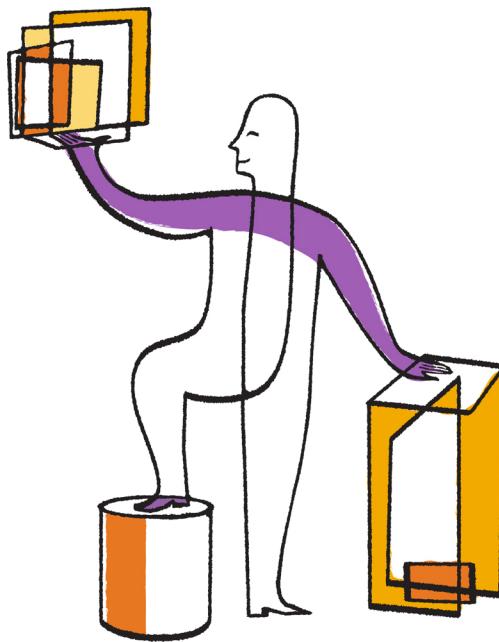




OnCommand® Cloud Manager 2.1

Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-10493_A0
December 2015

Contents

Backing up Cloud Manager	4
Removing Cloud ONTAP working environments from Cloud Manager	5
Managing Cloud Manager user accounts	6
Understanding user roles	6
Creating user accounts	6
Editing user accounts	8
Deleting user accounts	8
Managing Cloud Manager encryption settings for Cloud ONTAP	9
Renewing the Cloud Manager certificate	9
Managing available key managers and CA certificates	9
Configuring Cloud Manager settings	11
Configuring Cloud Manager to use a proxy server	11
Modifying aggregate capacity thresholds	12
Modifying the maximum autosize for volumes	12
Managing HTTPS certificates for secure access	14
Installing an HTTPS certificate for secure access	14
Renewing the Cloud Manager HTTPS certificate	15
Troubleshooting Cloud Manager and Cloud ONTAP	16
Restoring Cloud Manager from a backup	16
Working with Cloud Manager AutoSupport	17
How Cloud Manager is configured on Linux hosts	17
Uninstalling Cloud Manager	18
Cloud Manager REST APIs	19
Copyright information	20
Trademark information	21
How to send comments about documentation and receive update notifications	22
Index	23

Backing up Cloud Manager

It is a good practice to back up the Cloud Manager database on a periodic basis. If you experience problems, you can restore Cloud Manager from a previous backup.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
2. Click **Backup**:

Tools

Backup

Back up Cloud Manager to a .7z file, which you can use later to restore your configuration.



3. When prompted, save the backup file to a secure location so that you can retrieve it when needed.

Removing Cloud ONTAP working environments from Cloud Manager

The Cloud Manager Admin can remove a Cloud ONTAP working environment, which removes the working environment from Cloud Manager but does not delete it. You can later rediscover the working environment. This action enables you to move a working environment and troubleshoot discovery issues.

About this task

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

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

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
2. From the **Tools** page, click **Launch**.
3. Select the Cloud 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.

Managing Cloud Manager user accounts

Each Cloud Manager user has access to the Users page. Users can modify their own user account and other accounts, if they have appropriate privileges. Privileges are defined by the user's role.

Understanding user roles

Each Cloud Manager user account is assigned a role that defines permissions.

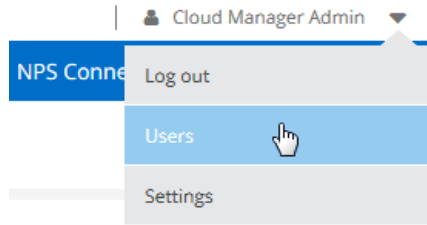
Task	Cloud Manager Admin	Tenant Admin	Working Environment Admin
Manage tenants	Yes	No	No
Manage working environments	Yes	Yes, for the assigned tenant	Yes, for assigned working environments
View data replication status	Yes	Yes, for the assigned tenant	Yes, for assigned working environments
View the timeline	Yes	Yes	Yes
Create and delete user accounts	Yes	Yes, for the assigned tenant	No
Modify user accounts	Yes	Yes, for the assigned tenant	Yes, for their own account
Modify settings	Yes	No	No
Manage AutoSupport	Yes	No	No
Back up and restore Cloud Manager	Yes	No	No
Remove a working environment	Yes	No	No
Update Cloud Manager	Yes	No	No
Set up encryption	Yes	No	No
Install an HTTPS certificate	Yes	No	No

Creating user accounts

If multiple people in your organization need to use Cloud Manager, then you need to create Cloud Manager user accounts for each user. You can create several types of users: Cloud Manager administrators, tenant administrators, and working environment administrators.

