Setting up Cloud Manager

Cloud Manager 3.6

NetApp
June 10, 2024

Table of Contents

Setting up Cloud Manager

Adding cloud provider accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different cloud accounts, then you need to provide the required permissions to those accounts and then add the details to Cloud Manager.

When you deploy Cloud Manager from Cloud Central, Cloud Manager automatically adds a cloud provider account for the account in which you deployed Cloud Manager. An initial cloud provider account is not added if you manually installed the Cloud Manager software on an existing system.

Setting up and adding AWS accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different AWS accounts, then you need to provide the required permissions to those accounts and then add the details to Cloud Manager. 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.

- Granting permissions when providing AWS keys
- Granting permissions by assuming IAM roles in other accounts

Granting permissions when 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 Cloud Manager 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 Cloud Manager 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 Cloud Manager instance resides and select the IAM role that is attached to the instance.
   a. Click **Trust Relationships > Edit trust relationship**.
   b. Add the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

      Example

```
{
 "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 accounts to Cloud Manager

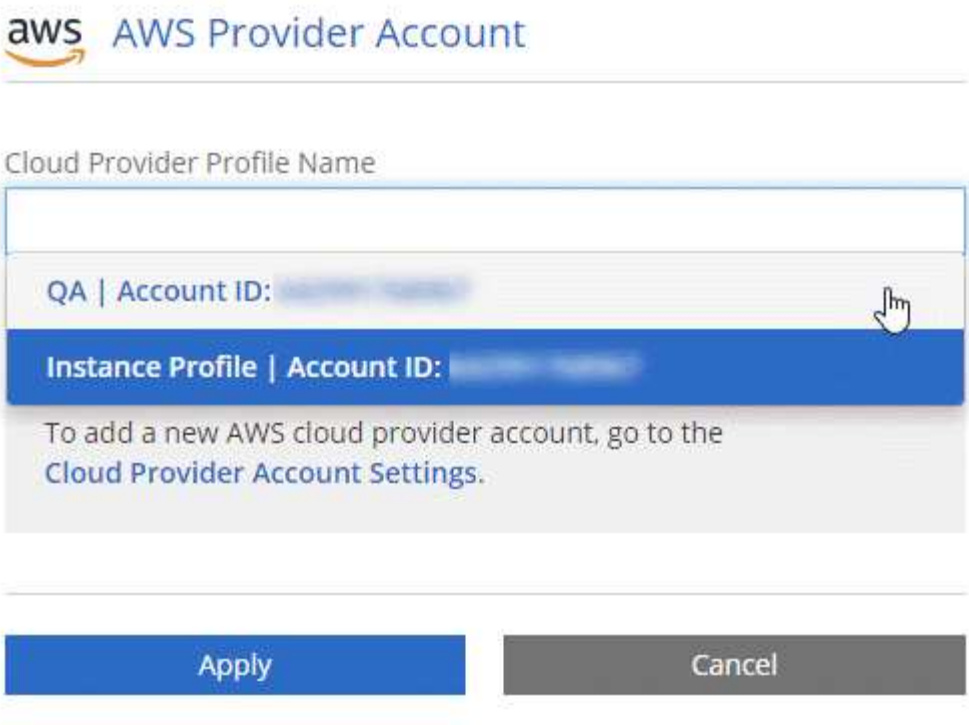
After you provide an AWS account with the required permissions, you can add the account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Account Settings**.
2. Click **Add New Account** and select **AWS**.
3. Choose whether you want to provide AWS keys or the ARN of a trusted IAM role.
4. Confirm that the policy requirements have been met and then click **Create Account**.

Result

You can now switch to another account from the Details and Credentials page when creating a new working environment:



Setting up and adding Azure accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different Azure accounts, then you need to provide the required permissions to those accounts and then add details about the accounts to Cloud Manager.

- Granting Azure permissions using a service principal
- Adding Azure accounts 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.

The following steps use the new Azure portal. If you experience any issues, you should use the Azure classic portal.

Steps

1. Create a custom role with the required Cloud Manager permissions.
2. Create an Active Directory service principal.
3. Assign the custom Cloud Manager Operator role to the service principal.

Creating a custom role with the required Cloud Manager permissions

A custom role is required to provide Cloud Manager with the permissions that it needs to launch and manage Cloud Volumes ONTAP in Azure.

