Cloud provider credentials

Cloud Manager

NetApp
June 15, 2020

Table of Contents

Cloud provider credentials . . . 1

AWS credentials and permissions . . . 1

Azure credentials and permissions . . . 3

Google Cloud projects, permissions, and accounts . . . 5

Cloud provider credentials

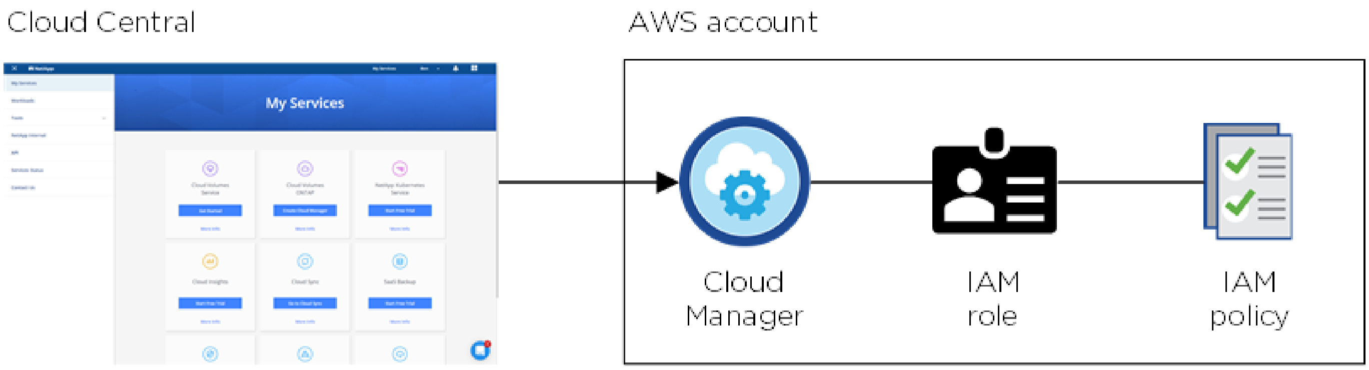
AWS credentials and permissions

Cloud Manager enables you to choose the AWS credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

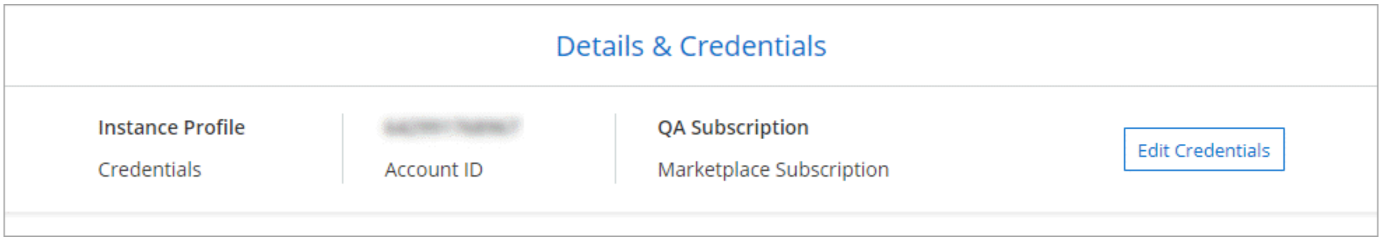
Initial AWS credentials

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an AWS account that has permissions to launch the Cloud Manager instance. The required permissions are listed in the NetApp Cloud Central policy for AWS.

When Cloud Central launches the Cloud Manager instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP in that AWS account. Review how Cloud Manager uses the permissions.



Cloud Manager selects these AWS credentials by default when you create a new working environment:

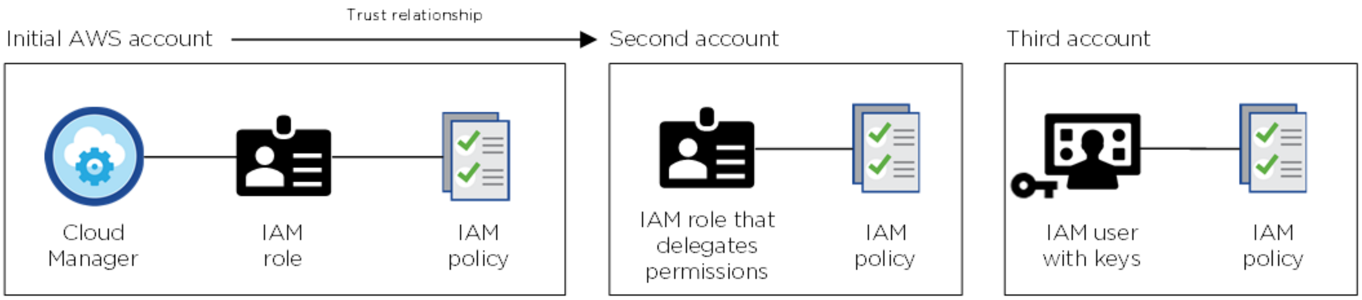


Details & Credentials

Instance Profile	[redacted]	QA Subscription	Edit Credentials
Credentials	Account ID	Marketplace Subscription	

