Technical White Paper: April 2022

VMware Sovereign Cloud Technical Guidance

Encryption – BYOK with Fortanix

Table of contents

Table of figures

Introduction

The VMware Sovereign Cloud Technical Guidance is a technical reference point for VMware Sovereign Cloud Providers which will help in understanding how to configure encryption for your Sovereign Cloud using Fortanix DSM. This document will also cover how your customers can "Bring Your Own Keys" (BYOK) into a dedicated private sovereign cloud.

VMware's Sovereign Cloud Initiative recognizes VMware Cloud Verified partners that meet VMware's definition of a Sovereign Cloud. Partners who implement the VMware Sovereign Cloud guidance will be better able to protect the sovereignty of their customers workloads and data.

While the definition of what a Sovereign Cloud is, continues to evolve and is truly based on the Sovereign Nation or entity where the workloads/data/people will reside, technical guidance is needed to make our VMware Sovereign Cloud Providers successful in serving their customers. This guidance will be flexible enough to allow different configurations and implementations to comply with the entity that is providing the requirements of their Sovereign Cloud.

VMware Sovereign Cloud Providers benefit from clear guidelines around data sovereignty, data residency, data access, jurisdiction, control, and much more to provide customers with the assurance that their most sensitive data is managed securely. With sovereign cloud capabilities, customers benefit from the scale of a multi-tenant, hybrid cloud environment while maintaining security, access, and control like a traditional on-premises, legacy computing environment.

Legal Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided "AS IS". VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.

Audience

This document is intended for VMware Cloud Provider architects and technical leads responsible for planning and performing the implementation and maintenance of a VMware Sovereign Cloud environment.

Scope

This document addresses the following aspects:

Why is Encryption needed in a Sovereign Cloud?

Providers will need to use encryption to protect the data and communications that take place in a VMware Sovereign Cloud. To accomplish this, you will use both vSphere Virtual Machine Encryption, Storage Encryption, and Network Encryption to secure all workloads, data, and communications.

VMware Sovereign Dedicated Private Cloud Use Cases

There are 3 main uses cases that are provided to show how a VMware Sovereign Cloud Provider can implement the Fortanix solution which would provide the Cloud Provider's customer to BYOK and enable data privacy.

How Fortanix can enable data privacy in a VMware Sovereign Cloud

Fortanix DSM with built-in multi-tenancy, when integrated together with VMware Sovereign cloud, enables service provider partners the ability to offer Bring Your Own Key (BYOK) for VM encryption and vSAN Encryption, FIPS 140-2 Level 3 HSM protection, key management, tokenization, and secrets management through a single platform, hosted within the VMware Sovereign Cloud boundary.

Why is Encryption Necessary?

Securing a customer's data and then making sure those security measures remain in compliance with the requirements or criteria of what makes a VMware Sovereign Cloud, is of vital importance to each Cloud Provider. This protection of data includes preventing unauthorized access, modification, and duplication as well as to prevent both intentional and unintentional loss or corruption. One of those areas that will need to be considered is encryption. Providers will need to use encryption to protect the data and communications that take place in a VMware Sovereign Cloud. To accomplish this, you will use both vSphere Virtual Machine Encryption, Storage Encryption, and Network Encryption to secure all workloads, data, and communications.

Data at-rest Encryption

Encrypting data at-rest can be achieved at the virtual machine and storage levels using virtual machine and vSAN encryption.

vSphere Virtual Machine Encryption

Encryption is applied to the virtual disk files attached to the virtual machine as well as the memory swap file and snapshots.

vSphere Encryption relies on a compliant KMS server to generate and manage keys, vCenter requests the private key for a virtual machine when it powers on the virtual machine and so the KMS becomes a critical dependency. Referencing the Virtual Machine Encryption documents will help direct you in implementing encryption for your sensitive workloads. You will need to consider which Key Provider is needed. Understanding the different components of Virtual Machine Encryption and how to implement it will also be covered.

vSAN Encryption

vSAN can perform data at rest encryption in your datastores. Encrypting your vSAN datastores in your Sovereign Cloud is a requirement. Data-at-rest encryption protects data on storage devices in case a device is removed from the cluster. The document called vSAN Data-At-Rest Encryption will help you to learn how Data-At-Rest Encryption works, design considerations, and how to manage it after the initial configuration.

Data in-flight Encryption

Data in motion, also referred to as data in transit or data in flight, is digital information that is in the process of being transported between locations either within or between computer systems. All data that goes over your internal network or the internet is potentially vulnerable. Encrypting data in-flight means that you encrypt data when it's being transmitted over a network.

