Manage cloud provider credentials

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Manage cloud provider credentials . . . 1
- AWS . . . 1
  - Learn about AWS credentials and permissions in NetApp Console . . . 1
  - Manage AWS credentials and marketplace subscriptions for NetApp Console . . . 4
- Azure . . . 14
  - Learn about Azure credentials and permissions in NetApp Console . . . 14
  - Manage Azure credentials and marketplace subscriptions for NetApp Console . . . 16
- Google Cloud . . . 28
  - Learn about Google Cloud projects and permissions . . . 28
  - Manage Console agent permissions for Google Cloud deployments . . . 29

Manage cloud provider credentials

AWS

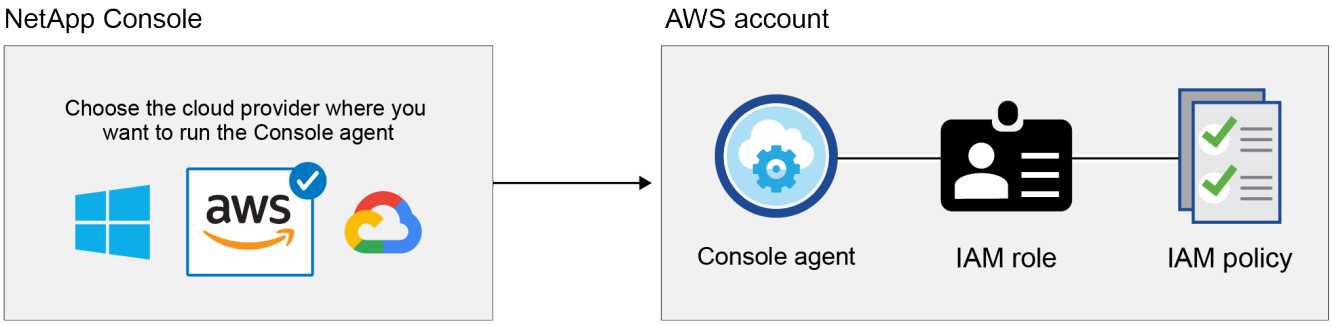
Learn about AWS credentials and permissions in NetApp Console

You manage AWS credentials and marketplace subscriptions directly from NetApp Console to ensure secure deployment of Cloud Volumes ONTAP and other data services by providing appropriate IAM credentials during Console agent deployment and associating them with AWS Marketplace subscriptions for billing.

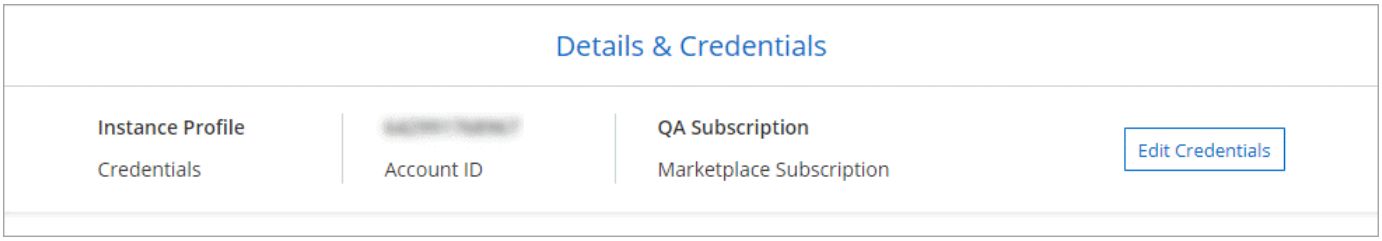
Initial AWS credentials

When you deploy an Console agent from the Console, you need to provide the ARN of an IAM role or access keys for an IAM user. The authentication method must have permissions to deploy the Console agent in AWS. The required permissions are listed in the Agent deployment policy for AWS.

When the Console launches the Console agent in AWS, it creates an IAM role and a profile for the agent. It also attaches a policy that provides the Console agent with permissions to manage resources and processes within that AWS account. Review how the Agent uses the permissions.



If you add a new Cloud Volumes ONTAP system, the Console selects these AWS credentials by default:



Deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

Additional AWS credentials

You might add additional AWS credentials to the Console in the following cases:

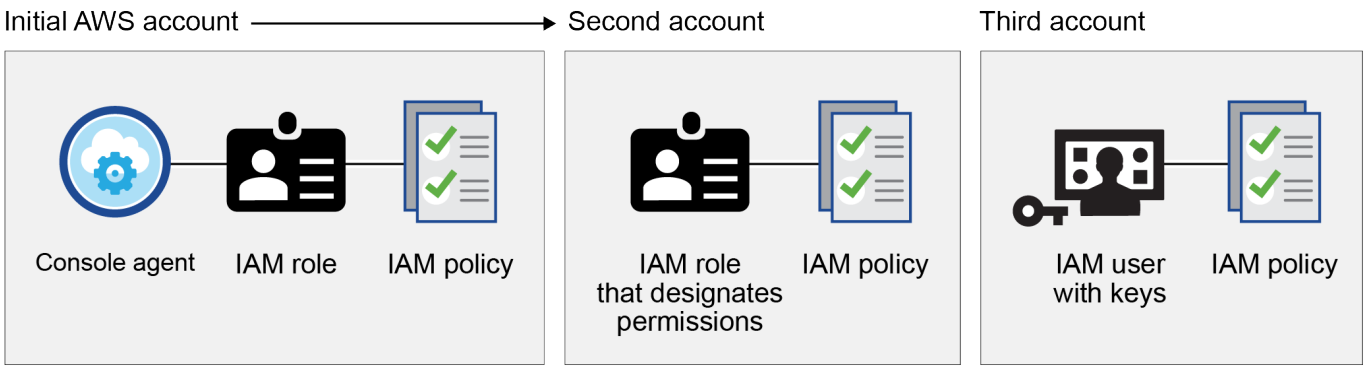
- To use your existing Console agent with an additional AWS account
- To create a new agent in a specific AWS account

- To create and manage FSx for ONTAP file systems

Review the sections below for more details.

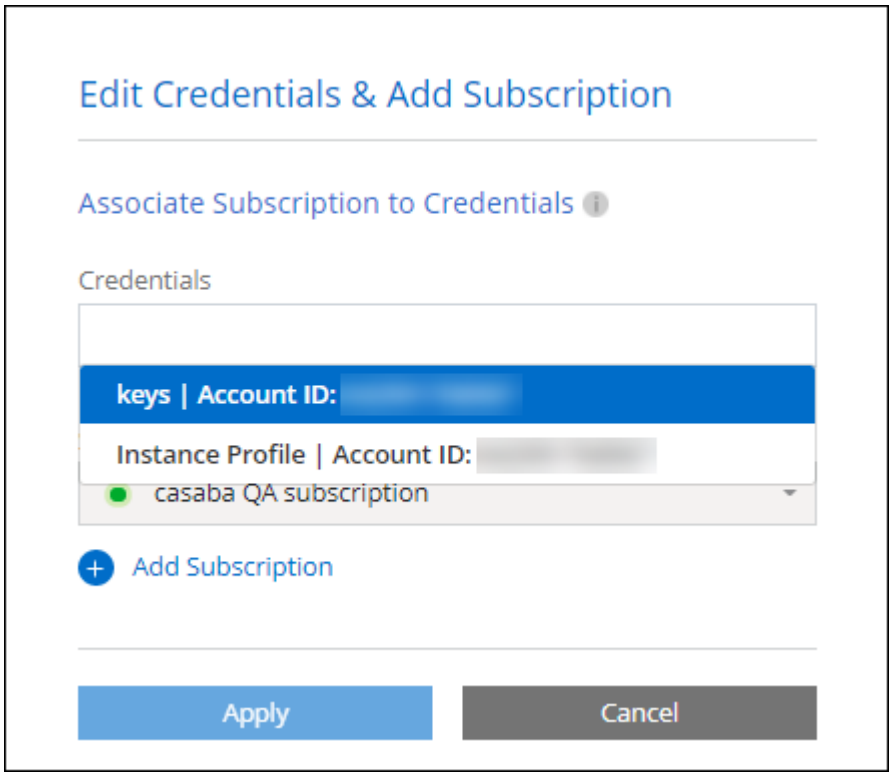
Add AWS credentials to use a Console agent with another AWS account

To use the Console with additional AWS accounts, provide AWS keys 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 add account credentials to the Console by specifying the Amazon Resource Name (ARN) of IAM role or the AWS keys for the IAM user.

For example, you can switch between credentials when creating a new Cloud Volumes ONTAP system:



Learn how to add AWS credentials to an existing agent.

Add AWS credentials to create a Console agent

Adding AWS credentials provides permissions to create a Console agent.

Learn how to add AWS credentials to the Console for creating a Console agent

Add AWS credentials for FSx for ONTAP

Add AWS credentials to the Console to provide the necessary permissions to create and manage an FSx for ONTAP system.

Learn how to add AWS credentials to the Console for Amazon FSx for ONTAP

Credentials and marketplace subscriptions

You must associate the credentials that you add to a Console agent with an AWS Marketplace subscription to pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) and other NetApp data services or through an annual contract.
Learn how to associate an AWS subscription.

Note the following about AWS credentials and marketplace subscriptions:

- You can associate only one AWS Marketplace subscription with a set of AWS credentials
- You can replace an existing marketplace subscription with a new subscription

FAQ

The following questions are related to credentials and subscriptions.

How can I securely rotate my AWS credentials?

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

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

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

Can I change the AWS Marketplace subscription for Cloud Volumes ONTAP systems?

