OnCommand® Cloud Manager 3.3

Updating and Administering Cloud Manager

October 2017 | 215-12283_C0
doccomments@netapp.com

Updated for Cloud Manager 3.3.4

NetApp®

Contents

Updating Cloud Manager

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

Choices

Enabling automatic updates

Cloud Manager can automatically update itself to the latest maintenance or minor release whenever 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 task drop-down list, and then select **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.

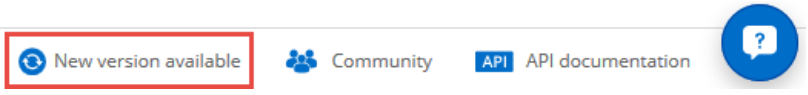
What's new in OnCommand Cloud Manager

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**:
    a. Keep the option to download a backup because you can use it to restore your Cloud Manager configuration, if necessary.
    b. Read the terms and conditions, and then select the **I read and approve the terms and conditions (EULA)** check box.
6. When prompted, save the Cloud Manager backup.

Result

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

Updating Cloud Manager with a patch

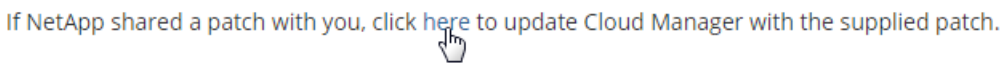
If NetApp shared a patch with you, you can update Cloud Manager with the supplied patch directly from the Cloud Manager web console.

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 hand corner of the Cloud Manager console, click the task drop-down list, and then select **Update**.
2. Click the link to update Cloud Manager with the supplied patch.



3. Complete the confirmation dialog box and then click **OK**:
    a. Keep the option to download a backup enabled because you can use it to restore your Cloud Manager configuration, if necessary.
    b. Read the terms and conditions and then select the **I read and approve the terms and conditions (EULA)** check box.
4. Select the patch that you were provided.
5. When prompted, save the Cloud Manager backup.

Result

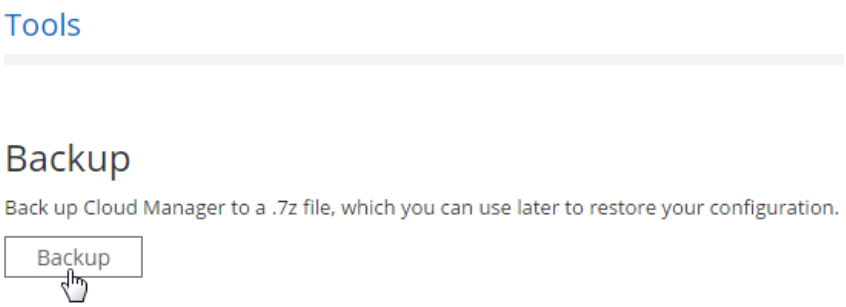
Cloud Manager applies the patch. You can log in to the console after a few minutes.

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**:



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

Removing ONTAP Cloud working environments

The Cloud Manager Admin can remove an ONTAP Cloud 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 ONTAP Cloud 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
Integrate a working environment with Cloud Sync	Yes	Yes	No
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
Switch between the Storage System View and the Volume View	Yes	No	No
Modify settings	Yes	No	No
View and manage the Support Dashboard	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
Set up Active Directory	Yes	No	No

Setting up Cloud Manager to work with AD user accounts

Rather than create new credentials for each Cloud Manager user account, you can set up Cloud Manager so users can log in using your organization's Active Directory (AD) authentication.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Active Directory Setup**.
2. Enter details about your Active Directory server and then click **Save**:

Field	Description
Host	Enter the fully qualified domain name for the Active Directory server.
Port	Enter the TCP port that the Active Directory server uses for LDAP.
User Name and Password	Enter the user name and password for an Active Directory user account, and then click **Test Connectivity**.

After you finish

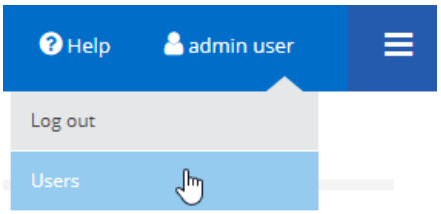
Create new user accounts in Cloud Manager by selecting the **Active Directory** authentication type.