Data in motion includes the following scenarios: data moving from an Internet-capable endpoint device to a web-facing service in the cloud; data moving between virtual machines within and between cloud services and data that is traversing trusted private networks and an untrusted network such as the Internet. Once the data arrives at its destination, it becomes data-at-rest.

VMware Sovereign Dedicated Private Cloud Use Cases

The following three use cases show a Private Dedicated Sovereign Cloud provisioned by a Cloud Provider and how a Fortanix HSM Cluster can be deployed and used in enabling data security.

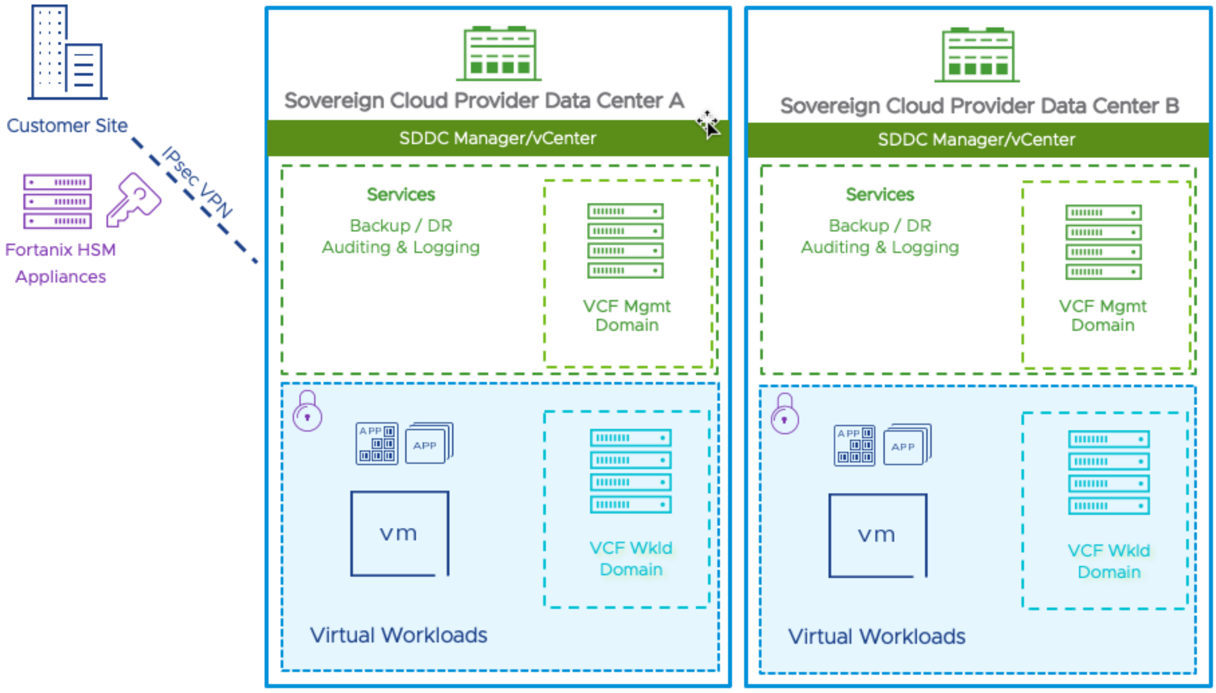


Figure 1: Use Case #1 – Customer provided

In the above figure, you can see how it shows that the Fortanix implementation is pre-existing at the Customer's location. It will connect over IPsec VPN to securely provide cryptography operations into the provisioned Sovereign Cloud. The keys stay with the appliance and are owned by the Customer. This is just one way that we illustrate the ability for a customer to "BYOK" (Bring Your Own Key) to the Sovereign Cloud.

In the below figure you can see that the Sovereign Cloud Provider has provisioned a dedicated, highly available Fortanix Cluster for sole use by that one customer. This deployment option can allow for the Cloud Provider to manage the infrastructure of the appliances and yet still provides sole ownership of all cryptography by the customer.

