Anschlüsse

Set up and administration

NetApp
January 09, 2023

Inhaltsverzeichnis

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

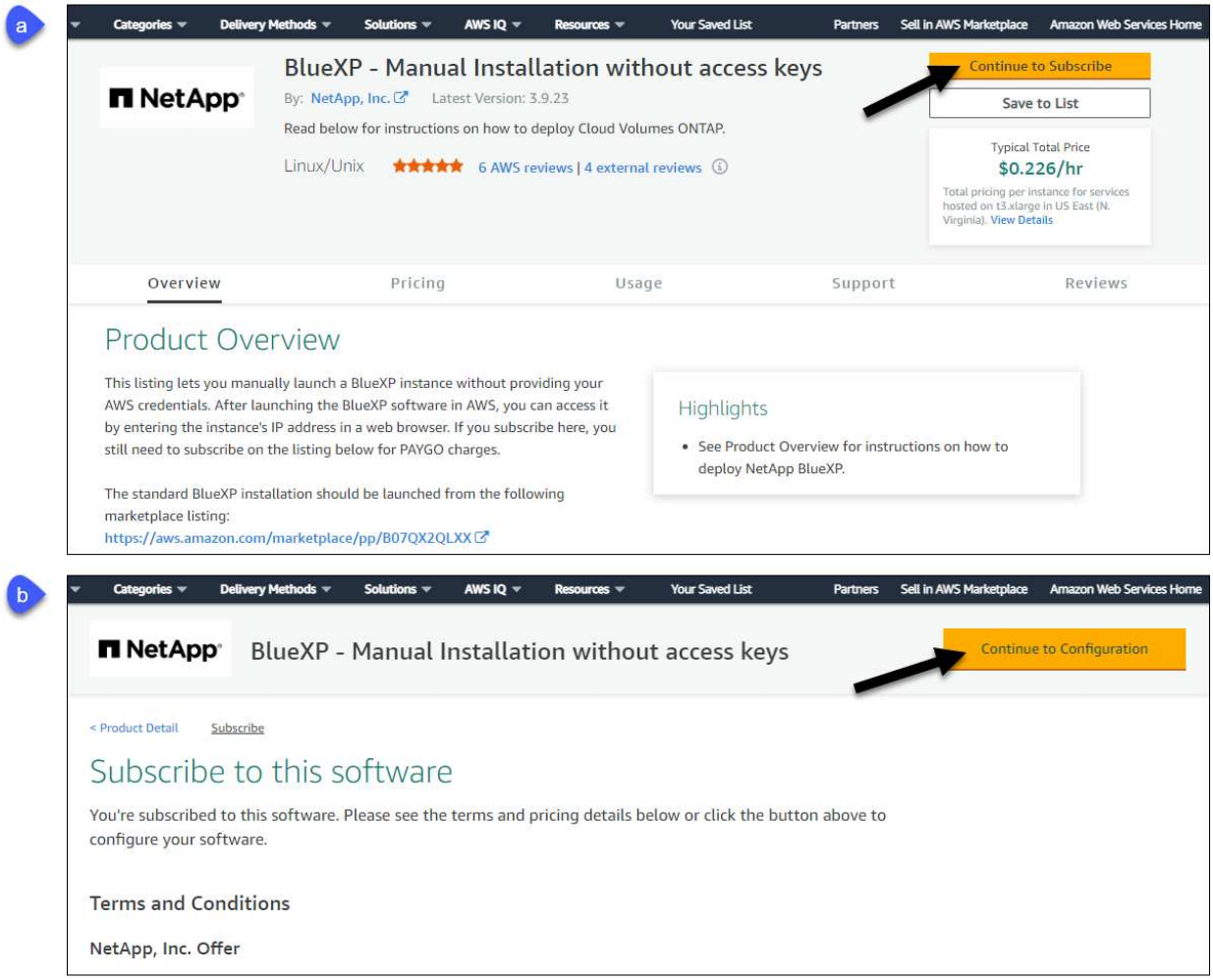
Sie können die Connector-Instanz direkt aus dem AWS Marketplace-Angebot für BlueXP in einer kommerziellen AWS-Region starten.

Bevor Sie beginnen

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**.



4. Ändern Sie eine der Standardoptionen, und klicken Sie auf **Weiter zum Starten**.
5. 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.

6. 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://console.bluexp.netapp.com Um den Connector mit BlueXP zu verwenden.

