Einen Konnektor erstellen

Setup and administration

NetApp
August 05, 2024

Inhalt

Einen Konnektor erstellen

AWS

Installationsoptionen für Konnektoren in AWS

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

Folgende Installationsoptionen sind verfügbar:

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

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

- "Erstellen Sie einen Connector aus dem AWS Marketplace"

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

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

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

Erstellen Sie einen Connector in AWS von BlueXP

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Outbound-Internetzugang

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

Vom Connector kontaktierte Endpunkte

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

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

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

Endpunkte wurden über die BlueXP Konsole kontaktiert

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

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

Proxy-Server

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

- 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".

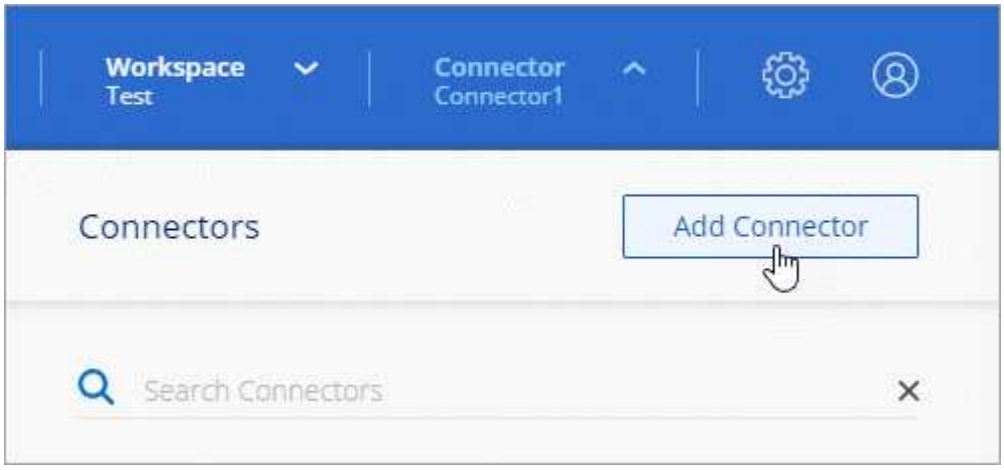
Bevor Sie beginnen

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

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Outbound-Internetzugang

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

Vom Connector kontaktierte Endpunkte

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

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

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

Proxy-Server

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

- 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

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Schritt 4: Erstellen Sie den Konnektor

Erstellen Sie den Connector direkt über AWS Marketplace.

Über diese Aufgabe

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

Bevor Sie beginnen

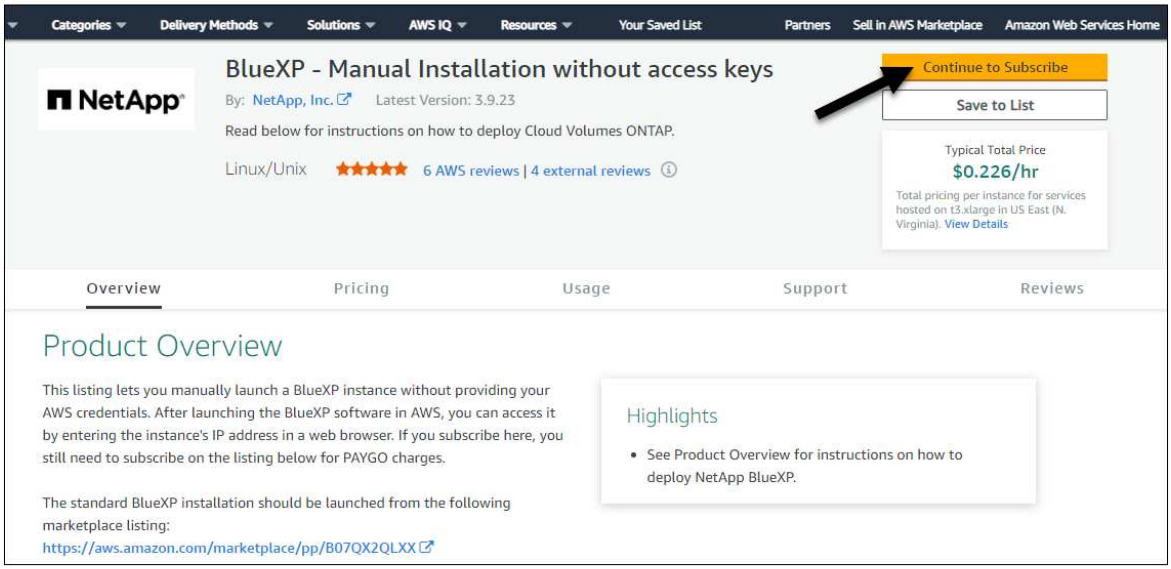
Sie sollten Folgendes haben:

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

Schritte

1. Go to the "BlueXP Connector listing on the AWS Marketplace"
2. Wählen Sie auf der Marketplace-Seite **Weiter zu Abonnieren** und wählen Sie dann **Weiter zu Konfiguration**.

a



b

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

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

5. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:

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

     - Wählen Sie die gewünschte VPC und das Subnetz.
     - Geben Sie an, ob die Instanz eine öffentliche IP-Adresse haben soll.

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

  Für spezifische Konfigurationen sind noch einige Regeln erforderlich.

  "Sicherheitsgruppen-Regeln für AWS ansehen".

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

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

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

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

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

   https://ipaddress

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

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

   d. Wählen Sie **Start**.

Ergebnis

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

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

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

Installieren Sie den Connector manuell in AWS

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6 bis 8.10
  - 9.1 bis 9.3

    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 gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Schlüsselpaar

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

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

BlueXP nutzt `/opt` Um den zu installieren `/opt/application/netapp` Verzeichnis und es ist Inhalt.

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.

Container-Orchestrierungstool

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

- Podman Version 4.6.1 ist für Red hat Enterprise Linux 8 und 9 erforderlich.

  Für Podman müssen folgende Voraussetzungen erfüllt sein:

  - Der podman.Socket-Dienst muss aktiviert und gestartet werden
  - python3 muss installiert sein
  - Das Paket podman-compose Version 1.0.6 muss installiert sein
  - Podman-compose muss der Umgebungsvariable PATH hinzugefügt werden
- Docker Engine ist für Ubuntu erforderlich.
  - Die unterstützte Version ist mindestens 23.0.6.
  - Die maximal unterstützte Version ist 25.0.5.

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.
- Docker Engine ist für Ubuntu erforderlich.

Beispiel 1. Schritte

Podman

Installieren Sie Podman 4.6.1.

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-2:4.6.1
```

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:4.6.1
```

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

Installieren Sie eine Version der Docker Engine zwischen 23.0.6 und 25.0.5.

Schritte

1. Installieren Sie Die Docker Engine.

   "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 wurden während der manuellen Installation kontaktiert

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

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

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

Vom Connector kontaktierte Endpunkte

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

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

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

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

Proxy-Server

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

- 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 Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie nach der Installation des Connectors zu BlueXP hinzufügen können.

Ergebnis

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

Schritt 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.

  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. 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 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-v3.9.40--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 nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

5. 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.

6. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung mit der virtuellen

Verbindungsmaschine hat, und geben Sie die folgende URL ein:

https://ipaddress

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

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

   d. Wählen Sie **Start**.

Ergebnis

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

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

Schritt 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

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

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

Azure Region

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

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

Vnet und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Outbound-Internetzugang

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

Vom Connector kontaktierte Endpunkte

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

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

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

Endpunkte wurden über die BlueXP Konsole kontaktiert

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

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

Proxy-Server

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

- 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 Sie eine benutzerdefinierte Rolle

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

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

Schritte

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

Diese benutzerdefinierte Rolle enthält nur die Berechtigungen, die zum Starten der Connector-VM in Azure von BlueXP erforderlich sind. Verwenden Sie diese Richtlinie nicht für andere Situationen. Wenn BlueXP den Connector erstellt, wendet 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

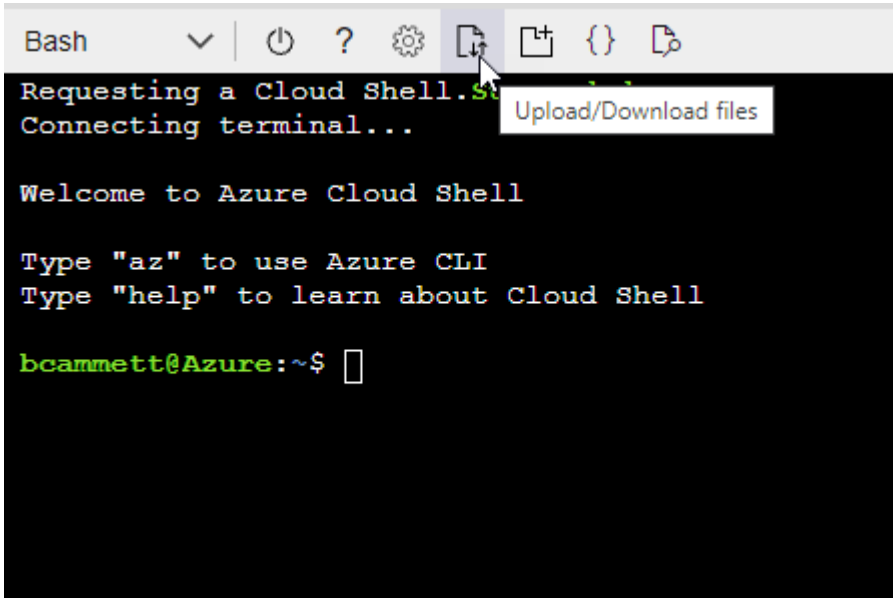
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

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.

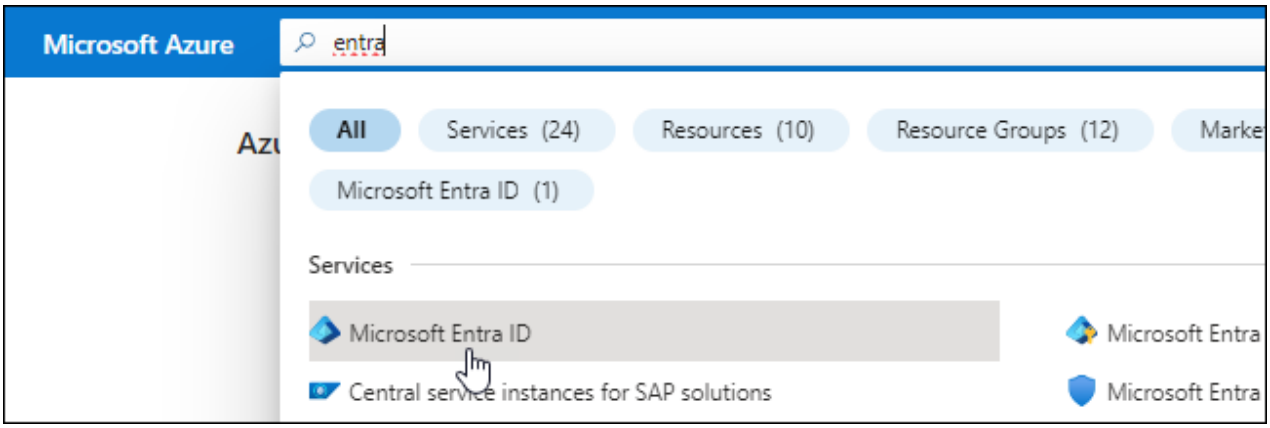
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

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**.

