



Richten Sie BlueXP ein und verwalten Sie sie

Set up and administration

NetApp
December 01, 2022

Inhaltsverzeichnis

| | |
|--|-----|
| Richten Sie BlueXP ein und verwalten Sie sie | 1 |
| Versionshinweise | 2 |
| Was ist neu | 2 |
| Bekannte Einschränkungen | 12 |
| Los geht's | 15 |
| Erfahren Sie mehr über BlueXP | 15 |
| Checkliste für die ersten Schritte | 16 |
| Melden Sie sich bei BlueXP an | 20 |
| Richten Sie einen NetApp Account ein | 22 |
| Richten Sie einen Konnektor ein | 31 |
| Weitere Schritte | 71 |
| Verwalten von BlueXP | 72 |
| NetApp Accounts | 72 |
| Anschlüsse | 87 |
| PAYGO-Abonnements und -Verträge verwalten | 119 |
| Cloud Storage erkannt | 121 |
| AWS Zugangsdaten | 126 |
| Azure Zugangsdaten | 135 |
| Google Cloud-Anmeldedaten | 148 |
| Fügen Sie Konten der NetApp Support Site in BlueXP hinzu und managen Sie sie | 156 |
| Meine Opportunitys | 163 |
| Referenz | 164 |
| Berechtigungen | 164 |
| Ports | 216 |
| Wissen und Support | 221 |
| Für den Support anmelden | 221 |
| Holen Sie sich Hilfe | 225 |
| Rechtliche Hinweise | 229 |
| Urheberrecht | 229 |
| Marken | 229 |
| Patente | 229 |
| Datenschutzrichtlinie | 229 |
| Open Source | 229 |

Richten Sie BlueXP ein und verwalten Sie sie

Versionshinweise

Was ist neu

Neue Funktionen bei der Administration von BlueXP (ehemals Cloud Manager): NetApp Accounts, Connectors, Anmeldedaten für Cloud-Provider und vieles mehr.

6. November 2022

Anschluss 3.9.23

- Ihre PAYGO-Abonnements und Jahresverträge für BlueXP sind jetzt für die Anzeige und Verwaltung über das Digital Wallet verfügbar.

["Hier erfahren Sie, wie Sie Ihre Abonnements verwalten"](#)

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

["Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"](#)

November 2022

Cloud Manager fordert Sie jetzt auf, die mit Ihren Accounts der NetApp Support Website verbundenen Anmeldeinformationen zu aktualisieren, wenn das mit Ihrem Konto verknüpfte Aktualisierungs-Token nach 3 Monaten abläuft. ["Erfahren Sie, wie Sie NSS-Konten verwalten"](#)

18. September 2022

Anschluss 3.9.22

- Wir haben den Connector Deployment Wizard erweitert, indem wir eine *in-Product Guide* hinzufügen, die Schritte zur Erfüllung der Mindestanforderungen für die Installation von Konnektor enthält: Berechtigungen, Authentifizierung und Netzwerke.
- Sie können nun einen NetApp Support-Fall direkt über Cloud Manager im **Support Dashboard** erstellen.

["Erfahren Sie, wie Sie einen Fall erstellen"](#).

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

["Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"](#)

31 Juli 2022

Anschluss 3.9.21

- Wir haben eine neue Methode eingeführt, um die vorhandenen Cloud-Ressourcen zu ermitteln, die Sie noch nicht in Cloud Manager verwalten.

Auf dem Canvas bietet die Registerkarte ** My Opportunities** einen zentralen Ort, um vorhandene Ressourcen zu entdecken, die Sie in Cloud Manager hinzufügen können, um konsistente Datenservices

und Abläufe in Ihrer gesamten hybriden Multi-Cloud zu erhalten.

In dieser ersten Version können Sie mit My Opportunities vorhandene FSX für ONTAP Dateisysteme in Ihrem AWS-Konto entdecken.

["Entdecken Sie FSX für ONTAP mithilfe von My Opportunities"](#)

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

["Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"](#)

15 Juli 2022

Richtlinienänderungen

Wir haben die Dokumentation aktualisiert und die Cloud Manager Richtlinien direkt in den Dokumenten hinzugefügt. Das bedeutet, dass Sie nun die erforderlichen Berechtigungen für den Konnektor und Cloud Volumes ONTAP direkt neben den Schritten anzeigen können, wie Sie diese einrichten. Auf diese Richtlinien konnte bisher über eine Seite der NetApp Support Site zugegriffen werden.

["Das Beispiel zeigt die AWS IAM-Rollenberechtigungen, die zum Erstellen eines Konnektors verwendet werden"](#).

Außerdem haben wir eine Seite erstellt, die Links zu den einzelnen Richtlinien enthält. ["Zeigen Sie die Berechtigungsübersicht für Cloud Manager an"](#).

3 Juli 2022

Anschluss 3.9.20

- Jetzt haben wir eine neue Methode eingeführt, um auf die wachsende Liste von Funktionen in der Cloud Manager Benutzeroberfläche zu navigieren. Alle vertrauten Funktionen von Cloud Manager sind jetzt leicht zu finden, indem Sie den Mauszeiger über das linke Feld halten.



- Sie können Cloud Manager jetzt so konfigurieren, dass Sie Benachrichtigungen per E-Mail versenden, damit Sie über wichtige Systemaktivitäten informiert werden können, auch wenn Sie nicht im System angemeldet sind.

["Weitere Informationen zu Überwachungsvorgängen in Ihrem Konto".](#)

- Cloud Manager unterstützt jetzt Azure Blob Storage und Google Cloud Storage als Arbeitsumgebungen, ähnlich der Unterstützung von Amazon S3.

Nach der Installation eines Connectors in Azure oder Google Cloud erkennt Cloud Manager jetzt automatisch Informationen über Azure Blob Storage in Ihrem Azure Abonnement oder Google Cloud Storage in dem Projekt, in dem der Connector installiert wird. Cloud Manager zeigt den Objekt-Storage als Arbeitsumgebung an, in der detailliertere Informationen angezeigt werden können.

Hier ein Beispiel für eine Azure Blob-Arbeitsumgebung:

Azure blob

Overview

637

Total Storage Accounts

1.5

TiB

Total Capacity

16

Total Locations

637

Storage Accounts

| Storage Account Name | Subscription | Location | Creation Date | Resource Group | Blob Capacity |
|----------------------|--------------|----------------|-------------------|----------------|---------------|
| ovu8llxvqdfypxn | OCCM QA1 | West US | June 24, 2021 | AdmAzureHa-rg | 170 B |
| rootsa9ktpjzcm | OCCM QA1 | West US | June 24, 2021 | AdmAzureHa-rg | 950.22 GiB |
| scvdwjcwehswli | OCCM QA1 | West US | June 24, 2021 | AdmAzureHa-rg | 22.12 MiB |
| 65qtx0smegmq2vt | OCCM QA1 | West US | June 24, 2021 | AdmAzureVsa-rg | 170 B |
| bu9klxthymr1be | OCCM QA1 | West US | June 24, 2021 | AdmAzureVsa-rg | 1.01 MiB |
| 8jzsvybvjiwieww8 | OCCM QA1 | Canada Central | December 12, 2019 | aff1-rg | 170 B |

- Wir haben die Seite „Ressourcen“ für eine Amazon S3-Arbeitsumgebung neu gestaltet und ausführlichere Informationen zu S3-Buckets wie Kapazität, Verschlüsselungsdetails usw. bereitgestellt.
- Der Connector wird nun in folgenden Google Cloud Regionen unterstützt:
 - Madrid (europa-Südwest1)
 - Paris (europawest9)
 - Warschau (europa-Zentralin2)
- Der Connector wird nun in der Region Azure West US 3 unterstützt.

["Hier finden Sie die vollständige Liste der unterstützten Regionen"](#)

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen.

["Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"](#)

28. Juni 2022

Loggen Sie sich mit NetApp Anmeldedaten ein

Wenn sich neue Benutzer bei Cloud Central anmelden, können sie jetzt die Option **mit NetApp** anmelden und sich mit ihren NetApp Support Site Anmeldedaten anmelden. Dies ist eine Alternative zur Eingabe einer E-Mail-Adresse und eines Kennworts.



Vorhandene Anmeldungen, die eine E-Mail-Adresse und ein Passwort verwenden, müssen diese Anmeldemethode beibehalten. Die Option „mit NetApp anmelden“ ist für neue Benutzer verfügbar, die sich anmelden.

7. Juni 2022

Anschluss 3.9.19

- Der Connector wird nun in der Region AWS Jakarta unterstützt (AP-Südost-3).

- Der Connector wird nun in der Region Azure Brazil Southeast unterstützt.

["Hier finden Sie die vollständige Liste der unterstützten Regionen"](#)

- Diese Version des Connectors enthält außerdem Cloud Volumes ONTAP-Verbesserungen und On-Premises-ONTAP-Cluster-Verbesserungen.
 - ["Erfahren Sie mehr über Verbesserungen bei Cloud Volumes ONTAP"](#)
 - ["Die ONTAP-On-Premises-Cluster-Verbesserungen"](#)

12 Mai 2022

Patch-Anschluss 3.9.18

Wir haben den Connector aktualisiert, um Bug Fixes einzuführen. Die bemerkenswerteste Lösung ist ein Problem, das die Cloud Volumes ONTAP-Implementierung in Google Cloud beeinflusst, wenn der Connector in einer gemeinsamen VPC ausgeführt wird.

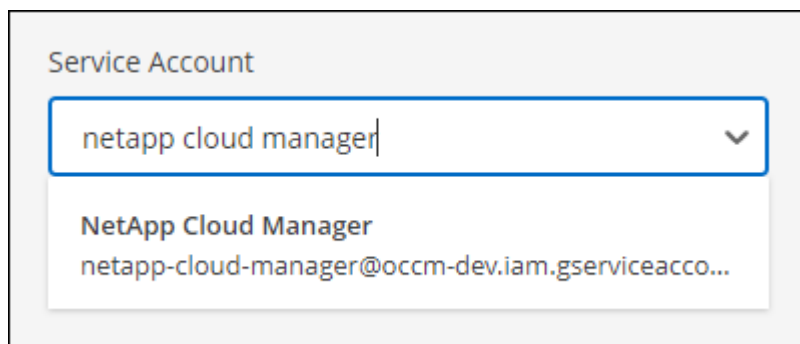
Mai 2022

Anschluss 3.9.18

- Der Connector wird nun in folgenden Google Cloud Regionen unterstützt:
 - Delhi (asien-Süd-2)
 - Melbourne (australien-Südheast2)
 - Mailand (europa-West8)
 - Santiago (southamerica-west1)

["Hier finden Sie die vollständige Liste der unterstützten Regionen"](#)

- Wenn Sie das Google Cloud-Servicekonto auswählen, das mit dem Connector verwendet werden soll, zeigt Cloud Manager jetzt die E-Mail-Adresse an, die mit jedem Dienstkonto verknüpft ist. Durch das Anzeigen der E-Mail-Adresse kann es leichter sein, zwischen Servicekonten, die denselben Namen haben, zu unterscheiden.



- Wir haben den Connector in Google Cloud auf einer VM-Instanz mit einem Betriebssystem zertifiziert, das unterstützt ["Geschirmte VM-Funktionen"](#)
- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen. ["Erfahren Sie mehr über diese Verbesserungen"](#)
- Für den Connector zur Implementierung von Cloud Volumes ONTAP sind neue AWS Berechtigungen

erforderlich.

Bei der Implementierung eines HA-Paars in einer einzelnen Verfügbarkeitszone (AZ) sind nun die folgenden Berechtigungen erforderlich, um eine AWS Spread-Placement-Gruppe zu erstellen:

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy"
```

Diese Berechtigungen sind nun erforderlich, um die Erstellung der Platzierungsgruppe durch Cloud Manager zu optimieren.

Stellen Sie unbedingt diese Berechtigungen für jeden Satz von AWS Zugangsdaten bereit, die Sie Cloud Manager hinzugefügt haben. ["Sehen Sie sich die aktuelle IAM-Richtlinie für den Connector an"](#).

3. April 2022

Anschluss 3.9.17

- Sie können jetzt einen Connector erstellen, indem Sie Cloud Manager eine IAM-Rolle übernehmen lassen, die Sie in Ihrer Umgebung eingerichtet haben. Diese Authentifizierungsmethode ist sicherer als die gemeinsame Nutzung eines AWS Zugriffsschlüssels und eines Geheimschlüssels.

["Erfahren Sie, wie Sie einen Konnektor mithilfe einer IAM-Rolle erstellen"](#).

- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen. ["Erfahren Sie mehr über diese Verbesserungen"](#)

27 Februar 2022

Anschluss 3.9.16

- Wenn Sie einen neuen Connector in Google Cloud erstellen, zeigt Cloud Manager jetzt alle bestehenden Firewall-Richtlinien an. Zuvor wurden in Cloud Manager keine Richtlinien angezeigt, für die kein Ziel-Tag vorhanden war.
- Diese Version des Connectors enthält auch Cloud Volumes ONTAP-Verbesserungen. ["Erfahren Sie mehr über diese Verbesserungen"](#)

30 Januar 2022

Anschluss 3.9.15

Diese Version des Connectors enthält Cloud Volumes ONTAP-Verbesserungen. ["Erfahren Sie mehr über diese Verbesserungen"](#)

Januar 2022

Verringerte Endpunkte für den Konnektor

Wir reduzieren die Anzahl der Endpunkte, die ein Connector kontaktieren muss, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu verwalten.

"Zeigen Sie die Liste der erforderlichen Endpunkte an"

EBS-Festplattenverschlüsselung für den Connector

Wenn Sie einen neuen Connector in AWS über Cloud Manager implementieren, können Sie sich jetzt entscheiden, die EBS-Festplatten des Connectors über den Standard-Master-Schlüssel oder einen gemanagten Schlüssel zu verschlüsseln.

The screenshot displays the 'Details' configuration page for an AWS Connector. At the top, a progress bar shows steps: Get Ready, AWS Credentials, Details (active), Network, Security Group, and Review. The 'Connector Instance Name' is set to 'Connector1'. Under 'Connector Role', the 'Create Role' option is selected. The 'Role Name' is 'Cloud-Manager-Operator-9yils3K'. A black arrow points to the 'AWS Managed Encryption' toggle, which is turned on. Below this, the 'Master Key' is 'aws/ebs (default)' with a 'Change Key' link. There is also a link to 'Add Tags to Connector Instance'.

E-Mail-Adresse für NSS-Konten

Cloud Manager kann jetzt die E-Mail-Adresse anzeigen, die mit einem NetApp Support Site Konto verknüpft ist.



28. November 2021

Update für NetApp Support Site Accounts erforderlich

Ab Dezember 2021 verwendet NetApp jetzt Microsoft Azure Active Directory als Identitäts-Provider für speziell auf Support und Lizenzierung spezifische Authentifizierungs-Services. Aufgrund dieses Updates werden Sie von Cloud Manager aufgefordert, die Anmeldedaten für alle bereits hinzugefügten NetApp Support Site Konten zu aktualisieren.

Wenn Sie Ihr NSS-Konto noch nicht zu IDaaS migriert haben, müssen Sie zunächst das Konto migrieren und dann Ihre Zugangsdaten in Cloud Manager aktualisieren.

- ["Erfahren Sie, wie Sie ein NSS-Konto auf die neue Authentifizierungsmethode aktualisieren"](#).
- ["Erfahren Sie mehr über die Verwendung von Microsoft Azure AD durch NetApp zum Identitätsmanagement"](#)

NSS-Konten für Cloud Volumes ONTAP ändern

Wenn Ihr Unternehmen über mehrere NetApp Support Site Accounts verfügt, können Sie jetzt ändern, welches Konto einem Cloud Volumes ONTAP System zugeordnet ist.

["Erfahren Sie, wie Sie eine Arbeitsumgebung an ein anderes NSS-Konto anschließen"](#).

4. November 2021

SOC 2 Typ 2-Zertifizierung

Ein unabhängiger, zertifizierter Wirtschaftsprüfer hat Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense und Cloud Backup (Cloud Manager Plattform) geprüft und bestätigt, dass sie SOC 2 Typ 2 Berichte basierend auf den entsprechenden Kriterien der Trust Services erstellt haben.

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

Connector wird nicht mehr als Proxy unterstützt

Sie können den Cloud-Manageranschluss nicht mehr als Proxyserver verwenden, um AutoSupport-Nachrichten von Cloud Volumes ONTAP zu senden. Diese Funktion wurde entfernt und wird nicht mehr unterstützt. Sie müssen AutoSupport-Konnektivität über eine NAT-Instanz oder Proxy-Services Ihrer Umgebung bereitstellen.

["Erfahren Sie mehr über die Überprüfung von AutoSupport mit Cloud Volumes ONTAP"](#)

Oktober 31 2021

Authentifizierung mit Service-Principal

Wenn Sie einen neuen Connector in Microsoft Azure erstellen, können Sie sich jetzt mit einem Azure-Dienstprincipal authentifizieren, anstatt mit den Azure-Konto-Anmeldedaten.

["Informieren Sie sich, wie Sie sich mit einem Azure-Service-Principal authentifizieren"](#).

Verbesserung der Anmeldeinformationen

Die Credentials-Seite wurde neu gestaltet. Dies ist benutzerfreundlich und passt genau zu dem aktuellen Look and Feel der Cloud Manager-Oberfläche.

September 2021

Ein neuer Benachrichtigungsdienst wurde hinzugefügt

Der Benachrichtigungsservice wurde eingeführt, sodass Sie den Status der Cloud Manager Vorgänge anzeigen können, die Sie während Ihrer aktuellen Anmeldesitzung initiiert haben. Sie können überprüfen, ob der Vorgang erfolgreich war oder ob er fehlgeschlagen ist. ["Erfahren Sie, wie Sie die Vorgänge in Ihrem Konto überwachen"](#).

August 2021

Unterstützung für RHEL 7.9 mit dem Connector

Der Connector wird jetzt auf einem Host unterstützt, auf dem Red hat Enterprise Linux 7.9 ausgeführt wird.

["Lesen Sie die Systemanforderungen für den Konnektor"](#).

7 Juli 2021

Erweiterungen des Assistenten zum Hinzufügen von Konnektor

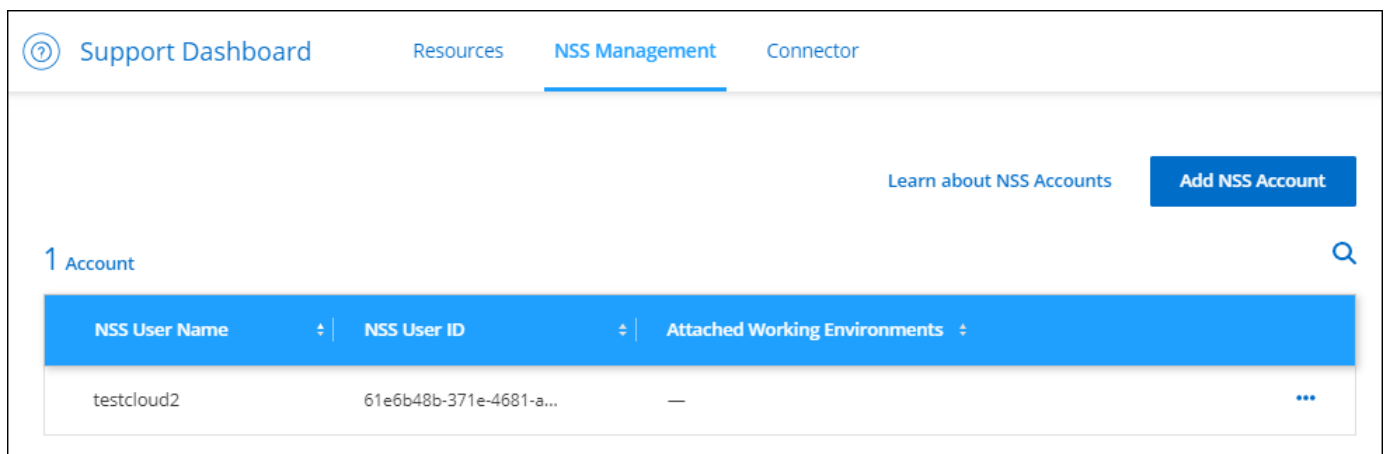
Wir haben den Assistenten **Connector** neu gestaltet, um neue Optionen hinzuzufügen und die Bedienung zu vereinfachen. Sie können nun Tags hinzufügen, eine Rolle angeben (für AWS oder Azure), ein Root-Zertifikat für einen Proxy-Server hochladen, Code für die Terraform-Automatisierung anzeigen, Fortschrittsdetails anzeigen und mehr.

- ["Connector in AWS erstellen"](#)
- ["Connector in Azure erstellen"](#)
- ["Connector in GCP erstellen"](#)

NSS Account-Management über das Support Dashboard

NSS-Konten (NetApp Support Site) werden jetzt über das Support-Dashboard gemanagt anstatt über das Menü „Einstellungen“. Durch diese Änderung finden und managen Sie alle Support-Informationen einfacher über eine zentrale Stelle.

["Erfahren Sie, wie Sie NSS-Konten verwalten"](#).



| NSS User Name | NSS User ID | Attached Working Environments |
|---------------|-------------------------|-------------------------------|
| testcloud2 | 61e6b48b-371e-4681-a... | — |

5 Mai 2021

Konten in der Zeitleiste

In der Zeitleiste in Cloud Manager werden jetzt Aktionen und Ereignisse im Zusammenhang mit der Kontoverwaltung angezeigt. Zu den Aktionen gehören u. a. die Verknüpfung von Benutzern, die Erstellung von Arbeitsbereichen und die Erstellung von Connectors. Das Prüfen der Zeitleiste kann hilfreich sein, wenn Sie feststellen müssen, wer eine bestimmte Aktion durchgeführt hat oder ob Sie den Status einer Aktion identifizieren müssen.

["Erfahren Sie, wie Sie den Zeitplan für den Service für die Mandantenfähigkeit filtern"](#).

11. April 2021

API-Aufrufe direkt an Cloud Manager

Wenn Sie einen Proxy-Server konfiguriert haben, können Sie nun eine Option aktivieren, mit der Sie API-Aufrufe direkt an Cloud Manager senden können, ohne über den Proxy zu gehen. Diese Option wird mit Connectors unterstützt, die in AWS oder in Google Cloud ausgeführt werden.

["Erfahren Sie mehr über diese Einstellung".](#)

Benutzer des Servicekontos

Sie können jetzt ein Dienstkonto-Benutzer erstellen.

Ein Service-Konto fungiert als „Benutzer“, der autorisierte API-Aufrufe an Cloud Manager zur Automatisierung vornehmen kann. So ist das Management der Automatisierung einfacher, da keine Automatisierungsskripts auf Basis des Benutzerkontos eines echten Mitarbeiters erstellt werden müssen, der das Unternehmen jederzeit verlassen kann. Und bei Verwendung von Federation können Sie ein Token erstellen, ohne ein Update-Token aus der Cloud zu generieren.

["Erfahren Sie mehr über die Verwendung von Servicekonten".](#)

Private Vorschauen

Private Vorschauen in Ihrem Konto können Sie jetzt auf neue NetApp Cloud-Services zugreifen, sobald diese in Cloud Manager als Vorschau verfügbar gemacht werden.

["Weitere Informationen zu dieser Option".](#)

Drittanbieter-Services

Sie haben auch die Möglichkeit, dass Drittanbieterservices in Ihrem Konto Zugriff auf in Cloud Manager verfügbare Drittanbieter-Services erhalten.

["Weitere Informationen zu dieser Option".](#)

9 Februar 2021

Verbesserungen am Support Dashboard

Wir haben das Support Dashboard aktualisiert, damit Sie Ihre Zugangsdaten für die NetApp Support Website hinzufügen können. Damit registrieren Sie sich für den Support. Sie können auch einen NetApp Support-Fall direkt über das Dashboard initiieren. Klicken Sie einfach auf das Hilfesymbol und dann auf **Support**.

Bekannte Einschränkungen

Bekannte Einschränkungen identifizieren Plattformen, Geräte oder Funktionen, die von dieser Version des Produkts nicht unterstützt werden oder nicht korrekt mit dem Produkt zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Diese Einschränkungen gelten insbesondere für die Einrichtung und Administration von BlueXP: Der Connector, die SaaS-Plattform und vieles mehr.

Einschränkungen an den Anschlüssen

Möglicher Konflikt mit IP-Adressen im Bereich 172

BlueXP implementiert den Connector mit zwei Schnittstellen, die IP-Adressen in den Bereichen 172.17.0.0/16 und 172.18.0.0/16 haben.

Wenn Ihr Netzwerk über ein Subnetz verfügt, das mit einem dieser Bereiche konfiguriert ist, können

Verbindungsfehler von BlueXP auftreten. Beispielsweise schlägt die Erkennung von lokalen ONTAP Clustern in BlueXP fehl.

Siehe Knowledge Base-Artikel ["BlueXP Connector IP-Konflikt mit vorhandenem Netzwerk"](#) Anweisungen zum Ändern der IP-Adresse der Schnittstellen des Connectors.

Es wird nur ein HTTP-Proxyserver unterstützt

Wenn Sie in Ihren Unternehmensrichtlinien einen Proxyserver für die gesamte HTTP-Kommunikation mit dem Internet verwenden müssen, müssen Sie Ihre Connectors so konfigurieren, dass sie diesen HTTP-Proxyserver verwenden. Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.

BlueXP unterstützt die Verwendung eines HTTPS-Proxys mit dem Connector nicht.

SSL-Entschlüsselung wird nicht unterstützt

BlueXP unterstützt keine Firewall-Konfigurationen, bei denen die SSL-Entschlüsselung aktiviert ist. Wenn die SSL-Entschlüsselung aktiviert ist, werden Fehlermeldungen in BlueXP angezeigt, und die Connector-Instanz wird als inaktiv angezeigt.

Um die Sicherheit zu erhöhen, haben Sie die Möglichkeit ["Installieren eines von einer Zertifizierungsstelle \(CA\) signierten HTTPS-Zertifikats"](#).

Leere Seite beim Laden der lokalen Benutzeroberfläche

Wenn Sie die lokale Benutzeroberfläche für einen Konnektor laden, wird die Benutzeroberfläche manchmal nicht angezeigt, und Sie erhalten nur eine leere Seite.

Dieses Problem bezieht sich auf ein Caching-Problem. Die Problemumgehung besteht darin, eine Inkognito- oder private Webbrowser-Sitzung zu verwenden.

Freigegebene Linux-Hosts werden nicht unterstützt

Der Connector wird nicht von einer VM unterstützt, die gemeinsam mit anderen Anwendungen genutzt wird. Die VM muss der Connector-Software zugewiesen sein.

Agenten und Erweiterungen von Drittanbietern

Agenten von Drittanbietern oder VM-Erweiterungen werden auf der Connector-VM nicht unterstützt.

SaaS-Einschränkungen

Die SaaS-Plattform ist für Regierungsregionen deaktiviert

Wenn Sie einen Connector in einer AWS GovCloud Region, einer Azure Gov-Region oder einer Azure DoD-Region bereitstellen, steht der Zugriff auf BlueXP nur über die Host-IP-Adresse eines Connectors zur Verfügung. Der Zugriff auf die SaaS-Plattform ist für das gesamte Konto deaktiviert.

Das bedeutet, dass nur privilegierte Benutzer, die auf die interne VPC/vnet des Endbenutzers zugreifen können, die UI oder API von BlueXP verwenden können.

Beachten Sie, dass nur Cloud Volumes ONTAP, Cloud-Backup, Cloud-Datensense und Replizierung unterstützt werden. Andere NetApp Services werden in Regionen der öffentlichen Hand nicht unterstützt.

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

Einschränkungen des Marktes

Für Azure und Google Cloud Partner ist kein „Pay-as-you-go“-Modell verfügbar

Wenn Sie ein Microsoft Cloud Solution Provider (CSP)-Partner oder Google Cloud-Partner sind, stehen NetApp Pay-as-you-go-Abonnements nicht zur Verfügung. Kunden müssen eine Lizenz erwerben und NetApp Cloud-Lösungen mit einer BYOL-Lizenz implementieren.

Abonnements auf Nutzung sind für die folgenden NetApp Cloud-Services nicht verfügbar:

- Cloud Volumes ONTAP
- Cloud Tiering
- Cloud-Backup
- Cloud-Daten Sinnvoll

Los geht's

Erfahren Sie mehr über BlueXP

BlueXP (früher Cloud Manager) bietet IT-Experten und Cloud-Architekten die Möglichkeit, ihre Hybrid-Multi-Cloud-Infrastruktur mithilfe der Cloud-Lösungen von NetApp zentral zu managen.

Funktionen

BlueXP ist eine SaaS-basierte Managementplattform der Enterprise-Klasse, die Ihnen unabhängig vom Speicherort die Kontrolle über Ihre Daten gibt.

- Einrichtung und Verwendung ["Cloud Volumes ONTAP"](#) Für effizientes, Cloud-übergreifendes Multi-Protokoll-Datenmanagement
- Einrichten und Verwenden von File-Storage-Services:
 - ["Azure NetApp Dateien"](#)
 - ["Amazon FSX für ONTAP"](#)
 - ["Cloud Volumes Service für AWS"](#)
 - ["Cloud Volumes Service für Google Cloud"](#)
- Lokale ONTAP-Cluster erkennen und managen, indem sie Volumes erstellen, Backups in der Cloud erstellen, Daten in der gesamten Hybrid Cloud replizieren und selten genutzte Daten per Tiering in die Cloud verschieben.
- Nutzung integrierter Cloud-Services wie:
 - ["Cloud-Daten Sinnvoll"](#)
 - ["Einblicke in die Cloud"](#)
 - ["Cloud-Backup"](#)

["Erfahren Sie mehr über BlueXP"](#).

Unterstützte Objekt-Storage-Provider

Mit BlueXP können Sie Cloud-Storage managen und Cloud-Services in Amazon Web Services, Microsoft Azure und Google Cloud nutzen.

Kosten

NetApp Software BlueXP ist kostenfrei.

Bei den meisten Aufgaben fordert BlueXP Sie zur Bereitstellung eines Connectors in Ihrem Cloud-Netzwerk auf. Dies führt zu Gebühren Ihres Cloud-Providers für die Computing-Instanz und den zugehörigen Speicher. Sie haben die Möglichkeit, die Connector-Software vor Ort auszuführen.

["Informieren Sie sich über die Standardkonfiguration des Connectors"](#).

Funktionsweise von BlueXP

BlueXP verfügt über eine SaaS-basierte Schnittstelle, die in die BlueXP-Website integriert ist, und Connectors, die Cloud Volumes ONTAP und andere Cloud-Services verwalten.

Software-as-a-Service

Auf BlueXP kann über eine zugriffen werden ["SaaS-basierte Benutzeroberfläche"](#) Und APIs. Mit dieser SaaS-Erfahrung können Sie bei Veröffentlichung automatisch auf die neuesten Funktionen zugreifen und einfach zwischen Ihren NetApp Konten und Connectors wechseln.



Wenn Sie in einer Umgebung arbeiten, in der kein abgehender Internetzugang verfügbar ist, können Sie die Connector-Software in dieser Umgebung installieren und auf die lokale Benutzeroberfläche zugreifen, die auf dem Connector verfügbar ist. ["Erfahren Sie mehr über Steckverbinder"](#).

BlueXP-Website

["Die BlueXP-Website"](#) Bietet einen zentralen Standort für den Zugriff und das Management ["NetApp Cloud-Services"](#). Dank der zentralen Benutzerauthentifizierung können Sie dieselben Anmeldedaten für den Zugriff auf BlueXP und andere Cloud-Services wie Cloud Insights verwenden.

NetApp Konto

Wenn Sie sich zum ersten Mal bei BlueXP anmelden, werden Sie aufgefordert, ein *NetApp Konto* zu erstellen. Dieses Konto bietet Mandantenfähigkeit und ermöglicht es Ihnen, Benutzer und Ressourcen in isolierten Arbeitsbereichen zu organisieren_.

Anschlüsse

In den meisten Fällen muss ein BlueXP Account Admin einen *Connector* in Ihrer Cloud oder Ihrem On-Premises-Netzwerk bereitstellen. Mit dem Connector kann BlueXP Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung verwalten.

["Erfahren Sie mehr darüber, wann Anschlüsse erforderlich sind und wie sie funktionieren"](#).

SOC 2 Typ 2-Zertifizierung

Ein unabhängiger, zertifizierter Wirtschaftsprüfer hat BlueXP, Cloud Sync, Cloud Tiering, Cloud Data Sense und Cloud Backup (BlueXP Plattform) geprüft und bestätigt, dass sie SOC 2 Type 2 Berichte basierend auf den entsprechenden Kriterien für die Trust Services erstellt haben.

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

Checkliste für die ersten Schritte

In dieser Checkliste erfahren Sie, was für die Inbetriebnahme von BlueXP in einer typischen Bereitstellung, in der der Connector über Outbound-Internetzugang verfügt, erforderlich ist.

Ein Login

Zur Anmeldung bei BlueXP können Sie Ihre Zugangsdaten für die NetApp Support Website nutzen oder sich mithilfe Ihrer E-Mail und eines Passworts für eine NetApp Cloud-Anmeldung anmelden. ["Erfahren Sie mehr über die Anmeldung"](#).

Netzwerkzugriff über einen Webbrowser zu mehreren Endpunkten

Die BlueXP-Benutzeroberfläche ist über einen Webbrowser zugänglich. Wenn Sie die Benutzeroberfläche von BlueXP verwenden, kontaktiert sie mehrere Endpunkte, um die Datenmanagement-Aufgaben abzuschließen. Das Gerät, auf dem der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen.

| Endpunkte | Zweck |
|--|---|
| http://cloudmanager.netapp.com | Ihr Webbrowser kontaktiert diese URL, wenn Sie die SaaS-Benutzeroberfläche verwenden. |
| AWS-Services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Cognito• Elastic Compute Cloud (EC2)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3) | Für die Bereitstellung eines Connectors von BlueXP in AWS erforderlich. Der genaue Endpunkt hängt von der Region ab, in der Sie den Connector bereitstellen. "Weitere Informationen finden Sie in der AWS-Dokumentation." |
| https://management.azure.com https://login.microsoftonline.com | Für die Implementierung eines Connectors von BlueXP in den meisten Azure Regionen erforderlich. |
| https://management.microsoftazure.de https://login.microsoftonline.de | Für die Implementierung eines Connectors von BlueXP in Azure-Regionen in Deutschland erforderlich. |
| https://management.usgovcloudapi.net https://login.microsoftonline.com | Erforderlich für die Bereitstellung eines Connectors von BlueXP in Azure US Gov Regionen. |
| https://www.googleapis.com | Erforderlich, um einen Connector von BlueXP in Google Cloud bereitzustellen. |
| https://signin.b2c.netapp.com | Erforderlich, um die Zugangsdaten für die NetApp Support Site (NSS) zu aktualisieren oder neue NSS-Zugangsdaten für BlueXP hinzuzufügen |
| https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com | Ihr Webbrowser stellt eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung über BlueXP zu ermöglichen. |
| https://widget.intercom.io | Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht. |

| Endpunkte | Zweck |
|-------------------------------|--|
| Die IP-Adresse des Connectors | <p>In den meisten Fällen sollten Sie mit BlueXP von der SaaS-UI arbeiten, aber "Wenn Sie die lokale UI verwenden", Dann müssen Sie die IP-Adresse des Hosts von einem Web-Browser eingeben.</p> <p>Verwenden Sie je nach Anbindung an Ihren Cloud-Provider die private IP oder eine dem Host zugewiesene öffentliche IP:</p> <ul style="list-style-type: none"> • Eine private IP funktioniert, wenn Sie über ein VPN und direkten Zugriff auf Ihr virtuelles Netzwerk verfügen • Eine öffentliche IP funktioniert in jedem Netzwerkszenario <p>In beiden Fällen ist ein sicherer Netzwerkzugriff möglich, da die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.</p> |

Ausgehende Netzwerke für einen Konnektor

Nach der Anmeldung bei BlueXP muss ein BlueXP Account Admin einen *Connector* bei einem Cloud-Provider oder in Ihrem On-Premises-Netzwerk bereitstellen. Mit dem Connector kann BlueXP Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung verwalten. Beachten Sie, dass für die meisten, aber nicht für alle Services und Funktionen in BlueXP ein Connector erforderlich ist. "[Erfahren Sie mehr über Steckverbinder und deren Funktionsweise](#)".

- Der Netzwerkspeicherort, an dem Sie den Connector bereitstellen, muss über eine ausgehende Internetverbindung verfügen.

Für den Konnektor ist ein abgehender Internetzugang erforderlich, um die folgenden Endpunkte zu kontaktieren, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu verwalten.

| Endpunkte | Zweck |
|--|---|
| https://support.netapp.com | Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden. |
| https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com | 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. |

- Wenn Sie den Connector manuell auf Ihrem eigenen Linux-Host installieren möchten (und dies nicht direkt über die BlueXP-Schnittstelle), benötigt das Installationsprogramm für den Connector während des Installationsvorgangs Zugriff auf die folgenden Endpunkte:
 - <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
 - https://*.blob.core.windows.net oder <https://hub.docker.com>

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

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

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.

Berechtigungen für Cloud-Provider

Sie benötigen ein Konto, das über die Berechtigungen zum Bereitstellen des Connectors bei Ihrem Cloud-Provider direkt über BlueXP verfügt.



Es gibt alternative Möglichkeiten, einen Konnektor zu erstellen: Sie können einen Konnektor aus dem erstellen "[AWS Marketplace](#)", Das "[Azure Marketplace](#)", Oder Sie können "[Software manuell installieren](#)".

| Standort | Allgemeine Schritte | Detaillierte Schritte |
|----------|--|---|
| AWS | <ol style="list-style-type: none">1. Verwenden Sie eine JSON-Datei mit den erforderlichen Berechtigungen zum Erstellen einer IAM-Richtlinie in AWS.2. Hängen Sie die Richtlinie an eine IAM-Rolle oder einen IAM-Benutzer an.3. Wenn Sie den Connector erstellen, stellen Sie BlueXP das ARN der IAM-Rolle oder den AWS-Zugriffsschlüssel und den geheimen Schlüssel für den IAM-Benutzer zur Verfügung. | " Klicken Sie hier, um die detaillierten Schritte anzuzeigen ". |
| Azure | <ol style="list-style-type: none">1. Verwenden Sie eine JSON-Datei, die die erforderlichen Berechtigungen zum Erstellen einer benutzerdefinierten Rolle in Azure enthält.2. Weisen Sie die Rolle dem Benutzer zu, der den Connector aus BlueXP erstellt.3. Wenn Sie den Connector erstellen, melden Sie sich mit dem Microsoft-Konto an, das über die erforderlichen Berechtigungen verfügt (die Anmeldeaufforderung, die Eigentum von Microsoft ist und von Microsoft gehostet wird). | " Klicken Sie hier, um die detaillierten Schritte anzuzeigen ". |

| Standort | Allgemeine Schritte | Detaillierte Schritte |
|--------------|---|--|
| Google Cloud | <ol style="list-style-type: none"> 1. Verwenden Sie eine YAML-Datei, die die erforderlichen Berechtigungen zum Erstellen einer benutzerdefinierten Rolle in Google Cloud enthält. 2. Fügen Sie diese Rolle dem Benutzer an, der den Connector aus BlueXP erstellen wird. 3. Wenn Sie Cloud Volumes ONTAP verwenden möchten, richten Sie ein Servicekonto ein, das über die erforderlichen Berechtigungen verfügt. 4. Aktivieren Sie Google Cloud-APIs. 5. Wenn Sie den Connector erstellen, melden Sie sich mit dem Google-Konto an, das über die erforderlichen Berechtigungen verfügt (die Anmeldeaufforderung ist im Besitz von Google und wird von Google gehostet). | "Klicken Sie hier, um die detaillierten Schritte anzuzeigen" . |

Vernetzung für einzelne Services

Nach Abschluss der Einrichtung können Sie die Services von BlueXP nutzen. Beachten Sie, dass für jeden Service eigene Netzwerkanforderungen gelten. Weitere Informationen finden Sie auf den folgenden Seiten.

- ["Cloud Volumes ONTAP für AWS"](#)
- ["Cloud Volumes ONTAP für Azure"](#)
- ["Cloud Volumes ONTAP für GCP"](#)
- ["Datenreplizierung zwischen ONTAP Systemen"](#)
- ["Cloud Data Sense Implementieren"](#)
- ["ONTAP-Cluster vor Ort"](#)
- ["Cloud Tiering"](#)
- ["Cloud-Backup"](#)

Melden Sie sich bei BlueXP an

Über eine SaaS-basierte Benutzeroberfläche ist BlueXP über Ihren Webbrowser zugänglich.

Wenn Sie über eine Regierungsregion oder eine Website ohne Outbound-Internetzugang auf BlueXP zugreifen, müssen Sie sich bei der BlueXP-Benutzeroberfläche anmelden, die lokal auf dem Connector ausgeführt wird. ["Erfahren Sie, wie Sie auf die lokale Benutzeroberfläche des Connectors zugreifen können"](#).

Sie können sich unter BlueXP mit einer der folgenden Optionen anmelden:

- Ihre vorhandenen Zugangsdaten für die NetApp Support Site (NSS)

Wenn Sie diese Option verwenden, werden Ihre NSS-Anmeldedaten (NetApp Support Site) BlueXP im Support Dashboard nicht hinzugefügt. Um wichtige Workflows für Cloud Volumes ONTAP zu aktivieren, müssen Sie BlueXP Ihre NSS-Anmeldeinformationen hinzufügen. ["Erfahren Sie, wie Sie Ihre NSS-Anmeldedaten in BlueXP einfügen"](#).

- Nutzen Sie Ihre E-Mail-Adresse und ein Passwort, um sich bei einem NetApp Cloud-Login anzumelden

Diese Option unterstützt verbundene Verbindungen. Sie können sich mit Single Sign-On über Anmeldedaten aus Ihrem Unternehmensverzeichnis (föderierte Identität) anmelden. Weitere Informationen erhalten Sie im ["Hilfe-Center für BlueXP"](#) Und klicken Sie dann auf **Anmelde-Optionen**.

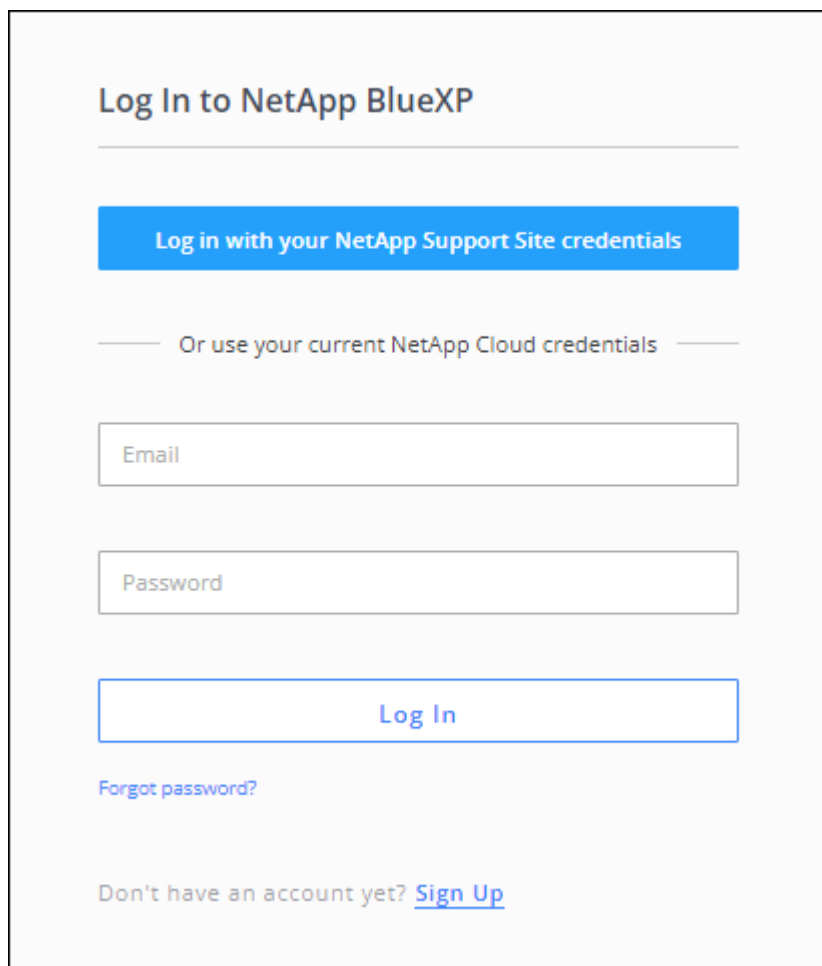
Bei jeder Anmeldung müssen Sie dieselbe Option verwenden, die Sie bei der ersten Anmeldung gewählt haben.

- Wenn Sie sich mit Ihren NetApp Support Site Anmeldedaten anmelden, müssen Sie diese Login-Option jedes Mal verwenden.
- Wenn Sie sich durch Eingabe Ihrer E-Mail und Ihres Kennworts angemeldet haben, müssen Sie diese Anmeldedaten jedes Mal eingeben, wenn Sie sich anmelden.

Schritte

1. Öffnen Sie einen Webbrowser, und rufen Sie den auf ["BlueXP-Konsole"](#)

Die Anmeldeseite für NetApp BlueXP wird angezeigt.



The screenshot shows the 'Log In to NetApp BlueXP' login page. At the top, the title 'Log In to NetApp BlueXP' is displayed. Below it is a blue button labeled 'Log in with your NetApp Support Site credentials'. Underneath this button is a separator line with the text 'Or use your current NetApp Cloud credentials'. Below the separator are two input fields: 'Email' and 'Password'. A 'Log In' button is positioned below the password field. At the bottom left, there is a link for 'Forgot password?'. At the bottom center, there is a link that says 'Don't have an account yet? Sign Up'.

2. Wählen Sie eine der Anmeldeoptionen:

- Wenn Sie zuvor NetApp Cloud-Anmeldedaten erstellt haben, melden Sie sich mit Ihrer E-Mail und Ihrem Passwort an.
- Wenn Sie keine Cloud-Anmeldedaten haben, aber bereits über einen NSS Account (NetApp Support

Site) verfügen, wählen Sie **Melden Sie sich mit Ihren NetApp Support Site-Anmeldedaten** an.

- Wenn Sie keinen NSS-Account besitzen und noch keine NetApp Cloud-Anmeldedaten erstellt haben, klicken Sie auf **Registrieren**, um einen NetApp Cloud-Login zu erstellen.

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

Nachdem Sie sich angemeldet haben, erhalten Sie eine E-Mail von NetApp. Klicken Sie auf den Link in der E-Mail, um Ihre E-Mail-Adresse zu überprüfen und sich dann anzumelden.

Sie sind jetzt angemeldet und können mit BlueXP Ihre Hybrid-Multi-Cloud-Infrastruktur managen.

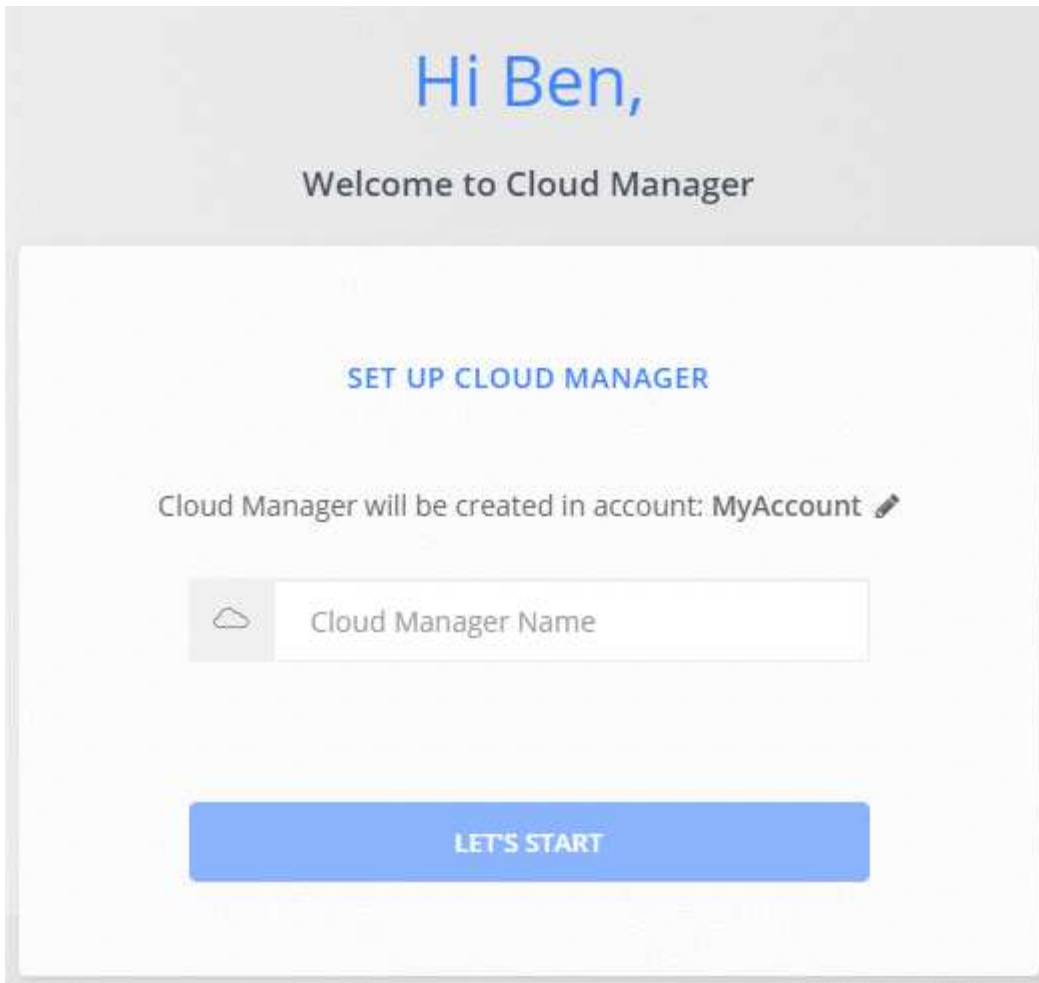
Richten Sie einen NetApp Account ein

Informationen zu NetApp Accounts

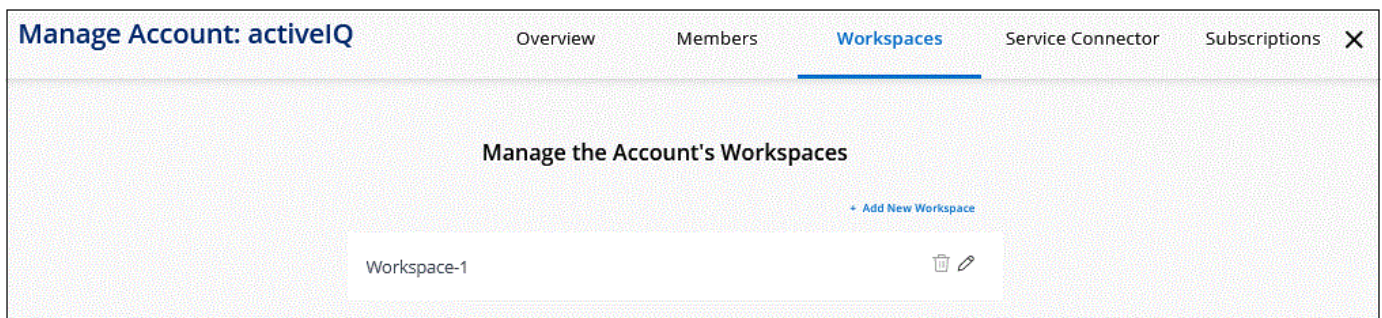
Ein *NetApp Konto* bietet Mandantenfähigkeit und ermöglicht es Ihnen, Benutzer und Ressourcen in isolierten Arbeitsbereichen innerhalb von BlueXP zu organisieren.

So können beispielsweise mehrere Benutzer Cloud Volumes ONTAP Systeme in isolierten Umgebungen, sogenannte *Workspaces*, implementieren und managen. Diese Arbeitsbereiche sind für andere Benutzer unsichtbar, es sei denn, sie werden gemeinsam genutzt.

Wenn Sie zum ersten Mal auf BlueXP zugreifen, werden Sie aufgefordert, ein NetApp Konto auszuwählen oder zu erstellen:



BlueXP-Kontoadministratoren können dann die Einstellungen für dieses Konto ändern, indem sie Benutzer (Mitglieder), Arbeitsbereiche, Connectors und Abonnements verwalten:



Schritt-für-Schritt-Anweisungen finden Sie unter "[NetApp Konto einrichten](#)".

Kontoeinstellungen

Im Widget „Manage Account“ in BlueXP können Account-Administratoren ein NetApp Konto verwalten. Wenn Sie gerade Ihr Konto erstellt, dann beginnen Sie von Grund auf. Wenn Sie jedoch bereits ein Konto eingerichtet haben, sehen Sie *all* die Benutzer, Arbeitsbereiche, Connectors und Abonnements, die mit dem Konto verknüpft sind.

Überblick

Auf der Seite Übersicht werden der Kontoname und die Konto-ID angezeigt. Bei der Registrierung einiger Services müssen Sie unter Umständen Ihre Konto-ID angeben. Diese Seite enthält auch einige BlueXP-Konfigurationsoptionen.

Mitglieder

Die Mitglieder sind BlueXP Benutzer, die Sie mit Ihrem NetApp Konto verknüpfen. Wenn Sie einen Benutzer mit einem Konto und einem oder mehreren Arbeitsbereichen in diesem Konto verknüpfen, können diese Benutzer Arbeitsumgebungen in BlueXP erstellen und verwalten.

Wenn Sie einen Benutzer zuordnen, weisen Sie ihm eine Rolle zu:

- *Account Admin*: Kann jede Aktion in BlueXP ausführen.
- *Workspace Admin*: Kann Ressourcen im zugewiesenen Arbeitsbereich erstellen und verwalten.
- *Compliance Viewer*: Kann nur Informationen zur Compliance von Cloud Data Sense anzeigen und Berichte für Systeme erstellen, auf die sie zugreifen können.
- *SnapCenter Admin*: Kann den SnapCenter Service verwenden, um mit diesen Backups applikationskonsistente Backups zu erstellen und Daten wiederherzustellen. *Dieser Dienst befindet sich derzeit in der Beta.*

["Hier erfahren Sie mehr über diese Rollen".](#)

Arbeitsbereiche

In BlueXP isoliert ein Arbeitsbereich beliebig viele *Arbeitsumgebungen* aus anderen Arbeitsumgebungen. Workspace-Administratoren können nicht auf die Arbeitsumgebungen in einem Arbeitsbereich zugreifen, es sei denn, der Kontoadministrator ordnet den Administrator diesem Arbeitsbereich zu.

Eine Arbeitsumgebung ist ein Speichersystem:

- Single Node Cloud Volumes ONTAP System oder ein HA-Paar
- Ein On-Premises ONTAP Cluster in Ihrem Netzwerk
- Ein ONTAP Cluster in einer NetApp Private Storage-Konfiguration

["Erfahren Sie, wie Sie einen Arbeitsbereich hinzufügen".](#)

Anschlüsse

Mit einem Connector kann BlueXP Ressourcen und Prozesse innerhalb Ihrer Public Cloud-Umgebung verwalten. Der Connector wird auf einer Virtual-Machine-Instanz ausgeführt, die Sie bei Ihrem Cloud-Provider implementieren, oder auf einem von Ihnen konfigurierten On-Premises-Host.

Sie können einen Connector mit mehr als einem NetApp Cloud-Datenservice verwenden. Wenn Sie beispielsweise bereits über einen Connector für BlueXP verfügen, können Sie ihn auswählen, wenn Sie den Cloud Tiering Service einrichten.

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

Abonnements

Dies sind die NetApp Abonnements, die mit dem ausgewählten Konto verknüpft sind.

Wenn Sie BlueXP über den Marktplatz eines Cloud-Providers abonnieren, werden Sie auf die BlueXP-Website weitergeleitet, auf der Sie Ihr Abonnement speichern und mit bestimmten Konten verknüpfen müssen.

Nach dem Abonnement steht jedes Abonnement über das Widget „Konto verwalten“ zur Verfügung. Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

Sie haben die Möglichkeit, ein Abonnement umzubenennen und das Abonnement von einem oder mehreren Konten zu entfernen.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

["Erfahren Sie, wie Sie Abonnements verwalten".](#)

Beispiele

In den folgenden Beispielen wird veranschaulicht, wie Sie Ihre Konten einrichten könnten.

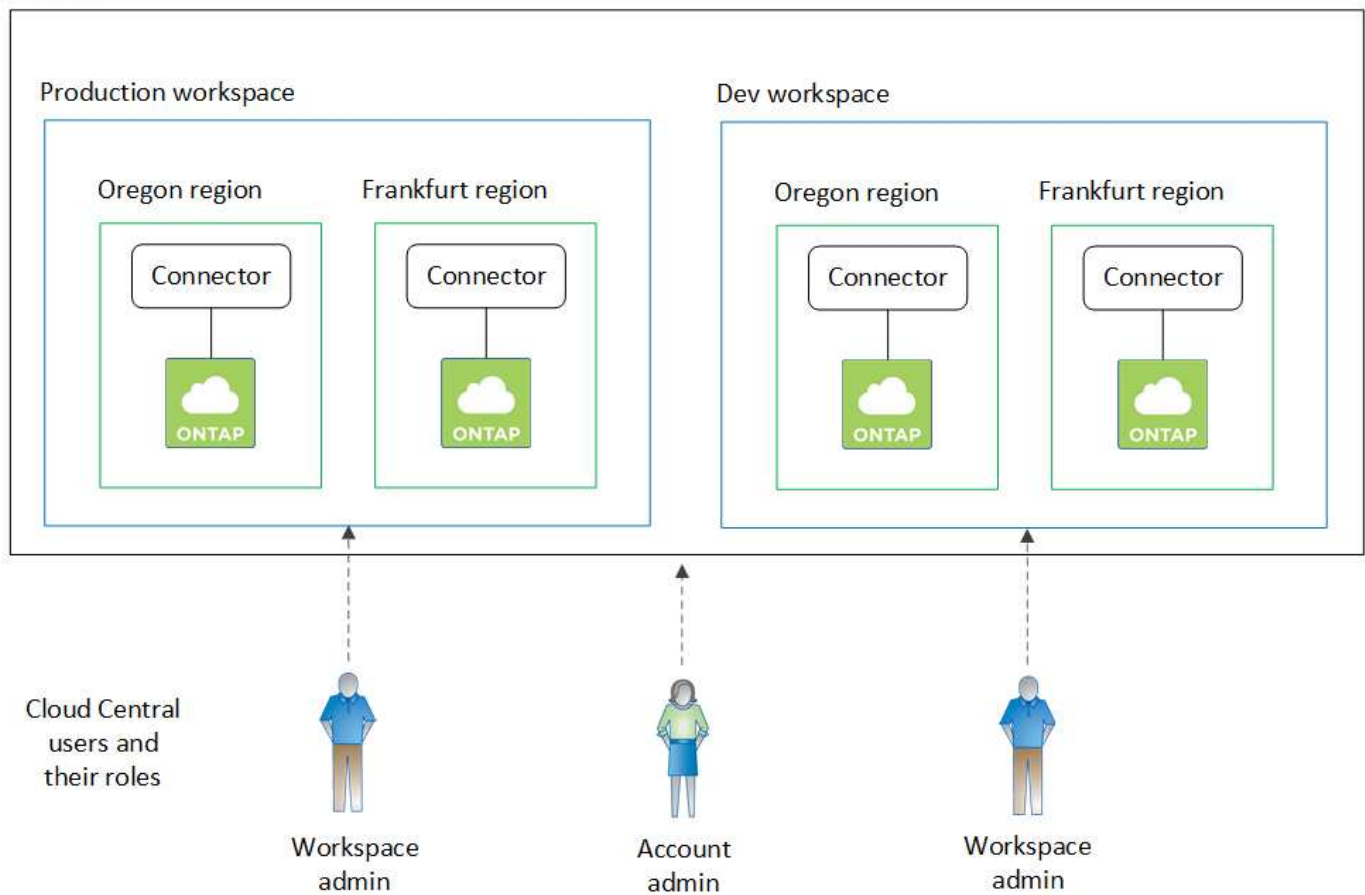


In den folgenden Beispielbildern befinden sich der Connector und die Cloud Volumes ONTAP Systeme nicht *in* dem NetApp Konto - sie laufen bei einem Cloud-Provider. Dies ist eine konzeptionelle Darstellung der Beziehung zwischen den einzelnen Komponenten.

Beispiel 1

Das folgende Beispiel zeigt ein Konto, das zwei Arbeitsbereiche zum Erstellen isolierter Umgebungen verwendet. Der erste Arbeitsbereich ist für eine Produktionsumgebung und der zweite für eine Entwicklungsumgebung.

Account



Beispiel 2

Das nachfolgend ein weiteres Beispiel zeigt die höchste Mandantenfähigkeit mit zwei separaten NetApp Konten. So kann ein Service Provider beispielsweise BlueXP in einem Konto für die Bereitstellung von Services für seine Kunden nutzen und gleichzeitig einen anderen Account für die Disaster Recovery einer seiner Geschäftsbereiche verwenden.

Beachten Sie, dass Konto 2 zwei separate Anschlüsse enthält. Dies kann passieren, wenn Systeme in verschiedenen Regionen oder separaten Cloud-Providern vorhanden sind.



Einrichtung von Workspaces und Benutzern in Ihrem NetApp Konto

Wenn Sie sich zum ersten Mal bei BlueXP anmelden, werden Sie aufgefordert, ein *NetApp Konto* zu erstellen. Dieses Konto bietet Mandantenfähigkeit und ermöglicht es Ihnen, Benutzer und Ressourcen in isolierten Arbeitsbereichen zu organisieren_.

["Erfahren Sie mehr über die Funktionsweise von NetApp Accounts".](#)

Richten Sie Ihr NetApp Konto ein, damit Benutzer über einen Arbeitsbereich auf BlueXP zugreifen können. Fügen Sie einfach einen einzelnen Benutzer hinzu oder fügen Sie mehrere Benutzer und Arbeitsbereiche hinzu.

Fügen Sie Arbeitsbereiche hinzu

In BlueXP können Sie mithilfe von Workspaces eine Reihe von Arbeitsumgebungen von anderen Arbeitsumgebungen und anderen Benutzern isolieren. Sie können beispielsweise zwei Arbeitsbereiche erstellen und jedem Arbeitsbereich separate Benutzer zuordnen.

Schritte

1. Von oben "[BlueXP](#)" Klicken Sie auf das Dropdown-Menü **Konto**.



2. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



3. Klicken Sie Auf **Arbeitsbereiche**.
4. Klicken Sie Auf **Neuen Arbeitsbereich Hinzufügen**.
5. Geben Sie einen Namen für den Arbeitsbereich ein und klicken Sie auf **Hinzufügen**.

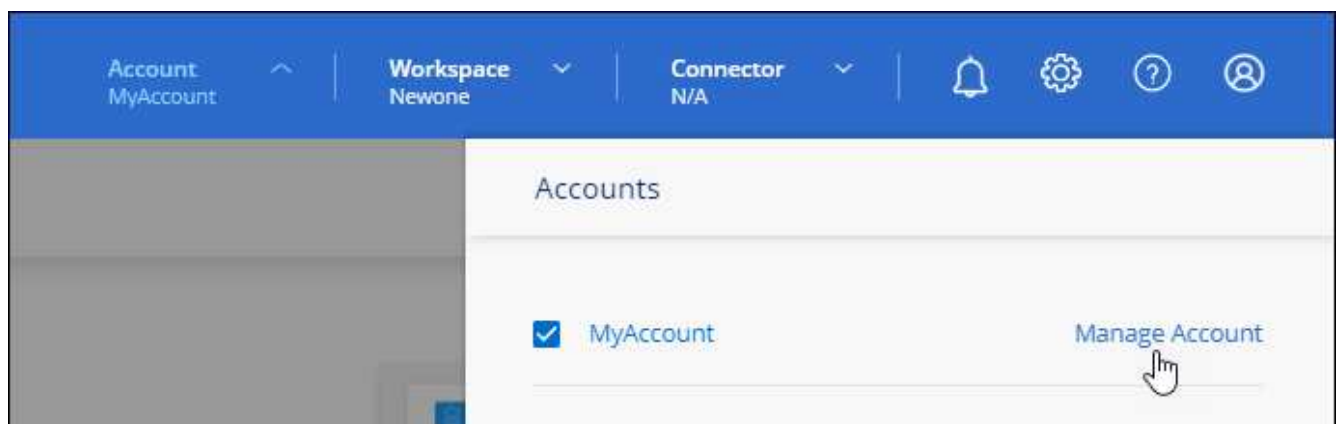
Wenn ein Workspace-Administrator Zugriff auf diesen Arbeitsbereich benötigt, müssen Sie den Benutzer zuordnen. Außerdem müssen Sie Connectors mit dem Arbeitsbereich verknüpfen, damit Arbeitsbereichsadministratoren diese Connectors verwenden können.

Benutzer hinzufügen

Verknüpfen Sie Benutzer mit Ihrem NetApp Konto, damit diese Benutzer Arbeitsumgebungen in BlueXP erstellen und verwalten können.

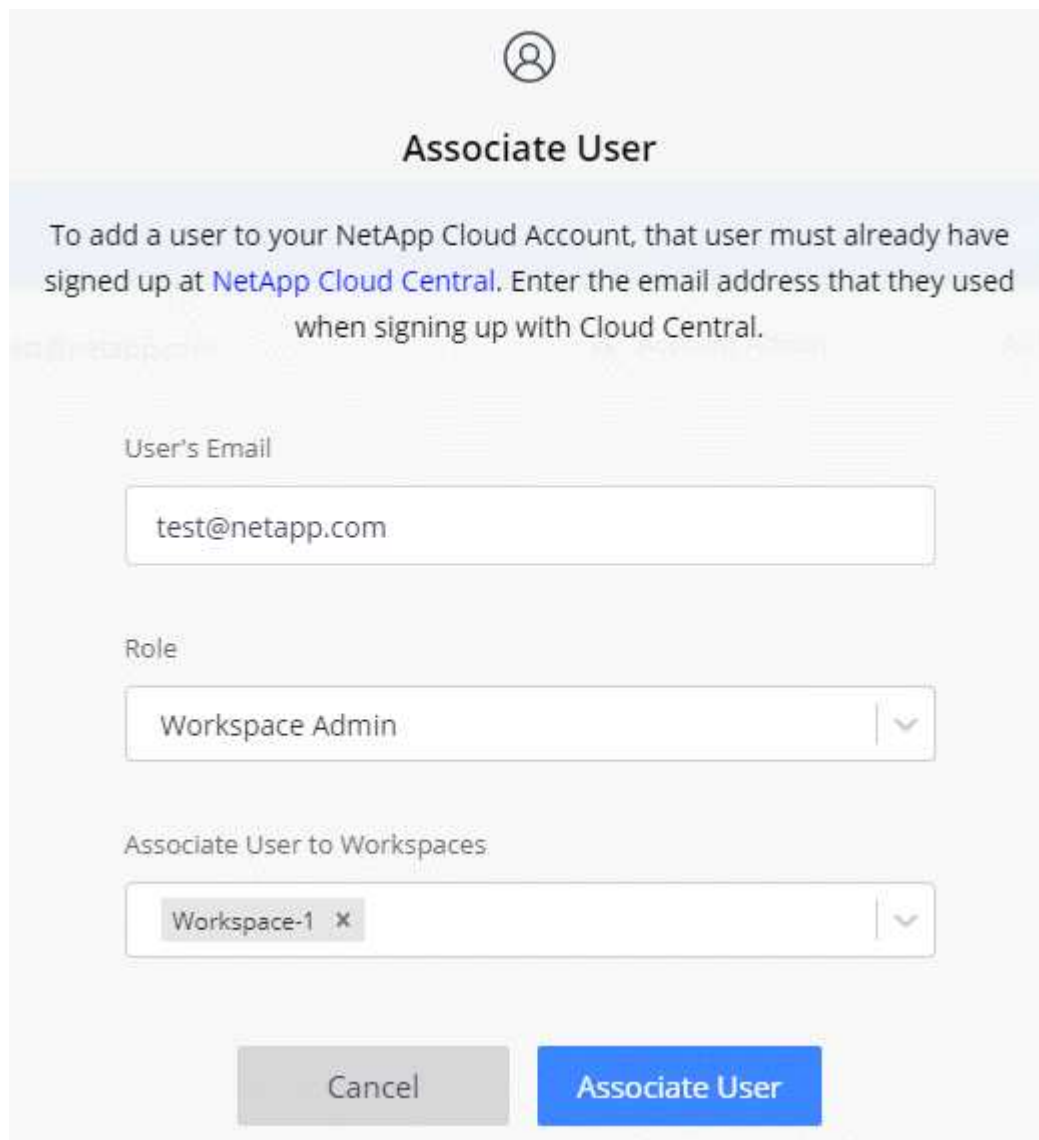
Schritte

1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "[NetApp BlueXP Website](#)" Und melden Sie sich an.
2. Von oben "[BlueXP](#)"Klicken Sie auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



3. Klicken Sie auf der Registerkarte Mitglieder auf **Benutzer verknüpfen**.
4. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
 - **Account Admin:** Kann jede Aktion in BlueXP ausführen.
 - **Workspace Admin:** Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
 - **Compliance Viewer:** Kann nur Informationen zu Cloud Data Sense Governance und Compliance anzeigen und Berichte für Arbeitsbereiche erstellen, auf die sie zugreifen können.

- **SnapCenter Admin:** Kann den SnapCenter Service verwenden, um mit diesen Backups anwendungskonsistente Backups zu erstellen und Daten wiederherzustellen. Dieser Service befindet sich derzeit in Beta.
5. Wenn Sie ein anderes Konto als Kontoadministrator ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 x

Cancel Associate User

6. Klicken Sie Auf **Mitarbeiter**.

Der Benutzer sollte eine E-Mail von der NetApp BlueXP Website mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die Informationen, die für den Zugriff auf BlueXP erforderlich sind.

Workspace-Administratoren mit Arbeitsbereichen verknüpfen

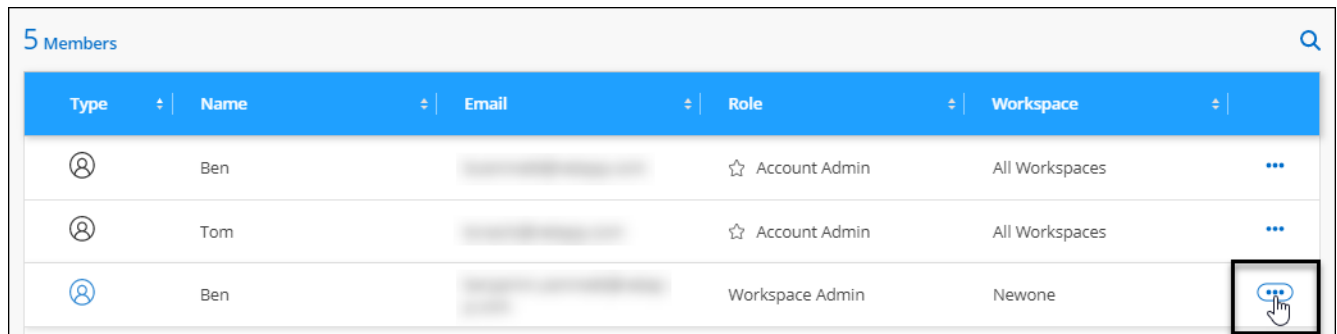
Sie können Workspace-Administratoren jederzeit mit zusätzlichen Arbeitsbereichen verknüpfen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie Auf **Arbeitsbereiche Verwalten**.
4. Wählen Sie einen oder mehrere Arbeitsbereiche aus, und klicken Sie auf **Anwenden**.

Der Benutzer kann jetzt von BlueXP auf diese Arbeitsbereiche zugreifen, solange der Connector auch mit den Arbeitsbereichen verknüpft war.

Verbinden Sie Connectors mit Arbeitsbereichen

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.

["Erfahren Sie mehr über Benutzer, Arbeitsbereiche und Connectors"](#).

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie Auf **Connector**.
3. Klicken Sie auf **Arbeitsbereiche verwalten** für den Konnektor, den Sie verknüpfen möchten.
4. Wählen Sie einen oder mehrere Arbeitsbereiche aus, und klicken Sie auf **Anwenden**.

Workspace-Administratoren können diese Anschlüsse jetzt verwenden, um Cloud Volumes ONTAP-Systeme zu erstellen.

Was kommt als Nächstes?

Nachdem Sie Ihr Konto eingerichtet haben, können Sie es jederzeit verwalten, indem Sie Benutzer entfernen, Arbeitsbereiche, Connectors und Abonnements verwalten. ["Erfahren Sie, wie Sie Ihr Konto verwalten"](#).

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.

["Informieren Sie sich, wann ein Anschluss erforderlich ist"](#).

Auf dieser Seite wird beschrieben, wie Sie einen Connector in AWS 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.

Schnellstart

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

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.

an IAM policy, IAM-Rolle anzeigen Oder up AWS authentication, Befolgen Sie die Schritt-für-Schritt-Anweisungen.

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.

up networking, Netzwerkanforderungen anzeigen.

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

a Connector, 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**.

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.

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.

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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com | 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

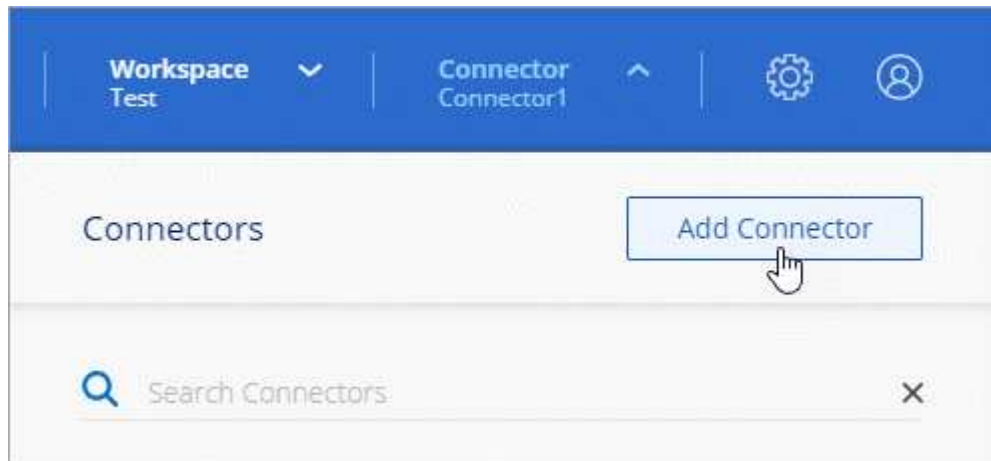
Es besteht ein möglicher Konflikt mit IP-Adressen im Bereich 172. "[Erfahren Sie mehr über diese Einschränkung](#)".

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.

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.

["Informieren Sie sich, wann ein Anschluss erforderlich ist"](#).

Auf dieser Seite wird beschrieben, wie Sie einen Connector in Azure 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.

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.

a Connector using your Azure account, 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.

a Connector using a service principal, 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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com | 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](#)".

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.

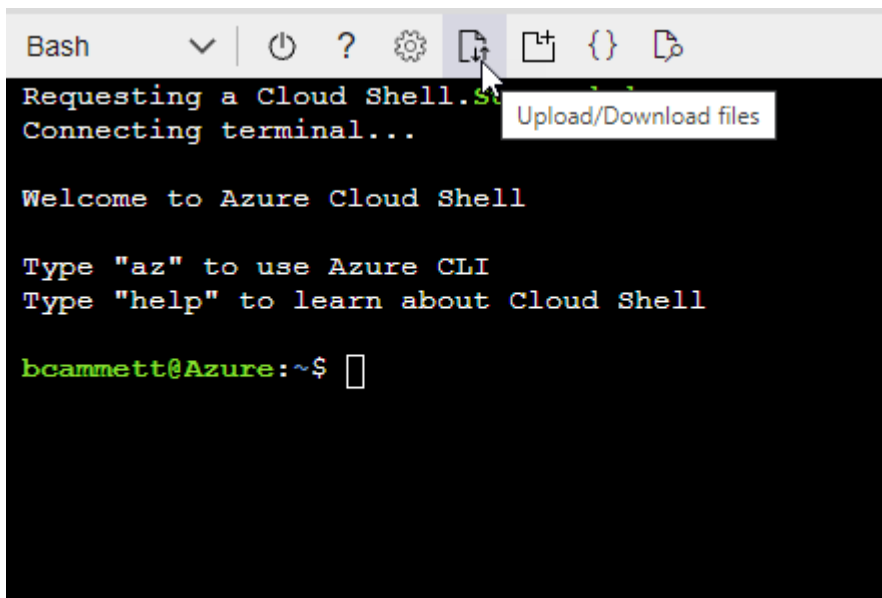
Beispiel

