AWS credentials

Set up and administration

NetApp
April 01, 2022

Table of Contents

AWS credentials

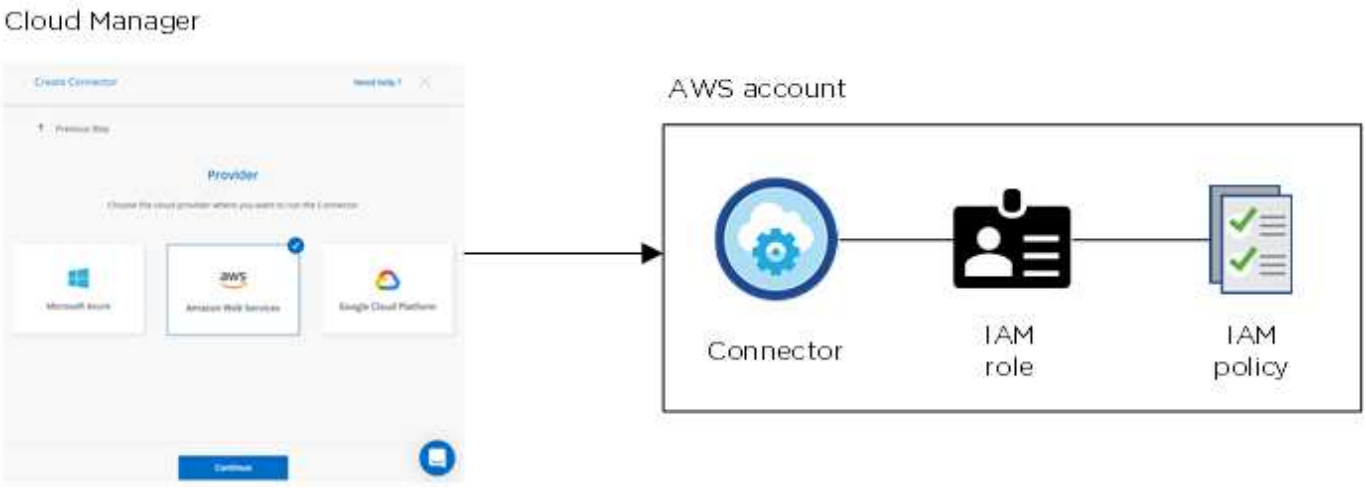
AWS credentials and permissions

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.

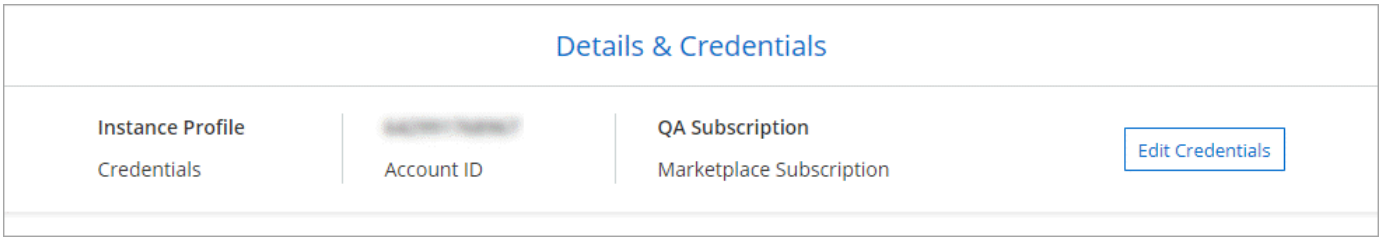
Initial AWS credentials

When you deploy 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.

