∏ NetApp

Manage cloud provider credentials

Cloud Manager

NetApp
March 01, 2022

Table of Contents

Manage cloud provider credentials

AWS

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 a Connector from Cloud Manager, you need to use an AWS account that has permissions to launch the Connector instance. The required permissions are listed in the Connector deployment policy for AWS.

When Cloud Manager launches the Connector 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 manage resources and processes within 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 for Cloud Volumes ONTAP:

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:

Instance Profile | Account ID:

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

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from Cloud Manager. You can also deploy a Connector in AWS from the AWS Marketplace and you can install the Connector 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.

How can I securely rotate my AWS credentials?

As described above, Cloud Manager enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys.

With the first two options, Cloud Manager uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice—it's automatic and it's secure.

If you provide Cloud Manager with AWS access keys, you should rotate the keys by updating them in Cloud Manager at a regular interval. This is a completely manual process.

Manage AWS credentials and subscriptions for Cloud Manager

Add and manage AWS credentials so that Cloud Manager has the permissions that it needs to deploy and manage cloud resources in your AWS accounts. If you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

Overview

You can add AWS credentials to an existing Connector or directly to Cloud Manager:

- Add AWS credentials to an existing Connector

  Adding new AWS credentials to an existing Connector enables you to deploy Cloud Volumes ONTAP in another AWS account using the same Connector. Learn how to add AWS credentials to a Connector.

- Add AWS credentials directly to Cloud Manager

  Adding new AWS credentials to Cloud Manager enable you to create an FSx for ONTAP working environment. Learn how to add AWS credentials to Cloud Manager.

How to rotate credentials

Cloud Manager enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys. Learn more about AWS credentials and permissions.

With the first two options, Cloud Manager uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice because it's automatic and it's secure.

If you provide Cloud Manager with AWS access keys, you should rotate the keys by updating them in Cloud Manager at a regular interval. This is a completely manual process.

Add credentials to a Connector

Add AWS credentials to enable the Connector to deploy and manage Cloud Volumes ONTAP in other AWS accounts. You can either provide the ARN of an IAM role in another account or provide AWS access keys.

Grant permissions

Before you add additional AWS credentials to a Connector, you need to provide the required permissions. The permissions enable Cloud Manager to manage resources and processes within that AWS account. How you provide the permissions depends on whether you want to provide Cloud Manager with the ARN of a role in a trusted account or AWS keys.

> ⓘ When you deployed a Connector from Cloud Manager, Cloud Manager automatically added AWS credentials for the account in which you deployed the Connector. This initial account is not added if you manually installed the Connector software on an existing system. Learn about AWS credentials and permissions.

Choices

- Grant permissions by assuming an IAM role in another account
- Grant permissions by providing AWS keys

Grant permissions by assuming an IAM role in another account

You can set up a trust relationship between the source AWS account in which you deployed the Connector instance and other AWS accounts by using IAM roles. You would then provide Cloud Manager with the ARN of the IAM roles from the trusted accounts.

Steps

1. Go to the IAM console in the target account where you want to deploy Cloud Volumes ONTAP.

2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the account where the Connector instance resides.
   - Create a policy using the Cloud Manager IAM policy, which is available from the Cloud Manager Policies page.

3. Copy the Role ARN of the IAM role so that you can paste it in Cloud Manager later on.

Result

The account now has the required permissions. You can now add the credentials to a Connector.

Grant permissions by providing AWS keys

If you want to provide Cloud Manager with AWS keys for an IAM user, then you need to grant the required permissions to that user. The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use.

Steps

1. Download the Cloud Manager IAM policy from the Cloud Manager Policies page.

2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.

   AWS Documentation: Creating IAM Policies

3. Attach the policy to an IAM role or an IAM user.
   - AWS Documentation: Creating IAM Roles
   - AWS Documentation: Adding and Removing IAM Policies

Result

The account now has the required permissions. You can now add the credentials to a Connector.

