# Anschlüsse

## Setup and administration

NetApp
April 26, 2024

# Inhalt

# Anschlüsse

## Suchen Sie die System-ID für einen Anschluss

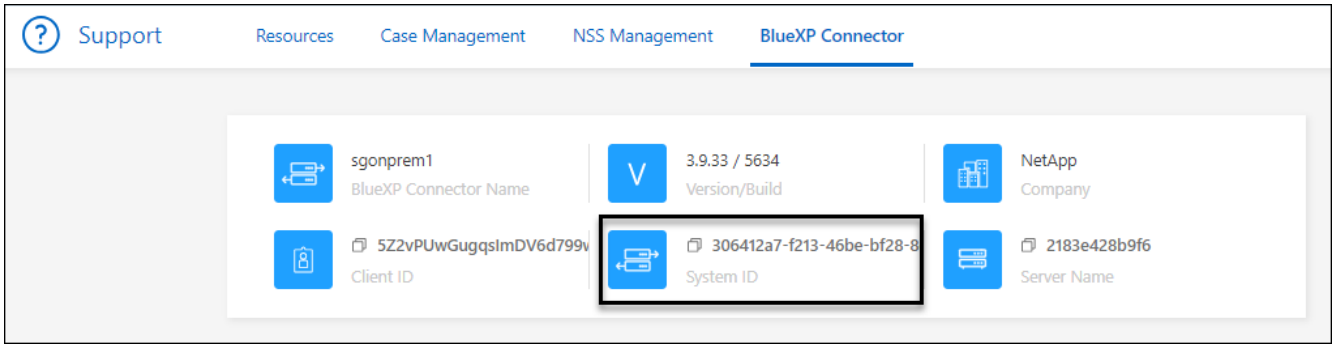
Um Ihnen bei den ersten Schritten zu helfen, fragen Sie möglicherweise Ihr NetApp Ansprechpartner nach der System-ID Ihres Connectors. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

**Schritte**

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol aus.
2. Wählen Sie **Support > BlueXP Connector**.

   Die System-ID wird oben auf der Seite angezeigt.

   **Beispiel**




## Verwalten Sie vorhandene Anschlüsse

Nachdem Sie einen Connector erstellt haben, müssen Sie ihn möglicherweise ab und zu verwalten. Sie können beispielsweise zwischen den Anschlüssen wechseln, wenn Sie über mehrere verfügen. Oder Sie müssen den Connector möglicherweise manuell aktualisieren, wenn Sie BlueXP im privaten Modus verwenden.

"Erfahren Sie, wie Anschlüsse funktionieren".

> Der Connector enthält eine lokale Benutzeroberfläche, auf die über den Connector-Host zugegriffen werden kann. Diese UI steht Kunden zur Verfügung, die BlueXP im eingeschränkten Modus oder im privaten Modus verwenden. Wenn Sie BlueXP im Standardmodus verwenden, sollten Sie über die auf die Benutzeroberfläche zugreifen "BlueXP SaaS-Konsole"
>
> "Weitere Informationen zu BlueXP Implementierungsmodi".

### Betriebssystem- und VM-Wartung

Die Wartung des Betriebssystems auf dem Connector-Host liegt in Ihrer Verantwortung. Sie sollten beispielsweise Sicherheitsupdates auf dem Betriebssystem auf dem Connector-Host anwenden, indem Sie die Standardverfahren Ihres Unternehmens für die Betriebssystemverteilung befolgen.

Beachten Sie, dass Sie keine Dienste auf dem Connector-Host anhalten müssen, wenn Sie ein Betriebssystem-Update ausführen.

Wenn Sie die Connector VM anhalten und dann starten müssen, sollten Sie dies über die Konsole Ihres Cloud-Providers oder mithilfe der Standardverfahren für das On-Premises-Management tun.

"Beachten Sie, dass der Connector jederzeit betriebsbereit sein muss".

## VM oder Instanztyp

Wenn Sie einen Connector direkt aus BlueXP erstellt haben, hat BlueXP eine Virtual Machine-Instanz in Ihrem Cloud-Provider implementiert, die eine Standardkonfiguration verwendet. Nachdem Sie den Connector erstellt haben, sollten Sie nicht zu einer kleineren VM-Instanz wechseln, die weniger CPU oder RAM hat.

Die CPU- und RAM-Anforderungen lauten wie folgt:

**CPU**

4 Kerne oder 4 vCPUs

**RAM**

14 GB

"Informieren Sie sich über die Standardkonfiguration des Connectors".

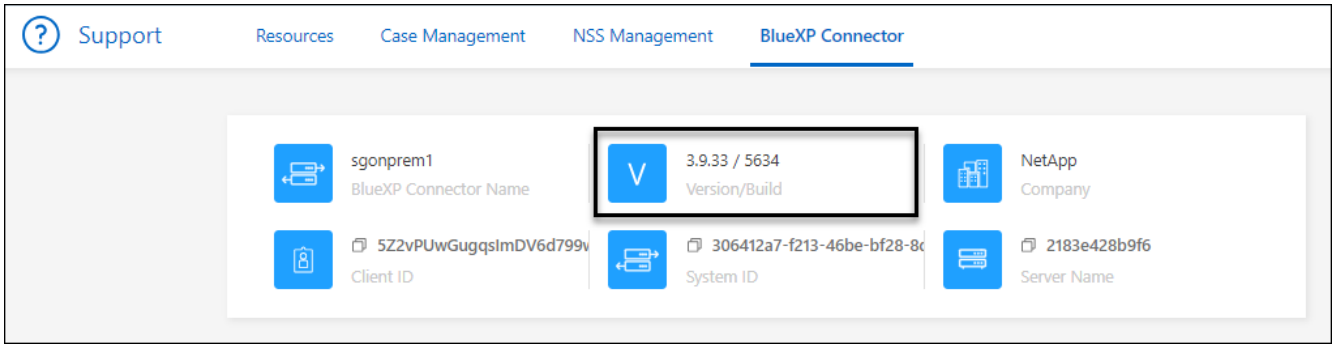
## Anzeigen der Version eines Connectors

Sie können die Version Ihres Connectors anzeigen, um zu überprüfen, ob der Connector automatisch auf die neueste Version aktualisiert wurde, oder weil Sie ihn mit Ihrem NetApp-Vertreter teilen müssen.

