Anschlüsse Verwalten

Cloud Manager 3.8

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/de-de/occm38/task_managing_connectors.html on March 25, 2024. Always check docs.netapp.com for the latest.

Inhalt

Anschlüsse Verwalten

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.

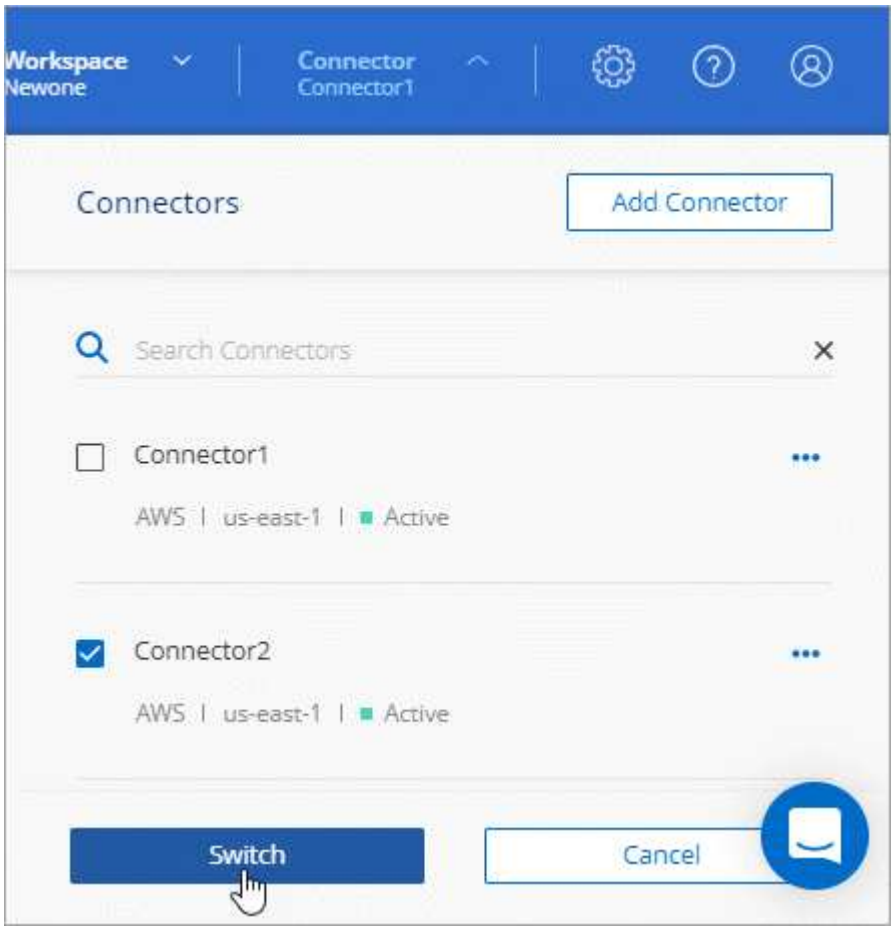
Wechseln zwischen den Anschlüssen

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**.



Cloud Manager aktualisiert und zeigt die Arbeitsumgebungen an, die mit dem ausgewählten Connector verknüpft sind.

Zugriff auf die lokale Benutzeroberfläche

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Diese Schnittstelle wird für einige Aufgaben benötigt, die über den Connector selbst ausgeführt werden müssen:

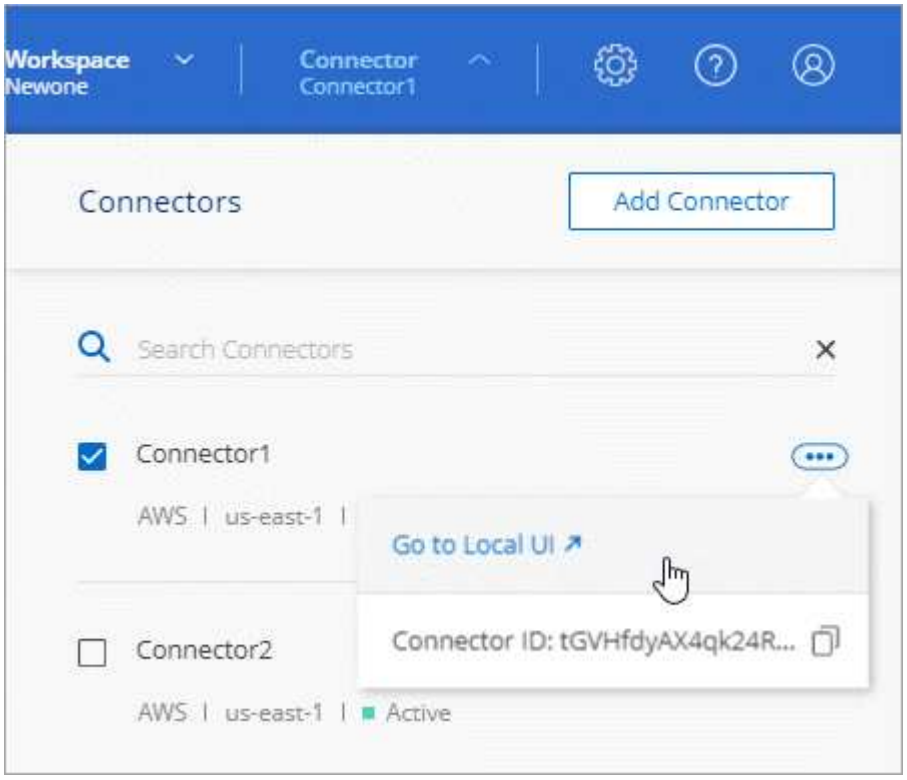
- "Festlegen eines Proxyservers"
- Installation eines Patches (Sie arbeiten in der Regel mit NetApp Mitarbeitern zusammen, um einen Patch zu installieren)
- Herunterladen von AutoSupport-Meldungen (normalerweise gerichtet von NetApp Mitarbeitern, wenn Sie Probleme haben)

