Vault

Implementation Foundations

Module 1: Architecture

An Overview of Vault (1/2)

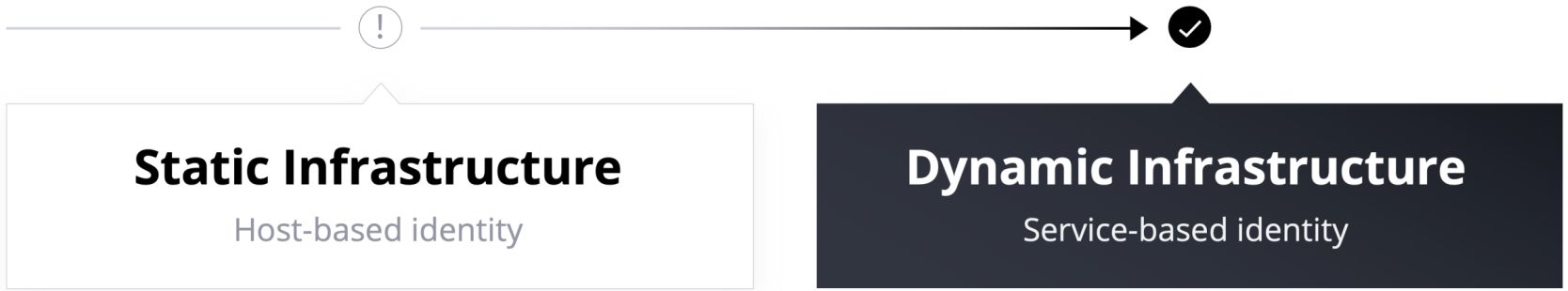
- The Vault Workflow
- Authentication
  - Policies
  - Secrets
- Vault Terminology

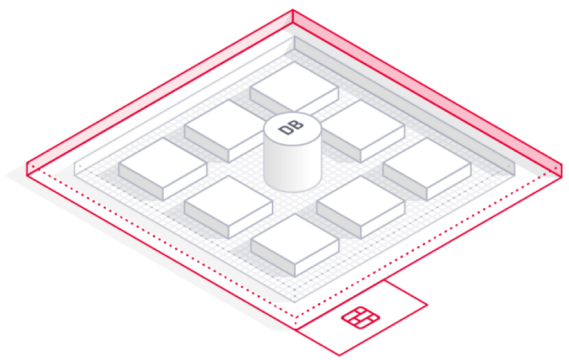
An Overview of Vault (2/2)

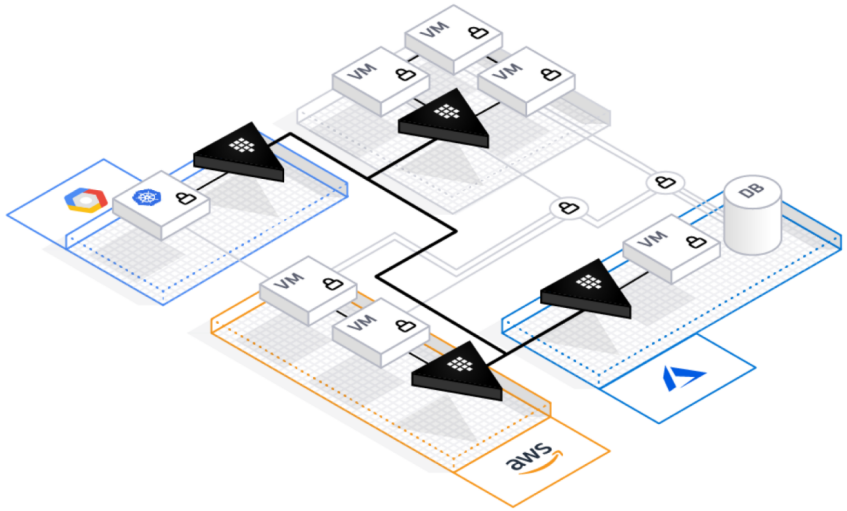
- Vault Server Architecture
  - High Availability Mode
  - Vault with Consul
  - Network Connectivity
- Vault Replication
  - Disaster Recovery
  - Performance Replication

Introduction To Vault

The Shift From Static to Dynamic (1/3)







The Shift From Static to Dynamic (2/3)

Static Infrastructure (Host-based identity)

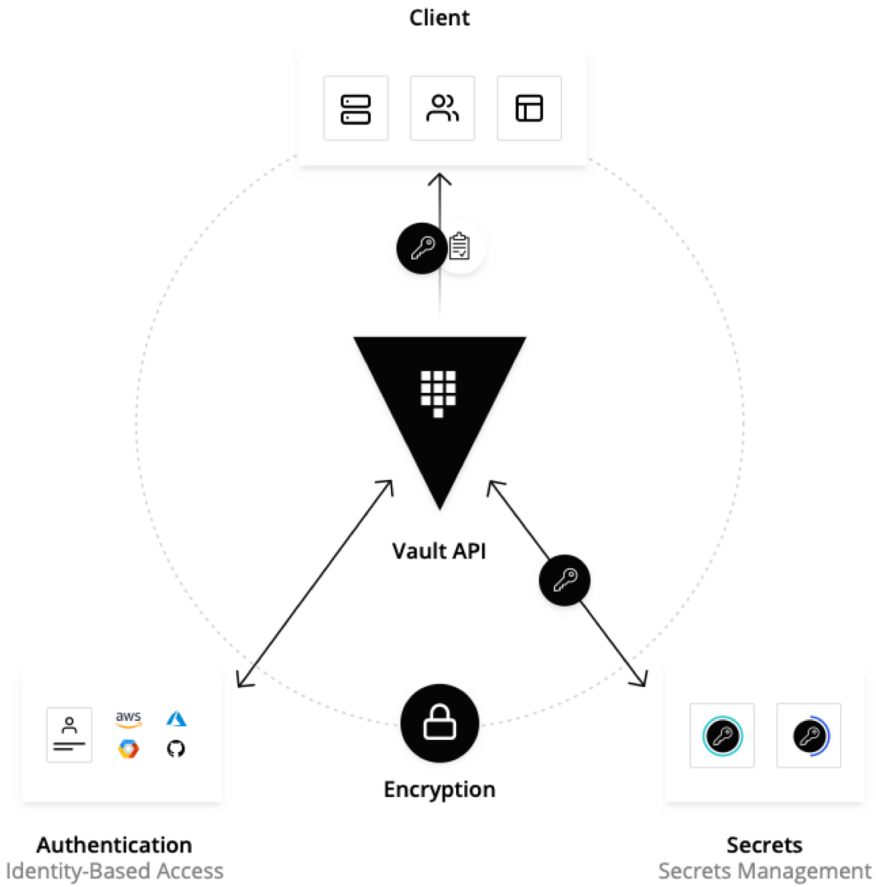
- Traditional Approach
- Relies on high-trust networks with clear network perimeters.
- High Trust Networks
- A Clear Network Perimeter
- Tight Infrastructure Security

The Shift From Static to Dynamic (3/3)

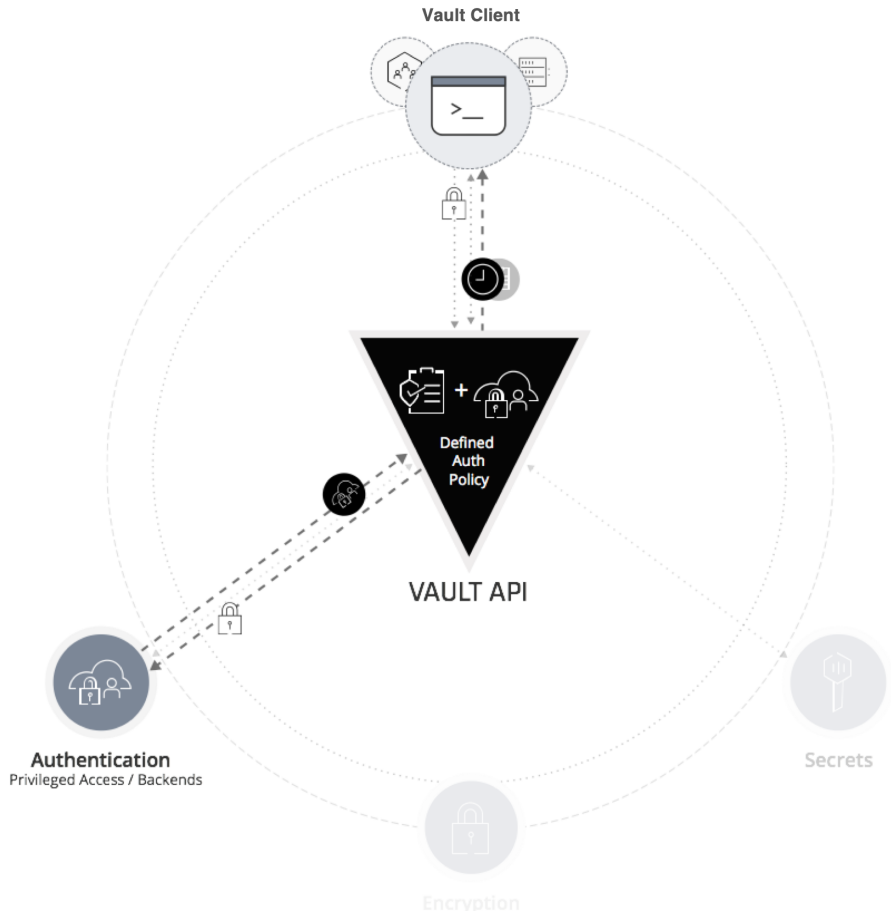
Dynamic Infrastructure (Service-based Identity)

- Dynamic Approach
- No clear network perimeter.
- Low-trust networks in public clouds
- Network perimeter across clouds
- Identity verification security