**Schritte**

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol aus.
2. Wählen Sie **Support > BlueXP Connector**.

   Die Version wird oben auf der Seite angezeigt.




## Zwischen den Anschlüssen wechseln

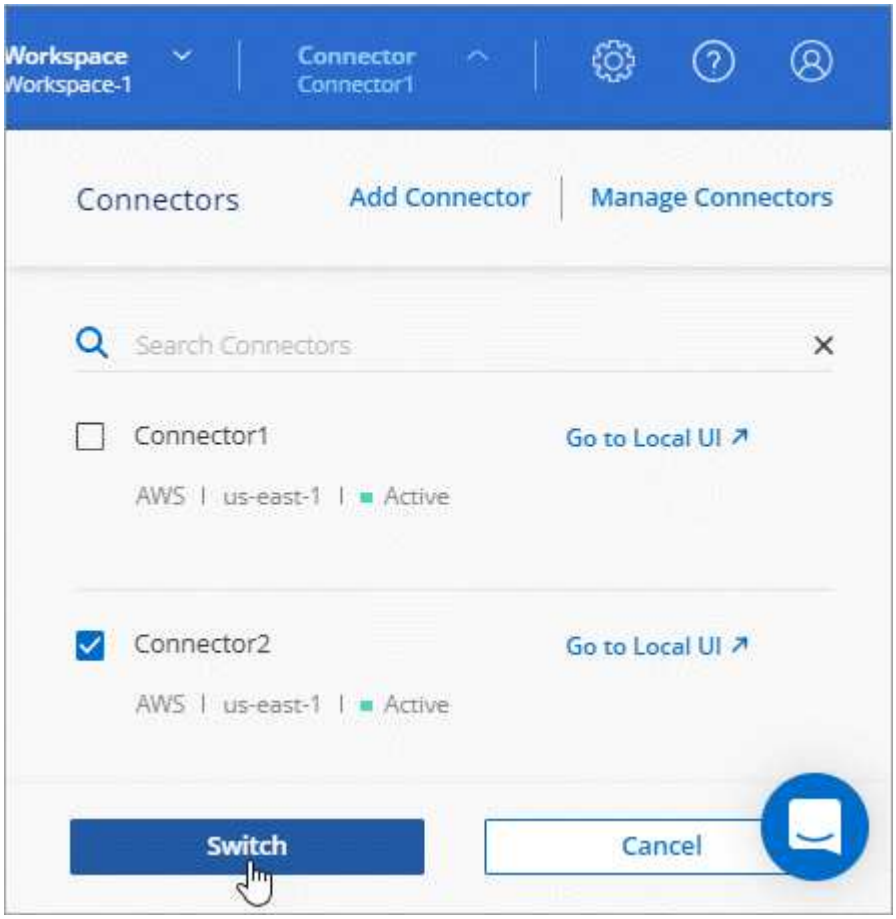
Wenn Sie über mehrere Anschlüsse verfügen, können Sie zwischen diesen wechseln, um die Arbeitsumgebungen zu sehen, die mit einem bestimmten Konnektor verknüpft sind.

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. Wählen Sie die Dropdown-Liste **Connector** aus, wählen Sie einen anderen Konnektor aus und wählen Sie dann **Switch** aus.




**Ergebnis**

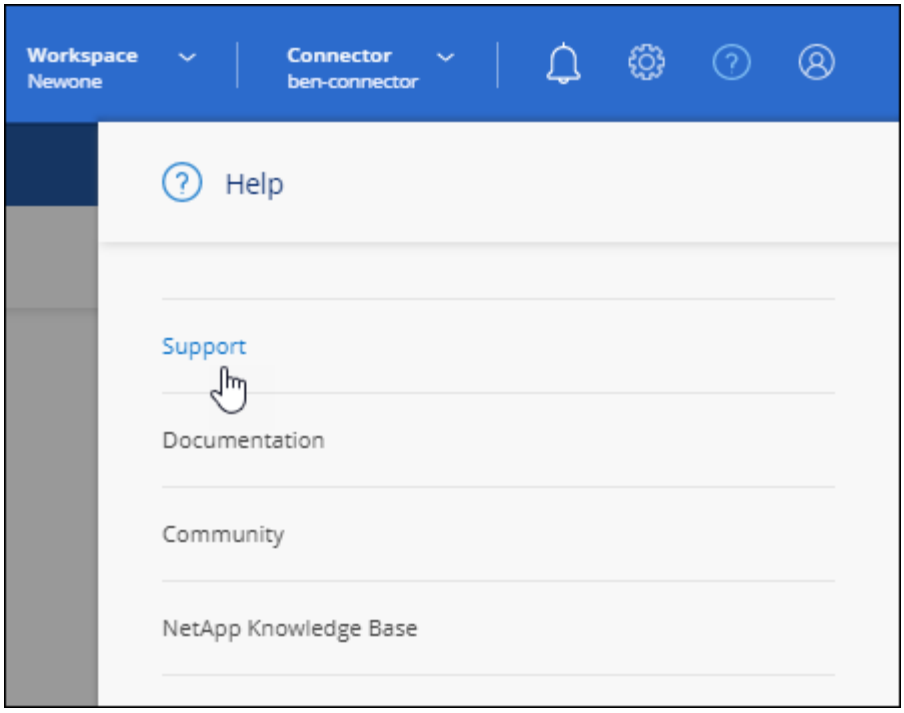
BlueXP aktualisiert und zeigt die Arbeitsumgebungen, die mit dem ausgewählten Connector verknüpft sind.

