Additional ways to provide permissions

Cloud Manager 3.5

NetApp
July 23, 2020

Table of Contents

Additional ways to provide permissions

Granting permissions when Cloud Manager is not launched from Cloud Central

If you cannot launch Cloud Manager in AWS from NetApp Cloud Central, then you must provide Cloud Manager with the permissions that it needs if you want to launch and manage Cloud Volumes ONTAP in AWS.

About this task

The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use. You can grant the permissions defined in the IAM policy in one of two ways:

- You can attach an IAM role to the Cloud Manager instance in AWS.
- You can attach the IAM policy to IAM users or groups.

  You would then specify the AWS access keys for those users in Cloud Manager.

Steps

1. Download the Cloud Manager IAM policy from the following location:

   NetApp OnCommand Cloud Manager: AWS and Azure Policies

2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.
3. Grant permissions to the Cloud Manager instance or to IAM users:

Option	Description
Grant permissions to the Cloud Manager instance	a. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role. b. Attach the IAM role to Cloud Manager when you launch it from the AWS Marketplace (choose **Custom Launch**) or by modifying an existing instance from the EC2 console.
Grant permissions to IAM users	Attach the policy to IAM users or groups. For instructions, refer to AWS Documentation: Managing IAM Policies.

Result

Cloud Manager now has the permissions that it needs. If you attached the policy to IAM users, you must specify the AWS access keys for those IAM users when you set up user accounts in Cloud Manager.

Granting Azure permissions to Cloud Manager using a service principal and credentials

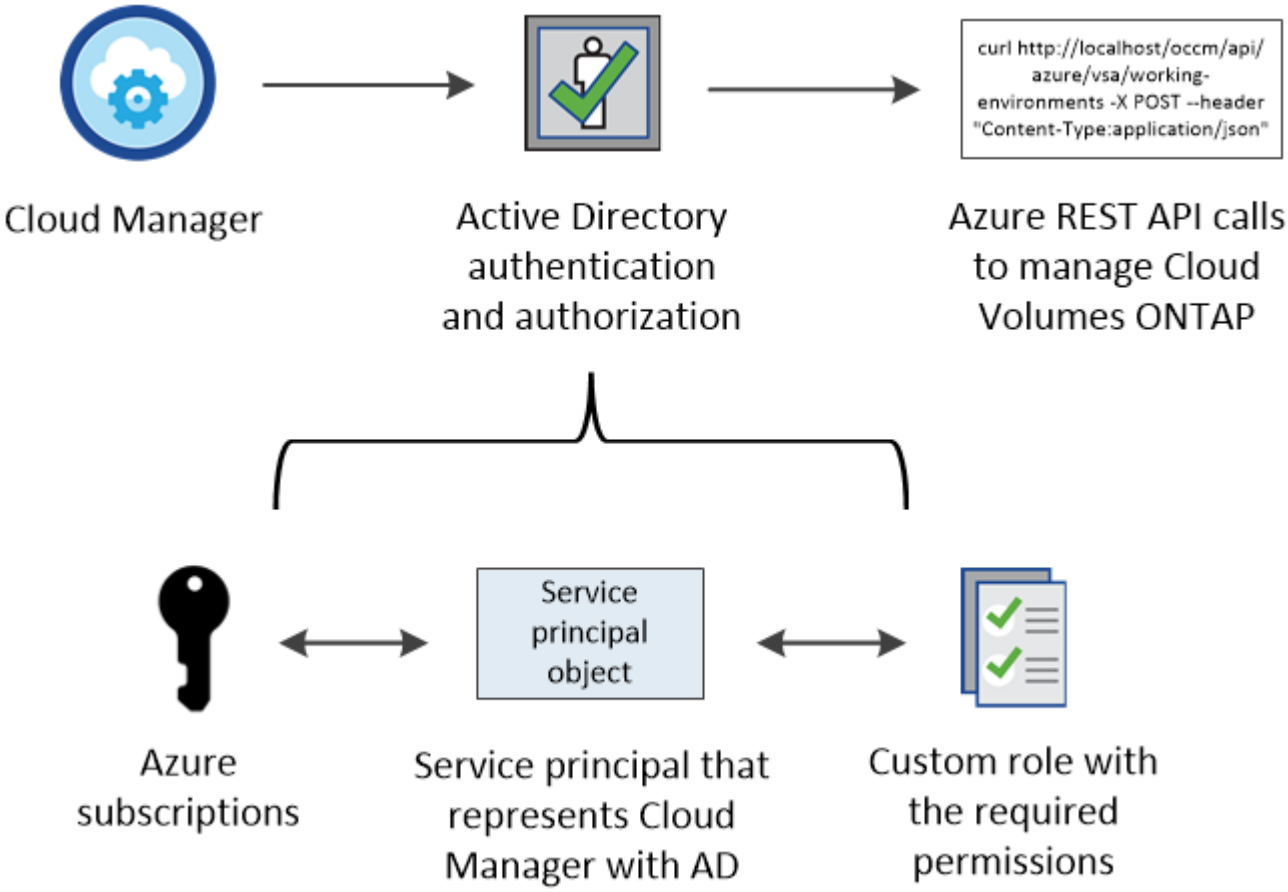
Cloud Manager needs permissions to perform actions in Azure. You can grant the required permissions by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that Cloud Manager needs.