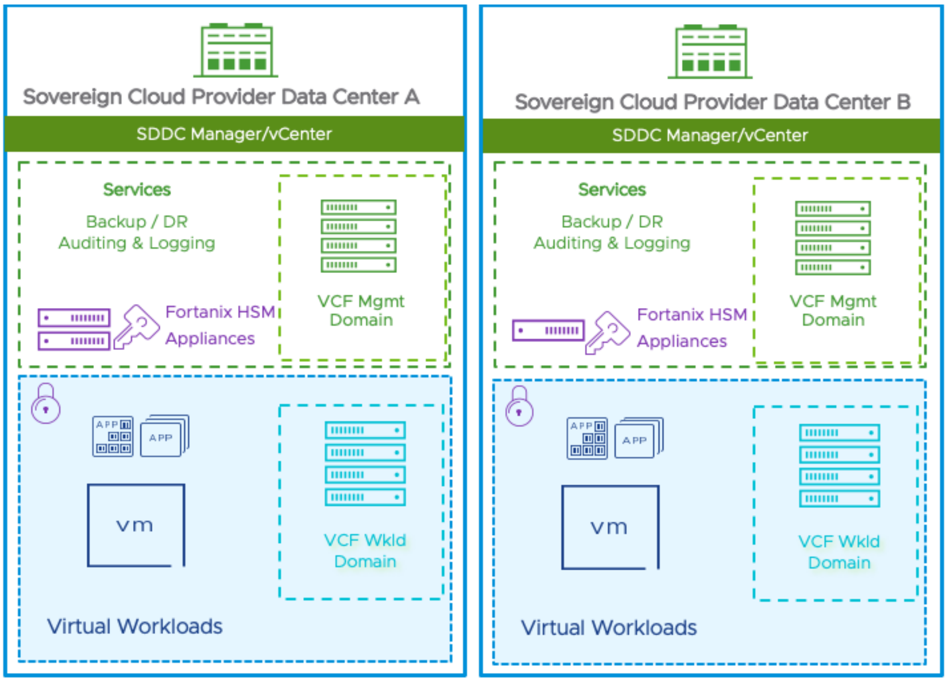


Figure 2: Use Case #2 – Cloud Provider provisions dedicated per customer.

Figure 3 below shows a Highly Available Fortanix Cluster deployed in a way that allows for the provider to centrally manage multiple customers while still maintaining complete separateness from the cryptography operations of each customer. All customers in this model are also completely separate. Central management by the provider offers flexibility, a lower cost, and scalability.

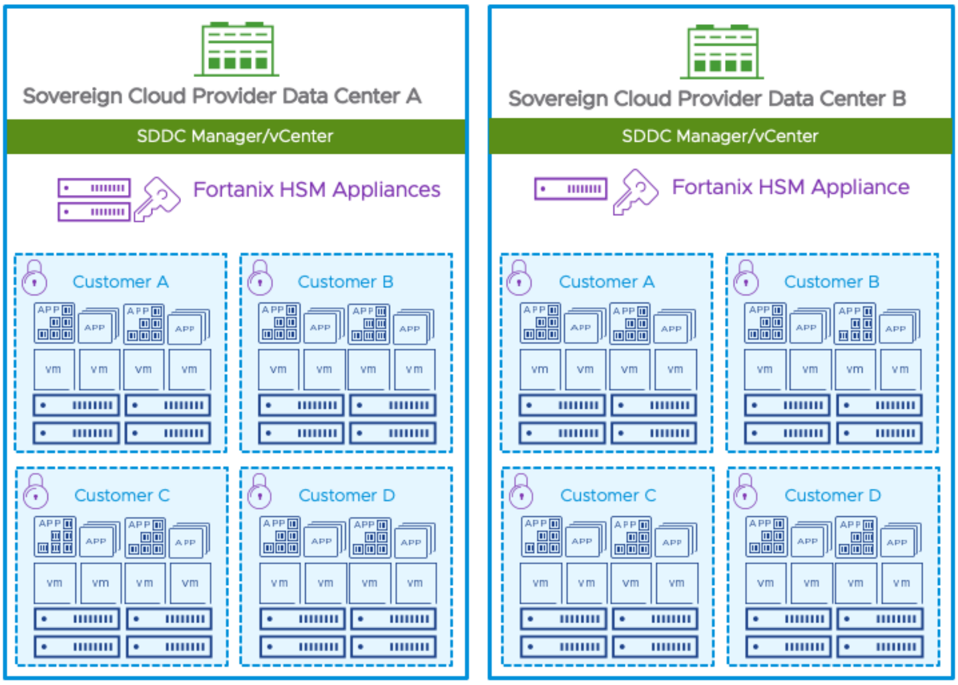


Figure 3: Use Case #3 – Centrally deployed by the Cloud Provider for multiple comers.

Using Fortanix Data Security Manager to Enable Data Privacy

Overview

The joint VMware and Fortanix Data Security solution offer scalable data protection and compliance for VMware Sovereign cloud environments. Fortanix DSM, is a unified HSM and Key Management solution that easily integrates via KMIP for VMware vSAN and vSphere VM encryption, enabling sovereign cloud customer to bring and manager their own keys. Fortanix DSM makes it possible for VMware Sovereign cloud providers to deliver Data Protection and compliance to the end customers (tenants). Secured with Intel® SGX, Fortanix DSM delivers HSM security with software defined simplicity, and a cloud scale architecture.