Steps

1. Download the Cloud Manager Azure policy.
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 example shows how to create a custom role using the Azure CLI 2.0:

   az role definition create --role-definition C:\Policy_for_cloud_Manager_Azure_3.6.1.json

Result

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

Creating an Active Directory service principal

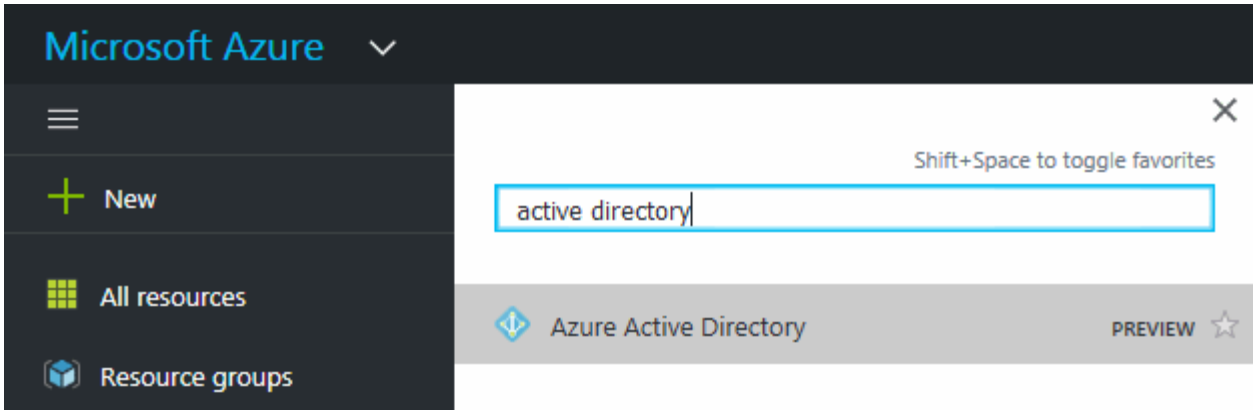
You must create an Active Directory service principal so Cloud Manager can authenticate with Azure Active Directory.

Before you begin

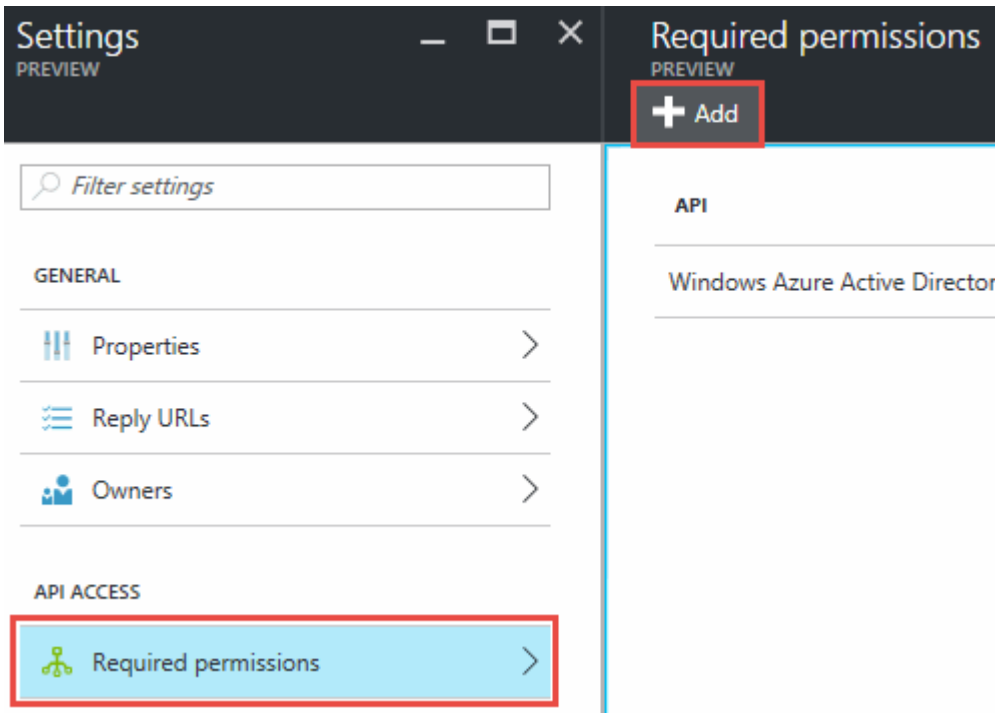
You must have the appropriate permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Use portal to create Active Directory application and service principal that can access resources.