Yes, you can. When you change the AWS Marketplace subscription that's associated with a set of credentials, all existing and new Cloud Volumes ONTAP systems are charged against the new subscription.

Learn how to associate an AWS subscription.

Can I add multiple AWS credentials, each with different marketplace subscriptions?

All AWS credentials that belong to the same AWS account will be associated with the same AWS Marketplace subscription.

If you have multiple AWS credentials that belong to different AWS accounts, then those credentials can be associated with the same AWS Marketplace subscription or with different subscriptions.

Can I move existing Cloud Volumes ONTAP systems to a different AWS account?

No, it's not possible to move the AWS resources associated with your Cloud Volumes ONTAP system to a different AWS account.

How do credentials work for marketplace deployments and on-premises deployments?

The sections above describe the recommended deployment method for the Console agent, which is from the Console. You can also deploy an agent in AWS from the AWS Marketplace and you can manually install the Console agent software on your own Linux host or in your VCenter.

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 Console, but you can provide permissions using AWS access keys.

To learn how to set up permissions, refer to the following pages:

- Standard mode
  - Set up permissions for an AWS Marketplace deployment
  - Set up permissions for on-premises deployments
- Restricted mode
  - Set up permissions for restricted mode

Manage AWS credentials and marketplace subscriptions for NetApp Console

Add and manage AWS credentials so that you deploy and manage cloud resources in your AWS accounts from the NetApp Console. If you manage multiple AWS Marketplace 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 Console agent or directly to the Console:

- Add additional AWS credentials to an existing agent

  Add AWS credentials to a Console agent to manage cloud resources. Learn how to add AWS credentials to a Console agent.

- Add AWS credentials to the Console for creating a Console agent

  Adding new AWS credentials to the Console provides the permissions needed to create a Console agent. Learn how to add AWS credentials to the NetApp Console.

- Add AWS credentials to the Console for FSx for ONTAP

  Add new AWS credentials to the Console to create and manage FSx for ONTAP. Learn how to set up permissions for FSx for ONTAP

How to rotate credentials

The NetApp Console enables you to provide AWS credentials in a few ways: an IAM role associated with the agent 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, the Console 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.

Manually rotate AWS access keys by updating them in the Console.

Add additional credentials to a Console agent

Add additional AWS credentials to a Console agent so that it has the permissions needed to manage resources and processes within your public cloud environment. You can either provide the ARN of an IAM role in another account or provide AWS access keys.

Learn how the NetApp Console uses AWS credentials and permissions.

Grant permissions

Grant permissions before adding AWS credentials to a Console agent. The permissions allow a Console agent to manage resources and processes within that AWS account. You can provide the permissions with the ARN of a role in a trusted account or AWS keys.

> If you deployed a Console agent from the Console, it automatically added AWS credentials for the account in which you deployed a Console agent. This ensures the necessary permissions are in place for managing resources.

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 a Console agent and other AWS accounts by using IAM roles. You would then provide the Console with the ARN of the IAM roles from the trusted accounts.

If a Console agent is installed on-premises, you can't use this authentication method. You must use AWS keys.

Steps

1. Go to the IAM console in the target account in which you want to provide a Console agent with permissions.
2. Under Access Management, select **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 a Console agent instance resides.

- Create the required policies by copying and pasting the contents of the IAM policies for a Console agent.

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

Result

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

Grant permissions by providing AWS keys

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

You must use this authentication method if a Console agent is installed on-premises. You can't use an IAM role.

Steps

1. From the IAM console, create policies by copying and pasting the contents of the IAM policies for a Console agent.

   AWS Documentation: Creating IAM Policies

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

Add the credentials to an existing agent

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

New credentials in your cloud provider may take a few minutes to become available.

Steps

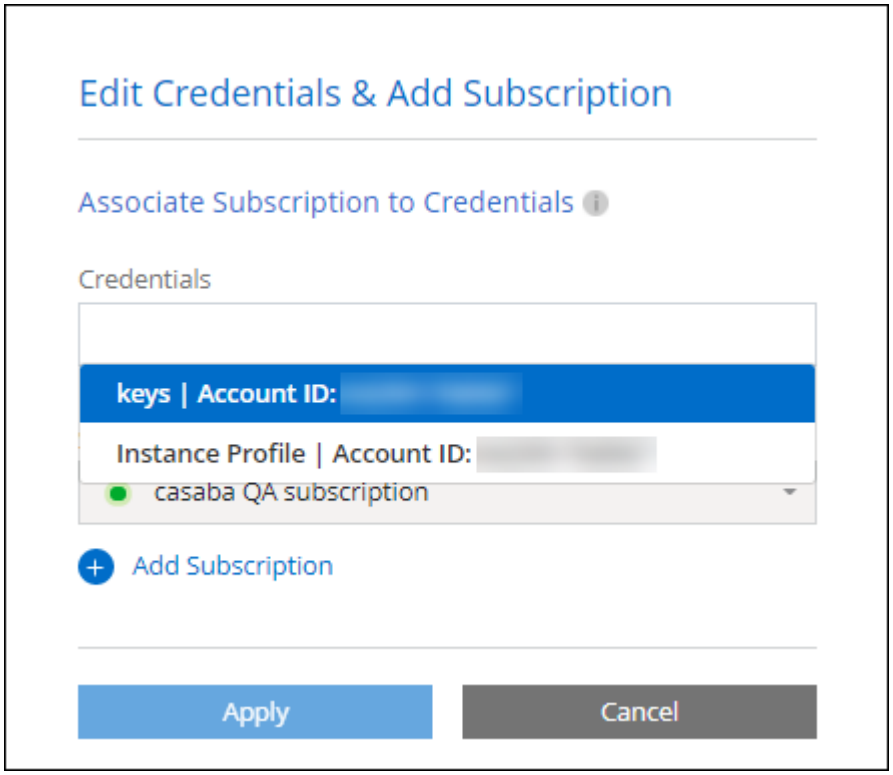
1. Use the top navigation bar to select a Console agent to which you want to add credentials.
2. In the left navigation bar, select **Administration > Credentials**.
3. On the **Organization credentials** page, select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > Agent**.
   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 services at an hourly rate (PAYGO) or with an annual contract, you must associate AWS credentials with your AWS Marketplace subscription.

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

Result

You can now switch to a different set of credentials from the Details and Credentials page when adding a subscription to the Console.



Add credentials to the Console for creating a Console agent

Add AWS credentials by providing the ARN of an IAM role that gives the permissions needed to create a Console agent. You can choose these credentials when creating a new agent.

Set up the IAM role

Set up an IAM role that enables the NetApp Console software as a service (SaaS) layer to assume the role.

Steps

1. Go to the IAM console in the target account.
2. Under Access Management, select **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 NetApp Console SaaS: 952013314444
   - For Amazon FSx for NetApp ONTAP specifically, edit the **Trust relationships** policy to include "AWS": "arn:aws:iam::952013314444:root".

     For example, the policy should look like this:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Refer to AWS Identity and Access Management (IAM) documentation for more information on cross account resource access in IAM.

- Create a policy that includes the permissions required to create a Console agent.
  - View the permissions needed for FSx for ONTAP
  - View the agent deployment policy

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

Result

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

Add the credentials

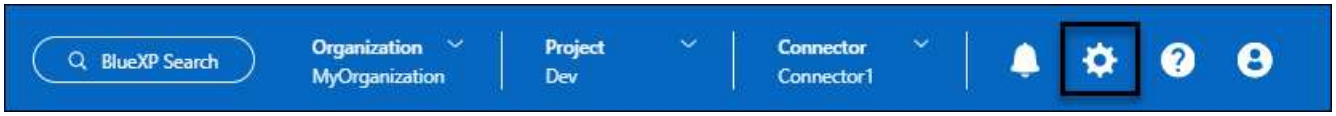
After you provide the IAM role with the required permissions, add the role ARN to the Console.

Before you begin

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 the Console.

Steps

1. Select **Administration > Credentials**.



2. On the **Organization credentials** page, select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > Console**.
   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of the IAM role.
   c. **Review**: Confirm the details about the new credentials and select **Add**.

Add credentials to the Console for Amazon FSx for ONTAP

For details, refer to the the Console documentation for Amazon FSx for ONTAP

Configure an AWS subscription

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

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

- You didn't configure a subscription when you initially added the credentials.
- You want to change the AWS Marketplace subscription that is configured to the AWS credentials.

  Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP systems and all new systems.

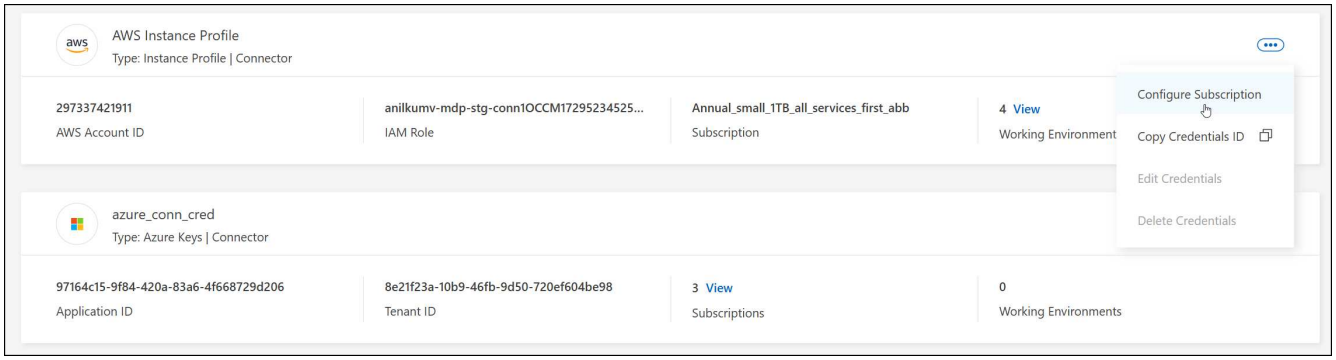
Before you begin

You need to create a Console agent before you can configure a subscription. Learn how to create a Console agent.

