Erste Schritte

Cloud Manager 3.6

NetApp
March 25, 2024

Inhalt

Erste Schritte

Implementierungsübersicht

Bevor Sie beginnen, sollten Sie sich vielleicht besser mit Ihren Optionen für die Implementierung von OnCommand Cloud Manager und Cloud Volumes ONTAP vertraut machen.

Installation von Cloud Manager

Cloud Manager Software ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich. Sie können Cloud Manager an einem der folgenden Standorte bereitstellen:

- Amazon Web Services (AWS)
- Microsoft Azure
- IBM Cloud
- In Ihrem eigenen Netzwerk

Wie Sie Cloud Manager implementieren, hängt davon ab, für welchen Standort Sie sich entscheiden:

Standort	So implementieren Sie Cloud Manager
AWS	"Cloud Manager über NetApp Cloud Central implementieren"
AWS C2S	"Implementieren Sie Cloud Manager über den AWS Intelligence Community Marketplace"
Azure allgemein verfügbare Region	"Cloud Manager über NetApp Cloud Central implementieren"
Azure Government	"Implementieren von Cloud Manager über den Azure US Government Marketplace"
Azure Deutschland	"Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"
IBM Cloud	"Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"
Des On-Premises-Netzwerks	"Laden Sie die Software auf einem Linux-Host herunter, und installieren Sie sie"

Einrichtung von Cloud Manager

Möglicherweise möchten Sie nach der Installation von Cloud Manager zusätzliche Einrichtung durchführen, z. B. das Hinzufügen weiterer Cloud-Provider-Konten, das Installieren eines HTTPS-Zertifikats und mehr.

- "Cloud Provider Accounts zu Cloud Manager hinzufügen"
- "Installieren eines HTTPS-Zertifikats"
- "Benutzer und Mandanten einrichten"
- "Einrichten des AWS KMS"

Implementierung von Cloud Volumes ONTAP

Nachdem Sie Cloud Manager in Betrieb genommen haben, können Sie mit der Implementierung von Cloud Volumes ONTAP in AWS und Microsoft Azure beginnen.

"Erste Schritte in AWS" Und "Erste Schritte in Azure" Anweisungen zur schnellen Inbetriebnahme von Cloud Volumes ONTAP Weitere Hilfe finden Sie unter:

- "Unterstützte Konfigurationen für Cloud Volumes ONTAP 9.5"
- "Planung Ihrer Konfiguration"
- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Volumes ONTAP in Azure"

Erste Schritte mit Cloud Volumes ONTAP in AWS

Die ersten Schritte mit Cloud Volumes ONTAP in AWS sind über NetApp Cloud Central möglich.

Richten Sie Ihr Netzwerk ein

1. Aktivieren Sie ausgehenden Internetzugriff vom Ziel-VPC aus, sodass Cloud Manager und Cloud Volumes ONTAP mit mehreren Endpunkten in Verbindung treten können.

   Dieser Schritt ist wichtig, da Cloud Manager Cloud Volumes ONTAP nicht ohne ausgehenden Internetzugang implementieren kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für "Cloud Manager" Und "Cloud Volumes ONTAP".

2. Richten Sie einen VPC-Endpunkt für den S3-Dienst ein.

   Ein VPC-Endpunkt ist erforderlich, wenn Sie kalte Daten von Cloud Volumes ONTAP auf kostengünstigen Objekt-Storage einstufen möchten.

Abonnieren Sie Cloud Volumes ONTAP über den AWS Marketplace

Abonnieren von "AWS Marketplace" Ist zur Annahme der Softwarebedingungen erforderlich. Sie sollten sich nur über Marketplace anmelden. Starten von Cloud Volumes ONTAP von überall aus, Cloud Manager wird jedoch nicht unterstützt.

Stellen Sie die erforderlichen AWS-Berechtigungen bereit

Wenn Sie Cloud Manager über NetApp Cloud Central implementieren, müssen Sie ein AWS-Konto verwenden, das über die Berechtigung zum Bereitstellen der Instanz verfügt.

1. Gehen Sie zur AWS IAM-Konsole und erstellen Sie eine Richtlinie durch Kopieren und Einfügen der Inhalte des "NetApp Cloud Central-Richtlinie für AWS".
2. Hängen Sie die Richtlinie an den IAM-Benutzer an.

Starten Sie Cloud Manager über NetApp Cloud Central

Cloud Manager Software ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich. Es dauert nur ein paar Minuten, um eine Cloud Manager Instanz von zu starten "Cloud Central".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Wenn Cloud Manager fertig ist, klicken Sie einfach auf Erstellen, wählen Sie den Systemtyp aus, den Sie starten möchten, und führen Sie die Schritte im Assistenten aus. Nach 25 Minuten sollte Ihr erstes Cloud Volumes ONTAP System betriebsbereit sein.

Weiterführende Links

- "Bewertung"
- "Netzwerkanforderungen für Cloud Manager"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"
- "Sicherheitsgruppenregeln für AWS"
- "Cloud Provider Accounts zu Cloud Manager hinzufügen"
- "Was Cloud Manager mit AWS-Berechtigungen macht"
- "Starten von Cloud Volumes ONTAP in AWS"
- "Starten von Cloud Manager über den AWS Marketplace"

Erste Schritte mit Cloud Volumes ONTAP in Azure

Erste Schritte mit Cloud Volumes ONTAP in Azure sind über NetApp Cloud Central möglich. Für die Implementierung von Cloud Manager in stehen separate Anweisungen zur Verfügung "Azure Regionen der US-Regierung" Und ein "Azure Deutschland Regionen".

Richten Sie Ihr Netzwerk ein

Aktivieren Sie ausgehenden Internetzugriff vom Ziel-VNet aus, sodass Cloud Manager und Cloud Volumes ONTAP mit mehreren Endpunkten in Verbindung treten können.

Dieser Schritt ist wichtig, da Cloud Manager Cloud Volumes ONTAP nicht ohne ausgehenden Internetzugang implementieren kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für "Cloud Manager" Und "Cloud Volumes ONTAP".

Stellen Sie die erforderlichen Azure Berechtigungen bereit

Wenn Sie Cloud Manager über NetApp Cloud Central implementieren, müssen Sie ein Azure Konto verwenden, das über Berechtigungen zum Bereitstellen der Virtual Machine von Cloud Manager verfügt.

1. Laden Sie die herunter "NetApp Cloud Central-Richtlinie für Azure".

2. Ändern Sie die JSON-Datei, indem Sie im Feld "AssignableScopes" Ihre Azure Abonnement-ID hinzufügen.
3. Verwenden Sie die JSON-Datei, um in Azure namens *Azure SetupAsService* eine benutzerdefinierte Rolle zu erstellen.

   Beispiel: **Az Rollendefinition erstellen --Role-Definition C:\Policy_for_Setup_as_Service_Azure.json**

4. Weisen Sie die benutzerdefinierte Rolle über das Azure Portal dem Benutzer zu, der Cloud Manager über Cloud Central bereitstellt.

Starten Sie Cloud Manager über NetApp Cloud Central

Cloud Manager Software ist für die Implementierung und das Management von Cloud Volumes ONTAP erforderlich. Es dauert nur ein paar Minuten, um eine Cloud Manager Instanz von zu starten "Cloud Central".

Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Sobald Cloud Manager bereit ist, klicken Sie einfach auf Erstellen, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. Nach 25 Minuten sollte Ihr erstes Cloud Volumes ONTAP System betriebsbereit sein.

Weiterführende Links

- "Bewertung"
- "Netzwerkanforderungen für Cloud Manager"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in Azure"
- "Sicherheitsgruppenregeln für Azure"
- "Cloud Provider Accounts zu Cloud Manager hinzufügen"
- "Was Cloud Manager mit Azure-Berechtigungen tut"
- "Starten von Cloud Volumes ONTAP in Azure"
- "Cloud Manager über den Azure Marketplace starten"

Einrichten von Cloud Manager

Cloud-Provider-Konten zu Cloud Manager hinzufügen

Wenn Sie Cloud Volumes ONTAP in verschiedenen Cloud-Konten implementieren möchten, müssen Sie diese Konten die erforderlichen Berechtigungen erteilen und anschließend die Details zu Cloud Manager hinzufügen.

Bei der Implementierung von Cloud Manager über Cloud Central fügt Cloud Manager automatisch einen hinzu "Konto eines Cloud-Providers" Für das Konto, in dem Sie Cloud Manager implementiert haben. Ein anfängliches Cloud-Provider-Konto wird nicht hinzugefügt, wenn Sie die Cloud Manager Software manuell auf einem vorhandenen System installieren.

Einrichten und Hinzufügen von AWS Konten zu Cloud Manager

Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Konten implementieren möchten, müssen Sie diese Konten die erforderlichen Berechtigungen erteilen und anschließend die Details zu Cloud Manager hinzufügen. 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.

- Gewähren von Berechtigungen bei der Bereitstellung von AWS Schlüsseln
- Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

Gewähren von Berechtigungen bei der 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

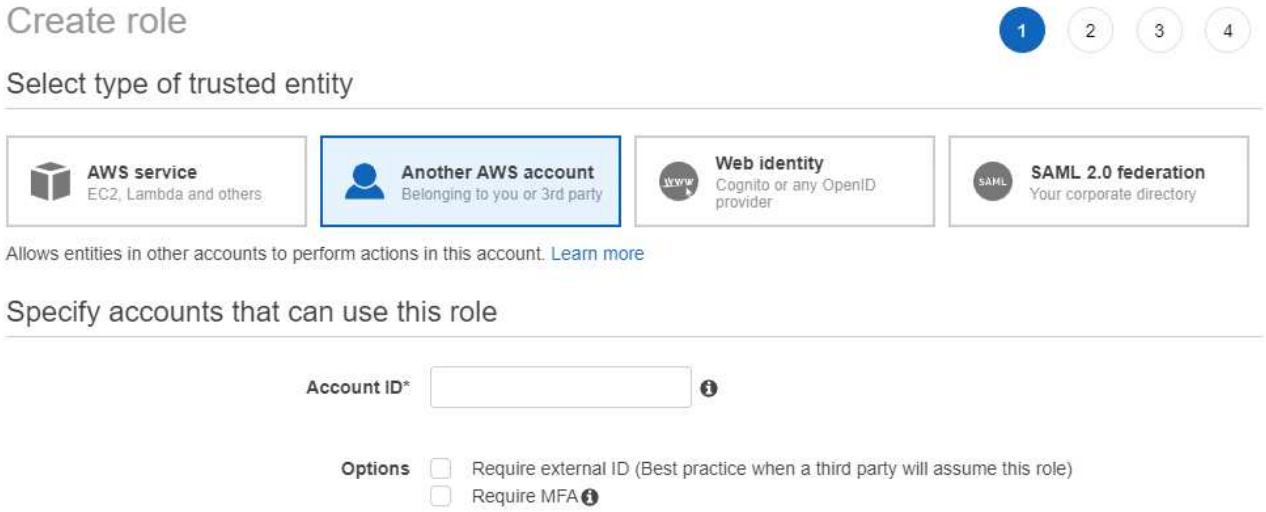
Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Cloud Manager-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie Cloud Manager über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

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 Cloud Manager Instanz befindet.
   - Hängen Sie die Cloud Manager IAM-Richtlinie an, die über die erhältlich ist "Seite „Cloud Manager Policies“ aufgeführt".



2. Wechseln Sie zum Quellkonto, in dem sich die Cloud Manager Instanz befindet, und wählen Sie die IAM-Rolle aus, die mit der Instanz verbunden ist.

   a. Klicken Sie auf **Vertrauensverhältnis > Vertrauensverhältnis bearbeiten**.

   b. Fügen Sie die Aktion „STS:AssumeRole“ und den ARN der Rolle hinzu, 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.

Hinzufügen von AWS Konten zu Cloud Manager

Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie das Konto zu Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

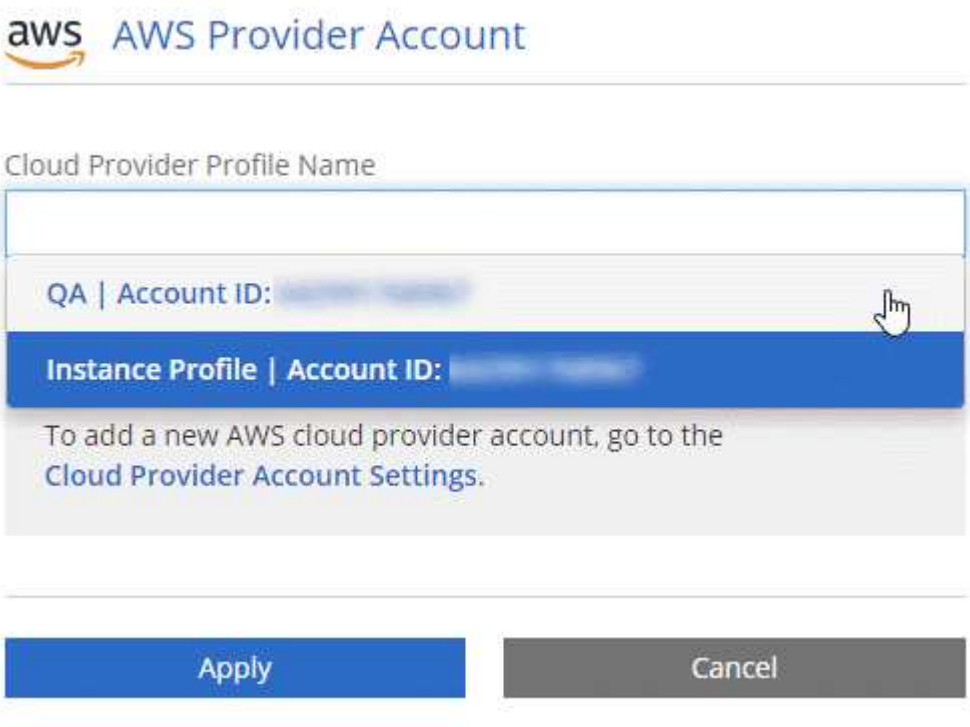
Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Kontoeinstellungen** aus.
2. Klicken Sie auf **Neues Konto hinzufügen** und wählen Sie **AWS**.

3. Sie können entscheiden, ob Sie AWS Schlüssel oder den ARN einer vertrauenswürdigen IAM-Rolle bereitstellen möchten.
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Konto erstellen**.

Ergebnis

Sie können jetzt auf der Seite Details und Anmeldeinformationen zu einem anderen Konto wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Einrichten und Hinzufügen von Azure-Konten zu Cloud Manager

Wenn Sie Cloud Volumes ONTAP in verschiedenen Azure-Konten implementieren möchten, müssen Sie diese Konten die erforderlichen Berechtigungen erteilen und anschließend Details zu den Konten in Cloud Manager einfügen.