Steps

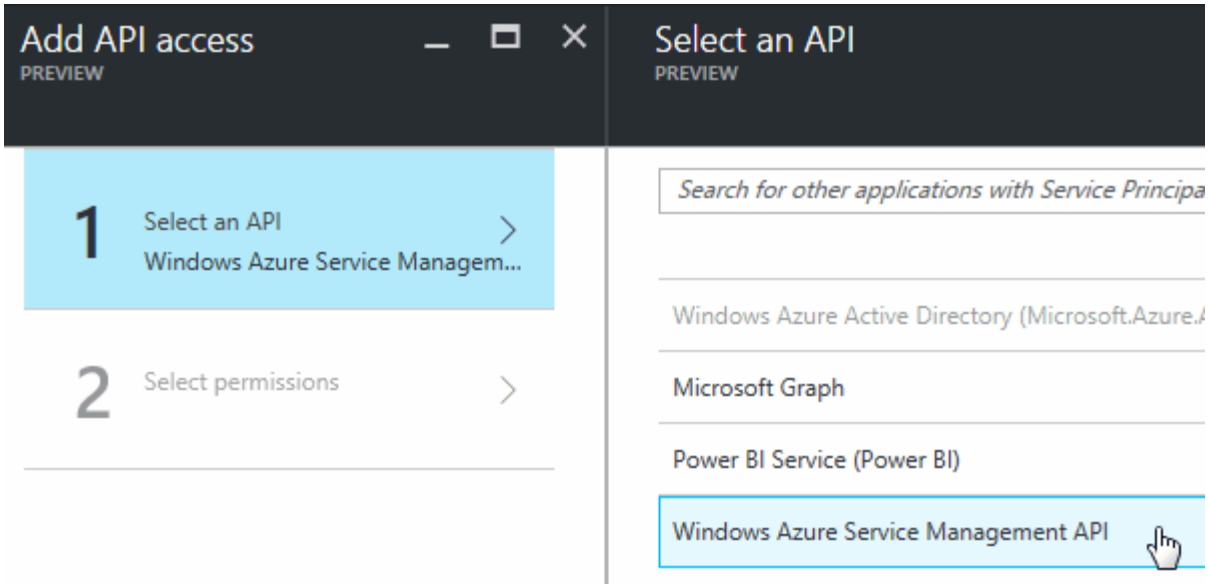
1. From the Azure portal, open the **Azure Active Directory** service.



2. In the menu, click **App registrations (Legacy)**.
3. Create the service principal:
   a. Click **New application registration**.
   b. Enter a name for the application, keep **Web app / API** selected, and then enter any URL—for example, http://url
   c. Click **Create**.
4. Modify the application to add the required permissions:
   a. Select the created application.
   b. Under Settings, click **Required permissions** and then click **Add**.



   c. Click **Select an API**, select **Windows Azure Service Management API**, and then click **Select**.



d. Click **Access Azure Service Management as organization users**, click **Select** and then click **Done**.

5. Create a key for the service principal:

   a. Under Settings, click **Keys**.