Steps

1. In the upper right corner of the Cloud Manager console, click the task drop-down list, and then select **Users**.



2. In the **Users** page, click **New User**.
3. In the **New User** page, specify details for the new user account.

Most of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Email Address	Enter the email address that the user must use to log in to Cloud Manager. Cloud Manager does not send emails to this address.
Role	Select one of the three roles: • Cloud Manager Admin: Administers the product and has access to all tenants and working environments. • Tenant Admin: Administers a single tenant. Can create and manage all working environments and users in the tenant. • Working Environment Admin: Administers one or more working environments in a tenant. When you create a Working Environment Admin user, you need to assign the user to a tenant and, optionally, a working environment. If the selected tenant does not have a working environment, you can modify the assigned working environments later. Note: Working Environment Admin users automatically have privileges to the working environments that they create.
AWS Access Key and AWS Secret Key	Enter the access key and secret key assigned to the user in AWS. Cloud Manager uses the keys to perform AWS actions on the user's behalf. Identity and Access Management (IAM) users must have specific AWS permissions. You can use a NetApp-provided IAM policy that includes the required permissions. NetApp OnCommand Cloud Manager: AWS IAM Policy
AWS Cost S3 Bucket	Optionally enter the S3 bucket that contains detailed billing reports, if you specified keys for an AWS account under which the bucket was created. Giving Cloud Manager access to detailed billing reports enables users to see AWS storage and compute costs associated with Cloud ONTAP. If you are using AWS consolidated billing, you do not need to specify the bucket each time you create a user account. You just specify the bucket for one Cloud Manager user account that corresponds to an IAM user created under the AWS payer account, or the payer account itself. If you have not set up an S3 bucket and enabled billing reports, see the OnCommand Cloud Manager Installation and Setup Guide for details.

4. Click **Save**.

Result

Cloud Manager creates the user account. The user can now log in to Cloud Manager.

Related information

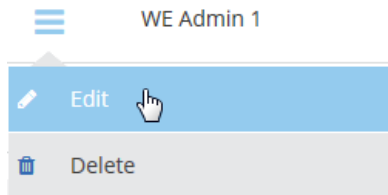
[OnCommand Cloud Manager 2.1 Installation and Setup Guide](#)

Editing user accounts

You can modify Cloud Manager user accounts by changing the user's name and email address, by resetting the user's password, by changing the AWS keys associated with the account, and by changing the S3 cost bucket in which detailed billing reports are stored.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Users**.
2. Select the menu icon next to the user's name and then click **Edit**.



3. In the **Edit User** page, modify the user account and then click **Save**.

Deleting user accounts

You can delete a user account, as long as no working environments created by that user exist. For example, if a user created a Cloud ONTAP working environment, you cannot delete that user's account until you delete the working environment.

About this task

You can delete a user account that is assigned to a working environment that the user did not create.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Users**.
2. Hover over the user's name, select the menu icon, and then click **Delete**.
3. Click **OK** to confirm.

Managing Cloud Manager encryption settings for Cloud ONTAP

You might need to periodically manage Cloud Manager encryption settings to ensure that Cloud ONTAP systems can communicate with key managers. The tasks include renewing the Cloud Manager intermediate CA certificate if it is about to expire, and managing the key managers and CA certificates available to Cloud ONTAP systems.

If you have not yet set up Cloud Manager to be an intermediate CA or added key managers and their CA certificates to Cloud Manager, see the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).

Renewing the Cloud Manager certificate

You must renew the Cloud Manager certificate before it expires; otherwise, Cloud Manager cannot sign client certificates for Cloud ONTAP systems.

About this task

If you renew the Cloud Manager intermediate CA certificate, Cloud Manager uses the renewed certificate to generate client certificates for *new* Cloud ONTAP systems. You can renew client certificates for *existing* Cloud ONTAP systems from the working environment.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then click **Encryption Setup**.
2. In the **Intermediate CA** tab, click **Renew Intermediate CA**.
3. Click **Generate CSR**.
4. Use the CSR to submit a certificate request to a CA.
The intermediate CA certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.
5. Copy the contents of the signed certificate and paste it in the **Cloud Manager certificate** field.
6. Click **Install Cloud Manager Certificate**.

Managing available key managers and CA certificates

You can modify the key managers and key manager CA certificates that Cloud Manager users can use with their Cloud ONTAP systems. For example, you can add a new key manager that is available in your environment and you can add a new CA certificate, if a previous certificate expired.

