



Administer Cloud Manager

Cloud Manager

NetApp

June 15, 2020

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

Table of Contents

- Administer Cloud Manager 1
 - Updating Cloud Manager 1
 - Managing workspaces and users in the Cloud Central account 2
 - Removing Cloud Volumes ONTAP working environments. 5
 - Configuring Cloud Manager to use a proxy server 6
 - Renewing the Cloud Manager HTTPS certificate 7
 - Overriding CIFS locks for Cloud Volumes ONTAP HA in Azure. 7
 - Restoring Cloud Manager 8
 - Uninstalling Cloud Manager 9

Administer Cloud Manager

Updating Cloud Manager

You can update Cloud Manager to the latest version or with a patch that NetApp personnel shared with you.

Enabling automatic updates

Cloud Manager can automatically update itself when a new version is available. This ensures that you are running the latest version.

About this task

Cloud Manager automatically updates at 12:00 midnight if no operations are running.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Manager Settings**.
2. Select the checkbox under Automatic Cloud Manager Updates and then click **Save**.

Updating Cloud Manager to the latest version

You should enable automatic updates to Cloud Manager, but you can always do a manual update directly from the web console. Cloud Manager obtains the software update from a NetApp-owned S3 bucket in AWS.

Before you begin

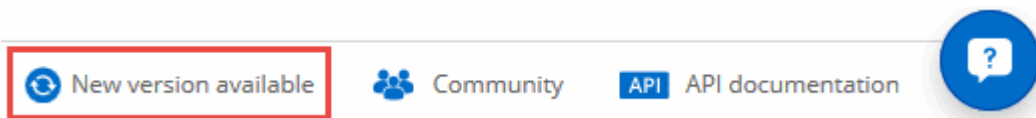
You should have reviewed [what is new in the release](#) to identify new requirements and changes in support.

About this task

The software update takes a few minutes. Cloud Manager will not be available during the update.

Steps

1. Check whether a new version is available by looking at the lower-right corner of the console:



2. If a new version is available, click **Timeline** to determine whether any tasks are in progress.

If any tasks are in progress, wait for them to finish before you proceed to the next step.

3. In the lower-right of the console, click **New version available**.
4. On the Cloud Manager Software Update page, click **Update** next to the version that you want.
5. Complete the confirmation dialog box, and then click **OK**.

Result

Cloud Manager starts the update process. You can log in to the console after a few minutes.

Updating Cloud Manager with a patch

If NetApp shared a patch with you, you can update Cloud Manager with the supplied patch directly from the Cloud Manager web console.

About this task

The patch update typically takes a few minutes. Cloud Manager will not be available during the update.

Steps

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



2. Click the link to update Cloud Manager with the supplied patch.

If NetApp shared a patch with you, click [here](#) to update Cloud Manager with the supplied patch.



3. Complete the confirmation dialog box and then click **OK**.
4. Select the patch that you were provided.

Result

Cloud Manager applies the patch. You can log in to the console after a few minutes.

Managing workspaces and users in the Cloud Central account

[After you perform initial setup](#), you might need to later manage users, workspaces, and service connectors.

