Fortanix®

Integration Guide

USING DATA SECURITY MANAGER FOR VMWARE CLOUD DIRECTOR

Fortanix Inc. | 800 West El Camino Real | Suite 180 | Mountain View, CA 94040 | United States of America |
+1 (650) 943-2484 | info@fortanix.com | www.fortanix.com

1.0 INTRODUCTION

This article describes how to use **Fortanix Data Security Manager (DSM)** for **VM encryption** through **VMware Cloud Director.** It also contains the information that a user requires for:

- Facilitating the communication and authentication between Fortanix DSM and vCenter using KMIP interface
- Setting up Fortanix DSM.
- Exposing VM Encryption storage policy to tenants
- Enabling VM Encryption storage policy for VM encryption

1.1 FORTANIX DATA SECURITY MANAGER

Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

2.0 KMIP AND CERTIFICATE REQUIREMENTS

The Key Management Interoperability Protocol (KMIP) is used to facilitate communication between the vCentre and Fortanix DSM. KMIP uses Transport Layer Security (TLS) to provide a secure connection and Fortanix DSM also uses this to Authentication a KMIP client to successfully create, retrieve and use the keys stored inside Fortanix DSM.

2.1 PRE-REQUISITES

- vCenter connected to Cloud Director 10.0 or later is installed and operational
- Fortanix DSM version 3.20 or later
- Fortanix DSM is installed and operational, and is accessible by the vCentre on port 5696 (for default) or custom KMIP port

2.2 CONSIDERATIONS

The following are some key points to understanding the Fortanix DSM for VM encryption:

- The VMs needs to be power off to apply the VM encryption storage policy.
- vCenter supports only one (1) external KMS at a time, and the IP address of the KMS cannot be altered once configured.

3.0 SETTING UP FORTANIX DATA SECURITY MANAGER

Fortanix DSM supports KMIP clients to authenticate using a certificate through Apps.

3.1 CONFIGURE APP IN FORTANIX DATA SECURITY MANAGER

1. Log in to the Fortanix DSM UI.
2. Click the Application icon  , and then click  to create a new application.
3. Enter the following details:
   - **App name**: This is the name to authenticate Fortanix DSM with vCentre
   - **Interface**: `KMIP`
   - **Authentication method**: The default value of **API Key** is fine.
   - **Assigning the new app to groups**: Keys created by vCenter will be owned by this Group.

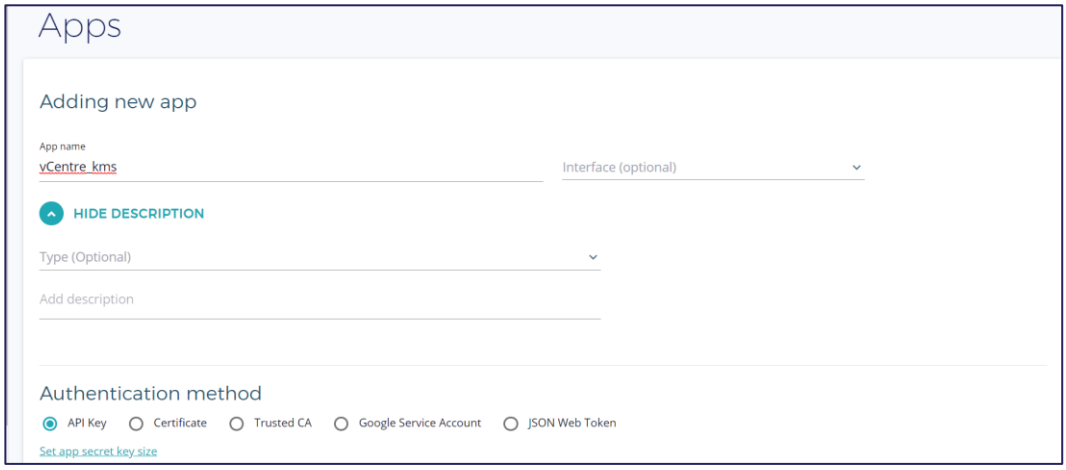

FIGURE 1: CREATE AN APP

4.0 CONFIGURE VCENTER KEY MANAGEMENT SETTINGS

You may configure Fortanix DSM as an external KMS in vCenter using the vSphere Client UI.

