Management Von Cloud Manager

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

Management Von Cloud Manager

Suchen der System-ID des Cloud Manager

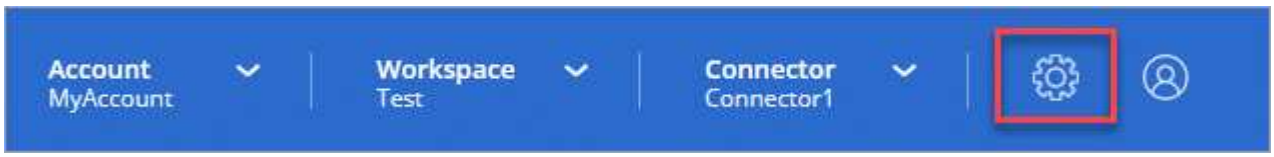
Um Ihnen bei den ersten Schritten zu helfen, wird Sie möglicherweise von Ihrem NetApp Vertriebsmitarbeiter nach Ihrer Cloud Manager System-ID gefragt. Die ID wird in der Regel für Lizenzierungs- und Fehlerbehebungszwecke verwendet.

Was Sie benötigen

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

Schritte

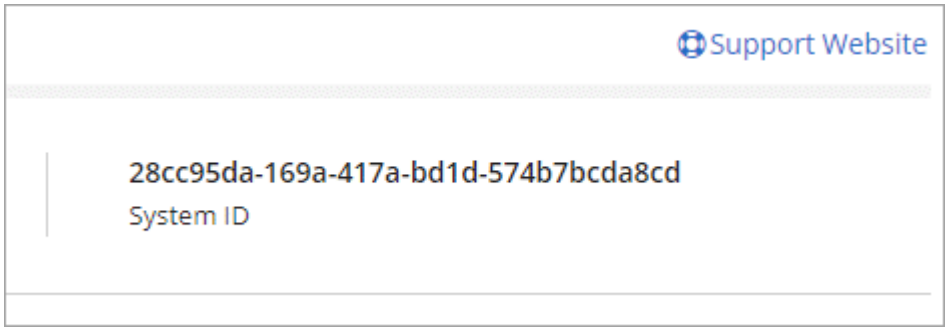
1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen.



2. Klicken Sie Auf **Support Dashboard**.

   Ihre System-ID wird oben rechts angezeigt.

   Beispiel



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.

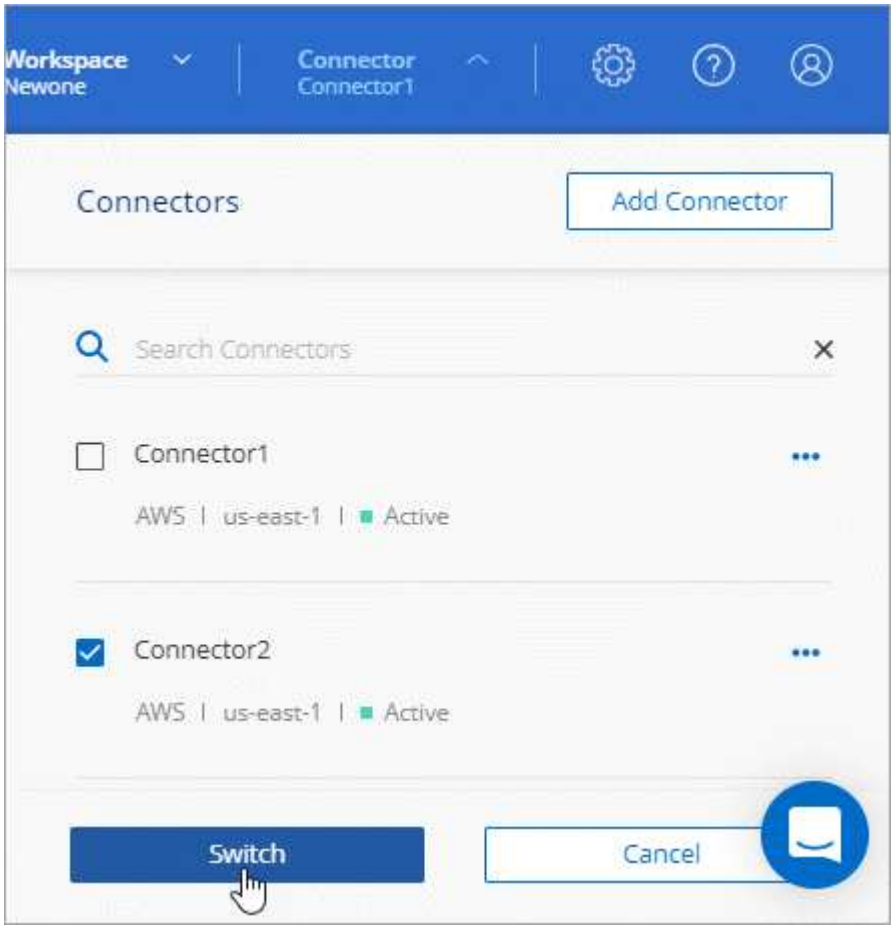
Wechseln zwischen den Anschlüssen

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)

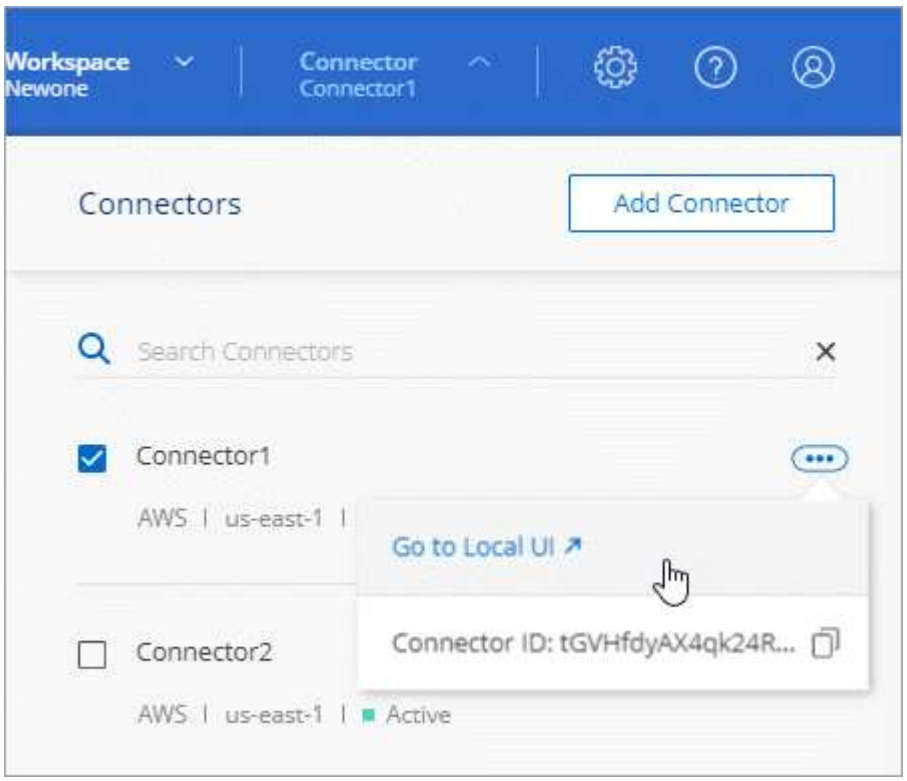
Schritte

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

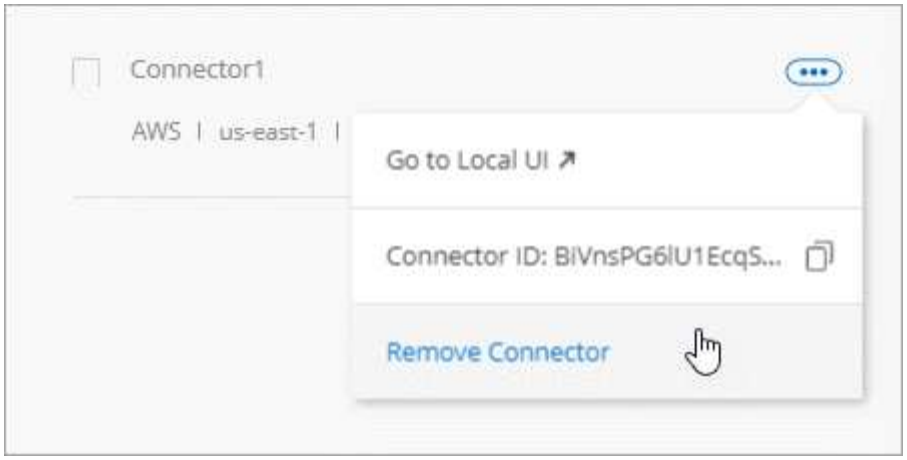
Wenn ein Connector inaktiv ist, können Sie ihn aus der Liste der Anschlüsse in Cloud Manager entfernen. Sie können dies tun, wenn Sie die virtuelle Connector-Maschine gelöscht oder die Connector-Software deinstalliert haben.

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

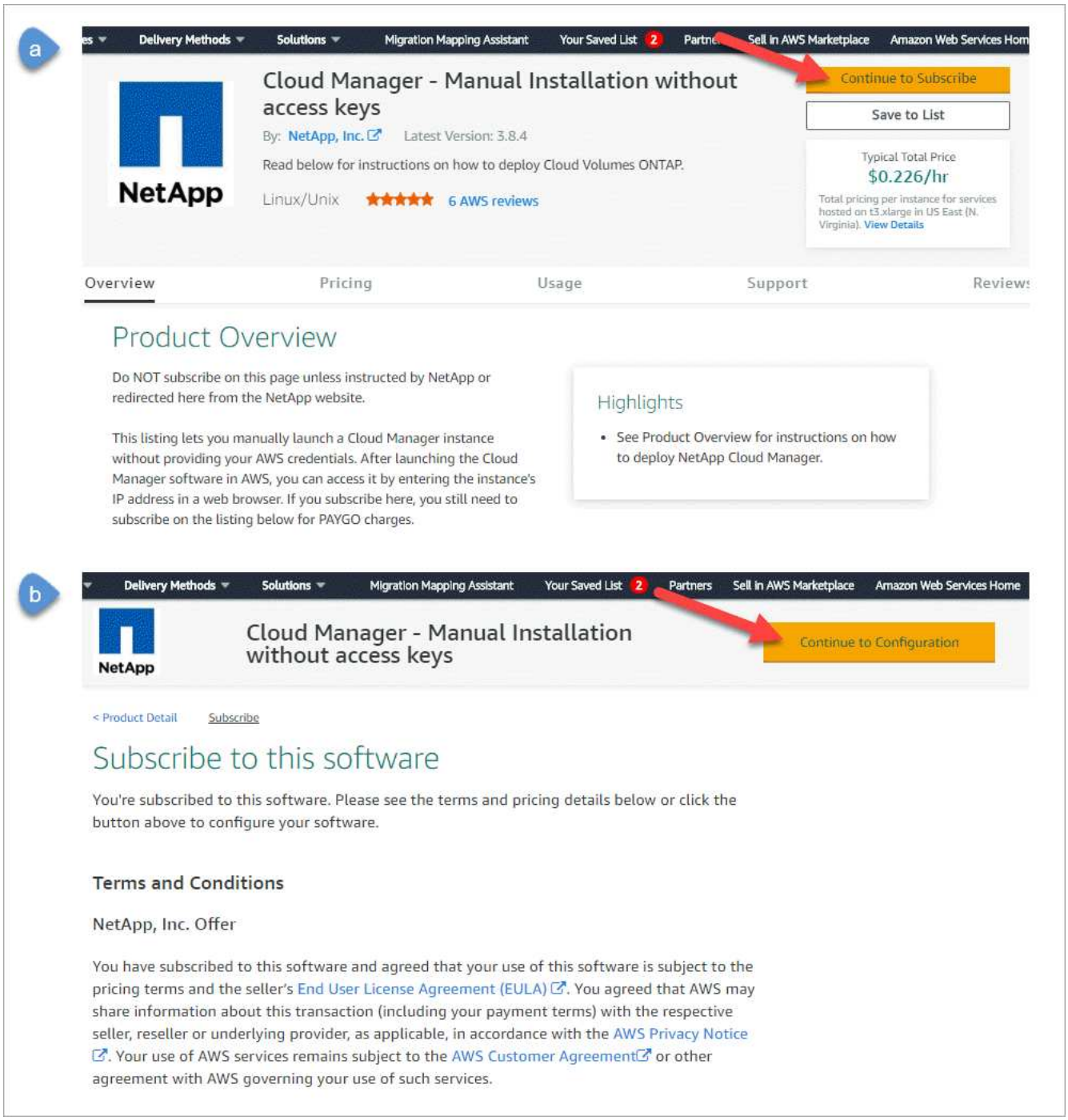
1. IAM-Richtlinie und -Rolle für die EC2-Instanz erstellen:
   a. Laden Sie die Cloud Manager IAM-Richtlinie von folgendem Speicherort herunter:

      "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**.



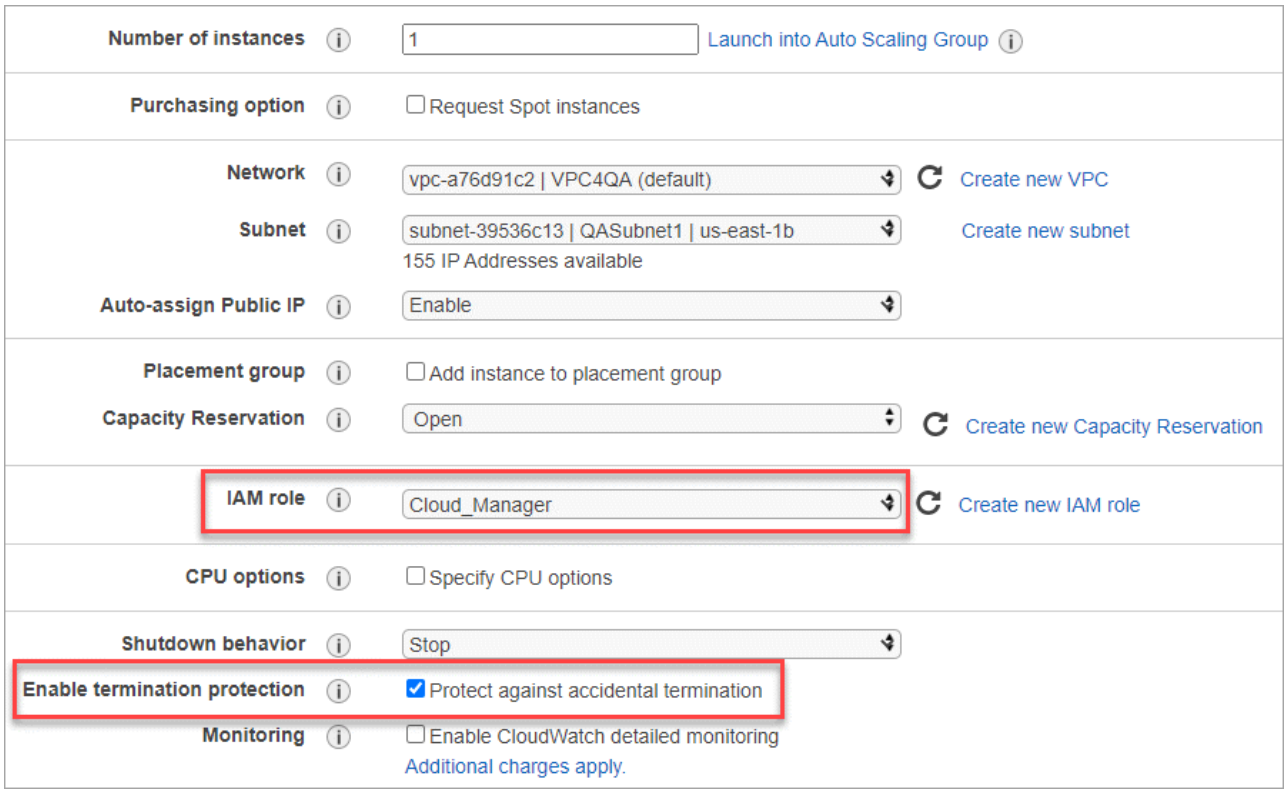
4. Ändern Sie eine der Standardoptionen, und klicken Sie auf **Weiter zum Starten**.
5. Wählen Sie unter **Aktion auswählen über EC2 starten** und klicken Sie dann auf **Start**.

   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.

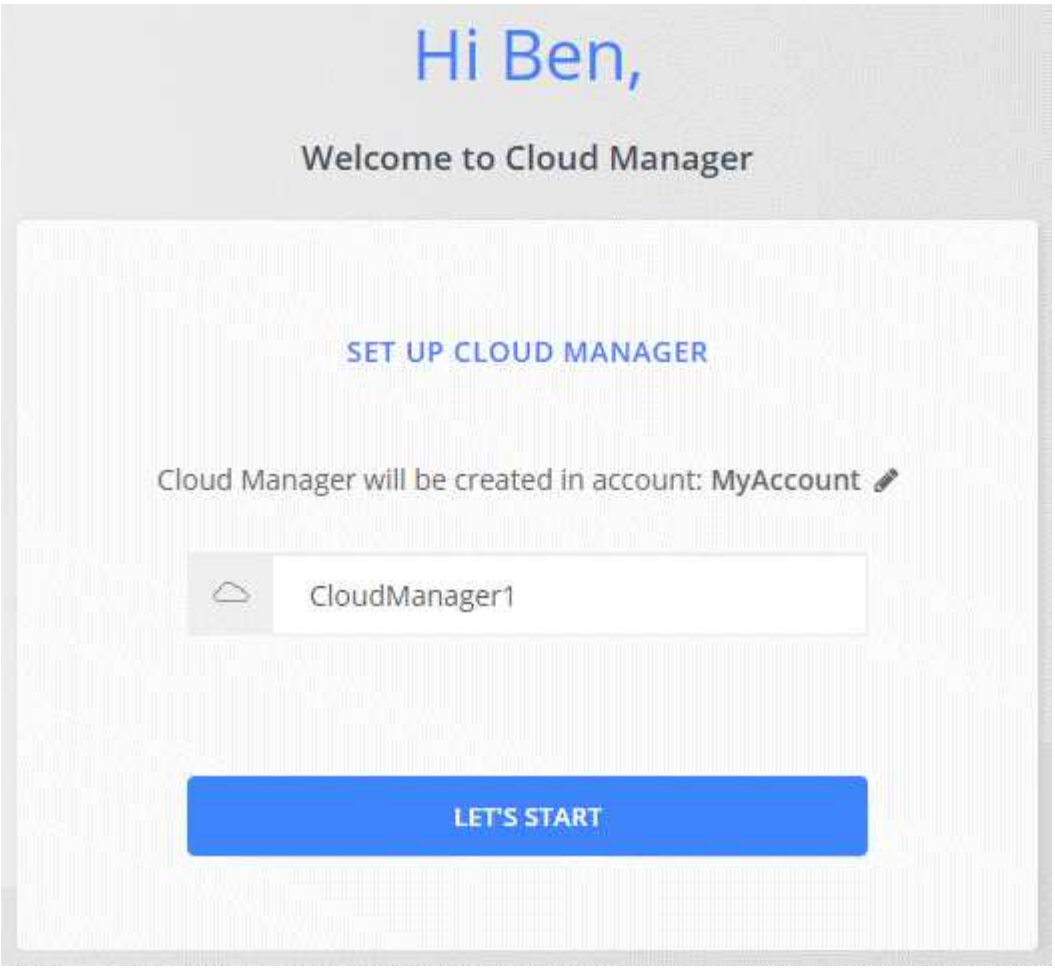
7. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung zur Verbindungsinstanz hat, und geben Sie die folgende URL ein:

   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.

