



# **Richten Sie einen Konnektor ein**

## **Set up and administration**

NetApp

December 15, 2022

# Inhaltsverzeichnis

- Richten Sie einen Konnektor ein ..... 1
  - Erfahren Sie mehr über Steckverbinder ..... 1
  - Erstellen Sie einen Connector in AWS von BlueXP ..... 5
  - Erstellen Sie einen Connector in Azure von BlueXP ..... 12
  - Erstellen Sie einen Connector in Google Cloud von BlueXP ..... 28
  - Einen Konnektor in einer Regierungsregion erstellen ..... 41

# Richten Sie einen Konnektor ein

## Erfahren Sie mehr über Steckverbinder

In den meisten Fällen muss ein BlueXP Account Admin einen *Connector* in Ihrer Cloud oder Ihrem On-Premises-Netzwerk bereitstellen. Der Connector ist eine entscheidende Komponente für die tägliche Nutzung von BlueXP. BlueXP kann die Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung verwalten.

### Wenn ein Stecker erforderlich ist

Für die Nutzung vieler Funktionen und Services in BlueXP ist ein Connector erforderlich.

#### Services

- Managementfunktionen von Amazon FSX für ONTAP
- Ermittlung von Amazon S3
- Azure Blob-Erkennung
- Cloud-Backup
- Cloud-Daten Sinnvoll
- Cloud Tiering
- Cloud Volumes ONTAP
- E-Series Systeme
- Globaler Datei-Cache
- Erkennung von Google Cloud Storage
- Kubernetes-Cluster
- On-Premises ONTAP Cluster
- StorageGRID

Für die folgenden Dienste ist ein Connector **Not** erforderlich:

- Digital Advisor
- Amazon FSX für die Erstellung von Arbeitsumgebungen durch ONTAP Obwohl für die Erstellung eines Connectors keine Arbeitsumgebung erforderlich ist, müssen Volumes erstellt und gemanagt, Daten repliziert und FSX für ONTAP in NetApp Cloud-Services wie Data Sense und Cloud Sync integriert werden.
- Azure NetApp Dateien

Während kein Connector für die Einrichtung und Verwaltung von Azure NetApp Files erforderlich ist, ist für die Überprüfung von Azure NetApp Files-Daten ein Connector erforderlich.

- Cloud Volumes Service für Google Cloud
- Cloud-Synchronisierung

## Digital Wallet

In fast allen Fällen können Sie eine Lizenz für das Digital Wallet ohne Connector hinzufügen.

Der einzige Zeitpunkt, zu dem ein Konnektor erforderlich ist, um eine Lizenz zum digitalen Wallet hinzuzufügen, sind Cloud Volumes ONTAP\_Node-basierte\_-Lizenzen. In diesem Fall ist ein Connector erforderlich, da die Daten aus den auf Cloud Volumes ONTAP-Systemen installierten Lizenzen stammen.

## Unterstützte Standorte

Ein Connector wird an folgenden Stellen unterstützt:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Vor Ort
- In Ihrem Haus, ohne Internetzugang

## Hinweis zu Azure Implementierungen

Wenn Sie den Connector in Azure implementieren, sollte er in derselben Azure-Region wie die Cloud Volumes ONTAP-Systeme, die er managt, oder in 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"](#).

## Hinweis zu Google Cloud-Bereitstellungen

Wenn Sie ein Cloud Volumes ONTAP-System in Google Cloud erstellen möchten, dann müssen Sie über einen Connector verfügen, der auch in Google Cloud läuft. Es kann kein Connector verwendet werden, der in AWS, Azure oder lokal ausgeführt wird.

## Anschlüsse sollten weiterhin ausgeführt werden

Ein Steckverbinder sollte immer weiter laufen. Es ist wichtig für den fortwährenden Zustand und Betrieb der Services, die Sie ermöglichen.

Ein Connector ist beispielsweise eine wichtige Komponente im Zustand und Betrieb von Cloud Volumes ONTAP. Wenn ein Connector heruntergefahren wird, werden Cloud Volumes ONTAP PAYGO-Systeme und kapazitätsbasierte BYOL-Systeme heruntergefahren, nachdem die Kommunikation mit einem Connector über einen Zeitraum von mehr als 14 Tagen unterbrochen wurde. Dies geschieht, weil der Connector jeden Tag die Lizenzierung auf dem System aktualisiert.



Wenn Ihr Cloud Volumes ONTAP System über eine Node-basierte BYOL-Lizenz verfügt, wird das System nach 14 Tagen weiter ausgeführt, da die Lizenz auf dem Cloud Volumes ONTAP System installiert wird.

## So erstellen Sie einen Konnektor

Ein BlueXP-Kontoadministrator kann auf verschiedene Arten einen Connector erstellen:

- Direkt von BlueXP (empfohlen)

- ["In AWS erstellen"](#)
- ["In Azure erstellen"](#)
- ["In GCP erstellen"](#)
- Durch manuelle Installation der Software auf Ihrem eigenen Linux-Host
  - ["Auf einem Host mit Internetzugang"](#)
  - ["Auf einem lokalen Host, der keinen Internetzugang hat"](#)
- Über den Markt Ihres Cloud-Providers
  - ["AWS Marketplace"](#)
  - ["Azure Marketplace"](#)

Wenn Sie in einer Regierungsregion tätig sind, müssen Sie einen Connector vom Markt Ihres Cloud-Providers bereitstellen oder die Connector-Software manuell auf einem vorhandenen Linux-Host installieren. Sie können den Connector nicht auf der SaaS-Website von BlueXP in einer Regierungsregion bereitstellen.

## Berechtigungen

Zur Erstellung des Connectors sind spezielle Berechtigungen erforderlich, und für die Instanz des Connectors selbst sind weitere Berechtigungen erforderlich.

### Berechtigungen zum Erstellen eines Connectors

Der Benutzer, der einen Connector von BlueXP erstellt, benötigt spezielle Berechtigungen, um die Instanz bei Ihrem bevorzugten Cloud-Provider bereitzustellen.

- ["Zeigen Sie die erforderlichen AWS Berechtigungen an"](#)
- ["Zeigen Sie die erforderlichen Azure Berechtigungen an"](#)
- ["Zeigen Sie die erforderlichen Google Cloud-Berechtigungen an"](#)

### Berechtigungen für die Connector-Instanz

Für die Ausführung von Vorgängen in Ihrem Auftrag benötigt der Connector spezielle Cloud-Provider-Berechtigungen. Beispiel für die Implementierung und das Management von Cloud Volumes ONTAP.

Wenn Sie einen Connector direkt aus BlueXP erstellen, erstellt BlueXP den Connector mit den erforderlichen Berechtigungen. Es gibt nichts, was Sie tun müssen.

Wenn Sie den Connector selbst über AWS Marketplace, Azure Marketplace oder die Software manuell installieren, müssen Sie sicherstellen, dass die entsprechenden Berechtigungen vorhanden sind.

- ["Erfahren Sie, wie der Connector AWS-Berechtigungen nutzt"](#)
- ["Erfahren Sie, wie der Connector Azure-Berechtigungen nutzt"](#)
- ["Erfahren Sie, wie der Connector Google Cloud-Berechtigungen nutzt"](#)

## Connector-Upgrades

Wir aktualisieren die Connector-Software in der Regel jeden Monat, um neue Funktionen einzuführen und Stabilitätsverbesserungen zu ermöglichen. Während die meisten Services und Funktionen der BlueXP-Plattform über SaaS-basierte Software angeboten werden, sind einige Funktionen von der Version des Connectors abhängig. Dazu gehören Cloud Volumes ONTAP-Management, On-Premises-ONTAP-Cluster-

Management, Einstellungen und Hilfe.

Der Connector aktualisiert seine Software automatisch auf die neueste Version, solange er ausgehenden Internetzugriff hat, um das Softwareupdate zu erhalten.