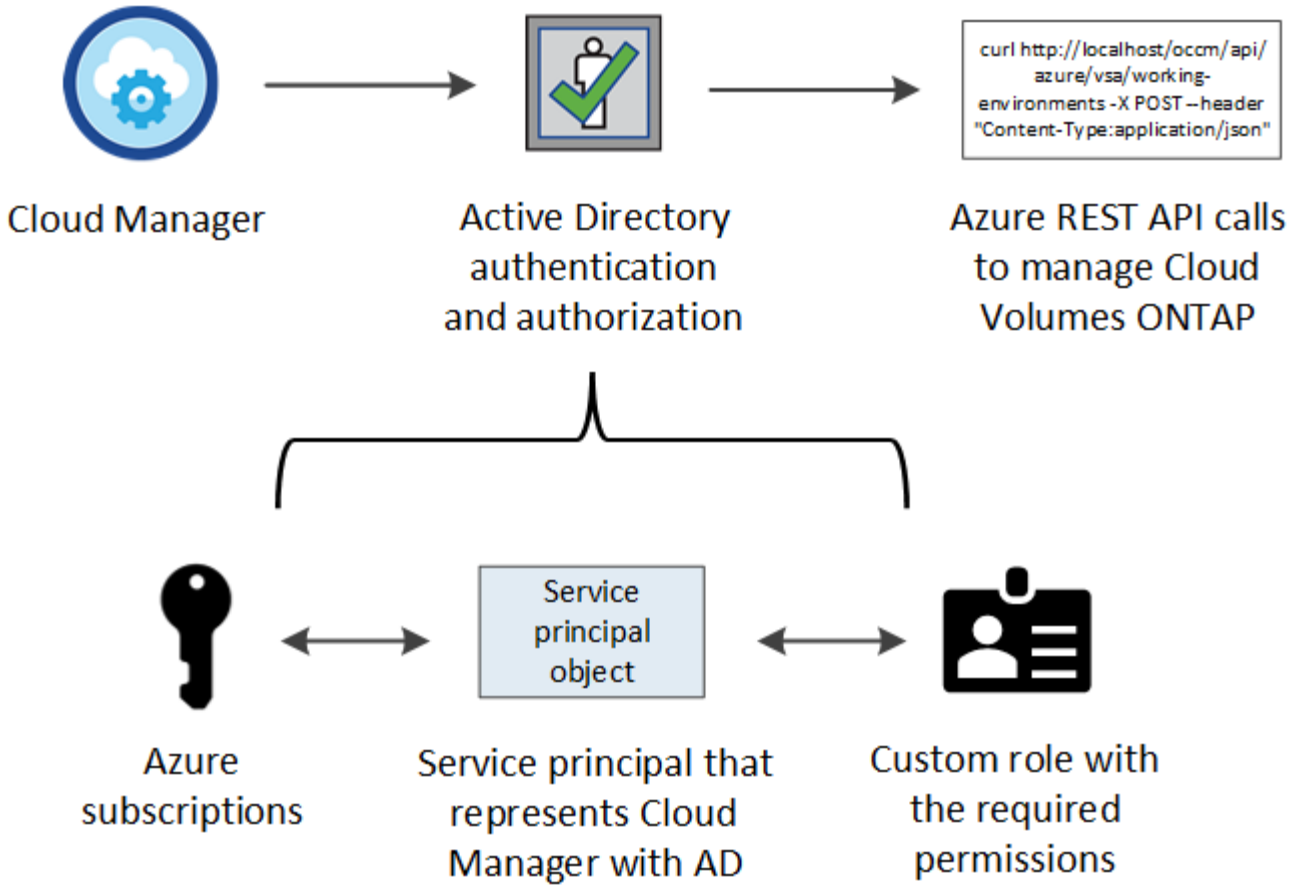
- Azure-Berechtigungen über einen Service-Principal gewähren
- Hinzufügen von Azure-Konten zu Cloud Manager

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.



Die folgenden Schritte verwenden das neue Azure Portal. Wenn Probleme auftreten, sollten Sie das klassische Azure Portal verwenden.

Schritte

1. Erstellen einer benutzerdefinierten Rolle mit den erforderlichen Cloud Manager-Berechtigungen.
2. Erstellen eines Active Directory-Dienstprinzipals.
3. Weisen Sie der Service-Principal die benutzerdefinierte Cloud Manager-Rolle zu.

Erstellen einer benutzerdefinierten Rolle mit den erforderlichen Cloud Manager-Berechtigungen

Eine benutzerdefinierte Rolle ist erforderlich, um Cloud Manager die Berechtigungen zu geben, die er zum Starten und Managen von Cloud Volumes ONTAP in Azure benötigt.