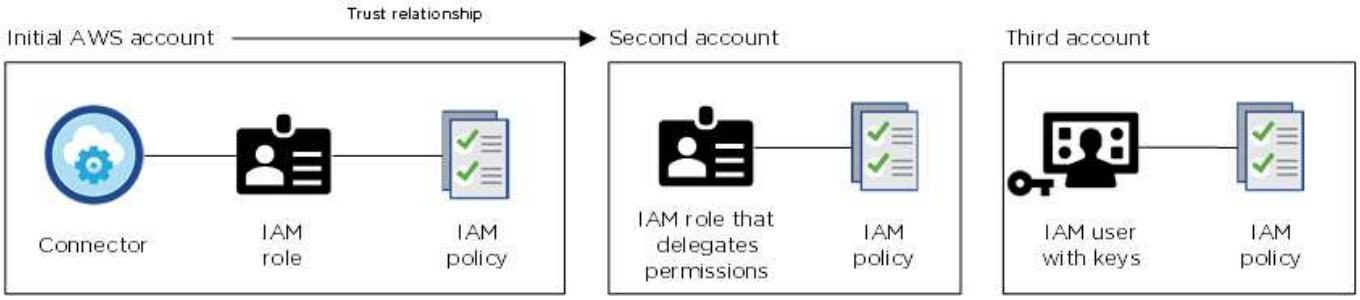


Cloud Manager selects these AWS credentials by default when you create a new working environment for Cloud Volumes ONTAP:



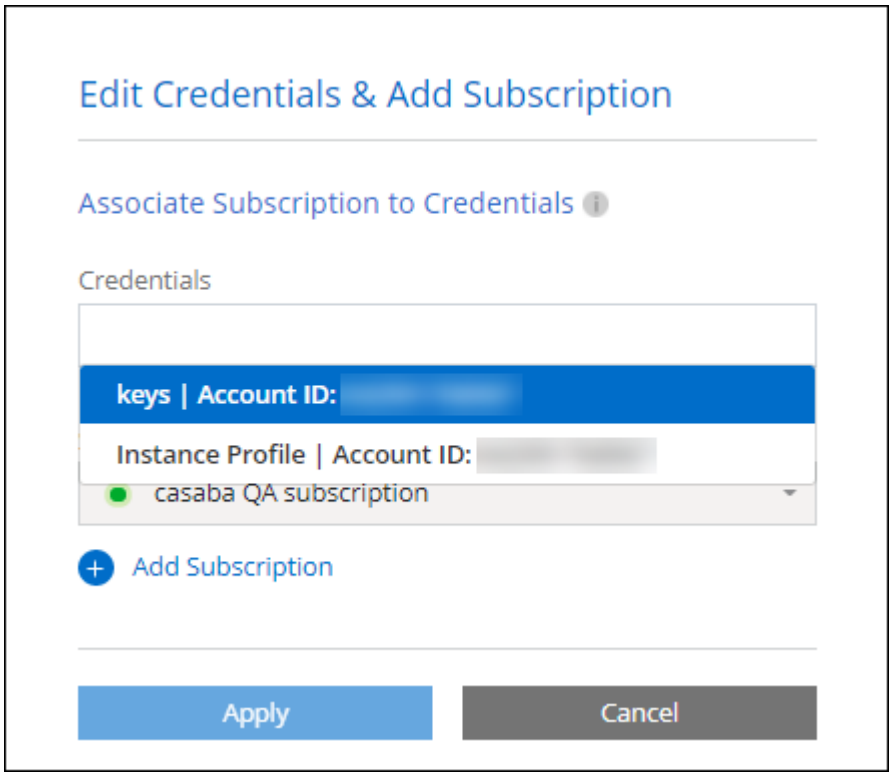
Additional AWS credentials

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:



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**.