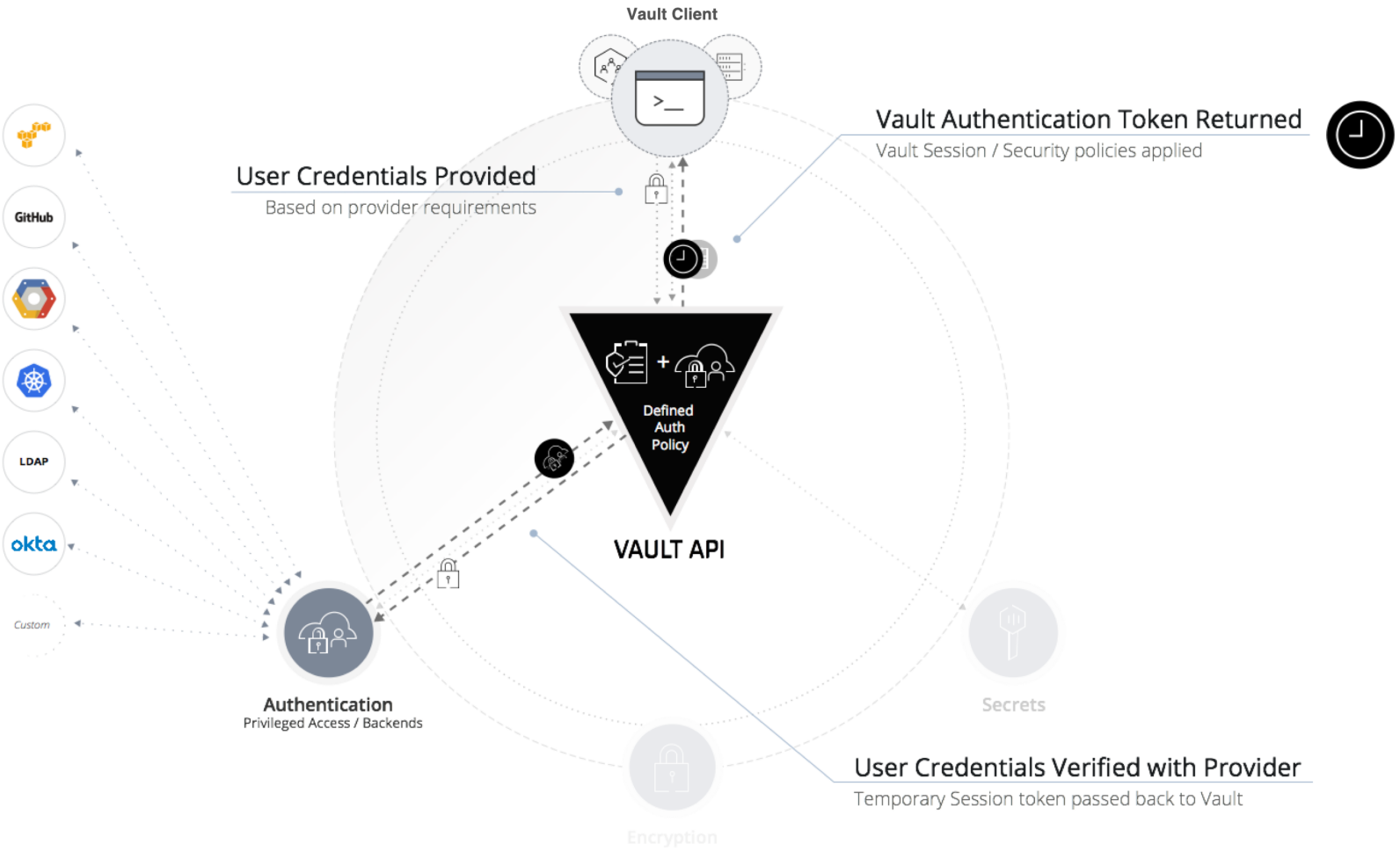
How Vault Works



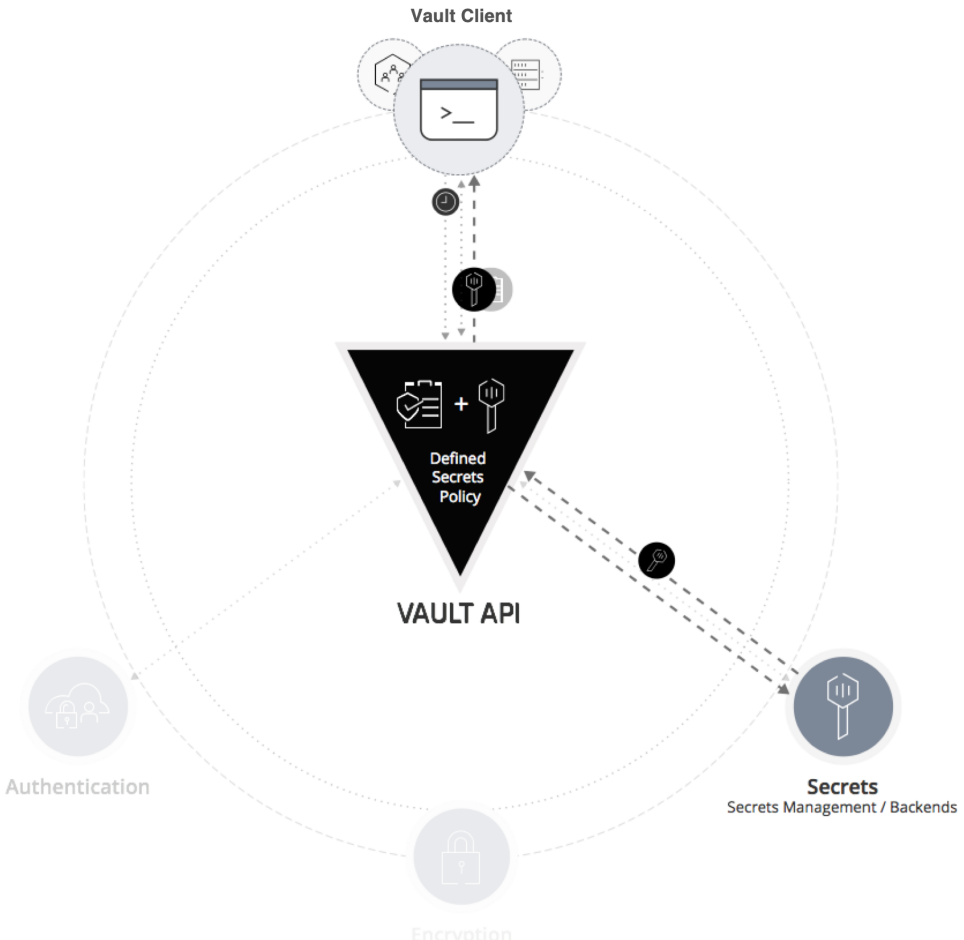
Client Authentication



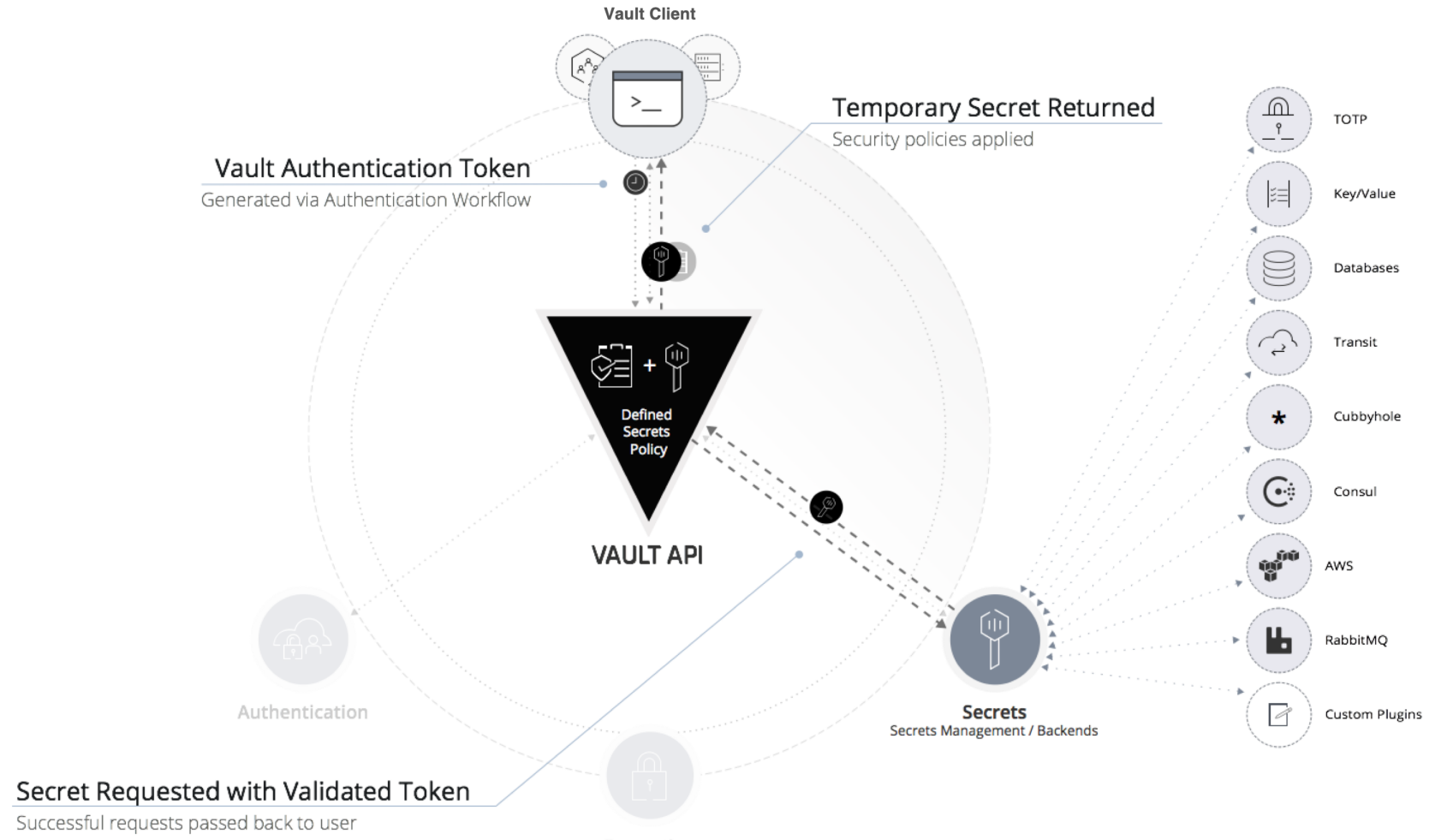
Trusted Source Of ID



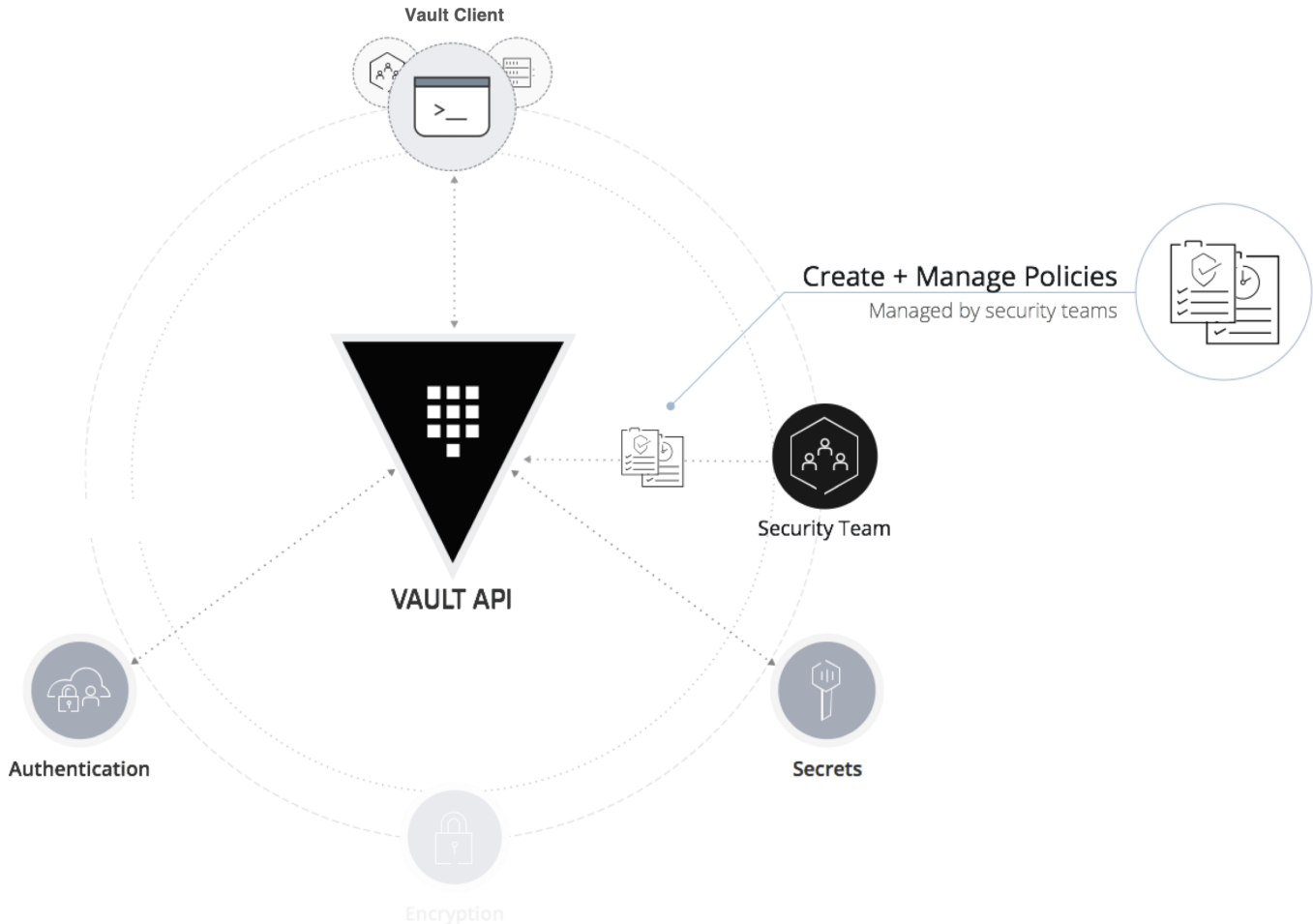
Vault Token



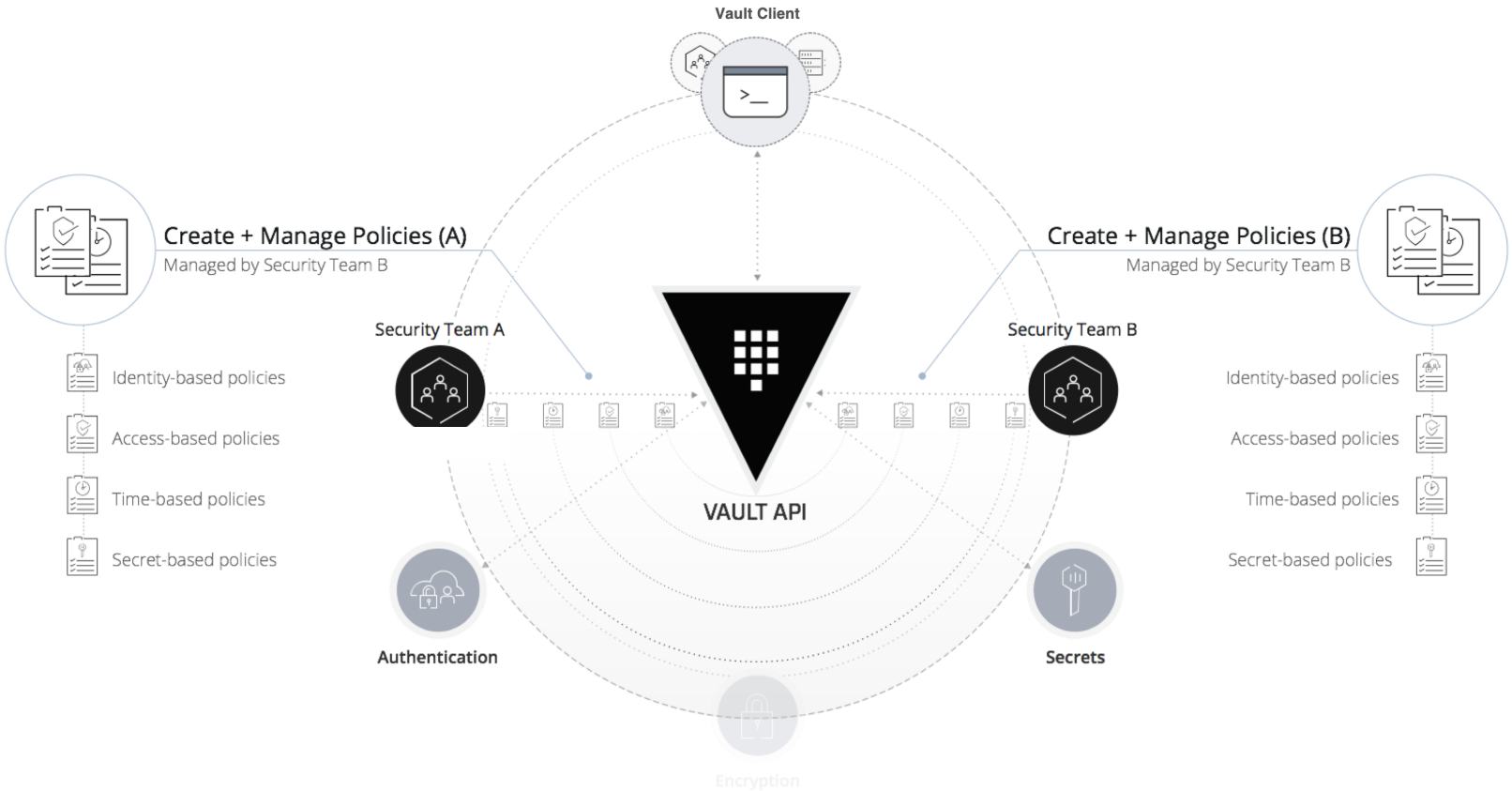
Secrets Engine



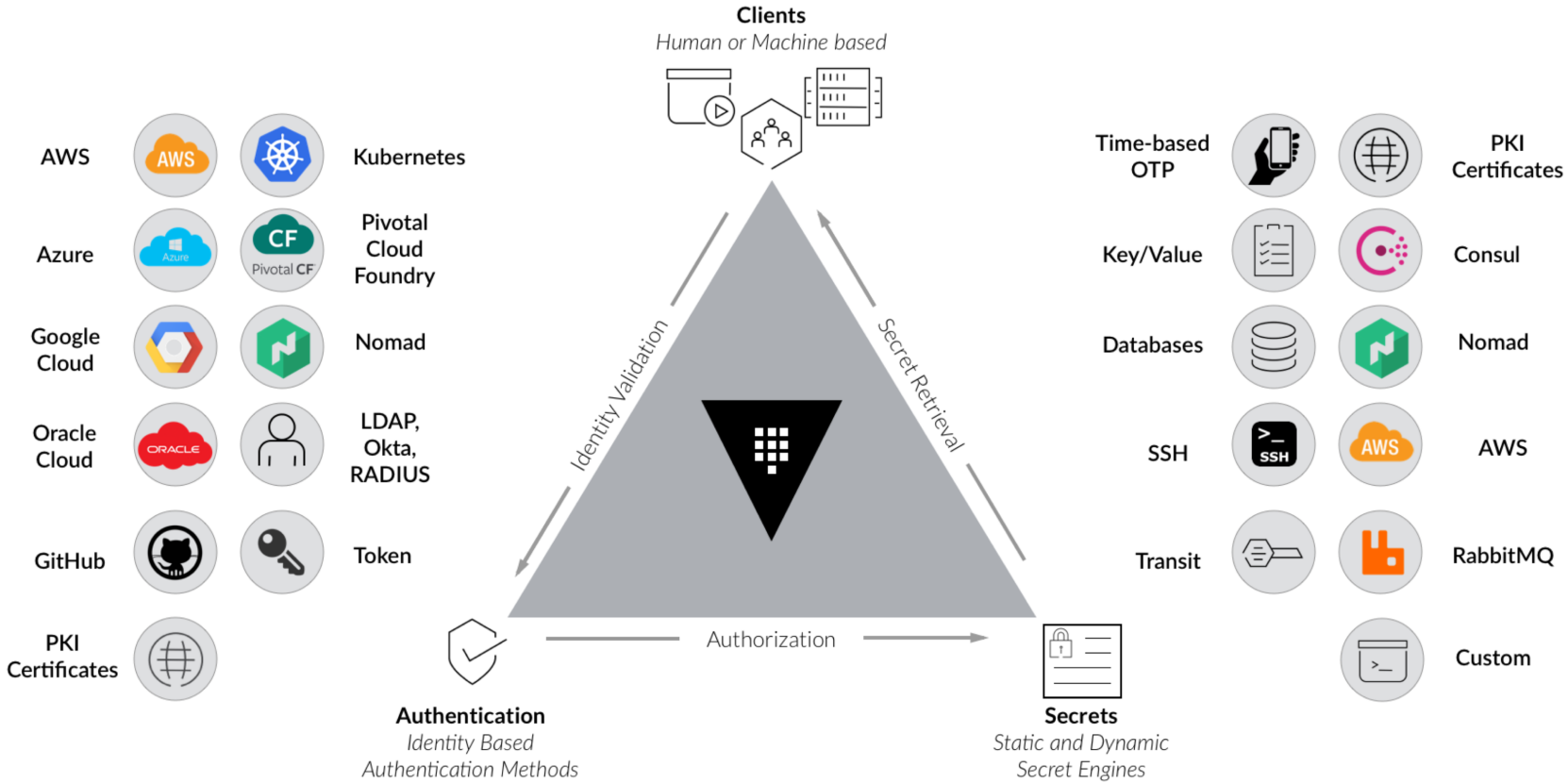
Vault Security Policies



Vault Namespaces

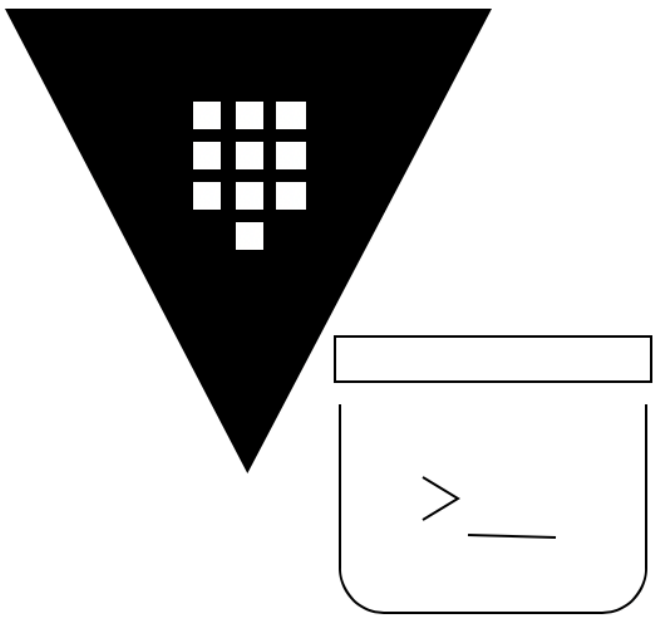


Vault Support