Schritte

1. Laden Sie die herunter "Cloud Manager Azure-Richtlinie".
2. 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"
```

3. 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 Rollendefinition erstellen --Role-Definition C:\Policy_for_Cloud_Manager_Azure_3.6.1.json

Ergebnis

Sie sollten nun eine benutzerdefinierte Rolle namens OnCommand Cloud Manager Operator haben.

Erstellen eines Active Directory-Dienstprinzipals

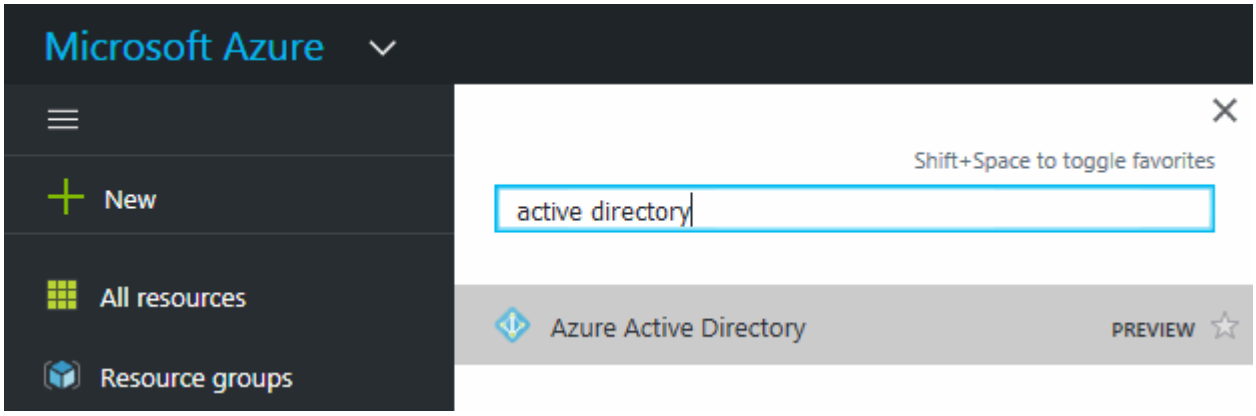
Sie müssen einen Active Directory-Dienstprinzipal erstellen, damit Cloud Manager sich mit Azure Active Directory authentifizieren kann.

Bevor Sie beginnen

Sie müssen über die entsprechenden 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: Erstellen Sie mithilfe eines Portals eine Active Directory-Applikation und einen Service-Principal, die auf Ressourcen zugreifen können".

Schritte

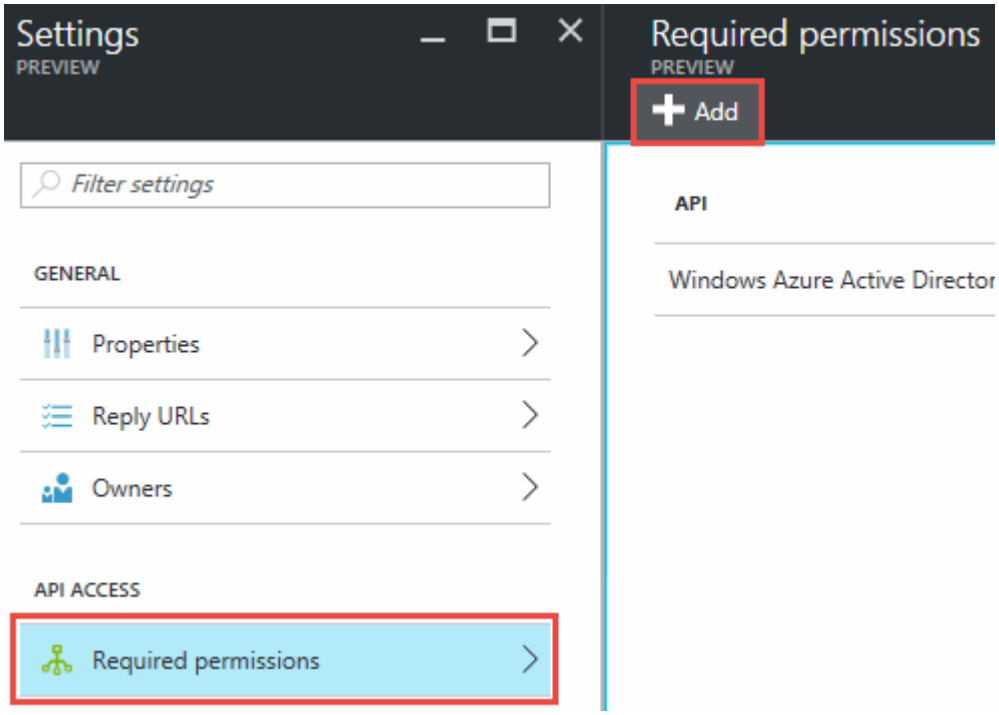
1. Öffnen Sie über das Azure-Portal den **Azure Active Directory**-Service.



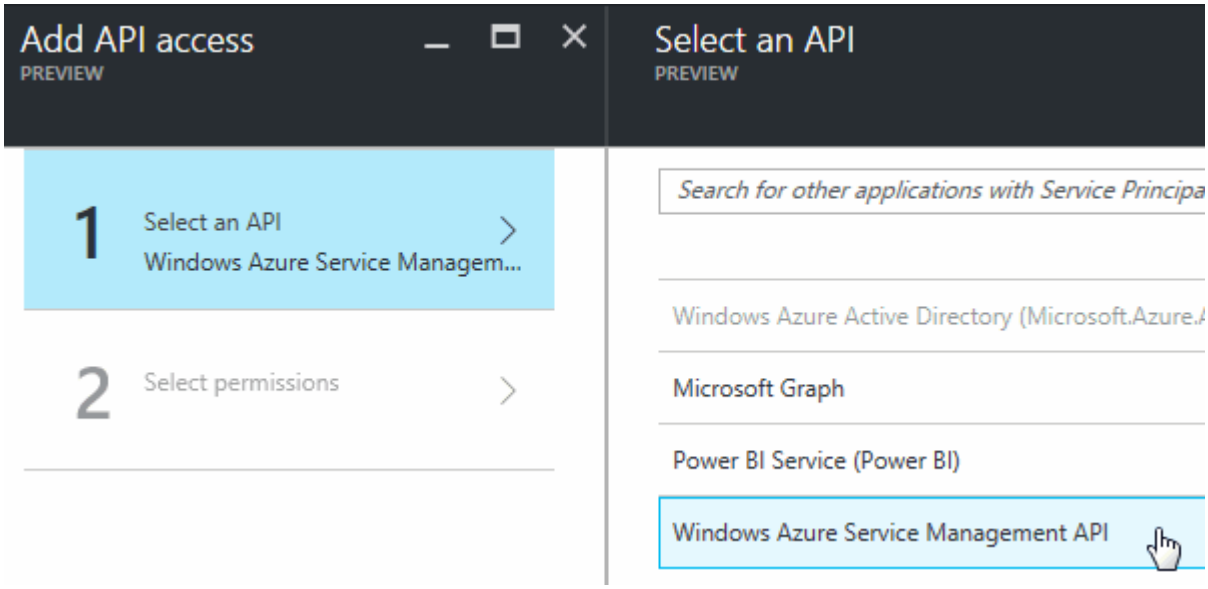
2. Klicken Sie im Menü auf **App-Registrierungen (Legacy)**.
3. Erstellen Sie den Service-Prinzipal:
   a. Klicken Sie auf **Registrierung neuer Anwendungen**.
   b. Geben Sie einen Namen für die Anwendung ein, lassen Sie **Web App / API** ausgewählt, und geben Sie dann eine beliebige URL ein, z. B. http://url
   c. Klicken Sie Auf **Erstellen**.
4. Ändern Sie die Anwendung, um die erforderlichen Berechtigungen hinzuzufügen:

a. Wählen Sie die erstellte Anwendung aus.

b. Klicken Sie unter Einstellungen auf **erforderliche Berechtigungen** und dann auf **Hinzufügen**.



c. Klicken Sie auf **Wählen Sie eine API**, wählen Sie **Windows Azure Service Management API** und klicken Sie dann auf **Auswählen**.



d. Klicken Sie auf **Zugriff auf Azure Service Management als Organisationsbenutzer**, klicken Sie auf **Auswählen** und dann auf **Fertig**.

5. Erstellen Sie einen Schlüssel für den Service Principal:

a. Klicken Sie unter Einstellungen auf **Schlüssel**.

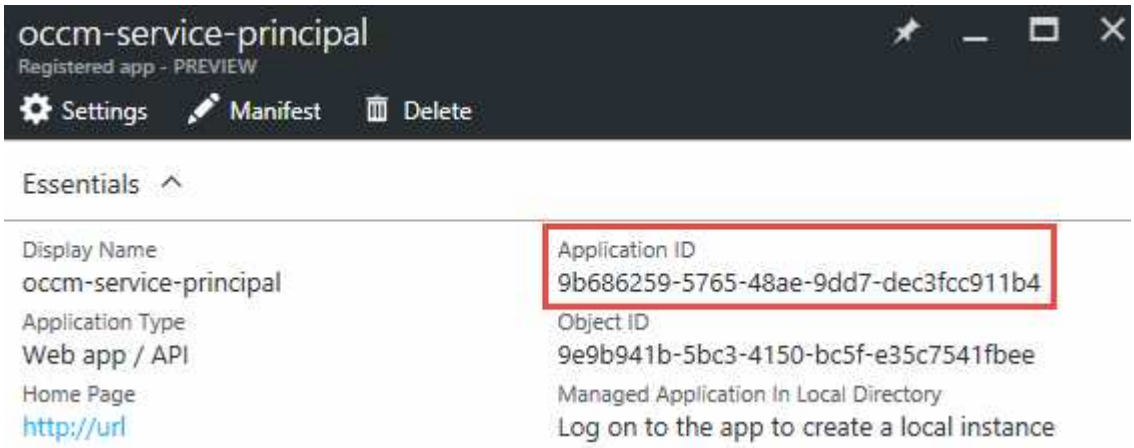
b. Geben Sie eine Beschreibung ein, wählen Sie eine Dauer aus und klicken Sie dann auf **Speichern**.

c. Kopieren Sie den Schlüsselwert.

Wenn Sie Cloud Manager einem Cloud-Provider-Konto hinzufügen, müssen Sie den Hauptwert eingeben.

d. Klicken Sie auf **Eigenschaften** und kopieren Sie dann die Anwendungs-ID für den Service-Principal.

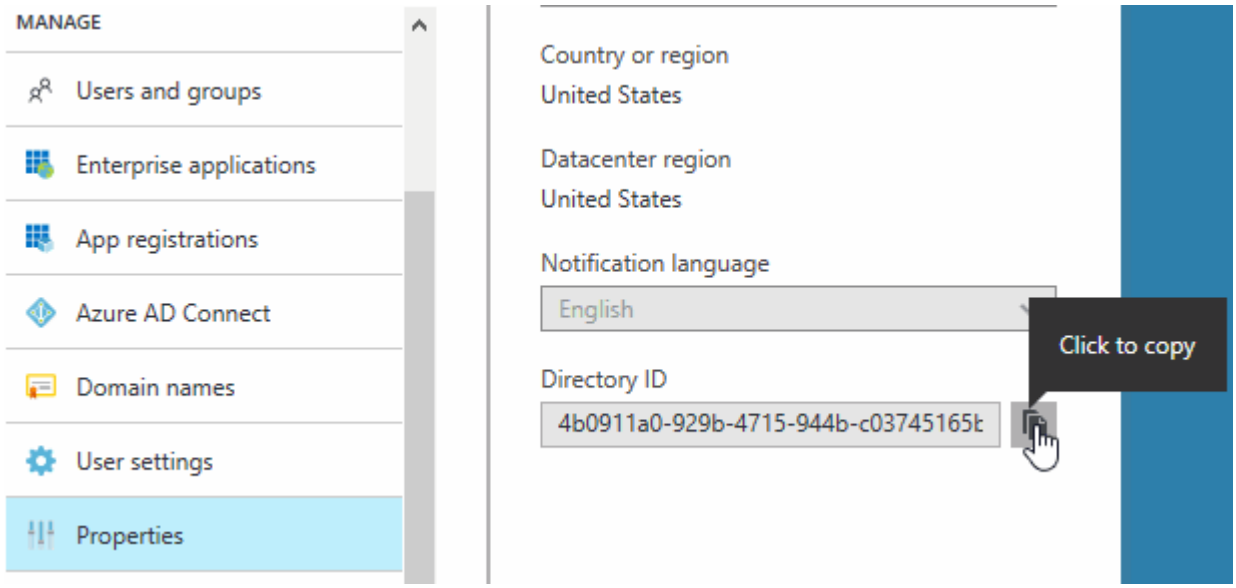
Ähnlich dem Schlüsselwert müssen Sie bei Cloud Manager ein Cloud-Provider-Konto hinzufügen, indem Sie die Anwendungs-ID in Cloud Manager eingeben.



6. Ermitteln Sie die Active Directory-Mandanten-ID für Ihr Unternehmen:

a. Klicken Sie im Menü Active Directory auf **Eigenschaften**.

b. Kopieren Sie die Verzeichnis-ID.



Genau wie die Anwendungs-ID und der Anwendungsschlüssel müssen Sie die Active Directory-Mandanten-ID eingeben, wenn Sie Cloud Manager ein Cloud-Provider-Konto hinzufügen.

Ergebnis

Sie sollten nun über einen Active Directory-Dienstprinzipal verfügen und die Anwendungs-ID, den Anwendungsschlüssel und die Active Directory-Mandanten-ID kopiert haben. Sie müssen diese Informationen in Cloud Manager eingeben, wenn Sie ein Cloud-Provider-Konto hinzufügen.

Zuweisen der Rolle "Cloud Manager Operator" zum Serviceprinzipal

Sie müssen den Dienstprinzipal an ein oder mehrere Azure Subscriptions binden und ihm die Rolle "Cloud Manager Operator" zuweisen, damit Cloud Manager über Berechtigungen in Azure verfügt.

Über diese Aufgabe

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.

Schritte

1. Wählen Sie im Azure-Portal im linken Bereich die Option **Abonnements** aus.
2. Wählen Sie das Abonnement aus.
3. Klicken Sie auf **Access Control (IAM)** und dann auf **Add**.
4. Wählen Sie die Rolle **OnCommand Cloud Manager Operator** aus.
5. Suchen Sie nach dem Namen der Anwendung (Sie können die Anwendung nicht in der Liste finden, indem Sie blättern).
6. Wählen Sie die Anwendung aus, klicken Sie auf **Auswählen** und dann auf **OK**.

Ergebnis

Der Dienstprinzipal für Cloud Manager verfügt jetzt über die erforderlichen Azure Berechtigungen.

Hinzufügen von Azure-Konten zu Cloud Manager

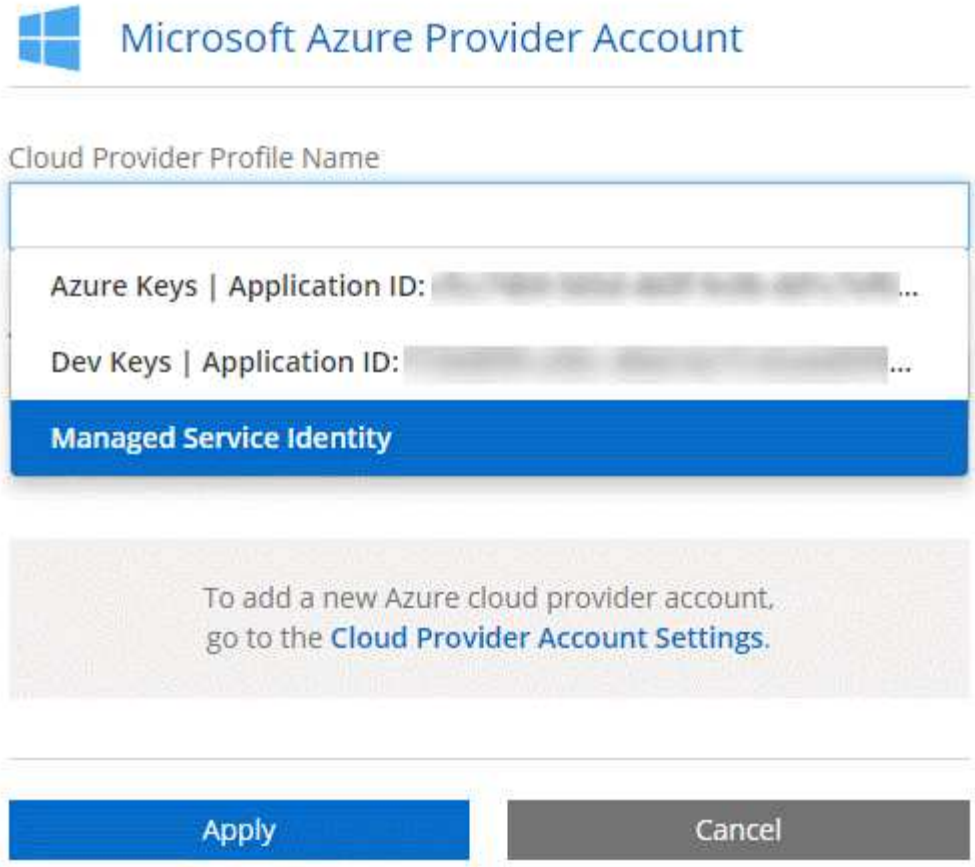
Nachdem Sie ein Azure Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie das Konto zu Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Kontoeinstellungen** aus.
2. Klicken Sie auf **Neues Konto hinzufügen** und wählen Sie **Microsoft Azure**.
3. Geben Sie Informationen zum Azure Active Directory Service Principal ein, der die erforderlichen Berechtigungen erteilt.
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Konto erstellen**.

Ergebnis

Sie können jetzt auf der Seite Details und Anmeldeinformationen zu einem anderen Konto wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Verknüpfen weiterer Azure-Abonnements mit einer gemanagten Identität

Mit Cloud Manager können Sie das Azure Konto und das 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 die erste "Konto eines Cloud-Providers" Wenn Sie Cloud Manager über NetApp Cloud Central implementieren. Bei der Implementierung von Cloud Manager erstellte Cloud Central die Rolle "OnCommand Cloud Manager Operator" und wies sie der virtuellen Cloud Manager-Maschine zu.

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-Systeme 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 **OnCommand Cloud Manager Operator** aus.

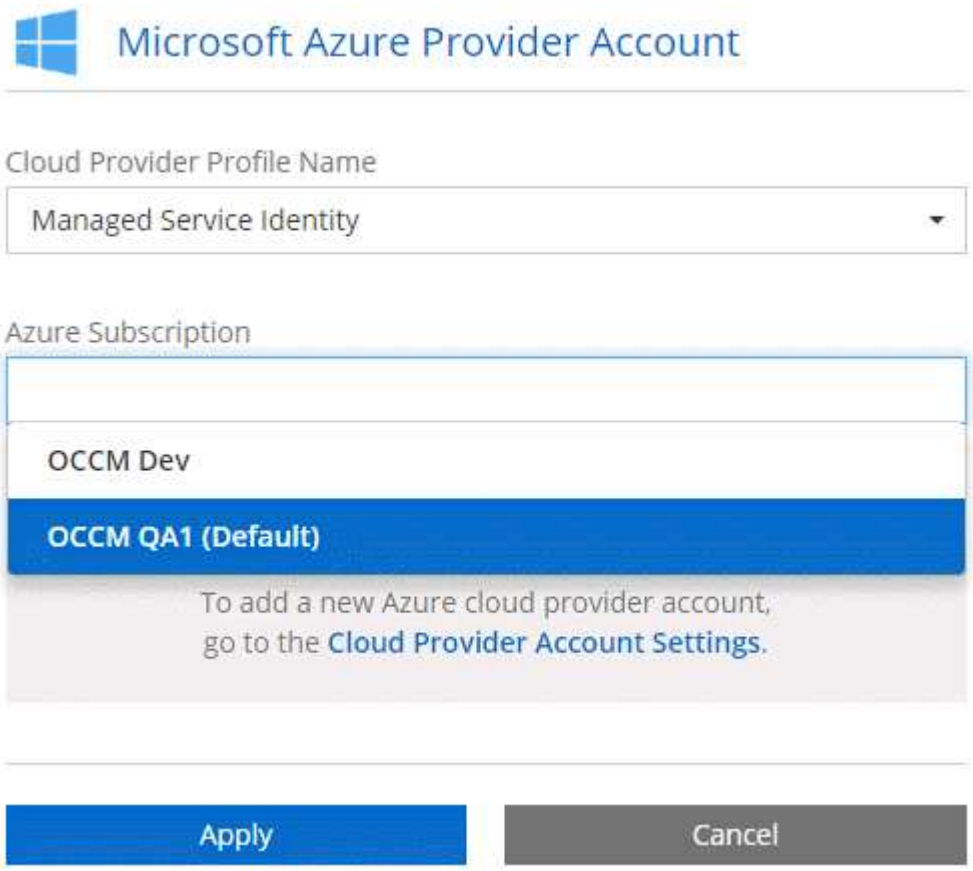
      OnCommand Cloud Manager Operator ist der im angegebene Standardname "Cloud Manager-Richtlinie". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

- Weisen Sie einer **virtuellen Maschine** Zugriff zu.
- Wählen Sie das Abonnement aus, in dem die virtuelle Cloud Manager-Maschine erstellt wurde.
- Wählen Sie die virtuelle Cloud Manager-Maschine 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.



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*

Schritte

1. Wenn Sie noch keinen NetApp Support Site Account haben, "Eine anmeldung".

2. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task und wählen Sie dann **Kontoeinstellungen** aus.
3. Klicken Sie auf **Neues Konto hinzufügen** und wählen Sie **NetApp Support Site** aus.
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"

Installieren 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.

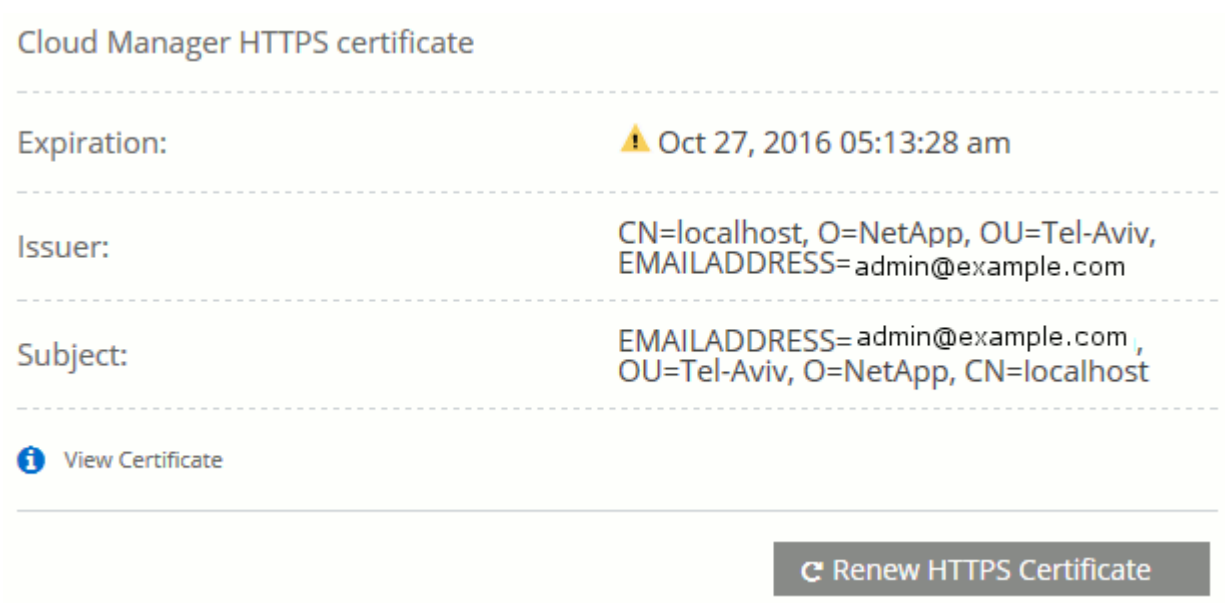
Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf die Dropdown-Liste Task, und wählen Sie dann **HTTPS-Setup** aus.
2. Installieren Sie auf der Seite HTTPS Setup ein Zertifikat, indem Sie eine Zertifikatsignierungsanforderung (CSR) erstellen oder Ihr eigenes, von der Zertifizierungsstelle signiertes Zertifikat installieren:

Option	Beschreibung
Erstellen Sie eine CSR	a. Geben Sie den Hostnamen oder DNS des Cloud Manager-Hosts (dessen allgemeiner Name) ein, und klicken Sie dann auf **CSR generieren**. 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:



Benutzer und Mandanten einrichten

Mit Cloud Manager können Sie Cloud Manager um weitere Cloud Central Benutzer erweitern und Arbeitsumgebungen durch die Verwendung von Mandanten isolieren.

Hinzufügen von Benutzern zu Cloud Manager