## 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**

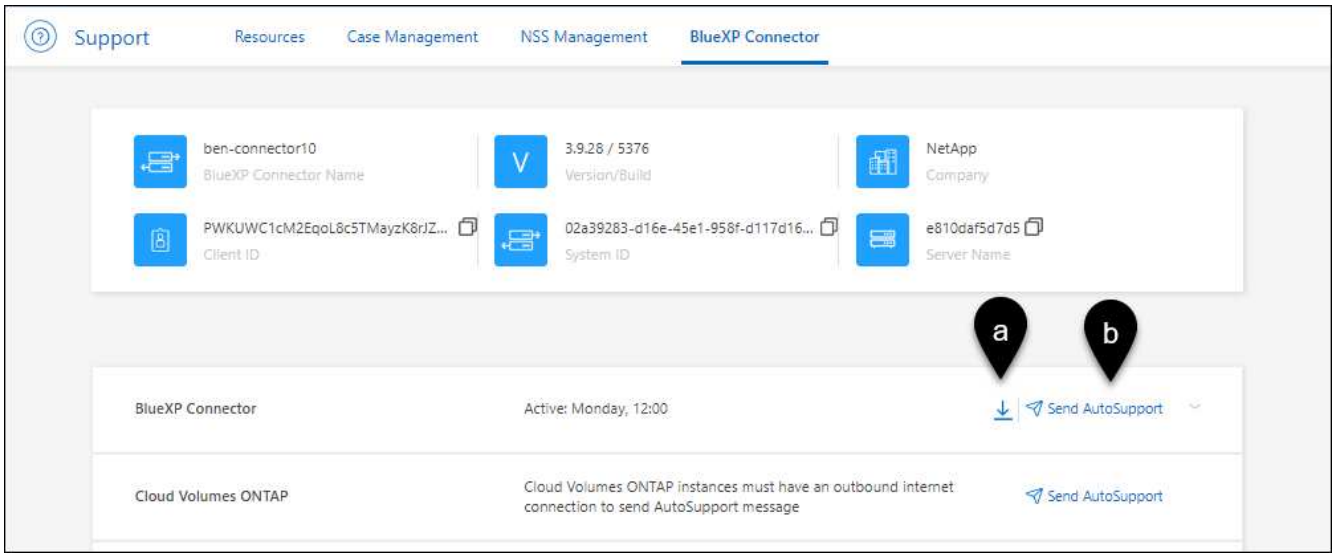
1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.




2. Wählen Sie **BlueXP Connector** aus.
3. 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. Wählen Sie **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. Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).

"AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"

**Azure**

Beim Erstellen der Connector-VM in Azure haben Sie einen Benutzernamen angegeben und sich für die Authentifizierung mit einem Kennwort oder einem öffentlichen SSH-Schlüssel entschieden. 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 (gcloudd) herstellen.

"Google Cloud Docs: Verbindung zu Linux-VMs herstellen"

## Erfordern die Verwendung von IMDSv2 auf Amazon EC2 Instanzen

Ab März 2024 unterstützt BlueXP jetzt den Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) mit dem Connector und Cloud Volumes ONTAP (einschließlich des Mediators für HA-Implementierungen). In den meisten Fällen wird IMDSv2 automatisch auf neuen EC2-Instanzen konfiguriert. IMDSv1 wurde vor März 2024 aktiviert. Falls dies durch Ihre Sicherheitsrichtlinien erforderlich ist, müssen Sie IMDSv2 möglicherweise manuell auf Ihren EC2-Instanzen konfigurieren.

### Über diese Aufgabe

IMDSv2 bietet einen verbesserten Schutz vor Schwachstellen. "Weitere Informationen zu IMDSv2 finden Sie im AWS Security Blog"

Der Instance Metadata Service (IMDS) wird in EC2-Instanzen wie folgt aktiviert:

- Für neue Connector-Implementierungen von BlueXP oder durch die Nutzung von "Terraform-Skripte", IMDSv2 ist standardmäßig auf der EC2-Instanz aktiviert.
- Wenn Sie eine neue EC2-Instanz in AWS starten und dann die Connector-Software manuell installieren, ist IMDSv2 standardmäßig ebenfalls aktiviert.
- Wenn Sie den Connector vom AWS Marketplace starten, ist IMDSv1 standardmäßig aktiviert. Sie können IMDSv2 auf der EC2-Instanz manuell konfigurieren.
- Für bestehende Connectors wird IMDSv1 weiterhin unterstützt, Sie können IMDSv2 jedoch manuell auf der EC2-Instanz konfigurieren, wenn Sie dies wünschen.
- Für Cloud Volumes ONTAP ist IMDSv1 standardmäßig auf neuen und bestehenden Instanzen aktiviert. Sie können IMDSv2 auf den EC2-Instanzen manuell konfigurieren, wenn Sie möchten.

### Bevor Sie beginnen

- Die Connector-Version muss 3.9.38 oder höher sein.
- Cloud Volumes ONTAP muss eine der folgenden Versionen ausführen:

- 9.12.1 P2 (oder jedes weitere Patch)
- 9.13.0 P4 (oder jedes weitere Patch)
- 9.13.1 oder eine beliebige Version nach dieser Version

- Diese Änderung erfordert einen Neustart der Cloud Volumes ONTAP-Instanzen.