Add the credentials

After you provide an AWS account with the required permissions, you can add the credentials for that account to an existing Connector. This enables you to launch Cloud Volumes ONTAP systems in that account using the same Connector.

Before you get started

If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to Cloud Manager.

Steps

1. Ensure that the correct Connector is currently selected in Cloud Manager.

2. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

3. Click **Add Credentials** and follow the steps in the wizard.

   a. **Credentials Location**: Select **Amazon Web Services > Connector**.

   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of a trusted IAM role, or enter an AWS access key and secret key.

   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

   To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or with an annual contract, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

   d. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:

Add credentials to Cloud Manager

Add AWS credentials to Cloud Manager by providing the ARN of an IAM role that gives Cloud Manager the permissions needed to create an FSx for ONTAP working environment.

Set up the IAM role

Set up an IAM role that enables the Cloud Manager SaaS to assume the role.

Steps

1. Go to the IAM console in the target account.

2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.

   - Select **Another AWS account** and enter the ID of the Cloud Manager SaaS: 733004784675

   - Create a policy that includes the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "fsx:*",
                "ec2:Describe*",
                "ec2:CreateTags",
                "kms:Describe*",
                "kms:List*",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Copy the Role ARN of the IAM role so that you can paste it in Cloud Manager in the next step.

Result

The IAM role now has the required permissions. You can now add it to Cloud Manager.

Add the credentials

After you provide the IAM role with the required permissions, add the role ARN to Cloud Manager.

Before you get started

If you just created the IAM role, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to Cloud Manager.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click **Add Credentials** and follow the steps in the wizard.

   a. **Credentials Location**: Select **Amazon Web Services > Cloud Manager**.

   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of the IAM role.

   c. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now use the credentials when creating an FSx for ONTAP working environment.

Associate an AWS subscription

After you add your AWS credentials to Cloud Manager, you can associate an AWS Marketplace subscription with those credentials. The subscription enables you to pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or using an annual contract, and to use other NetApp cloud services.

There are two scenarios in which you might associate an AWS Marketplace subscription after you've already added the credentials to Cloud Manager:

- You didn't associate a subscription when you initially added the credentials to Cloud Manager.
- You want to replace an existing AWS Marketplace subscription with a new subscription.

What you'll need

You need to create a Connector before you can change Cloud Manager settings. Learn how to create a Connector.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Associate Subscription**.
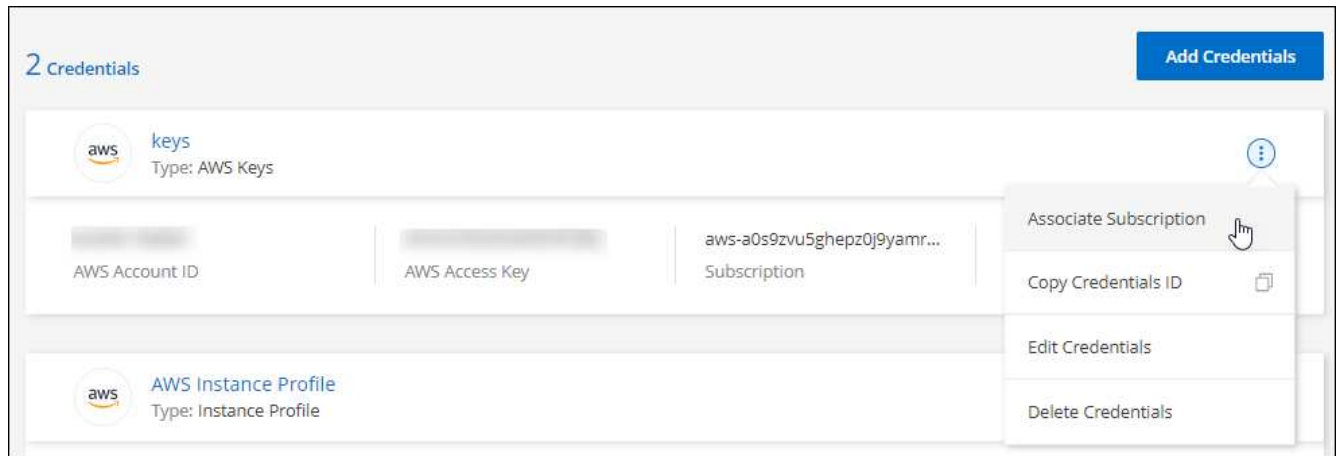
3. Select an existing subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

