



Anmeldeinformationen verwalten

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

- Anmeldeinformationen verwalten 1
 - AWS 1
 - Azure 8
 - GCP 19
- Hinzufügen von NetApp Support Site Konten zu Cloud Manager 24

Anmeldeinformationen verwalten

AWS

AWS Zugangsdaten und Berechtigungen

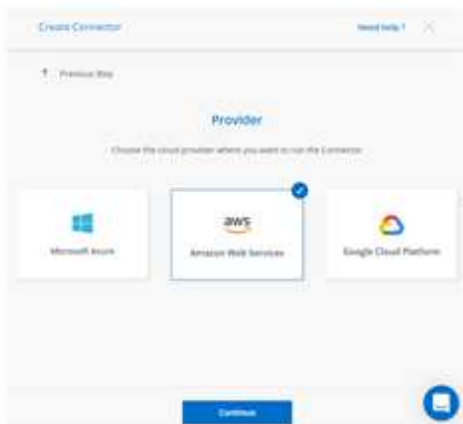
Mit Cloud Manager können Sie die AWS Zugangsdaten auswählen, die Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten. Alle Cloud Volumes ONTAP Systeme können über die ersten AWS Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

Erste AWS Zugangsdaten

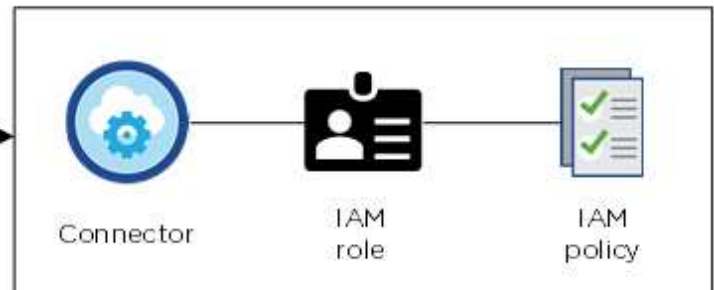
Wenn Sie einen Connector von Cloud Manager bereitstellen, müssen Sie ein AWS-Konto mit Berechtigungen zum Starten der Connector-Instanz verwenden. Die erforderlichen Berechtigungen werden im aufgeführt ["Connector-Implementierungsrichtlinie für AWS"](#).

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

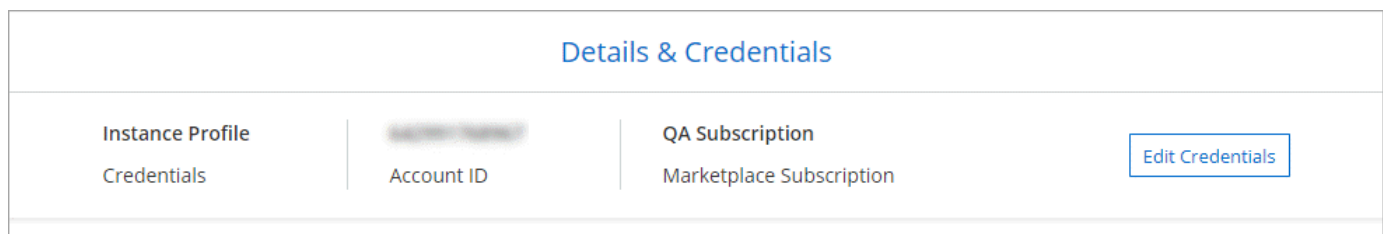
Cloud Manager



AWS account



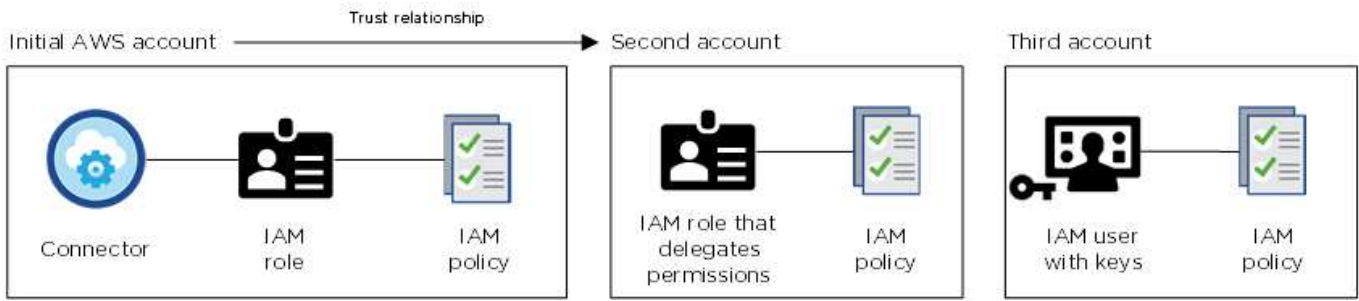
Cloud Manager wählt die AWS Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:



