HashiCorp
Vault

Securing NetApp Data

HashiCorp

Contents

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 NetApp product interoperability validation against ONTAP 9.7, 9.6, and 9.3 to satisfy our customers requirements for certified solutions when using Vault and NetApp.

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.

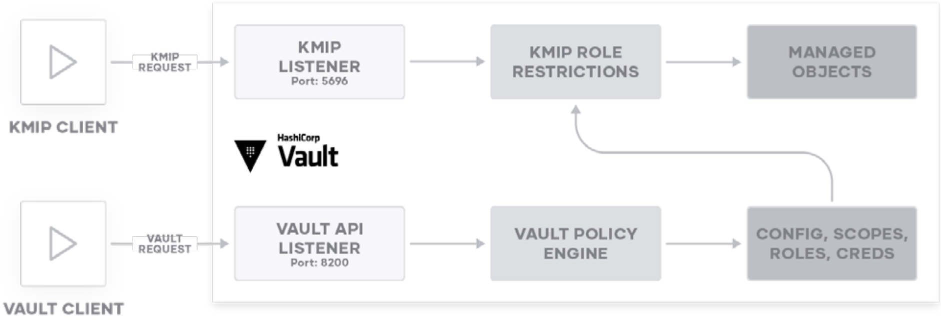

Figure 1: High Level Client Server Architecture Overview

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 NetApp Data with HashiCorp Vault

NetApp Encryption

NetApp offers state of the art secure data management, file-shares, backup, recovery, replication and disaster recovery solutions to a large number of enterprises all around the globe. The NetApp ONTAP system, which is one of the most popular storage operating systems in the world, offers FIPS compliant encryption technology that also supports the OASIS KMIP protocol.

NetApp Storage Encryption (NSE) is NetApp's implementation of Full Disk Encryption while NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) are software-based, data-at-rest encryption solutions, available in NetApp ONTAP based systems. Although NetApp does offer an onboard key manager, most enterprises must use an external key manager for compliance reasons as the keys must be stored outside of the storage system.

Vault as an External Key Manager for NetApp

HashiCorp Vault is the de-facto standard for managing secrets in multi-cloud and hybrid enterprise environments. It is a simple, modern, scalable and highly automatable solution for management of all kinds of sensitive and secret data including passwords, keys, certificates, and encryption keys. One of the latest enterprise capabilities of Vault is a KMIP Secrets Engine which is the best solution for external key manager requirements for enterprise storage systems like NetApp ONTAP. Moreover, Vault can be integrated with an HSM for master key wrapping and auto unsealing.

As mentioned earlier, Vault recently completed NetApp product interoperability validation against ONTAP 9.7, 9.6, and 9.3 to satisfy our customers requirements for certified solutions when using Vault and NetApp. See NetApp's Interoperability Matrix Tool (IMT) for the latest validations of Vault with NetApp.

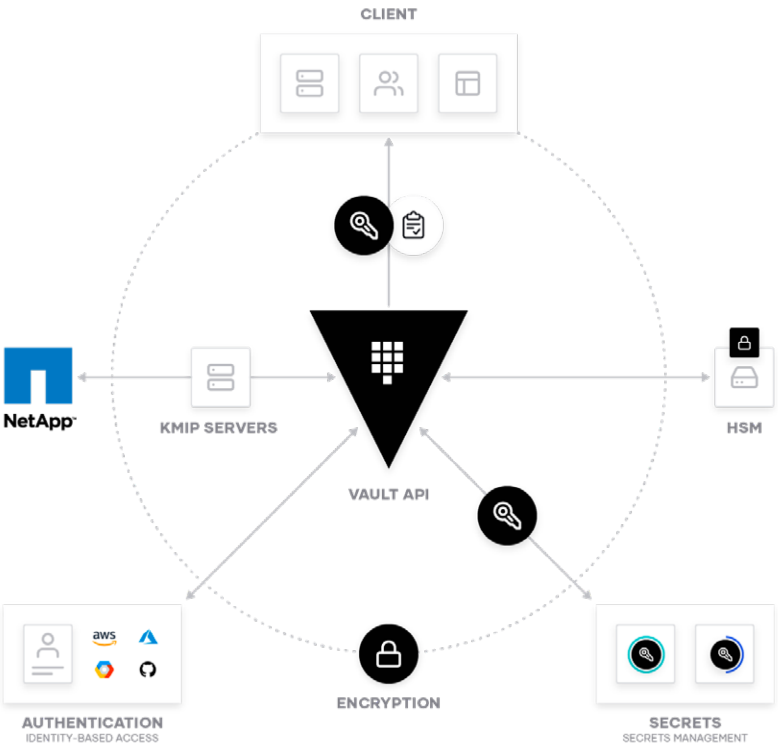

Figure 2: How NetApp works with HashiCorp Vault

Note: the KMIP and HSM features are Vault Enterprise features.