Fortanix DSM with built-in multi-tenancy, when integrated together with VMware Sovereign cloud, enables service provider partners the ability to offer Bring Your Own Key (BYOK) for VM encryption and vSAN Encryption, FIPS 140-2 Level 3 HSM protection, key management, tokenization, and secrets management through a single platform, hosted within the VMware Sovereign Cloud boundary.

How to Integrate Fortanix DSM with VMware vCenter

The following instructions describe how to set up Fortanix Data Security Manager (DSM) as an External KMS server in vCenter from the vSphere Web Client in a VMware Sovereign Cloud. The customer will have complete access and control of the keys to secure their VMs. There are two proven ways of establishing trust/authentication to vSphere from Fortanix DSM:

- Using API Keys
- Using Certificates

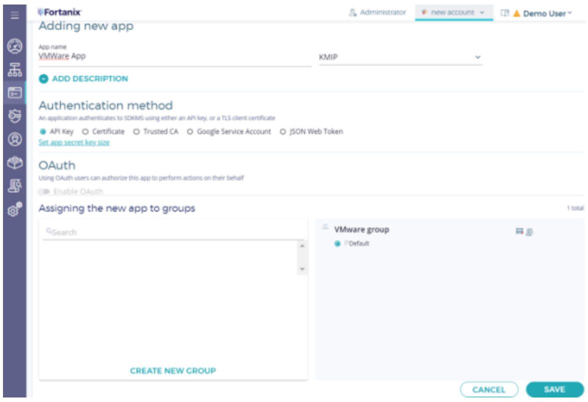
Once set up, Fortanix DSM can be used for both vSphere VM encryption and VSAN encryption.

Prerequisites

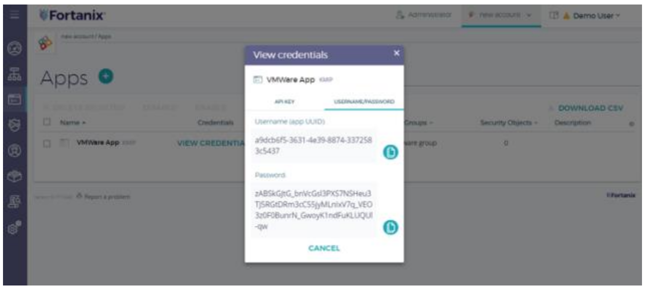
- Fortanix Data Security Manager account
- Access to vCenter (vSphere Client) for VMware Sovereign Cloud

Integration Steps for Fortanix DSM to VMware

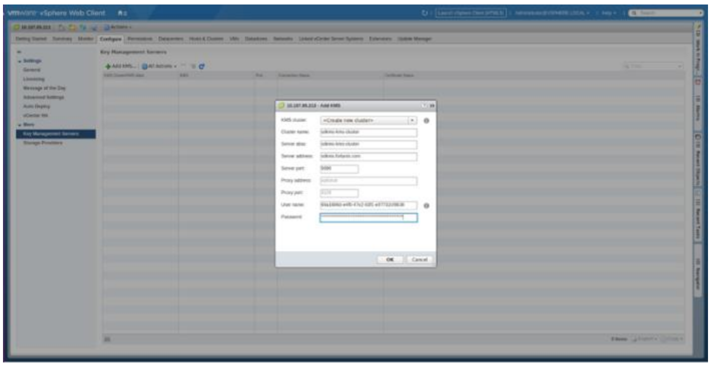
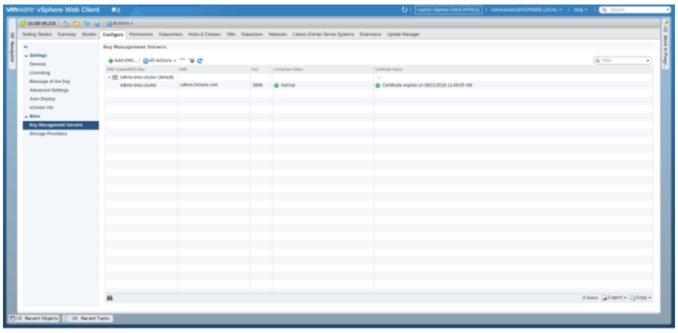
Create a Fortanix Data Security Manager App for VMware