   ► https://docs.netapp.com/us-en/occm//media/video_subscribing_aws.mp4 *(video)*

Edit credentials

Edit your AWS credentials in Cloud Manager by changing the account type (AWS keys or assume role), by editing the name, or by updating the credentials themselves (the keys or the role ARN).

> You can't edit the credentials for an instance profile that is associated with a Connector instance.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then click **Apply**.

Deleting credentials

If you no longer need a set of credentials, you can delete them from Cloud Manager. You can only delete credentials that aren't associated with a working environment.

> 💡 You can't delete the credentials for an instance profile that is associated with a Connector instance.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click the action menu for a set of credentials and then select **Delete Credentials**.

3. Click **Delete** to confirm.

Azure

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 a Connector from Cloud Manager, you need to use an Azure account or service principal that has permissions to deploy the Connector virtual machine. The required permissions are listed in the Connector deployment policy for Azure.

When Cloud Manager deploys the Connector virtual machine in Azure, it enables a system-assigned managed identity on virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides Cloud Manager with permissions to manage resources and processes within 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 for Cloud Volumes ONTAP:

Additional Azure subscriptions for a managed identity

The managed identity is associated with the subscription in which you launched the Connector. 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:
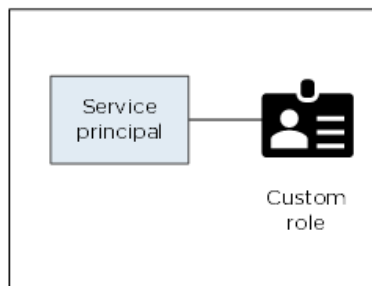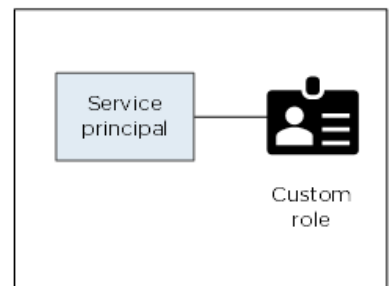
You would then add the account credentials to Cloud Manager by providing details about the AD service principal.

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

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from NetApp Cloud Central. You can also deploy a Connector in Azure from the Azure Marketplace, and you can install the Connector 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 the Connector, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Connector, but you can provide permissions just like you would for additional accounts by using a service principal.

Managing Azure credentials and subscriptions for Cloud Manager

When you create a Cloud Volumes ONTAP system, you need to select the Azure credentials to use with that system. You also need to choose a Marketplace subscription, if you're using pay-as-you-go licensing. Follow the steps on this page if you need to use multiple Azure credentials or multiple Azure Marketplace subscriptions for Cloud Volumes ONTAP.

There are two ways to add additional Azure subscriptions and credentials in Cloud Manager.

1. Associate additional Azure subscriptions with the Azure managed identity.
2. If you want to deploy Cloud Volumes ONTAP using different Azure credentials, grant Azure permissions using a service principal and add its credentials to Cloud Manager.

Associating additional Azure subscriptions with a managed identity

Cloud Manager enables you to choose the Azure credentials and Azure subscription in which you want to deploy Cloud Volumes ONTAP. You can't select a different Azure subscription for the managed identity profile unless you associate the managed identity with those subscriptions.

