# Table of Contents

AWS ........................................................................................................................................... 1

AWS credentials and permissions .............................................................................................. 1

Adding AWS credentials and subscriptions in Cloud Manager ............................................... 4
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.

Adding AWS credentials and subscriptions in Cloud Manager

When you create a Cloud Volumes ONTAP system, you need to select the AWS credentials and subscription to use with that system. If you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

Before you add AWS credentials to Cloud Manager, you need to provide the required permissions to that account. 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 AWS keys or the ARN of a role in a trusted account.

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

- Granting permissions by providing AWS keys
- Granting permissions by assuming IAM roles in other accounts
How can I securely rotate my AWS 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, 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.

Granting 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 it to Cloud Manager.

Granting permissions by assuming IAM roles in other accounts

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 target account where you want to deploy Cloud Volumes ONTAP and create an IAM role by selecting Another AWS account.
Be sure to do the following:

- Enter the ID of the account where the Connector instance resides.
- Attach the Cloud Manager IAM policy, which is available from the Cloud Manager Policies page.

2. Go to the source account where the Connector instance resides and select the IAM role that is attached to the instance.
   
   a. Click **Attach policies** and then click **Create policy**.
   
   b. Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

   **Example**

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

   **Result**

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

### Adding AWS credentials to Cloud Manager

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

**Steps**

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

2. Click **Add Credentials** and select **AWS**.

3. Provide AWS keys or the ARN of a trusted IAM role.

4. Confirm that the policy requirements have been met and click **Continue**.
5. Choose the pay-as-you-go subscription that you want to associate with the credentials, or click Add Subscription if you don't have one yet.

To create a pay-as-you-go Cloud Volumes ONTAP system, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

6. Click Go.

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

If you haven’t yet added an AWS subscription to a set of AWS credentials, you can do so any time from the Credentials page. To create a pay-as-you-go Cloud Volumes ONTAP system, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

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. Hover over a set of credentials and click the action menu.
3. From the menu, click **Add Subscription**.
4. Click **Add Subscription**, click **Continue**, and follow the steps.

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