Instruction Steps	Screenshots
1. Inside the Fortanix DSM account, go to the Applications tab and create a new Fortanix DSM app. a. For the “Interface” field **choose** “KMIP” b. For the “Authentication method” option **choose** “API key” c. **Click** “Save” d. After reviewing **click** “Finish”.	 Fortanix Administrator new account Demo User Adding new app App name VMWare App KMIP ADD DESCRIPTION Authentication method An application authenticates to SDKMS using either an API key, or a TLS client certificate ● API Key ○ Certificate ○ Trusted CA ○ Google Service Account ○ JSON Web Token Set app secret key size OAuth Using OAuth users can authorize this app to perform actions on their behalf Enable OAuth Assigning the new app to groups 1 total Search VMware group ● Default CREATE NEW GROUP CANCEL SAVE

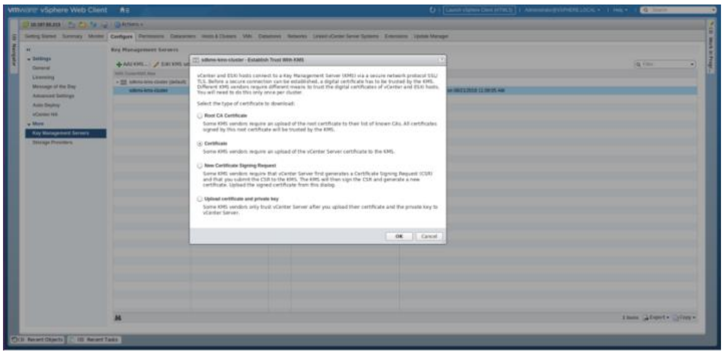
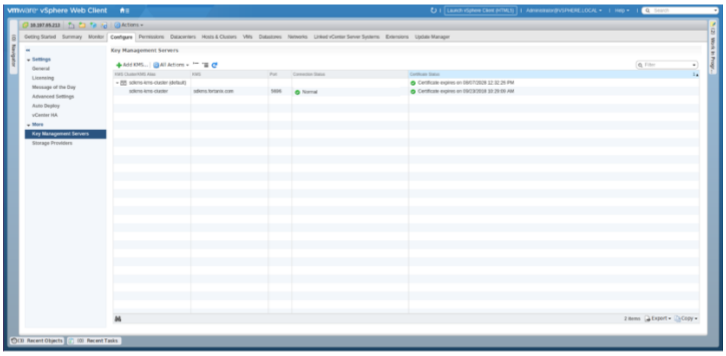
Obtain App Credentials

Instruction Steps	Screenshots
1. Go back to the "Applications" page and **click** "VIEW CREDENTIALS" of the app you just created. 2. Then, **click** the "USERNAME/PASSWORD" tab	 View credentials VMWare App KMIP API KEY USERNAME/PASSWORD Username (app UUID) a9dcb6f5-3631-4e39-8874-3372583c5437 Password zABSkGjtG_bnVcGsl3PXS7NSHeu3TJ5RGtDRm3cCS5jyMLnixV7q_VEO3z0F0BunrN_GwoyK1ndFuKLUQUl-qw CANCEL Fortanix Administrator Demo User Apps DOWNLOAD CSV Name Credentials Groups Security Objects Description VMWare App VIEW CREDENTIA Report a problem

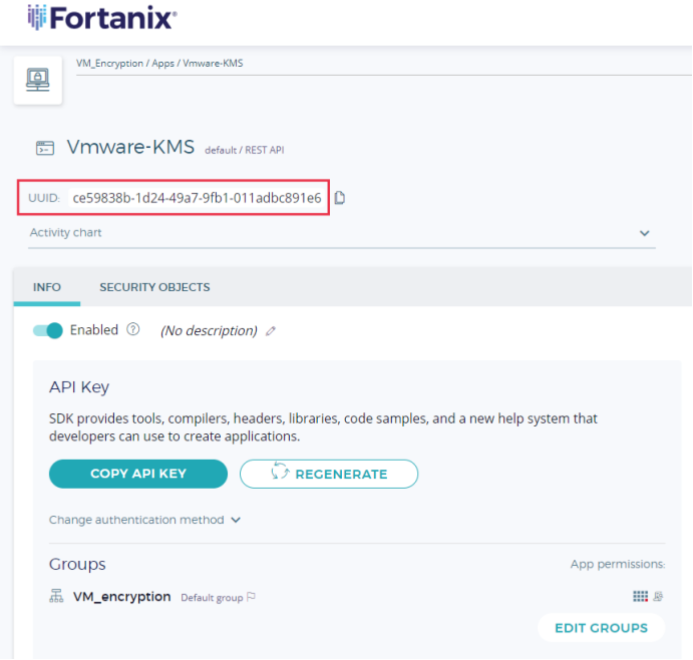
Method 1: Configuring KMS in vCenter Using Password

