

Anschlüsse BlueXP setup and administration

NetApp September 09, 2024

This PDF was generated from https://docs.netapp.com/de-de/bluexp-setup-admin/task-maintainconnectors.html on September 09, 2024. Always check docs.netapp.com for the latest.

Inhalt

Anschlüsse	1
Wartung der Connector VM und des Betriebssystems	1
Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff	3
Konfigurieren Sie einen Konnektor für die Verwendung eines Proxy-Servers	5
Erfordern die Verwendung von IMDSv2 auf Amazon EC2 Instanzen	11
Aktualisieren Sie einen Connector, wenn Sie den privaten Modus verwenden	13
Arbeiten Sie mit mehreren Anschlüssen	14
Fehlersuche für den Anschluss durchführen	15
Deinstallieren Sie den Connector, und entfernen Sie ihn	18
Standardkonfiguration für den Konnektor	20

Anschlüsse

Wartung der Connector VM und des Betriebssystems

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.



Wenn Sie bereits über einen Connector verfügen, sollten Sie sich dessen bewusst sein "Änderungen an unterstützten Linux-Betriebssystemen".

Betriebssystem-Patches und der Connector

Sie müssen keine Dienste auf dem Connector-Host anhalten, wenn Sie OS-Sicherheitspatches anwenden.

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

8 Kerne oder 8 vCPUs

RAM

32 GB

"Informieren Sie sich über die Standardkonfiguration des Connectors".

Beenden des Starting der Konnektor-VM

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".

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"

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.

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

a. Legen Sie über die Cloud Volumes ONTAP-CLI die Berechtigungsebene auf erweitert fest:

set -privilege advanced

b. Führen Sie den folgenden Befehl aus, um das aktuelle Backup-Ziel anzuzeigen:

```
system configuration backup settings show
```

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

system configuration backup settings modify -destination <targetlocation>

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.

Installieren Sie ein CA-signiertes Zertifikat für den webbasierten Konsolenzugriff

Wenn Sie BlueXP im eingeschränkten oder privaten Modus verwenden, kann auf die Benutzeroberfläche über die virtuelle Connector-Maschine zugegriffen werden, die in Ihrer Cloud-Region oder vor Ort bereitgestellt wird. Standardmäßig verwendet BlueXP ein selbstsigniertes SSL-Zertifikat, um einen sicheren HTTPS-Zugriff auf die webbasierte Konsole zu ermöglichen, die auf dem Connector ausgeführt wird. Falls Ihr Unternehmen dies erfordert, können Sie ein von einer Zertifizierungsstelle signiertes Zertifikat installieren, das einen besseren Schutz bietet als ein selbstsigniertes Zertifikat. Nach der Installation des Zertifikats verwendet BlueXP das CA-signierte Zertifikat, wenn Benutzer auf die webbasierte Konsole zugreifen.

Bevor Sie beginnen

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

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.
	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 wählen Sie dann Installieren.
Installieren Sie Ihr	a. Wählen Sie CA-signiertes Zertifikat installieren.
eigenes CA-signiertes Zertifikat	 b. Laden Sie sowohl die Zertifikatdatei als auch den privaten Schlüssel und wählen Sie dann 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 einen Connector, der für sicheren Zugriff konfiguriert ist:

0	
HTTPS Set	up is active
Expiration:	Aug 15, 2029 10:09:01 am
Issuer:	C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com
Subject:	C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com
Certificate:	View CSR

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.

Workspace Workspace-1	Connector Connector Connector
	Connectors Add Connector Manage Connectors
	Q Search BlueXP Connectors
	gsireeshconnector Go to Local UI ≯
	On-Premises - Active

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

Status	₹ Region	≂
Active	 N/A	
Inactive	 Go to Local UI 🖄	
Active	Connector Id: itPwkiYsU6iMCLn9	Dg60hX7 🗇
Inactive	Edit Connector	
Active	Remove BlueXP Connector	

Eingeschränkter oder privater Modus

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

inectors	Add Connector 2
Q Search BlueXP Connectors	
OCCMsaasDemo	Edit Connector

- 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 http://address:port Oder https://address:port
 - 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.

Workspace Workspace-1	Connector Connector Sirveshconnec
	Connectors Add Connector Manage Connectors
	Q Search BlueXP Connectors
	Go to Local UI >
	Succession 1 - L - contra

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

Status	≅ Region	Ŧ
Active	N/A	
 Inactive 	Go to Local UI 😰	
Active	Connector Id: itPwkiYsU6iMCL	n9Dg60hX7 🗇
Inactive	Edit Connector	
	 Remove BlueXP Connector	
ALLIVE		

Eingeschränkter oder privater Modus

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

nectors	Add Connector 🤊
Q Search BlueXP Connectors	
OCCMsaasDemo AWS us-west-2 = Active	Edit Connector

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

Erfordern die Verwendung von IMDSv2 auf Amazon EC2 Instanzen

BlueXP unterstützt 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.

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

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.

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 einen 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.



Wenn Sie BlueXP im Standardmodus oder im eingeschränkten Modus verwenden, müssen Sie den Connector nicht manuell aktualisieren. BlueXP aktualisiert einen Connector automatisch auf die neueste Version, sofern der Connector über Outbound-Internetzugang verfügt, um das Softwareupdate zu erhalten.

Über diese Aufgabe

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

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.

