HashiCorp Vault

Securing VMware Data

HashiCorp

Contents

Introduction 3

Key Management Interoperability Protocol (KMIP) 3

- Challenge 3
- Solution 4

Securing VMware Data with HashiCorp Vault 5

- VMware Encryption 5
- HashiCorp Vault as a KMS for VMware 7

Summary 8

- Additional Resources 8

Advanced Data Protection with Vault 9

- Additional Resources 10

Introduction

Vault allows you to secure, store and tightly control access to tokens, passwords, certificates, encryption keys, and other sensitive data using a UI, CLI, or HTTP API. Vault recently completed VMware product compatibility validation against vSphere 6.5 and 6.7 to satisfy our customers requirements for certified solutions when using Vault and VMware.

You can increase productivity, control costs by reducing systems, licenses and overhead by centrally managing all secrets operations. Vault can also assist with reducing the risk of breach by eliminating static, hard-coded credentials by centralizing secrets.

- **Identity Brokering** for authentication and access to different clouds, policy enforcement, and easy automation.
- **Single Workflow** that integrates with existing infrastructure, reduces costs, and provides a unified audit trail.
- **Open & Extensible** strong open source community, large partner ecosystem, and full featured multi-cloud secrets engines.

Key Management Interoperability Protocol (KMIP)

Challenge

Organizations store sensitive, personal and valuable data, which must be protected. Leakage of such data can lead to financial loss, reputational damage, legal ramifications and more. There are often requirements to comply with data protection standards and regulations like the PCI DSS, GDPR, HIPAA, etc.

The OASIS Key Management Interoperability Protocol (KMIP) standard is a widely adopted protocol for handling cryptographic workloads and secrets management for enterprise infrastructure such as databases, network storage, and virtual/physical servers.

When an organization has services and applications that need to perform cryptographic operations (e.g. transparent database encryption, full disk encryption, etc), it often delegates the key management task to an external provider via KMIP protocol. As a result, your organization may have existing services or applications that implement KMIP or use wrapper clients with libraries/drivers that implement KMIP. This makes it difficult for an organization to adopt the Vault API in place of KMIP.

Solution

Vault Enterprise v1.2 introduced the KMIP secrets engine which allows Vault to act as a KMIP server for clients that retrieve cryptographic keys for encrypting data via KMIP protocol.

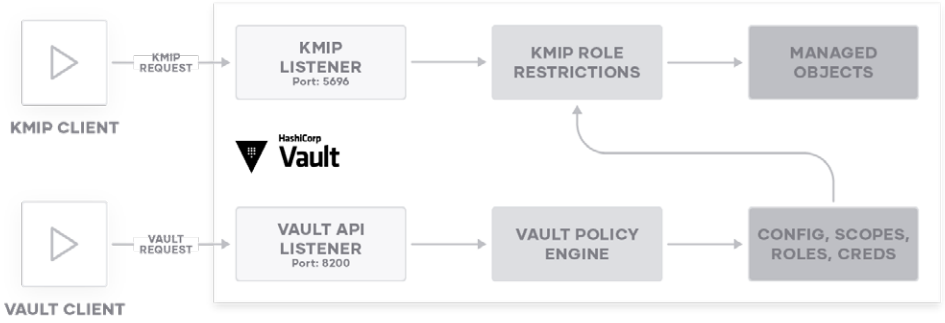

Figure 1: High Level Client Server Architecture Overview

Vault's KMIP secrets engine manages its own listener to service KMIP requests which operate on KMIP managed objects. Vault policies do not come into play during these KMIP requests. The KMIP secrets engine determines the set of KMIP operations the clients are allowed to perform based on the roles that are applied to a TLS client certificate.

This enables existing systems to continue using the KMIP APIs instead of Vault APIs.

Securing VMware Data with HashiCorp Vault

VMware Encryption

VMware Encryption was introduced with version 6.5 of VMware vSphere and allows integration with different types of Key Management Servers (KMS) for managing encryption keys.

