



Deploying Cloud Manager in an Azure US Government region

Cloud Manager

Ben Cammett
May 29, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_installing_azure_gov.html on June 15, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Deploying Cloud Manager in an Azure US Government region 1
 - Deploying Cloud Manager from the Azure US Government Marketplace 1
 - Granting Azure permissions to Cloud Manager using a managed identity 3

Deploying Cloud Manager in an Azure US Government region

To get Cloud Manager up and running in a US Government region, first deploy Cloud Manager from the Azure Government Marketplace. Then provide the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP systems.

For a list of supported Azure US Government regions, see [Cloud Volumes Global Regions](#).

Deploying Cloud Manager from the Azure US Government Marketplace

Cloud Manager is available as an image in the Azure US Government Marketplace.

Steps

1. Ensure that the Azure Government Marketplace is enabled in your subscription:
 - a. Log into the portal as an Enterprise Administrator.
 - b. Navigate to **Manage**.
 - c. Under **Enrollment Details**, click the pencil icon next to **Azure Marketplace**.
 - d. Select **Enabled**.
 - e. Click **Save**.

[Microsoft Azure Documentation: Azure Government Marketplace](#)

2. Search for OnCommand Cloud Manager in the Azure US Government portal.
3. Click **Create** and follow the steps to configure the virtual machine.

Note the following as you configure the virtual machine:

- Cloud Manager can perform optimally with either HDD or SSD disks.
- You should choose a VM size that has at least 4 vCPUs and 7 GB of RAM. We recommend DS3 v2.
- For the network security group, it is best to choose **Advanced**.

The **Advanced** option creates a new security group that includes the required inbound rules for Cloud Manager. If you choose Basic, refer to [Security group rules](#) for the list of required rules.

4. On the summary page, review your selections and click **Create** to start the deployment.

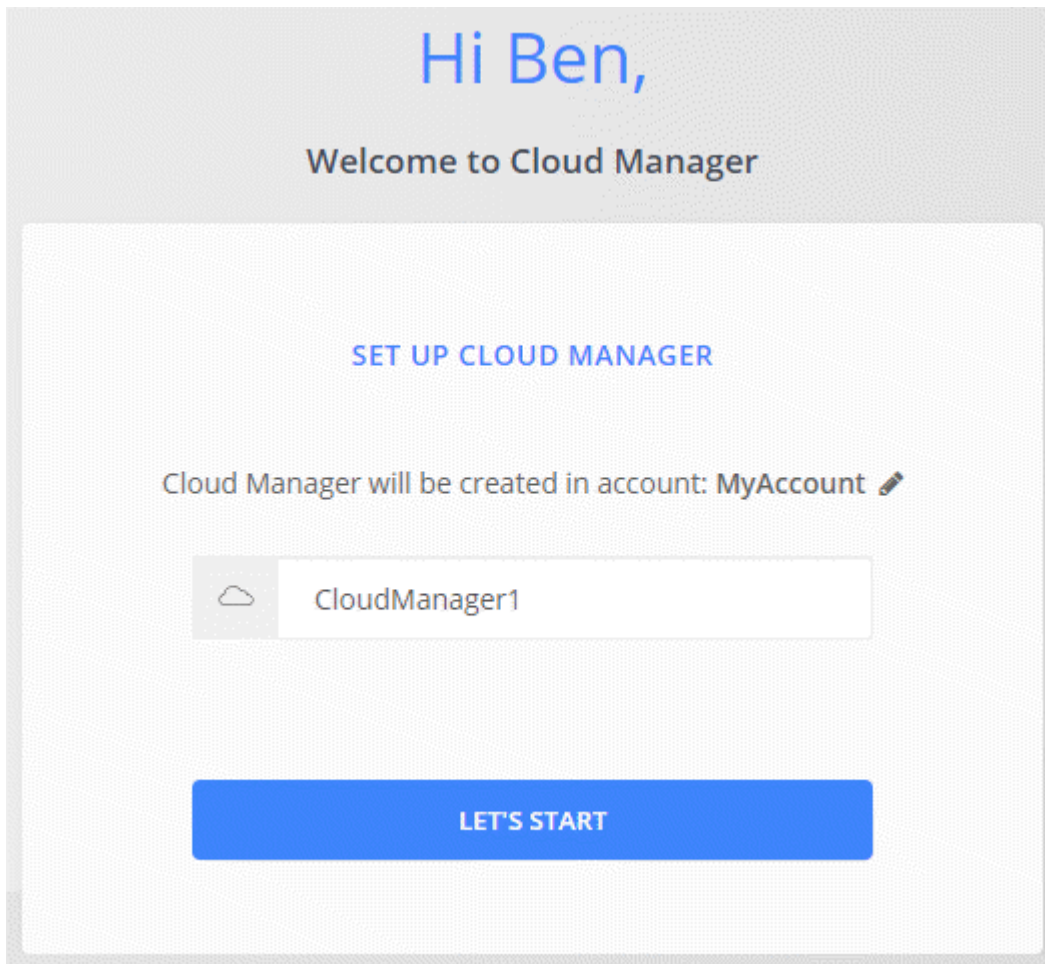
Azure deploys the virtual machine with the specified settings. The virtual machine and Cloud

Manager software should be running in approximately five minutes.

5. Open a web browser from a host that has a connection to the Cloud Manager virtual machine and enter the following URL:

`http://ipaddress:80`

6. After you log in, set up Cloud Manager:
 - a. Specify the Cloud Central account to associate with this Cloud Manager system.
[Learn about Cloud Central accounts.](#)
 - b. Enter a name for the system.



Result

Cloud Manager is now installed and set up. You must grant Azure permissions before users can deploy Cloud Volumes ONTAP in Azure.

Granting Azure permissions to Cloud Manager using a managed identity

The easiest way to provide permissions is by enabling a [managed identity](#) on the Cloud Manager virtual machine and then by assigning the required permissions to the virtual machine. If preferred, an alternative way is to [grant Azure permissions using a service principal](#).

Steps

1. Enable a managed identity on the Cloud Manager virtual machine:
 - a. Navigate to the Cloud Manager virtual machine and select **Identity**.
 - b. Under **System Assigned**, click **On** and then click **Save**.
2. Create a custom role using the Cloud Manager policy:
 - a. Download the [Cloud Manager Azure policy](#).
 - 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 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_3.8.5.json
```

You should now have a custom role called OnCommand Cloud Manager Operator that you can assign to the Cloud Manager virtual machine.

3. Assign the role 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**, click **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.
 - Type the name of the virtual machine and then select it.
 - Click **Save**.
- d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, switch to that subscription and then repeat these steps.

Result

Cloud Manager now has the permissions that it needs to deploy and manage Cloud Volumes ONTAP in Azure.

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.