## Anzahl der Arbeitsumgebungen pro Connector

Ein Connector kann mehrere Arbeitsumgebungen in BlueXP verwalten. Die maximale Anzahl von Arbeitsumgebungen, die ein einzelner Connector managen sollte, variiert. Das hängt von der Art der Arbeitsumgebungen, der Anzahl der Volumes, der zu verwaltenden Kapazität und der Anzahl der Benutzer ab.

Nutzen Sie eine umfangreiche Implementierung, arbeiten Sie mit Ihrem NetApp Ansprechpartner zusammen, um die Größe Ihrer Umgebung zu dimensionieren. Sollten Sie während des gesamten Chats Probleme haben, können Sie sich mit uns in Verbindung setzen.

## Wann werden mehrere Anschlüsse verwendet

In einigen Fällen benötigen Sie möglicherweise nur einen Connector, aber Sie benötigen möglicherweise zwei oder mehr Anschlüsse.

Hier nur ein paar Beispiele:

- Sie nutzen eine Multi-Cloud-Umgebung (AWS und Azure), d. h. einen Connector in AWS und einen anderen in Azure. Jedes managt die Cloud Volumes ONTAP Systeme, die in diesen Umgebungen ausgeführt werden.
- Ein Service Provider nutzt möglicherweise ein NetApp Konto, um seinen Kunden Services bereitzustellen, während er einen seiner Geschäftsbereiche mithilfe eines anderen Kontos Disaster Recovery unterstützt. Jedes Konto hätte separate Anschlüsse.

## Verwendung mehrerer Steckverbinder mit derselben Arbeitsumgebung

Sie können eine Arbeitsumgebung mit mehreren Connectors gleichzeitig für Disaster Recovery-Zwecke verwalten. Wenn ein Anschluss ausfällt, können Sie zum anderen Connector wechseln, um die Arbeitsumgebung sofort zu verwalten.

So richten Sie diese Konfiguration ein:

1. ["Wechseln Sie zu einem anderen Anschluss"](#)
2. Erkennung der vorhandenen Arbeitsumgebung
  - ["Fügen Sie vorhandene Cloud Volumes ONTAP-Systeme zu BlueXP hinzu"](#)
  - ["ONTAP Cluster erkennen"](#)
3. Stellen Sie die ein ["Kapazitätsmanagement -Modus"](#)

Nur der Hauptanschluss sollte auf **Automatikmodus** eingestellt sein. Wenn Sie zu DR-Zwecken auf einen anderen Connector wechseln, können Sie den Kapazitätsverwaltungsmodus bei Bedarf ändern.

## Wann muss zwischen den Anschlüssen gewechselt werden

Wenn Sie Ihren ersten Connector erstellen, verwendet BlueXP diesen Connector automatisch für jede zusätzliche Arbeitsumgebung, die Sie erstellen. Wenn Sie einen zusätzlichen Connector erstellen, müssen Sie zwischen diesen wechseln, um die für jeden Connector spezifischen Arbeitsumgebungen zu sehen.

["Erfahren Sie, wie Sie zwischen den Anschlüssen wechseln".](#)

## Die lokale Benutzeroberfläche

Während Sie fast alle Aufgaben aus dem ausführen sollten ["SaaS-Benutzeroberfläche"](#), Eine lokale Benutzeroberfläche ist weiterhin auf dem Connector verfügbar. Diese Schnittstelle ist erforderlich, wenn Sie den Connector in einer Umgebung installieren, die keinen Internetzugang hat (wie eine Regierungsregion) und für einige Aufgaben, die über den Connector selbst ausgeführt werden müssen, anstatt über die SaaS-Schnittstelle:

- ["Festlegen eines Proxyservers"](#)
- Installation eines Patches (Sie arbeiten in der Regel mit NetApp Mitarbeitern zusammen, um einen Patch zu installieren)
- Herunterladen von AutoSupport-Meldungen (normalerweise gerichtet von NetApp Mitarbeitern, wenn Sie Probleme haben)

["Erfahren Sie, wie Sie auf die lokale Benutzeroberfläche zugreifen".](#)

## Erstellen Sie einen Connector in AWS von BlueXP

Ein BlueXP-Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten BlueXP-Funktionen nutzen können. Mit dem Connector kann BlueXP Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung verwalten.

In diesen Schritten wird beschrieben, wie Sie einen Connector in einer kommerziellen AWS-Region direkt von der BlueXP SaaS-Website erstellen.

- ["Erfahren Sie, wie Sie einen Connector in einer Regierungsregion bereitstellen"](#)
- ["Erfahren Sie mehr über andere Möglichkeiten zur Bereitstellung eines Connectors"](#)

## Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1

### Richten Sie die Authentifizierung ein

Um den Connector in AWS zu starten, muss BlueXP sich mit AWS authentifizieren, indem er entweder eine IAM-Rolle übernimmt oder AWS-Zugriffsschlüssel verwendet. Bei beiden Optionen ist eine IAM-Richtlinie erforderlich.

[IAM-Rolle anzeigen](#) Oder [Befolgen Sie die Schritt-für-Schritt-Anweisungen.](#)

2

### Netzwerk einrichten

Sie benötigen eine VPC und ein Subnetz mit Outbound-Internetzugang zu bestimmten Endpunkten. Wenn ein HTTP-Proxy für das ausgehende Internet erforderlich ist, benötigen Sie die IP-Adresse, die Anmeldeinformationen und das HTTPS-Zertifikat.

[Netzwerkanforderungen anzeigen.](#)

### Erstellen Sie den Konnektor

Klicken Sie auf das Dropdown-Menü Connector, wählen Sie **Anschluss hinzufügen** aus, und folgen Sie den Anweisungen.

[Befolgen Sie die Schritt-für-Schritt-Anweisungen.](#)

## AWS-Authentifizierung 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 müssen Sie zunächst mit der Erstellung einer IAM-Richtlinie beginnen, die die erforderlichen Berechtigungen enthält.

### IAM-Richtlinie erstellen

Diese Richtlinie enthält nur die Berechtigungen, die zum Starten der Connector-Instanz in AWS von BlueXP erforderlich sind. Verwenden Sie diese Richtlinie nicht für andere Situationen.

Wenn BlueXP den Connector erstellt, wendet er eine neue Reihe von Berechtigungen auf die Connector-Instanz an, die es dem Connector ermöglicht, die Ressourcen in Ihrer Public Cloud-Umgebung zu verwalten.

### Schritte

1. Wechseln Sie zur AWS IAM-Konsole.
2. Klicken Sie auf **Richtlinien > Richtlinien erstellen**.
3. Klicken Sie auf **JSON**.
4. Kopieren Sie die folgende Richtlinie:

```
{
  "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",
      "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",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    }
},

```

```
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
]
}
```

5. Klicken Sie auf **Weiter** und fügen Sie ggf. Tags hinzu.
6. Klicken Sie auf **Weiter** und geben Sie einen Namen und eine Beschreibung ein.
7. Klicken Sie auf **Create Policy**.

### Was kommt als Nächstes?

Hängen Sie die Richtlinie entweder an eine IAM-Rolle an, die BlueXP übernehmen kann, oder an einen IAM-Benutzer.

### Einrichten einer IAM-Rolle

Richten Sie eine IAM-Rolle ein, von der BlueXP ausgehen kann, um den Connector in AWS bereitzustellen.

#### Schritte

1. Wechseln Sie im Zielkonto zur AWS IAM-Konsole.
2. Klicken Sie unter Zugriffsverwaltung auf **Rollen > Rolle erstellen** und befolgen Sie die Schritte zum Erstellen der Rolle.