About this task

The changes that you make from the Encryption Setup page affect only *new* Cloud ONTAP systems. Changes to *existing* Cloud ONTAP systems must be made from the working environment.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then click **Encryption Setup**.
2. Click **Key Manager**.
3. Manage your key managers as necessary:

To...	Do this...
Change the KMIP port for communicating with key managers	Modify the port and then click Save. The port change affects only new Cloud ONTAP systems. To change the port for an existing Cloud ONTAP system, connect to the CLI and then run the <code>security key-manager setup</code> command.
Add a new key manager	Click Add, enter details about the key manager, and then click Add again. This action does not add the key manager to existing Cloud ONTAP systems. You must add the key manager from the working environment, if necessary.
Edit the details for a key manager	Select the menu icon next to the key manager, click Edit, modify the details, and then click Save. Any changes affect only new Cloud ONTAP systems that will use this key manager. To apply this change to existing Cloud ONTAP systems, go to the working environment, remove the key manager, and then add it back.
Delete an existing key manager	Select the menu icon next to the key manager, click Delete, and then click Delete again. If you delete a key manager, you cannot configure Cloud ONTAP systems to use it. Existing systems that are using this key manager can continue to use it.

4. Manage the key managers' CA certificates as necessary:

To...	Do this...
Add a new certificate	Click Add , paste the certificate, and then click Add again.
View a certificate	Select the menu icon next to the key manager and click View .
Delete a certificate	Select the menu icon next to the certificate, click Delete, and then click Delete again. If you delete a certificate, you cannot configure Cloud ONTAP systems to use it. Existing systems that are using the certificate can continue to use it.

Configuring Cloud Manager settings

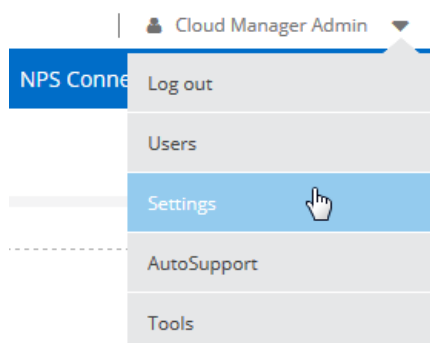
Cloud Manager includes a few settings that determine how it sets up aggregates and volumes, whether Cloud Manager and Cloud ONTAP use an HTTP proxy, and how Cloud Manager logs API calls and responses. You should enable full API logging only when requested by NetApp technical support.

Configuring Cloud Manager to use a proxy server

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 AWS or in your network.

Steps

1. In the upper-right hand corner of the Cloud Manager console, click the task drop-down list, and then select **Settings**.



2. Under **HTTP Proxy**, enter the server using the syntax **http://address:port**, and then click **Save**.

Example

HTTP Proxy

Set up Proxy configuration to allow Cloud Manager and Cloud ONTAP instances to access the Internet.

Enter an empty value to disable the proxy.

Result

After you specify the proxy server, new Cloud 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 ONTAP systems, then they must use System Manager to manually set the proxy server in the AutoSupport options for each system.

Related information

[OnCommand Cloud Manager 2.1 Storage Management Guide](#)

Modifying aggregate capacity thresholds

Cloud Manager notifies you when an aggregate's free space ratio declines below the configured threshold or when an aggregate's overcommitment ratio grows beyond the configured threshold. You can modify the default thresholds if they do not meet your needs.

About this task

You can define capacity thresholds for the following:

Aggregate free space ratio

The percentage of free space available in the aggregate. The threshold is 10 percent by default. The calculation for the ratio is: the aggregate's capacity minus the aggregate's used capacity divided by the aggregate's capacity.

Aggregate overcommitment ratio

The ratio between the amount of storage over provisioned in the aggregate and the free space available in the aggregate. The threshold is 500 percent by default. The calculation for the ratio is: the total allocated capacity on the aggregate minus the aggregate's used capacity divided by the aggregate's free capacity. The total allocated capacity on the aggregate is derived from all volumes, whether they are thick or thin provisioned.

For example, suppose a 1,000 GB aggregate has 100 GB of free space and contains two volumes:

- A 1,000-GB thin-provisioned volume with 600 GB used size
- A 300-GB thick-provisioned volume

The overcommitment ratio for this aggregate is: 1,300 minus 900 divided by 100 which translates to 400 percent. If you wanted to provision a 200-GB thin-provisioned volume on this aggregate, the overcommitment would increase: 1,500 minus 900 divided by 100 which translates to 600 percent. Provisioning this volume would cross the threshold.

If an aggregate crosses either of these thresholds, Cloud Manager displays a notification in the working environment page, notifying you that additional disks are needed.