Schritte

1. "Melden Sie sich bei der SaaS-Schnittstelle von Cloud Manager 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**, klicken Sie auf das Aktionsmenü für einen Connector und dann auf **Gehe zu lokaler Benutzeroberfläche**.



   Die Cloud Manager-Schnittstelle, die auf dem Connector ausgeführt wird, wird in einer neuen Browser-Registerkarte geladen.

Entfernen von Anschlüssen aus Cloud Manager

Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in Cloud Manager entfernen. Sie

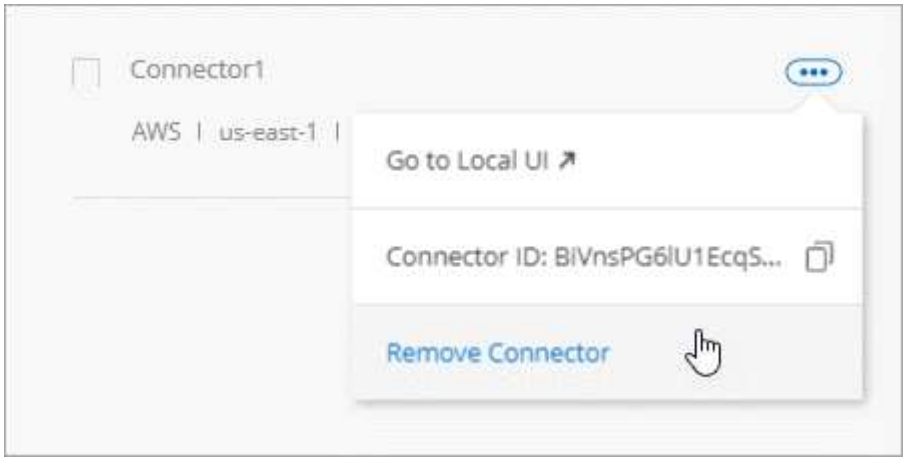
können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

Beachten Sie Folgendes zum Entfernen eines Konnektors:

- Durch diese Aktion wird die virtuelle Maschine nicht gelöscht.
- Diese Aktion kann nicht rückgängig gemacht werden: Sobald ein Connector aus Cloud Manager entfernt wurde, kann er nicht wieder zu Cloud Manager hinzugefügt werden.

Schritte

1. Klicken Sie in der Kopfzeile des Cloud Manager auf das Dropdown-Menü Connector.
2. Klicken Sie auf das Aktionsmenü für einen inaktiven Konnektor und klicken Sie auf **Connector entfernen**.



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

Ergebnis

Cloud Manager entfernt den Connector aus seinen Datensätzen.

Deinstallieren der Connector-Software

Der Connector enthält ein Deinstallationsskript, mit dem Sie die Software deinstallieren können, um Probleme zu beheben oder die Software dauerhaft vom Host zu entfernen.

Schritt

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

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

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

Wie sieht es mit Software-Upgrades aus?

Der Connector aktualisiert seine Software automatisch auf die neueste Version, solange er hat "Outbound-Internetzugang" Um das Softwareupdate zu erhalten.

Weitere Möglichkeiten zum Erstellen von Anschlüssen

Connector-Host-Anforderungen

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 und verwenden diesen Instanztyp, wenn Sie den Connector direkt über Cloud Manager bereitstellen.

Azure VM-Größe

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen DS3 v2 und verwenden die VM-Größe, wenn Sie den Connector direkt aus Cloud Manager implementieren.