Ergebnis

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

Wenn Sie 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

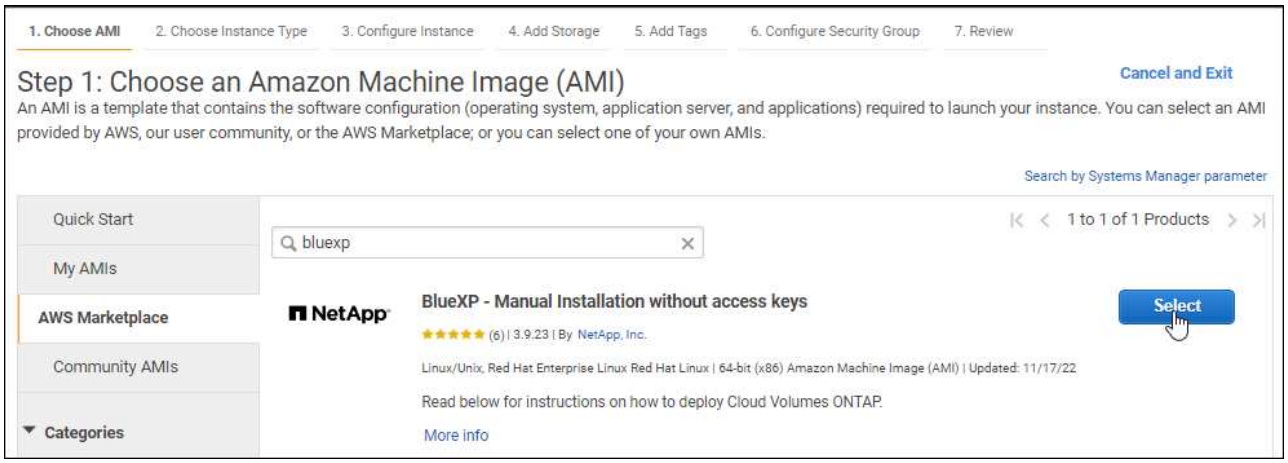
1. Einrichten von Berechtigungen in AWS:
   a. Erstellen Sie von der IAM-Konsole aus Ihre eigene Richtlinie, indem Sie die Inhalte von kopieren und einfügen "Die IAM-Richtlinie für den Connector".
   b. Erstellen Sie eine IAM-Rolle mit dem Rollentyp Amazon EC2, und hängen Sie die im vorherigen Schritt 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.



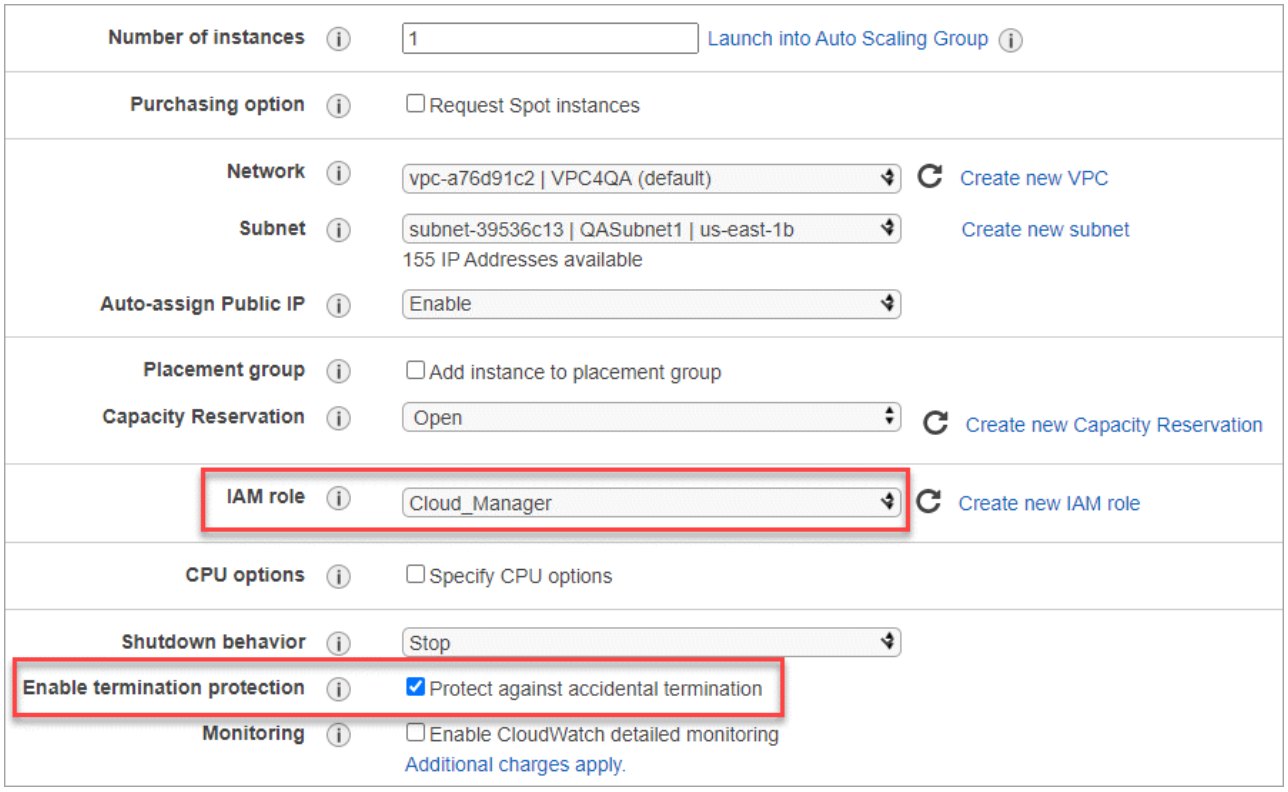
d. Klicken Sie Auf **Weiter**.