Before you begin

Using a service principal and credentials is an alternative to using a Managed Service Identity, which is simpler and does not require credentials. To use a Managed Service Identity with Cloud Manager instead, follow instructions for new Cloud Manager virtual machines or instructions for existing Cloud Manager virtual machines.

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_5_2.json

Result

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

Creating an Active Directory service principal

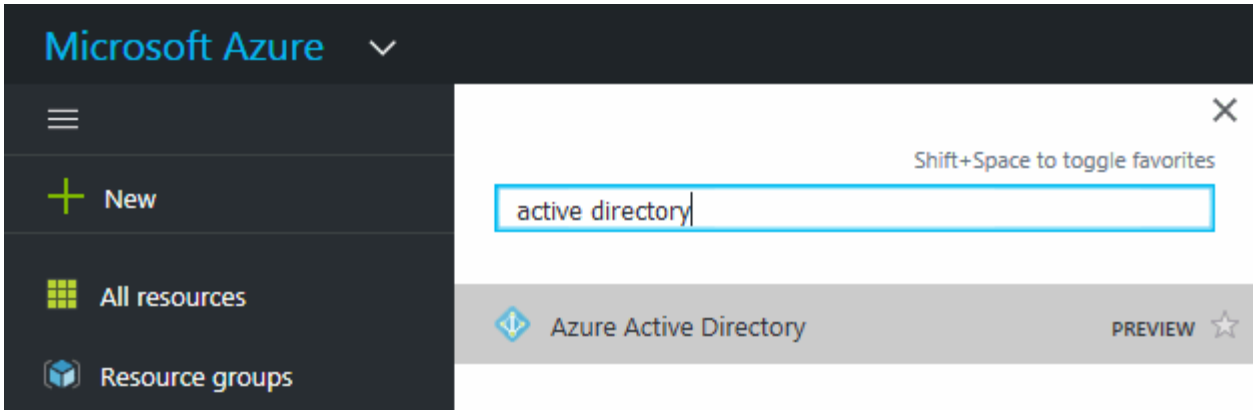
You must create an Active Directory service principal so Cloud Manager can authenticate with Azure Active Directory.

Before you begin

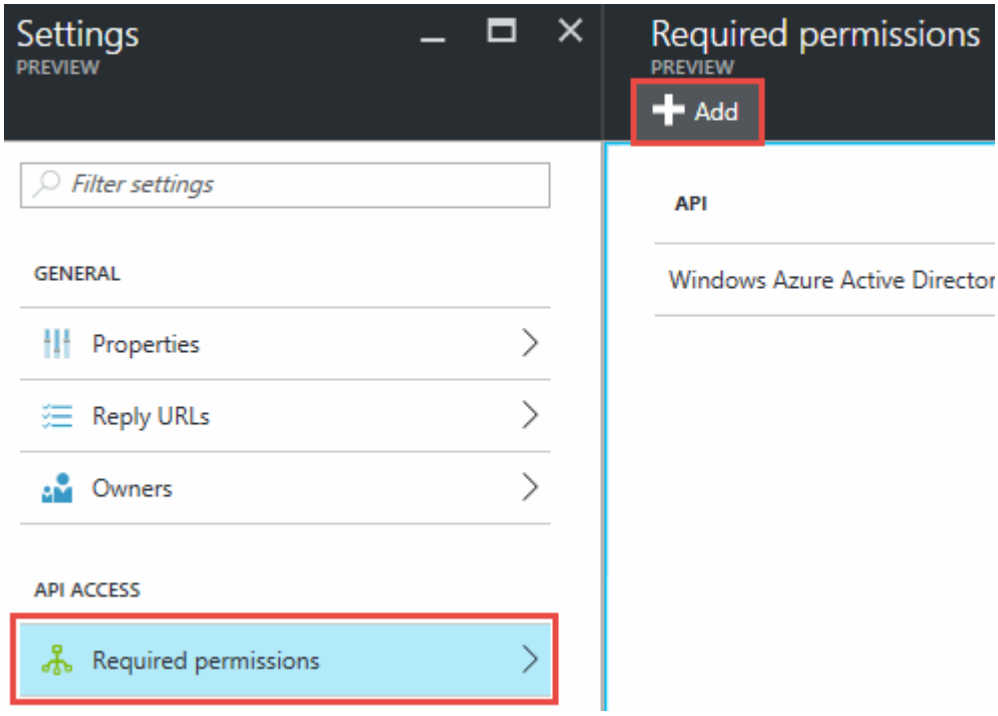
You must have the appropriate permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Use portal to create Active Directory application and service principal that can access resources