Zusätzliche AWS Zugangsdaten

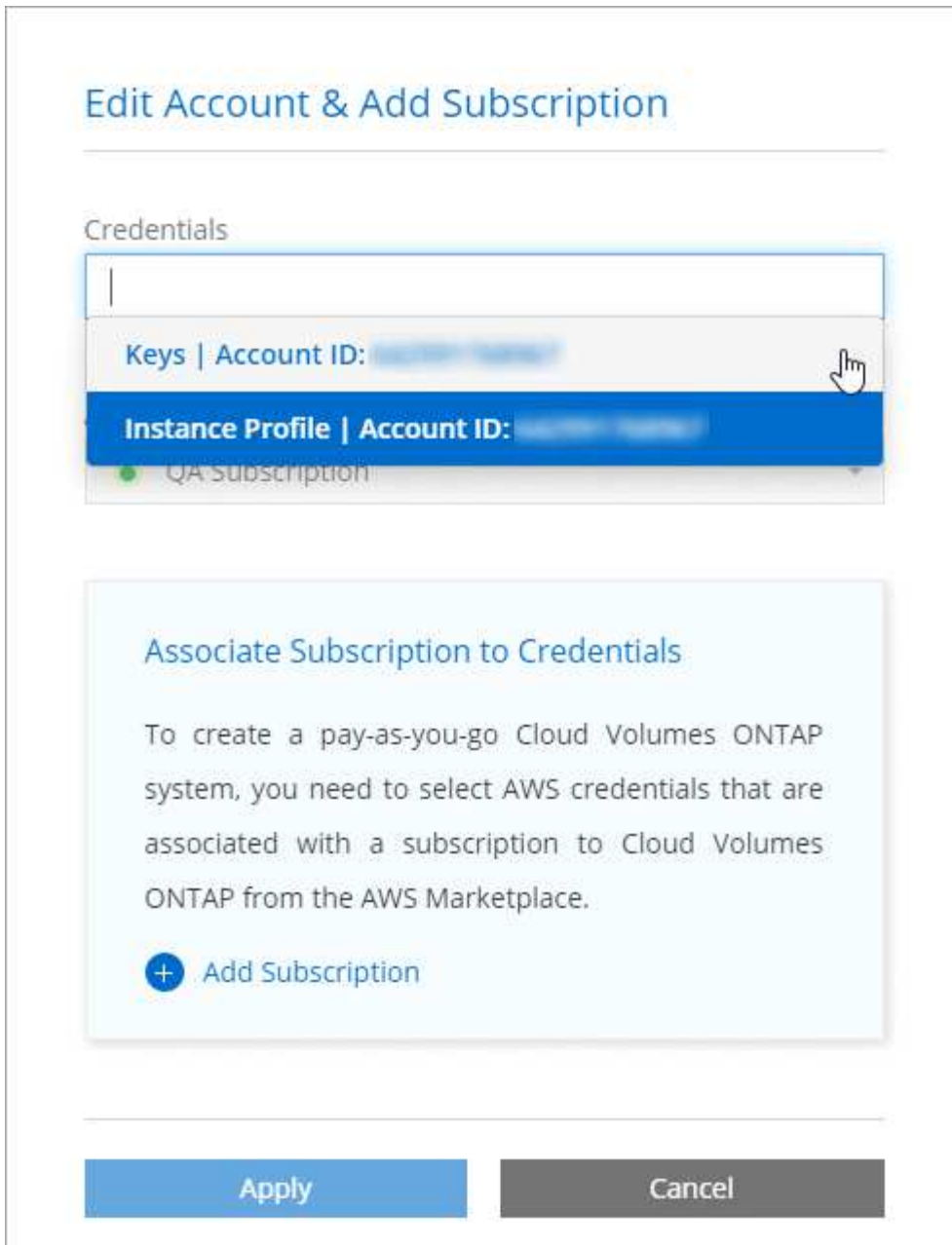
Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Accounts starten möchten, haben Sie eine der

Möglichkeiten "AWS Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen". Die folgende Abbildung zeigt zwei zusätzliche Konten: Eines mit Berechtigungen über eine IAM-Rolle in einem vertrauenswürdigen Konto und ein weiteres über die AWS Schlüssel eines IAM-Benutzers:



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

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



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

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

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

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

Wie kann ich meine AWS Zugangsdaten sicher drehen?

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

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

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

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

Verwalten von AWS Anmeldedaten und Abonnements für Cloud Manager

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

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



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

Auswahl

- [Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln](#)
- [Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten](#)

Wie kann ich meine AWS Zugangsdaten sicher drehen?

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

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

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

Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln

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

Schritte

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

["AWS Dokumentation: Erstellung von IAM-Richtlinien"](#)

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

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. [Sie können es jetzt zu Cloud Manager hinzufügen.](#)

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

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

Schritte

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





Gehen Sie wie folgt vor:

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

Create role



Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

- Options**
- Require external ID (Best practice when a third party will assume this role)
 - Require MFA ⓘ

2. Gehen Sie zum Quellkonto, auf dem sich die Konnektorinstanz befindet, und wählen Sie die IAM-Rolle aus, die an die Instanz angehängt ist.
 - a. Klicken Sie auf **Richtlinien anhängen** und dann auf **Richtlinien erstellen**.
 - b. Erstellen Sie eine Richtlinie, die die Aktion „STS:AssumeRole“ und den ARN der Rolle umfasst, die Sie im Zielkonto erstellt haben.

Beispiel

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

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. [Sie können es jetzt zu Cloud Manager hinzufügen](#).