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.



- **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.

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

   https://*ipaddress*[]

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

      "Informationen zu NetApp Accounts".

   b. Geben Sie einen Namen für das System ein.

Ergebnis

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

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

Da der Connector in einer Regierungsregion eingesetzt wurde, ist er von nicht zugänglich https://console.bluexp.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*[]

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

      "Informationen zu NetApp Accounts".

b. Geben Sie einen Namen für das System ein.

Ergebnis

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

Wenn sich der Connector in einer kommerziellen Azure-Region befindet, öffnen Sie einen Webbrowser, und gehen Sie zu https://console.bluexp.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*[]

Da der Connector in einer Regierungsregion eingesetzt wurde, ist er von nicht zugänglich https://console.bluexp.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.

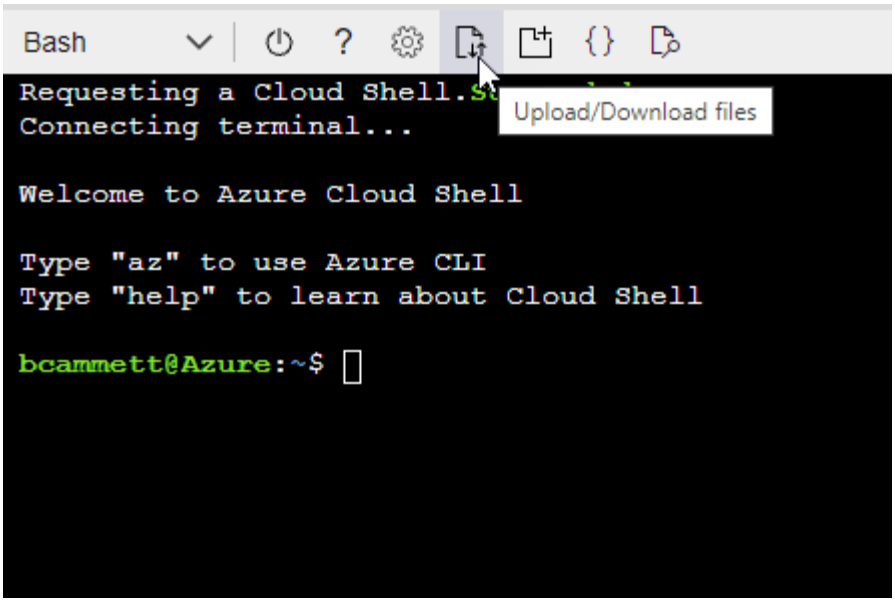
      Beispiel

      ```
      "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.



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

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

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

2. 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.

Ergebnis

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 isthttps://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 19.3.1 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://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://cloudmanagerinfraprod.azurecr.io
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net

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.

Was Sie benötigen

- Root-Berechtigungen zum Installieren des Connectors.
- Details zu einem Proxy-Server, falls ein Proxy für den Internetzugriff über den Connector erforderlich ist.

  Sie haben die Möglichkeit, nach der Installation einen Proxyserver zu konfigurieren, aber dafür muss der Connector neu gestartet werden.

- Ein von einer Zertifizierungsstelle signiertes Zertifikat, wenn der Proxy-Server HTTPS verwendet.

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.

