Einrichten von Cloud Manager

Cloud Manager 3.6

NetApp
March 25, 2024

Inhalt

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

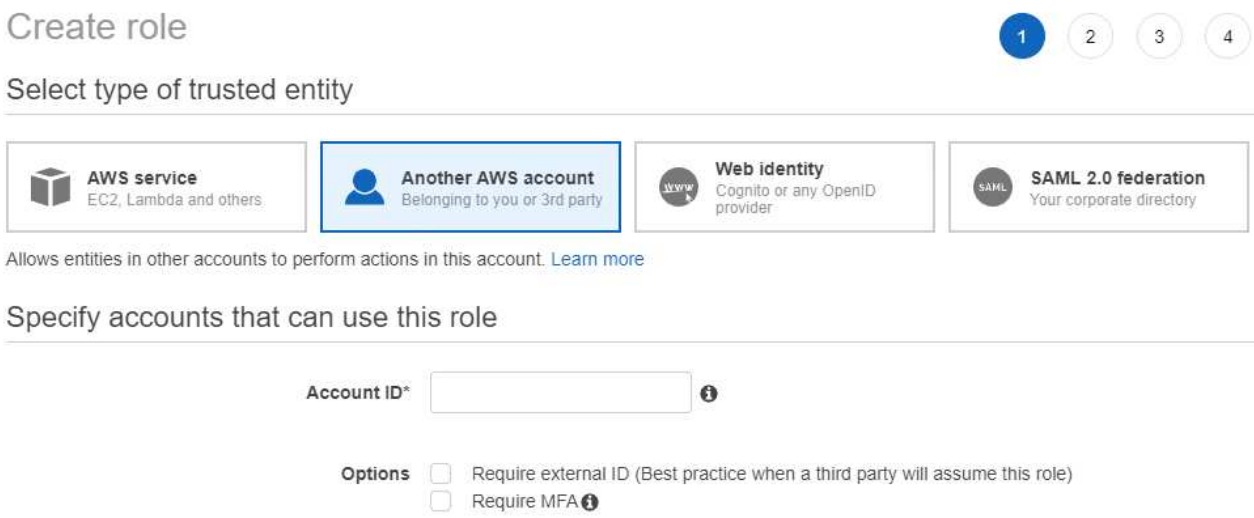
Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Cloud Manager-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie Cloud Manager über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

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

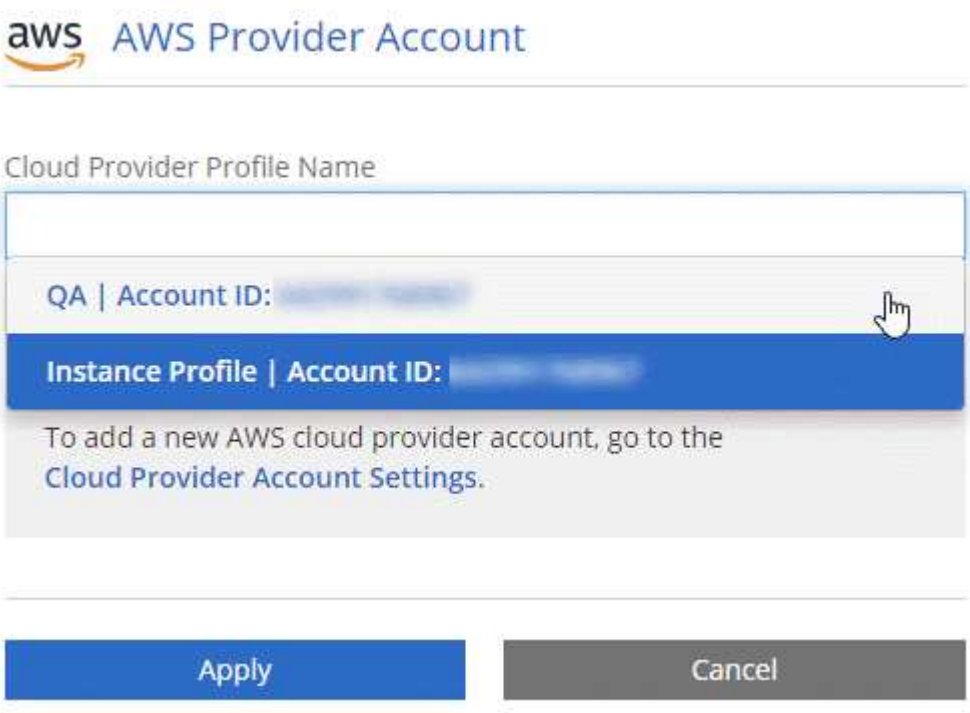
Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen bereitgestellt haben, können Sie das Konto zu Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