Wenn zusätzliche Benutzer Ihr Cloud Manager-System verwenden müssen, müssen sie sich bei NetApp Cloud Central registrieren. Sie können die Benutzer dann zu Cloud Manager hinzufügen.

Schritte

1. Wenn der Benutzer noch kein Konto in NetApp Cloud Central hat, senden Sie ihm einen Link zu Ihrem Cloud Manager-System, und lassen Sie ihn sich registrieren.

   Warten Sie, bis der Benutzer bestätigt, dass er sich für ein Konto angemeldet hat.

2. Klicken Sie in Cloud Manager auf das Benutzersymbol und dann auf **Benutzer anzeigen**.
3. Klicken Sie Auf **Neuer Benutzer**.
4. Geben Sie die dem Benutzerkonto zugeordnete E-Mail-Adresse ein, wählen Sie eine Rolle aus und klicken Sie auf **Hinzufügen**.

Was kommt als Nächstes?

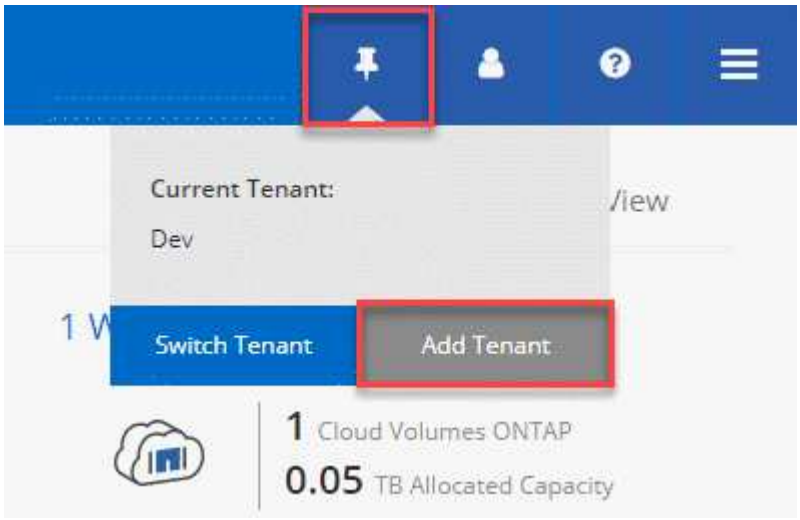
Informieren Sie den Benutzer, dass er sich jetzt beim Cloud Manager-System anmelden kann.

Erstellen von Mandanten

Mit Mandanten lassen sich Arbeitsumgebungen in separate Gruppen isolieren. Sie erstellen eine oder mehrere Arbeitsumgebungen innerhalb eines Mandanten. "Erfahren Sie mehr über Mandanten".

Schritte

1. Klicken Sie auf das Mietersymbol und dann auf **Mieter hinzufügen**.



2. Geben Sie ggf. einen Namen, eine Beschreibung und eine Kostenstelle ein.
3. Klicken Sie Auf **Speichern**.

Was kommt als Nächstes?

Sie können jetzt zu diesem neuen Mandanten wechseln und diesem Mandanten Mandantenadministratoren und Arbeitsumgebungsadministratoren hinzufügen.

Einrichten des AWS KMS

Wenn Sie die Amazon Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, müssen Sie den AWS KMS (Key Management Service) einrichten.

Schritte

1. Stellen Sie sicher, dass ein aktiver Kundenstammschlüssel (CMK) vorhanden ist.

   Bei CMK kann es sich um ein von AWS gemanagtes CMK oder um ein vom Kunden gemanagtes CMK handeln. Sie kann sich im selben AWS Konto wie Cloud Manager und Cloud Volumes ONTAP oder in einem anderen AWS Konto befinden.

   "AWS Dokumentation: Customer Master Keys (CMKs)"

2. Ändern Sie die Schlüsselrichtlinie für jedes CMK, indem Sie die IAM-Rolle hinzufügen, die Berechtigungen für Cloud Manager als *Key Benutzer* bereitstellt.

   Durch Hinzufügen der IAM-Rolle als Schlüsselbenutzer erhalten Cloud Manager Berechtigungen zur Verwendung des CMK mit Cloud Volumes ONTAP.

   "AWS Dokumentation: Schlüssel bearbeiten"

3. Wenn sich das CMK in einem anderen AWS Konto befindet, führen Sie folgende Schritte aus:

   a. Wechseln Sie von dem Konto, in dem sich der CMK befindet, zur KMS-Konsole.

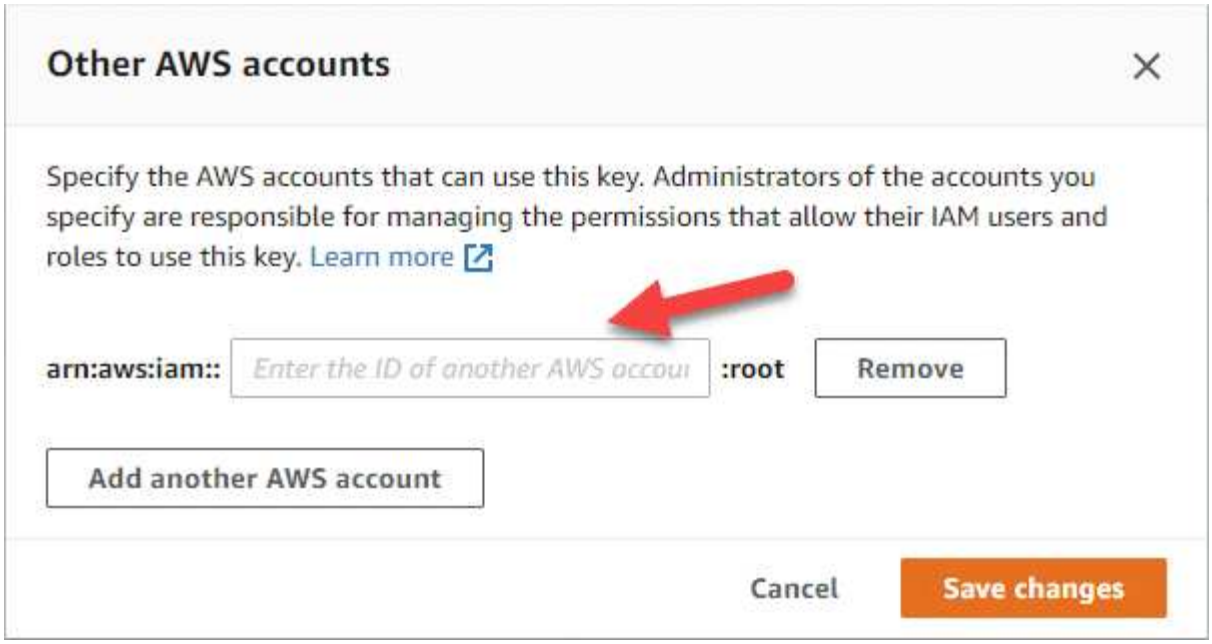
   b. Wählen Sie die Taste.

   c. Kopieren Sie im Fenster **Allgemeine Konfiguration** den ARN des Schlüssels.

      Wenn Sie das Cloud Volumes ONTAP-System erstellen, müssen Sie dem Cloud Manager ARN zur Verfügung stellen.

   d. Fügen Sie im Fensterbereich **andere AWS-Konten** das AWS-Konto hinzu, das Cloud Manager mit Berechtigungen versorgt.

      In den meisten Fällen ist dies der Account, in dem sich Cloud Manager befindet. Falls Cloud Manager nicht in AWS installiert wurde, stellen Sie als Konto die AWS Zugriffsschlüssel für Cloud Manager bereit.



e. Wechseln Sie jetzt zum AWS Konto, das Cloud Manager über Berechtigungen verfügt, und öffnen Sie die IAM-Konsole.

f. Erstellen Sie eine IAM-Richtlinie, die die unten aufgeführten Berechtigungen enthält.

g. Hängen Sie die Richtlinie an die IAM-Rolle oder den IAM-Benutzer an, der Berechtigungen für Cloud Manager bereitstellt.

   Die folgende Richtlinie bietet die Berechtigungen, die Cloud Manager zur Verwendung des CMK aus dem externen AWS-Konto benötigt. Denken Sie daran, die Region und die Account-ID in den Abschnitten „Ressource“ zu ändern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Weitere Details zu diesem Prozess finden Sie unter "AWS Dokumentation: Zugriff auf einen CMK für externe AWS Konten".

Netzwerkanforderungen

Netzwerkanforderungen für Cloud Manager

Sie müssen Ihr Netzwerk so einrichten, dass Cloud Manager Cloud Volumes ONTAP Systeme in AWS oder in Microsoft Azure bereitstellen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.

Wenn Ihr Netzwerk einen Proxyserver für die gesamte Kommunikation mit dem Internet verwendet, fordert Cloud Manager Sie auf, den Proxy während der Einrichtung anzugeben. Sie können den Proxyserver auch auf der Seite Einstellungen angeben. Siehe "Konfigurieren von Cloud Manager für die Verwendung eines Proxyservers".

Verbindung zu Zielnetzwerken

Cloud Manager erfordert eine Netzwerkverbindung zu den AWS VPCs und Azure VNets, in denen Sie Cloud Volumes ONTAP bereitstellen möchten.

Wenn Sie beispielsweise Cloud Manager in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zum AWS VPC oder Azure VNet einrichten, in dem Sie Cloud Volumes ONTAP starten.

Outbound-Internetzugang

Cloud Manager erfordert ausgehenden Internetzugang, um Cloud Volumes ONTAP bereitzustellen und zu managen. Outbound-Internetzugang ist auch erforderlich, wenn Sie über Ihren Webbrowser auf Cloud Manager zugreifen und das Cloud Manager-Installationsprogramm auf einem Linux-Host ausführen.

In den folgenden Abschnitten werden die spezifischen Endpunkte beschrieben.

Outbound-Internetzugang zum Management von Cloud Volumes ONTAP in AWS

Cloud Manager erfordert ausgehenden Internetzugang, um bei der Implementierung und dem Management von Cloud Volumes ONTAP in AWS die folgenden Endpunkte zu kontaktieren:

Endpunkte	Zweck
AWS-Services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) Der genaue Endpunkt hängt von der Region ab, in der Sie Cloud Volumes ONTAP implementieren. "Weitere Informationen finden Sie in der AWS-Dokumentation."	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in AWS.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.

Endpunkte	Zweck
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://cloudmanager.cloud.netapp.com	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Kommunikation mit NetApp zur Lizenzierung und Support-Registrierung
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Outbound-Internetzugang zum Management von Cloud Volumes ONTAP in Azure

Cloud Manager erfordert ausgehenden Internetzugang, um bei der Bereitstellung und Verwaltung von Cloud Volumes ONTAP in Microsoft Azure folgende Endpunkte zu kontaktieren:

Endpunkte	Zweck
https://management.azure.com https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den meisten Azure Regionen.
https://management.microsoftazure.de https://login.microsoftonline.de	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure Germany Regionen.

Endpunkte	Zweck
https://management.usgovcloudapi.net https://login.microsoftonline.com	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure US Gov Regionen.
https://api.services.cloud.netapp.com:443	API-Anfragen an NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
https://kinesis.us-east-1.amazonaws.com	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
https://netapp-cloud-account.auth0.com	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
https://mysupport.netapp.com	Kommunikation mit NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Kommunikation mit NetApp zur Lizenzierung und Support-Registrierung
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org An Standorten von Drittanbietern können Änderungen vorgenommen werden.	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