4.1 CONFIGURE FORTANIX DATA SECURITY MANAGER IN VCENTER

1. Log in to vCenter using vSphere Client UI.
2. Navigate to **Configure** -> **Key Providers**.

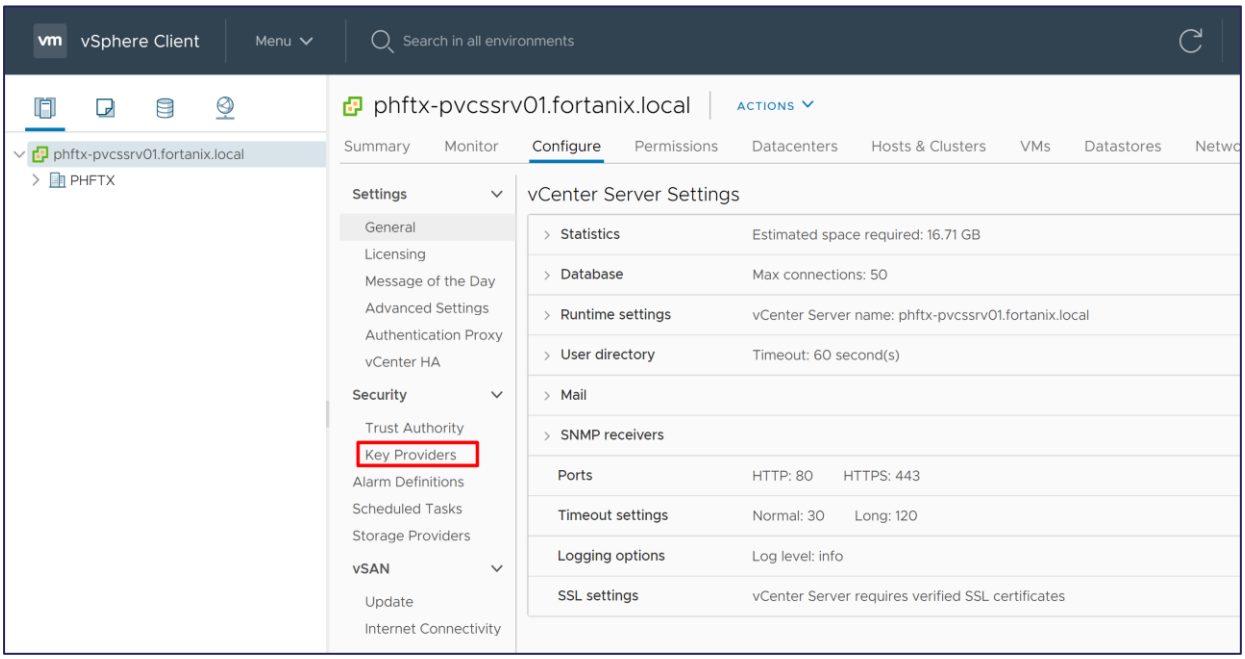

FIGURE 2: VSPHERE CLIENT UI

3. In the Key Management **ADD STANDARD KEY PROVIDER** form, enter the following details:
   - **Name:** Name of KMS - **`SDKMS`**
   - **Address**: Fortanix DSM IP address. In this case, **`apps.sdkms.fortanix.com`**
   - **Port**: **`5696`**
   - **Username**: Copy the value from Fortanix DSM App
   - **Password**: Copy the value from Fortanix DSM App