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.

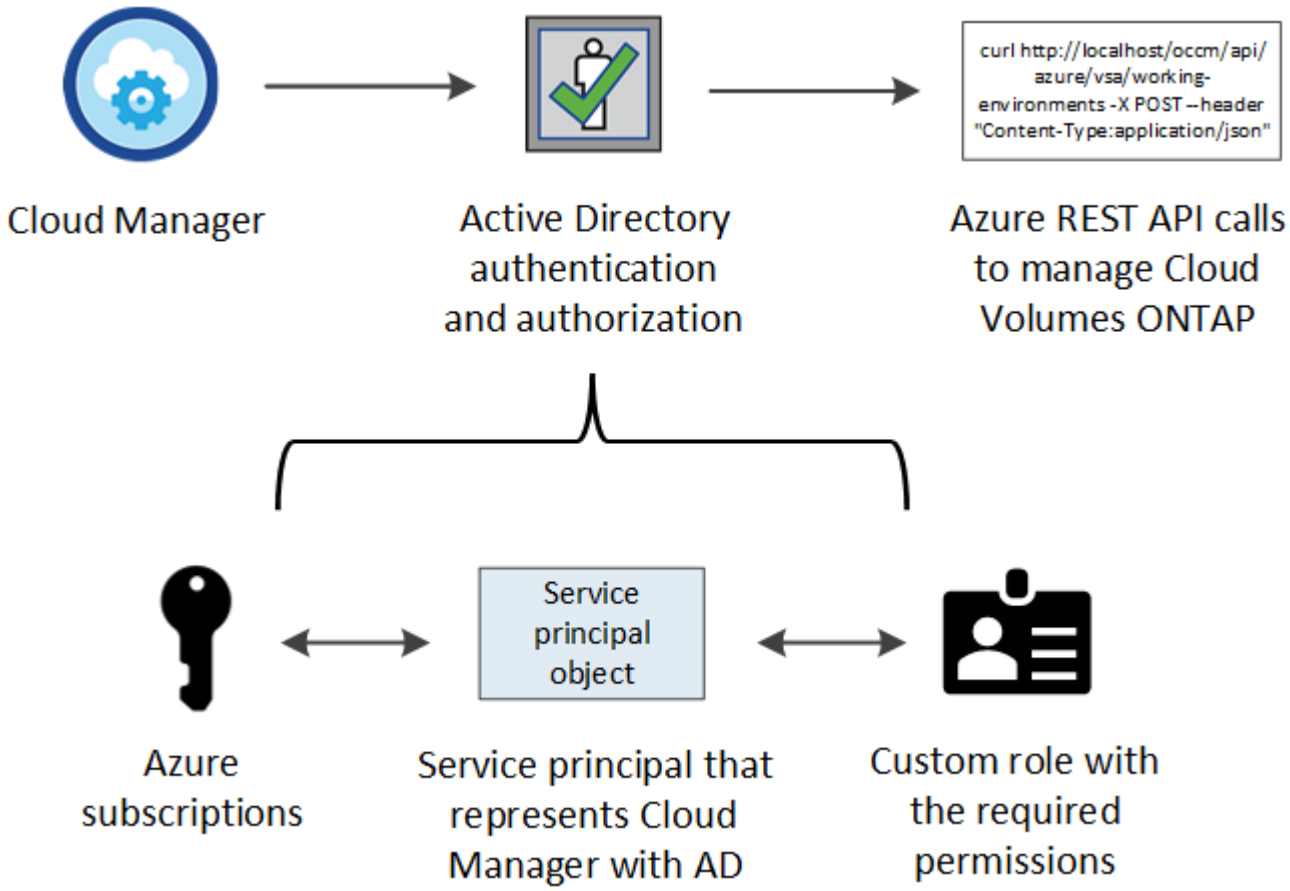
- Azure-Berechtigungen über einen Service-Principal gewähren
- Hinzufügen von Azure-Konten zu Cloud Manager

