HashiCorp
Vault

Vault Enterprise Technical Overview & Architectural Deep-Dive

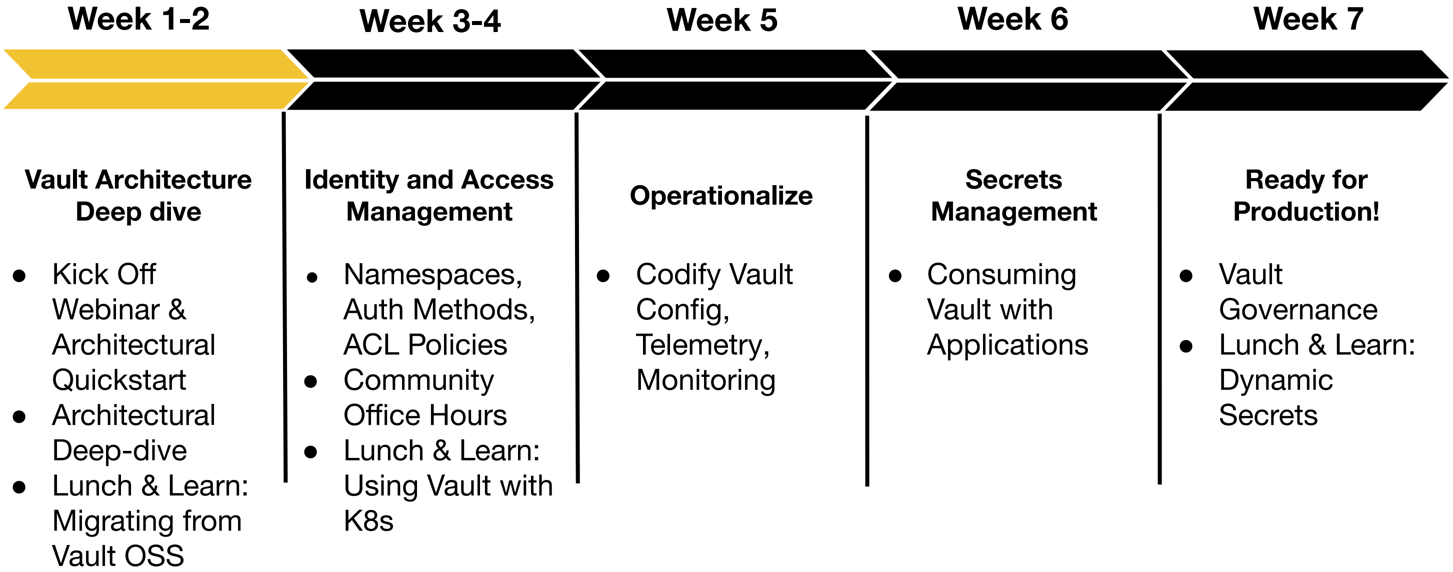
August 2022

Copyright © 2021 HashiCorp

Agenda

1. Overview
2. Architecture
3. Deployment Patterns
4. Operations
5. Next Steps

Vault Enterprise Path to Production



Week 1-2

Vault Architecture Deep dive

- Kick Off Webinar & Architectural Quickstart
- Architectural Deep-dive
- Lunch & Learn: Migrating from Vault OSS

Week 3-4

Identity and Access Management

- Namespaces, Auth Methods, ACL Policies
- Community Office Hours
- Lunch & Learn: Using Vault with K8s

Week 5

Operationalize

- Codify Vault Config, Telemetry, Monitoring

Week 6

Secrets Management

- Consuming Vault with Applications

Week 7

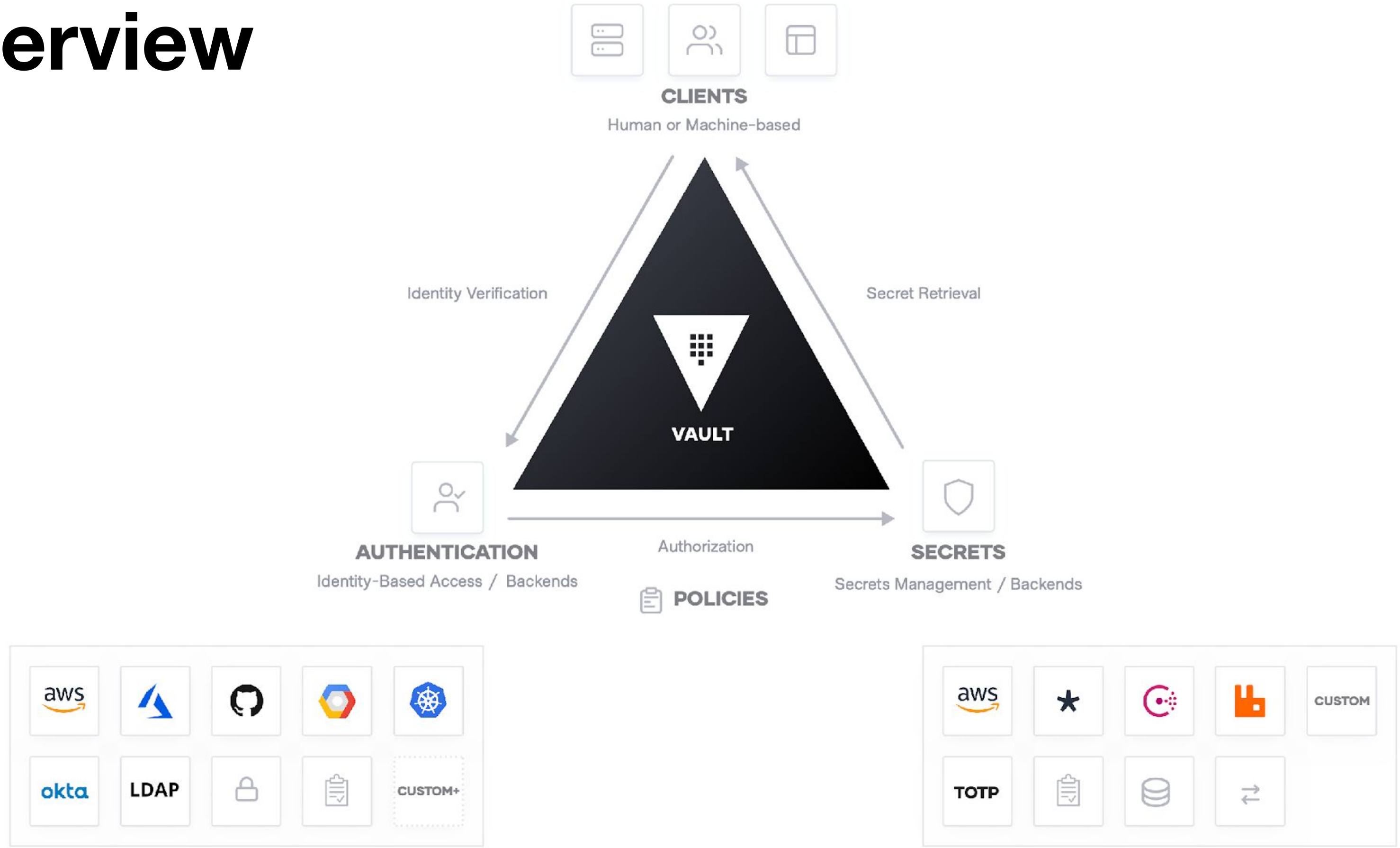
Ready for Production!