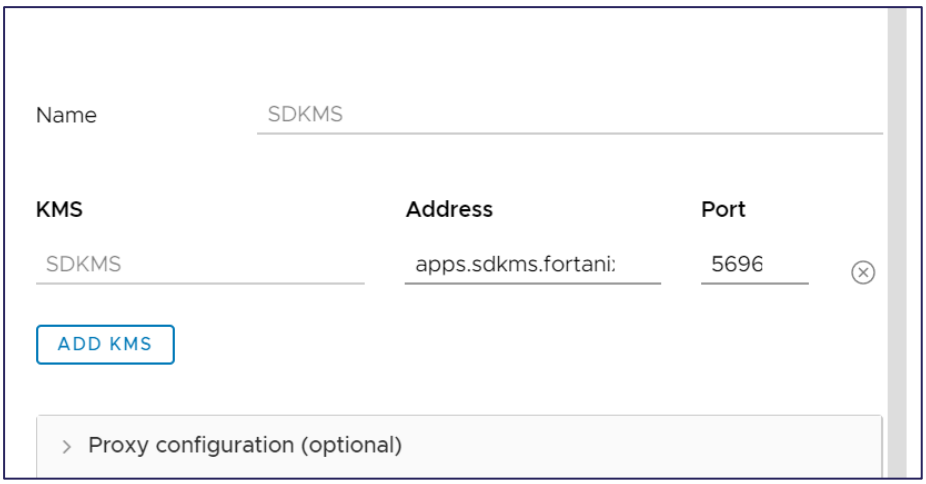

FIGURE 3: KEY MANAGEMENT CONFIGURATION DETAILS

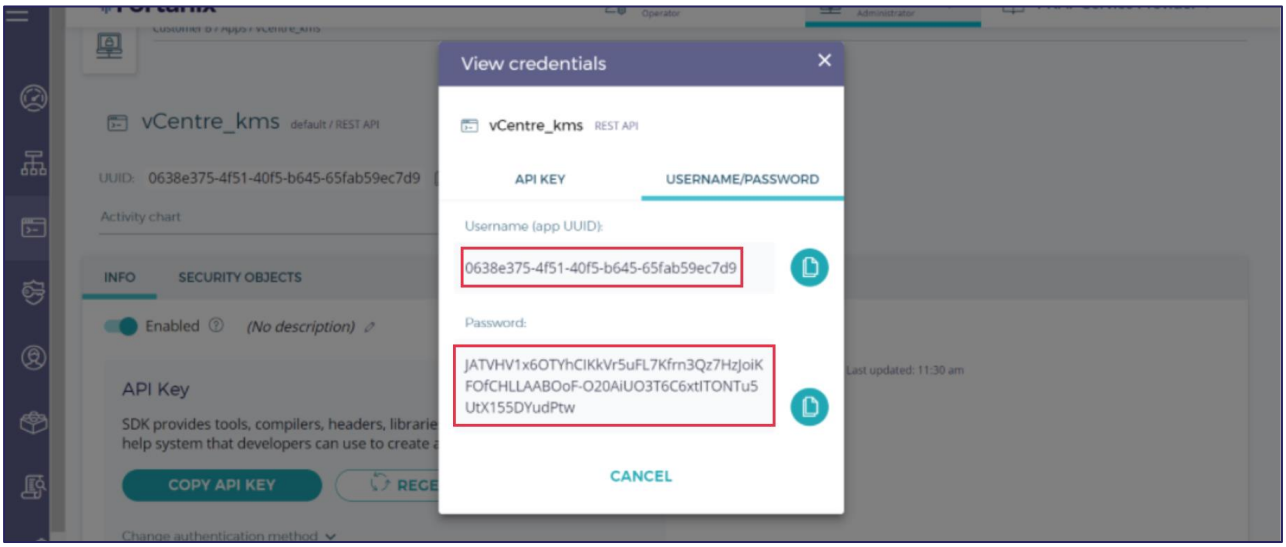

FIGURE 4: USERNAME AND PASSWORD FROM FORTANIX DSM

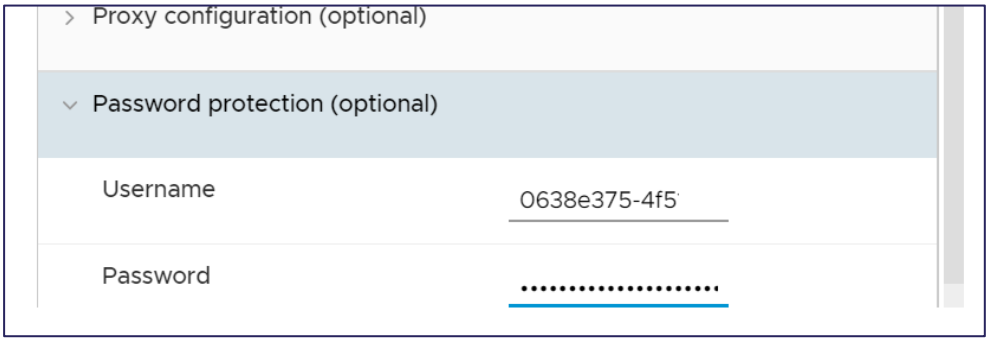

FIGURE 5: KEY MANAGEMENT CONFIGURATION DETAILS

4. Click **Add Key Provider**.
5. Establish trust between Fortanix DSM and vCentre by clicking **Establish Trust -> Make vCenter Trust KMS**. Click **TRUST**.