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

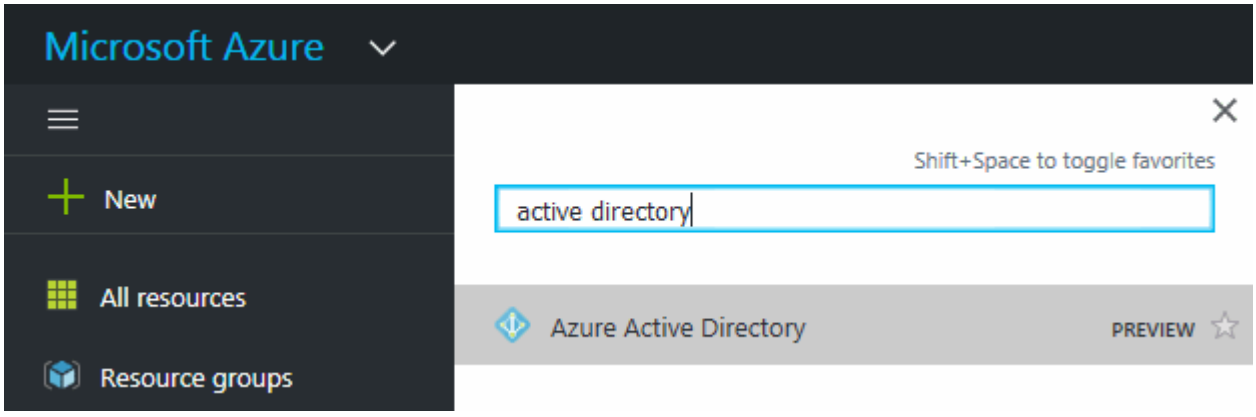
Sie müssen einen Active Directory-Dienstprinzipal erstellen, damit Cloud Manager sich mit Azure Active Directory authentifizieren kann.

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".