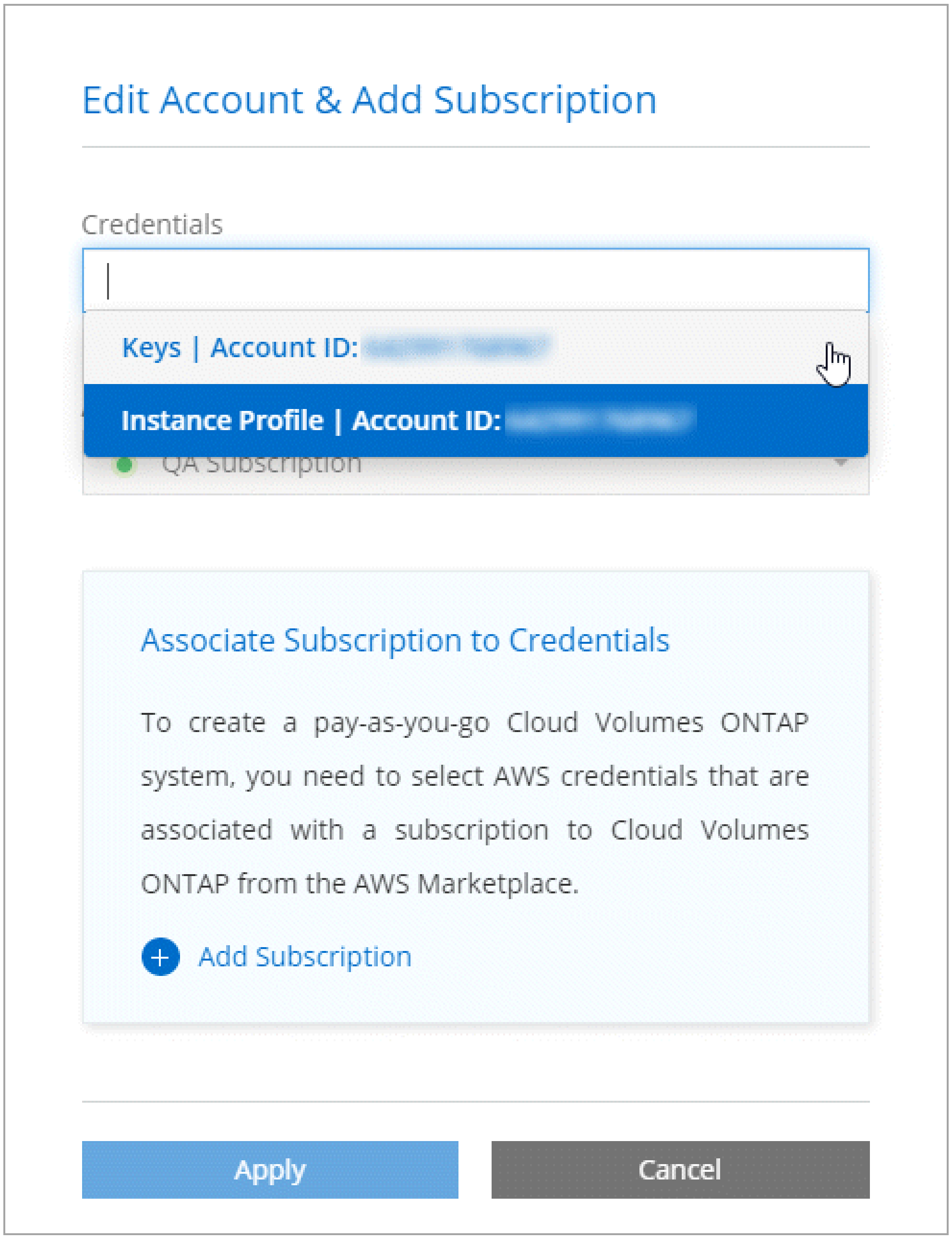
Additional AWS credentials

If you want to launch Cloud Volumes ONTAP in different AWS accounts, then you can either provide AWS keys for an IAM user or the ARN of a role in a trusted account. The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:



You would then add the account credentials to Cloud Manager by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

After you add another set of credentials, you can switch to them when creating a new working environment:



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.