 Nachdem die Aktualisierung abgeschlossen ist, können Sie die Version des Connectors überpr
üfen, indem Sie Hilfe > Support > Connector aufrufen.

Arbeiten Sie mit mehreren Anschlüssen

Wenn Sie mehrere Connectors verwenden, können Sie mit BlueXP direkt von der Konsole aus zwischen diesen Connectors wechseln. Sie können auch eine einzige Arbeitsumgebung mit mehreren Connectors verwalten.

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.

Richten Sie eine Disaster Recovery-Konfiguration ein

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

Schritte

- 1. Wechseln Sie zu dem anderen Connector, den Sie mit der Arbeitsumgebung verwalten möchten.
- 2. Erkennung der vorhandenen Arbeitsumgebung
 - "Fügen Sie vorhandene Cloud Volumes ONTAP-Systeme zu BlueXP hinzu"
 - "ONTAP Cluster erkennen"
- Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung verwalten, wählen Sie Einstellungen > Verbindungseinstellungen und stellen Sie den Modus f
 ür die Kapazit
 ätsverwaltung auf manueller Modus ein.

Um Konflikte zu vermeiden, sollte nur der Hauptanschluss auf Automatischer Modus gesetzt werden.

"Erfahren Sie mehr über den Kapazitätsmanagement-Modus"

Fehlersuche für den Anschluss durchführen

Um Probleme mit dem Konnektor zu beheben, können Sie mit dem NetApp-Support zusammenarbeiten, der Sie möglicherweise nach Ihrer System-ID, der Connector-Version oder den neuesten AutoSupport-Meldungen fragt. Sie können auch die NetApp Wissensdatenbank anzeigen, um Fehler selbst zu beheben.

Verwandter Link

"Holen Sie sich Hilfe vom NetApp-Support".

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



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.

? Support	Resources	Case Management	NSS Manager	ment BlueXP Connector	
		sgonprem1		3.9.33 / 5634	 NetApp
	€ B	BlueXP Connector Name	99v 📑	Version/Build	Company 2183e428b9f6
		Client ID		System ID	Server Name

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.

Workspa Newone	e ~ Connector ~ ሷ 😳 🕜 😣
	Help
	Support
	Community
	NetApp Knowledge Base

- 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.

9	Support	Resources	Case Management	NSS Manag	gement BlueXP Connector	-		
	ņ	ben-connector10 BlueXP Connector M	Name	V 3.9.2	8 / 5376 arv/Build	8	NetApp Company	
	8	PWKUWC1cM2Eqol Client ID	L8c5TMayzK8rJZ 🗇	02a3 Syste	9283-d16e-45e1-958f-d117d16 m ID	ð	e810daf5d7d5 🗇 Server Name	
							a b	
	BlueXP	Connector		Active: Mor	nday, 12:00		↓ Send AutoSupport	
	Cloud V	olumes ONTAP		Cloud Volu connection	mes ONTAP instances must have a to send AutoSupport message	an outbound in	nternet 🛛 🦪 Send AutoSupport	

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"

Holen Sie sich Hilfe in der NetApp Knowledge Base

"Zeigen Sie die vom NetApp-Supportteam erstellten Fehlerbehebungsinformationen an".

Deinstallieren Sie den Connector, und entfernen Sie ihn

Deinstallieren Sie die Connector-Software, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen. Welche Schritte Sie durchführen müssen, hängt vom verwendeten Bereitstellungsmodus ab. Sobald ein Connector aus Ihrer Umgebung entfernt wurde, können Sie ihn aus BlueXP entfernen.

"Weitere Informationen zu BlueXP Implementierungsmodi".

Deinstallieren Sie den Connector, wenn Sie den Standard- oder eingeschränkten Modus verwenden

Wenn Sie BlueXP im Standardmodus oder im eingeschränkten Modus verwenden (d. h. der Connector-Host verfügt über ausgehende Verbindungen), sollten Sie die nachstehenden Schritte ausführen, um die Connector-Software zu deinstallieren.

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.

Ergebnis

Die Connector-Software wird jetzt vom Linux-Host deinstalliert.

Deinstallieren Sie den Connector, wenn Sie den privaten Modus verwenden

Wenn Sie BlueXP im privaten Modus verwenden (d. h. der Connector-Host verfügt über *no* Outbound-Verbindungen), sollten Sie die nachstehenden Schritte ausführen, um die Connector-Software zu deinstallieren.

Schritt

- 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

Ergebnis

Die Connector-Software wird jetzt vom Linux-Host deinstalliert.

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.

nectors				
Connector Name	+ Status	⇒ Cloud Provider	≂ Region ⇒	
Connector1	Active	aws	US East (N. Virginia)	
Connector2	• Inactive	aws	US East (N. Virginia)	
			Go to Local UI 🗷	
			Connector Id: iEMkyjlEyG4U5fXpmpmsnZ5.	0
			Edit URIs	
			Remove Connector പ്രിപ്പ	

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

BlueXP entfernt den Connector aus seinen Datensätzen.

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 t3.2xlarge.
- 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 Installation beinhaltet die Docker Engine, das erforderliche Tool zur Container-Orchestrierung.
- 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 Standard_D8S_v3.
- 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 Installation beinhaltet die Docker Engine, das erforderliche Tool zur Container-Orchestrierung.
- 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-8.
- 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 Installation beinhaltet die Docker Engine, das erforderliche Tool zur Container-Orchestrierung.
- 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 zum Connector.

/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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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