GCP-Maschinentyp

Einen Instanztyp, der die oben aufgeführten CPU- und RAM-Anforderungen erfüllt. Wir empfehlen n1-Standard-4 und verwenden diesen Maschinentyp, wenn Sie den Connector direkt von Cloud Manager bereitstellen.

Unterstützte Betriebssysteme

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  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 GB Speicherplatz müssen verfügbar sein

Outbound-Internetzugang

Für die Installation des Connectors und des Connectors ist ein Outbound-Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu managen. Eine Liste der Endpunkte finden Sie unter "Netzwerkanforderungen für den Connector".

Erstellen eines Connectors über den AWS Marketplace

Es empfiehlt sich, einen Connector direkt aus Cloud Manager zu erstellen, aber Sie können einen Connector aus dem AWS Marketplace starten, wenn Sie keine AWS Zugriffsschlüssel angeben möchten. Nachdem Sie den Connector erstellt und eingerichtet haben, wird er automatisch bei der Erstellung neuer Arbeitsumgebungen verwendet.

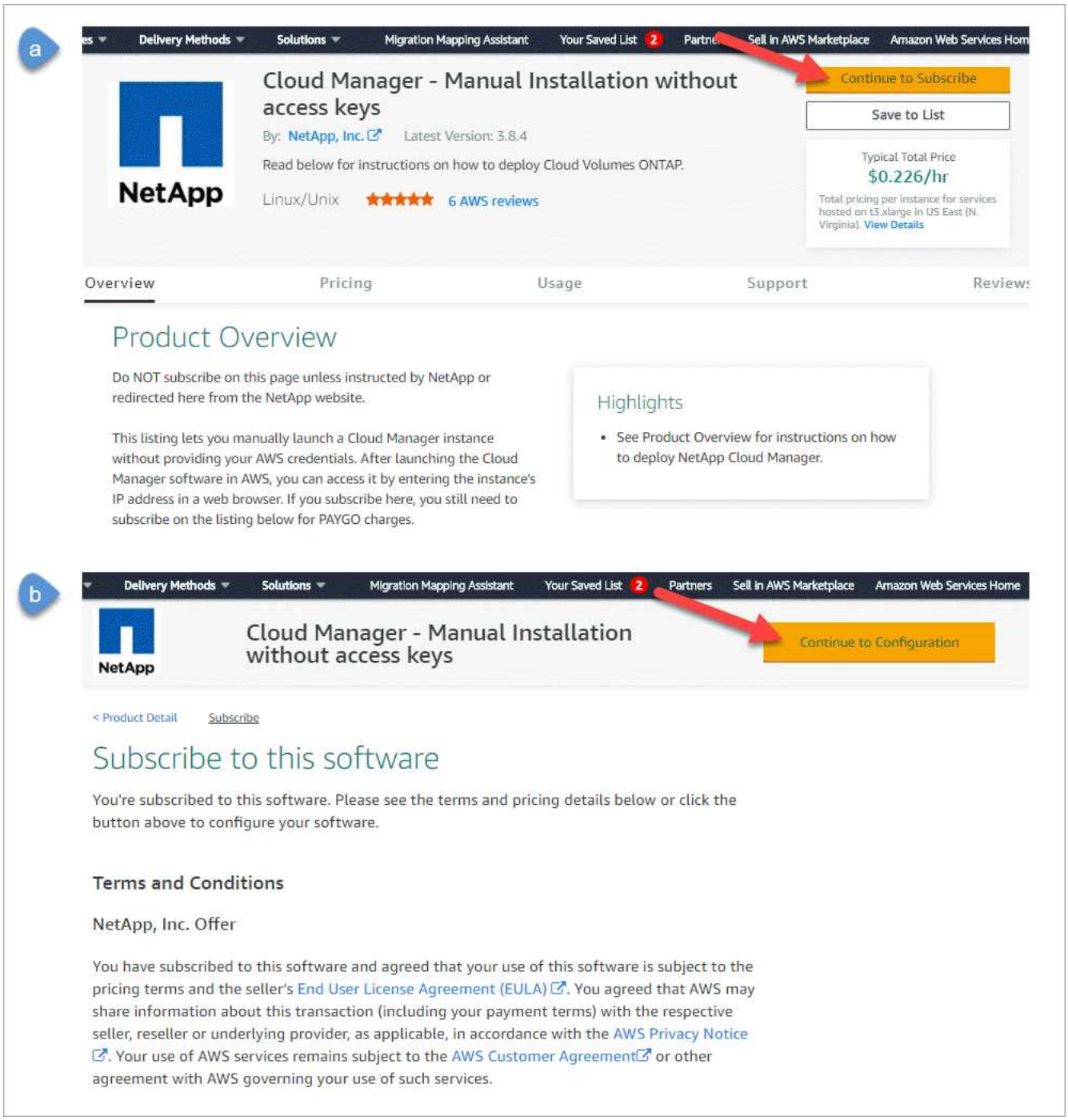
Schritte

1. IAM-Richtlinie und -Rolle für die EC2-Instanz erstellen:
   a. Laden Sie die Cloud Manager IAM-Richtlinie von folgendem Speicherort herunter:

      "NetApp Cloud Manager: AWS, Azure und GCP-Richtlinien"

   b. Erstellen Sie über die IAM-Konsole Ihre eigene Richtlinie, indem Sie den Text aus der Cloud Manager IAM-Richtlinie kopieren und einfügen.
   c. 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 jetzt zum "Seite zu Cloud Manager im AWS Marketplace" Um Cloud Manager über eine AMI bereitzustellen.

