Dell EMC CloudLink

Key Management for VMware vCenter Server Configuration Guide

6.9, 7.0.2, 7.1, and 7.1.1

October 2021
Rev. A00

Notes, cautions, and warnings

ⓘ **NOTE:** A NOTE indicates important information that helps you make better use of your product.

△ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

Contents

1

Introduction

Dell EMC CloudLink versions 6.9, 7.0.2, 7.1, and 7.1.1 support the Key Management Interoperability Protocol (KMIP) to allow applications supporting that protocol to securely store keys and certificates. The applications, or KMIP clients, are given access to a single KMIP partition. A KMIP partition is a container for keys and certificates that are created by the client.

All objects within a partition are encrypted using a key that is saved to the keystore of a partition and are stored in the CloudLink Center database. The KMIP Server menu is only available in the CloudLink Center Contents pane after a KMIP license is uploaded.

Use the following procedures to create a trusted connection between CloudLink Center and a vCenter Server by adding a KMIP partition and a client.

ⓘ **NOTE:** CloudLink versions 6.9, 7.0.2, 7.1, and 7.1.1 support KMIP 1.1 through 1.4.

2

Add a KMIP partition

Use this procedure to add a KMIP partition.

Steps

1. Log in to CloudLink Center as an administrator with permission to configure KMIP partitions and clients.
2. Ensure that you have a valid KMIP license.
   a. Click **System** > **License**.
   b. Confirm that there is a valid KMIP license assigned.

   Add a new KMIP partition to store keys and certificates separately from other KMIP clients.
3. Click **KMIP Server** > **Partitions**.
4. Click **Add**.
5. In the **Add New Partition** dialog box, enter the following values:
   - **Partition Name**—A name for the KMIP partition
   - **Description (optional)**—A brief description of the partition
   - **Keystore**—The keystore used to store the encryption key that encrypts the KMIP objects
   - **Key Caching**—You can choose to cache or not cache the KMIP partition protection key. Key caching stores the protection key locally in CloudLink Center.
   - **Managed By**—The names of the roles that administer this KMIP partition

3

Add a KMIP client

Use this procedure to add a KMIP client to allow vCenter Server to connect to and authenticate the connection with CloudLink Center.

Steps

1. Log in to CloudLink Center.
2. Click **KMIP Server** > **Clients** > **Add**.
3. In the **Add New Client** dialog box, provide the following values:
   - **Username**—Username for client authentication from the KMIP client.
   - **Partition**—The KMIP partition created in Add a KMIP partition.
   - **Credential Type**—A username and password.
   - **Password**—Password for client authentication from the KMIP client.
   - **Certificate Format**—Use the default PEM certificate.
   - **Notes**—Enter the name of the application using the KMIP client.
4. Click **Add**
   The required keys and certificates are automatically downloaded in a `ZIP` file.
5. Extract the files `ca.pem`, `cert.pem`, and `key.pem` to an accessible location.

Configure the Key Management Server

Use this procedure to configure CloudLink Center as the Key Management Server in vSphere Web Client.

Steps

1. Use the vSphere Web Client to log in to the vCenter Server.
2. Select the vCenter Server in the **Object Navigator**.
3. Select **Configure** > **Key Management Servers** in vSphere Web Client.
4. Click **Add KMS** > **Create a new cluster** and provide the following values:
   - **Cluster name**—A name for the cluster
   - **Server alias**—A name for the CloudLink Center instance
   - **Server address**—Address of the CloudLink Center instance
   - **Server port**—Enter `5696`
   - **Proxy Address**—Leave it blank
   - **Proxy Port**—Leave it blank
   - (Optional) **Username**—Enter the username added in Add a KMIP client
   - (Optional) **Password**—Enter the password added in Add a KMIP client

Configure the Key Management Server for CloudLink in VMware vSphere 7.0

Use this procedure to configure CloudLink Center as the Key Management Server in vSphere Web Client.

Steps

1. Use the vSphere Web Client to log in to the vCenter Server.
2. Select the vCenter Server in the **Object Navigator**.
3. Select **Configure** > **Key Providers** in vSphere Web Client.
4. Click **Add Standard Key Provider** and provide the following values:
   - **Name**—A name for the Key Provider
   - **KMS**—A name for the CloudLink Center instance
   - **Address**—Address of the CloudLink Center instance
   - **Server port**—Enter `5696`
   - **Proxy Address**—Leave it blank
   - **Proxy Port**—Leave it blank
   - (Optional) **Username**—Enter the username added in Add a KMIP client
   - (Optional) **Password**—Enter the password added in Add a KMIP client
5. Select the key provider you added.
6. Select the KMS from the **Provider <Key provider name> - Key Management Servers** table, and then click **Establish Trust**.

6

Upload the KMS certificate

Use this procedure to upload the KMS certificate to vSphere Web Client.

Steps

1. In **Key Management Servers**, select the KMS created in Configure Key Management server.
2. Click **All Actions** > **Upload KMS certificate**.
3. Click **Upload file** and select the `ca.pem` file.
4. Click **OK**.

Establish a trusted connection in vSphere 6.5

Use this procedure to establish a trusted connection between CloudLink Center and vSphere Server.

Steps

1. Click **Establish trust with KMS in Key Management Servers**.
2. Click **Upload certificate and private key**, and then click **OK**.
3. Click **KMS certificate** > **Upload file**, and then select the `cert.pem` file.
4. Click **Upload file** in the private key section and select the `key.pem` file, and then click **OK**.
   The Connection Status changes to **Normal**.
5. If you are using a CloudLink Center cluster, separately add each CloudLink Center server in the cluster to the KMS cluster.
   Repeat step 4, but select the KMS cluster you have already created.

Establish a trusted connection in vSphere 6.7

Use this procedure to establish a trusted connection between CloudLink Center and vSphere Server.

Steps

1. Click **Establish trust** > **Make KMS trust vCenter**.
2. Select **Upload certificate and private key**, and then click **OK**.
3. Select **Upload file** in the **KMS certificate** section and select the `cert.pem` file.
4. Select **Upload file** in the private key section and select the `key.pem` file, and then click **Establish Trust**.
   The Connection Status changes to **Normal**.
5. If you are using a CloudLink Center cluster, separately add each CloudLink Center server in the cluster to the KMS cluster.
   Repeat step 4, but select the KMS cluster you have already created.

Establish a trusted connection in vSphere 7.0

Use this procedure to establish a trusted connection between CloudLink Center and vSphere Server.

Steps

1. Click **Establish trust** > **Make KMS trust vCenter**.
2. Select **KMS certificate and private key**, and then click **Next**.
   The Upload KMS Credentials page is displayed.
3. In the **KMS Certificate** section, click **Upload file** to select the `cert.pem` file.
4. In the **KMS Private Key section** section, click **Upload file** to select the `key.pem` file, and then click **Establish Trust**.
   The Connection Status changes to **Normal**.
5. If you are using a CloudLink Center cluster, separately add each CloudLink Center server in the cluster to the KMS cluster.
   Repeat step 4, but select the KMS cluster you have already created.

10

Troubleshooting and getting help

Go to Dell Technologies Online Support and click **MyService360**. You will see several options for contacting Dell Technologies Technical Support. To open a service request, you must have a valid support agreement. Contact your Dell Technologies sales representative for details about obtaining a valid support agreement or with questions about your account.

Dell Technologies support, product, and licensing information can also be obtained from your Dell Technologies account manager.