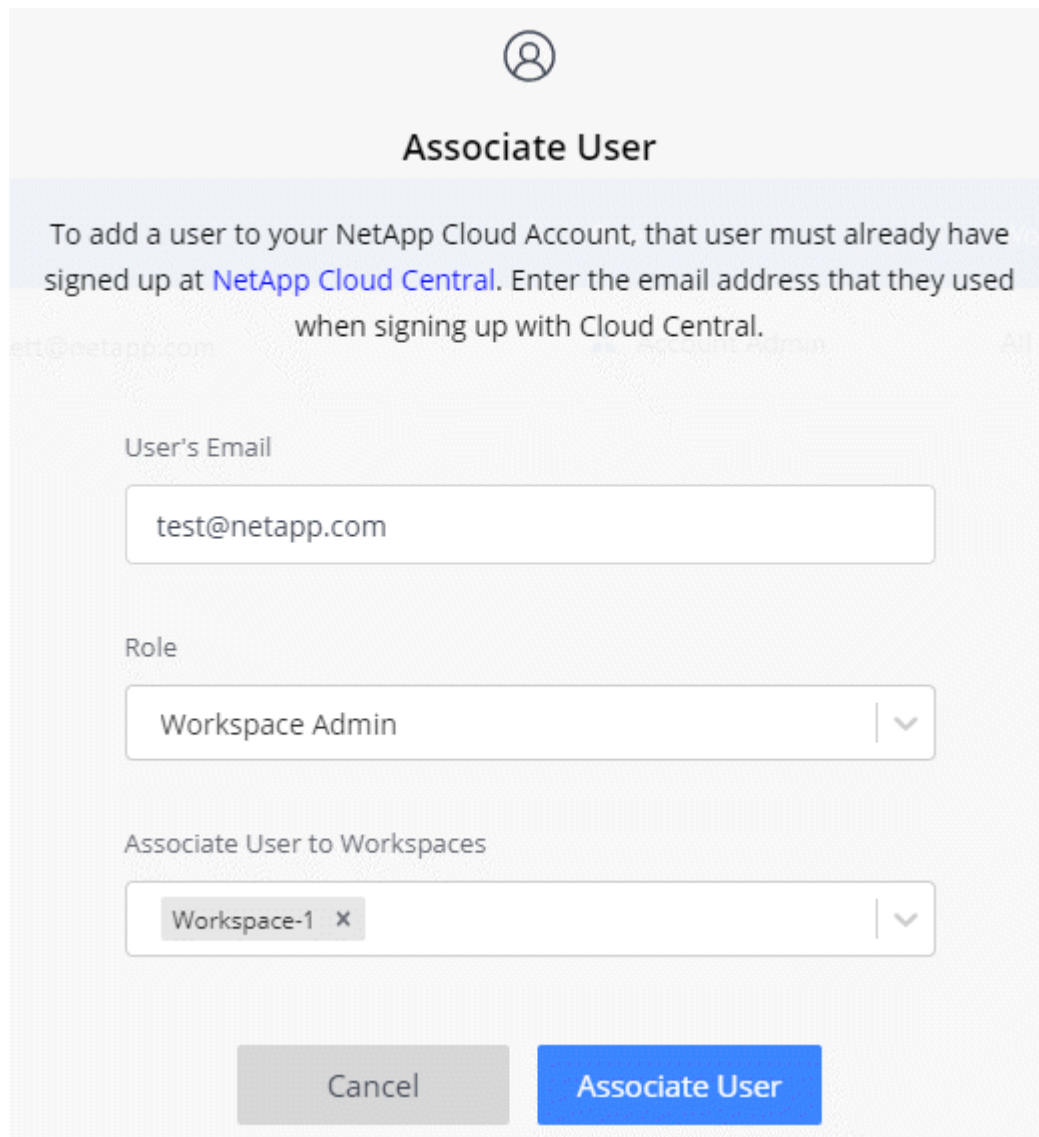
[Learn more about how Cloud Central accounts work.](#)

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 modal dialog box titled "Associate User" with a user icon at the top. The dialog contains 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 the instructions are three input fields: "User's Email" with the value "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (x). At the bottom are two buttons: "Cancel" and "Associate User".



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

Role

Workspace Admin | v

Associate User to Workspaces

Workspace-1 x | v

Cancel

Associate User

6. Click **Associate User**.

Result

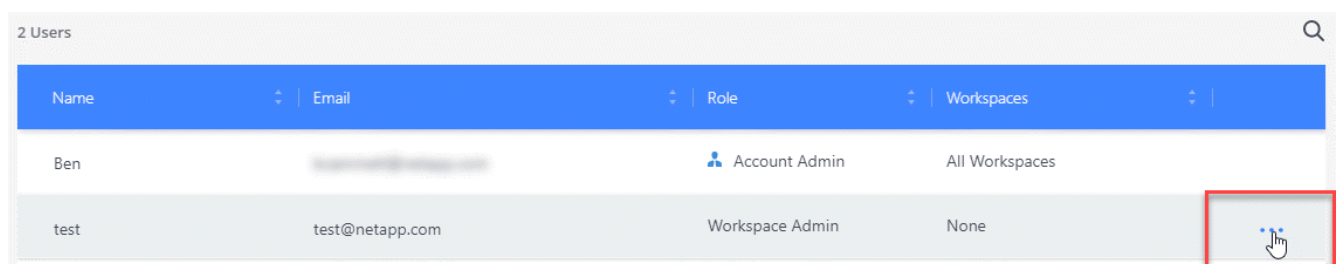
The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

Removing users

Disassociating a user makes it so they can no longer access the resources in a Cloud Central account.

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 **Disassociate User** and click **Disassociate** to confirm.

Result

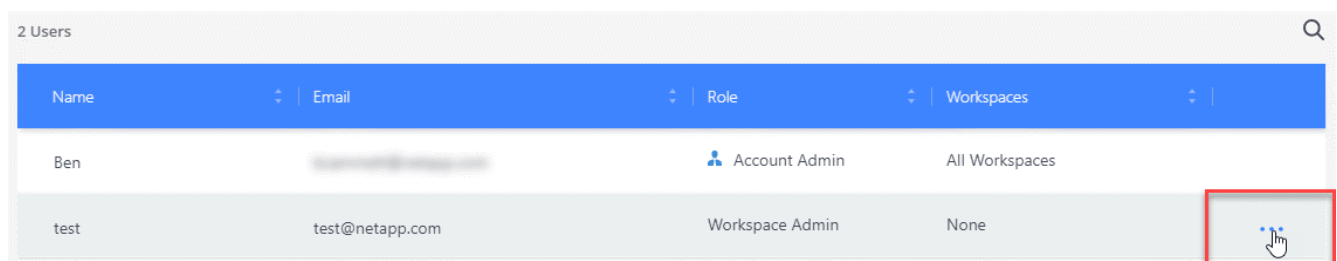
The user can no longer access the resources in this Cloud Central account.