   Der IAM-Benutzer muss über AWS Marketplace-Berechtigungen zum Abonnieren und Abbestellen verfügen.
3. Klicken Sie auf der Marketplace-Seite auf **Weiter zur Anmeldung** und dann auf **Weiter zur Konfiguration**.



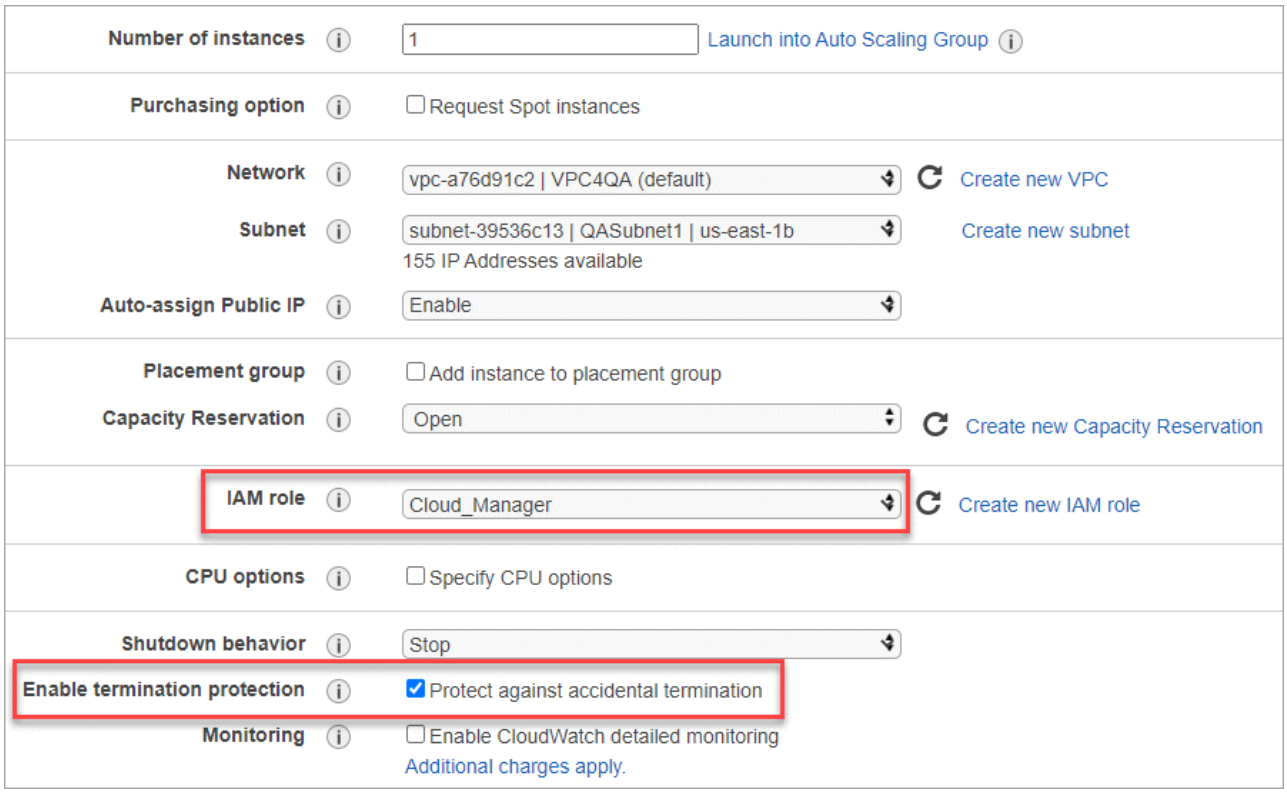
4. Ändern Sie eine der Standardoptionen, und klicken Sie auf **Weiter zum Starten**.
5. Wählen Sie unter **Aktion auswählen über EC2 starten** und klicken Sie dann auf **Start**.

   In diesen Schritten wird beschrieben, wie Sie die Instanz über die EC2-Konsole starten, da Sie über die Konsole eine IAM-Rolle an die Cloud Manager-Instanz anhängen können. Dies ist mit der Aktion * von Website starten* nicht möglich.

