



Set up Cloud Manager

Cloud Manager

NetApp

June 15, 2020

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

Table of Contents

- Set up Cloud Manager 1
 - Setting up workspaces and users in the Cloud Central account 1
 - Adding AWS credentials and subscriptions in Cloud Manager 4
 - Setting up and adding Azure credentials to Cloud Manager 8
 - Setting up and adding GCP accounts for data tiering with 9.6 16
 - Adding NetApp Support Site accounts to Cloud Manager 19
 - Installing an HTTPS certificate for secure access..... 20
 - Setting up the AWS KMS..... 21

Set up Cloud Manager

Setting up workspaces and users in the Cloud Central account

Each Cloud Manager system is associated with a *NetApp Cloud Central account*. Set up the Cloud Central account associated with your Cloud Manager system so a user can access Cloud Manager and deploy Cloud Volumes ONTAP systems in workspaces. Just add a user or add multiple users and workspaces.

The account is maintained in Cloud Central, so any changes that you make are available to other Cloud Manager systems and to other NetApp cloud data services. [Learn more about how Cloud Central accounts work](#).

Adding workspaces

In Cloud Manager, workspaces enable you to isolate a set of working environments from other working environments and from other users. For example, you can create two workspaces and associate separate users with the workspaces.

Steps

1. Click **Account Settings**.



2. Click **Workspaces**.
3. Click **Add New Workspace**.
4. Enter a name for the workspace and click **Add**.

After you finish

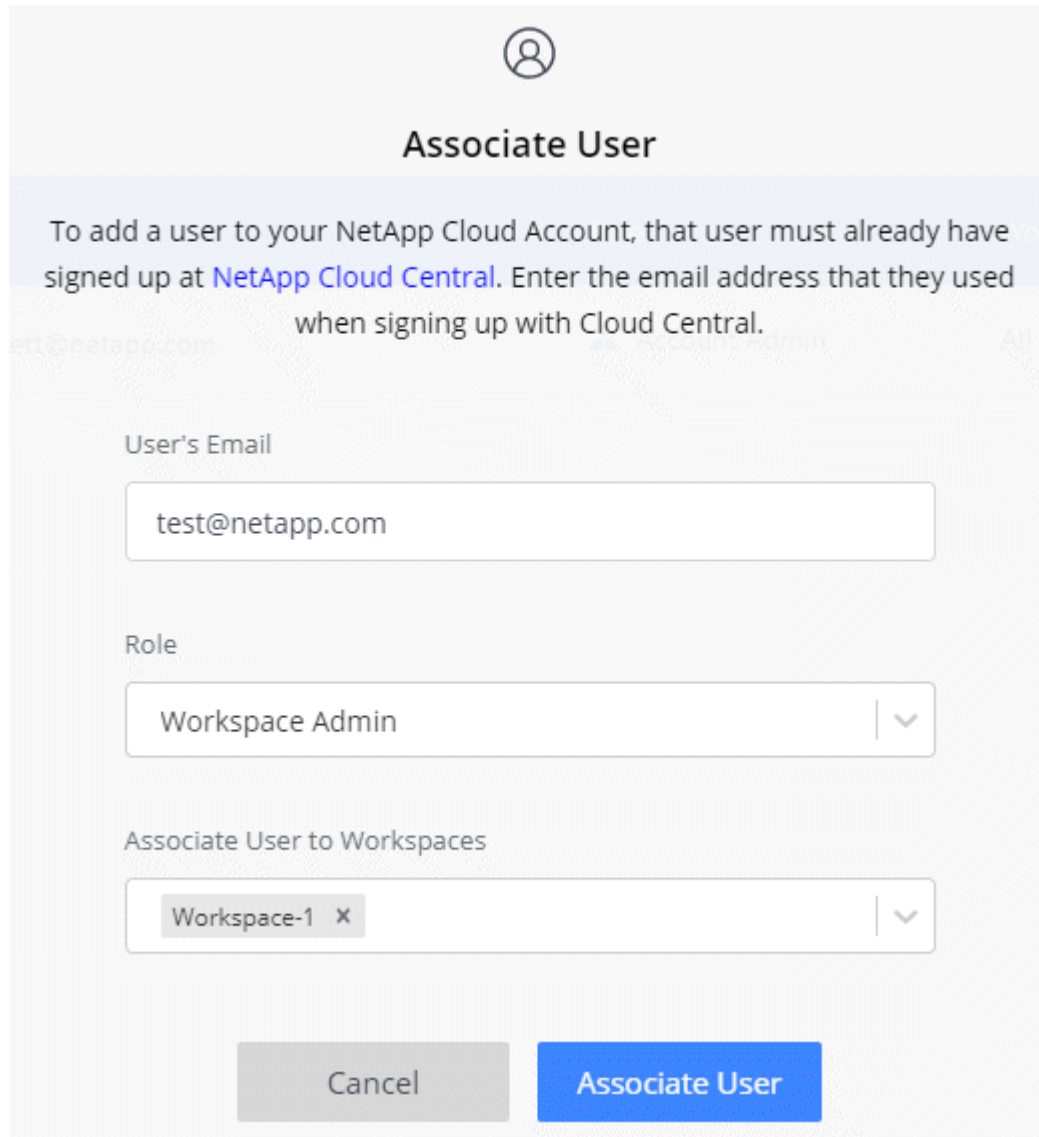
You can now associate users and service connectors with the workspace.