Outbound-Internetzugang über Ihren Webbrowser

Benutzer müssen über einen Webbrowser auf Cloud Manager zugreifen. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Cloud Manager-Host	Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden. Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden: • Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben • Eine öffentliche IP funktioniert in jedem Netzwerkszenario In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.
https://widget.intercom.io	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

Outbound-Internetzugang zur Installation von Cloud Manager auf einem Linux-Host

Das Cloud Manager-Installationsprogramm muss während des Installationsvorgangs auf die folgenden URLs zugreifen:

- 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

Ports und Sicherheitsgruppen

- Wenn Sie Cloud Manager über Cloud Central oder über Marktplatz-Images bereitstellen, lesen Sie Folgendes:
  - "Sicherheitsgruppenregeln für Cloud Manager in AWS"
  - "Sicherheitsgruppenregeln für Cloud Manager in Azure"
- Wenn Sie Cloud Manager auf einem vorhandenen Linux-Host installieren, lesen Sie "Anforderungen an den Cloud Manager Host".

Netzwerkanforderungen für Cloud Volumes ONTAP in AWS

Richten Sie das AWS Netzwerk ein, um Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren zu können.

Suchen Sie nach der Liste der Endpunkte, auf die Cloud Manager Zugriff benötigt? Sie werden jetzt an einem einzigen Ort gepflegt. "Details finden Sie hier".

Allgemeine AWS Netzwerkanforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in AWS erfüllt sein.

Outbound-Internetzugang für Cloud Volumes ONTAP Nodes

Cloud Volumes ONTAP Nodes erfordern ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen AWS HTTP-/HTTPS-Datenverkehr an die folgenden Endpunkte ermöglichen, damit Cloud Volumes ONTAP AutoSupport-Meldungen senden kann:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

  Wenn Sie über eine NAT-Instanz verfügen, müssen Sie eine eingehende Sicherheitsgruppenregel definieren, die HTTPS-Datenverkehr vom privaten Subnetz zum Internet zulässt.

Outbound-Internetzugang für den HA Mediator

Die HA-Mediatorinstanz muss über eine ausgehende Verbindung zum AWS EC2-Service verfügen, damit sie beim Storage-Failover unterstützt werden kann. Um die Verbindung bereitzustellen, können Sie eine öffentliche IP-Adresse hinzufügen, einen Proxyserver angeben oder eine manuelle Option verwenden.

Die manuelle Option kann ein NAT-Gateway oder ein VPC-Endpunkt der Schnittstelle vom Ziel-Subnetz zum AWS EC2-Dienst sein. Details zu VPC-Endpunkten finden Sie unter "AWS Dokumentation: Interface VPC Endpunkte (AWS PrivateLink)".

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da Cloud Manager dies für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie "Regeln für Sicherheitsgruppen".

Verbindung von Cloud Volumes ONTAP zu AWS S3 für Data Tiering

Wenn Sie EBS als Performance-Tier und AWS S3 als Kapazitäts-Tier verwenden möchten, müssen Sie sicherstellen, dass Cloud Volumes ONTAP eine Verbindung zu S3 hat. Die beste Möglichkeit, diese Verbindung bereitzustellen, besteht darin, einen VPC-Endpunkt für den S3-Dienst zu erstellen. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Erstellen eines Gateway-Endpunkts".

Wenn Sie den VPC-Endpunkt erstellen, wählen Sie die Region, den VPC und die Routing-Tabelle aus, die der Cloud Volumes ONTAP Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Volumes ONTAP keine Verbindung zum S3-Service herstellen.

Informationen zu Problemen finden Sie unter "AWS Support Knowledge Center: Warum kann ich mich nicht über einen Gateway VPC Endpunkt mit einem S3-Bucket verbinden?"

Verbindungen zu ONTAP Systemen in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP System in AWS und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie eine VPN-Verbindung zwischen AWS VPC und dem anderen Netzwerk haben, z. B. ein Azure VNet oder Ihr Unternehmensnetzwerk. Anweisungen hierzu finden Sie

unter "AWS Dokumentation: Einrichten einer AWS VPN-Verbindung".

DNS und Active Directory für CIFS

Wenn Sie CIFS-Storage bereitstellen möchten, müssen Sie DNS und Active Directory in AWS einrichten oder Ihre lokale Einrichtung auf AWS erweitern.

Der DNS-Server muss Namensauflösungsdienste für die Active Directory-Umgebung bereitstellen. Sie können DHCP-Optionssätze so konfigurieren, dass sie den Standard-EC2-DNS-Server verwenden, der nicht der von der Active Directory-Umgebung verwendete DNS-Server sein darf.

Anweisungen finden Sie unter "AWS Dokumentation: Active Directory Domain Services in der AWS Cloud Quick Start Reference Deployment".

AWS Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZS

Zusätzliche AWS Netzwerkanforderungen gelten für Cloud Volumes ONTAP HA-Konfigurationen, die mehrere Verfügbarkeitszonen (AZS) verwenden. Sie sollten diese Anforderungen prüfen, bevor Sie ein HA-Paar starten, da Sie die Netzwerkdetails in Cloud Manager eingeben müssen.

Informationen zur Funktionsweise von HA-Paaren finden Sie unter "Hochverfügbarkeitspaare".

Verfügbarkeitszonen

Dieses HA-Bereitstellungsmodell verwendet mehrere AZS, um eine hohe Verfügbarkeit Ihrer Daten zu gewährleisten. Sie sollten für jede Cloud Volumes ONTAP Instanz und die Mediatorinstanz eine dedizierte AZ verwenden, die einen Kommunikationskanal zwischen dem HA-Paar bereitstellt.

Fließende IP-Adressen für NAS- und Cluster-/SVM-Management

HA-Konfigurationen in mehreren Verfügbarkeitszonen verwenden fließende IP-Adressen, die bei einem Ausfall zwischen Nodes migriert werden. Außerhalb der VPC ist nicht nativ zugänglich. Es sei denn, Sie können darauf zugreifen "AWS Transit Gateway einrichten".

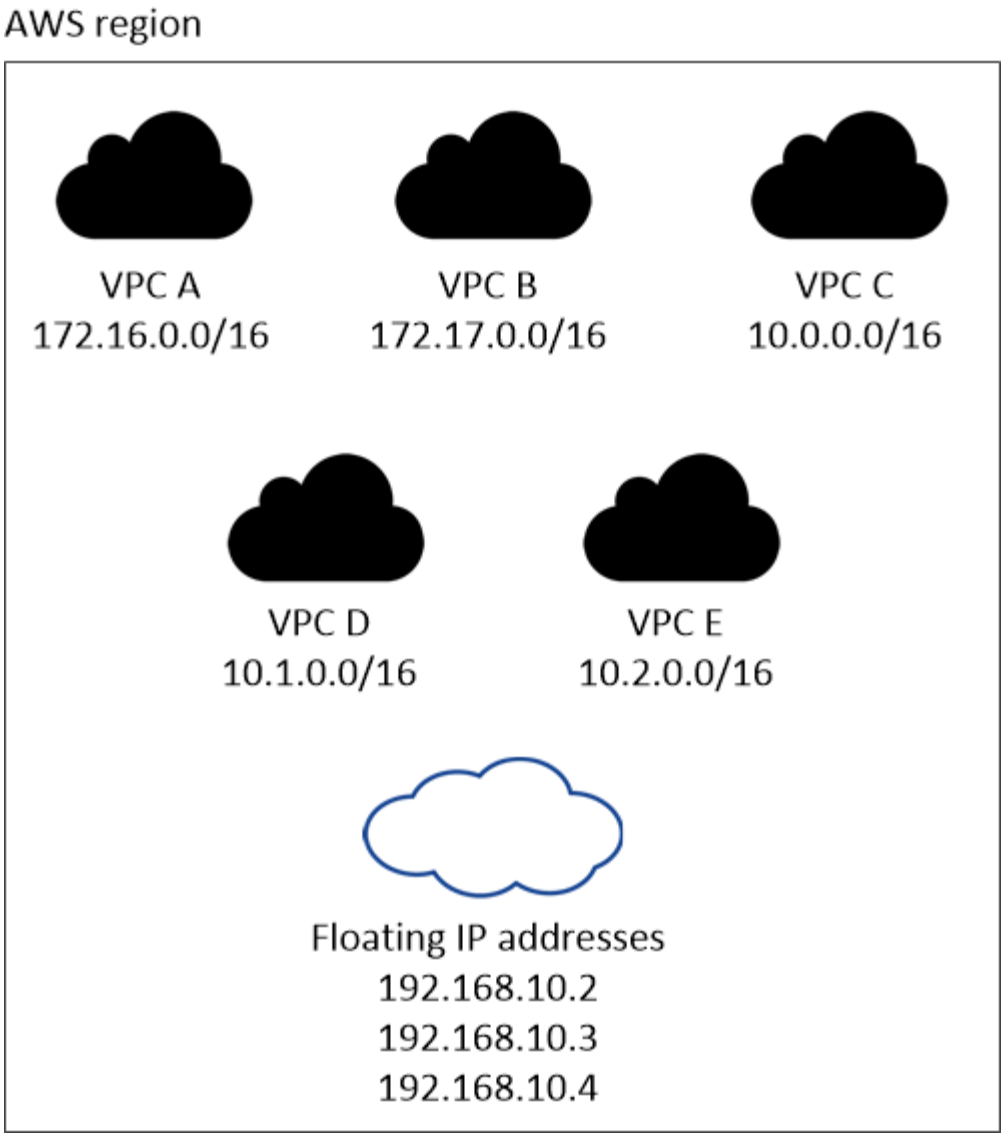
Eine Floating-IP-Adresse ist für das Cluster-Management, eine für NFS/CIFS-Daten auf Node 1 und eine für NFS/CIFS-Daten auf Node 2. Eine vierte Floating IP-Adresse für SVM-Management ist optional.

> Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist eine unverankerte IP-Adresse für die SVM-Management-LIF erforderlich. Wenn Sie die IP-Adresse nicht angeben, wenn Sie das System implementieren, können Sie später die LIF erstellen. Weitere Informationen finden Sie unter "Einrichten von Cloud Volumes ONTAP".

Sie müssen die unverankerten IP-Adressen in Cloud Manager eingeben, wenn Sie eine Cloud Volumes ONTAP HA-Arbeitsumgebung erstellen. Cloud Manager weist dem HA-Paar die IP-Adressen zu, wenn es das System startet.

Die fließenden IP-Adressen müssen sich für alle VPCs in der AWS Region, in der Sie die HA-Konfiguration implementieren, außerhalb der CIDR-Blöcke befinden. Stellen Sie sich die fließenden IP-Adressen als logisches Subnetz vor, das sich außerhalb der VPCs in Ihrer Region befindet.

Das folgende Beispiel zeigt die Beziehung zwischen Floating-IP-Adressen und den VPCs in einer AWS-Region. Während sich die fließenden IP-Adressen für alle VPCs außerhalb der CIDR-Blöcke befinden, sind sie über Routing-Tabellen in Subnetze routingfähig.



Cloud Manager erstellt automatisch statische IP-Adressen für den iSCSI-Zugriff und für den NAS-Zugriff von Clients außerhalb des VPC. Für diese Art von IP-Adressen müssen Sie keine Anforderungen erfüllen.