- Vault Governance
- Lunch & Learn: Dynamic Secrets

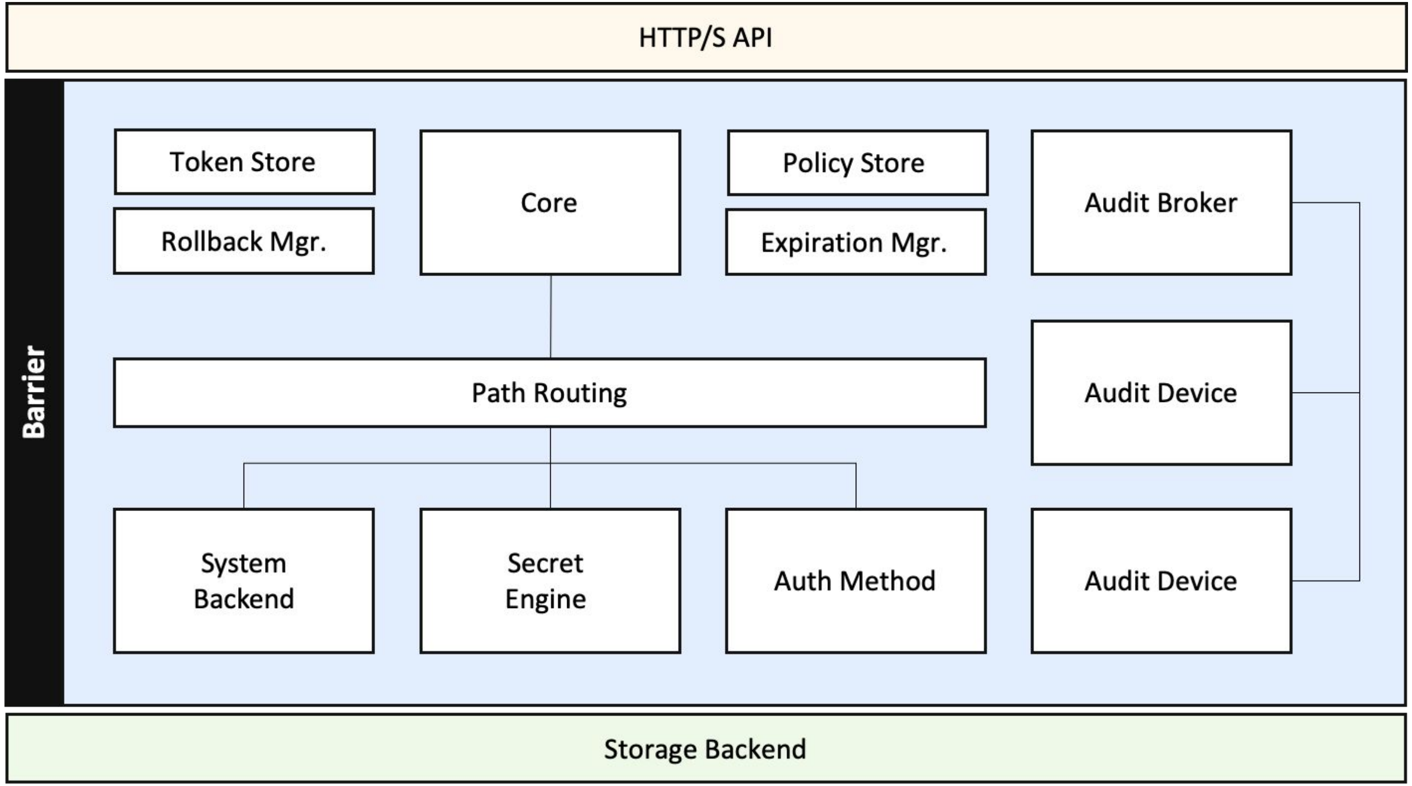
01

Vault Overview

Overview


CLIENTS
Human or Machine-based
Identity Verification
Secret Retrieval
VAULT
AUTHENTICATION
Identity-Based Access / Backends
Authorization
SECRETS
Secrets Management / Backends
POLICIES
aws
okta
LDAP
CUSTOM+
aws
CUSTOM
TOTP