   Sie sollten das Connector-Installationsprogramm herunterladen, das für die Verwendung in Ihrem

Netzwerk oder in der Cloud bestimmt ist.

3. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

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

4. Führen Sie das Installationsskript aus.

```
 ./OnCommandCloudManager-V3.9.23 --proxy <HTTP or HTTPS proxy server>
--cacert <path and file name of a CA-signed certificate>
```

Die Parameter --Proxy und --cacert sind optional. Wenn Sie über einen Proxyserver verfügen, müssen Sie die Parameter wie dargestellt eingeben. Das Installationsprogramm fordert Sie nicht auf, Informationen über einen Proxy einzugeben.

Hier sehen Sie ein Beispiel für den Befehl mit beiden optionalen Parametern:

```
 ./OnCommandCloudManager-V3.9.23 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--Proxy konfiguriert den Connector so, dass er einen HTTP- oder HTTPS-Proxy-Server in einem der folgenden Formate verwendet:

- http://address:port
- http://username:password@address:port
- https://address:port
- https://username:password@address:port

--cacert gibt ein CA-signiertes Zertifikat für den HTTPS-Zugriff zwischen dem Connector und dem Proxy-Server an. Dieser Parameter ist nur erforderlich, wenn Sie einen HTTPS-Proxyserver angeben.

Ergebnis

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

Richten Sie den Anschluss ein

Melden Sie sich an oder melden Sie sich an, und richten Sie dann den Konnektor ein, um mit Ihrem Konto zu arbeiten.

Schritte

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

   https://*ipaddress*[]

   Ipaddress kann abhängig von der Konfiguration des Hosts localhost, eine private IP-Adresse oder eine

öffentliche IP-Adresse sein. Wenn sich der Connector beispielsweise ohne öffentliche IP-Adresse in der Public Cloud befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-Host hat.

2. Anmelden oder anmelden.
3. 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.
4. 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.

Ergebnis

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

Nachdem Sie fertig sind

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 3 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 isthttps://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.

Erforderliche Berechtigungen

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
```