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 user icon, 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
Authentication Type	Select Cloud Manager to create a user account internal to Cloud Manager or select Active Directory if Cloud Manager was set up to work with your organization's Active Directory user accounts.
Email Address	Enter the email address that the user must use to log in to Cloud Manager.

Field	Description
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 Secret Key	Enter the access key and secret key assigned to the user in AWS, unless you associated an IAM role with the Cloud Manager instance. 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 and Azure Policies*
AWS Cost S3 Bucket	Optionally enter the S3 bucket that contains detailed billing reports. Giving Cloud Manager access to detailed billing reports enables users to see AWS storage and compute costs associated with ONTAP Cloud. If you are using AWS consolidated billing and you specified AWS keys, 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.
Azure Permissions	Enter the application ID and Azure key for the Active Directory service principal, the subscription ID for the user, and the Active Directory tenant ID for your organization. Cloud Manager needs this information to log in programmatically to Azure.

4. Click **Save**.

Result

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

Related information

Getting up and running: Granting Azure permissions to Cloud Manager

Editing user accounts

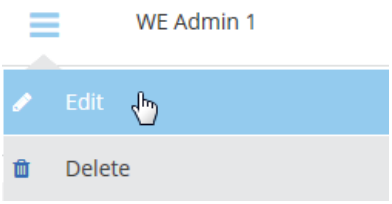
You can modify Cloud Manager user accounts by changing the user's name and email address, by resetting the user's password, by changing the AWS and Azure permissions associated with the account, and by changing the S3 cost bucket in which detailed billing reports are stored.

About this task

You cannot change the account type when you edit a user account. If you want to change between a Cloud Manager and Active Directory (AD) account, then you must create a new user account and then delete the previous account.

Steps

1. In the upper-right corner of the Cloud Manager console, click the user icon, 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 an ONTAP Cloud 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 user icon, 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 encryption settings for ONTAP Cloud

You might need to periodically manage Cloud Manager encryption settings to ensure that ONTAP Cloud systems in AWS 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 ONTAP Cloud systems.

Related information

Learning about Cloud Manager and ONTAP Cloud: How ONTAP Cloud encryption works

Renewing the Cloud Manager certificate

You must renew the Cloud Manager certificate before it expires; otherwise, Cloud Manager cannot sign client certificates for ONTAP Cloud 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* ONTAP Cloud systems. You can renew client certificates for *existing* ONTAP Cloud 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 ONTAP Cloud 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* ONTAP Cloud systems. Changes to *existing* ONTAP Cloud 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 ONTAP Cloud systems. To change the port for an existing ONTAP Cloud system, connect to the CLI and then run the `security key-manager setup` 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 ONTAP Cloud 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 ONTAP Cloud systems that will use this key manager. To apply this change to existing ONTAP Cloud 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 ONTAP Cloud 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 ONTAP Cloud systems to use it. Existing systems that are using the certificate can continue to use it.

Configuring Cloud Manager settings

Cloud Manager includes settings that determine how it allocates capacity, whether it uses an HTTP proxy server, how it makes storage capacity decisions, and whether it automatically updates itself to the latest version.

Choosing how storage capacity decisions are made

When you set up Cloud Manager, you chose to either automate capacity management decisions or to prompt users for approval. You can change the mode at any time.

About this task

Additional cloud resources are required as ONTAP Cloud volumes grow. The capacity management mode determines whether Cloud Manager notifies users of storage capacity decisions or whether Cloud Manager automatically manages capacity requirements for you.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Settings**.
2. Choose a capacity management mode:

Choice	Action
You want Cloud Manager to automate storage capacity decisions for users	Select **Automatic Mode**. Cloud Manager automatically purchases new disks for ONTAP Cloud instances when more capacity is needed, deletes unused collections of disks (aggregates), and moves volumes between aggregates, as needed. **Important:** When you choose this mode, Cloud Manager allocates the appropriate cloud resources as needed, without asking for your approval.
You want users to make storage capacity decisions	Select **Manual Mode**. Cloud Manager displays Action Required messages when capacity decisions must be made. It is up to the user to accept the actions.

3. Click **Save**.

Result

Cloud Manager updates the settings.