**Über diese Aufgabe**

Für diese Schritte ist die Verwendung der AWS CLI erforderlich, da Sie das Limit für den Response-Hop auf 3 ändern müssen.

**Schritte**

1. Erfordern die Verwendung von IMDSv2 auf der Connector-Instanz:

   a. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.

      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. Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername ec2-user).

      "AWS Docs: Stellen Sie eine Verbindung zu Ihrer Linux-Instanz her"

   b. Installieren Sie die AWS CLI.

      "AWS Docs: Installieren oder aktualisieren Sie auf die neueste Version der AWS CLI"

   c. Verwenden Sie die `aws ec2 modify-instance-metadata-options` Befehl, um die Verwendung von IMDSv2 zu erfordern und das PUT Response Hop Limit auf 3 zu ändern.

      **Beispiel**

      ```
      aws ec2 modify-instance-metadata-options \
          --instance-id <instance-id> \
          --http-put-response-hop-limit 3 \
          --http-tokens required \
          --http-endpoint enabled
      ```

      Der `http-tokens` Parameter setzt IMDSv2 auf erforderlich. Wenn `http-tokens` Ist erforderlich, müssen Sie auch festlegen `http-endpoint` Auf aktiviert.

2. Erfordern die Verwendung von IMDSv2 auf Cloud Volumes ONTAP Instanzen:

   a. Wechseln Sie zum "Amazon EC2 Konsole"

   b. Wählen Sie im Navigationsbereich **instances** aus.

   c. Wählen Sie eine Cloud Volumes ONTAP-Instanz aus.

   d. Wählen Sie **Aktionen > Instanzeinstellungen > Optionen für Instanzmetadaten ändern**.

   e. Wählen Sie im Dialogfeld **Modify Instance Metadata options** Folgendes aus:

      - Wählen Sie für **Instance Metadata Service enable** aus.

    - Wählen Sie für **IMDSv2 required** aus.
    - Wählen Sie **Speichern**.
  f. Wiederholen Sie diese Schritte für andere Cloud Volumes ONTAP Instanzen, einschließlich des HA Mediators.
  g. "Stoppen und starten Sie die Cloud Volumes ONTAP-Instanzen"

**Ergebnis**

Die Connector-Instanz und die Cloud Volumes ONTAP-Instanzen sind jetzt so konfiguriert, dass sie IMDSv2 verwenden.

## Aktualisieren Sie den Connector, wenn Sie den privaten Modus verwenden

Wenn Sie BlueXP im privaten Modus nutzen, können Sie den Connector aktualisieren, wenn eine neuere Version von der NetApp Support Site verfügbar ist.

Der Connector muss während des Upgrade-Vorgangs neu gestartet werden, damit die webbasierte Konsole während des Upgrades nicht verfügbar ist.

> Wenn Sie BlueXP im Standardmodus oder im eingeschränkten Modus verwenden, aktualisiert der Connector seine Software automatisch auf die neueste Version, sofern er über ausgehenden Internetzugang verfügt, um das Softwareupdate zu erhalten.

**Schritte**

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

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

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

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

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

4. Führen Sie das Installationsskript aus:

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

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

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

## 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.

   Sie müssen den Backup-Speicherort für jedes Cloud Volumes ONTAP-System aktualisieren.

   a. Führen Sie den folgenden Befehl über die Cloud Volumes ONTAP-CLI aus, um das aktuelle Backup-Ziel anzuzeigen:

   ```
   system configuration backup show
   ```

   b. Führen Sie den folgenden Befehl aus, um die IP-Adresse für das Backup-Ziel zu aktualisieren:

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

## Bearbeiten Sie die URIs eines Connectors

Fügen Sie den Uniform Resource Identifier (URI) für einen Connector hinzu und entfernen Sie ihn.

**Schritte**

1. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.
2. Wählen Sie **Connectors Verwalten**.
3. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **URIs bearbeiten**.
4. Fügen Sie URIs hinzu und entfernen Sie sie, und wählen Sie dann **Apply**.

## 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"

## Entfernen Sie die Anschlüsse von BlueXP

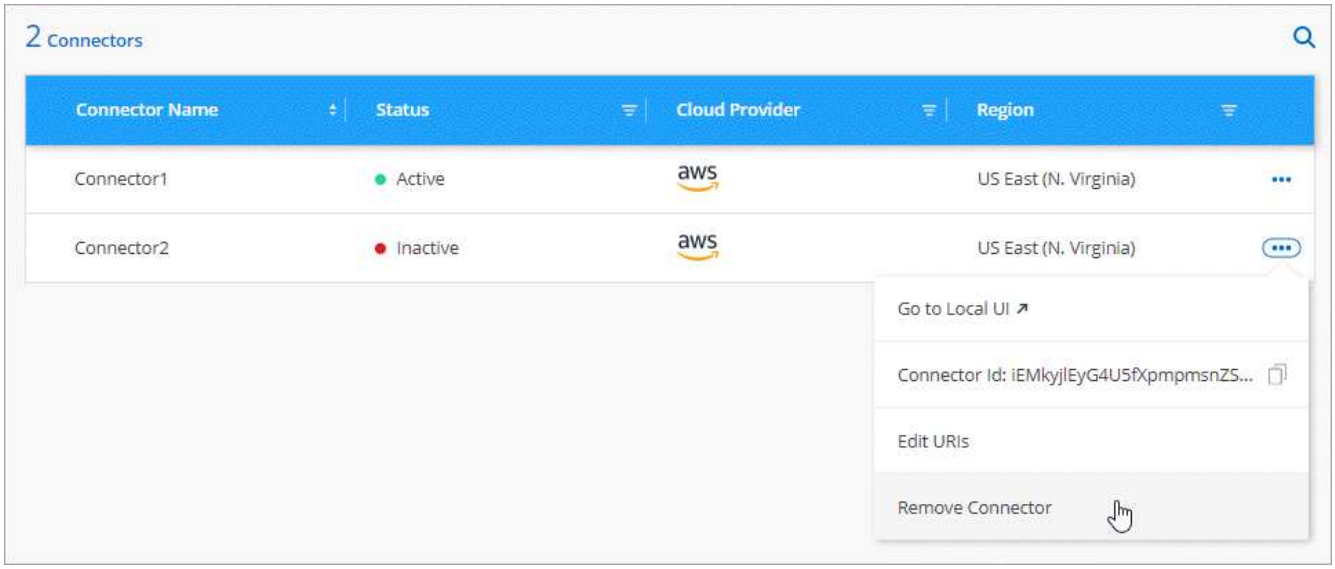
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in BlueXP entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

