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

Cloud Manager 3.5

Aksel Davis, Ben Cammett
March 12, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm35/task_creating_service_principal.html on April 25, 2020. Always check docs.netapp.com for the latest.

Table of Contents

Granting Azure permissions to Cloud Manager using a service principal and credentials 1
Creating a custom role with the required Cloud Manager permissions 2
Creating an Active Directory service principal 2
Assigning the Cloud Manager Operator role to the service principal 6

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

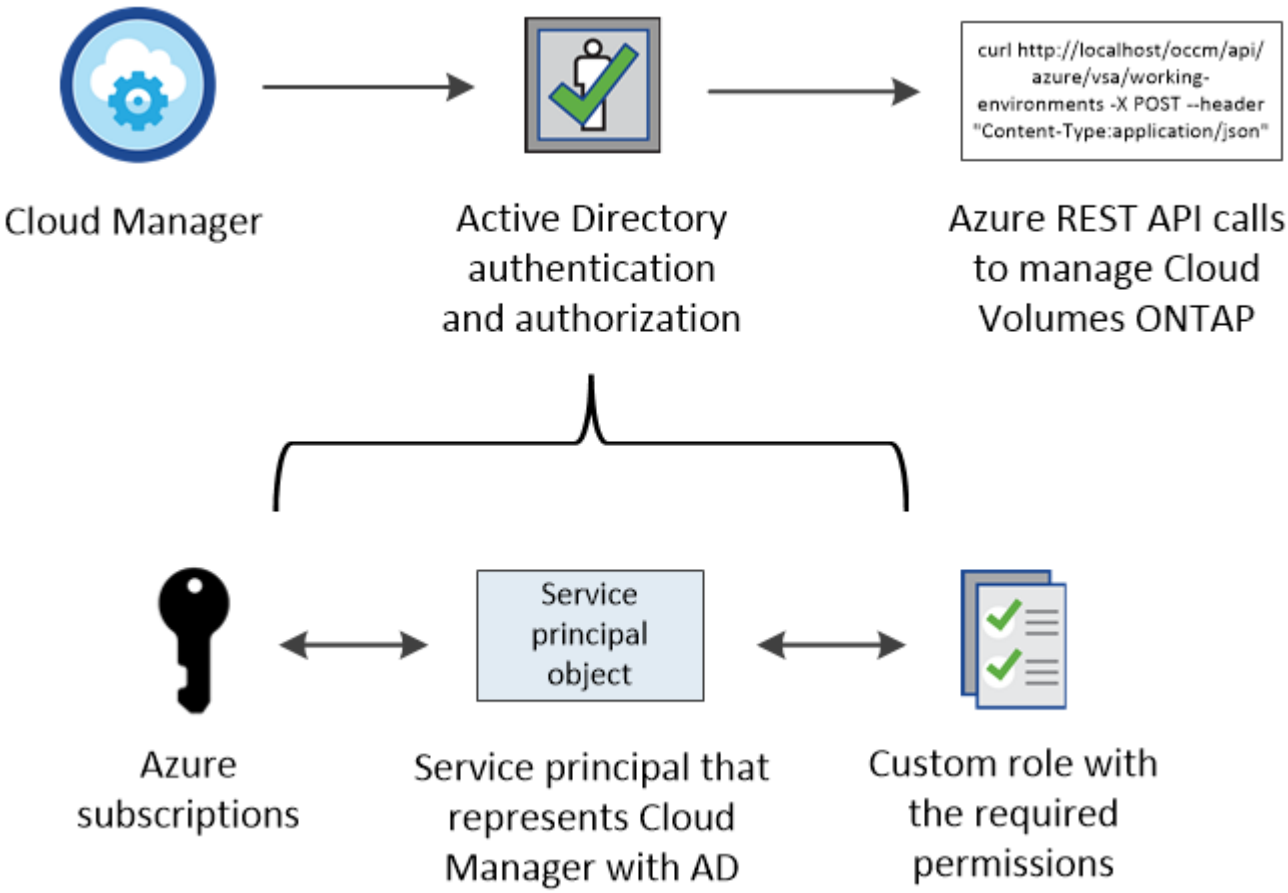
Cloud Manager needs permissions to perform actions in Azure. You can grant the required permissions by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that Cloud Manager needs.