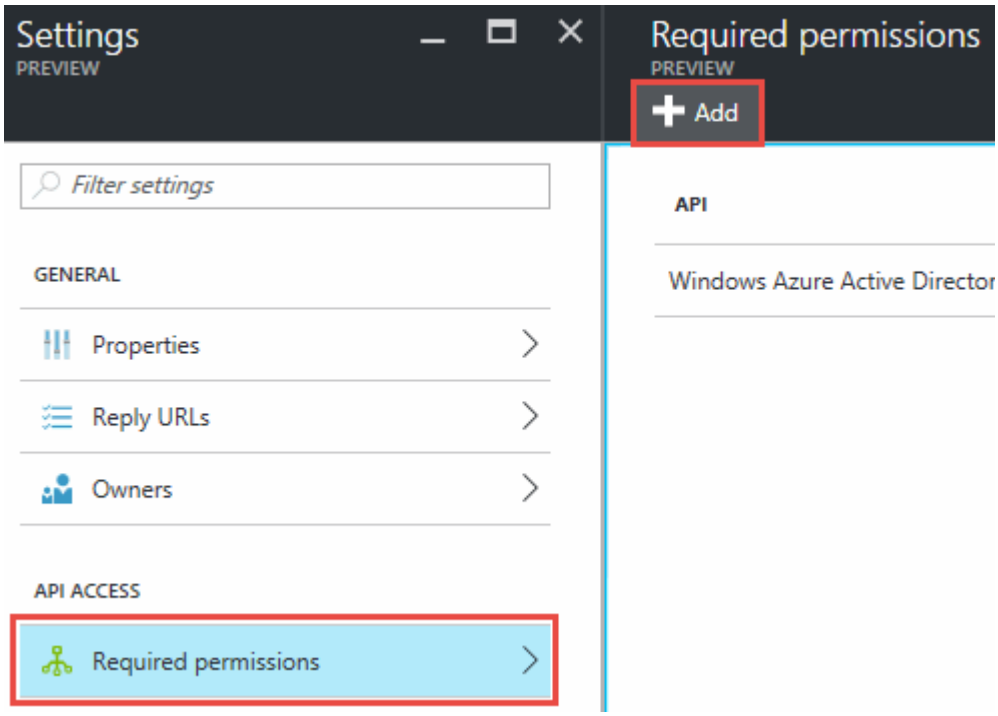
Schritte

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

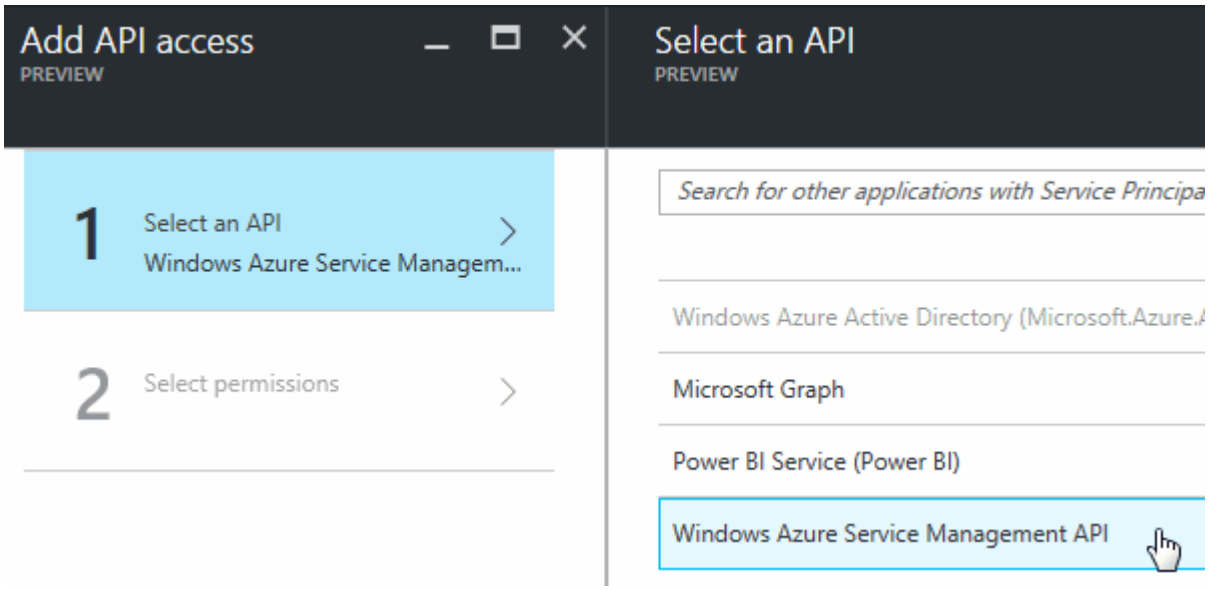


2. Klicken Sie im Menü auf **App-Registrierungen (Legacy)**.

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**.