Transit-Gateway zur Aktivierung des Floating IP-Zugriffs von außerhalb der VPC

"AWS Transit Gateway einrichten" Um den Zugriff auf die unverankerten IP-Adressen eines HA-Paars von außerhalb der VPC zu ermöglichen, in der sich das HA-Paar befindet.

Routentabellen

Nachdem Sie in Cloud Manager die unverankerten IP-Adressen angegeben haben, müssen Sie die Routing-Tabellen auswählen, die Routen zu den Floating IP-Adressen enthalten sollen. Dies ermöglicht den Client-Zugriff auf das HA-Paar.

Wenn Sie nur eine Routing-Tabelle für die Subnetze in Ihrem VPC (der Hauptroutentabelle) haben, fügt Cloud Manager dieser Routing-Tabelle automatisch die unverankerten IP-Adressen hinzu. Wenn Sie mehr als eine Routing-Tabelle haben, ist es sehr wichtig, beim Starten des HA-Paars die richtigen Routing-Tabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf Cloud Volumes ONTAP.

Sie können beispielsweise zwei Subnetze haben, die mit verschiedenen Routing-Tabellen verknüpft sind. Wenn Sie Routing-Tabelle A auswählen, jedoch nicht Route-Tabelle B, können Clients in der mit Routing-Tabelle A verknüpften Subnetz auf das HA-Paar zugreifen, die Clients im Subnetz der Routing-Tabelle B können jedoch nicht.

Weitere Informationen zu Routingtabellen finden Sie unter "AWS Documentation: Routingtabellen".

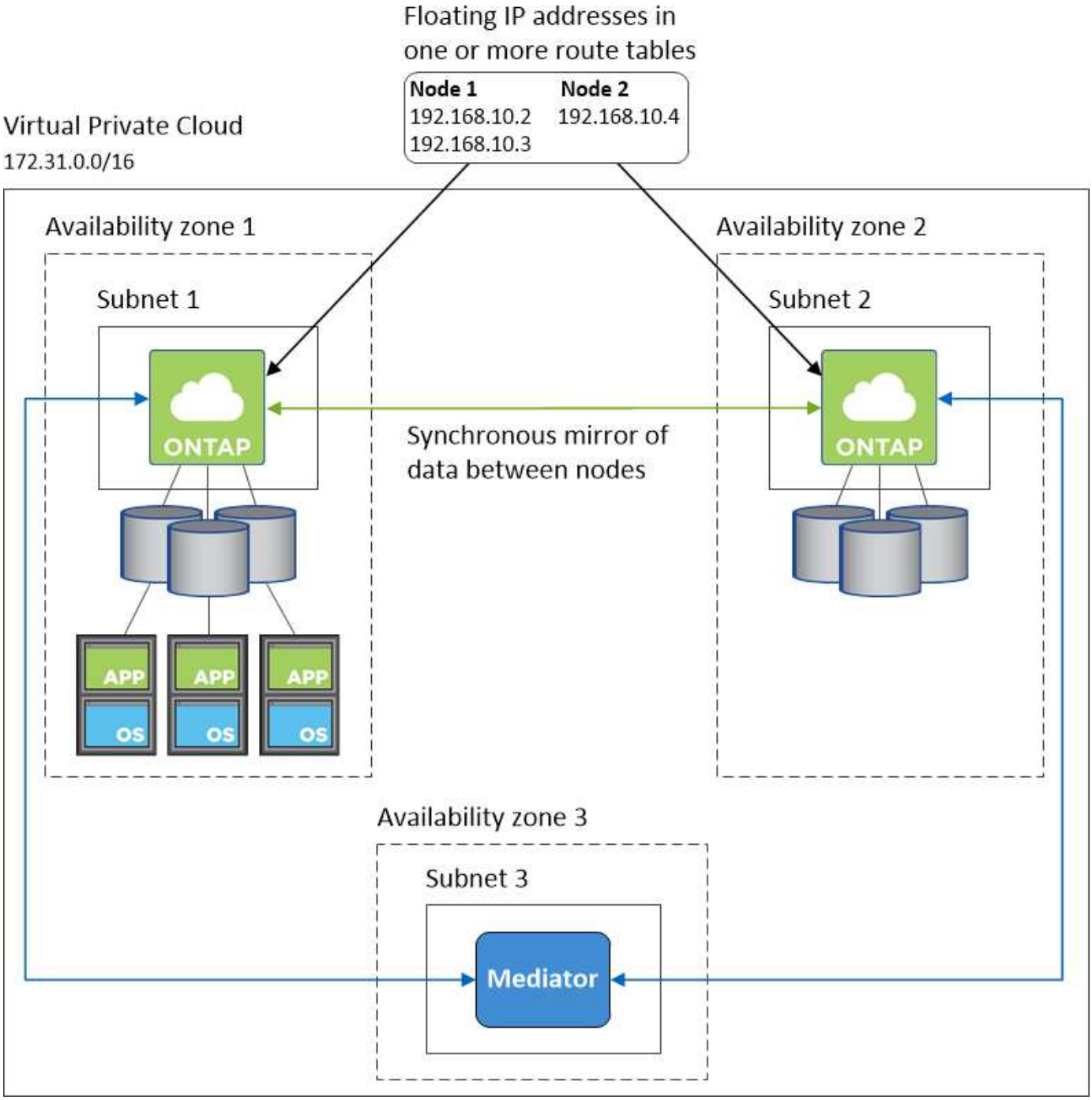
Anbindung an NetApp Management Tools

Für den Einsatz von NetApp Management Tools mit HA-Konfigurationen in mehreren Verfügbarkeitszonen stehen zwei Verbindungsoptionen zur Verfügung:

1. Die NetApp Management Tools in einer anderen VPC und implementieren "AWS Transit Gateway einrichten". Das Gateway ermöglicht den Zugriff auf die unverankerte IP-Adresse für die Cluster-Managementoberfläche von außerhalb der VPC aus.
2. Implementieren Sie die NetApp Management-Tools in derselben VPC mit einer ähnlichen Routing-Konfiguration wie NAS-Clients.

Beispielkonfiguration

Die folgende Abbildung zeigt eine optimale HA-Konfiguration in AWS, die als Aktiv/Passiv-Konfiguration betrieben wird:



Beispiele für VPC-Konfigurationen

Um besser zu verstehen, wie Sie Cloud Manager und Cloud Volumes ONTAP in AWS implementieren können, sollten Sie sich die gängigsten VPC-Konfigurationen ansehen.

- Ein VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gerät
- Ein VPC mit einem privaten Subnetz und einer VPN-Verbindung zu Ihrem Netzwerk

Ein VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gerät

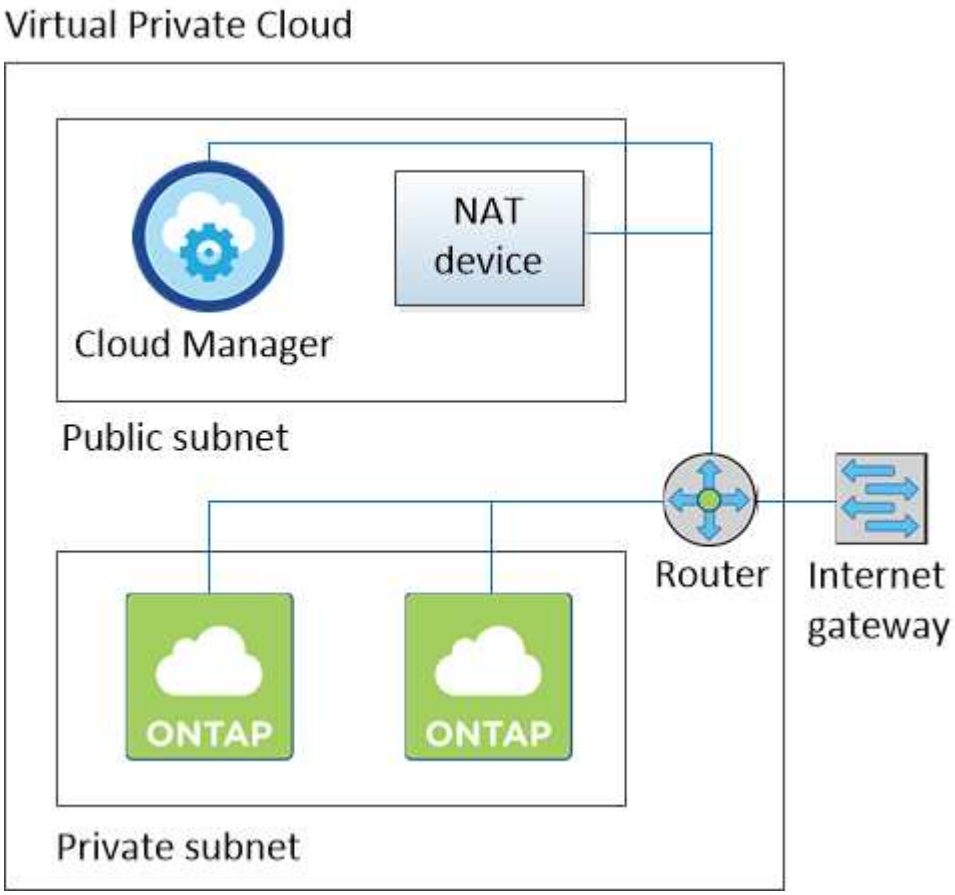
Diese VPC-Konfiguration umfasst öffentliche und private Subnetze, ein Internet-Gateway, das den VPC mit dem Internet verbindet, und ein NAT-Gateway oder eine NAT-Instanz im öffentlichen Subnetz, die

ausgehenden Internetverkehr vom privaten Subnetz aus ermöglicht. In dieser Konfiguration können Sie Cloud Manager in einem öffentlichen oder privaten Subnetz ausführen. Das öffentliche Subnetz wird jedoch empfohlen, da es den Zugriff von Hosts außerhalb des VPC ermöglicht. Sie können dann Cloud Volumes ONTAP Instanzen im privaten Subnetz starten.

Anstelle eines NAT-Geräts können Sie einen HTTP-Proxy verwenden, um Internetverbindungen bereitzustellen.

Weitere Informationen zu diesem Szenario finden Sie unter "AWS Dokumentation: Szenario 2: VPC mit öffentlichen und privaten Subnetzen (NAT)".

Die folgende Grafik zeigt Cloud Manager, der in einem öffentlichen Subnetz und in Einzelknoten-Systemen in einem privaten Subnetz ausgeführt wird:



Ein VPC mit einem privaten Subnetz und einer VPN-Verbindung zu Ihrem Netzwerk

Bei dieser VPC-Konfiguration handelt es sich um eine Hybrid Cloud-Konfiguration, bei der Cloud Volumes ONTAP zu einer Erweiterung Ihrer privaten Umgebung wird. Die Konfiguration umfasst ein privates Subnetz und ein virtuelles privates Gateway mit einer VPN-Verbindung zu Ihrem Netzwerk. Durch das Routing über den VPN-Tunnel können EC2-Instanzen über das Netzwerk und Firewalls auf das Internet zugreifen. Sie können Cloud Manager im privaten Subnetz oder in Ihrem Datacenter ausführen. Sie starten dann Cloud Volumes ONTAP im privaten Subnetz.

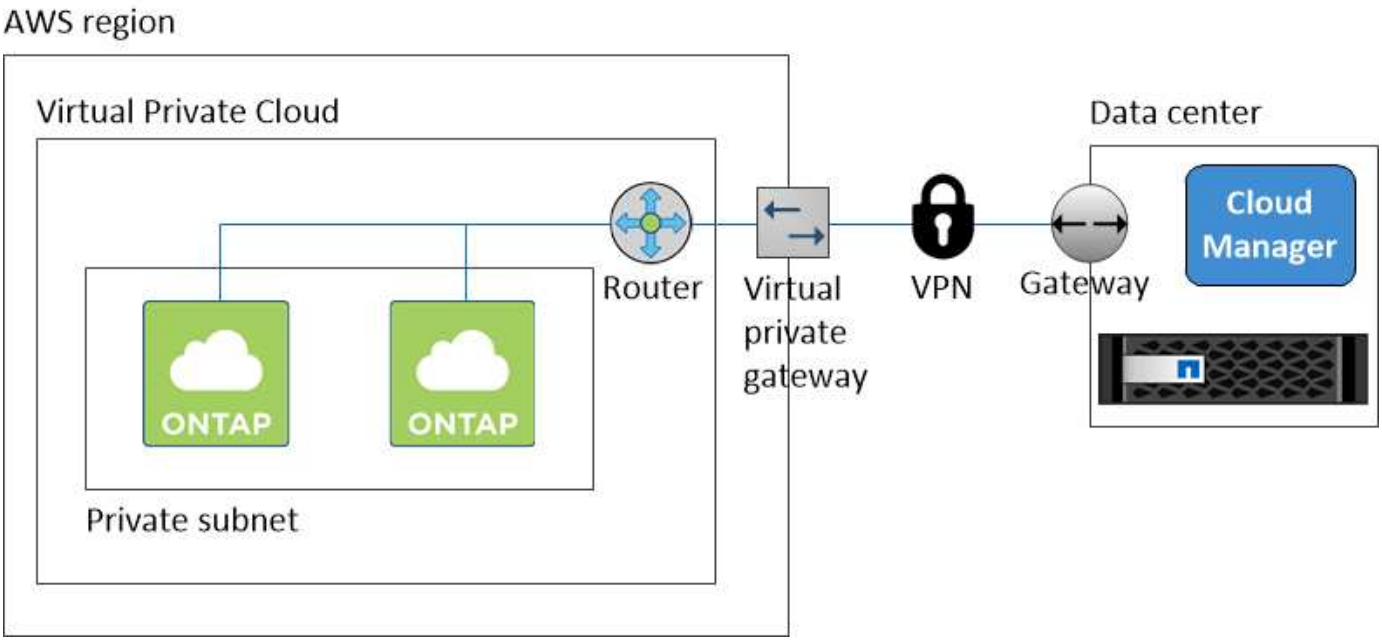
Sie können in dieser Konfiguration auch einen Proxyserver verwenden, um den Internetzugang zu ermöglichen. Der Proxy-Server kann sich in Ihrem Datacenter oder in AWS befinden.

Wenn Sie Daten zwischen FAS Systemen in Ihrem Datacenter und Cloud Volumes ONTAP Systemen in AWS

replizieren möchten, sollten Sie eine VPN-Verbindung verwenden, damit die Verbindung sicher ist.

Weitere Informationen zu diesem Szenario finden Sie unter "AWS Dokumentation: Szenario 4: VPC mit privatem Subnetz und von AWS gemanagtem VPN-Zugriff".

Die folgende Grafik zeigt Cloud Manager, der in Ihrem Datacenter und in Einzelknotensystemen in einem privaten Subnetz ausgeführt wird:



Einrichten eines AWS-Transit-Gateways für HA-Paare in mehreren Verfügbarkeitszonen

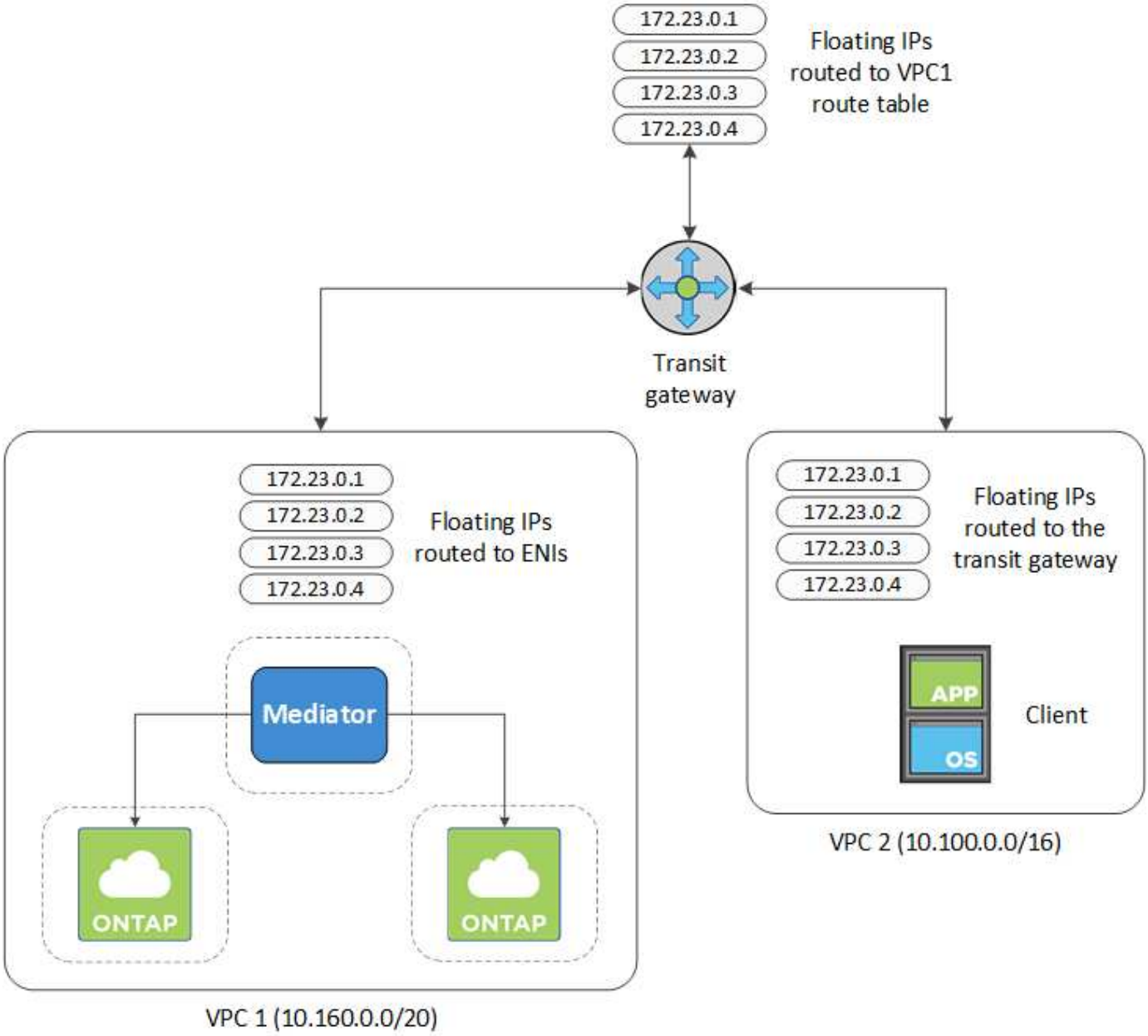
Einrichten eines AWS-Transit-Gateways für den Zugriff auf die unverankerten IP-Adressen eines HA-Paars von außerhalb der VPC aus, wo sich das HA-Paar befindet.

Wenn eine Cloud Volumes ONTAP-HA-Konfiguration über mehrere AWS-Verfügbarkeitszonen verteilt ist, sind unverankerte IP-Adressen für den NAS-Datenzugriff über die VPC erforderlich. Diese fließenden IP-Adressen können bei Ausfällen zwischen Nodes migriert werden, sind aber außerhalb der VPC nicht nativ zugänglich. Separate private IP-Adressen ermöglichen den Datenzugriff von außerhalb der VPC, bieten jedoch kein automatisches Failover.

Floating IP-Adressen sind außerdem für die Cluster-Managementoberfläche und die optionale SVM Management LIF erforderlich.

Wenn Sie ein AWS-Transit-Gateway einrichten, ermöglichen Sie den Zugriff auf die unverankerten IP-Adressen von außerhalb der VPC, wo sich das HA-Paar befindet. Das bedeutet, dass NAS-Clients und NetApp Managementtools außerhalb der VPC auf die fließenden IPs zugreifen können.

Das Beispiel zeigt zwei VPCs, die über ein Transit-Gateway verbunden sind. Ein HA-System befindet sich in einer VPC, während ein Client im anderen befindet. Sie können dann mithilfe der fließenden IP-Adresse ein NAS-Volume auf den Client mounten.

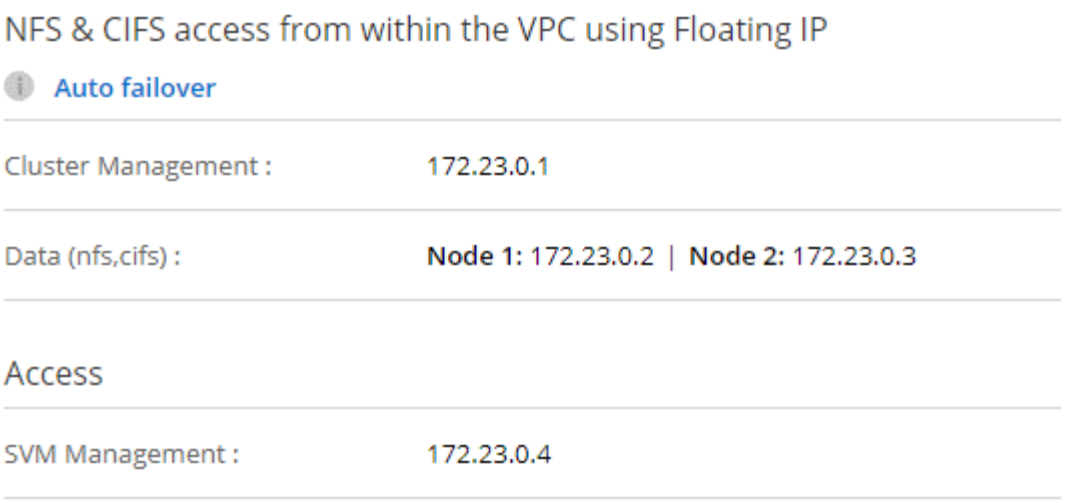


Die folgenden Schritte veranschaulichen die Einrichtung einer ähnlichen Konfiguration.

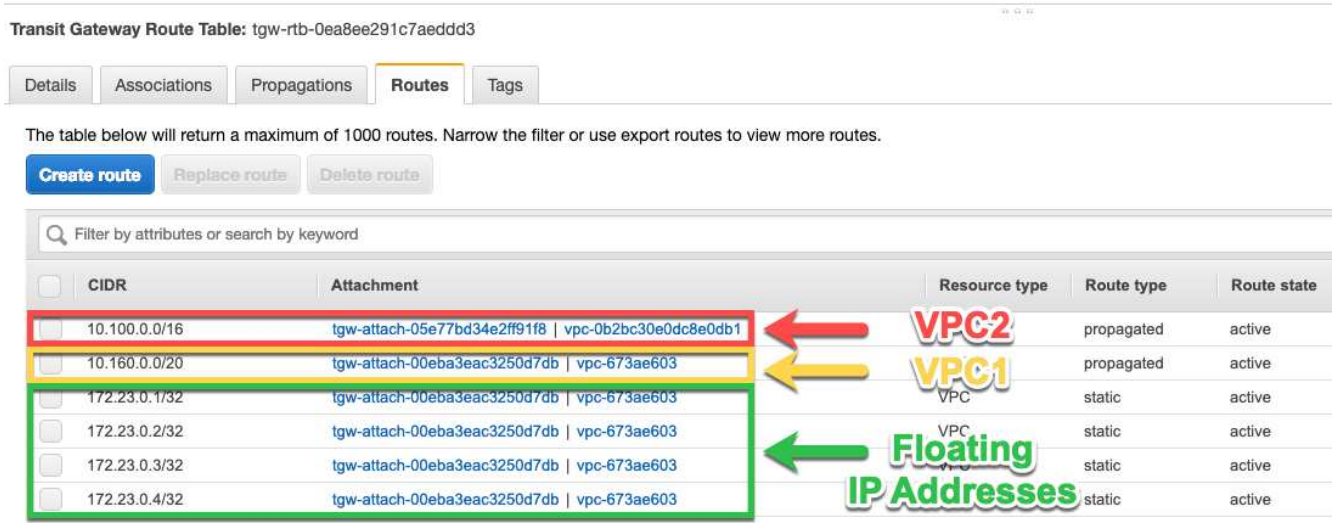
Schritte

1. "Erstellen Sie ein Transit-Gateway, und verbinden Sie die VPCs mit dem Gateway".
2. Erstellen Sie Routen in der Routing-Tabelle des Transit-Gateways durch Angabe der Floating-IP-Adressen des HA-Paars.

   Die unverankerten IP-Adressen finden Sie auf der Seite „Informationen zur Arbeitsumgebung“ in Cloud Manager. Hier ein Beispiel:



Das folgende Beispielbild zeigt die Routingtabelle für das Transit Gateway. Er umfasst Routen zu den CIDR-Blöcken der zwei VPCs und vier von Cloud Volumes ONTAP verwendete Floating IP-Adressen.

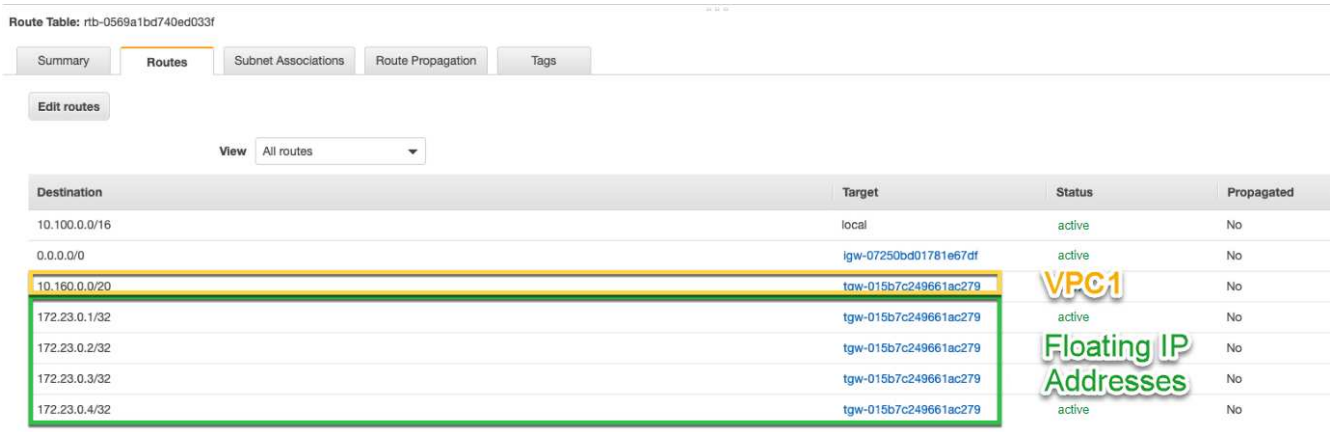


3. Ändern Sie die Routingtabelle von VPCs, die auf die fließenden IP-Adressen zugreifen müssen.

   a. Fügen Sie den unverankerten IP-Adressen Routeneinträge hinzu.

   b. Fügen Sie einen Routeneintrag zum CIDR-Block des VPC hinzu, wo das HA-Paar residiert.