Steps

1. In the upper-right hand corner of the Cloud Manager console, click the task-drop down list, and then select **Settings**.
2. Under **Capacity Thresholds**, change the percentages and click **Save**.

Result

Cloud Manager updates the threshold percentages and notifies users when they are reached.

Modifying the maximum autosize for volumes

If you need finer control over volume growth, you can modify the maximum size to which volumes can grow. By default, Cloud Manager sets the maximum size to 1,000 percent of a volume's size.

About this task

Cloud Manager sets the autosize mode to *grow* for all read-write volumes that it creates for Cloud ONTAP and FAS clusters. The grow mode enables a volume to automatically grow when its used

space is above the grow threshold, which is 85 percent by default. When a volume reaches the grow threshold, it grows until it reaches the maximum autosize.

The maximum autosize is specified in a percentage, which is the additional amount from a volume's size that it is allowed to grow. For example, 100 percent means the volume can grow up to double its size, 1,000 percent means the volume can grow up to 11 times its size, and 0 percent turns the feature off.

Note: Autosize is disabled for data protection volumes.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Settings**.
2. Specify the additional amount that volumes can grow by specifying a percentage (0% to 1000%).
3. Click **Save**.

Result

Cloud Manager applies the maximum autosize value to new volumes.

Managing HTTPS certificates for secure access

You can install and renew SSL/TLS certificates for secure HTTPS access to the Cloud Manager web console.

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 task drop-down list, and then select **HTTPS Setup**.
2. In the **HTTPS Setup** page, 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.

3. 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.
4. Copy the content of the signed certificate, paste it in the **Certificate** field, and then click **Install**.

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](#)

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 task drop-down list, and then select **HTTPS Setup**.
Details about the Cloud Manager certificate displays, including the expiration date.
2. Click **Renew HTTPS Certificate**.
3. 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.
4. 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.
5. Copy the content of the signed certificate, paste it in the **Certificate** field, and then click **Install**.

Result

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

Troubleshooting Cloud Manager and Cloud ONTAP

Several resources are available to help you with Cloud Manager and Cloud ONTAP.

Task	Resource
View known issues and limitations	OnCommand Cloud Manager 2.1 Release Notes Find the Release Notes for your version of Cloud ONTAP Find the Release Notes for your version of Data ONTAP 8
View cloud-related KB articles and frequently asked questions or chat with technical support	NetApp Cloud ONTAP Support
Connect with peers and ask questions	NetApp Community: Hybrid Cloud
Restore Cloud Manager from a backup	Restoring Cloud Manager from a backup on page 16
View logs	Working with Cloud Manager AutoSupport on page 17
Understand how Cloud Manager is configured on Linux	How Cloud Manager is configured on Linux hosts on page 17
Uninstall Cloud Manager to troubleshoot issues	Uninstalling Cloud Manager on page 18

Restoring Cloud Manager from a backup

You can restore Cloud Manager from a backup to restore it to a previous configuration.

About this task

Restoring Cloud Manager from a backup replaces existing data with the data from the backup.

Steps

1. In the upper-right hand corner of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
2. Click **Restore**.
3. Click **OK** to confirm.
4. Select the backup.

Result

Cloud Manager restores the database from the backup file.

Related tasks

[Backing up Cloud Manager](#) on page 4

Working with Cloud Manager AutoSupport

AutoSupport is enabled by default for Cloud Manager. It proactively monitors the health of your system and sends messages to NetApp technical support. You can change the AutoSupport schedule, download AutoSupport messages for troubleshooting, and send an immediate AutoSupport message to NetApp technical support.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task-drop down list, and then select **AutoSupport**.
2. Work with AutoSupport as follows:

Task	Action
Change the schedule	Change the day of week and time of day that Cloud Manager should send AutoSupport messages to NetApp technical support, and then click Save .
Download an AutoSupport message, which includes logs that you or NetApp technical support can use to troubleshoot issues	Click Download Now .
Send an immediate AutoSupport message to NetApp technical support, which you might do at the request of support personnel	Click Send Now .
Disable AutoSupport	Ensure that Send support information to NetApp is not selected.

How Cloud Manager is configured on Linux hosts

If you need to troubleshoot Cloud Manager or your Linux host, it might help to know how Cloud Manager is configured on the host.