Gehen Sie wie folgt vor:

- Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
  - Wählen Sie **ein weiteres AWS-Konto** aus und geben Sie die ID des BlueXP SaaS-Kontos ein: 952013314444
  - Wählen Sie die Richtlinie aus, die Sie im vorherigen Abschnitt erstellt haben.
3. Nachdem Sie die Rolle erstellt haben, kopieren Sie die Rolle ARN, sodass Sie sie bei der Erstellung des Connectors in BlueXP einfügen können.

### Ergebnis

Die IAM-Rolle verfügt nun über die erforderlichen Berechtigungen.

### Einrichten von Berechtigungen für einen IAM-Benutzer

Wenn Sie einen Connector erstellen, können Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel für einen IAM-Benutzer bereitstellen, der über die erforderlichen Berechtigungen zum Bereitstellen der Connector-Instanz verfügt.

#### Schritte

1. Klicken Sie auf der AWS IAM-Konsole auf **Users** und wählen Sie dann den Benutzernamen aus.
2. Klicken Sie auf **Berechtigungen hinzufügen > vorhandene Richtlinien direkt anhängen**.
3. Wählen Sie die von Ihnen erstellte Richtlinie aus.
4. Klicken Sie auf **Weiter** und dann auf **Berechtigungen hinzufügen**.

5. Stellen Sie sicher, dass Sie Zugriff auf einen Zugriffsschlüssel und einen geheimen Schlüssel für den IAM-Benutzer haben.

## Ergebnis

Der AWS-Benutzer verfügt nun über die erforderlichen Berechtigungen, um den Connector von BlueXP zu erstellen. Wenn Sie dazu aufgefordert werden, müssen Sie die AWS-Zugriffsschlüssel für diesen Benutzer angeben.

## Netzwerk einrichten

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


### Verbindung zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu der Art der Arbeitsumgebung, die Sie erstellen und die Dienste, die Sie planen zu ermöglichen.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zu der VPC einrichten, in der Sie Cloud Volumes ONTAP starten.

### Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen.

Endpunkte	Zweck
https://support.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	<div> Der Connector kontaktiert derzeit „cloudmanager.cloud.netapp.com“, er beginnt jedoch mit der Kontaktaufnahme mit „api.bluexp.netapp.com“ in einer kommenden Version.</div> Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen.
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Aktualisierung des Connectors und seiner Docker Komponenten.

### Proxy-Server

Wenn Ihr Unternehmen einen HTTP-Proxy für den gesamten ausgehenden Internet-Datenverkehr benötigt, informieren Sie sich über Ihren HTTP-Proxy:

- IP-Adresse
- Anmeldedaten

- HTTPS-Zertifikat

## Sicherheitsgruppe

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy für AutoSupport-Nachrichten verwendet wird. HTTP und HTTPS bieten den Zugriff auf "[Lokale Benutzeroberfläche](#)", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

## Einschränkung der IP-Adresse

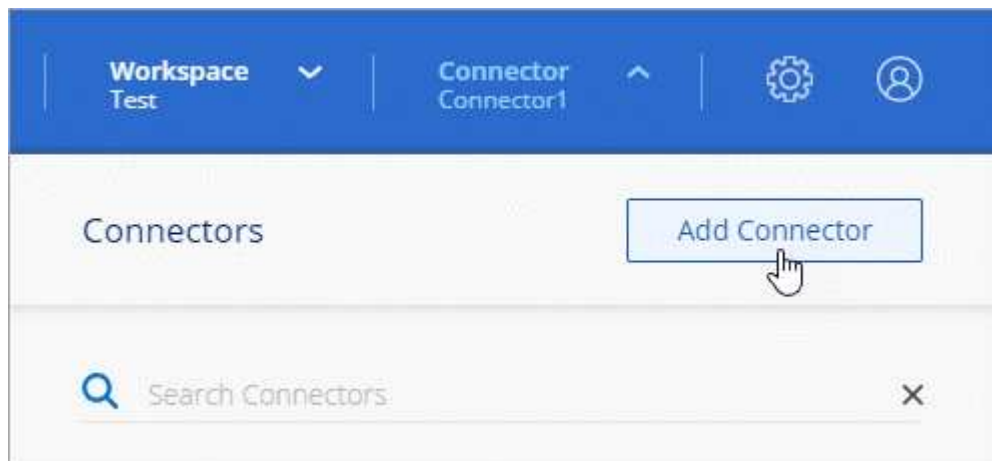
Es besteht ein möglicher Konflikt mit IP-Adressen im Bereich 172. "[Erfahren Sie mehr über diese Einschränkung](#)".

## Einen Konnektor erstellen

Mit BlueXP können Sie einen Connector in AWS direkt von der Benutzeroberfläche aus erstellen.

### Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Wählen Sie als Cloud-Provider \* Amazon Web Services\* und klicken Sie auf **Weiter**.
3. Lesen Sie auf der Seite **Bereitstellen eines Konnektors** die Details dazu, was Sie benötigen. Sie haben zwei Möglichkeiten:
  - a. Klicken Sie auf **Weiter**, um die Bereitstellung mithilfe des Produktleitfadens vorzubereiten. Jeder Schritt im Produktleitfaden enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.
  - b. Klicken Sie auf **Skip to Deployment**, wenn Sie bereits mit den Schritten auf dieser Seite vorbereitet sind.
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 aus, ob eine neue Sicherheitsgruppe erstellt werden soll oder ob eine vorhandene Sicherheitsgruppe ausgewählt werden soll, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.
- **Review:** Überprüfen Sie Ihre Auswahl, um zu überprüfen, ob Ihre Einrichtung korrekt ist.

## 5. Klicken Sie Auf **Hinzufügen**.

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

### Nachdem Sie fertig sind

Wenn Sie Amazon S3 Buckets im gleichen AWS-Konto haben, in dem Sie den Connector erstellt haben, wird automatisch eine Amazon S3-Arbeitsumgebung auf dem Canvas angezeigt. ["Erfahren Sie mehr darüber, was Sie mit dieser Arbeitsumgebung tun können"](#).

## Offener Port 3128 für AutoSupport-Meldungen

Wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen möchten, in dem keine ausgehende Internetverbindung verfügbar ist, konfiguriert BlueXP Cloud Volumes ONTAP automatisch für die Verwendung des Connectors als Proxyserver.

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.

Wenn Sie die Standardsicherheitsgruppe für Cloud Volumes ONTAP verwenden, sind keine Änderungen an der Sicherheitsgruppe erforderlich. Wenn Sie aber strenge ausgehende Regeln für Cloud Volumes ONTAP definieren möchten, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

# Erstellen Sie einen Connector in Azure von BlueXP

Ein BlueXP-Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten BlueXP-Funktionen nutzen können. Mit dem Connector kann BlueXP Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung verwalten.

In diesen Schritten wird beschrieben, wie Sie einen Connector in einer kommerziellen Azure-Region direkt von der BlueXP SaaS-Website erstellen.

- ["Erfahren Sie, wie Sie einen Connector in einer Regierungsregion bereitstellen"](#)
- ["Erfahren Sie mehr über andere Möglichkeiten zur Bereitstellung eines Connectors"](#)

## Überblick

Um einen Connector bereitzustellen, müssen Sie BlueXP mit einer Anmeldung bereitstellen, die über die erforderlichen Berechtigungen zum Erstellen der Connector-VM in Azure verfügt.

Sie haben zwei Möglichkeiten:

1. Melden Sie sich bei Aufforderung mit Ihrem Microsoft-Konto an. Dieses Konto muss über spezifische Azure Berechtigungen verfügen. Dies ist die Standardoption.

[Führen Sie die nachstehenden Schritte aus, um zu starten.](#)

2. Geben Sie Details zu einem Azure AD-Serviceprincipal an. Dieser Service-Principal erfordert auch spezielle Berechtigungen.

