Nächste Schritte (privater Modus)

Nachdem Sie BlueXP im privaten Modus eingerichtet haben, können Sie die BlueXP Services, die vom privaten Modus unterstützt werden, sofort nutzen.

Hilfe finden Sie in der folgenden Dokumentation:

- "Erstellen von Cloud Volumes ONTAP Systemen"
- "Erkennen von ONTAP Clustern vor Ort"
- "Datenreplizierung"
- "Scannen Sie On-Premises-ONTAP-Volume-Daten mithilfe der BlueXP Klassifizierung"
- "Sichern Sie lokale ONTAP Volume-Daten mithilfe von BlueXP Backup- und Recovery-Funktionen in StorageGRID"

Verwandter Link

"BlueXP Implementierungsmodi"