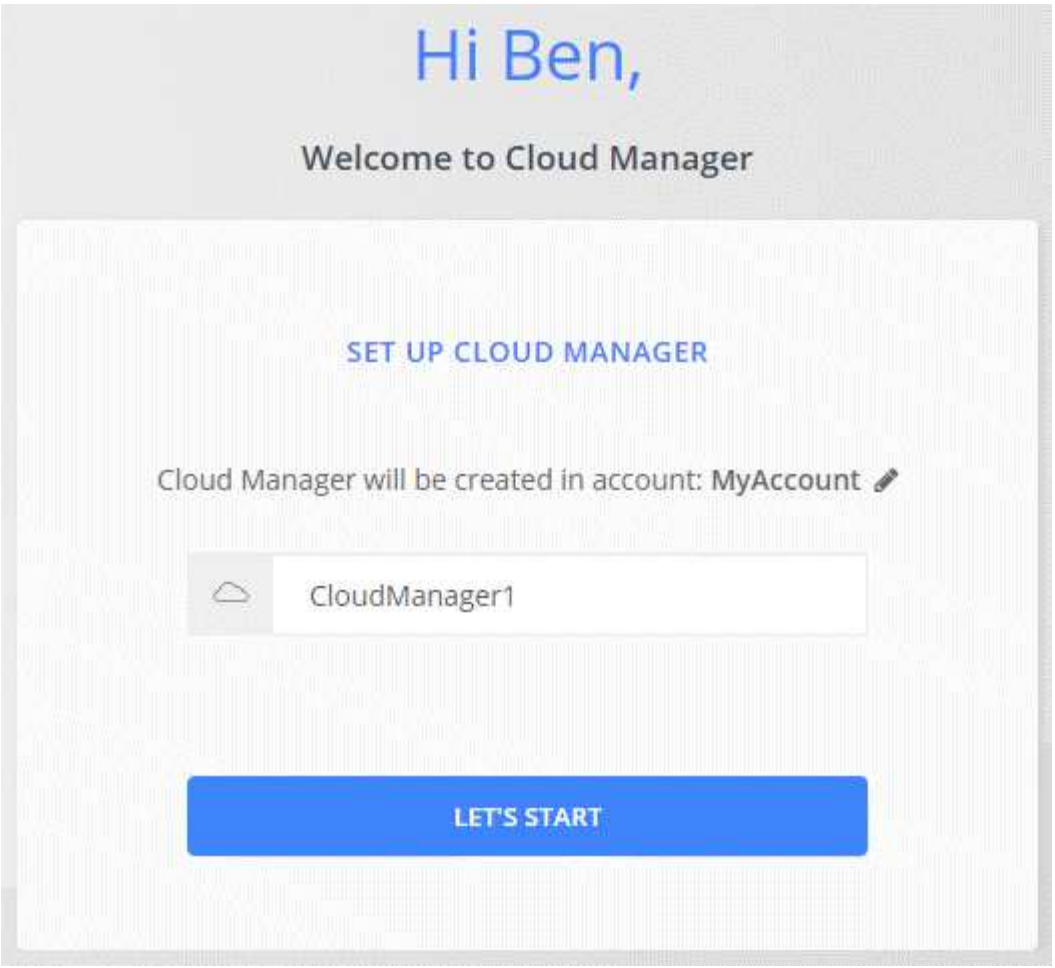
5. Öffnen Sie einen Webbrowser von einem Host, der eine Verbindung mit der virtuellen Verbindungsmaschine hat, und geben Sie die folgende URL ein:

   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

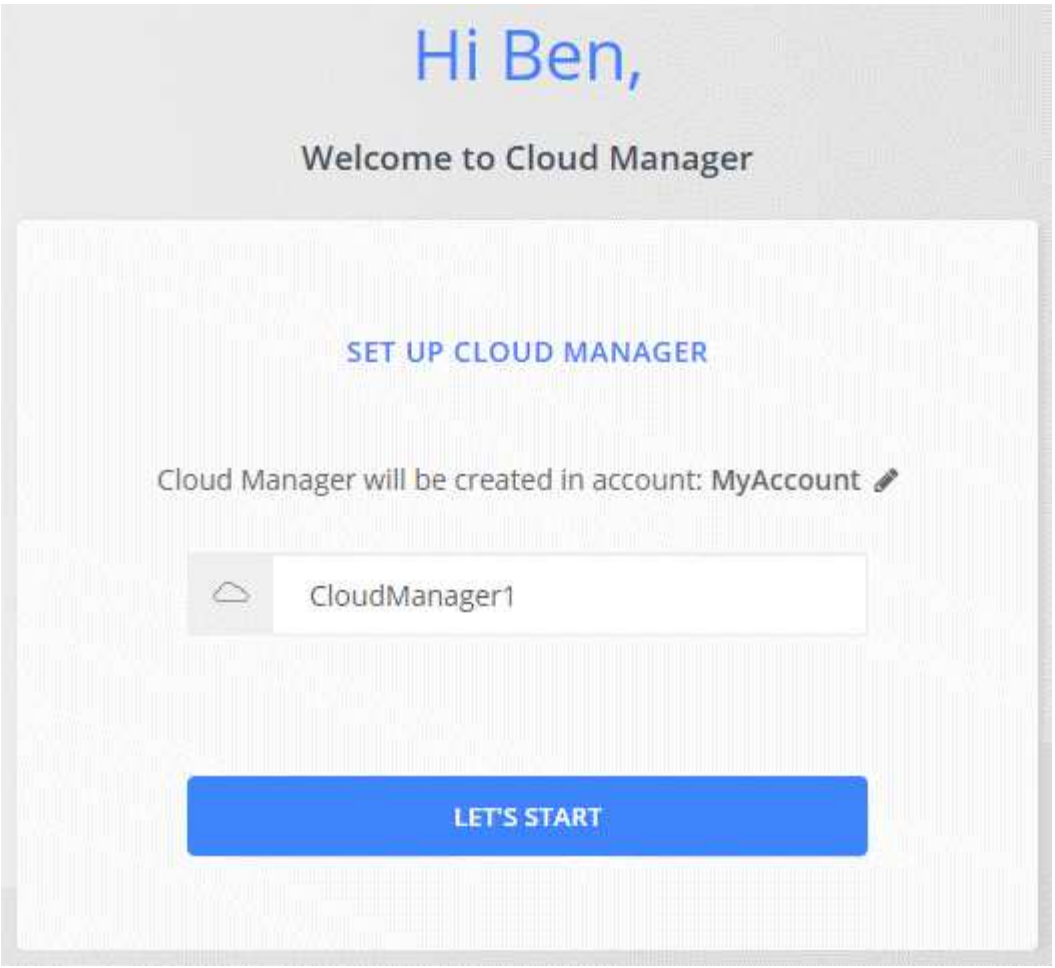
   Ipaddress kann abhängig von der Konfiguration des Hosts localhost, eine private IP-Adresse oder eine öffentliche IP-Adresse sein. Wenn sich der Connector beispielsweise ohne öffentliche IP-Adresse in der Public Cloud befindet, müssen Sie eine private IP-Adresse von einem Host eingeben, der eine Verbindung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

Anmeldeinformationen verwalten

AWS

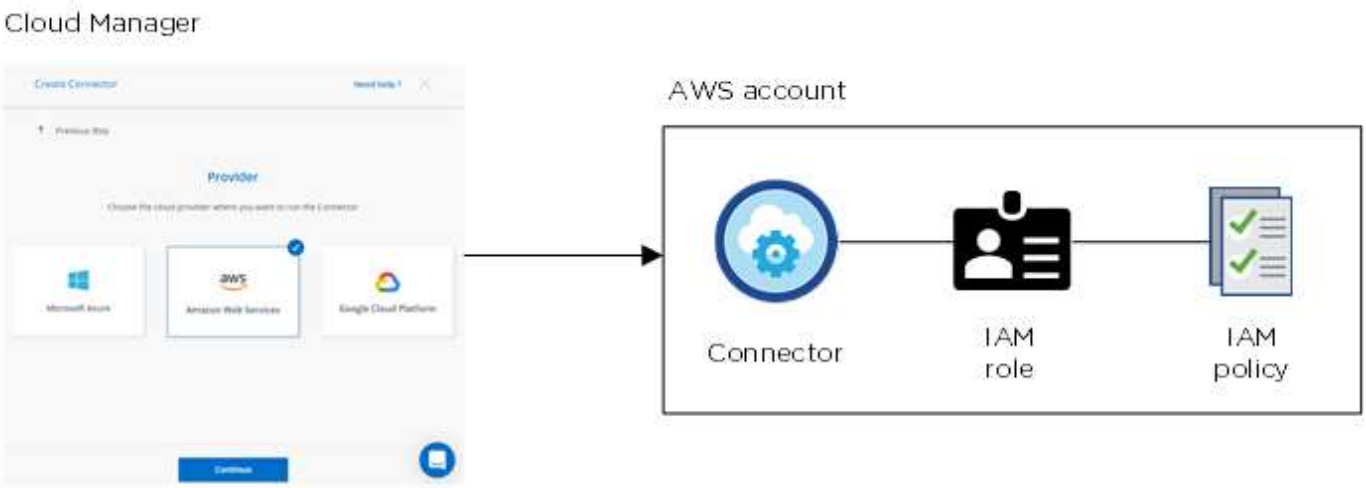
AWS Zugangsdaten und Berechtigungen

Mit Cloud Manager können Sie die AWS Zugangsdaten auswählen, die Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten. Alle Cloud Volumes ONTAP Systeme können über die ersten AWS Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

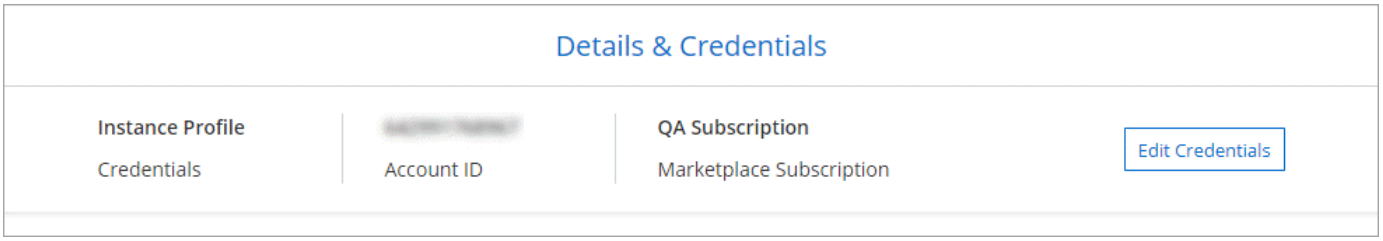
Erste AWS Zugangsdaten

Wenn Sie einen Connector von Cloud Manager bereitstellen, müssen Sie ein AWS-Konto mit Berechtigungen zum Starten der Connector-Instanz verwenden. Die erforderlichen Berechtigungen werden im aufgeführt "Connector-Implementierungsrichtlinie für AWS".

Wenn Cloud Manager die Connector-Instanz in AWS startet, erstellt sie eine IAM-Rolle und ein Instanzprofil für die Instanz. Zudem wird eine Richtlinie angehängt, die Cloud Manager Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. "Überprüfen Sie, wie Cloud Manager die Berechtigungen verwendet".

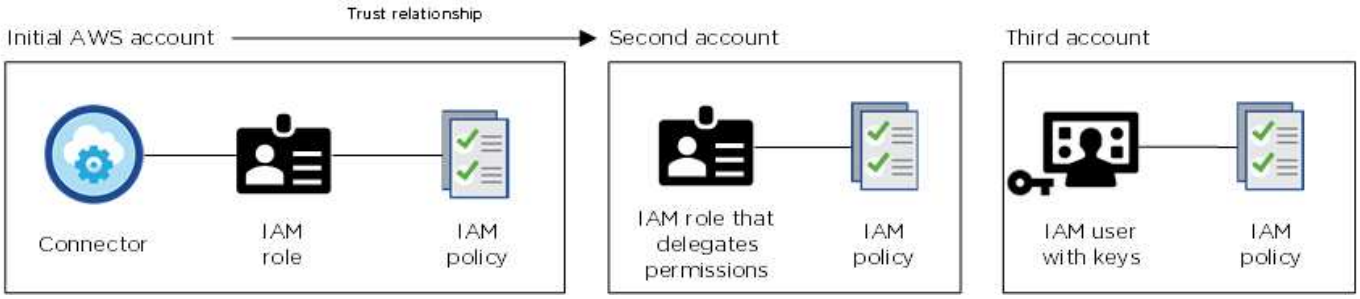


Cloud Manager wählt die AWS Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:



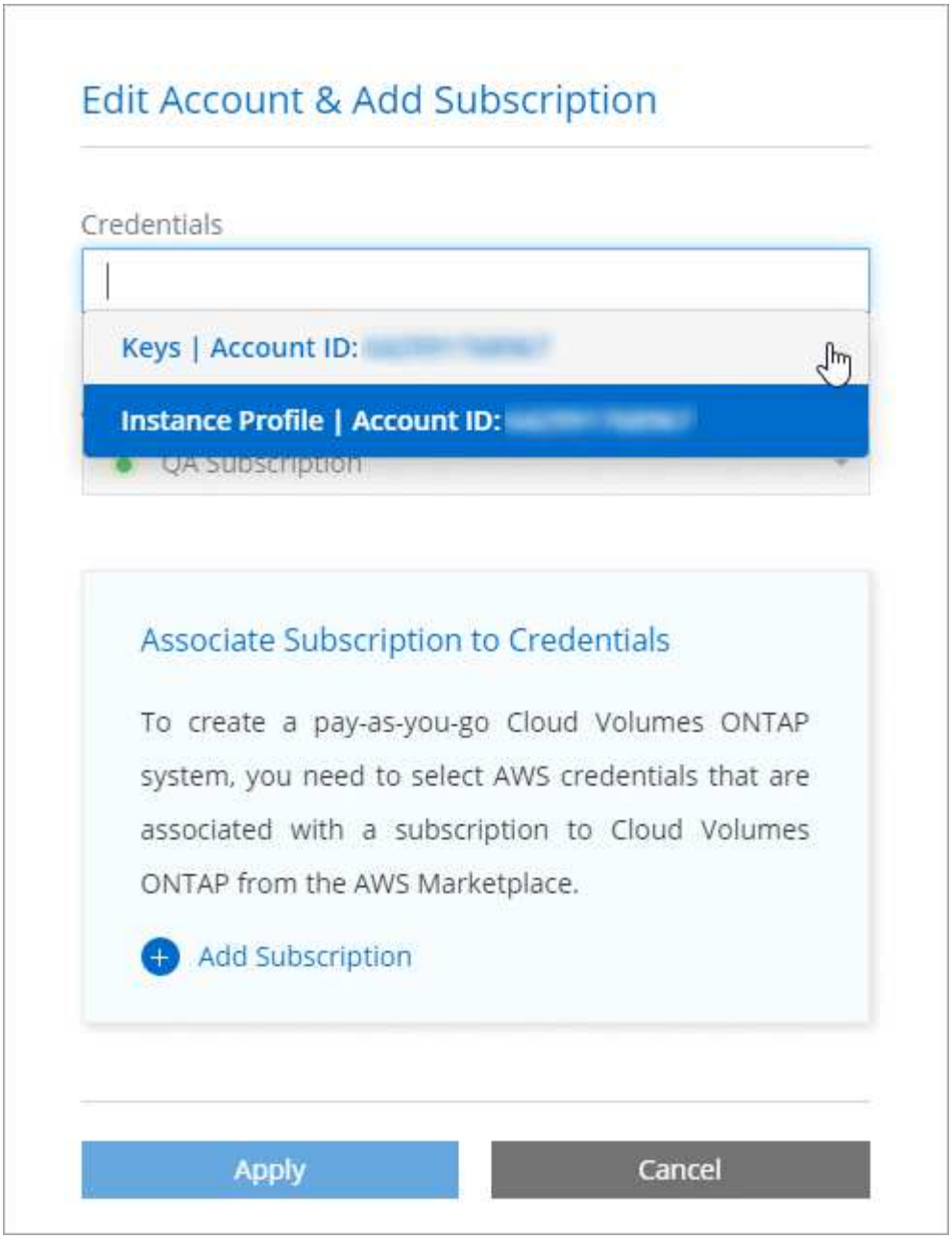
Zusätzliche AWS Zugangsdaten

Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Accounts starten möchten, haben Sie eine der Möglichkeiten "AWS Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen". Die folgende Abbildung zeigt zwei zusätzliche Konten: Eines mit Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto und ein weiteres über die AWS Schlüssel eines IAM-Benutzers:



Das würden Sie dann tun "Fügen Sie die Kontoanmeldeinformationen zu Cloud Manager hinzu" Indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Nachdem Sie einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Wie sieht es mit Marketplace-Implementierungen und On-Premises-Implementierungen aus?

In den obigen Abschnitten wird die empfohlene Implementierungsmethode für den Connector, der aus Cloud Manager stammt, beschrieben. Sie können auch einen Connector in AWS von der bereitstellen "AWS Marketplace" Und das können Sie auch "Installieren Sie den Steckverbinder vor Ort".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Bei On-Premises-Implementierungen können nicht eine IAM-Rolle für das Cloud Manager-System eingerichtet werden, Sie können aber Berechtigungen wie bei zusätzlichen AWS-Konten bereitstellen.

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Wie oben beschrieben, können Sie mit Cloud Manager AWS Zugangsdaten auf verschiedene Arten

bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel.

Bei den ersten beiden Optionen verwendet Cloud Manager den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dies ist die Best Practice, also automatisch und sicher.

Wenn Sie Cloud Manager mit AWS-Zugriffsschlüsseln bereitstellen, sollten Sie die Schlüssel drehen, indem Sie sie in Cloud Manager in einem regelmäßigen Intervall aktualisieren. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Verwalten von AWS Anmeldedaten und Abonnements für Cloud Manager

Wenn Sie ein Cloud Volumes ONTAP System erstellen, müssen Sie die AWS Zugangsdaten und das Abonnement auswählen, die mit diesem System verwendet werden sollen. Wenn Sie mehrere AWS-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen AWS Zugangsdaten zuweisen.

Bevor Sie Cloud Manager mit AWS Zugangsdaten ergänzen, müssen Sie die erforderlichen Berechtigungen für dieses Konto bereitstellen. Mit den Berechtigungen kann Cloud Manager Ressourcen und Prozesse innerhalb dieses AWS Kontos verwalten. Wie Sie die Berechtigungen bereitstellen, hängt davon ab, ob Sie Cloud Manager mit AWS Schlüsseln oder dem ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen möchten.

Bei der Bereitstellung eines Connectors von Cloud Manager fügte Cloud Manager automatisch AWS Zugangsdaten für das Konto hinzu, in dem Sie den Connector implementiert haben. Dieses erste Konto wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. "Weitere Informationen zu AWS Zugangsdaten und Berechtigungen".

Auswahl

- Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln
- Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Mit Cloud Manager können Sie AWS Zugangsdaten auf verschiedene Arten bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder die Bereitstellung von AWS Zugriffsschlüssel. "Weitere Informationen zu AWS Zugangsdaten und Berechtigungen".

Bei den ersten beiden Optionen verwendet Cloud Manager den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dieser Prozess gilt als Best Practice, also automatisch und sicher.

Wenn Sie Cloud Manager mit AWS-Zugriffsschlüsseln bereitstellen, sollten Sie die Schlüssel drehen, indem Sie sie in Cloud Manager in einem regelmäßigen Intervall aktualisieren. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Wenn Sie Cloud Manager mit AWS Schlüsseln für einen IAM-Benutzer bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die Cloud Manager IAM-Richtlinie definiert die AWS-Aktionen und -Ressourcen, die Cloud Manager verwenden darf.

Schritte

1. Laden Sie die IAM-Richtlinie von Cloud Manager aus herunter "Seite „Cloud Manager Policies“ aufgeführt".
2. Erstellen Sie über die IAM-Konsole Ihre eigene Richtlinie, indem Sie den Text aus der Cloud Manager IAM-Richtlinie kopieren und einfügen.

   "AWS Dokumentation: Erstellung von IAM-Richtlinien"

3. Hängen Sie die Richtlinie an eine IAM-Rolle oder einen IAM-Benutzer an.
   - "AWS Documentation: Erstellung von IAM-Rollen"
   - "AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien"

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu Cloud Manager hinzufügen.

Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

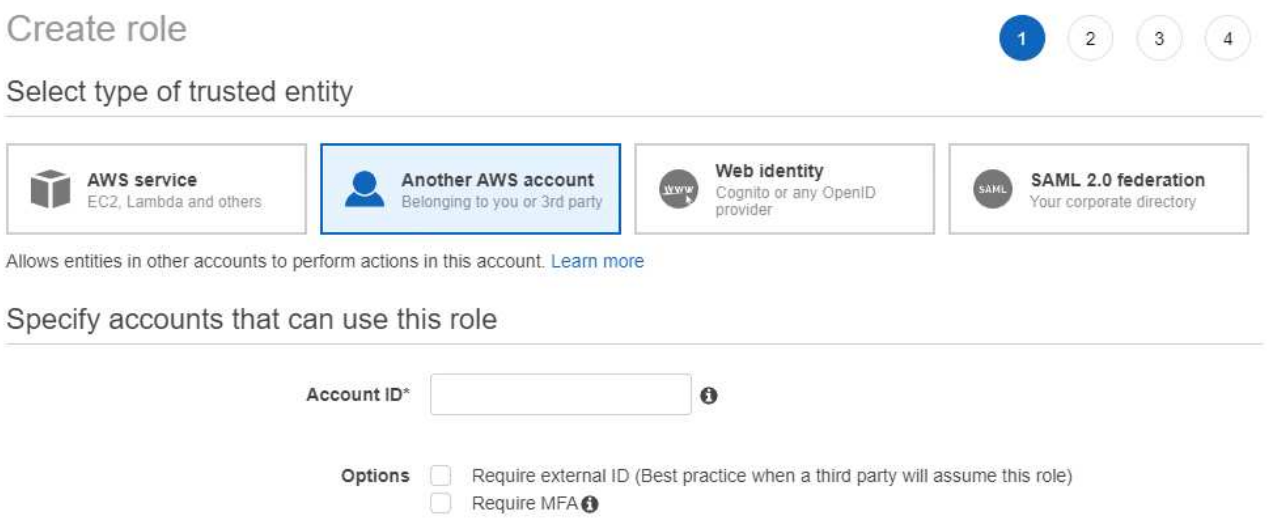
Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Connector-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie Cloud Manager über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

Schritte

1. Rufen Sie das Zielkonto auf, in dem Sie Cloud Volumes ONTAP bereitstellen und eine IAM-Rolle erstellen möchten, indem Sie **ein weiteres AWS-Konto** auswählen.

   Gehen Sie wie folgt vor:

   - Geben Sie die ID des Kontos ein, auf dem sich die Connector-Instanz befindet.
   - Hängen Sie die Cloud Manager IAM-Richtlinie an, die über die erhältlich ist "Seite „Cloud Manager Policies“ aufgeführt".



2. Gehen Sie zum Quellkonto, auf dem sich die Konnektorinstanz befindet, und wählen Sie die IAM-Rolle aus, die an die Instanz angehängt ist.

   a. Klicken Sie auf **Richtlinien anhängen** und dann auf **Richtlinien erstellen**.

   b. Erstellen Sie eine Richtlinie, die die Aktion „STS:AssumeRole“ und den ARN der Rolle umfasst, die Sie im Zielkonto erstellt haben.

      Beispiel

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Ergebnis

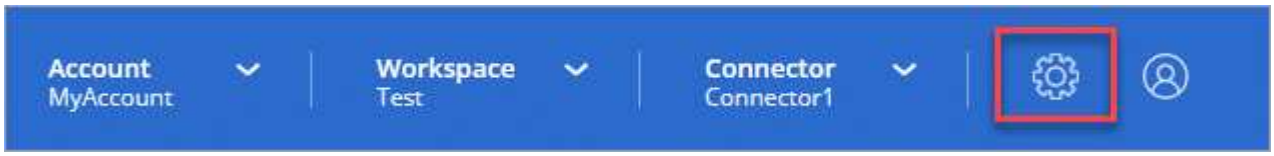
Das Konto verfügt nun über die erforderlichen Berechtigungen. Sie können es jetzt zu Cloud Manager hinzufügen.