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method from NetApp Cloud Central. You can also deploy Cloud Manager in AWS from the AWS Marketplace and you can install Cloud Manager on-premises.

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the IAM role, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up an IAM role for the Cloud Manager system, but you can provide permissions just like you would for additional AWS accounts.

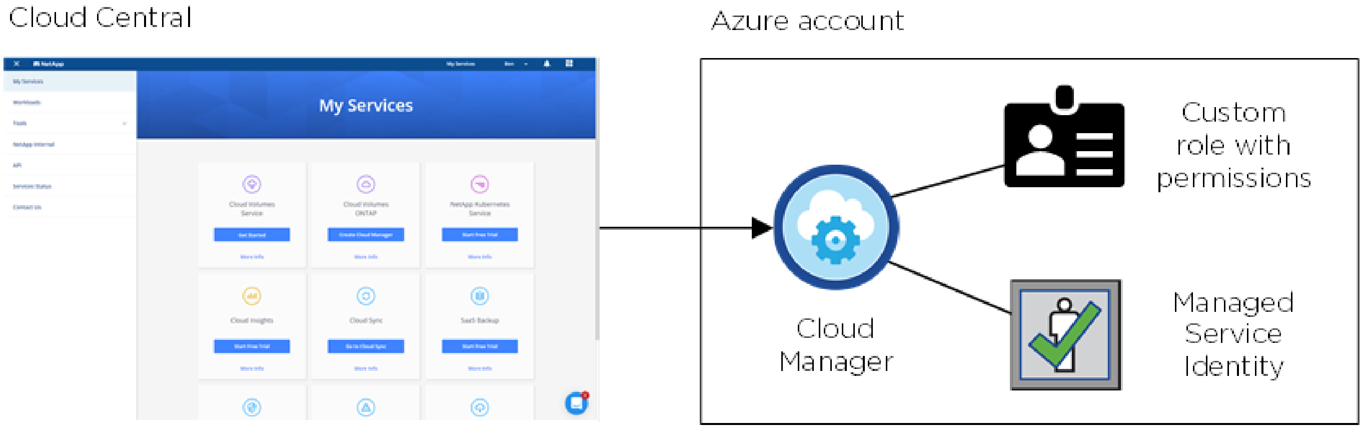
Azure credentials and permissions

Cloud Manager enables you to choose the Azure credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

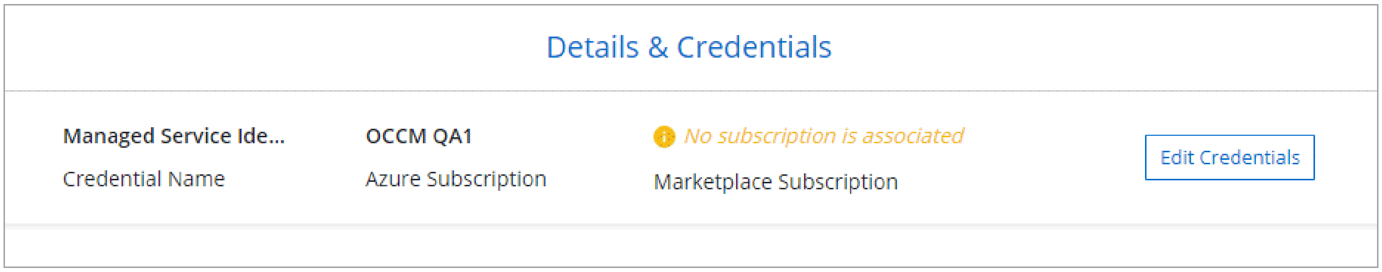
Initial Azure credentials

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an Azure account that has permissions to deploy the Cloud Manager virtual machine. The required permissions are listed in the NetApp Cloud Central policy for Azure.

When Cloud Central deploys the Cloud Manager virtual machine in Azure, it enables a system-assigned managed identity on the Cloud Manager virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP in that Azure subscription. Review how Cloud Manager uses the permissions.