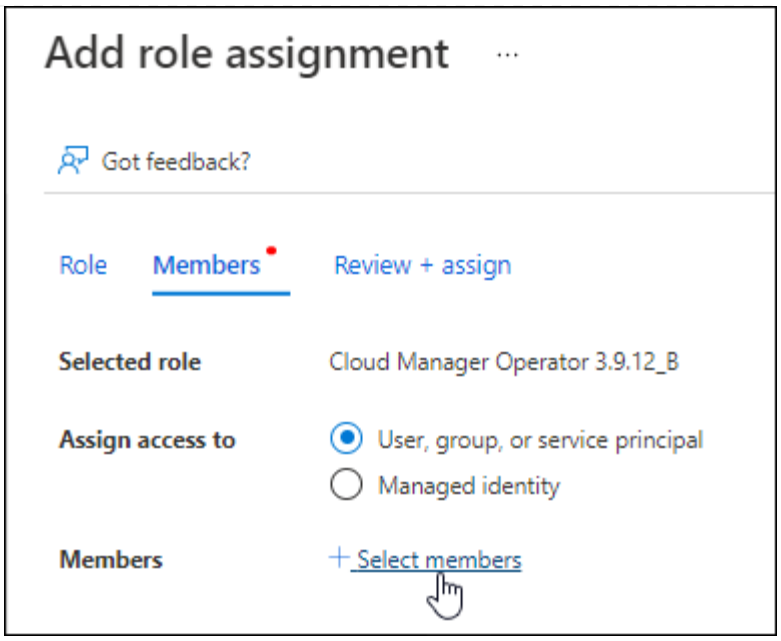
   Sie haben die AD-Anwendung und den Service-Principal erstellt.

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:

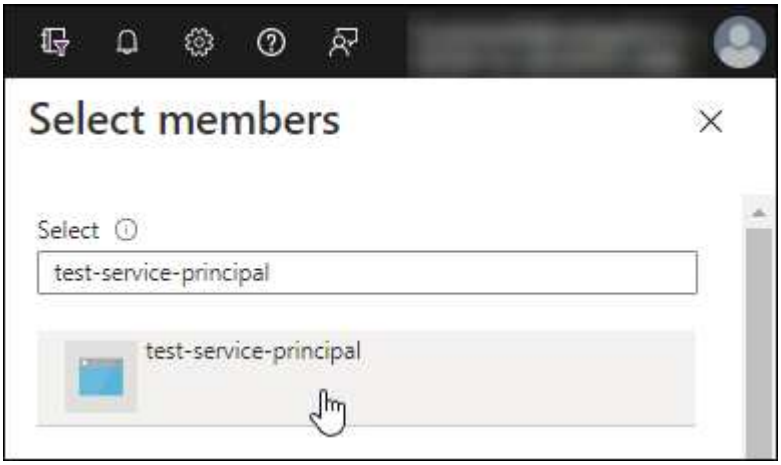
   a. **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.

   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**.

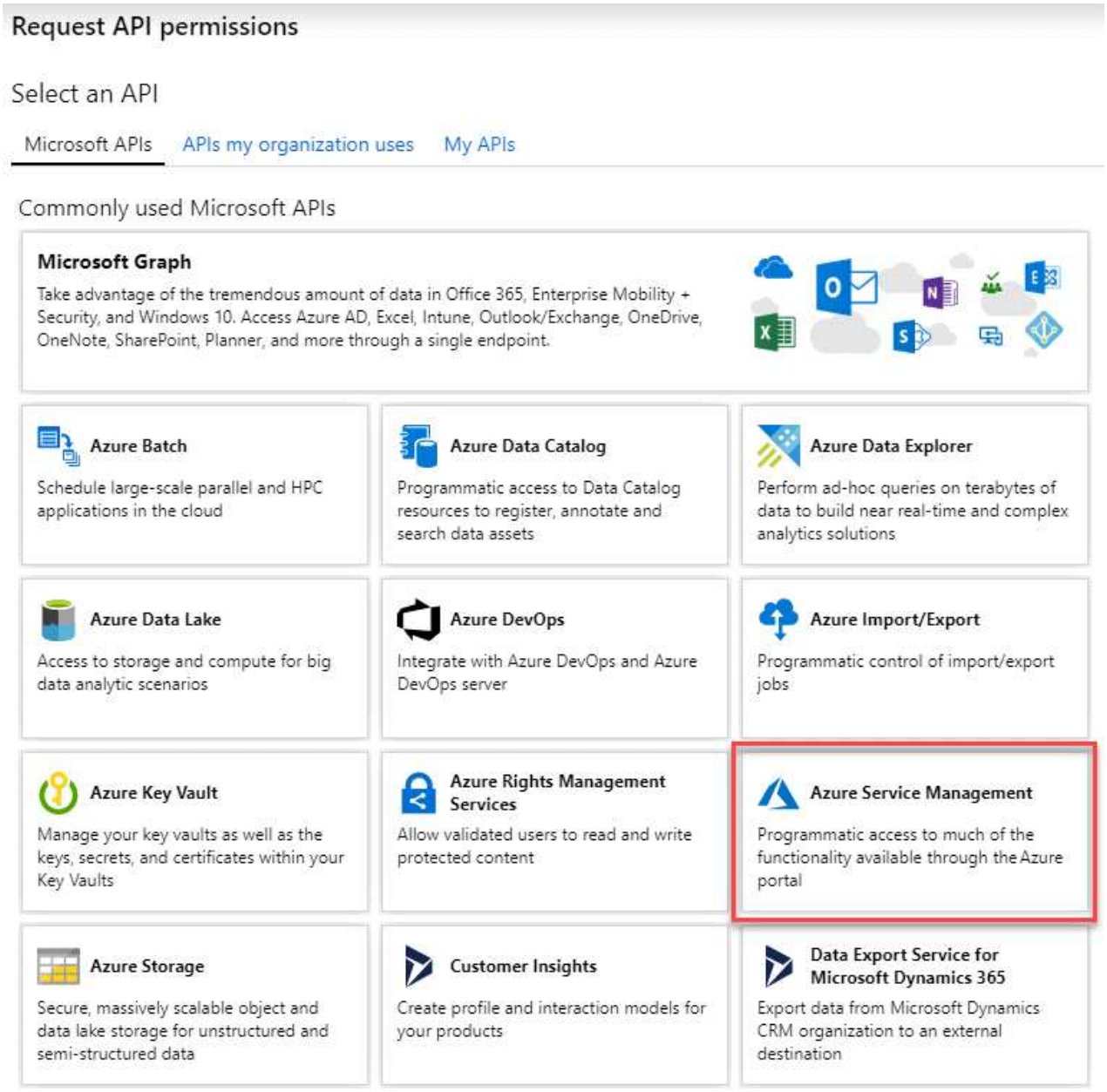
Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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.

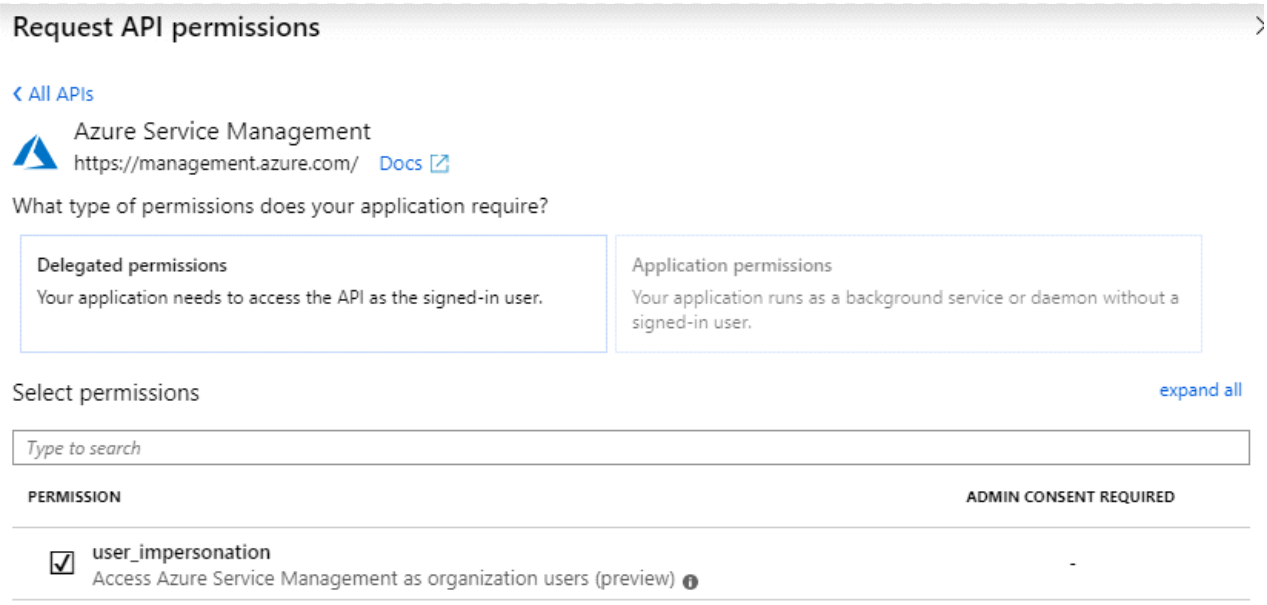
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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.

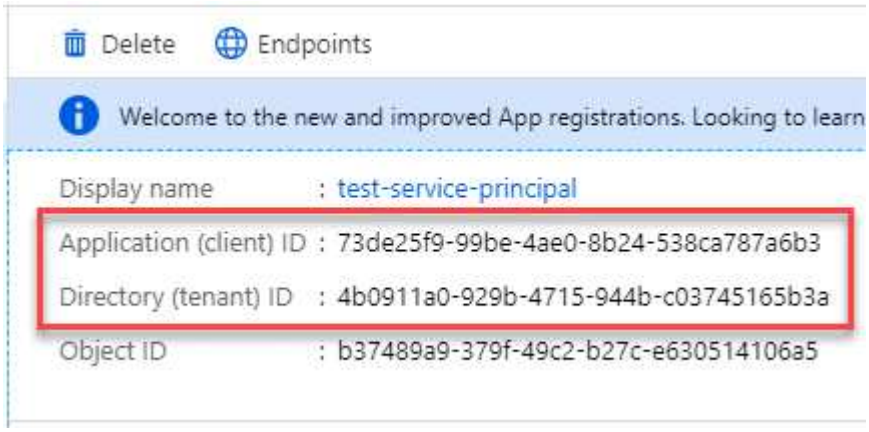


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen Sie einen Clientschlüssel

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

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

Ergebnis

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

Schritt 4: Erstellen Sie den Konnektor

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

Über diese Aufgabe

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

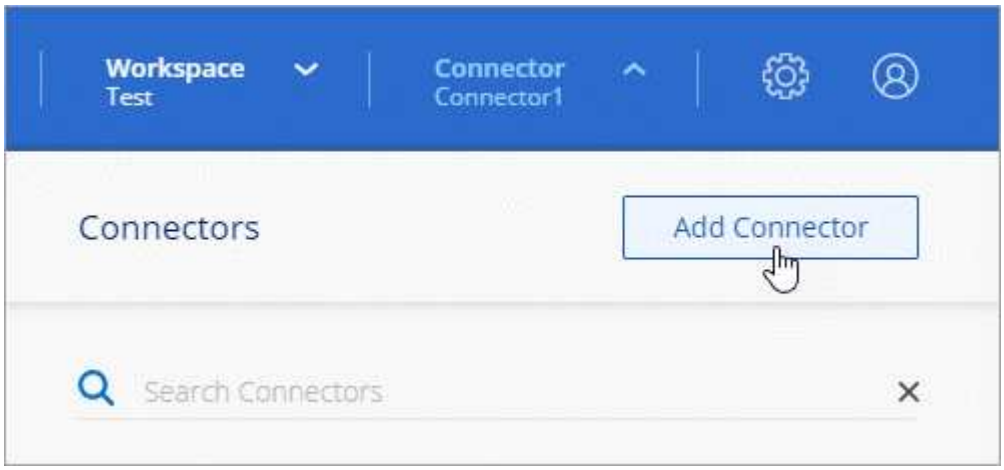
- Wenn Sie nicht möchten, dass BlueXP automatisch eine Azure-Rolle für den Connector erstellt, müssen