```
"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**.

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.

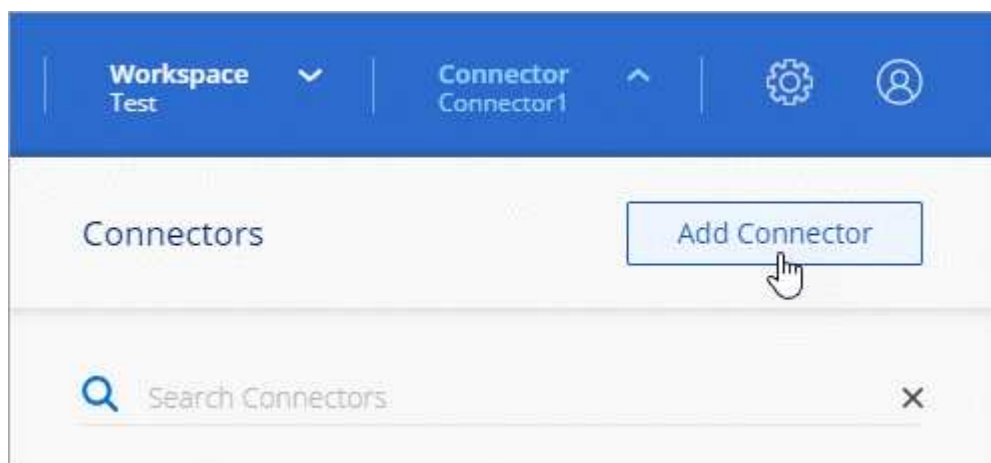
Was Sie und#8217;ll benötigen

- 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.

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. an Azure Active Directory application.
2. the application to a role.
3. Windows Azure Service Management API permissions.
4. the application ID and directory ID.
5. a client secret.

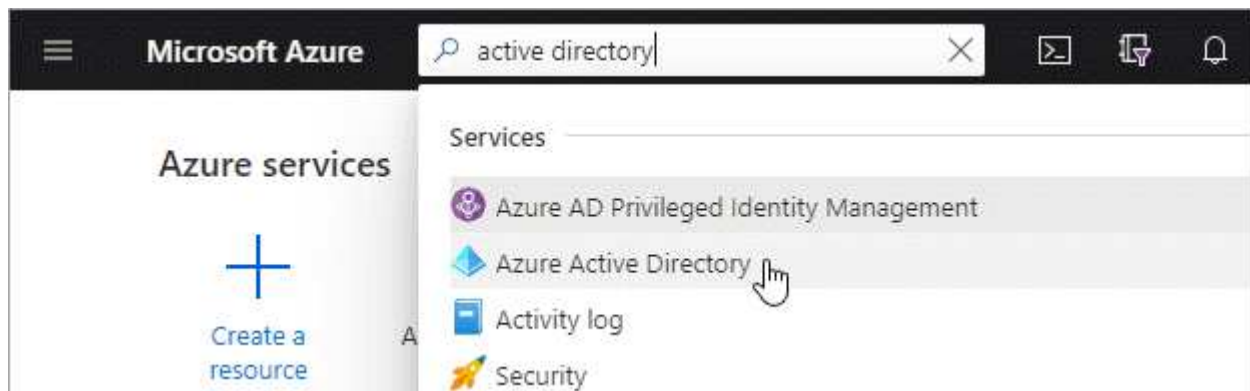
Erstellen Sie eine Azure Active Directory-Anwendung

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

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**.

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.

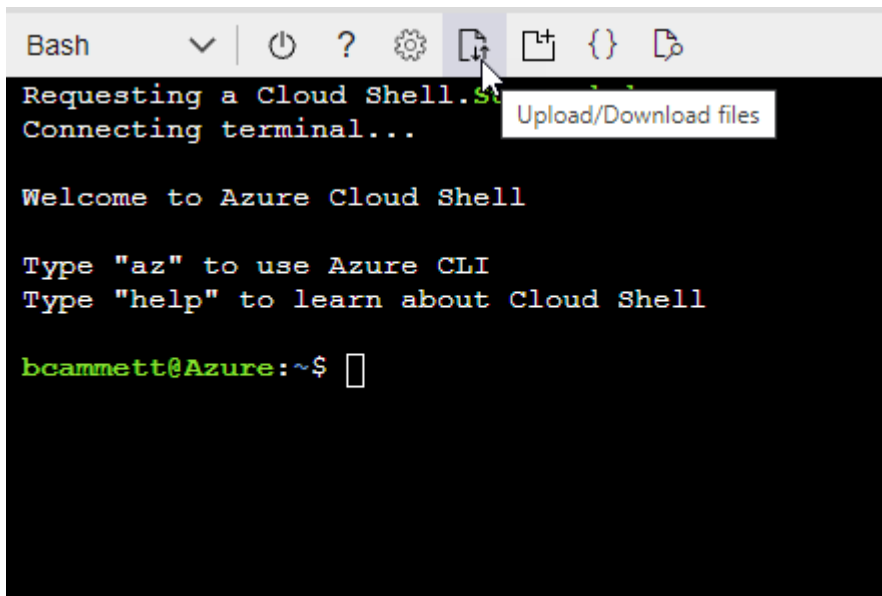
Beispiel

```
"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**.

Add role assignment ...

[Got feedback?](#)

[Role](#) **[Members](#)** [Review + assign](#)

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- Suchen Sie nach dem Namen der Anwendung.

Hier ein Beispiel:

Select members [X]

Select ⓘ

test-service-principal

test-service-principal

- 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.

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

4. 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"/> user_impersonation 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.

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

Copy to clipboard

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 und#8217;ll 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 the application ID and directory ID.
 - Verzeichnis-ID (Mandant): Siehe the application ID and directory ID.
 - Client Secret: Siehe a client secret.
 - 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.

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.

 **Berechtigungen einrichten**

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

```
up permissions to deploy the Connector.
```

- 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.


```
up a service account for the Connector.
```

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

```
up shared VPC permissions.
```

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.

```
up networking,Netzwerkanforderungen anzeigen.
```

 **Google Cloud APIs aktivieren**

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

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

```
a Connector,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.

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.

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"> "Die Berechtigungen, die in diesem Abschnitt oben gefunden wurden" | <ul style="list-style-type: none"> compute.networkUser | Bereitstellen des Connectors im Serviceprojekt |
| Connector-Servicekonto | Individuell | Service-Projekt | <ul style="list-style-type: none"> "Die Berechtigungen, die in diesem Abschnitt oben gefunden wurden" | <ul style="list-style-type: none"> compute.networkUser Bereitsmanager.Editor | 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"> Storage.Administration mitglied: BlueXP Dienstkonto als serviceAccount.user | K. A. | (Optional) für Daten-Tiering und Cloud Backup |

| Identität | Ersteller | Gehostet in | Berechtigungen für Serviceprojekte | Host-Projektberechtigungen | Zweck |
|---|--------------|-----------------|------------------------------------|----------------------------|---|
| Google APIs-Serviceaccount | 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 `enclmentmanager.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 |
|--|---|
| https://support.netapp.com | Um Lizenzinformationen zu erhalten und AutoSupport Meldungen an den NetApp Support zu senden. |
| https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com | 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](#)".

Aktivieren Sie Google Cloud-APIs

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

Schritt

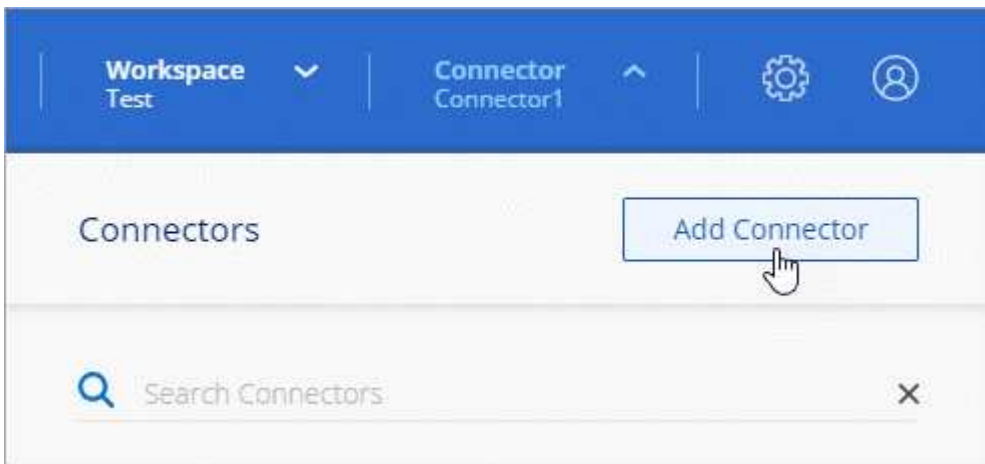
1. "[Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt](#)".
 - Cloud Deployment Manager V2-API
 - Cloud-ProtokollierungsAPI
 - Cloud Resource Manager API
 - Compute Engine-API
 - IAM-API (Identitäts- und Zugriffsmanagement)

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:

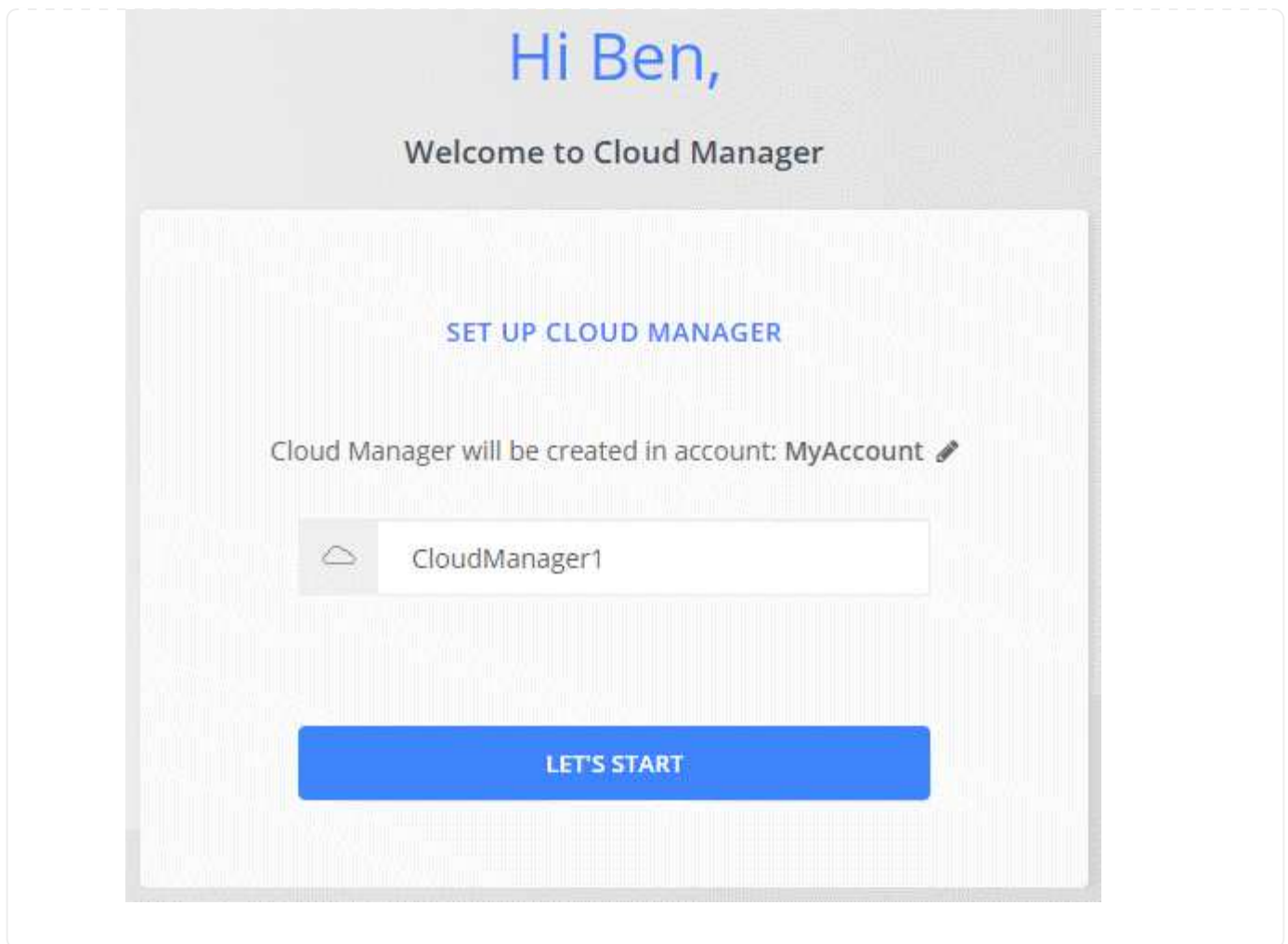
`https://ipaddress[]`

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.



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://cloudmanager.netapp.com>.

Weitere Schritte

Nachdem Sie sich angemeldet und BlueXP eingerichtet haben, können Benutzer jetzt mit dem Erstellen und Erkennen von Arbeitsumgebungen beginnen.

- ["Erste Schritte mit Cloud Volumes ONTAP für AWS"](#)
- ["Erste Schritte mit Cloud Volumes ONTAP für Azure"](#)
- ["Erste Schritte mit Cloud Volumes ONTAP für Google Cloud"](#)
- ["Azure NetApp Files einrichten"](#)
- ["Amazon FSX für ONTAP einrichten"](#)
- ["Cloud Volumes Service für AWS einrichten"](#)
- ["Ermitteln eines lokalen ONTAP Clusters"](#)
- ["Amazon S3 Buckets entdecken"](#)

Verwalten von BlueXP

NetApp Accounts

Managen Ihres NetApp Kontos

"[Nach der ersten Einrichtung](#)", Sie können Ihre Kontoeinstellungen später verwalten, indem Sie Benutzer, Servicekonten, Arbeitsbereiche, Anschlüsse und Abonnements verwalten.

"[Erfahren Sie mehr über die Funktionsweise von NetApp Accounts](#)".