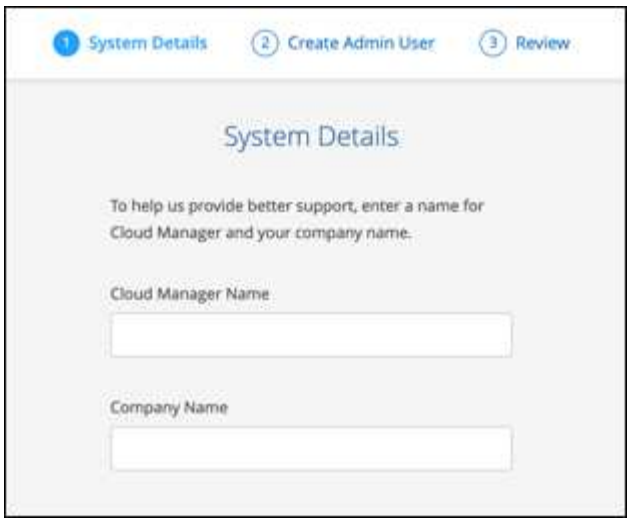
5. Führen Sie das Installationsskript aus:

```
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.



- **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.

Ergebnis

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

Was kommt 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

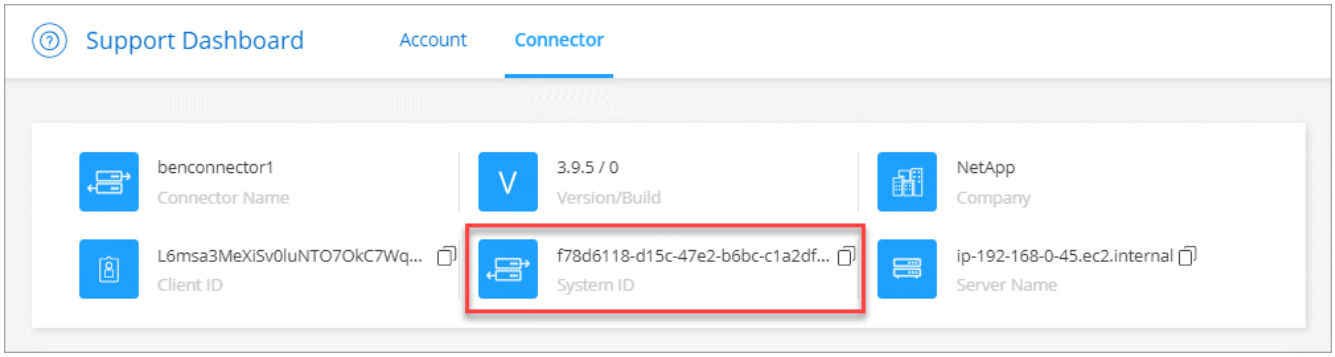
Um Ihnen bei den ersten Schritten zu helfen, bittet Ihr NetApp Mitarbeiter Sie möglicherweise um die System-ID für einen Connector. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