Adding users

Associate Cloud Central users with the Cloud Central account so those users can create and manage working environments in Cloud Manager.

Steps

1. If the user has not already done so, ask the user to go to [NetApp Cloud Central](#) and create an account.
2. In Cloud Manager, click **Account Settings**.
3. In the Users tab, click **Associate User**.
4. Enter the user's email address and select a role for the user:
 - **Account Admin**: Can perform any action in Cloud Manager.
 - **Workspace Admin**: Can create and manage resources in assigned workspaces.
5. If you selected Workspace Admin, select one or more workspaces to associate with that user.



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title is a light blue banner with instructions: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below this are three input fields: "User's Email" containing "test@netapp.com", "Role" set to "Workspace Admin", and "Associate User to Workspaces" containing "Workspace-1". At the bottom are "Cancel" and "Associate User" buttons.

Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

6. Click **Associate User**.

Result

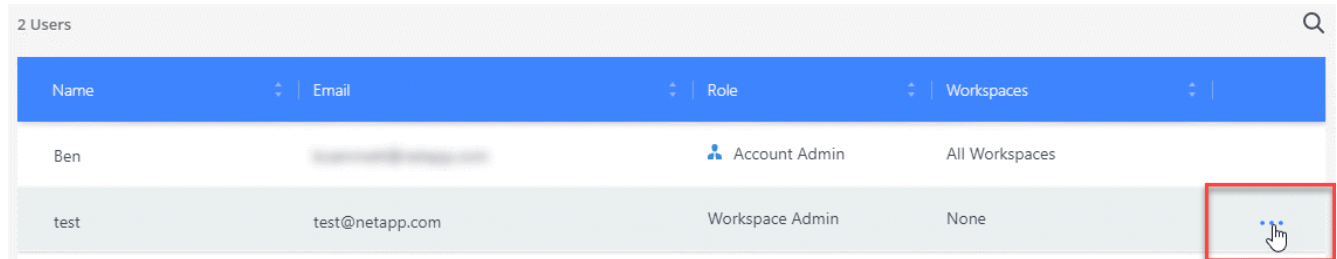
The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

Associating Workspace Admins with workspaces

You can associate Workspace Admins with additional workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.

Steps

1. Click **Account Settings**.
2. Click the action menu in the row that corresponds to the user.



Name	Email	Role	Workspaces
Ben		Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

3. Click **Manage Workspaces**.
4. Select one or more workspaces and click **Apply**.

Result

The user can now access those workspaces from Cloud Manager, as long as the service connector was also associated with the workspaces.

Associating service connectors with workspaces

A service connector is part of the Cloud Manager system. It runs on the virtual machine instance that was deployed in your cloud provider, or on an on-prem host that you configured. You need to associate this service connector with workspaces so Workspace Admins can access those workspaces from Cloud Manager.

If you only have Account Admins, then associating the service connector with workspaces isn't required. Account Admins have the ability to access all workspaces in Cloud Manager by default.

[Learn more about users, workspaces, and service connectors.](#)

Steps

1. Click **Account Settings**.
2. Click **Service Connector**.
3. Click **Manage Workspaces** for the service connector that you want to associate.
4. Select one or more workspaces and click **Apply**.

Result

Workspace Admins can now access the associated workspaces, as long as the user was also associated with the workspace.

Adding AWS credentials and subscriptions in Cloud Manager

When you create a Cloud Volumes ONTAP system, you need to select the AWS credentials and subscription to use with that system. If you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

Before you add AWS credentials to Cloud Manager, you need to provide the required permissions to that account. The permissions enable Cloud Manager to deploy and manage Cloud Volumes ONTAP in that AWS account. How you provide the permissions depends on whether you want to provide Cloud Manager with AWS keys or the ARN of a role in a trusted account.



When you deployed Cloud Manager from Cloud Central, Cloud Manager automatically added AWS credentials for the account in which you deployed Cloud Manager. This initial account is not added if you manually installed the Cloud Manager software on an existing system. [Learn about AWS accounts and permissions.](#)

Choices

- [Granting permissions by providing AWS keys](#)
- [Granting permissions by assuming IAM roles in other accounts](#)

Granting permissions by providing AWS keys

If you want to provide Cloud Manager with AWS keys for an IAM user, then you need to grant the required permissions to that user. The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use.

Steps

1. Download the Cloud Manager IAM policy from the [Cloud Manager Policies](#) page.
2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.

