Vault

Implementation Foundations

Module: Vault Operations

What You Will Learn

Vault Operations

- Overview
- Initialization
- Seal Keys
- Auto-Unseal
- Root Tokens

Logging and Monitoring

- Vault Audit Logs
- Vault Telemetry
- Vault Vault Operations Monitoring
- Vault Systems Monitoring

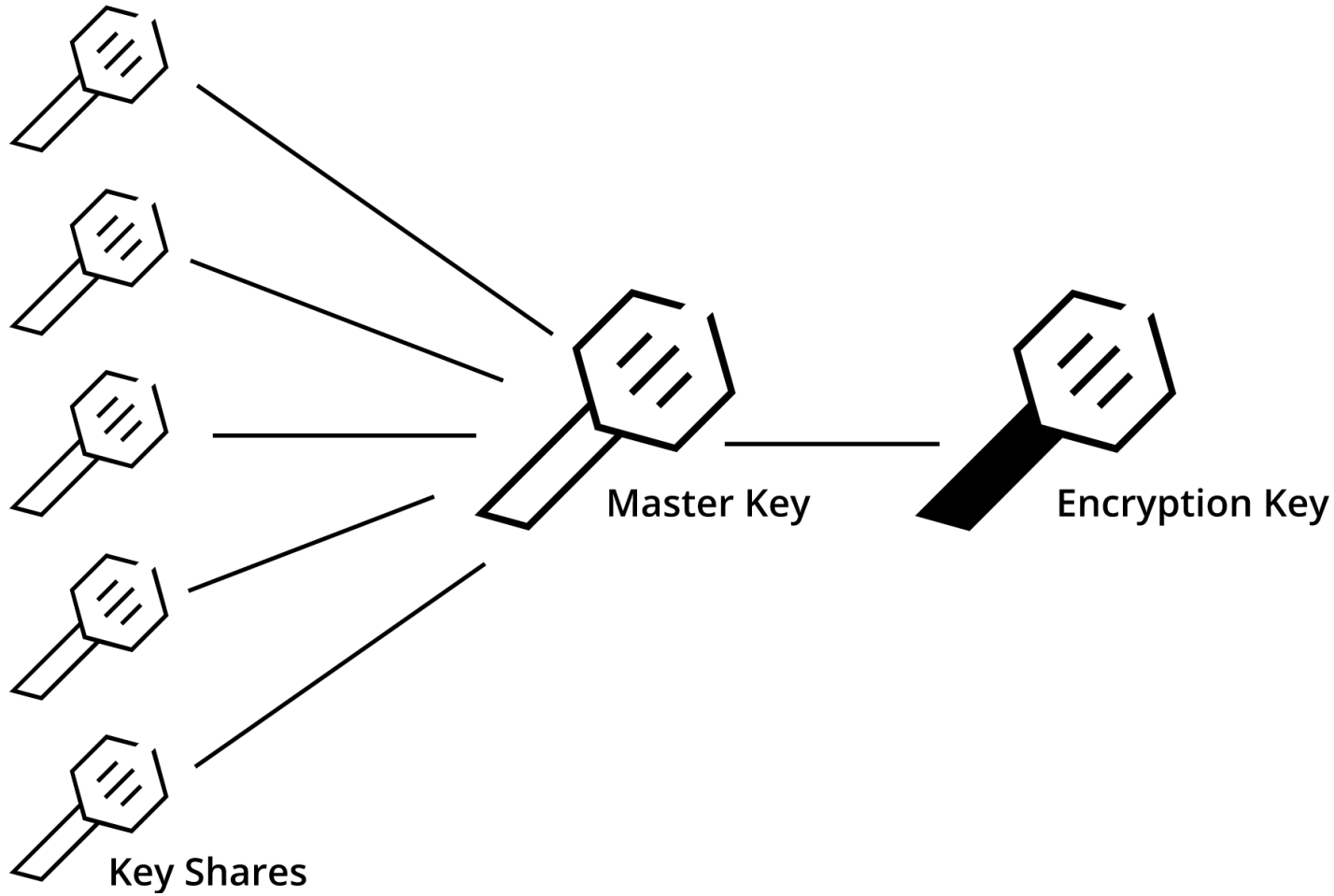
Operations Overview

Introduction to Vault Operations

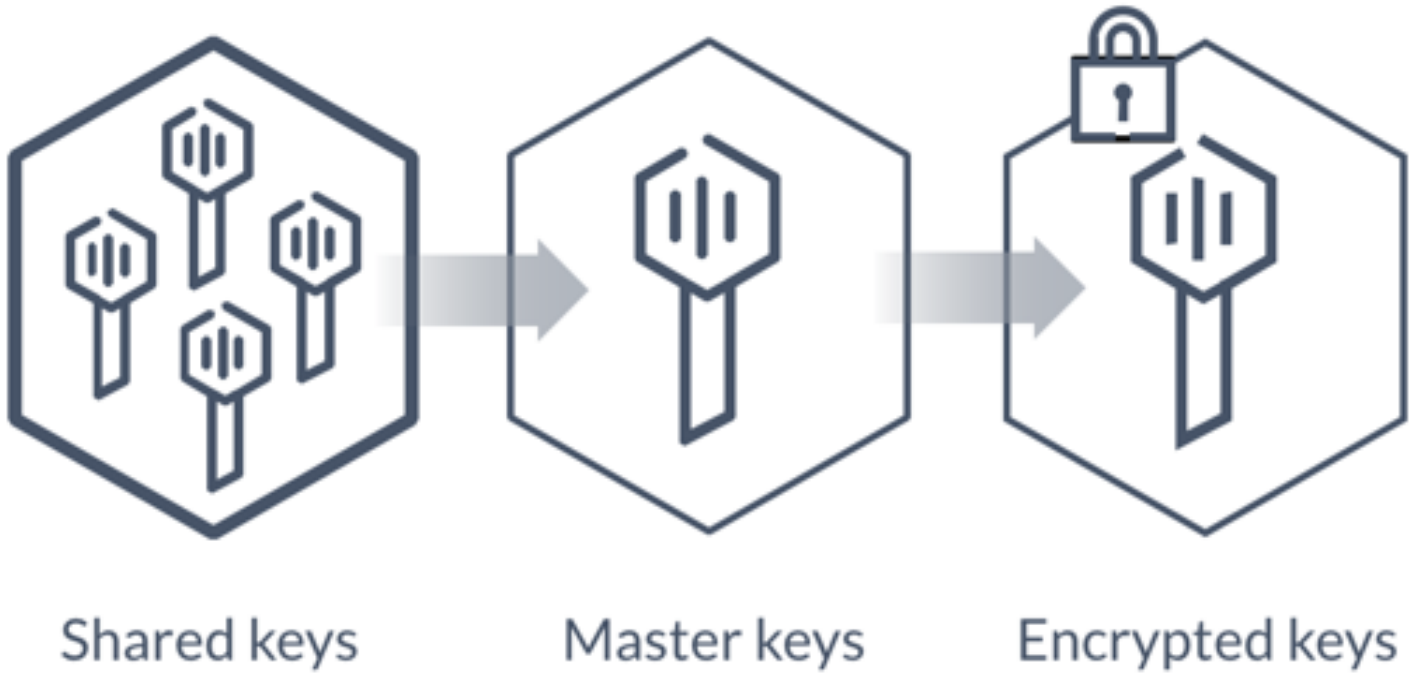
Initial operational steps are:

- Initialize Vault
- Management of Seal Keys and Root Tokens
- Configuring Logging and Monitoring of the Vault Service

Seal Keys - Overview



Seal Keys - Default Behavior



Seal Keys - Best Practices

- Bash history disabled
- Keep a physical copy somewhere
- Rotate seal keys after every use
- Store seal key shares in a secure place
- Use PGP public keys to encrypt the seal keys
  - Preferably a Hardware Security Module (HSM)
- Access to seal keys should be tightly controlled, monitored, and audited
- A rekey is possible and should be preformed anytime the seal keys are exposed

If the key shares are lost they cannot be recovered!