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.

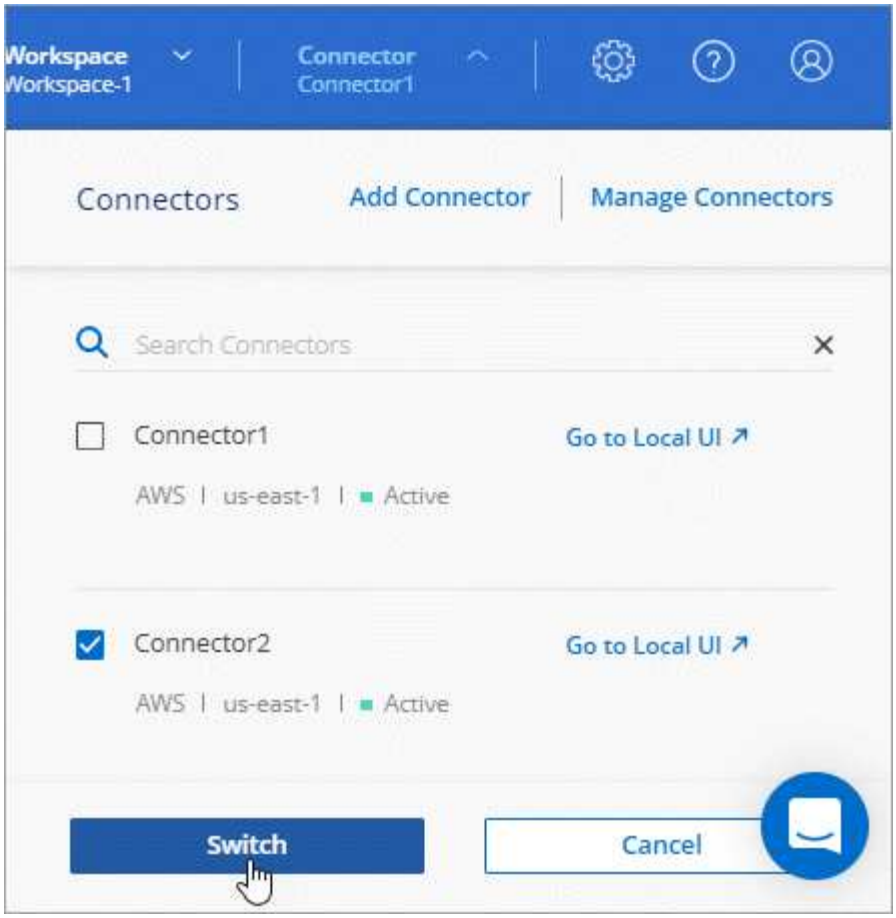
Zwischen den Anschlüssen wechseln

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.

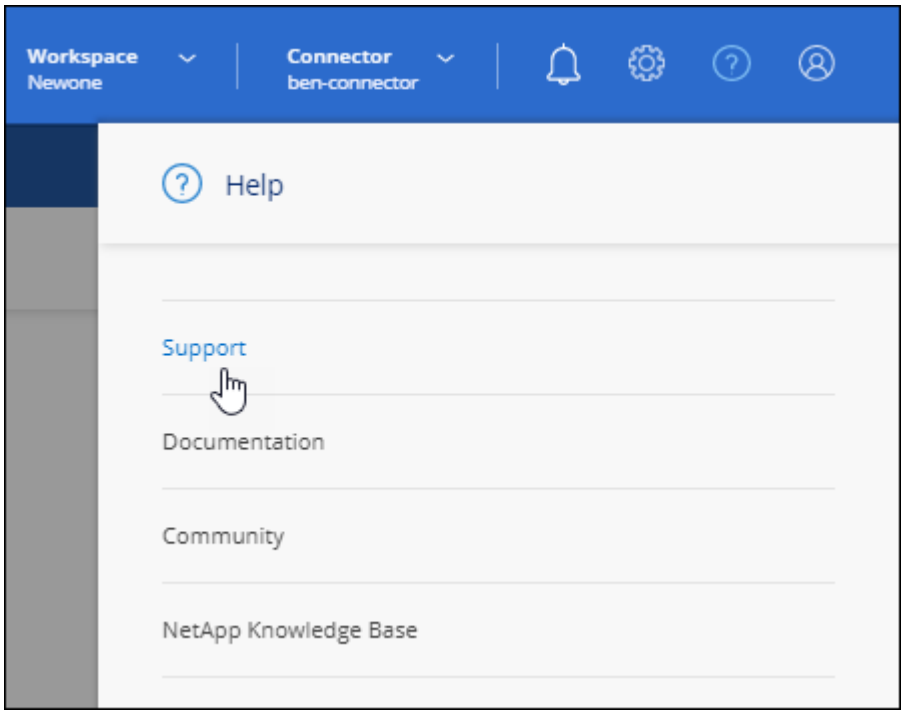
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um sich anzumelden.

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

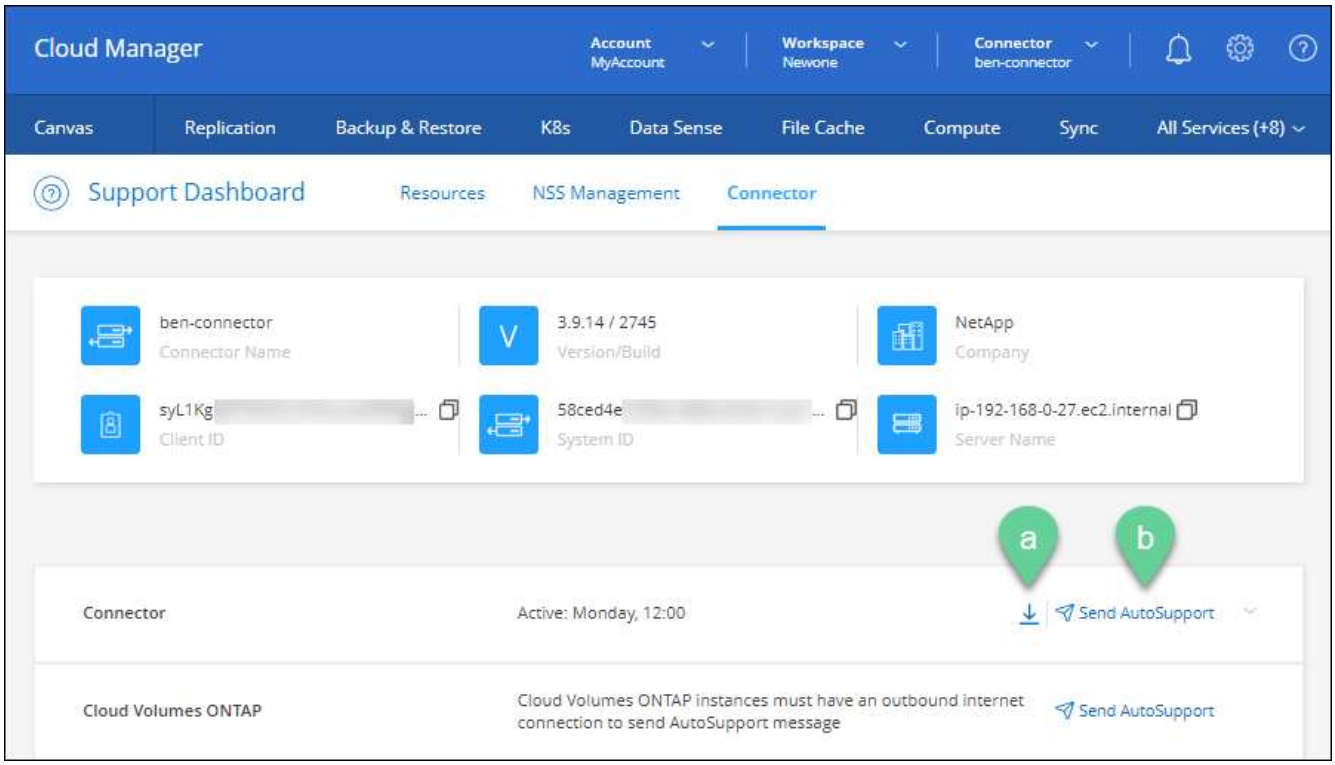
1. Stellen Sie eine Verbindung zur lokalen Benutzeroberfläche des Connectors her, wie im Abschnitt oben beschrieben.
2. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