AWS Zugangsdaten zu Cloud Manager hinzufügen

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

Schritte

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



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

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

6. Klicken Sie Auf **Hinzufügen**.

Ergebnis

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

Edit Account & Add Subscription

Credentials

Keys | Account ID: [redacted]

Instance Profile | Account ID: [redacted]

QA Subscription

Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

+ Add Subscription

Apply Cancel

Verknüpfen eines AWS Abonnements mit den Zugangsdaten

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

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

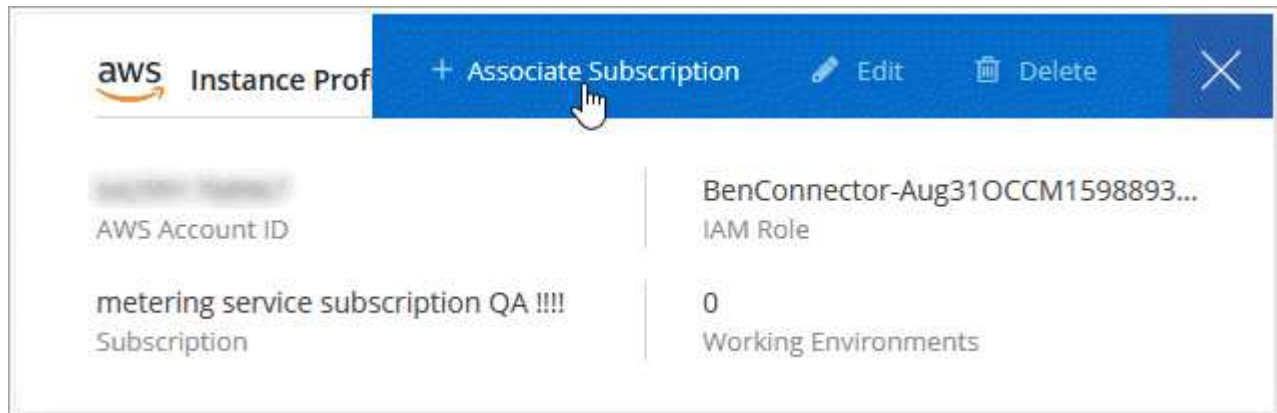
- Sie haben ein Abonnement nicht zugeordnet, wenn Sie zum ersten Mal die Anmeldedaten zu Cloud Manager hinzugefügt haben.
- Sie möchten ein vorhandenes AWS Marketplace Abonnement durch ein neues Abonnement ersetzen.

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "[Erfahren Sie, wie](#)".

Schritte

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



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

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

Azure

Azure Zugangsdaten und Berechtigungen

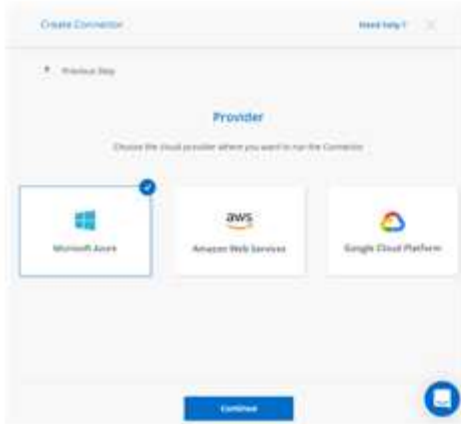
Mit Cloud Manager können Sie die Azure Zugangsdaten auswählen, die Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten. Alle Cloud Volumes ONTAP Systeme können über die ersten Azure Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

Erste Azure Zugangsdaten

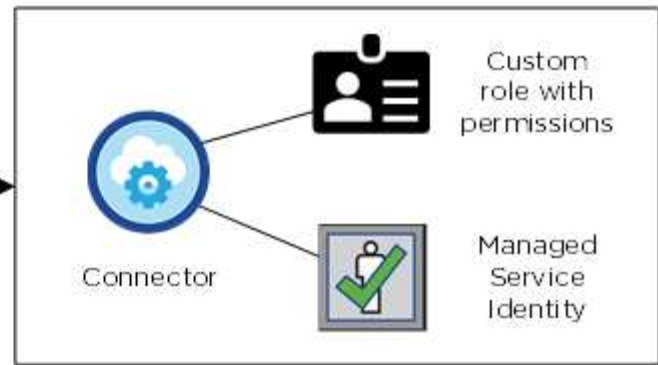
Wenn Sie einen Connector von Cloud Manager bereitstellen, müssen Sie ein Azure-Konto mit Berechtigungen verwenden, um die Virtual Machine Connector bereitzustellen. Die erforderlichen Berechtigungen werden im aufgeführt "[Connector-Implementierungsrichtlinie für Azure](#)".

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

Cloud Manager



Azure account



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

Details & Credentials			
Managed Service Ide...	OCCM QA1	ⓘ No subscription is associated	<button>Edit Credentials</button>
Credential Name	Azure Subscription	Marketplace Subscription	

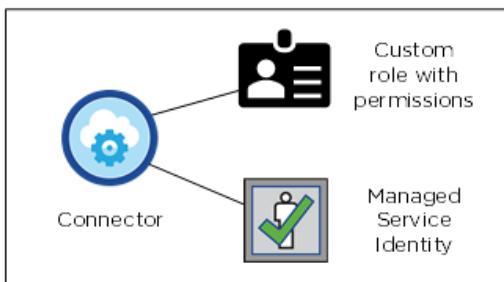
Zusätzliche Azure-Abonnements für eine gemanagte Identität