Cloud Manager selects these Azure credentials by default when you create a new working environment:


Details & Credentials

Managed Service Ide...
Credential Name

OCCM QA1
Azure Subscription

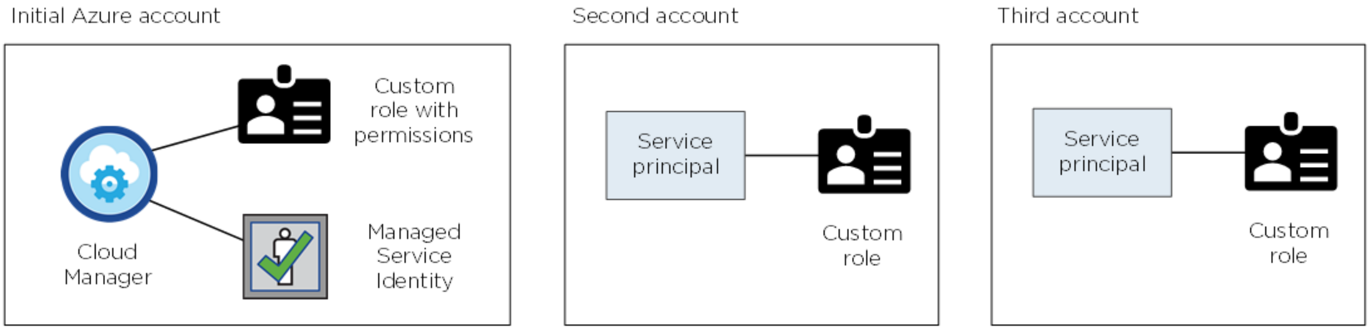
No subscription is associated
Marketplace Subscription

Additional Azure subscriptions for managed identity

The managed identity is associated with the subscription in which you launched Cloud Manager. If you want to select a different Azure subscription, then you need to associate the managed identity with those subscriptions.

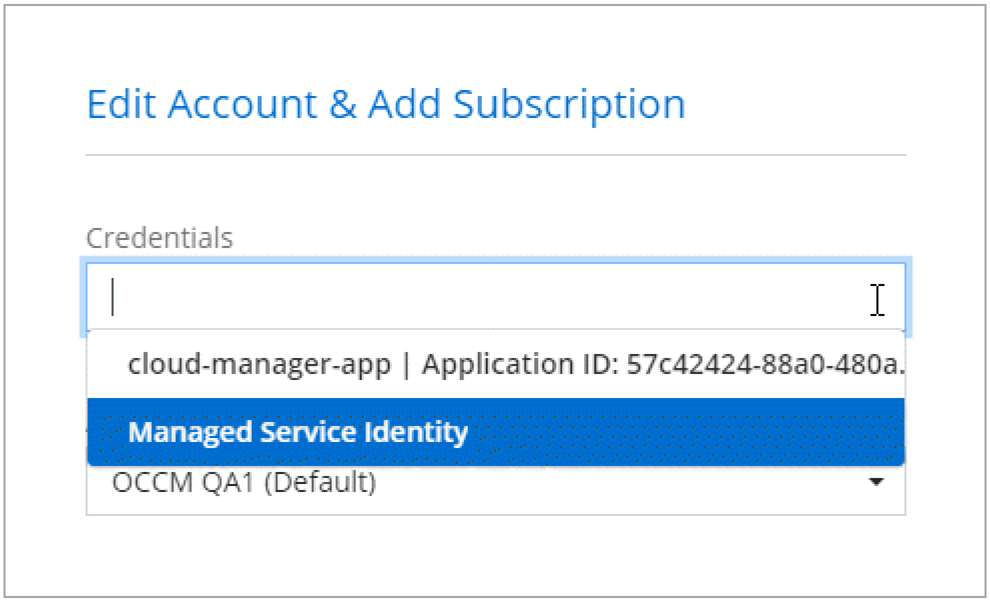
Additional Azure credentials

If you want to deploy Cloud Volumes ONTAP using different Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Azure Active Directory for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom role that provides permissions:



You would then add the account credentials to Cloud Manager by providing details about the AD service principal.

After you add another set of credentials, you can switch to them when creating a new working environment:



Edit Account & Add Subscription

Credentials

cloud-manager-app | Application ID: 57c42424-88a0-480a.

Managed Service Identity

OCCM QA1 (Default)

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method from NetApp Cloud Central. You can also deploy Cloud Manager in Azure from the Azure Marketplace, and you can install Cloud Manager on-premises.

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the managed identity for Cloud Manager, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Cloud Manager system, but you can provide permissions just like you would for additional accounts.

Google Cloud projects, permissions, and accounts

A service account provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP systems in the same project as Cloud Manager, or in different projects. Google Cloud accounts that you add to Cloud Manager are used to enable data tiering.