[AWS Documentation: Creating IAM Policies](#)

3. Attach the policy to an IAM role or an IAM user.
 - [AWS Documentation: Creating IAM Roles](#)
 - [AWS Documentation: Adding and Removing IAM Policies](#)

Result

The account now has the required permissions. [You can now add it to Cloud Manager.](#)

Granting permissions by assuming IAM roles in other accounts

You can set up a trust relationship between the source AWS account in which you deployed the Cloud Manager instance and other AWS accounts by using IAM roles. You would then provide Cloud Manager with the ARN of the IAM roles from the trusted accounts.

Steps

1. Go to the target account where you want to deploy Cloud Volumes ONTAP and create an IAM role by selecting **Another AWS account**.

Be sure to do the following:

- Enter the ID of the account where the Cloud Manager instance resides.
- Attach the Cloud Manager IAM policy, which is available from the [Cloud Manager Policies](#) page.

2. Go to the source account where the Cloud Manager instance resides and select the IAM role that is attached to the instance.
 - a. Click **Attach policies** and then click **Create policy**.
 - b. Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

Example

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAM"
  }
}
```

Result

The account now has the required permissions. [You can now add it to Cloud Manager](#).

Adding AWS credentials to Cloud Manager

After you provide an AWS account with the required permissions, you can add the credentials for that account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.



2. Click **Add Credentials** and select **AWS**.
3. Provide AWS keys or the ARN of a trusted IAM role.
4. Confirm that the policy requirements have been met and click **Continue**.
5. Choose the pay-as-you-go subscription that you want to associate with the credentials, or click **Add Subscription** if you don't have one yet.

To create a pay-as-you-go Cloud Volumes ONTAP system, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

6. Click **Go**.

Result

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:

Edit Account & Add Subscription

Credentials

Keys | Account ID: [REDACTED]

Instance Profile | Account ID: [REDACTED]

QA Subscription

Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

[+ Add Subscription](#)

Apply

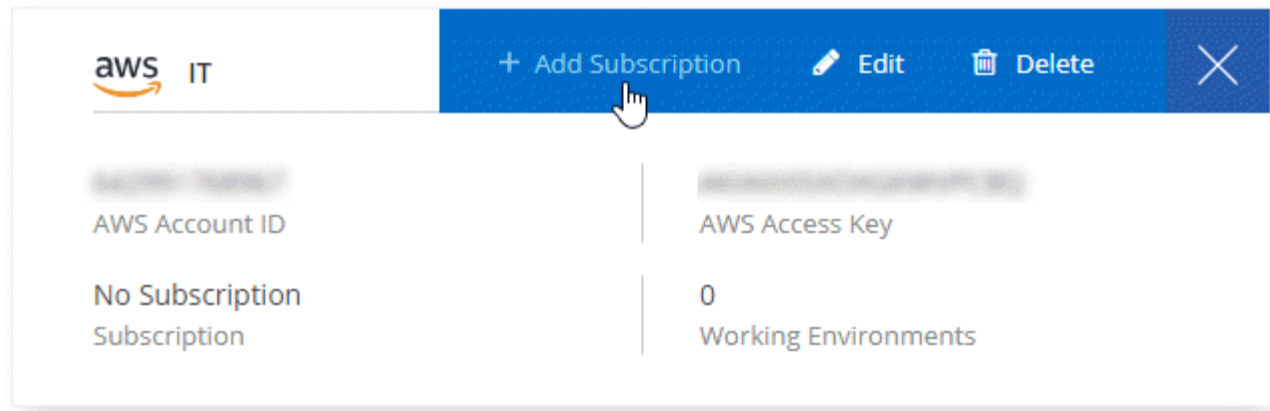
Cancel

Assigning an AWS subscription to credentials