Architecture & Cryptographic Barrier



Vault Security Model

- **It's all about access to the Encryption Key**
- Configuring `“cap_ipc_lock=+ep”, LimitNOFILE, and LimitMEMLOCK` prevent Memory Swapping to Disk, so secrets are not written in plain text to disk
- The Vault Encryption Key is stored in memory in **PLAIN TEXT**
  - This is done for performance
  - Root access to an unlocked vault server could compromise this
  - Isolation technologies which allow reading of memory could compromise this (VM issues, but principally Kubernetes)
- Master Root Key protects the Encryption key, so it also must be secure
- Auto-Unseal is a recommended pattern as it shifts the risk profile

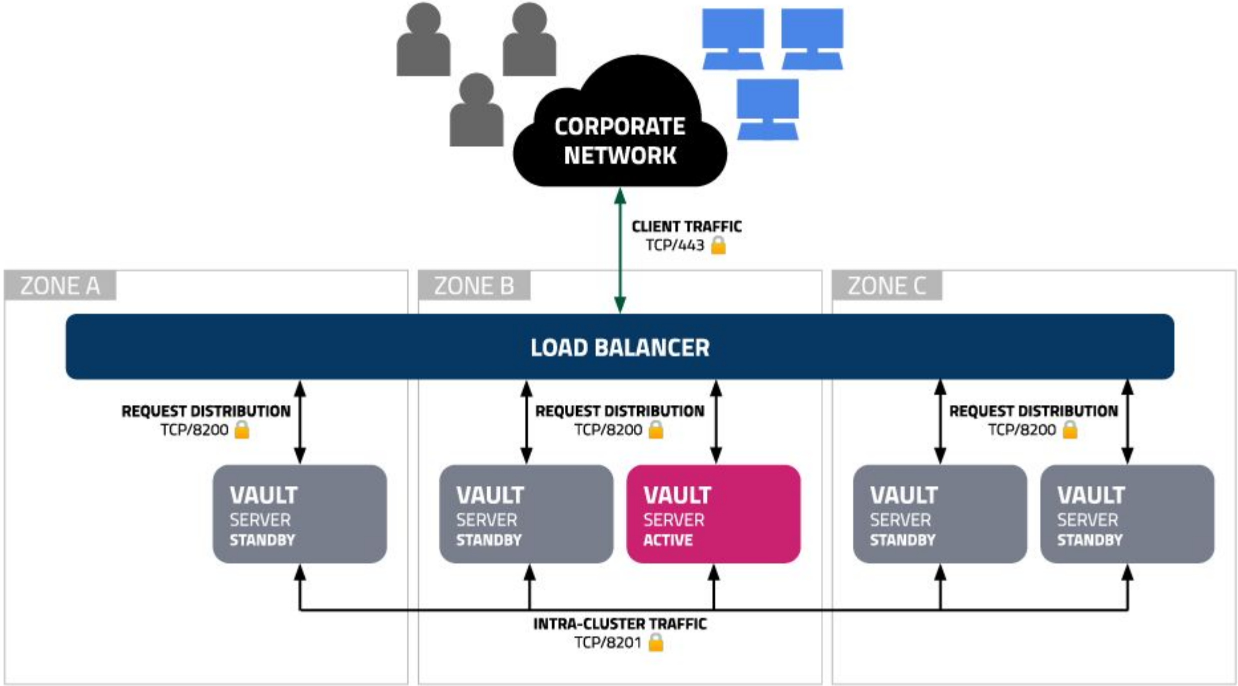
Cryptography Security Model

- **Vault uses publicly available cryptographic technologies**
- P vs NP - Good cryptographic algorithms are exponential in difficulty to solve but polynomial in difficulty to validate answers for
- Numerous algorithms (SHA1) were exposed to have defects that allowed them, or a subset of them to be reduced to polynomial difficulty problems
- Short encryption keys and faster computers has made brute-forcing older encryption standards possible
- Software based random number generations suffer from a lack of randomness

02

Vault Architecture

Integrated Storage Reference Architecture



5 Vault Servers across 3 Availability Zones

Vault Integrated Storage Architecture

- **Integrated Storage Autopilot**
  - Monitors node health status
  - Server stabilization - prevent quorum disruption from an unstable node
  - Dead server cleanup
  - Enabled by default in Vault 1.7.0 and higher
- **Vault 1.11.0 new features**
  - Automated upgrades promotes new versioned nodes to voter nodes removed old versioned nodes
  - Redundancy zones allows for deployment of non-voter nodes in an AZ with automatic promotion is a node is lost

Sizing

Per instance sizing recommendations

	Small (Dev/Test/Staging /QA)	Large (Production)
CPU	2 - 4 Core	4 - 8 Core
Memory	8 - 16 GB RAM	32 - 64 GB RAM
Disk Capacity	100+ GB	200+ GB
Disk IO	3000+ IOPS	10000+ IOPS
Disk Throughput	75+ MB/s	250+ MB/s