AWS Zugangsdaten zu Cloud Manager hinzufügen

Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen eingerichtet haben, können Sie die Anmeldedaten für dieses Konto bei Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



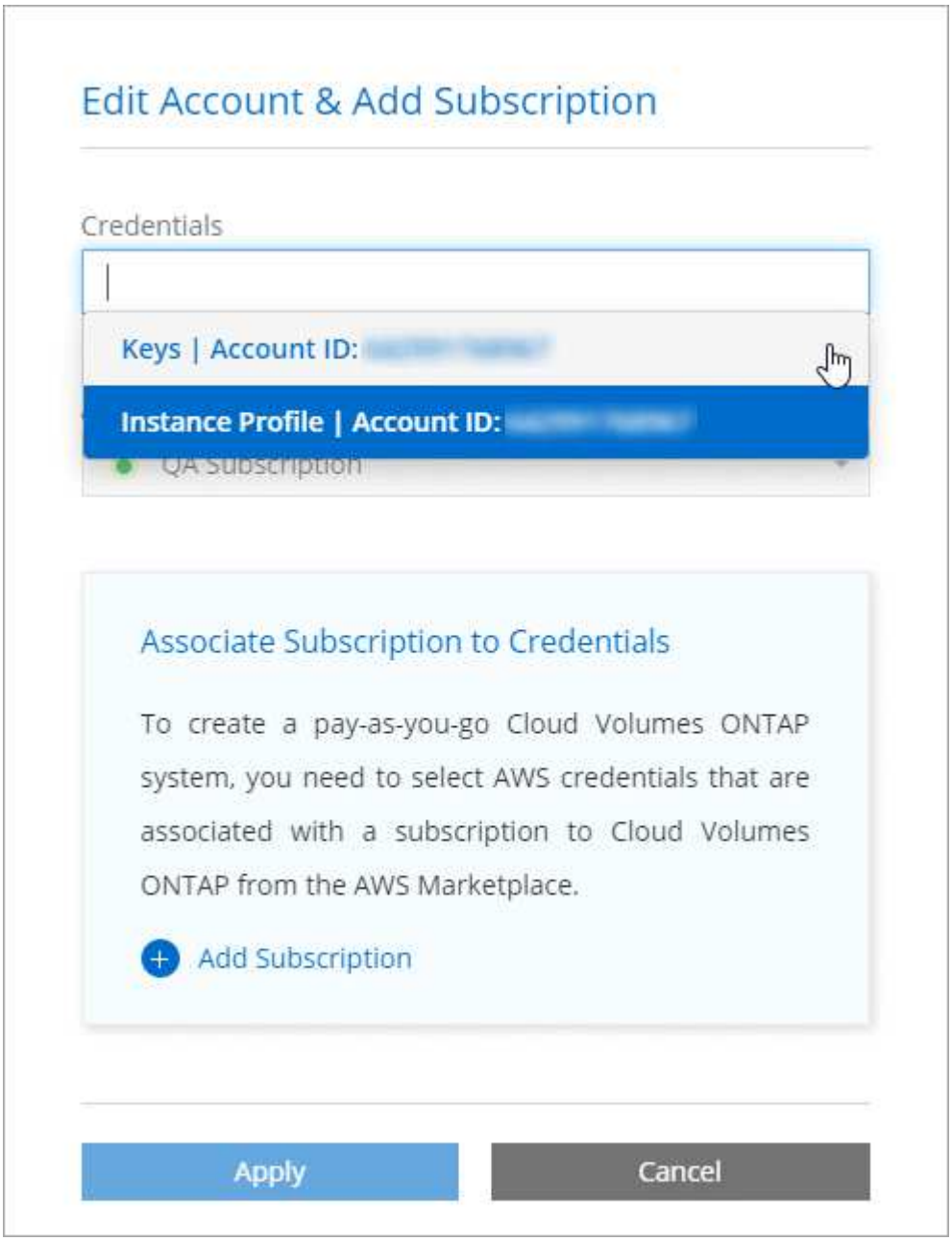
2. Klicken Sie auf **Anmeldedaten hinzufügen** und wählen Sie **AWS**.
3. Bereitstellen von AWS Schlüsseln oder dem ARN einer vertrauenswürdigen IAM-Rolle
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie auf **Weiter**.
5. Wählen Sie das Pay-as-you-go-Abonnement aus, das Sie mit den Anmeldedaten verknüpfen möchten, oder klicken Sie auf **Abonnement hinzufügen**, wenn Sie noch nicht über ein Abonnement verfügen.

   Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen AWS Zugangsdaten über den AWS Marketplace mit einem Abonnement für Cloud Volumes ONTAP verknüpft werden.

6. Klicken Sie Auf **Hinzufügen**.

Ergebnis

Sie können jetzt bei der Erstellung einer neuen Arbeitsumgebung auf eine andere Gruppe von Anmeldeinformationen von der Seite Details und Anmeldeinformationen wechseln:



Verknüpfen eines AWS Abonnements mit den Zugangsdaten

Nachdem Sie Ihre AWS Zugangsdaten zu Cloud Manager hinzugefügt haben, können Sie ein AWS Marketplace Abonnement mit diesen Anmeldedaten verknüpfen. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement verknüpfen können, nachdem Sie bereits die Anmeldedaten zu Cloud Manager hinzugefügt haben:

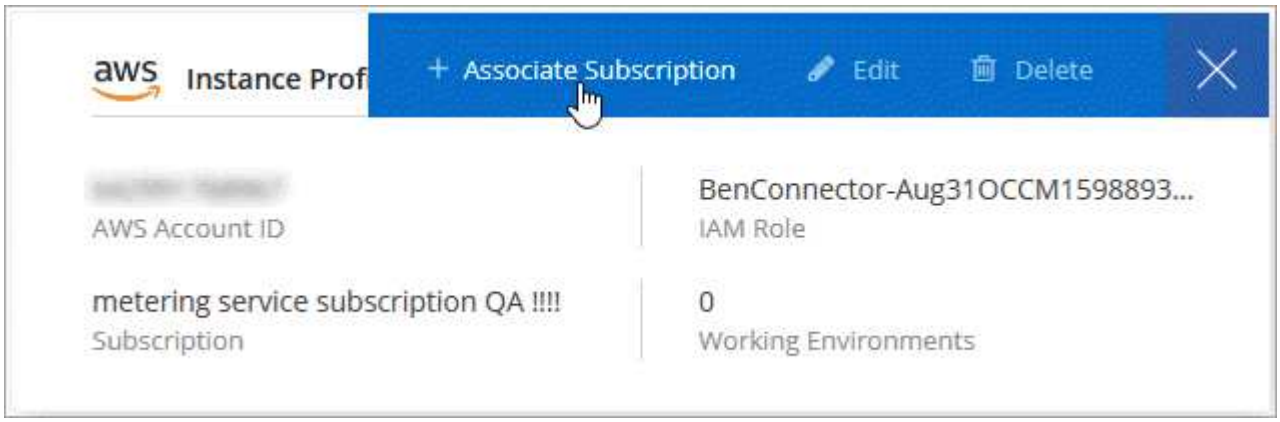
- Sie haben ein Abonnement nicht zugeordnet, wenn Sie zum ersten Mal die Anmeldedaten zu Cloud Manager hinzugefügt haben.
- Sie möchten ein vorhandenes AWS Marketplace Abonnement durch ein neues Abonnement ersetzen.

Was Sie benötigen

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

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Bewegen Sie den Mauszeiger über einen Satz von Anmeldeinformationen, und klicken Sie auf das Aktivitätsmenü.
3. Klicken Sie im Menü auf **Abonnement verknüpfen**.



4. Wählen Sie ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

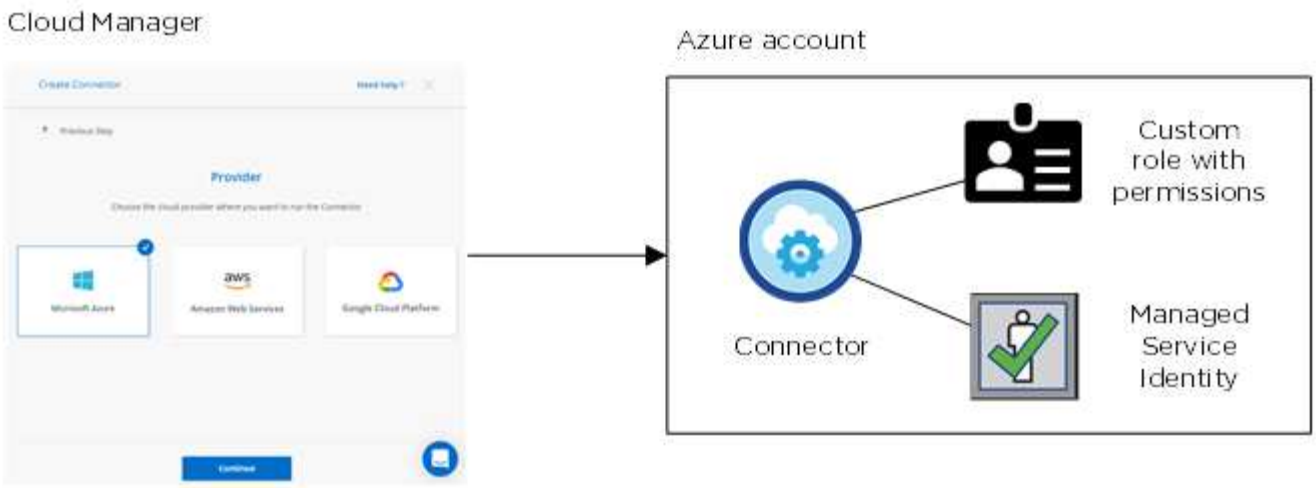
Azure Zugangsdaten und Berechtigungen

Mit Cloud Manager können Sie die Azure Zugangsdaten auswählen, die Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten. Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

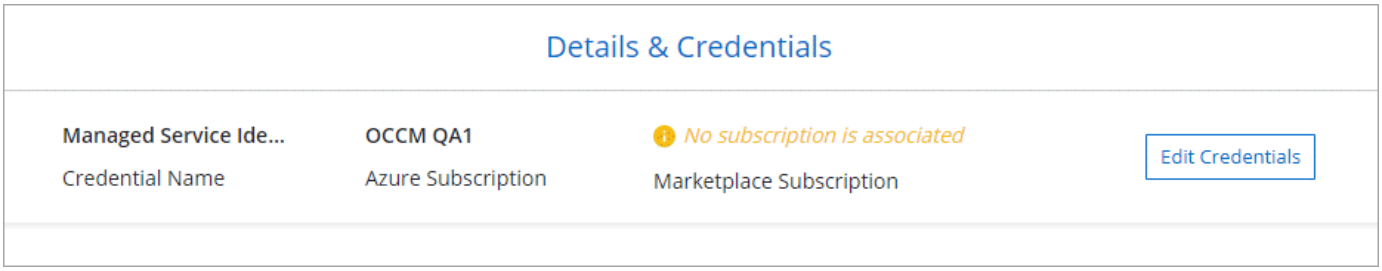
Erste Azure Zugangsdaten

Wenn Sie einen Connector von Cloud Manager bereitstellen, müssen Sie ein Azure-Konto mit Berechtigungen verwenden, um die Virtual Machine Connector bereitzustellen. Die erforderlichen Berechtigungen werden im aufgeführt "Connector-Implementierungsrichtlinie für Azure".

Wenn Cloud Manager die Connector Virtual Machine in Azure implementiert, kann sie ein "Vom System zugewiesene verwaltete Identität" Erstellt auf einer virtuellen Maschine eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Cloud Manager erhält Berechtigungen für das Management von Ressourcen und Prozessen im Rahmen des Azure Abonnements. "Überprüfen Sie, wie Cloud Manager die Berechtigungen verwendet".



Cloud Manager wählt die Azure Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:

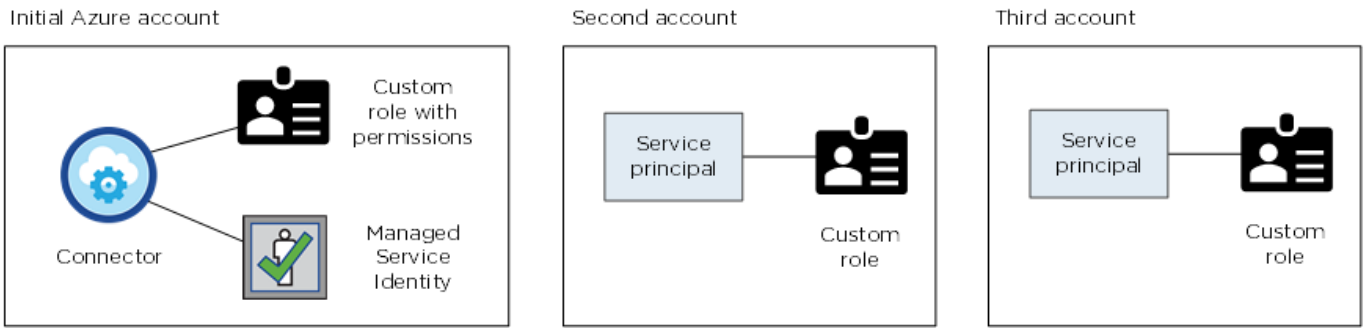


Zusätzliche Azure-Abonnements für eine gemanagte Identität

Die verwaltete Identität ist mit dem Abonnement verbunden, in dem Sie den Connector gestartet haben. Wenn Sie ein anderes Azure Abonnement auswählen möchten, müssen Sie es ausführen "Verknüpfen Sie die verwaltete Identität mit diesen Abonnements".

Zusätzliche Azure Zugangsdaten

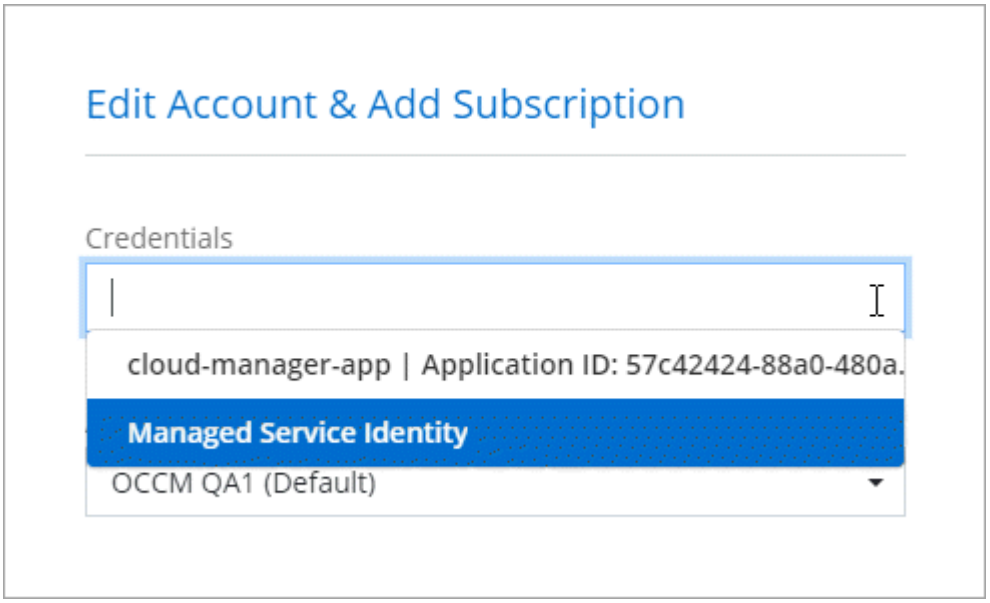
Wenn Sie Cloud Volumes ONTAP mit unterschiedlichen Azure Zugangsdaten implementieren möchten, müssen Sie die erforderlichen Berechtigungen von erteilen "Erstellen und Einrichten eines Service Principal in Azure Active Directory" Für jedes Azure Konto. Das folgende Bild zeigt zwei zusätzliche Konten, die jeweils mit einer Dienstprinzipal- und einer benutzerdefinierten Rolle eingerichtet sind, die Berechtigungen bereitstellt:



Das würden Sie dann tun "Fügen Sie die Kontoanmeldeinformationen zu Cloud Manager hinzu" Durch Angabe von Details zum AD-Dienstprinzipal.

Nachdem Sie einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen

wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Wie sieht es mit Marketplace-Implementierungen und On-Premises-Implementierungen aus?

In den obigen Abschnitten wird die empfohlene Implementierungsmethode für den Connector beschrieben, der aus NetApp Cloud Central stammt. Sie können auch einen Connector in Azure über die bereitstellen "Azure Marketplace", Und Sie können "Installieren Sie den Steckverbinder vor Ort".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die verwaltete Identität für den Connector manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Für On-Premises-Bereitstellungen können Sie keine verwaltete Identität für den Connector einrichten, aber Sie können Berechtigungen wie bei zusätzlichen Konten mit einem Service-Principal bereitstellen.

Verwalten von Azure Anmeldedaten und Abonnements für Cloud Manager

Wenn Sie ein Cloud Volumes ONTAP System erstellen, müssen Sie die Azure Zugangsdaten und das Marketplace-Abonnement auswählen, die mit diesem System verwendet werden sollen. Wenn Sie mehrere Azure Marketplace-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen Azure Zugangsdaten zuweisen.

Es gibt zwei Möglichkeiten, die Azure Zugangsdaten in Cloud Manager zu managen: Wenn Sie Cloud Volumes ONTAP zunächst in verschiedenen Azure-Konten bereitstellen möchten, müssen Sie die erforderlichen Berechtigungen angeben und die Zugangsdaten zu Cloud Manager hinzufügen. Die zweite Möglichkeit besteht darin, zusätzliche Abonnements mit der verwalteten Identität von Azure zu verknüpfen.

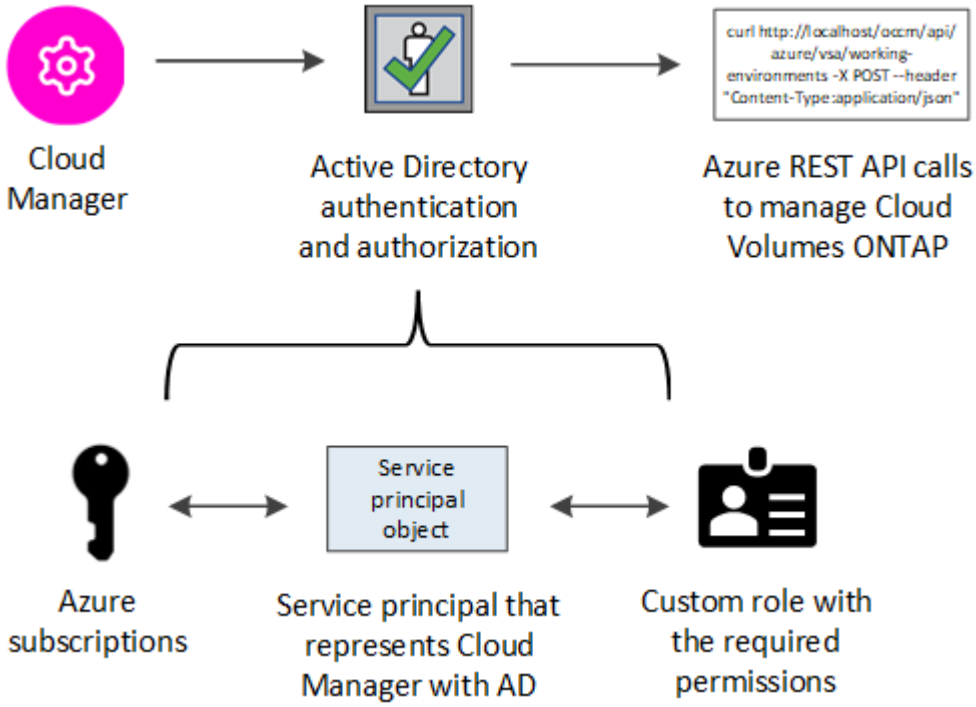
Wenn Sie einen Connector von Cloud Manager bereitstellen, fügt Cloud Manager automatisch das Azure-Konto hinzu, in dem Sie den Connector bereitgestellt haben. Ein erstes Konto wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. "Weitere Informationen zu Azure Konten und Berechtigungen".

Azure-Berechtigungen über einen Service-Principal gewähren

Cloud Manager benötigt Berechtigungen zum Ausführen von Aktionen in Azure. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie einen Service-Principal in Azure Active Directory erstellen und einrichten, sowie die für Cloud Manager erforderlichen Azure Zugangsdaten erhalten.

Über diese Aufgabe

In der folgenden Abbildung wird dargestellt, wie Cloud Manager Berechtigungen zum Ausführen von Vorgängen in Azure erhält. Ein Service-Prinzipalobjekt, das an ein oder mehrere Azure Subscriptions gebunden ist, stellt Cloud Manager in Azure Active Directory dar und wird einer benutzerdefinierten Rolle zugewiesen, die die erforderlichen Berechtigungen zulässt.



Schritte

1. Erstellen Sie eine Azure Active Directory-Anwendung.
2. Anwendung einer Rolle zuweisen.
3. Fügen Sie Windows Azure Service Management-API-Berechtigungen hinzu.
4. Holen Sie die Anwendungs-ID und die Verzeichnis-ID ab.
5. Erstellen Sie einen Clientschlüssel.