If you haven't yet added an AWS subscription to a set of AWS credentials, you can do so any time from the Credentials page. To create a pay-as-you-go Cloud Volumes ONTAP system, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Hover over a set of credentials and click the action menu.
3. From the menu, click **Add Subscription**.



4. Click **Add Subscription**, click **Continue**, and follow the steps.

► https://docs.netapp.com/us-en/occm/media/video_subscribing_aws.mp4 (video)

Setting up and adding Azure credentials to Cloud Manager

There are two ways to manage Azure credentials in Cloud Manager. First, if you want to deploy Cloud Volumes ONTAP in different Azure accounts, then you need to provide the required permissions and add the credentials to Cloud Manager. The second way is to associate additional subscriptions with the Azure managed identity.



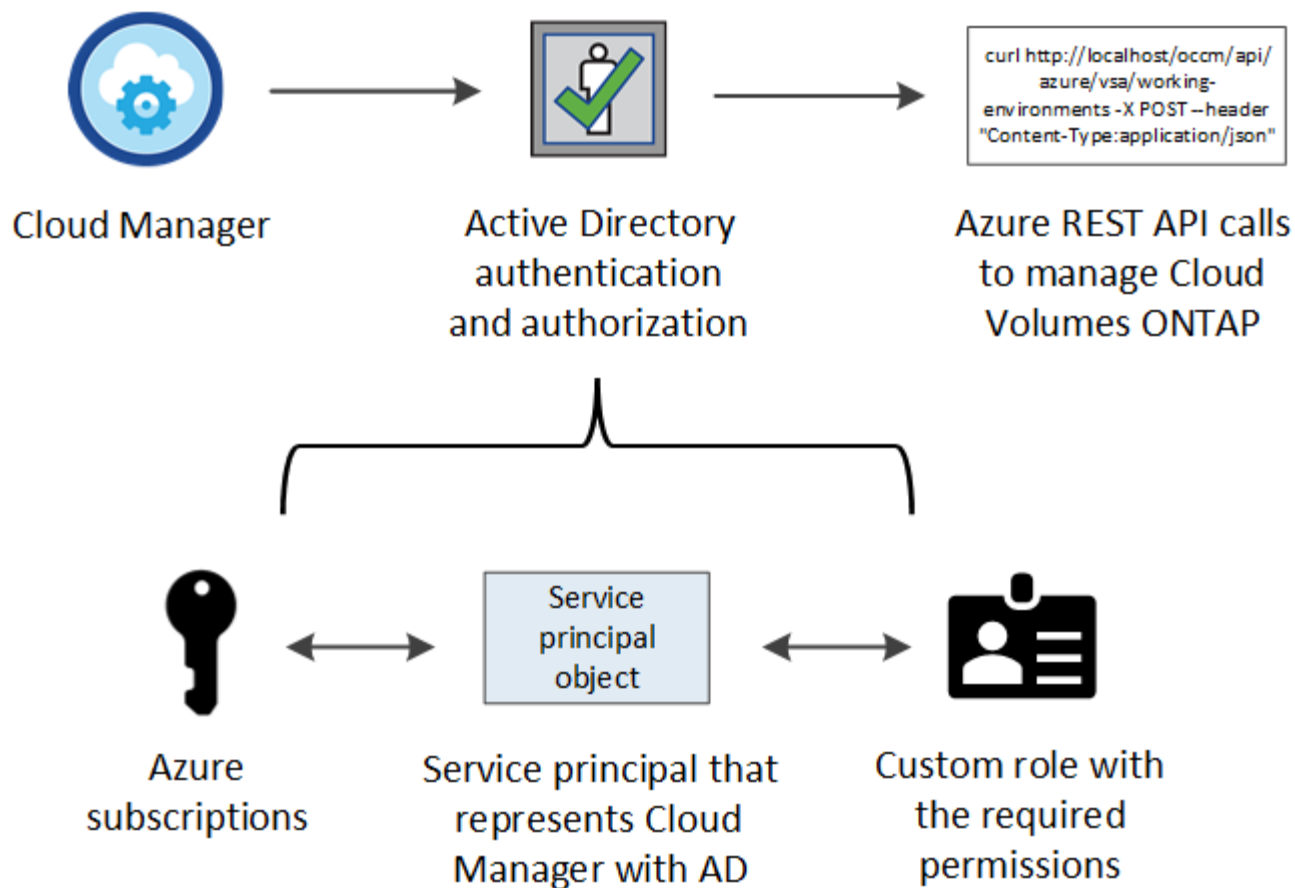
When you deploy Cloud Manager from Cloud Central, Cloud Manager automatically adds the Azure account in which you deployed Cloud Manager. An initial account is not added if you manually installed the Cloud Manager software on an existing system. [Learn about Azure accounts and permissions.](#)

Granting Azure permissions using a service principal

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

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.



Steps

1. [Create an Azure Active Directory application.](#)
2. [Assign the application to a role.](#)
3. [Add Windows Azure Service Management API permissions.](#)
4. [Get the application ID and directory ID.](#)
5. [Create a client secret.](#)

Creating an Azure Active Directory application

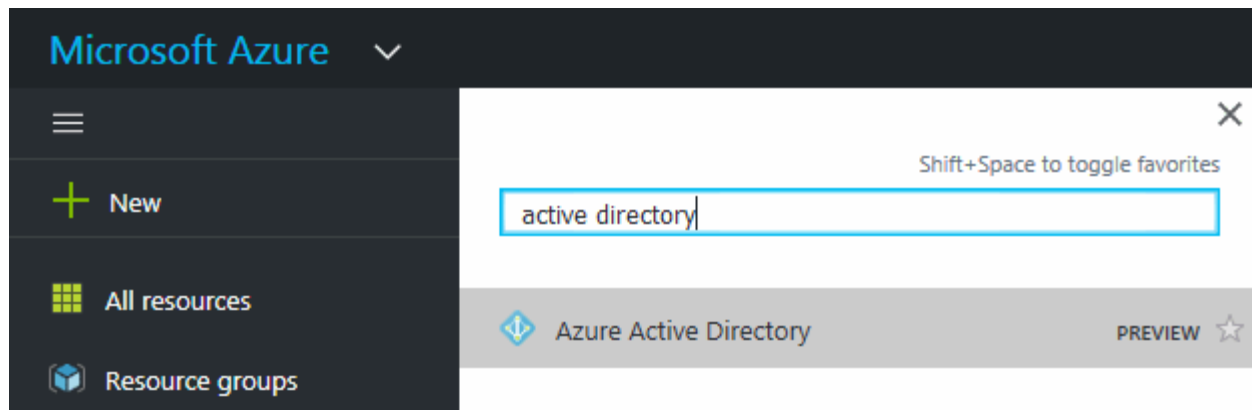
Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Required permissions](#).

Steps

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



2. In the menu, click **App registrations**.
3. Click **New registration**.
4. Specify details about the application:
 - **Name**: Enter a name for the application.
 - **Account type**: Select an account type (any will work with Cloud Manager).
 - **Redirect URI**: Select **Web** and then enter any URL—for example, `https://url`
5. Click **Register**.

Result

You've created the AD application and service principal.

Assigning the application to a role

You must bind the service principal to one or more Azure subscriptions and assign it the custom "OnCommand Cloud Manager Operator" role so Cloud Manager has permissions in Azure.

Steps

1. Create a custom role:
 - 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"
```