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

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

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

Azure Region

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

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

Vnet und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Outbound-Internetzugang

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

Vom Connector kontaktierte Endpunkte

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

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

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

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

Proxy-Server

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

- 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: Überprüfung der VM-Anforderungen

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

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Azure VM-Größe

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

Schritt 3: Berechtigungen einrichten

Sie haben folgende Möglichkeiten, Berechtigungen bereitzustellen:

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

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

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

   Beispiel

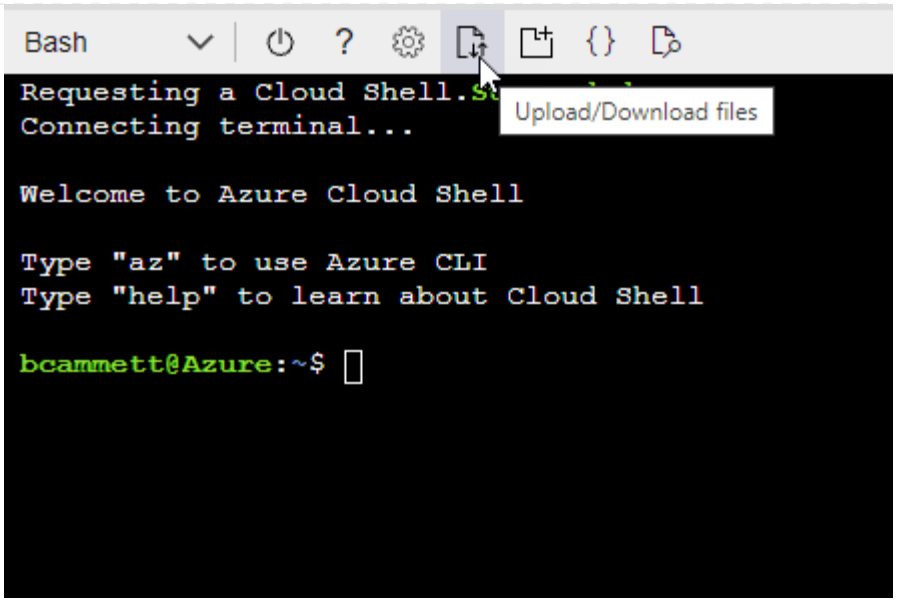
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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

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

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

   b. Laden Sie die JSON-Datei hoch.



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

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

Ergebnis

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

Service-Principal

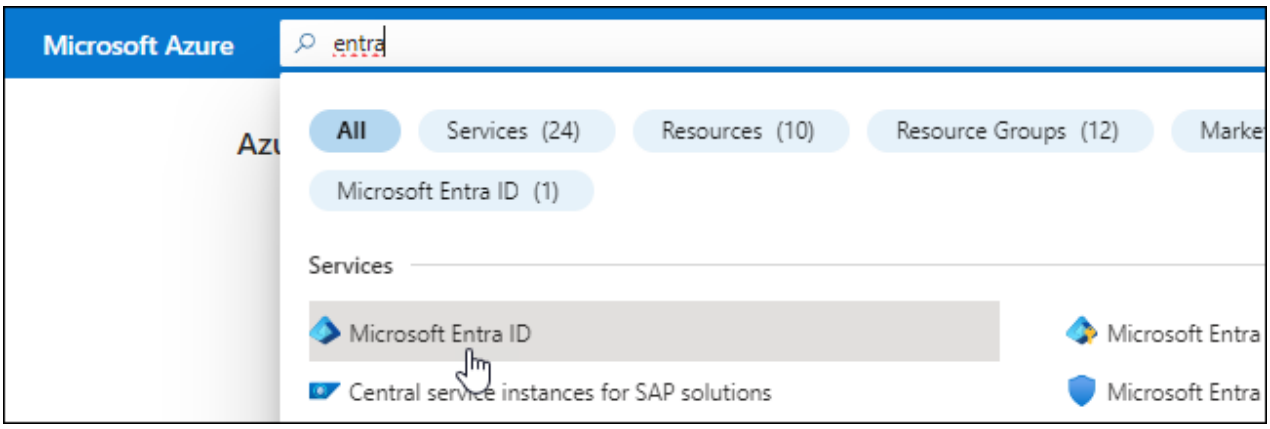
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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

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

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



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

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

Anwendung einer Rolle zuweisen

1. Erstellen einer benutzerdefinierten Rolle:

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

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

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

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

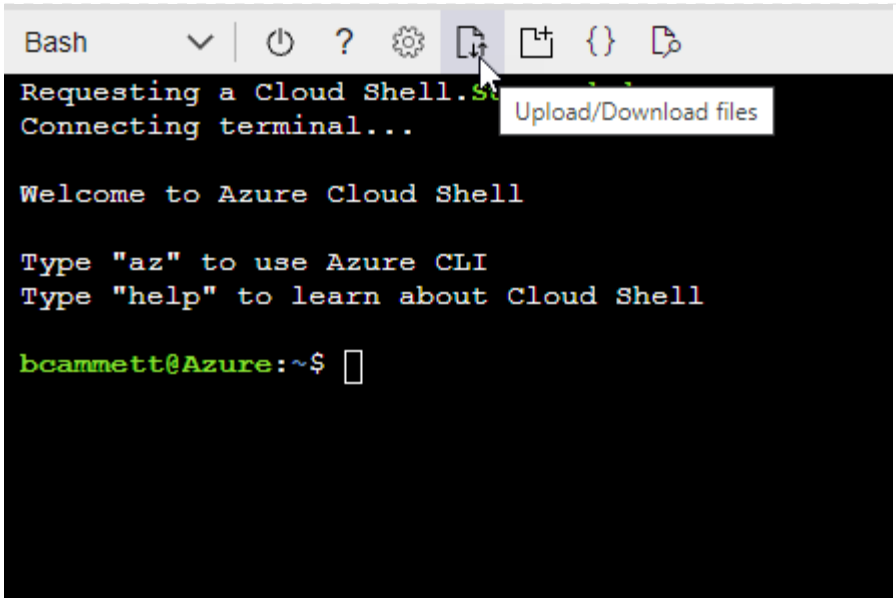
      Beispiel

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

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

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

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



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

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

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

2. Applikation der Rolle zuweisen:

   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.

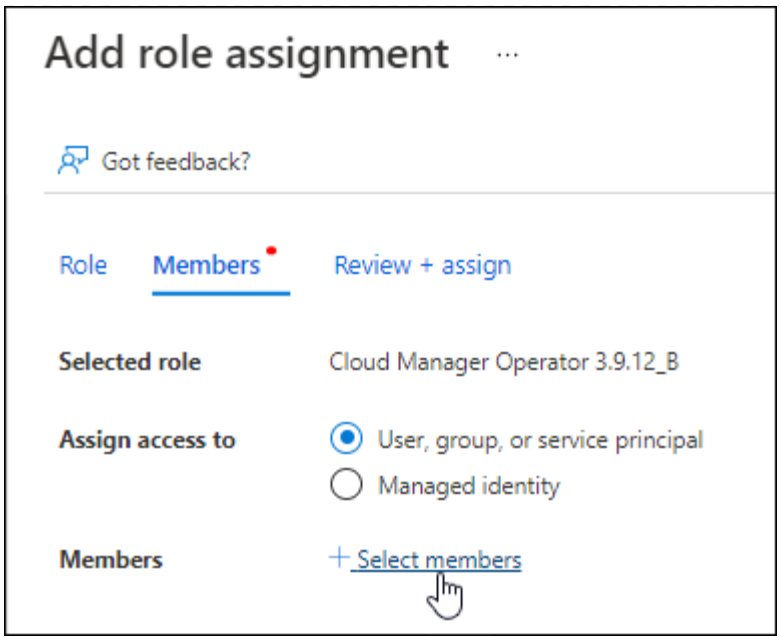
   b. Wählen Sie das Abonnement aus.

   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.

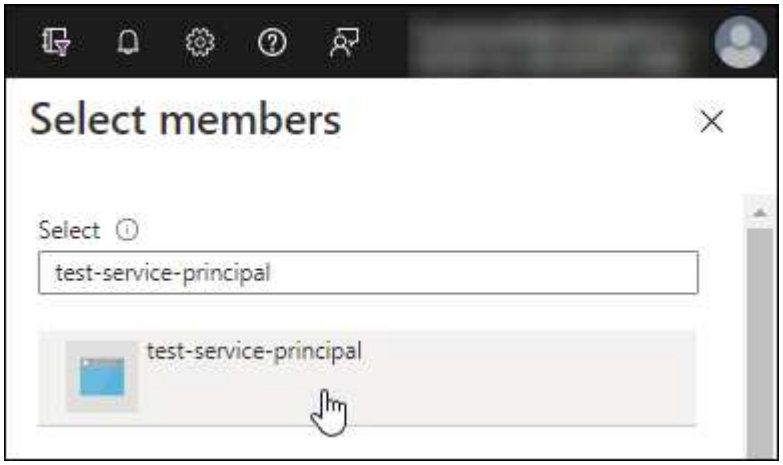
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ein Beispiel:



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

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

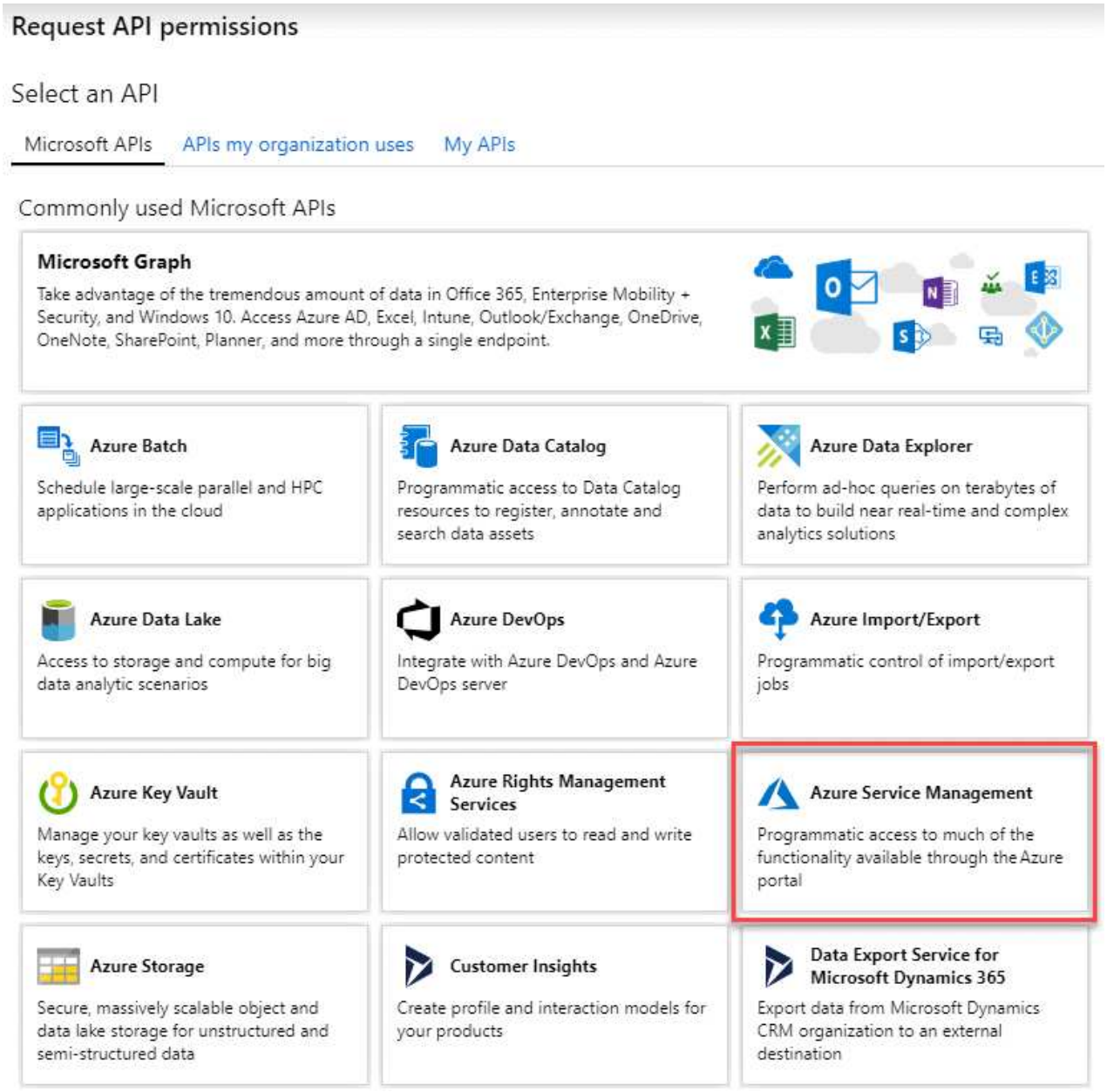
Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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