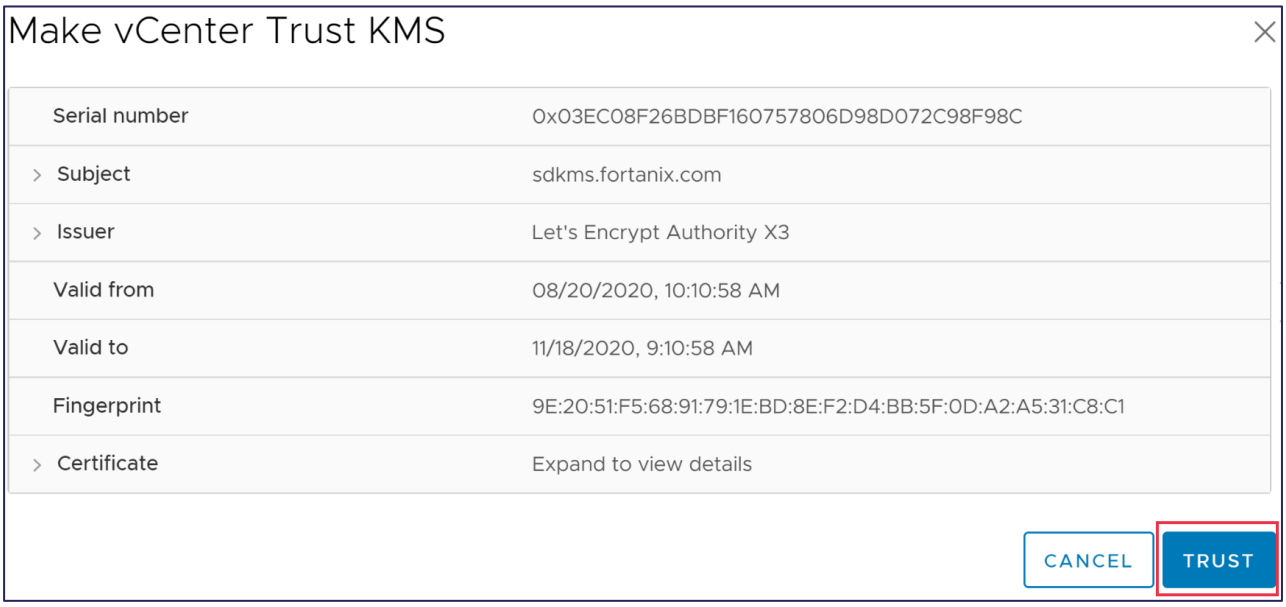

FIGURE 6: ESTABLISH TRUST

4.2 EXPOSE VM ENCRYPTION POLICY TO TENANTS

As a service provider, make sure you exposed VM encryption storage policy to the tenants.

1. Log in to the VMware Cloud Director provider portal.
2. Click **Organization VDCs** and enable VM encryption policy for the organization.