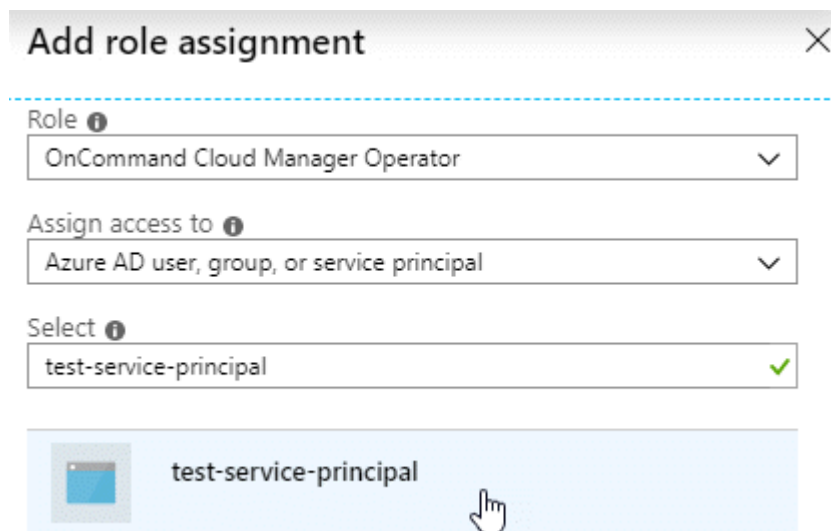
- c. Use the JSON file to create a custom role in Azure.

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 *Cloud Manager Operator*.

2. Assign the application to the role:
 - a. From the Azure portal, open the **Subscriptions** service.
 - b. Select the subscription.
 - c. Click **Access control (IAM)** > **Add** > **Add role assignment**.
 - d. Select the **Cloud Manager Operator** role.
 - e. Keep **Azure AD user, group, or service principal** selected.
 - f. Search for the name of the application (you can't find it in the list by scrolling).



- g. Select the application and click **Save**.

The service principal for Cloud Manager now has the required Azure permissions for that subscription.

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.

Adding Windows Azure Service Management API permissions

The service principal must have "Windows Azure Service Management API" permissions.

Steps














1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions** > **Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

<div>Microsoft Graph Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.</div> 		
<div>Azure Batch Schedule large-scale parallel and HPC applications in the cloud</div>	<div>Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets</div>	<div>Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</div>
<div>Azure Data Lake Access to storage and compute for big data analytic scenarios</div>	<div>Azure DevOps Integrate with Azure DevOps and Azure DevOps server</div>	<div>Azure Import/Export Programmatic control of import/export jobs</div>
<div>Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</div>	<div>Azure Rights Management Services Allow validated users to read and write protected content</div>	<div>Azure Service Management Programmatic access to much of the functionality available through the Azure portal</div>
<div>Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data</div>	<div>Customer Insights Create profile and interaction models for your products</div>	<div>Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination</div>

4. Click **Access Azure Service Management as organization users** and then click **Add permissions**.

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

Getting the application ID and directory ID

When you add the Azure account to Cloud Manager, you need to provide the application (client) ID and the directory (tenant) ID for the application. Cloud Manager uses the IDs to programmatically sign in.

Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

Creating a client secret

You need to create a client secret and then provide Cloud Manager with the value of the secret so Cloud Manager can use it to authenticate with Azure AD.



When you add the account to Cloud Manager, Cloud Manager refers to the client secret as the Application Key.

Steps

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Click **Add**.
6. Copy the value of the client secret.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA

Copy to clipboard

Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in Cloud Manager when you add an Azure account.

