



# **Erweiterte Implementierung**

## **Set up and administration**

NetApp

December 15, 2022

# Inhaltsverzeichnis

- Erweiterte Implementierung ..... 1
  - Erstellen Sie einen Connector aus dem AWS Marketplace ..... 1
  - Erstellen Sie einen Connector aus dem Azure Marketplace ..... 5
  - Installieren Sie den Connector auf einem vorhandenen Linux-Host mit Internetzugang ..... 9
  - Installieren Sie den Connector On-Prem ohne Internetzugang ..... 13

# 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

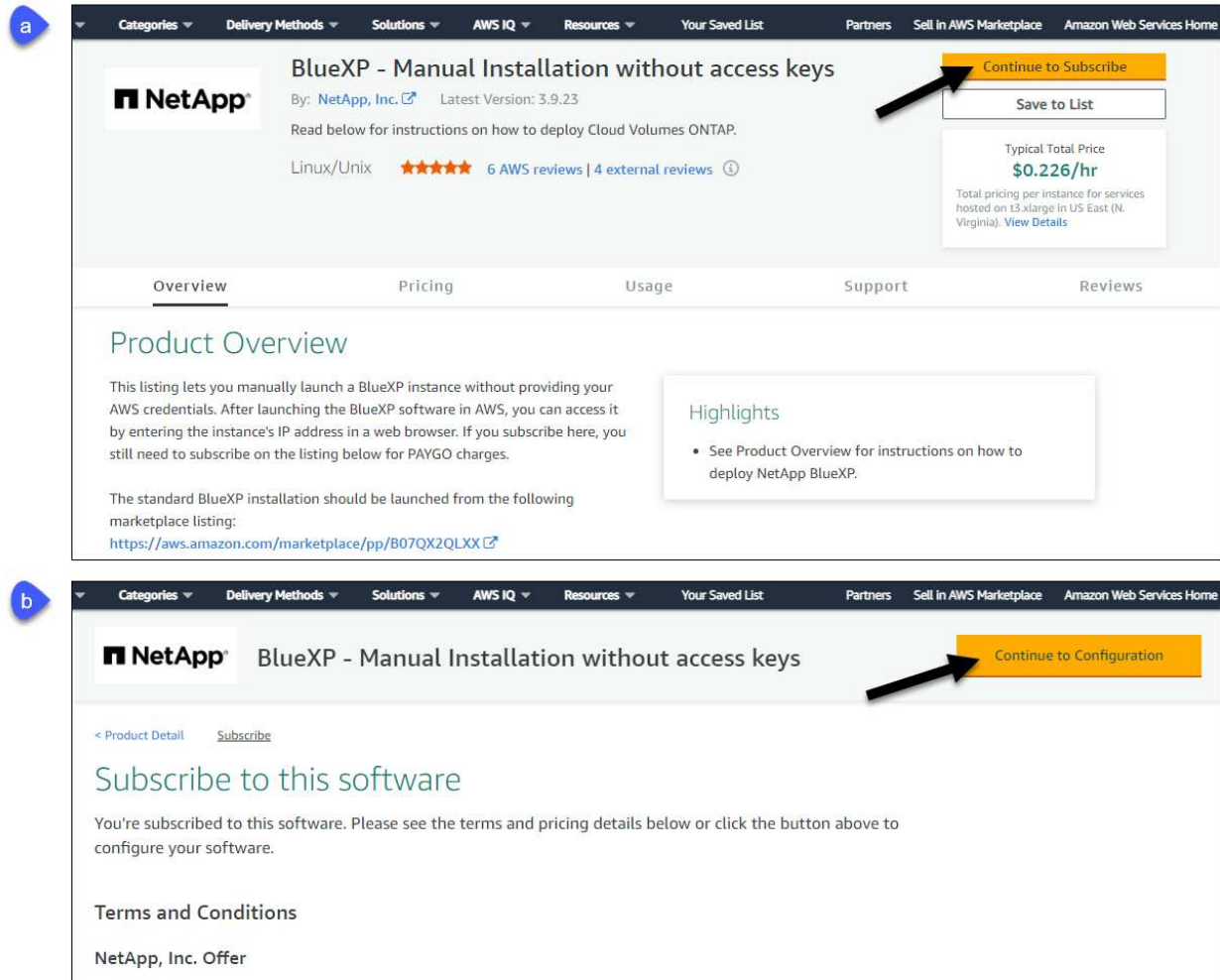
Sie können die Connector-Instanz direkt aus dem AWS Marketplace-Angebot für BlueXP in einer kommerziellen AWS-Region starten.