6. Befolgen Sie die Anweisungen zur Konfiguration und Bereitstellung der Instanz:
   - **Wählen Sie Instanztyp**: Wählen Sie je nach Verfügbarkeit der Region einen der unterstützten Instanztypen (t3.xlarge wird empfohlen).

     "Prüfen Sie die Anforderungen an die Instanz".

- **Instanz 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.

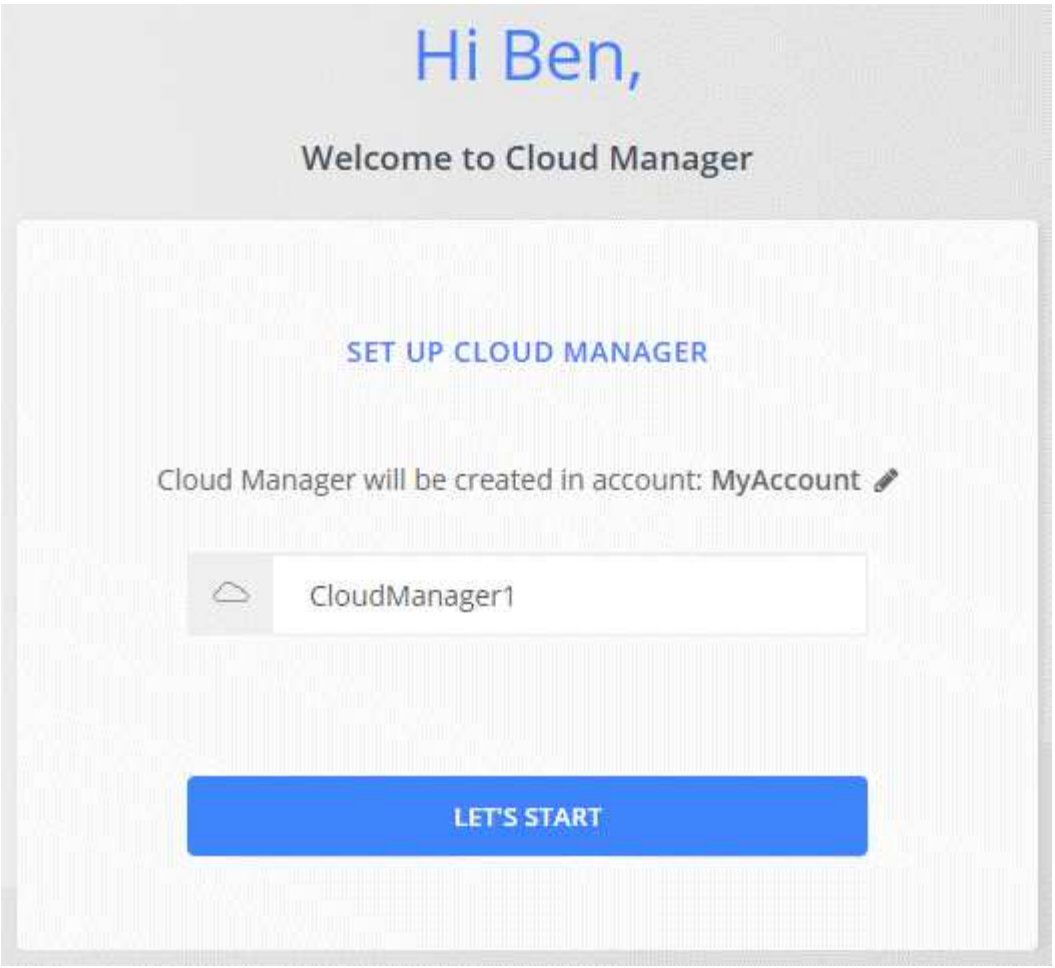
7. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung zur Verbindungsinstanz hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

8. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das Cloud Central-Konto an, das mit dem Connector verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Der Connector ist jetzt mit Ihrem Cloud Central-Konto installiert und eingerichtet. Cloud Manager nutzt diesen Connector automatisch bei der Erstellung neuer Arbeitsumgebungen. Aber wenn Sie mehr als einen Connector haben, müssen Sie dies tun "Wechseln Sie zwischen ihnen".

Erstellen eines Connectors über den Azure Marketplace

Am besten sollte ein Connector direkt aus Cloud Manager erstellt werden, aber Sie können einen Connector auf Wunsch im Azure Marketplace starten. Nachdem Sie den Connector erstellt und eingerichtet haben, wird er automatisch bei der Erstellung neuer Arbeitsumgebungen verwendet.

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 Ihr Cloud Central Konto anzugeben.

Schritte

1. "Wechseln Sie zur Azure Marketplace-Seite für Cloud Manager".
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:

- Cloud Manager kann mit HDD- oder SSD-Festplatten 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.