- The user name for the EC2 Linux instance is `ec2-user`.
- The operating system for the Cloud Manager AMI is Red Hat Enterprise Linux 7.1 (HVM). The operating system does not include a GUI. You must use a terminal to access the instance.
- The Cloud Manager installation folder resides in the following location:
`/opt/application/netapp/cloudmanager`
- Log files are contained in the following folder:
`/opt/application/netapp/cloudmanager/log`
- The Cloud Manager service is named `occm`.
- The `occm` service is dependent on the MySQL service.
If the MySQL service is down, then the `occm` service is down too.
- Cloud Manager installs the following packages on the Linux host, if they are not already installed:
 - 7Zip
 - AWSCLI

- Java
- MySQL
- Wget

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.

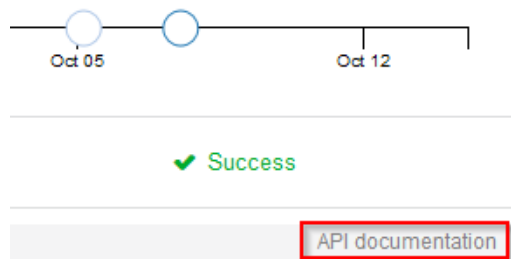
Steps

1. If you are going to reinstall Cloud Manager, back up the database before you uninstall the software:
 - a. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
 - b. Click **Backup** and save the backup file to your local machine.
2. 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.

Cloud Manager REST APIs

Cloud Manager includes REST APIs that enable software developers to automate the management of NetApp storage in the cloud. There is an API for every action that is available from the user interface.

Cloud Manager provides interactive API documentation using the Swagger interface. A link to the API documentation is available in the lower-right corner of the console:



If you need help getting started with the APIs, see the [OnCommand Cloud Manager 2.1 API Getting Started Guide](#).

Copyright information

Copyright © 1994–2015 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, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- accounts
 - creating Cloud Manager users [6](#)
- accounts, user
 - deleting [8](#)
- aggregate free space ratio
 - modifying [12](#)
 - what it is [12](#)
- aggregate overcommitment ratio
 - modifying [12](#)
 - what it is [12](#)
- APIs
 - overview of [19](#)
- autosize
 - modifying maximum size [12](#)
- AutoSupport
 - changing the schedule for [17](#)
 - downloading messages [17](#)
 - sending messages [17](#)
- AWS keys
 - changing for Cloud Manager user account [8](#)

B

- backups
 - backing up Cloud Manager [4](#)

C

- capacity thresholds
 - modifying [12](#)
- certificates
 - installing HTTPS certificate [14](#)
 - managing CA certificates [9](#)
 - renewing Cloud Manager certificate [9](#)
 - renewing HTTPS certificate [15](#)
- Cloud Manager
 - backing up [4](#)
 - moving a working environment [5](#)
 - removing a working environment [5](#)
- comments
 - how to send feedback about documentation [22](#)

D

- database backups
 - backing up Cloud Manager [4](#)
- documentation
 - how to receive automatic notification of changes to [22](#)
 - how to send feedback about [22](#)

E

- encryption
 - managing [9](#)

F

- feedback
 - how to send comments about documentation [22](#)

H

- HTTPS
 - renewing certificate [15](#)
- HTTPS certificate
 - installing [14](#)
 - renewing [15](#)

I

- information
 - how to send feedback about improving documentation [22](#)
- intermediate CA
 - renewing certificate for [9](#)

K

- key managers
 - managing [9](#)

L

- Linux
 - how OnCommand Cloud Manager is configured [17](#)
- logs
 - viewing [17](#)

O

- OnCommand Cloud Manager
 - backing up [4](#)
 - configuration on Linux hosts [17](#)
 - configuring settings [11](#)
 - configuring to use a proxy server [11](#)
 - creating admin user of [6](#)
 - creating user accounts [6](#)
 - restoring [16](#)
 - uninstalling [18](#)

P

- password
 - resetting [8](#)
- permissions
 - for Cloud Manager user accounts [6](#)
- proxy servers
 - configuring Cloud Manager to use [11](#)

R

- restoring

Cloud Manager [16](#)
roles
for Cloud Manager user accounts [6](#)

S

S3 cost bucket
changing for Cloud Manager user [8](#)
settings
configuring for Cloud Manager [11](#)
suggestions
how to send feedback about documentation [22](#)

T

tenants
creating admin user of [6](#)
troubleshooting
resources and tools [16](#)
uninstalling software first [18](#)
twitter
how to receive automatic notification of
documentation changes [22](#)

U

uninstalling
OnCommand Cloud Manager [18](#)
user accounts
creating [6](#)
deleting [8](#)
editing [8](#)
permissions for each role [6](#)

V

volumes
modifying maximum autosize [12](#)

W

working environments
creating admin user of [6](#)
moving [5](#)
removing from Cloud Manager [5](#)