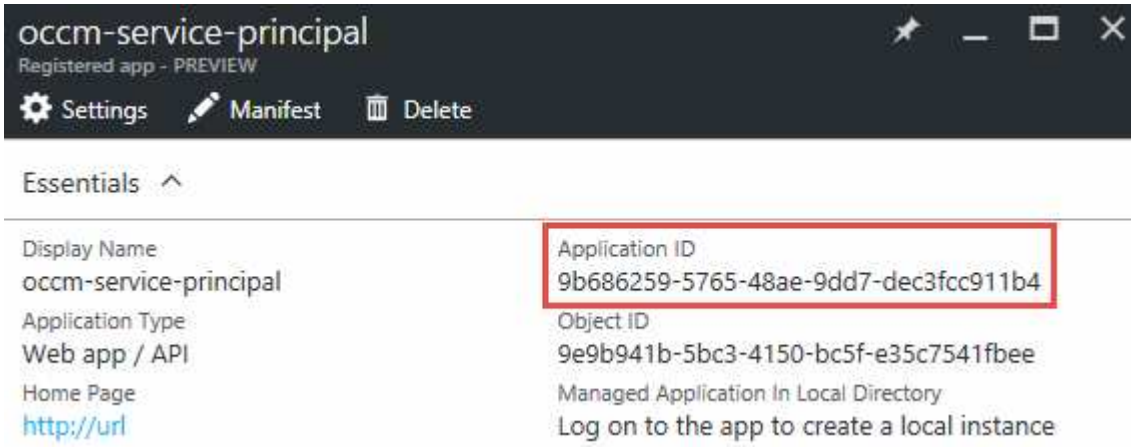
   b. Geben Sie eine Beschreibung ein, wählen Sie eine Dauer aus und klicken Sie dann auf **Speichern**.

   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.

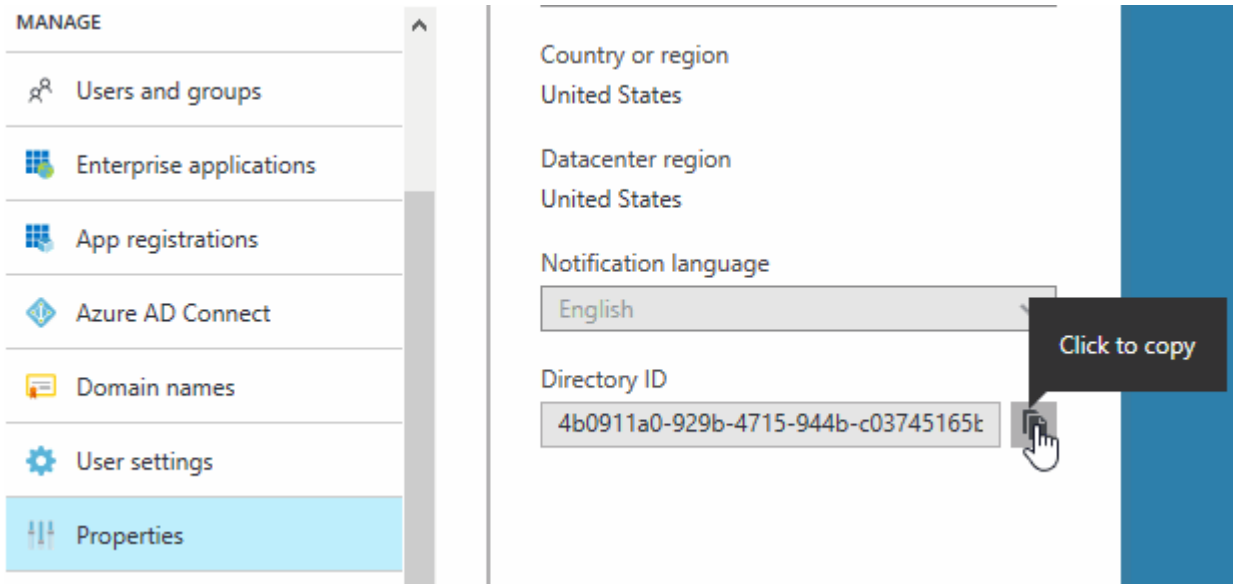
      Ähnlich dem Schlüsselwert müssen Sie bei Cloud Manager ein Cloud-Provider-Konto hinzufügen, indem Sie die Anwendungs-ID in Cloud Manager eingeben.