Managing a Workspace Admin's workspaces

You can associate and disassociate Workspace Admins with 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 the workspaces to associate with the user 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.

Managing workspaces

Manage your workspaces by creating, renaming, and deleting them. Note that you can't delete a workspace if it contains any resources. It must be empty.

Steps

1. Click **Account Settings**.
2. Click **Workspaces**.
3. Choose one of the following options:
 - Click **Add New Workspace** to create a new workspace.
 - Click **Rename** to rename the workspace.
 - Click **Delete** to delete the workspace.

Managing a service connector's workspaces

You need to associate the 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 the workspaces to associate with the service connector and click **Apply**.

Removing Cloud Volumes ONTAP working environments

The Account Admin can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

About this task

Removing a Cloud Volumes ONTAP working environment removes it from Cloud Manager. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment.

Removing a working environment from Cloud Manager enables you to do the following:

- Rediscover it in another workspace
- Rediscover it from another Cloud Manager system
- Rediscover it if you had problems during the initial discovery

Steps

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



2. From the Tools page, click **Launch**.
3. Select the Cloud Volumes ONTAP working environment that you want to remove.
4. On the Review and Approve page, click **Go**.

Result

Cloud Manager removes the working environment. Users can rediscover this working environment from the Working Environments page at any time.

Configuring Cloud Manager to use a proxy server

When you first deploy Cloud Manager, it prompts you to enter a proxy server if the system does not have internet access. You can also manually enter and modify the proxy from Cloud Manager's settings.

About this task

If your corporate policies dictate that you use a proxy server for all HTTP communication to the internet, then you must configure Cloud Manager to use that proxy server. The proxy server can be in the cloud or in your network.

When you configure Cloud Manager to use a proxy server, Cloud Manager, Cloud Volumes ONTAP, and the HA mediator all use the proxy server.

Steps

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



2. Under HTTP Proxy, enter the server using the syntax `http://address:port`, specify a user name and password if basic authentication is required for the server, and then click **Save**.



Cloud Manager does not support passwords that include the @ character.

Result

After you specify the proxy server, new Cloud Volumes ONTAP systems are automatically configured to use the proxy server when sending AutoSupport messages. If you do not specify the proxy server before users create Cloud Volumes ONTAP systems, then they must use System Manager to manually set the proxy server in the AutoSupport options for each system.

Renewing the Cloud Manager HTTPS certificate

You should renew the Cloud Manager HTTPS certificate before it expires to ensure secure access to the Cloud Manager web console. If you do not renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

Steps

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

Details about the Cloud Manager certificate displays, including the expiration date.

2. Click **Renew HTTPS Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

Result

Cloud Manager uses the new CA-signed certificate to provide secure HTTPS access.

Overriding CIFS locks for Cloud Volumes ONTAP HA in Azure

The Account Admin can enable a setting in Cloud Manager that prevents issues with Cloud Volumes ONTAP storage failover during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a node in a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent

storage failover.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage failover during these maintenance events.



This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

Steps

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



2. Under **HA CIFS Locks**, select the checkbox and click **Save**.

Restoring Cloud Manager

Your [NetApp Cloud Central account](#) makes it easy for you to restore a Cloud Manager configuration. The account is a service running in Cloud Central so the users, workspaces, and service connectors that you associated with the account are always accessible. Even if your Cloud Manager system was accidentally deleted.



Starting with the 3.7.1 release, Cloud Manager no longer supports downloading a backup and using it to restore your configuration. You need to follow these steps to restore Cloud Manager.

Steps

1. Deploy a new Cloud Manager system in your existing Cloud Central account.

[Deployment options](#)

2. Add your cloud provider accounts and NetApp Support Site accounts to Cloud Manager.

This step gets Cloud Manager ready so you can create additional Cloud Volumes ONTAP systems in your cloud provider.

It's important to complete this step if you used AWS keys to deploy an existing Cloud Volumes ONTAP system that you want to discover on this new Cloud Manager system. Cloud Manager needs the AWS keys to properly discover and manage Cloud Volumes ONTAP.

- [Adding AWS accounts to Cloud Manager](#)

- [Adding Azure accounts to Cloud Manager](#)
 - [Adding NetApp Support Site accounts to Cloud Manager](#)
3. Rediscover your working environments: Cloud Volumes ONTAP systems, on-premises clusters, and NetApp Private Storage for Cloud configurations.
 - [Adding existing Cloud Volumes ONTAP systems to Cloud Manager](#)
 - [Discovering ONTAP clusters](#)

Result

Your Cloud Manager configuration is now restored with your accounts, settings, and working environments.

Uninstalling Cloud Manager

Cloud Manager includes an uninstallation script that you can use to uninstall the software to troubleshoot issues or to permanently remove the software from the host.

Steps

1. From the Linux host, run the uninstallation script:

```
/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]
```

silent runs the script without prompting you for confirmation.

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.