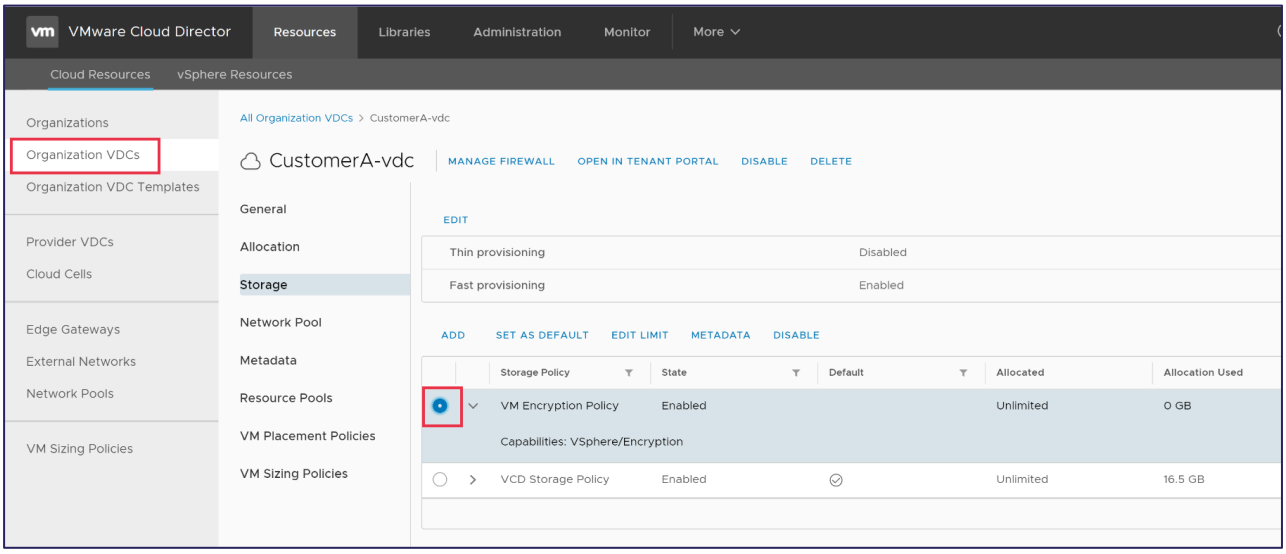

FIGURE 7: ENABLE VM ENCRYPTION POLICY

4.3 TENANTS APPLY VM ENCRYPTION STORAGE POLICY TO VM

The tenants can apply the VM encryption storage policy to the VM(s) they want to encrypt.

1. The Tenants can log in to the VMware Cloud Director tenant portal.
2. Click the VM that needs to be encrypted. Make sure that the VM is powered off.