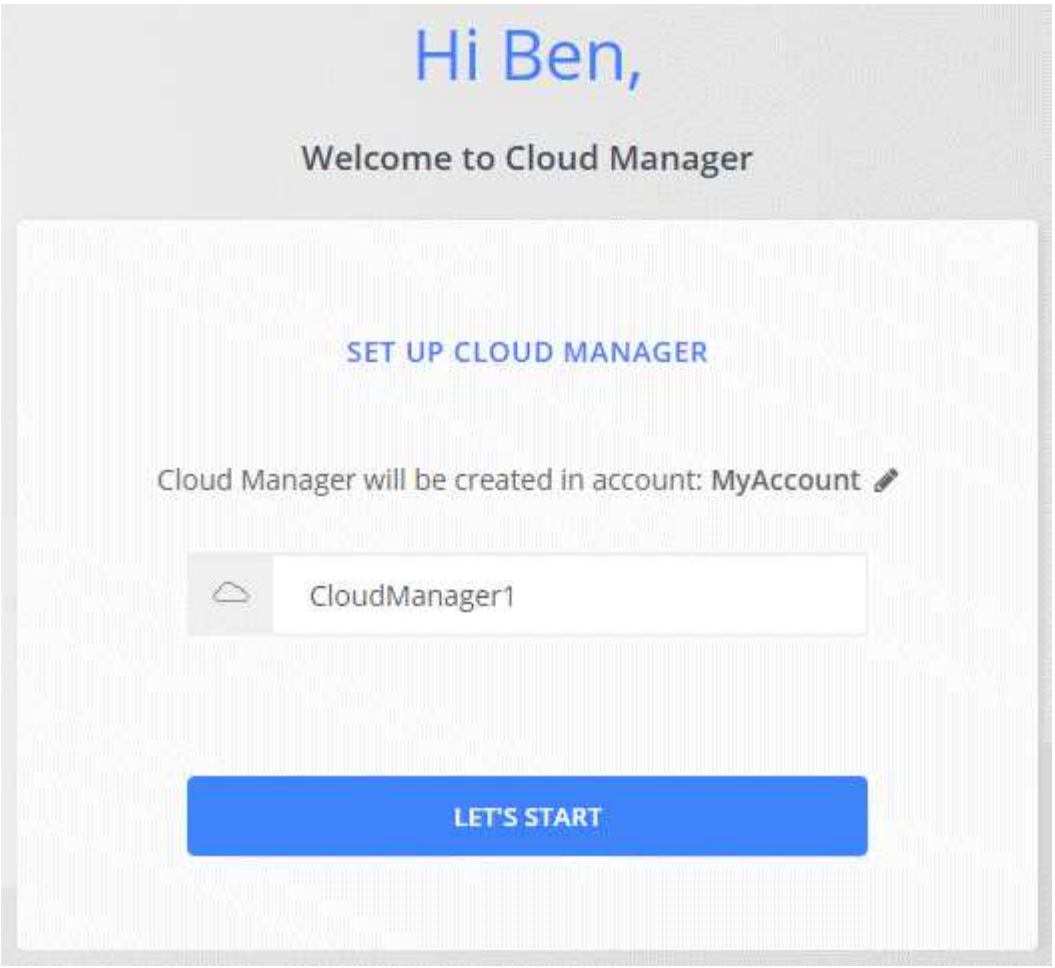
5. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung mit der virtuellen Verbindungsmaschine hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

6. Richten Sie nach der Anmeldung den Konnektor ein:
   a. Geben Sie das Cloud Central-Konto an, das mit dem Connector verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Der Connector ist jetzt installiert und eingerichtet. Sie müssen Azure Berechtigungen erteilen, bevor Benutzer Cloud Volumes ONTAP in Azure bereitstellen können.

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 Sie eine benutzerdefinierte Rolle mithilfe der Cloud Manager-Richtlinie:

   a. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".

   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-c25fbzzzzzzzzzzzzz", "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzzzz", "/subscriptions/398e471c-3b42-4zzae7-

9b59-zzz"

c. Verwenden Sie die JSON-Datei, um eine benutzerdefinierte Rolle in Azure zu erstellen.

   Im folgenden Beispiel wird gezeigt, wie eine benutzerdefinierte Rolle mithilfe der Azure CLI 2.0 erstellt wird:

   ```
   az role definition create --role-definition
   C:\Policy_for_cloud_Manager_Azure_3.8.7.json
   ```

Sie sollten nun eine benutzerdefinierte Rolle namens Cloud Manager 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 **Access Control (IAM)**.
   c. Klicken Sie auf **Hinzufügen** > **Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **Cloud Manager Operator** aus.