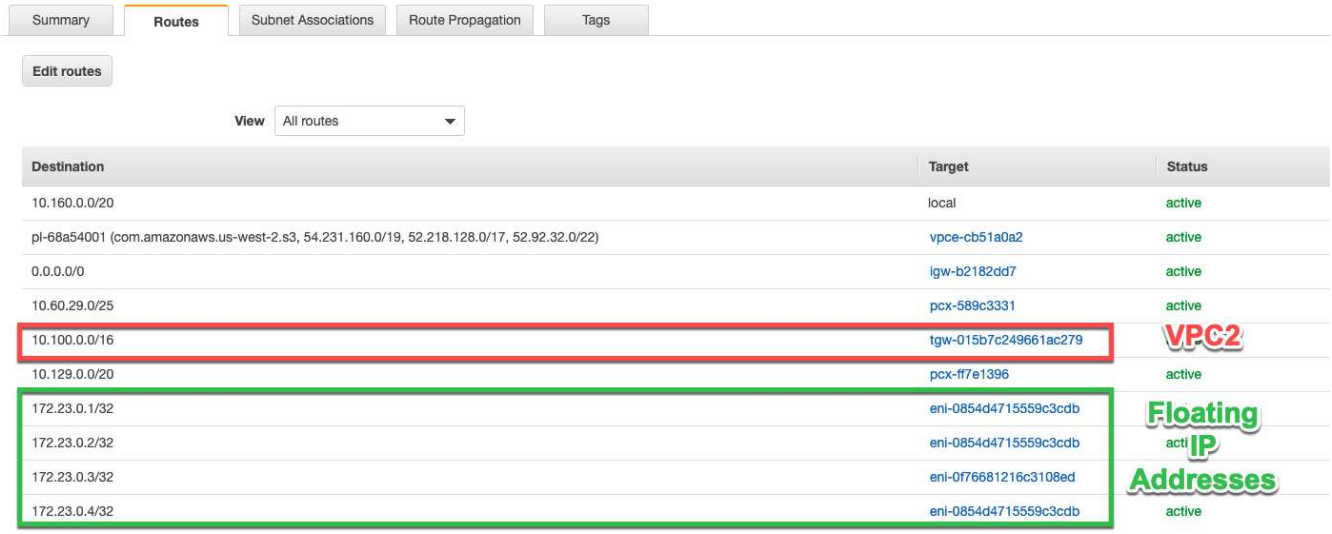
      Das folgende Beispielbild zeigt die Routingtabelle für VPC 2, die auch Routen zu VPC 1 und die fließenden IP-Adressen umfasst.



4. Ändern Sie die Routing-Tabelle für die VPC des HA-Paars, indem Sie der VPC eine Route hinzufügen, die Zugriff auf die fließenden IP-Adressen benötigt.

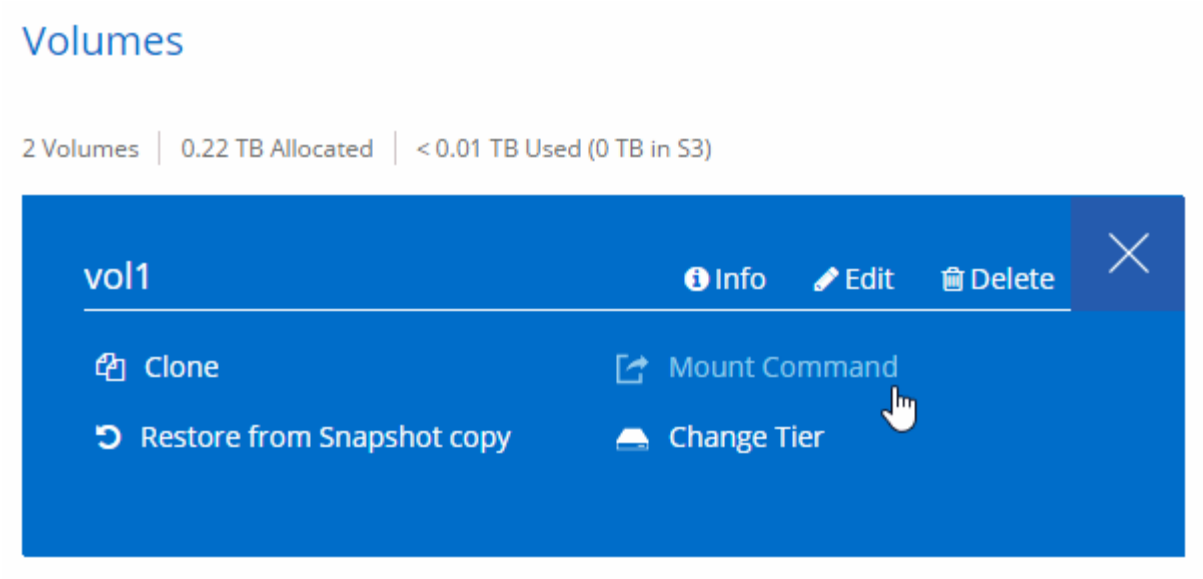
   Dieser Schritt ist wichtig, da er die Weiterleitung zwischen den VPCs abgeschlossen hat.

   Das folgende Beispielbild zeigt die Routing-Tabelle für VPC 1. Sie umfasst eine Route zu den unverankerten IP-Adressen und zu VPC 2, wo sich der Client befindet. Cloud Manager hat bei der Implementierung des HA-Paars automatisch die Floating IPs zur Routing-Tabelle hinzugefügt.



5. Volumes werden mithilfe der Floating IP-Adresse an Clients gemountet.

   Die richtige IP-Adresse finden Sie in Cloud Manager, indem Sie ein Volume auswählen und auf **Mount Command** klicken.



Verwandte Links

- "Hochverfügbarkeitspaare in AWS"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"

Netzwerkanforderungen für Cloud Volumes ONTAP in Azure

Sie müssen Ihr Azure Networking so einrichten, dass Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren.

Suchen Sie nach der Liste der Endpunkte, auf die Cloud Manager Zugriff benötigt? Sie werden jetzt an einem einzigen Ort gepflegt. "Details finden Sie hier".

Outbound-Internetzugang für Cloud Volumes ONTAP

Cloud Volumes ONTAP erfordert ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen AWS HTTP-/HTTPS-Datenverkehr an die folgenden Endpunkte ermöglichen, damit Cloud Volumes ONTAP AutoSupport-Meldungen senden kann:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da Cloud Manager dies für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie "Regeln für Sicherheitsgruppen".

Verbindung von Cloud Volumes ONTAP zu Azure Blob Storage für Data Tiering

Wenn Sie „kalte“ Daten für Azure Blob Storage Tiering möchten, müssen Sie keinen vnet Service-Endpunkt einrichten, wenn Cloud Manager über die erforderlichen Berechtigungen verfügt:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Diese Berechtigungen sind in der neuesten enthalten "Cloud Manager-Richtlinie".

Weitere Informationen zum Einrichten von Daten-Tiering finden Sie unter "Tiering von kalten Daten auf kostengünstigen Objekt-Storage".

Verbindungen zu ONTAP Systemen in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP System in Azure und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie über eine VPN-Verbindung zwischen Azure VNet und dem anderen Netzwerk verfügen, z. B. einem AWS VPC oder Ihrem Unternehmensnetzwerk.

Anweisungen finden Sie unter "Microsoft Azure Dokumentation: Erstellen Sie eine Site-to-Site-Verbindung im Azure-Portal".

Zusätzliche Bereitstellungsoptionen

Anforderungen an den Cloud Manager Host

Wenn Sie Cloud Manager auf Ihrem eigenen Host installieren, müssen Sie die Unterstützung für Ihre Konfiguration überprüfen, die Betriebssystemanforderungen, Portanforderungen usw. umfasst.

Unterstützte AWS EC2-Instanztypen

t3.Medium (empfohlen), t2.Medium und m4.Large

Unterstützte Azure VM-Größen

A2, D2 v2 oder D2 v3 (je nach Verfügbarkeit)

Unterstützte Betriebssysteme

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4

  Das Red Hat Enterprise Linux System muss beim Red Hat Subscription Management registriert sein. Wenn sie nicht registriert ist, kann das System während der Cloud Manager-Installation nicht auf Repositorys zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

  Cloud Manager wird auf englischsprachigen 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?"^]

CPU

2,27 GHz oder höher mit zwei Cores

RAM

4 GB

Freier Speicherplatz

50 GB

Outbound-Internetzugang

Bei der Installation von Cloud Manager und bei der Implementierung von Cloud Volumes ONTAP ist ein Outbound-Internetzugang erforderlich. Eine Liste der Endpunkte finden Sie unter "Netzwerkanforderungen für Cloud Manager".

Ports

Folgende Ports müssen verfügbar sein:

- 80 für HTTP-Zugriff
- 443 für HTTPS-Zugriff
- 3306 für die Cloud Manager-Datenbank
- 8080 für den Cloud Manager-API-Proxy

Wenn andere Services diese Ports verwenden, schlägt die Installation von Cloud Manager fehl.

Es besteht ein potenzieller Konflikt mit Port 3306. Wenn eine andere Instanz von MySQL auf dem Host ausgeführt wird, verwendet es standardmäßig Port 3306. Sie müssen den Port ändern, den die vorhandene MySQL-Instanz verwendet.

Sie können die standardmäßigen HTTP- und HTTPS-Ports ändern, wenn Sie Cloud Manager installieren. Sie können den Standardport für die MySQL-Datenbank nicht ändern. Wenn Sie die HTTP- und HTTPS-Ports ändern, müssen Sie sicherstellen, dass Benutzer von einem Remote-Host aus auf die Cloud Manager-Webkonsole zugreifen können:

- Ändern Sie die Sicherheitsgruppe, um eingehende Verbindungen über die Ports zuzulassen.
- Geben Sie den Port an, wenn Sie die URL für die Cloud Manager-Webkonsole eingeben.

Installieren von Cloud Manager auf einem vorhandenen Linux-Host

Die geläufigste Methode für die Implementierung von Cloud Manager besteht aus Cloud Central oder aus dem Markt eines Cloud-Providers. Sie haben jedoch die Möglichkeit, die Cloud Manager-Software auf einem vorhandenen Linux-Host in Ihrem Netzwerk oder in der Cloud herunterzuladen und zu installieren.

Bevor Sie beginnen

- Ein Red Hat Enterprise Linux-System muss bei Red Hat Subscription Management registriert sein. Wenn sie nicht registriert ist, kann das System während der Cloud Manager-Installation nicht auf Repositorys zugreifen, um die erforderliche Software von Drittanbietern zu aktualisieren.

- Das Cloud Manager-Installationsprogramm greift während des Installationsvorgangs auf mehrere URLs zu. Sie müssen sicherstellen, dass ausgehende Internetzugriffe auf diese Endpunkte zulässig sind. Siehe "Netzwerkanforderungen für Cloud Manager".

Über diese Aufgabe

- Für die Installation von Cloud Manager sind keine Root-Berechtigungen erforderlich.
- Cloud Manager installiert die AWS-Befehlszeilentools (awscli), um Recovery-Verfahren vom NetApp Support zu ermöglichen.

  Wenn Sie eine Meldung erhalten, dass die Installation des awscli fehlgeschlagen ist, können Sie die Meldung ignorieren. Cloud Manager kann ohne die Tools erfolgreich arbeiten.

- Das Installationsprogramm, das auf der NetApp Support-Website verfügbar ist, kann möglicherweise eine frühere Version sein. Nach der Installation aktualisiert sich Cloud Manager automatisch, wenn eine neue Version verfügbar ist.

Schritte

1. Netzwerkanforderungen prüfen:
   - "Netzwerkanforderungen für Cloud Manager"
   - "Netzwerkanforderungen für Cloud Volumes ONTAP für AWS"
   - "Netzwerkanforderungen für Cloud Volumes ONTAP für Azure"
2. Prüfen "Anforderungen an den Cloud Manager Host".
3. Laden Sie die Software von 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".

4. Weisen Sie Berechtigungen zum Ausführen des Skripts zu.

   Beispiel

   ```
    chmod +x OnCommandCloudManager-V3.6.3.sh
   . Führen Sie das Installationsskript aus:
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.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 Cloud Manager-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.