Beachten Sie Folgendes zum Entfernen eines Konnektors:

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

**Schritte**

1. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.
2. Wählen Sie **Connectors Verwalten**.
3. Wählen Sie das Aktionsmenü für einen inaktiven Konnektor aus und wählen Sie **Connector entfernen**.




4. Geben Sie den Namen des zu bestätigten Connectors ein, und wählen Sie dann **Entfernen**.

**Ergebnis**

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 (Standardmodus oder eingeschränkter Modus) oder auf einem Host in einem Netzwerk ohne Internetzugang (privater Modus) installiert haben.

#### Deinstallieren, wenn Sie den Standardmodus oder den eingeschränkten Modus verwenden

Mit den folgenden Schritten können Sie die Connector-Software deinstallieren, wenn Sie BlueXP im Standardmodus oder im eingeschränkten Modus verwenden.

**Schritte**

1. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.
2. Führen Sie auf dem Linux-Host das Deinstallationsskript aus:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

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

#### Deinstallieren Sie die Software, wenn Sie den privaten Modus verwenden

Mit den folgenden Schritten können Sie die Connector-Software deinstallieren, wenn Sie BlueXP im privaten Modus verwenden, auf den kein Internetzugang verfügbar ist.

**Schritte**

1. Stellen Sie eine Verbindung zur Linux-VM für den Connector her.
2. Führen Sie auf dem Linux-Host die folgenden Befehle aus:

   ```
   ./opt/application/netapp/ds/cleanup.sh
   rm -rf /opt/application/netapp/ds
   ```

# Installieren Sie ein HTTPS-Zertifikat für sicheren Zugriff

Standardmäßig verwendet BlueXP ein selbstsigniertes Zertifikat für HTTPS-Zugriff auf die Webkonsole. Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle signiertes Zertifikat installieren, das einen besseren Schutz bietet als ein selbstsigniertes Zertifikat.

## Bevor Sie beginnen

Sie müssen einen Konnektor erstellen, bevor Sie BlueXP-Einstellungen ändern können. "Erfahren Sie, wie".

## Installieren Sie ein HTTPS-Zertifikat

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

**Schritte**

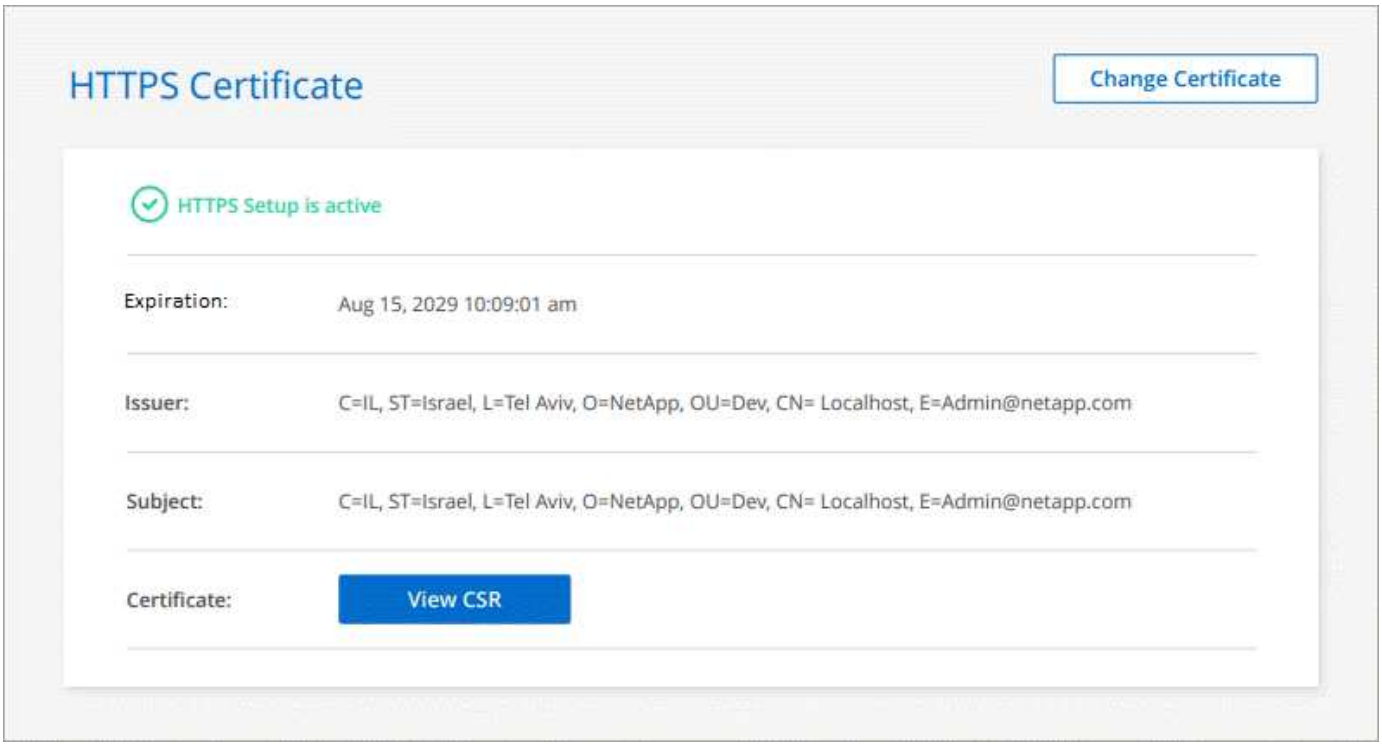
1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS Setup** aus.