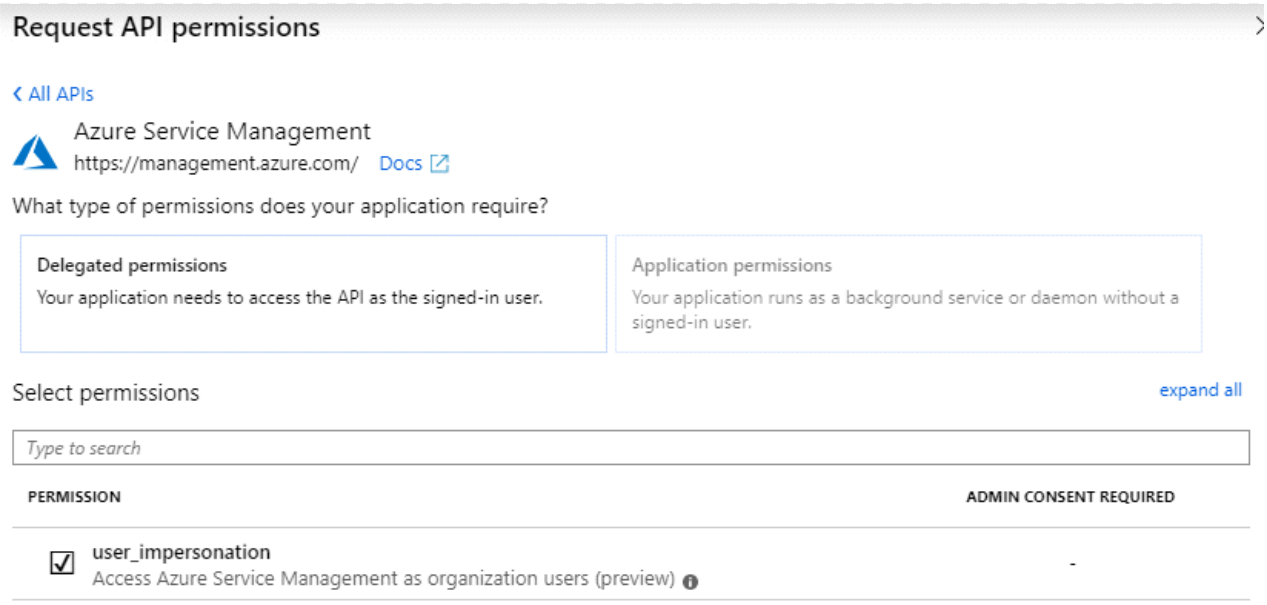
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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

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

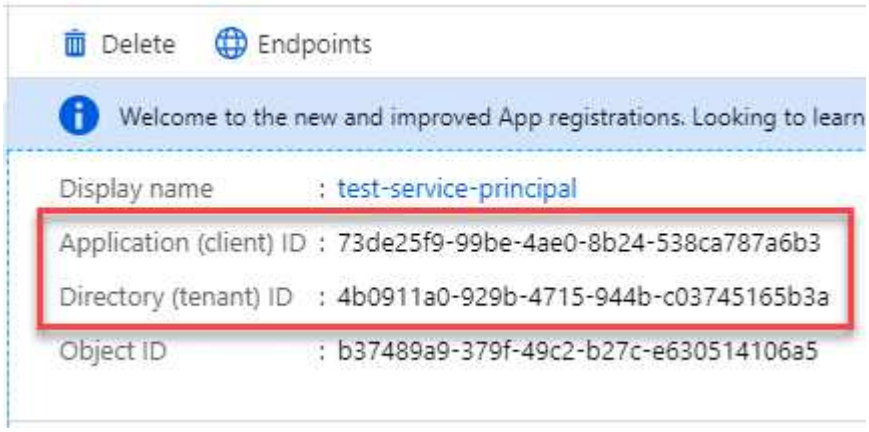


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen Sie einen Clientschlüssel

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

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

Ergebnis

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

Schritt 4: Erstellen Sie den Konnektor

Starten Sie den Connector direkt über den Azure Marketplace.

Über diese Aufgabe

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

Bevor Sie beginnen

Sie sollten Folgendes haben:

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

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

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

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

Schritte

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

"Azure Marketplace-Seite für kommerzielle Regionen"

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

   Beachten Sie beim Konfigurieren der VM Folgendes:

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

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

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

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

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

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

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

   https://ipaddress

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

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

   d. Wählen Sie **Start**.

Ergebnis

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

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

Schritt 5: Berechtigungen für BlueXP bereitstellen

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

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

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

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

Ergebnis

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

Was kommt als Nächstes?

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

Service-Principal

Schritte

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

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

Ergebnis

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

Installieren Sie den Connector manuell in Azure

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
    - 8.6 bis 8.10
    - 9.1 bis 9.3

      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 gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Azure VM-Größe

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

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

BlueXP nutzt `/opt` Um den zu installieren `/opt/application/netapp` Verzeichnis und es ist Inhalt.

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.

Container-Orchestrierungstool

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

- Podman Version 4.6.1 ist für Red hat Enterprise Linux 8 und 9 erforderlich.

  Für Podman müssen folgende Voraussetzungen erfüllt sein:

  - Der podman.Socket-Dienst muss aktiviert und gestartet werden
  - python3 muss installiert sein
  - Das Paket podman-compose Version 1.0.6 muss installiert sein
  - Podman-compose muss der Umgebungsvariable PATH hinzugefügt werden
- Docker Engine ist für Ubuntu erforderlich.
  - Die unterstützte Version ist mindestens 23.0.6.
  - Die maximal unterstützte Version ist 25.0.5.

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.
- Docker Engine ist für Ubuntu erforderlich.

Beispiel 2. Schritte

Podman

Installieren Sie Podman 4.6.1.

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-2:4.6.1
```

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:4.6.1
```

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

Installieren Sie eine Version der Docker Engine zwischen 23.0.6 und 25.0.5.

Schritte

1. Installieren Sie Die Docker Engine.

   "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 wurden während der manuellen Installation kontaktiert

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

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

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

Vom Connector kontaktierte Endpunkte

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

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

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

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

Proxy-Server

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

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

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

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

Benutzerdefinierte Rolle

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

Schritte

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

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

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

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

   Beispiel

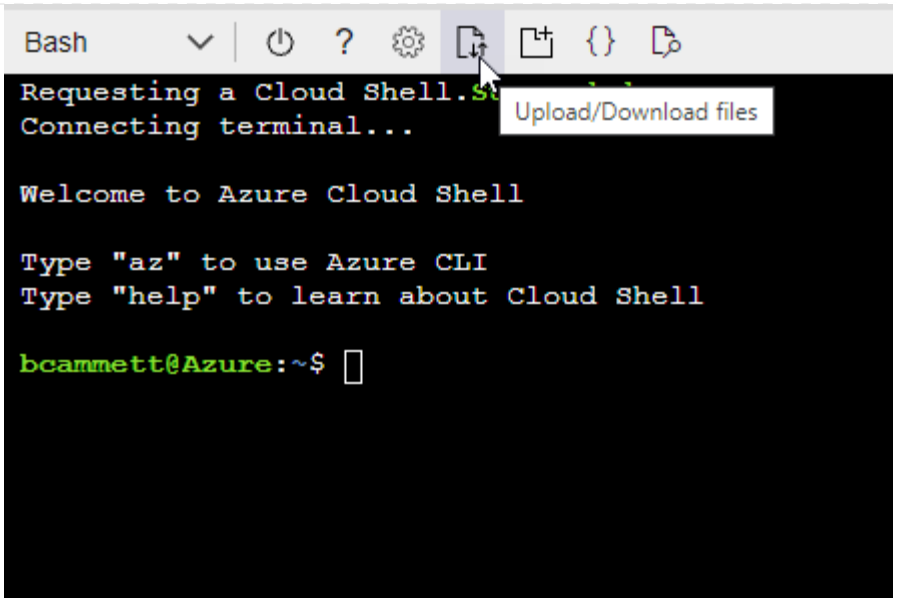
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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

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

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

   b. Laden Sie die JSON-Datei hoch.



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

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

Ergebnis

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

Service-Principal

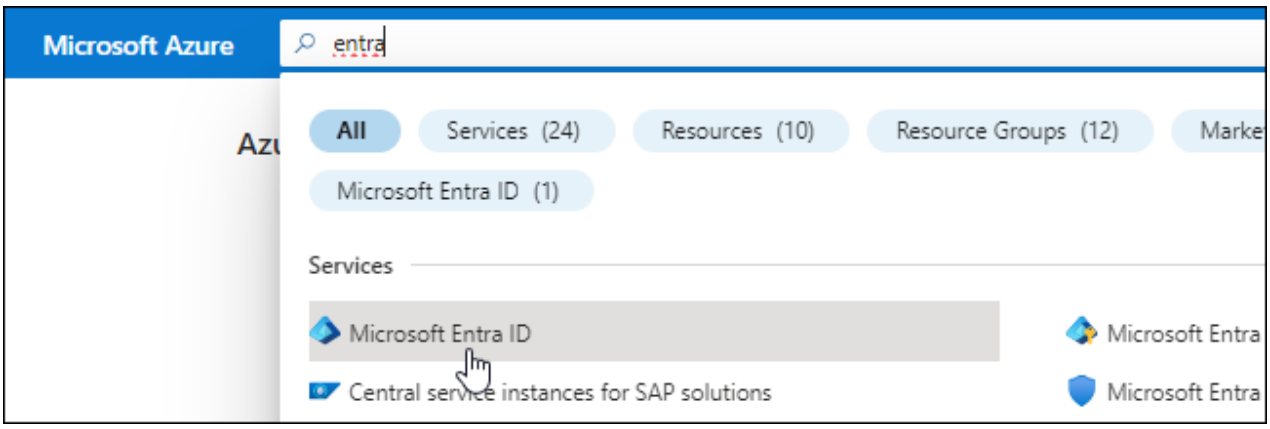
Ein Service-Principal in der Microsoft Entra ID erstellen und einrichten, um die für BlueXP erforderlichen Azure Zugangsdaten zu erhalten.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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

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

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



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

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

Anwendung einer Rolle zuweisen

1. Erstellen einer benutzerdefinierten Rolle:

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

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

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

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

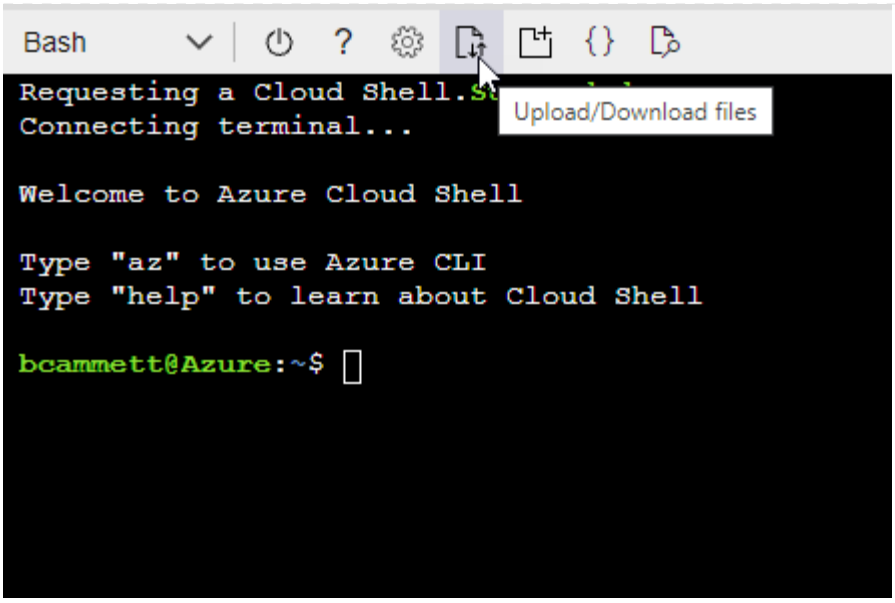
      Beispiel

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

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

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

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



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

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

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

2. Applikation der Rolle zuweisen:

   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.