About this task

A managed identity is the initial Azure account when you deploy a Connector from Cloud Manager. When you deployed the Connector, Cloud Manager created the Cloud Manager Operator role and assigned it to the Connector virtual machine.

Steps

1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.
3. Click **Access control (IAM)**.
    a. Click **Add** > **Add role assignment** and then add the permissions:
        ▪ Select the **Cloud Manager Operator** role.

        ⓘ Cloud Manager Operator is the default name provided in the Cloud Manager policy. If you chose a different name for the role, then select that name instead.

- Assign access to a **Virtual Machine**.

- Select the subscription in which the Connector virtual machine was created.

- Select the Connector virtual machine.

- Click **Save**.

4. Repeat these steps for additional subscriptions.

Result

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions for the managed identity profile.

Adding additional Azure credentials to Cloud Manager

When you deploy a Connector from Cloud Manager, Cloud Manager enables a system-assigned managed identity on the virtual machine that has the required permissions. Cloud Manager selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP.

An initial set of credentials isn't added if you manually installed the Connector software on an existing system. Learn about Azure credentials and permissions.

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. You can then add the new credentials to Cloud Manager.

Granting Azure permissions using a service principal

Cloud Manager needs permissions to perform actions in Azure. You can grant the required permissions to an Azure account by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that Cloud Manager needs.

About this task

The following image depicts how Cloud Manager obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents Cloud Manager in Azure Active Directory and is assigned to a custom role that allows the required permissions.
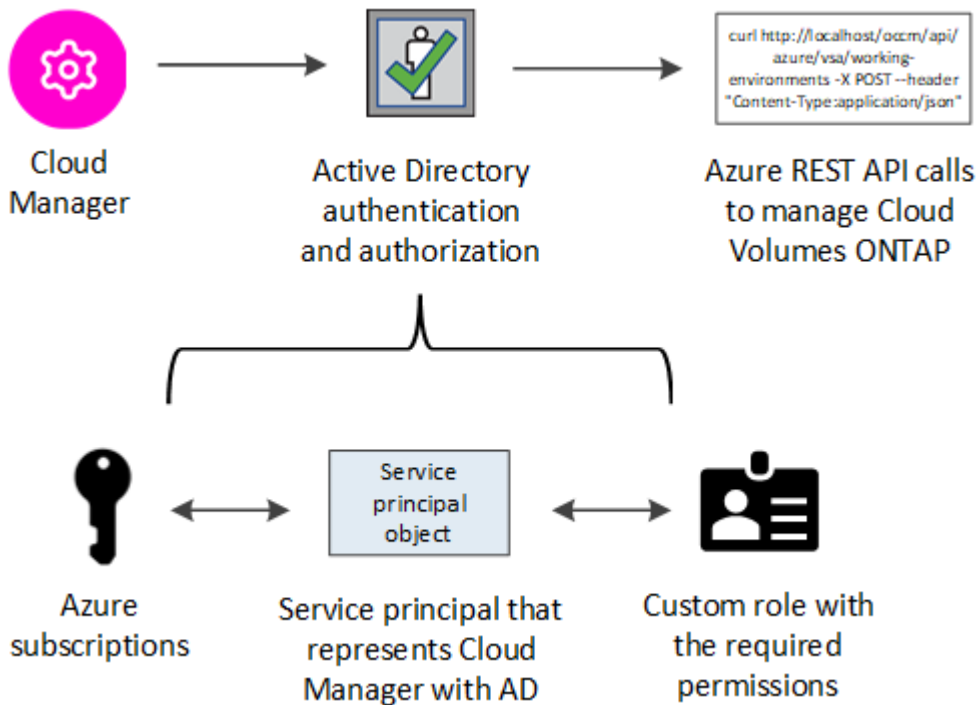
Steps

1. Create an Azure Active Directory application.
2. Assign the application to a role.
3. Add Windows Azure Service Management API permissions.
4. Get the application ID and directory ID.
5. Create a client secret.