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 (gcloudd) 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

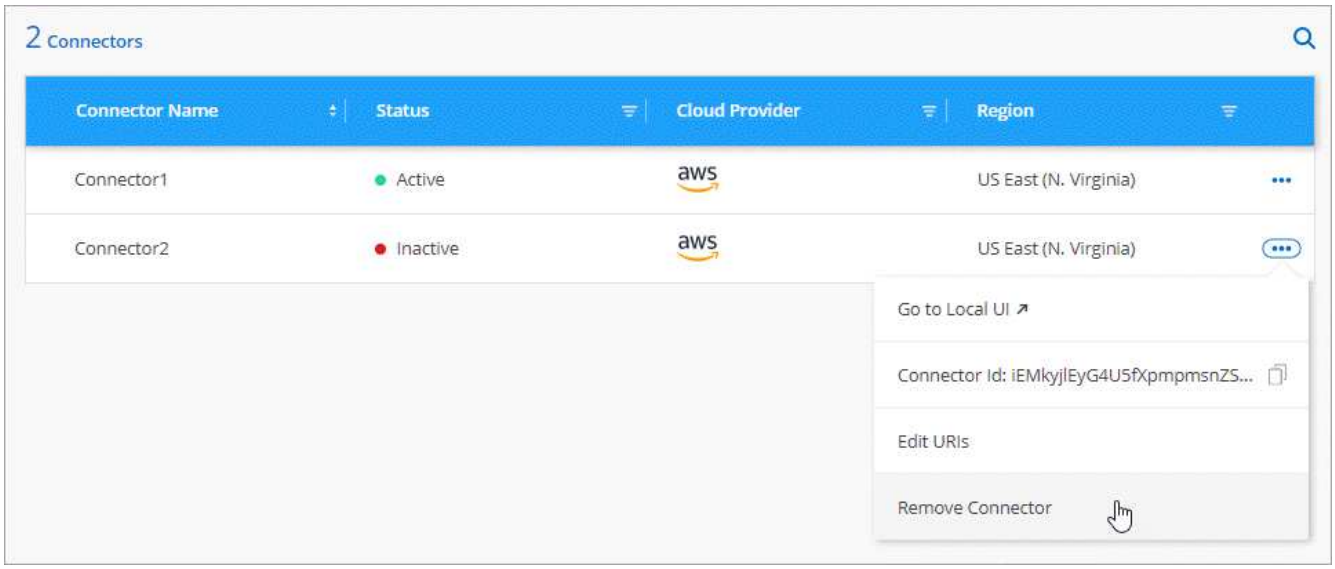
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in BlueXP entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

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.

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 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/Service-Manager-2/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

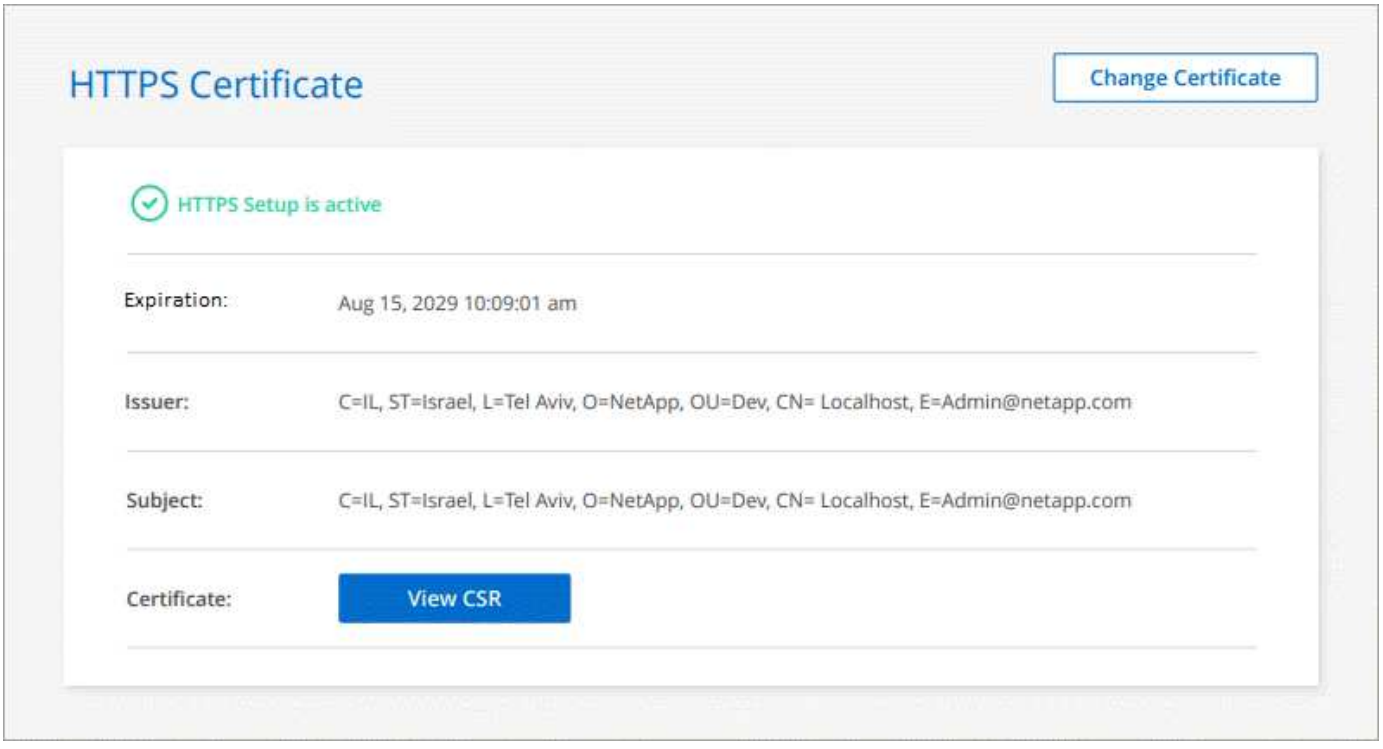