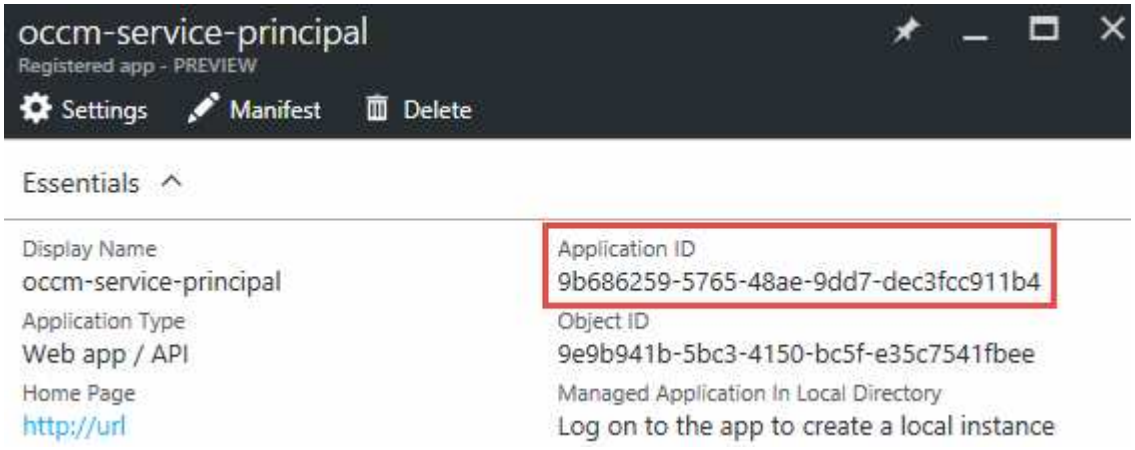
   b. Enter a description, select a duration, and then click **Save**.

   c. Copy the key value.

      You need to enter the key value when you add a cloud provider account to Cloud Manager.

   d. Click **Properties** and then copy the application ID for the service principal.

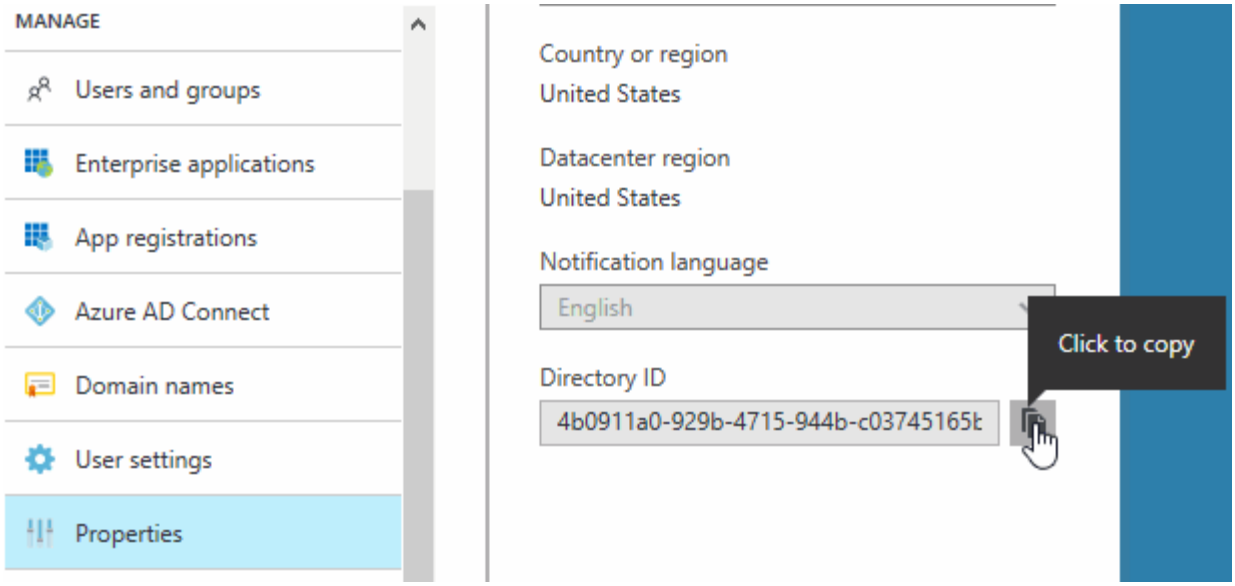
      Similar to the key value, you need to enter the application ID in Cloud Manager when you add a cloud provider account to Cloud Manager.



6. Obtain the Active Directory tenant ID for your organization:

   a. In the Active Directory menu, click **Properties**.

   b. Copy the Directory ID.



Just like the application ID and application key, you must enter the Active Directory tenant ID when you add a cloud provider account to Cloud Manager.

Result

You should now have an Active Directory service principal and you should have copied the application ID, the application key, and the Active Directory tenant ID. You need to enter this information in Cloud Manager when you add a cloud provider account.