Managen Ihres Kontos mit der Tenancy API

Wenn Sie Ihre Kontoeinstellungen durch Senden von API-Anfragen verwalten möchten, müssen Sie die API *Tenancy* verwenden. Diese API unterscheidet sich von der BlueXP API, die Sie zum Erstellen und Verwalten von Cloud Volumes ONTAP-Arbeitsumgebungen verwenden.

"[Anzeige von Endpunkten für die Mandanten-API](#)"

Erstellen und Verwalten von Benutzern

Die Benutzer in Ihrem Konto können auf die Ressourcen in den Arbeitsbereichen Ihres Kontos verwalten zugreifen.

Benutzer hinzufügen

Verknüpfen Sie Benutzer mit Ihrem NetApp Konto, damit diese Benutzer Arbeitsumgebungen in BlueXP erstellen und verwalten können.

Schritte

1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "[NetApp BlueXP Website](#)" Und melden Sie sich an.
2. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto**.



3. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



4. Klicken Sie auf der Registerkarte Mitglieder auf **Benutzer verknüpfen**.
5. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
 - **Account Admin:** Kann jede Aktion in BlueXP ausführen.
 - **Workspace Admin:** Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
 - **Compliance Viewer:** Kann nur Informationen zur Compliance von Cloud Data Sense anzeigen und Berichte für Arbeitsbereiche erstellen, auf die sie zugreifen können.
 - **SnapCenter Admin:** Kann den SnapCenter Service verwenden, um mit diesen Backups anwendungskonsistente Backups zu erstellen und Daten wiederherzustellen. *Dieser Dienst befindet sich derzeit in der Beta.*
6. Wenn Sie Workspace Admin oder Compliance Viewer ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title is a light blue banner with instructions: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below this are three input fields: "User's Email" containing "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom are two buttons: "Cancel" and "Associate User".



Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 X

Cancel Associate User

7. Klicken Sie Auf **Mitarbeiter**.

Der Benutzer sollte eine E-Mail von NetApp BlueXP mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die Informationen, die für den Zugriff auf BlueXP erforderlich sind.

Benutzer werden entfernt

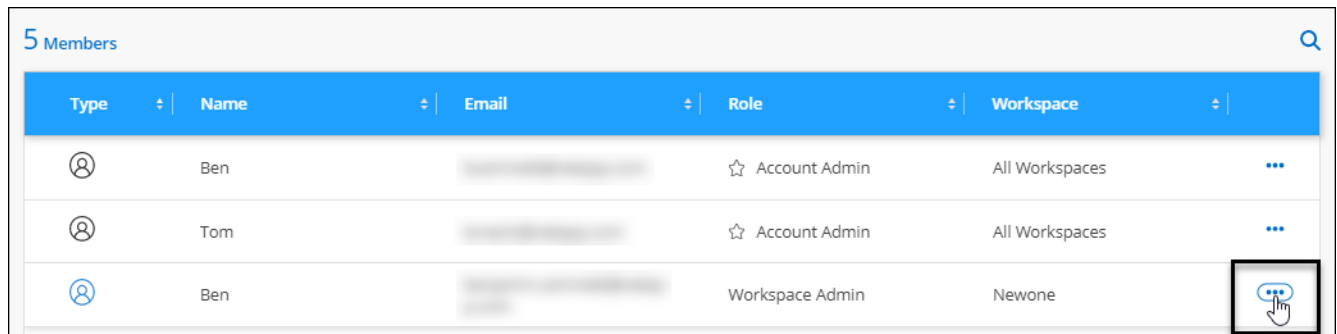
Die Trennung der Verknüpfung eines Benutzers wird dadurch ermöglicht, dass er nicht mehr auf die Ressourcen eines NetApp Kontos zugreifen kann.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie zur Bestätigung auf **Benutzer entzuordnen** und klicken Sie zur Bestätigung auf **Mitarbeiter nicht zuordnen**.

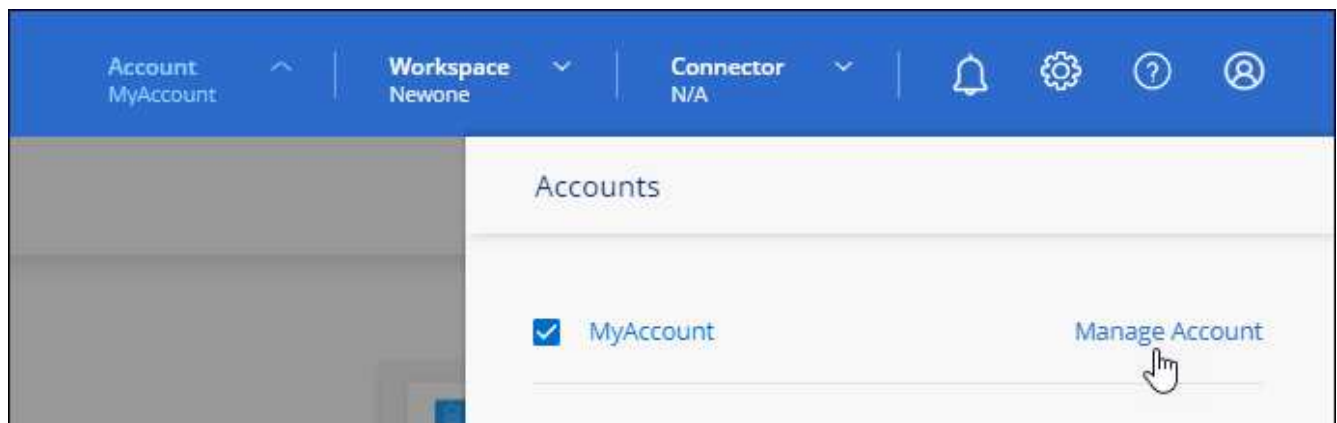
Der Anwender kann nicht mehr auf die Ressourcen in diesem NetApp Konto zugreifen.

Arbeitsbereiche eines Arbeitsbereichs-Administrators verwalten

Sie können Workspace-Administratoren jederzeit mit Arbeitsbereichen verknüpfen und sie ablösen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.












Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.

5 Members

| Type | Name | Email | Role | Workspace | |
|---|------|---|---|----------------|---|
|  | Ben |  |  Account Admin | All Workspaces |  |
|  | Tom |  |  Account Admin | All Workspaces |  |
|  | Ben |  | Workspace Admin | Newone |  |

3. Klicken Sie Auf **Arbeitsbereiche Verwalten**.

4. Wählen Sie die Arbeitsbereiche aus, die dem Benutzer zugeordnet werden sollen, und klicken Sie auf **Anwenden**.

Der Benutzer kann jetzt von BlueXP auf diese Arbeitsbereiche zugreifen, solange der Connector auch mit den Arbeitsbereichen verknüpft war.

Erstellen und Verwalten von Servicekonten

Ein Servicekonto fungiert als „Benutzer“, der autorisierte API-Aufrufe zu Automatisierungszwecken an BlueXP vornehmen kann. So ist das Management der Automatisierung einfacher, da keine Automatisierungsskripts auf Basis des Benutzerkontos eines echten Mitarbeiters erstellt werden müssen, der das Unternehmen jederzeit verlassen kann. Und bei Verwendung von Federation können Sie ein Token erstellen, ohne ein Update-Token aus der Cloud zu generieren.

Sie erteilen einem Servicekonto Berechtigungen, indem Sie ihm eine Rolle zuweisen, genau wie jeder andere BlueXP-Benutzer. Sie können das Servicekonto auch mit bestimmten Arbeitsbereichen verknüpfen, um die Arbeitsumgebungen (Ressourcen) zu kontrollieren, auf die der Service zugreifen kann.

Wenn Sie das Dienstkonto erstellen, können Sie mit BlueXP eine Client-ID und einen Clientschlüssel für das Dienstkonto kopieren oder herunterladen. Dieses Schlüsselpaar wird für die Authentifizierung mit BlueXP verwendet.

Erstellen eines Dienstkontos

Erstellen Sie so viele Service-Konten wie für das Management der Ressourcen in Ihren Arbeitsumgebungen erforderlich.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto**.



2. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



3. Klicken Sie auf der Registerkarte Mitglieder auf **Dienstkonto erstellen**.
4. Geben Sie einen Namen ein, und wählen Sie eine Rolle aus. Wenn Sie eine andere Rolle als Kontoadministrator auswählen, wählen Sie den Arbeitsbereich aus, der mit diesem Dienstkonto verknüpft werden soll.
5. Klicken Sie Auf **Erstellen**.
6. Kopieren Sie die Client-ID und den Clientschlüssel, oder laden Sie sie herunter.

Das Clientgeheimnis ist nur einmal sichtbar und wird von BlueXP nirgendwo gespeichert. Kopieren oder laden Sie das Geheimnis herunter und speichern Sie es sicher.

7. Klicken Sie Auf **Schließen**.

Abrufen eines Inhabertoken für ein Dienstkonto

Um API-Aufrufe an das zu tätigen "**Mandanten-API**", Sie müssen ein Inhaberzeichen für ein Service-Konto zu erhalten.

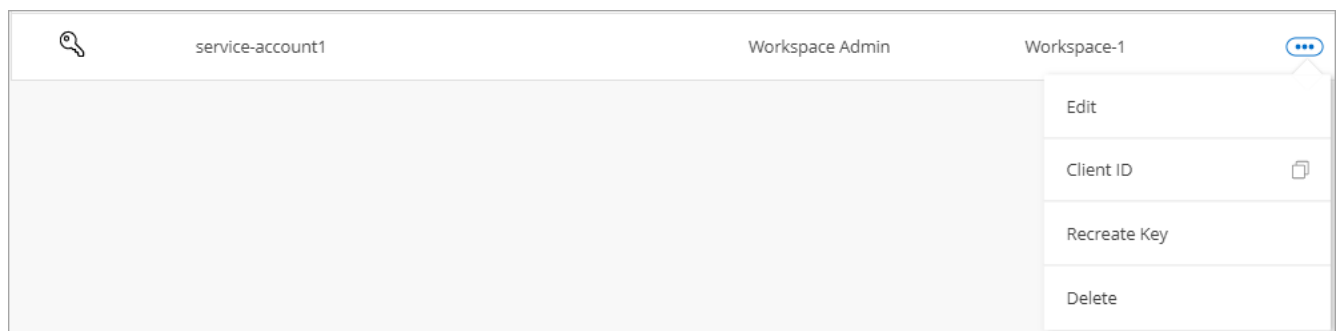
"Erfahren Sie, wie Sie ein Service-Konto-Token erstellen"

Kopieren der Client-ID

Sie können die Client-ID eines Dienstkontos jederzeit kopieren.

Schritte

1. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Dienstkonto entspricht.



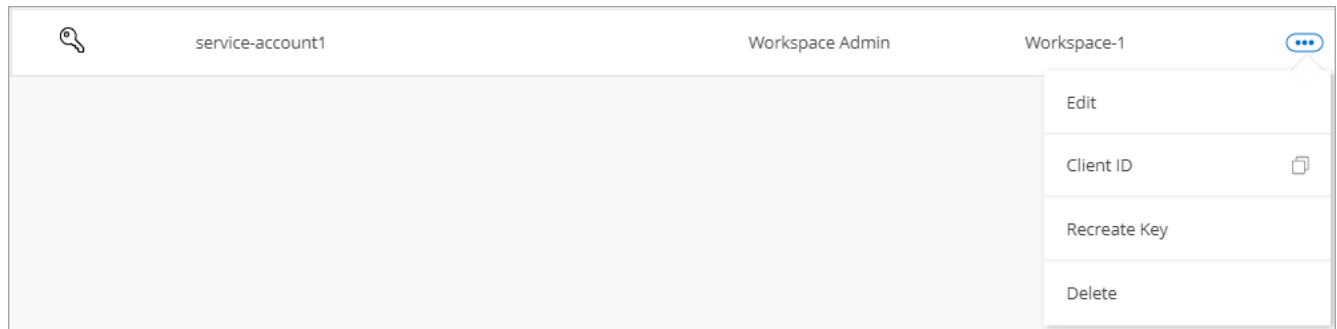
2. Klicken Sie auf **Client-ID**.
3. Die ID wird in die Zwischenablage kopiert.

Schlüssel werden neu erstellt

Durch Neuerstellen des Schlüssels wird der vorhandene Schlüssel für dieses Servicekonto gelöscht und anschließend ein neuer Schlüssel erstellt. Sie können den vorherigen Schlüssel nicht verwenden.

Schritte

1. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Dienstkonto entspricht.



2. Klicken Sie Auf **Reproduzieren Schlüssel**.
3. Klicken Sie zur Bestätigung auf **reproduzieren**.
4. Kopieren Sie die Client-ID und den Clientschlüssel, oder laden Sie sie herunter.

Das Clientgeheimnis ist nur einmal sichtbar und wird von BlueXP nirgendwo gespeichert. Kopieren oder laden Sie das Geheimnis herunter und speichern Sie es sicher.

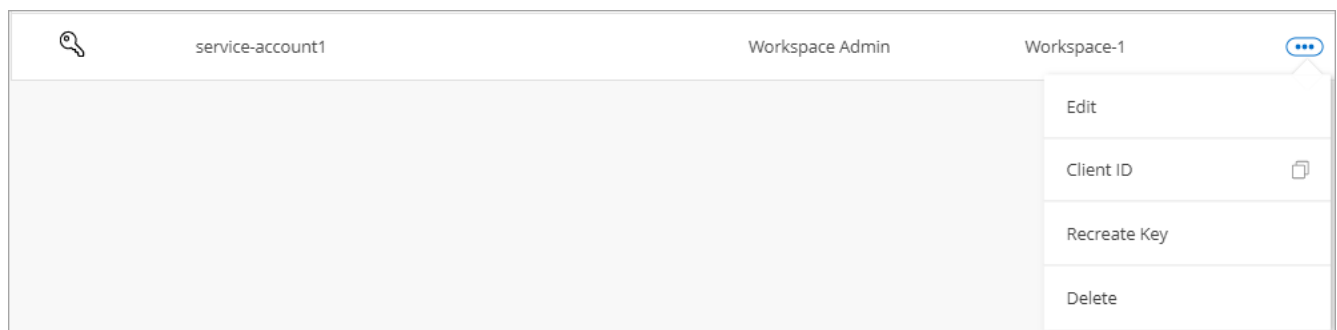
5. Klicken Sie Auf **Schließen**.

Löschen eines Dienstkontos

Löschen Sie ein Dienstkonto, wenn Sie es nicht mehr verwenden müssen.

Schritte

1. Klicken Sie auf der Registerkarte Mitglieder auf das Aktionsmenü in der Zeile, die dem Dienstkonto entspricht.



2. Klicken Sie Auf **Löschen**.
3. Klicken Sie zur Bestätigung erneut auf **Löschen**.

Arbeitsbereiche verwalten

Verwalten Sie Ihre Arbeitsbereiche, indem Sie sie erstellen, umbenennen und löschen. Beachten Sie, dass Sie

einen Arbeitsbereich nicht löschen können, wenn er Ressourcen enthält. Er muss leer sein.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Arbeitsbereiche**.
3. Wählen Sie eine der folgenden Optionen:
 - Klicken Sie auf **Neuen Arbeitsbereich hinzufügen**, um einen neuen Arbeitsbereich zu erstellen.
 - Klicken Sie auf **Umbenennen**, um den Arbeitsbereich umzubenennen.
 - Klicken Sie auf **Löschen**, um den Arbeitsbereich zu löschen.

Verwalten der Arbeitsbereiche eines Connectors

Sie müssen den Connector mit Arbeitsbereichen verknüpfen, damit Workspace-Administratoren von BlueXP auf diese Arbeitsbereiche zugreifen 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.

["Erfahren Sie mehr über Benutzer, Arbeitsbereiche und Connectors"](#).

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Connector**.
3. Klicken Sie auf **Arbeitsbereiche verwalten** für den Konnektor, den Sie verknüpfen möchten.
4. Wählen Sie die Arbeitsbereiche aus, die mit dem Connector verknüpft werden sollen, und klicken Sie auf **Anwenden**.

Verwalten von Abonnements

Nachdem Sie den Marketplace eines Cloud-Providers abonniert haben, steht jedes Abonnement über das Widget „Account Settings“ (Kontoeinstellungen) zur Verfügung. Sie haben die Möglichkeit, ein Abonnement umzubenennen und das Abonnement von einem oder mehreren Konten zu entfernen.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

["Weitere Informationen zu Abonnements"](#).

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Abonnements**.

Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

3. Klicken Sie in der Zeile auf das Aktionsmenü, das dem Abonnement entspricht, das Sie verwalten möchten.

2 Subscriptions

| Name | Service | Cloud Provider | Status |
|---------------------------------------|---------------------|----------------|--------------|
| QA Subscription | test-service | aws | Unsubscribed |
| metering service subscription QA !!!! | cloud-volumes-ontap | aws | Subscribed |

Rename Subscription
Manage Accounts

4. Wählen Sie diese Option, um das Abonnement umzubenennen oder um die Konten zu verwalten, die mit dem Abonnement verbunden sind.

Ihren Kontonamen ändern

Ändern Sie Ihren Kontonamen jederzeit, um ihn in etwas Sinnvolles für Sie zu ändern.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie auf der Registerkarte **Übersicht** neben dem Kontonamen auf das Bearbeiten-Symbol.
3. Geben Sie einen neuen Kontonamen ein und klicken Sie auf **Speichern**.

Private Vorschauen zulassen

Ermöglichen Sie privaten Vorschau in Ihrem Konto, um Zugriff auf die neuen NetApp Cloud-Services zu erhalten, die in BlueXP als Vorschau zur Verfügung gestellt werden.

Services in der privaten Vorschau sind nicht garantiert, dass sich wie erwartet verhalten und können Ausfälle aufrecht erhalten und fehlende Funktionen sein.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Aktivieren Sie auf der Registerkarte **Übersicht** die Einstellung **Private Vorschau zulassen**.

Durch die Nutzung von Services anderer Anbieter

Lassen Sie Drittanbieter-Services in Ihrem Konto zu, um Zugriff auf Dienste von Drittanbietern zu erhalten, die in BlueXP verfügbar sind. Drittanbieter-Services sind ähnlich wie die Services von NetApp, werden aber von Drittanbieter gemanagt und unterstützt.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Aktivieren Sie auf der Registerkarte **Übersicht** die Option **Drittanbieter-Services zulassen**.

Deaktivieren der SaaS-Plattform

Wir empfehlen nicht, die SaaS-Plattform zu deaktivieren, es sei denn, Sie müssen, um die Sicherheitsrichtlinien Ihres Unternehmens zu erfüllen. Durch die Deaktivierung der SaaS-Plattform ist Ihre Fähigkeit zur Nutzung von integrierten NetApp Cloud-Services begrenzt.

Die folgenden Dienste stehen bei BlueXP nicht zur Verfügung, wenn Sie die SaaS-Plattform deaktivieren:

- Cloud-Daten Sinnvoll
- Kubernetes
- Cloud Tiering
- Globaler Datei-Cache

Wenn Sie die SaaS-Plattform deaktivieren, müssen Sie alle Aufgaben von ausführen ["Die lokale Benutzeroberfläche, die auf einem Connector verfügbar ist"](#).



Dies ist eine irreversible Aktion, die Sie daran hindert, die BlueXP SaaS-Plattform zu verwenden. Sie müssen Aktionen über den lokalen Konnektor durchführen. Sie können nicht viele integrierte Cloud-Services von NetApp nutzen und die erneute Aktivierung der SaaS-Plattform erfordert die Unterstützung durch NetApp.

Schritte

1. Klicken Sie oben in BlueXP auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Schalten Sie auf der Registerkarte Übersicht die Option ein, um die Nutzung der SaaS-Plattform zu deaktivieren.

Überwachen von Vorgängen in Ihrem Konto


Sie können den Status der Operationen überwachen, die BlueXP durchführt, um zu sehen, ob Probleme auftreten, die Sie beheben müssen. Sie können den Status im Benachrichtigungscenter, in der Zeitleiste anzeigen oder Benachrichtigungen an Ihre E-Mail senden.

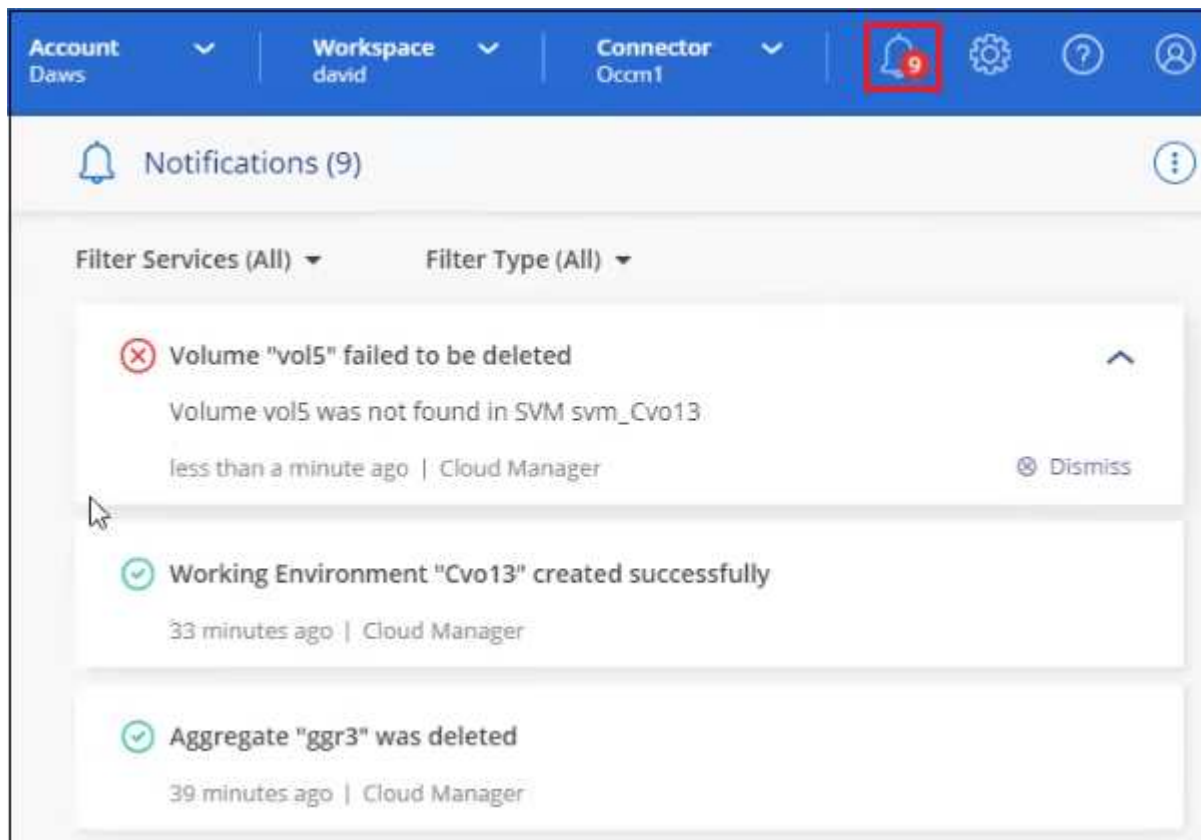
In dieser Tabelle werden das Benachrichtigungscenter und die Zeitleiste verglichen, damit Sie verstehen können, was die einzelnen Angebote zu bieten haben.

| Notification Center | Zeitachse |
|--|---|
| Zeigt den allgemeinen Status von Ereignissen und Aktionen an | Enthält Details zu jedem Ereignis oder jeder Aktion zur weiteren Untersuchung |
| Zeigt den Status der aktuellen Anmeldesitzung an. Die Informationen werden nach der Abmeldung nicht im Benachrichtigungscenter angezeigt | Behält den Status des letzten Monats bei |
| Zeigt nur Aktionen an, die in der Benutzeroberfläche initiiert wurden | Zeigt alle Aktionen der UI oder der APIs an |
| Zeigt benutzerinitiierte Aktionen an | Zeigt alle Aktionen an, ob vom Benutzer initiiert oder vom System initiiert |
| Ergebnisse nach Bedeutung filtern | Filtern nach Dienst, Aktion, Benutzer, Status und mehr |
| Ermöglicht das E-Mail-Versenden von Benachrichtigungen an Benutzer von Konten und an andere Benutzer | Keine E-Mail-Funktion |

Überwachen von Aktivitäten mithilfe des Benachrichtigungszentrums

Benachrichtigungen verfolgen den Fortschritt der Vorgänge, die Sie in BlueXP initiiert haben, damit Sie überprüfen können, ob der Vorgang erfolgreich war oder nicht. Mit diesen können Sie den Status vieler BlueXP-Aktionen anzeigen, die Sie während Ihrer aktuellen Anmeldesitzung initiiert haben. Nicht alle Dienste berichten zu diesem Zeitpunkt Informationen in das Benachrichtigungszentrum.

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Benachrichtigungs-Bell (klicken ) In der Menüleiste. Die Farbe der kleinen Blase in der Glocke zeigt die Meldung mit dem höchsten Schweregrad an, die aktiv ist. Wenn Sie also eine rote Blase sehen, bedeutet dies, dass eine wichtige Benachrichtigung angezeigt wird, die Sie sich ansehen sollten.



Außerdem können Sie BlueXP so konfigurieren, dass Benachrichtigungen per E-Mail versendet werden, damit Sie auch dann über wichtige Systemaktivitäten informiert werden können, wenn Sie nicht am System angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihres NetApp Cloud Kontos sind, oder an andere Empfänger, die bestimmte Arten von Systemaktivitäten kennen müssen. Siehe [email notification settings](#), Einstellen der Einstellungen für E-Mail-Benachrichtigungen Unten.

Benachrichtigungstypen

Benachrichtigungen werden in die folgenden Kategorien eingeteilt:

| Benachrichtigungstyp | Beschreibung |
|----------------------|---|
| Kritisch | Ein Problem, das zu einer Serviceunterbrechung führen kann, wenn keine Korrekturmaßnahmen sofort ergriffen werden. |
| Fehler | Eine Aktion oder ein Prozess wurde mit einem Fehler beendet oder könnte zu einem Fehler führen, wenn keine Korrekturmaßnahmen ergriffen werden. |

| Benachrichtigungstyp | Beschreibung |
|----------------------|---|
| Warnung | Ein Problem, das Sie beachten sollten, um sicherzustellen, dass es den kritischen Schweregrad nicht erreicht. Benachrichtigungen dieses Schweregrades verursachen keine Serviceunterbrechungen und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich. |
| Empfehlung | Eine Systemempfehlung für Sie, Maßnahmen zur Verbesserung des Systems oder eines bestimmten Dienstes zu ergreifen, zum Beispiel: Kostenersparnis, Vorschlag für neue Dienste, empfohlene Sicherheitskonfiguration, etc |
| Informationsdaten | Eine Meldung, die zusätzliche Informationen zu einer Aktion oder einem Prozess enthält. |
| Erfolg | Eine Aktion oder ein Prozess erfolgreich abgeschlossen. |

Filtern von Benachrichtigungen

Standardmäßig werden alle Benachrichtigungen angezeigt. Sie können die Benachrichtigungen filtern, die im Benachrichtigungscenter angezeigt werden, um nur die Benachrichtigungen anzuzeigen, die für Sie wichtig sind. Sie können nach BlueXP „Service“ und nach Benachrichtigung „Typ“ filtern.

Wenn Sie beispielsweise nur „Fehler“ und „Warnung“ für BlueXP-Vorgänge sehen möchten, wählen Sie diese Einträge aus, und Sie werden nur die Arten von Benachrichtigungen sehen.

Einstellen der Einstellungen für E-Mail-Benachrichtigungen

Sie können bestimmte Arten von Benachrichtigungen per E-Mail versenden, damit Sie über wichtige Systemaktivitäten informiert werden können, auch wenn Sie nicht bei BlueXP angemeldet sind. E-Mails können an alle Benutzer gesendet werden, die Teil Ihres NetApp Kontos sind, oder an andere Empfänger, die bestimmte Arten von Systemaktivitäten kennen müssen.



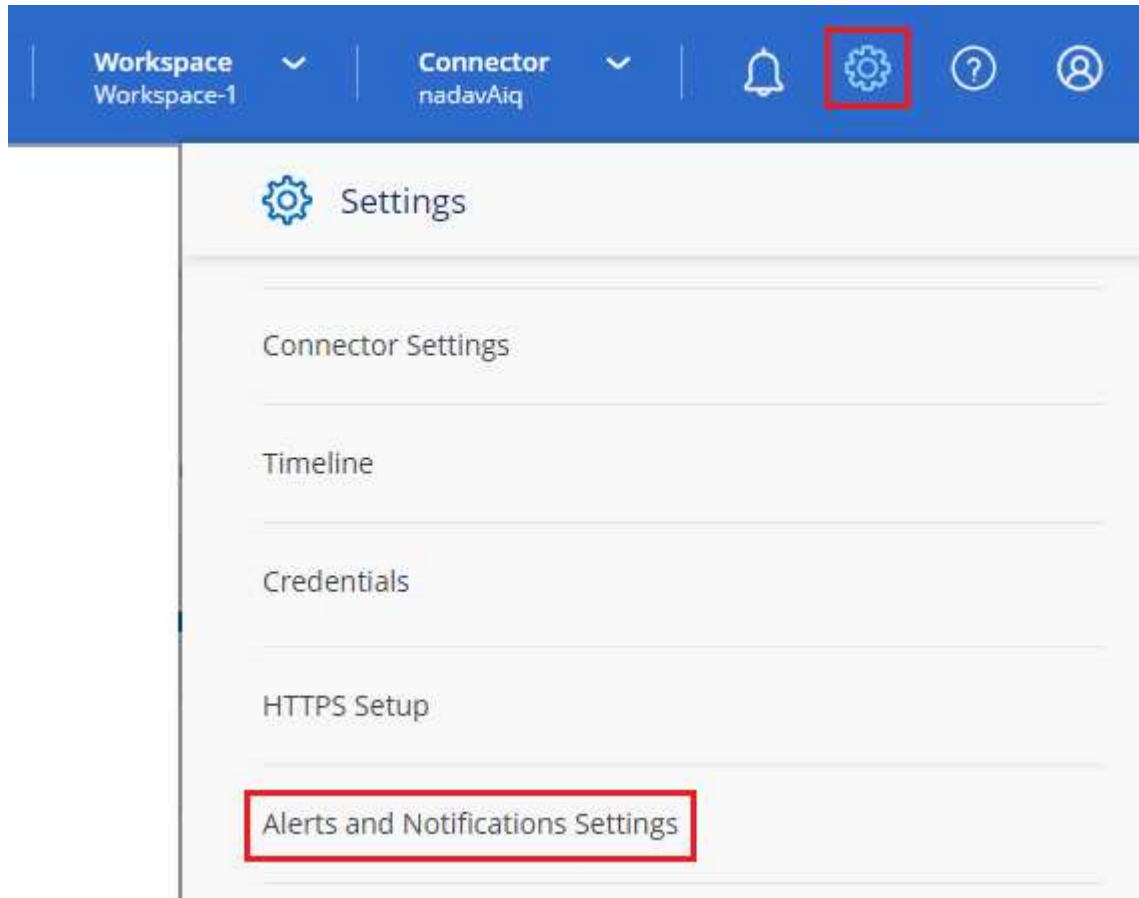
- Derzeit senden nur Cloud Sync und Cloud Backup Benachrichtigungen per E-Mail. Weitere Services werden in zukünftigen Versionen hinzugefügt.
- Das Senden von E-Mail-Benachrichtigungen wird nicht unterstützt, wenn der Connector auf einer Website ohne Internetzugang installiert ist.

Standardmäßig erhalten BlueXP-Kontoadministratoren E-Mails für alle „kritischen“ und „Empfehlungsbenachrichtigungen“. Alle anderen Benutzer und Empfänger sind standardmäßig so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten.

Sie müssen ein Kontoadministrator sein, um die Benachrichtigungseinstellungen anzupassen.

Schritte

1. Klicken Sie in der Menüleiste von BlueXP auf **Einstellungen > Einstellungen für Warnungen und Benachrichtigungen**.



2. Wählen Sie einen Benutzer oder mehrere Benutzer entweder auf der Registerkarte *Account Users* oder auf der Registerkarte *Additional Recipients* aus, und wählen Sie den Typ der zu sendenden Benachrichtigungen aus:
 - Um Änderungen an einem einzelnen Benutzer vorzunehmen, klicken Sie in der Spalte Benachrichtigungen für diesen Benutzer auf das Menü, überprüfen Sie die zu sendenden Benachrichtigungsarten und klicken Sie auf **Anwenden**.
 - Um Änderungen für mehrere Benutzer vorzunehmen, aktivieren Sie das Kontrollkästchen für jeden Benutzer, klicken Sie auf **E-Mail-Benachrichtigungen verwalten**, markieren Sie die zu sendenden Benachrichtigungsarten und klicken Sie auf **Anwenden**.

| Email | Name | Role |
|--|---------|-----------------|
| <input type="checkbox"/> Sabar@netapp.com | Sabar V | Account Admin |
| <input checked="" type="checkbox"/> activeiq@netapp-st.com | nadav | Account Admin |
| <input checked="" type="checkbox"/> nand@netapp.com | AnanK | Account Admin |
| <input type="checkbox"/> apra@netapp.com | Aradev | Workspace Admin |
| <input type="checkbox"/> ash@netapp.com | AshG | Account Admin |

Hinzufügen von zusätzlichen E-Mail-Empfängern

Die Benutzer, die auf der Registerkarte „Account Users“ angezeigt werden, werden automatisch von den Benutzern Ihres NetApp Kontos ausgefüllt (von der [Seite „Konto verwalten“](#)). Sie können E-Mail-Adressen auf der Registerkarte „Additional Recipients“ für andere Personen oder Gruppen hinzufügen, die keinen Zugriff auf BlueXP haben, aber über bestimmte Arten von Warnungen und Benachrichtigungen benachrichtigt werden müssen.

Schritte

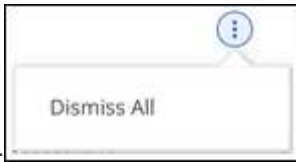
1. Klicken Sie auf der Seite Einstellungen für Warnungen und Benachrichtigungen auf **Neue Empfänger hinzufügen**.

2. Geben Sie den Namen, die E-Mail-Adresse ein, und wählen Sie die Art der Benachrichtigungen aus, die der Empfänger empfangen wird, und klicken Sie auf **Neuen Empfänger hinzufügen**.

Benachrichtigungen nicht vorhanden

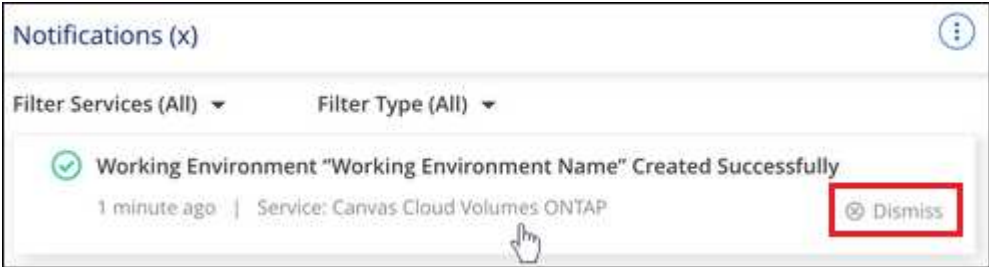
Sie können Benachrichtigungen von der Seite entfernen, wenn Sie sie nicht mehr sehen müssen. Sie können alle Benachrichtigungen auf einmal verwerfen oder einzelne Benachrichtigungen verwerfen.

Um alle Benachrichtigungen auszublenden, klicken Sie im Benachrichtigungscenter auf Und wählen Sie **Alle**



verwerfen.

Um einzelne Benachrichtigungen zu verwerfen, bewegen Sie den Cursor über die Benachrichtigung und



klicken auf **abweisen**.

Benutzeraktivitäten in Ihrem Konto prüfen

In der Zeitleiste in BlueXP werden die Aktionen angezeigt, die Benutzer zur Verwaltung Ihres Kontos abgeschlossen haben. Dazu gehören Verwaltungsaktionen wie das Verknüpfen von Benutzern, das Erstellen von Arbeitsbereichen, das Erstellen von Connectors und vieles mehr.

Das Prüfen der Zeitleiste kann hilfreich sein, wenn Sie feststellen müssen, wer eine bestimmte Aktion durchgeführt hat oder ob Sie den Status einer Aktion identifizieren müssen.

Schritte

1. Klicken Sie in der Menüleiste von BlueXP auf **Einstellungen > Timeline**.
2. Klicken Sie unter Filter auf **Service**, aktivieren Sie **Tenancy** und klicken Sie auf **Apply**.

Die Zeitleiste wird aktualisiert, um Ihnen Aktionen zur Kontoverwaltung anzuzeigen.

Rollen

Die Rollen Kontoverwaltung, Arbeitsbereichsverwaltung, Compliance Viewer und SnapCenter-Admin bieten Benutzern spezifische Berechtigungen.

Die Compliance Viewer-Rolle dient dem schreibgeschützten Cloud Data Sense Zugriff.

| Aufgabe | Kontoadministrat or | Workspace- Verwaltung | Compliance Viewer | SnapCenter Admin |
|---|------------------------|--------------------------|----------------------|---------------------|
| Verwalten von Arbeitsumgebungen | Ja. | Ja. | Nein | Nein |
| Services in Arbeitsumgebungen ermöglichen | Ja. | Ja. | Nein | Nein |
| Anzeigen des Status der Datenreplizierung | Ja. | Ja. | Nein | Nein |
| Zeitachse anzeigen | Ja. | Ja. | Nein | Nein |
| Wechseln Sie zwischen Arbeitsbereichen | Ja. | Ja. | Ja. | Nein |

| Aufgabe | Kontoadministrat or | Workspace- Verwaltung | Compliance Viewer | SnapCenter Admin |
|--|------------------------|--------------------------|----------------------|---------------------|
| Zeigen Sie die Ergebnisse des Data Sense-Scans an | Ja. | Ja. | Ja. | Nein |
| Arbeitsumgebungen löschen | Ja. | Nein | Nein | Nein |
| Kubernetes-Cluster mit Arbeitsumgebungen verbinden | Ja. | Nein | Nein | Nein |
| Cloud Volumes ONTAP Bericht erhalten | Ja. | Nein | Nein | Nein |
| Anschlüsse Erstellen | Ja. | Nein | Nein | Nein |
| NetApp Accounts managen | Ja. | Nein | Nein | Nein |
| Anmeldeinformationen verwalten | Ja. | Nein | Nein | Nein |
| Ändern Sie die Einstellungen von BlueXP | Ja. | Nein | Nein | Nein |
| Anzeigen und Verwalten des Support-Dashboards | Ja. | Nein | Nein | Nein |
| Entfernen Sie Arbeitsumgebungen aus BlueXP | Ja. | Nein | Nein | Nein |
| Installieren Sie ein HTTPS-Zertifikat | Ja. | Nein | Nein | Nein |
| Verwenden Sie den SnapCenter-Dienst | Ja. | Ja. | Nein | Ja. |

Weiterführende Links

- ["Einrichtung von Workspaces und Benutzern im NetApp Konto"](#)
- ["Managen von Workspaces und Benutzern im NetApp Account"](#)

Anschlüsse

Erweiterte Implementierung

Erstellen Sie einen Connector aus dem AWS Marketplace

Für eine kommerzielle AWS Region empfiehlt es sich, einen Connector direkt aus BlueXP zu erstellen, aber Sie können einen Connector auf dem AWS Marketplace starten, falls Sie es bevorzugen. Für Regionen der AWS Regierung kann der Connector nicht über die BlueXP SaaS-Website in einer Regierungsregion bereitgestellt werden. Die nächste

Option ist daher der AWS Marketplace.



Sie können die Connector-Software auch auf einem bestehenden Linux-Host in Ihrem Netzwerk oder in der Cloud herunterladen und installieren. ["Erfahren Sie, wie Sie den Connector auf einem vorhandenen Linux-Host installieren"](#).

Connector in einer kommerziellen AWS-Region erstellen

Sie können die Connector-Instanz direkt aus dem AWS Marketplace-Angebot für BlueXP in einer kommerziellen AWS-Region starten.

Der IAM-Benutzer, der den Connector erstellt, muss über AWS Marketplace-Berechtigungen zum Abonnieren und Abbestellen verfügen.

Schritte

1. Einrichten von Berechtigungen in AWS:
 - a. Erstellen Sie über die IAM-Konsole die erforderlichen Richtlinien, indem Sie die Inhalte von kopieren und einfügen ["Die IAM-Richtlinien für den Connector"](#).
 - b. Erstellen Sie eine IAM-Rolle mit dem Rollentyp Amazon EC2 und hängen Sie die Richtlinien an, die Sie im vorherigen Schritt erstellt haben.
2. Wechseln Sie zum ["Seite „BlueXP“ im AWS Marketplace"](#) So stellen Sie den Stecker über eine AMI bereit:
3. Klicken Sie auf der Marketplace-Seite auf **Weiter zur Anmeldung** und dann auf **Weiter zur Konfiguration**.

a

es ▾ Delivery Methods ▾ Solutions ▾ Migration Mapping Assistant Your Saved List **2** Partners Sell in AWS Marketplace Amazon Web Services Home

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price
\$0.226/hr

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

Overview Pricing Usage Support Reviews

Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

Highlights

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

b

es ▾ Delivery Methods ▾ Solutions ▾ Migration Mapping Assistant Your Saved List **2** Partners Sell in AWS Marketplace Amazon Web Services Home

Cloud Manager - Manual Installation without access keys

[Continue to Configuration](#)

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

Subscribe to this software

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

Terms and Conditions

NetApp, Inc. Offer

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

- Ändern Sie eine der Standardoptionen, und klicken Sie auf **Weiter zum Starten**.
- Wählen Sie unter **Aktion auswählen über EC2 starten** und klicken Sie dann auf **Start**.

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.

- 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 der unterstützten Instanztypen (t3.xlarge wird empfohlen).

["Prüfen Sie die Anforderungen an die Instanz".](#)

- **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.
- **Storage konfigurieren:** Behalten Sie die standardmäßigen Speicheroptionen bei.
- **Erweiterte Details:** Wählen Sie unter **IAM-Instanzprofil** die IAM-Rolle aus, die Sie in Schritt 1 erstellt haben.
- **Zusammenfassung:** Lesen Sie die Zusammenfassung durch und klicken Sie auf **Instanz starten**.

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

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

`https://ipaddress[]`

8. 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.



9. Öffnen Sie einen Webbrowser, und gehen Sie zu <https://cloudmanager.netapp.com> Um den Connector mit BlueXP zu verwenden.

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 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](#)".

Connector in einer AWS-Regierungsregion erstellen

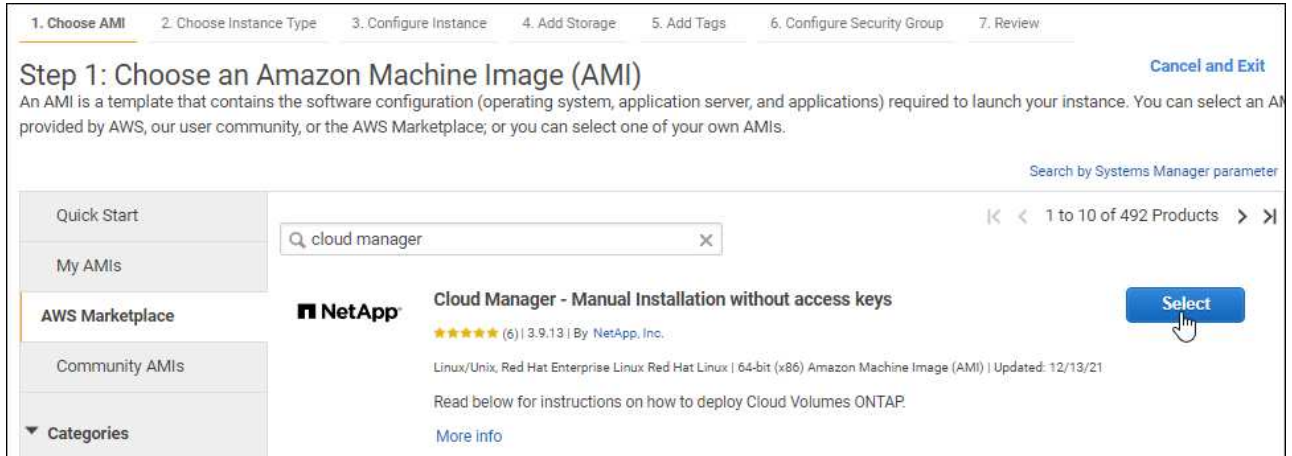
Für die Implementierung des Connectors in einer AWS Government-Region müssen Sie den EC2 Service besuchen und das BlueXP-Angebot im AWS Marketplace auswählen.

Schritte

1. Einrichten von Berechtigungen in AWS:
 - a. Erstellen Sie von der IAM-Konsole aus Ihre eigene Richtlinie, indem Sie die Inhalte von kopieren und einfügen "[Die IAM-Richtlinie für den Connector](#)".
 - b. Erstellen Sie eine IAM-Rolle mit dem Rollentyp Amazon EC2, und hängen Sie die im vorherigen Schritt erstellte Richtlinie an die Rolle an.
2. Gehen Sie zum BlueXP Angebot im AWS Marketplace.

Der IAM-Benutzer muss über AWS Marketplace-Berechtigungen zum Abonnieren und Abbestellen verfügen.

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



- d. Klicken Sie Auf **Weiter**.