Creating an Azure Active Directory application

Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Required permissions.

Steps

1. From the Azure portal, open the **Azure Active Directory** service.

2. In the menu, click **App registrations**.

3. Click **New registration**.

4. Specify details about the application:

   ◦ **Name**: Enter a name for the application.

   ◦ **Account type**: Select an account type (any will work with Cloud Manager).

   ◦ **Redirect URI**: You can leave this field blank.

5. Click **Register**.

Result

You've created the AD application and service principal.

Assigning the application to a role

You must bind the service principal to one or more Azure subscriptions and assign it the custom "OnCommand Cloud Manager Operator" role so Cloud Manager has permissions in Azure.

Steps

1. Download the Cloud Manager Azure policy.

    Right-click the link and click **Save link as…** to download the file.

2. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

   You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

   Example

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

3. Use the JSON file to create a custom role in Azure.

   The following steps describe how to create the role by using Bash in Azure Cloud Shell.

a. Start Azure Cloud Shell and choose the Bash environment.

b. Upload the JSON file.

c. Enter the following Azure CLI command:

```
az role definition create --role-definition
Policy_for_cloud_Manager_Azure_3.9.8.json
```

You should now have a custom role called *Cloud Manager Operator*.

4. Assign the application to the role:

   a. From the Azure portal, open the **Subscriptions** service.

   b. Select the subscription.

   c. Click **Access control (IAM) > Add > Add role assignment**.

   d. In the **Role** tab, select the **Cloud Manager Operator** role and click **Next**.

   e. In the **Members** tab, complete the following steps:

      ▪ Keep **User, group, or service principal** selected.

      ▪ Click **Select members**.

- Search for the name of the application.

  Here's an example:

- Select the application and click **Select**.
- Click **Next**.

f. Click **Review + assign**.

The service principal now has the required Azure permissions to deploy the Connector.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. Cloud Manager enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

Adding Windows Azure Service Management API permissions

The service principal must have "Windows Azure Service Management API" permissions.

Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

4. Click **Access Azure Service Management as organization users** and then click **Add permissions**.

Getting the application ID and directory ID

When you add the Azure account to Cloud Manager, you need to provide the application (client) ID and the directory (tenant) ID for the application. Cloud Manager uses the IDs to programmatically sign in.

Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.

Creating a client secret

You need to create a client secret and then provide Cloud Manager with the value of the secret so Cloud Manager can use it to authenticate with Azure AD.

Steps

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.

4. Provide a description of the secret and a duration.

5. Click **Add**.

6. Copy the value of the client secret.

Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in Cloud Manager when you add an Azure account.

Adding the credentials to Cloud Manager

After you provide an Azure account with the required permissions, you can add the credentials for that account to Cloud Manager. Completing this step enables you to launch Cloud Volumes ONTAP using different Azure credentials.

Before you get started

If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to Cloud Manager.

What you'll need

You need to create a Connector before you can change Cloud Manager settings. Learn how.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click **Add Credentials** and follow the steps in the wizard.

   a. **Credentials Location**: Select **Microsoft Azure > Connector**.

   b. **Define Credentials**: Enter information about the Azure Active Directory service principal that grants the required permissions:

      ▪ Application (client) ID: See Getting the application ID and directory ID.

      ▪ Directory (tenant) ID: See Getting the application ID and directory ID.

      ▪ Client Secret: See Creating a client secret.

   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO), these Azure credentials must be associated with a subscription from the Azure Marketplace.

d. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now switch to different set of credentials from the Details and Credentials page when creating a new working environment:

Manage existing credentials

Manage the Azure credentials that you've already added to Cloud Manager by associating a Marketplace subscription, editing credentials, and deleting them.

Associating an Azure Marketplace subscription to credentials

After you add your Azure credentials to Cloud Manager, you can associate an Azure Marketplace subscription to those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

There are two scenarios in which you might associate an Azure Marketplace subscription after you've already added the credentials to Cloud Manager:

- You didn't associate a subscription when you initially added the credentials to Cloud Manager.
- You want to replace an existing Azure Marketplace subscription with a new subscription.