[Führen Sie die nachstehenden Schritte aus, um zu starten.](#)

## Ein Hinweis zu Azure Regionen

Der Connector sollte in derselben Azure-Region wie die Cloud Volumes ONTAP-Systeme, die er verwaltet, oder in der implementiert 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"](#)

## Netzwerk einrichten

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


### Verbindung zu Zielnetzwerken

Ein Connector erfordert eine Netzwerkverbindung zu der Art der Arbeitsumgebung, die Sie erstellen und die Dienste, die Sie planen zu ermöglichen.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zu dem vnet einrichten, in dem Sie Cloud Volumes ONTAP starten.

## Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen.

Endpunkte	Zweck
https://support.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	<div> Der Connector kontaktiert derzeit „cloudmanager.cloud.netapp.com“, er beginnt jedoch mit der Kontaktaufnahme mit „api.bluexp.netapp.com“ in einer kommenden Version.</div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Aktualisierung des Connectors und seiner Docker Komponenten.

## Proxy-Server

Wenn Ihr Unternehmen einen HTTP-Proxy für den gesamten ausgehenden Internet-Datenverkehr benötigt, informieren Sie sich über Ihren HTTP-Proxy:

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

## Sicherheitsgruppe

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy für AutoSupport-Nachrichten verwendet wird. HTTP und HTTPS bieten den Zugriff auf "[Lokale Benutzeroberfläche](#)", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

## Einschränkung der IP-Adresse

Es besteht ein möglicher Konflikt mit IP-Adressen im Bereich 172. "[Erfahren Sie mehr über diese Einschränkung](#)".

## Erstellen Sie mit Ihrem Azure Konto einen Connector

Zum Erstellen eines Konnektors in Azure müssen Sie sich bei einer entsprechenden Aufforderung bei Ihrem Azure-Konto anmelden. Das Anmeldeformular ist Eigentum von Microsoft und wird von Microsoft gehostet. Ihre Zugangsdaten werden nicht an NetApp bereitgestellt.

## Richten Sie Berechtigungen für Ihr Azure Konto ein

Bevor Sie einen Connector von BlueXP bereitstellen können, müssen Sie sicherstellen, dass Ihr Azure-Konto über die entsprechenden Berechtigungen verfügt.

### Schritte

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



Diese Richtlinie enthält nur die Berechtigungen, die zum Starten der Connector VM in Azure von BlueXP erforderlich sind. Verwenden Sie diese Richtlinie nicht für andere Situationen. Wenn BlueXP den Connector erstellt, wendet er eine neue Gruppe von Berechtigungen auf die Connector-VM an, die es dem Connector ermöglicht, die Ressourcen in Ihrer Public-Cloud-Umgebung zu verwalten.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
```



```

        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/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.