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

**Ergebnis**

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 Sie das BlueXP HTTPS-Zertifikat

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 auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS Setup** aus.

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

2. Wählen Sie **Zertifikat ändern** und folgen Sie den Schritten, um eine CSR zu generieren oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

**Ergebnis**

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

# Konfigurieren Sie einen Konnektor für die Verwendung eines Proxy-Servers

Wenn Sie in Ihren Unternehmensrichtlinien einen Proxyserver für die gesamte Kommunikation mit dem Internet verwenden müssen, müssen Sie Ihre Connectors so konfigurieren, dass sie diesen Proxy-Server verwenden. Wenn Sie während der Installation keinen Connector so konfiguriert haben, dass er einen Proxyserver verwendet, können Sie den Connector so konfigurieren, dass er diesen Proxyserver verwendet.

Wenn der Connector für die Verwendung eines Proxy-Servers konfiguriert wird, erhält der ausgehende Internetzugriff, wenn eine öffentliche IP-Adresse oder ein NAT-Gateway nicht 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. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

## Unterstützte Konfigurationen

- BlueXP unterstützt HTTP und HTTPS.
- Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.
- BlueXP unterstützt keine transparenten Proxyserver.

## 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 Vorgänge ausführt, bevor Sie fortfahren.

**Schritte**

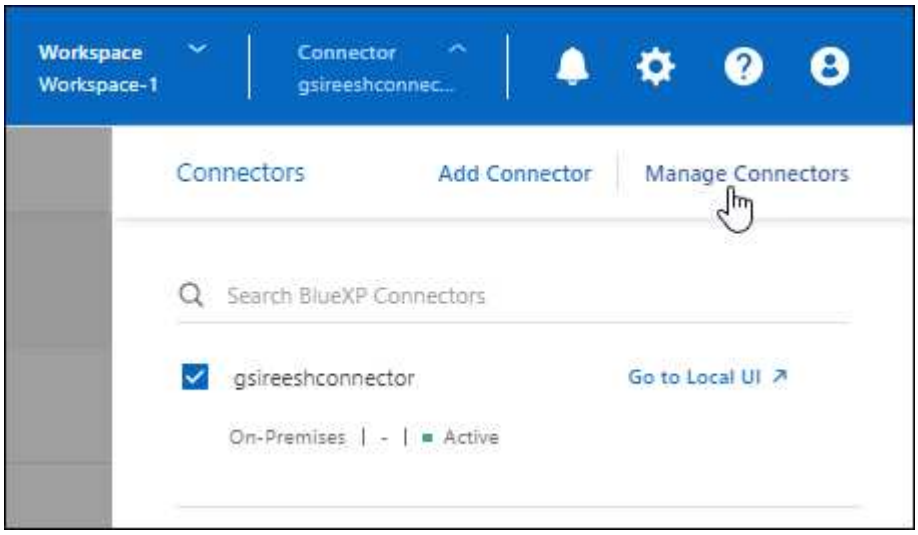
1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**.

   Die Navigation hängt davon ab, ob Sie BlueXP im Standardmodus (Zugriff auf die BlueXP Schnittstelle über die SaaS-Website) oder BlueXP im eingeschränkten Modus oder privaten Modus nutzen (lokaler Zugriff auf die BlueXP Schnittstelle vom Connector-Host aus).