Steps

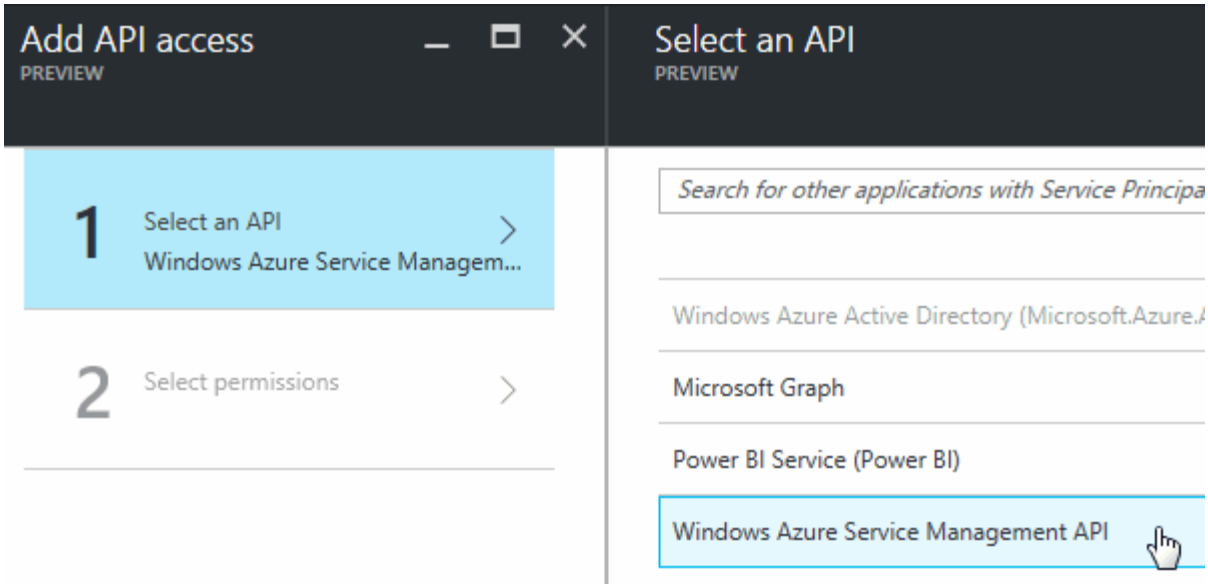
1. From the Azure portal, open the **Azure Active Directory** service.



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

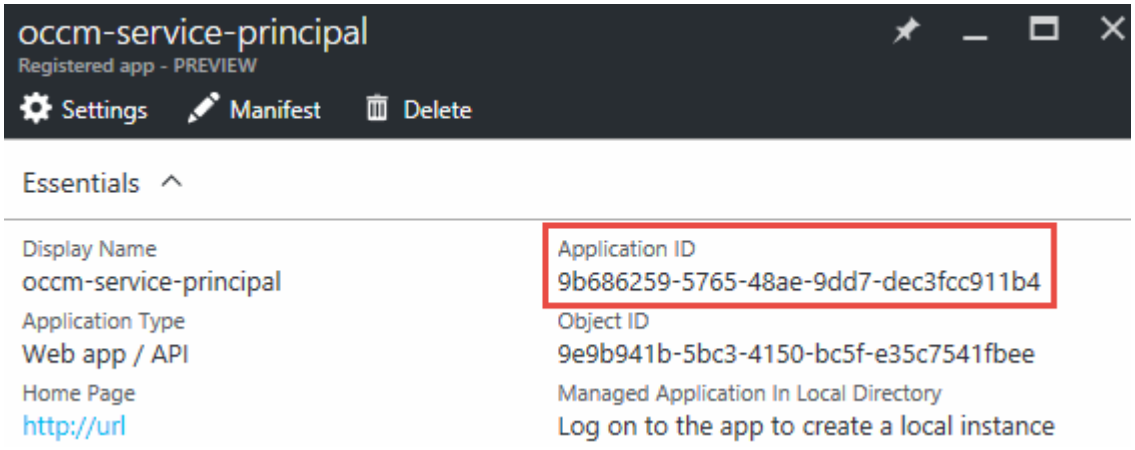
   b. Enter a description, select a duration, and then click **Save**.

   c. Copy the key value.