Vault Terminology: A Component Overview

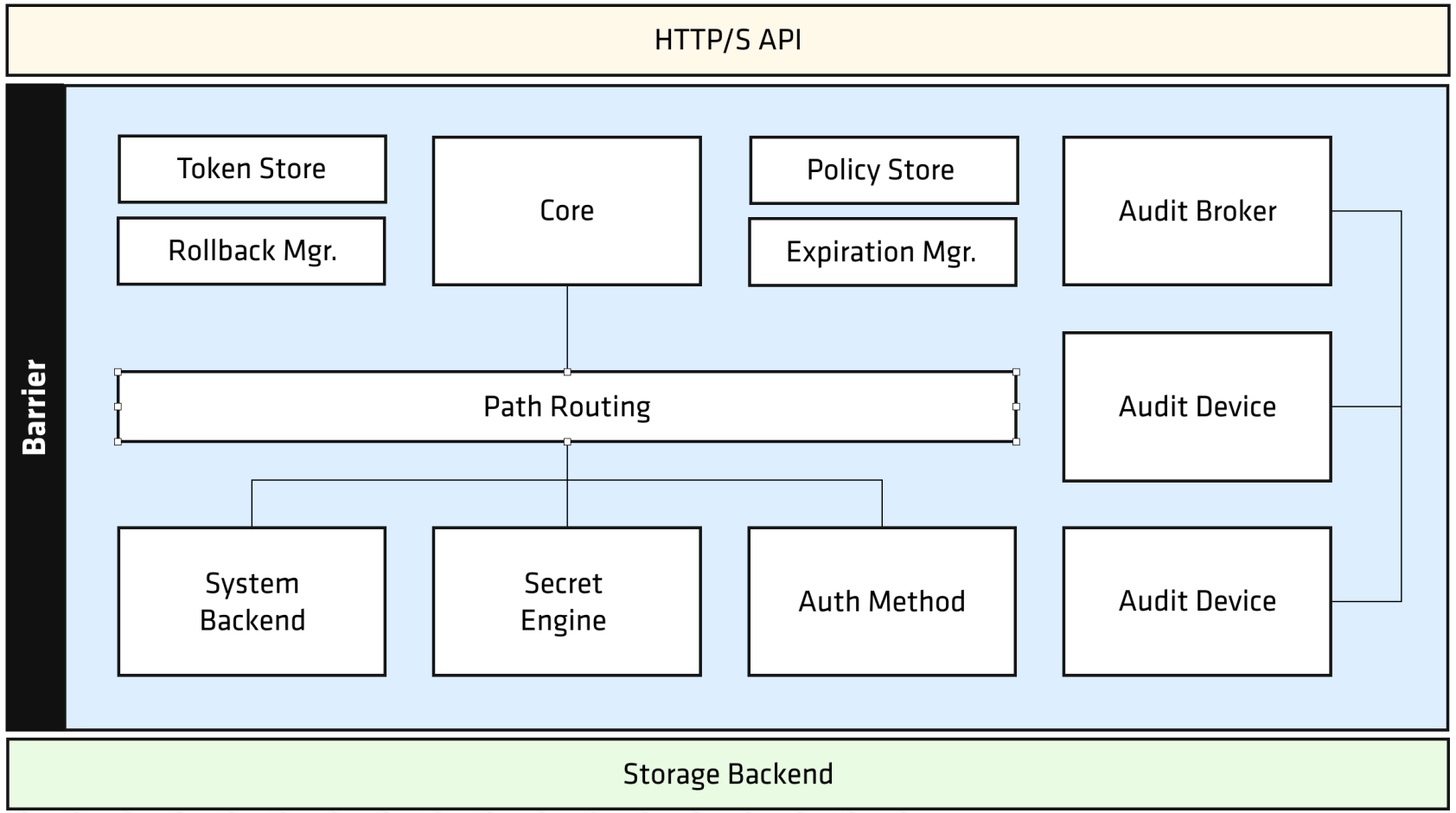
Vault Server



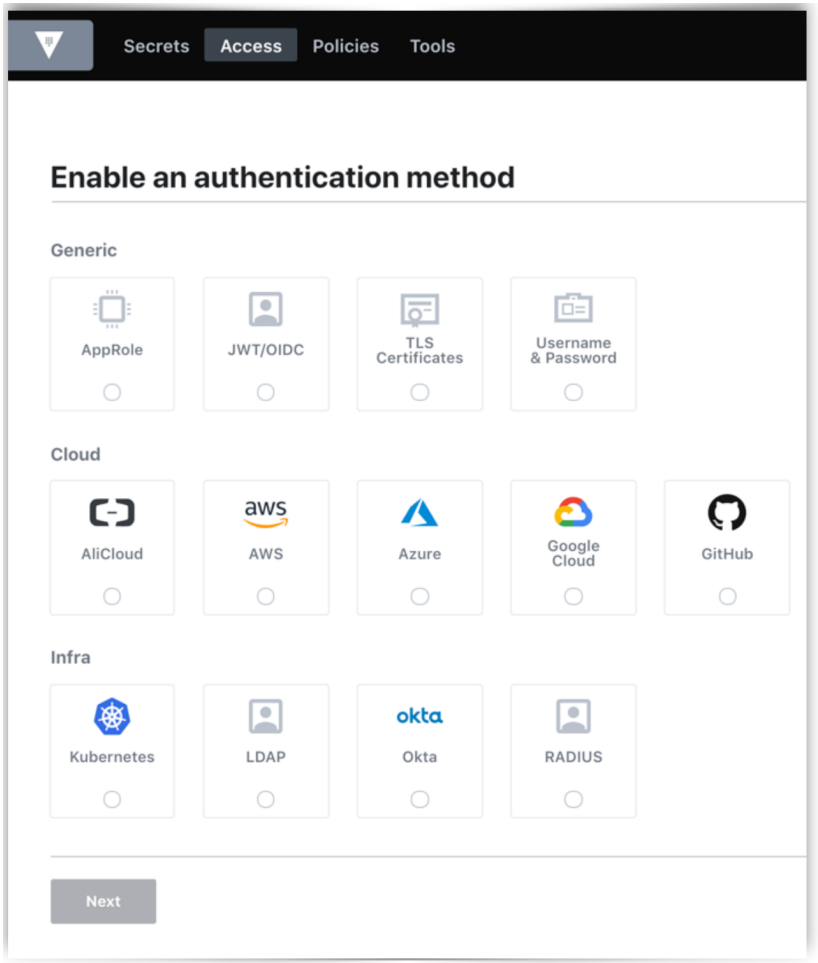
Manages all client interactions

- Clients
- Authentication Methods
- Policy and ACLs
- Secrets Engines
- Tokens

Architecture



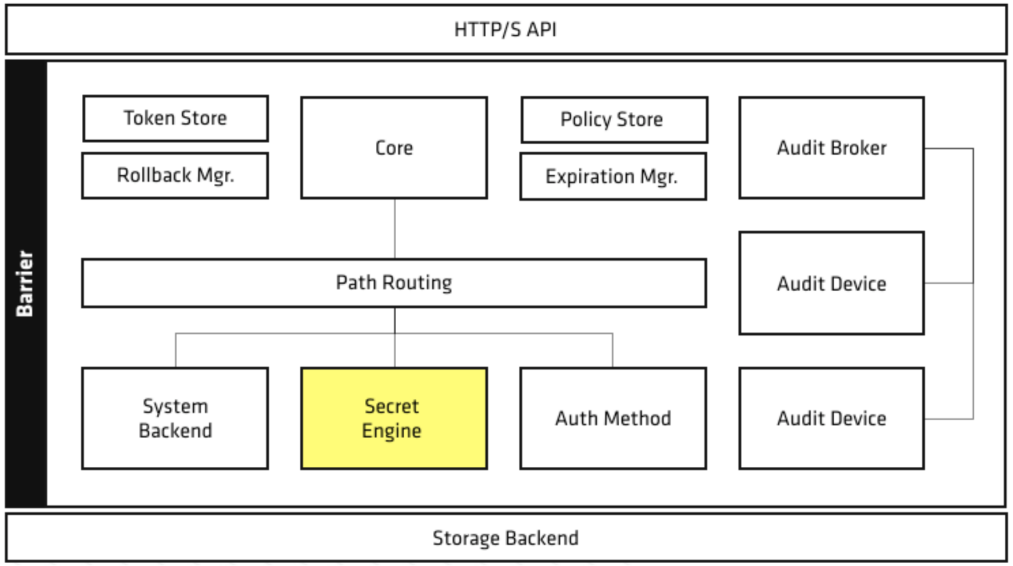
Authentication Methods



Controls Authentication Configurations

- Credential based
- Connects to trusted identity systems
- Operator Specific Methods