Assigning the Cloud Manager Operator role to the service principal

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

About this task

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.

Steps

1. From the Azure portal, select **Subscriptions** in the left pane.
2. Select the subscription.
3. Click **Access control (IAM)** and then click **Add**.
4. Select the **OnCommand Cloud Manager Operator** role.
5. Search for the name of the application (you cannot find it in the list by scrolling).
6. Select the application, click **Select**, and then click **OK**.

Result

The service principal for Cloud Manager now has the required Azure permissions.

Adding Azure accounts to Cloud Manager

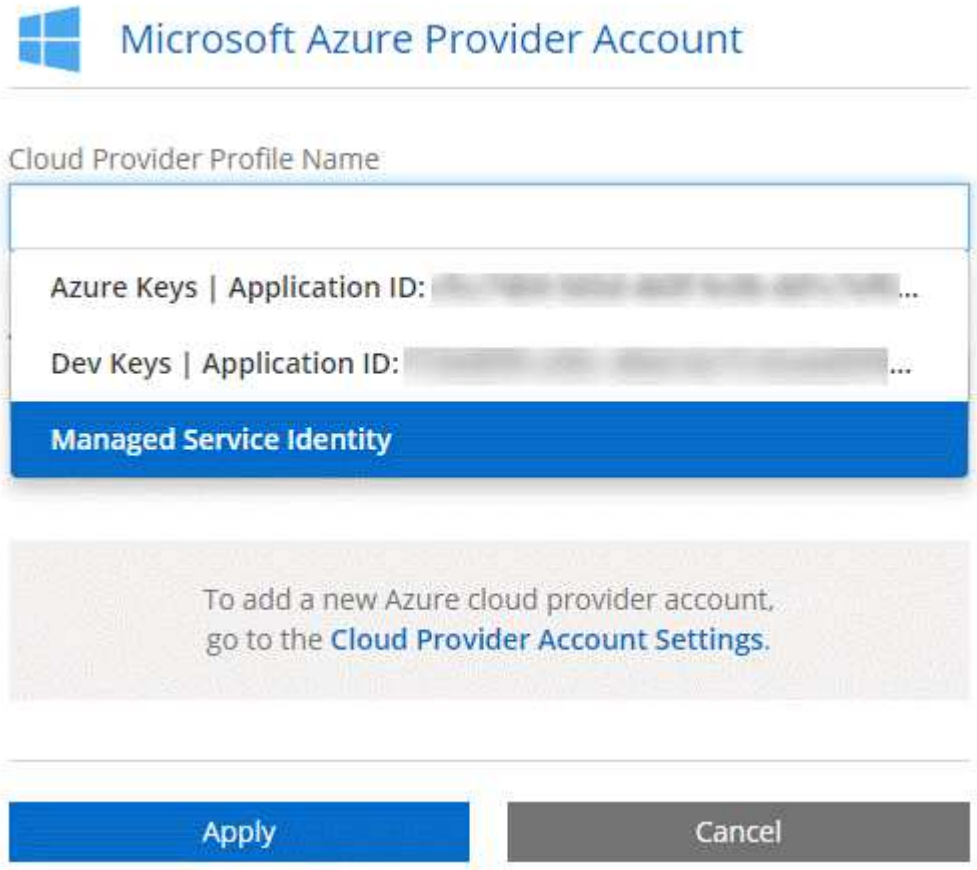
After you provide an Azure account with the required permissions, you can add the account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Account Settings**.
2. Click **Add New Account** and select **Microsoft Azure**.
3. Enter information about the Azure Active Directory service principal that grants the required permissions.
4. Confirm that the policy requirements have been met and then click **Create Account**.

Result

You can now switch to another account from the Details and Credentials page when creating a new working environment:



Associating additional Azure subscriptions with a managed identity

Cloud Manager enables you to choose the Azure account and 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 cloud provider account when you deploy Cloud Manager from NetApp Cloud Central. When you deployed Cloud Manager, Cloud Central created the OnCommand Cloud Manager Operator role and assigned it to the Cloud Manager virtual machine.

