Managing encryption settings for Cloud Volumes ONTAP

You might need to periodically manage Cloud Manager encryption settings to ensure that Cloud Volumes ONTAP systems in AWS can communicate with key managers.

Data-at-rest encryption provided by Cloud Volumes ONTAP is no longer supported when launching new Cloud Volumes ONTAP systems in AWS. Existing systems that use this feature are still supported. See What's new in Cloud Manager for more details.

Table of Contents

Renewing the Cloud Manager intermediate CA certificate 1
Managing available key managers and CA certificates 2

Renewing the Cloud Manager intermediate CA certificate

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

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 Volumes ONTAP systems. You can renew client certificates for *existing* Cloud Volumes 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 Volumes 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 Volumes ONTAP systems. Changes to existing Cloud Volumes 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:

Action	Steps
Change the KMIP port for communicating with key managers	Modify the port and then click **Save**. The port change affects only new Cloud Volumes ONTAP systems. To change the port for an existing Cloud Volumes ONTAP 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 Cloud Volumes 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 Volumes ONTAP systems that will use this key manager. To apply this change to existing Cloud Volumes 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 Volumes 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:

Action	Steps
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 Volumes ONTAP systems to use it. Existing systems that are using the certificate can continue to use it.