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

- **Wählen Sie einen Instanztyp:** Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.xlarge wird empfohlen).

"Prüfen Sie die Anforderungen an die Instanz".

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

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

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

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

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

`https://ipaddress[]`

- Richten Sie nach der Anmeldung den Konnektor ein:
 - Geben Sie den NetApp Account an, der mit dem Connector verknüpft werden soll.
["Informationen zu NetApp Accounts"](#).
 - Geben Sie einen Namen für das System ein.



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

Wenn Sie BlueXP verwenden möchten, öffnen Sie Ihren Webbrowser und stellen Sie eine Verbindung zur IP-Adresse der Connector-Instanz her: [https://ipaddress\[\]](https://ipaddress[])

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

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 aus dem Azure Marketplace

Für eine kommerzielle Azure-Region ist es am besten, einen Connector direkt aus BlueXP zu erstellen, aber Sie können einen Connector im Azure Marketplace starten, falls Sie es bevorzugen. Für Azure-Regierungsregionen kann der Connector nicht über die BlueXP SaaS-Website in einer Regierungsregion bereitgestellt werden. Die nächste Option ist daher der Azure Marketplace.



Sie können die Connector-Software auch auf einem bestehenden Linux-Host in Ihrem Netzwerk oder in der Cloud herunterladen und installieren. ["Erfahren Sie, wie Sie den Connector auf einem vorhandenen Linux-Host installieren"](#).

Erstellen eines Connectors in Azure

Implementieren Sie den Connector in Azure mithilfe des Images im Azure Marketplace. Melden Sie sich dann bei Connector an, um Ihren NetApp Account anzugeben.

Schritte

1. Wechseln Sie im Azure Marketplace auf die Seite NetApp Connector VM.
 - ["Azure Marketplace-Seite für kommerzielle Regionen"](#)
 - ["Azure Marketplace-Seite für Azure Government Regions"](#)
2. Klicken Sie auf **Jetzt holen** und klicken Sie dann auf **Weiter**.
3. Klicken Sie im Azure-Portal auf **Erstellen** und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

Beachten Sie beim Konfigurieren der VM Folgendes:

- Der Connector kann mit Festplatten der Festplatte oder der SSD optimal arbeiten.
- Wählen Sie eine VM-Größe aus, die den CPU- und RAM-Anforderungen entspricht. Wir empfehlen DS3 v2.

["VM-Anforderungen prüfen"](#).

- Für die Netzwerksicherheitsgruppe benötigt der Connector eingehende Verbindungen unter Verwendung von SSH, HTTP und HTTPS.

["Erfahren Sie mehr über die Regeln für Sicherheitsgruppen für den Connector"](#).

- Aktivieren Sie unter **Management** * * die vom System zugewiesene verwaltete Identität* für den Connector, indem Sie **ein** wählen.

Diese Einstellung ist wichtig, da sich die Virtual Machine Connector mit Azure Active Directory identifizieren kann, ohne dass Anmeldedaten vorhanden sind. ["Erfahren Sie mehr über Managed Identitäten für Azure Ressourcen"](#).

4. Überprüfen Sie auf der Seite **Überprüfen + erstellen** Ihre Auswahl und klicken Sie auf **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.

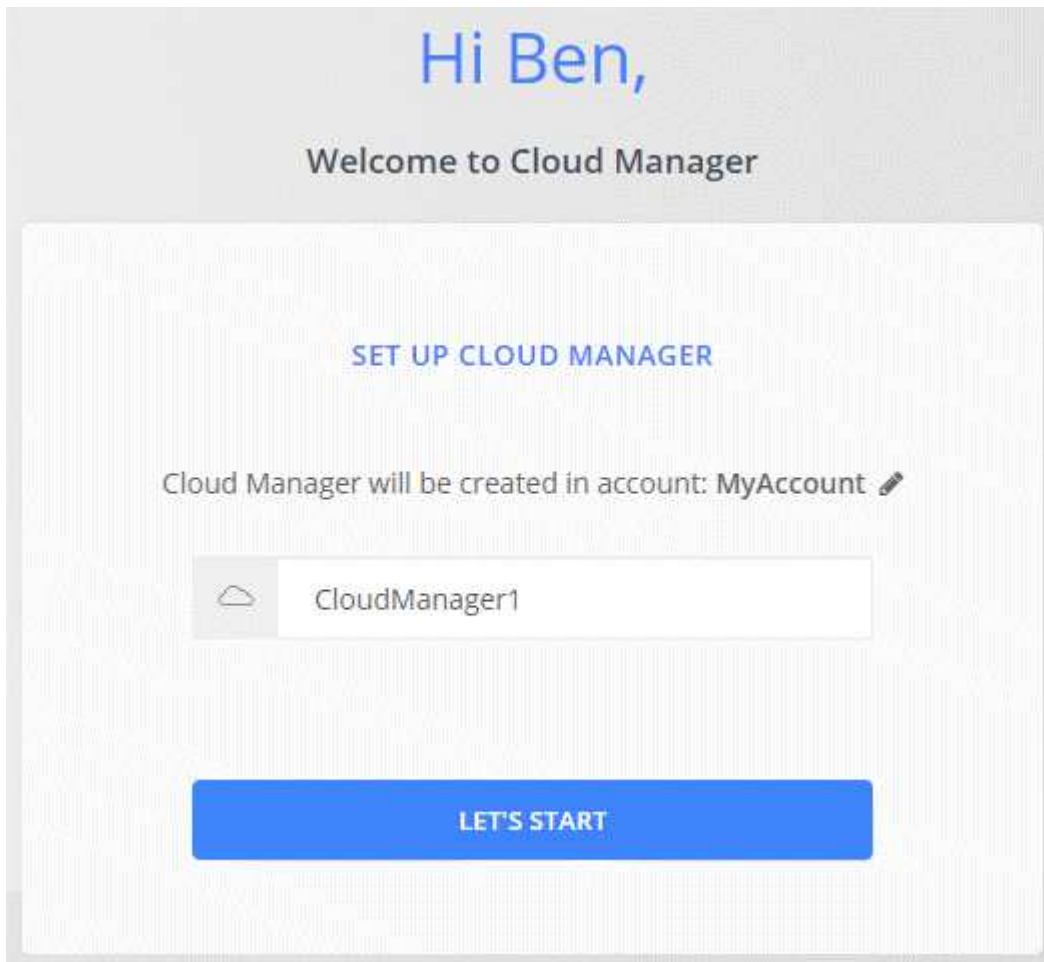
5. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung mit der virtuellen Verbindungsmaschine hat, und geben Sie die folgende URL ein:

[https://ipaddress\[\]](https://ipaddress[])

6. Richten Sie nach der Anmeldung den Konnektor ein:
- Geben Sie den NetApp Account an, der mit dem Connector verknüpft werden soll.

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

- Geben Sie einen Namen für das System ein.



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

Wenn sich der Connector in einer kommerziellen Azure-Region befindet, öffnen Sie einen Webbrowser, und gehen Sie zu <https://cloudmanager.netapp.com> Um den Connector mit BlueXP zu verwenden.

Wenn sich der Connector in einer Region der Azure-Regierung befindet, können Sie BlueXP verwenden, indem Sie Ihren Webbrowser öffnen und eine Verbindung zur IP-Adresse der Connector-Instanz herstellen: [https://ipaddress\[\]](https://ipaddress[])

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

Azure-Berechtigungen werden gewährt

Bei der Implementierung des Connectors in Azure sollten Sie a aktiviert haben "[Vom System zugewiesene verwaltete Identität](#)". Sie müssen nun die erforderlichen Azure-Berechtigungen erteilen, indem Sie eine benutzerdefinierte Rolle erstellen und dann die Rolle der virtuellen Connector-Maschine für ein oder mehrere Abonnements zuweisen.

Schritte

1. Erstellen einer benutzerdefinierten Rolle:
 - 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.

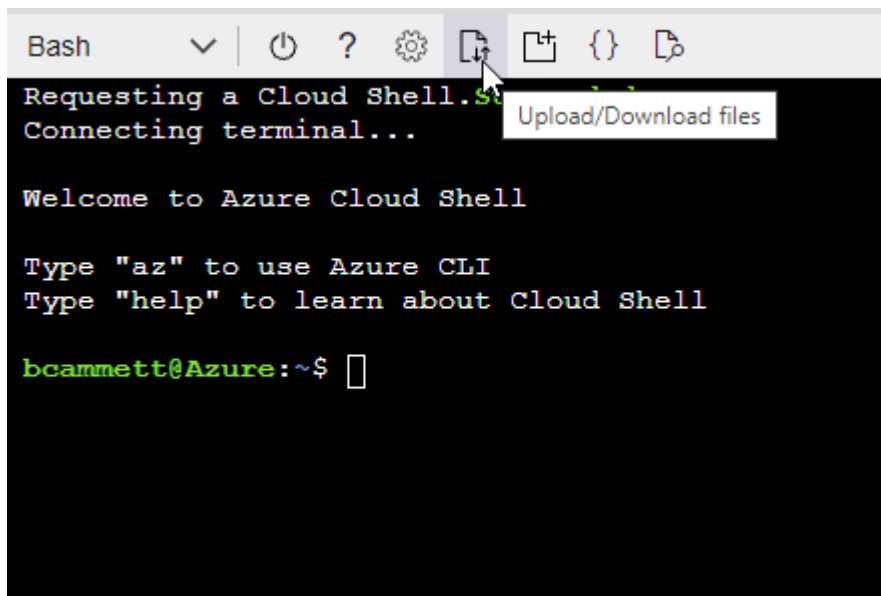
Beispiel

```
"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.



- Geben Sie den folgenden Befehl der Azure CLI ein:

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

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

2. Weisen Sie der virtuellen Verbindungsmaschine die Rolle für eine oder mehrere Abonnements zu:
 - a. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP-Systeme bereitstellen möchten.
 - b. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
 - c. Wählen Sie auf der Registerkarte * Role* die Rolle **BlueXP Operator** aus und klicken Sie auf **Next**.



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.

- d. Führen Sie auf der Registerkarte **Mitglieder** die folgenden Schritte aus:
 - Weisen Sie einer * verwalteten Identität* Zugriff zu.
 - Klicken Sie auf **Mitglieder auswählen**, wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde, wählen Sie **Virtuelle Maschine** und wählen Sie dann die virtuelle Connector-Maschine aus.
 - Klicken Sie Auf **Auswählen**.
 - Klicken Sie Auf **Weiter**.
- e. Klicken Sie auf **Review + Assign**.
- f. Wenn Sie Cloud Volumes ONTAP von zusätzlichen Abonnements aus implementieren möchten, wechseln Sie zu diesem Abonnement, und wiederholen Sie diese Schritte.

Der Connector verfügt nun über die Berechtigungen, die die IT für das Management von Ressourcen und Prozessen in Ihrer Public Cloud-Umgebung benötigt. 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 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.

Installieren Sie den Connector auf einem vorhandenen Linux-Host mit Internetzugang

Die häufigste Möglichkeit zur Erstellung eines Connectors liegt direkt über BlueXP oder über den Markt eines Cloud-Providers. Sie haben jedoch die Möglichkeit, die Connector-Software auf einem bestehenden Linux-Host in Ihrem Netzwerk oder in der Cloud herunterzuladen und zu installieren. Diese Schritte sind spezifisch für Hosts mit Internetzugang.

["Erfahren Sie mehr über andere Möglichkeiten zur Bereitstellung eines Connectors"](#).



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.

Host-Anforderungen prüfen

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

Ein dedizierter Host ist erforderlich

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

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Instanztyp für AWS EC2

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

Azure VM-Größe

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

GCP-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"](#)

Unterstützte Betriebssysteme

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9

- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

Das Red Hat Enterprise Linux System muss beim Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Connector-Installation nicht auf Repositories zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

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

Hypervisor

Ein Bare Metal- oder gehosteter Hypervisor, der für die Ausführung von CentOS oder Red hat Enterprise Linux zertifiziert ist <https://access.redhat.com/certified-hypervisors>["Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"^]

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine Version 19 oder höher ist auf dem Host erforderlich, bevor Sie den Connector installieren. ["Installationsanweisungen anzeigen"](#)

Outbound-Internetzugang

Das Installationsprogramm für den Connector muss während der Installation auf die folgenden URLs zugreifen:

- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
- https://*.blob.core.windows.net oder <https://hub.docker.com>

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

Den Stecker einbauen

Nachdem Sie sich vergewissern, dass Sie über einen unterstützten Linux-Host verfügen, können Sie die Connector-Software erwerben und dann installieren.

Zur Installation des Connectors sind Root-Berechtigungen erforderlich.

Über diese Aufgabe

- Die Installation installiert die AWS Befehlszeilen-Tools (awscli), um Recovery-Verfahren durch den NetApp Support zu ermöglichen.

Wenn Sie eine Meldung erhalten, dass die Installation des awscli fehlgeschlagen ist, können Sie die Meldung ignorieren. Der Steckverbinder kann ohne Werkzeuge erfolgreich betrieben werden.

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

Schritte

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

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

2. Laden Sie die Connector-Software von der herunter "[NetApp Support Website](#)", Und dann kopieren Sie es auf den Linux-Host.

Informationen zum Verbinden und Kopieren der Datei auf eine EC2-Instanz in AWS finden Sie unter "[AWS Documentation: Herstellen einer Verbindung zu Ihrer Linux-Instanz mithilfe von SSH](#)".

3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x OnCommandCloudManager-V3.9.23.sh
```

4. Führen Sie das Installationsskript aus.

Wenn Sie über einen Proxy-Server verfügen, müssen Sie die unten aufgeführten Befehlsparameter eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

```
./OnCommandCloudManager-V3.9.23.sh --proxy  
http://occm:password@10.0.0.30:9090/ --cacert /root/rootca.pem
```

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

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

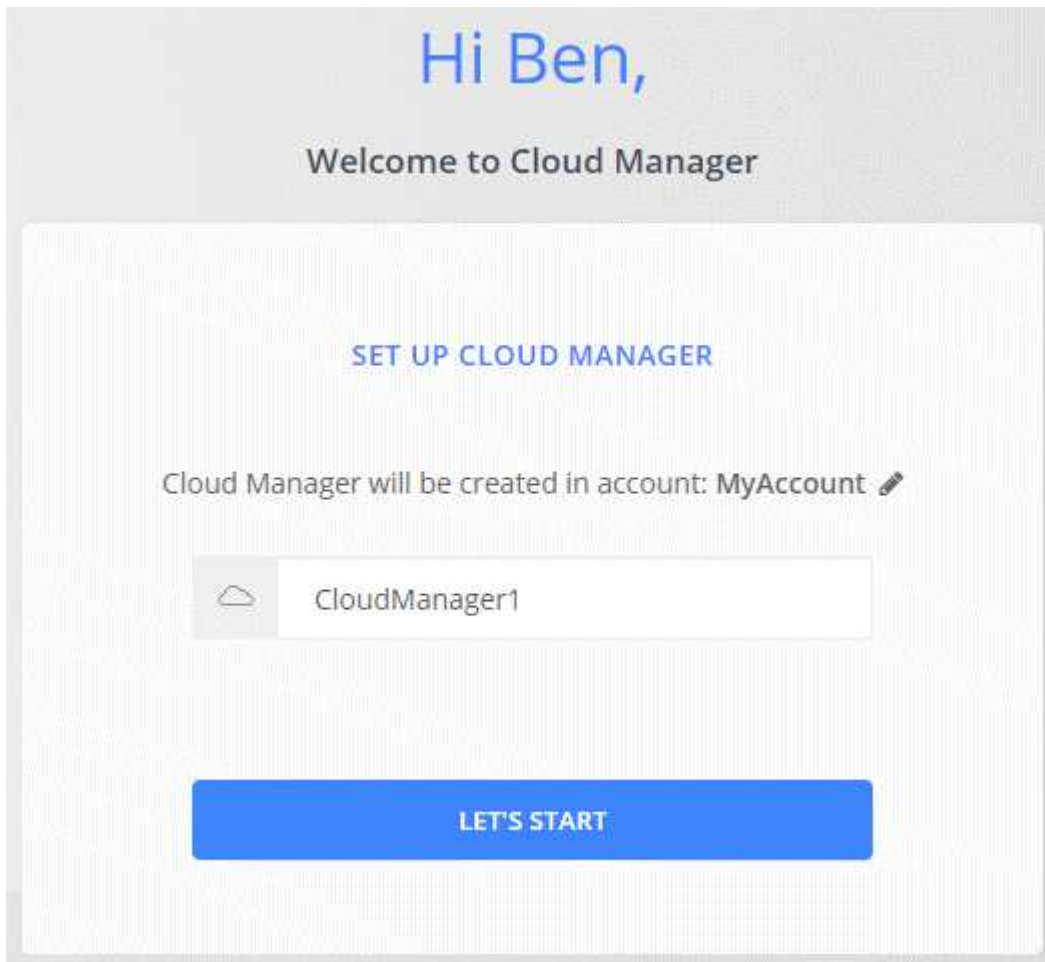
[https://ipaddress\[\]](https://ipaddress[])

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.

6. Anmelden oder anmelden.
7. Wenn Sie den Connector in Google Cloud installiert haben, richten Sie ein Servicekonto ein, das über die Berechtigungen verfügt, die BlueXP zum Erstellen und Verwalten von Cloud Volumes ONTAP-Systemen in Projekten benötigt.
 - a. "[Rolle in GCP anlegen](#)" Dazu gehören die im definierten Berechtigungen "[Connector-Richtlinie für GCP](#)".
 - b. "[Erstellen Sie ein GCP-Service-Konto und wenden Sie die benutzerdefinierte Rolle an, die Sie gerade erstellt haben](#)".

- c. "Verknüpfen Sie dieses Servicekonto mit der Connector-VM".
 - d. 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.
8. Richten Sie nach der Anmeldung BlueXP 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.



Der Connector ist jetzt mit Ihrem NetApp Konto installiert und eingerichtet. BlueXP verwendet diesen Connector automatisch, wenn Sie neue Arbeitsumgebungen erstellen.

Richten Sie Berechtigungen ein, damit BlueXP Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung verwalten kann:

- AWS, "[Richten Sie ein AWS-Konto ein und fügen Sie es dann BlueXP hinzu](#)"
- Azure: "[Richten Sie ein Azure-Konto ein und fügen Sie es dann BlueXP hinzu](#)"
- Google Cloud: Siehe Schritt 7 oben

Installieren Sie den Connector On-Prem ohne Internetzugang

Sie können den Connector auf einem lokalen Linux-Host installieren, der keinen Internetzugang hat. Anschließend können Sie ONTAP-Cluster vor Ort erkennen, Daten zwischen ihnen replizieren, Volumes mit Cloud Backup sichern und mithilfe von Cloud Data Sense scannen.

Diese Installationsanweisungen richten sich speziell an den oben beschriebenen Anwendungsfall. ["Erfahren Sie mehr über andere Möglichkeiten zur Bereitstellung eines Connectors"](#).

Host-Anforderungen prüfen

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

Ein dedizierter Host ist erforderlich

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

CPU

4 Kerne oder 4 vCPUs

RAM

14 GB

Unterstützte Betriebssysteme

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

Das Red Hat Enterprise Linux System muss beim Red Hat Subscription Management registriert sein. Wenn es nicht registriert ist, kann das System während der Connector-Installation nicht auf Repositories zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

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

Hypervisor

Ein Bare Metal- oder gehosteter Hypervisor, der für die Ausführung von CentOS oder Red hat Enterprise Linux zertifiziert ist <https://access.redhat.com/certified-hypervisors>["Red hat Solution: Welche Hypervisoren sind für die Ausführung von Red hat Enterprise Linux zertifiziert?"^]

Festplattentyp

Eine SSD ist erforderlich

Speicherplatz in /opt

100 gib Speicherplatz muss verfügbar sein

Festplattenspeicher in /var

20 gib Speicherplatz muss verfügbar sein

Docker Engine

Docker Engine Version 19 oder höher ist auf dem Host erforderlich, bevor Sie den Connector installieren.

["Installationsanweisungen anzeigen"](#)

Den Stecker einbauen

Nachdem Sie sich vergewissern, dass Sie über einen unterstützten Linux-Host verfügen, können Sie die Connector-Software erwerben und dann installieren.

Zur Installation des Connectors sind Root-Berechtigungen erforderlich.

Schritte

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

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

2. Laden Sie die Connector-Software von der herunter ["NetApp Support Website"](#)
3. Kopieren Sie das Installationsprogramm auf den Linux-Host.
4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

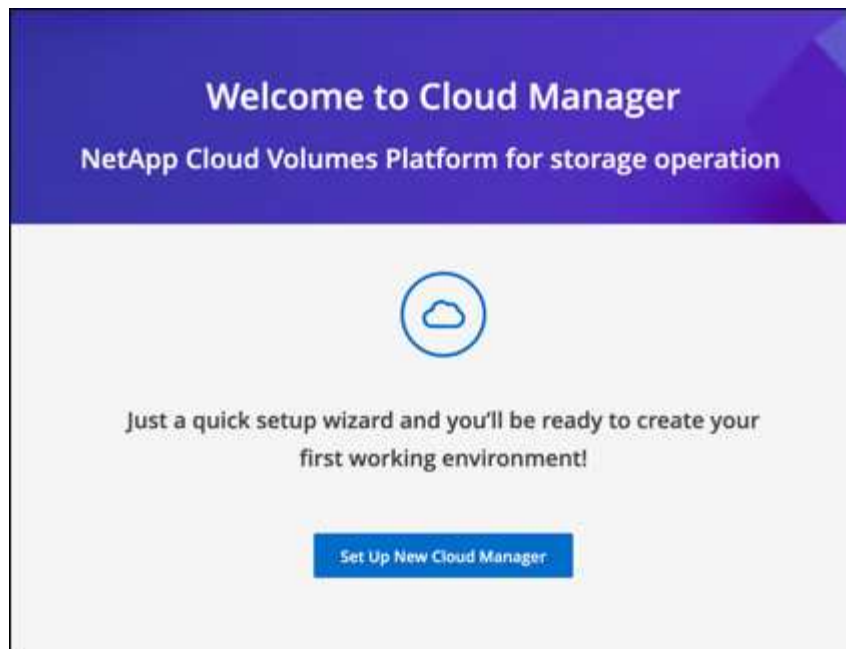
```
chmod +x /path/cloud-manager-connector-offline-v3.9.23
```

5. Führen Sie das Installationsskript aus:

```
sudo /path/cloud-manager-connector-offline-v3.9.23
```

6. Öffnen Sie einen Webbrowser, und geben Sie ein `https://ipaddress[]` Wobei *ipaddress* die IP-Adresse des Linux-Hosts ist.

Der folgende Bildschirm sollte angezeigt werden.



7. Klicken Sie auf **Neues BlueXP** einrichten und befolgen Sie die Anweisungen zur Einrichtung des Systems.
- **Systemdetails:** Geben Sie einen Namen für den Connector und Ihren Firmennamen ein.

A screenshot of the 'System Details' setup screen. At the top, there are three steps: '1 System Details', '2 Create Admin User', and '3 Review'. The main heading is 'System Details'. Below it, a message says: 'To help us provide better support, enter a name for Cloud Manager and your company name.' There are two input fields: 'Cloud Manager Name' and 'Company Name'.

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

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

- **Review:** Lesen Sie die Details durch, akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Einrichten**.

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

Der Connector ist jetzt installiert und Sie können die BlueXP-Funktionen nutzen, die bei der Installation an dunklen Standorten verfügbar sind.

Was und#8217;s als Nächstes?

- ["Erkennen von On-Premises-ONTAP-Clustern"](#)

- "Replizieren von Daten zwischen lokalen ONTAP Clustern"
- "On-Premises-ONTAP-Volume-Daten werden mit Cloud-Backup in StorageGRID gesichert"
- "Scannen Sie ONTAP-Volume-Daten vor Ort mit Cloud-Data Sense"

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

Suchen der System-ID für einen Konnektor

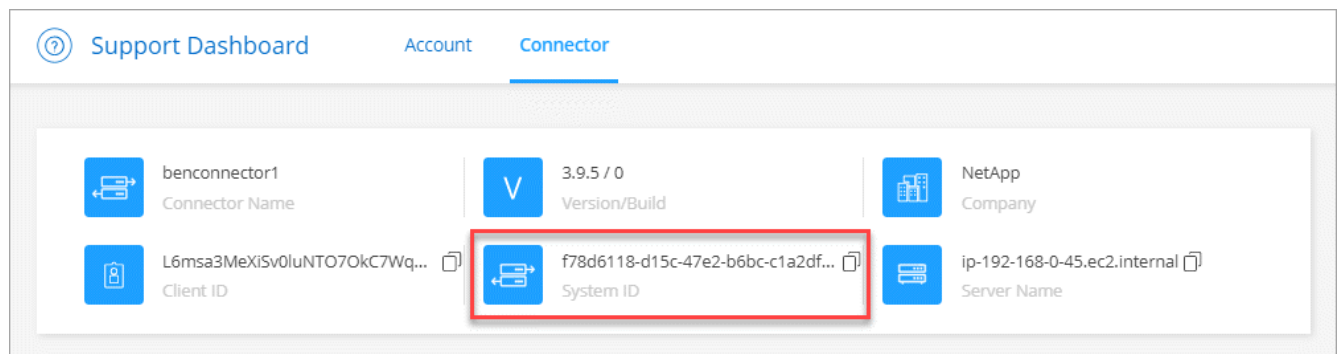
Um Ihnen bei den ersten Schritten zu helfen, bittet Ihr NetApp Mitarbeiter Sie möglicherweise um die System-ID für einen Connector. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol.
2. Klicken Sie Auf **Support > Connector**.

Die System-ID wird oben angezeigt.

Beispiel



Verwalten vorhandener Anschlüsse

Nachdem Sie einen oder mehrere Anschlüsse erstellt haben, können Sie diese verwalten, indem Sie zwischen den Anschlüssen wechseln, eine Verbindung zur lokalen Benutzeroberfläche herstellen, die auf einem Connector ausgeführt wird, und mehr.

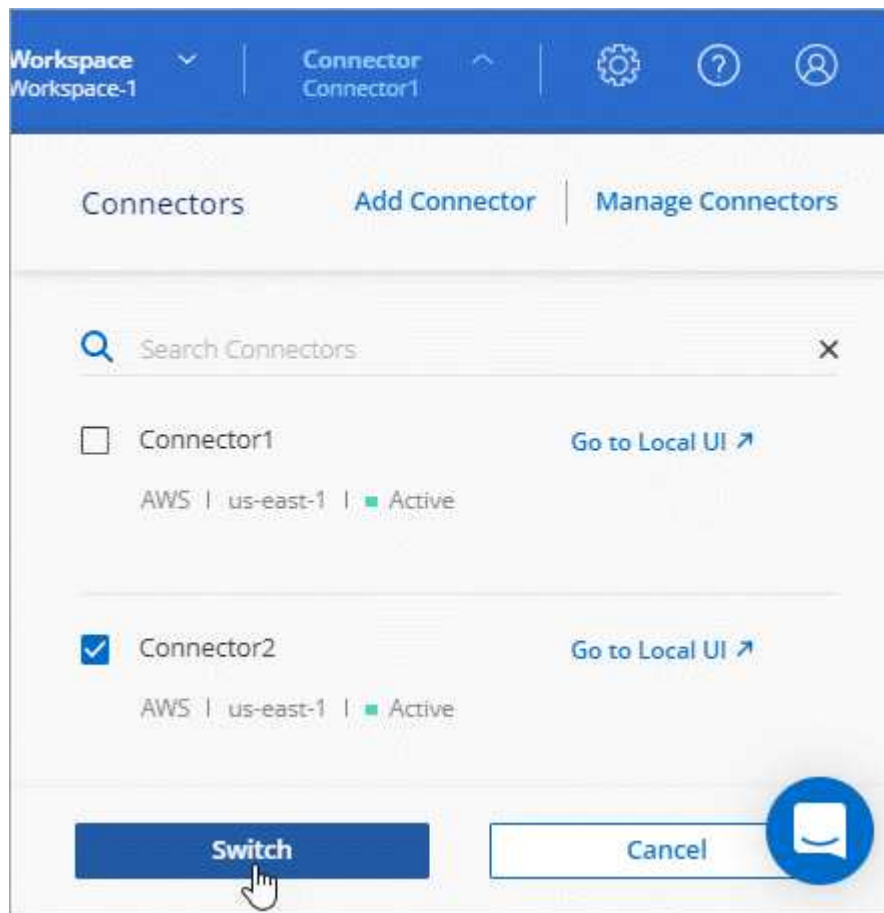
Zwischen den Anschlüssen wechseln

Wenn Sie über mehrere Anschlüsse verfügen, können Sie zwischen diesen wechseln, um die Arbeitsumgebungen zu sehen, die mit einem bestimmten Konnektor verknüpft sind.

Nehmen wir zum Beispiel an, dass Sie in einer Multi-Cloud-Umgebung arbeiten. Möglicherweise verfügen Sie über einen Connector in AWS und einen anderen in Google Cloud. Zum Managen der Cloud Volumes ONTAP Systeme, die in diesen Clouds ausgeführt werden, müsste zwischen diesen Anschlüssen gewechselt werden.

Schritt

1. Klicken Sie auf das Dropdown-Menü **Connector**, wählen Sie einen anderen Anschluss aus und klicken Sie dann auf **Switch**.



BlueXP aktualisiert und zeigt die Arbeitsumgebungen, die mit dem ausgewählten Connector verknüpft sind.

Greifen Sie auf die lokale UI zu

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Wenn Sie über eine Regierungsregion oder eine Website ohne Outbound-Internetzugang auf BlueXP zugreifen, müssen Sie die lokale Benutzeroberfläche verwenden, die auf dem Connector ausgeführt wird.

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.

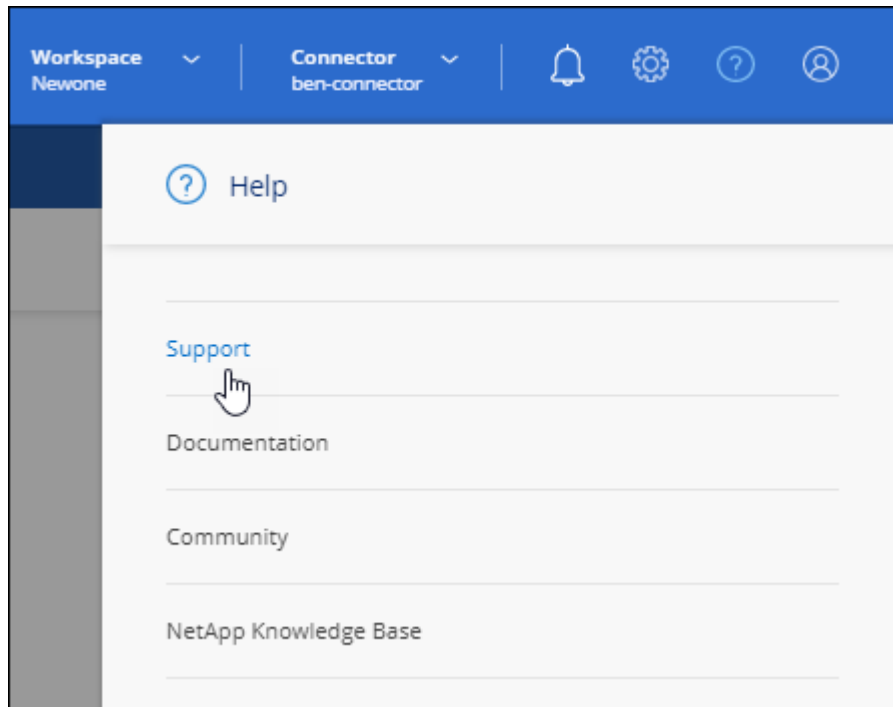
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um sich anzumelden.

Laden Sie eine AutoSupport Nachricht herunter oder senden Sie sie

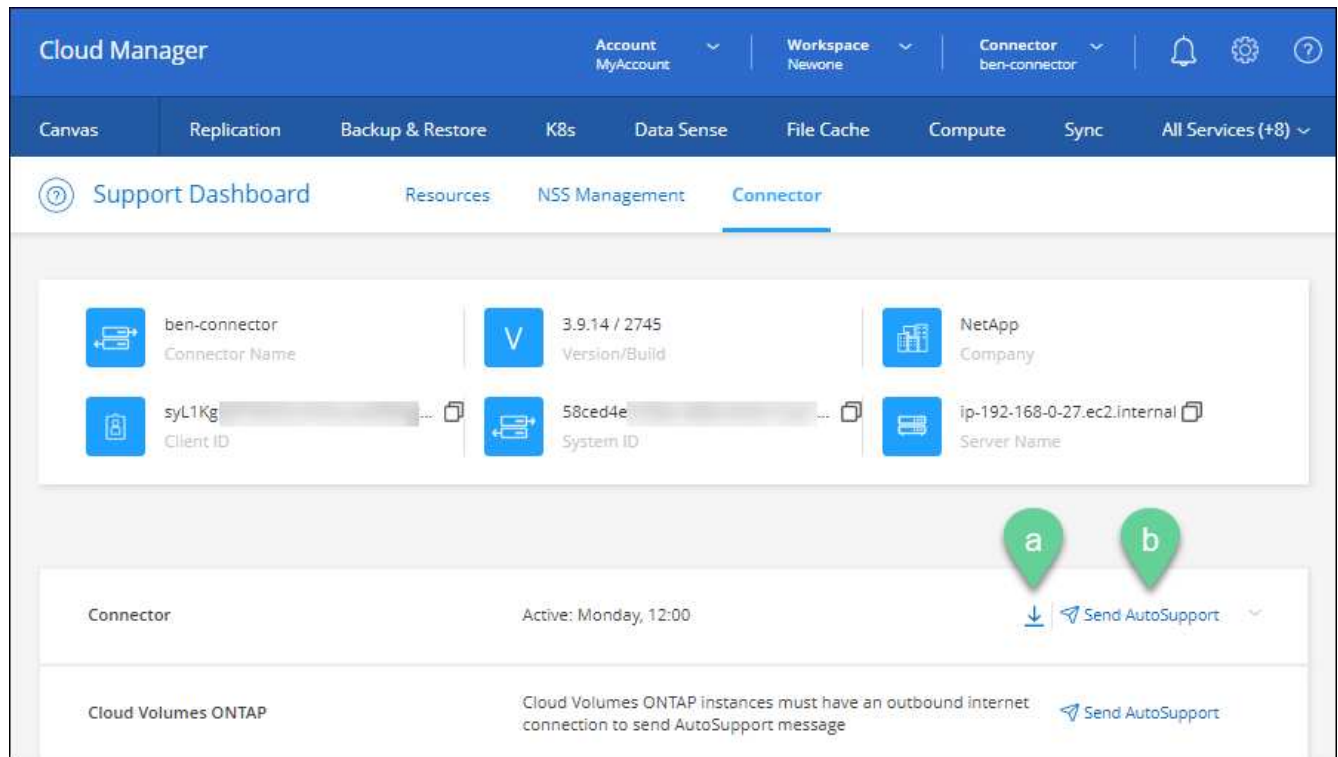
Wenn Sie Probleme haben, werden Sie möglicherweise von den Mitarbeitern von NetApp gebeten, zur Fehlerbehebung eine AutoSupport Nachricht an den NetApp Support zu senden.

Schritte

1. Stellen Sie eine Verbindung zur lokalen Benutzeroberfläche des Connectors her, wie im Abschnitt oben beschrieben.
2. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



3. Klicken Sie Auf **Connector**.
4. Je nachdem, wie Sie die Informationen an den NetApp Support senden, wählen Sie eine der folgenden Optionen:
 - a. Wählen Sie die Option, um die AutoSupport-Nachricht auf Ihren lokalen Computer herunterzuladen. Sie können es dann auf bevorzugte Art und Weise an den NetApp Support senden.
 - b. Klicken Sie auf **AutoSupport senden**, um die Nachricht direkt an den NetApp Support zu senden.



Stellen Sie eine Verbindung zur Linux VM her

Wenn Sie eine Verbindung zur Linux-VM herstellen möchten, auf der der Connector ausgeführt wird, können Sie dies über die Verbindungsoptionen Ihres Cloud-Providers tun.

AWS

Als Sie die Connector-Instanz in AWS erstellt haben, haben Sie einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel angegeben. Sie können dieses Schlüsselpaar für SSH zur Instanz verwenden.

["AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"](#)

Azure

Bei der Erstellung der Connector-VM in Azure wählen Sie die Authentifizierung mit einem Passwort oder einem öffentlichen SSH-Schlüssel aus. Verwenden Sie die Authentifizierungsmethode, die Sie für die Verbindung zur VM ausgewählt haben.

["Azure Docs: SSH in Ihre VM"](#)

Google Cloud

Sie können keine Authentifizierungsmethode angeben, wenn Sie einen Connector in Google Cloud erstellen. Sie können eine Verbindung zur Linux VM-Instanz jedoch über die Google Cloud Console oder Google Cloud CLI (gcloud) herstellen.

["Google Cloud Docs: Verbindung zu Linux-VMs herstellen"](#)

Sicherheitsupdates anwenden

Aktualisieren Sie das Betriebssystem auf dem Konnektor, um sicherzustellen, dass es mit den neuesten

Sicherheitsupdates gepatcht wird.

Schritte

1. Greifen Sie auf die CLI-Shell auf dem Connector-Host zu.
2. Führen Sie folgende Befehle mit erhöhten Berechtigungen aus:

```
sudo -s
service netapp-service-manager stop
yum -y update --security
service netapp-service-manager start
```

Ändern Sie die IP-Adresse für einen Konnektor

Wenn es für Ihr Unternehmen erforderlich ist, können Sie die interne IP-Adresse und die öffentliche IP-Adresse der Connector-Instanz ändern, die automatisch von Ihrem Cloud-Provider zugewiesen wird.

Schritte

1. Befolgen Sie die Anweisungen Ihres Cloud-Providers, um die lokale IP-Adresse oder die öffentliche IP-Adresse (oder beide) für die Connector-Instanz zu ändern.
2. Wenn Sie die öffentliche IP-Adresse geändert haben und eine Verbindung zur lokalen Benutzeroberfläche auf dem Connector herstellen müssen, starten Sie die Connector-Instanz neu, um die neue IP-Adresse bei BlueXP zu registrieren.
3. Wenn Sie die private IP-Adresse geändert haben, aktualisieren Sie den Backup-Speicherort für Cloud Volumes ONTAP-Konfigurationsdateien, so dass die Backups an die neue private IP-Adresse des Connectors gesendet werden.
 - a. Führen Sie den folgenden Befehl aus der Cloud Volumes ONTAP-CLI aus, um das aktuelle Backup-Ziel zu entfernen:

```
system configuration backup settings modify -destination ""
```

- b. Gehen Sie zu BlueXP, und öffnen Sie die Arbeitsumgebung.
- c. Klicken Sie auf das Menü und wählen Sie **Erweitert > Konfigurations-Backups**.
- d. Klicken Sie Auf **Backup-Ziel Festlegen**.

Bearbeiten Sie die URIs eines Connectors

Fügen Sie die URIs für einen Konnektor hinzu und entfernen Sie sie.

Schritte

1. Klicken Sie in der BlueXP-Kopfzeile auf das Dropdown-Menü **Connector**.
2. Klicken Sie Auf **Connectors Verwalten**.
3. Klicken Sie auf das Aktionsmenü für einen Konnektor und klicken Sie auf **URIs bearbeiten**.
4. Fügen Sie URIs hinzu und entfernen Sie sie, und klicken Sie dann auf **Anwenden**.

Beheben Sie Download-Fehler bei Verwendung eines Google Cloud NAT-Gateways

Der Connector lädt automatisch Software-Updates für Cloud Volumes ONTAP herunter. Der Download kann fehlschlagen, wenn Ihre Konfiguration ein Google Cloud NAT Gateway verwendet. Sie können dieses Problem beheben, indem Sie die Anzahl der Teile begrenzen, in die das Software-Image unterteilt ist. Dieser Schritt muss mithilfe der BlueXP API abgeschlossen werden.

Schritt

1. SENDEN SIE EINE PUT-Anforderung an `/occm/config` mit dem folgenden JSON als Text:

```
{
  "maxDownloadSessions": 32
}
```

Der Wert für `maxDownloadSessions` kann 1 oder eine beliebige Ganzzahl größer als 1 sein. Wenn der Wert 1 ist, wird das heruntergeladene Bild nicht geteilt.

Beachten Sie, dass 32 ein Beispielwert ist. Der Wert, den Sie verwenden sollten, hängt von Ihrer NAT-Konfiguration und der Anzahl der Sitzungen ab, die Sie gleichzeitig haben können.

["Erfahren Sie mehr über den Aufruf der `/occm/config` API"](#).

Upgrade des Connectors On-Prem ohne Internetzugang

Wenn Sie ["Der Connector wurde auf einem lokalen Host installiert, der keinen Internetzugang hat"](#), Sie können den Connector aktualisieren, wenn eine neuere Version von der NetApp Support-Website verfügbar ist.

Der Connector muss während des Aktualisierungsvorgangs neu gestartet werden, damit die Benutzeroberfläche während des Upgrades nicht verfügbar ist.

Schritte

1. Laden Sie die Connector-Software von der herunter ["NetApp Support Website"](#).
2. Kopieren Sie das Installationsprogramm auf den Linux-Host.
3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. Führen Sie das Installationsskript aus:

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. Nachdem die Aktualisierung abgeschlossen ist, können Sie die Version des Connectors überprüfen, indem Sie **Hilfe > Support > Connector** aufrufen.

Wie sieht es mit Software-Upgrades auf Hosts mit Internetzugang aus?

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

Entfernen Sie die Anschlüsse von BlueXP

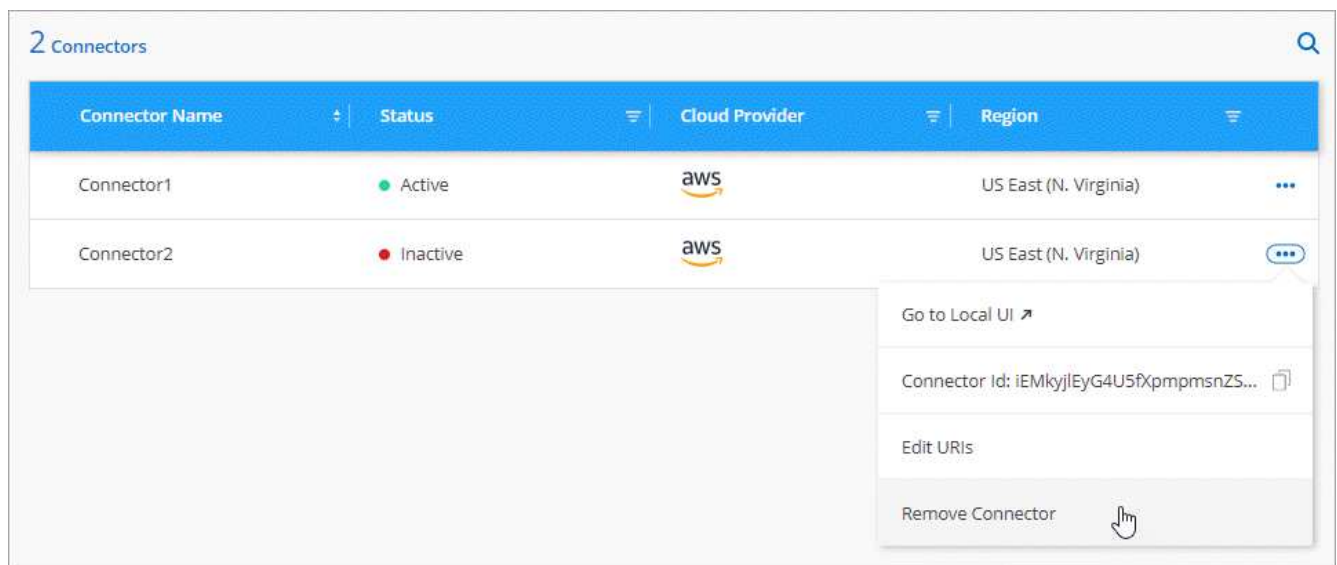
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in BlueXP entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

Beachten Sie Folgendes zum Entfernen eines Konnektors:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden. Wenn Sie einen Connector aus BlueXP entfernen, können Sie ihn nicht wieder hinzufügen

Schritte

1. Klicken Sie in der BlueXP-Kopfzeile auf das Dropdown-Menü **Connector**.
2. Klicken Sie Auf **Connectors Verwalten**.
3. Klicken Sie auf das Aktionsmenü für einen inaktiven Konnektor und klicken Sie auf **Connector entfernen**.



4. Geben Sie den Namen des zu bestätigenden Connectors ein, und klicken Sie anschließend auf Entfernen.

BlueXP entfernt den Connector aus seinen Datensätzen.

Deinstallieren Sie die Connector-Software

Deinstallieren Sie die Connector-Software, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Die Schritte, die Sie verwenden müssen, hängen davon ab, ob Sie den Connector auf einem Host mit Internetzugang oder einem Host in einem eingeschränkten Netzwerk installiert haben, das keinen Internetzugang hat.

Deinstallieren Sie von einem Host mit Internetzugang

Der Online Connector enthält ein Deinstallationsskript, mit dem Sie die Software deinstallieren können.

Schritt

1. Führen Sie auf dem Linux-Host das Deinstallationsskript aus:

```
/opt/Application/netapp/cloudmanager/bin/uninstall.sh [Silent]
```

Silent führt das Skript aus, ohne dass Sie zur Bestätigung aufgefordert werden.

