VMware vSphere and Entrust KeyControl

nShield® HSM Integration Guide

14 Jan 2022

Contents

1. Introduction . . . 3
    1.1. Product configuration . . . 3
2. Procedures . . . 4
    2.1. Prerequisites . . . 4
    2.2. Documents to read first . . . 4
    2.3. Install and setup Entrust KeyControl . . . 4
    2.4. Create the KMS cluster in vCenter . . . 4
    2.5. Establish a trusted connection between the KMS cluster and the Entrust KeyControl server . . . 6
    2.6. Enable Encryption for target servers . . . 8
    2.7. Enable Data-At-Rest encryption on an existing vSAN cluster . . . 10

1. Introduction

This guide describes the procedure to integrate Entrust KeyControl and VMware encryptions solutions, vSAN and VM encryption. vSAN and VM encryption use the Key Management Interoperability Protocol (KMIP). Entrust KeyControl provides a KMIP interface to a Key Management System (KMS) object that is protected by an nShield Hardware Security Module (HSM).

1.1. Product configuration

Product	Version
VMware vSphere	7.0.2
KeyControl	5.5 Multi Tenant
nShield HSM hardware	Connect XC
nShield firmware	12.50.11 - Image 12.80.4

2. Procedures

2.1. Prerequisites

- Entrust KeyControl has been deployed and configured.
- VMware vSphere has been deployed and configured using vCenter.
- You have administrator rights to manage the KMS configuration in vCenter.

2.2. Documents to read first

This guide describes how to configure the Entrust KeyControl server as a KMS in vCenter.

To install and configure the Entrust KeyControl server as a KMIP server, see the `Entrust KeyControl nShield HSM Integration Guide`.

Also refer to VMware documentation: * Using Encryption in a vSAN Cluster. * Virtual Machine Encryption.

2.3. Install and setup Entrust KeyControl

Follow the installation and setup instructions in the `Entrust KeyControl nShield HSM Integration Guide`.

Make sure the Entrust KeyControl tenant gets created and KMIP certificates are generated for VMware vSphere. These certificates are used in the configuration of the KMS described below.

2.4. Create the KMS cluster in vCenter

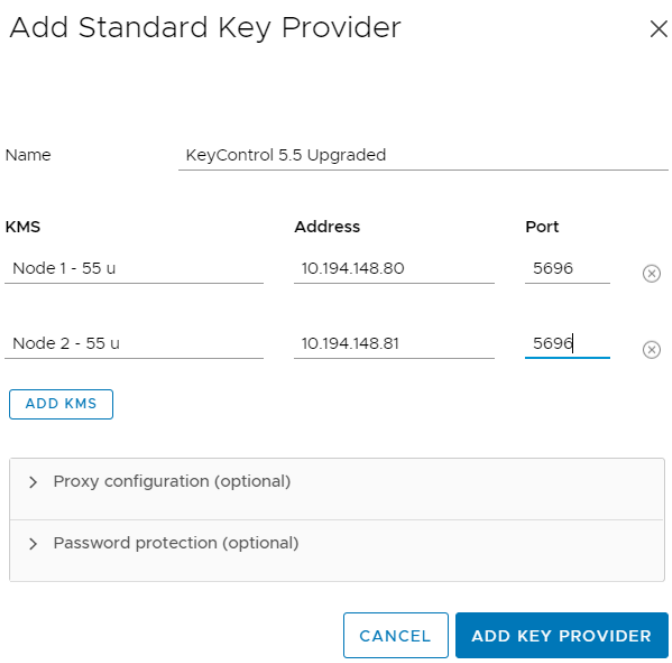
For more detail on how to do this, see Creating the KMS Cluster in vSphere.

1. Launch the vSphere Web Client and log into the vCenter server that you want to add to Entrust KeyControl.
2. Select the required vCenter Server in the **Global Inventory Lists**.
3. Select the **Configure** tab.
4. In the left-hand pane, select **Security > Key Providers**.
5. Select **Add Standard Key Provider**.
6. In the **Add Standard Key Provider** dialog, set the following configuration options:
    - For **Name**, enter the name of the cluster.
    - For each node in the KeyControl cluster, enter the **KMS** (node name), **IP Address**

and **Port**. The default port is 5696.