Steps

1. Log in to the Azure portal.

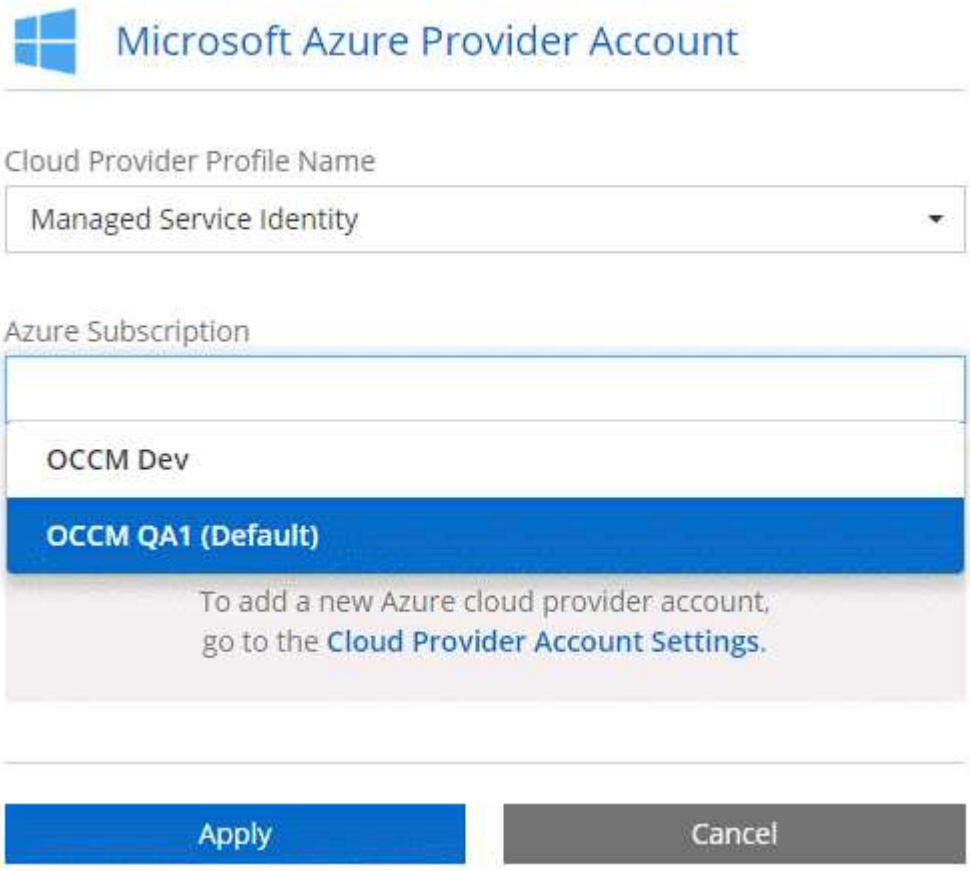
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
3. Click **Access control (IAM)**.
   a. Click **Add** > **Add role assignment** and then add the permissions:
      - Select the **OnCommand Cloud Manager Operator** role.

        OnCommand 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 Cloud Manager virtual machine was created.
      - Select the Cloud Manager 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 NetApp Support Site accounts to Cloud Manager

Adding your NetApp Support Site account to Cloud Manager is required to deploy a BYOL system. It's also required to register pay-as-you-go systems and to upgrade ONTAP software.

Watch the following video to learn how to add NetApp Support Site accounts to Cloud Manager. Or scroll down to read the steps.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Steps

1. If you don't have a NetApp Support Site account yet, register for one.
2. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Account Settings**.
3. Click **Add New Account** and select **NetApp Support Site**.
4. Specify a name for the account and then enter the user name and password.
    - The account must be a customer-level account (not a guest or temp account).
    - If you plan to deploy BYOL systems:
        - The account must be authorized to access the serial numbers of the BYOL systems.
        - If you purchased a secure BYOL subscription, then a secure NSS account is required.
5. Click **Create Account.**

What's next?

Users can now select the account when creating new Cloud Volumes ONTAP systems and when registering existing systems.