What you'll need

You need to create a Connector before you can change Cloud Manager settings. Learn how.

Steps

1. Select an existing subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

   ► https://docs.netapp.com/us-en/occm//media/video_subscribing_aws.mp4 *(video)*

2. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

3. Click the action menu for a set of credentials and then select **Associate Subscription**.

4. Select a subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

The following video starts from the context of the working environment wizard, but shows you the same workflow after you click **Add Subscription**:

► https://docs.netapp.com/us-en/occm//media/video_subscribing_azure.mp4 *(video)*

Editing credentials

Edit your Azure credentials in Cloud Manager by modifying the details about your Azure service credentials. For example, you might need to update the client secret if a new secret was created for the service principal application.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click the action menu for a set of credentials and then select **Edit Credentials**.

3. Make the required changes and then click **Apply**.

Deleting credentials

If you no longer need a set of credentials, you can delete them from Cloud Manager. You can only delete credentials that aren't associated with a working environment.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click the action menu for a set of credentials and then select **Delete Credentials**.

3. Click **Delete** to confirm.

GCP

Google Cloud projects, permissions, and accounts

A service account provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP systems that are in the same project as the Connector, or in

different projects.

Project and permissions for Cloud Manager

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

Two sets of permissions must be in place before you deploy a Connector directly from Cloud Manager:

1. You need to deploy a Connector using a Google account that has permissions to launch the Connector VM instance from Cloud Manager.

2. When deploying the Connector, 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:
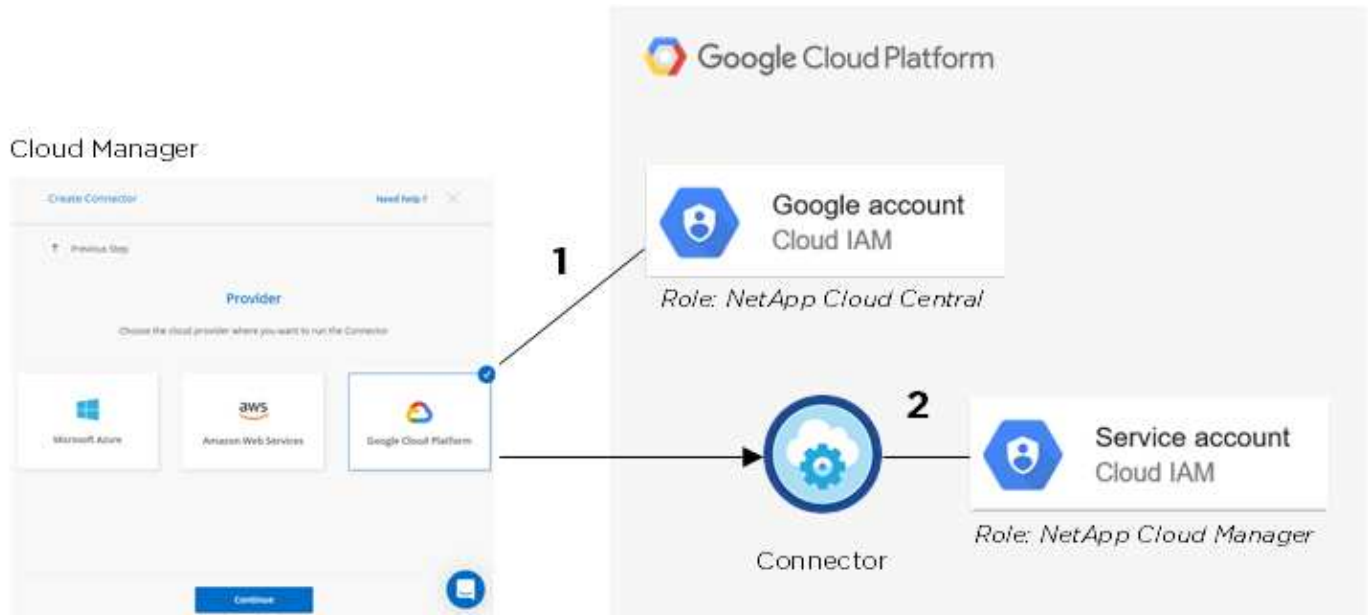
Project for Cloud Volumes ONTAP

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

- Learn how to set up 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 or later, then follow step 4 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.