Adding Azure credentials to Cloud Manager

After you provide an Azure account with the required permissions, you can add the credentials for that account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

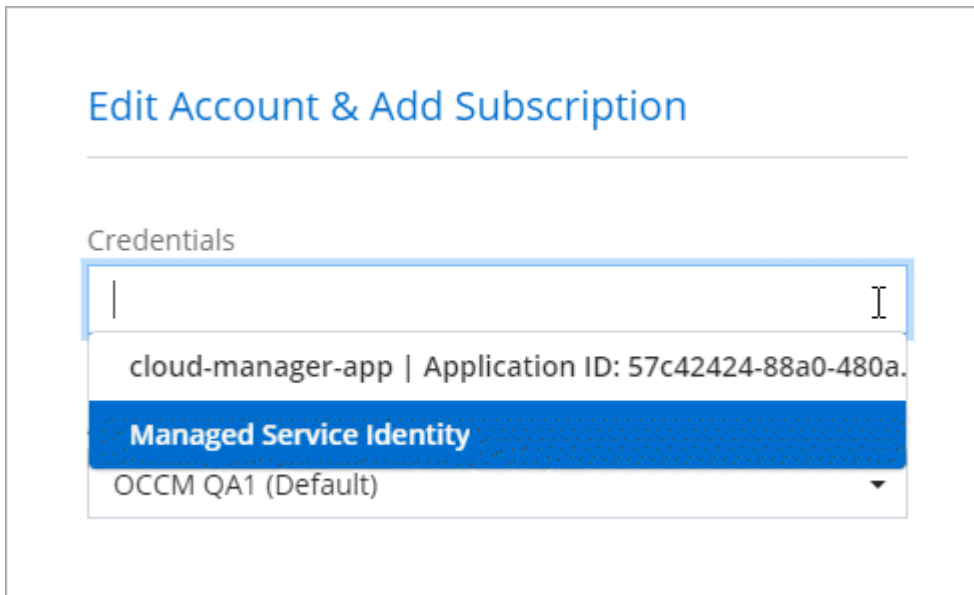


2. Click **Add Credentials** and select **Microsoft Azure**.
3. Enter information about the Azure Active Directory service principal that grants the required permissions:
 - Application (client) ID: See [Getting the application ID and directory ID](#).
 - Directory (tenant) ID: See [Getting the application ID and directory ID](#).
 - Client Secret: See [Creating a client secret](#).

4. Confirm that the policy requirements have been met and then click **Create Account**.

Result

You can now switch to different set of credentials from the Details and Credentials page [when creating a new working environment](#):



Associating additional Azure subscriptions with a managed identity

Cloud Manager enables you to choose the Azure credentials and Azure subscription in which you want to deploy Cloud Volumes ONTAP. You can't select a different Azure subscription for the managed identity profile unless you associate the [managed identity](#) with those subscriptions.

About this task

A managed identity is [the initial Azure account](#) when you deploy Cloud Manager from NetApp Cloud Central. When you deployed Cloud Manager, Cloud Central created the Cloud Manager Operator role and assigned it to the Cloud Manager virtual machine.

Steps

1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.
3. Click **Access control (IAM)**.
 - a. Click **Add > Add role assignment** and then add the permissions:
 - Select the **Cloud Manager Operator** role.



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.
- Select the Cloud Manager virtual machine.
- Click **Save**.

4. Repeat these steps for additional subscriptions.

Result

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions for the managed identity profile.

Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

Setting up and adding GCP accounts for data tiering with 9.6

If you want to enable [data tiering](#) on a Cloud Volumes ONTAP 9.6 system, 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.



If you want to use data tiering with Cloud Volumes ONTAP 9.7, then follow step 3 in [Getting started with Cloud Volumes ONTAP in Google Cloud Platform](#).