Deinstallieren Sie von einem Host ohne Internetzugang

Verwenden Sie diese Befehle, wenn Sie die Connector Software von der NetApp Support Site heruntergeladen und in einem Netzwerk mit beschränktem Zugriff installiert haben.

Schritt

1. Führen Sie auf dem Linux-Host die folgenden Befehle aus:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

Verwalten eines HTTPS-Zertifikats für sicheren Zugriff

Standardmäßig verwendet BlueXP ein selbstsigniertes Zertifikat für HTTPS-Zugriff auf die Webkonsole. Sie können ein Zertifikat installieren, das von einer Zertifizierungsstelle (CA) signiert wurde. Dies bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. ["Erfahren Sie, wie"](#).

Installieren eines HTTPS-Zertifikats

Installieren Sie ein von einer Zertifizierungsstelle signiertes Zertifikat, um den sicheren Zugriff zu gewährleisten.

Schritte

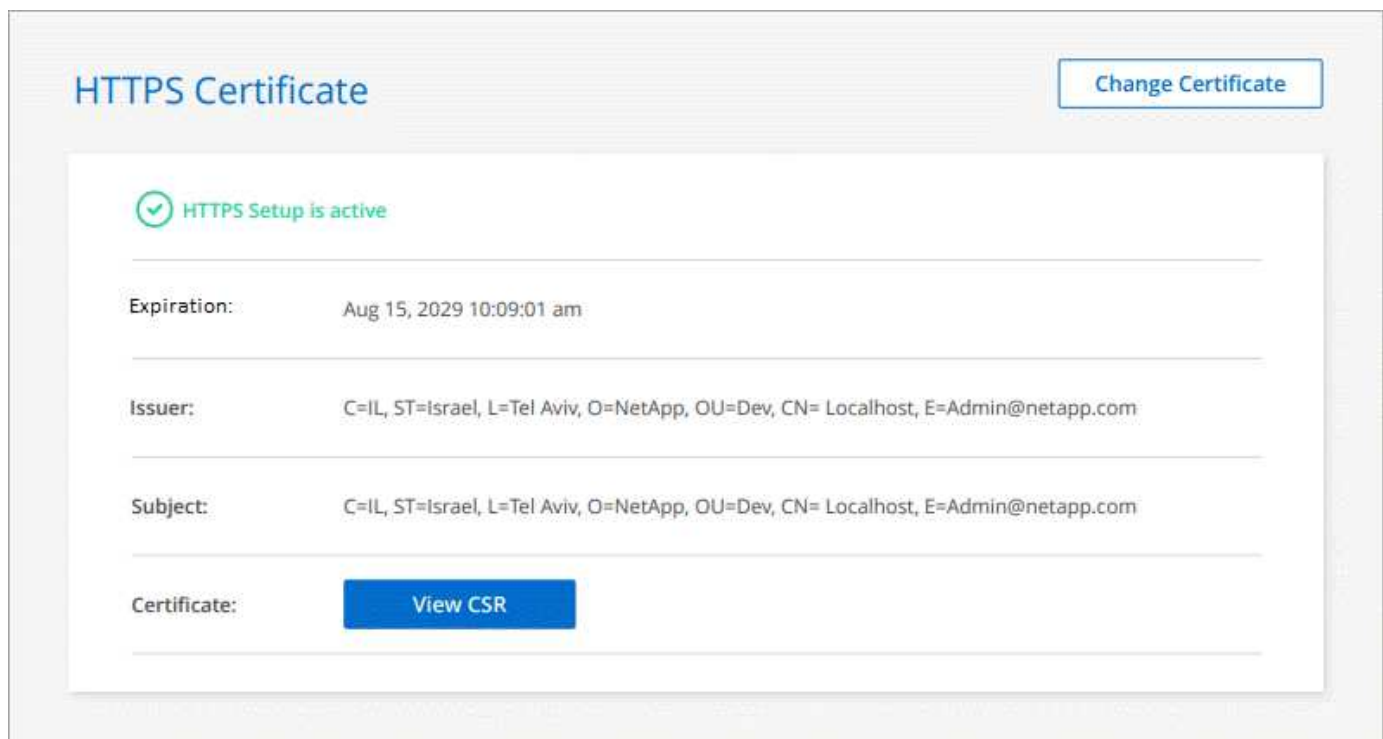
1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS-Setup**.



2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung (CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

| Option | Beschreibung |
|---|--|
| Erstellen Sie eine CSR | <p>a. Geben Sie den Hostnamen oder den DNS des Connector-Hosts (dessen allgemeiner Name) ein, und klicken Sie dann auf CSR erstellen.</p> <p>BlueXP zeigt eine Anfrage zum Signieren des Zertifikats an.</p> <p>b. Verwenden Sie die CSR, um eine SSL-Zertifikatsanforderung an eine Zertifizierungsstelle zu senden.</p> <p>Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.</p> <p>c. Laden Sie die Zertifikatsdatei hoch und klicken Sie dann auf Installieren.</p> |
| Installieren Sie Ihr eigenes CA-signiertes Zertifikat | <p>a. Wählen Sie CA-signiertes Zertifikat installieren.</p> <p>b. Laden Sie sowohl die Zertifikatsdatei als auch den privaten Schlüssel und klicken Sie dann auf Installieren.</p> <p>Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.</p> |

BlueXP verwendet jetzt das von der Zertifizierungsstelle signierte Zertifikat, um einen sicheren HTTPS-Zugriff zu ermöglichen. Die folgende Abbildung zeigt ein BlueXP-Konto, das für den sicheren Zugriff konfiguriert ist:



Erneuern des HTTPS-Zertifikats von BlueXP

Sie sollten das BlueXP HTTPS-Zertifikat erneuern, bevor es abläuft, um einen sicheren Zugriff auf die BlueXP-Konsole zu gewährleisten. Wenn Sie das Zertifikat nicht erneuern, bevor es abläuft, wird eine Warnung

angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS-Setup**.

Es werden Details zum BlueXP-Zertifikat angezeigt, einschließlich des Ablaufdatums.

2. Klicken Sie auf **Zertifikat ändern** und befolgen Sie die Schritte, um eine CSR zu erstellen oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

BlueXP verwendet das neue CA-signierte Zertifikat, um sicheren HTTPS-Zugriff bereitzustellen.

Konfigurieren eines Connectors für die Verwendung eines HTTP-Proxyservers

Wenn Sie in Ihren Unternehmensrichtlinien einen Proxyserver für die gesamte HTTP-Kommunikation mit dem Internet verwenden müssen, müssen Sie Ihre Connectors so konfigurieren, dass sie einen HTTP-Proxyserver verwenden. Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.



BlueXP unterstützt die Verwendung eines HTTPS-Proxys mit dem Connector nicht.

Die Konfiguration des Connectors zur Verwendung eines HTTP-Proxyservers bietet ausgehenden Internetzugriff, wenn keine öffentliche IP-Adresse oder ein NAT-Gateway verfügbar ist. Dieser Proxy-Server stellt nur den Connector mit einer ausgehenden Verbindung bereit. Es bietet keine Konnektivität für Cloud Volumes ONTAP Systeme.

Wenn Cloud Volumes ONTAP-Systeme keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten haben, konfiguriert BlueXP diese Cloud Volumes ONTAP-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. Sie müssen diesen Port öffnen, nachdem Sie den Connector bereitgestellt haben.

Aktivieren Sie einen Proxy auf einem Konnektor

Wenn Sie einen Connector so konfigurieren, dass er einen Proxy-Server verwendet, verwenden dieser Connector und die von ihm verwalteten Cloud Volumes ONTAP-Systeme (einschließlich aller HA-Mediatoren) den Proxy-Server.

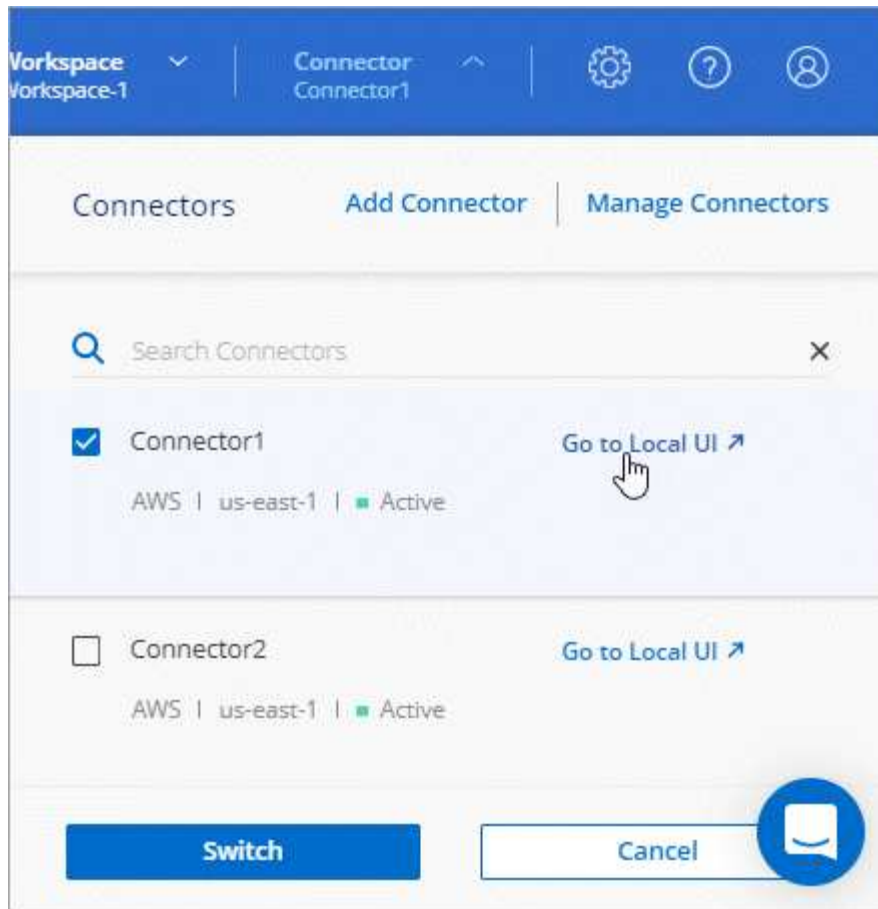
Beachten Sie, dass mit diesem Vorgang der Anschluss neu gestartet wird. Stellen Sie sicher, dass der Connector keine Operationen durchführt, bevor Sie fortfahren.

Schritte

1. "[Melden Sie sich bei der BlueXP SaaS-Schnittstelle an](#)" Von einem Computer mit einer Netzwerkverbindung zur Instanz des Connectors.

Wenn der Connector keine öffentliche IP-Adresse hat, benötigen Sie eine VPN-Verbindung oder Sie müssen eine Verbindung von einem Jump-Host herstellen, der sich im gleichen Netzwerk wie der Connector befindet.

2. Klicken Sie auf das Dropdown-Menü **Connector** und dann auf **zur lokalen Benutzeroberfläche** für einen bestimmten Konnektor.



Die BlueXP-Schnittstelle, die auf dem Connector ausgeführt wird, wird in einem neuen Browser-Tab geladen.

3. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Verbindungseinstellungen**.



4. Klicken Sie unter **Allgemein** auf **HTTP Proxy Configuration**.
5. Richten Sie den Proxy ein:
 - a. Klicken Sie Auf **Proxy Aktivieren**.
 - b. Geben Sie den Server mithilfe der Syntax an `http://address:port[]`
 - c. Geben Sie einen Benutzernamen und ein Kennwort an, wenn eine grundlegende Authentifizierung für den Server erforderlich ist
 - d. Klicken Sie Auf **Speichern**.



BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.

Aktivieren Sie direkten API-Verkehr

Wenn Sie einen Proxyserver konfiguriert haben, können Sie API-Anrufe direkt an BlueXP senden, ohne über den Proxy zu gehen. Diese Option wird mit Connectors unterstützt, die in AWS, in Azure oder in Google Cloud ausgeführt werden.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Verbindungseinstellungen**.



2. Klicken Sie unter **Allgemein** auf **direkte API-Traffic unterstützen**.
3. Klicken Sie auf das Kontrollkästchen, um die Option zu aktivieren, und klicken Sie dann auf **Speichern**.

Standardkonfiguration für den Konnektor

Möglicherweise möchten Sie mehr über den Connector erfahren, bevor Sie ihn bereitstellen, oder wenn Sie Probleme beheben müssen.

Standardkonfiguration mit Internetzugang

Die folgenden Konfigurationsdetails gelten, wenn Sie den Connector von BlueXP, vom Markt Ihres Cloud-Providers oder manuell auf einem lokalen Linux-Host mit Internetzugang installiert haben.

AWS – Details

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Der EC2-Instanztyp ist t3.xlarge.
- Das Betriebssystem für das Image ist Red hat Enterprise Linux 7.6 (HVM).

Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Der Benutzername für die EC2 Linux Instanz ist ec2-user.
- Die Standardfestplatte des Systems ist eine 100 gib gp2-Festplatte.

Azure – Details

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Der VM-Typ ist DS3 v2.
- Das Betriebssystem für das Image ist CentOS 7.6.

Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Standardfestplatte des Systems beträgt 100 gib Premium-SSD-Festplatte.

Google Cloud-Details

Wenn Sie den Connector von BlueXP oder vom Marktplatz des Cloud-Providers implementiert haben, beachten Sie Folgendes:

- Die VM-Instanz ist n2-Standard-4.
- Das Betriebssystem für das Image ist Red hat Enterprise Linux 8.6.

Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.

- Die Standardfestplatte des Systems beträgt eine persistente SSD-Festplatte mit 100 gib.

Installationsordner

Der Installationsordner des Connectors befindet sich an folgender Stelle:

`/opt/application/netapp/cloudmanager`

Log-Dateien

Protokolldateien sind in den folgenden Ordnern enthalten:

- `/opt/application/netapp/cloudmanager/log`

Die Protokolle in diesem Ordner enthalten Details zu den Konnektor- und Docker-Images.

- `/Opt/Application/netapp/CloudManager/docker_occm/Data/log`

Die Protokolle in diesem Ordner enthalten Details zu Cloud-Diensten und zum BlueXP-Dienst, der auf dem Connector ausgeführt wird.

Verbindungsdienst

- Der BlueXP-Dienst heißt occm.
- Der occm-Dienst ist vom MySQL-Dienst abhängig.

Wenn der MySQL-Dienst nicht verfügbar ist, ist auch der occm-Dienst nicht verfügbar.

Pakete

BlueXP installiert die folgenden Pakete auf dem Linux-Host, falls diese noch nicht installiert sind:

- 7-Zip
- AWSCLI
- Java
- Kubectl
- MySQL
- Tridnetctl

- Ziehen
- Wget

Ports

Der Connector verwendet die folgenden Ports auf dem Linux-Host:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff
- 3306 für die BlueXP-Datenbank
- 8080 für den BlueXP API Proxy
- 8666 für die Service Manager API
- 8777 für die Health-Checker Container Service API

Standardkonfiguration ohne Internetzugang

Die folgende Konfiguration gilt, wenn Sie den Connector manuell auf einem lokalen Linux-Host installiert haben, der keinen Internetzugang hat. ["Erfahren Sie mehr über diese Installationsoption"](#).

- Der Installationsordner des Connectors befindet sich an folgender Stelle:

`/Opt/Application/netapp/ds`

- Protokolldateien sind in den folgenden Ordnern enthalten:

`/Var/lib/docker/Volumes/ds_occmdata/data-data/log`

Die Protokolle in diesem Ordner enthalten Details zu den Konnektor- und Docker-Images.

- Alle Services werden in Docker Containern ausgeführt

Die Dienste sind abhängig vom laufenden Docker Runtime Service

- Der Connector verwendet die folgenden Ports auf dem Linux-Host:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff

PAYGO-Abonnements und -Verträge verwalten

Wenn Sie BlueXP über den Marktplatz eines Cloud-Providers abonnieren, werden Sie auf die BlueXP-Website weitergeleitet, auf der Sie Ihr Abonnement speichern und mit bestimmten Konten verknüpfen müssen. Nach dem Abonnement können Sie jedes Abonnement über Digital Wallet verwalten.

Ihre Abonnements anzeigen

Das Digital Wallet enthält Details zu jedem PAYGO-Abonnement und einem Jahresvertrag, der mit Ihrem BlueXP-Konto und mit Astra verbunden ist (Astra nutzt den BlueXP-Gebührendienst).

Schritte

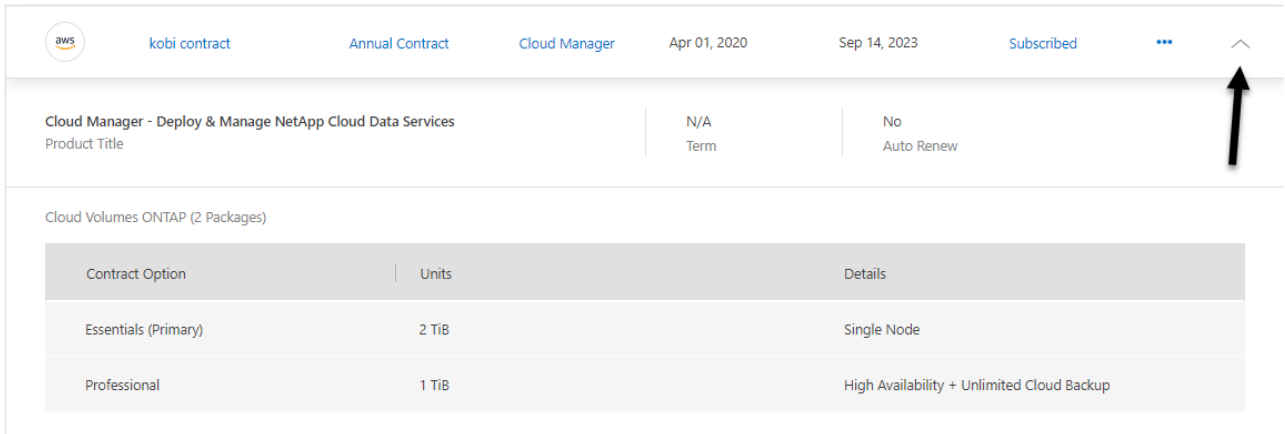
1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.

2. Wählen Sie **Abonnements**.

Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

3. Wenn Sie die Informationen zu Ihren Abonnements anzeigen, können Sie wie folgt mit den Details in der Tabelle interagieren:

- Erweitern Sie eine Zeile, um weitere Details anzuzeigen.



| Cloud Manager - Deploy & Manage NetApp Cloud Data Services | | |
|--|-------------|--|
| Product Title | N/A Term | No Auto Renew |
| Cloud Volumes ONTAP (2 Packages) | | |
| Contract Option | Units | Details |
| Essentials (Primary) | 2 TiB | Single Node |
| Professional | 1 TiB | High Availability + Unlimited Cloud Backup |

- Klicken Sie Auf  So legen Sie fest, welche Spalten in der Tabelle angezeigt werden sollen.

Beachten Sie, dass die Spalten „Begriff“ und „Automatische Verlängerung“ standardmäßig nicht angezeigt werden. In der Spalte „Automatische Erneuerung“ werden nur Informationen zur Verlängerung von Azure-Verträgen angezeigt.

Beachten Sie Folgendes zu den in der Tabelle aufgeführten Informationen:

Startdatum

Das Startdatum ist, wenn Sie das Abonnement erfolgreich mit Ihrem Konto verknüpft haben und der Ladevorgang gestartet wurde.

K. A.

Wenn in der Tabelle „N/A“ angezeigt wird, sind die Informationen derzeit nicht über die API des Cloud-Providers verfügbar.

Verträge

- Wenn Sie die Details für einen Vertrag erweitern, zeigt das Digital Wallet an, was für Ihren aktuellen Plan zur Verfügung steht: Die Vertragsoptionen und Einheiten (Kapazität oder Anzahl der Knoten).
- Das Digital Wallet identifiziert das Enddatum und gibt an, ob der Vertrag bald verlängert, bald beendet wird oder ob er bereits beendet ist.
- Wenn Sie über einen AWS-Vertrag verfügen und nach dem Startdatum eine der Optionen des Vertrags geändert haben, sollten Sie Ihre Vertragsoptionen von AWS validieren.

Verwalten Sie Ihre Abonnements

Sie können Ihre Abonnements über das Digital Wallet verwalten, indem Sie ein Abonnement umbenennen und

die Konten auswählen, die mit dem Abonnement verknüpft sind.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie **Abonnements**.
3. Klicken Sie in der Zeile auf das Aktionsmenü, das dem Abonnement entspricht, das Sie verwalten möchten.

| Provider | Name | Type | Service | Start Date | End Date | Status | |
|----------|-------------------------|-----------------|---------------|--------------|--------------|------------|---|
| aws | aws-sub-a2 | PAYGO | Cloud Manager | Apr 02, 2020 | N/A | Subscribed | ⋮ |
| aws | Aleksey_aws_marketplace | Annual Contract | Astra | Oct 18, 2022 | Oct 18, 2023 | | ⋮ |
| aws | By Capacity By Node 3 | PAYGO | Cloud Manager | Mar 31, 2020 | N/A | Subscribed | ⋮ |

4. Sie können das Abonnement umbenennen oder die NetApp Konten, die dem Abonnement zugeordnet sind, verwalten.

Cloud Storage erkannt

Anzeigen Ihrer Amazon S3 Buckets

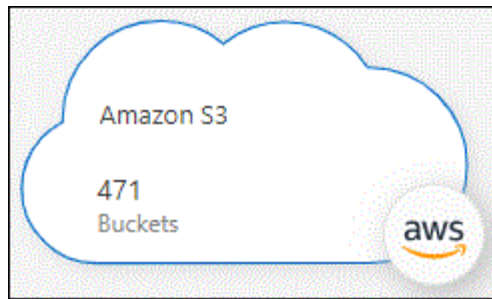
Nach der Installation eines Connectors in AWS erkennt BlueXP automatisch Informationen zu den Amazon S3 Buckets, die sich im AWS Konto befinden, in dem der Connector installiert ist. Eine Amazon S3-Arbeitsumgebung wird dem Canvas hinzugefügt, damit Sie diese Informationen anzeigen können.

Sie erhalten Details zu Ihren S3 Buckets, einschließlich Region, Zugriffsrichtlinien, Konto, Gesamt- und genutzter Kapazität, und mehr. Diese Buckets können als Ziele für Cloud-Backup, Cloud-Tiering oder Cloud Sync-Vorgänge verwendet werden. Zudem können Sie mit Cloud Data Sense diese Buckets scannen.

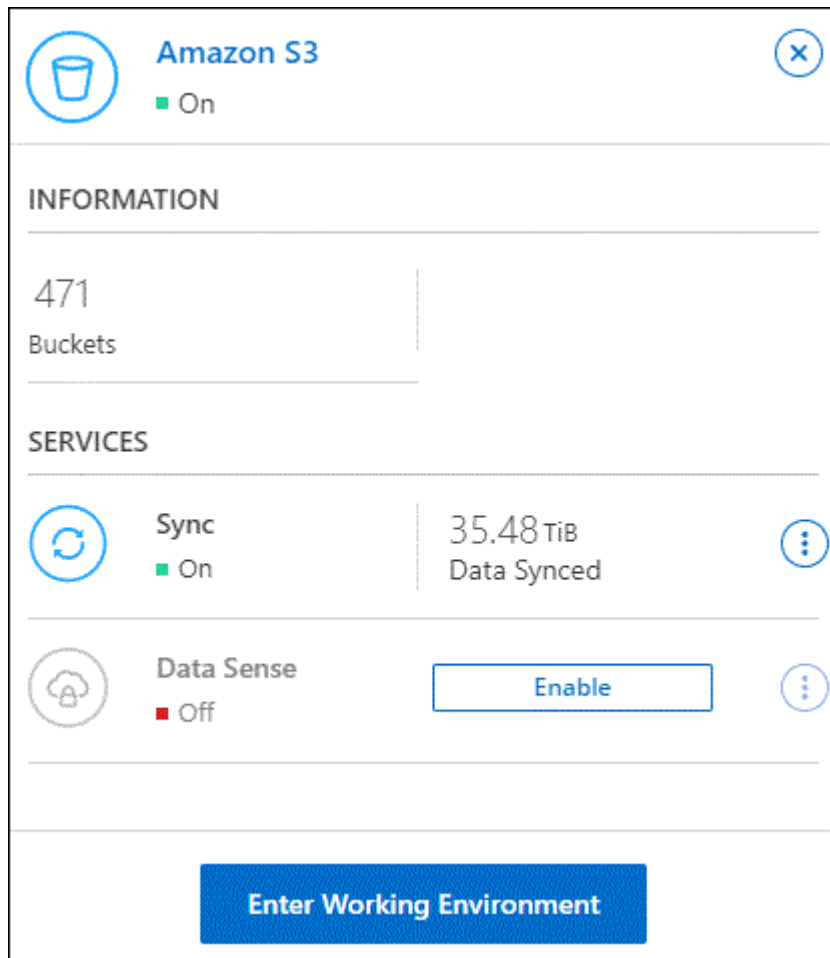
Schritte

1. **"Installieren Sie einen Anschluss"** In dem AWS Konto, wo Sie Ihre Amazon S3 Buckets anzeigen möchten.
2. Wählen Sie im Navigationsmenü die Option **Storage > Canvas** aus.

Sie sollten bald automatisch eine Amazon S3-Arbeitsumgebung sehen.



3. Klicken Sie auf die Arbeitsumgebung, und wählen Sie eine Aktion im rechten Fensterbereich aus.



4. Klicken Sie auf **Daten synchronisieren**, um Daten mit oder von S3 Buckets zu synchronisieren.

Weitere Informationen finden Sie unter ["Überblick über den Cloud Sync Service"](#).

5. Klicken Sie auf **Aktivieren**, wenn Cloud Data Sense die S3 Buckets nach persönlichen und sensiblen Daten scannen soll.

Weitere Informationen finden Sie unter ["Erste Schritte mit Cloud Data Sense für Amazon S3"](#).

6. Klicken Sie auf **Arbeitsumgebung eingeben**, um Details zu den S3-Buckets in Ihrem AWS-Konto anzuzeigen.

Amazon S3

Overview

471 Total Buckets | 6,94 TiB Total Capacity | 23 Total Regions

471 Buckets

| Bucket Name | AWS Account | Region | Creation Date | Encryption | Is Public | Size | Total Objects |
|--------------------------------|-------------|-----------------------|--------------------|------------|-------------------------------|-----------|---------------|
| athena-query-results-us-east-1 | 4642620614 | US East (N. Virginia) | September 27, 2021 | Disabled | Bucket and objects not public | 35.27 GiB | 3,01K |
| catalog-sg | 4642620614 | US East (N. Virginia) | October 1, 2021 | Disabled | Bucket and objects not public | 1.35 GiB | 1,44K |
| cbsqa | 4642620614 | US East (N. Virginia) | August 9, 2021 | Disabled | Public | 33.95 GiB | 185 |
| template-19-ap-southeast-3 | 4642620614 | ap-southeast-3 | March 10, 2022 | Enabled ⓘ | Objects can be public | 21.38 KiB | 3 |
| template-7dxc-ca-central-1 | 4642620614 | Canada (Central) | November 2, 2020 | Enabled ⓘ | Objects can be public | 24.01 KiB | 2 |

Anzeigen Ihrer Azure Blob Konten

Nach der Installation eines Connectors in Azure erkennt BlueXP automatisch Informationen zu den Azure Storage-Konten, die sich in den Azure-Abonnements befinden, in denen der Connector installiert ist. Eine Azure Blob Arbeitsumgebung wird dem Canvas hinzugefügt, damit Sie diese Informationen anzeigen können.

Sie sehen Details zu Ihren Azure Storage-Konten, einschließlich Standort, Ressourcengruppe, Gesamt- und genutzter Kapazität und mehr. Diese Konten können als Ziele für Cloud-Backup, Cloud-Tiering oder Cloud Sync-Vorgänge verwendet werden.

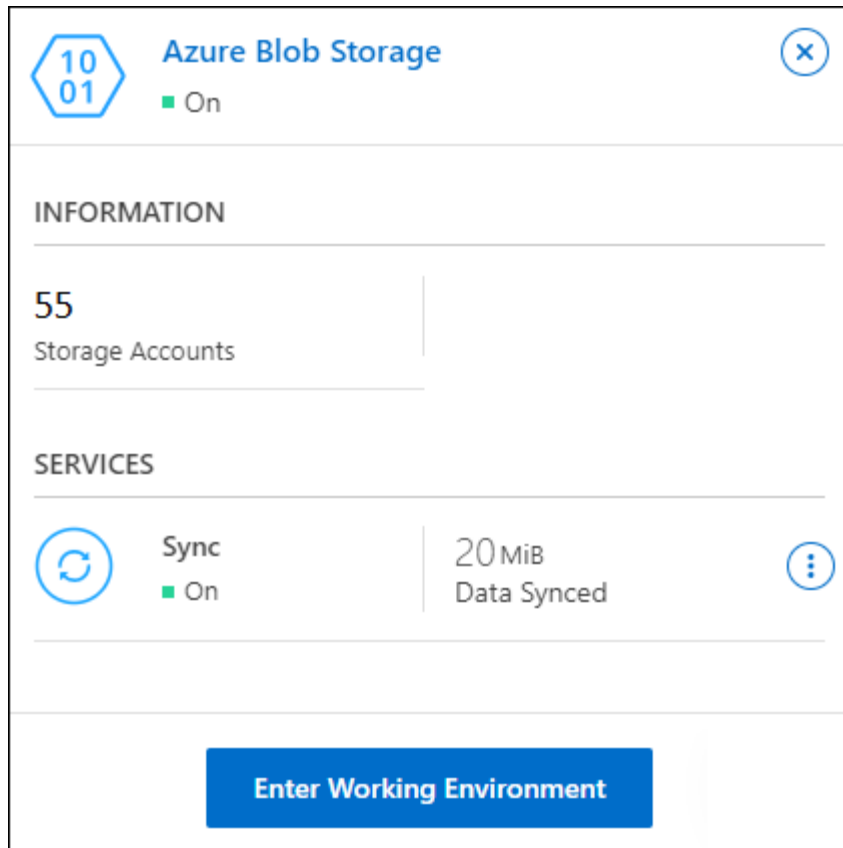
Schritte

1. "Installieren Sie einen Anschluss" Geben Sie im Azure-Konto Ihre Azure-Storage-Konten an.
2. Wählen Sie im Navigationsmenü die Option **Storage > Canvas** aus.

Kurz danach wird eine Azure Blob Arbeitsumgebung bereitgestellt.



3. Klicken Sie auf die Arbeitsumgebung, und wählen Sie eine Aktion im rechten Fensterbereich aus.



4. Klicken Sie auf **Synchronisierungsdaten**, um Daten mit oder von Azure Blob Storage zu synchronisieren.
Weitere Informationen finden Sie unter "[Überblick über den Cloud Sync Service](#)".
5. Klicken Sie auf **Enter Working Environment**, um Details zu den Azure Storage-Konten in Ihren Azure Blobs anzuzeigen.

Azure blob

Overview

637

Total Storage Accounts

1.5

TiB

Total Capacity

16

Total Locations

637

Storage Accounts

| Storage Account Name | Subscription | Location | Creation Date | Resource Group | Blob Capacity |
|----------------------|--------------|----------------|-------------------|----------------|---------------|
| ovu8llxvqdfypxn | OCCM QA1 | West US | June 24, 2021 | AdmAzureHa-rg | 170 B |
| rootsa9ktpjzcm | OCCM QA1 | West US | June 24, 2021 | AdmAzureHa-rg | 950.22 GiB |
| scvdwjcwehswli | OCCM QA1 | West US | June 24, 2021 | AdmAzureHa-rg | 22.12 MiB |
| 65qtx0smegmq2vt | OCCM QA1 | West US | June 24, 2021 | AdmAzureVsa-rg | 170 B |
| bu9klxthymr1be | OCCM QA1 | West US | June 24, 2021 | AdmAzureVsa-rg | 1.01 MiB |
| 8jzsvybvjiwieww8 | OCCM QA1 | Canada Central | December 12, 2019 | aff1-rg | 170 B |

Anzeigen Ihrer Google Cloud Storage Buckets

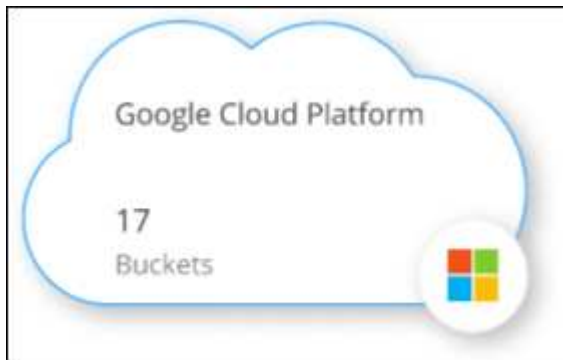
Nach der Installation eines Connectors in Google Cloud kann BlueXP automatisch Informationen über die Google Cloud Storage Buckets finden, die sich im Google-Konto befinden, in dem der Connector installiert ist. Eine Google Cloud Storage Arbeitsumgebung wird dem Canvas hinzugefügt, damit Sie diese Informationen anzeigen können.

Sie erhalten Details zu Ihren Google Cloud Storage Buckets, einschließlich Standort, Zugriffsstatus, Storage-Klasse, Gesamt- und genutzter Kapazität und mehr. Diese Buckets können als Ziele für Cloud-Backup, Cloud-Tiering oder Cloud Sync-Vorgänge verwendet werden.

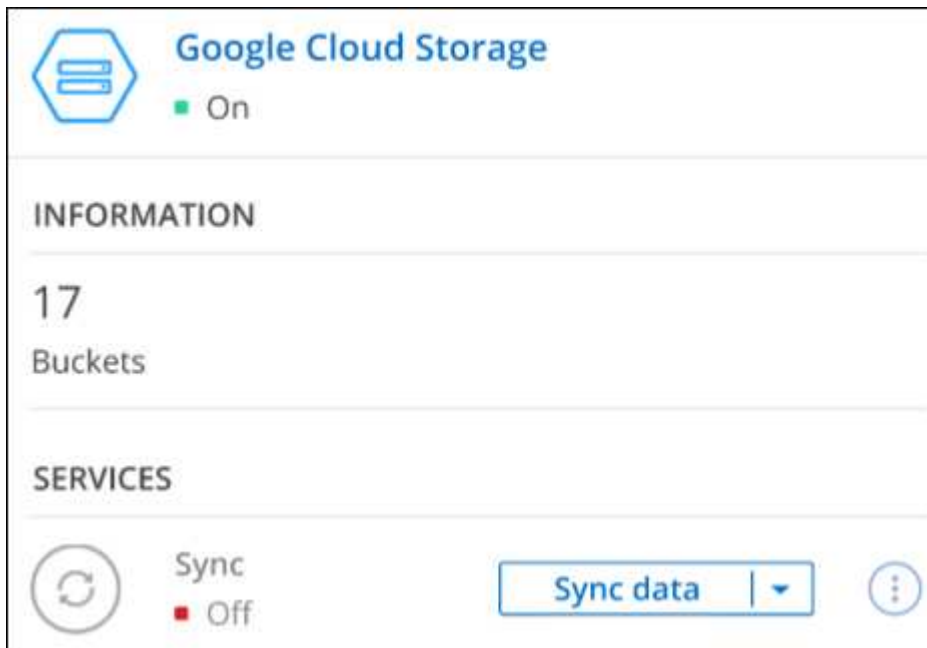
Schritte

1. ["Installieren Sie einen Anschluss"](#) In dem Google-Konto, in dem Sie Ihre Google Cloud Storage Buckets anzeigen möchten.
2. Wählen Sie im Navigationsmenü die Option **Storage > Canvas** aus.

Kurz darauf sollten Sie automatisch eine Google Cloud Storage Arbeitsumgebung sehen.



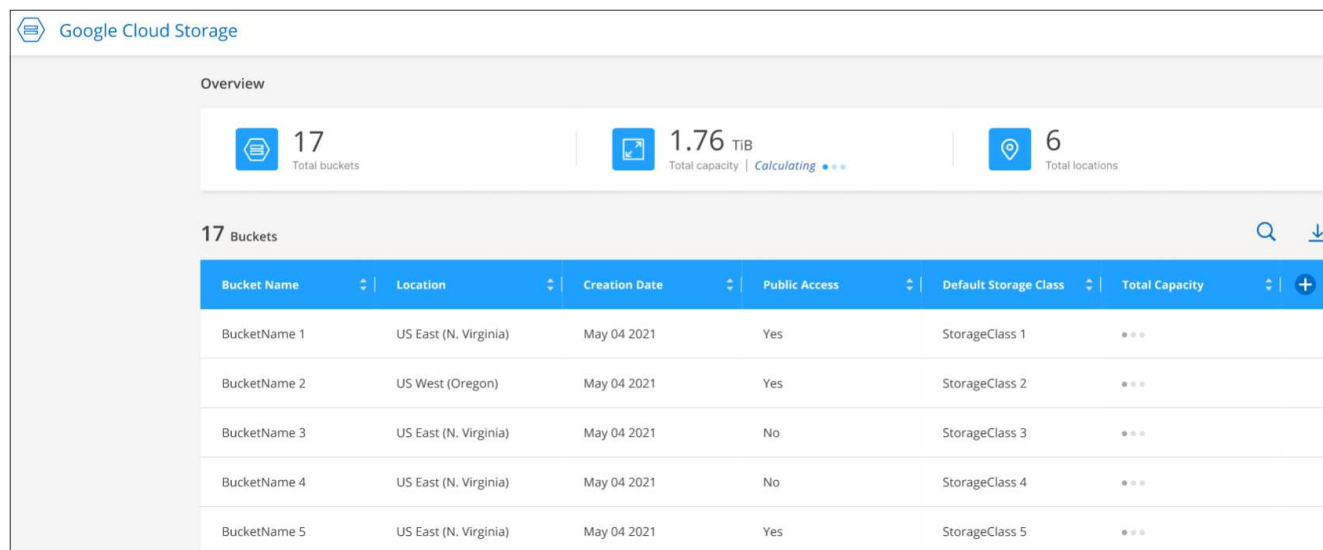
3. Klicken Sie auf die Arbeitsumgebung, und wählen Sie eine Aktion im rechten Fensterbereich aus.



4. Klicken Sie auf **Daten synchronisieren**, um Daten mit oder von Google Cloud Storage Buckets zu synchronisieren.

Weitere Informationen finden Sie unter ["Überblick über den Cloud Sync Service"](#).

5. Klicken Sie auf **Arbeitsumgebung eingeben**, um Details zu den Buckets in Ihrem Google-Konto anzuzeigen.



The screenshot shows the Google Cloud Storage Overview page. At the top, there are three summary cards: '17 Total buckets', '1.76 TiB Total capacity | Calculating', and '6 Total locations'. Below these, a table lists 17 buckets. The table has columns for Bucket Name, Location, Creation Date, Public Access, Default Storage Class, and Total Capacity. The first five rows are visible, showing buckets named BucketName 1 through 5, all created on May 04 2021, with various locations and public access settings.

| Bucket Name | Location | Creation Date | Public Access | Default Storage Class | Total Capacity |
|--------------|-----------------------|---------------|---------------|-----------------------|----------------|
| BucketName 1 | US East (N. Virginia) | May 04 2021 | Yes | StorageClass 1 | ... |
| BucketName 2 | US West (Oregon) | May 04 2021 | Yes | StorageClass 2 | ... |
| BucketName 3 | US East (N. Virginia) | May 04 2021 | No | StorageClass 3 | ... |
| BucketName 4 | US East (N. Virginia) | May 04 2021 | No | StorageClass 4 | ... |
| BucketName 5 | US East (N. Virginia) | May 04 2021 | Yes | StorageClass 5 | ... |

AWS Zugangsdaten

AWS Zugangsdaten und Berechtigungen

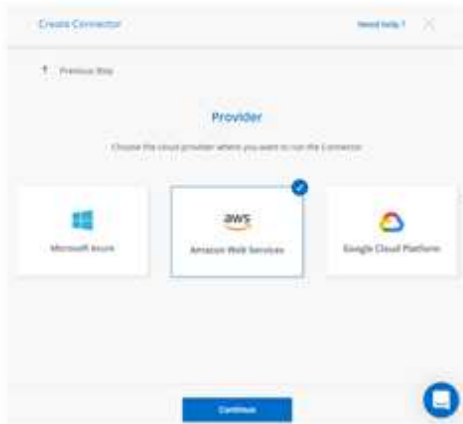
Mit BlueXP können Sie die AWS Zugangsdaten für die Bereitstellung von Cloud Volumes ONTAP auswählen. Alle Cloud Volumes ONTAP Systeme können über die ersten AWS Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

Erste AWS Zugangsdaten

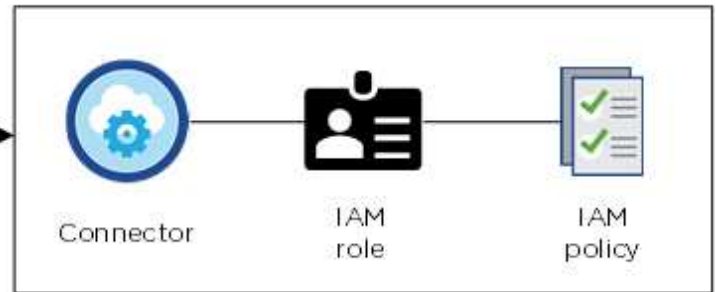
Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie das ARN einer IAM-Rolle oder Zugriffsschlüssel für einen IAM-Benutzer bereitstellen. Die verwendete Authentifizierungsmethode muss über die erforderlichen Berechtigungen für die Bereitstellung der Connector-Instanz in AWS verfügen. Die erforderlichen Berechtigungen werden im aufgeführt ["Connector-Implementierungsrichtlinie für AWS"](#).

Wenn BlueXP die Connector-Instanz in AWS startet, erstellt sie eine IAM-Rolle und ein Instanzprofil für die Instanz. Zudem wird eine Richtlinie angehängt, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. ["Überprüfen Sie, wie BlueXP die Berechtigungen verwendet"](#).

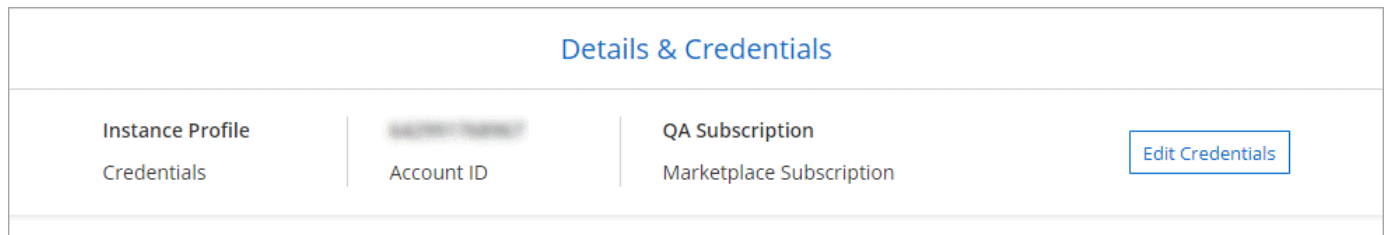
Cloud Manager



AWS account



BlueXP wählt die AWS Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:

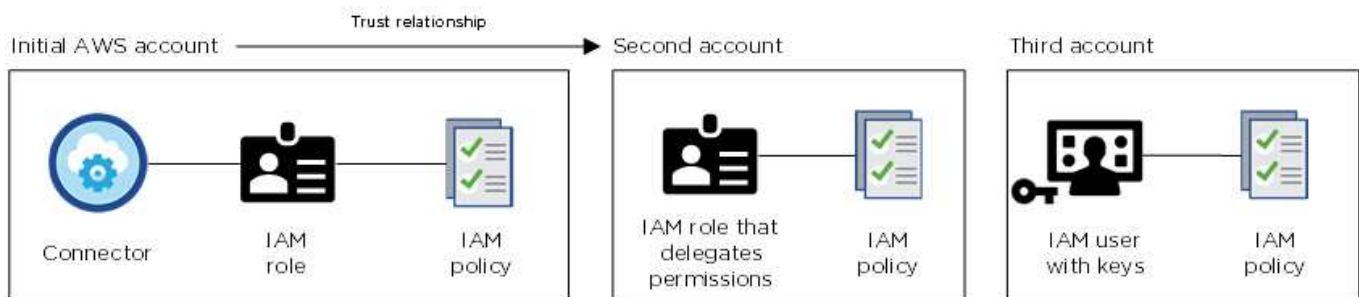


Zusätzliche AWS Zugangsdaten

Es gibt zwei Möglichkeiten, zusätzliche AWS Zugangsdaten hinzuzufügen.

Fügen Sie AWS Zugangsdaten zu einem vorhandenen Connector hinzu

Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Accounts starten möchten, haben Sie eine der Möglichkeiten ["AWS Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen"](#). Die folgende Abbildung zeigt zwei zusätzliche Konten: Eines mit Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto und ein weiteres über die AWS Schlüssel eines IAM-Benutzers:



Das würden Sie dann tun ["Fügen Sie die Kontoanmeldeinformationen zu BlueXP hinzu"](#) Indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Nachdem Sie einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

Fügen Sie AWS Zugangsdaten direkt in BlueXP hinzu

Beim Hinzufügen neuer AWS Zugangsdaten zu BlueXP stehen die erforderlichen Berechtigungen zum Erstellen und Managen einer FSX für ONTAP Arbeitsumgebung oder zum Erstellen eines Connectors zur Verfügung.