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

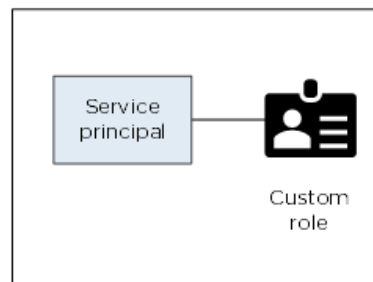
Zusätzliche Azure Zugangsdaten

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

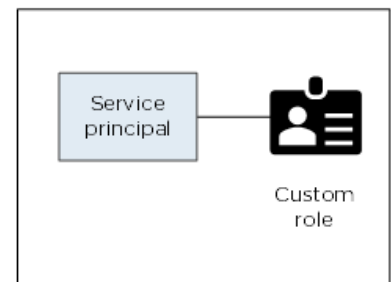
Initial Azure account



Second account



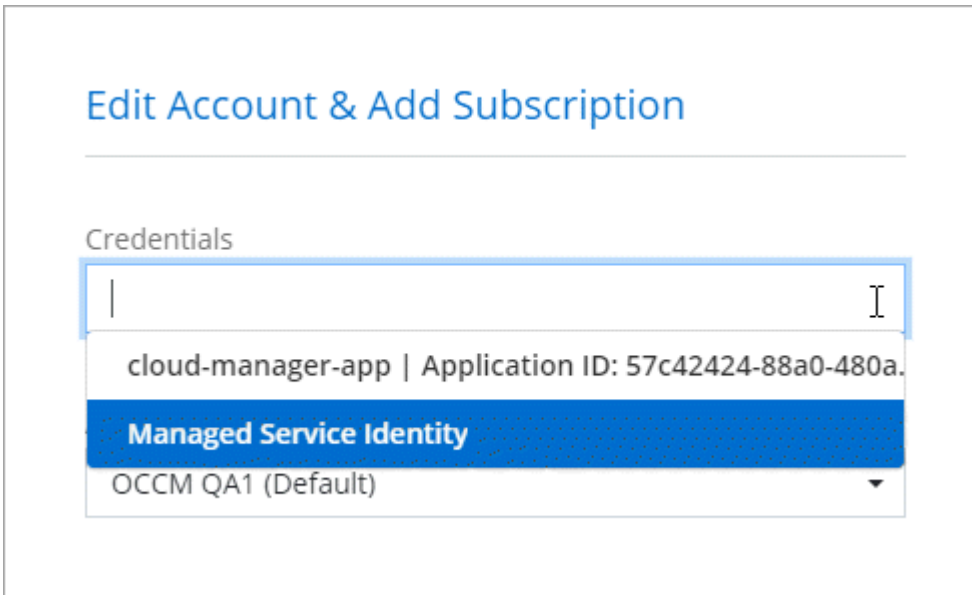
Third account



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

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

wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



The screenshot shows a web interface titled "Edit Account & Add Subscription". Below the title is a section labeled "Credentials". Inside this section is a dropdown menu. The menu is currently open, showing several options. The top option is "cloud-manager-app | Application ID: 57c42424-88a0-480a.". The second option, "Managed Service Identity", is highlighted with a blue background. Below it is "OCCM QA1 (Default)".

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

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

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

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

Verwalten von Azure Anmeldedaten und Abonnements für Cloud Manager

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

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



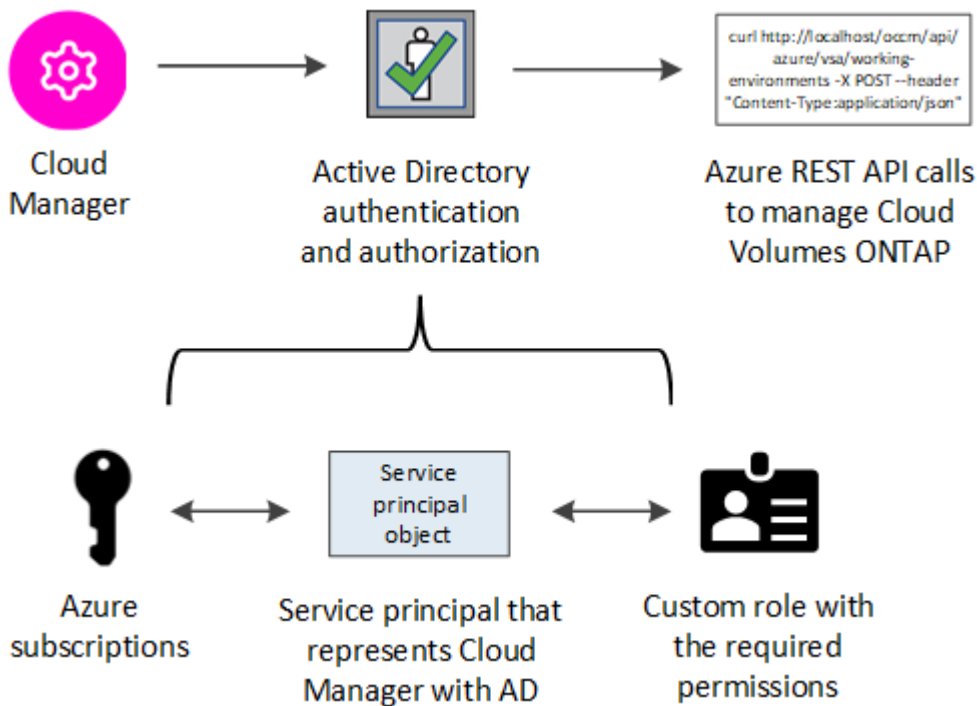
Wenn Sie einen Connector von Cloud Manager bereitstellen, fügt Cloud Manager automatisch das Azure-Konto hinzu, in dem Sie den Connector bereitgestellt haben. Ein erstes Konto wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. ["Weitere Informationen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