The process flow includes the KMS, the vCenter Server, and the ESXi host.

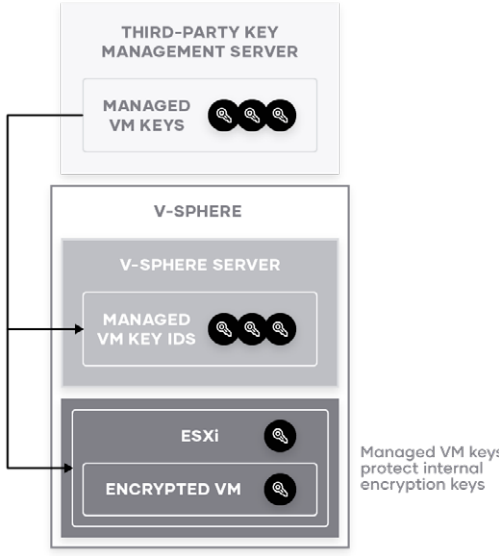

Figure 2: vSphere Virtual Encryption Architecture

During the encryption process, different vSphere components interact as follows.

1. When the user performs an encryption task, for example, creating an encrypted virtual machine, vCenter Server requests a new key from the default KMS. This key is used as the Key Encryption Key (KEK).

2. vCenter Server stores the key ID and passes the key to the ESXi host. If the ESXi host is part of a cluster, vCenter Server sends the KEK to each host in the cluster. The key itself is not stored on the vCenter Server system. Only the key ID is known.

3. The ESXi host generates internal Data Encryption Keys (DEKs) for the virtual machine and its disks. It keeps the internal keys in memory only, and uses the KEKs to encrypt internal keys. Unencrypted internal keys are never stored on disk. Only encrypted data is stored. Because the KEKs come from the KMS, the host continues to use the same KEKs.

4. The ESXi host encrypts the virtual machine with the encrypted internal key. Any hosts that have the KEK and that can access the encrypted key file can perform operations on the encrypted virtual machine or disk.

vSphere Virtual Machine Encryption works with any supported storage type (NFS, iSCSI, Fiber Channel, and so on), including VMware vSAN.

What is encrypted	Details
Virtual machine files	Most virtual machine files, in particular, guest data that are not stored in the VMDK file, are encrypted. This set of files includes but is not limited to the NVRAM, VSWP, and VMSN files. The key that vCenter Server retrieves from the KMS unlocks an encrypted bundle in the VMX file that contains internal keys and other secrets. When you use the vSphere Client to create an encrypted virtual machine, you can encrypt and decrypt virtual disks separate from virtual machine files. All virtual disks are encrypted by default. For other encryption tasks, such as encrypting an existing virtual machine, you can encrypt and decrypt virtual disks separate from virtual machine files.
Virtual disk files	Data in an encrypted virtual disk (VMDK) file is never written in cleartext to storage or physical disk, and is never transmitted over the network in cleartext. The VMDK descriptor file is mostly cleartext, but contains a key ID for the KEK and the internal key (DEK) in the encrypted bundle. You can use the vSphere API to perform either a shallow recrypt operation with a new KEK or deep recrypt operation with a new internal key.
Core dumps	Core dumps on an ESXi host that has encryption mode enabled are always encrypted.

HashiCorp Vault as a KMS for VMware

Using KMIP, Vault Enterprise and VMware can be seamlessly integrated to secure data within a VMware environment. As mentioned earlier, Vault recently completed VMware product compatibility validation against vSphere 6.5 and 6.7 to satisfy our customers requirements for certified solutions when using Vault and VMware. See the VMware Compatibility Guide for the latest validations of Vault with vSphere.