Managing GCP credentials and subscriptions for Cloud Manager

You can manage two types of Google Cloud Platform credentials from Cloud Manager: the credentials that are associated with the Connector VM instance and storage access keys used with a Cloud Volumes ONTAP 9.6 system for data tiering.

Associating a Marketplace subscription with GCP credentials

When you deploy a Connector in GCP, Cloud Manager creates a default set of credentials that are associated with the Connector VM instance. These are the credentials that Cloud Manager uses to deploy Cloud Volumes ONTAP.

At any time, you can change the Marketplace subscription that's associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click the action menu for a set of credentials and then select **Associate Subscription**.
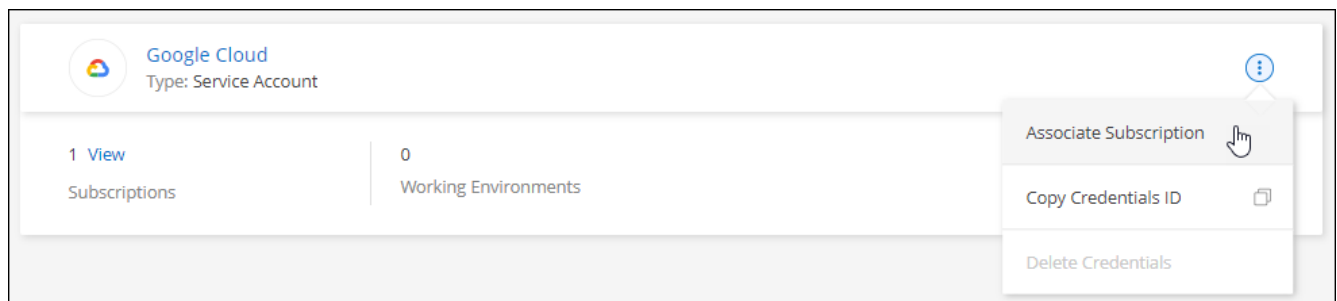
3. Select a Google Cloud project and subscription from the down-down list.

4. Click **Associate**.

5. If you don't already have a subscription, click **Add Subscription** and follow the steps to create a new subscription below.

> ⓘ Before you complete the following steps, ensure that you have both Billing Admin privileges in your Google Cloud account as well as a NetApp Cloud Central login.

6. Reivew the subscription steps and click **Continue**.

Add Subscription

Subscription Steps:

(1) Cloud Manager
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.

(2) Google Cloud Marketplace
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.

(3) Cloud Central
Save your subscription.

(4) Cloud Manager
Associate the Marketplace subscription with your Google Cloud project.

▶ View video instructions

[Continue] [Cancel]

7. After you're redirected to the NetApp Cloud Manager page on the Google Cloud Marketplace, ensure that the correct project is selected at the top navigation menu.

8. Click **Subscribe**.

9. Select the appropriate billing account and agree to the terms and conditions.

2. Purchase details

Select a billing account *

Secondary_Billing_Account ▼

3. Terms

Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

Additional terms

☑ I understand this subscription will be automatically renewed at the end of the current term.

☑ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.

☑ By deploying the software or accessing the service you are agreeing to comply with the End User License Agreement ⤴, GCP Marketplace Terms of Service, and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.

By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ❓

Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. Click **Subscribe**.

    This step sends your transfer request to NetApp.