Related information

Learning about Cloud Manager and ONTAP Cloud: How Cloud Manager helps with capacity decisions

Configuring Cloud Manager to use a proxy server

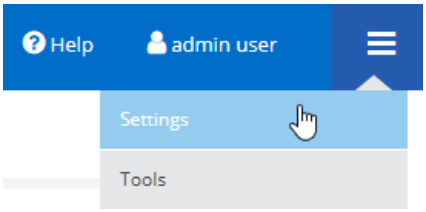
If your corporate policies dictate that you use a proxy server for all HTTP communication to the Internet, then you must configure Cloud Manager to use that proxy server. The proxy server can be in the cloud or in your network.

About this task

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

Steps

1. In the upper-right 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`, specify a user name and password if basic authentication is required for the server, and then click **Save**.

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

Result

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

Modifying aggregate capacity thresholds

Several thresholds determine how much free space is required in an aggregate. In most cases, you should keep the default values, but you can modify them 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.

Ratio of EBS free capacity to S3 used data capacity, per aggregate

This ratio defines how much free space is required on EBS storage when tiering data to Amazon S3. The ratio is important for disaster recovery scenarios because as data is read from S3, ONTAP Cloud moves the data to EBS storage to provide better performance. If there is not sufficient space, then ONTAP Cloud cannot move the data.

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 **Aggregate 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 ONTAP Cloud 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 it 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.

Enabling automatic updates

Cloud Manager can automatically update itself to the latest maintenance or minor release whenever 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 task drop-down list, and then select **Settings**.
2. Select the checkbox under **Automatic Cloud Manager Updates** and then click **Save**.

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.

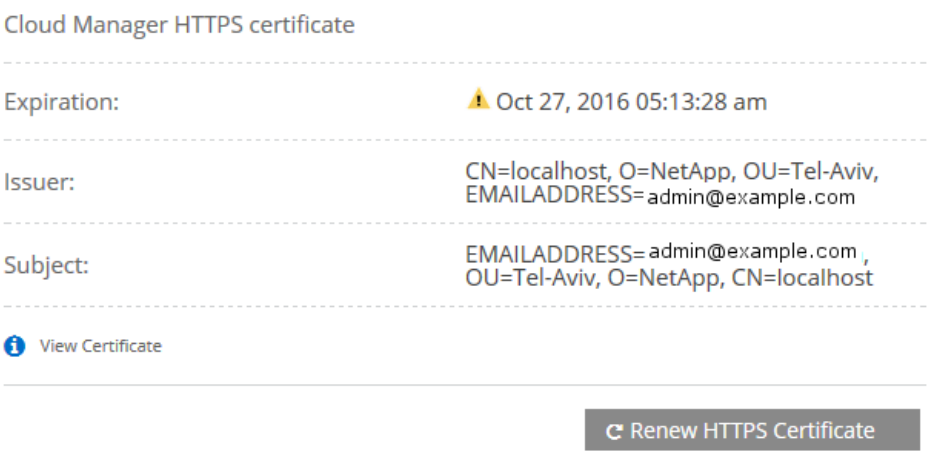
Steps

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, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	**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 content of the signed certificate, paste it in the Certificate field, and then click **Install**.
Install your own CA-signed certificate	**a.** Select **Install CA-signed certificate**. **b.** Load both the certificate file and the private key and then click **Install**. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

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:



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** 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.

Troubleshooting Cloud Manager and ONTAP Cloud

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

Task	Resource
View known issues and limitations	*OnCommand Cloud Manager 3.3 Release Notes* *Find the Release Notes for your version of ONTAP Cloud* *Find the Release Notes for your version of ONTAP 9*
View cloud-related KB articles and frequently asked questions or chat with technical support	*NetApp ONTAP Cloud 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 20
View logs	Click the menu icon and then select **Support Dashboard**. You can access logs by downloading AutoSupport messages.
Understand how Cloud Manager is configured on Linux	*Learning about Cloud Manager and ONTAP Cloud: How Cloud Manager is configured on Linux hosts*
Uninstall Cloud Manager to troubleshoot issues	*Uninstalling Cloud Manager* on page 22

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 6

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.

Copyright information

Trademark information

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.

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

S

T

U

V

W