        Cloud Manager Operator ist der im angegebene Standardname "Cloud Manager-Richtlinie". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

      - Weisen Sie einer **virtuellen Maschine** Zugriff zu.
      - Wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde.
      - Wählen Sie die virtuelle Verbindungsmaschine aus.
      - Klicken Sie Auf **Speichern**.
   d. 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. Cloud Manager nutzt diesen Connector automatisch bei der Erstellung neuer Arbeitsumgebungen. Aber wenn Sie mehr als einen Connector haben, müssen Sie dies tun "Wechseln Sie zwischen ihnen".

Installieren der Connector-Software auf einem vorhandenen Linux-Host

Die geläufigste Methode zur Erstellung eines Connectors besteht direkt über Cloud Manager 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.

Wenn Sie ein Cloud Volumes ONTAP-System in Google Cloud erstellen möchten, dann müssen Sie einen Connector in Google Cloud laufen, sowie. Sie können keinen Konnektor verwenden, der an einem anderen Standort ausgeführt wird.

Anforderungen

- Der Host muss sich erfüllen "Anforderungen an den Steckverbinder".
- Ein Red Hat Enterprise Linux-System muss bei Red Hat Subscription Management registriert sein. Wenn sie nicht registriert ist, kann das System während der Installation nicht auf Repositorys zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.
- Das Connector-Installationsprogramm greift während der Installation auf mehrere URLs zu. Sie müssen sicherstellen, dass für folgende Endpunkte der ausgehende Internetzugang zugelassen ist:
  - http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
  - https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  - https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

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

Über diese Aufgabe

- Root-Berechtigungen sind zur Installation des Connectors nicht erforderlich.
- 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. Laden Sie die Software von Cloud Manager herunter "NetApp Support Website", Und dann kopieren Sie es auf den Linux-Host.

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

2. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   Beispiel

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Führen Sie das Installationsskript aus:
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   Silent führt die Installation aus, ohne dass Sie zur Information aufgefordert werden.

   Proxy ist erforderlich, wenn sich der Host hinter einem Proxy-Server befindet.

proxyport ist der Port für den Proxy-Server.

Proxyuser ist der Benutzername für den Proxy-Server, wenn eine grundlegende Authentifizierung erforderlich ist.

Proxypwd ist das Passwort für den von Ihnen angegebenen Benutzernamen.

3. Wenn Sie den Silent-Parameter nicht angegeben haben, geben Sie **Y** ein, um das Skript fortzusetzen, und geben Sie anschließend die HTTP- und HTTPS-Ports ein, wenn Sie dazu aufgefordert werden.

   Cloud Manager ist jetzt installiert. Nach Abschluss der Installation wird der Cloud Manager-Dienst (occm) zweimal neu gestartet, wenn Sie einen Proxyserver angegeben haben.

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

   https://ipaddress:port

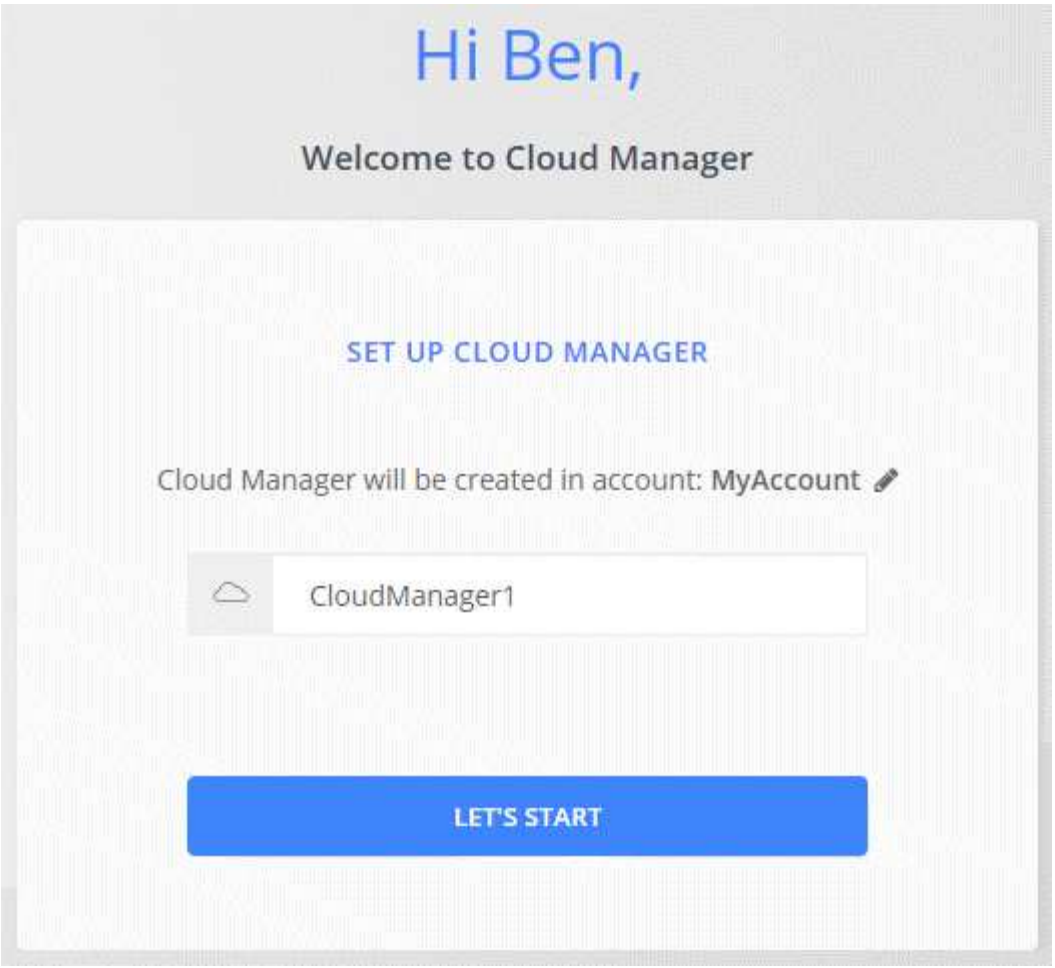
   Ipaddress kann abhängig von der Konfiguration des Hosts localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Connector beispielsweise ohne öffentliche IP-Adresse in der Public Cloud befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung zum Connector-Host hat.