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

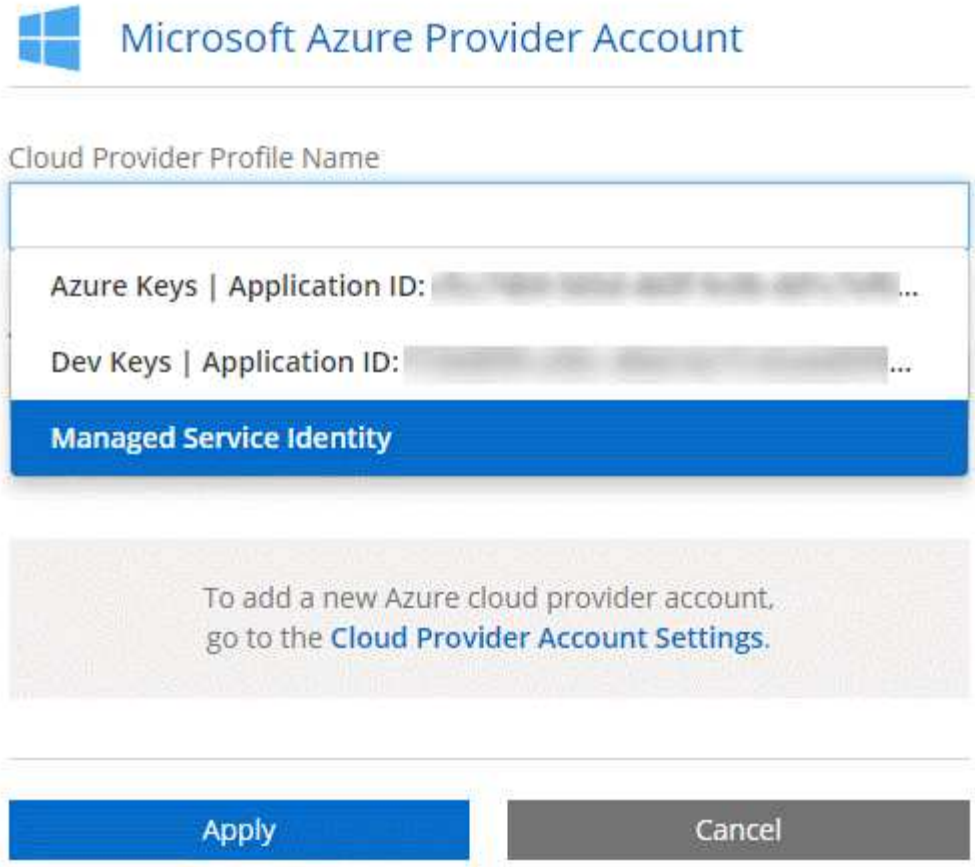
Nachdem Sie ein Azure Konto mit den erforderlichen Berechtigungen angegeben haben, können Sie das Konto zu Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

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.

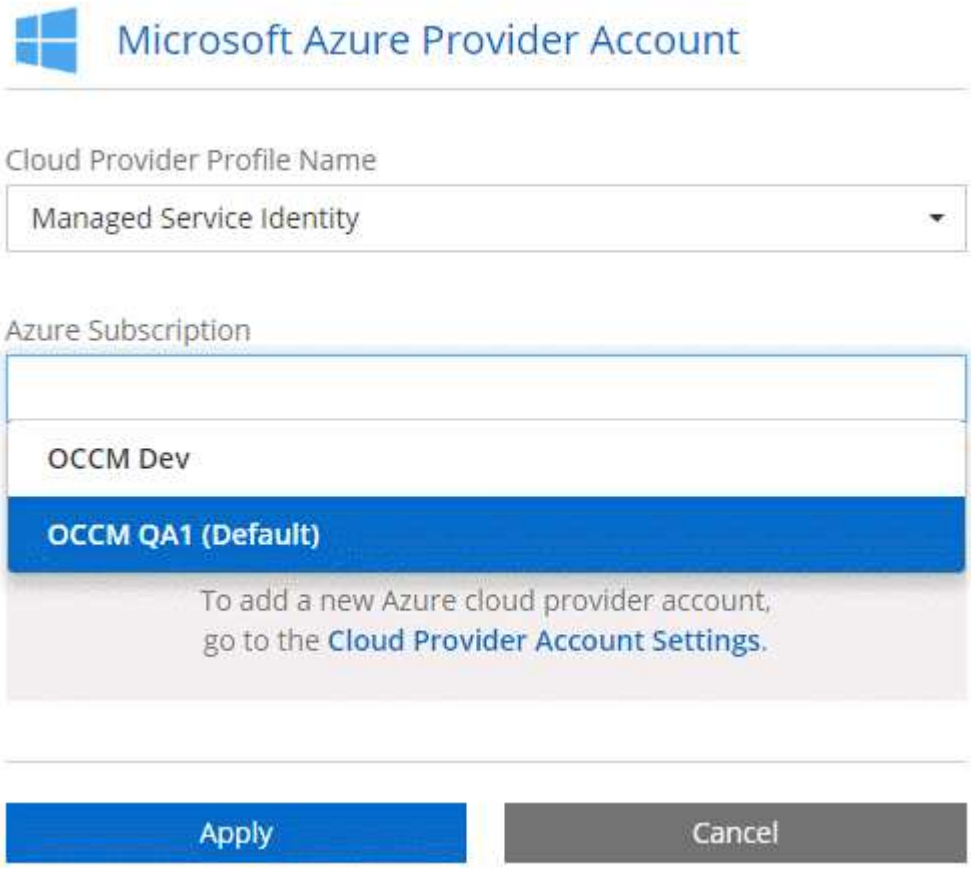
      OnCommand Cloud Manager Operator ist der im angegebene Standardname "Cloud Manager-Richtlinie". Wenn Sie einen anderen Namen für die Rolle ausgewählt haben, wählen Sie stattdessen diesen Namen aus.