- Launching Cloud Volumes ONTAP in AWS
- Launching Cloud Volumes ONTAP in Azure
- Registering pay-as-you-go systems
- Learn how Cloud Manager manages license files

Installing an HTTPS certificate for secure access

By default, Cloud Manager uses a self-signed certificate for HTTPS access to the web console. You can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

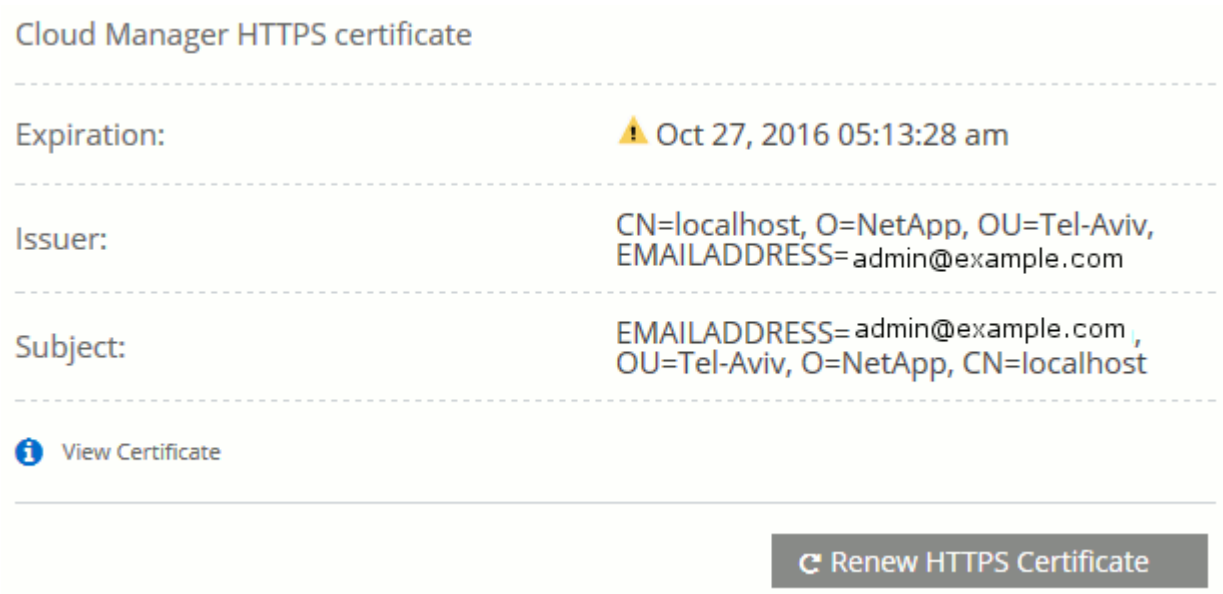
Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **HTTPS Setup**.
2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	a. Enter the host name or DNS of the Cloud Manager host (its Common Name), and then click **Generate CSR**. Cloud Manager displays a certificate signing request. b. Use the CSR to submit an SSL certificate request to a CA. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. c. Copy the contents of the signed certificate, paste it in the Certificate field, and then click **Install**.
Install your own CA-signed certificate	a. Select **Install CA-signed certificate**. b. Load both the certificate file and the private key and then click **Install**. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

Result

Cloud Manager now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a Cloud Manager system that is configured for secure access:



Setting up users and tenants

Cloud Manager enables you to add additional Cloud Central users to Cloud Manager and to isolate working environments by using tenants.

Adding users to Cloud Manager

If additional users need to use your Cloud Manager system, they must sign up for an account in NetApp Cloud Central. You can then add the users to Cloud Manager.

Steps

1. If the user does not yet have an account in NetApp Cloud Central, send them a link to your Cloud Manager system and have them sign up.

   Wait until the user confirms that they have signed up for an account.

2. In Cloud Manager, click the user icon and then click **View Users**.
3. Click **New User**.
4. Enter the email address associated with the user account, select a role, and click **Add**.

What's next?

Inform the user that they can now log in to the Cloud Manager system.

Creating tenants

Tenants enable you to isolate your working environments into separate groups. You create one or more working environments within a tenant. Learn more about tenants.

Steps

1. Click the tenants icon and then click **Add Tenant**.

2. Enter a name, description, and cost center, if needed.
3. Click **Save**.

What's next?

You can now switch to this new tenant and add Tenant Admins and Working Environment Admins to this tenant.

Setting up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to set up the AWS Key Management Service (KMS).