Azure-Berechtigungen über einen Service-Principal gewähren

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

Über diese Aufgabe

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



Schritte

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

Erstellen einer Azure Active Directory-Anwendung

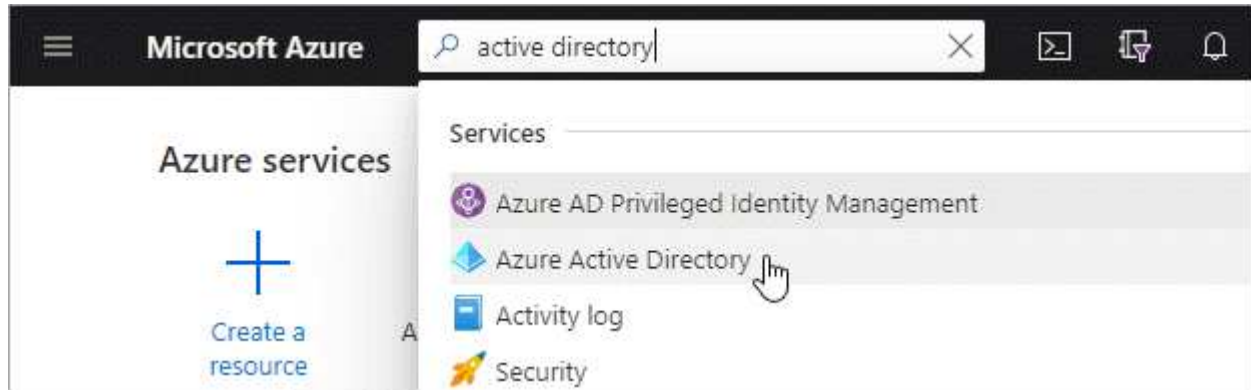
Erstellen einer Azure Active Directory (AD)-Applikation und eines Service-Principal, den Cloud Manager für die rollenbasierte Zugriffssteuerung nutzen kann

Bevor Sie beginnen

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

Schritte

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



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

Ergebnis

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

Anwendung einer Rolle zuweisen

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

Schritte

1. Erstellen einer benutzerdefinierten Rolle:
 - a. Laden Sie die herunter "[Cloud Manager Azure-Richtlinie](#)".
 - b. Ändern Sie die JSON-Datei, indem Sie dem zuweisbaren Bereich Azure-Abonnement-IDs hinzufügen.

Sie sollten die ID für jedes Azure Abonnement hinzufügen, aus dem Benutzer Cloud Volumes ONTAP Systeme erstellen.

Beispiel

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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

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

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

Sie sollten nun über eine benutzerdefinierte Rolle namens *Cloud Manager Operator* verfügen.

2. Applikation der Rolle zuweisen:

- a. Öffnen Sie im Azure-Portal den Service **Abonnements**.
- b. Wählen Sie das Abonnement aus.
- c. Klicken Sie auf **Zugriffskontrolle (IAM) > Hinzufügen > Rollenzuweisung hinzufügen**.
- d. Wählen Sie die Rolle **Cloud Manager Operator** aus.
- e. * Azure AD Benutzer, Gruppe oder Serviceprincipal* ausgewählt lassen.
- f. Suchen Sie nach dem Namen der Anwendung (Sie finden sie nicht in der Liste durch Scrollen).

Add role assignment [X]

Role ⓘ
OnCommand Cloud Manager Operator [v]

Assign access to ⓘ
Azure AD user, group, or service principal [v]

Select ⓘ
test-service-principal [v]

test-service-principal

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

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

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

Windows Azure Service Management-API-Berechtigungen werden hinzugefügt

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

Schritte














1. Klicken Sie im **Azure Active Directory**-Dienst auf **App-Registrierungen** und wählen Sie die Anwendung aus.
2. Klicken Sie auf **API-Berechtigungen > Berechtigung hinzufügen**.
3. Wählen Sie unter **Microsoft APIs Azure Service Management** aus.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint. 		
 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Abrufen der Anwendungs-ID und der Verzeichnis-ID

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

Schritte

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

The screenshot shows the 'Endpoints' page for an application registration in Azure Active Directory. At the top, there are 'Delete' and 'Endpoints' buttons. Below them is a blue banner with an information icon and the text 'Welcome to the new and improved App registrations. Looking to learn...'. The main content area displays the following details:

- Display name : test-service-principal
- Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3
- Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a
- Object ID : b37489a9-379f-49c2-b27c-e630514106a5

The 'Application (client) ID' and 'Directory (tenant) ID' fields are highlighted with a red rectangular box.

Erstellen eines Clientgeheimnisses

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



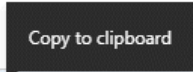
Wenn Sie das Konto zu Cloud Manager hinzufügen, bezieht sich Cloud Manager auf das Kundengeheimnis als Applikationsschlüssel.

Schritte

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

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

Ergebnis

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

Hinzufügen von Azure Zugangsdaten zu Cloud Manager

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

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "[Erfahren Sie, wie](#)".