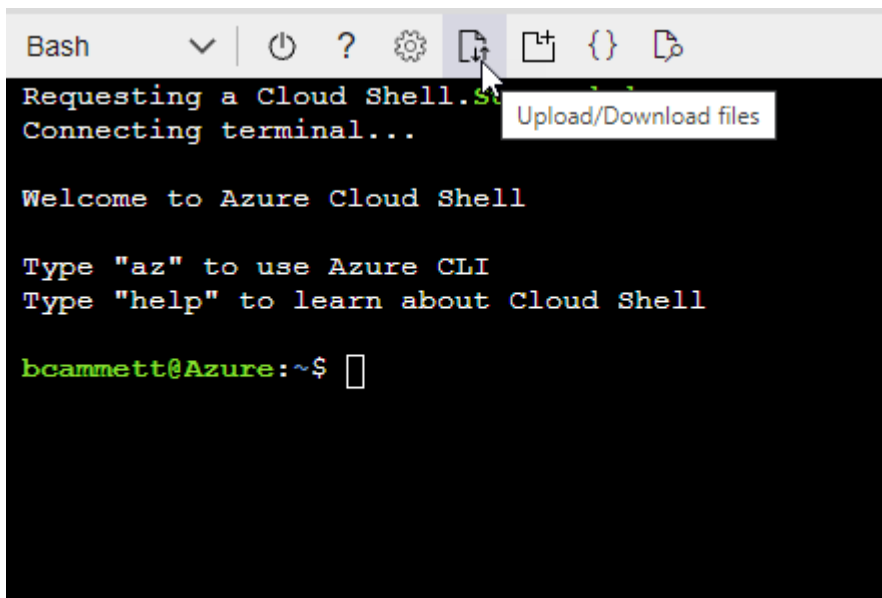
## Beispiel

```
"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.

4. Weisen Sie die Rolle dem Benutzer zu, der den Connector von BlueXP bereitstellen wird:
  - a. Öffnen Sie den Dienst **Abonnements** und wählen Sie das Abonnement des Benutzers aus.
  - b. Klicken Sie auf **Access Control (IAM)**.
  - c. Klicken Sie auf **Hinzufügen > Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
    - 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.

- **Benutzer, Gruppe oder Serviceprincipal** ausgewählt lassen.
- Klicken Sie auf **Mitglieder auswählen**, wählen Sie Ihr Benutzerkonto aus und klicken Sie auf **Auswählen**.
- Klicken Sie Auf **Weiter**.
- Klicken Sie auf **Review + Assign**.

## Ergebnis

Der Azure-Benutzer verfügt nun über die erforderlichen Berechtigungen für die Bereitstellung des Connectors von BlueXP.

## Erstellen Sie den Connector, indem Sie sich mit Ihrem Azure Konto anmelden

Mit BlueXP können Sie einen Connector in Azure direkt über die Benutzeroberfläche erstellen.

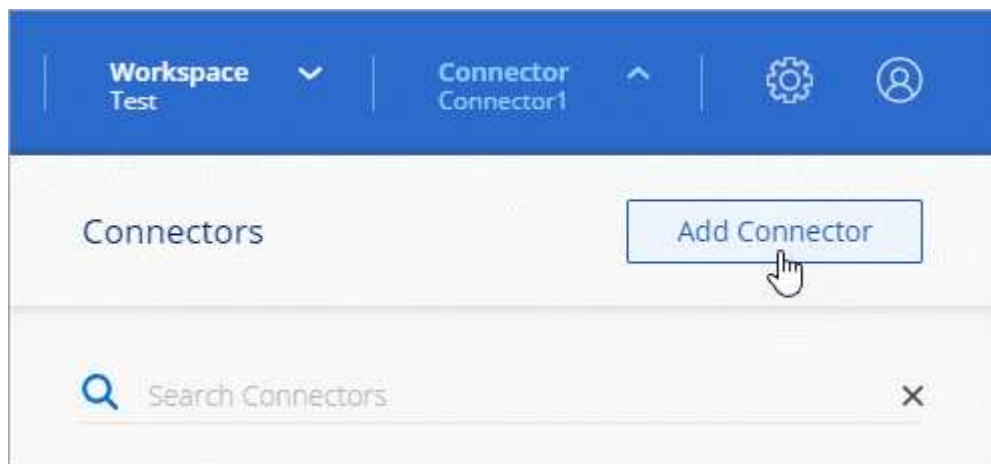
### Was Sie benötigen

- Ein Azure Abonnement.
- Eine vnet und Subnetz in Ihrer bevorzugten Azure-Region.
- 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 eine andere Gruppe von Berechtigungen als das, was Sie zuvor für die einfache Bereitstellung des Connectors eingerichtet haben.

## Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Wählen Sie als Cloud-Provider \* Microsoft Azure\* aus.
3. Lesen Sie auf der Seite **Bereitstellen eines Konnektors** die Details dazu, was Sie benötigen. Sie haben zwei Möglichkeiten:

- a. Klicken Sie auf **Weiter**, um die Bereitstellung mithilfe des Produktleitfadens vorzubereiten. Jeder Schritt enthält Informationen, die auf dieser Seite der Dokumentation enthalten sind.
- b. Klicken Sie auf **Skip to Deployment**, wenn Sie bereits mit den Schritten auf dieser Seite vorbereitet sind.

4. Befolgen Sie die Schritte im Assistenten, um den Konnektor zu erstellen:

- Wenn Sie dazu aufgefordert werden, melden Sie sich bei Ihrem Microsoft-Konto an, das über die erforderlichen Berechtigungen zum Erstellen der virtuellen Maschine verfügt.

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.

- **VM Authentication:** Wählen Sie ein Azure-Abonnement, einen Speicherort, eine neue Ressourcengruppe oder eine vorhandene Ressourcengruppe aus und wählen Sie dann eine Authentifizierungsmethode aus.
- **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 Abonnements für diese Rolle auswählen können. Jedes von Ihnen gewählte Abonnement bietet dem Konnektor Berechtigungen zum Bereitstellen von Cloud Volumes ONTAP in diesen Abonnements.

- **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 aus, ob eine neue Sicherheitsgruppe erstellt werden soll oder ob eine vorhandene Sicherheitsgruppe ausgewählt werden soll, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.
- **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.

### Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Kontoadministratoren haben standardmäßig die Möglichkeit, auf alle Arbeitsbereiche in BlueXP zuzugreifen. "[Weitere Informationen](#)".

Wenn Sie Azure Blob Storage in demselben Azure Konto haben, in dem Sie den Connector erstellt haben, wird automatisch eine Azure Blob Arbeitsumgebung auf dem Canvas angezeigt. "[Erfahren Sie mehr darüber, was Sie mit dieser Arbeitsumgebung tun können](#)".

## Erstellen Sie einen Konnektor mithilfe eines Service-Principal

Anstatt sich beim Azure-Konto anzumelden, haben Sie auch die Möglichkeit, BlueXP die Zugangsdaten für einen Azure-Service-Principal mit den erforderlichen Berechtigungen bereitzustellen.

### Azure-Berechtigungen über einen Service-Principal gewähren

Gewähren Sie die erforderlichen Berechtigungen für die Bereitstellung eines Konnektors in Azure, indem Sie einen Service-Principal in Azure Active Directory erstellen und einrichten, sowie die von BlueXP benötigten Azure Zugangsdaten.

#### Schritte

1. [Erstellen Sie eine Azure Active Directory-Anwendung.](#)
2. [Anwendung einer Rolle zuweisen.](#)
3. [Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.](#)
4. [Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.](#)
5. [Erstellen Sie einen Clientschlüssel.](#)

#### Erstellen Sie eine Azure Active Directory-Anwendung

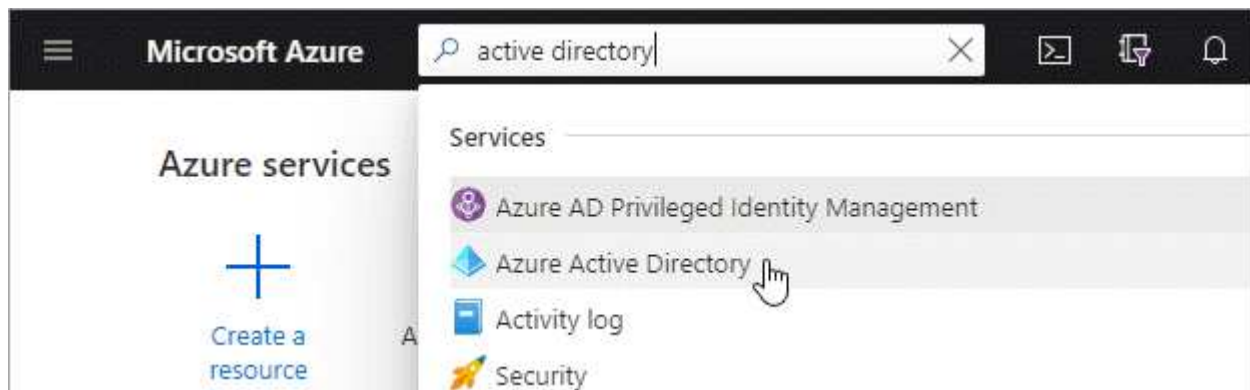
Erstellen Sie eine Applikation und einen Service-Principal für Azure Active Directory (AD), die BlueXP zur Bereitstellung des Connectors verwenden kann.

#### Bevor Sie beginnen

Sie müssen über die richtigen Berechtigungen in Azure verfügen, um eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen. Weitere Informationen finden Sie unter "[Microsoft Azure-Dokumentation: Erforderliche Berechtigungen](#)".

#### Schritte

1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



2. Klicken Sie im Menü auf **App-Registrierungen**.
3. Klicken Sie auf **Neue Registrierung**.
4. 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.

## 5. Klicken Sie Auf **Registrieren**.

### Ergebnis

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

### Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an das Azure-Abonnement binden, in dem Sie den Connector bereitstellen möchten, und ihm die benutzerdefinierte Rolle „Azure SetupAsService“ zuweisen.

### Schritte

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



Diese Richtlinie enthält nur die Berechtigungen, die zum Starten der Connector VM in Azure von BlueXP erforderlich sind. Verwenden Sie diese Richtlinie nicht für andere Situationen. Wenn BlueXP den Connector erstellt, wendet er eine neue Gruppe von Berechtigungen auf die Connector-VM an, die es dem Connector ermöglicht, die Ressourcen in Ihrer Public-Cloud-Umgebung zu verwalten.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
```

```

    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

    "Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/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 die JSON-Datei, indem Sie Ihre Azure Abonnement-ID dem zuweisbaren Umfang hinzufügen.

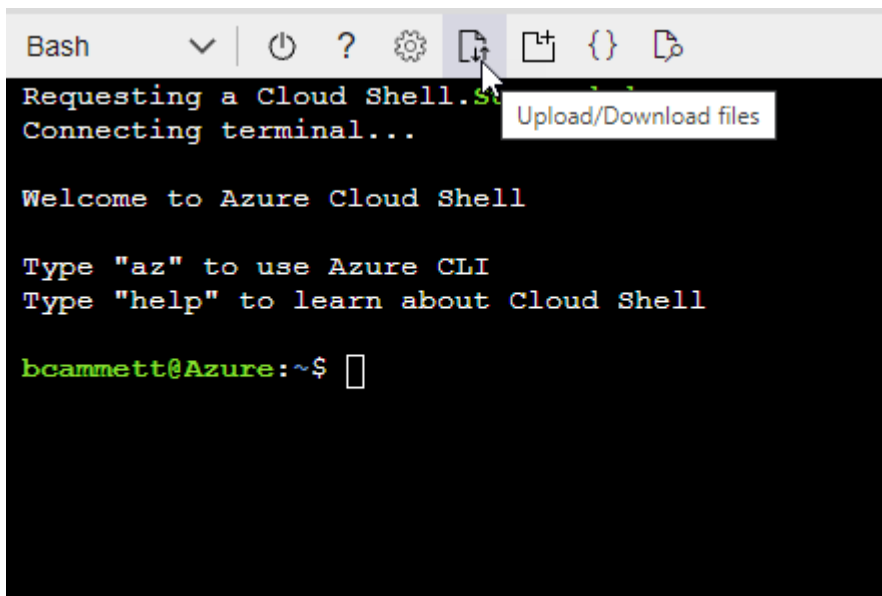
### Beispiel