Cloud Instance Sizing

Provider	Size	Instance/VM Types	Disk Volume Specs
AWS	Small	m5.large, m5.xlarge	100+ GB gp3, 3000 IOPS, 125 MB/s
	Large	m5.2xlarge, m5.4xlarge	200+ GB gp3, 10000 IOPS, 250 MB/s
Azure	Small	standard_d2s_v3, standard_d4s_v3	1024 GB Premium_LRS
	Large	standard_d8s_v3, standard_d16s_v3	1024 GB Premium_LRS
GCP	Small	n2-standard-2, n2-standard-4	500 GB pd-balanced
	Large	n2-standard-8, n2-standard-16	1000 GB pd-ssd

Performance Considerations

Profile Workloads

- As Vault adoption scales throughout an organization there will be varying workloads utilizing Vault.
- Different workloads have varying impacts to resources (RAM, CPU, I/O)
- Leverage Telemetry monitoring to ensure an understanding of implications to Vault Cluster resources usage
- As new applications/services/teams/users are onboarded to Vault, profile the usage patterns to ensure optimal authentication and consumption patterns are used

External Systems

- Authentication Methods & Secrets Engines have external systems dependencies that can impact Vault's ability to process requests
- Ensure telemetry is enabled on those systems and services and proactively monitor for performance issues

Networking Considerations

Integrated Storage is network latency dependent

- <8ms RT network connection required to ensure Raft Storage remains consistent across all Vault Nodes.
- Restrict communication to only required ports and CIDRs
- Standard HTTPS TLS encryption should be used to protect network traffic

Networking Requirements

Source	Destination	Port	Protocol	Direction	Purpose
Client Machines	Load Balancer	443	tcp	incoming	Request distribution
Load Balancer	Vault Servers	8200	tcp	incoming	Vault API
Vault Servers	Vault Servers	8200	tcp	bidirectional	Cluster Bootstrapping
Vault Servers	Vault Servers	8201	tcp	bidirectional	Raft, replication, request forwarding
Vault Servers	External Systems	various	various	varios	External APIs

Load Balancing

Vault does not include built in load balancing capabilities

- To ensure Vault availability and reliability either an external load balancer or Consul should be used to distribute client requests
- **TLS should terminate at Vault** and not the load balancer to ensure end-to-end encryption
- Use Vault’s health endpoint to determine active node and node health https://<vaultnode>:8200/v1/sys/health

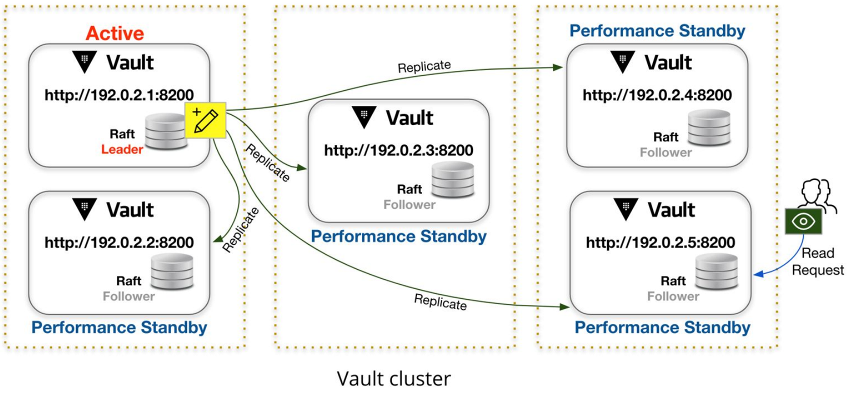
Scaling Considerations

Managed scaling services should be leveraged when deploying in a cloud environment to ensure the Vault cluster remains populated with health nodes

- Additional nodes will not increase performance
- Do not replace all instances at once in a scaling group otherwise data-loss will occur

Cloud	Managed Auto Scaling Service
AWS	Auto Scaling Group
Azure	Virtual Machine Scale Sets
GCP	Managed Instance Groups

Scaling Performance Standby Nodes



Horizontal scalability for read requests

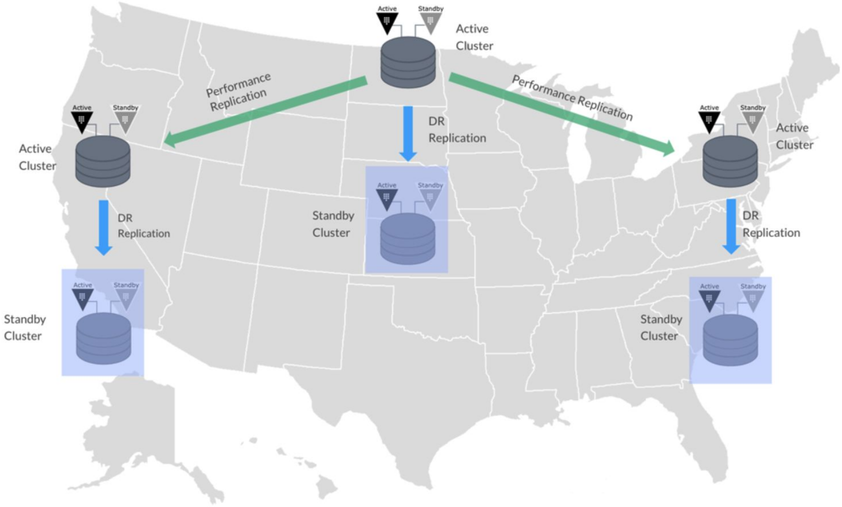
- Performance Standby Nodes can be used to respond to read-only requests
- Performance Standby Nodes are enabled by default and process read-only requests locally
- Write requests are forwarded to the Active Node
- Integrated Storage uses eventual consistency and data may not be available across all nodes immediately
- Vault 1.7+ includes multiple methods to control how requests are handled

Vault Replication

- Vault can be extended to multiple regions using replication

- The primary cluster uses asynchronous replication to ship data to the secondaries