Steps

1. Select **Administration > Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.

   You must select credentials that are associated with a Console agent. You can't associate a marketplace subscription with credentials that are associated with the NetApp Console.



4. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
5. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
   a. Select **View purchase options**.
   b. Select **Subscribe**.
   c. Select **Set up your account**.

You'll be redirected to the NetApp Console.

d. From the **Subscription Assignment** page:

- Select the Console organizations or accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

  The Console replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

  For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

Associate an existing subscription with your organization

When you subscribe to from the AWS Marketplace, the last step in the process is to associate the subscription with your organization. If you didn't complete this step, then you can't use the subscription with your organization.

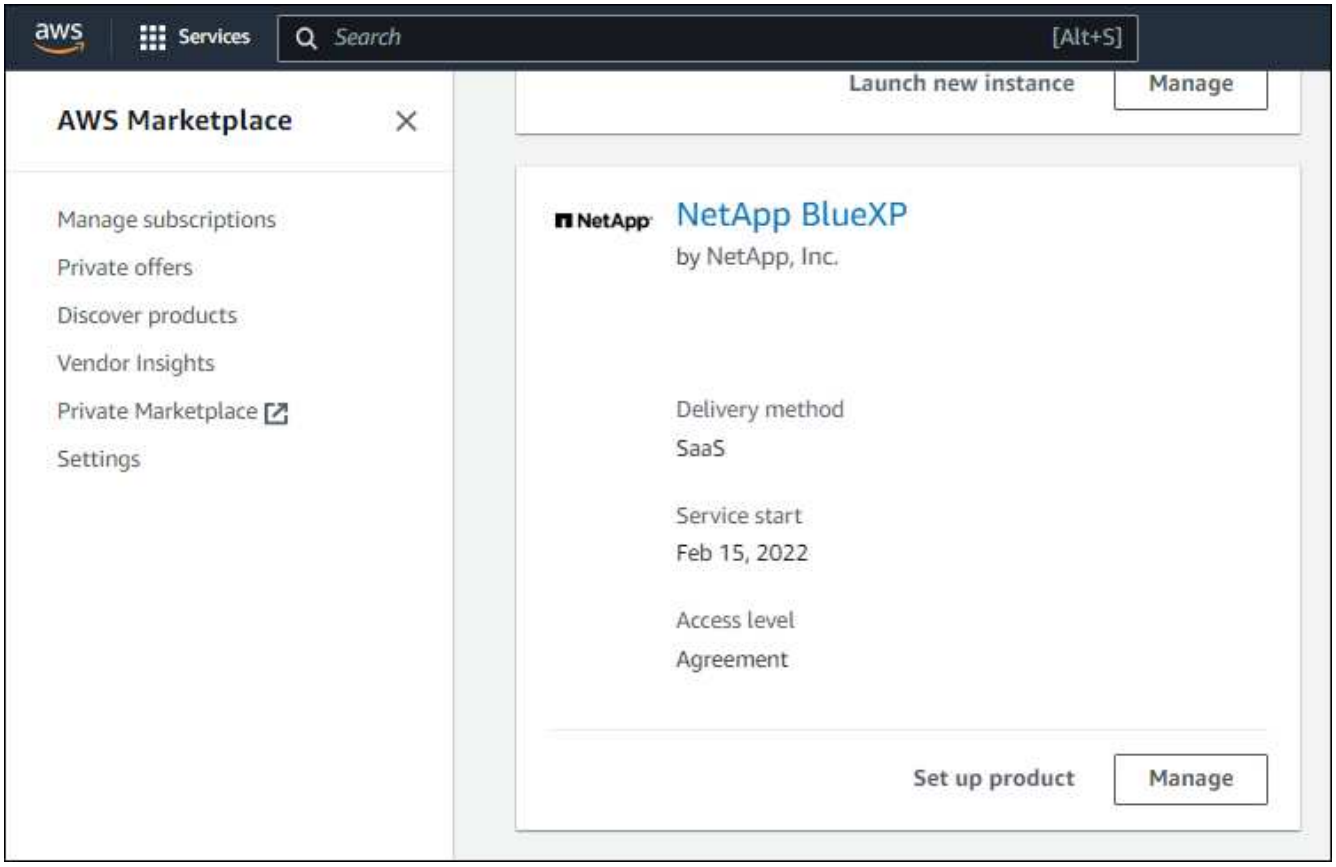
- Learn about the Console deployment modes
- Learn about the Console identity and access management

Follow the steps below if you subscribed to NetApp Intelligent Services from the AWS Marketplace, but you missed the step to associate the subscription with your account.

Steps

1. Confirm that you didn't associate your subscription with your Console organization.
   a. From the navigation menu, select **Administration > Licenses and subscriptions**.
   b. Select **Subscriptions**.
   c. Verify that your subscription doesn't appear.

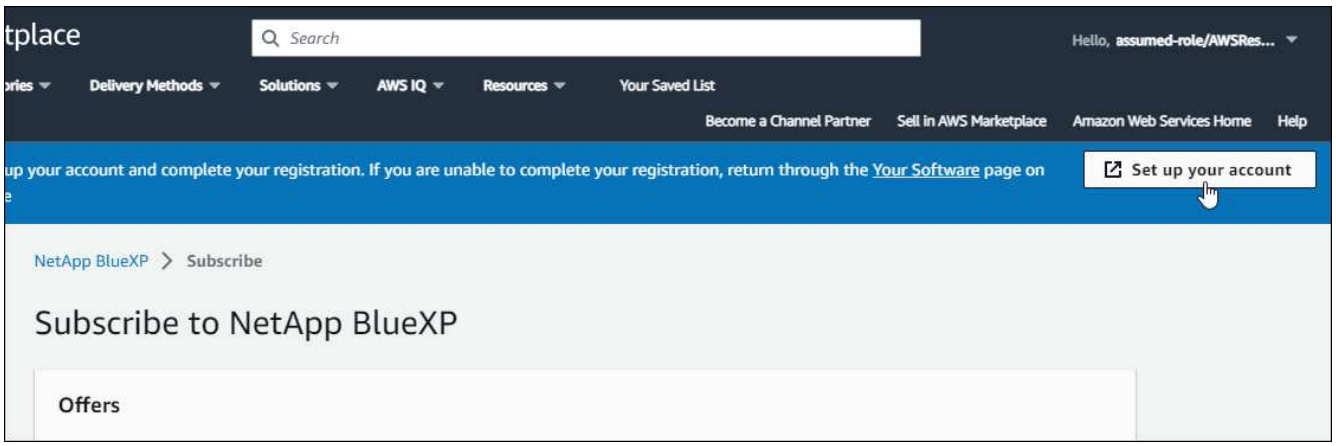
      You'll only see the subscriptions that are associated with the organization or account that you're currently viewing. If you don't see your subscription, proceed with the following steps.
2. Log in to the AWS Console and navigate to **AWS Marketplace Subscriptions**.
3. Find the subscription.



4. Select **Set up product**.

   The subscription offer page should load in a new browser tab or window.

5. Select **Set up your account**.



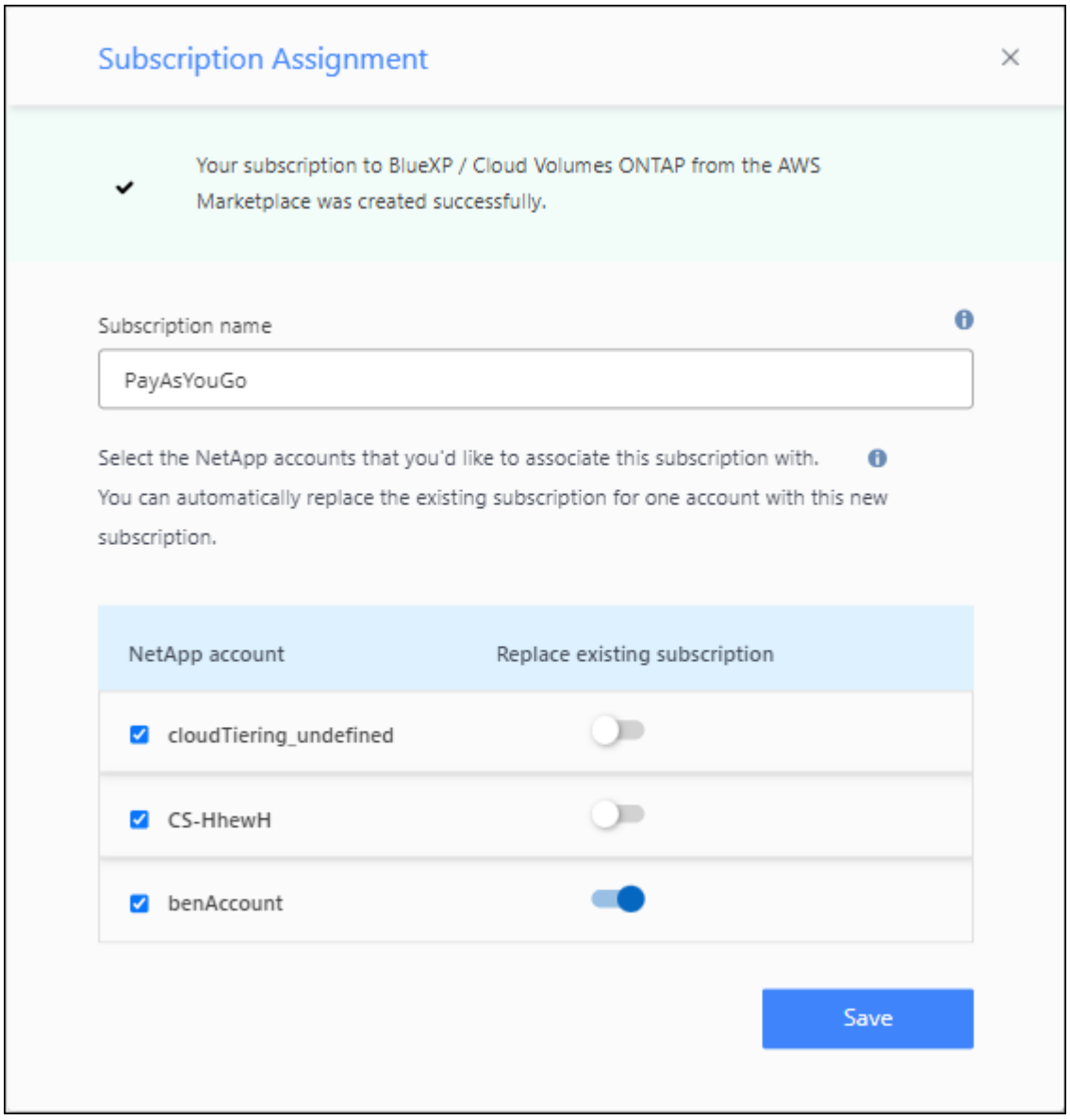
   The **Subscription Assignment** page on netapp.com should load in a new browser tab or window.