```
"AssignableScopes": [  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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
```

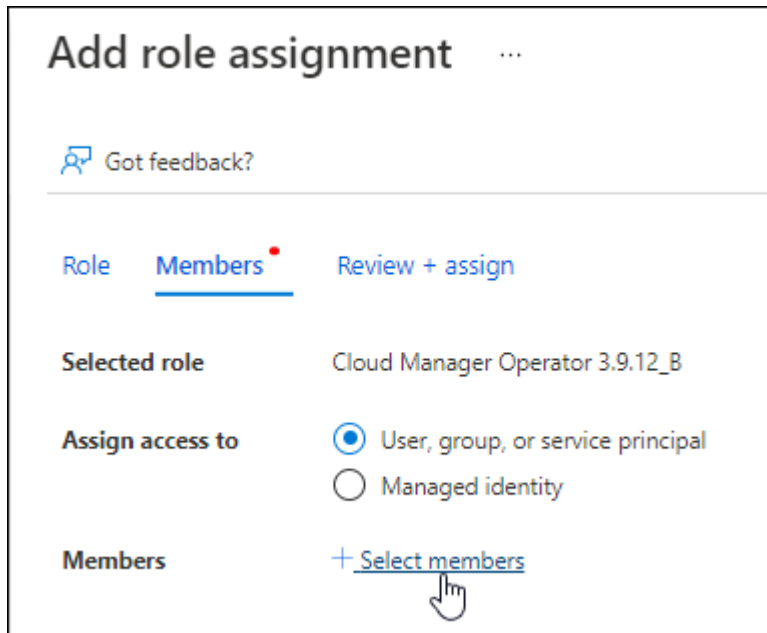
Sie sollten jetzt eine benutzerdefinierte Rolle namens *Azure SetupAsService* haben.

4. Applikation der Rolle zuweisen:
  - a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
  - b. Wählen Sie das Abonnement aus.
  - c. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
  - d. Wählen Sie auf der Registerkarte **Role** die Rolle **Azure SetupAsService** aus und klicken Sie auf **Next**.



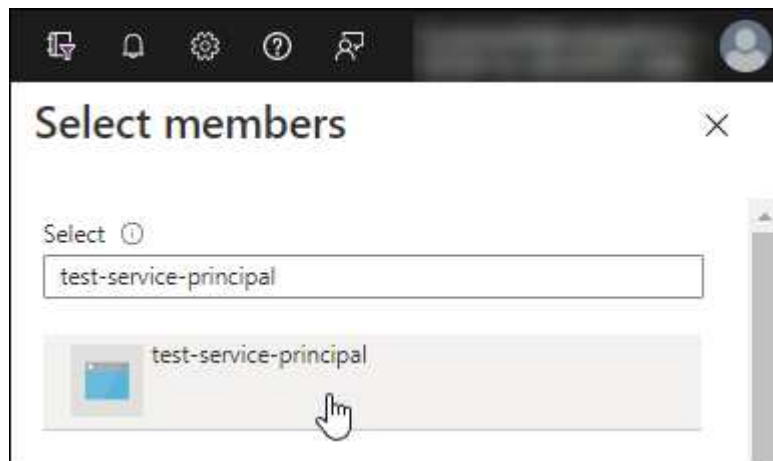
e. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:

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



- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:



- Wählen Sie die Anwendung aus und klicken Sie auf **Auswählen**.
- Klicken Sie Auf **Weiter**.
- a. Klicken Sie auf **Review + Assign**.

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

#### Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu

Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

## Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Klicken Sie auf **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.













### Request API permissions

#### Select an API

Microsoft APIs   APIs my organization uses   My APIs

#### Commonly used Microsoft APIs

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

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

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

## Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

### Delegated permissions

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

### Application permissions

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

Select permissions

[expand all](#)

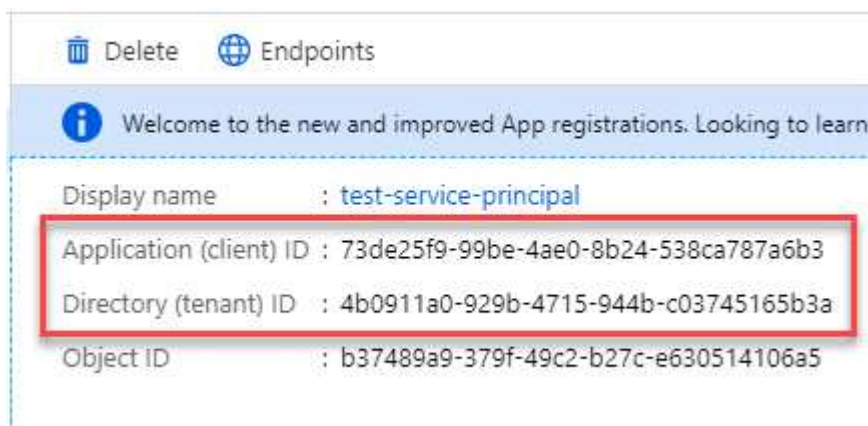
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

## Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab

Wenn Sie den Connector von BlueXP erstellen, müssen Sie die Anwendungs- (Client)-ID und die Verzeichnis- (Mandanten-)ID für die Anwendung angeben. BlueXP verwendet die IDs, um sich programmatisch anzumelden.

### Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) ID**.



## Erstellen Sie einen Clientschlüssel

Sie müssen ein Clientgeheimnis erstellen und dann BlueXP den Wert des Geheimnisses zur Verfügung stellen, damit BlueXP es zur Authentifizierung mit Azure AD nutzen kann.

### Schritte

1. Öffnen Sie den Dienst **Azure Active Directory**.
2. Klicken Sie auf **App-Registrierungen** und wählen Sie Ihre Anwendung aus.

3. Klicken Sie auf **Zertifikate & Geheimnisse > Neuer Client Secret**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Klicken Sie Auf **Hinzufügen**.
6. Kopieren Sie den Wert des Clientgeheimnisses.

#### Client secrets

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

<a href="#">+ New client secret</a>		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

### 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.

### Erstellen Sie den Connector, indem Sie sich beim Service-Principal anmelden

Mit BlueXP können Sie einen Connector in Azure direkt über die Benutzeroberfläche erstellen.

#### Was Sie benötigen

- Ein Azure Abonnement.
- Eine vnet und Subnetz in Ihrer bevorzugten Azure-Region.
- Details zu einem HTTP-Proxy, wenn Ihr Unternehmen einen Proxy für den gesamten ausgehenden Internet-Datenverkehr benötigt:
  - IP-Adresse
  - Anmeldedaten
  - HTTPS-Zertifikat
- 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 eine andere Gruppe von Berechtigungen als das, was Sie zuvor für die einfache Bereitstellung des Connectors eingerichtet haben.

#### Schritte

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** und wählen Sie **Connector hinzufügen** aus.



2. Wählen Sie als Cloud-Provider \* Microsoft Azure\* aus.
3. Auf der Seite \* Ansetzen eines Konnektors\*:
  - a. Klicken Sie unter **Authentifizierung** auf **Active Directory Service Principal** und geben Sie Informationen über den Azure Active Directory Service Principal ein, der die erforderlichen Berechtigungen erteilt:
    - Anwendungs-ID (Client): Siehe [Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab](#).
    - Verzeichnis-ID (Mandant): Siehe [Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab](#).
    - Client Secret: Siehe [Erstellen Sie einen Clientschlüssel](#).
  - b. Klicken Sie auf **Anmelden**.
  - c. Sie haben nun zwei Möglichkeiten:
    - Klicken Sie auf **Weiter**, um die Bereitstellung mithilfe des Produktleitfadens vorzubereiten. Jeder Schritt im Produktleitfaden enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.
    - Klicken Sie auf **Skip to Deployment**, wenn Sie bereits mit den Schritten auf dieser Seite vorbereitet sind.
4. Befolgen Sie die Schritte im Assistenten, um den Konnektor zu erstellen:
  - **VM Authentication:** Wählen Sie ein Azure-Abonnement, einen Speicherort, eine neue Ressourcengruppe oder eine vorhandene Ressourcengruppe aus und wählen Sie dann eine Authentifizierungsmethode aus.
  - **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 Abonnements für diese Rolle auswählen können. Jedes von Ihnen gewählte Abonnement bietet dem Konnektor Berechtigungen zum Bereitstellen von Cloud Volumes ONTAP in diesen Abonnements.

  - **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 aus, ob eine neue Sicherheitsgruppe erstellt werden soll oder ob eine vorhandene Sicherheitsgruppe ausgewählt werden soll, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.

- **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.

#### Nachdem Sie fertig sind

Sie müssen einen Connector mit Arbeitsbereichen verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors zum Erstellen von Cloud Volumes ONTAP-Systemen verwenden können. Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Kontoadministratoren haben standardmäßig die Möglichkeit, auf alle Arbeitsbereiche in BlueXP zuzugreifen. ["Weitere Informationen ."](#)

Wenn Sie Azure Blob Storage in demselben Azure Konto haben, in dem Sie den Connector erstellt haben, wird automatisch eine Azure Blob Arbeitsumgebung auf dem Canvas angezeigt. ["Erfahren Sie mehr darüber, was Sie mit dieser Arbeitsumgebung tun können"](#).

### Offener Port 3128 für AutoSupport-Meldungen

Wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen möchten, in dem keine ausgehende Internetverbindung verfügbar ist, konfiguriert BlueXP Cloud Volumes ONTAP automatisch für die Verwendung des Connectors als Proxyserver.

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.

Wenn Sie die Standardsicherheitsgruppe für Cloud Volumes ONTAP verwenden, sind keine Änderungen an der Sicherheitsgruppe erforderlich. Wenn Sie aber strenge ausgehende Regeln für Cloud Volumes ONTAP definieren möchten, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

## Erstellen Sie einen Connector in Google Cloud von BlueXP

Ein BlueXP-Kontoadministrator muss einen *Connector* bereitstellen, bevor Sie die meisten BlueXP-Funktionen nutzen können. ["Informieren Sie sich, wann ein Anschluss erforderlich ist"](#). Mit dem Connector kann BlueXP Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung verwalten.

Auf dieser Seite wird beschrieben, wie Sie einen Connector in Google Cloud direkt aus BlueXP erstellen. ["Erfahren Sie mehr über andere Möglichkeiten zur Bereitstellung eines Connectors"](#).

Diese Schritte müssen von einem Benutzer ausgeführt werden, der die Rolle „Account Admin“ hat. Ein Workspace-Administrator kann keinen Konnektor erstellen.



Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von BlueXP aufgefordert, einen Konnektor zu erstellen, falls Sie noch keinen haben.

### Schnellstart

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um

ausführliche Informationen zu erhalten.

1

### Berechtigungen einrichten

- Stellen Sie sicher, dass Ihr Google Cloud-Konto über die richtigen Berechtigungen verfügt, indem Sie eine benutzerdefinierte Rolle erstellen und anhängen.

[Richten Sie Berechtigungen für die Bereitstellung des Connectors ein.](#)

- Wenn Sie die Connector-VM erstellen, müssen Sie sie einem Servicekonto zuordnen. Dieses Servicekonto muss über eine benutzerdefinierte Rolle verfügen, die Berechtigungen zum Managen von Ressourcen in Google Cloud hat.

[Richten Sie ein Servicekonto für den Konnektor ein.](#)

- Wenn Sie eine gemeinsame VPC verwenden, legen Sie Berechtigungen im Service-Projekt und im Host-Projekt ein.

[Gemeinsame VPC-Berechtigungen einrichten.](#)

2

### Netzwerk einrichten

Sie benötigen eine VPC und ein Subnetz mit Outbound-Internetzugang zu bestimmten Endpunkten. Wenn ein HTTP-Proxy für das ausgehende Internet erforderlich ist, benötigen Sie die IP-Adresse, die Anmeldeinformationen und das HTTPS-Zertifikat.

[Netzwerkanforderungen anzeigen.](#)

3

### Aktivieren Sie Google Cloud-APIs

- Cloud Deployment Manager V2-API
- Cloud-ProtokollierungsAPI
- Cloud Resource Manager API
- Compute Engine-API
- IAM-API (Identitäts- und Zugriffsmanagement)

4

### Erstellen Sie den Konnektor

Klicken Sie auf das Dropdown-Menü Connector, wählen Sie **Anschluss hinzufügen** aus, und folgen Sie den Anweisungen.

[Befolgen Sie die Schritt-für-Schritt-Anweisungen.](#)

## Berechtigungen einrichten

Für Folgendes sind Berechtigungen erforderlich:

- Der Benutzer, der die Connector-VM bereitstellen wird

- Ein Servicekonto, das Sie während der Bereitstellung mit der Connector-VM verbinden müssen
- Gemeinsame VPC-Berechtigungen, wenn Sie eine gemeinsame VPC verwenden, um Ressourcen in einem Service-Projekt zu implementieren

## Richten Sie Berechtigungen für die Bereitstellung des Connectors ein

Bevor Sie einen Connector bereitstellen können, müssen Sie sicherstellen, dass Ihr Google Cloud-Konto über die entsprechenden Berechtigungen verfügt.

### Schritte

1. "Erstellen Sie eine benutzerdefinierte Rolle" Dazu gehören die 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`

2. Fügen Sie die benutzerdefinierte Rolle dem Benutzer an, der den Connector von BlueXP bereitstellen wird.

## Ergebnis

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

## Richten Sie ein Servicekonto für den Konnektor ein

Ein Dienstkonto ist erforderlich, um dem Connector die Berechtigung zu geben, dass er Ressourcen in Google Cloud verwalten muss. Sie verknüpfen dieses Servicekonto mit der Connector-VM, wenn Sie es erstellen.

Die Berechtigungen für das Dienstkonto unterscheiden sich von den Berechtigungen, die Sie im vorherigen Abschnitt eingerichtet haben.

## Schritte

1. "Erstellen Sie eine benutzerdefinierte Rolle" Dazu gehören die folgenden Berechtigungen:

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
```