- 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.

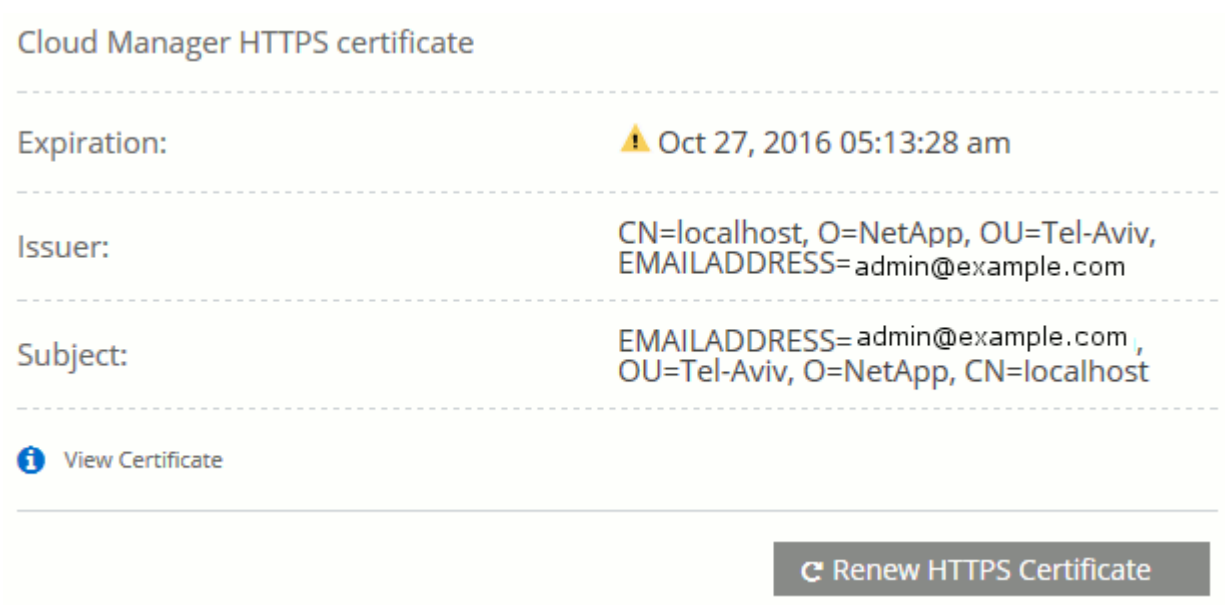
Schritte

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?