   Note that you might be prompted to log in to the Console first.

6. From the **Subscription Assignment** page:
   - Select the Console organizations or accounts that you'd like to associate this subscription with.
   - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

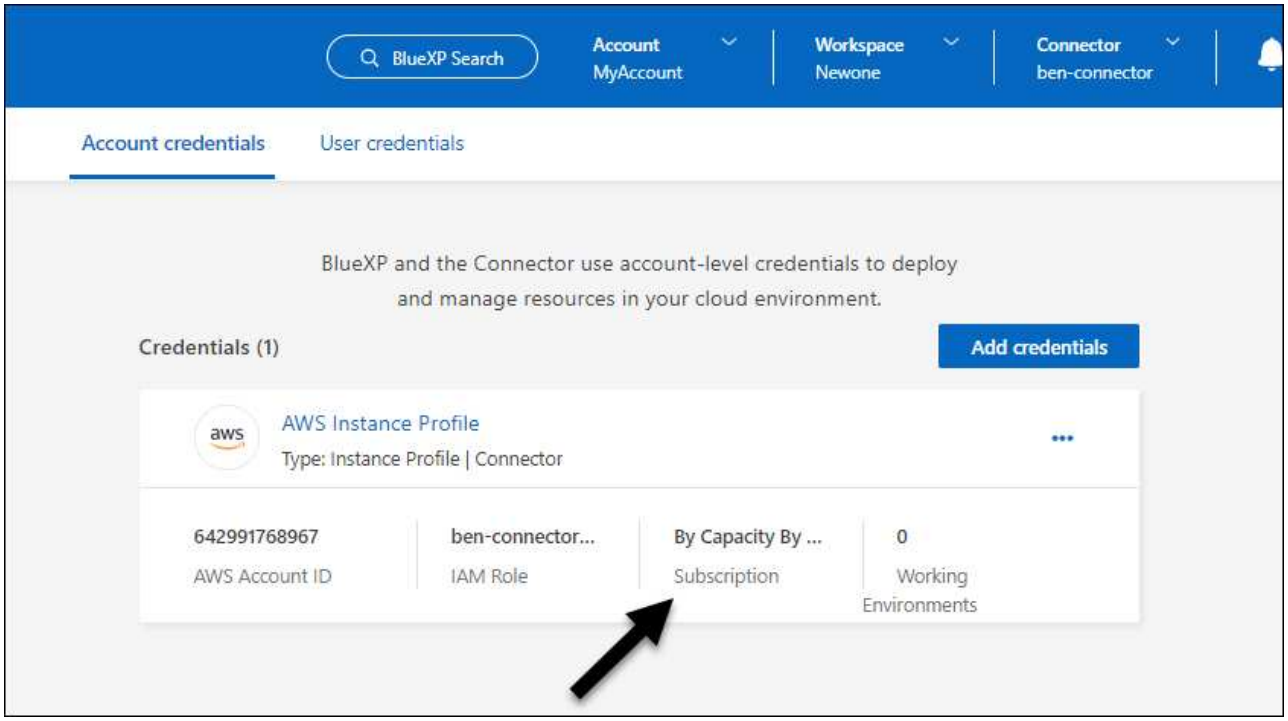
The Console replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.



7. Confirm that the subscription is associated with your organization.
   a. From the navigation menu, select **Administration > License and subscriptions**.
   b. Select **Subscriptions**.
   c. Verify that your subscription appears.
8. Confirm that the subscription is associated with your AWS credentials.
   a. Select **Administration > Credentials**.
   b. On the **Organization credentials** page, verify that the subscription is associated with your AWS credentials.

Here's an example.



Edit credentials

Edit your AWS credentials 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 are associated with a Console agent instance or an Amazon FSx for ONTAP instance. You can only rename the credentials for an FSx for ONTAP instance.

Steps

1. Select **Administration > Credentials**.
2. On the **Organization credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

Delete credentials

If you no longer need a set of credentials, you can delete them. You can only delete credentials that aren't associated with a system.

You can't delete the credentials for an instance profile that is associated with a Console agent.

Steps

1. Select **Administration > Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

Azure

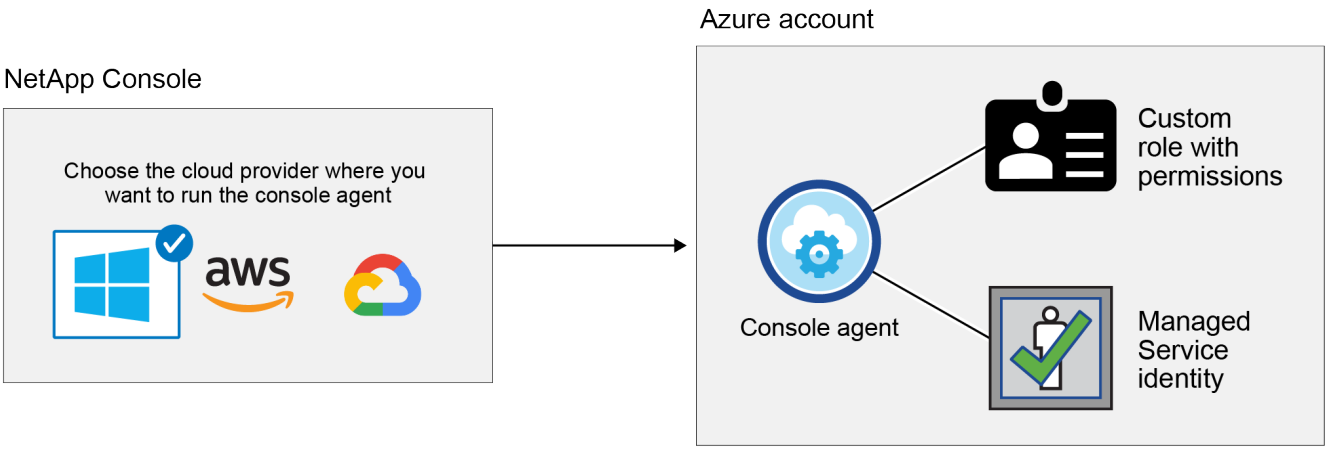
Learn about Azure credentials and permissions in NetApp Console

Learn how the NetApp Console uses Azure credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more Azure subscriptions. For example, you might want to learn when to add additional Azure credentials to the Console.

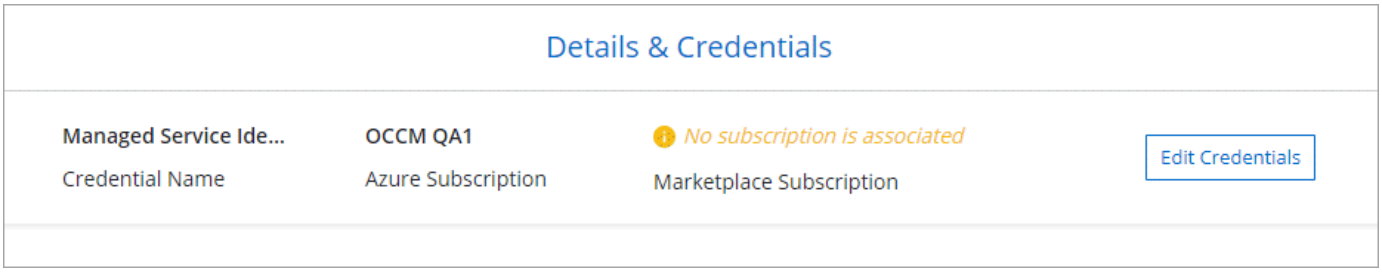
Initial Azure credentials

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

When the Console deploys the Console agent virtual machine in Azure, it enables a system-assigned managed identity on the virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides the Console with the permissions required to manage resources and processes within that Azure subscription. Review how the Console uses the permissions.