      You need to enter the key value in Cloud Manager when you create user accounts for this subscription.

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

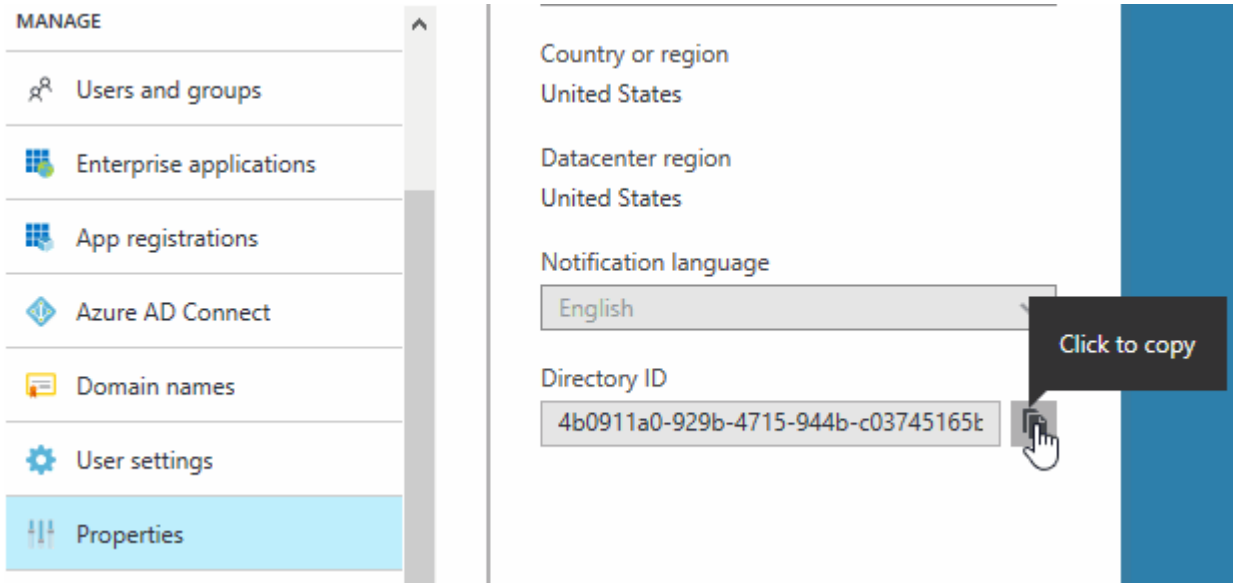
      Similar to the key value, you need to enter the application ID in Cloud Manager when you create user accounts for this subscription.



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 create Cloud Manager user accounts.

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 set up user accounts.

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.

Providing Azure permissions to an existing Cloud Manager virtual machine using a Managed Service Identity

You can provide Azure permissions to Cloud Manager by using a Managed Service Identity. A Managed Service Identity allows the Cloud Manager virtual machine to identify itself to Azure Active Directory without providing any credentials.

Managed Service Identities are not supported in the Azure US Gov regions and in the Germany regions. You must grant Azure permissions to Cloud Manager using a service principal and credentials.

About this task

If you currently provide Cloud Manager with Azure permissions through a service principal, you can change to using a Managed Service Identity instead. This method is simpler than manually setting up an Azure service principal and providing the credentials to Cloud Manager.

For more information about Managed Service Identities, refer to Azure documentation.

Steps

1. Log in to the Azure portal using an account that is associated with the Cloud Manager virtual machine.
2. Enable a Managed Service Identity on the virtual machine:
    a. Navigate to the virtual machine.
    b. Under Settings, select **Configuration**.
    c. Click **Yes** next to Managed Service Identity and then click **Save**.
3. Provide permissions to the Cloud Manager virtual machine for one or more subscriptions:
    a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
    b. Click **Access control (IAM)**.
    c. Click **Add** 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.

If you have not yet created this role, follow these instructions.

- 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**.

d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, click **Subscriptions** again, select a subscription, and then repeat the steps for that subscription.

Result

Cloud Manager now has permissions that are controlled by a Managed Service Identity. If you repeated the steps for several subscriptions, then you can choose a different subscription when creating a new working environment.