Example - Lost Seal Keys

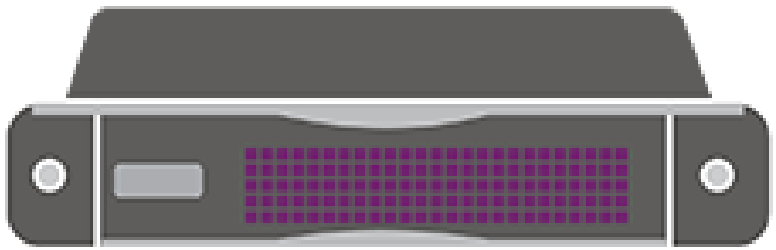
- Company deploys standalone Vault cluster with SSL certificates
- Customer-facing services are onboarded to Vault
- SSL certificates expire, causing Vault to enter a sealed state
- Until the key shares are found Vault is stuck in the sealed state
- Keys that were used to encrypt all customer data were stored in Vault

Without the seal keys all of the data is innaccessible!

Auto-Unseal - Overview

- Avoids frequent use of seal keys
- Minimizes the use and exposure of key shares
- A method of auto-healing after an outage or scheduled downtime
- Encourages secure storage and management of seal keys

Auto-Unseal - Recovery Keys



- Only one seal key is created and stored in the HSM
- A set of recovery keys are created
  - Used for very high privileged access

Root Token - Overview

- The second item that is provisioned during initialization of Vault
- Gives access to manage and read everything in Vault when unsealed
  - While Vault is in a sealed state the root token is essentially useless

Root Token - Best Practices

- Only use for break glass situations
- Create appropriate administrative policies, assign them to administrative users, then delete the root token
- Root tokens should be treated in a similar fashion to the seal keys
  - Access to the root token shoudl be tightly controlled, monitored, and audited
- The root token can be protected by a public/private key set

Audit Logging
&
Health Monitoring

Logging and Monitoring - Overview

Knowing the health or status of your service is key to making a great experience for users

The health of the Vault service can be gathered via:

- Audit logs
- System logs
- API endpoints
- Telemetry data

Vault Audit Logging

- File:
  - Simply appends audit data to a specified file
- Syslog:
  - Uses the *nix syslog mechanism to write audit data
- Socket:
  - Uses a specified IP address, port, and protocol to write audit data

Vault Logging - Best Practices

- Log Rotate
- Systems Logs
- Logical Seperation
- Sane Retention Policies
- External Logging Service

Vault Telemetry Endpoints

Monitor the health of vault through native integrations:

- statsite
- statsd
- Circonus
- DataDog
- Prometheus
- StackDriver

Vault Monitoring - Operations

What is critical to understanding the health of the Vault service?

- Seal State
- Failed Requests
- Replication State
- Backup/Snapshot Status
- Number of Secrets Created
- Request Volume per Cluster
- Number of Service Tokens Created Per Time Period

Vault Monitoring - Host OS

What is critical to understanding the health of the underlying OS?

- CPU
- Memory
- Disk I/O
- Disk Space
- Disk Inodes
- File Descriptors
- Network Throughput

Vault Monitoring - Security

What is critical to understanding the security posture of the Vault service?

- Root Token Use
- Seal Keys Re-key
- Tokens With Long TTL
- Repeated Access Failures
- Root Token Creation/Rotation
- Repeated Authentication Failures
- Vault/Secret Accessed from New IP

Vault Operations : API Endpoints

Some of the more useful API operations for monitoring the health of the service are listed here:

- `sys/audit`
- `sys/health`
- `sys/leader`
- `sys/metrics`
- `sys/host-info`
- `sys/seal-status`
- `sys/replication/dr`
- `sys/replication/performance`

Chapter Summary

- Initial Vault Commands
- Best Practices around encryption keys and key shares
- API endpoints and functional endpoints to monitor Vault
- Overview of the day to day concerns and operational concerns of running Vault

Reference links

- Vault Operator Commands
- Vault Telemetry
- Vault HTTP API Reference for System Backend

Vault Operations Module Complete!