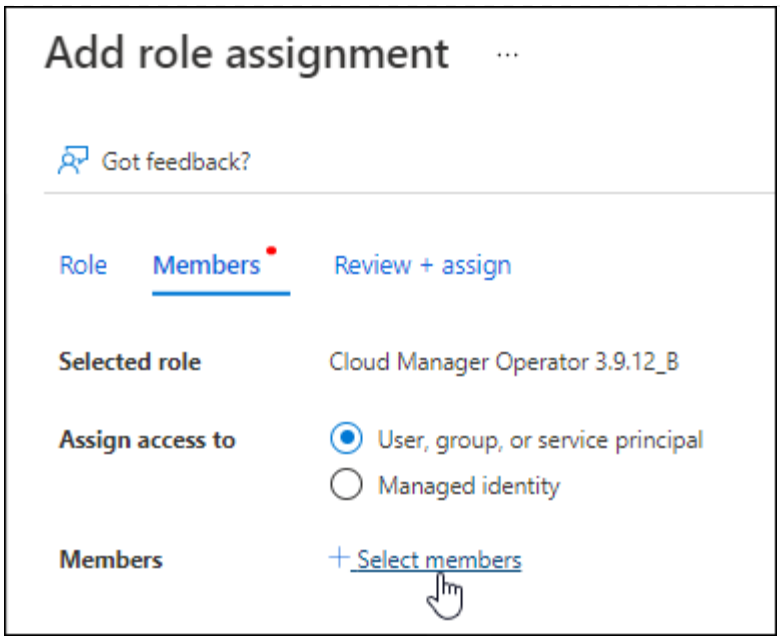
   b. Wählen Sie das Abonnement aus.

   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.

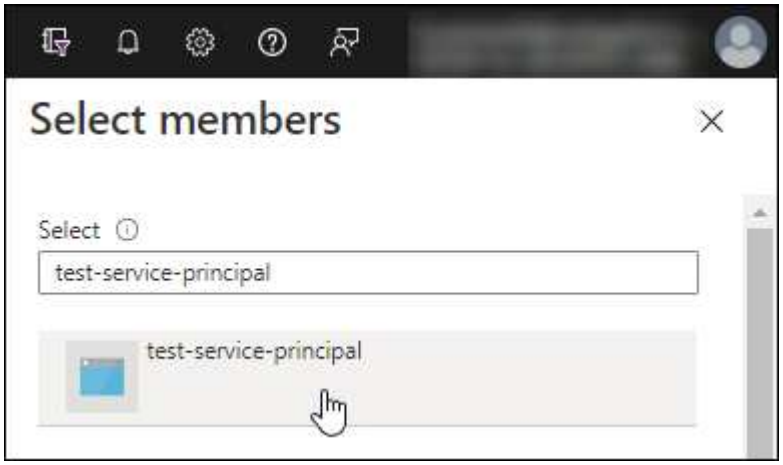
   e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ein Beispiel:



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

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

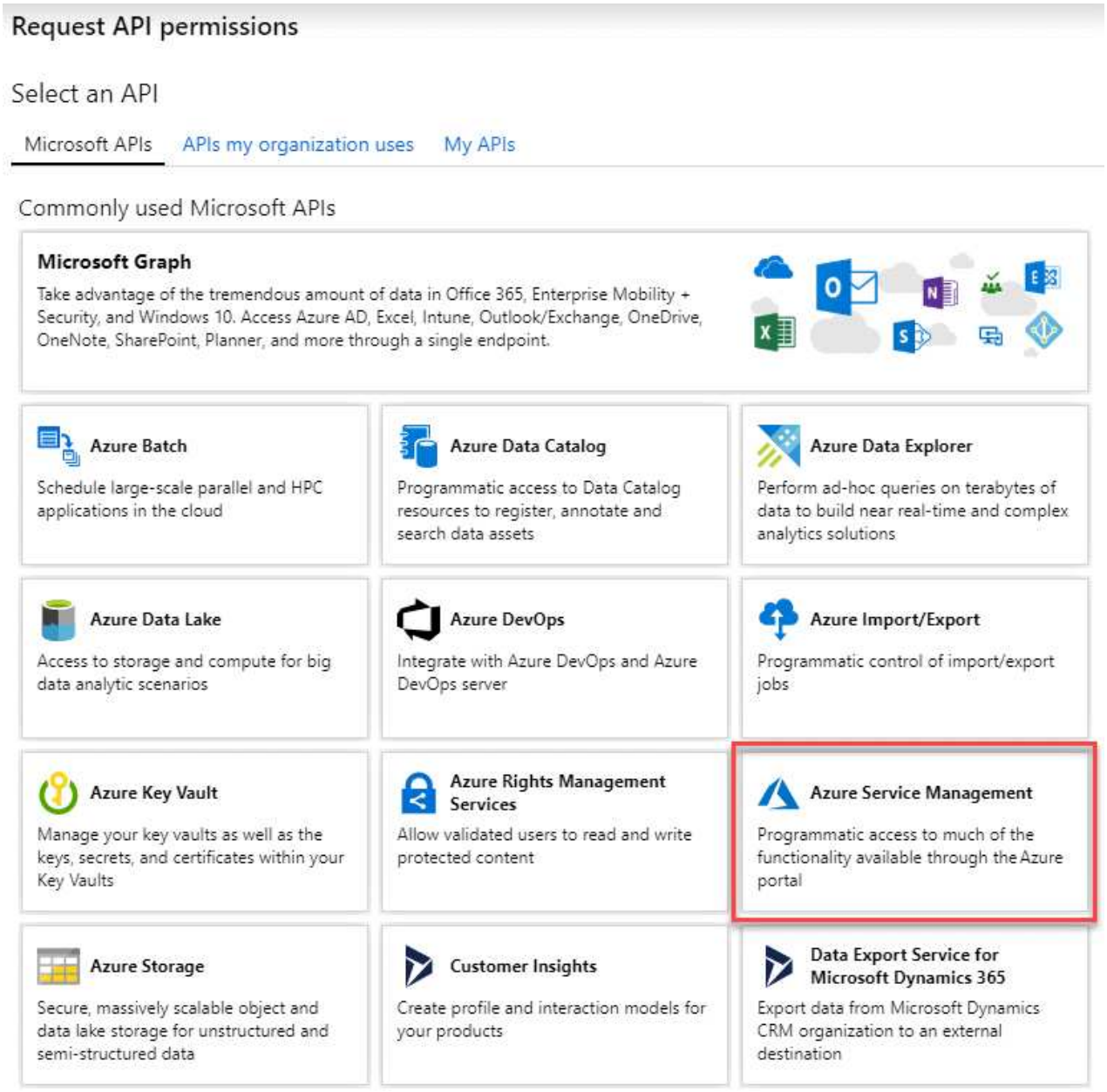
Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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

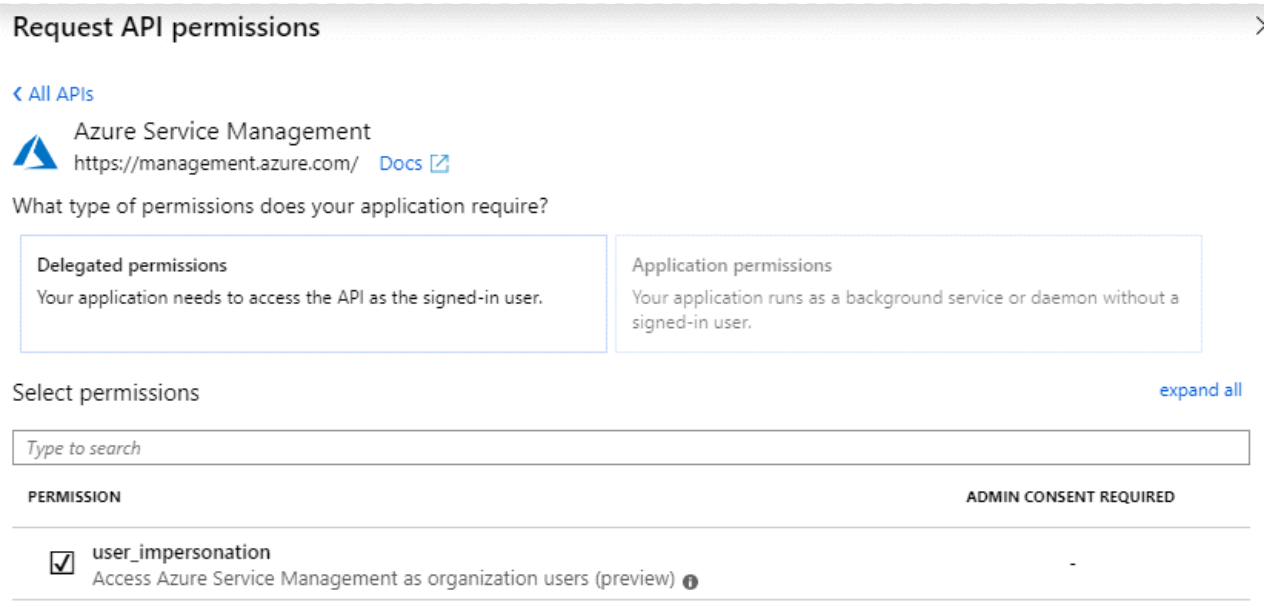
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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

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

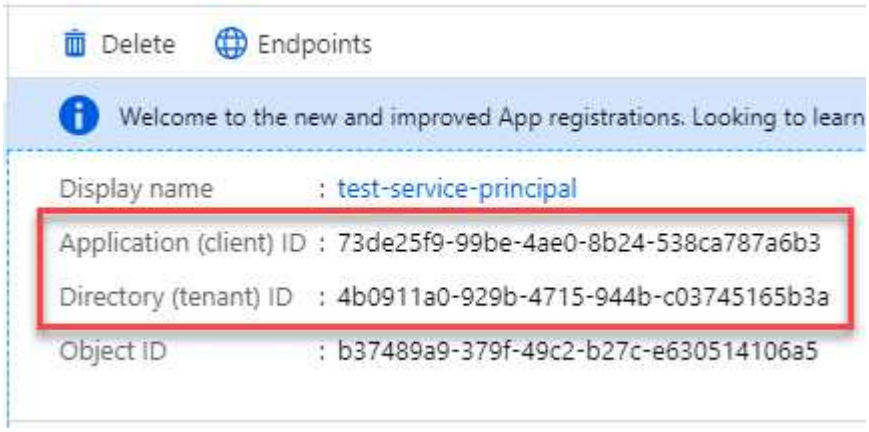


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen Sie einen Clientschlüssel

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

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

Ergebnis

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

Schritt 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.