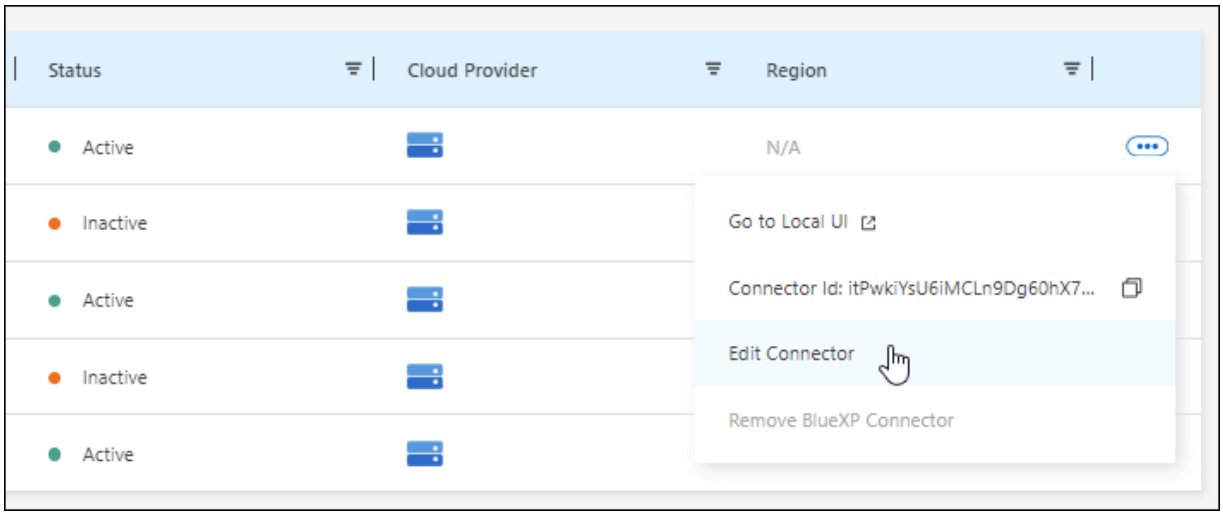
**Standardmodus**

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connectors Verwalten**.



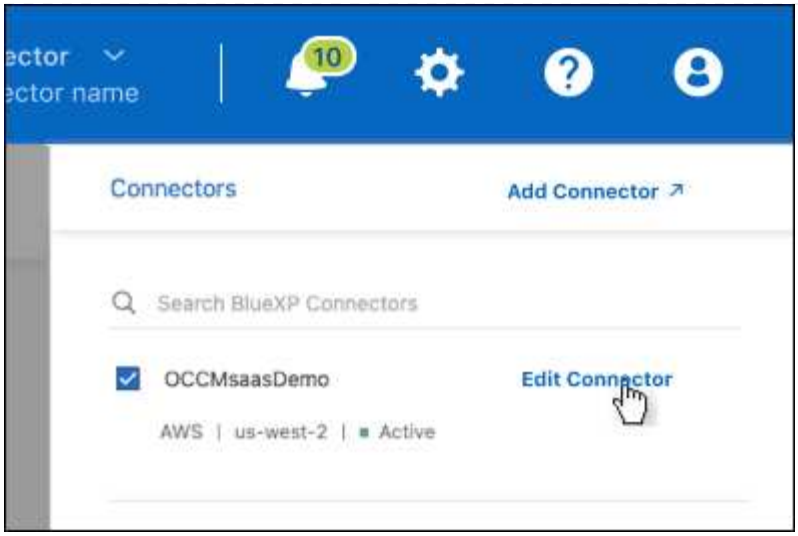

c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.




**Eingeschränkter oder privater Modus**

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connector Bearbeiten**.




2. Wählen Sie **HTTP Proxy Configuration** aus.
3. Richten Sie den Proxy ein:
   a. Wählen Sie **Proxy Aktivieren**.
   b. Geben Sie den Server mithilfe der Syntax an <a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a> Oder <a href="https://<em>address:port</em>" class="bare">https://<em>address:port</em></a>
   c. Geben Sie einen Benutzernamen und ein Kennwort an, wenn eine grundlegende Authentifizierung für den Server erforderlich ist.

      Beachten Sie Folgendes:

      - Der Benutzer kann ein lokaler Benutzer oder ein Domänenbenutzer sein.
      - Für einen Domänenbenutzer müssen Sie den ASCII-Code für den \ wie folgt eingeben: Domain-Name%92user-Name

        Beispiel: netapp%92Proxy

      - BlueXP unterstützt keine Passwörter, die das Zeichen @ enthalten.
   d. Wählen Sie **Speichern**.

## Aktivieren Sie direkten API-Verkehr

Wenn Sie einen Connector für die Verwendung eines Proxy-Servers konfiguriert haben, können Sie direkten API-Datenverkehr auf dem Connector aktivieren, um API-Aufrufe direkt an Cloud-Provider-Dienste zu senden, ohne über den Proxy zu gehen. Diese Option wird mit Connectors unterstützt, die in AWS, in Azure oder in Google Cloud ausgeführt werden.

Wenn Sie die Verwendung von privaten Azure-Links mit Cloud Volumes ONTAP deaktiviert und stattdessen Service-Endpunkte verwenden, müssen Sie direkten API-Datenverkehr aktivieren. Andernfalls wird der Datenverkehr nicht korrekt geleitet.

"Weitere Informationen zur Verwendung eines Azure Private Links oder von Service-Endpunkten mit Cloud Volumes ONTAP"

**Schritte**

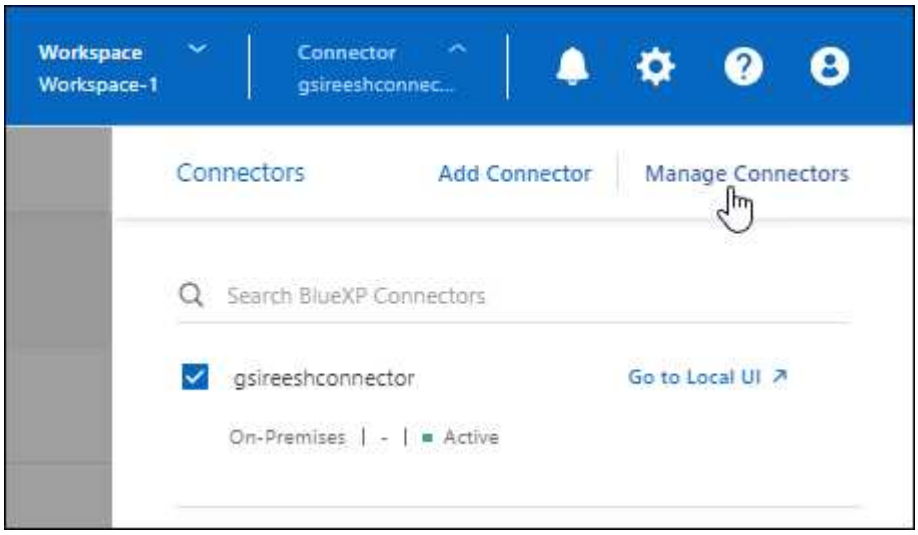
1. Navigieren Sie zur Seite **BlueXP Connector bearbeiten**:

   Die Navigation hängt davon ab, ob Sie BlueXP im Standardmodus (Zugriff auf die BlueXP Schnittstelle über die SaaS-Website) oder BlueXP im eingeschränkten Modus oder privaten Modus nutzen (lokaler Zugriff auf die BlueXP Schnittstelle vom Connector-Host aus).