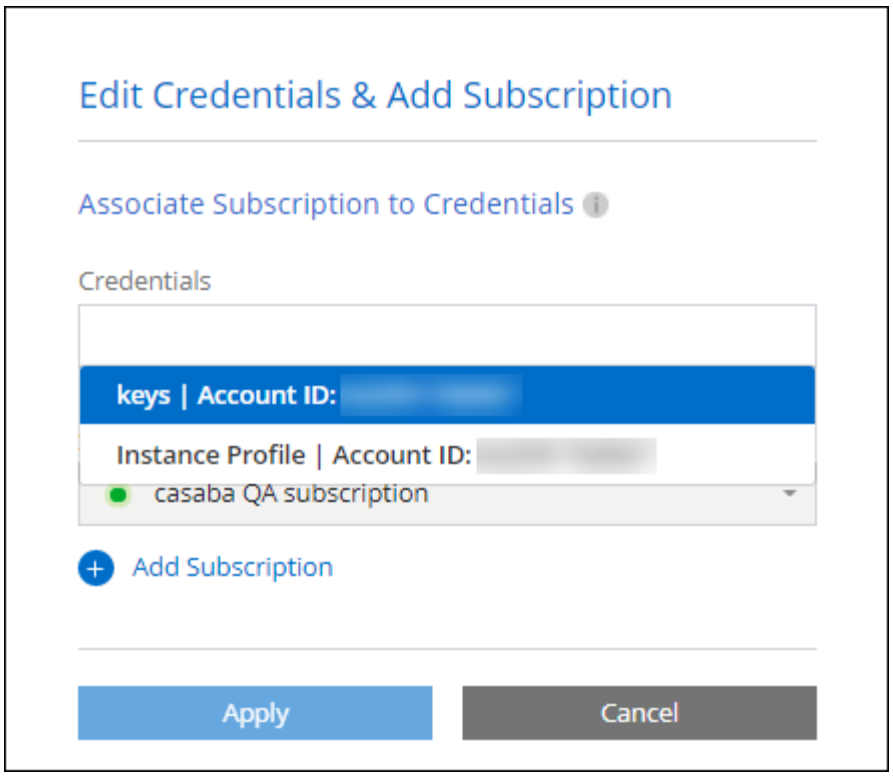
3. Click **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > Connector**.
   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of a trusted IAM role, or enter an AWS access key and secret key.
   c. **Marketplace Subscription**: 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: 952013314444
   - 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:

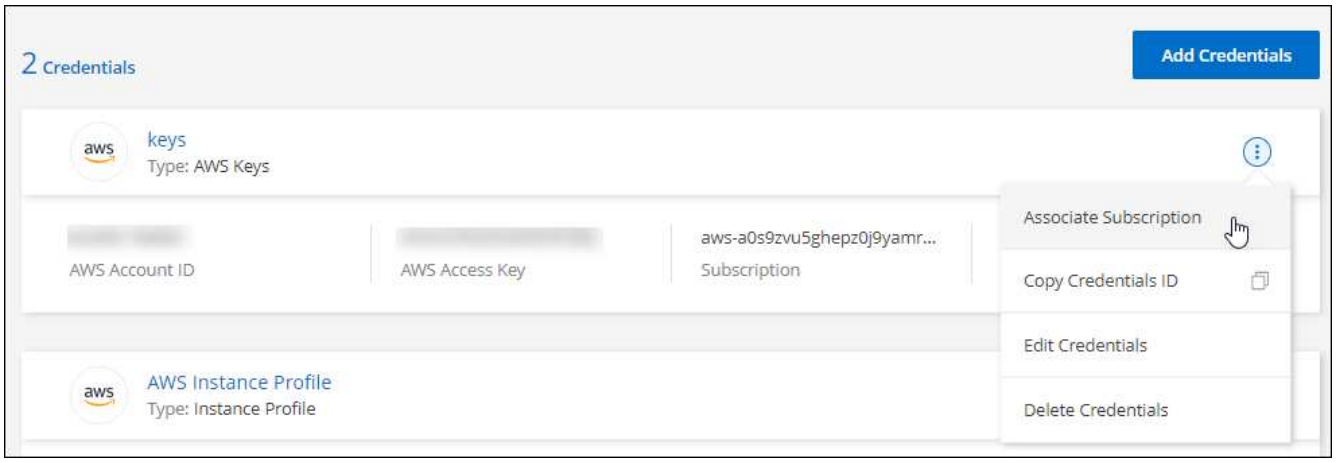
- You didn't associate a subscription when you initially added the credentials to Cloud Manager.
- You want to replace an existing AWS Marketplace subscription with a new subscription.

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/cloud-manager-setup-admin//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.