- Multiple replication modes can be combined to provide resilience and performance



Replication Types

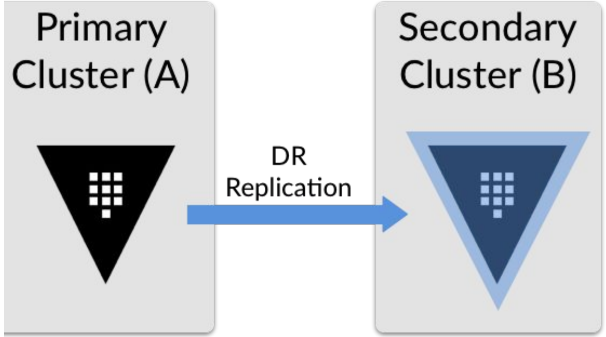
Disaster Recovery

Provides a warm standby cluster that contains all data from the primary Vault cluster. **It is strongly recommended to deploy at least one DR cluster.**

Performance Replication

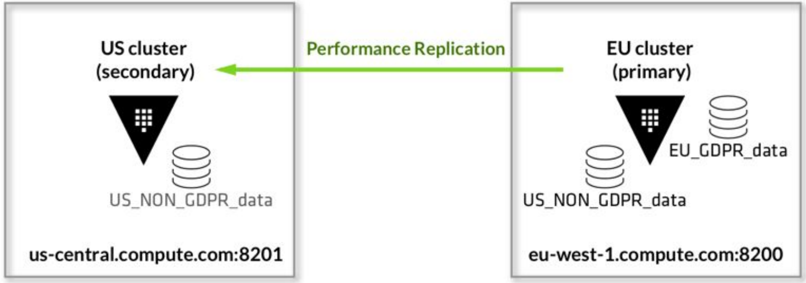
Provides an active Vault cluster with shared state of the primary. This includes secrets, authentication methods, policies, and other shared data. Token and leases are not replicated to performance secondaries.

Vault Replication



Disaster Recovery (DR) Replication

- Achieve RPO/RTO requirements
- Vault is typically considered a Tier 0 application



Performance Replication

- Additional cluster closer to source of requests
- Latency reduction, compliance and data sovereignty
- Segment certain types of workloads

03

Deployment Patterns

Recommended Patterns

Immutable Builds

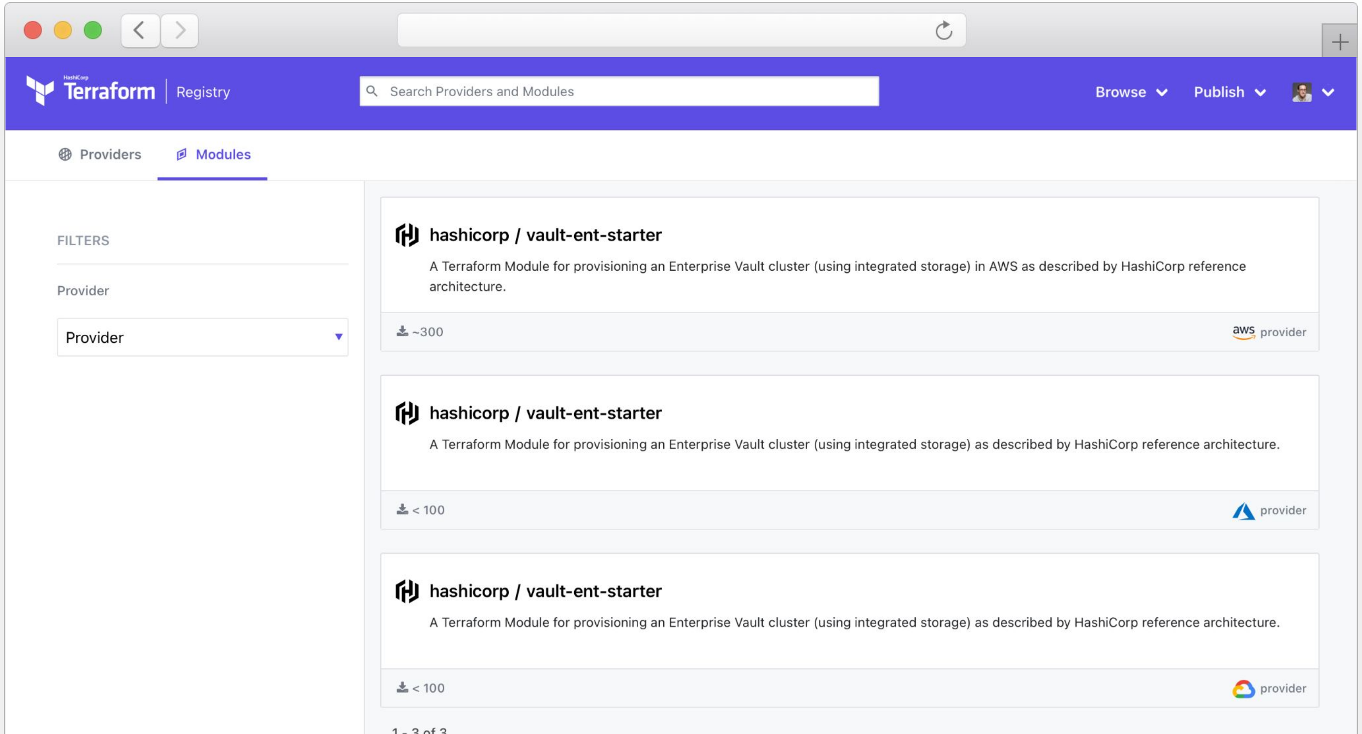
Tooling like Packer can be used to build immutable images of Vault and perform blue/green deployment using your existing CI/CD orchestration. This can streamline your lifecycle processes. However, when using integrated storage, you will need to take measures to ensure quorum is maintained as new image versions are introduced to the cluster.

