



# Cloud provider accounts

## Cloud Manager 3.7

NetApp  
June 06, 2022

# Table of Contents

- Cloud provider accounts . . . . . 1
  - AWS accounts and permissions . . . . . 1
  - Azure accounts and permissions . . . . . 3
  - Google Cloud projects, permissions, and accounts . . . . . 4

# Cloud provider accounts

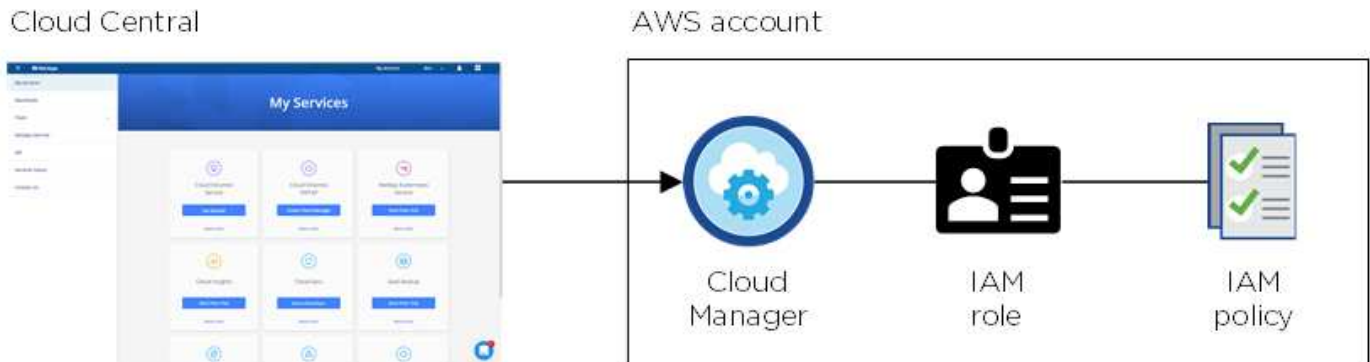
## AWS accounts and permissions

Cloud Manager enables you to choose the AWS account in which you want to deploy a Cloud Volumes ONTAP system. You can deploy all of your Cloud Volumes ONTAP systems in the initial AWS account, or you can set up additional accounts.

### The initial AWS account

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an AWS account that has permissions to launch the Cloud Manager instance. The required permissions are listed in the [NetApp Cloud Central policy for AWS](#).

When Cloud Central launches the Cloud Manager instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP in that AWS account. [Review how Cloud Manager uses the permissions](#).



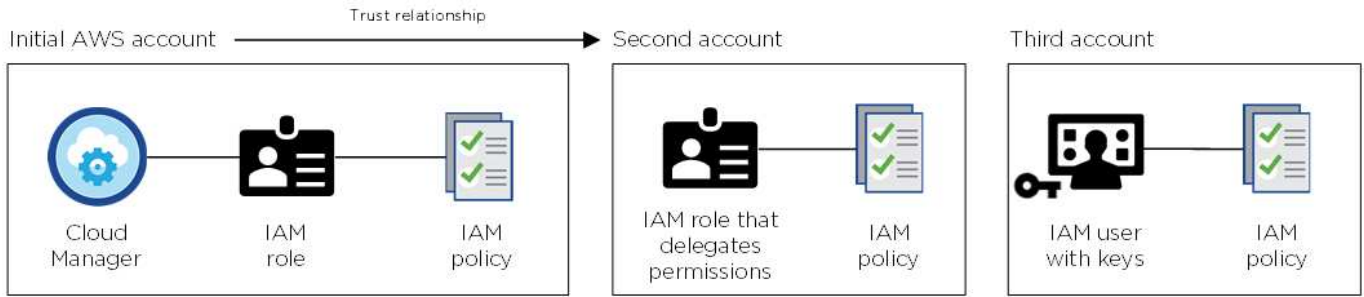
Cloud Manager selects this cloud provider account by default when you create a new working environment:

### Details & Credentials

This working environment will be created in Cloud Provider Account: Instance Profile | Account ID: [REDACTED] | [Switch Account](#)

### Additional AWS accounts

If you want to launch Cloud Volumes ONTAP in different AWS accounts, then you can either [provide AWS keys for an IAM user or the ARN of a role in a trusted account](#). The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:



You would then [add the cloud provider accounts to Cloud Manager](#) by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

After you add another account, you can switch to it when creating a new working environment:

## aws AWS Provider Account

Cloud Provider Profile Name

QA | Account ID: XXXXXXXXXX

Instance Profile | Account ID: XXXXXXXXXX

To add a new AWS cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

### What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method from NetApp Cloud Central. You can also deploy Cloud Manager in AWS from the [AWS Marketplace](#) and you can [install Cloud Manager on-premises](#).

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

For on-premises deployments, you can't set up an IAM role for the Cloud Manager system, but you can provide permissions just like you would for additional AWS accounts.

# Azure accounts and permissions

Cloud Manager enables you to choose the Azure account in which you want to deploy a Cloud Volumes ONTAP system. You can deploy all of your Cloud Volumes ONTAP systems in the initial Azure account, or you can set up additional accounts.

## The initial Azure account

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

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



Cloud Manager selects this cloud provider account by default when you create a new working environment:

### Details & Credentials

This working environment will be created in Cloud Provider Account: Managed Service Identity | Azure Subscription: OCCM QA1 | [Switch Account](#)

## Additional Azure subscriptions for the initial account

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

## Additional Azure accounts

If you want to deploy Cloud Volumes ONTAP in different Azure accounts, 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 cloud provider accounts to Cloud Manager](#) by providing details about the AD service principal.