11. On the pop-up dialog box, click **Register with NetApp, Inc.** to be redirected to NetApp Cloud Central.

Your order request has been sent to NetApp, Inc.

Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

VIEW ORDERS   REGISTER WITH NETAPP, INC.

> ⓘ This step must be completed to link the GCP subscription to your NetApp account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to NetApp Cloud Central.

12. After you're redirected to Cloud Central, log in to NetApp Cloud Central or sign up, and then click **Done** to proceed.

The GCP subscription will be linked to all NetApp accounts that your user login is associated with.

Subscription Assignment

✔ Your subscription to Cloud Manager / Cloud Volumes ONTAP from GCP Marketplace was created successfully!

Done

> ⓘ If someone from your organization has already subscribed to the NetApp Cloud Manager subscription from your billing account, then you will be redirected to the Cloud Volumes ONTAP page on NetApp Cloud Central instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

13. Once this process is complete, navigate back to the Credentials page in Cloud Manager and select this new subscription.

Troubleshooting the Marketplace subscription process

Sometimes subscribing to Cloud Volumes ONTAP through the Google Cloud Marketplace can become fragmented due to incorrect permissions or accidentally not following the redirection to NetApp Cloud Central. If this happens, use the following steps to complete the subscription process.

Steps

1. Navigate to the NetApp Cloud Manager page on the Google Cloud Marketplace to check on the state of the order. If the page states **Manage on Provider**, scroll down and click **Manage Orders**.

   a. If the order shows a green check mark and this is unexpected, somebody else from the organization using the same billing account might already be subscribed. If this is unexpected or you require the details of this subscription, contact your NetApp sales team.

   b. If the order shows a clock and **Pending** status, go back to the marketplace page and choose **Manage on Provider** to complete the process as documented above.

Setting up and adding GCP accounts for data tiering with Cloud Volumes ONTAP 9.6

If you want to enable a Cloud Volumes ONTAP 9.6 system for data tiering, 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.

> If you want to use data tiering with Cloud Volumes ONTAP 9.7 or later, then follow step 4 in Getting started with Cloud Volumes ONTAP in Google Cloud Platform.

Setting up a service account and access keys for Google Cloud Storage

A service account enables Cloud Manager to authenticate and access Cloud Storage buckets used for data tiering. The keys are required so that Google Cloud Storage knows who is making the request.

Steps

1. Open the GCP IAM console and create a service account that has the Storage Admin role.

2. Go to GCP Storage Settings.

3. If you're prompted, select a project.

4. Click the **Interoperability** tab.

5. If you haven't already done so, click **Enable interoperability access**.

6. Under **Access keys for service accounts**, click **Create a key for a service account**.

7. Select the service account that you created in step 1.

Select a service account

	Email	Name	Keys
⦿	data-tiering-for-netapp@top-monitor-250116.iam.gserviceaccount.com	data tiering for netapp	—

CANCEL   CREATE KEY | CREATE NEW ACCOUNT

8. Click **Create Key**.

9. Copy the access key and secret.

You'll need to enter this information in Cloud Manager when you add the GCP account for data tiering.

Adding a GCP account to Cloud Manager

Now that you have an access key for a service account, you can add it to Cloud Manager.

What you'll need

You need to create a Connector before you can change Cloud Manager settings. Learn how.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

Account MyAccount ⌄	Workspace Test ⌄	Connector Connector1 ⌄	🔔 ⚙ ⑦ ⑧

2. Click **Add Credentials** and select **Google Cloud**.

3. Enter the access key and secret for the service account.

The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering.

4. Confirm that the policy requirements have been met and then click **Create Account**.

What's next?

You can now enable data tiering on individual volumes on a Cloud Volumes ONTAP 9.6 system when you create, modify, or replicate them. For details, see Tiering inactive data to low-cost object storage.

But before you do, be sure that the subnet in which Cloud Volumes ONTAP resides is configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.