`includedPermissions:`

- `iam.serviceAccounts.actAs`
- `compute.regionBackendServices.create`
- `compute.regionBackendServices.get`
- `compute.regionBackendServices.list`
- `compute.networks.updatePolicy`
- `compute.backendServices.create`
- `compute.addresses.list`
- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `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.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`

- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- 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
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list

- `storage.buckets.getIamPolicy`

2. "Erstellen Sie ein Google Cloud-Servicekonto, und wenden Sie die soeben erstellte benutzerdefinierte Rolle an".
3. Wenn Sie Cloud Volumes ONTAP in anderen Projekten implementieren möchten, "Gewähren Sie Zugriff, indem Sie dem Projekt das Servicekonto mit der Rolle BlueXP hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.

## Ergebnis

Das Servicekonto für die Connector-VM wird eingerichtet.

## Gemeinsame VPC-Berechtigungen einrichten

Wenn Sie eine gemeinsame VPC zur Implementierung von Ressourcen in einem Service-Projekt verwenden, sind die folgenden Berechtigungen erforderlich. Diese Tabelle dient als Referenz. Ihre Umgebung sollte nach Abschluss der IAM-Konfiguration die Berechtigungstabelle widerspiegeln.

Identität	Ersteller	Gehostet in	Berechtigungen für Serviceprojekte	Host-Projektberechtigungen	Zweck
Google-Konto verwendet, um den Connector bereitzustellen	Individuell	Service-Projekt	<ul style="list-style-type: none"><li>"Die Berechtigungen, die in diesem Abschnitt oben gefunden wurden"</li></ul>	<ul style="list-style-type: none"><li>compute.networkUser</li></ul>	Bereitstellen des Connectors im Serviceprojekt
Connector-Servicekonto	Individuell	Service-Projekt	<ul style="list-style-type: none"><li>"Die Berechtigungen, die in diesem Abschnitt oben gefunden wurden"</li></ul>	<ul style="list-style-type: none"><li>compute.networkUser</li><li>Bereitsmanager.Editor</li></ul>	Implementierung und Wartung von Cloud Volumes ONTAP und Services im Service-Projekt
Cloud Volumes ONTAP-Servicekonto	Individuell	Service-Projekt	<ul style="list-style-type: none"><li>Storage.Administration</li><li>mitglied: BlueXP Dienstkonto als serviceAccount.user</li></ul>	K. A.	(Optional) für Daten-Tiering und Cloud Backup
Google APIs-Serviceagent	Google Cloud	Service-Projekt	<ul style="list-style-type: none"><li>(Standard) Editor</li></ul>	<ul style="list-style-type: none"><li>compute.networkUser</li></ul>	Arbeitet im Auftrag der Implementierung mit Google Cloud APIs zusammen. Ermöglicht BlueXP die Nutzung des gemeinsam genutzten Netzwerks.