If you create a new system for Cloud Volumes ONTAP, the Console selects these Azure credentials by default:



You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

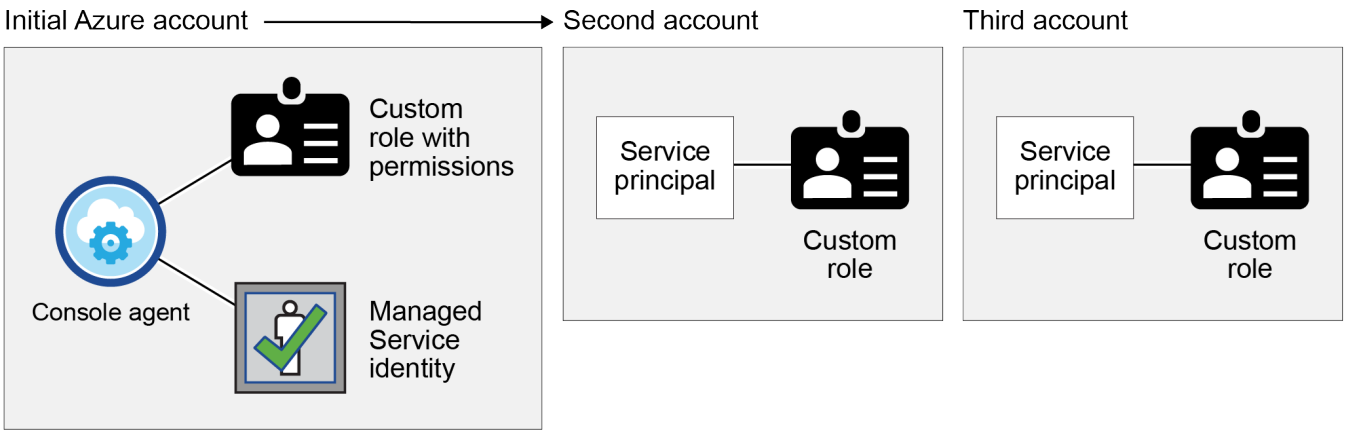
Additional Azure subscriptions for a managed identity

The system-assigned managed identity assigned to the Console agent VM is associated with the subscription

in which you launched the Console agent. If you want to select a different Azure subscription, then you need to associate the managed identity with those subscriptions.

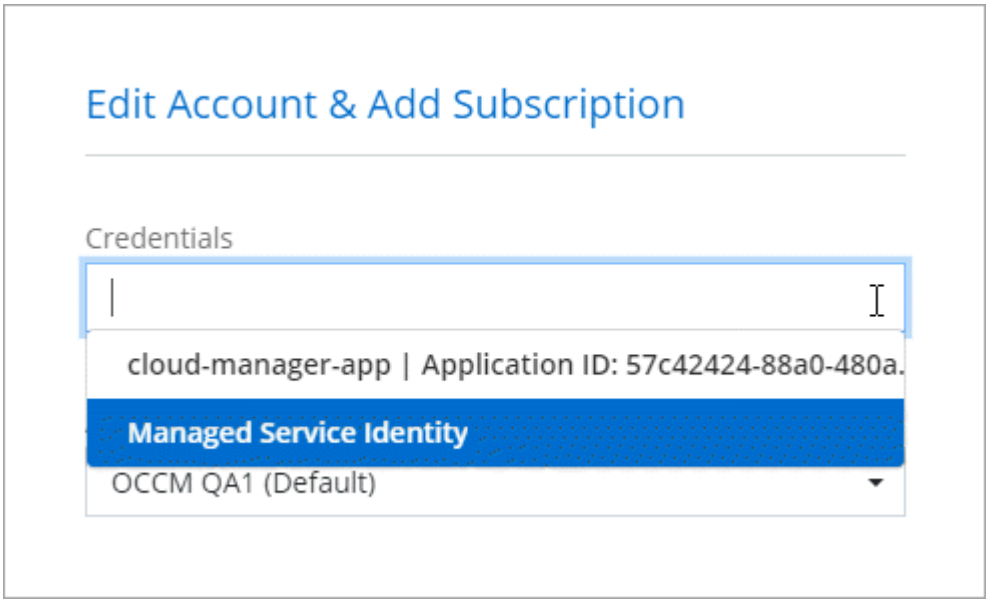
Additional Azure credentials

If you want to use different Azure credentials with the Console, then you must grant the required permissions by creating and setting up a service principal in Microsoft Entra ID 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 the Console by providing details about the AD service principal.

For example, you can switch between credentials when creating a new Cloud Volumes ONTAP system:



Credentials and marketplace subscriptions

The credentials that you add to a console agent must be associated with an Azure Marketplace subscription so that you can pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or NetApp data services or through an annual contract.

Learn how to associate an Azure subscription.

Note the following about Azure credentials and marketplace subscriptions:

- You can associate only one Azure Marketplace subscription with a set of Azure credentials
- You can replace an existing marketplace subscription with a new subscription

FAQ

The following question is related to credentials and subscriptions.

Can I change the Azure Marketplace subscription for Cloud Volumes ONTAP systems?

Yes, you can. When you change the Azure Marketplace subscription that's associated with a set of Azure credentials, all existing and new Cloud Volumes ONTAP systems will be charged against the new subscription.

Learn how to associate an Azure subscription.

Can I add multiple Azure credentials, each with different marketplace subscriptions?

All Azure credentials that belong to the same Azure subscription will be associated with the same Azure Marketplace subscription.

If you have multiple Azure credentials that belong to different Azure subscriptions, then those credentials can be associated with the same Azure Marketplace subscription or with different marketplace subscriptions.

Can I move existing Cloud Volumes ONTAP systems to a different Azure subscription?

No, it's not possible to move the Azure resources associated with your Cloud Volumes ONTAP system to a different Azure subscription.

How do credentials work for marketplace deployments and on-premises deployments?

The sections above describe the recommended deployment method for the Console agent, which is from the Console. You can also deploy a console agent in Azure from the Azure Marketplace, and you can install the Console agent software on your own Linux host.

If you use the Marketplace, you can provide permissions by assigning a custom role to the Console agent VM and to a system-assigned managed identity, or you can use a Microsoft Entra service principal.

For on-premises deployments, you can't set up a managed identity for the Console agent, but you can provide permissions by using a service principal.

To learn how to set up permissions, refer to the following pages:

- Standard mode
  - Set up permissions for an Azure Marketplace deployment
  - Set up permissions for on-premises deployments
- Restricted mode
  - Set up permissions for restricted mode

Manage Azure credentials and marketplace subscriptions for NetApp Console

Add and manage Azure credentials so that the NetApp Console has the permissions that it needs to deploy and manage cloud resources in your Azure subscriptions. If you manage multiple Azure Marketplace subscriptions, you can assign each one of them to

different Azure credentials from the Credentials page.

Overview

There are two ways to add additional Azure subscriptions and credentials in the Console.

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

Associate additional Azure subscriptions with a managed identity

The Console 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 Console agent from the Console. When you deploy the Console agent, the Console assigns the Console Operator role to the Console agent virtual machine.

Steps

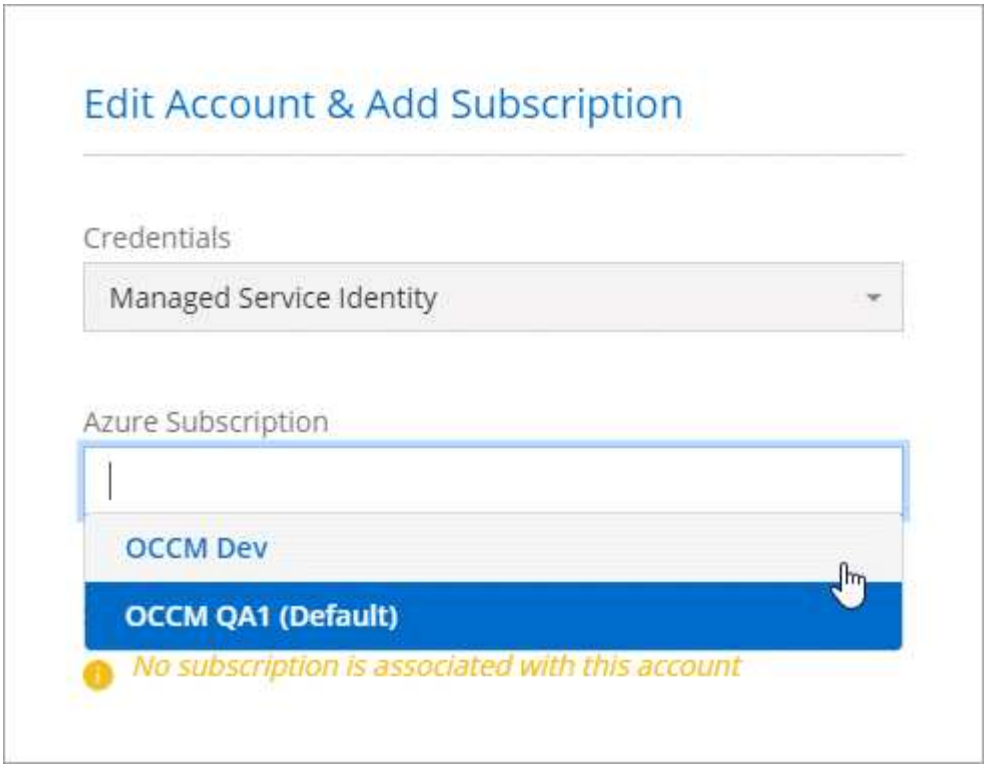
1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.
3. Select **Access control (IAM)**.
   a. Select **Add** > **Add role assignment** and then add the permissions:
      - Select the **Console Operator**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

        Console Operator is the default name provided in a Console agent 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 a Console agent virtual machine was created.
      - Select a Console agent virtual machine.
      - Select **Save**.
4. Repeat these steps for additional subscriptions.