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

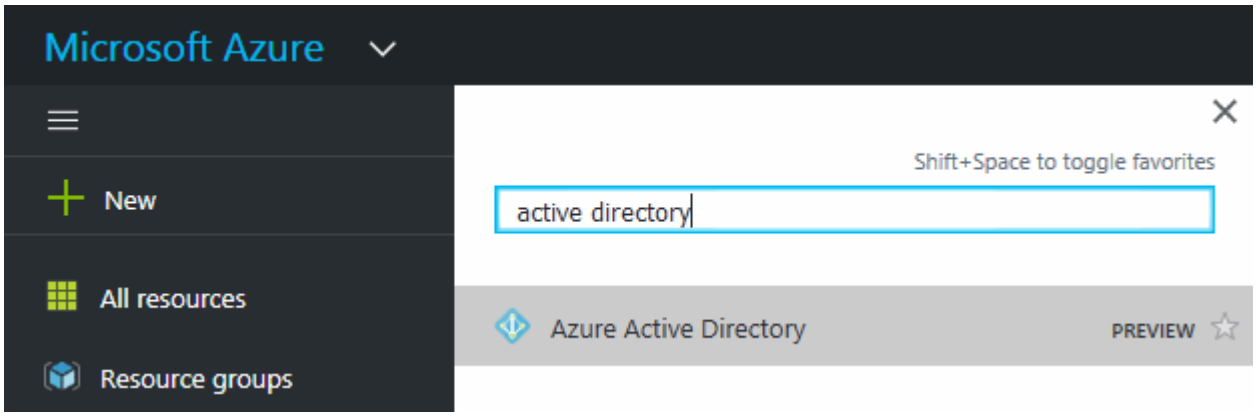
You must create an Active Directory service principal so Cloud Manager can authenticate with Azure Active Directory.

Before you begin

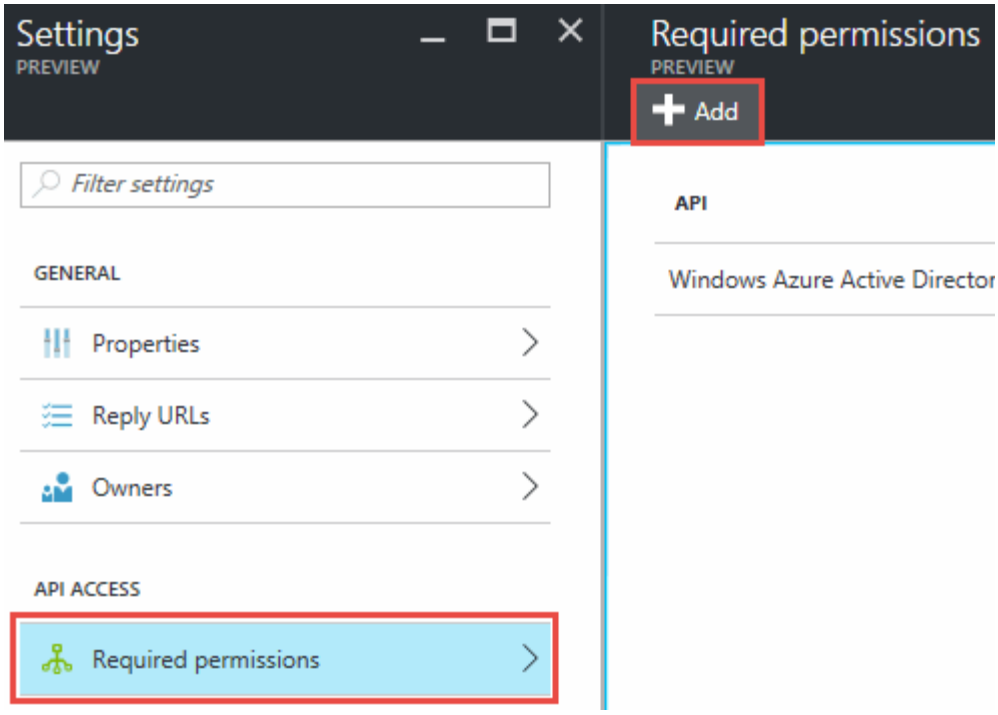
You must have the appropriate permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Use portal to create Active Directory application and service principal that can access resources

Steps

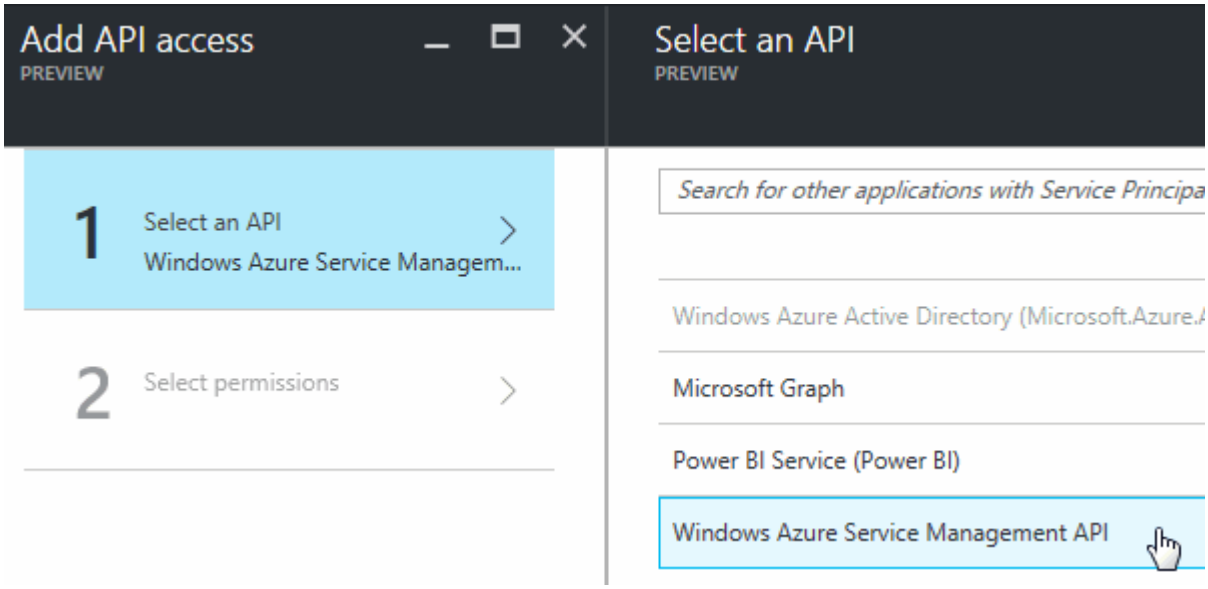
1. From the Azure portal, open the **Azure Active Directory** service.