Setting up a service account and access keys for Google Cloud Storage

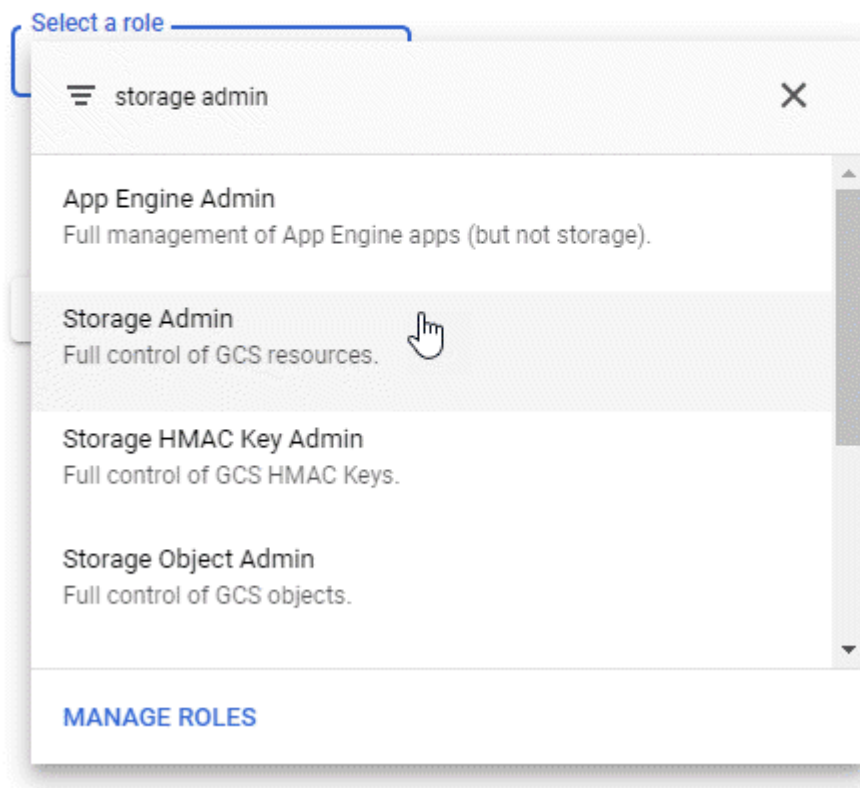
A service account enables Cloud Manager to authenticate and access Cloud Storage buckets used for data tiering. The keys are required so that Google Cloud Storage knows who is making the request.

Steps

1. Open the GCP IAM console and [create a service account that has the Storage Admin role](#).

Service account permissions (optional)

Grant this service account access to My Project 99247 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)



2. Go to [GCP Storage Settings](#).
3. If you're prompted, select a project.
4. Click the **Interoperability** tab.
5. If you haven't already done so, click **Enable interoperability access**.
6. Under **Access keys for service accounts**, click **Create a key for a service account**.
7. Select the service account that you created in step 1.

Select a service account

Email	Name	Keys
<input checked="" type="radio"/> data-tiering-for-netapp@top-monitor-250116.iam.gserviceaccount.com	data tiering for netapp	—

[CANCEL](#) [CREATE KEY](#) | [CREATE NEW ACCOUNT](#)

8. Click **Create Key**.

9. Copy the access key and secret.

You'll need to enter this information in Cloud Manager when you add the GCP account for data tiering.

Adding a GCP account to Cloud Manager

Now that you have an access key for a service account, you can add it to Cloud Manager.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.



2. Click **Add Credentials** and select **Google Cloud**.

3. Enter the access key and secret for the service account.

The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering.

4. Confirm that the policy requirements have been met and then click **Create Account**.

What's next?

You can now enable data tiering on individual volumes on a Cloud Volumes ONTAP 9.6 system when you create, modify, or replicate them. For details, see [Tiering inactive data to low-cost object storage](#).

But before you do, be sure that the subnet in which Cloud Volumes ONTAP resides is configured for Private Google Access. For instructions, refer to [Google Cloud Documentation: Configuring Private Google Access](#).

Adding NetApp Support Site accounts to Cloud Manager

Adding your NetApp Support Site account to Cloud Manager is required to deploy a BYOL system. It's also required to register pay-as-you-go systems and to upgrade ONTAP software.

Watch the following video to learn how to add NetApp Support Site accounts to Cloud Manager. Or scroll down to read the steps.



Steps

1. If you don't have a NetApp Support Site account yet, [register for one](#).
2. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.



3. Click **Add Credentials** and select **NetApp Support Site**.
4. Specify a name for the account and then enter the user name and password.
 - The account must be a customer-level account (not a guest or temp account).
 - If you plan to deploy BYOL systems:
 - The account must be authorized to access the serial numbers of the BYOL systems.

- If you purchased a secure BYOL subscription, then a secure NSS account is required.

5. Click **Create Account**.

What's next?

Users can now select the account when creating new Cloud Volumes ONTAP systems and when registering existing systems.

- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)
- [Registering pay-as-you-go systems](#)
- [Learn how Cloud Manager manages license files](#)

Installing an HTTPS certificate for secure access

By default, Cloud Manager uses a self-signed certificate for HTTPS access to the web console. You can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **HTTPS Setup**.



2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	<ol style="list-style-type: none">a. Enter the host name or DNS of the Cloud Manager host (its Common Name), and then click Generate CSR. Cloud Manager displays a certificate signing request.b. Use the CSR to submit an SSL certificate request to a CA. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.c. Copy the contents of the signed certificate, paste it in the Certificate field, and then click Install.

Option	Description
Install your own CA-signed certificate	<p>a. Select Install CA-signed certificate.</p> <p>b. Load both the certificate file and the private key and then click Install.</p> <p>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</p>

Result

Cloud Manager now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a Cloud Manager system that is configured for secure access:

Cloud Manager HTTPS certificate

Expiration:

⚠ Oct 27, 2016 05:13:28 am

Issuer:

CN=localhost, O=NetApp, OU=Tel-Aviv, EMAILADDRESS=admin@example.com

Subject:

EMAILADDRESS=admin@example.com, OU=Tel-Aviv, O=NetApp, CN=localhost

View Certificate

Renew HTTPS Certificate

Setting up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to set up the AWS Key Management Service (KMS).