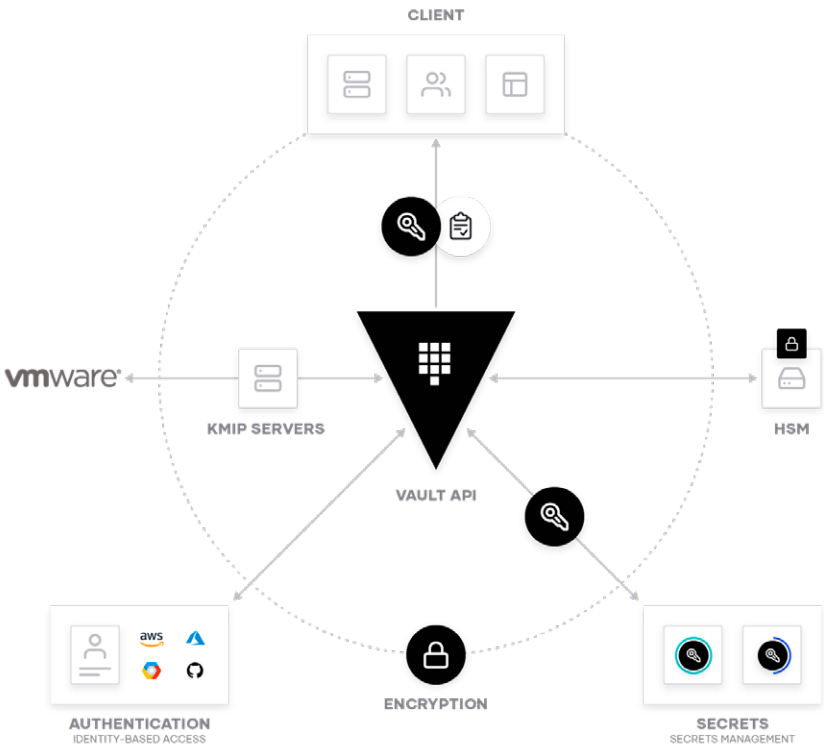

Figure 3: How VMware works with HashiCorp Vault

- **Workflows, not Technologies:** Request secrets for any system through one consistent, audited, and secured workflow.
- **Secure Multi-tenancy:** Isolate different tenant environments for security and compliance. Different teams and departments can work independently of each other and have access to only their own keys and systems.
- **HSM Support:** Vault supports integration with any HSM that supports PKCS #11. Most hardware-based KMIP Servers only support specific HSMs.

- **Flexibility:** Most key managers are hardware devices and difficult to procure, manage and maintain. Vault gives you more flexibility as it is distributed as a binary and can be deployed across multiple platforms.
- **Cost and Efficiency:** One deployment of Vault can create multiple independent KMIP servers. Save time and cost as you don't need to buy and manage hardware devices for each department.
- **Management:** Vault is easy to manage and use, as it offers Web UI, CLI, and HTTP API interfaces.
- **High Availability:** Built-in High Availability using Consul as the storage back-end. Using Consul also provides automated registration, tagging, and health checks for Vault services within Consul.
- **Multi-datacenter replication:** Built-in multi-datacenter replication for horizontal scalability and disaster recovery use-cases.
- **Audit Logging:** With Vault's audit log, monitoring secret access across multiple environments and clouds is easy and automated.
- **Future-proof:** Vault comes power packed with multiple integrations like AWS, Azure, GCP, Kubernetes, Databases, and more to provide a central service for secret and certificate management, cryptographic and advanced data protection needs.

Summary

HashiCorp Vault Enterprise with KMIP Secret Engine is the perfect solution for protecting your Data in virtual environments. The ease of deployment and configuration of Vault added to other enterprise features like "Performance Replication", "Disaster Recovery" and "HSM Integration" provide to our customers the maximum level of Service and Security without compromise.

Additional Resources

- Securing VMware Data: A HashiCorp Vault KMIP Story
- KMIP Secrets Engine
- Learn - KMIP Secrets Engine

Advanced Data Protection with Vault

Advanced Data Protection (ADP) is a module for Vault Enterprise focused on Enterprise-grade Data Protection and Encryption.