- Machine Specific Methods
- Multiple methods can be configured and chained together

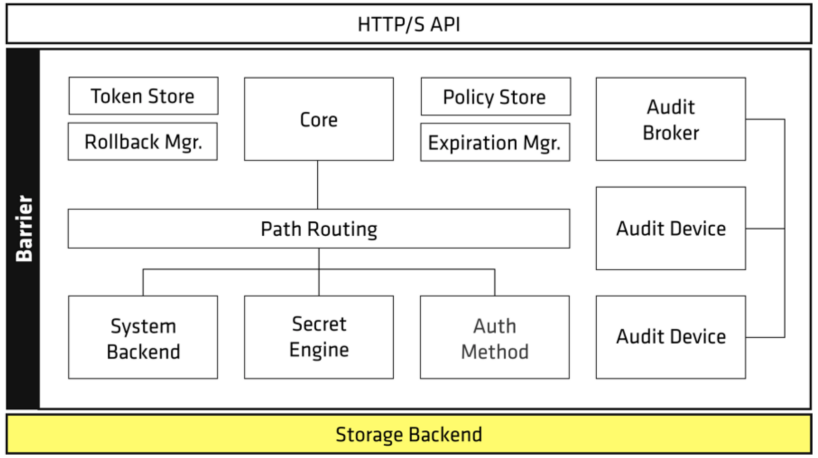
Secrets Engine



Controls Secrets Configurations

- Responsible for managing secrets
- A secret engine stores, generates, or encrypts sensitive materials
- Can store static sensitive data
- Can generate secret material dynamically
- Multiple engines can be configured

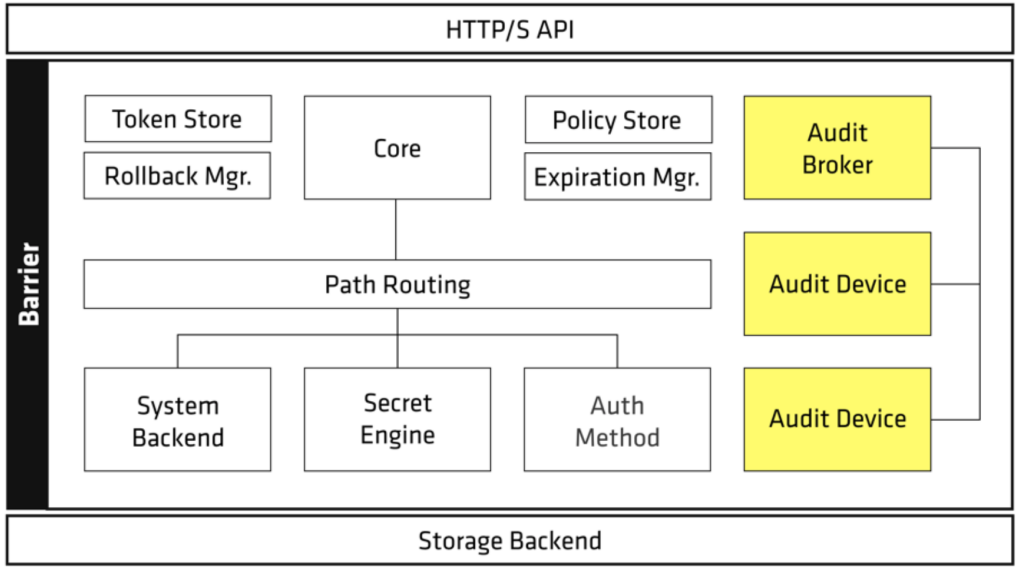