   Port ist erforderlich, wenn Sie die Standard-HTTP (80)- oder HTTPS (443)-Ports geändert haben. Wenn beispielsweise der HTTPS-Port in 8443 geändert wurde, würden Sie eingeben https://ipaddress:8443

5. Melden Sie sich bei NetApp Cloud Central an oder melden Sie sich an.
6. Richten Sie Cloud Manager nach dem Einloggen ein:
   a. Geben Sie das Cloud Central-Konto an, das mit dem Connector verknüpft werden soll.

      "Weitere Informationen zu Cloud Central Accounts".

   b. Geben Sie einen Namen für das System ein.



Ergebnis

Der Connector ist jetzt mit Ihrem Cloud Central-Konto installiert und eingerichtet. Cloud Manager nutzt diesen Connector automatisch bei der Erstellung neuer Arbeitsumgebungen.

Nachdem Sie fertig sind

Einrichtung von Berechtigungen, damit Cloud Manager Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung managen kann:

- AWS, "AWS Konto einrichten und dann zu Cloud Manager hinzufügen".
- Azure: "Richten Sie ein Azure-Konto ein, und fügen Sie es anschließend zu Cloud Manager hinzu".
- GCP: Richten Sie ein Service-Konto ein, das über die Berechtigungen verfügt, die Cloud Manager für die Erstellung und das Management von Cloud Volumes ONTAP-Systemen in Projekten benötigt.
  a. "Rolle in GCP anlegen" Dazu gehören die im definierten Berechtigungen "Cloud Manager-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, "Sie gewähren Zugriff, indem Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzufügen". Sie müssen diesen Schritt für jedes Projekt wiederholen.

Standardkonfiguration für den Konnektor

Wenn Sie eine Fehlerbehebung für den Konnektor benötigen, können Sie die Konfiguration des Connectors unter Umständen besser verstehen.

- Bei der Implementierung des Connectors über Cloud Manager (oder direkt über den Marketplace eines Cloud-Providers) ist Folgendes zu beachten:
  - In AWS lautet der Benutzername für die EC2 Linux-Instanz ec2-user.
  - Das Betriebssystem für das Image lautet wie folgt:
    - AWS: Red hat Enterprise Linux 7.5 (HVM)
    - Azure: Red hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6

      Das Betriebssystem enthält keine GUI. Sie müssen ein Terminal verwenden, um auf das System zuzugreifen.
- Der Installationsordner des Connectors befindet sich an folgender Stelle:

  /opt/application/netapp/cloudmanager
- Protokolldateien befinden sich im folgenden Ordner:

  /opt/application/netapp/cloudmanager/log
- Der Cloud Manager Service heißt occm.
- Der occm-Dienst ist vom MySQL-Dienst abhängig.

  Wenn der MySQL-Dienst nicht verfügbar ist, ist auch der occm-Dienst nicht verfügbar.
- Cloud Manager installiert die folgenden Pakete auf dem Linux-Host, sofern sie noch nicht installiert sind:
  - 7-Zip
  - AWSCLI
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Ziehen
  - Wget
- Der Connector verwendet die folgenden Ports auf dem Linux-Host:
  - 80 für HTTP-Zugriff
  - 443 für HTTPS-Zugriff
  - 3306 für die Cloud Manager-Datenbank
  - 8080 für den Cloud Manager-API-Proxy

- 8666 für die Service Manager API
- 8777 für die Health-Checker Container Service API

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.