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

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

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

Über diese Aufgabe

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

Schritte

1. 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 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-v3.9.40--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 nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

5. 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.

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

   https://ipaddress

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

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

   d. Wählen Sie **Start**.

Ergebnis

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

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

Schritt 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 gcloude erstellen

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt 1: Netzwerk einrichten

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

VPC und Subnetz

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

Verbindungen zu Zielnetzwerken

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

Outbound-Internetzugang

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

Vom Connector kontaktierte Endpunkte

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

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

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

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

Endpunkte wurden über die BlueXP Konsole kontaktiert

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

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

Proxy-Server

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

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

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

Schritte

1. Benutzerdefinierte Rolle in Google Cloud erstellen:

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

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

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

b. Aktivieren Sie in Google Cloud die Cloud Shell.

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

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

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

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

"Google Cloud docs: Erstellen und Verwalten benutzerdefinierter Rollen"

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

"Google Cloud docs: Gewähren Sie eine einzige Rolle"

Ergebnis

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

Schritt 3: Berechtigungen für den Connector einrichten

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

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.networkUser	Bereitstellen des Connectors im Serviceprojekt
Connector-Servicekonto	Individuell	Service-Projekt	"Kontorichtlinie für Connector-Service"	compute.networkUser 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.networkUser	Arbeitet im Auftrag der Implementierung mit Google Cloud APIs zusammen. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.
Google Compute Engine Standard-Servicekonto	Google Cloud	Service-Projekt	(Standard) Editor	compute.networkUser	Implementiert Google Cloud-Instanzen und Computing-Infrastrukturen im Auftrag der Implementierung. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.

Hinweise:

1. Wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen, ist encmentmanager.Editor nur beim Host-Projekt erforderlich. BlueXP erstellt eine Bereitstellung im Hostprojekt, die die VPC0-Firewall-Regel enthält, wenn keine Regel angegeben ist.
2. Firewall.create und firewall.delete sind nur erforderlich, wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen. Diese Berechtigungen liegen im BlueXP-Konto .yaml-Datei. Wenn Sie ein HA-Paar mithilfe eines gemeinsam genutzten VPC implementieren, werden diese Berechtigungen verwendet, um die Firewall-Regeln für VPC1, 2 und 3 zu erstellen. Für alle anderen Bereitstellungen werden diese Berechtigungen auch verwendet, um Regeln für VPC0 zu erstellen.
3. Für das Daten-Tiering muss das Tiering-Servicekonto die serviceAccount.user-Rolle auf dem Servicekonto haben, nicht nur auf Projektebene. Derzeit werden serviceAccount.user auf

Projektebene zugewiesen, wenn Sie das Servicekonto mit getIAMPolicy abfragen.

Schritt 5: Google Cloud APIs aktivieren

Bevor Sie den Connector und die Cloud Volumes ONTAP in Google Cloud bereitstellen können, müssen Sie mehrere Google Cloud APIs aktivieren.

Schritt

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

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

"Google Cloud-Dokumentation: Aktivieren von APIs"

Schritt 6: Erstellen Sie den Konnektor

Erstellen Sie einen Connector direkt über die webbasierte Konsole von BlueXP oder über gcloude.

Über diese Aufgabe

Beim Erstellen des Connectors wird eine Virtual Machine-Instanz in Google Cloud mit einer Standardkonfiguration bereitgestellt. Nachdem Sie den Connector erstellt haben, sollten Sie nicht zu einer kleineren VM-Instanz wechseln, die weniger CPU oder RAM hat. "Informieren Sie sich über die Standardkonfiguration des Connectors".

BlueXP

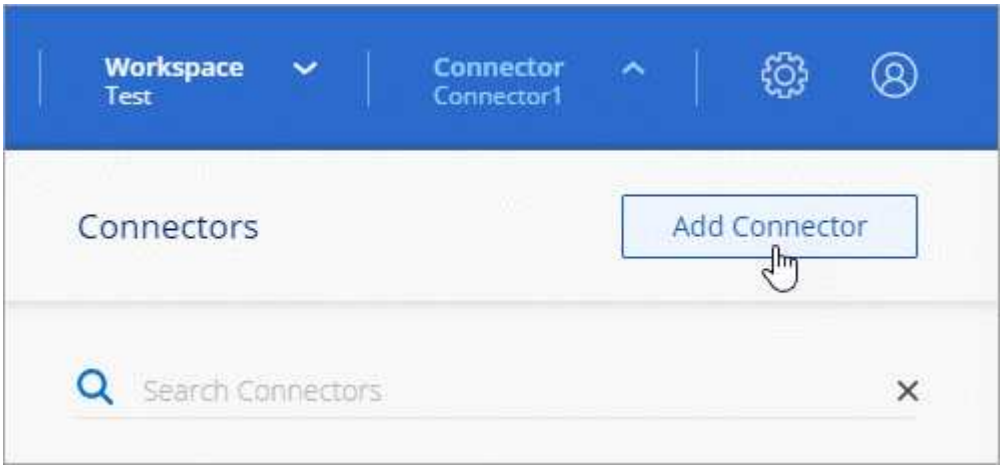
Bevor Sie beginnen

Sie sollten Folgendes haben:

- Die erforderlichen Google Cloud Berechtigungen, um den Connector und ein Servicekonto für die Connector VM zu erstellen.
- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

Schritte

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



2. Wählen Sie **Google Cloud Platform** als Cloud-Provider.
3. Lesen Sie auf der Seite **Bereitstellen eines Konnektors** die Details dazu, was Sie benötigen. Sie haben zwei Möglichkeiten:
   a. Wählen Sie **Weiter**, um die Bereitstellung mithilfe des Produktleitfadens vorzubereiten. Jeder Schritt im Produktleitfaden enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.
   b. Wählen Sie **Skip to Deployment**, wenn Sie bereits vorbereitet haben, indem Sie die Schritte auf dieser Seite befolgen.
4. Befolgen Sie die Schritte im Assistenten, um den Konnektor zu erstellen:
   - Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Google-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der virtuellen Maschineninstanz verfügen sollte.

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

   - **Details**: Geben Sie einen Namen für die virtuelle Maschineninstanz ein, geben Sie Tags an, wählen Sie ein Projekt aus, und wählen Sie dann das Servicekonto aus, das über die erforderlichen Berechtigungen verfügt (Details finden Sie im Abschnitt oben).
   - **Ort**: Geben Sie eine Region, Zone, VPC und Subnetz für die Instanz an.
   - **Netzwerk**: Wählen Sie, ob eine öffentliche IP-Adresse aktiviert werden soll und geben Sie optional eine Proxy-Konfiguration an.

- **Firewallrichtlinie**: Wählen Sie aus, ob eine neue Firewallrichtlinie erstellt werden soll oder ob eine vorhandene Firewallrichtlinie ausgewählt werden soll, die die erforderlichen ein- und ausgehenden Regeln zulässt.

  "Firewall-Regeln in Google Cloud"

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

5. Wählen Sie **Hinzufügen**.

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

Ergebnis

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

Wenn sich in demselben Google Cloud-Konto, bei dem der Connector erstellt wurde, Google Cloud Storage-Buckets befinden, wird automatisch eine Arbeitsumgebung von Google Cloud Storage auf dem BlueXP-Bildschirm angezeigt. "Erfahren Sie, wie Sie Google Cloud Storage von BlueXP managen"

GCloud

Bevor Sie beginnen

Sie sollten Folgendes haben:

- Die erforderlichen Google Cloud Berechtigungen, um den Connector und ein Servicekonto für die Connector VM zu erstellen.
- Ein VPC und ein Subnetz, das die Netzwerkanforderungen erfüllt
- Informationen über die Anforderungen der VM-Instanz.
  - **CPU**: 4 Kerne oder 4 vCPUs
  - **RAM**: 14 GB
  - **Maschinentyp**: Wir empfehlen n2-Standard-4.

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

Schritte

1. Melden Sie sich am gCloud SDK mit Ihrer bevorzugten Methode an.

   In unseren Beispielen verwenden wir eine lokale Shell mit installiertem gCloud SDK, aber Sie könnten die native Google Cloud Shell in der Google Cloud-Konsole verwenden.

   Weitere Informationen zum Google Cloud SDK finden Sie auf der "Dokumentationsseite für Google Cloud SDK".

2. Stellen Sie sicher, dass Sie als Benutzer angemeldet sind, der über die erforderlichen Berechtigungen verfügt, die im Abschnitt oben definiert sind:

   ```
   gcloud auth list
   ```

   Die Ausgabe sollte Folgendes anzeigen, wobei das * -Benutzerkonto das gewünschte Benutzerkonto

ist, das angemeldet werden soll:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Führen Sie die aus `gcloud compute instances create` Befehl:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

Instanzname
: Der gewünschte Instanzname für die VM-Instanz.

Projekt
: (Optional) das Projekt, in dem die VM implementiert werden soll.

Service-Konto
: Das in der Ausgabe von Schritt 2 angegebene Servicekonto.

Zone
: Der Zone, in der die VM implementiert werden soll

Keine Adresse
: (Optional) Es wird keine externe IP-Adresse verwendet (Sie benötigen eine Cloud NAT oder einen Proxy, um den Datenverkehr zum öffentlichen Internet zu leiten).

Network-Tag

(Optional) Fügen Sie das Netzwerk-Tagging hinzu, um eine Firewall-Regel mithilfe von Tags zur Connector-Instanz zu verknüpfen

Netzwerkpfad

(Optional) Fügen Sie den Namen des Netzwerks hinzu, in dem der Connector bereitgestellt werden soll (für eine gemeinsame VPC benötigen Sie den vollständigen Pfad).

Subnetz-Pfad

(Optional) Fügen Sie den Namen des Subnetzes hinzu, in dem der Connector bereitgestellt werden soll (für eine freigegebene VPC benötigen Sie den vollständigen Pfad)

Km-Schlüsselpfad

(Optional) Hinzufügen eines KMS-Schlüssels zur Verschlüsselung der Festplatten des Connectors (IAM-Berechtigungen müssen auch angewendet werden)

Weitere Informationen zu diesen Flaggen finden Sie im "Dokumentation des Google Cloud Compute SDK".

+
Wenn der Befehl ausgeführt wird, wird der Connector mit dem Golden Image von NetApp implementiert. Die Connector-Instanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

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

   https://ipaddress

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

      "Mehr zu BlueXP Accounts".

   b. Geben Sie einen Namen für das System ein.

Ergebnis

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

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

Installieren Sie den Connector manuell in Google Cloud

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

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

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

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6 bis 8.10
  - 9.1 bis 9.3

    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 gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Google Cloud-Maschinentyp

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

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

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

BlueXP nutzt `/opt` Um den zu installieren `/opt/application/netapp` Verzeichnis und es ist Inhalt.

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.

Container-Orchestrierungstool

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

- Podman Version 4.6.1 ist für Red hat Enterprise Linux 8 und 9 erforderlich.

  Für Podman müssen folgende Voraussetzungen erfüllt sein:

  - Der podman.Socket-Dienst muss aktiviert und gestartet werden
  - python3 muss installiert sein
  - Das Paket podman-compose Version 1.0.6 muss installiert sein
  - Podman-compose muss der Umgebungsvariable PATH hinzugefügt werden
- Docker Engine ist für Ubuntu erforderlich.
  - Die unterstützte Version ist mindestens 23.0.6.
  - Die maximal unterstützte Version ist 25.0.5.

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.
- Docker Engine ist für Ubuntu erforderlich.

Beispiel 3. Schritte

Podman

Installieren Sie Podman 4.6.1.

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-2:4.6.1
```

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:4.6.1
```

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

Installieren Sie eine Version der Docker Engine zwischen 23.0.6 und 25.0.5.

Schritte

1. Installieren Sie Die Docker Engine.

   "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 wurden während der manuellen Installation kontaktiert

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

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

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

Vom Connector kontaktierte Endpunkte

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

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

Endpunkte	Zweck
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Zum Managen von Ressourcen in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.