Configuration Management

For organizations who have not adopted the above pattern, Vault can be integrated into your configuration management patterns to install, upgrade, and configure Vault.

Terraform Modules

Quickly deploy Vault cluster based on reference architecture - link



hashicorp / vault-ent-starter

A Terraform Module for provisioning an Enterprise Vault cluster (using integrated storage) in AWS as described by HashiCorp reference architecture.

~300 — aws provider

hashicorp / vault-ent-starter

A Terraform Module for provisioning an Enterprise Vault cluster (using integrated storage) as described by HashiCorp reference architecture.

< 100 — provider

hashicorp / vault-ent-starter

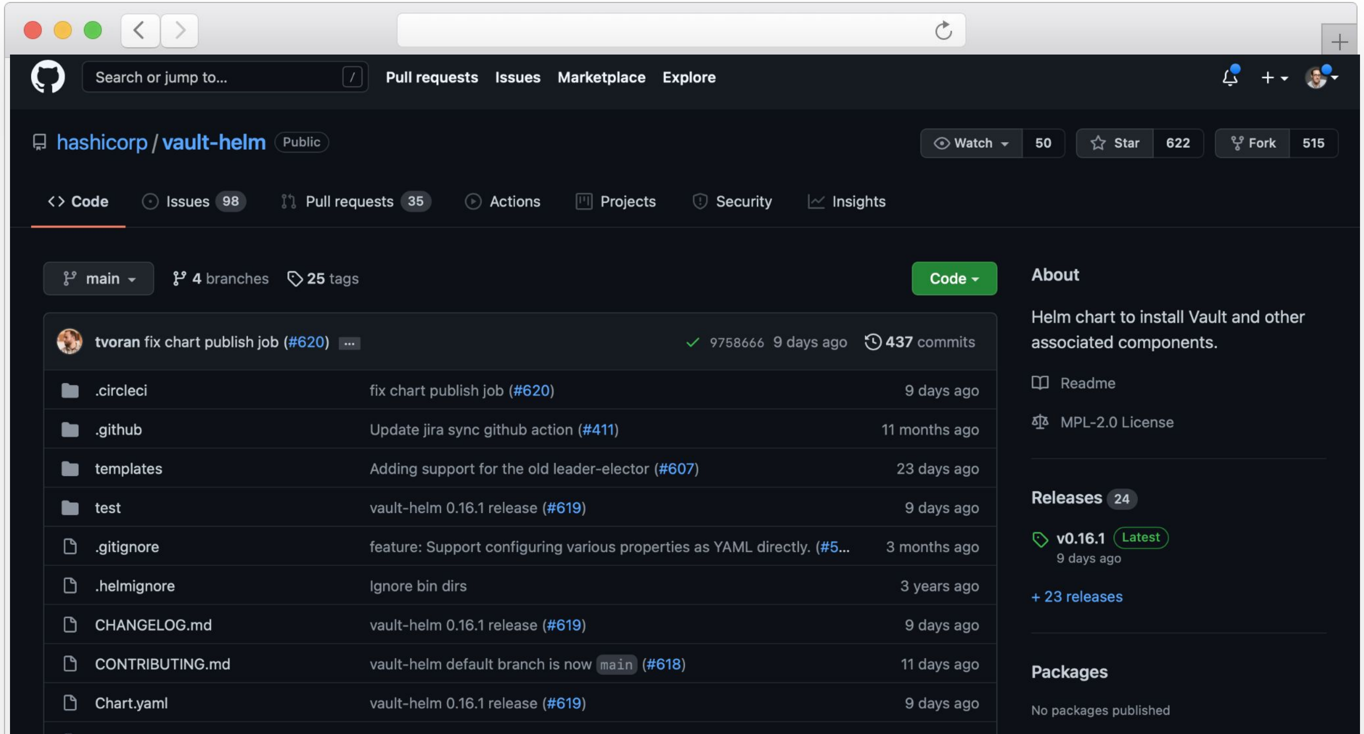
A Terraform Module for provisioning an Enterprise Vault cluster (using integrated storage) as described by HashiCorp reference architecture.

< 100 — provider

1 - 3 of 3

Vault Helm Chart

Deploy Vault Reference Architecture inside Kubernetes



hashicorp / vault-helm Public

4 branches 25 tags

tvoran fix chart publish job (#620) ... ✓ 9758666 9 days ago 437 commits

.circleci	fix chart publish job (#620)	9 days ago
.github	Update jira sync github action (#411)	11 months ago
templates	Adding support for the old leader-elector (#607)	23 days ago
test	vault-helm 0.16.1 release (#619)	9 days ago
.gitignore	feature: Support configuring various properties as YAML directly. (#5...	3 months ago
.helmignore	Ignore bin dirs	3 years ago
CHANGELOG.md	vault-helm 0.16.1 release (#619)	9 days ago
CONTRIBUTING.md	vault-helm default branch is now `main` (#618)	11 days ago
Chart.yaml	vault-helm 0.16.1 release (#619)	9 days ago

About

Helm chart to install Vault and other associated components.