Advanced Data Protection includes:

- **KMIP Integration:** The KMIP secrets engine allows Vault to act as a Key Management Interoperability Protocol (KMIP) server provider and handle the lifecycle of its KMIP managed objects. KMIP is a standardized protocol that allows services and applications to perform cryptographic operations without having to manage cryptographic material, otherwise known as managed objects, by delegating its storage and lifecycle to a key management server.

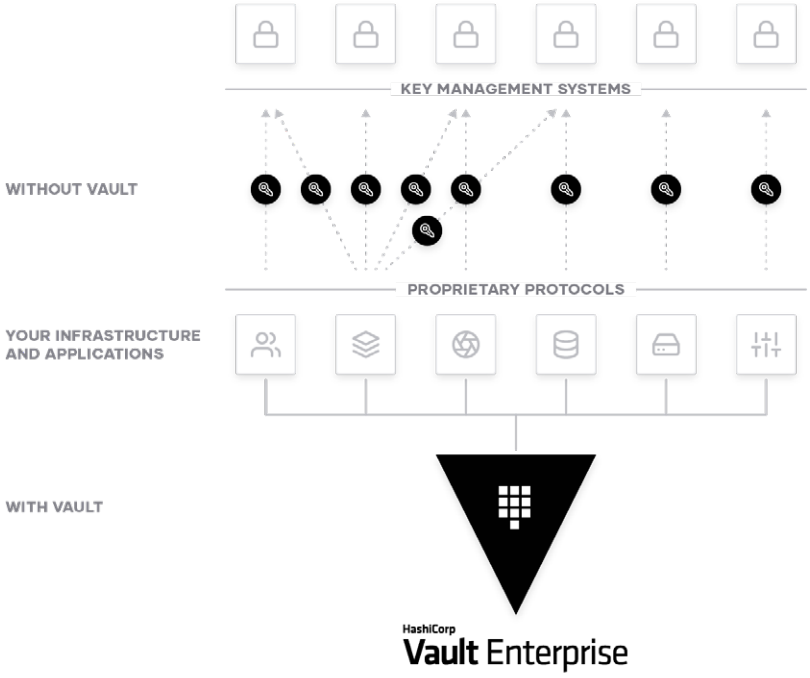

Figure 4: Advanced Data Protection with Vault

- **Transform:** The Transform secrets engine handles secure data transformation and tokenization against provided input value. Transformation methods may encompass NIST vetted cryptographic standards such as format-preserving encryption (FPE) via FF3-1, but can also be pseudonymous transformations of the data through other means, such as masking.

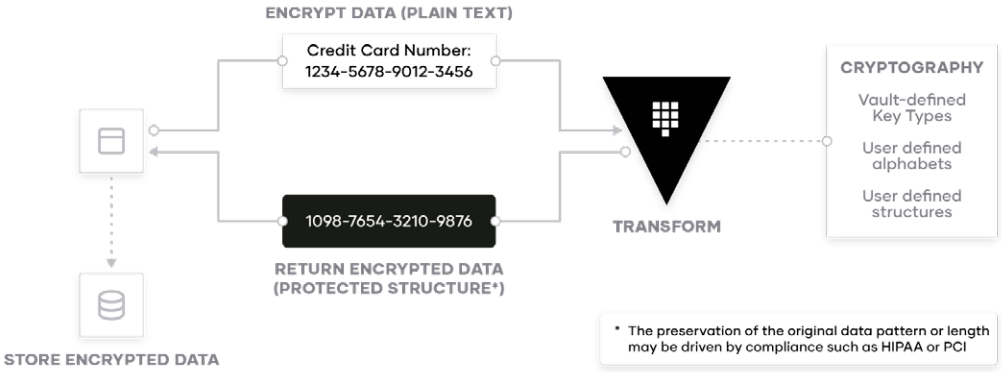

Figure 5: Transform Secret Engine Overview

Additional Resources

- Introducing the KMIP Server Secret Engine
- Vault Transform: Protecting Secrets in External Systems
- Learn: Using KMIP to Secure MongoDB and MySQL
- Learn: Secure Data Transformation Using Format Preserving Encryption


HashiCorp