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**.

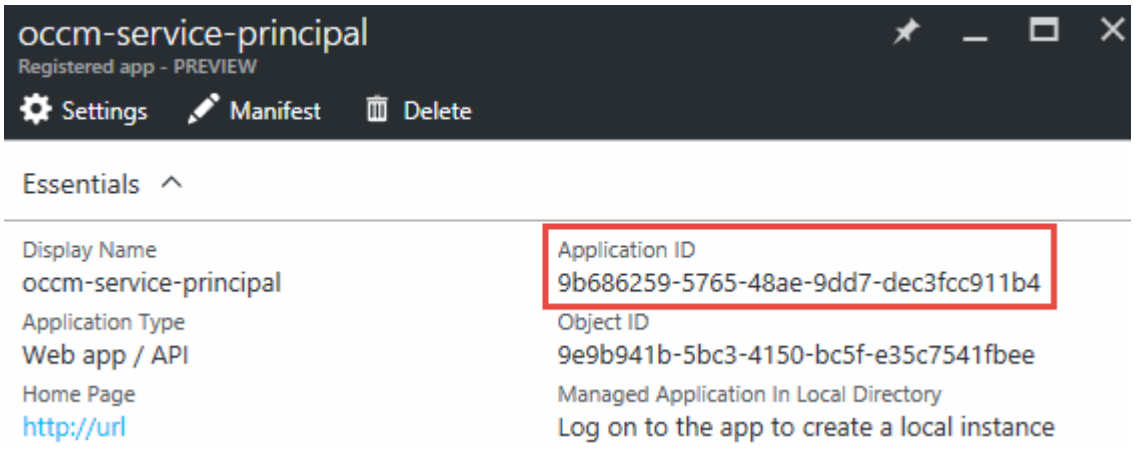
   b. Enter a description, select a duration, and then click **Save**.

   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.

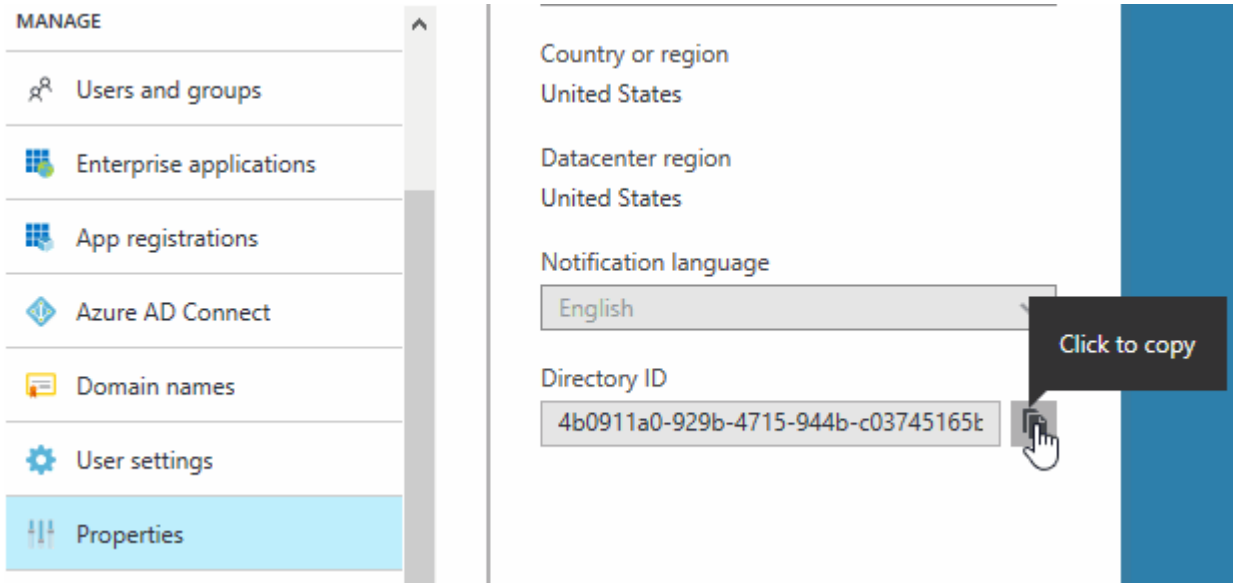
   Similar to the key value, you need to enter the application ID in Cloud Manager when you create user accounts for this subscription.



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.

Copyright Information

Copyright © 2019–2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.