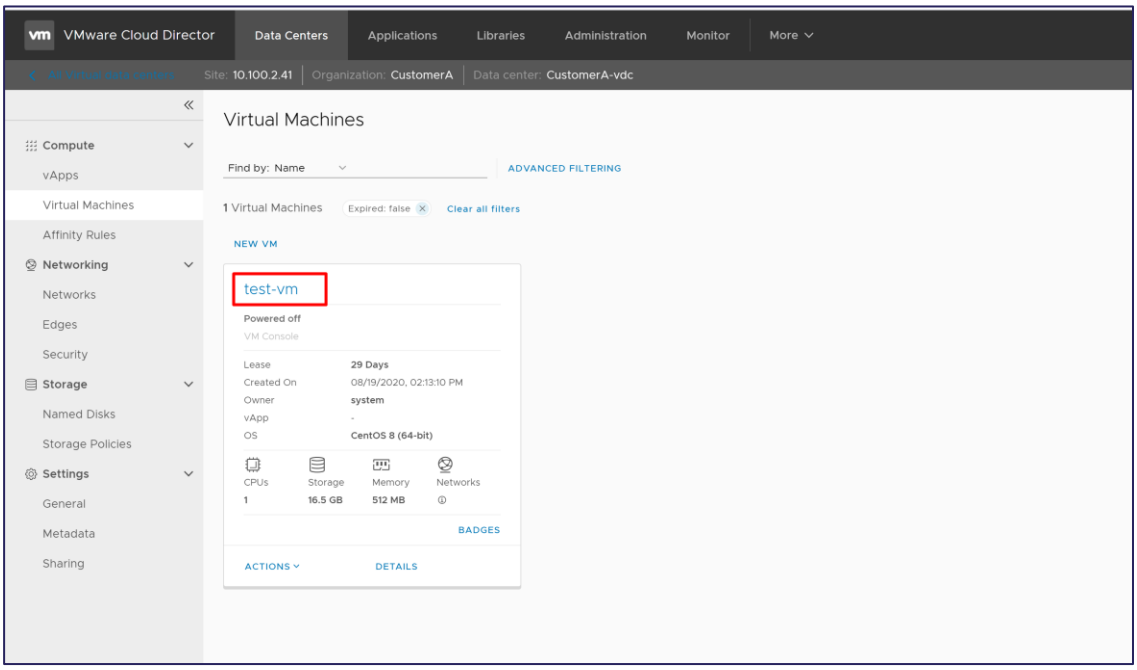

FIGURE 8: TENANT PORTAL

3. Apply VM Encryption storage policy to the VM.

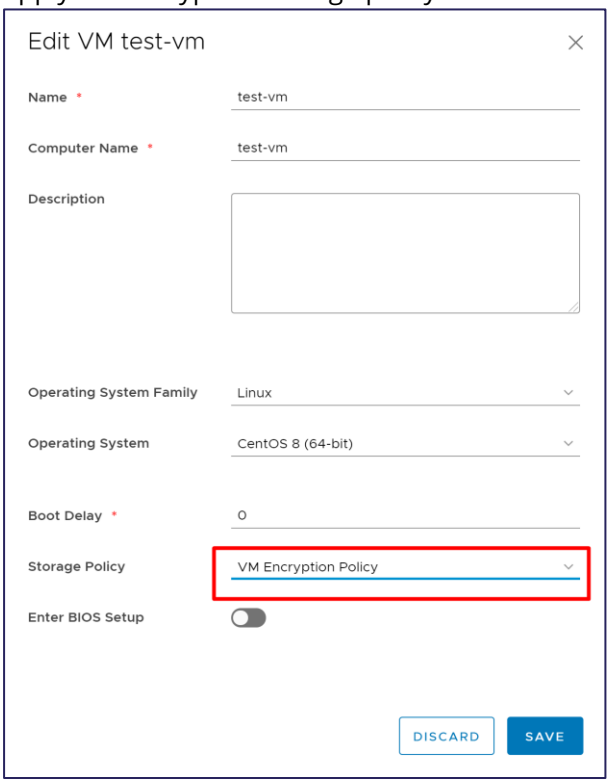

FIGURE 9: APPLY VM ENCRYPTION POLICY

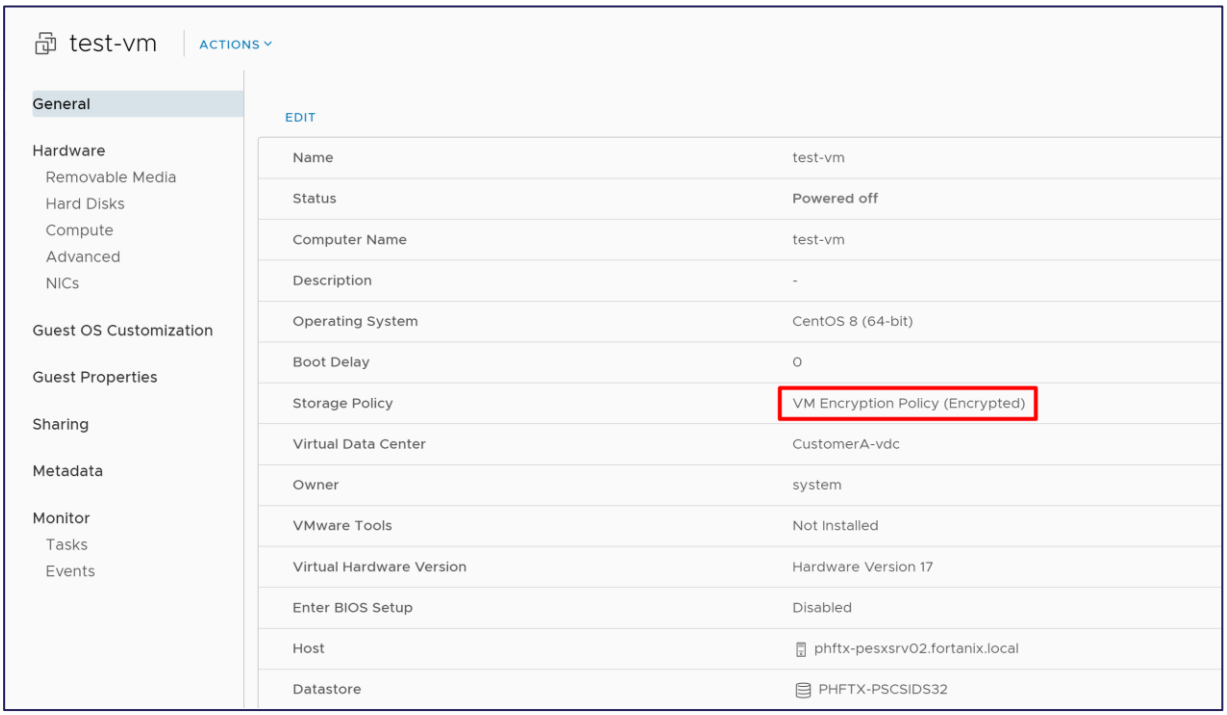

FIGURE 10: VM ENCRYPTION POLICY

4.4 VERIFICATION ON FORTANIX DATA SECURITY MANAGER

Service providers can log in to Fortanix DSM to see the logs of the connection and the key created as well.