Instruction Steps	Screenshots
1. **Go** to the "Key Management Servers" page in the vSphere Web Client a. **Click** "+ Add KMS". b. **Fill** in the required information on the KMS server. i. Server address: <DSM endpoint> (Eg: amer.smartkey.io). ii. In the **"**Username" and **"**Password" fields **paste the values** from the previous step.	 Add KMS KMS cluster: <Create new cluster> Cluster name: sdkms-kms-cluster Server alias: sdkms-kms-cluster Server address: sdkms.fortanix.com Server port: 5696 Proxy address: Proxy port: User name: Password: vSphere Web Client Key Management Servers Add KMS... OK Cancel
2. After **clicking** "OK" the "Connection Status" column should show "Normal", and the "Certificate Status" column should show a green check with the expiration date of the certificate.	 Key Management Servers KMS Cluster/KMS Alias: sdkms-kms-cluster (default) sdkms-kms-cluster | sdkms.fortanix.com | 5696 | Normal | Certificate expires on 08/21/2018 11:08:05 AM vSphere Web Client Launch vSphere Client (HTML5) Administrator@VSPHERE.LOCAL Help Actions Monitor Configure Permissions Datacenters Hosts & Clusters VMs Datastores Networks Linked vCenter Server Systems Extensions Update Manager Add KMS... All Actions Filter

Establishing Trust with Fortanix Data Security Manager

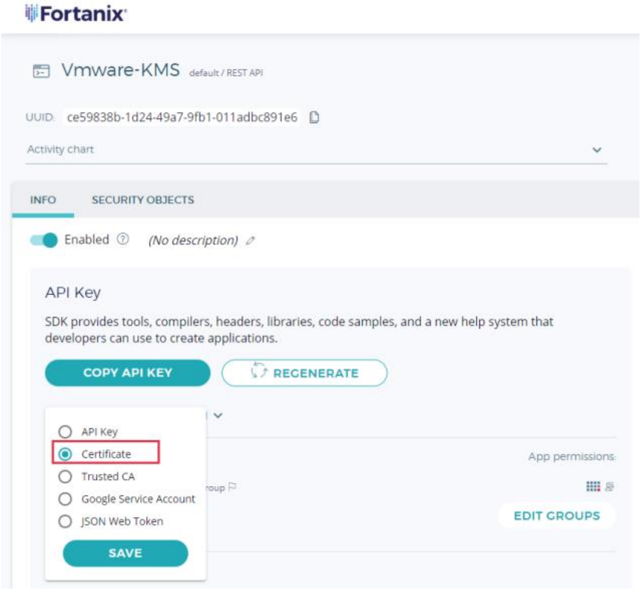
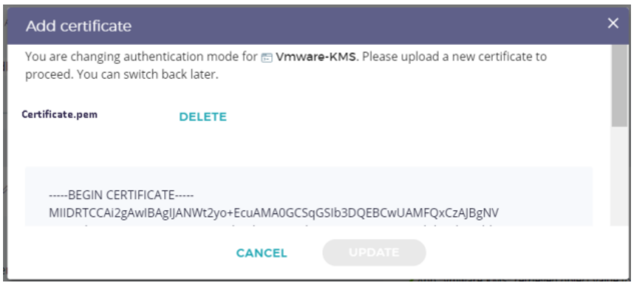
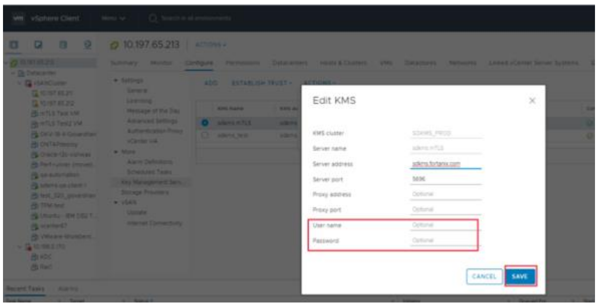
Installation Steps	Screenshots
1. After **adding** the Fortanix DSM KMS server in the vSphere Web Client it is necessary to establish trust with the server. 2. In the "Key Management Servers" page **click** "Establish trust with KMS" and **select** "Certificate". 3. If desired, **save** the Certificate and then **click** "OK".	 sdemo-kms-cluster - Establish Trust With KMS vCenter and ESXi hosts connect to a Key Management Server (KMS) via a secure network protocol SSL/TLS. Before a secure connection can be established, a digital certificate has to be trusted by the KMS. Different KMS vendors require different means to trust the digital certificates of vCenter and ESXi hosts. You will need to do this only once per cluster. Select the type of certificate to download: ○ Root CA Certificate Some KMS vendors require an upload of the root certificate to their list of known CAs. All certificates signed by this root certificate will be trusted by the KMS. ● Certificate Some KMS vendors require an upload of the vCenter Server certificate to the KMS. ○ New Certificate Signing Request Some KMS vendors require that vCenter Server first generates a Certificate Signing Request (CSR) and that you submit the CSR to the KMS. The KMS will then sign the CSR and generate a new certificate. Upload the signed certificate from this dialog. ○ Upload certificate and private key Some KMS vendors only trust vCenter Server after you upload their certificate and the private key to vCenter Server. OK Cancel
4. A second green check should appear in the "Certificate Status" column of the KMS cluster. **NOTE:** Fortanix DSM is ready for use with VSAN encryption and vSphere VM encryption.	