Erstellen einer Azure Active Directory-Anwendung

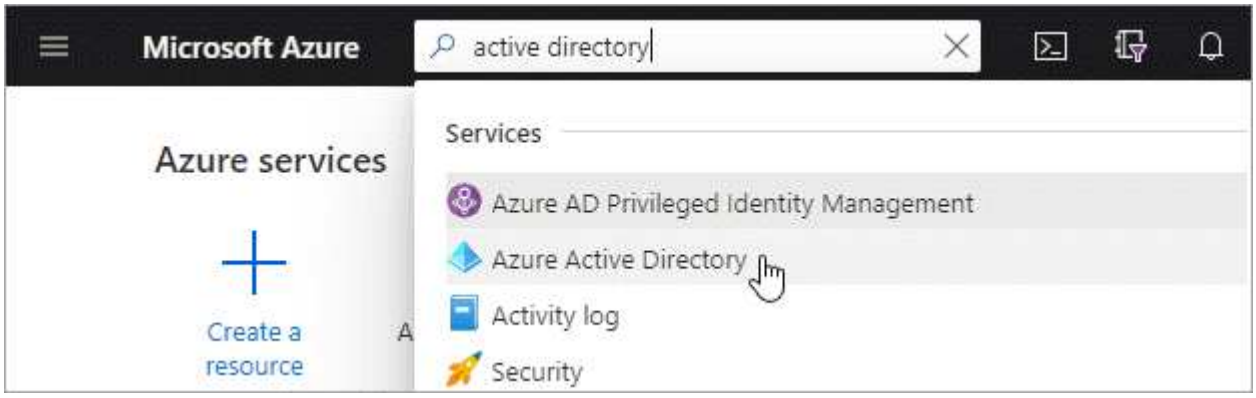
Erstellen einer Azure Active Directory (AD)-Applikation und eines Service-Principal, den Cloud Manager für die rollenbasierte Zugriffssteuerung nutzen kann

Bevor Sie beginnen

Sie müssen über die richtigen Berechtigungen in Azure verfügen, um eine Active Directory-Anwendung zu erstellen und die Anwendung einer Rolle zuzuweisen. Weitere Informationen finden Sie unter "Microsoft Azure-Dokumentation: Erforderliche Berechtigungen".

Schritte

1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



2. Klicken Sie im Menü auf **App-Registrierungen**.
3. Klicken Sie auf **Neue Registrierung**.
4. Geben Sie Details zur Anwendung an:
   - **Name**: Geben Sie einen Namen für die Anwendung ein.
   - **Kontotyp**: Wählen Sie einen Kontotyp aus (jeder funktioniert mit Cloud Manager).
   - **Redirect URI**: Wählen Sie **Web** und geben Sie dann eine beliebige URL ein – z. B. https://url
5. Klicken Sie Auf **Registrieren**.

Ergebnis

Sie haben die AD-Anwendung und den Service-Principal erstellt.

Anwendung einer Rolle zuweisen

Sie müssen den Service-Principal an ein oder mehrere Azure-Abonnements binden und ihm die benutzerdefinierte Rolle „OnCommand Cloud Manager Operator“ zuweisen, damit Cloud Manager über Berechtigungen in Azure verfügt.

Schritte

1. Erstellen einer benutzerdefinierten Rolle:

   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-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.

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 über eine benutzerdefinierte Rolle namens *Cloud Manager Operator* verfügen.

2. Applikation der Rolle zuweisen:

   a. Öffnen Sie im Azure-Portal den Service **Abonnements**.

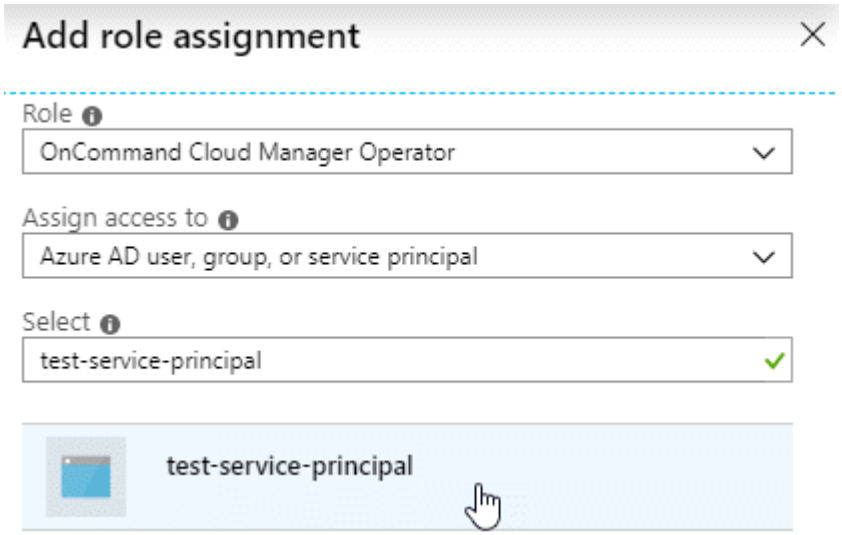
   b. Wählen Sie das Abonnement aus.

   c. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.

   d. Wählen Sie die Rolle **Cloud Manager Operator** aus.

   e. * Azure AD Benutzer, Gruppe oder Serviceprincipal* ausgewählt lassen.

   f. Suchen Sie nach dem Namen der Anwendung (Sie finden sie nicht in der Liste durch Scrollen).



   g. Wählen Sie die Anwendung aus und klicken Sie auf **Speichern**.

   Der Service Principal für den Cloud Manager verfügt jetzt über die erforderlichen Azure Berechtigungen für das Abonnement.

Wenn Sie Cloud Volumes ONTAP aus mehreren Azure Subscriptions bereitstellen möchten, müssen Sie den Service-Prinzipal an jedes dieser Subscriptions binden. Mit Cloud Manager können Sie das Abonnement auswählen, das Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten.

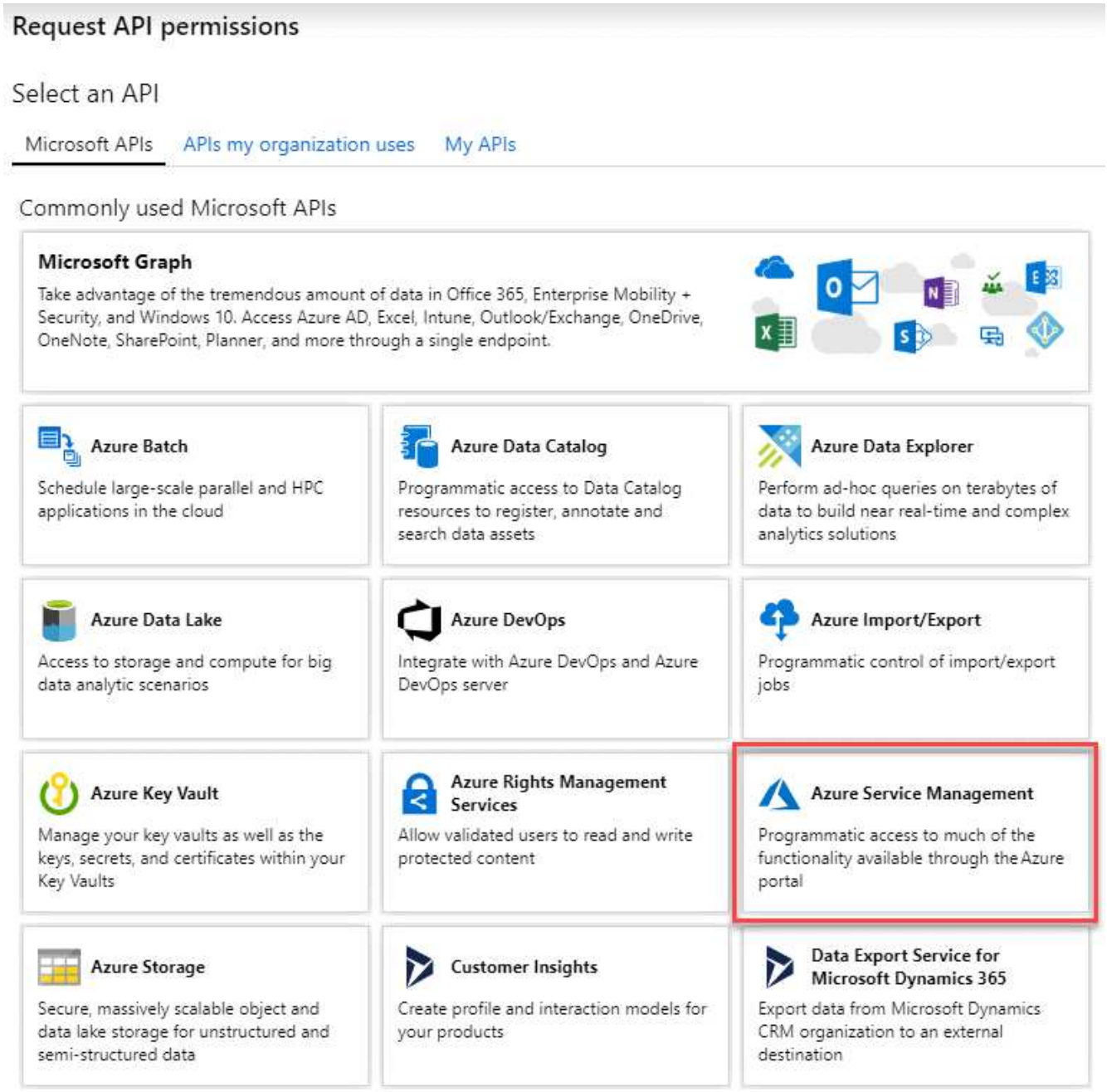
Windows Azure Service Management-API-Berechtigungen werden hinzugefügt

Der Service-Principal muss über die Berechtigungen „Windows Azure Service Management API“ verfügen.

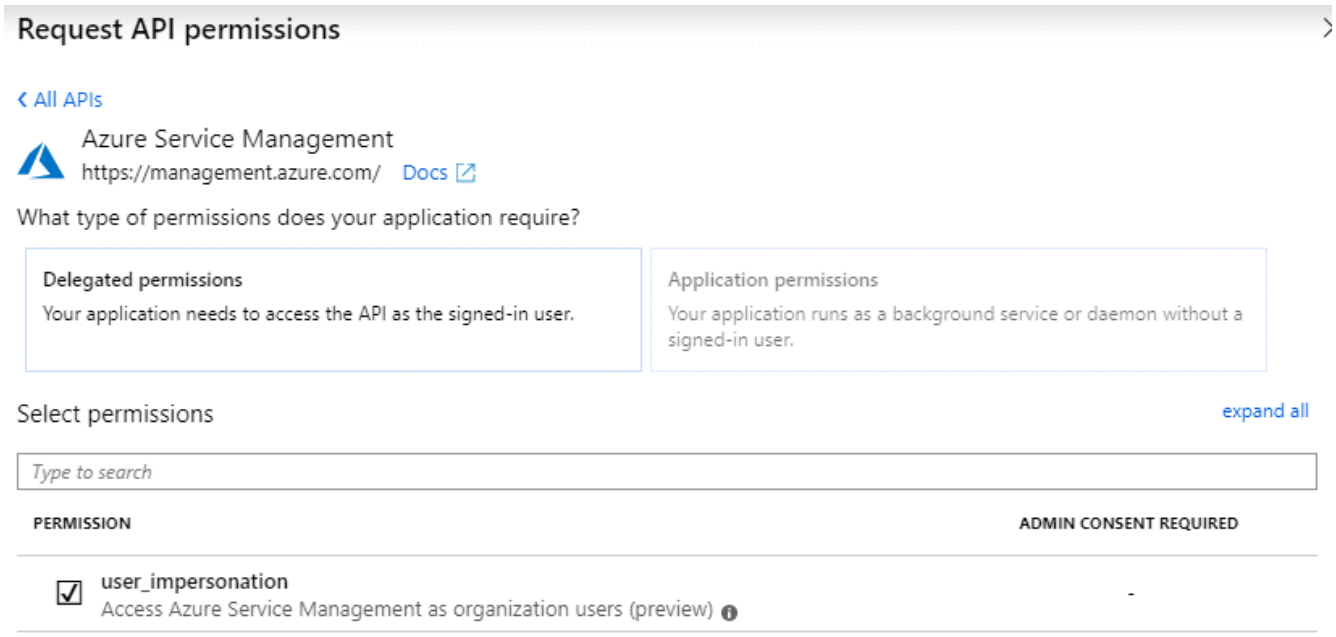
Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.

2. Klicken Sie auf **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.



4. Klicken Sie auf **Zugriff auf Azure Service Management als Benutzer der Organisation** und dann auf **Berechtigungen hinzufügen**.

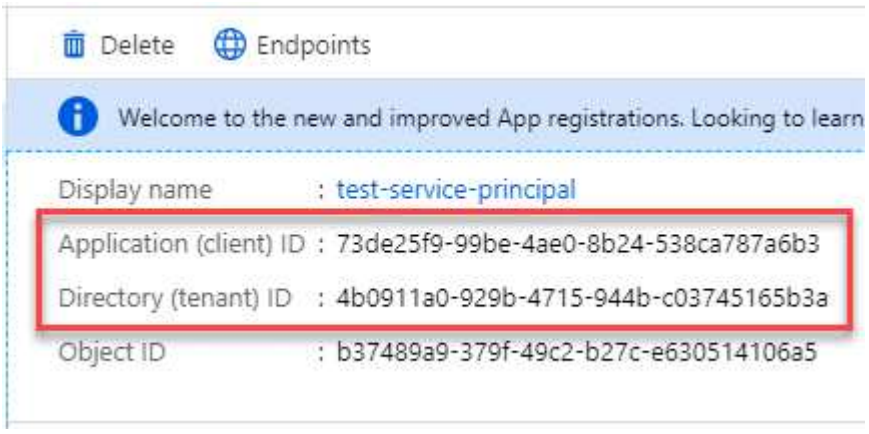


Abrufen der Anwendungs-ID und der Verzeichnis-ID

Wenn Sie dem Cloud Manager das Azure-Konto hinzufügen, müssen Sie die Anwendungs- (Client-) ID und die Verzeichnis- (Mandanten-)ID für die Applikation angeben. Cloud Manager verwendet die IDs, um sich programmatisch anzumelden.

Schritte

1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Kopieren Sie die **Application (Client) ID** und die **Directory (Tenant) ID**.



Erstellen eines Clientgeheimnisses

Sie müssen ein Client-Geheimnis erstellen und Cloud Manager dann den Wert des Geheimnisses zur Verfügung stellen, damit Cloud Manager es zur Authentifizierung mit Azure AD verwenden kann.

Wenn Sie das Konto zu Cloud Manager hinzufügen, bezieht sich Cloud Manager auf das Kundengeheimnis als Applikationsschlüssel.

Schritte

1. Öffnen Sie den Dienst **Azure Active Directory**.
2. Klicken Sie auf **App-Registrierungen** und wählen Sie Ihre Anwendung aus.
3. Klicken Sie auf **Zertifikate & Geheimnisse > Neuer Client Secret**.
4. Geben Sie eine Beschreibung des Geheimnisses und eine Dauer an.
5. Klicken Sie Auf **Hinzufügen**.
6. Kopieren Sie den Wert des Clientgeheimnisses.

Ergebnis

Ihr Service-Principal ist jetzt eingerichtet und Sie sollten die Anwendungs- (Client-)ID, die Verzeichnis- (Mandanten-)ID und den Wert des Clientgeheimnisses kopiert haben. Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie ein Azure-Konto hinzufügen.

Hinzufügen von Azure Zugangsdaten zu Cloud Manager

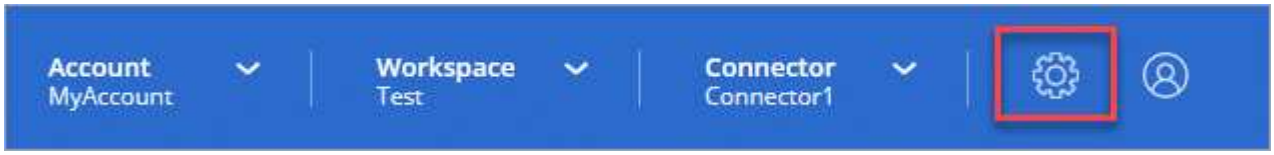
Nachdem Sie ein Azure Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie die Anmeldedaten für dieses Konto Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

Was Sie benötigen

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

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und wählen Sie **Microsoft Azure**.
3. Geben Sie Informationen zum Azure Active Directory Service Principal ein, der die erforderlichen Berechtigungen erteilt:
   - Anwendungs-ID (Client): Siehe Abrufen der Anwendungs-ID und der Verzeichnis-ID.
   - Verzeichnis-ID (Mandant): Siehe Abrufen der Anwendungs-ID und der Verzeichnis-ID.
   - Client Secret: Siehe Erstellen eines Clientgeheimnisses.

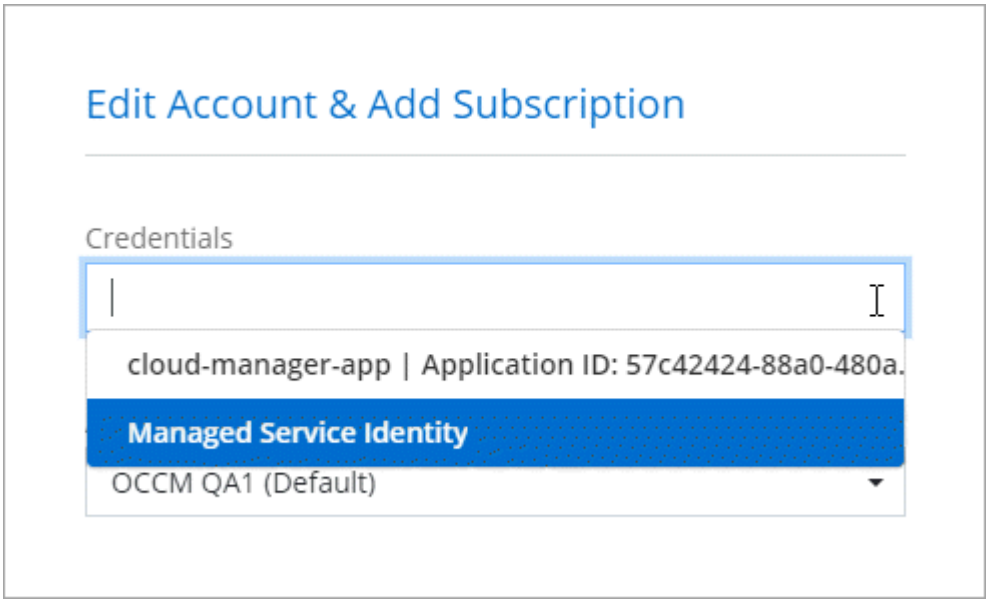
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Weiter**.
5. Wählen Sie das Pay-as-you-go-Abonnement aus, das Sie mit den Anmeldedaten verknüpfen möchten, oder klicken Sie auf **Abonnement hinzufügen**, wenn Sie noch nicht über ein Abonnement verfügen.

   Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen Azure Zugangsdaten über den Azure Marketplace mit einem Abonnement für Cloud Volumes ONTAP verknüpft werden.

6. Klicken Sie Auf **Hinzufügen**.

Ergebnis

Auf der Seite Details und Anmeldeinformationen können Sie nun zu verschiedenen Anmeldeinformationen wechseln "Beim Erstellen einer neuen Arbeitsumgebung":



Verknüpfen eines Azure Marketplace Abonnements mit den Zugangsdaten

Nachdem Sie Ihre Azure Zugangsdaten zu Cloud Manager hinzugefügt haben, können Sie diesen Anmeldedaten ein Azure Marketplace Abonnement zuweisen. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein Azure Marketplace-Abonnement verknüpfen können, nachdem Sie bereits die Anmeldedaten zu Cloud Manager hinzugefügt haben:

- Sie haben ein Abonnement nicht zugeordnet, wenn Sie zum ersten Mal die Anmeldedaten zu Cloud Manager hinzugefügt haben.
- Sie möchten ein vorhandenes Azure Marketplace Abonnement durch ein neues Abonnement ersetzen.

Was Sie benötigen

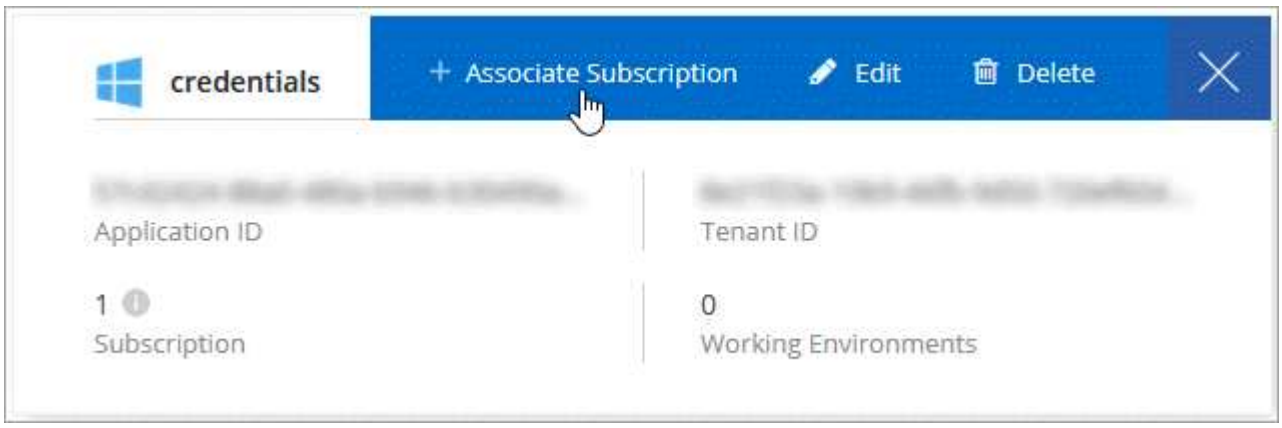
Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Bewegen Sie den Mauszeiger über einen Satz von Anmeldeinformationen, und klicken Sie auf das

Aktivitätsmenü.