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

Proxy-Server

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

- 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.networkUser	Bereitstellen des Connectors im Serviceprojekt
Connector-Servicekonto	Individuell	Service-Projekt	"Kontorichtlinie für Connector-Service"	compute.networkUser 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.networkUser	Arbeitet im Auftrag der Implementierung mit Google Cloud APIs zusammen. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.
Google Compute Engine Standard-Servicekonto	Google Cloud	Service-Projekt	(Standard) Editor	compute.networkUser	Implementiert Google Cloud-Instanzen und Computing-Infrastrukturen im Auftrag der Implementierung. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.

Hinweise:

1. Wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen, ist encmentmanager.Editor nur beim Host-Projekt erforderlich. BlueXP erstellt eine Bereitstellung im Hostprojekt, die die VPC0-Firewall-Regel enthält, wenn keine Regel angegeben ist.
2. Firewall.create und firewall.delete sind nur erforderlich, wenn Sie Firewall-Regeln nicht an die Bereitstellung übergeben und BlueXP diese für Sie erstellen lassen. Diese Berechtigungen liegen im BlueXP-Konto .yaml-Datei. Wenn Sie ein HA-Paar mithilfe eines gemeinsam genutzten VPC implementieren, werden diese Berechtigungen verwendet, um die Firewall-Regeln für VPC1, 2 und 3 zu erstellen. Für alle anderen Bereitstellungen werden diese Berechtigungen auch verwendet, um Regeln für VPC0 zu erstellen.
3. Für das Daten-Tiering muss das Tiering-Servicekonto die serviceAccount.user-Rolle auf dem Servicekonto haben, nicht nur auf Projektebene. Derzeit werden serviceAccount.user auf

Projektebene zugewiesen, wenn Sie das Servicekonto mit getIAMPolicy abfragen.

Schritt 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.

  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. 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 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-v3.9.40--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 nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

5. 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.

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

   https://ipaddress

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

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

   d. Wählen Sie **Start**.

Ergebnis

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

Wenn sich in demselben Google Cloud-Konto, bei dem der Connector erstellt wurde, Google Cloud Storage-Buckets befinden, wird automatisch eine Arbeitsumgebung von Google Cloud Storage auf dem BlueXP-Bildschirm angezeigt. "Erfahren Sie, wie Sie Google Cloud Storage von BlueXP managen"

Schritt 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 auf dem Gelände

Installieren Sie einen Connector vor Ort, melden Sie sich anschließend an und richten Sie ihn für die Nutzung mit Ihrem BlueXP Konto ein.

Bevor Sie beginnen

Sie sollten es überprüfen "Einschränkungen an den Anschlüssen".

Schritt: Überprüfung der Host-Anforderungen

Die Connector-Software muss auf einem Host ausgeführt werden, der bestimmte Betriebssystemanforderungen, RAM-Anforderungen, Port-Anforderungen usw. erfüllt. Stellen Sie sicher, dass Ihr Host diese Anforderungen erfüllt, bevor Sie den Connector installieren.

Dedizierter Host

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

Unterstützte Betriebssysteme

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6 bis 8.10
  - 9.1 bis 9.3

    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 gehosteter Hypervisor, der für die Ausführung eines unterstützten Betriebssystems zertifiziert ist, ist erforderlich.

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

BlueXP nutzt `/opt` Um den zu installieren `/opt/application/netapp` Verzeichnis und es ist Inhalt.

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.

Container-Orchestrierungstool

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

- Podman Version 4.6.1 ist für Red hat Enterprise Linux 8 und 9 erforderlich.

  Für Podman müssen folgende Voraussetzungen erfüllt sein:

  - Der podman.Socket-Dienst muss aktiviert und gestartet werden
  - python3 muss installiert sein
  - Das Paket podman-compose Version 1.0.6 muss installiert sein
  - Podman-compose muss der Umgebungsvariable PATH hinzugefügt werden
- Docker Engine ist für Ubuntu erforderlich.
  - Die unterstützte Version ist mindestens 23.0.6.
  - Die maximal unterstützte Version ist 25.0.5.

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.
- Docker Engine ist für Ubuntu erforderlich.

Beispiel 4. Schritte

Podman

Installieren Sie Podman 4.6.1.

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-2:4.6.1
```

   Für Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:4.6.1
```

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

Installieren Sie eine Version der Docker Engine zwischen 23.0.6 und 25.0.5.

Schritte

1. Installieren Sie Die Docker Engine.

   "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 wurden während der manuellen Installation kontaktiert

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

URLs:

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

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

Vom Connector kontaktierte Endpunkte

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

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

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Managen von Ressourcen in AWS. Der genaue Endpunkt hängt von der von Ihnen verwendeten AWS-Region ab. "Details finden Sie in der AWS-Dokumentation"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Für das Managen von Ressourcen in Azure Public Regionen.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Für das Management von Ressourcen in Azure China Regionen.

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. Beachten Sie, dass der Connector sich derzeit mit „cloudmanager.cloud.netapp.com" in Verbindung setzt, jedoch in einer kommenden Version mit „api.bluexp.netapp.com"“ in Verbindung steht.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Aktualisierung des Connectors und seiner Docker Komponenten.

Proxy-Server

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

- 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. Der Connector muss in Google Cloud installiert sein, um alle dort residieren zu managen.

AWS

Wenn der Connector vor Ort installiert ist, müssen Sie BlueXP mit AWS Berechtigungen versehen, indem Sie Zugriffsschlüssel für einen IAM-Benutzer mit den erforderlichen Berechtigungen hinzufügen.

Sie müssen diese Authentifizierungsmethode verwenden, wenn der Connector vor Ort installiert ist. Sie können keine IAM-Rolle verwenden.

Schritte

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

   a. Wählen Sie **Policies > Create Policy** aus.

   b. Wählen Sie **JSON** aus, kopieren Sie den Inhalt des "IAM-Richtlinie für den Connector".

   c. Beenden Sie die verbleibenden Schritte, um die Richtlinie zu erstellen.

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

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

3. Fügen Sie die Richtlinien einem IAM-Benutzer hinzu.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"
4. Stellen Sie sicher, dass der Benutzer über einen Zugriffsschlüssel verfügt, den Sie nach der Installation des Connectors zu BlueXP hinzufügen können.

Ergebnis

Sie sollten nun über Zugriffsschlüssel für einen IAM-Benutzer verfügen, der über die erforderlichen Berechtigungen verfügt. Nach der Installation des Connectors müssen Sie diese Anmeldeinformationen mit dem Connector von BlueXP verknüpfen.

Azure

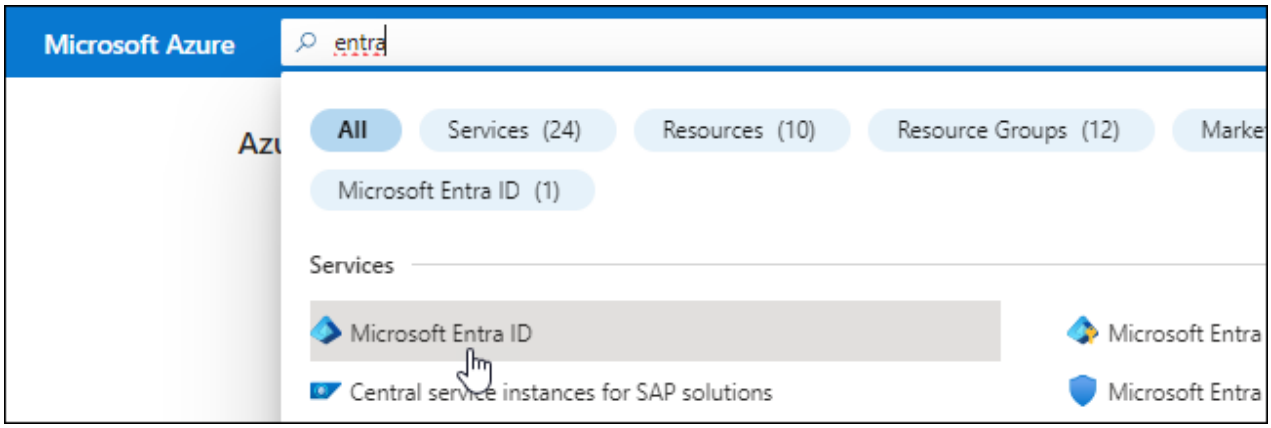
Wenn der Connector vor Ort installiert ist, müssen Sie BlueXP mit Azure-Berechtigungen versehen, indem Sie einen Service-Prinzipal in der Microsoft Entra-ID einrichten und die für BlueXP erforderlichen Azure-Berechtigungen erhalten.

Erstellen Sie eine Microsoft Entra-Anwendung für die rollenbasierte Zugriffssteuerung

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

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

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



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

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

Anwendung einer Rolle zuweisen

1. Erstellen einer benutzerdefinierten Rolle:

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

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

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

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

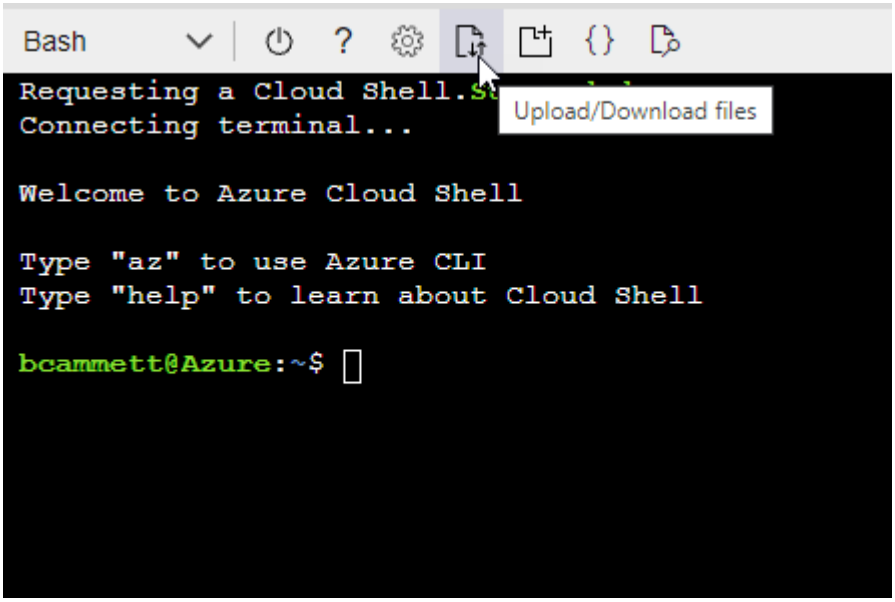
      Beispiel

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

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

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

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



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

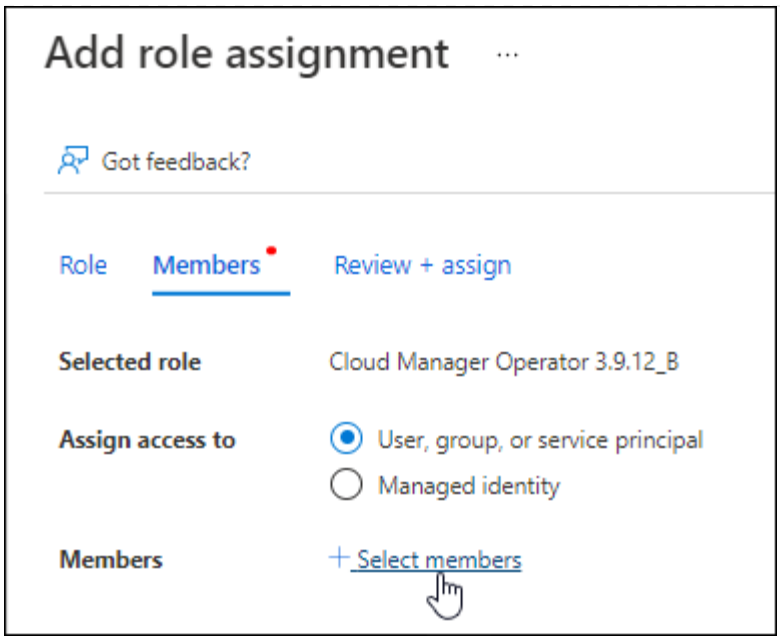
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Applikation der Rolle zuweisen:

