Creating a Connector in Azure from Cloud Manager

Cloud Manager

Ben Cammett
October 07, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_creating_connectors_azure.html on December 07, 2020. Always check docs.netapp.com for the latest.

Table of Contents

Creating a Connector in Azure from Cloud Manager 1
Setting up Azure permissions to create a Connector 1
Creating a Connector in Azure 2

Creating a Connector in Azure from Cloud Manager

An Account Admin needs to deploy a *Connector* before you can use most Cloud Manager features. Learn when a Connector is required. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment.

This page describes how to create a Connector in Azure directly from Cloud Manager. You also have the option to create the Connector from the Azure Marketplace, or to download the software and install it on your own host.

These steps must be completed by a user who has the Account Admin role. A Workspace Admin can't create a Connector.

When you create your first Cloud Volumes ONTAP working environment, Cloud Manager will prompt you to create a Connector if you don't have one yet.

Setting up Azure permissions to create a Connector

Before you can deploy a Connector from Cloud Manager, you need to ensure that your Azure account has the correct permissions.

Steps

1. Create a custom role using the Azure policy for the Connector:
   a. Download the Azure policy for the Connector.

      Right-click the link and click **Save link as...** to download the file.

   b. Modify the JSON file by adding your Azure subscription ID to the assignable scope.

      Example

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      ],
      ```

   c. 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_Setup_As_Service_Azure.json
      ```

You should now have a custom role called *Azure SetupAsService*.

2. Assign the role to the user who will deploy the Connector from Cloud Manager:
   a. Open the **Subscriptions** service and select the user's subscription.
   b. Click **Access control (IAM)**.
   c. Click **Add** > **Add role assignment** and then add the permissions:
      - Select the **Azure SetupAsService** role.

Azure SetupAsService is the default name provided in the Connector deployment policy for Azure. If you chose a different name for the role, then select that name instead.

      - Assign access to an **Azure AD user, group, or application**.
      - Select the user account.
      - Click **Save**.

Result

The Azure user now has the permissions required to deploy the Connector from Cloud Manager.

Creating a Connector in Azure

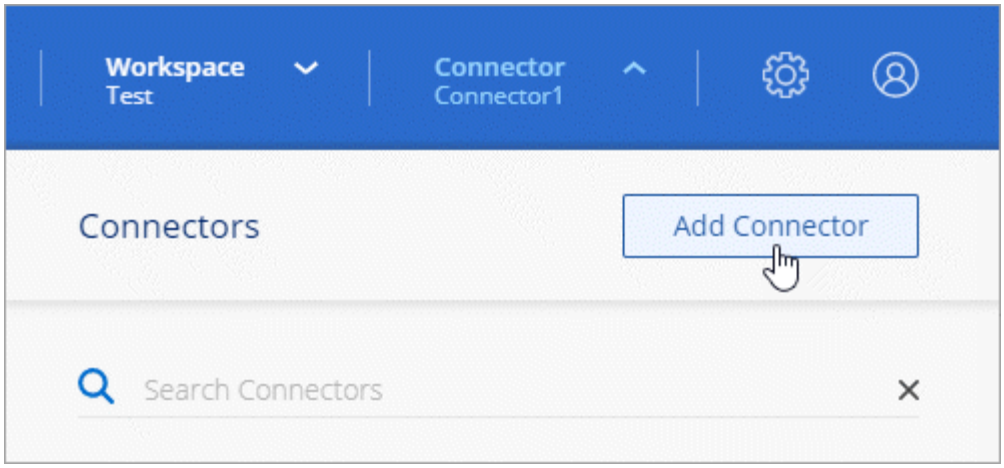
Cloud Manager enables you to create a Connector in Azure directly from its user interface.

What you'll need

- The required permissions for your Azure account.
- An Azure subscription.
- A VNet and subnet in your Azure region of choice.

Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Click **Let's Start**.
3. Choose **Microsoft Azure** as your cloud provider.

   Remember that the Connector must have a network connection to the type of working environment that you're creating and the services that you're planning to enable.

   Learn more about networking requirements for the Connector.

4. Review what you'll need and click **Continue**.
5. If you're prompted, log in to your Microsoft account, which should have the required permissions to create the virtual machine.

   The form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.

   If you're already logged in to an Azure account, then Cloud Manager will automatically use that account. If you have multiple accounts, then you might need to log out first to ensure that you're using the right account.

6. Provide the required information:
   - **VM Authentication**: Enter a name for the virtual machine and a user name and password or public key.
   - **Basic Settings**: Choose an Azure subscription, an Azure region, and whether to create a new resource group or to use an existing resource group.
   - **Network**: Choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
   - **Security Group**: Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.

     There's no incoming traffic to the Connector, unless you initiate it. HTTP and HTTPS provide access to the local UI, which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

7. Click **Create**.

   The virtual machine should be ready in about 7 minutes. You should stay on the page until the process is complete.

After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default. Learn more.

Copyright Information

Copyright © 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.