3. Klicken Sie im Menü auf **Abonnement verknüpfen**.



4. Wählen Sie ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

   Das folgende Video beginnt im Kontext des Assistenten zur Arbeitsumgebung, zeigt Ihnen aber den gleichen Workflow, nachdem Sie auf **Abonnement hinzufügen** geklickt haben:

   ► https://docs.netapp.com/de-de/occm38//media/video_subscribing_azure.mp4 *(video)*

Verknüpfen weiterer Azure-Abonnements mit einer gemanagten Identität

Mit Cloud Manager können Sie die Azure Zugangsdaten und das Azure Abonnement auswählen, in dem Sie Cloud Volumes ONTAP implementieren möchten. Sie können kein anderes Azure-Abonnement für das verwaltete Identitätsprofil auswählen, es sei denn, Sie verknüpfen das "Verwaltete Identität" Mit diesen Abonnements.

Über diese Aufgabe

Eine verwaltete Identität ist "Zunächst das Azure-Konto" Wenn Sie einen Connector von Cloud Manager bereitstellen. Wenn Sie den Connector bereitgestellt haben, hat Cloud Manager die Rolle Cloud Manager Operator erstellt und der virtuellen Maschine Connector zugewiesen.

Schritte

1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Klicken Sie auf **Access Control (IAM)**.
   a. 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.

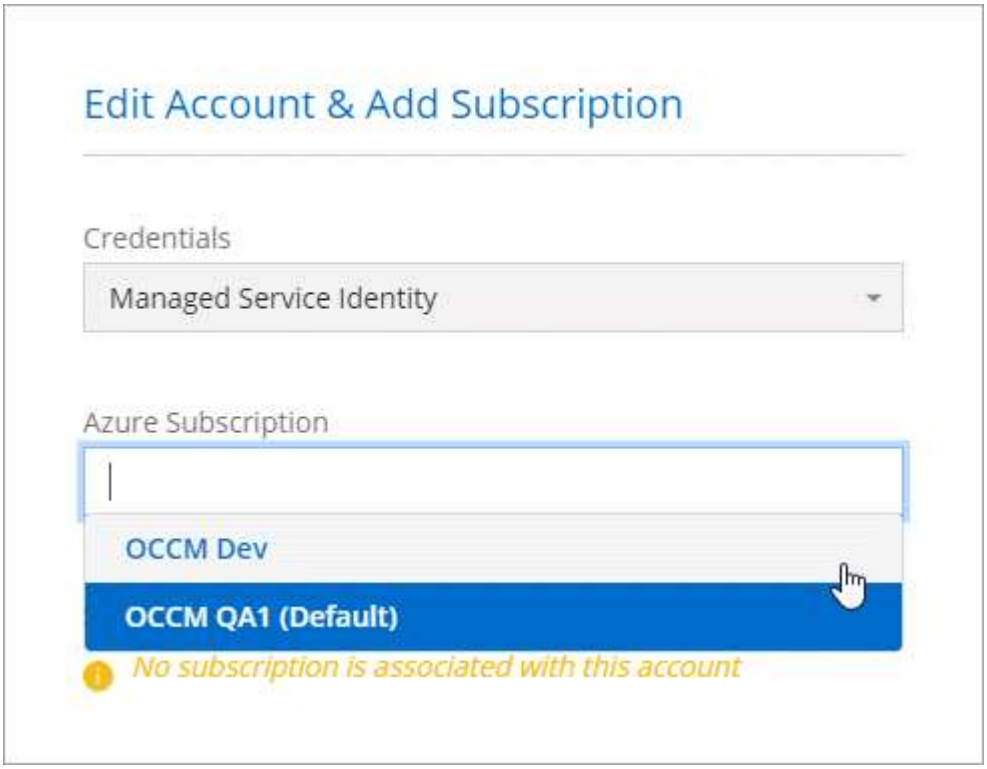
      - Weisen Sie einer **virtuellen Maschine** Zugriff zu.

- Wählen Sie das Abonnement aus, in dem die virtuelle Connector-Maschine erstellt wurde.
- Wählen Sie die virtuelle Verbindungsmaschine aus.
- Klicken Sie Auf **Speichern**.

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

Wenn Sie eine neue Arbeitsumgebung erstellen, sollten Sie nun über mehrere Azure-Abonnements für das verwaltete Identitätsprofil verfügen.



GCP

Google Cloud Projekte, Berechtigungen und Konten

Ein Service-Konto bietet Cloud Manager Berechtigungen für die Implementierung und das Management von Cloud Volumes ONTAP Systemen in demselben Projekt wie Cloud Manager oder in verschiedenen Projekten.

Projekt und Berechtigungen für Cloud Manager

Bevor Sie Cloud Volumes ONTAP in Google Cloud bereitstellen können, müssen Sie zunächst einen Connector in einem Google Cloud-Projekt bereitstellen. Der Connector kann nicht vor Ort oder bei einem anderen Cloud-Provider ausgeführt werden.

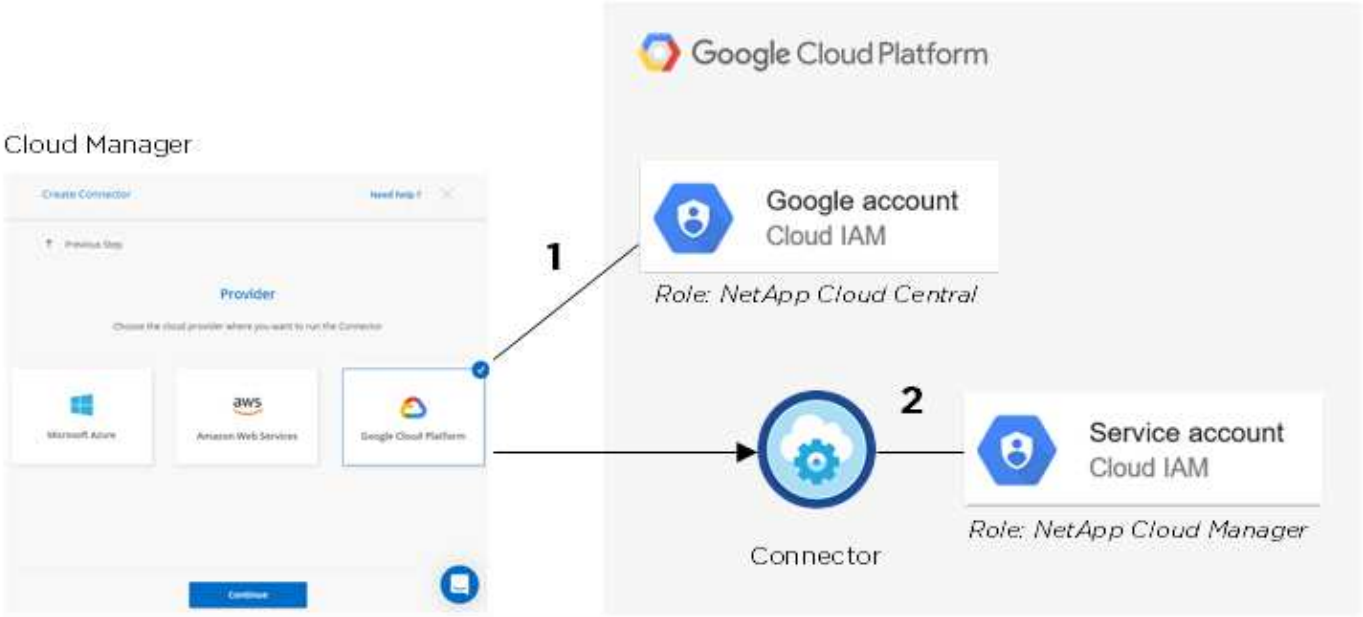
Vor der Bereitstellung eines Connectors direkt aus Cloud Manager müssen zwei Berechtigungssätze vorhanden sein:

1. Sie müssen einen Connector mit einem Google-Konto bereitstellen, das über Berechtigungen zum Starten der Connector-VM-Instanz von Cloud Manager verfügt.

2. Bei der Bereitstellung des Connectors werden Sie aufgefordert, ein auszuwählen "Servicekonto" Für die VM-Instanz. Cloud Manager erhält Berechtigungen vom Service-Konto, um Cloud Volumes ONTAP Systeme in Ihrem Auftrag zu erstellen und zu managen. Berechtigungen werden durch Hinzufügen einer benutzerdefinierten Rolle an das Servicekonto bereitgestellt.

Wir haben zwei YAML-Dateien eingerichtet, die die erforderlichen Berechtigungen für den Benutzer und das Dienstkonto enthalten. "Erfahren Sie, wie Sie mit den YAML-Dateien Berechtigungen einrichten".

Das folgende Bild zeigt die in den Nummern 1 und 2 oben beschriebenen Berechtigungsanforderungen:



Projekt für Cloud Volumes ONTAP

Cloud Volumes ONTAP kann im selben Projekt wie der Connector oder in einem anderen Projekt residieren. Um Cloud Volumes ONTAP in einem anderen Projekt bereitzustellen, müssen Sie zunächst das Connector-Servicekonto und die Rolle zu diesem Projekt hinzufügen.

- "Informationen zur Einrichtung eines Service-Kontos (siehe Schritt 2)".
- "Erfahren Sie, wie Cloud Volumes ONTAP in GCP implementiert und ein Projekt ausgewählt wird".

Konto für Daten-Tiering

Cloud Manager erfordert ein GCP-Konto für Cloud Volumes ONTAP 9.6, nicht jedoch für 9.7 und höher. Wenn Sie Daten-Tiering mit Cloud Volumes ONTAP 9.7 verwenden möchten, folgen Sie Schritt 4 in "Erste Schritte mit Cloud Volumes ONTAP in der Google Cloud Platform".

Um Daten-Tiering auf einem Cloud Volumes ONTAP 9.6 System zu ermöglichen, ist das Hinzufügen eines Google Cloud Kontos zu Cloud Manager erforderlich. Daten-Tiering verlagert selten genutzte Daten automatisch auf kostengünstigen Objekt-Storage, sodass Sie Speicherplatz auf dem primären Storage freigeben und den sekundären Storage reduzieren können.

Wenn Sie das Konto hinzufügen, müssen Sie Cloud Manager mit einem Speicherzugriffsschlüssel für ein Servicekonto bereitstellen, das Storage Admin-Berechtigungen hat. Cloud Manager verwendet die Zugriffssteuerung zum Einrichten und Managen eines Cloud Storage-Buckets für Daten-Tiering.

Nachdem Sie ein Google Cloud Konto hinzugefügt haben, können Sie auf einzelnen Volumes das Daten-

Tiering aktivieren, wenn Sie sie erstellen, ändern oder replizieren.

- "Erfahren Sie, wie Sie GCP-Konten in Cloud Manager einrichten und hinzufügen".
- "Verschieben Sie inaktive Daten auf kostengünstigen Objekt-Storage".

Verwalten von GCP-Anmeldedaten und -Abonnements für Cloud Manager

Sie können zwei Arten von Anmeldeinformationen für die Google Cloud-Plattform über Cloud Manager verwalten: Die Anmeldeinformationen, die der VM-Instanz von Connector zugewiesen sind, und die mit einem Cloud Volumes ONTAP 9.6-System für verwendeten Storage-Zugriffsschlüssel "Daten-Tiering".

Verknüpfen eines Marketplace-Abonnements mit GCP-Zugangsdaten

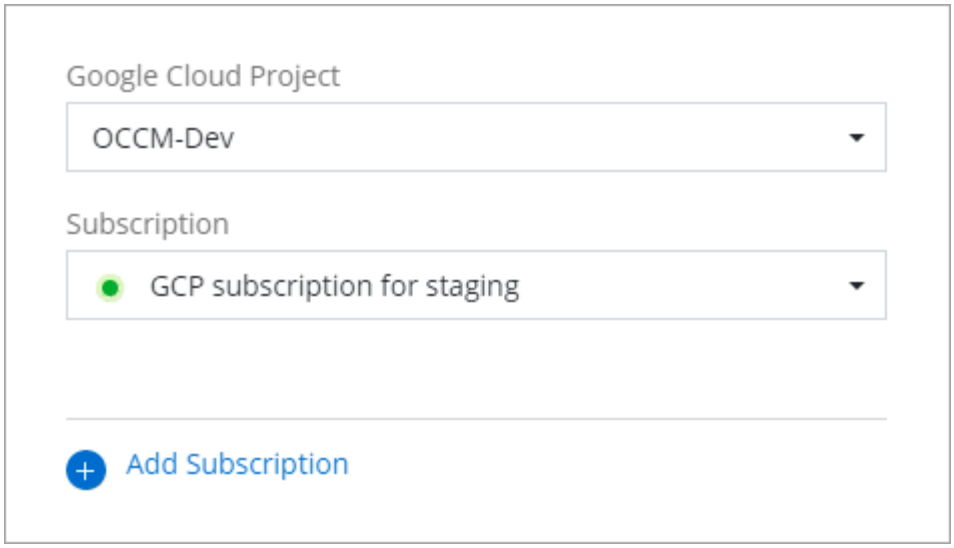
Wenn Sie einen Connector in GCP bereitstellen, erstellt Cloud Manager einen Standardsatz von Anmeldeinformationen, die der Connector-VM-Instanz zugeordnet sind. Diese sind die Zugangsdaten, die Cloud Manager zur Implementierung von Cloud Volumes ONTAP verwendet.

Sie können das Marketplace-Abonnement jederzeit ändern, das mit diesen Anmeldedaten verknüpft ist. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Bewegen Sie den Mauszeiger über einen Satz von Anmeldeinformationen, und klicken Sie auf das Aktivitätsmenü.
3. Klicken Sie im Menü auf **Abonnement verknüpfen**.

4. Wählen Sie ein Google Cloud-Projekt und ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.



5. Klicken Sie Auf **Mitarbeiter**.

Einrichten und Hinzufügen von GCP-Konten für Daten-Tiering mit Cloud Volumes ONTAP 9.6

Wenn Sie ein Cloud Volumes ONTAP 9.6-System für aktivieren möchten "Daten-Tiering", Sie müssen Cloud Manager mit einem Storage-Zugriffschlüssel für ein Service-Konto bereitstellen, das Storage-Admin-Berechtigungen hat. Cloud Manager verwendet die Zugriffssteuerung zum Einrichten und Managen eines Cloud Storage-Buckets für Daten-Tiering.

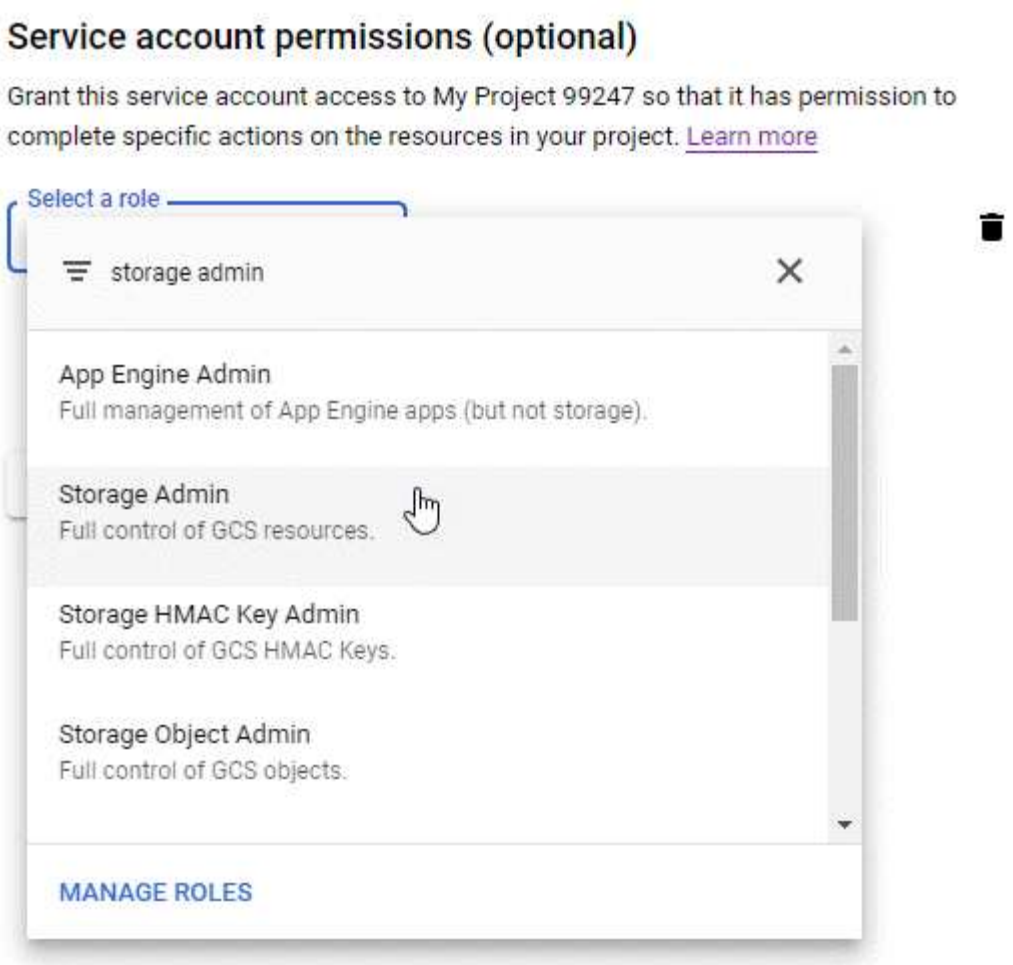
Wenn Sie Daten-Tiering mit Cloud Volumes ONTAP 9.7 verwenden möchten, folgen Sie Schritt 4 in "Erste Schritte mit Cloud Volumes ONTAP in der Google Cloud Platform".

Einrichten eines Servicekontos und Zugriffsschlüssel für Google Cloud Storage

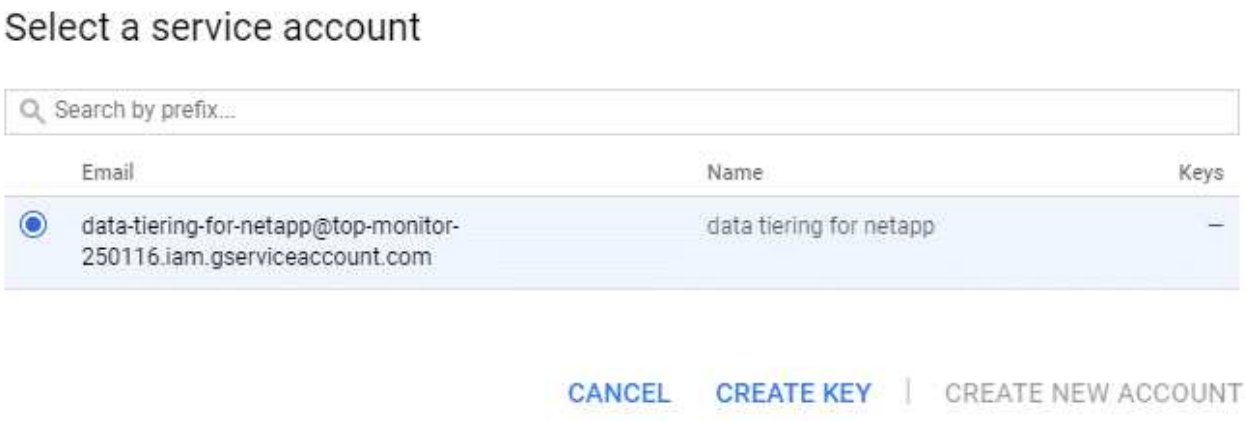
Mithilfe eines Service-Kontos kann Cloud Manager Cloud Storage-Buckets authentifizieren und auf sie zugreifen, die für Daten-Tiering verwendet werden. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Öffnen Sie die GCP IAM-Konsole und "Erstellen Sie ein Dienstkonto mit der Rolle Storage Admin".



2. Gehen Sie zu "GCP-Speichereinstellungen".
3. Wenn Sie aufgefordert werden, wählen Sie ein Projekt aus.
4. Klicken Sie auf die Registerkarte **Interoperabilität**.
5. Falls Sie dies noch nicht getan haben, klicken Sie auf **Interoperabilitätszugriff aktivieren**.
6. Klicken Sie unter **Zugriffsschlüssel für Servicekonten** auf **Schlüssel für ein Servicekonto erstellen**.
7. Wählen Sie das Servicekonto aus, das Sie in Schritt 1 erstellt haben.



8. Klicken Sie Auf **Schlüssel Erstellen**.

9. Kopieren Sie den Zugriffsschlüssel und den Schlüssel.

   Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie das GCP-Konto für das Daten-Tiering hinzufügen.

Hinzufügen eines GCP-Kontos zu Cloud Manager

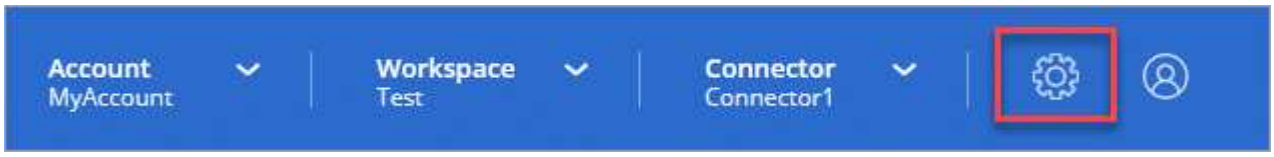
Nachdem Sie nun über einen Zugriffsschlüssel für ein Service-Konto verfügen, können Sie ihn dem Cloud Manager hinzufügen.

Was Sie benötigen

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

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



2. Klicken Sie auf **Anmeldeinformationen hinzufügen** und wählen Sie **Google Cloud**.
3. Geben Sie den Zugriffsschlüssel und den Schlüssel für das Servicekonto ein.