Result

When creating a new system, you can now select from multiple Azure subscriptions for the managed identity profile.



Add additional Azure credentials to NetApp Console

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

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

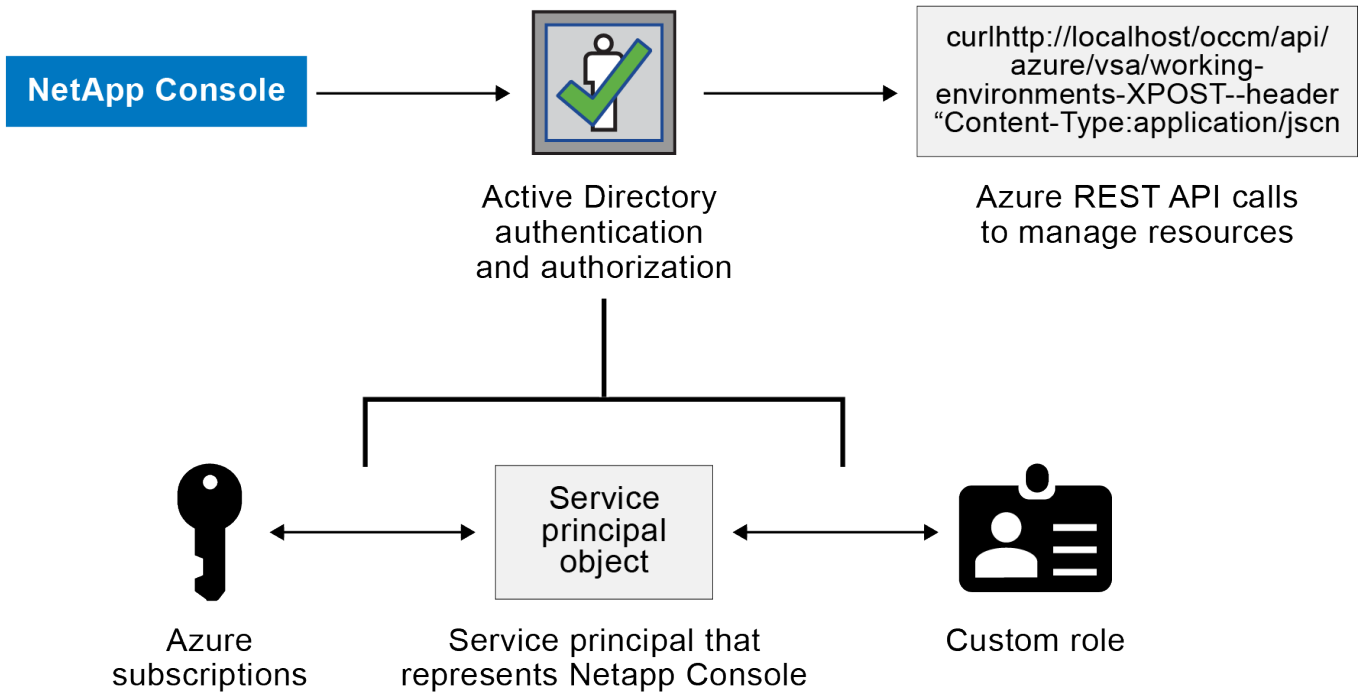
If you want to deploy Cloud Volumes ONTAP using *different* Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Microsoft Entra ID for each Azure account. You can then add the new credentials to the Console.

Grant Azure permissions using a service principal

The Console 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 Microsoft Entra ID and by obtaining the Azure credentials that the Console needs.

About this task

The following image depicts how the Console obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents the Console in Microsoft Entra ID and is assigned to a custom role that allows the required permissions.



Steps

1. Create a Microsoft Entra 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.

Create a Microsoft Entra application

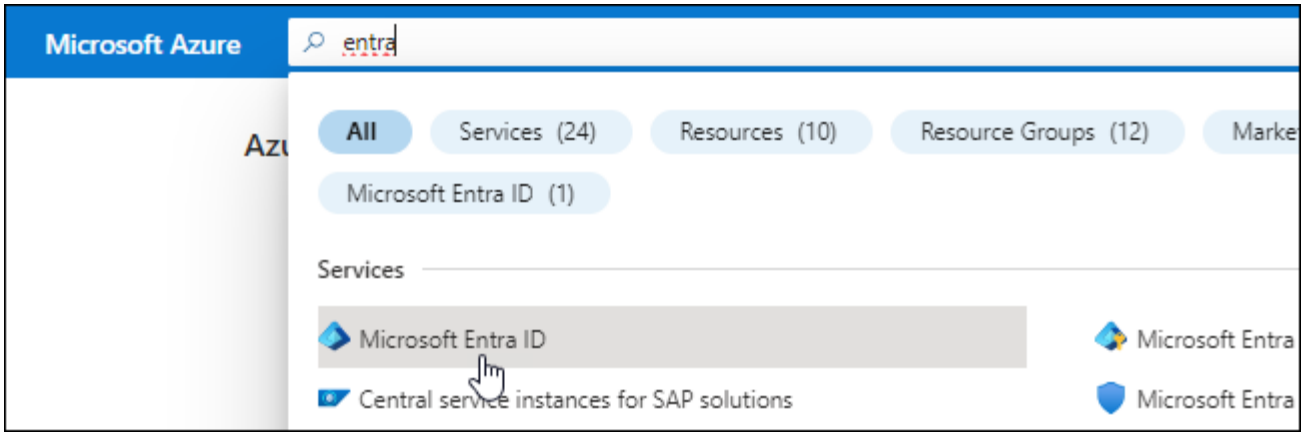
Create a Microsoft Entra application and service principal that the Console can use for role-based access control.

Steps

1. Ensure that you have 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

2. From the Azure portal, open the **Microsoft Entra ID** service.



3. In the menu, select **App registrations**.
4. Select **New registration**.
5. Specify details about the application:
   - **Name**: Enter a name for the application.
   - **Account type**: Select an account type (any will work with the NetApp Console).
   - **Redirect URI**: You can leave this field blank.
6. Select **Register**.

   You've created the AD application and service principal.

Assign the application to a role

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

Steps

1. Create a custom role:

   Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to Azure documentation

   a. Copy the contents of the custom role permissions for the Console agent and save them in a JSON file.

   b. 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.

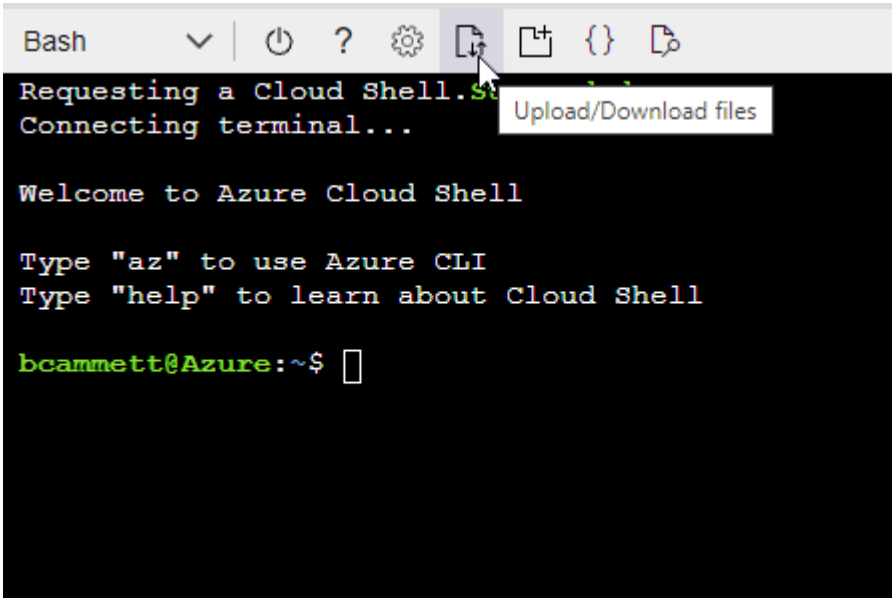
      Example

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

c. 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.

   - Start Azure Cloud Shell and choose the Bash environment.
   - Upload the JSON file.