Steps

1. Ensure that an active Customer Master Key (CMK) exists.

   The CMK can be an AWS-managed CMK or a customer-managed CMK. It can be in the same AWS account as Cloud Manager and Cloud Volumes ONTAP or in a different AWS account.

   AWS Documentation: Customer Master Keys (CMKs)

2. Modify the key policy for each CMK by adding the IAM role that provides permissions to Cloud Manager as a *key user*.

Adding the IAM role as a key user gives Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

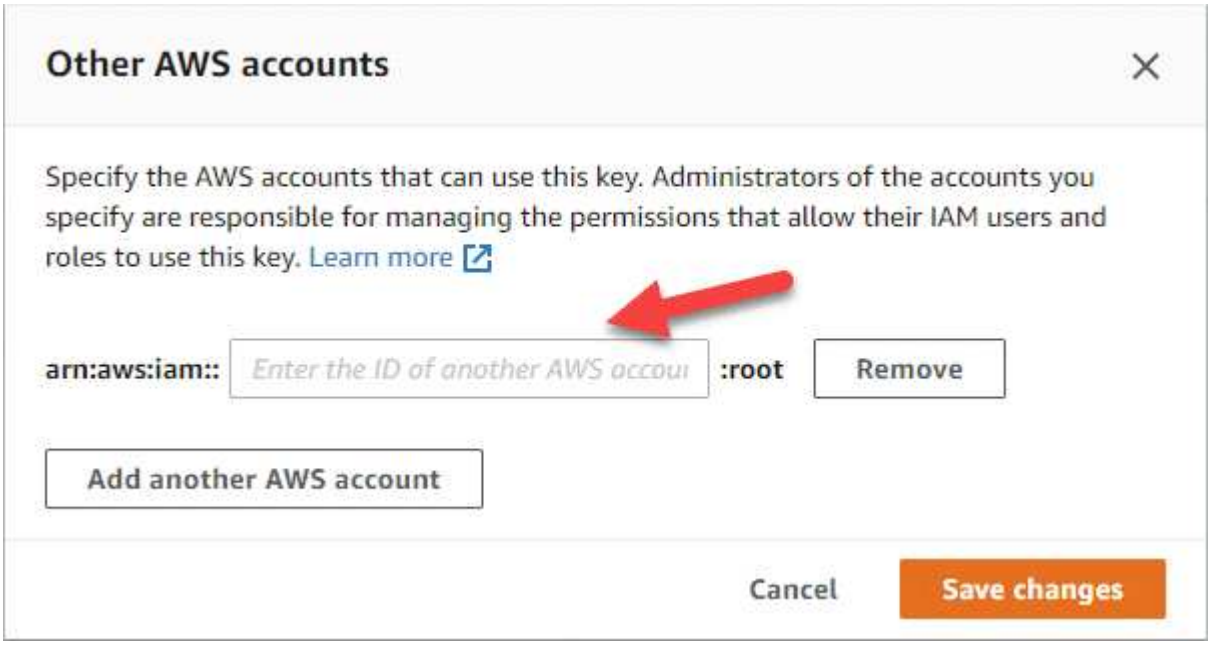
AWS Documentation: Editing Keys

3. If the CMK is in a different AWS account, complete the following steps:
   a. Go to the KMS console from the account where the CMK resides.
   b. Select the key.
   c. In the **General configuration** pane, copy the ARN of the key.

      You'll need to provide the ARN to Cloud Manager when you create the Cloud Volumes ONTAP system.

   d. In the **Other AWS accounts** pane, add the AWS account that provides Cloud Manager with permissions.

      In most cases, this is the account where Cloud Manager resides. If Cloud Manager wasn't installed in AWS, it would be the account for which you provided AWS access keys to Cloud Manager.



   e. Now switch to the AWS account that provides Cloud Manager with permissions and open the IAM console.
   f. Create an IAM policy that includes the permissions listed below.
   g. Attach the policy to the IAM role or IAM user that provides permissions to Cloud Manager.

      The following policy provides the permissions that Cloud Manager needs to use the CMK from the

external AWS account. Be sure to modify the region and account ID in the "Resource" sections.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

For additional details about this process, see AWS Documentation: Allowing External AWS Accounts to Access a CMK.

Copyright information

Trademark information