Schritte

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



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

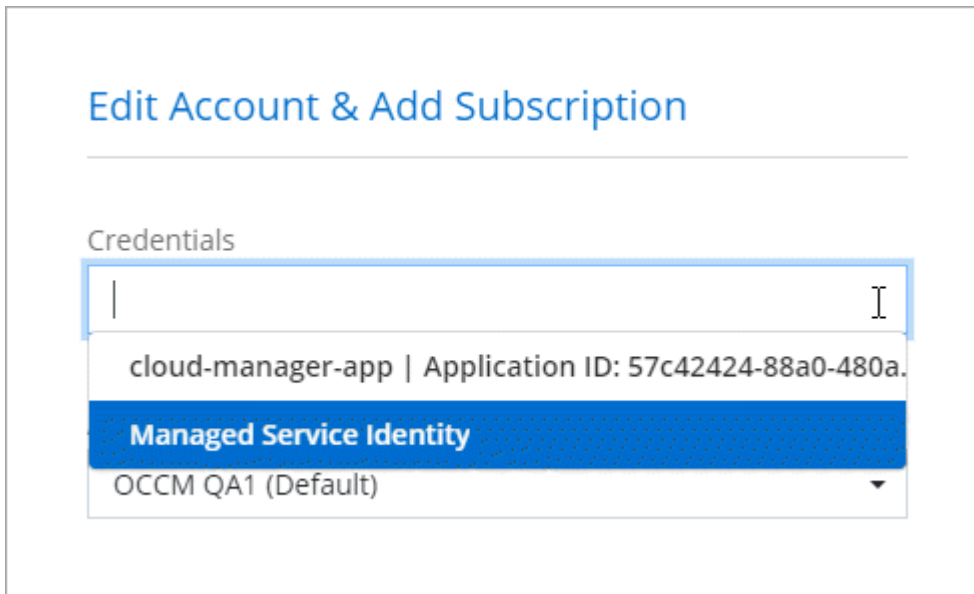
- Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie dann auf **Weiter**.
- Wählen Sie das Pay-as-you-go-Abonnement aus, das Sie mit den Anmeldedaten verknüpfen möchten, oder klicken Sie auf **Abonnement hinzufügen**, wenn Sie noch nicht über ein Abonnement verfügen.

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

- Klicken Sie Auf **Hinzufügen**.

Ergebnis

Auf der Seite Details und Anmeldeinformationen können Sie nun zu verschiedenen Anmeldeinformationen wechseln "[Beim Erstellen einer neuen Arbeitsumgebung](#)":



Verknüpfen eines Azure Marketplace Abonnements mit den Zugangsdaten

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

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

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

Was Sie benötigen

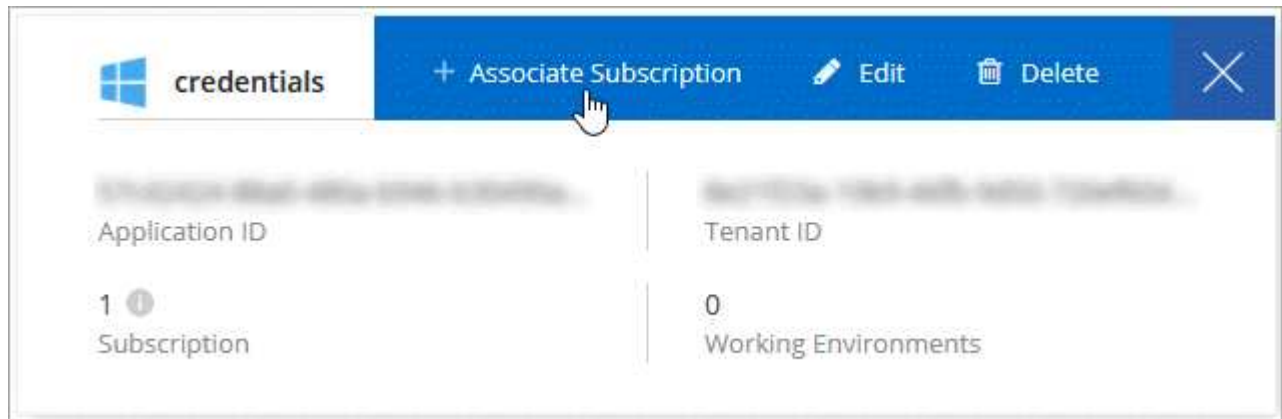
Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "[Erfahren Sie, wie](#)".

Schritte

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

Aktivitätsmenü.

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



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

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

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

Verknüpfen weiterer Azure-Abonnements mit einer gemanagten Identität

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

Über diese Aufgabe

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

Schritte

1. Melden Sie sich beim Azure Portal an.
2. Öffnen Sie den Dienst **Abonnements** und wählen Sie dann das Abonnement aus, in dem Sie Cloud Volumes ONTAP bereitstellen möchten.
3. Klicken Sie auf **Access Control (IAM)**.
 - a. Klicken Sie auf **Hinzufügen > Rollenzuordnung hinzufügen** und fügen Sie dann die Berechtigungen hinzu:
 - Wählen Sie die Rolle **Cloud Manager Operator** aus.



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

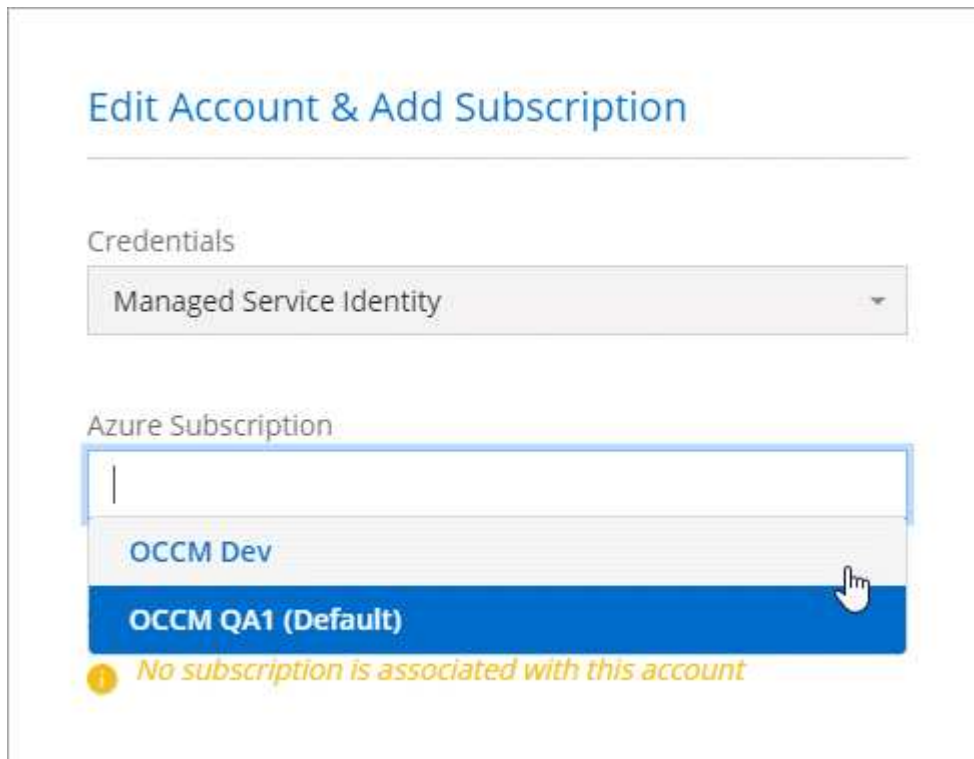
- Weisen Sie einer **virtuellen Maschine** Zugriff zu.