Readme

MPL-2.0 License

Releases 24

v0.16.1 Latest
9 days ago

+ 23 releases

Packages

No packages published

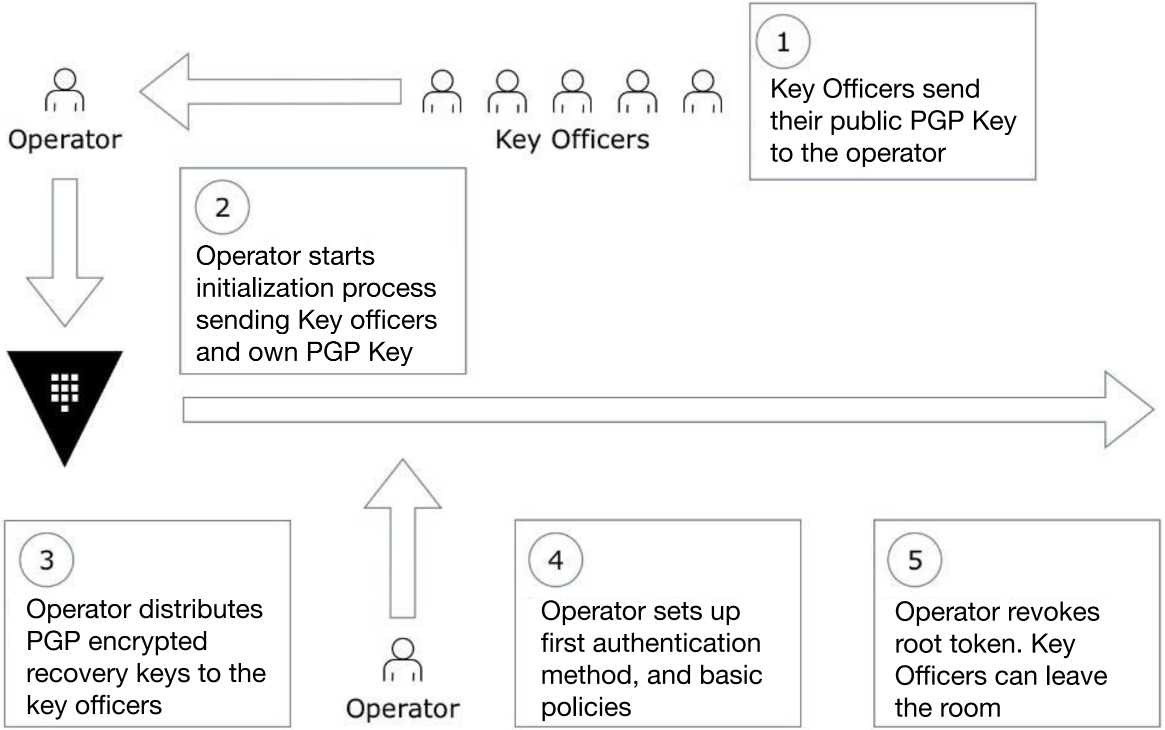
Upgrades

- Major releases of Vault are released quarterly and we release minor releases monthly and as needed
- Major version upgrade 2X per year
- Automate Vault upgrades as much as possible. (i.e. Terraform, and Autopilot)
- Review the Changelog, and version specific upgrade guides, test against version in QA environment and ensure snapshots are up to date

04

Operations

Vault Cluster Initialization



Key Officers send their public PGP Key to the operator

Operator starts initialization process sending Key officers and own PGP Key

Operator distributes PGP encrypted recovery keys to the key officers

Operator sets up first authentication method, and basic policies

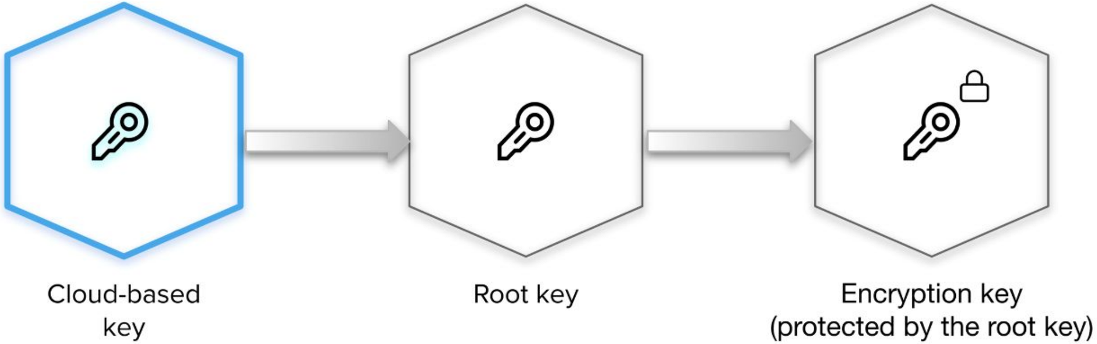
Operator revokes root token. Key Officers can leave the room

Auto-unseal

Unsealing is the process of constructing the master key necessary to decrypt the data encryption key because by default, Vault needs to be unsealed before any operation can be performed.

Vault supports auto-unseal from

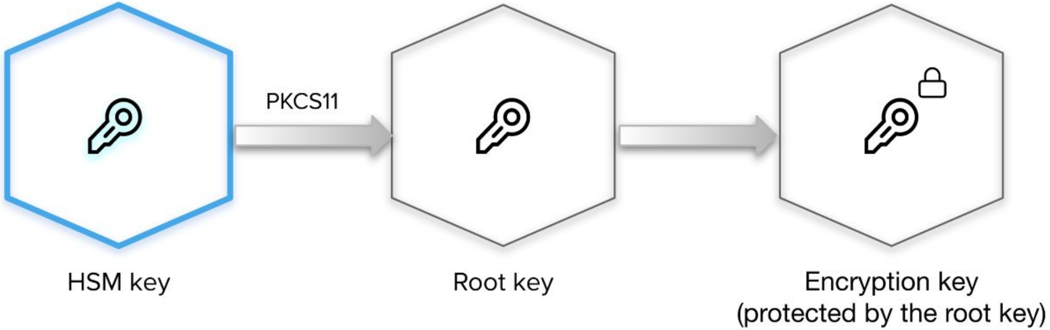
- HSM
- AliCloud KMS
- AWS KMS
- Azure Key Vault
- Google Cloud KMS
- OCI KMS