   Mithilfe der Schlüssel kann Cloud Manager einen Cloud Storage-Bucket für das Daten-Tiering einrichten.

4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Konto erstellen**.

Was kommt als Nächstes?

Sie können jetzt Daten-Tiering für einzelne Volumes auf einem Cloud Volumes ONTAP 9.6 System aktivieren, wenn Sie sie erstellen, ändern oder replizieren. Weitere Informationen finden Sie unter "Tiering inaktiver Daten in kostengünstigen Objektspeicher".

Bevor Sie jedoch das tun, stellen Sie sicher, dass das Subnetz, in dem sich Cloud Volumes ONTAP befindet, für privaten Google-Zugriff konfiguriert ist. Anweisungen finden Sie unter "Google Cloud Documentation: Configuring Private Google Access".

Hinzufügen von NetApp Support Site Konten zu Cloud Manager

Um ein BYOL-System zu implementieren, muss ein NetApp Support Site Konto in Cloud Manager hinzugefügt werden. Zudem müssen Pay-as-you-go-Systeme registriert und ein Upgrade der ONTAP Software durchgeführt werden.

Sehen Sie sich das folgende Video an und erfahren Sie, wie Sie NetApp Support Site Accounts in Cloud Manager hinzufügen. Oder blättern Sie nach unten, um die Schritte zu lesen.

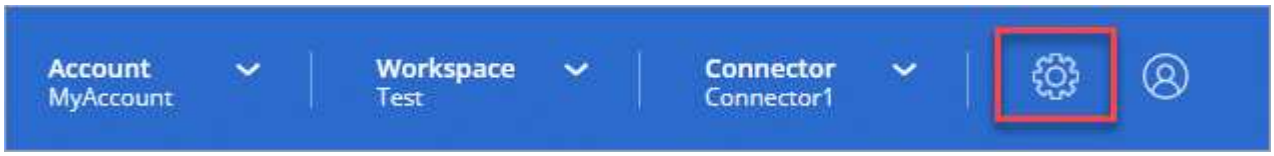
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Was Sie benötigen

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

Schritte

1. Wenn Sie noch keinen NetApp Support Site Account haben, "Eine anmeldung".
2. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.



3. Klicken Sie auf **Anmeldedaten hinzufügen** und wählen Sie **NetApp Support Site**.
4. Geben Sie einen Namen für das Konto an, und geben Sie dann den Benutzernamen und das Kennwort ein.
   - Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
   - Wenn Sie Byol-Systeme implementieren möchten:
     - Das Konto muss für den Zugriff auf die Seriennummern der BYOL-Systeme autorisiert sein.
     - Wenn Sie ein sicheres BYOL-Abonnement erworben haben, ist ein sicheres NSS-Konto erforderlich.
5. Klicken Sie Auf **Konto Erstellen.**

Was kommt als Nächstes?

Benutzer können jetzt das Konto beim Erstellen neuer Cloud Volumes ONTAP Systeme und bei der Registrierung vorhandener Systeme auswählen.

- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Registrieren von Pay-as-you-go-Systemen"
- "Cloud Manager managt Lizenzdateien"

Verwalten von Benutzern, Arbeitsbereichen, Connectors und Abonnements

"Nach der ersten Einrichtung", Möglicherweise müssen Sie Ihre Kontoeinstellungen später durch die Verwaltung von Benutzern, Workspaces, Connectors und Abonnements verwalten.

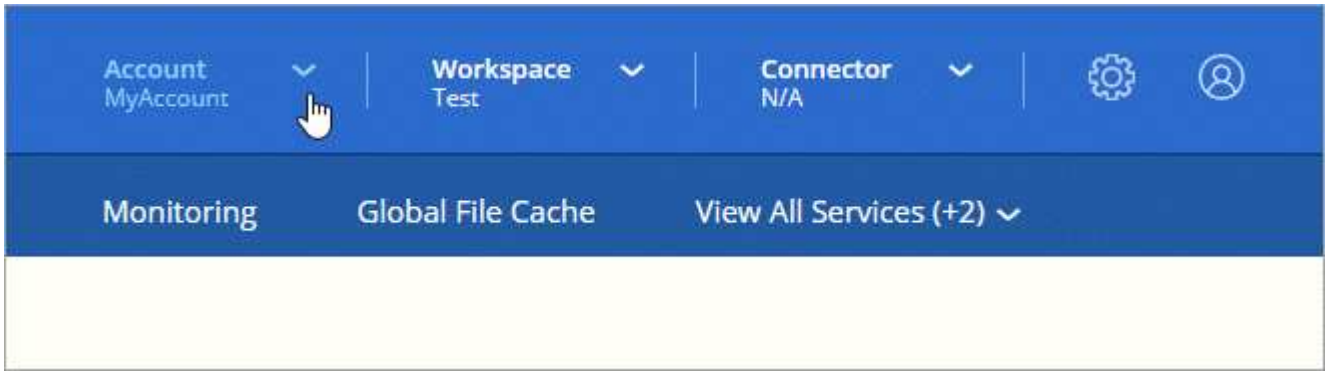
"Erfahren Sie mehr über die Funktionsweise von Cloud Central-Accounts".

Benutzer hinzufügen

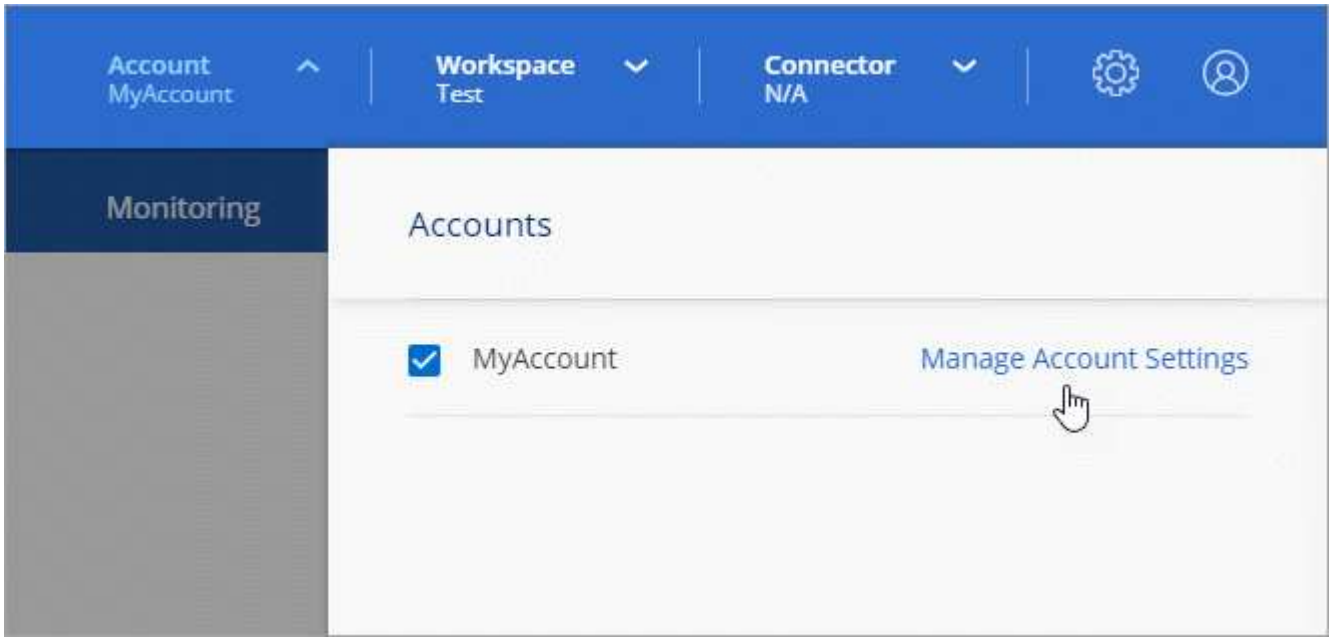
Cloud Central Benutzer werden mit dem Cloud Central Konto verknüpft, damit diese Arbeitsumgebungen in Cloud Manager erstellen und verwalten können.

Schritte

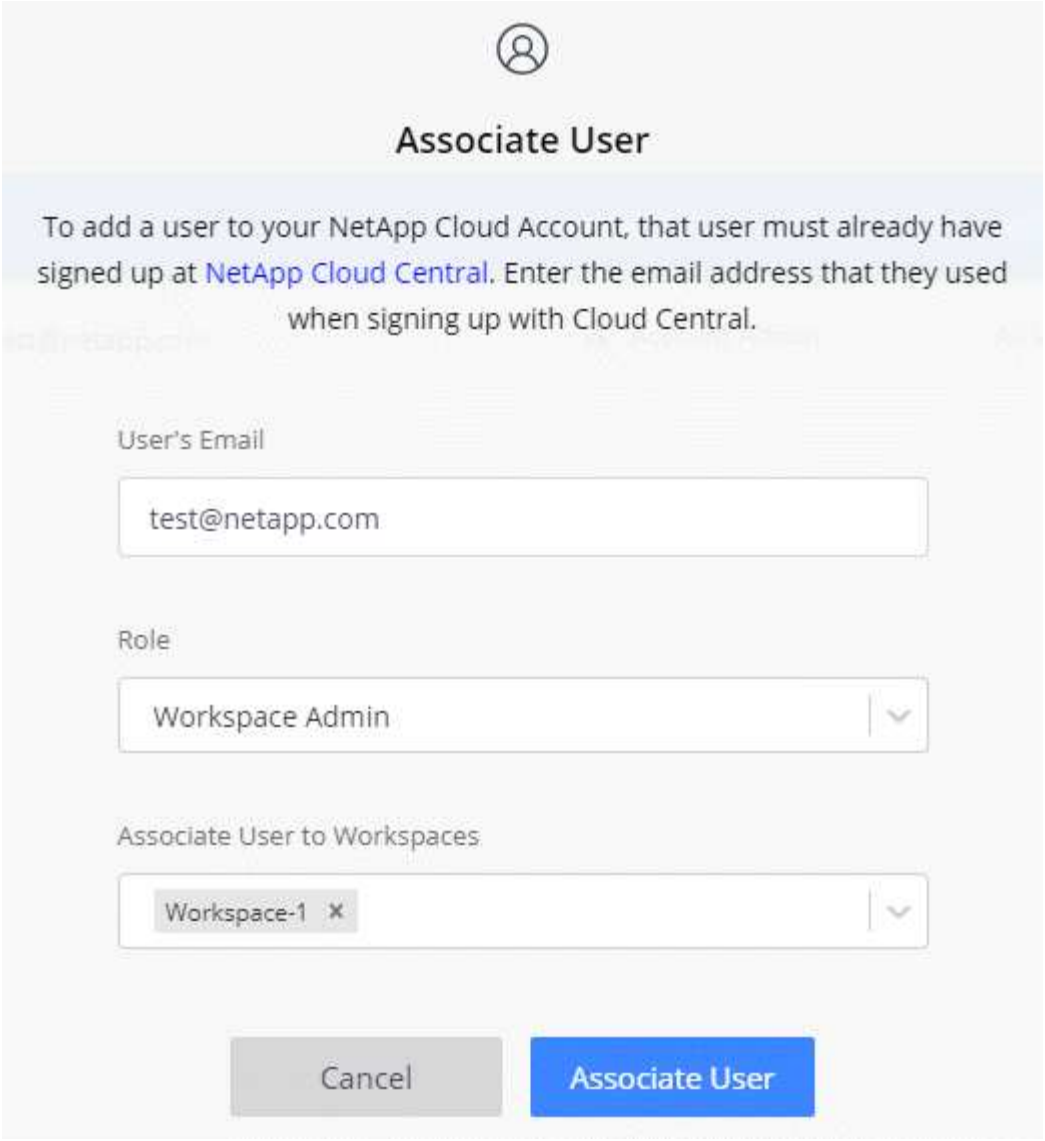
1. Wenn der Benutzer dies noch nicht getan hat, bitten Sie den Benutzer, zu wechseln "NetApp Cloud Central" Und melden Sie sich an.
2. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto**.



3. Klicken Sie neben dem aktuell ausgewählten Konto auf **Konto verwalten**.



4. Klicken Sie auf der Registerkarte Benutzer auf **Benutzer verknüpfen**.
5. Geben Sie die E-Mail-Adresse des Benutzers ein, und wählen Sie eine Rolle für den Benutzer aus:
   - **Account Admin**: Kann jede Aktion in Cloud Manager ausführen.
   - **Workspace Admin**: Kann Ressourcen in zugewiesenen Workspaces erstellen und verwalten.
   - **Compliance Viewer**: Kann nur Compliance-Informationen anzeigen und Berichte für Arbeitsbereiche erstellen, auf die sie zugreifen können.
6. Wenn Sie Workspace Admin oder Compliance Viewer ausgewählt haben, wählen Sie eine oder mehrere Arbeitsbereiche aus, die diesem Benutzer zugeordnet werden sollen.



7. Klicken Sie Auf * Benutzer Verknüpfen*.

Ergebnis

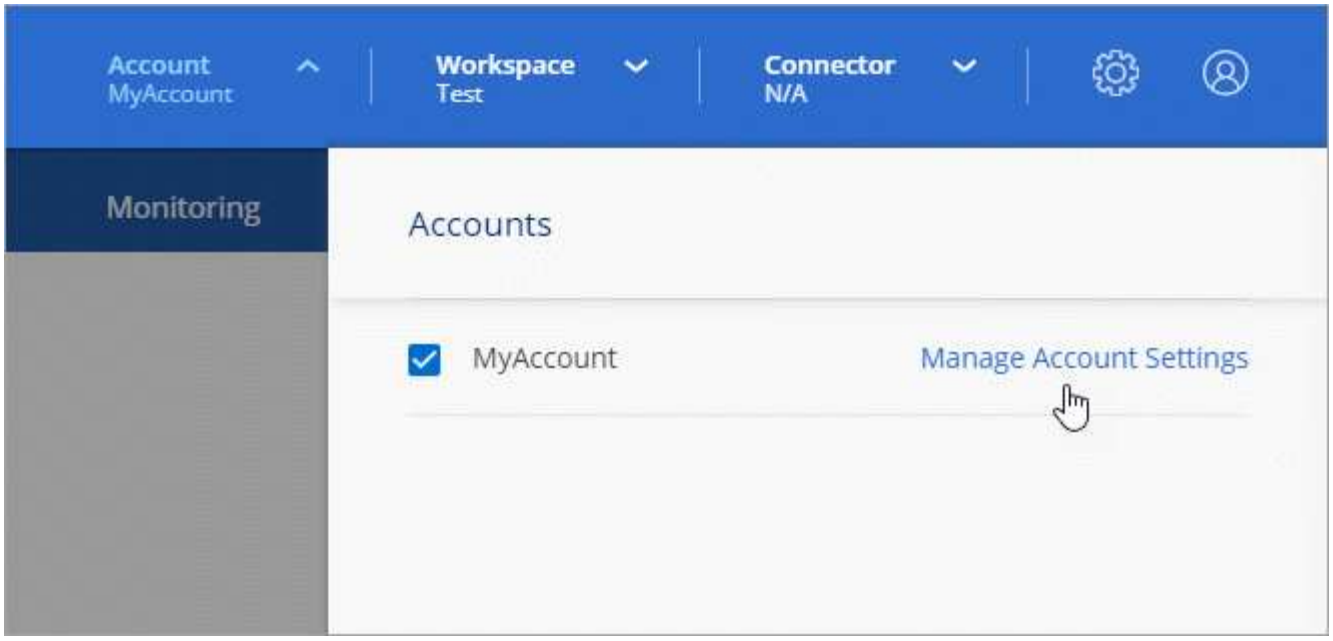
Der Benutzer sollte eine E-Mail von NetApp Cloud Central mit dem Titel „Account Association“ erhalten. Die E-Mail enthält die für den Zugriff auf Cloud Manager erforderlichen Informationen.

Benutzer werden entfernt

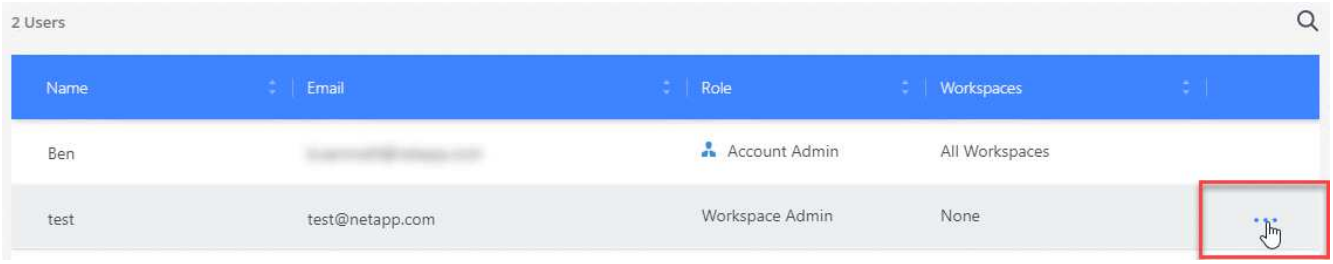
Die Trennung der Verknüpfung eines Benutzers wird dadurch erschwert, dass er nicht mehr auf die Ressourcen eines Cloud Central Kontos zugreifen kann.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Benutzer auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie zur Bestätigung auf **Benutzer entzuordnen** und klicken Sie zur Bestätigung auf **Mitarbeiter nicht zuordnen**.

Ergebnis

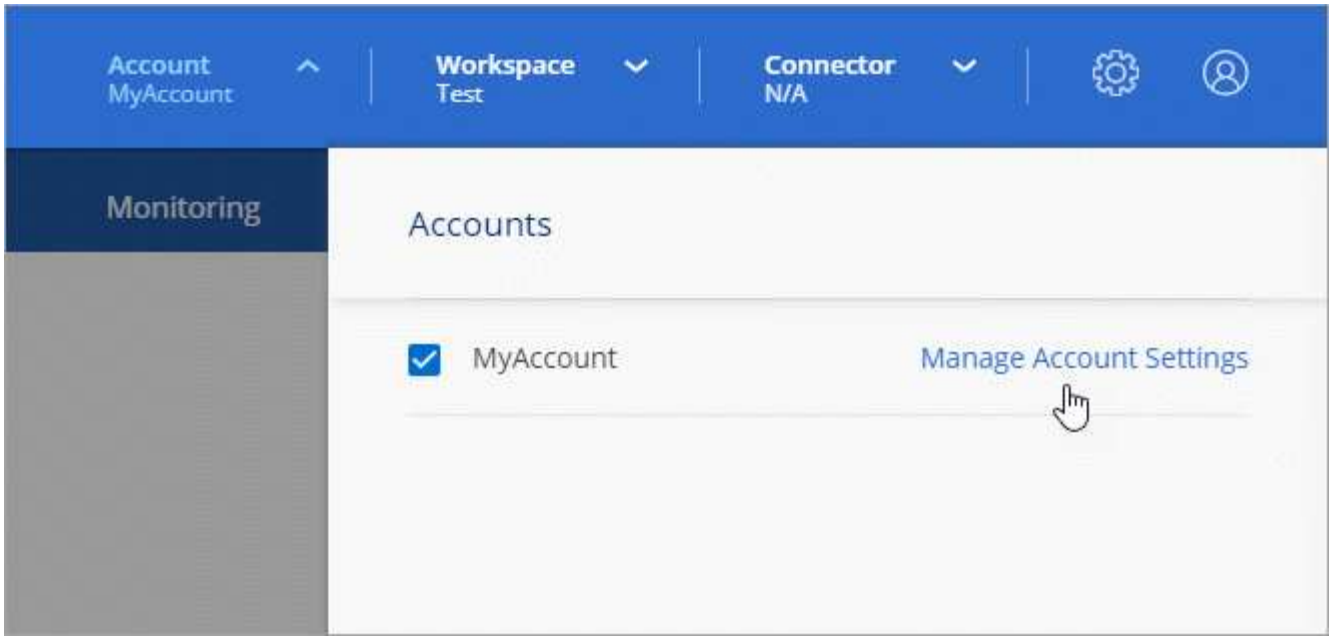
Der Benutzer kann nicht mehr auf die Ressourcen in diesem Cloud Central Konto zugreifen.

Arbeitsbereiche eines Arbeitsbereichs-Administrators verwalten

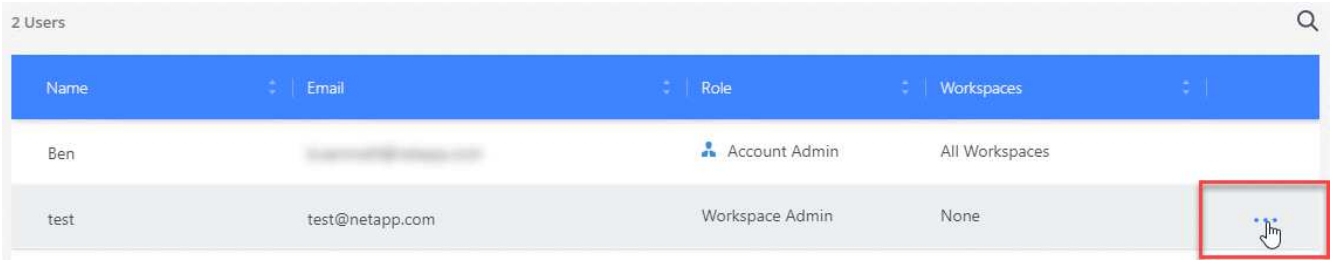
Sie können Workspace-Administratoren jederzeit mit Arbeitsbereichen verknüpfen und sie ablösen. Durch die Verknüpfung des Benutzers können die Arbeitsumgebungen in diesem Arbeitsbereich erstellt und angezeigt werden.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.