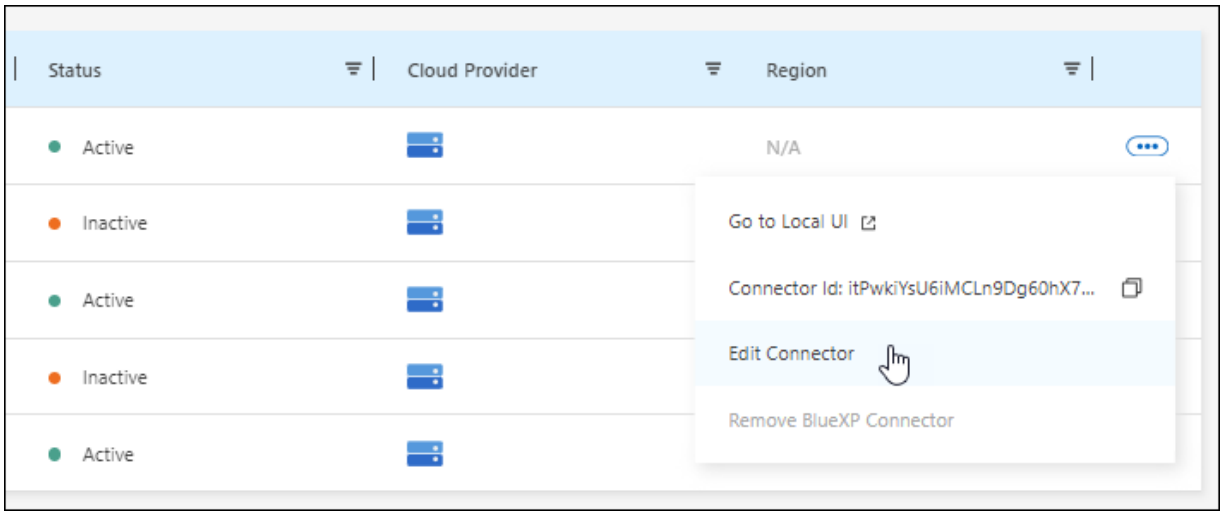
**Standardmodus**

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connectors Verwalten**.



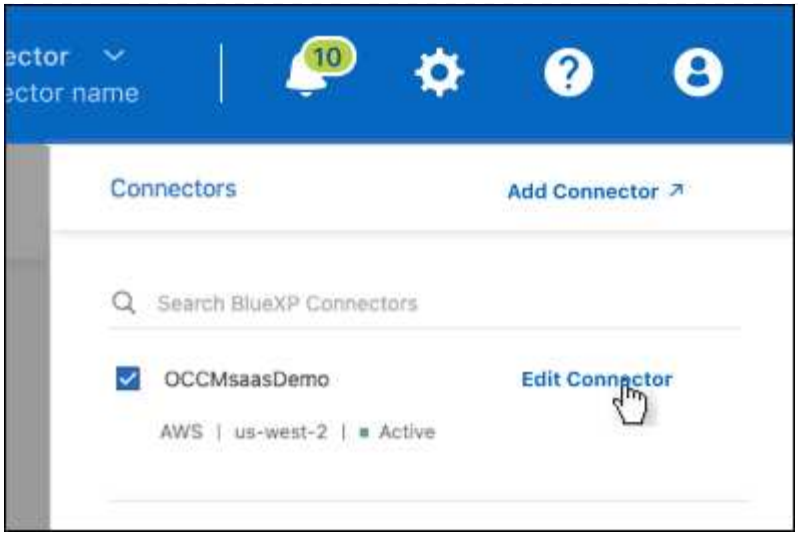

c. Wählen Sie das Aktionsmenü für einen Konnektor aus und wählen Sie **Connector bearbeiten**.




**Eingeschränkter oder privater Modus**

a. Wählen Sie im BlueXP Header das Dropdown-Menü **Connector** aus.

b. Wählen Sie **Connector Bearbeiten**.




2. Wählen Sie **Support Direct API Traffic**.
3. Aktivieren Sie das Kontrollkästchen, um die Option zu aktivieren, und wählen Sie dann **Speichern**.

# Standardkonfiguration für den Konnektor

Möglicherweise möchten Sie mehr über die Konfiguration des Connectors 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 Ubuntu 22.04 LTS.

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

- Der Benutzername für die EC2 Linux-Instanz ist ubuntu (für Connectors, die vor Mai 2023 erstellt wurden, war der Benutzername 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 Ubuntu 22.04 LTS.

  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 implementiert haben, beachten Sie Folgendes:

- Die VM-Instanz ist n2-Standard-4.
- Das Betriebssystem für das Image ist Ubuntu 22.04 LTS.

  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
  Oder
- /Opt/Application/netapp/Service-Manager-2/logs (beginnend mit den neuen 3.9.23 Installationen)

  Die Protokolle in diesen Ordnern 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.

**Ports**

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

- 80 für HTTP-Zugriff

- 443 für HTTPS-Zugriff

## 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