



Azure credentials and permissions

Cloud Manager

Ben Cammett
July 19, 2021

Table of Contents

- Azure credentials and permissions 1
 - Initial Azure credentials 1
 - Additional Azure subscriptions for a managed identity..... 1
 - Additional Azure credentials..... 2

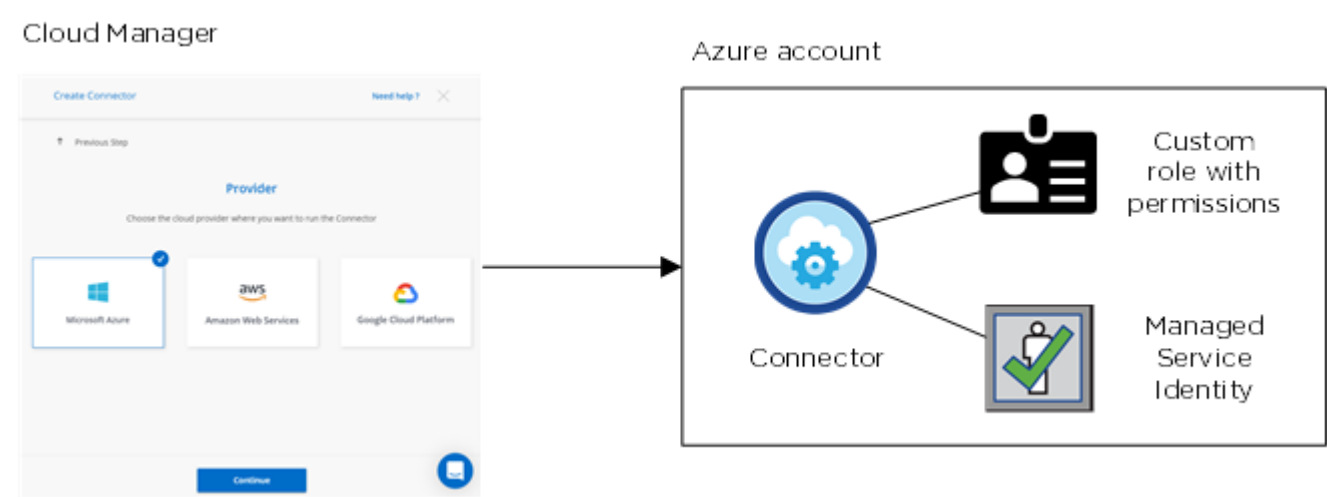
Azure credentials and permissions

Cloud Manager enables you to choose the Azure credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

Initial Azure credentials

When you deploy a Connector from Cloud Manager, you need to use an Azure account that has permissions to deploy the Connector virtual machine. The required permissions are listed in the [Connector deployment policy for Azure](#).

When Cloud Manager deploys the Connector virtual machine in Azure, it enables a [system-assigned managed identity](#) on virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides Cloud Manager with permissions to manage resources and processes within that Azure subscription. [Review how Cloud Manager uses the permissions](#).



Cloud Manager selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP:

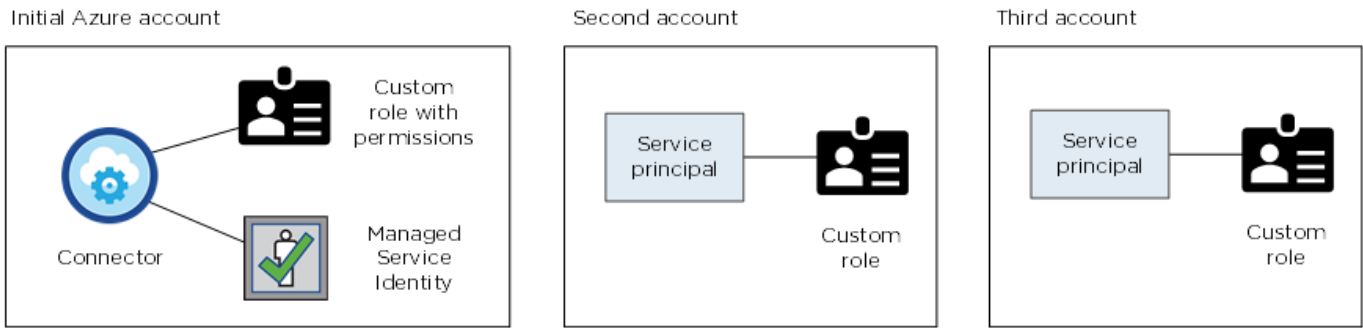
Details & Credentials			
Managed Service Ide...	OCCM QA1	ⓘ No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

Additional Azure subscriptions for a managed identity

The managed identity is associated with the subscription in which you launched the Connector. If you want to select a different Azure subscription, then you need to [associate the managed identity with those subscriptions](#).

Additional Azure credentials

If you want to deploy Cloud Volumes ONTAP using different Azure credentials, then you must grant the required permissions by [creating and setting up a service principal in Azure Active Directory](#) for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom role that provides permissions:



You would then [add the account credentials to Cloud Manager](#) by providing details about the AD service principal.

After you add another set of credentials, you can switch to them when creating a new working environment:

The screenshot shows the 'Edit Account & Add Subscription' form. The 'Credentials' dropdown menu is open, displaying the following options:

- cloud-manager-app | Application ID: 57c42424-88a0-480a.
- Managed Service Identity** (highlighted in blue)
- OCCM QA1 (Default)

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from NetApp Cloud Central. You can also deploy a Connector in Azure from the [Azure Marketplace](#), and you can [install the Connector on-premises](#).

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the managed identity for the Connector, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Connector, but you can provide permissions just like you would for additional accounts by using a service principal.

Copyright Information

Copyright © 2021 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.