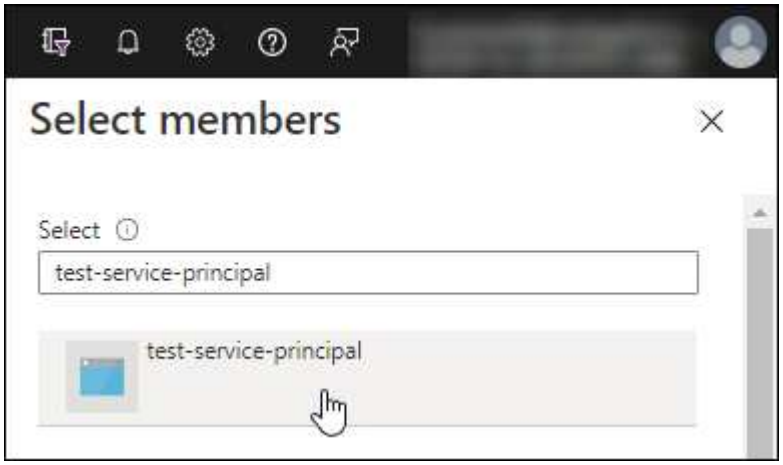
   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
   b. Wählen Sie das Abonnement aus.
   c. Wählen Sie **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
   d. Wählen Sie auf der Registerkarte **role** die Rolle **BlueXP Operator** aus und wählen Sie **Next** aus.
   e.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

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



- Suchen Sie nach dem Namen der Anwendung.

  Hier ein Beispiel:



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

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

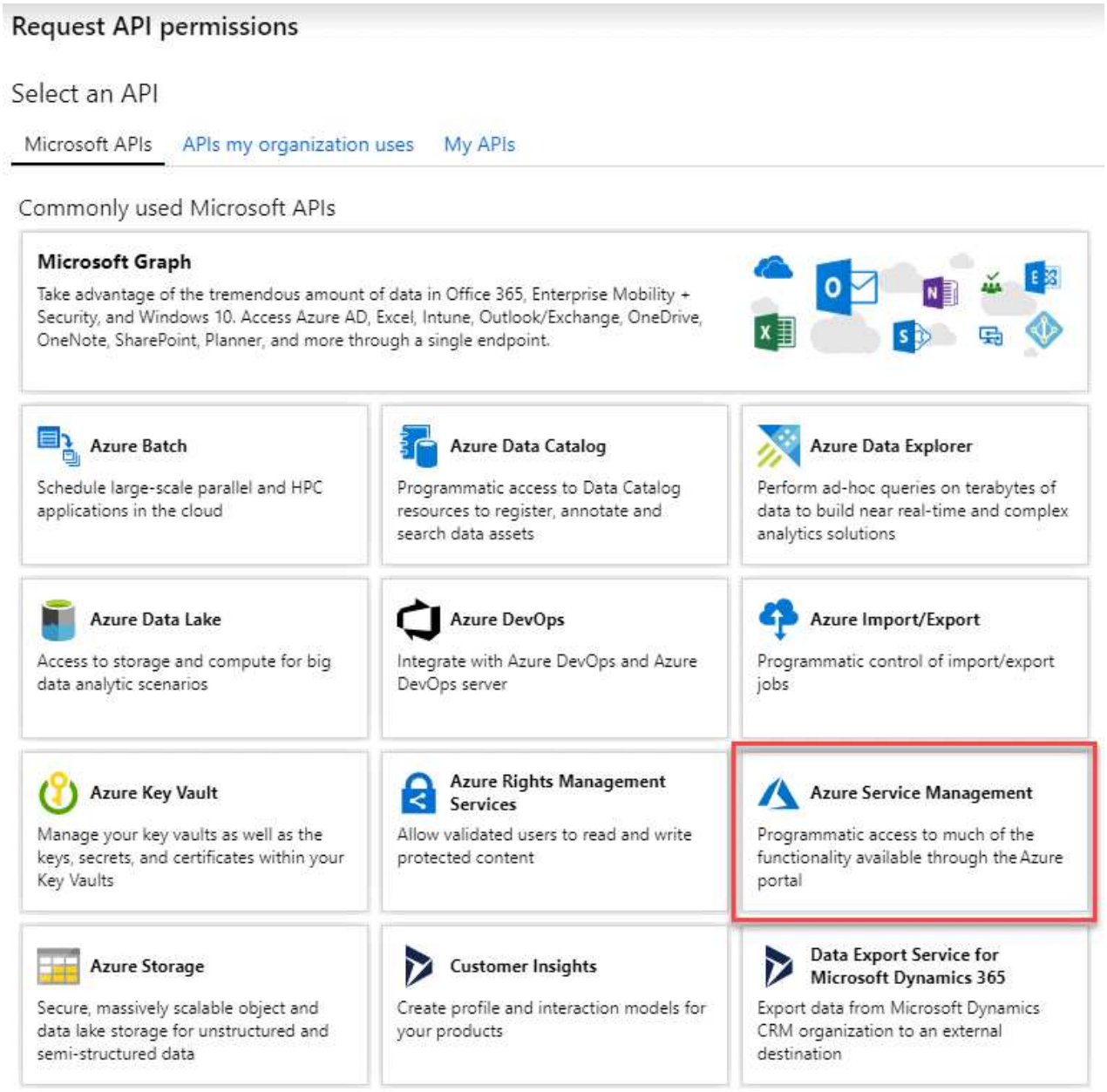
Der Service-Principal verfügt jetzt über die erforderlichen Azure-Berechtigungen zur Bereitstellung des Connectors.

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

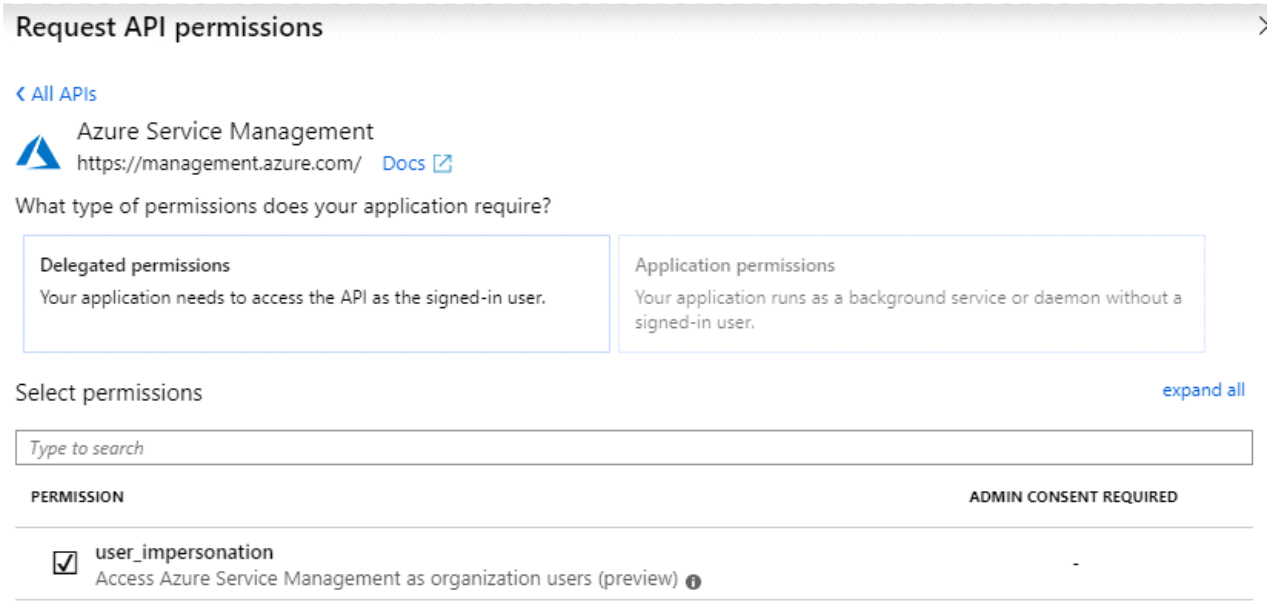
Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

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

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

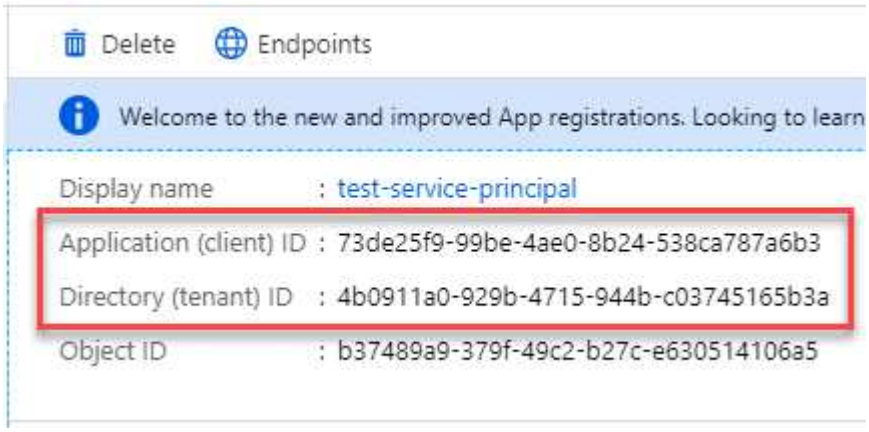


4. Wählen Sie **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann **Berechtigungen hinzufügen**.



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

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



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

Erstellen Sie einen Clientschlüssel

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

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

Ergebnis

Ihr Service-Principal ist jetzt eingerichtet und Sie sollten die Anwendungs- (Client-)ID, die Verzeichnis- (Mandanten-)ID und den Wert des Clientgeheimnisses kopiert haben. Nach der Installation des Connectors müssen Sie diese Anmeldeinformationen mit dem Connector von BlueXP verknüpfen.

Schritt 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.

  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. 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 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-v3.9.40--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 nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben oder wenn der Proxy ein abfangenden Proxy ist.

Ergebnis

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

Schritt 6: Richten Sie den Connector ein

Melden Sie sich an, oder melden Sie sich an, und richten Sie den Connector dann für die Arbeit mit Ihrem BlueXP Konto ein.

Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

   https://ipaddress

   Ipaddress kann abhängig von der Konfiguration des Hosts localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Connector beispielsweise ohne öffentliche IP-Adresse in der Public Cloud befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-Host hat.

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

      Sie sollten den eingeschränkten Modus deaktiviert halten, da nachfolgend beschrieben wird, wie Sie BlueXP im Standardmodus verwenden. (Außerdem wird der eingeschränkte Modus nicht unterstützt, wenn der Connector vor Ort installiert ist.)

   d. Wählen Sie **Start**.

Ergebnis

BlueXP ist jetzt mit dem Connector eingerichtet, den Sie gerade installiert haben.

Schritt 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 Anmeldedaten gerade in AWS erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

Schritte

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

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

Ergebnis

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

Sie können jetzt die öffnen "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.

Azure

Bevor Sie beginnen

Wenn Sie diese Anmeldedaten gerade in Azure erstellt haben, kann es ein paar Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

Schritte

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

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

- ID des Verzeichnisses (Mandant)
- Client-Schlüssel

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

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

Ergebnis

BlueXP verfügt jetzt über die Berechtigungen, die es für Sie zum Ausführen von Aktionen in Azure benötigt. Sie können jetzt die öffnen "BlueXP-Konsole" Um den Connector mit BlueXP zu verwenden.