Project and permissions for Cloud Manager

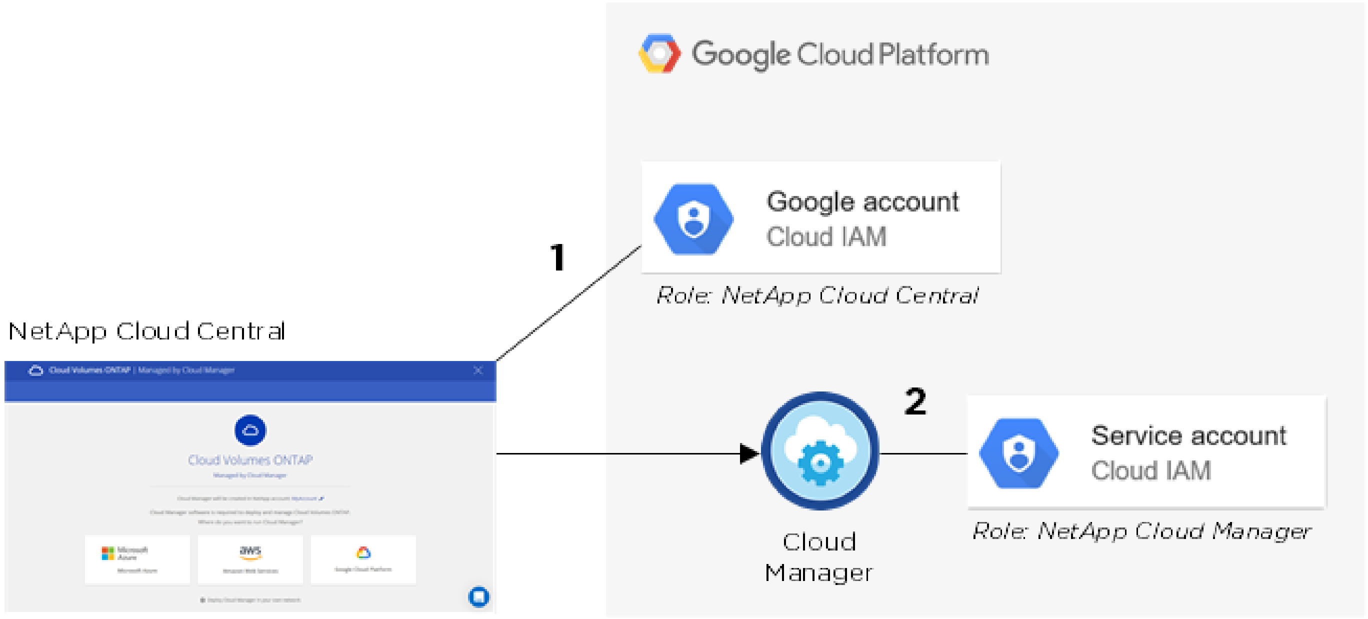
Before you can deploy Cloud Volumes ONTAP in Google Cloud, you must first deploy Cloud Manager in a Google Cloud project. Cloud Manager can't be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy Cloud Manager from NetApp Cloud Central:

1. You need to deploy Cloud Manager using a Google account that has permissions to launch the Cloud Manager VM instance from Cloud Central.
2. When deploying Cloud Manager, you are prompted to select a service account for the VM instance. Cloud Manager gets permissions from the service account to create and manage Cloud Volumes ONTAP systems on your behalf. Permissions are provided by attaching a custom role to the service account.

We have set up two YAML files that include the required permissions for the user and the service account. Learn how to use the YAML files to set up permissions.

The following image depicts the permission requirements described in numbers 1 and 2 above:



Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as Cloud Manager, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Cloud Manager service account and role to that project.

- Learn how to set up the Cloud Manager service account (see step 2).
- Learn how to deploy Cloud Volumes ONTAP in GCP and select a project.

Account for data tiering

Cloud Manager requires a GCP account for Cloud Volumes ONTAP 9.6, but not for 9.7 and later. If you want to use data tiering with Cloud Volumes ONTAP 9.7, then follow step 3 in Getting started with Cloud Volumes ONTAP in Google Cloud Platform.

Adding a Google Cloud account to Cloud Manager is required to enable data tiering on a Cloud Volumes ONTAP 9.6 system. Data tiering automatically tiers cold data to low-cost object storage, enabling you to reclaim space on your primary storage and shrink secondary storage.

When you add the account, you need to provide Cloud Manager with a storage access key for a service account that has Storage Admin permissions. Cloud Manager uses the access keys to set up and manage a Cloud Storage bucket for data tiering.

After you add a Google Cloud account, you can then enable data tiering on individual volumes when you create, modify, or replicate them.

- Learn how to set up and add GCP accounts to Cloud Manager.
- Learn how to tier inactive data to low-cost object storage.

Copyright Information

Trademark Information