Storage Backend



Persistant Data Management

- Responsible for durable data storage
- Data is encrypted at rest using 256bit AES
- Enterprise supports Vault managed or Consul managed
- Others can work but are not officially supported
- Only one can be used

Audit Devices

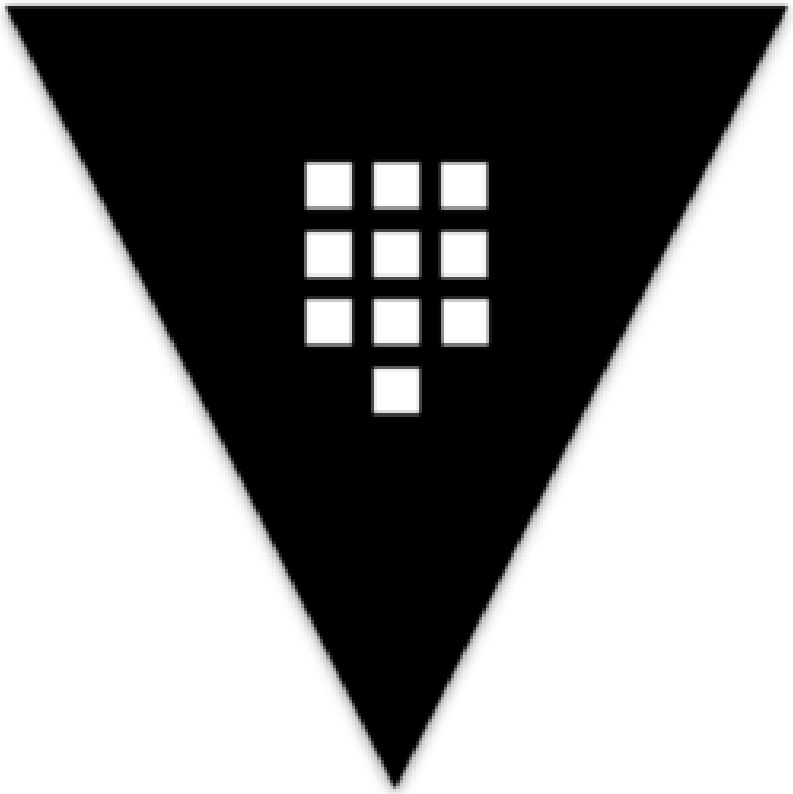


Interaction Logging

- Records every interaction
- Must be explicitly enabled
- Multiple supported devices
- Can configure multiple