2. Klicken Sie auf der Registerkarte Benutzer auf das Aktionsmenü in der Zeile, die dem Benutzer entspricht.



3. Klicken Sie Auf **Arbeitsbereiche Verwalten**.
4. Wählen Sie die Arbeitsbereiche aus, die dem Benutzer zugeordnet werden sollen, und klicken Sie auf **Anwenden**.

Ergebnis

Der Benutzer kann jetzt über Cloud Manager auf diese Arbeitsbereiche zugreifen, solange der Connector auch mit den Arbeitsbereichen verknüpft war.

Arbeitsbereiche verwalten

Verwalten Sie Ihre Arbeitsbereiche, indem Sie sie erstellen, umbenennen und löschen. Beachten Sie, dass Sie einen Arbeitsbereich nicht löschen können, wenn er Ressourcen enthält. Er muss leer sein.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Arbeitsbereiche**.
3. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **Neuen Arbeitsbereich hinzufügen**, um einen neuen Arbeitsbereich zu erstellen.
   - Klicken Sie auf **Umbenennen**, um den Arbeitsbereich umzubenennen.
   - Klicken Sie auf **Löschen**, um den Arbeitsbereich zu löschen.

Verwalten von Arbeitsumgebungen eines Connectors

Sie müssen den Connector mit Arbeitsbereichen verknüpfen, damit Workspace-Administratoren über Cloud Manager auf diese Arbeitsbereiche zugreifen können.

Wenn Sie nur Kontoadministratoren haben, ist es nicht erforderlich, den Connector mit Arbeitsbereichen zu verknüpfen. Account-Administratoren haben standardmäßig die Möglichkeit, auf alle Workspaces in Cloud Manager zuzugreifen.

"Erfahren Sie mehr über Benutzer, Arbeitsbereiche und Connectors".

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Connector**.
3. Klicken Sie auf **Arbeitsbereiche verwalten** für den Konnektor, den Sie verknüpfen möchten.
4. Wählen Sie die Arbeitsbereiche aus, die mit dem Connector verknüpft werden sollen, und klicken Sie auf **Anwenden**.

Verwalten von Abonnements

Nachdem Sie den Marketplace eines Cloud-Providers abonniert haben, steht jedes Abonnement über das Widget „Account Settings“ (Kontoeinstellungen) zur Verfügung. Sie haben die Möglichkeit, ein Abonnement umzubenennen und das Abonnement von einem oder mehreren Konten zu entfernen.

Nehmen wir zum Beispiel an, dass Sie zwei Konten haben und jedes über separate Abonnements abgerechnet wird. Sie können ein Abonnement von einem der Konten ablösen, so dass die Benutzer in diesem Konto nicht versehentlich das falsche Abonnement wählen, wenn Sie eine Cloud Volume ONTAP Arbeitsumgebung erstellen.

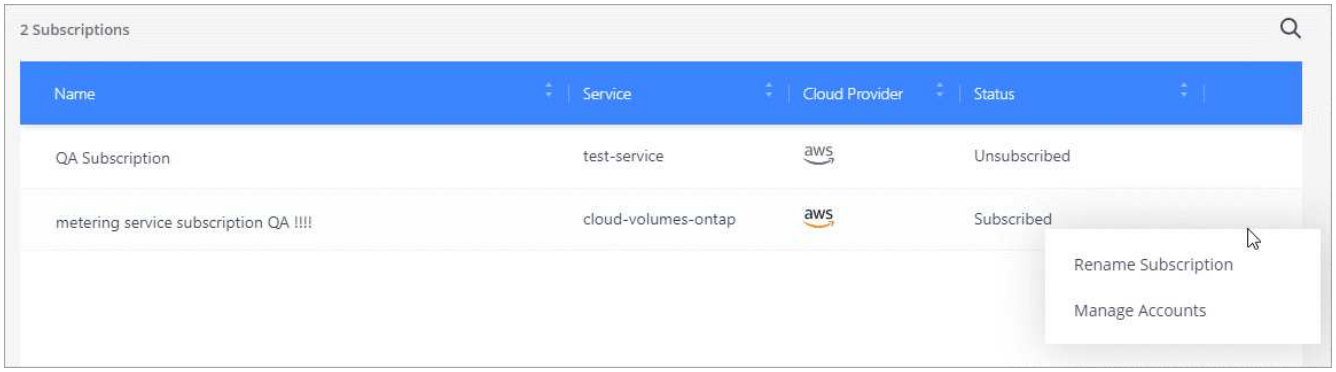
"Weitere Informationen zu Abonnements".

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie Auf **Abonnements**.

   Sie sehen nur die Abonnements, die mit dem Konto verknüpft sind, das Sie derzeit anzeigen.

3. Klicken Sie in der Zeile auf das Aktionsmenü, das dem Abonnement entspricht, das Sie verwalten möchten.



4. Wählen Sie diese Option, um das Abonnement umzubenennen oder um die Konten zu verwalten, die mit dem Abonnement verbunden sind.

Ändern des Kontonamens

Ändern Sie Ihren Kontonamen jederzeit, um ihn in etwas Sinnvolles für Sie zu ändern.

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Klicken Sie auf der Registerkarte **Übersicht** neben dem Kontonamen auf das Bearbeiten-Symbol.
3. Geben Sie einen neuen Kontonamen ein und klicken Sie auf **Speichern**.

Aktivieren oder Deaktivieren der SaaS-Plattform

Wir empfehlen nicht, die SaaS-Plattform zu deaktivieren, es sei denn, Sie müssen, um die Sicherheitsrichtlinien Ihres Unternehmens zu erfüllen. Durch die Deaktivierung der SaaS-Plattform ist Ihre Fähigkeit zur Nutzung von integrierten NetApp Cloud-Services begrenzt.

Die folgenden Services stehen bei Cloud Manager nicht zur Verfügung, wenn Sie die SaaS-Plattform deaktivieren:

- Cloud-Compliance
- Kubernetes
- Cloud Tiering
- Globaler Datei-Cache
- Monitoring (Cloud Insights)

Schritte

1. Klicken Sie oben im Cloud Manager auf das Dropdown-Menü **Konto** und klicken Sie auf **Konto verwalten**.
2. Aktivieren Sie auf der Registerkarte **Übersicht** die Option zur Nutzung der SaaS-Plattform.

Verwalten eines HTTPS-Zertifikats für sicheren Zugriff

Standardmäßig verwendet Cloud Manager ein selbstsigniertes Zertifikat für den HTTPS-Zugriff auf die Webkonsole. Sie können ein Zertifikat installieren, das von einer Zertifizierungsstelle (CA) signiert wurde. Dies bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

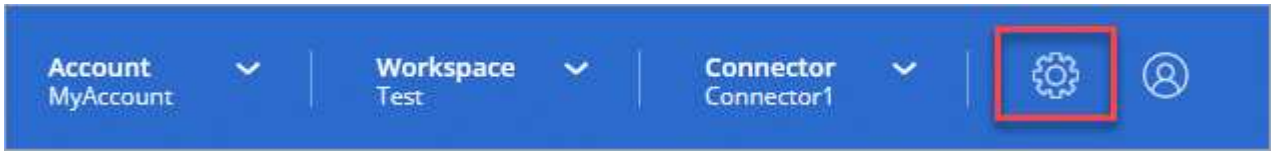
Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "Erfahren Sie, wie".

Installieren eines HTTPS-Zertifikats

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

Schritte

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

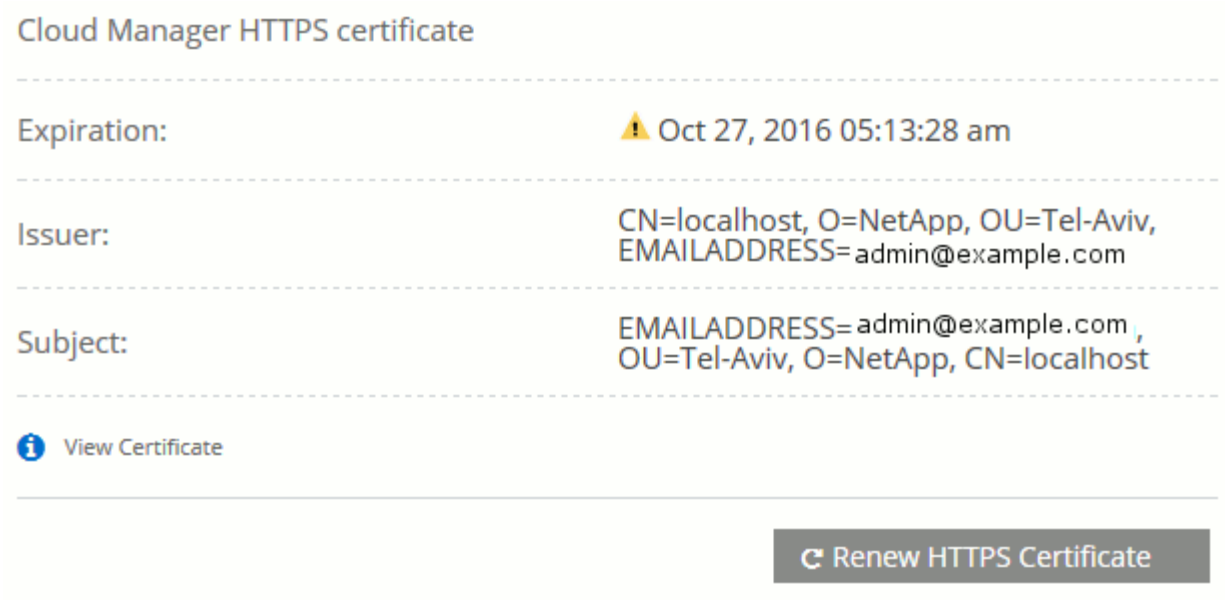


2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung (CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Hostnamen oder den DNS des Connector-Hosts (dessen allgemeiner Name) ein, und klicken Sie dann auf **CSR erstellen**. Cloud Manager zeigt eine Zertifikatsignierungsanforderung 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. Kopieren Sie den Inhalt des signierten Zertifikats, fügen Sie es in das Feld Zertifikat ein und klicken Sie dann auf **Installieren**.
Installieren Sie Ihr eigenes CA-signiertes Zertifikat	a. Wählen Sie **CA-signiertes Zertifikat installieren**. b. Laden Sie sowohl die Zertifikatdatei als auch den privaten Schlüssel und klicken Sie dann auf **Installieren**. Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.

Ergebnis

Cloud Manager verwendet jetzt das CA-signierte Zertifikat, um sicheren HTTPS-Zugriff zu ermöglichen. Die folgende Abbildung zeigt ein Cloud Manager-System, das für den sicheren Zugriff konfiguriert ist:



Erneuerung des Cloud Manager HTTPS-Zertifikats

Sie sollten das HTTPS-Zertifikat von Cloud Manager vor dessen Ablauf erneuern, um einen sicheren Zugriff auf die Cloud Manager-Webkonsole zu gewährleisten. Wenn Sie das Zertifikat nicht vor Ablauf erneuern, wird eine Warnung angezeigt, wenn Benutzer über HTTPS auf die Webkonsole zugreifen.

Schritte

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

   Details zum Cloud Manager-Zertifikat werden angezeigt, einschließlich des Ablaufdatums.

2. Klicken Sie auf **HTTPS-Zertifikat erneuern** und befolgen Sie die Schritte, um eine CSR zu erstellen oder Ihr eigenes CA-signiertes Zertifikat zu installieren.

Ergebnis

Cloud Manager verwendet das neue CA-signierte Zertifikat, um sicheren HTTPS-Zugriff zu ermöglichen.

Entfernen von Cloud Volumes ONTAP Arbeitsumgebungen

Der Kontoadministrator kann eine Cloud Volumes ONTAP Arbeitsumgebung entfernen, in der sie auf ein anderes System verschoben oder Fehler bei der Erkennung behoben werden.

Über diese Aufgabe

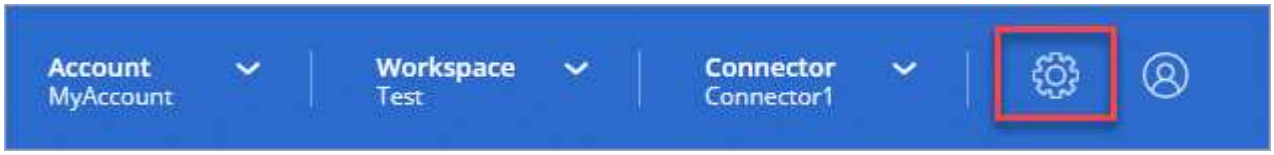
Durch das Entfernen einer Cloud Volumes ONTAP Arbeitsumgebung wird sie aus Cloud Manager entfernt. Das Cloud Volumes ONTAP System wird nicht gelöscht. Sie können die Arbeitsumgebung später neu entdecken.

Durch das Entfernen einer Arbeitsumgebung aus Cloud Manager können Sie Folgendes tun:

- In einem anderen Arbeitsbereich neu entdecken
- Entdecken Sie es von einem anderen Cloud Manager-System neu
- Entdecken Sie es erneut, wenn Sie während der ersten Erkennung Probleme hatten

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Tools**.



2. Klicken Sie auf der Seite Extras auf **Starten**.
3. Wählen Sie die Cloud Volumes ONTAP Arbeitsumgebung aus, die Sie entfernen möchten.
4. Klicken Sie auf der Seite „Prüfen und genehmigen“ auf **Los**.

Ergebnis

Cloud Manager entfernt die Arbeitsumgebung. Benutzer können diese Arbeitsumgebung jederzeit über die Seite Arbeitsumgebungen neu entdecken.

Konfigurieren eines Connectors für die Verwendung eines Proxy-Servers

Wenn Ihre Unternehmensrichtlinien festlegen, dass Sie für die gesamte HTTP-Kommunikation mit dem Internet einen Proxyserver verwenden, müssen Sie Ihre Connectors so konfigurieren, dass sie diesen Proxy-Server verwenden. Der Proxyserver kann sich in der Cloud oder im Netzwerk befinden.

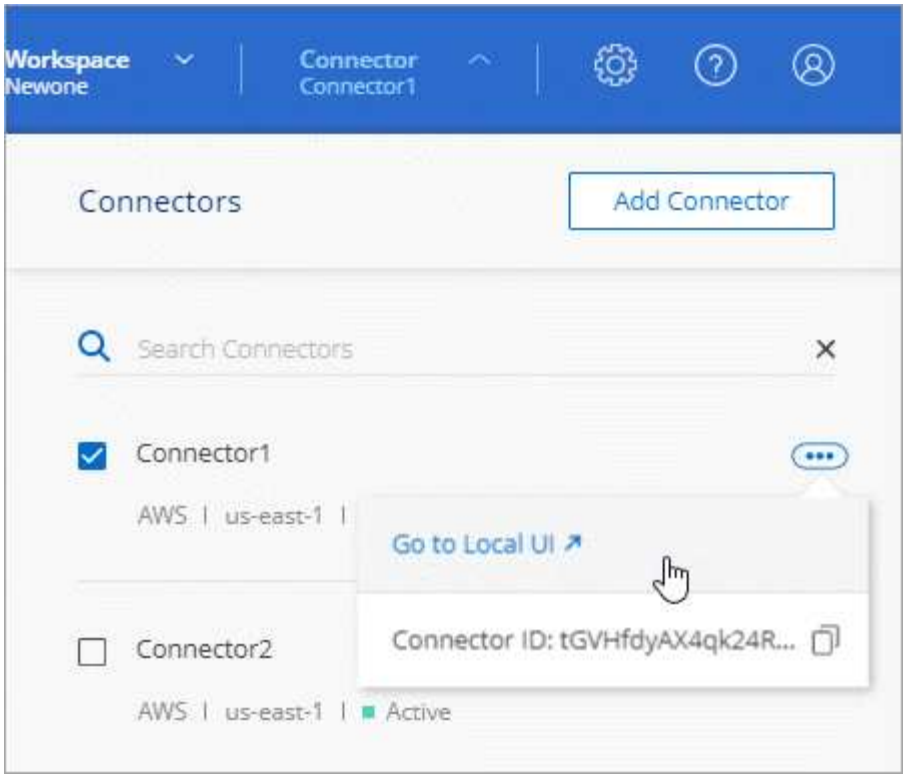
Wenn Sie einen Connector so konfigurieren, dass er einen Proxy-Server verwendet, verwenden dieser Connector und die von ihm verwalteten Cloud Volumes ONTAP-Systeme (einschließlich aller HA-Mediatoren) den Proxy-Server.

Schritte

1. "Melden Sie sich bei der SaaS-Schnittstelle von Cloud Manager an" Von einem Computer mit einer Netzwerkverbindung zur Instanz des Connectors.

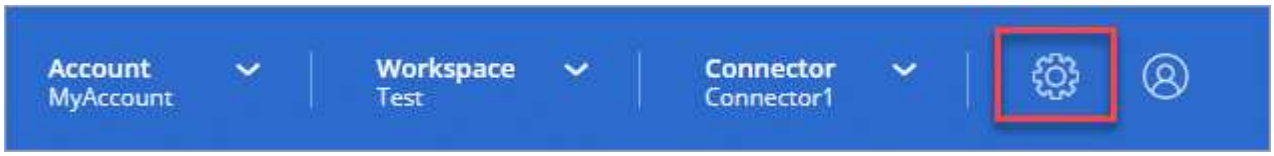
   Wenn der Connector keine öffentliche IP-Adresse hat, benötigen Sie eine VPN-Verbindung oder Sie müssen eine Verbindung von einem Jump-Host herstellen, der sich im gleichen Netzwerk wie der Connector befindet.

2. Klicken Sie auf das Dropdown-Menü **Connector** und dann auf **zur lokalen Benutzeroberfläche** für einen bestimmten Konnektor.



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

3. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Manager-Einstellungen**.



4. Geben Sie unter HTTP Proxy den Server mithilfe der Syntax ein http://address:portGeben Sie einen Benutzernamen und ein Passwort an, wenn eine grundlegende Authentifizierung für den Server erforderlich ist, und klicken Sie dann auf Speichern.

Cloud Manager unterstützt keine Passwörter, die das Zeichen @ enthalten.

Ergebnis

Nachdem Sie den Proxyserver angegeben haben, werden neue Cloud Volumes ONTAP Systeme automatisch so konfiguriert, dass sie den Proxyserver beim Senden von AutoSupport Nachrichten verwenden. Wenn Sie den Proxy-Server nicht angegeben haben, bevor Benutzer Cloud Volumes ONTAP-Systeme erstellen, müssen sie mit System Manager den Proxyserver manuell in den AutoSupport-Optionen für jedes System festlegen.

Überschreiben von CIFS-Sperren für Cloud Volumes ONTAP HA in Azure

Der Kontoadministrator kann eine Einstellung in Cloud Manager aktivieren, die Probleme

mit dem Cloud Volumes ONTAP Storage Failover bei Azure-Wartungereignissen verhindert. Wenn Sie diese Einstellung aktivieren, sperrt Cloud Volumes ONTAP Vetoes CIFS und setzt aktive CIFS-Sitzungen zurück.

Über diese Aufgabe

Microsoft Azure plant regelmäßige Wartungsereignisse auf seinen Virtual Machines. Wenn auf einem Node in einem Cloud Volumes ONTAP HA-Paar ein Wartungsereignis stattfindet, initiiert das HA-Paar das Storage Takeover. Wenn während dieses Wartungsereignisses aktive CIFS-Sitzungen vorhanden sind, können die Sperren von CIFS-Dateien das Storage-Failover verhindern.

Wenn Sie diese Einstellung aktivieren, setzt Cloud Volumes ONTAP die Sperren zurück und setzt die aktiven CIFS-Sitzungen zurück. So kann das HA-Paar während dieser Wartungsereignisse das Storage Failover abschließen.

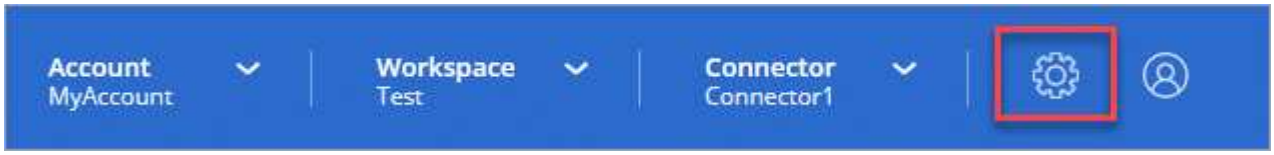
Dieser Prozess kann CIFS-Clients stören. Daten, die nicht von CIFS-Clients übertragen werden, können verloren gehen.

Was Sie benötigen

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

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Cloud Manager-Einstellungen**.



2. Aktivieren Sie unter **HA CIFS locks** das Kontrollkästchen und klicken Sie auf **Speichern**.

Referenz

Rollen

Die Rollen Kontoverwaltung, Workspace Admin und Cloud Compliance Viewer bieten Benutzern spezifische Berechtigungen.

Aufgabe	Kontoadministrator	Workspace-Verwaltung	Cloud Compliance Viewer
Verwalten von Arbeitsumgebungen	Ja.	Ja.	Nein
Services in Arbeitsumgebungen ermöglichen	Ja.	Ja.	Nein
Anzeigen des Status der Datenreplizierung	Ja.	Ja.	Nein
Zeitachse anzeigen	Ja.	Ja.	Nein

Aufgabe	Kontoadministrator	Workspace-Verwaltung	Cloud Compliance Viewer
Wechseln Sie zwischen Arbeitsbereichen	Ja.	Ja.	Ja.
Anzeigen von Compliance-Scanergebnissen	Ja.	Ja.	Ja.
Arbeitsumgebungen löschen	Ja.	Nein	Nein
Kubernetes-Cluster mit Arbeitsumgebungen verbinden	Ja.	Nein	Nein
Cloud Volumes ONTAP Bericht erhalten	Ja.	Nein	Nein
Anschlüsse Erstellen	Ja.	Nein	Nein
Managen von Cloud Central Konten	Ja.	Nein	Nein
Anmeldeinformationen verwalten	Ja.	Nein	Nein
Ändern der Cloud Manager-Einstellungen	Ja.	Nein	Nein
Anzeigen und Verwalten des Support-Dashboards	Ja.	Nein	Nein
Entfernen Sie Arbeitsumgebungen aus Cloud Manager	Ja.	Nein	Nein
Installieren Sie ein HTTPS-Zertifikat	Ja.	Nein	Nein

Weiterführende Links

- "Einrichtung von Workspaces und Benutzern im Cloud Central Konto"
- "Managen von Workspaces und Benutzern im Cloud Central Konto"

Wie Cloud Manager die Berechtigungen von Cloud-Providern nutzt

Für die Ausführung von Aktionen bei Ihrem Cloud-Provider sind für Cloud Manager Berechtigungen erforderlich. Diese Berechtigungen sind in enthalten "Die von NetApp bereitgestellten Richtlinien". Sie möchten vielleicht wissen, was Cloud Manager mit diesen Berechtigungen macht.