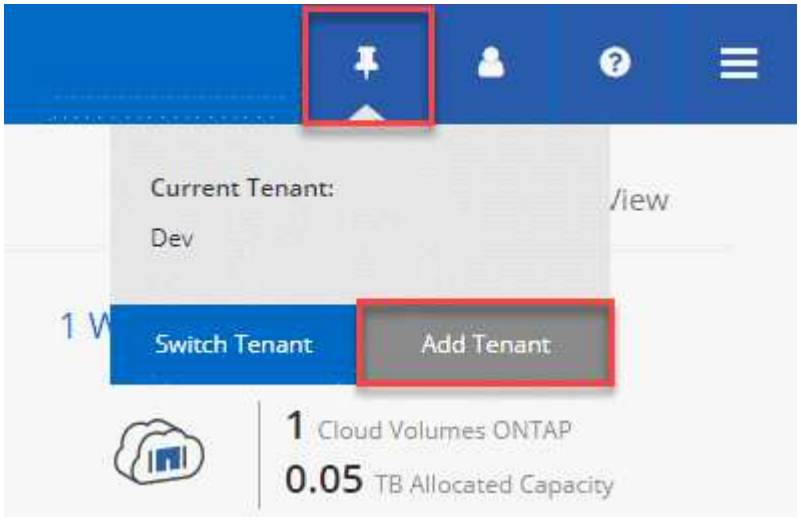
Informieren Sie den Benutzer, dass er sich jetzt beim Cloud Manager-System anmelden kann.

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"

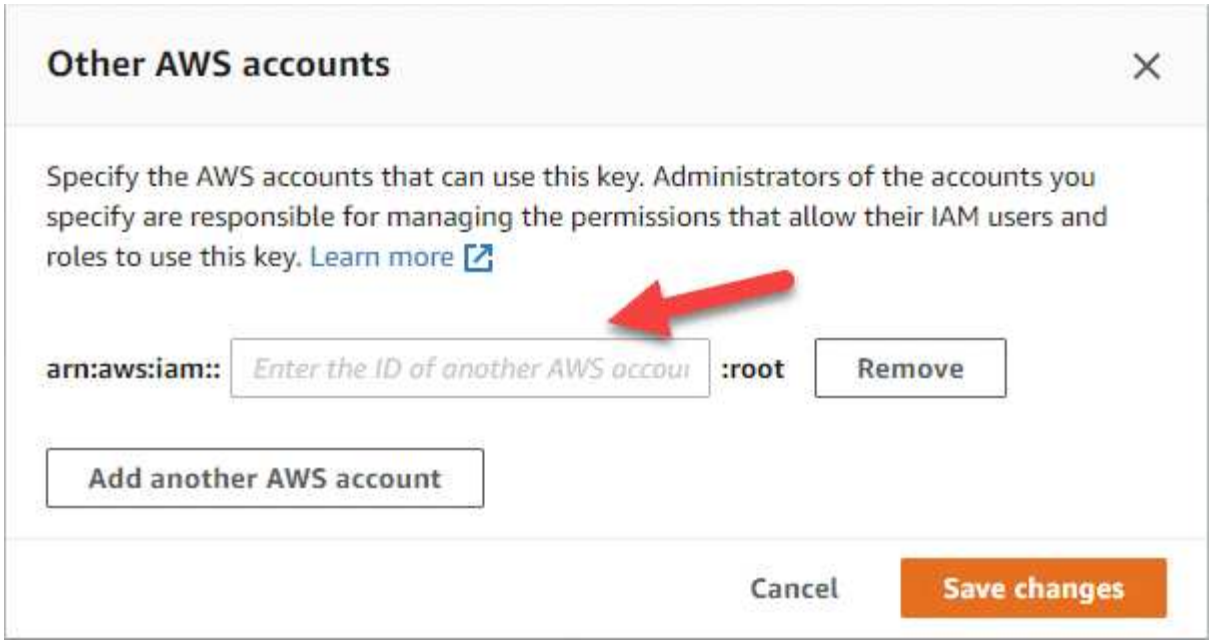
3. Wenn sich das CMK in einem anderen AWS Konto befindet, führen Sie folgende Schritte aus:

   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".