Clustering & High-Availability

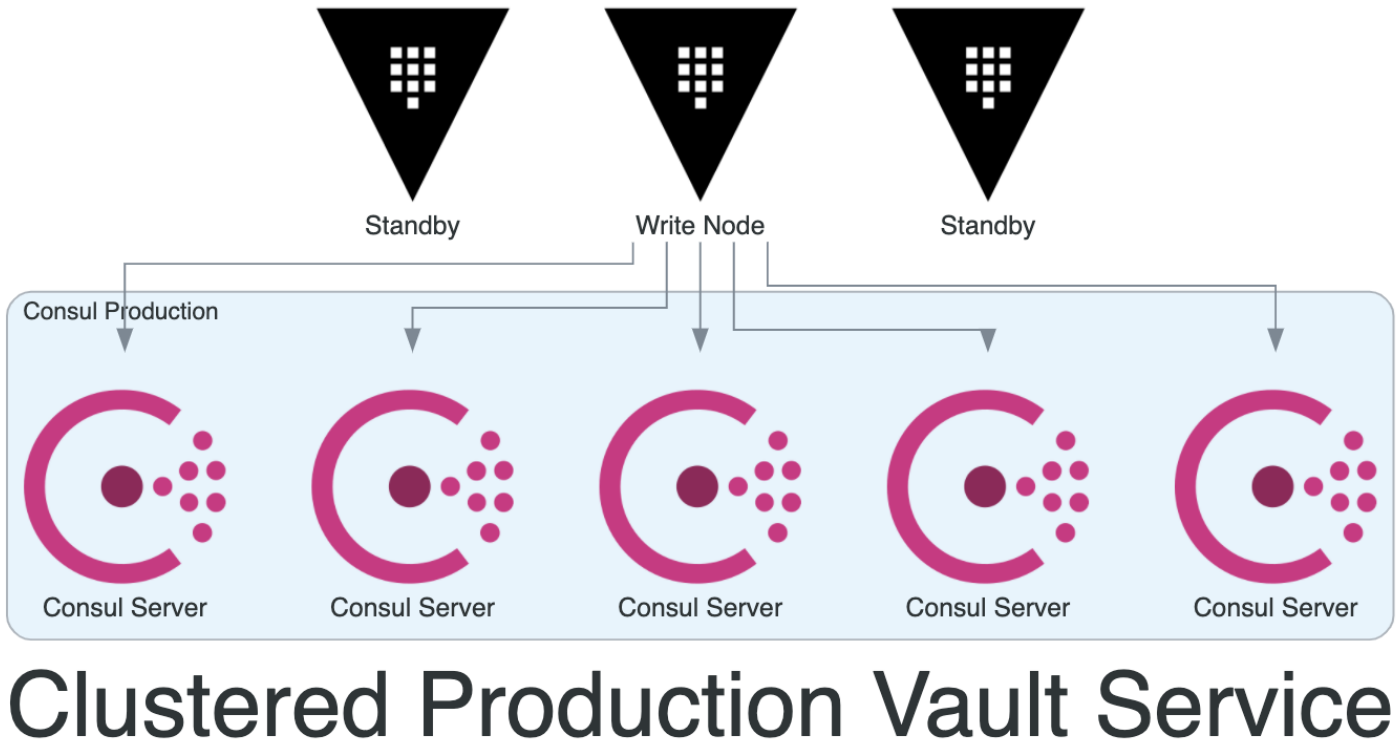
High Availability Mode



Multi-server Mode

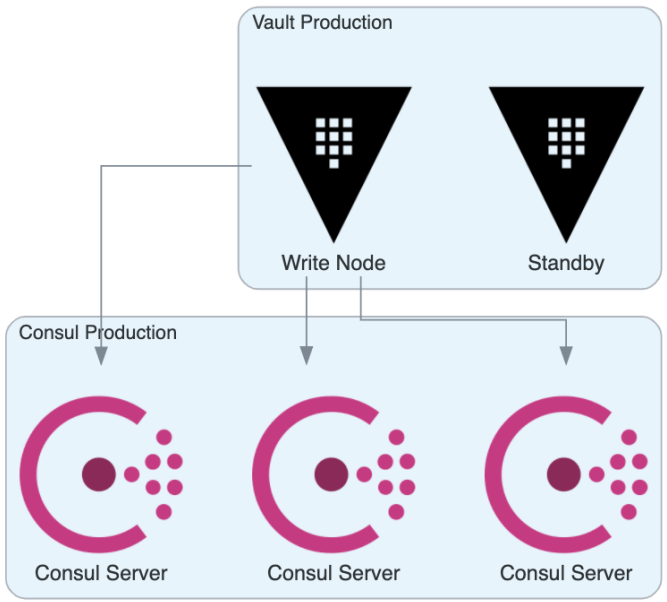
- Vault supports high availability
- Protects against local outages
- Automatically enabled with Vault Enterprise