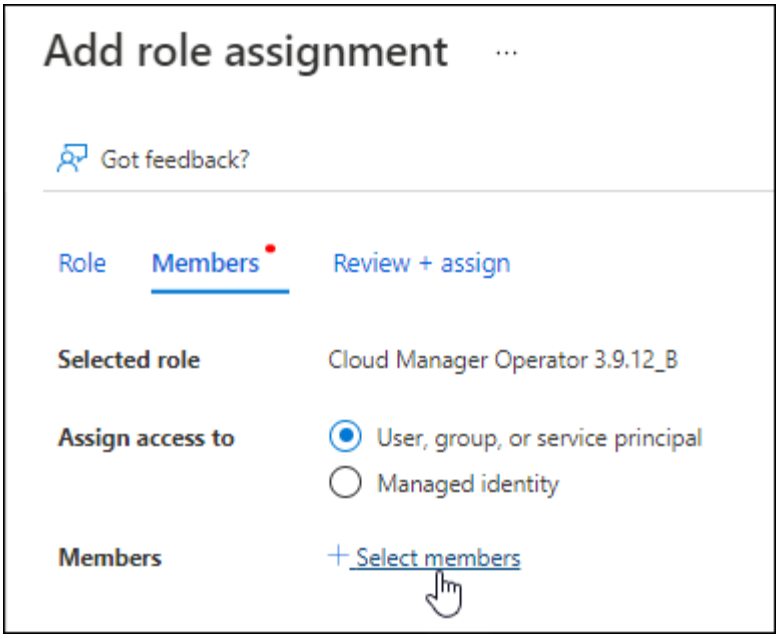


   - Use the Azure CLI to create the custom role:

```
az role definition create --role-definition agent_Policy.json
```

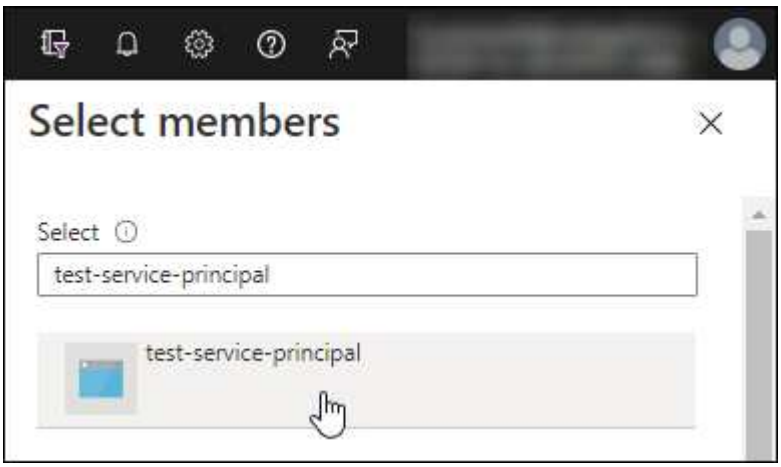
     You should now have a custom role called Console Operator that you can assign to the Console agent virtual machine.

2. Assign the application to the role:
   a. From the Azure portal, open the **Subscriptions** service.
   b. Select the subscription.
   c. Select **Access control (IAM) > Add > Add role assignment**.
   d. In the **Role** tab, select the **Console Operator** role and select **Next**.
   e. In the **Members** tab, complete the following steps:
      - Keep **User, group, or service principal** selected.
      - Select **Select members**.



- Search for the name of the application.

  Here's an example:



- Select the application and select **Select**.
- Select **Next**.

f. Select **Review + assign**.

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

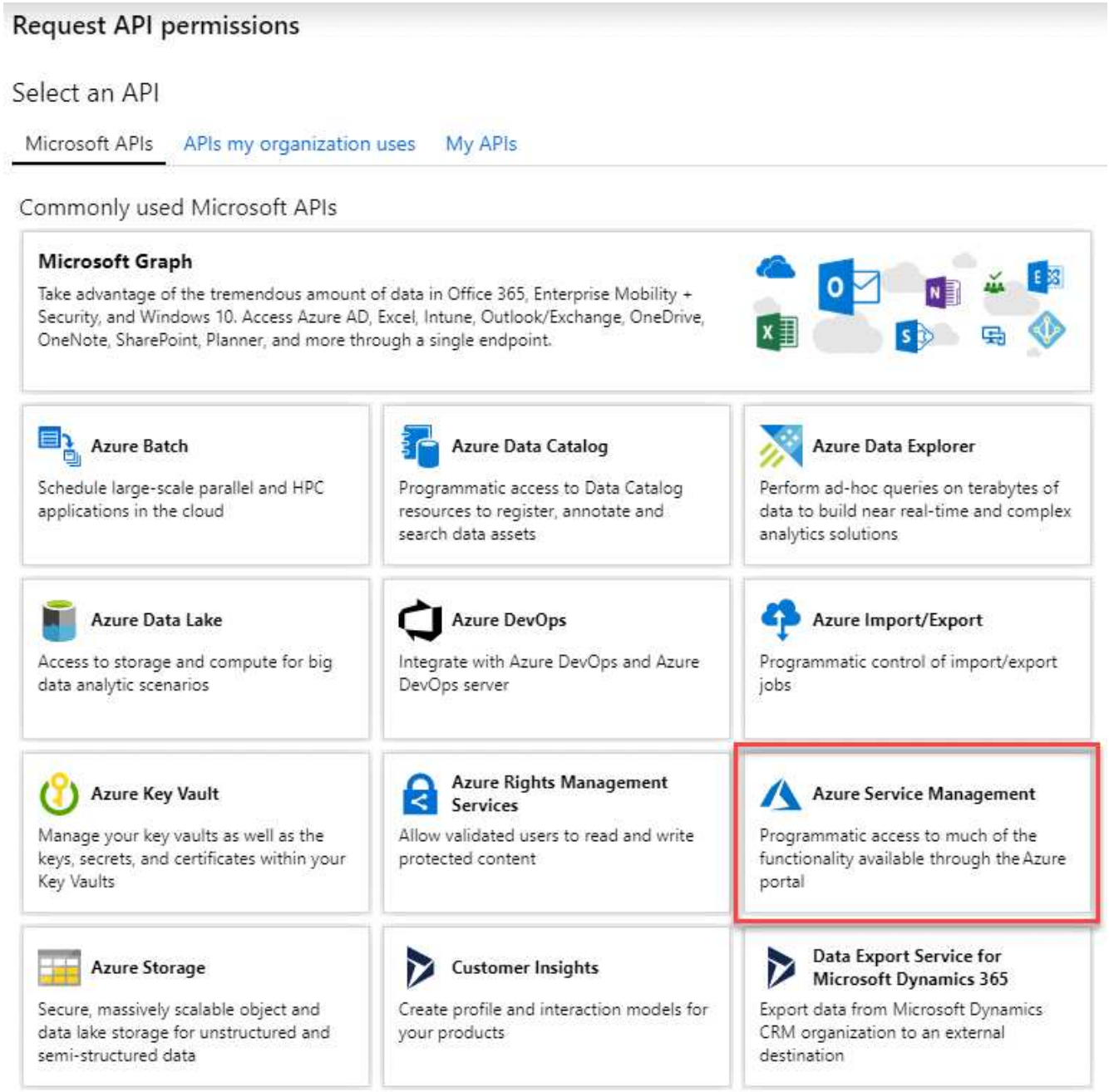
   If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. In the NetApp Console, you can select the subscription that you want to use when deploying Cloud Volumes ONTAP.

Add Windows Azure Service Management API permissions

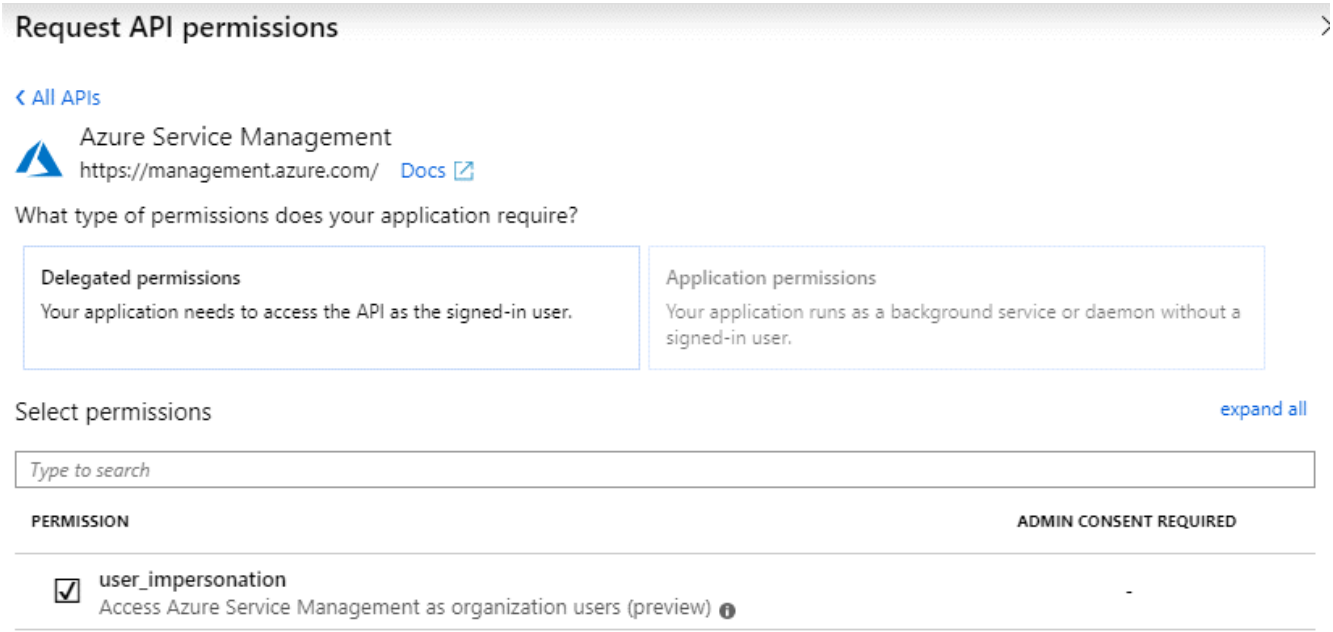
You must assign "Windows Azure Service Management API" permissions to the service principal.

Steps

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.