After you add another account, you can switch to it when creating a new working environment:

The screenshot shows the 'Microsoft Azure Provider Account' configuration window. At the top left is the Microsoft logo. The title is 'Microsoft Azure Provider Account'. Below the title is a section for 'Cloud Provider Profile Name' with a text input field. Underneath are two rows of configuration options: 'Azure Keys | Application ID: [redacted] ...' and 'Dev Keys | Application ID: [redacted] ...'. A blue button labeled 'Managed Service Identity' is positioned below these options. A grey informational box contains the text: 'To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).' At the bottom of the window are two buttons: a blue 'Apply' button and a grey 'Cancel' button.

### What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method from NetApp Cloud Central. You can also deploy Cloud Manager in Azure from the [Azure Marketplace](#), and you can [install Cloud Manager 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 Cloud Manager, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Cloud Manager system, but you can provide permissions just like you would for additional accounts.

## Google Cloud projects, permissions, and accounts

A service account provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP systems in the same project as Cloud Manager, or in different projects. Google Cloud accounts that you add to Cloud Manager are used to enable data tiering.

## Project and permissions for Cloud Manager

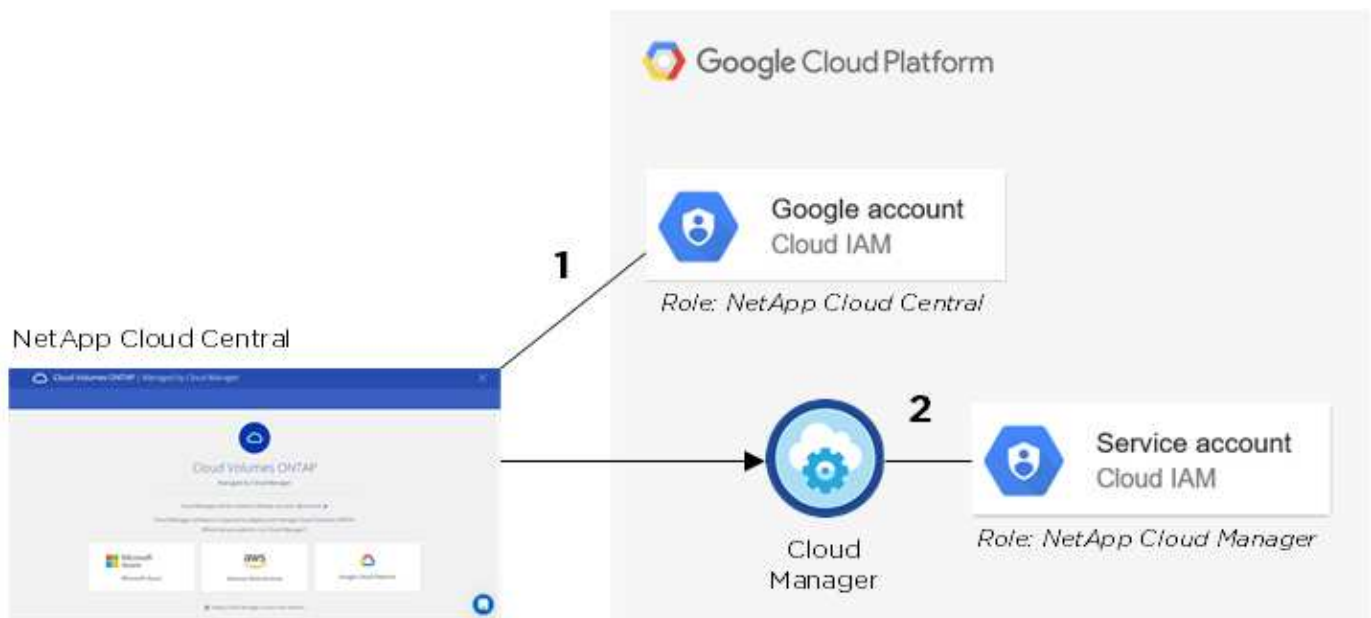
Before you can deploy Cloud Volumes ONTAP in Google Cloud, you must first deploy Cloud Manager in a Google Cloud project. Cloud Manager can't be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy Cloud Manager from [NetApp Cloud Central](#):

1. You need to deploy Cloud Manager using a Google account that has permissions to launch the Cloud Manager VM instance from Cloud Central.
2. When deploying Cloud Manager, you are prompted to select a [service account](#) for the VM instance. Cloud Manager gets permissions from the service account to create and manage Cloud Volumes ONTAP systems on your behalf. Permissions are provided by attaching a custom role to the service account.

We have set up two YAML files that include the required permissions for the user and the service account. [Learn how to use the YAML files to set up permissions.](#)

The following image depicts the permission requirements described in numbers 1 and 2 above:



## Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as Cloud Manager, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Cloud Manager service account and role to that project.

- [Learn how to set up the Cloud Manager service account \(see step 4\).](#)
- [Learn how to deploy Cloud Volumes ONTAP in GCP and select a project.](#)

## Account for data tiering

Adding a Google Cloud account to Cloud Manager is required to enable data tiering on a Cloud Volumes ONTAP system. Data tiering automatically tiers cold data to low-cost object storage, enabling you to reclaim space on your primary storage and shrink secondary storage.

When you add the account, you need to provide Cloud Manager with a storage access key for a service

account that has Storage Admin permissions. Cloud Manager uses the access keys to set up and manage a Cloud Storage bucket for data tiering.

After you add a Google Cloud account, you can then enable data tiering on individual volumes when you create, modify, or replicate them.

- [Learn how to set up and add GCP accounts to Cloud Manager.](#)
- [Learn how to tier inactive data to low-cost object storage.](#)



## Copyright Information

Copyright © 2022 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.