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

4. Wiederholen Sie diese Schritte für weitere Abonnements.

Ergebnis

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



GCP

Google Cloud Projekte, Berechtigungen und Konten

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

Projekt und Berechtigungen für Cloud Manager

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

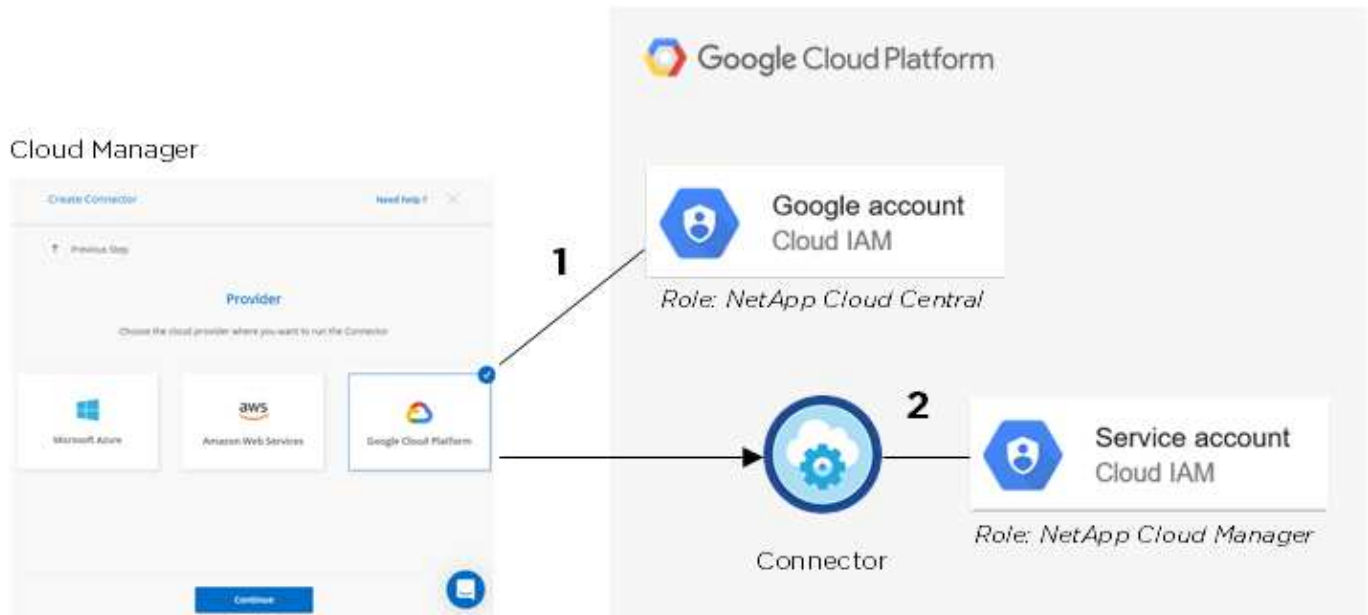
Vor der Bereitstellung eines Connectors direkt aus Cloud Manager müssen zwei Berechtigungssätze vorhanden sein:

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

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

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

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



Projekt für Cloud Volumes ONTAP

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

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

Konto für Daten-Tiering



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

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

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

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

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

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

Verwalten von GCP-Anmeldedaten und -Abonnements für Cloud Manager

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

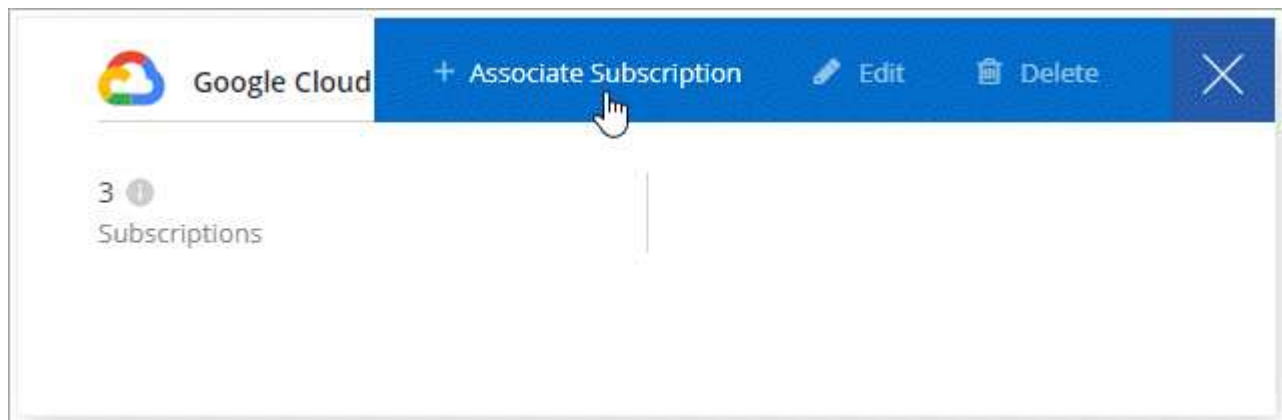
Verknüpfen eines Marketplace-Abonnements mit GCP-Zugangsdaten