Identität	Ersteller	Gehostet in	Berechtigungen für Serviceprojekte	Host-Projektberechtigungen	Zweck
Google Compute Engine Standard-Servicekonto	Google Cloud	Service-Projekt	<ul style="list-style-type: none"> <li>(Standard) Editor</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	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.

## Netzwerk einrichten

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

### Verbindung zu Zielnetzwerken


Ein Connector erfordert eine Netzwerkverbindung zu der Art der Arbeitsumgebung, die Sie erstellen und die Dienste, die Sie planen zu ermöglichen.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zu der VPC einrichten, in der Sie Cloud Volumes ONTAP starten.

### Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen.

Endpunkte	Zweck
<a href="https://support.netapp.com">https://support.netapp.com</a>	Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden.

Endpunkte	Zweck
<a href="https://*.api.bluexp.netapp.com">https://*.api.bluexp.netapp.com</a> <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Um SaaS-Funktionen und -Services in BlueXP zur Verfügung zu stellen.  <div>  Der Connector kontaktiert derzeit „cloudmanager.cloud.netapp.com“, er beginnt jedoch mit der Kontaktaufnahme mit „api.bluexp.netapp.com“ in einer kommenden Version. </div>
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	Aktualisierung des Connectors und seiner Docker Komponenten.

## Proxy-Server

Wenn Ihr Unternehmen einen HTTP-Proxy für den gesamten ausgehenden Internet-Datenverkehr benötigt, informieren Sie sich über Ihren HTTP-Proxy:

- IP-Adresse
- Anmeldedaten
- HTTPS-Zertifikat

## Sicherheitsgruppe

Es gibt keinen eingehenden Datenverkehr zum Konnektor, es sei denn, Sie initiieren ihn oder wenn der Connector als Proxy für AutoSupport-Nachrichten verwendet wird. HTTP und HTTPS bieten den Zugriff auf "[Lokale Benutzeroberfläche](#)", Die Sie in seltenen Fällen verwenden. SSH ist nur erforderlich, wenn Sie eine Verbindung zum Host zur Fehlerbehebung herstellen müssen.

## Einschränkung der IP-Adresse

Es besteht ein möglicher Konflikt mit IP-Adressen im Bereich 172. "[Erfahren Sie mehr über diese Einschränkung](#)".

## Aktivieren Sie Google Cloud-APIs

Für die Bereitstellung des Connectors und der Cloud Volumes ONTAP sind mehrere APIs erforderlich.

### Schritt

1. "[Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt](#)".

- Cloud Deployment Manager V2-API
- Cloud-ProtokollierungsAPI
- Cloud Resource Manager API
- Compute Engine-API
- IAM-API (Identitäts- und Zugriffsmanagement)

## **Einen Konnektor erstellen**

Erstellen Sie einen Connector in Google Cloud direkt über die BlueXP-Benutzeroberfläche oder über gcloudbasierte Benutzeroberfläche.

## BlueXP

1. Wenn Sie Ihre erste Arbeitsumgebung erstellen, klicken Sie auf **Arbeitsumgebung hinzufügen** und befolgen Sie die Anweisungen. Klicken Sie andernfalls auf das Dropdown-Menü **Connector** 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. Klicken Sie auf **Weiter**, um die Bereitstellung mithilfe des Produktleitfadens vorzubereiten. Jeder Schritt im Produktleitfaden enthält die Informationen, die auf dieser Seite der Dokumentation enthalten sind.
  - b. Klicken Sie auf **Skip to Deployment**, wenn Sie bereits mit den Schritten auf dieser Seite vorbereitet sind.
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.
  - **Firewall-Richtlinie:** Wählen Sie, ob Sie eine neue Firewall-Richtlinie erstellen oder eine vorhandene Firewall-Richtlinie auswählen möchten, die einen eingehenden HTTP-, HTTPS- und SSH-Zugriff erlaubt.
  - **Review:** Überprüfen Sie Ihre Auswahl, um zu überprüfen, ob Ihre Einrichtung korrekt ist.
5. Klicken Sie Auf **Hinzufügen**.

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



## GCloud

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 den NetApp Account an, der mit dem Connector verknüpft werden soll.

["Informationen zu NetApp Accounts"](#).

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

## Ergebnis

Der Connector ist jetzt mit Ihrem NetApp Konto installiert und eingerichtet. BlueXP verwendet diesen Connector automatisch, wenn Sie neue Arbeitsumgebungen erstellen. Aber wenn Sie mehr als einen Connector haben, müssen Sie dies tun ["Wechseln Sie zwischen ihnen"](#).

Wenn Sie Google Cloud Storage Buckets im gleichen Google Cloud-Konto haben, wo Sie den Connector erstellt haben, wird automatisch eine Google Cloud Storage-Arbeitsumgebung auf dem Bildschirm angezeigt. ["Erfahren Sie mehr darüber, was Sie mit dieser Arbeitsumgebung tun können"](#).

## Offener Port 3128 für AutoSupport-Meldungen

Wenn Sie Cloud Volumes ONTAP-Systeme in einem Subnetz bereitstellen möchten, in dem keine ausgehende Internetverbindung verfügbar ist, konfiguriert BlueXP Cloud Volumes ONTAP automatisch für die Verwendung des Connectors als Proxyserver.

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.

Wenn Sie die Standardsicherheitsgruppe für Cloud Volumes ONTAP verwenden, sind keine Änderungen an der Sicherheitsgruppe erforderlich. Wenn Sie aber strenge ausgehende Regeln für Cloud Volumes ONTAP definieren möchten, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *Outbound*-Verbindungen über Port 3128 zulässt.

## Einen Konnektor in einer Regierungsregion erstellen

Wenn Sie in einer Regierungsregion tätig sind, müssen Sie einen Connector vom Markt Ihres Cloud-Providers bereitstellen oder die Connector-Software manuell auf einem vorhandenen Linux-Host installieren. Sie können den Connector nicht auf der SaaS-Website von BlueXP in einer Regierungsregion bereitstellen.

Verwenden Sie einen der folgenden Links, um Anweisungen zum Erstellen eines Connectors anzuzeigen:

- ["Erstellen Sie einen Connector aus dem AWS Marketplace"](#)
- ["Erstellung eines Connectors und einer Cloud Volumes ONTAP in der AWS C2S-Umgebung"](#)
- ["Erstellen Sie einen Connector aus dem Azure Marketplace"](#)
- ["Installieren Sie einen Connector auf Ihrem eigenen Linux-Host"](#)

Für manuelle Installationen auf Ihrem eigenen Linux-Host müssen Sie den Connector mit dem „Online“-Installationsprogramm auf einem Host mit Internetzugang installieren. Für den Connector steht ein separates „Offline“-Installationsprogramm zur Verfügung, es wird jedoch nur von On-Prem-Websites unterstützt, die keinen Internetzugang haben. In Regierungsregionen wird es nicht unterstützt.

Nachdem Sie den Connector bereitgestellt haben, können Sie auf BlueXP zugreifen, indem Sie Ihren Webbrowser öffnen und eine Verbindung mit der IP-Adresse der Connector-Instanz herstellen:  
`https://ipaddress[]`

Da der Connector in einer Regierungsregion eingesetzt wurde, ist er von nicht zugänglich <https://console.bluelxp.netapp.com>.

## Copyright-Informationen

Copyright © 2022 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.