Was Cloud Manager mit AWS-Berechtigungen macht

Cloud Manager verwendet ein AWS-Konto, um API-Aufrufe an mehrere AWS-Services durchzuführen, darunter EC2, S3, CloudFormation, IAM, den Security Token Service (STS) und den Key Management Service (KMS).

Aktionen	Zweck
„ec2:StartInstances“, „ec2:StopInstances“, „ec2:DescribeInstances“, „ec2:DescribeInstanceStatus“, „ec2:RunInstances“, „ec2:TerminateInstances“, „ec2:ModifyInstanceAttribut“,	Startet eine Cloud Volumes ONTAP Instanz und stoppt, startet und überwacht die Instanz.
"EC2:DescribeInstanceAttribute",	Überprüft, ob das erweiterte Netzwerk für unterstützte Instanztypen aktiviert ist.
„ec2:DescribeRouteTables“, „ec2:DescribeImages“,	Startet eine Cloud Volumes ONTAP HA-Konfiguration.
"EC2:CreateTags",	Kennzeichnet jede Ressource, die Cloud Manager erstellt, mit den Tags "workingenvironment" und "WorkingEnvironmentId". Cloud Manager verwendet diese Tags für Wartung und Kostenzuordnung.
„ec2:CreateVolume“, „ec2:DescribeVolumes“, „ec2:ModifyVolumeAttribute“, „ec2:AttachVolume“, „ec2:DeleteVolume“, „ec2:DetachVolume“,	Managt die EBS Volumes, die Cloud Volumes ONTAP als Back-End Storage verwendet.
„ec2:CreateSecurityGroup“, „ec2:DeleteSecurityGroup“, „ec2:DescribeSecurityGroups“, „ec2:RevokeSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupEgress“, „ec2:AuthoriseSecurityGroupIngress“, „ec2:RevokeSecurityGroupIngress“,	Erstellt vordefinierte Sicherheitsgruppen für Cloud Volumes ONTAP.
„ec2:CreateNetworkInterface“, „ec2:DescribeNetworkInterfaces“, „ec2:DeleteNetworkInterface“, „ec2:ModifyNetworkInterface“,	Erstellt und managt Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz.
„ec2:DescribeSubnets“, „ec2:DescribeVpcs“,	Ruft die Liste der Zielsubnetze und Sicherheitsgruppen ab, die beim Erstellen einer neuen Arbeitsumgebung für Cloud Volumes ONTAP benötigt wird.
"EC2:DescribeDhcpOptions",	Bestimmt DNS-Server und den Standarddomänennamen beim Starten von Cloud Volumes ONTAP Instanzen.
„ec2:CreateSnapshot“, „ec2:DeleteSnapshot“, „ec2:DescribeSnapshots“,	Erstellt Snapshots von EBS Volumes während der Ersteinrichtung und bei jedem Anhalten einer Cloud Volumes ONTAP Instanz.
"EC2:GetConsoleOutput",	Erfasst die Cloud Volumes ONTAP Konsole, die an AutoSupport Nachrichten angehängt ist.
"EC2:DescribeKeyPairs",	Ruft beim Starten von Instanzen die Liste der verfügbaren Schlüsselpaare ab.
"EC2:DescribeRegions",	Ruft eine Liste der verfügbaren AWS-Regionen ab.
„ec2:DeleteTags“, „ec2:DescribeTags“,	Managt Tags für Ressourcen, die mit Cloud Volumes ONTAP Instanzen verbunden sind.

Aktionen	Zweck
„Cloudformation:CreateStack“, „Cloudformation:DeleteStack“, „Cloudformation:DescribeStacks“, „Cloudformation:DescribeStackEvents“, „Cloudformation:ValidateTemplate“,	Startet Cloud Volumes ONTAP Instanzen.
„iam:PassRollenole“, „iam:CreateRollenole“, „iam:DeleteRollenole“, „iam:PutRolePolicy“, „iam:CreateInstanceProfil“, „iam:DeleteRolePolicy“, „iam:AddRoleToInstanceProfile“, „iam:RemoveRoleFromInstanceProfile“, „iam:DeleteInstanceProfile“,	Startet eine Cloud Volumes ONTAP HA-Konfiguration.
„iam:ListInstanceProfiles“, „STS:DecodeAuthorisationMessage“, „ec2:AssociateIamInstanceProfil“, „ec2:DescribeIamInstanceProfilAssociations“, „ec2:DisassotionIamInstanceProfile“,	Managt Instanzprofile für Cloud Volumes ONTAP Instanzen.
„s3:GetBucketTagging“, „s3:GetBucketLocation“, „s3:ListAllMyBuckets“, „s3:ListBucket“	Informationen zu AWS S3-Buckets, damit Cloud Manager in den NetApp Data Fabric Cloud Sync Service integriert werden kann
„s3:CreateBucket“, „s3:DeleteBucket“, „s3:GetLifecycleConfiguration“, „s3:PutLifecycleConfiguration“, „s3:PutBucketTagging“, „s3:ListBucketVersions“, „s3:GetBucketPolicyStatus“, „s3:GetBucketPublicAccessBlock“, „s3:GetBucketAcl“, „s3:GetBucketPolicy“, „s3:PutBucketPublicAccessBlock“	Managt den S3-Bucket, den ein Cloud Volumes ONTAP System als Kapazitäts-Tier für das Daten-Tiering verwendet
„Kms:Liste*“, „Kms:Reverschlüsselt*“, „Kms:Beschreiben*“, „Kms:CreateGrant“,	Aktiviert die Datenverschlüsselung von Cloud Volumes ONTAP mithilfe des AWS KMS (Key Management Service).
„ce:GetReservationUtilisation“, „ce:GetDimensionValues“, „ce:GetCostAndUsage“, „ce:GetTags“	Abrufen von AWS-Kostendaten für Cloud Volumes ONTAP
„ec2:CreatePlacementGroup“, „ec2:DeletePlacementGroup“	Wenn Sie eine HA-Konfiguration in einer einzigen AWS Availability Zone implementieren, startet Cloud Manager die beiden HA-Nodes und den Mediator in einer AWS Spread-Placement-Gruppe.
„ec2:DescribeReserviertInstanceAngebote“	Cloud Manager verwendet die Berechtigung als Teil der Cloud Compliance-Implementierung, um den Instanztyp auszuwählen, der verwendet werden soll.

Aktionen	Zweck
„s3:DeleteBucket“, „s3:GetLifecycleConfiguration“, „s3:PutLifecycleConfiguration“, „s3:PutBucketTagging“, „s3:ListBucketVersions“, „s3:GetObject“, „s3:ListBucket“, „s3:ListAllMyBuckets“, „s3:GetBucketTagging“, „s3:GetBucketLocation“ „s3:GetBucketPolicyStatus“, „s3:GetBucketPublicAccessBlock“, „s3:GetBucketAcl“, „s3:GetBucketPolicy“, „s3:PutBucketPublicAccessBlock“	Cloud Manager verwendet diese Berechtigungen, wenn Sie den Service „Backup in S3“ aktivieren.

Was Cloud Manager mit Azure-Berechtigungen tut

Die Cloud Manager Azure Policy enthält die Berechtigungen, die Cloud Manager für die Bereitstellung und das Management von Cloud Volumes ONTAP in Azure benötigt.

Aktionen	Zweck
„Microsoft.Compute/locations/operations/read", „Microsoft.Compute/locations/vmSizes/read", „Microsoft.Compute/operations/read", „Microsoft.Compute/virtualMachines/instanceView/read", „Microsoft.Compute/virtualMachines/powerOff/action", „Microsoft.Compute/virtualMachines/read", „Microsoft.Compute/virtualMachines/restart/action", „Microsoft.Compute/virtualMachines/start/action", „Microsoft.Compute/virtualMachines/deallocate/action", „Microsoft.Compute/virtualMachines/vmSizes/read", „Microsoft.Compute/virtualMachines/write",	Erstellt Cloud Volumes ONTAP und beendet, startet, löscht und erhält den Status des Systems.
„Microsoft.Compute/images/write", „Microsoft.Compute/images/read",	Ermöglicht die Implementierung von Cloud Volumes ONTAP über eine VHD.
„Microsoft.Compute/disks/delete", „Microsoft.Compute/disks/read", „Microsoft.Compute/disks/write", „Microsoft.Storage/ChecknameAvailability/read“, „Microsoft.Storage/Operations/read“, „Microsoft.Storage/StorageAccounts/Listkeys/Action“, „Microsoft.Storage/StorageAccounts/read“, „Microsoft.Storage/storageAccounts/Retgeneratekey/Action“, „Microsoft.Storage/storageAccounts/write“, „Microsoft.Storage/storageAccounts/delete“, „Microsoft.Storage/Nutzungs/Lesevorgang“,	Verwaltet Azure Storage-Konten und -Festplatten und hängt die Festplatten an Cloud Volumes ONTAP an.
„Microsoft.Network/networkInterfaces/read", „Microsoft.Network/networkInterfaces/write", „Microsoft.Network/networkInterfaces/join/action",	Erstellt und managt Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz.
„Microsoft.Network/networkSecurityGroups/read", „Microsoft.Network/networkSecurityGroups/write", „Microsoft.Network/networkSecurityGroups/join/action",	Erstellt vordefinierte Netzwerksicherheitsgruppen für Cloud Volumes ONTAP.

Aktionen	Zweck
„Microsoft.Ressourcen/Abonnements/Standorte/gelesen“, „Microsoft.Network/locations/operationResults/read", „Microsoft.Network/locations/operations/read", „Microsoft.Network/virtualNetworks/read", „Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", „Microsoft.Network/virtualNetworks/subnets/read", „Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", „Microsoft.Network/virtualNetworks/virtualMachines/read", „Microsoft.Network/virtualNetworks/subnets/join/action",	Ruft Netzwerkinformationen zu Regionen, dem Ziel-VNet und dem Subnetz ab und fügt Cloud Volumes ONTAP VNets hinzu.
„Microsoft.Network/virtualNetworks/subnets/write", „Microsoft.Network/routeTables/join/action",	Aktiviert VNet Service-Endpunkte für das Daten-Tiering.
„Microsoft.Ressourcen/Implementierungen/Betrieb/Lesen“, „Microsoft.Resources/Deployments/read“, „Microsoft.Resources/Deployments/write“,	Implementierung von Cloud Volumes ONTAP anhand einer Vorlage
„Microsoft.Resources/Deployments/Operations/read“, „Microsoft.Resources/Deployments/read“, „Microsoft.Resources/Deployments/write“, „Microsoft.Resources/Resources/read“, „Microsoft.Resources/Subscriptions/Operationresults/read“, „Microsoft.Resources/subskriptions/resourceGroups/delete“, „Microsoft.Resources/Subskriptions/resourceGroups/read“, „Microsoft.Resources/subskriptions/resourcegruppen/Resources/read“, „Microsoft.Resources/subskriptions/resourceGroups/write“,	Erstellt und managt Ressourcengruppen für Cloud Volumes ONTAP.
„Microsoft.Compute/snapshots/write", „Microsoft.Compute/snapshots/read", „Microsoft.Compute/disks/beginGetAccess/action"	Erstellt und managt von Azure verwaltete Snapshots.
„Microsoft.Compute/availabilitySets/write", „Microsoft.Compute/availabilitySets/read",	Erstellt und managt Verfügbarkeitssätze für Cloud Volumes ONTAP.
„Microsoft.MarketplaceOrdering/offertypes/Publisher/offerers/Plans/Agreements/read“, „Microsoft.MarketplaceOrdering/offertypes/Publisher/Offerers/Plans/Agreements/write“	Ermöglicht programmatische Implementierungen über Azure Marketplace.

Aktionen	Zweck
„Microsoft.Network/loadBalancers/read", „Microsoft.Network/loadBalancers/write", „Microsoft.Network/loadBalancers/delete", „Microsoft.Network/loadBalancers/backendAddressPools/read", „Microsoft.Network/loadBalancers/backendAddressPools/join/action", „Microsoft.Network/loadBalancers/frontendIPConfigurations/read", „Microsoft.Network/loadBalancers/loadBalancingRules/read", „Microsoft.Network/loadBalancers/probes/read", „Microsoft.Network/loadBalancers/probes/join/action",	Managt einen Azure Load Balancer für HA-Paare.
"Microsoft.Authorization/locks/*"	Ermöglicht das Management von Sperren auf Azure Festplatten.
„Microsoft.Authorization/roleDefinitions/write“, „Microsoft.Authorization/roleAssignments/write“, „Microsoft.Web/sites/*“	Managt Failover für HA-Paare
„Microsoft.Network/privateEndpoints/write", „Microsoft.Storage/StoragebAccounts/PrivateEndpointConnectionsApproval/Action“, „Microsoft.Storage/storageAccounts/privateEndpointConnections/read“, „Microsoft.Network/privateEndpoints/read", „Microsoft.Network/privateDnsZones/write", „Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", „Microsoft.Network/virtualNetworks/join/action", „Microsoft.Network/privateDnsZones/A/write", „Microsoft.Network/privateDnsZones/read", „Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Ermöglicht das Management privater Endpunkte. Private Endpunkte werden verwendet, wenn keine Konnektivität außerhalb des Subnetzes bereitgestellt wird. Cloud Manager erstellt das Storage-Konto für HA mit nur der internen Konnektivität im Subnetz.
„Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Ermöglicht Cloud Manager das Löschen von Volumes für Azure NetApp Files.
„Microsoft.Resources/Deployments/OperationStatuses/read“	Azure erfordert diese Berechtigung für einige Implementierungen von Virtual Machines (das hängt von der zugrunde liegenden physischen Hardware ab, die während der Implementierung verwendet wird).
„Microsoft.Resources/Deployments/OperationStatuses/read“, „Microsoft.Insights/Metrics/Read“, „Microsoft.Compute/virtualMachines/extensions/write", „Microsoft.Compute/virtualMachines/extensions/read", „Microsoft.Compute/virtualMachines/extensions/delete", „Microsoft.Compute/virtualMachines/delete", „Microsoft.Network/networkInterfaces/delete", „Microsoft.Network/networkSecurityGroups/delete", „Microsoft.Resources/Deployments/delete“,	Ermöglicht die Verwendung von Global File Cache.

Aktionen	Zweck
„Microsoft.Compute/diskEncryptionSets/read"	Cloud Manager ermöglicht die Verschlüsselung von über Azure gemanagten Festplatten auf Cloud Volumes ONTAP-Systemen mit einem einzelnen Node mithilfe von externen Schlüsseln eines anderen Kontos. Diese Funktion wird durch APIs unterstützt.

Was Cloud Manager mit GCP-Berechtigungen macht

Die Cloud Manager-Richtlinie für GCP beinhaltet die Berechtigungen, die Cloud Manager für die Implementierung und das Management von Cloud Volumes ONTAP benötigt.

Aktionen	Zweck
- Compute.Disks.create - Compute.Disks.createSnapshot - compute.disks.delete - Compute.Disks.get - Compute.Disks.list - compute.disks.setLabels - compute.disks.use	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.
- Compute.Firewalls.create - compute.firewalls.delete - Compute.Firewalls.get - Compute.Firewalls.list	Um Firewall-Regeln für Cloud Volumes ONTAP zu erstellen.
- Compute.globalOperations.get	Um den Status von Vorgängen anzuzeigen.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Um Images für VM-Instanzen zu erhalten.
- compute.instances.attachDisk - compute.instances.detachDisk	Zum Verbinden und Trennen von Festplatten mit Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Um Cloud Volumes ONTAP VM-Instanzen zu erstellen und zu löschen.
- compute.instances.get	Um VM-Instanzen aufzulisten.
- compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.
- compute.instances.list	Um die Liste der Instanzen in einer Zone abzurufen.
- compute.instances.setDeletionProtection	So legen Sie den Löschschutz für die Instanz fest:
- compute.instances.setLabels	So fügen Sie Etiketten hinzu:
- compute.instances.setMachineType	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.
- compute.instances.setMetadata	Um Metadaten hinzuzufügen.
- compute.instances.setTags	Um Tags für Firewall-Regeln hinzuzufügen.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Um Cloud Volumes ONTAP zu starten und anzuhalten.
- Compute.machineTypes.get	Um die Anzahl der Kerne zu erhalten, um qouten zu überprüfen.
- compute.projects.get	Zur Unterstützung mehrerer Projekte.

Aktionen	Zweck
- Compute.Snapshots.create - compute.snapshots.delete - Compute.Snapshots.get - Compute.Snapshots.list - compute.snapshots.setLabels	Um persistente Festplatten-Snapshots zu erstellen und zu managen.
- compute.networks.get - compute.networks.list - Compute.Regions.get - Compute.Regions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.Zones.get - Compute.Zones.list	Um die Netzwerkinformationen zu erhalten, die für die Erstellung einer neuen Instanz einer Cloud Volumes ONTAP Virtual Machine erforderlich sind.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - istmentmanager.Manifeste.get - istmentmanager.manifeste.list - istmentmanager.Operations.get - istmentmanager.Operations.list - bereitsmanager.Resources.get - bereitsmanager.Resources.list - Bereitstellungmanager.typeProviders.get - istmentmanager.tyArten.list	Um die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereitzustellen.
- Logging.logEntries.list - Logging.privateLogEntries.list	Zum Abrufen von Stack-Protokolllaufwerken.
- resourcemanager.projects.get	Zur Unterstützung mehrerer Projekte.
- Storage.Buckets.create - storage.buckets.delete - Storage.Buckets.get - Storage.Buckets.list - Storage.Buckets.Update	Zur Erstellung und Verwaltung eines Google Cloud Storage Buckets für Daten-Tiering
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.kryptoKeys.get - cloudkms.kryptoKeys.list - cloudkms.Keyrings.list	Verwenden von vom Kunden gemanagten Verschlüsselungen aus dem Cloud-Verschlüsselungsmanagement-Service mit Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	So legen Sie ein Servicekonto für die Cloud Volumes ONTAP-Instanz fest: Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket.

AWS Marketplace-Seiten für Cloud Manager und Cloud Volumes ONTAP

Im AWS Marketplace für Cloud Manager und Cloud Volumes ONTAP sind diverse Angebote erhältlich. Wenn Sie Hilfe zum Verständnis des Zwecks jeder Seite benötigen, lesen Sie die Beschreibungen unten.

Vergessen Sie in jedem Fall nicht, dass Sie Cloud Volumes ONTAP nicht über den AWS Marketplace in AWS starten können. Sie müssen es direkt über Cloud Manager starten.

Ziel	Zu verwendende AWS Marketplace Seite	Weitere Informationen
Ermöglichen Sie die Nutzung von Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance und anderen Add-on-Services	"Cloud Manager – Implementierung und Management von NetApp Cloud Data Services"	Mit diesem Abonnement können Sie die PAYGO-Version von Cloud Volumes ONTAP 9.6 und höher berechnen. Es ermöglicht zudem eine Abrechnung auf Cloud Tiering, Cloud Compliance und weitere Add-on-Services. Sie sollten dieses Angebot abonnieren, wenn Sie von Cloud Manager aufgefordert werden und Sie zur Seite umgeleitet werden. Cloud Manager fordert Sie auf, sich im Assistenten für die Arbeitsumgebung zu befinden oder neue Anmeldedaten in den Einstellungen hinzuzufügen. Auf dieser Seite können Sie Cloud Manager nicht in AWS starten. Das sollte von geschehen "NetApp Cloud Central", Oder alternativ das AMI in Zeile 3 dieser Tabelle verwenden.
Ermöglichen Sie die Nutzung von Cloud Volumes ONTAP-PAYGO, Cloud Tiering, Cloud Compliance und anderen Add-on-Services *unter Verwendung eines jährlichen Vertrags*	"Cloud Manager (Verträge) – Deploy amp; Manage NetApp Cloud Data Services"	Dieses Abonnement ist eine Alternative zum Abonnement in der ersten Zeile. Es ermöglicht Ihnen, eine jährliche Vorauszahlung für die Angebote zu erhalten. Das gilt vor allem für NetApp Partner.
Implementieren Sie Cloud Manager über AWS Marketplace über ein AMI	"Cloud Manager - Manuelle Installation ohne Zugriffsschlüssel"	Wir empfehlen Ihnen, Cloud Manager in AWS ab zu starten "NetApp Cloud Central", Aber Sie können es auf dieser AWS Marketplace Seite starten, wenn Sie es bevorzugen.
Implementierung von Cloud Volumes ONTAP PAYGO (9.5 oder früher) ermöglichen	• "Cloud Volumes ONTAP für AWS" • "Cloud Volumes ONTAP für AWS – Hochverfügbarkeit"	Auf diesen AWS Marketplace-Seiten können Sie für Version 9.5 und früher die Single Node- oder HA-Versionen von Cloud Volumes ONTAP PAYGO abonnieren. Ab Version 9.6 müssen Sie die Anmeldung über die in Zeile 1 dieser Tabelle aufgeführten AWS Marketplace-Seite für PAYGO-Implementierungen durchführen.