Vault Reference Architecture



Consul-based Storage Backend

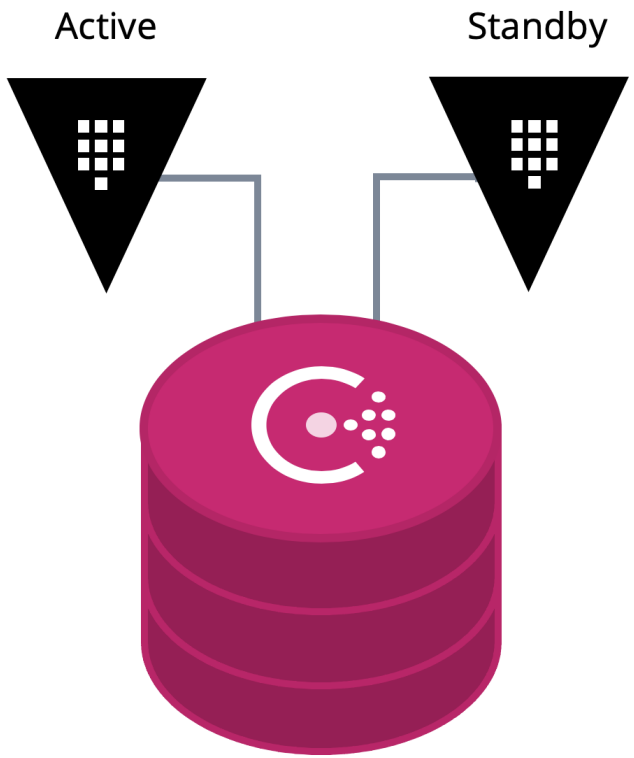
Vault Non-Production Architecture



Clustered Non Production Vault Service

Consul-based Storage Backend

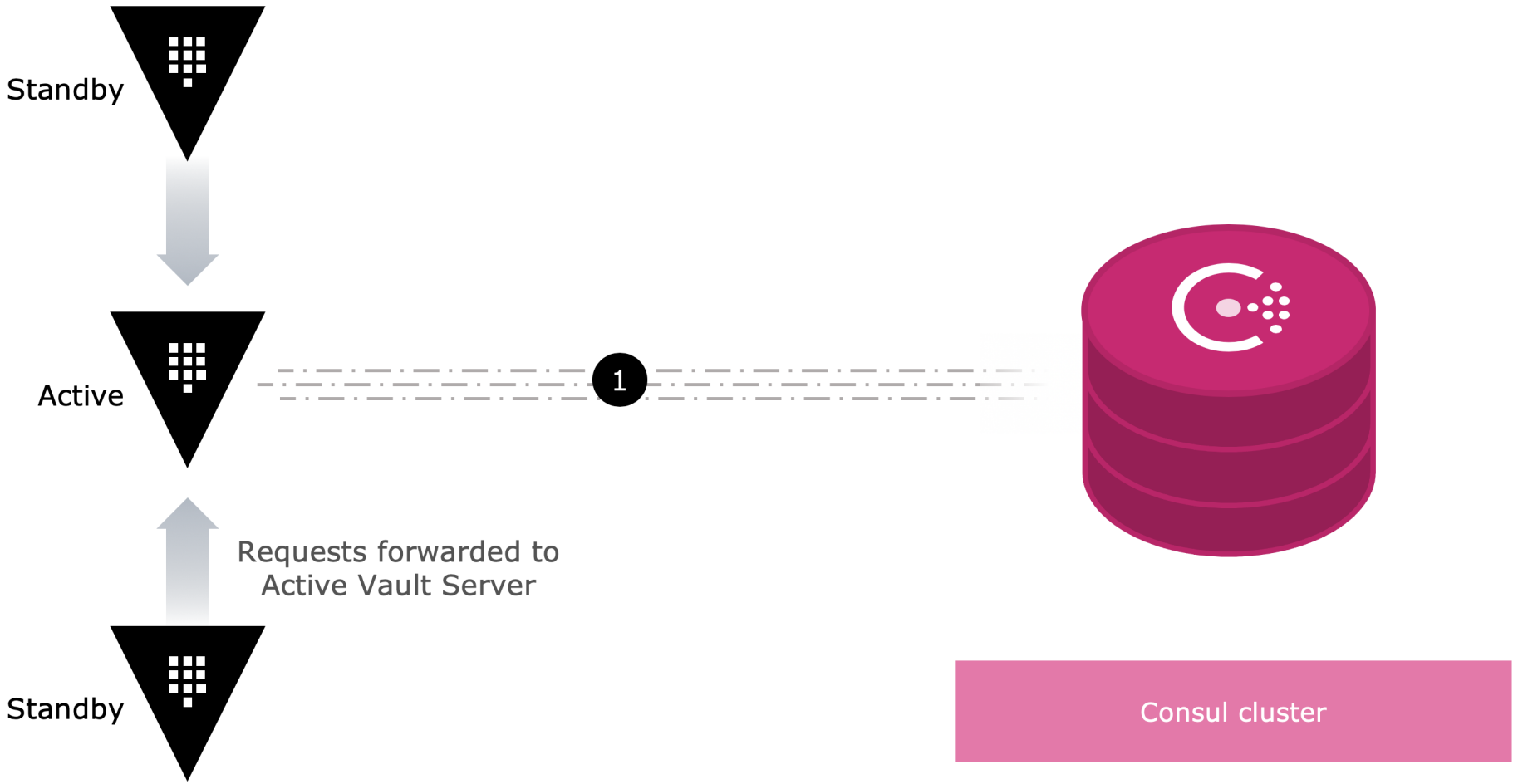
HA with Consul Storage



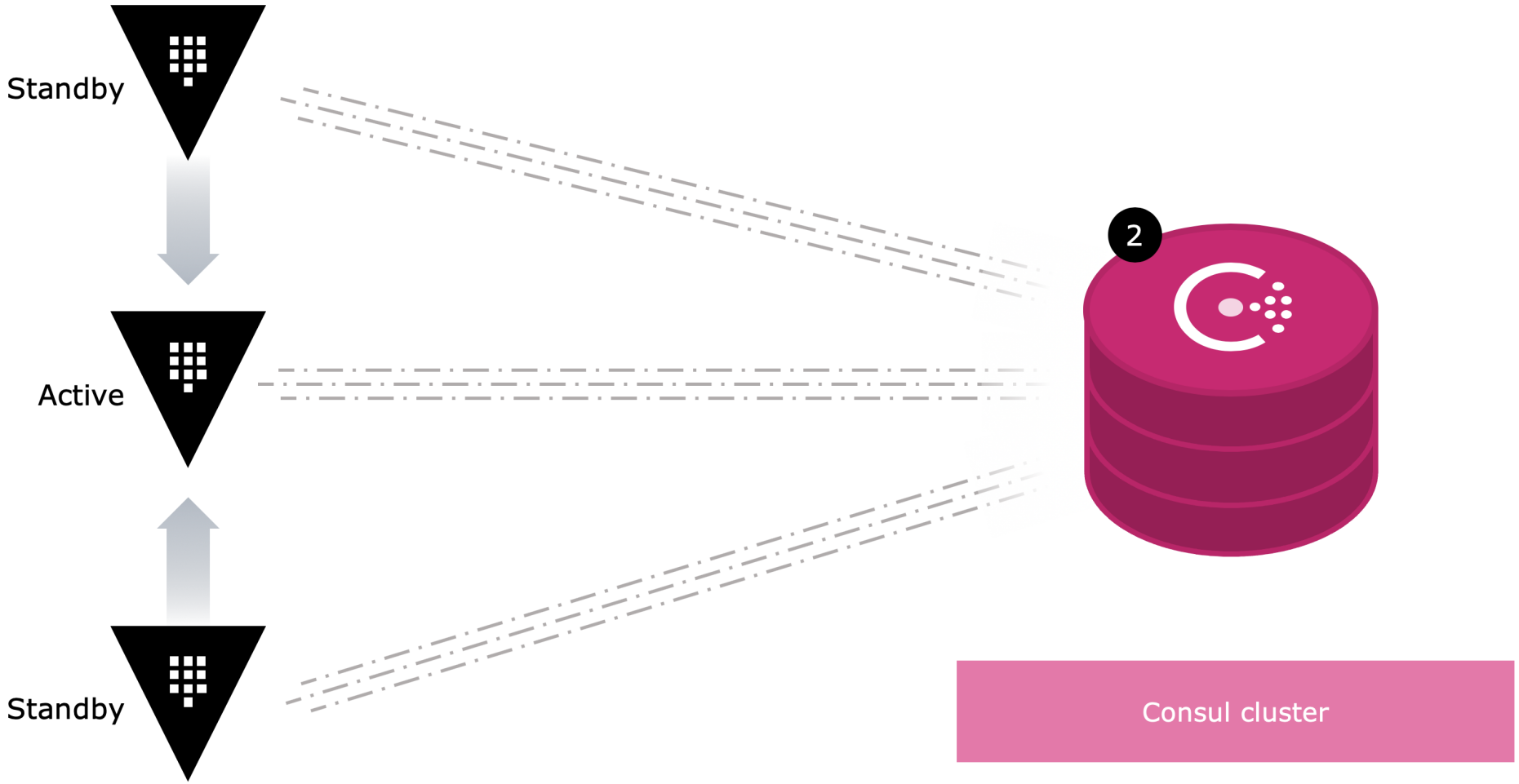
Consul Storage

- Enterprise Supported
- Highly scalable distributed KV store
- Vault HA leverages Consul for failover detection
- Native Consul integration for vault health