- **Certified:** Vault is validated, supported and certified for use by NetApp. Vault complies with the OASIS KMIP standard.
- **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 on 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.

- **Disaster Recovery:** 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. One Central service for secret and certificate management, cryptographic and advanced data protection needs.

Summary

When using HashiCorp Vault Enterprise as an external key manager for NetApp Encryption, organizations can save money, time, and resources. Vault is fully software-based and scalable and offers multiple integrations including for public clouds. It offers great automation capabilities which reduce risks.

Additional Resources

- Securing NetApp 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.

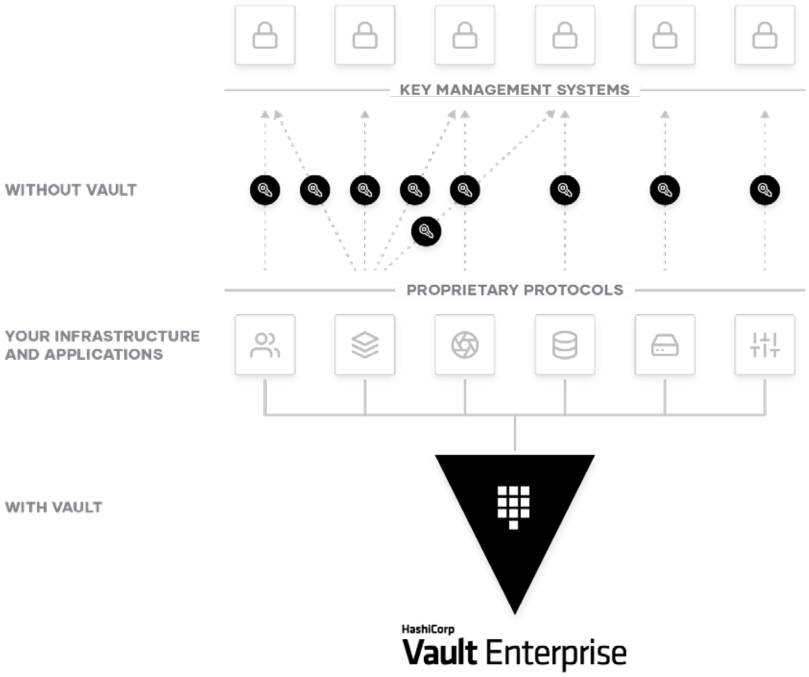

Figure 3: Advanced Data Protection with Vault

- **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.

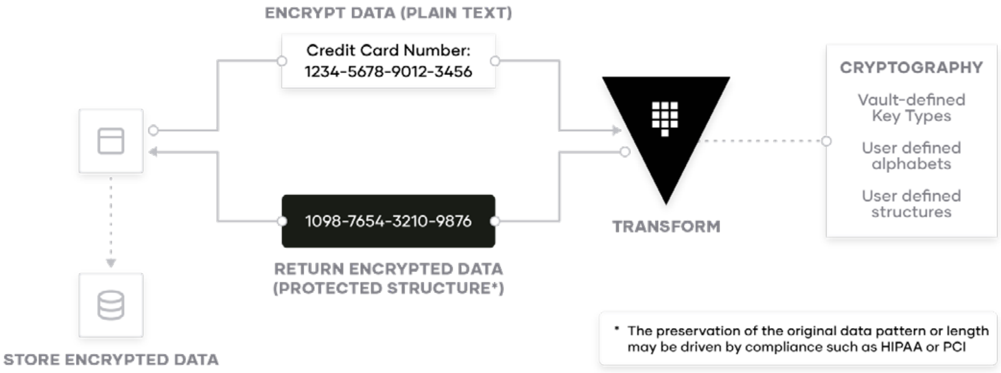

Figure 4: Transform Secret Engine Overview

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