Wie sieht es mit Marketplace-Implementierungen und On-Premises-Implementierungen aus?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Connector beschrieben, der aus BlueXP stammt. Sie können auch einen Connector in AWS von der bereitstellen ["AWS Marketplace"](#) Und das können Sie auch ["Installieren Sie den Steckverbinder vor Ort"](#).

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Bei On-Premises-Implementierungen können Sie keine IAM-Rolle für das BlueXP-System einrichten, Sie können aber auch Berechtigungen wie bei zusätzlichen AWS-Konten bereitstellen.

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Wie oben beschrieben, können Sie mit BlueXP auf verschiedene Weise AWS Zugangsdaten bereitstellen: Eine mit der Konnektor-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel.

Bei den ersten beiden Optionen verwendet BlueXP den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dies ist die Best Practice, also automatisch und sicher.

Wenn Sie BlueXP mit AWS-Zugriffsschlüsseln zur Verfügung stellen, sollten Sie die Schlüssel durch Aktualisierung in BlueXP in einem regelmäßigen Intervall drehen. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Managen Sie AWS Anmeldeinformationen und Abonnements für BlueXP

Fügen Sie AWS Anmeldedaten hinzu und managen Sie diese, damit BlueXP über die erforderlichen Berechtigungen verfügt, um Cloud-Ressourcen in Ihren AWS-Konten bereitzustellen und zu managen. Wenn Sie mehrere AWS-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen AWS Zugangsdaten zuweisen.

Überblick

AWS Zugangsdaten können zu einem vorhandenen Connector oder direkt zu BlueXP hinzugefügt werden:

- Fügen Sie einem vorhandenen Connector zusätzliche AWS Zugangsdaten hinzu

Wenn Sie einem vorhandenen Connector AWS Zugangsdaten hinzufügen, erhalten Sie die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen in Ihrer Public-Cloud-Umgebung. [credentials to a Connector](#), Erfahren Sie, wie Sie AWS Zugangsdaten zu einem Connector hinzufügen.

- Fügen Sie zur Erstellung eines Connectors AWS Credentials zu BlueXP hinzu

Wenn Sie BlueXP neue AWS-Anmeldeinformationen hinzufügen, erhalten Sie mit BlueXP die erforderlichen Berechtigungen zum Erstellen eines Connectors. [credentials to BlueXP for creating a Connector](#), Erfahren Sie, wie Sie AWS Zugangsdaten zu BlueXP hinzufügen.

- Fügen Sie AWS Credentials zu BlueXP für FSX für ONTAP hinzu

Wenn Sie BlueXP neue AWS Zugangsdaten hinzufügen, erhalten Sie unter BlueXP die erforderlichen Berechtigungen zum Erstellen und Managen von FSX für ONTAP. ["Erfahren Sie, wie Sie Berechtigungen für FSX für ONTAP einrichten"](#)

So drehen Sie die Anmeldeinformationen

Mit BlueXP können Sie AWS Zugangsdaten auf verschiedene Arten bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel. ["Weitere Informationen zu AWS Zugangsdaten und Berechtigungen"](#).

Bei den ersten beiden Optionen verwendet BlueXP den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dieser Prozess ist die Best Practice, da er automatisch und sicher ist.

Wenn Sie BlueXP mit AWS-Zugriffsschlüsseln zur Verfügung stellen, sollten Sie die Schlüssel durch Aktualisierung in BlueXP in einem regelmäßigen Intervall drehen. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Anmeldedaten zu einem Konnektor hinzufügen

Fügen Sie AWS Zugangsdaten zu einem Connector hinzu, damit die IT auch über die erforderlichen Berechtigungen zum Management von Ressourcen und Prozessen in Ihrer Public Cloud-Umgebung verfügt. Sie können entweder den ARN einer IAM-Rolle in einem anderen Konto bereitstellen oder AWS-Zugriffsschlüssel bereitstellen.

Berechtigungen erteilen

Bevor Sie AWS Zugangsdaten zu einem Connector hinzufügen, müssen Sie die erforderlichen Berechtigungen bereitstellen. Mithilfe der Berechtigungen kann BlueXP Ressourcen und Prozesse innerhalb dieses AWS Kontos verwalten. Wie Sie die Berechtigungen bereitstellen, hängt davon ab, ob Sie BlueXP mit dem ARN einer Rolle in einem vertrauenswürdigen Konto oder AWS Schlüsseln bereitstellen möchten.



Wenn Sie einen Connector von BlueXP bereitgestellt haben, hat BlueXP automatisch AWS-Anmeldeinformationen für das Konto hinzugefügt, in dem Sie den Connector bereitgestellt haben. Dieses Erstkonto wird nicht hinzugefügt, wenn Sie den Connector über den AWS Marketplace bereitgestellt haben oder wenn Sie die Connector-Software manuell auf einem vorhandenen System installieren. "[Weitere Informationen zu AWS Zugangsdaten und Berechtigungen](#)".

Auswahl

- permissions by assuming an IAM role in another account
- permissions by providing AWS keys

Erteilen Sie Berechtigungen, indem Sie eine IAM-Rolle in einem anderen Konto übernehmen

Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Connector-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie BlueXP über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

Schritte

1. Rufen Sie die IAM-Konsole im Zielkonto auf, in dem Sie dem Connector Berechtigungen erteilen möchten.
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 Kontos ein, auf dem sich die Connector-Instanz befindet.
 - Erstellen Sie die erforderlichen Richtlinien, indem Sie den Inhalt von kopieren und einfügen "[Die IAM-Richtlinien für den Connector](#)".
3. Kopieren Sie die Rolle ARN der IAM-Rolle, damit Sie sie später in BlueXP einfügen können.

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können die Anmeldeinformationen jetzt einem Connector hinzufügen.

Erteilen Sie Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Wenn Sie BlueXP für einen IAM-Benutzer AWS-Schlüssel bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die BlueXP IAM-Richtlinie definiert die AWS Aktionen und Ressourcen, die BlueXP verwenden darf.

Schritte

1. Erstellen Sie Richtlinien von der IAM-Konsole aus, indem Sie die Inhalte von kopieren und einfügen "[Die IAM-Richtlinien für den Connector](#)".

"AWS Dokumentation: Erstellung von IAM-Richtlinien"

2. Hängen Sie die Richtlinien an eine IAM-Rolle oder einen IAM-Benutzer an.

- ["AWS Documentation: Erstellung von IAM-Rollen"](#)
- ["AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"](#)

Das Konto verfügt nun über die erforderlichen Berechtigungen. ,Sie können die Anmeldeinformationen jetzt einem Connector hinzufügen.

Fügen Sie die Anmeldeinformationen hinzu

Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie die Anmeldedaten für dieses Konto einem bestehenden Connector hinzufügen. Damit können Sie Cloud Volumes ONTAP-Systeme in diesem Konto mit demselben Connector starten.

Falls Sie diese Zugangsdaten gerade bei Ihrem Cloud-Provider 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. Stellen Sie sicher, dass derzeit in BlueXP der richtige Connector ausgewählt ist.
2. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



3. Klicken Sie auf **Anmeldeinformationen hinzufügen** und befolgen Sie die Schritte im Assistenten.
 - a. **Anmeldeort:** Wählen Sie **Amazon Web Services > Connector**.
 - b. **Identifizierungsdaten definieren:** Geben Sie den ARN (Amazon Resource Name) einer vertrauenswürdigen IAM-Rolle an, oder 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.

Damit Cloud Volumes ONTAP mit stündlichem Tarif (PAYGO) oder mit einem Jahresvertrag bezahlt werden kann, müssen AWS Zugangsdaten über den AWS Marketplace mit einem Abonnement für Cloud Volumes ONTAP verknüpft werden.

- d. **Review:** Bestätigen Sie die Angaben zu den neuen Anmeldedaten und klicken Sie auf **Hinzufügen**.

Sie können jetzt bei der Erstellung einer neuen Arbeitsumgebung auf eine andere Gruppe von Anmeldeinformationen von der Seite Details und Anmeldeinformationen wechseln:

Edit Credentials & Add Subscription

Associate Subscription to Credentials ?

Credentials

keys | Account ID:

Instance Profile | Account ID:

casaba QA subscription

+ Add Subscription

Apply

Cancel

Fügen Sie für die Erstellung eines Connectors Anmeldeinformationen zu BlueXP hinzu

Fügen Sie BlueXP die AWS Zugangsdaten hinzu, indem Sie das ARN einer IAM-Rolle bereitstellen, die BlueXP die zur Erstellung eines Connectors erforderlichen Berechtigungen erteilt. Sie können diese Anmeldeinformationen beim Erstellen eines neuen Connectors auswählen.

Einrichten der IAM-Rolle

Richten Sie eine IAM-Rolle ein, mit der BlueXP SaaS die Rolle übernehmen kann.

Schritte

1. Wechseln Sie im Zielkonto zur 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** und geben Sie die ID des BlueXP SaaS: 952013314444 ein
- Erstellen Sie eine Richtlinie, die die zum Erstellen eines Connectors erforderlichen Berechtigungen enthält.
 - ["Zeigen Sie die für FSX für ONTAP erforderlichen Berechtigungen an"](#)
 - ["Sehen Sie sich die Richtlinie zur Bereitstellung von Konnektor an"](#)

3. Kopieren Sie die Rolle ARN der IAM-Rolle, sodass Sie sie im nächsten Schritt in BlueXP einfügen können.

Die IAM-Rolle verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu BlueXP hinzufügen.

Fügen Sie die Anmeldeinformationen hinzu

Nachdem Sie die IAM-Rolle mit den erforderlichen Berechtigungen angegeben haben, fügen Sie die Rolle ARN zu BlueXP hinzu.

Wenn Sie gerade die IAM-Rolle 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 in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und befolgen Sie die Schritte im Assistenten.
 - a. **Anmeldeort:** Wählen Sie **Amazon Web Services > BlueXP**.
 - b. **Anmeldedaten definieren:** Geben Sie den ARN (Amazon Resource Name) der IAM-Rolle an.
 - c. **Review:** Bestätigen Sie die Angaben zu den neuen Anmeldedaten und klicken Sie auf **Hinzufügen**.

Sie können die Anmeldeinformationen jetzt beim Erstellen eines neuen Connectors verwenden.

AWS Abonnement zuordnen

Nachdem Sie Ihre AWS Zugangsdaten zu BlueXP hinzugefügt haben, können Sie ein AWS Marketplace Abonnement mit diesen Anmeldedaten verknüpfen. Mit dem Abonnement können Sie Cloud Volumes ONTAP auf Stundenbasis (PAYGO) oder bei Nutzung eines Jahresvertrags bezahlen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement verknüpfen können, nachdem Sie BlueXP bereits die Zugangsdaten hinzugefügt haben:

- Sie haben ein Abonnement nicht zugeordnet, wenn Sie die Anmeldeinformationen zu BlueXP hinzugefügt haben.
- Sie möchten ein vorhandenes AWS Marketplace Abonnement durch ein neues Abonnement ersetzen.

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. ["Erfahren Sie, wie Sie einen Konnektor erstellen"](#).

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für eine Reihe von Anmeldeinformationen und wählen Sie dann **Abonnement verknüpfen**.



3. Wählen Sie ein vorhandenes Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

► https://docs.netapp.com/de-de/cloud-manager-setup-admin//media/video_subscribing_aws.mp4 (video)

Anmeldedaten bearbeiten

Bearbeiten Sie Ihre AWS Zugangsdaten in BlueXP, indem Sie den Kontotyp (AWS Schlüssel oder ANGEEN Rolle) ändern, indem Sie den Namen bearbeiten oder die Anmeldeinformationen selbst aktualisieren (die Schlüssel oder die Rolle ARN).



Sie können die Anmeldeinformationen für ein Instanzprofil, das einer Connector-Instanz zugeordnet ist, nicht bearbeiten.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für eine Reihe von Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die gewünschten Änderungen vor und klicken Sie dann auf **Anwenden**.

Anmeldedaten werden gelöscht

Wenn Sie keine Anmeldedaten mehr benötigen, können Sie diese aus BlueXP löschen. Sie können nur Anmeldeinformationen löschen, die nicht mit einer Arbeitsumgebung verknüpft sind.



Sie können die Anmeldeinformationen für ein Instanzprofil nicht löschen, das einer Konnektor-Instanz zugeordnet ist.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für einen Satz von Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen löschen**.
3. Klicken Sie zur Bestätigung auf **Löschen**.

Azure Zugangsdaten

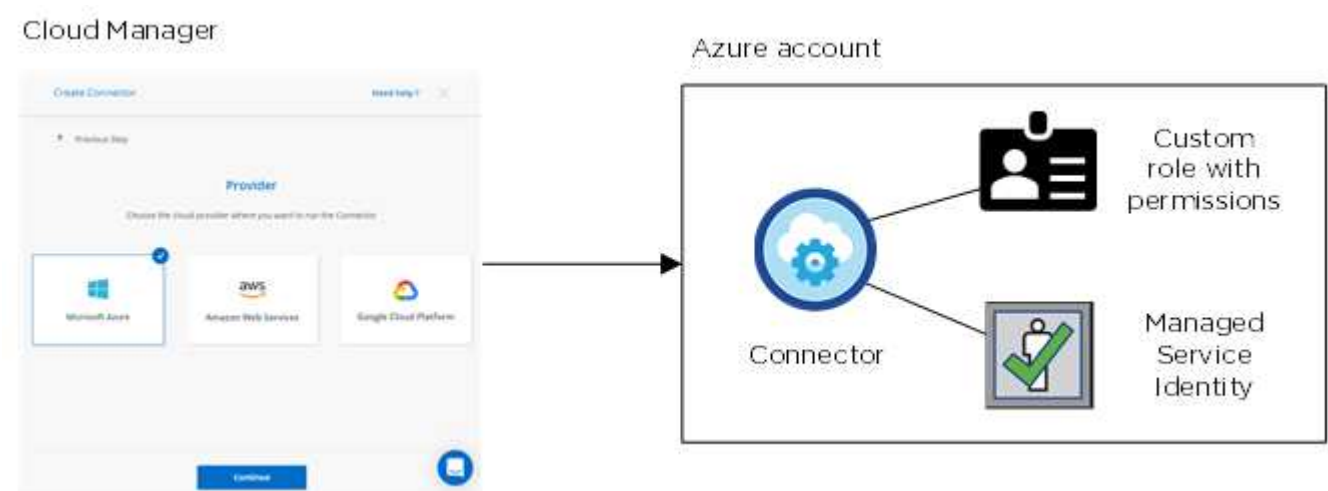
Azure Zugangsdaten und Berechtigungen

Mit BlueXP können Sie die für die Bereitstellung von Cloud Volumes ONTAP verwendeten Azure Zugangsdaten auswählen. Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

Erste Azure Zugangsdaten

Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie ein Azure-Konto oder einen Service-Principal verwenden, der über die Berechtigungen zum Bereitstellen der virtuellen Connector-Maschine verfügt. Die erforderlichen Berechtigungen werden im aufgeführt ["Connector-Implementierungsrichtlinie für Azure"](#).

Wenn BlueXP die Connector Virtual Machine in Azure implementiert, wird damit ein aktiviert ["Vom System zugewiesene verwaltete Identität"](#) Erstellt auf einer virtuellen Maschine eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Diese Rolle bietet BlueXP die Berechtigungen, die für das Management von Ressourcen und Prozessen innerhalb des Azure Abonnements erforderlich sind. ["Überprüfen Sie, wie BlueXP die Berechtigungen verwendet"](#).



Bei der Erstellung einer neuen Arbeitsumgebung für Cloud Volumes ONTAP wählt BlueXP die folgenden Azure-Anmeldedaten standardmäßig aus:

| Details & Credentials | | | |
|------------------------|--------------------|--|----------------------------------|
| Managed Service Ide... | OCCM QA1 | ⓘ No subscription is associated | Edit Credentials |
| Credential Name | Azure Subscription | Marketplace Subscription | |

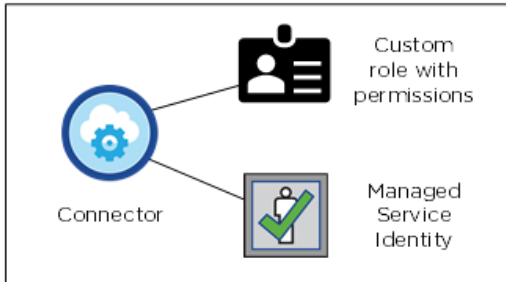
Zusätzliche Azure-Abonnements für eine gemanagte Identität

Die verwaltete Identität ist mit dem Abonnement verbunden, in dem Sie den Connector gestartet haben. Wenn Sie ein anderes Azure Abonnement auswählen möchten, müssen Sie es ausführen ["Verknüpfen Sie die verwaltete Identität mit diesen Abonnements"](#).

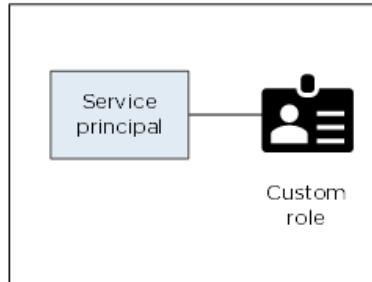
Zusätzliche Azure Zugangsdaten

Wenn Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten implementieren möchten, müssen Sie die erforderlichen Berechtigungen von erteilen "[Erstellen und Einrichten eines Service Principal in Azure Active Directory](#)" Für jedes Azure Konto. Das folgende Bild zeigt zwei zusätzliche Konten, die jeweils mit einer Dienstprinzipal- und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:

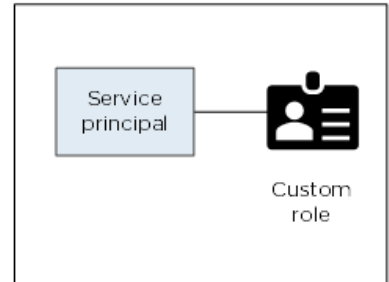
Initial Azure account



Second account



Third account



Das würden Sie dann tun "[Fügen Sie die Kontoanmeldeinformationen zu BlueXP hinzu](#)" Durch Angabe von Details zum AD-Dienstprinzipal.

Nachdem Sie einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:

The screenshot shows a dialog titled "Edit Account & Add Subscription". Under the "Credentials" section, there is a text input field with a dropdown menu. The dropdown menu is open, showing three options: "cloud-manager-app | Application ID: 57c42424-88a0-480a.", "Managed Service Identity" (which is highlighted in blue), and "OCCM QA1 (Default)".

Wie sieht es mit Marketplace-Implementierungen und On-Premises-Implementierungen aus?

In den obigen Abschnitten wird die empfohlene Bereitstellungsmethode für den Connector beschrieben, der aus BlueXP stammt. Sie können auch einen Connector in Azure über die bereitstellen "[Azure Marketplace](#)", Und Sie können "[Installieren Sie den Steckverbinder vor Ort](#)".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die verwaltete Identität für den Connector manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Für On-Premises-Bereitstellungen können Sie keine verwaltete Identität für den Connector einrichten, aber Sie können Berechtigungen wie bei zusätzlichen Konten mit einem Service-Principal bereitstellen.

Verwalten von Azure-Anmeldeinformationen und -Abonnements für BlueXP

Wenn Sie ein Cloud Volumes ONTAP-System erstellen, müssen Sie die Azure-Anmeldedaten auswählen, die mit diesem System verwendet werden sollen. Sie müssen auch ein Marketplace-Abonnement wählen, wenn Sie Pay-as-you-go-Lizenzen verwenden. Folgen Sie den Schritten auf dieser Seite, wenn Sie mehrere Azure Zugangsdaten oder mehrere Azure Marketplace Abonnements für Cloud Volumes ONTAP verwenden möchten.

Es gibt zwei Möglichkeiten, in BlueXP zusätzliche Azure-Abonnements und Anmeldedaten hinzuzufügen.

1. Verknüpfen Sie zusätzliche Azure-Abonnements mit der von Azure verwalteten Identität.
2. Wenn Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten bereitstellen möchten, erteilen Sie Azure Berechtigungen unter Verwendung eines Service-Principal und fügen dessen Zugangsdaten BlueXP hinzu.

Verknüpfen weiterer Azure-Abonnements mit einer gemanagten Identität

Mit BlueXP können Sie die Azure Zugangsdaten und das Azure Abonnement auswählen, in dem Sie Cloud Volumes ONTAP bereitstellen möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "[Verwaltete Identität](#)" Mit diesen Abonnements.

Eine verwaltete Identität ist "[Zunächst das Azure-Konto](#)" Wenn Sie einen Connector von BlueXP bereitstellen. Wenn Sie den Connector bereitgestellt haben, hat BlueXP die Rolle BlueXP Operator erstellt und der virtuellen Connector-Maschine zugewiesen.

Schritte

1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Klicken Sie auf **Access Control (IAM)**.
 - a. Klicken Sie auf **Hinzufügen > Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
 - Wählen Sie die Rolle **BlueXP Operator** aus.



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

- Weisen Sie einer **virtuellen Maschine** Zugriff zu.
- Wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde.
- Wählen Sie die virtuelle Verbindungsmaschine aus.
- Klicken Sie Auf **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Wenn Sie eine neue Arbeitsumgebung erstellen, sollten Sie nun über mehrere Azure-Abonnements für das verwaltete Identitätsprofil verfügen.

Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

Hinzufügen zusätzlicher Azure Zugangsdaten zu BlueXP

Wenn Sie einen Connector von BlueXP bereitstellen, aktiviert BlueXP eine vom System zugewiesene verwaltete Identität auf der virtuellen Maschine, die über die erforderlichen Berechtigungen verfügt. BlueXP wählt diese Azure-Anmeldedaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen.



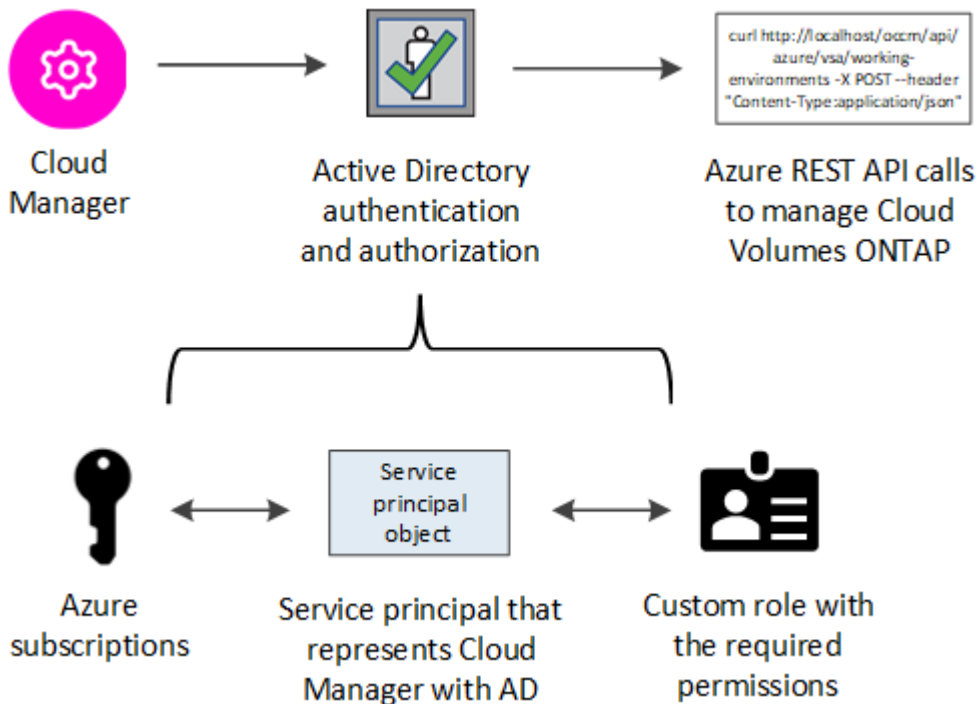
Ein erster Satz von Anmeldeinformationen wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. ["Informationen zu Azure Zugangsdaten und Berechtigungen"](#).

Wenn Sie Cloud Volumes ONTAP mit *different* Azure Zugangsdaten bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen erteilen, indem Sie für jedes Azure Konto einen Service-Principal in Azure Active Directory erstellen und einrichten. Anschließend können Sie die neuen Anmeldeinformationen zu BlueXP hinzufügen.

Azure-Berechtigungen über einen Service-Principal gewähren

Für Aktionen in Azure benötigt BlueXP Berechtigungen. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Service-Principal in Azure Active Directory erstellen und einrichten, sowie die für BlueXP erforderlichen Azure Zugangsdaten erhalten.

Die folgende Abbildung zeigt, wie BlueXP Berechtigungen zur Durchführung von Operationen in Azure erhält. Ein Service-Principal-Objekt, das an ein oder mehrere Azure-Abonnements gebunden ist, repräsentiert BlueXP in Azure Active Directory und wird einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen zulässt.



Schritte

1. an Azure Active Directory application, Erstellen Sie eine Azure Active Directory-Anwendung.
2. the application to a role, Anwendung einer Rolle zuweisen.
3. Windows Azure Service Management API permissions, Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.
4. the application ID and directory ID, Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.
5. a client secret, Erstellen Sie einen Clientschlüssel.

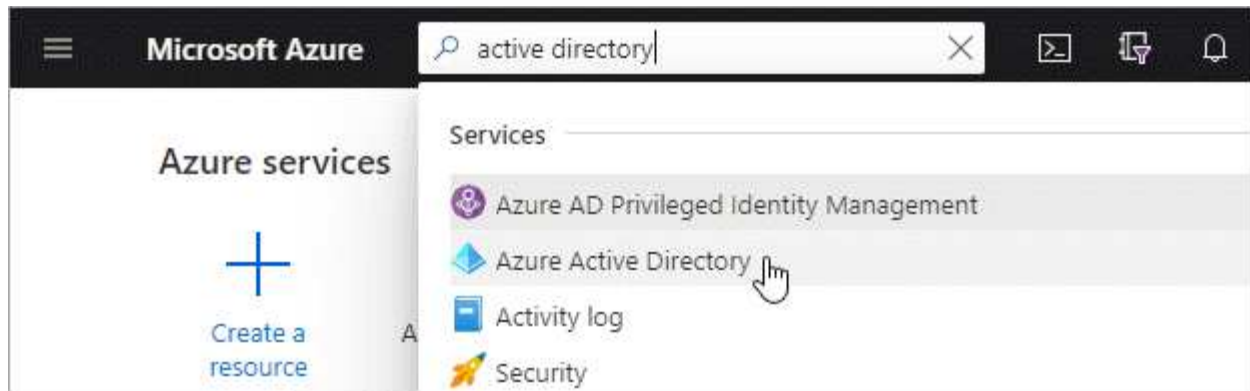
Erstellen einer Azure Active Directory-Anwendung

Erstellen Sie eine Applikation und einen Service-Principal für Azure Active Directory (AD), die BlueXP für die rollenbasierte Zugriffssteuerung verwenden kann.

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**.

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

Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „BlueXP Operator“ zuweisen, damit BlueXP über Berechtigungen in Azure verfügt.