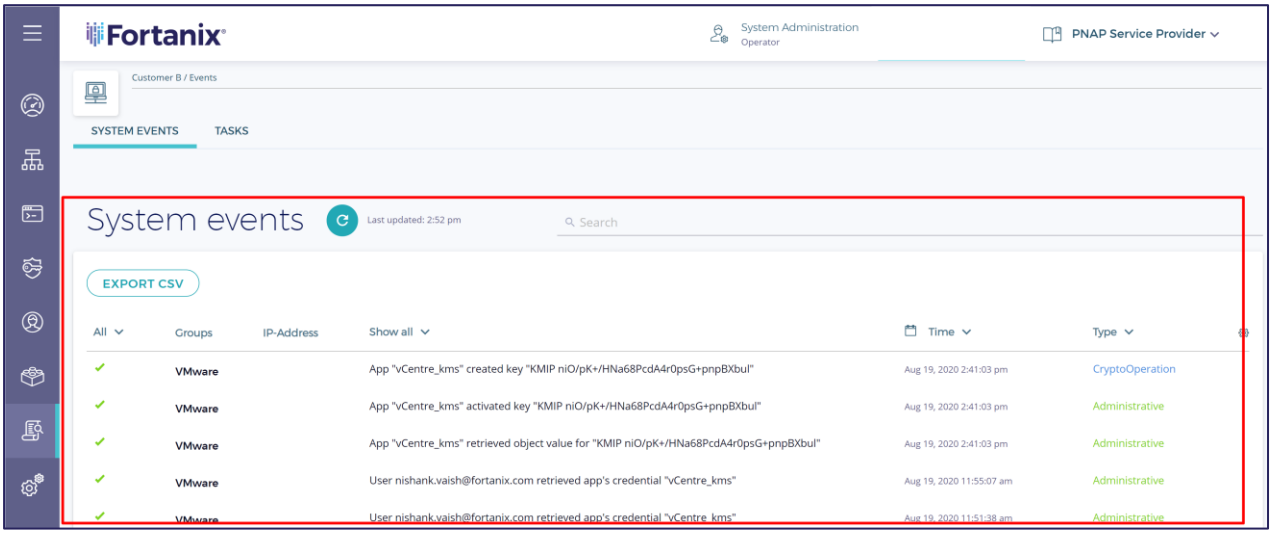

FIGURE 11: CONNECTION LOGS

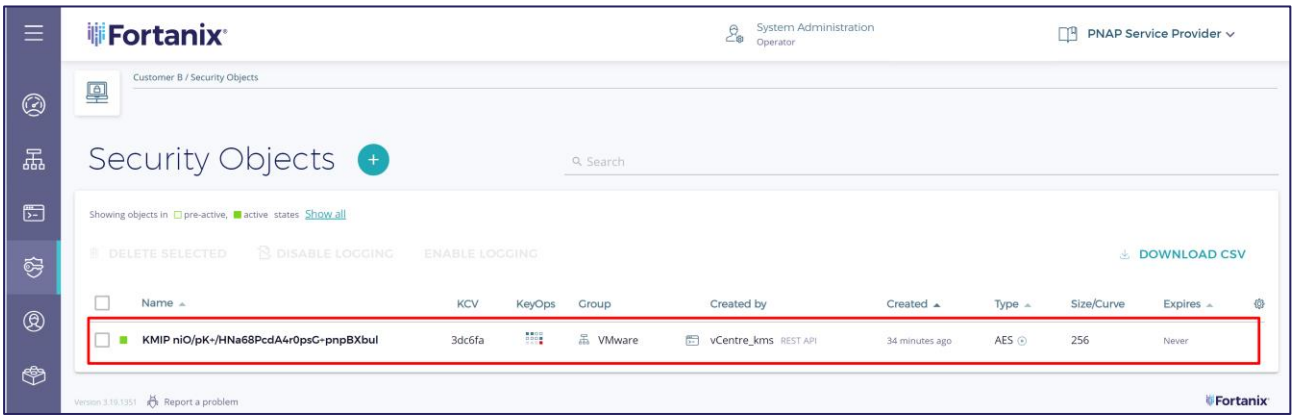

FIGURE 12: ENCRYPTION KEY CREATED

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

The latest published version of the document is located in the URL:

https://support.fortanix.com/hc/en-us/articles/360048672072-Using-Fortanix-Data-Security-Manager-for-VMware-Cloud-Director

5.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com