1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Symbol Einstellungen, und wählen Sie **HTTPS-Setup**.

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

Ergebnis

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.

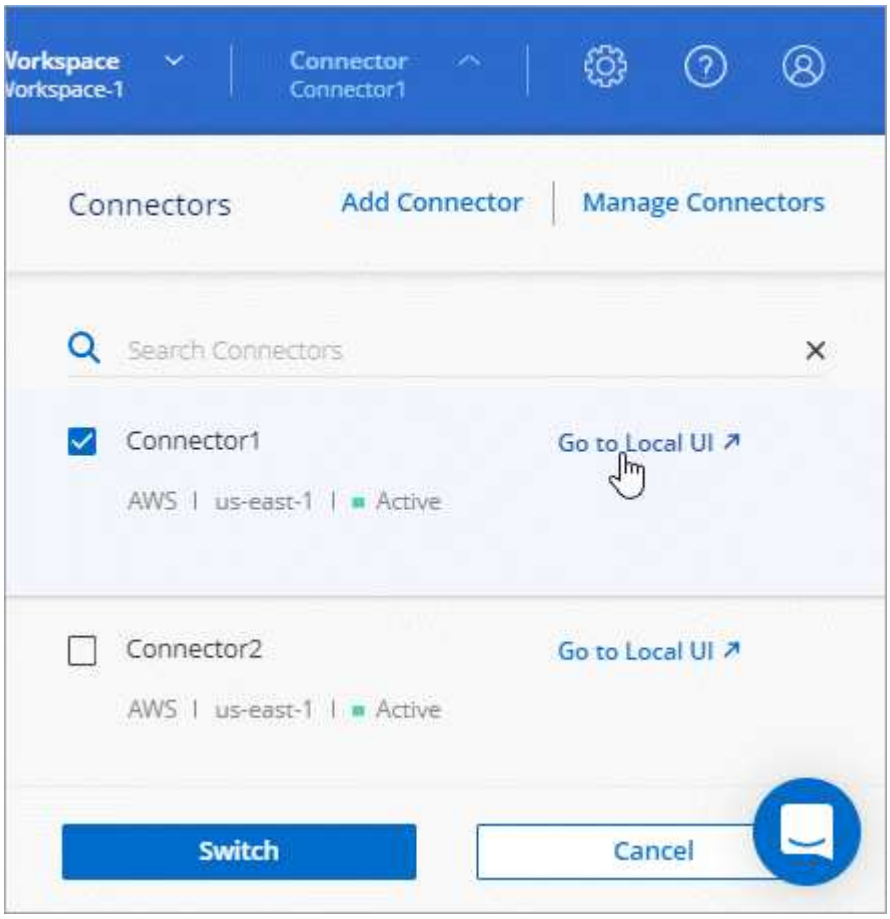
Beachten Sie, dass mit diesem Vorgang der Anschluss neu gestartet wird. Stellen Sie sicher, dass der Connector keine Operationen durchführt, bevor Sie fortfahren.

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/Applikation/netapp/Cloud Manager/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