Schritte

1. Erstellen einer benutzerdefinierten Rolle:
 - 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.

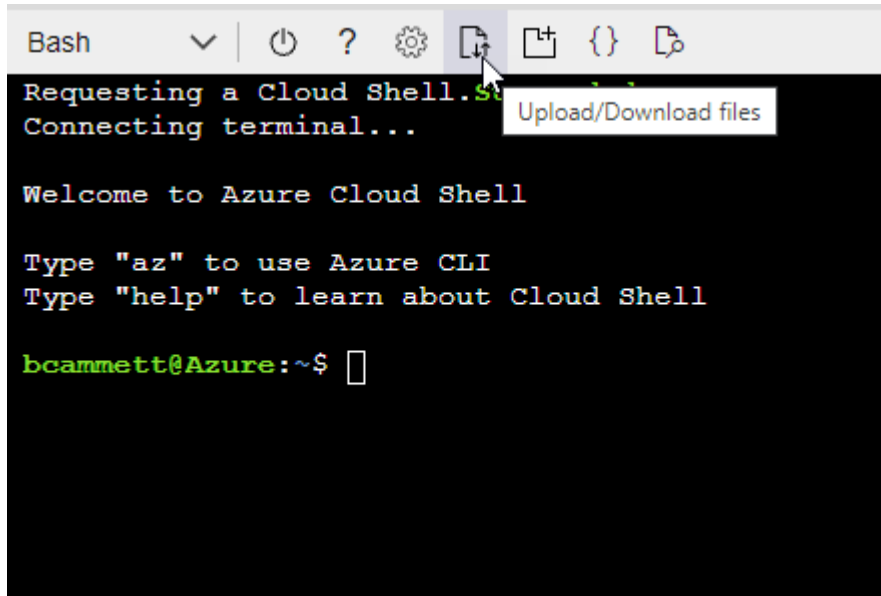
Beispiel

```
"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.



- Geben Sie den folgenden Befehl der Azure CLI ein:

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

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

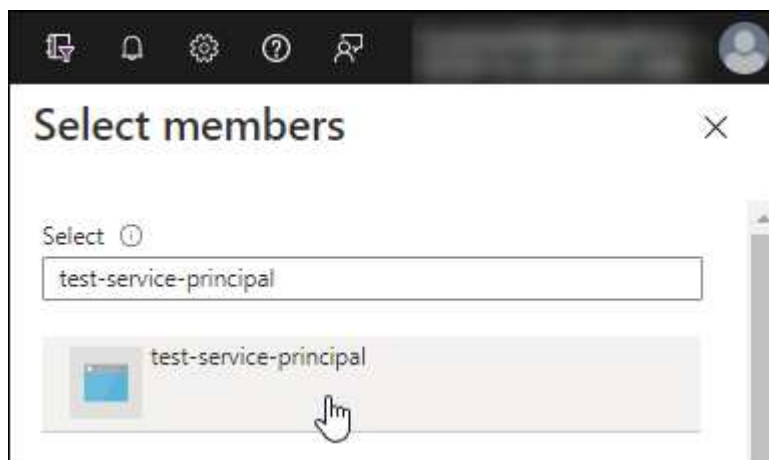
2. Applikation der Rolle zuweisen:

- Öffnen Sie im Azure-Portal den Service **Abonnements**.
- Wählen Sie das Abonnement aus.
- Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- Wählen Sie auf der Registerkarte * Role* die Rolle **BlueXP Operator** aus und klicken Sie auf **Next**.
- 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**.

f. Klicken Sie auf **Review + Assign**.

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.

Windows Azure Service Management-API-Berechtigungen werden hinzugefügt

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

| | | |
|---|--|---|
| <p>Microsoft Graph</p> <p>Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.</p>  | | |
| <p> Azure Batch</p> <p>Schedule large-scale parallel and HPC applications in the cloud</p> | <p> Azure Data Catalog</p> <p>Programmatic access to Data Catalog resources to register, annotate and search data assets</p> | <p> Azure Data Explorer</p> <p>Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p> |
| <p> Azure Data Lake</p> <p>Access to storage and compute for big data analytic scenarios</p> | <p> Azure DevOps</p> <p>Integrate with Azure DevOps and Azure DevOps server</p> | <p> Azure Import/Export</p> <p>Programmatic control of import/export jobs</p> |
| <p> Azure Key Vault</p> <p>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p> | <p> Azure Rights Management Services</p> <p>Allow validated users to read and write protected content</p> | <p> Azure Service Management</p> <p>Programmatic access to much of the functionality available through the Azure portal</p> |
| <p> Azure Storage</p> <p>Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p> | <p> Customer Insights</p> <p>Create profile and interaction models for your products</p> | <p> Data Export Service for Microsoft Dynamics 365</p> <p>Export data from Microsoft Dynamics CRM organization to an external destination</p> |

4. 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](#)

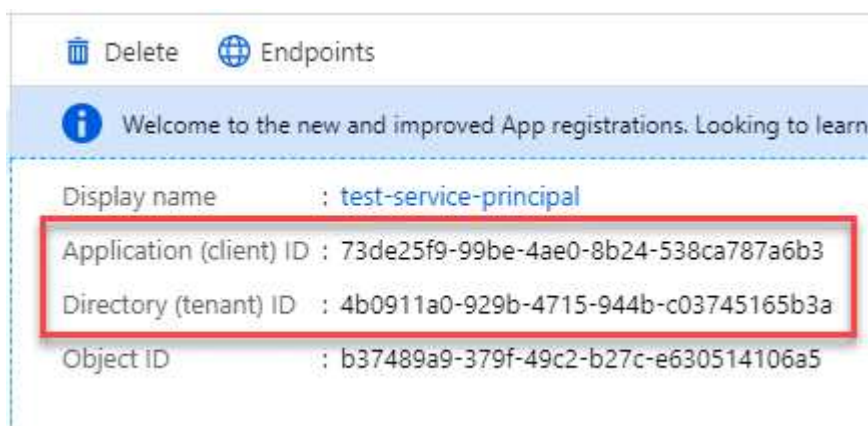
| Type to search | |
|--|------------------------|
| PERMISSION | ADMIN CONSENT REQUIRED |
| <input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) | - |

Abrufen der Anwendungs-ID und der Verzeichnis-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.

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 eines Clientgeheimnisses

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.

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

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.

Hinzufügen der Anmeldeinformationen zu BlueXP

Nachdem Sie ein Azure-Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie die Anmeldedaten für dieses Konto bei BlueXP hinzufügen. Durch diesen Schritt können Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten starten.

Falls Sie diese Zugangsdaten gerade bei Ihrem Cloud-Provider erstellt haben, kann es einige Minuten dauern, bis sie zur Verwendung verfügbar sind. Warten Sie einige Minuten, bevor Sie BlueXP die Anmeldeinformationen hinzufügen.

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. ["Erfahren Sie, wie"](#).

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.

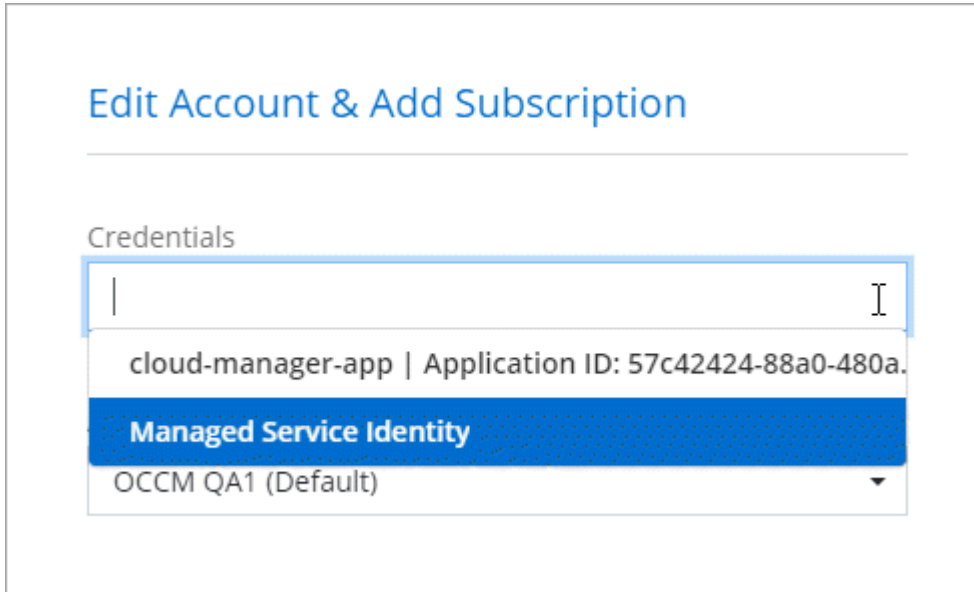


2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und befolgen Sie die Schritte im Assistenten.
 - a. **Anmeldeort:** Wählen Sie **Microsoft Azure > Connector**.
 - b. **Anmeldedaten definieren:** Geben Sie Informationen über den Azure Active Directory Service Principal ein, der die erforderlichen Berechtigungen erteilt:
 - Anwendungs-ID (Client): Siehe the application ID and directory ID.
 - Verzeichnis-ID (Mandant): Siehe the application ID and directory ID.
 - Client Secret: Siehe a client secret.
 - c. **Marketplace-Abonnement:** Verknüpfen Sie diese Anmeldedaten mit einem Marketplace-Abonnement, indem Sie jetzt abonnieren oder ein vorhandenes Abonnement auswählen.

Damit Sie für Cloud Volumes ONTAP mit einem stündlichen Tarif (PAYGO) bezahlen können, müssen diese Azure Zugangsdaten einem Abonnement im Azure Marketplace zugeordnet sein.

d. **Review**: Bestätigen Sie die Angaben zu den neuen Anmeldedaten und klicken Sie auf **Hinzufügen**.

Auf der Seite Details und Anmeldeinformationen können Sie nun zu verschiedenen Anmeldeinformationen wechseln "[Beim Erstellen einer neuen Arbeitsumgebung](#)"



Edit Account & Add Subscription

Credentials

cloud-manager-app | Application ID: 57c42424-88a0-480a.

Managed Service Identity

OCCM QA1 (Default)

Vorhandene Anmeldedaten verwalten

Verwalten Sie die Azure-Anmeldedaten, die Sie BlueXP bereits hinzugefügt haben, indem Sie ein Marketplace-Abonnement zuordnen, Anmeldedaten bearbeiten und löschen.

Verknüpfen eines Azure Marketplace Abonnements mit den Zugangsdaten

Nachdem Sie Ihre Azure Zugangsdaten zu BlueXP hinzugefügt haben, können Sie diesen Anmeldedaten ein Azure Marketplace Abonnement zuordnen. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement verknüpfen können, nachdem Sie BlueXP bereits die Zugangsdaten hinzugefügt haben:

- Sie haben ein Abonnement nicht zugeordnet, wenn Sie die Anmeldeinformationen zu BlueXP hinzugefügt haben.
- Sie möchten ein vorhandenes Azure Marketplace Abonnement durch ein neues Abonnement ersetzen.

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "[Erfahren Sie, wie](#)".

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für eine Reihe von Anmeldeinformationen und wählen Sie dann **Abonnement verknüpfen**.



3. Wählen Sie ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

Das folgende Video beginnt im Kontext des Assistenten zur Arbeitsumgebung, zeigt Ihnen aber den gleichen Workflow, nachdem Sie auf **Abonnement hinzufügen** geklickt haben:

► https://docs.netapp.com/de-de/cloud-manager-setup-admin//media/video_subscribing_azure.mp4

(video)

Anmeldedaten werden bearbeitet

Bearbeiten Sie Ihre Azure-Anmeldedaten in BlueXP, indem Sie die Details zu Ihren Azure-Serviceanmeldeinformationen ändern. Sie müssen beispielsweise den Clientschlüssel aktualisieren, wenn ein neues Geheimnis für die Service-Hauptanwendung erstellt wurde.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für eine Reihe von Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen bearbeiten**.
3. Nehmen Sie die gewünschten Änderungen vor und klicken Sie dann auf **Anwenden**.

Anmeldedaten werden gelöscht

Wenn Sie keine Anmeldedaten mehr benötigen, können Sie diese aus BlueXP löschen. Sie können nur Anmeldeinformationen löschen, die nicht mit einer Arbeitsumgebung verknüpft sind.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für einen Satz von Anmeldeinformationen und wählen Sie dann **Anmeldeinformationen löschen**.
3. Klicken Sie zur Bestätigung auf **Löschen**.

Google Cloud-Anmeldedaten

Google Cloud Projekte, Berechtigungen und Konten

Ein Servicekonto bietet BlueXP Berechtigungen zum Bereitstellen und Verwalten von Cloud Volumes ONTAP-Systemen, die sich im selben Projekt wie der Connector befinden, oder in verschiedenen Projekten.

Projekt und Berechtigungen für BlueXP

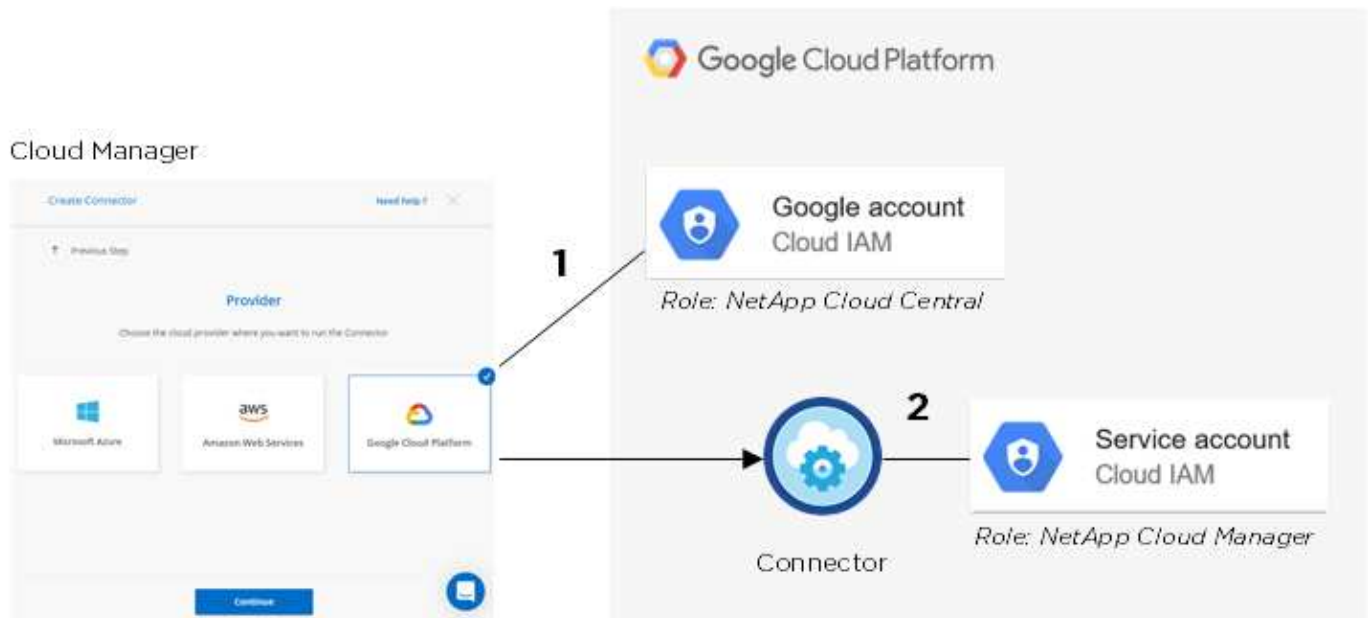
Bevor Sie Cloud Volumes ONTAP in Google Cloud bereitstellen können, müssen Sie zunächst einen Connector in einem Google Cloud-Projekt bereitstellen. Der Connector kann nicht vor Ort oder bei einem anderen Cloud-Provider ausgeführt werden.

Zwei Berechtigungsgruppen müssen vorhanden sein, bevor Sie einen Connector direkt von BlueXP bereitstellen:

1. Sie müssen einen Connector mit einem Google-Konto bereitstellen, das über Berechtigungen zum Starten der Connector VM-Instanz von BlueXP verfügt.
2. Bei der Bereitstellung des Connectors werden Sie aufgefordert, ein auszuwählen **"Servicekonto"** Für die VM-Instanz. BlueXP erhält über das Servicekonto Berechtigungen zum Erstellen und Verwalten von Cloud Volumes ONTAP-Systemen in Ihrem Auftrag. Berechtigungen werden durch Hinzufügen einer benutzerdefinierten Rolle an das Servicekonto bereitgestellt.

Wir haben zwei YAML-Dateien eingerichtet, die die erforderlichen Berechtigungen für den Benutzer und das Dienstkonto enthalten. ["Erfahren Sie, wie Sie mit den YAML-Dateien Berechtigungen einrichten"](#).

Das folgende Bild zeigt die in den Nummern 1 und 2 oben beschriebenen Berechtigungsanforderungen:



Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann im selben Projekt wie der Connector oder in einem anderen Projekt residieren. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zunächst das Connector-Servicekonto und die Rolle zu diesem Projekt hinzufügen.

- ["Erfahren Sie, wie Sie ein Servicekonto einrichten"](#)
- ["Erfahren Sie, wie Cloud Volumes ONTAP in GCP implementiert und ein Projekt ausgewählt wird"](#)

Verwalten von Google Cloud-Anmeldeinformationen und -Abonnements für BlueXP

Sie können die Anmeldeinformationen verwalten, die der Connector-VM-Instanz zugeordnet sind.

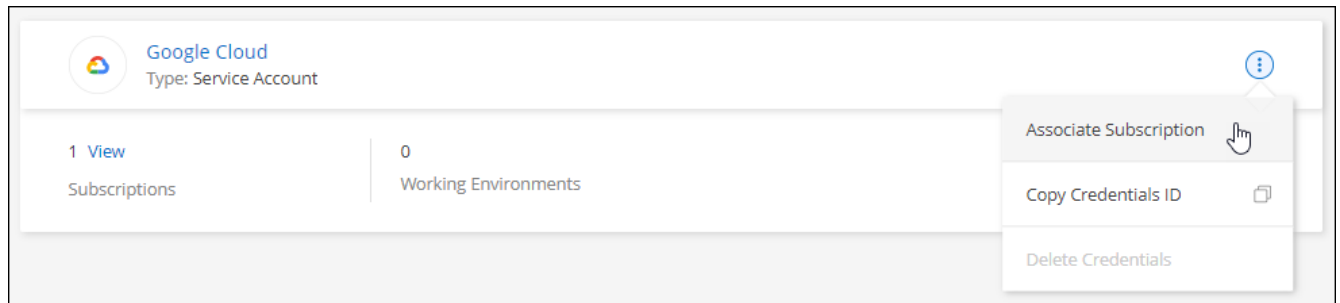
Verknüpfen eines Marketplace-Abonnements mit GCP-Zugangsdaten

Wenn Sie einen Connector in GCP bereitstellen, erstellt BlueXP einen Standardsatz von Anmeldeinformationen, die der Connector-VM-Instanz zugeordnet sind. Dies sind die Anmeldeinformationen, die BlueXP zur Bereitstellung von Cloud Volumes ONTAP verwendet.

Sie können das Marketplace-Abonnement jederzeit ändern, das mit diesen Anmeldedaten verknüpft ist. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Klicken Sie auf das Aktionsmenü für eine Reihe von Anmeldeinformationen und wählen Sie dann **Abonnement verknüpfen**.





3. Wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus.

Google Cloud Project

OCCM-Dev

Subscription

 GCP subscription for staging

 [Add Subscription](#)

4. Klicken Sie Auf **Mitarbeiter**.

5. Wenn Sie noch kein Abonnement haben, klicken Sie auf **Abonnement hinzufügen** und führen Sie die folgenden Schritte aus, um ein neues Abonnement zu erstellen.



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

6. Führen Sie die Schritte des Abonnements durch und klicken Sie auf **Weiter**.

Add Subscription


Subscription Steps:


- 1 **Cloud Manager**
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
 - 2 **Google Cloud Marketplace**
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
 - 3 **Cloud Central**
Save your subscription.
 - 4 **Cloud Manager**
Associate the Marketplace subscription with your Google Cloud project.
-  View video instructions

Continue

Cancel

7. Nachdem Sie auf die umgeleitet wurden "[Seite zu NetApp BlueXP im Google Cloud Marketplace](#)", Stellen Sie sicher, dass das richtige Projekt im oberen Navigationsmenü ausgewählt ist.


Google Cloud Platform
My First Project



Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

SUBSCRIBE

OVERVIEW
PRICING
SUPPORT

Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. Klicken Sie Auf **Abonnieren**.

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

2. Purchase details

Select a billing account *

Secondary_Billing_Account

3. Terms

Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

Additional terms

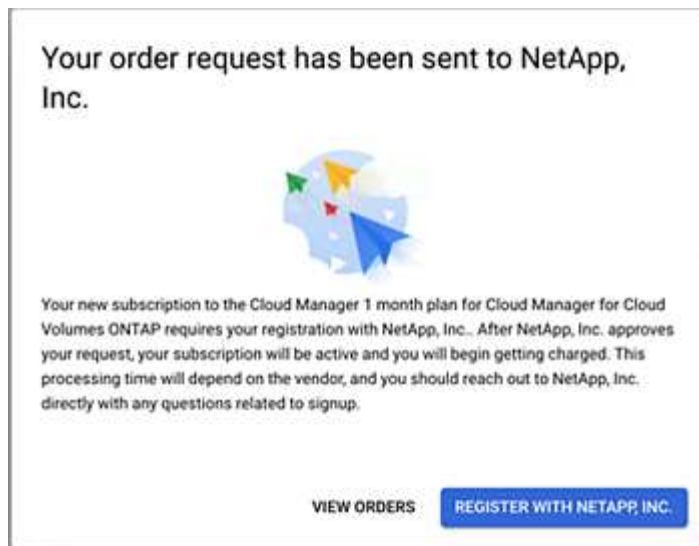
- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ⓘ
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. Klicken Sie Auf **Abonnieren**.

Dieser Schritt sendet Ihre Transferanfrage an NetApp.

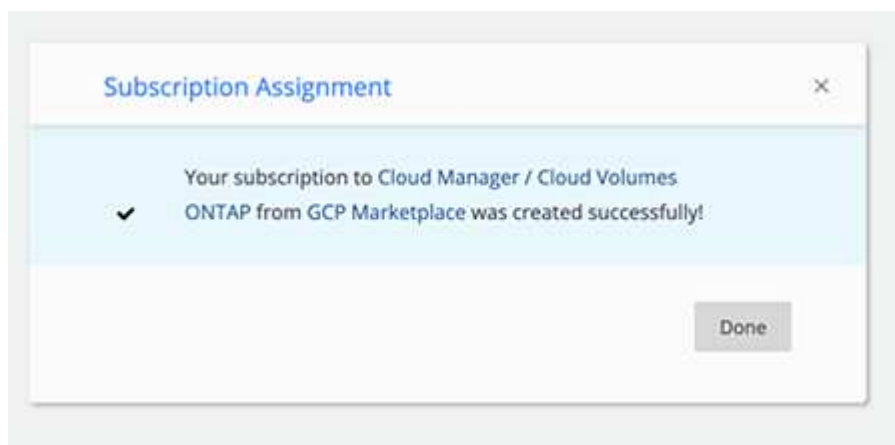
11. Klicken Sie im Popup-Dialogfeld auf **mit NetApp registrieren, Inc.**, um zur NetApp BlueXP Website umgeleitet zu werden.



Mit diesem Schritt müssen Sie das GCP-Abonnement mit Ihrem NetApp Konto verknüpfen. Der Vorgang der Verknüpfung eines Abonnements ist erst abgeschlossen, wenn Sie von dieser Seite umgeleitet und dann bei BlueXP angemeldet sind.

12. Nachdem Sie zu BlueXP umgeleitet wurden, melden Sie sich an oder registrieren Sie sich, und klicken Sie dann auf **Fertig**, um fortzufahren.

Das GCP-Abonnement ist mit allen NetApp Konten verknüpft, mit denen Ihre Benutzeranmeldung verknüpft ist.



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

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

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

+ Add Subscription

Fehlerbehebung beim Marketplace-Abonnementprozess

Manchmal kann das Abonnieren von Cloud Volumes ONTAP über den Google Cloud Marketplace fragmentiert werden aufgrund falscher Berechtigungen oder versehentlich nicht nach der Umleitung zur BlueXP-Website. Wenn dies geschieht, führen Sie die folgenden Schritte aus, um den Abonnementprozess abzuschließen.

Schritte

1. Navigieren Sie zum ["Seite zu NetApp BlueXP im Google Cloud Marketplace"](#) Um den Status der Bestellung zu überprüfen. Wenn auf der Seite **auf Anbieter verwalten** steht, scrollen Sie nach unten und klicken Sie auf **Bestellungen verwalten**.

Pricing

The product was purchased on 12/9/20.

MANAGE ORDERS

- a. Wenn der Auftrag ein grünes Häkchen anzeigt und dies unerwartet ist, kann bereits ein anderer Mitarbeiter des Unternehmens, der dasselbe Rechnungskonto verwendet, abonniert werden. Wenn das unerwartete vorbereitet ist oder wenn Sie die Details zu diesem Abonnement benötigen, wenden Sie sich an Ihr NetApp Vertriebsteam.

| Filter Enter property name or value | | | | | | | | | | |
|-------------------------------------|--------------|---------------|----------|--------------|---------------|----------|------------------|------------|-----------|--|
| Status | Order number | Plan | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan | |
| | 2eebbc... | Cloud Manager | - | 10/21/21 | 1 month | - | Postpay | N/A | N/A | |

- b. Wenn der Auftrag einen Clock- und **Ausstehend**-Status anzeigt, gehen Sie zurück zur Marktplatzseite und wählen Sie **auf Anbieter verwalten**, um den Prozess wie oben beschrieben abzuschließen.

| Filter Enter property name or value | | | | | | | | | | |
|-------------------------------------|--------------|---------------|----------|--------------|---------------|----------|------------------|------------|-----------|--|
| Status | Order number | Plan | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan | |
| | d56c66... | Cloud Manager | - | Pending | 1 month | Pending | Postpay | N/A | N/A | |

Fügen Sie Konten der NetApp Support Site in BlueXP hinzu und managen Sie sie

Bereitstellen von Zugangsdaten für Ihre NetApp Support Site (NSS) Accounts zur Registrierung für Support, zum Aktivieren wichtiger Workflows für Cloud Volumes ONTAP usw.

Überblick

Wenn Sie Ihr Konto auf der NetApp Support Site zu BlueXP hinzufügen, müssen Sie die folgenden Aufgaben aktivieren:

- Um sich für den Support zu registrieren
- Cloud Volumes ONTAP bei Nutzung einer eigenen Lizenz (BYOL)

Die Bereitstellung Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für den von Ihnen erworbenen Zeitraum aktivieren kann. Dies schließt automatische Updates für Vertragsverlängerungen ein.

- Um Pay-as-you-go Cloud Volumes ONTAP Systeme zu registrieren

Die Bereitstellung Ihres NSS Kontos ist erforderlich, um Support für Ihr System zu aktivieren und Zugang zu den technischen Support-Ressourcen von NetApp zu erhalten.

- Um ein Upgrade der Cloud Volumes ONTAP Software auf die neueste Version durchzuführen

Sie müssen außerdem Ihre NSS-Zugangsdaten eingeben, um Digital Advisor (ehemals Active IQ) aus BlueXP zu verwenden. Diese Anmeldedaten sind direkt mit Ihrem Benutzerkonto verknüpft und dürfen nur mit Digital Advisor verwendet werden. Lesen Sie im folgenden Abschnitt weitere Einzelheiten.

Verwalten eines NSS-Kontos im Zusammenhang mit Digital Advisor

Wenn Sie in BlueXP auf Digital Advisor zugreifen, werden Sie aufgefordert, sich bei Digital Advisor anzumelden, indem Sie Ihre NSS-Anmeldedaten eingeben. Nachdem Sie Ihre NSS-Anmeldedaten eingegeben haben, wird das NSS-Konto oben auf der NSS-Verwaltungsseite angezeigt. Diese Anmeldedaten können nach Bedarf gemanagt werden.

Beachten Sie Folgendes über dieses NSS-Konto:

- Das Konto wird auf Benutzerebene verwaltet, was bedeutet, dass es von anderen Benutzern, die sich anmelden, nicht angezeigt wird.
- Das Konto kann nicht mit anderen BlueXP Funktionen verwendet werden, nicht mit der Erstellung, Lizenzierung oder dem Support von Cloud Volumes ONTAP.
- Es kann nur ein NSS-Konto für Digital Advisor pro Benutzer vorhanden sein.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Klicken Sie auf **NSS Management**.
3. Klicken Sie unter **Ihre NSS-Anmeldeinformationen** auf **Aktion** und wählen Sie eine der folgenden Optionen:
 - **Associate NSS User:** Anmeldedaten für ein NetApp Support Site Konto hinzufügen, damit Sie in BlueXP auf Digital Advisor zugreifen können.
 - **Vorhandene Anmeldedaten aktualisieren:** Die Zugangsdaten für Ihr NetApp Support Site Konto aktualisieren.
 - **Löschen:** Entfernen Sie das Konto, das mit Digital Advisor verknüpft ist.

BlueXP aktualisiert das NSS-Konto im Zusammenhang mit Digital Advisor.

Fügen Sie ein NSS-Konto hinzu

Über das Support-Dashboard können Sie Ihre NetApp Support Site Konten zur Verwendung mit BlueXP auf der NetApp Kontoebene hinzufügen und managen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie ein Partner- oder Reseller-Konto haben, können Sie ein oder mehrere NSS-Konten hinzufügen, aber sie können nicht neben Kunden-Level-Accounts hinzugefügt werden.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Klicken Sie auf **NSS Management > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

Beachten Sie Folgendes:

- Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
- Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern. Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet wird. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen **...** Menü.
- Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option **...** Menü. Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden.

Sie können das Konto jetzt beim Erstellen neuer Cloud Volumes ONTAP Systeme auswählen, wenn Sie bestehende Cloud Volumes ONTAP Systeme registrieren und sich für Support registrieren.

- ["Starten von Cloud Volumes ONTAP in AWS"](#)
- ["Starten von Cloud Volumes ONTAP in Azure"](#)
- ["Einführung von Cloud Volumes ONTAP in GCP"](#)
- ["Registrieren von Pay-as-you-go-Systemen"](#)

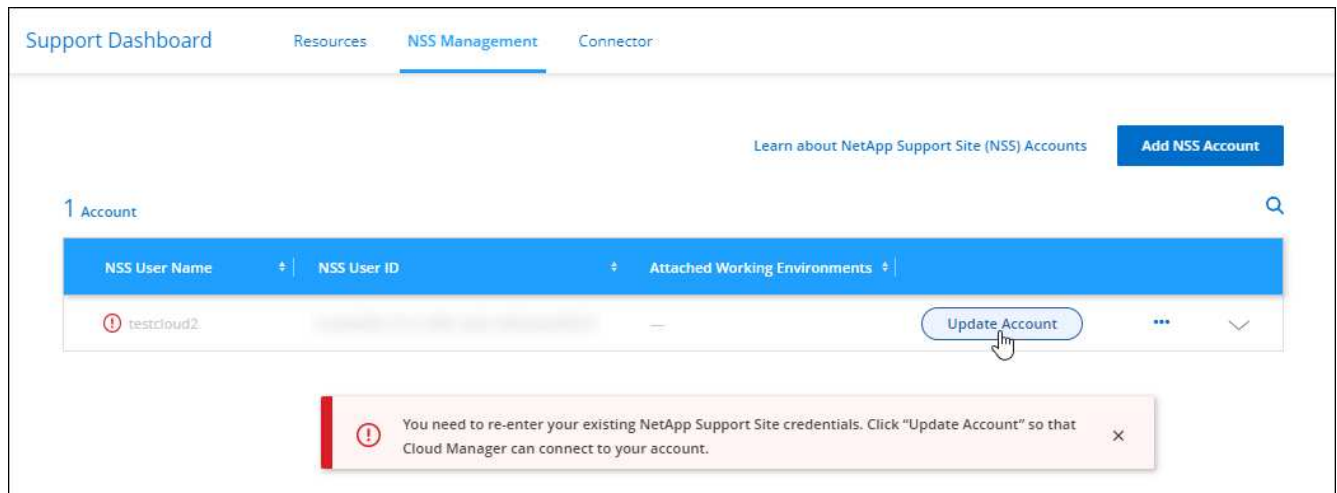
Aktualisieren Sie ein NSS-Konto für die neue Authentifizierungsmethode

Im November 2021 verwendet NetApp jetzt Microsoft Azure Active Directory als Identitäts-Provider für speziell auf Support und Lizenzierung applikationsspezifische Authentifizierungs-Services. Als Ergebnis dieses

Updates werden Sie von BlueXP aufgefordert, die Anmeldeinformationen für alle vorhandenen Konten, die Sie zuvor hinzugefügt haben, zu aktualisieren.

Schritte

1. Falls noch nicht geschehen, "[Erstellen Sie ein Microsoft Azure Active Directory B2C-Konto, das mit Ihrem aktuellen NetApp Konto verknüpft wird](#)".
2. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
3. Klicken Sie auf **NSS Management**.
4. Klicken Sie für das NSS-Konto, das Sie aktualisieren möchten, auf **Konto aktualisieren**.



5. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

6. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

Nach Abschluss des Vorgangs sollte das Konto, das Sie aktualisiert haben, nun als *New* Konto in der Tabelle aufgeführt werden. Die *ältere* Version des Kontos ist weiterhin in der Tabelle aufgeführt, zusammen mit allen vorhandenen Arbeitsumgebungsverknüpfungen.

7. Wenn vorhandene Cloud Volumes ONTAP-Arbeitsumgebungen an die ältere Version des Kontos angeschlossen sind, befolgen Sie die nachstehenden Schritte, um eine working environment to a different NSS account, Verbinden Sie die Arbeitsumgebungen mit einem anderen NSS-Konto.
8. Wechseln Sie zur älteren Version des NSS-Kontos, klicken Sie auf **...** Und wählen Sie dann **Löschen**.

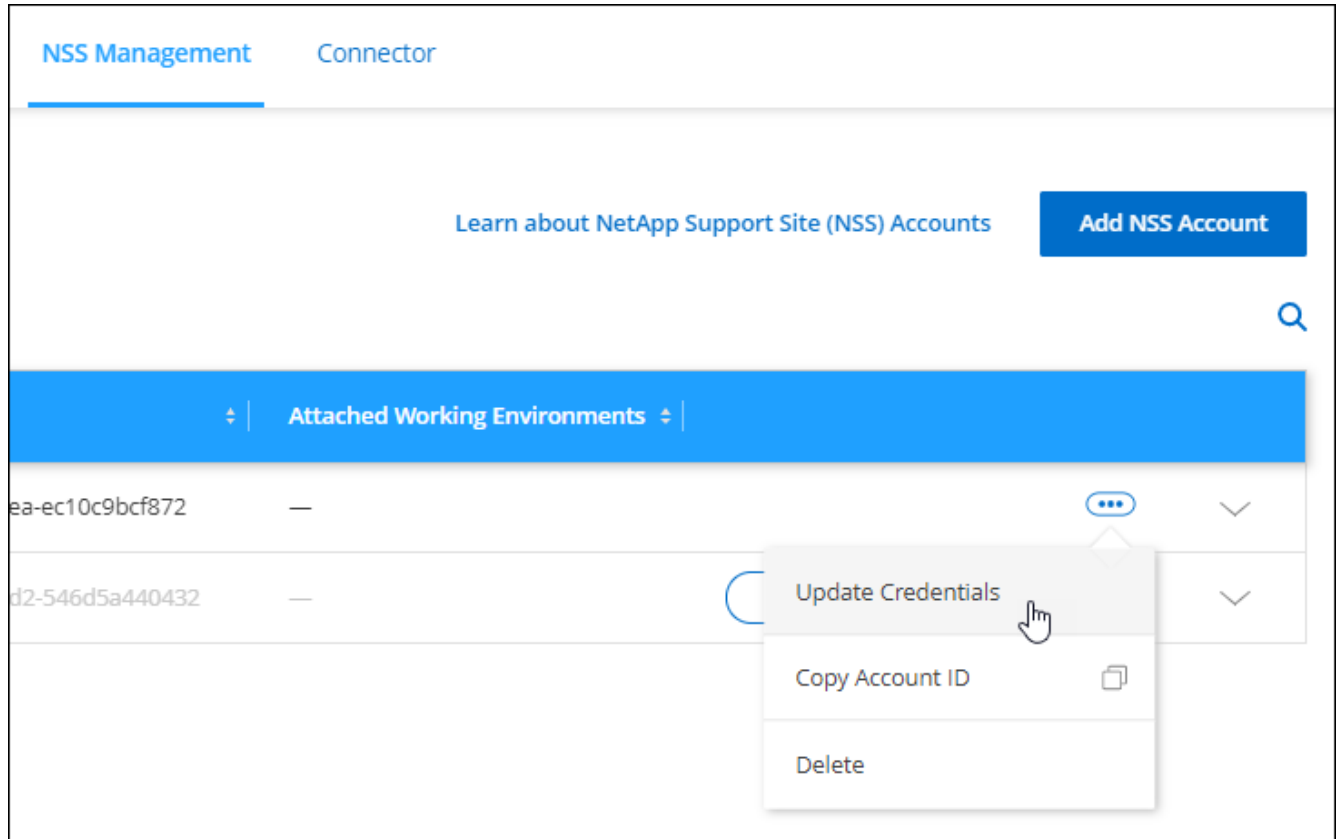
NSS-Anmeldeinformationen aktualisieren

Sie müssen die Anmeldeinformationen für Ihre NSS-Konten in BlueXP aktualisieren, wenn eine der folgenden Ereignisse eintritt:

- Sie ändern die Anmeldeinformationen für das Konto
- Das Aktualisieren-Token für Ihr Konto läuft nach 3 Monaten ab

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
2. Klicken Sie auf **NSS Management**.
3. Klicken Sie für das NSS-Konto, das Sie aktualisieren möchten, auf **...** Und wählen Sie dann **Anmeldeinformationen aktualisieren**.



4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

5. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

Verbinden Sie eine Arbeitsumgebung mit einem anderen NSS-Konto

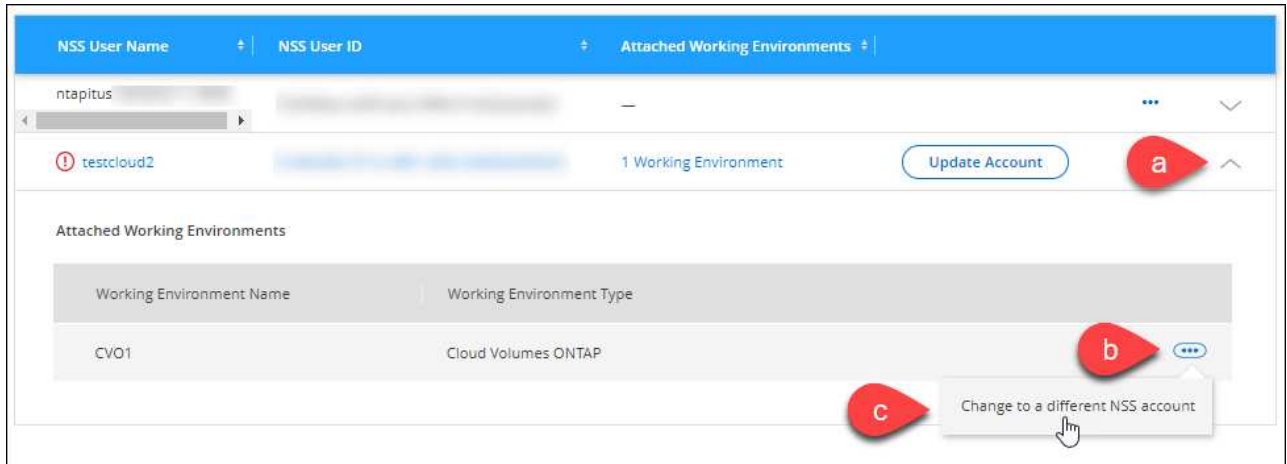
Wenn Ihr Unternehmen über mehrere NetApp Support Site Accounts verfügt, können Sie ändern, welches Konto einem Cloud Volumes ONTAP System zugeordnet ist.

Diese Funktion wird nur bei NSS-Konten unterstützt, die für die Verwendung von Microsoft Azure AD konfiguriert sind, das von NetApp zum Identitätsmanagement eingeführt wurde. Bevor Sie diese Funktion nutzen können, klicken Sie auf **NSS-Konto hinzufügen** oder **Konto aktualisieren**.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
2. Klicken Sie auf **NSS Management**.
3. Führen Sie die folgenden Schritte aus, um das NSS-Konto zu ändern:

- Erweitern Sie die Zeile für den NetApp Support Site Account, dem die Arbeitsumgebung derzeit zugeordnet ist.
- Klicken Sie für die Arbeitsumgebung, für die Sie die Zuordnung ändern möchten, auf ...
- Wählen Sie **Ändern Sie auf ein anderes NSS-Konto**.



- Wählen Sie das Konto aus und klicken Sie dann auf **Speichern**.

Zeigen Sie die E-Mail-Adresse für ein NSS-Konto an

Da für die Authentifizierungsdienste von NetApp Support-Site jetzt Microsoft Azure Active Directory verwendet wird, ist der NSS-Benutzername in BlueXP in der Regel eine vom Azure AD generierte Kennung. Als Ergebnis können Sie möglicherweise nicht sofort die E-Mail-Adresse kennen, die mit diesem Konto verknüpft ist. Aber BlueXP hat die Möglichkeit, Ihnen die zugehörige E-Mail-Adresse anzuzeigen.



Wenn Sie die NSS-Verwaltungsseite aufrufen, generiert BlueXP für jedes Konto in der Tabelle ein Token. Dieses Token enthält Informationen zur zugehörigen E-Mail-Adresse. Das Token wird dann entfernt, wenn Sie die Seite verlassen. Die Informationen werden niemals zwischengespeichert, wodurch Ihre Privatsphäre geschützt wird.

Schritte

- Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
- Klicken Sie auf **NSS Management**.
- Klicken Sie für das NSS-Konto, das Sie aktualisieren möchten, auf ... Und wählen Sie dann **E-Mail-Adresse anzeigen**.



BlueXP zeigt den Benutzernamen und die zugehörige E-Mail-Adresse der NetApp Support Website an. Sie können die Schaltfläche Kopieren verwenden, um die E-Mail-Adresse zu kopieren.

Entfernen Sie ein NSS-Konto

Löschen Sie alle NSS-Konten, die Sie nicht mehr mit BlueXP verwenden möchten.

Sie können kein Konto löschen, das derzeit einer Cloud Volumes ONTAP Arbeitsumgebung zugeordnet ist. Das müssen Sie zuerst a working environment to a different NSS account, Verbinden Sie die Arbeitsumgebungen mit einem anderen NSS-Konto.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.
2. Klicken Sie auf **NSS Management**.
3. Klicken Sie für das NSS-Konto, das Sie löschen möchten, auf **...** Und wählen Sie dann **Löschen**.



4. Klicken Sie zur Bestätigung auf **Löschen**.

Meine Opportunitys

Auf dem Canvas bietet die Registerkarte * My Opportunities* einen zentralen Ort, um vorhandene Ressourcen zu entdecken, die Sie BlueXP hinzufügen können, um konsistente Datenservices und Abläufe in Ihrer gesamten hybriden Multi-Cloud zu erhalten.

Mithilfe von My Opportunities können Sie derzeit bestehende FSX für ONTAP-Dateisysteme in Ihrem AWS-Konto erkennen.

["Entdecken Sie FSX für ONTAP mithilfe von My Opportunities"](#)

Referenz

Berechtigungen

Zusammenfassung der Berechtigungen für BlueXP

Um die Funktionen und Services in BlueXP nutzen zu können, müssen Sie Berechtigungen bereitstellen, damit BlueXP die Abläufe in Ihrer Cloud-Umgebung ausführen kann. Über die Links auf dieser Seite können Sie schnell auf die Berechtigungen zugreifen, die Sie basierend auf Ihrem Ziel benötigen.

AWS Berechtigungen

| Zweck | Beschreibung | Verlinken |
|-----------------------------|--|--|
| Connector-Bereitstellung | Der Benutzer, der einen Connector von BlueXP erstellt, benötigt spezielle Berechtigungen, um die Instanz in AWS bereitzustellen. | "Erstellen Sie einen Connector in AWS von BlueXP" |
| Verbindungsbetrieb | Beim Start des Connectors durch BlueXP wird eine Richtlinie an die Instanz angehängt, die die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen in Ihrem AWS-Konto bereitstellt. Sie müssen die Richtlinie selbst einrichten, wenn Sie dies tun "Starten Sie einen Connector vom Markt aus" Oder wenn Sie "Fügen Sie weitere AWS Zugangsdaten zu einem Connector hinzu" . Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden. | "AWS-Berechtigungen für den Connector" |
| Cloud Volumes ONTAP Betrieb | Eine IAM-Rolle muss mit jedem Cloud Volumes ONTAP-Node in AWS verbunden sein. Das gleiche gilt für den HA Mediator. Standardmäßig können BlueXP die IAM-Rollen für Sie erstellen lassen, Sie können jedoch Ihre eigenen Funktionen verwenden. | "Erfahren Sie, wie Sie die IAM-Rollen selbst einrichten" |

Azure-Berechtigungen

| Zweck | Beschreibung | Verlinken |
|--------------------------|--|---|
| Connector-Bereitstellung | Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie ein Azure-Konto oder einen Service-Principal verwenden, der über die Berechtigungen zum Bereitstellen der Connector-VM in Azure verfügt. | "Erstellen Sie einen Connector in Azure von BlueXP" |

| Zweck | Beschreibung | Verlinken |
|--------------------|---|--|
| Verbindungsbetrieb | <p>Wenn BlueXP die Connector VM in Azure implementiert, wird eine benutzerdefinierte Rolle erstellt, die die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen im Azure Abonnement bietet.</p> <p>Sie müssen die benutzerdefinierte Rolle selbst einrichten, wenn Sie "Starten Sie einen Connector vom Markt aus" Oder wenn Sie "Fügen Sie weitere Azure Credentials zu einem Connector hinzu".</p> <p>Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.</p> | "Azure-Berechtigungen für den Connector" |

Google Cloud-Berechtigungen

| Zweck | Beschreibung | Verlinken |
|--------------------------|--|--|
| Connector-Bereitstellung | Der Google Cloud-Benutzer, der einen Connector von BlueXP bereitstellt, benötigt spezielle Berechtigungen, um den Connector in Google Cloud bereitzustellen. | "Richten Sie Berechtigungen für die Bereitstellung des Connectors ein" |
| Verbindungsbetrieb | Das Servicekonto für die Connector-VM-Instanz muss über spezielle Berechtigungen für den täglichen Betrieb verfügen. Sie müssen das Servicekonto mit dem Connector verknüpfen, wenn Sie es über BlueXP bereitstellen. Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden. | "Richten Sie ein Servicekonto für den Konnektor ein" |

AWS-Berechtigungen für den Connector

Beim Start der Connector-Instanz in AWS hängt BlueXP eine Richtlinie an die Instanz an, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. Der Connector verwendet die Berechtigungen, um API-Aufrufe an verschiedene AWS Services wie EC2, S3, CloudFormation, IAM, Der Key Management Service (KMS) und vieles mehr.

IAM-Richtlinien

Die unten verfügbaren IAM-Richtlinien bieten die Berechtigungen, die ein Connector zur Verwaltung von Ressourcen und Prozessen innerhalb Ihrer Public-Cloud-Umgebung basierend auf Ihrer AWS-Region benötigt.

Wenn Sie einen Connector in einer standardmäßigen AWS-Region direkt aus BlueXP erstellen, wendet BlueXP automatisch Richtlinien auf den Connector an. Sie müssen in diesem Fall nichts tun.

Wenn Sie den Connector über den AWS Marketplace bereitstellen oder den Connector manuell auf einem

Linux-Host installieren, müssen Sie die Richtlinien selbst festlegen.

Außerdem müssen Sie sicherstellen, dass die Richtlinien immer auf dem neuesten Stand sind, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

Wählen Sie Ihre Region aus, um die erforderlichen Richtlinien anzuzeigen:

Standardregionen

Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich.

Die erste Richtlinie bietet Berechtigungen für folgende Dienste:

- Cloud-Backup
- Cloud-Daten Sinnvoll
- Cloud Tiering
- Cloud Volumes ONTAP
- FSX für ONTAP
- S3-Bucket-Erkennung

Die zweite Richtlinie bietet Berechtigungen für die folgenden Dienste:

- AppTemplate-Tagging
- Globaler Datei-Cache
- Kubernetes

Richtlinie #1

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cvoServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
```

```
"ec2:ReplaceRoute",
"ec2:UnassignPrivateIpAddresses",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"ec2:DescribePlacementGroups",
"cloudformation:CreateStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"cloudformation>DeleteStack",
"iam:PassRole",
"iam:CreateRole",
"iam:PutRolePolicy",
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"iam>DeleteRole",
"iam>DeleteRolePolicy",
"iam>DeleteInstanceProfile",
"iam:GetRolePolicy",
"iam:GetRole",
"sts:DecodeAuthorizationMessage",
"sts:AssumeRole",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3>CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"s3>DeleteObject",
"s3>DeleteObjectVersion",
"s3:PutObject",
"s3:ListAllMyBuckets",
"s3:GetObject",
"s3:GetEncryptionConfiguration",
```

```

        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "fsx:Describe*",
        "fsx:List*"
    ],
    "Resource": "*"
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:describeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
    ]
}

```

```

        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": "*"
},
{
    "Sid": "backupS3Policy",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
    ],

```

```

    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
},
{
    "Sid": "fabricPoolS3Policy",
    "Effect": "Allow",
    "Action": [
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3>DeleteBucket"
    ],
    "Resource": [
        "arn:aws:s3:::fabric-pool*"
    ]
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeRegions"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/netapp-adc-manager": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}

```

```

    ],
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:StopInstances",
        "ec2>DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2>DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    }
  ]
}

```

```
}
```

Richtlinie #2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "K8sServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GFCservicePolicy",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/GFCInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
```



```
"Sid": "tagServicePolicy",
"Effect": "Allow",
"Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:DescribeTags",
    "tag:getResources",
    "tag:getTagKeys",
    "tag:getTagValues",
    "tag:TagResources",
    "tag:UntagResources"
],
"Resource": "*"
}
]
```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2>DeleteVolume",
        "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:CreateSnapshot",
        "ec2>DeleteSnapshot",

```

```

        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",

```

```

        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::fabric-pool*"
    ]
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::netapp-backup-*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {

```

```

        "ec2:ResourceTag/WorkingEnvironment": "*"
    },
    "Resource": [
        "arn:aws-us-gov:ec2:*:*:instance/*"
    ],
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:volume/*"
        ]
    }
]
}

```

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",

```

```

        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",

```

```

        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

Wie werden die AWS Berechtigungen verwendet

In den folgenden Abschnitten wird die Nutzung der Berechtigungen für den jeweiligen NetApp Cloud-Service beschrieben. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf bereitgestellt werden.

AppTemplate-Tags

Der Connector stellt die folgenden API-Anforderungen zur Verwaltung von Tags auf AWS-Ressourcen bereit, wenn Sie den AppTemplate Tagging-Service verwenden:

- ec2:CreateTags
- ec2>DeleteTags
- ec2:DescribeTags
- Tag:getResources
- Tag:getTagKeys
- Tag:getTagValues
- Tag:TagResources
- Tag:UntagRessourcen

Cloud-Backup

Der Connector stellt die folgenden API-Anfragen zur Bereitstellung der Wiederherstellungsinstanz für Cloud-Backup bereit:

- ec2:StartInstances
- ec2:StopInstances
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:DescribeInstanceAttribut
- ec2:DescribeBilder
- ec2:CreateTags
- ec2:CreateVolume
- ec2:CreateSecurityGroup
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeRegionen
- CloudFormation:CreateStack
- CloudFormation>DeleteStack
- Wolkenbildung:DescribeStacks

Der Connector stellt folgende API-Anforderungen zum Management von Backups in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuchs
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleKonfiguration
- s3:PutLifecycleKonfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Km:Liste*
- Km:Beschreiben*
- s3:GetObject
- ec2:descbeVpcEndpunkte
- Km:ListAliase

- s3:PutVerschlüsselungskonfiguration

Der Connector stellt folgende API-Anforderungen vor, wenn Sie die Methode Suchen und Wiederherstellen verwenden, um Volumes und Dateien wiederherzustellen:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleKonfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMehrteilaUpload
- s3:ListeMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StoppQueryExecution
- Kleber>CreateDatabase
- Kleber>CreateTable
- Kleber:BatchDeletePartition

Der Connector macht die folgenden API-Anforderungen, wenn Sie DataLock und Ransomware-Schutz für Ihre Volume-Backups verwenden:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration

- s3:GetLifecycleKonfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersionierung
- s3:PutObjectVersionTagging
- s3:GetBucketVersionierung
- s3:GetBucketAcl
- s3:BypassGovernanceAufbewahrung
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Der Connector macht die folgenden API-Anforderungen, wenn Sie ein anderes AWS-Konto für Ihre Cloud Volumes ONTAP-Backups verwenden, als Sie für die Quell-Volumes verwenden:

- s3:PutBucketPolicy
- s3:PutBucketEigentümerControls

Cloud-Daten Sinnvoll

Der Connector stellt die folgenden API-Anforderungen zur Bereitstellung der Cloud Data Sense Instanz:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2>DeleteSecurityGroup
- ec2:DescribeSecurityGroups
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2>DeleteNetworkInterface
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:DescribeRegionen
- CloudFormation:CreateStack
- CloudFormation>DeleteStack
- Wolkenbildung:DescribeStacks
- Molkenbildung:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociatelamInstanceProfil
- ec2:DescribelamInstanceProfilVerbände

Der Connector erstellt bei Verwendung von Cloud Data Sense die folgenden API-Anforderungen zum Scannen von S3-Buckets:

- iam:AddRoleToInstanceProfile
- ec2:AssociatelamInstanceProfil
- ec2:DescribelamInstanceProfilVerbände
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuchs
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3>DeleteObject
- s3>DeleteObjectVersion
- s3:PutObject
- STS:AssumeRole

Cloud Tiering

Der Connector erstellt bei Verwendung von Cloud Tiering die folgenden API-Anforderungen an das Tiering von Daten in Amazon S3.

| Aktion | Wird zur Einrichtung verwendet? | Wird für den täglichen Betrieb verwendet? |
|------------------------------|---------------------------------|---|
| s3:CreateBucket | Ja. | Nein |
| s3:PutLifecycleKonfiguration | Ja. | Nein |
| s3:GetLifecycleKonfiguration | Ja. | Ja. |

| Aktion | Wird zur Einrichtung verwendet? | Wird für den täglichen Betrieb verwendet? |
|----------------------|---------------------------------|---|
| ec2:DescribeRegionen | Ja. | Ja. |

Cloud Volumes ONTAP

Der Connector stellt die folgenden API-Anforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in AWS.

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|--|--|---|---|------------------------|
| Erstellung und Management von IAM-Rollen und Instanzprofilen für Cloud Volumes ONTAP Instanzen | iam:ListInstanceProfiles | Ja. | Ja. | Nein |
| | iam:CreateRole | Ja. | Nein | Nein |
| | iam>DeleteRole | Nein | Ja. | Ja. |
| | iam:PutPolicy | Ja. | Nein | Nein |
| | iam:CreateInstanceProfile | Ja. | Nein | Nein |
| | iam>DeleteRolePolicy | Nein | Ja. | Ja. |
| | iam:AddRoleToInstanceProfile | Ja. | Nein | Nein |
| | iam:RemoveRoleFromInstanceProfile | Nein | Ja. | Ja. |
| | iam>DeleteInstanceProfile | Nein | Ja. | Ja. |
| | iam:PassRole | Ja. | Nein | Nein |
| | ec2:AssociateIAMInstanceProfile | Ja. | Ja. | Nein |
| | ec2:DescribeIAMInstanceProfileAssociations | Ja. | Ja. | Nein |
| | ec2:DisassociateIAMInstanceProfile | Nein | Ja. | Nein |
| Dekodieren von Autorisierungsstatusmeldungen | STS:DecodeAuthorizationMessage | Ja. | Ja. | Nein |
| Beschreiben Sie die angegebenen Bilder (Amis), die dem Konto zur Verfügung stehen | ec2:DescribeImages | Ja. | Ja. | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|---|-------------------------------|---|---|------------------------|
| Routingtabellen in einer VPC beschreiben (nur für HA-Paare erforderlich) | ec2:DescribeRouteTables | Ja. | Nein | Nein |
| Beenden, starten und überwachen Sie Instanzen | ec2:StartInstances | Ja. | Ja. | Nein |
| | ec2:StopInstances | Ja. | Ja. | Nein |
| | ec2:DescribeInstances | Ja. | Ja. | Nein |
| | ec2:DescribeInstanceStatus | Ja. | Ja. | Nein |
| | ec2:RunInstances | Ja. | Nein | Nein |
| | ec2:TerminateInstances | Nein | Nein | Ja. |
| | ec2:ModifyInstanceAttribute | Nein | Ja. | Nein |
| Vergewissern Sie sich, dass erweitertes Networking für unterstützte Instanztypen aktiviert ist | ec2:DescribeInstanceAttribute | Nein | Ja. | Nein |
| Markieren Sie Ressourcen mit den Tags „WorkingEnvironment“ und „WorkingEnvironment ID“, die zur Wartung und Kostenverteilung verwendet werden | ec2:CreateTags | Ja. | Ja. | Nein |
| Management von EBS Volumes, die Cloud Volumes ONTAP als Back-End Storage verwendet | ec2:CreateVolume | Ja. | Ja. | Nein |
| | ec2:DescribeVolumes | Ja. | Ja. | Ja. |
| | ec2:ModifyVolumeAttribute | Nein | Ja. | Ja. |
| | ec2:AttachVolume | Ja. | Ja. | Nein |
| | ec2>DeleteVolume | Nein | Ja. | Ja. |
| | ec2:DetachVolume | Nein | Ja. | Ja. |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|---|-------------------------------------|--|--|-------------------------------|
| Erstellen und Managen von Sicherheitsgruppen für Cloud Volumes ONTAP | ec2:CreateSecurityGroup | Ja. | Nein | Nein |
| | ec2:DeleteSecurityGroup | Nein | Ja. | Ja. |
| | ec2:DescribeSecurityGroups | Ja. | Ja. | Ja. |
| | ec2:RevokeSecurityGroupEgress | Ja. | Nein | Nein |
| | ec2:AuthoriseSecurityGroupEgress | Ja. | Nein | Nein |
| | ec2:AuthoriseSecurityGroupIngress | Ja. | Nein | Nein |
| | ec2:RevokeSecurityGroupIngress | Ja. | Ja. | Nein |
| Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz erstellen und verwalten | ec2:CreateNetworkInterface | Ja. | Nein | Nein |
| | ec2:DescribeNetworkInterfaces | Ja. | Ja. | Nein |
| | ec2:DeleteNetworkInterface | Nein | Ja. | Ja. |
| | ec2:ModifyNetworkInterfaceAttribute | Nein | Ja. | Nein |
| Abrufen der Liste der Zielnetze und -Sicherheitsgruppen | ec2:DescribeSubnets | Ja. | Ja. | Nein |
| | ec2:DescribeVpcs | Ja. | Ja. | Nein |
| Abrufen der DNS-Server und des Standard-Domain-Namens für Cloud Volumes ONTAP-Instanzen | ec2:DescribeDhcpOptions | Ja. | Nein | Nein |
| Erstellen von Snapshots von EBS Volumes für Cloud Volumes ONTAP | ec2:CreateSnapshot | Ja. | Ja. | Nein |
| | ec2:DeleteSnapshot | Nein | Ja. | Ja. |
| | ec2:DescribeSnapshots | Nein | Ja. | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|--|-----------------------------------|--|--|-------------------------------|
| Erfassen Sie die Cloud Volumes ONTAP Konsole, die an AutoSupport Meldungen angeschlossen ist | ec2:GetConsoleOutput | Ja. | Ja. | Nein |
| Erhalten Sie die Liste der verfügbaren Schlüsselpaare | ec2:DescribeKeyPairs | Ja. | Nein | Nein |
| Hier erhalten Sie eine Liste der verfügbaren AWS Regionen | ec2:DescribeRegions | Ja. | Ja. | Nein |
| Verwalten von Tags für Ressourcen, die Cloud Volumes ONTAP Instanzen zugeordnet sind | ec2:DeleteTags | Nein | Ja. | Ja. |
| | ec2:DescribeTags | Nein | Ja. | Nein |
| Stacks für AWS CloudFormation-Vorlagen erstellen und managen | CloudFormation:CreateStack | Ja. | Nein | Nein |
| | CloudFormation:DeleteStack | Ja. | Nein | Nein |
| | Wolkenbildung:DescribeStacks | Ja. | Ja. | Nein |
| | Molkenbildung:DescribeStackEvents | Ja. | Nein | Nein |
| | Cloudformation:ValidierteVorlage | Ja. | Nein | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|---|-------------------------------|---|---|------------------------|
| Es wird ein S3-Bucket erstellt und gemanagt, den ein Cloud Volumes ONTAP System als Kapazitäts-Tier für Daten-Tiering verwendet | s3:CreateBucket | Ja. | Ja. | Nein |
| | s3>DeleteBucket | Nein | Ja. | Ja. |
| | s3:GetLifecycleKonfiguration | Nein | Ja. | Nein |
| | s3:PutLifecycleKonfiguration | Nein | Ja. | Nein |
| | s3:PutBucketTagging | Nein | Ja. | Nein |
| | s3:ListBucketVersions | Nein | Ja. | Nein |
| | s3:GetBucketPolicyStatus | Nein | Ja. | Nein |
| | s3:GetBucketPublicAccessBlock | Nein | Ja. | Nein |
| | s3:GetBucketAcl | Nein | Ja. | Nein |
| | s3:GetBucketPolicy | Nein | Ja. | Nein |
| | s3:PutBucketPublicAccessBlock | Nein | Ja. | Nein |
| | s3:GetBucketTagging | Nein | Ja. | Nein |
| | s3:GetBucketLocation | Nein | Ja. | Nein |
| | s3:ListAllMyBuckets | Nein | Nein | Nein |
| | s3:ListBucket | Nein | Ja. | Nein |
| Datenverschlüsselung von Cloud Volumes ONTAP mithilfe des AWS KMS (Key Management Service) | Km:Liste* | Ja. | Ja. | Nein |
| | Km:ReVerschlüsseln* | Ja. | Nein | Nein |
| | Km:Beschreiben* | Ja. | Ja. | Nein |
| | Km>CreateGrant | Ja. | Ja. | Nein |
| AWS Kostendaten für Cloud Volumes ONTAP beziehen | ce:GetReservoir Utilisation | Nein | Ja. | Nein |
| | ce:GetDimensionValues | Nein | Ja. | Nein |
| | ce:GetCostAndUsage | Nein | Ja. | Nein |
| | ce:GetTags | Nein | Ja. | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|---|----------------------------------|---|---|------------------------|
| Erstellen und managen Sie eine AWS Spread-Platzierungsgruppe für zwei HA-Nodes und den Mediator in einer einzigen AWS Availability Zone | ec2:CreatePlacemen tGroup | Ja. | Nein | Nein |
| | ec2>DeletePlacemen tGroup | Nein | Ja. | Ja. |
| Erstellen von Berichten | fsx:Beschreiben* | Nein | Ja. | Nein |
| | fsx:Liste* | Nein | Ja. | Nein |
| Aggregate erstellen und managen, die die Amazon EBS Elastic Volumes Funktion unterstützen | ec2:DescribeVolumi esModified | Nein | Ja. | Nein |
| | ec2:ModifyVolume | Nein | Ja. | Nein |

Globaler Datei-Cache

Der Connector stellt folgende API-Anforderungen zur Bereitstellung von Global File Cache-Instanzen während der Bereitstellung bereit:

- Wolkenbildung:DescribeStacks
- cloudwatch:GetMetricStatistics
- CloudFormation:ListenStacks

FSX für ONTAP

Der Konnektor stellt die folgenden API-Anforderungen zur Verwaltung von FSX für ONTAP vor:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribut
- ec2:DescribeRouteTables
- ec2:DescribeBilder
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeDhcpOptions

- ec2:DescribeSnapshots
- ec2:DescribeKeypairs
- ec2:DescribeRegionen
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileVerbände
- ec2:DescribeReserviertInstanceAngebote
- ec2:describeVpcEndpunkte
- ec2:DescribeVpcs
- ec2:DescribeVolumesModified
- ec2:DescribePlacementGroups
- Km:Liste*
- Km:Beschreiben*
- Km>CreateGrant
- Km:ListAliase
- fsx:Beschreiben*
- fsx:Liste*

Kubernetes

Der Connector stellt folgende API-Anforderungen zur Erkennung und Verwaltung von Amazon EKS-Clustern vor:

- ec2:DescribeRegionen
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

S3-Bucket-Erkennung

Der Connector stellt folgende API-Anforderung vor, Amazon S3 Buckets zu erkennen:

s3:GetVerschlüsselungKonfiguration

Azure-Berechtigungen für den Connector

Beim Start der Connector-VM in Azure wird von BlueXP eine benutzerdefinierte Rolle an die VM angehängt, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb des Azure-Abonnements bietet. Der Connector nutzt die Berechtigungen, um API-Aufrufe an mehrere Azure-Services durchzuführen.