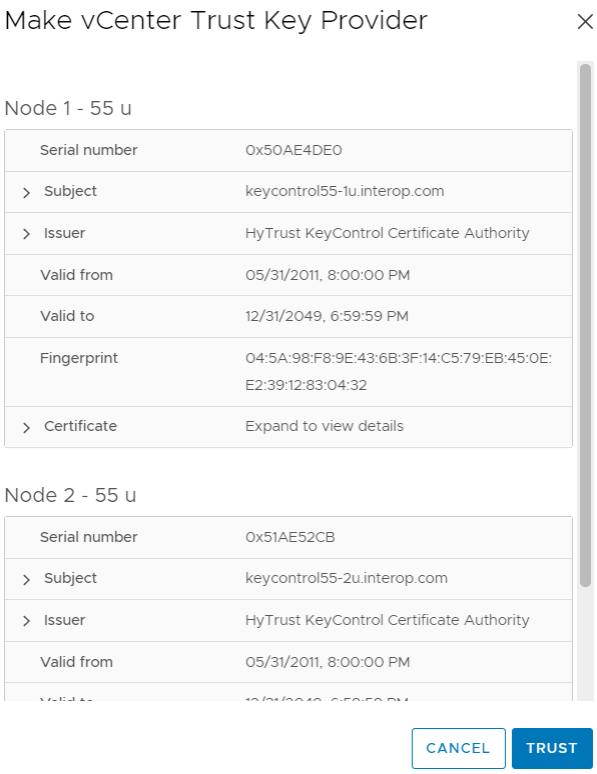
Make sure that the KMIP server resides on a device that is not encrypted. The KMIP server must be available to provide the keys for the encrypted devices before the encrypted devices can be accessed.

To add an extra node line, select **Add KMS**.

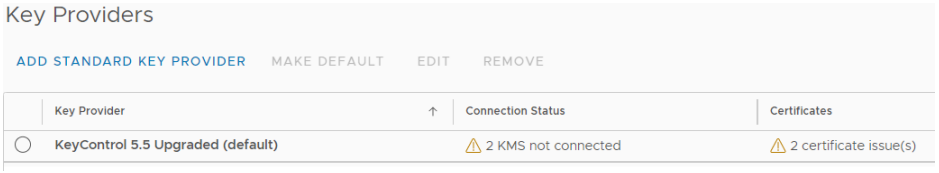


- Open and set **Proxy Configuration** if you are using a proxy.
- **Password protection** is optional.

7. Select **Add Key Provider**.
8. In the **Make vCenter Trust Key Provider** dialog, confirm the details for each node and then select **Trust**. For example:

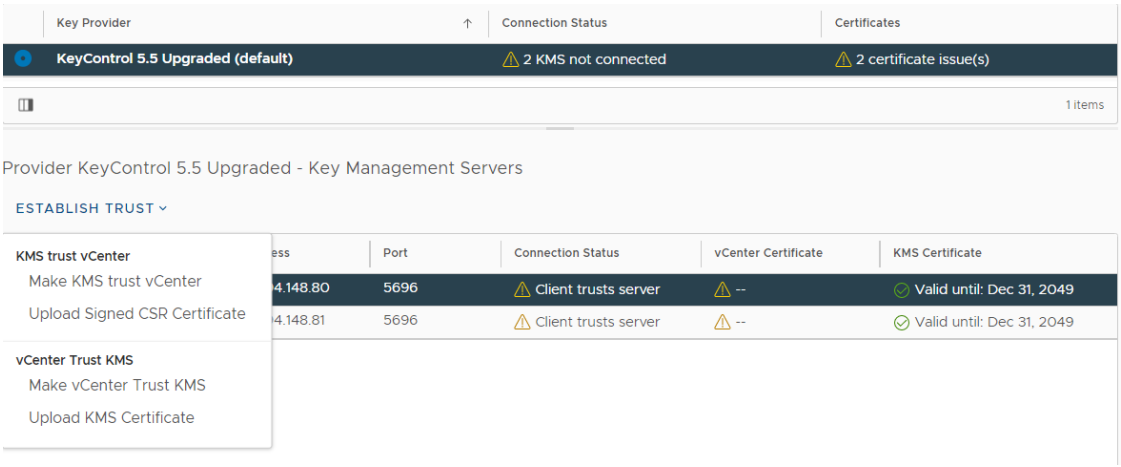


This adds the KMS cluster to vCenter but the connection status will be **KMS not connected** with **Certificate issues**. For example:

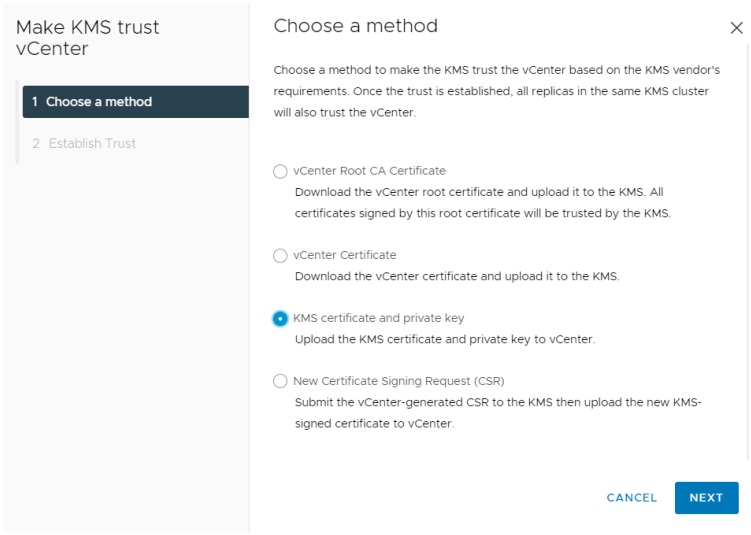


2.5. Establish a trusted connection between the KMS cluster and the Entrust KeyControl server

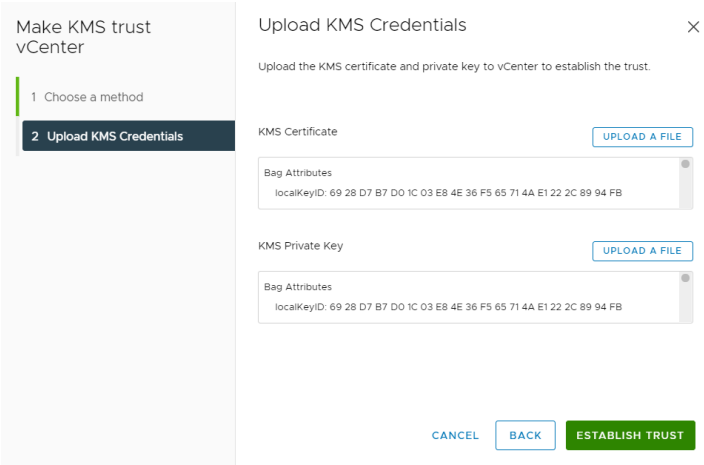
1. Launch the vCenter vSphere Web Client and log into the vCenter server to which you added the KeyControl KMS cluster.
2. Select the **Configure** tab for the server.
3. In the left-hand pane, select **Security > Key Providers**.
4. Select the KeyControl KMS cluster in the list, then scroll down to where the nodes are displayed.
5. Select one of the nodes, then select on **Establish Trust** > **Make KMS trust vCenter**. For example:



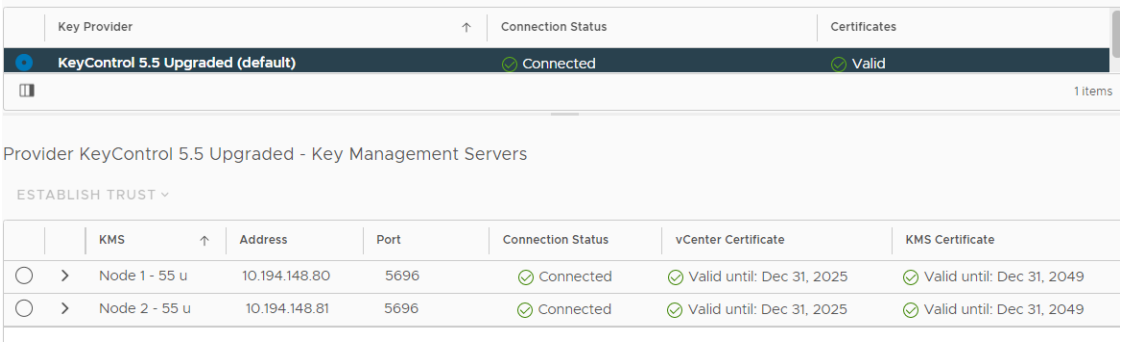
6. In the **Choose method** pane of the **Make KMS Trust vCenter** dialog, select **KMS certificate and private key**.



7. Select **Next**.
8. In the **Upload KMS Credentials** pane of the **Make KMS Trust vCenter** dialog, you need to upload the `certname.pem` file created during the certificate creation process described in the `Entrust KeyControl nShield Integration guide`. This file needs to be uploaded for the KMS certificate, and then uploaded again for the private key. To do this:
    - For **KMS certificate**, select **Upload file**. Then select the `certname.pem` file and select **Open**.
    - For **Private key**, select **Upload file**. Then select the `certname.pem` file again and select **Open**.
    - Select **Establish Trust**.