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

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

Schritte

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



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

The screenshot shows a configuration interface for Google Cloud. At the top, it says "Google Cloud Project" above a dropdown menu containing "OCCM-Dev". Below that, it says "Subscription" above another dropdown menu containing "GCP subscription for staging". At the bottom left, there is a blue button with a plus sign and the text "Add Subscription".

5. Klicken Sie Auf **Mitarbeiter**.

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

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



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

Einrichten eines Servicekontos und Zugriffsschlüssel für Google Cloud Storage

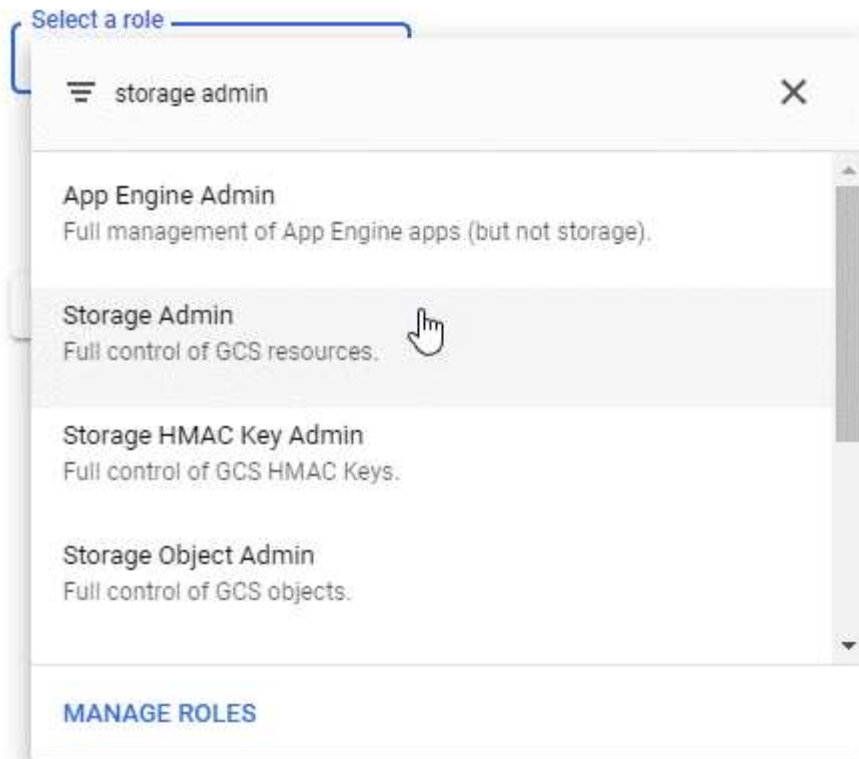
Mithilfe eines Service-Kontos kann Cloud Manager Cloud Storage-Buckets authentifizieren und auf sie zugreifen, die für Daten-Tiering verwendet werden. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Öffnen Sie die GCP IAM-Konsole und "[Erstellen Sie ein Dienstkonto mit der Rolle Storage Admin](#)".

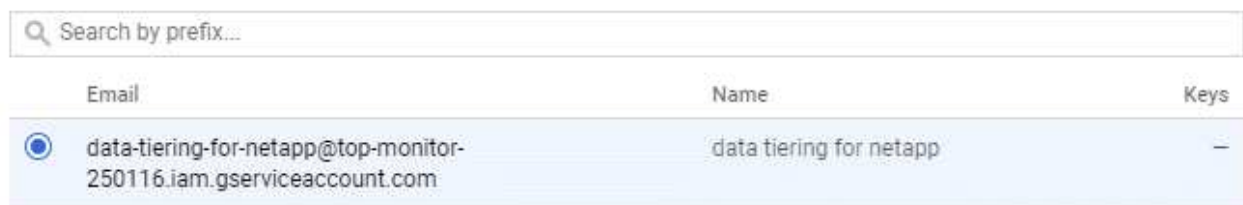
Service account permissions (optional)

Grant this service account access to My Project 99247 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)



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

Select a service account



[CANCEL](#) [CREATE KEY](#) | [CREATE NEW ACCOUNT](#)

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

9. Kopieren Sie den Zugriffsschlüssel und den Schlüssel.

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

Hinzufügen eines GCP-Kontos zu Cloud Manager

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

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. "[Erfahren Sie, wie](#)".

Schritte

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



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

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

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

Was kommt als Nächstes?

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

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

Hinzufügen von NetApp Support Site Konten zu Cloud Manager

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

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

📺 | <https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg>

Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. ["Erfahren Sie, wie"](#).

Schritte

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



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

Was kommt als Nächstes?

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

- ["Starten von Cloud Volumes ONTAP in AWS"](#)
- ["Starten von Cloud Volumes ONTAP in Azure"](#)
- ["Registrieren von Pay-as-you-go-Systemen"](#)
- ["Cloud Manager managt Lizenzdateien"](#)

Copyright-Informationen

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

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

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

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.