Berechtigungen für benutzerdefinierte Rollen

Die unten aufgeführte benutzerdefinierte Rolle stellt die Berechtigungen bereit, die ein Connector zur Verwaltung von Ressourcen und Prozessen in Ihrem Azure-Netzwerk benötigt.

Wenn Sie einen Connector direkt aus BlueXP erstellen, wendet BlueXP diese benutzerdefinierte Rolle automatisch auf den Connector an.

Wenn Sie den Connector über den Azure Marketplace bereitstellen oder den Connector manuell auf einem Linux-Host installieren, müssen Sie die benutzerdefinierte Rolle selbst einrichten.

Außerdem müssen Sie sicherstellen, dass die Rolle auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

```
{
  "Name": "BlueXP Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",

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

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

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

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

```

        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/write",
        "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.Storage/checknameavailability/read",
        "Microsoft.Storage/operations/read",
        "Microsoft.Storage/storageAccounts/listkeys/action",
        "Microsoft.Storage/storageAccounts/read",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/write",
        "Microsoft.Storage/usages/read",
        "Microsoft.Compute/snapshots/write",
        "Microsoft.Compute/snapshots/read",
        "Microsoft.Compute/availabilitySets/write",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Compute/disks/beginGetAccess/action",

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

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/write",
        "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
        "Microsoft.Network/loadBalancers/probes/read",
        "Microsoft.Network/loadBalancers/probes/join/action",
        "Microsoft.Authorization/locks/*",

```

```
"Microsoft.Network/routeTables/join/action",
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
"Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
"Microsoft.Network/loadBalancers/delete",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Compute/diskEncryptionSets/write",
```

```

        "Microsoft.KeyVault/vaults/deploy/action",
        "Microsoft.Compute/diskEncryptionSets/delete",
        "Microsoft.Resources/tags/read",
        "Microsoft.Resources/tags/write",
        "Microsoft.Resources/tags/delete",
        "Microsoft.Network/applicationSecurityGroups/write",
        "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",

"Microsoft.ContainerService/managedClusters/listClusterUserCredential/action",
        "Microsoft.ContainerService/managedClusters/read",
        "Microsoft.Synapse/workspaces/write",
        "Microsoft.Synapse/workspaces/read",
        "Microsoft.Synapse/workspaces/delete",
        "Microsoft.Synapse/register/action",
        "Microsoft.Synapse/checkNameAvailability/action",
        "Microsoft.Synapse/workspaces/operationStatuses/read",
        "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
        "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}

```

Verwendung von Azure Berechtigungen

In den folgenden Abschnitten wird die Nutzung der Berechtigungen für den jeweiligen NetApp Cloud-Service beschrieben. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf bereitgestellt werden.

AppTemplate-Tags

Der Connector stellt bei Verwendung des AppTemplate Tagging-Dienstes folgende API-Anforderungen zur Verwaltung von Tags auf Azure-Ressourcen bereit:

- Microsoft.Ressourcen/Ressourcen/Lesen
- Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen
- Microsoft.Ressourcen/Tags/lesen
- Microsoft.Ressourcen/Tags/schreiben

Azure NetApp Dateien

Der Connector stellt folgende API-Anforderungen zur Verwaltung von Azure NetApp Files-Arbeitsumgebungen vor:

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

Cloud-Backup

Der Connector stellt die folgenden API-Anforderungen für Backup- und Wiederherstellungsvorgänge:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/StorageAccounts/Listkeys/Action
- Microsoft.Storage/StorageAccounts/Lesevorgang
- Microsoft.Storage/StorageAccounts/write
- Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang
- Microsoft.KeyVault/Vaults/read
- Microsoft.KeyVault/Vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen
- Microsoft.Resources/Subskriptionen/resourceGroups/write
- Microsoft.Authorization/Locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read

- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressourcen/Bereitstellungen/löschen
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Storage/StorageAccounts/blobServices/Container/write
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/Action

Der Konnektor stellt folgende API-Anforderungen zur Verfügung, wenn Sie die Funktion Suchen & Wiederherstellen verwenden:

- Microsoft.Synapse/Workspaces/schreiben
- Microsoft.Synapse/Workspaces/Lesen
- Microsoft.Synapse/Workspaces/delete
- Microsoft.Synapse/Register/Aktion
- Microsoft.Synapse/CheckNameVerfügbarkeit/Aktion
- Microsoft.Synapse/Workspaces/OperationStatus/Lesen
- Microsoft.Synapse/Workspaces/Firewall Regeln/lesen
- Microsoft.Synapse/Workspaces/ersetzenAllIpFirewallRegeln/Aktion
- Microsoft.Synapse/Workspaces/OperationResults/read

Cloud-Daten Sinnvoll

Der Connector stellt bei der Verwendung von Cloud Data Sense die folgenden API-Anforderungen vor.

| Aktion | Wird zur Einrichtung verwendet? | Wird für den täglichen Betrieb verwendet? |
|---|---------------------------------|---|
| Microsoft.Compute/locations/operations/read | Ja. | Ja. |
| Microsoft.Compute/locations/vmSizes/read | Ja. | Ja. |
| Microsoft.Compute/operations/read | Ja. | Ja. |
| Microsoft.Compute/virtualMachines/instanceView/read | Ja. | Ja. |
| Microsoft.Compute/virtualMachines/powerOff/action | Ja. | Nein |

| Aktion | Wird zur Einrichtung verwendet? | Wird für den täglichen Betrieb verwendet? |
|--|---------------------------------|---|
| Microsoft.Compute/virtualMachines/read | Ja. | Ja. |
| Microsoft.Compute/virtualMachines/restart/action | Ja. | Nein |
| Microsoft.Compute/virtualMachines/start/action | Ja. | Nein |
| Microsoft.Compute/virtualMachines/vmSizes/read | Nein | Ja. |
| Microsoft.Compute/virtualMachines/write | Ja. | Nein |
| Microsoft.Compute/images/read | Ja. | Ja. |
| Microsoft.Compute/disks/delete | Ja. | Nein |
| Microsoft.Compute/disks/read | Ja. | Ja. |
| Microsoft.Compute/disks/write | Ja. | Nein |
| Microsoft.Storage/ChecknameVerfügbarkeit/Lesevorgang | Ja. | Ja. |
| Microsoft.Storage/Operations/Lesevorgang | Ja. | Ja. |
| Microsoft.Storage/StorageAccounts/Listkeys/Action | Ja. | Nein |
| Microsoft.Storage/StorageAccounts/Lesevorgang | Ja. | Ja. |
| Microsoft.Storage/StorageAccounts/write | Ja. | Nein |
| Microsoft.Storage/StorageAccounts/delete | Nein | Ja. |
| Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang | Ja. | Ja. |
| Microsoft.Network/networkInterfaces/read | Ja. | Ja. |
| Microsoft.Network/networkInterfaces/write | Ja. | Nein |
| Microsoft.Network/networkInterfaces/join/action | Ja. | Nein |
| Microsoft.Network/networkSecurityGroups/read | Ja. | Ja. |
| Microsoft.Network/networkSecurityGroups/write | Ja. | Nein |

| Aktion | Wird zur Einrichtung verwendet? | Wird für den täglichen Betrieb verwendet? |
|---|---------------------------------|---|
| Microsoft.Ressourcen/Abonnements/Standorte/gelesen | Ja. | Ja. |
| Microsoft.Network/locations/operationResults/read | Ja. | Ja. |
| Microsoft.Network/locations/operations/read | Ja. | Ja. |
| Microsoft.Network/virtualNetworks/read | Ja. | Ja. |
| Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Ja. | Ja. |
| Microsoft.Network/virtualNetworks/subnets/read | Ja. | Ja. |
| Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Ja. | Ja. |
| Microsoft.Network/virtualNetworks/virtualMachines/read | Ja. | Ja. |
| Microsoft.Network/virtualNetworks/subnets/join/action | Ja. | Nein |
| Microsoft.Network/virtualNetworks/subnets/write | Ja. | Nein |
| Microsoft.Network/routeTables/join/action | Ja. | Nein |
| Microsoft.Ressourcen/Implementierungen/Betrieb/Lesevorgang | Ja. | Ja. |
| Microsoft.Ressourcen/Implementierungen/lesen | Ja. | Ja. |
| Microsoft.Ressourcen/Implementierungen/schreiben | Ja. | Nein |
| Microsoft.Ressourcen/Ressourcen/Lesen | Ja. | Ja. |
| Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen | Ja. | Ja. |
| Microsoft.Resources/Subskriptionen/resourceGroups/delete | Ja. | Nein |
| Microsoft.Resources/Subskriptionen/resourceGroups/read | Ja. | Ja. |
| Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen | Ja. | Ja. |

| Aktion | Wird zur Einrichtung verwendet? | Wird für den täglichen Betrieb verwendet? |
|---|---------------------------------|---|
| Microsoft.Resources/Subskriptionen/resourceGroups/write | Ja. | Nein |

Cloud Tiering

Der Connector stellt bei der Einrichtung von Cloud Tiering die folgenden API-Anforderungen vor.

- Microsoft.Storage/StorageAccounts/Listkeys/Action
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen

Der Connector stellt folgende API-Anforderungen für den täglichen Betrieb.

- Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang
- Microsoft.Storage/StorageAccounts/blobServices/Container/write
- Microsoft.Storage/StorageAccounts/Management Policies/read
- Microsoft.Storage/StorageAccounts/Management Richtlinien/schreiben
- Microsoft.Storage/StorageAccounts/Lesevorgang

Cloud Volumes ONTAP

Der Connector stellt die folgenden API-Anforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in AWS.

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|--|---|--|--|-------------------------------|
| Erstellen Sie VMs, stoppen, starten, löschen und erhalten Sie den Status des Systems | Microsoft.Compute/locations/operations/read | Ja. | Ja. | Nein |
| | Microsoft.Compute/locations/vmSizes/read | Ja. | Ja. | Nein |
| | Microsoft.Ressourcen/Abonnements/Standorte/gelesen | Ja. | Nein | Nein |
| | Microsoft.Compute/operations/read | Ja. | Ja. | Nein |
| | Microsoft.Compute/virtualMachines/instanceView/read | Ja. | Ja. | Nein |
| | Microsoft.Compute/virtualMachines/powerOff/action | Ja. | Ja. | Nein |
| | Microsoft.Compute/virtualMachines/read | Ja. | Ja. | Nein |
| | Microsoft.Compute/virtualMachines/restart/action | Ja. | Ja. | Nein |
| | Microsoft.Compute/virtualMachines/start/action | Ja. | Ja. | Nein |
| | Microsoft.Compute/virtualMachines/deallocate/action | Nein | Ja. | Ja. |
| | Microsoft.Compute/virtualMachines/vmSizes/read | Nein | Ja. | Nein |
| | Microsoft.Compute/virtualMachines/write | Ja. | Ja. | Nein |
| Implementierung über eine VHD ermöglichen | Microsoft.Compute/images/read | Ja. | Nein | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|---|---|--|--|-------------------------------|
| Netzwerkschnittstellen im Ziel-Subnetz erstellen und verwalten | Microsoft.Network/networkInterfaces/read | Ja. | Ja. | Nein |
| | Microsoft.Network/networkInterfaces/write | Ja. | Ja. | Nein |
| | Microsoft.Network/networkInterfaces/join/action | Ja. | Ja. | Nein |
| Erstellen Sie vordefinierte Netzwerksicherheitsgruppen | Microsoft.Network/networkSecurityGroups/read | Ja. | Ja. | Nein |
| | Microsoft.Network/networkSecurityGroups/write | Ja. | Ja. | Nein |
| | Microsoft.Network/networkSecurityGroups/join/action | Ja. | Nein | Nein |
| Abrufen der Netzwerkinformationen zu Regionen, Ziel-vnet und Subnetz, und Hinzufügen der VMs zu VNets | Microsoft.Network/locations/operationResults/read | Ja. | Ja. | Nein |
| | Microsoft.Network/locations/operations/read | Ja. | Ja. | Nein |
| | Microsoft.Network/virtualNetworks/read | Ja. | Nein | Nein |
| | Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Ja. | Nein | Nein |
| | Microsoft.Network/virtualNetworks/subnets/read | Ja. | Ja. | Nein |
| | Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Ja. | Ja. | Nein |
| | Microsoft.Network/virtualNetworks/virtualMachines/read | Ja. | Ja. | Nein |
| | Microsoft.Network/virtualNetworks/subnets/join/action | Ja. | Ja. | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|---|---|--|--|-------------------------------|
| Erstellen und Verwalten von Ressourcengruppen | Microsoft.Ressourcen/Implementierung/Betrieb/Lesevorgang | Ja. | Ja. | Nein |
| | Microsoft.Ressourcen/Implementierung/lesen | Ja. | Ja. | Nein |
| | Microsoft.Ressourcen/Implementierung/schreiben | Ja. | Ja. | Nein |
| | Microsoft.Ressourcen/Ressourcen/Lesen | Ja. | Ja. | Nein |
| | Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen | Ja. | Ja. | Nein |
| | Microsoft.Resources/Subskriptionen/resourceGroups/delete | Ja. | Ja. | Ja. |
| | Microsoft.Resources/Subskriptionen/resourceGroups/read | Nein | Ja. | Nein |
| | Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen | Ja. | Ja. | Nein |
| | Microsoft.Resources/Subskriptionen/resourceGroups/write | Ja. | Ja. | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|---|--|--|--|-------------------------------|
| Azure-Storage-Konten und -Festplatten managen | Microsoft.Compute/disks/read | Ja. | Ja. | Ja. |
| | Microsoft.Compute/disks/write | Ja. | Ja. | Nein |
| | Microsoft.Compute/disks/delete | Ja. | Ja. | Ja. |
| | Microsoft.Storage/ChecknameVerfügbarkeit/Lesevorgang | Ja. | Ja. | Nein |
| | Microsoft.Storage/Operations/Lesevorgang | Ja. | Ja. | Nein |
| | Microsoft.Storage/StorageAccounts/Listkeys/Action | Ja. | Ja. | Nein |
| | Microsoft.Storage/StorageAccounts/Lesevorgang | Ja. | Ja. | Nein |
| | Microsoft.Storage/StorageAccounts/delete | Nein | Ja. | Ja. |
| | Microsoft.Storage/StorageAccounts/write | Ja. | Ja. | Nein |
| | Microsoft.Speicherung/Verwendung/Lesen | Nein | Ja. | Nein |
| Ermöglichen von Backups auf Blob Storage und Verschlüsselung von Storage-Konten | Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang | Ja. | Ja. | Nein |
| | Microsoft.KeyVault/Vaults/read | Ja. | Ja. | Nein |
| | Microsoft.KeyVault/Vaults/accessPolicies/write | Ja. | Ja. | Nein |
| Vnet-Service-Endpunkte für Daten-Tiering aktivieren | Microsoft.Network/virtualNetworks/subnets/write | Ja. | Ja. | Nein |
| | Microsoft.Network/routeTables/join/action | Ja. | Ja. | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|--|---|--|--|-------------------------------|
| Erstellen und managen Sie über Azure gemanagte Snapshots | Microsoft.Compute/snapshots/write | Ja. | Ja. | Nein |
| | Microsoft.Compute/snapshots/read | Ja. | Ja. | Nein |
| | Microsoft.Compute/snapshots/delete | Nein | Ja. | Ja. |
| | Microsoft.Compute/disks/beginGetAccess/action | Nein | Ja. | Nein |
| Erstellung und Management von Verfügbarkeitsgruppen | Microsoft.Compute/availabilitySets/write | Ja. | Nein | Nein |
| | Microsoft.Compute/availabilitySets/read | Ja. | Nein | Nein |
| Programmatische Implementierungen über den Markt ermöglichen | Microsoft.MarketplaceOrdering/offertypes/Publisher/Offer/Plans/Agreements/read | Ja. | Nein | Nein |
| | Microsoft.MarketplaceOrdering/offertypes/Publisher/Offer/Plans/Agreements/write | Ja. | Ja. | Nein |
| Managen Sie einen Load Balancer für HA-Paare | Microsoft.Network/loadBalancers/read | Ja. | Ja. | Nein |
| | Microsoft.Network/loadBalancers/write | Ja. | Nein | Nein |
| | Microsoft.Network/loadBalancers/delete | Nein | Ja. | Ja. |
| | Microsoft.Network/loadBalancers/backendAddressPools/read | Ja. | Ja. | Nein |
| | Microsoft.Network/loadBalancers/loadBalancingRules/read | Ja. | Nein | Nein |
| | Microsoft.Network/loadBalancers/probes/read | Ja. | Nein | Nein |
| | Microsoft.Network/loadBalancers/probes/join/action | Ja. | Nein | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|--|---|--|--|-------------------------------|
| Verwaltung von Sperren auf Azure Festplatten aktivieren | Microsoft.Authorization/Locks/* | Ja. | Ja. | Nein |
| Aktivieren Sie private Endpunkte für HA-Paare, wenn sich keine Verbindung außerhalb des Subnetzes befindet | Microsoft.Network/privateEndpoints/write | Ja. | Ja. | Nein |
| | Microsoft.Storage/Speicherkonten/PrivateEndpointConnectionsGenehmigung/Aktion | Ja. | Nein | Nein |
| | Microsoft.Storage/StorageAccounts/privateEndpointConnections/Lesevorgang | Ja. | Ja. | Ja. |
| | Microsoft.Network/privateEndpoints/read | Ja. | Ja. | Ja. |
| | Microsoft.Network/privateDnsZones/write | Ja. | Ja. | Nein |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/write | Ja. | Ja. | Nein |
| | Microsoft.Network/virtualNetworks/join/action | Ja. | Ja. | Nein |
| | Microsoft.Network/privateDnsZones/A/write | Ja. | Ja. | Nein |
| | Microsoft.Network/privateDnsZones/read | Ja. | Ja. | Nein |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/read | Ja. | Ja. | Nein |
| Erforderlich für einige VM-Implementierungen, abhängig von der zugrunde liegenden physischen Hardware | Microsoft.Resource/Implementierung/OperationStatuses/read | Ja. | Ja. | Nein |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|--|--|---|---|------------------------|
| Entfernen von Ressourcen aus einer Ressourcengruppe bei Ausfall oder Löschen der Bereitstellung | Microsoft.Network/privateEndpoints/delete | Ja. | Ja. | Nein |
| | Microsoft.Compute/availabilitySets/delete | Ja. | Ja. | Nein |
| Nutzen Sie die API, wenn Sie die vom Kunden gemanagten Schlüssel verwenden | Microsoft.Compute/diskEncryptionSets/read | Ja. | Ja. | Ja. |
| | Microsoft.Compute/diskEncryptionSets/write | Ja. | Ja. | Nein |
| | Microsoft.KeyVault/Vaults/Deploy/Action | Ja. | Nein | Nein |
| | Microsoft.Compute/diskEncryptionSets/delete | Ja. | Ja. | Ja. |
| Konfigurieren Sie eine Applikationssicherheitsgruppe für ein HA-Paar, um die HA Interconnect- und Cluster-Netzwerk-NICs zu isolieren | Microsoft.Network/applicationSecurityGroups/write | Nein | Ja. | Nein |
| | Microsoft.Network/applicationSecurityGroups/read | Nein | Ja. | Ja. |
| | Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action | Nein | Ja. | Nein |
| | Microsoft.Network/networkSecurityGroups/securityRules/write | Ja. | Ja. | Nein |
| | Microsoft.Network/applicationSecurityGroups/delete | Nein | Ja. | Nein |
| | Microsoft.Network/networkSecurityGroups/securityRules/delete | Nein | Ja. | Ja. |

| Zweck | Aktion | Werden sie für die Implementierung verwendet? | Wird für den täglichen Betrieb verwendet? | Zum Löschen verwendet? |
|--|--|---|---|------------------------|
| Lesen, Schreiben und Löschen von Tags im Zusammenhang mit Cloud Volumes ONTAP Ressourcen | Microsoft.Ressourcen/Tags/lesen | Nein | Ja. | Nein |
| | Microsoft.Ressourcen/Tags/schreiben | Ja. | Ja. | Nein |
| | Microsoft.Ressourcen/Tags/delete | Ja. | Nein | Nein |
| Verschlüsselung von Speicherkonten bei der Erstellung | Microsoft.ManagedIdentity/userAssignedIdentities/assign/Action | Ja. | Ja. | Nein |

Globaler Datei-Cache

Der Connector stellt bei Verwendung des globalen Datei-Caches folgende API-Anforderungen vor:

- Microsoft.Insights/Metriken/Lesevorgang
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressourcen/Bereitstellungen/löschen

Kubernetes

Der Connector stellt folgende API-Anforderungen zur Erkennung und Verwaltung von Clustern in Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen
- Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen
- Microsoft.ContainerService/manageCluster/lesen
- Microsoft.ContainerService/verwaltungCluster/listClusterUserCredential/Action

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

Die folgende Berechtigung wurde der JSON-Richtlinie hinzugefügt. Sie ist für Cloud Backup und Cloud Tiering erforderlich.

Microsoft.Storage/StorageAccounts/blobServices/Container/write

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt. Sie werden nicht mehr benötigt.

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/backendAddressPools/join/action
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read
- Microsoft.Storage/StorageAccounts/Generationkey/Aktion

Google Cloud-Berechtigungen für den Connector

Für Aktionen in Google Cloud sind für BlueXP Berechtigungen erforderlich. Diese Berechtigungen sind Bestandteil einer benutzerdefinierten Rolle, die NetApp zur Verfügung stellt. Vielleicht möchten Sie wissen, was BlueXP mit diesen Berechtigungen macht.

Berechtigungen für Dienstkonto

Die unten abgebildete benutzerdefinierte Rolle bietet die Berechtigungen, die ein Connector zur Verwaltung von Ressourcen und Prozessen in Ihrem Google Cloud-Netzwerk benötigt.

Sie müssen diese benutzerdefinierte Rolle auf ein Servicekonto anwenden, das mit der Connector-VM verbunden ist. "[Schritt-für-Schritt-Anleitungen anzeigen](#)".

Außerdem müssen Sie sicherstellen, dass die Rolle auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

```
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

Verwendung von Google Cloud-Berechtigungen

| Aktionen | Zweck |
|---|--|
| <ul style="list-style-type: none"> - Compute.Disks.create - Compute.Disks.createSnapshot - compute.disks.delete - Compute.Disks.get - Compute.Disks.list - compute.disks.setLabels - compute.disks.use | Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - Compute.Firewalls.create - compute.firewalls.delete - Compute.Firewalls.get - Compute.Firewalls.list | Um Firewall-Regeln für Cloud Volumes ONTAP zu erstellen. |

| Aktionen | Zweck |
|---|---|
| - Compute.globalOperations.get | Um den Status von Vorgängen anzuzeigen. |
| - Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly | Um Images für VM-Instanzen zu erhalten. |
| - compute.instances.attachDisk - compute.instances.detachDisk | Zum Verbinden und Trennen von Festplatten mit Cloud Volumes ONTAP. |
| - compute.instances.create - compute.instances.delete | Um Cloud Volumes ONTAP VM-Instanzen zu erstellen und zu löschen. |
| - compute.instances.get | Um VM-Instanzen aufzulisten. |
| - compute.instances.getSerialPortOutput | Um Konsolenprotokolle zu erhalten. |
| - compute.instances.list | Um die Liste der Instanzen in einer Zone abzurufen. |
| - compute.instances.setDeletionProtection | So legen Sie den Löschschutz für die Instanz fest: |
| - compute.instances.setLabels | So fügen Sie Etiketten hinzu: |
| - compute.instances.setMachineType - compute.instances.setMinCpuPlatform | So ändern Sie den Maschinentyp für Cloud Volumes ONTAP. |
| - compute.instances.setMetadata | Um Metadaten hinzuzufügen. |
| - compute.instances.setTags | Um Tags für Firewall-Regeln hinzuzufügen. |
| - compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice | Um Cloud Volumes ONTAP zu starten und anzuhalten. |
| - Compute.machineTypes.get | Um die Anzahl der Kerne zu erhalten, um qouten zu überprüfen. |
| - compute.projects.get | Zur Unterstützung mehrerer Projekte. |
| - Compute.Snapshots.create - compute.snapshots.delete - Compute.Snapshots.get - Compute.Snapshots.list - compute.snapshots.setLabels | Um persistente Festplatten-Snapshots zu erstellen und zu managen. |
| - compute.networks.get - compute.networks.list - Compute.Regions.get - Compute.Regions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.Zones.get - Compute.Zones.list | Um die Netzwerkinformationen zu erhalten, die für die Erstellung einer neuen Instanz einer Cloud Volumes ONTAP Virtual Machine erforderlich sind. |

| Aktionen | Zweck |
|---|---|
| <ul style="list-style-type: none"> - deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - istmentmanager.Manifeste.get - istmentmanager.manifeste.list - istmentmanager.Operations.get - istmentmanager.Operations.list - bereitsmanager.Resources.get - bereitsmanager.Resources.list - Bereitstellungmanager.typeProviders.get - istmentmanager.tyArten.list | Um die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereitzustellen. |
| <ul style="list-style-type: none"> - Logging.logEntries.list - Logging.privateLogEntries.list | Zum Abrufen von Stack-Protokollaufwerken. |
| <ul style="list-style-type: none"> - resourcemanager.projects.get | Zur Unterstützung mehrerer Projekte. |
| <ul style="list-style-type: none"> - Storage.Buckets.create - storage.buckets.delete - Storage.Buckets.get - Storage.Buckets.list - Storage.Buckets.Update | Zur Erstellung und Verwaltung eines Google Cloud Storage Buckets für Daten-Tiering |
| <ul style="list-style-type: none"> - cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.kryptoKeys.get - cloudkms.kryptoKeys.list - cloudkms.Keyrings.list | Verwenden von vom Kunden gemanagten Verschlüsselungen aus dem Cloud-Verschlüsselungsmanagement-Service mit Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - Storage.objects.get - Storage.objects.list | So legen Sie ein Servicekonto für die Cloud Volumes ONTAP-Instanz fest: Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket. |
| <ul style="list-style-type: none"> - Compute.Addresses.list | So rufen Sie die Adressen in einer Region ab, wenn Sie ein HA-Paar bereitstellen. |
| <ul style="list-style-type: none"> - Compute.backendServices.create - Compute.regionBackendServices.create - Compute.regionBackendServices.get - Compute.regionBackendServices.list | Um einen Backend-Service für die Verteilung von Datenverkehr in einem HA-Paar zu konfigurieren |
| <ul style="list-style-type: none"> - compute.networks.updatePolicy | So wenden Sie Firewall-Regeln auf die VPCs und Subnetze für ein HA-Paar an. |
| <ul style="list-style-type: none"> - compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig | Und Cloud-Daten sinnvoll nutzen. |
| <ul style="list-style-type: none"> - Container.Clusters.get - Container.Clusters.list | Um Kubernetes Cluster zu erkennen, die in der Google Kubernetes Engine ausgeführt werden. |
| <ul style="list-style-type: none"> - compute.instanceGroups.get - Compute.Addresses.get | Um Storage VMs auf HA-Paaren zu erstellen und zu managen. |

| Aktionen | Zweck |
|---|---|
| - Monitoring.Timeeries.list - Storage.Buckets.getIamPolicy | Um Informationen zu Google Cloud Storage Buckets zu erhalten. |

Ports

Sicherheitsgruppenregeln in AWS

Für die AWS Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich.

Regeln für eingehende Anrufe

| Protokoll | Port | Zweck |
|-----------|------|--|
| SSH | 22 | Bietet SSH-Zugriff auf den Connector-Host |
| HTTP | 80 | Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche |
| HTTPS | 443 | Bietet HTTPS-Zugriff von Client-Webbrowsern zur lokalen Benutzeroberfläche und Verbindungen aus der Cloud Data Sense Instanz |
| TCP | 3128 | Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. server for AutoSupport messages,Erfahren Sie mehr über den Proxy-Server des Connectors. |
| TCP | 9060 | Ermöglicht die Aktivierung und Nutzung von Cloud Data Sense und Cloud Backup in öffentlicher Cloud-Implementierungen. Dieser Port ist auch für Cloud Backup erforderlich, wenn Sie die SaaS-Schnittstelle in Ihrem BlueXP-Konto deaktivieren. |

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

| Protokoll | Port | Zweck |
|---------------------|------|----------------------------------|
| Alle TCP | Alle | Gesamter abgehender Datenverkehr |
| Alle UDP-Protokolle | Alle | Gesamter abgehender Datenverkehr |

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.



Die Quell-IP-Adresse ist der Connector-Host.

| Service | Protokoll | Port | Ziel | Zweck |
|-----------------------------|-----------|------|--|---|
| API-Aufrufe und AutoSupport | HTTPS | 443 | Outbound-Internet und ONTAP Cluster Management LIF | API-Aufrufe an AWS und ONTAP, Cloud Data Sense, zum Ransomware-Service und dem Senden von AutoSupport-Nachrichten an NetApp |
| API-Aufrufe | TCP | 3000 | ONTAP HA Mediator | Kommunikation mit dem ONTAP HA Mediator |
| | TCP | 8088 | Backup auf S3 | API-Aufrufe zur Sicherung in S3 |
| DNS | UDP | 53 | DNS | Wird für DNS Resolve von BlueXP verwendet |

Für Sicherheitsgruppen gibt es in Azure Regeln

Für die Azure-Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich.

Regeln für eingehende Anrufe

| Protokoll | Port | Zweck |
|-----------|------|--|
| SSH | 22 | Bietet SSH-Zugriff auf den Connector-Host |
| HTTP | 80 | Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche |
| HTTPS | 443 | Bietet HTTPS-Zugriff von Client-Webbrowsern zur lokalen Benutzeroberfläche und Verbindungen aus der Cloud Data Sense Instanz |

| Protokoll | Port | Zweck |
|-----------|------|--|
| TCP | 3128 | Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. server for AutoSupport messages,Erfahren Sie mehr über den Proxy-Server des Connectors. |
| TCP | 9060 | Ermöglicht die Aktivierung und Nutzung von Cloud Data Sense und Cloud Backup in öffentlicher Cloud-Implementierungen. Dieser Port ist auch für Cloud Backup erforderlich, wenn Sie die SaaS-Schnittstelle in Ihrem BlueXP-Konto deaktivieren. |

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

| Protokoll | Port | Zweck |
|---------------------|------|----------------------------------|
| Alle TCP | Alle | Gesamter abgehender Datenverkehr |
| Alle UDP-Protokolle | Alle | Gesamter abgehender Datenverkehr |

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.



Die Quell-IP-Adresse ist der Connector-Host.

| Service | Protokoll | Port | Ziel | Zweck |
|-----------------------------|-----------|------|--|---|
| API-Aufrufe und AutoSupport | HTTPS | 443 | Outbound-Internet und ONTAP Cluster Management LIF | API-Aufrufe an Azure und ONTAP, Cloud Data Sense, zum Ransomware-Service und Senden von AutoSupport-Nachrichten an NetApp |
| DNS | UDP | 53 | DNS | Wird für DNS Resolve von BlueXP verwendet |

Firewall-Regeln in Google Cloud

Die Google Cloud Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

| Protokoll | Port | Zweck |
|-----------|------|--|
| SSH | 22 | Bietet SSH-Zugriff auf den Connector-Host |
| HTTP | 80 | Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche |
| HTTPS | 443 | Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche |
| TCP | 3128 | Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. server for AutoSupport messages,Erfahren Sie mehr über den Proxy-Server des Connectors. |

Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector öffnen den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector enthalten die folgenden ausgehenden Regeln.

| Protokoll | Port | Zweck |
|---------------------|------|----------------------------------|
| Alle TCP | Alle | Gesamter abgehender Datenverkehr |
| Alle UDP-Protokolle | Alle | Gesamter abgehender Datenverkehr |

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor

erforderlich sind.



Die Quell-IP-Adresse ist der Connector-Host.

| Service | Protokoll | Port | Ziel | Zweck |
|-----------------------------|-----------|------|--|--|
| API-Aufrufe und AutoSupport | HTTPS | 443 | Outbound-Internet und ONTAP Cluster Management LIF | API-Aufrufe bei GCP und ONTAP, Cloud Data Sense, zum Ransomware-Service und dem Senden von AutoSupport Nachrichten an NetApp |
| DNS | UDP | 53 | DNS | Wird für DNS Resolve von BlueXP verwendet |

Anschlüsse für den On-Prem Connector

Der Connector verwendet die folgenden *Inbound*-Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird.

Diese eingehenden Regeln gelten für beide Bereitstellungsmodelle für den On-Prem Connector: Installiert mit Internetzugang oder ohne Internetzugang.

| Protokoll | Port | Zweck |
|-----------|------|---|
| HTTP | 80 | Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche |
| HTTPS | 443 | Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche |

Wissen und Support

Für den Support anmelden

Bevor Sie einen Support-Fall beim technischen Support von NetApp eröffnen können, müssen Sie BlueXP einen NetApp Support Site Account (NSS) hinzufügen und sich dann für den Support registrieren.

Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren Ihres BlueXP-Konto-ID-Support-Abonnements (Ihre 20-stellige Seriennummer 960xxxxxxxxx auf der Seite Support-Ressourcen in BlueXP).

Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

Diese Seriennummern werden als *PAYGO Seriennummern* bezeichnet und werden zum Zeitpunkt der Cloud Volumes ONTAP Implementierung von BlueXP generiert.

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen.

Ihre Anmeldung hängt davon ab, ob Sie ein neuer oder bereits bestehender Kunde oder Partner sind.

- Bestehender Kunde oder Partner

Als bestehender NetApp Kunde oder Partner können Sie mit Ihrem NSS SSO-Konto (NetApp Support Site) die oben genannten Registrierungen durchführen. Im Support Dashboard stellt BlueXP eine **NSS Management**-Seite zur Verfügung, auf der Sie Ihr NSS-Konto hinzufügen können. Sobald Sie Ihr NSS-Konto hinzugefügt haben, registriert BlueXP diese Seriennummern automatisch für Sie.

an NSS account to BlueXP, Erfahren Sie, wie Sie Ihr NSS-Konto hinzufügen.

- Neu bei NetApp

Wenn Sie neu bei NetApp sind, müssen Sie eine einmalige Registrierung Ihrer BlueXP Account ID Seriennummer auf der Support-Registrierungsseite von NetApp abschließen. Sobald Sie diese Registrierung abgeschlossen und ein neues NSS-Konto erstellt haben, können Sie dieses Konto in BlueXP verwenden, um sich in Zukunft automatisch zu registrieren.

with NetApp, Erfahren Sie, wie Sie sich mit NetApp anmelden können.

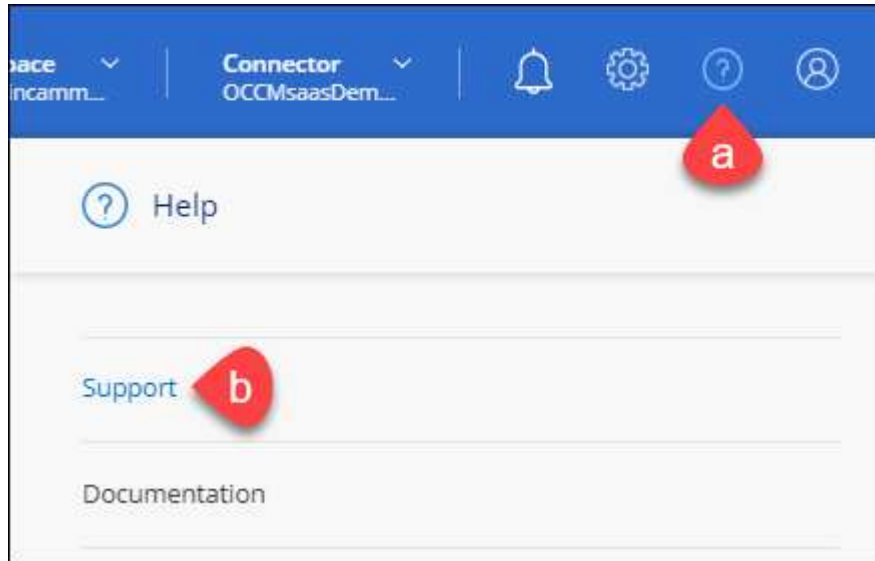
Fügen Sie ein NSS-Konto zu BlueXP hinzu

Über das Support Dashboard können Sie Ihre NetApp Support Site Konten zur Verwendung mit BlueXP hinzufügen und managen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie einen Partner- oder Reseller-Account haben, können Sie ein oder mehrere NSS-Konten hinzufügen, können aber nicht neben Kunden-Level Accounts hinzugefügt werden.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Klicken Sie auf **NSS Management > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

Beachten Sie Folgendes:

- Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
- Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern. Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet wird. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ... Menü.
- Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ... Menü. Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden.

Mit NetApp registrieren

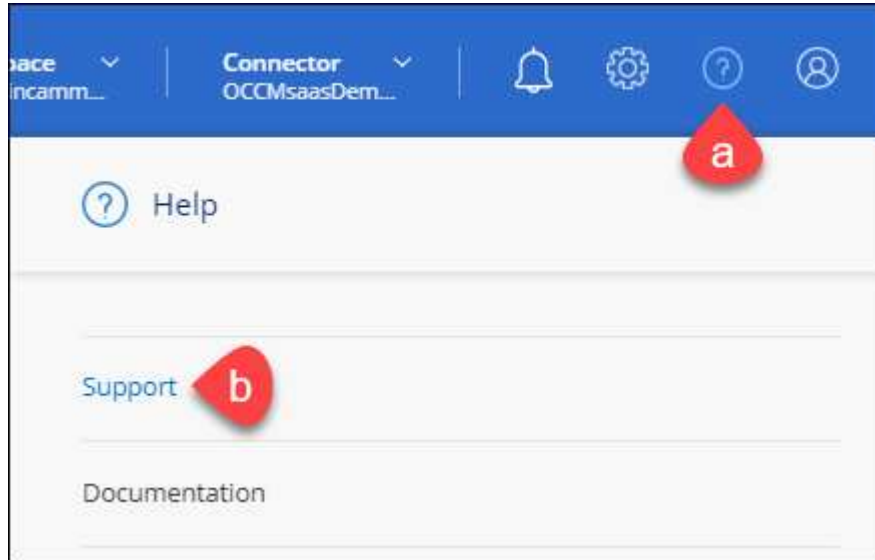
Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

Bestandskunde mit NSS-Konto

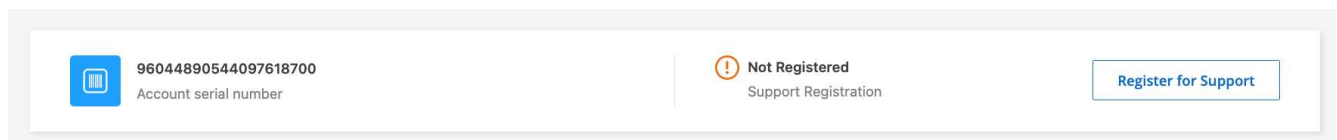
Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Wenn Sie dies noch nicht getan haben, fügen Sie Ihr NSS-Konto bei BlueXP hinzu.
3. Klicken Sie auf der Seite **Ressourcen** auf **für Support registrieren**.



Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits Kunde von NetApp mit vorhandenen Lizenzen und Seriennummern sind, aber *no* NSS Konto, müssen Sie nur ein NSS-Konto erstellen.

Schritte

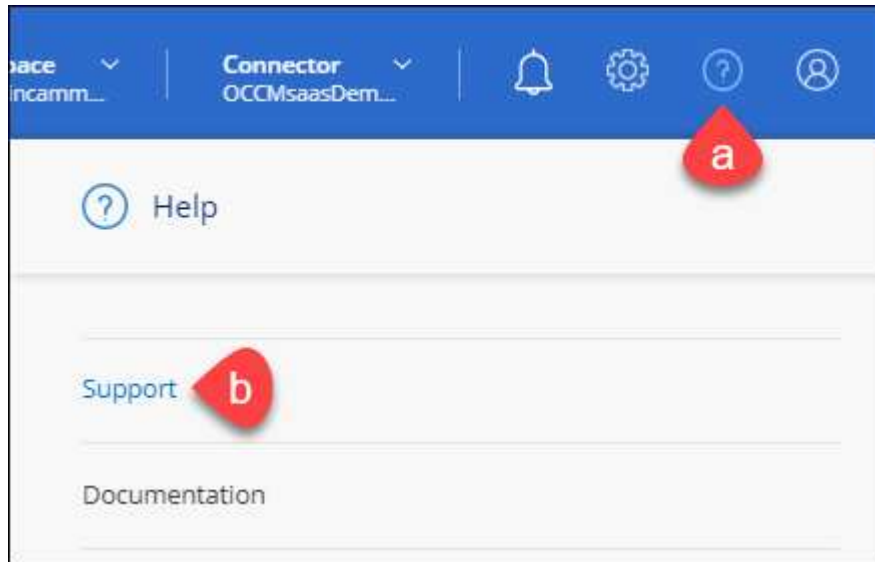
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "[NetApp Support Site-Formular zur Benutzerregistrierung](#)"
 - a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
 - b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.

Neu bei NetApp

Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.



3. Navigieren Sie zu "[Die Support-Registrierungs-Website von NetApp](#)" Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

7. Bestätigen Sie die Aktion in der E-Mail.

Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "[NetApp Support Site-Formular zur Benutzerregistrierung](#)"
 - a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
 - b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch

wird die Kontobearbeitung beschleunigt.

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Sobald Sie Ihren NetApp Support Site Account besitzen, können Sie im Portal BlueXP diesen NSS-Account für zukünftige Registrierungen hinzufügen.

Holen Sie sich Hilfe

NetApp bietet Unterstützung für BlueXP und seine Cloud-Services auf unterschiedliche Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Self-Support

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- ["Wissensdatenbank"](#)

Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- ["Communitys"](#)

Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

- Dokumentation

Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- [Mailto:ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)[Feedback email]

Wir wissen Ihre Vorschläge zu schätzen. Senden Sie uns Ihr Feedback, um BlueXP zu verbessern.

NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

Um die * Case erstellen*-Fähigkeit zu verwenden, müssen Sie zuerst eine einmalige Registrierung Ihrer BlueXP Account ID-Seriennummer (dh 960xxxx) mit NetApp ["Erfahren Sie, wie Sie sich für Support registrieren"](#).

Schritte

1. Klicken Sie in BlueXP auf **Hilfe > Support**.
2. Wählen Sie eine der verfügbaren Optionen unter Technical Support:
 - a. Klicken Sie auf **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.
 - b. Klicken Sie auf **Case erstellen**, um ein Ticket mit einem NetApp Support-Experten zu öffnen:

- **NetApp Support Site Account:** Wählen Sie das entsprechende NSS-Konto für die Person aus, die den Support-Case eröffnet. Diese Person ist der primäre Ansprechpartner bei NetApp, der Sie sich zusätzlich zu den unten aufgeführten zusätzlichen E-Mails mit anderen Kunden in Verbindung setzen kann.

Wenn Ihr NSS-Konto nicht angezeigt wird, können Sie im Support-Bereich von BlueXP zur Registerkarte **NSS Management** navigieren, um es dort hinzuzufügen.

- **Service:** Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
- **Arbeitsumgebung:** Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Case Priority:** Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung:** Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen:** Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.

Create a Case

TESTCLOUD2NTAP
✎

NetApp Support Site Account

Service

Working Environment

Cloud Manager ▼

Select... ▼

Case Priority

i

Low- General Guidance ▼

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) i

Attachment (Optional) Coming Soon

No files selected

↑

Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall und macht Sie umgehend mit.

Für eine Historie Ihrer Supportfälle können Sie auf **Einstellungen > Timeline** klicken und nach Aktionen mit dem Namen „Support Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Service zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh

960xxx) oder Seriennummer der Arbeitsumgebung. Sie können Ihre Liste der NSS-Konten oben im **Case erstellen**-Formular überprüfen, um die richtige Übereinstimmung zu finden, oder Sie können Hilfe mit einer der folgenden Optionen suchen:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter <https://mysupport.netapp.com/site/help>

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

<http://www.netapp.com/us/legal/copyright.aspx>

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

<https://www.netapp.com/us/media/patents-page.pdf>

Datenschutzrichtlinie

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- ["Hinweis für BlueXP"](#)

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.