Method 2: Configuring KMS in vCenter using Client Certificate

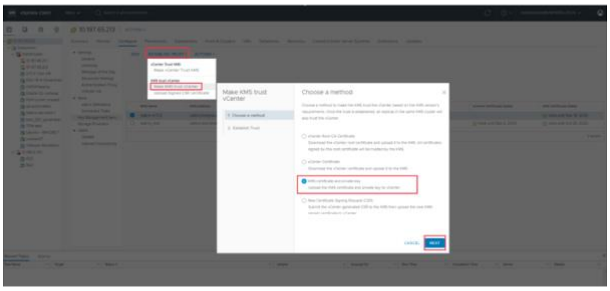
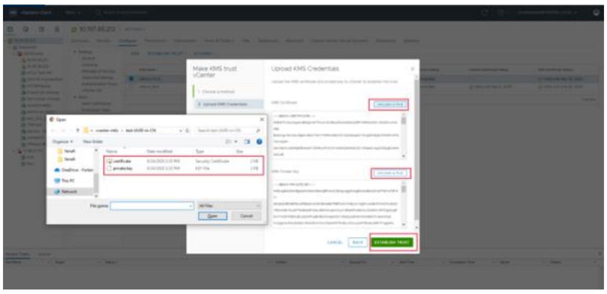
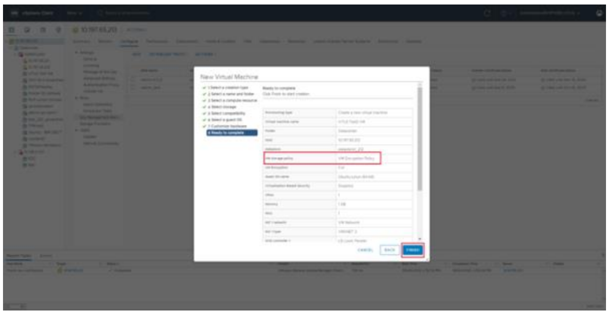
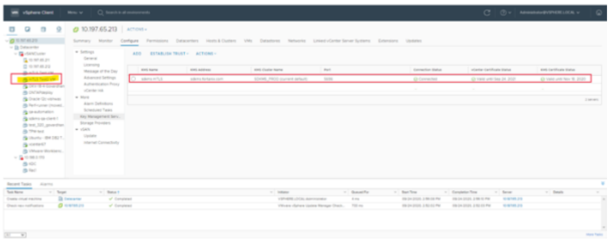
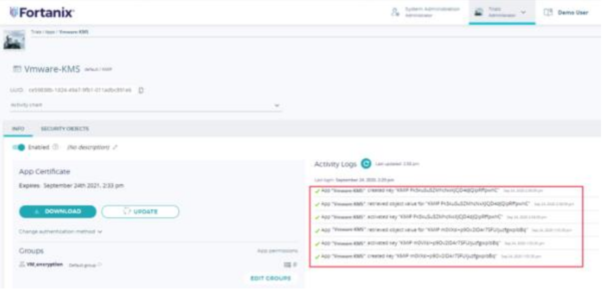
Installation Steps	Screenshots
1. To generate a client certificate, **use OpenSSL**, and create a new key+cert with CN=FORTANIX_APP_UUID. 2. **Note** the App UUID.	 VM_Encryption / Apps / Vmware-KMS Vmware-KMS default / REST API UUID: ce59838b-1d24-49a7-9fb1-011adbc891e6 Activity chart INFO SECURITY OBJECTS Enabled (No description) API Key SDK provides tools, compilers, headers, libraries, code samples, and a new help system that developers can use to create applications. COPY API KEY REGENERATE Change authentication method Groups App permissions: VM_encryption Default group EDIT GROUPS