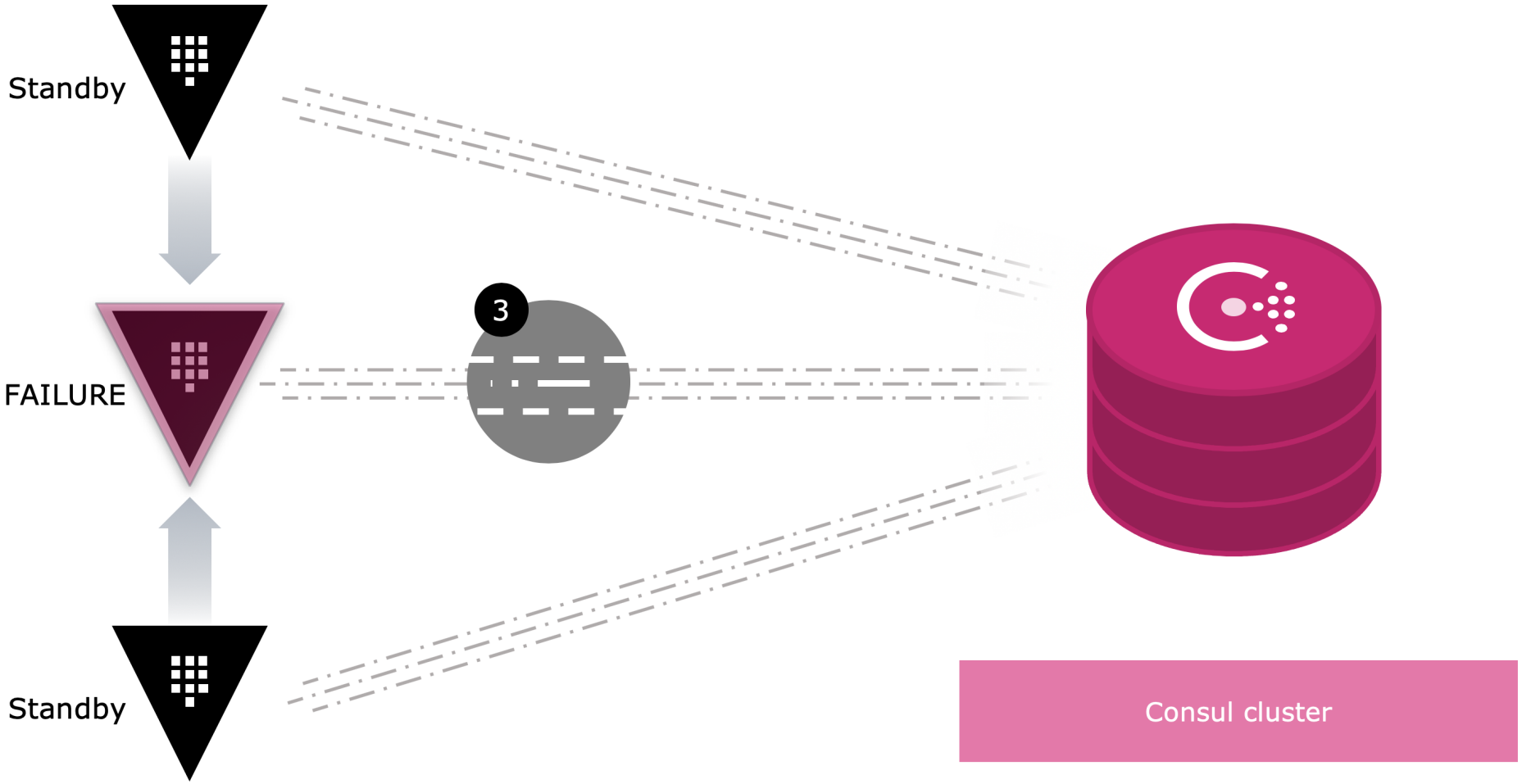
HA - Active Node



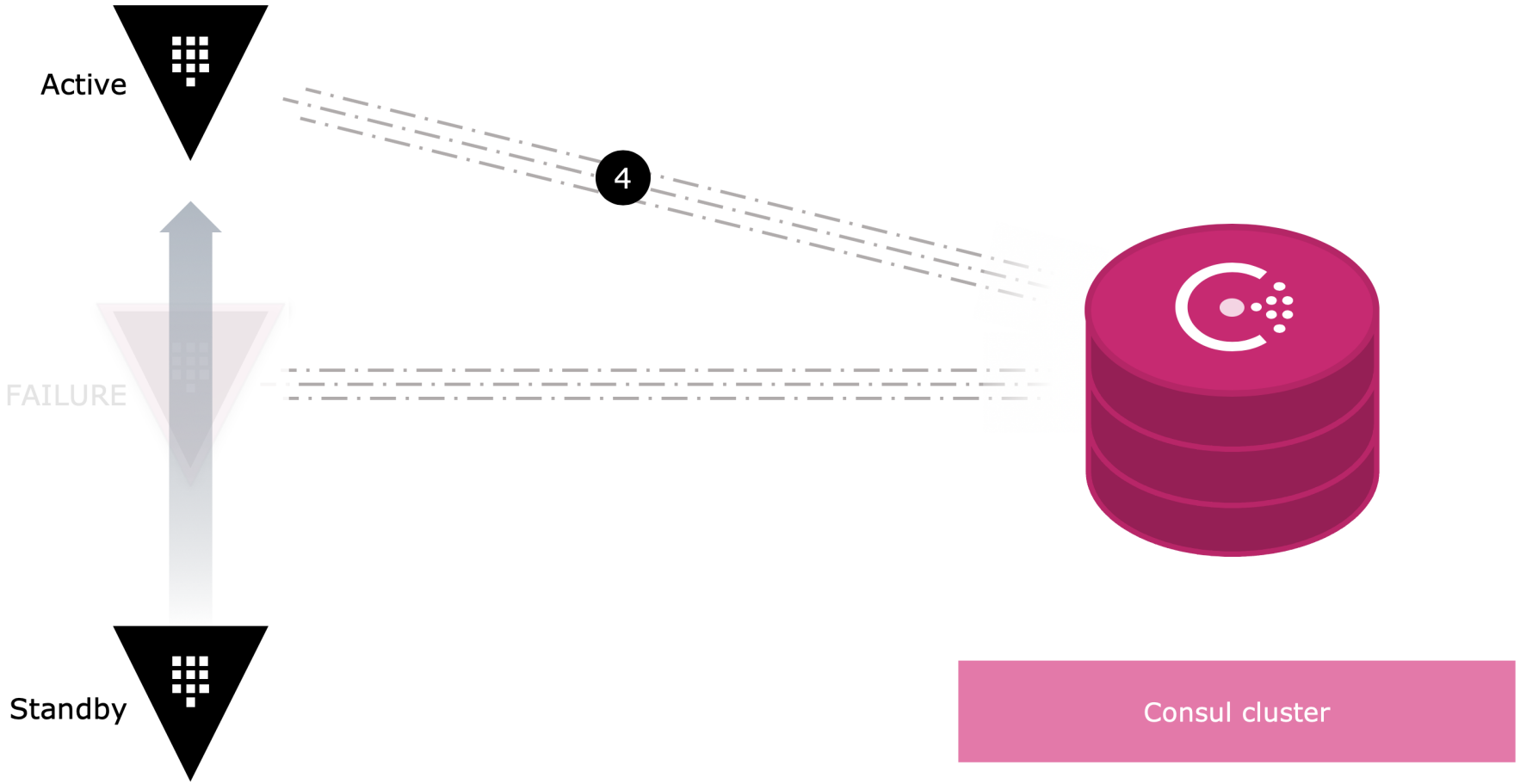
HA - Health Checks



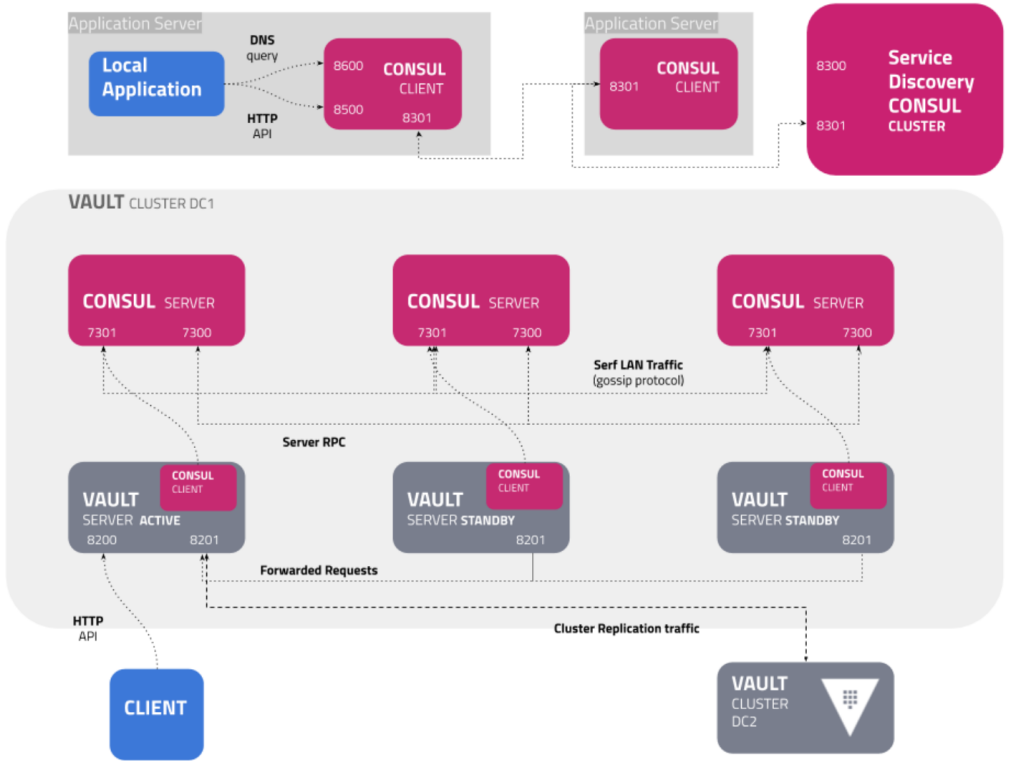
HA - Failure Detection



HA - Vault Failover

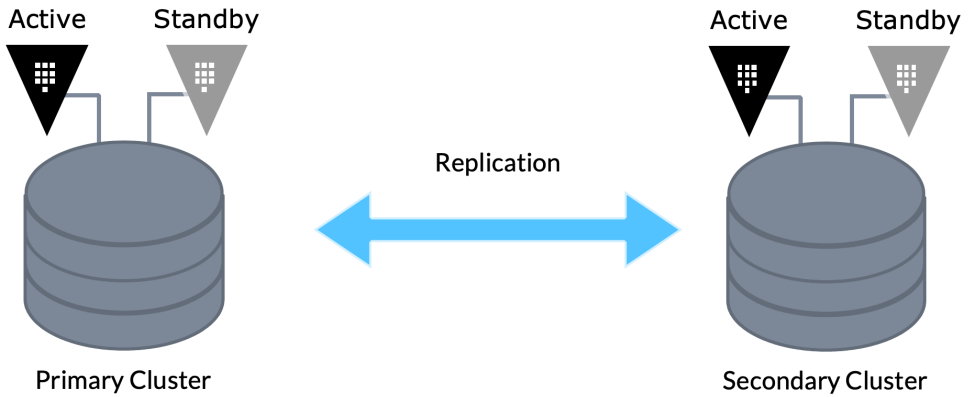


Network Connectivity Details



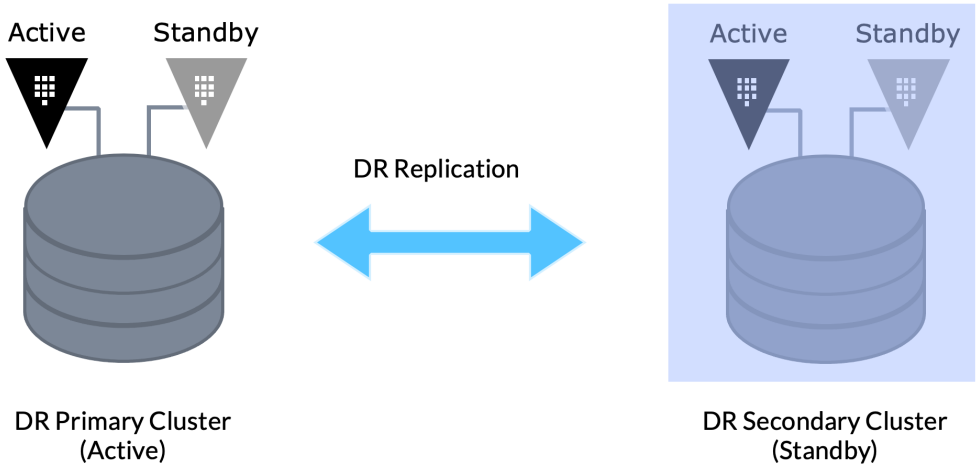
Vault Replication Overview
Disaster Recovery & Performance Replication

Vault Enterprise Replication



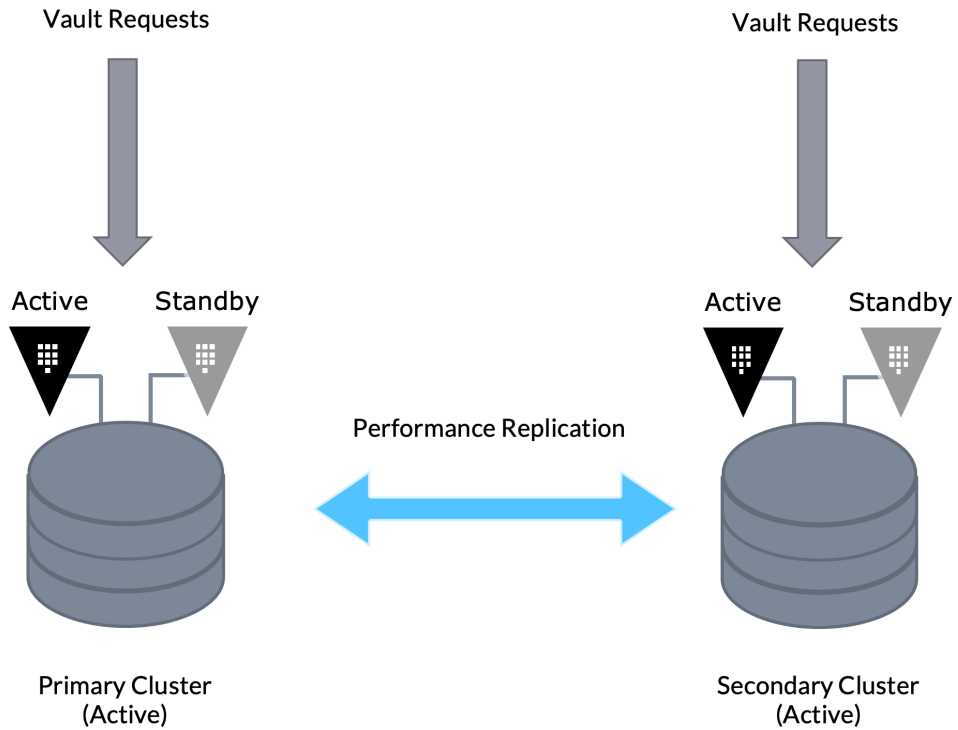
- Vault Cluster is the core replication unit
- Operates on a leader/follower model
- Primary Cluster linked to a series of secondaries
- Primary is the system of record
- Data is asynchronously replicated to secondaries

Disaster Recovery Replication



- Primary services all requests
- Primary replicates all data to linked secondary
- One DR to one Primary
- DR promoted in the event that a primary completely fails

Performance Replication



- Primary and secondaries service requests
- Primary replicates all data to all linked secondary
- One Primary to many secondaries
- "Configure centrally, access locally"

Replication Comparison

Capability	DR Replication	Performance Replication
Configuration Mirroring	Yes	Yes
Secrets Configuration	Yes	Yes
Static Secrets	Yes	Yes
Dynamic Secrets	Yes	No
Token Replication	Yes	No
Secondaries Handle Requests	No	Yes

Chapter Summary

- Vault allows you to secure, store and tightly control access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API

- Vault uses Secrets Engines for secrets, Audit Devices for auditing and Auth Methods for Authentication

- Vault has two replication methods
  - Performance Replication for scaling availability and throughput
  - Disaster Replication for business continuity planning

Module 1 Reference links

- Vault Overview
- Vault Whitepaper
- Introduction to Vault with Armon
- Replication Concepts

Vault Architecture Module Complete!