#### 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.blueexp.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.

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



- 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.

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

- **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.blueexp.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.blueexp.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.

## 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 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 19.3.1 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](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 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.

### 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.

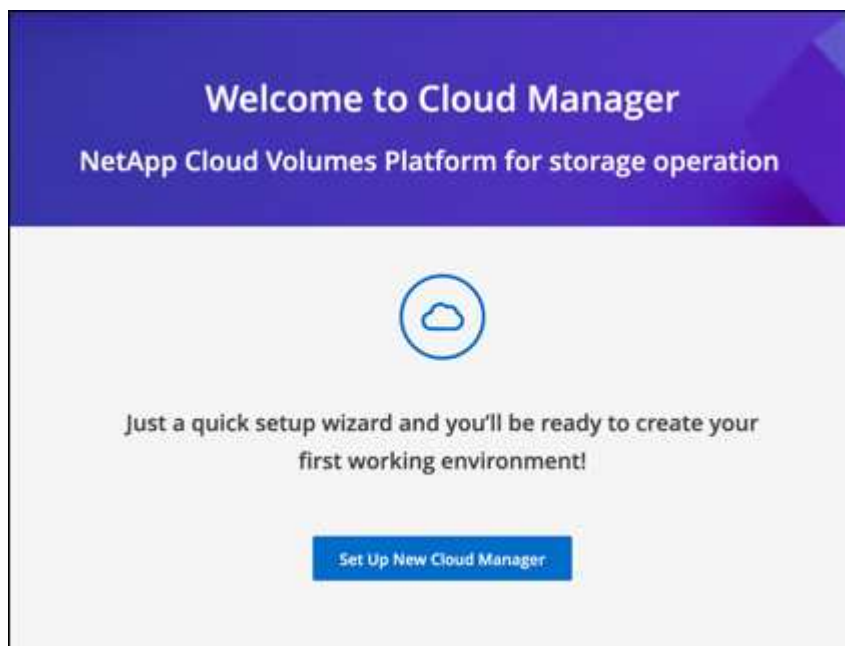
```
chmod +x /path/cloud-manager-connector-offline-v3.9.23
```

5. Führen Sie das Installationsskript aus:

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

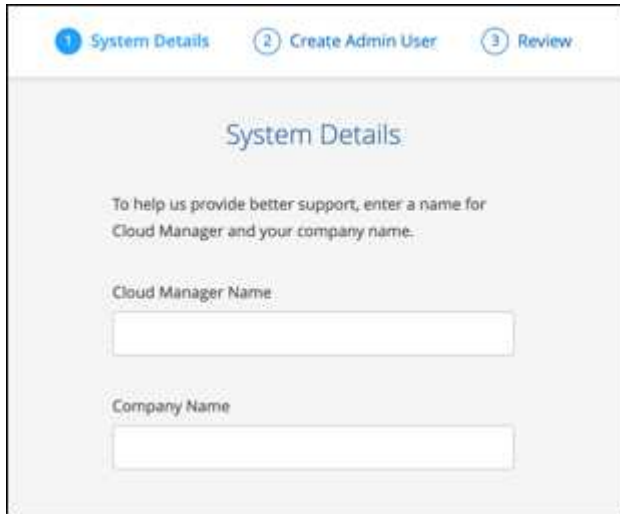
6. Öffnen Sie einen Webbrowser, und geben Sie ein `https://ipaddress[]` Wobei *ipaddress* die IP-Adresse des Linux-Hosts ist.

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"](#).

## 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, BEISPIELHAFT 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.