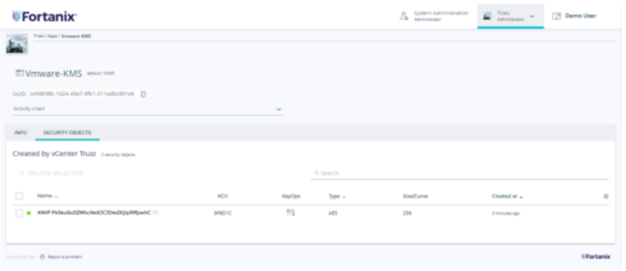
Installation Steps	Screenshots

3. Using OpenSSL **create** the certificate	`$ export FORTANIX_APP_UUID=ce59838b-1d24-49a7-9fb1-011adbc891e6`
	
	`$ openssl req -newkey rsa:2048 -nodes -keyout private.key -x509 \`
	`    -days 365 -out certificate.crt -subj \`
	`    "/C=US/ST=California/L=Mountain View/O=Fortanix, Inc./OU=SE/CN=$FORTANIX_APP_UUID"`

4. **Import** the vCenter Certificate into the Fortanix DSM App.	 Fortanix Vmware-KMS default / REST API UUID: ce59838b-1d24-49a7-9fb1-011adbc891e6 Activity chart INFO SECURITY OBJECTS Enabled (No description) API Key SDK provides tools, compilers, headers, libraries, code samples, and a new help system that developers can use to create applications. COPY API KEY REGENERATE ○ API Key ● Certificate ○ Trusted CA ○ Google Service Account ○ JSON Web Token SAVE App permissions EDIT GROUPS
5. **Upload** the certificate for authenticating the app.	 Add certificate You are changing authentication mode for Vmware-KMS. Please upload a new certificate to proceed. You can switch back later. Certificate.pem DELETE -----BEGIN CERTIFICATE----- MIIDRTCCAi2gAwIBAgIJANWt2yo+EcuAMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV CANCEL UPDATE
6. **Create** a new Fortanix DSM Cluster 7. **Make** it DEFAULT 8. **Make** sure the fields "Username" and "Password" are **empty**.	 vSphere Client 10.197.65.213 Edit KMS KMS cluster: SDKMS_PROD Server name: sdkms-mTLS Server address: sdkms.fortanix.com Server port: 5696 Proxy address: Optional Proxy port: Optional User name: Optional Password: Optional CANCEL SAVE

Establishing Trust with Fortanix Data Security Manager

Installation Steps	Screenshots
1. To **import** the "key+cert" to vSphere **click** "Establish Trust **>** Make KMS trust vCenter **>** KMS Certificate and Private Key".	
2. **Import** the certificate and private key 3. **Click** "Establish Trust".	
4. **Create** a VM and **select** the default **"**VM Encryption Policy" 5. **Enable** "Home/Disk" encryption. 6. **Click** "Finish"	
7. The VM is successfully created.	
8. **Log into** Fortanix DSM to see the logs of the connection that captures all the crypto operations performed by the application and the key created as well.	 Vmware-KMS App Certificate Expires: September 24th 2021, 2:33 pm Activity Logs Last login: September 24, 2020, 2:29 pm ✓ App "Vmware-KMS" created key "KMIP [illegible]" ✓ App "Vmware-KMS" retrieved object value for "KMIP [illegible]" ✓ App "Vmware-KMS" activated key "KMIP [illegible]" ✓ App "Vmware-KMS" retrieved object value for "KMIP [illegible]" ✓ App "Vmware-KMS" activated key "KMIP [illegible]" ✓ App "Vmware-KMS" created key "KMIP [illegible]" Groups VM_encryption Default group

Installation Steps	Screenshots
9. Click on “Security Objects” to see the newly created Key.	 Vmware-KMS UUID: ce59838b-1d24-49a7-9fb1-011adbc891e6 Created by vCenter Trust Name: KMIP PkSkuSu5ZMhcNxX3C3D4d3QIpRffpwhC KCV: 5F9D1C Type: AES Size/Curve: 256 Created at: 3 minutes ago

Summary

Having integrated the Fortanix DSM application into your VMware Sovereign Cloud allows for secure cryptography operations to take place enabling data security and compliance for your Customer’s Sovereign requirements.

To find out more about how to become a VMware Sovereign Cloud Provider please go to the VMware Sovereign Cloud Solutions website.

You can also visit the Fortanix VCPP website for more information on the Fortanix DSM application and how it works to secure your environment.

Revision History		
Date	Changes	Modified By
April 2022	Initial Document Creation	Cory Allen