9. Wait until vCenter reports that the connection status for the KMS cluster has changed to **Connected**. For example:

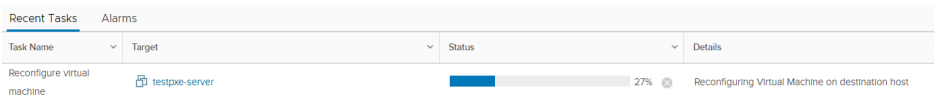


2.6. Enable Encryption for target servers

Enable encryption using VMware Storage Policies.

1. Launch the vSphere Web Client and log into the vCenter server.
2. Locate a VM that you would like to encrypt.
3. Make sure the **Power** state of the VM is **Powered Off**.
4. Right-click the VM for which you would like to enable encryption, and select **VM Policies > Edit VM Storage Policies**.
5. Select the storage policy **VM Encryption Policy** and select **OK**.

   This will trigger a reconfiguration of the VM.



   After the reconfiguration is complete, the disks are encrypted and the keys are managed by the configured KMS (KeyControl).

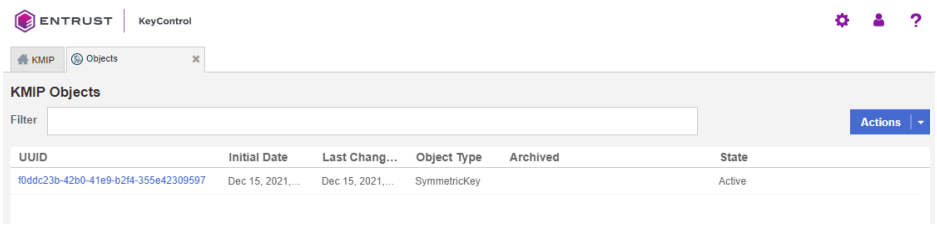
2.6.1. Check encryption at the VM level

1. Launch the vSphere Web Client and log into the vCenter server.
2. Locate a VM, and select it.
3. In **VM View**, select the **Summary** tab.
4. Under **VM Hardware** > **Encryption**, the status should be:

```
VM configuration files are encrypted.
Hard disk is encrypted.
```

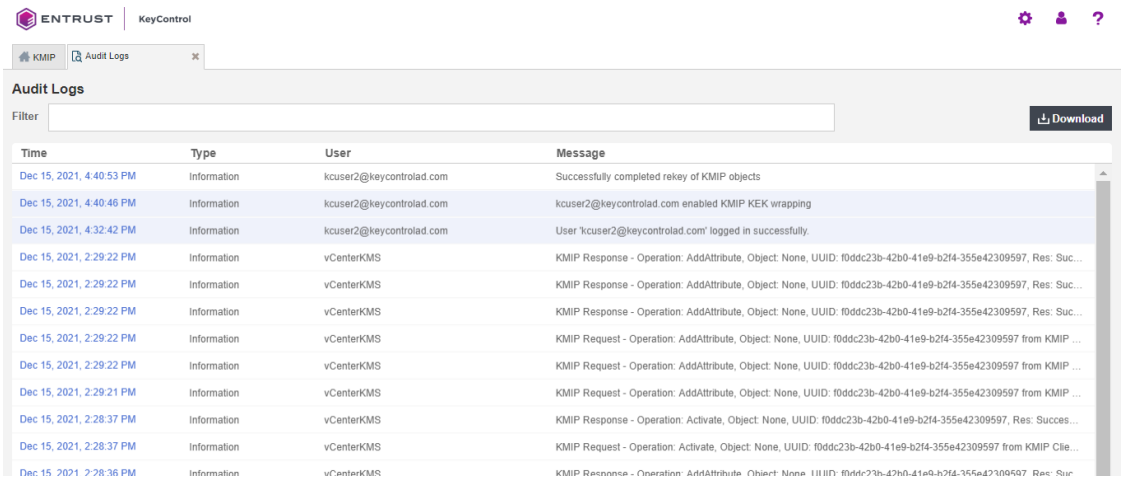
2.6.2. Check encryption by looking for the Keys in the Entrust KeyControl KMS

1. Log into the KeyControl web user interface using the **Tenant Login** URL.
2. Select the **Objects** tab to view a list of **KMIP Objects**. This will include the newly created keys. For example:



3. Select one of the keys to display its details. For example:

4. In the main screen, select the **Audit Logs** tab to view the log records related to the key creation process. For example:



For more information on this topic, refer to Virtual Machine Encryption on the VMware documentation site.

2.7. Enable Data-At-Rest encryption on an existing vSAN cluster

To enable Data-At-Rest encryption on an existing vSAN cluster, refer to Using Encryption in a vSAN Cluster. on the VMware documentation site.