4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

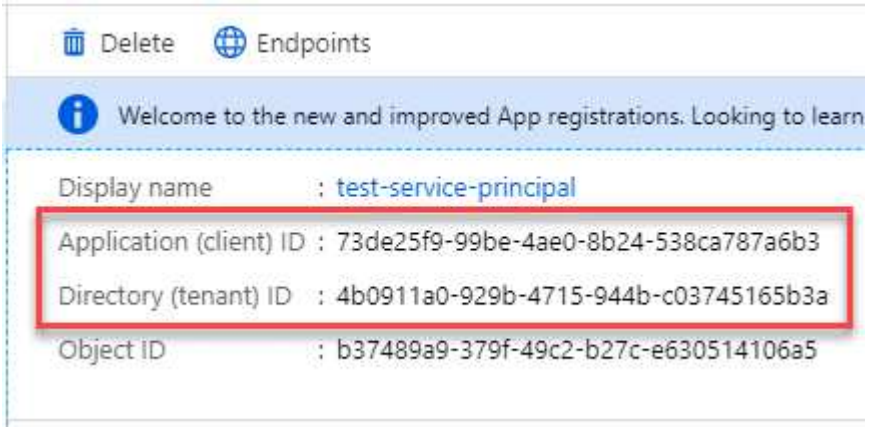


Get the application ID and directory ID

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

Steps

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



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

Create a client secret

Create a client secret and provide its value to the Console for authentication with Microsoft Entra ID.

Steps

1. Open the **Microsoft Entra ID** service.

2. Select **App registrations** and select your application.
3. Select **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Select **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 the Console when you add an Azure account.

Add the credentials to the Console

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

Before you begin

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 the Console.

Before you begin

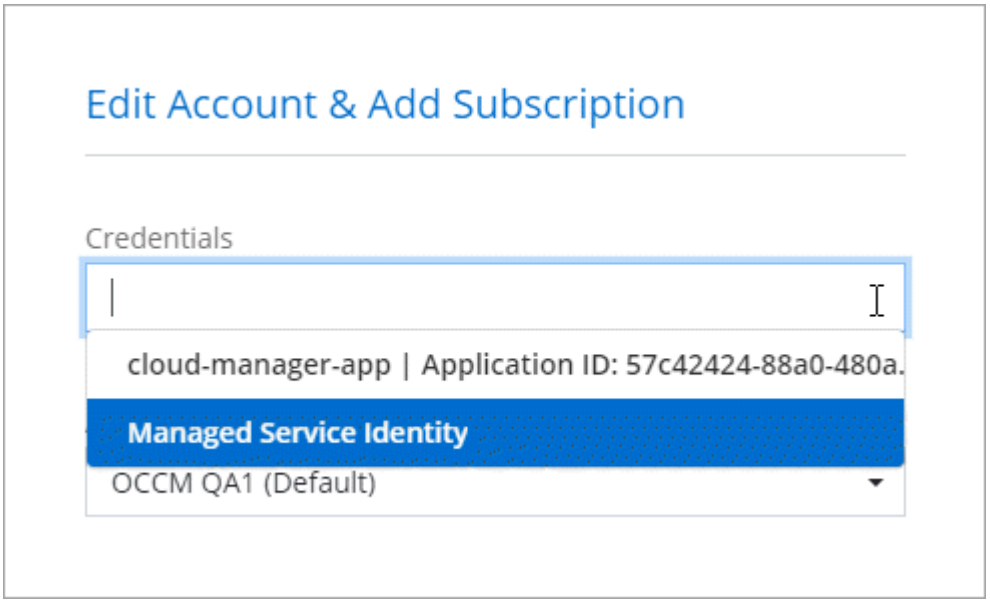
You need to create a Console agent before you can change Console settings. Learn how to create a Console agent.

Steps

1. Select **Administration > Credentials**.
2. Select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Microsoft Azure > Agent**.
   b. **Define Credentials**: Enter information about the Microsoft Entra service principal that grants the required permissions:
      - Application (client) ID
      - Directory (tenant) ID
      - Client Secret
   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
   d. **Review**: Confirm the details about the new credentials and select **Add**.

Result

You can switch to a different set of credentials from the Details and Credentials page when adding a system to the Console



Manage existing credentials

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

Associate an Azure Marketplace subscription to credentials

After you add your Azure credentials to the Console, you can associate an Azure Marketplace subscription to those credentials. You can use the subscription to create a pay-as-you-go Cloud Volumes ONTAP system and access NetApp data services.

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

- You didn't associate a subscription when you initially added the credentials to the Console.
- You want to change the Azure Marketplace subscription that is associated with Azure credentials.

  Replacing the current marketplace subscription updates it for existing and new Cloud Volumes ONTAP systems.

Steps

1. Select **Administration > Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.

   You must select credentials that are associated with a Console agent. You can't associate a marketplace subscription with credentials that are associated with the NetApp Console.

4. To associate the credentials with an existing subscription, select the subscription from the down-down list

and select **Configure**.

5. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
   a. If prompted, log in to your Azure account.
   b. Select **Subscribe**.
   c. Fill out the form and select **Subscribe**.
   d. After the subscription process is complete, select **Configure account now**.

      You'll be redirected to the NetApp Console.

   e. From the **Subscription Assignment** page:
      - Select the Console organizations or accounts that you'd like to associate this subscription with.
      - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

        The Console replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

        For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

      - Select **Save**.

Edit credentials

Edit your Azure credentials in the Console. For example, you can update the client secret if a new secret was created for the service principal application.

Steps

1. Select **Administration > Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials and then select **Edit Credentials**.
4. Make the required changes and then select **Apply**.

Delete credentials

If you no longer need a set of credentials, you can delete them. You can only delete credentials that aren't associated with a system.

Steps

1. Select **Administration > Credentials**.
2. Select **Organization credentials**.
3. On the **Organization credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
4. Select **Delete** to confirm.

Google Cloud

Learn about Google Cloud projects and permissions

Learn how the NetApp Console uses Google Cloud credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more Google Cloud projects. For example, you might want to learn about the service account that's associated with the Console agent VM.

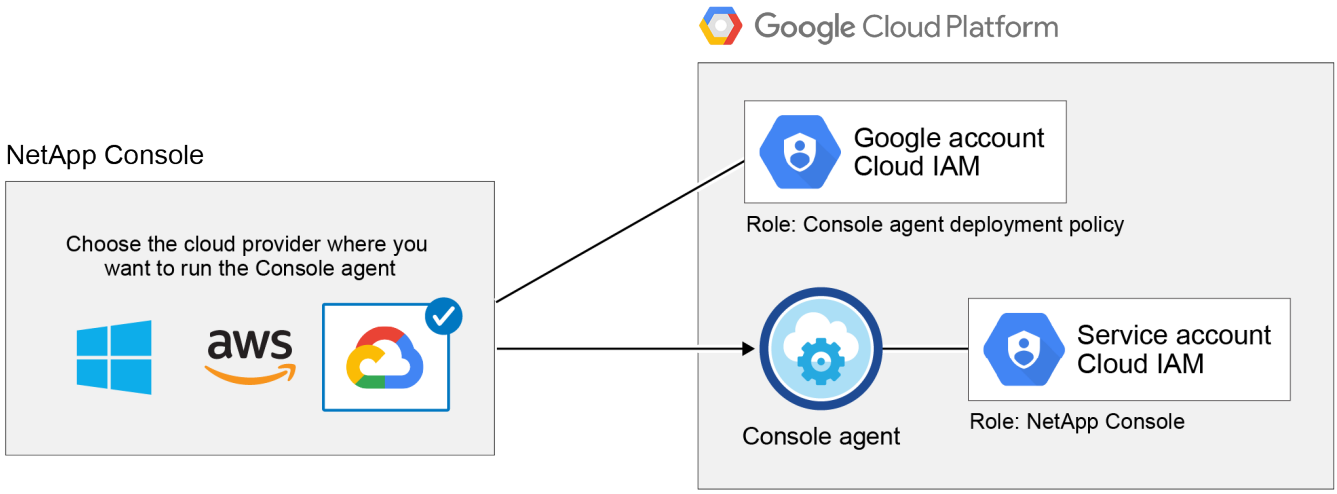
Project and permissions for NetApp Console

Before you can use the Console to manage resources in your Google Cloud project, you must first deploy a Console agent. The agent 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 Console agent directly from the Console:

1. You need to deploy a Console agent using a Google account that has permissions to launch the Console agent from the Console.
2. When deploying the Console agent, you are prompted to select a service account for the agent The Console gets permissions from the service account to create and manage Cloud Volumes ONTAP systems, to manage backups using NetApp backup and recovery, and more. Permissions are provided by attaching a custom role to the service account.

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



To learn how to set up permissions, refer to the following pages:

- Set up Google Cloud permissions for standard mode
- Set up permissions for restricted mode

Credentials and marketplace subscriptions

When you deploy a Console agent in Google Cloud, the Console creates a default set of credentials for the Google Cloud service account in the project in which the Console agent resides. These credentials must be associated with a Google Cloud Marketplace subscription so that you can pay for Cloud Volumes ONTAP and

NetApp data services.

Learn how to associate a Google Cloud Marketplace subscription.

Note the following about Google Cloud credentials and marketplace subscriptions:

- Only one set of Google Cloud credentials can be associated with a Console agent
- You can associate only one Google Cloud Marketplace subscription with the credentials
- You can replace an existing marketplace subscription with a new subscription

Project for Cloud Volumes ONTAP

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

- Learn how to set up the service account
- Learn how to deploy Cloud Volumes ONTAP in Google Cloud and select a project

Manage Console agent permissions for Google Cloud deployments

Occasionally, NetApp updates the permissions required for the service account used for the Console agent when it is deployed in Google Cloud.

Verify the required Google permissions list.

Use Google Cloud Console to update the IAM role assigned to the service account to match the new set of permissions.

Google Cloud docs: Edit a custom role

Copyright information

Trademark information