5. 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.

   Wenn Sie die HTTP- und HTTPS-Ports ändern, müssen Sie sicherstellen, dass Benutzer von einem Remote-Host aus auf die Cloud Manager-Webkonsole zugreifen können:

   - Ändern Sie die Sicherheitsgruppe, um eingehende Verbindungen über die Ports zuzulassen.
   - Geben Sie den Port an, wenn Sie die URL für die Cloud Manager-Webkonsole eingeben.

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

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

   https://ipaddress:port

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

7. Melden Sie sich für ein NetApp Cloud Central Konto an, oder melden Sie sich an, wenn Sie bereits über ein Konto verfügen.
8. Wenn Sie sich anmelden oder anmelden, fügt Cloud Manager Ihr Benutzerkonto automatisch als Administrator für dieses System hinzu.
9. Geben Sie nach der Anmeldung einen Namen für dieses Cloud Manager-System ein.

Nachdem Sie fertig sind

Richten Sie Berechtigungen für Ihre AWS und Azure Konten ein, damit Cloud Manager Cloud Volumes ONTAP implementieren kann:

- Wenn Sie Cloud Volumes ONTAP in AWS implementieren möchten, "AWS Konto einrichten und dann zu Cloud Manager hinzufügen".
- Wenn Sie Cloud Volumes ONTAP in Azure implementieren möchten, "Richten Sie ein Azure-Konto ein, und fügen Sie es anschließend zu Cloud Manager hinzu".

Starten von Cloud Manager über den AWS Marketplace

Am besten sollte Cloud Manager in AWS gestartet werden, indem verwendet wird "NetApp Cloud Central", Sie können diese jedoch bei Bedarf über den AWS Marketplace starten.

Wenn Sie Cloud Manager über den AWS Marketplace starten, ist Cloud Manager weiterhin in NetApp Cloud Central integriert. "Erfahren Sie mehr über die Integration".

Über diese Aufgabe

In den folgenden Schritten wird beschrieben, wie die Instanz von der EC2-Konsole aus gestartet wird, da Sie über die Konsole eine IAM-Rolle an die Cloud Manager-Instanz anhängen können. Dies ist mit der 1-Klick-Option nicht möglich.

Schritte

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

      "NetApp OnCommand Cloud Manager: AWS- und Azure Policies"

   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. Wechseln Sie zum "Seite zu Cloud Manager im AWS Marketplace".
3. Klicken Sie Auf **Weiter**.
4. Klicken Sie auf der Registerkarte Benutzerdefinierter Start auf **mit EC2-Konsole** für Ihre Region starten, und wählen Sie dann Ihre Auswahl aus:
   a. Wählen Sie je nach Verfügbarkeit der Region den Instanztyp t3.Medium (empfohlen), t2.Medium oder m4.Large aus.
   b. Wählen Sie eine VPC, ein Subnetz, eine IAM-Rolle und andere Konfigurationsoptionen aus, die Ihren Anforderungen entsprechen.
   c. Behalten Sie die Standardspeicheroptionen bei.
   d. Geben Sie bei Bedarf Tags für die Instanz ein.
   e. Geben Sie die erforderlichen Verbindungsmethoden für die Cloud Manager-Instanz an: SSH, HTTP und HTTPS.
   f. Klicken Sie Auf **Start**.

Ergebnis

AWS startet die Software mit den angegebenen Einstellungen. Die Cloud Manager-Instanz und -Software sollten in etwa fünf Minuten ausgeführt werden.

Nachdem Sie fertig sind

Melden Sie sich bei Cloud Manager an, indem Sie die öffentliche IP-Adresse oder die private IP-Adresse in einem Webbrowser eingeben und anschließend den Setup-Assistenten ausführen.

Bereitstellung von Cloud Manager über Azure Marketplace

Am besten implementieren Sie Cloud Manager in Azure "NetApp Cloud Central", Die Implementierung kann jedoch bei Bedarf im Azure Marketplace erfolgen.

Für die Implementierung von Cloud Manager in stehen separate Anweisungen zur Verfügung "Azure Regionen der US-Regierung" Und ein "Azure Deutschland Regionen".

Wenn Sie Cloud Manager über den Azure Marketplace implementieren, ist Cloud Manager weiterhin in NetApp Cloud Central integriert. "Erfahren Sie mehr über die Integration".

Bereitstellung von Cloud Manager in Azure

Sie müssen Cloud Manager installieren und einrichten, damit Sie Cloud Volumes ONTAP in Azure starten können.

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 der empfohlenen virtuellen Maschinengrößen: A2, D2 v2 oder D2 v3 (je nach Verfügbarkeit).
   - Für die Netzwerksicherheitsgruppe erfordert Cloud Manager eingehende Verbindungen unter Verwendung von SSH, HTTP und HTTPS.

     "Erfahren Sie mehr über die Regeln für Sicherheitsgruppen für Cloud Manager".

   - Aktivieren Sie unter **Management System zugewiesene verwaltete Identität** für Cloud Manager durch Auswahl von **ein**.

     Diese Einstellung ist wichtig, da eine gemanagte Identität es der Virtual Machine von Cloud Manager ermöglicht, sich in Azure Active Directory zu identifizieren, ohne Zugangsdaten angeben zu müssen. "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 Cloud Manager-Software sollten in etwa fünf Minuten ausgeführt werden.

5. Öffnen Sie einen Webbrowser von einem Host aus, der eine Verbindung zur virtuellen Cloud Manager-Maschine hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

   Wenn Sie sich anmelden, fügt Cloud Manager Ihr Benutzerkonto automatisch als Administrator für dieses System hinzu.

6. Geben Sie nach der Anmeldung einen Namen für das Cloud Manager-System ein.

Ergebnis

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

Azure Berechtigungen für Cloud Manager gewähren

Bei der Implementierung von Cloud Manager in Azure sollten Sie a aktiviert haben "Vom System zugewiesene verwaltete Identität". Sie müssen jetzt die erforderlichen Azure Berechtigungen erteilen, indem Sie eine benutzerdefinierte Rolle erstellen und dann die Rolle der virtuellen Cloud Manager-Maschine für eine 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-c25fbzzzzzzzzzzzz", "/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 Rollendefinition erstellen --Role-Definition C:\Policy_for_Cloud_Manager_Azure_3.6.1.json

   Sie sollten nun eine benutzerdefinierte Rolle namens OnCommand Cloud Manager Operator haben, die Sie der virtuellen Cloud Manager-Maschine zuweisen können.

2. Weisen Sie die Rolle der virtuellen Cloud Manager-Maschine für ein 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 **OnCommand Cloud Manager Operator** aus.

        OnCommand 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 Cloud Manager-Maschine erstellt wurde.
      - Wählen Sie die virtuelle Cloud Manager-Maschine 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

Cloud Manager verfügt jetzt über die Berechtigungen, die es für die Bereitstellung und das Management von Cloud Volumes ONTAP in Azure benötigt.

Cloud Manager in einer Region der US-Regierung von Azure implementieren

Wenn Cloud Manager in einer Region der US-Regierung starten soll, implementieren Sie zunächst Cloud Manager über den Azure Government Marketplace. Stellen Sie dann die Berechtigungen bereit, die Cloud Manager für die Implementierung und das Management von Cloud Volumes ONTAP Systemen benötigt.

Eine Liste der unterstützten Regionen der US-Regierung in Azure finden Sie unter "Cloud Volumes Regionen Weltweit".

Cloud Manager über den Azure Marketplace für die US-Regierung bereitstellen

Cloud Manager ist als Bild im Azure US Government Marketplace erhältlich.

Schritte

1. Suchen Sie im Azure US Government Portal nach OnCommand Cloud Manager.
2. Klicken Sie auf **Erstellen** und befolgen Sie die Schritte zur Konfiguration der virtuellen Maschine.

   Beachten Sie beim Konfigurieren der virtuellen Maschine Folgendes:

   - Cloud Manager kann mit HDD- oder SSD-Festplatten optimal arbeiten.
   - Sie sollten eine der empfohlenen virtuellen Maschinengrößen wählen: A2, D2 v2 oder D2 v3 (je nach Verfügbarkeit).
   - Für die Netzwerksicherheitsgruppe empfiehlt es sich, **Erweitert** zu wählen.

     Mit der Option **Erweitert** wird eine neue Sicherheitsgruppe erstellt, die die erforderlichen eingehenden Regeln für Cloud Manager enthält. Wenn Sie „Basis“ wählen, lesen Sie unter "Regeln für Sicherheitsgruppen" Für die Liste der erforderlichen Regeln.

3. Überprüfen Sie auf der Übersichtsseite 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 Cloud Manager-Software sollten in etwa fünf Minuten ausgeführt werden.

4. Öffnen Sie einen Webbrowser von einem Host aus, der eine Verbindung zur virtuellen Cloud Manager-Maschine hat, und geben Sie die folgende URL ein:

   http://ipaddress:80

   Wenn Sie sich anmelden, fügt Cloud Manager Ihr Benutzerkonto automatisch als Administrator für dieses System hinzu.

5. Geben Sie nach der Anmeldung einen Namen für das Cloud Manager-System ein.

Ergebnis

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

Zuweisen von Azure Berechtigungen für Cloud Manager unter Verwendung einer gemanagten Identität

Am einfachsten können Sie Berechtigungen bereitstellen, indem Sie ein aktivieren "Verwaltete Identität" Auf

der virtuellen Cloud Manager-Maschine und dann durch Zuweisen der erforderlichen Berechtigungen zu der virtuellen Maschine. Falls gewünscht, ist eine alternative Methode "Azure-Berechtigungen über einen Service-Principal gewähren".

Schritte

1. Aktivieren einer verwalteten Identität auf der virtuellen Cloud Manager-Maschine:
   a. Navigieren Sie zu der virtuellen Cloud Manager-Maschine und wählen Sie **Identität**.
   b. Klicken Sie unter **System Assigned** auf **on** und dann auf **Speichern**.
2. 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-c25fbzzzzzzzzzzzz", "/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 Rollendefinition erstellen --Role-Definition C:\Policy_for_Cloud_Manager_Azure_3.6.1.json

   Sie sollten nun eine benutzerdefinierte Rolle namens OnCommand Cloud Manager Operator haben, die Sie der virtuellen Cloud Manager-Maschine zuweisen können.

3. Weisen Sie die Rolle der virtuellen Cloud Manager-Maschine für ein 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**, klicken Sie auf **Rollenzuweisung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
      - Wählen Sie die Rolle **OnCommand Cloud Manager Operator** aus.

        OnCommand 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 Cloud Manager-Maschine erstellt wurde.
      - Geben Sie den Namen der virtuellen Maschine ein, und wählen Sie sie 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

Cloud Manager verfügt jetzt über die Berechtigungen, die es für die Bereitstellung und das Management von Cloud Volumes ONTAP in Azure benötigt.

Installieren von Cloud Manager in einer Azure Deutschland Region

Der Azure Marketplace ist in den Regionen von Azure Deutschland nicht verfügbar. Sie müssen daher das Cloud Manager-Installationsprogramm von der NetApp Support-Website herunterladen und auf einem vorhandenen Linux-Host in der Region installieren.

Schritte

1. "Netzwerkanforderungen für Azure prüfen".
2. "Host-Anforderungen für Cloud Manager prüfen".
3. "Laden Sie Cloud Manager herunter und installieren Sie es".
4. "Gewähren Sie Cloud Manager Azure Berechtigungen mit einem Service-Principal".

Nachdem Sie fertig sind

Cloud Manager ist jetzt bereit, Cloud Volumes ONTAP wie jede andere Region in Azure Deutschland zu implementieren. Möglicherweise möchten Sie jedoch zuerst ein zusätzliches Setup durchführen.