Steps

1. Ensure that an active Customer Master Key (CMK) exists.

The CMK can be an AWS-managed CMK or a customer-managed CMK. It can be in the same AWS account as Cloud Manager and Cloud Volumes ONTAP or in a different AWS account.

[AWS Documentation: Customer Master Keys \(CMKs\)](#)

2. Modify the key policy for each CMK by adding the IAM role that provides permissions to Cloud Manager as a *key user*.

Adding the IAM role as a key user gives Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

[AWS Documentation: Editing Keys](#)

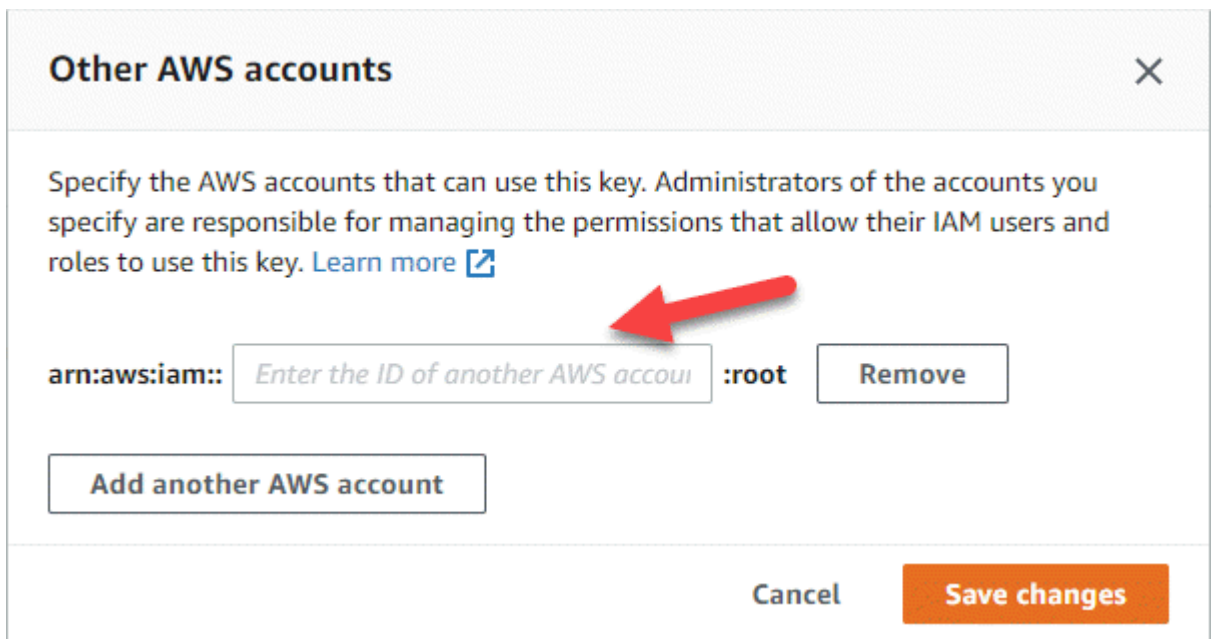
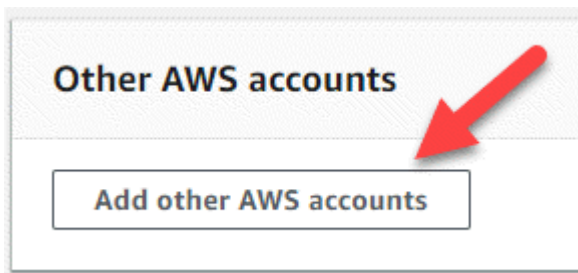
3. If the CMK is in a different AWS account, complete the following steps:

- a. Go to the KMS console from the account where the CMK resides.
- b. Select the key.
- c. In the **General configuration** pane, copy the ARN of the key.

You'll need to provide the ARN to Cloud Manager when you create the Cloud Volumes ONTAP system.

- d. In the **Other AWS accounts** pane, add the AWS account that provides Cloud Manager with permissions.

In most cases, this is the account where Cloud Manager resides. If Cloud Manager wasn't installed in AWS, it would be the account for which you provided AWS access keys to Cloud Manager.



- e. Now switch to the AWS account that provides Cloud Manager with permissions and open the

IAM console.

- f. Create an IAM policy that includes the permissions listed below.
- g. Attach the policy to the IAM role or IAM user that provides permissions to Cloud Manager.

The following policy provides the permissions that Cloud Manager needs to use the CMK from the external AWS account. Be sure to modify the region and account ID in the "Resource" sections.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

For additional details about this process, see [AWS Documentation: Allowing External AWS Accounts to Access a CMK](#).

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.