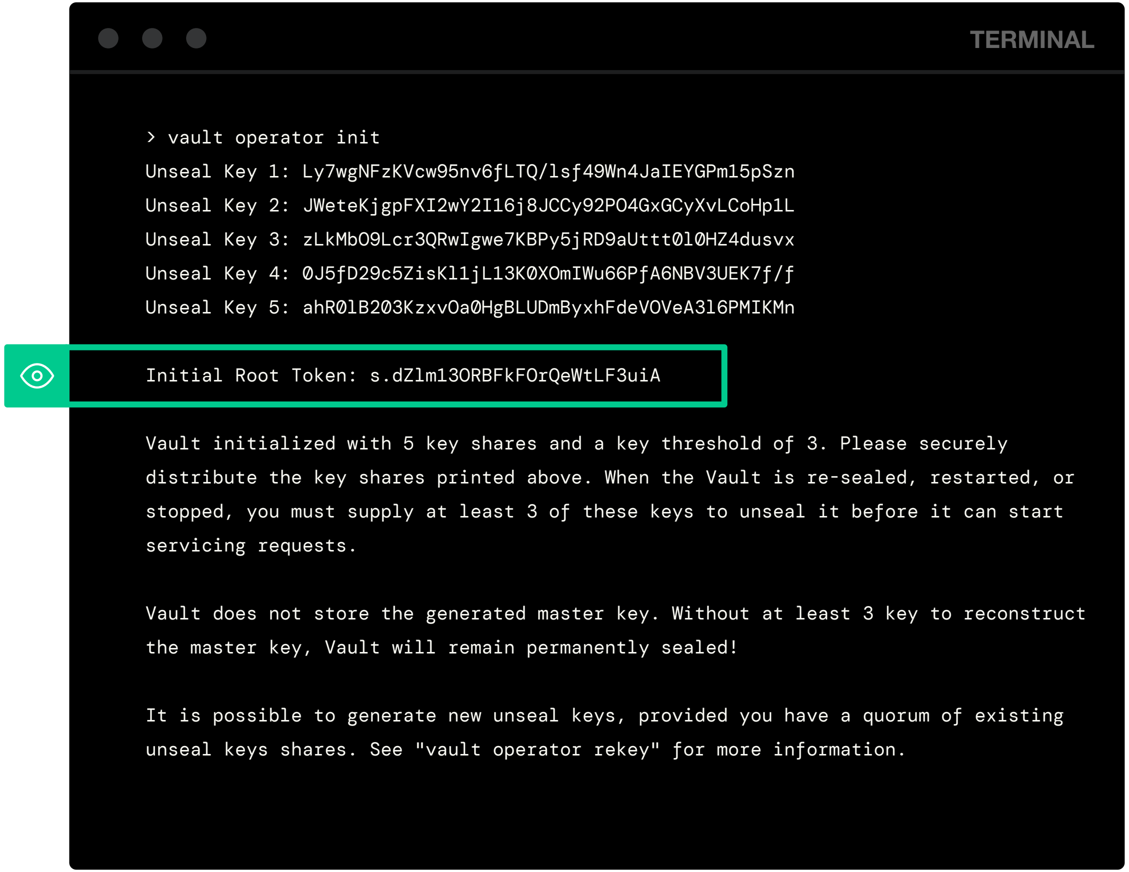


HSM Integration

- Integrate Vault with FIPS 140-2 certified HSM (Hardware Security Module) and enable the Seal Wrap feature to protect your data.

- Vault encrypts secrets using 256-bit AES in GCM mode with a randomly generated nonce prior to writing them to its persistent storage. When you enable seal wrap, Vault wraps your secrets with an extra layer of encryption leveraging the HSM encryption and decryption.





```
> vault operator init
Unseal Key 1: Ly7wgNFzKVcw95nv6fLTQ/lsf49Wn4JaIEYGPm15pSzn
Unseal Key 2: JWeteKjgpFXI2wY2I16j8JCCy92PO4GxGCyXvLCoHp1L
Unseal Key 3: zLkMbO9Lcr3QRwIgwe7KBPy5jRD9aUttt0l0HZ4dusvx
Unseal Key 4: 0J5fD29c5ZisKl1jL13K0XOmIWu66PfA6NBV3UEK7f/f
Unseal Key 5: ahR0lB203KzxvOa0HgBLUDmByxhFdeVOVeA3l6PMIKMn

Initial Root Token: s.dZlm13ORBFkFOrQeWtLF3uiA

Vault initialized with 5 key shares and a key threshold of 3. Please securely
distribute the key shares printed above. When the Vault is re-sealed, restarted, or
stopped, you must supply at least 3 of these keys to unseal it before it can start
servicing requests.

Vault does not store the generated master key. Without at least 3 key to reconstruct
the master key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum of existing
unseal keys shares. See "vault operator rekey" for more information.
```

Root Token Generation

Root Token Handling Practices

The root token is returned to the operator during the initialization ceremony. This token can do **anything** in Vault and its usage should be closely monitored.

- Once operator has configured a secondary authentication method and granted administrators sudo access, almost all operations can be performed
- Best practice is **NOT** persisting the root token
- Generate a root token only when absolutely necessary

Production Readiness

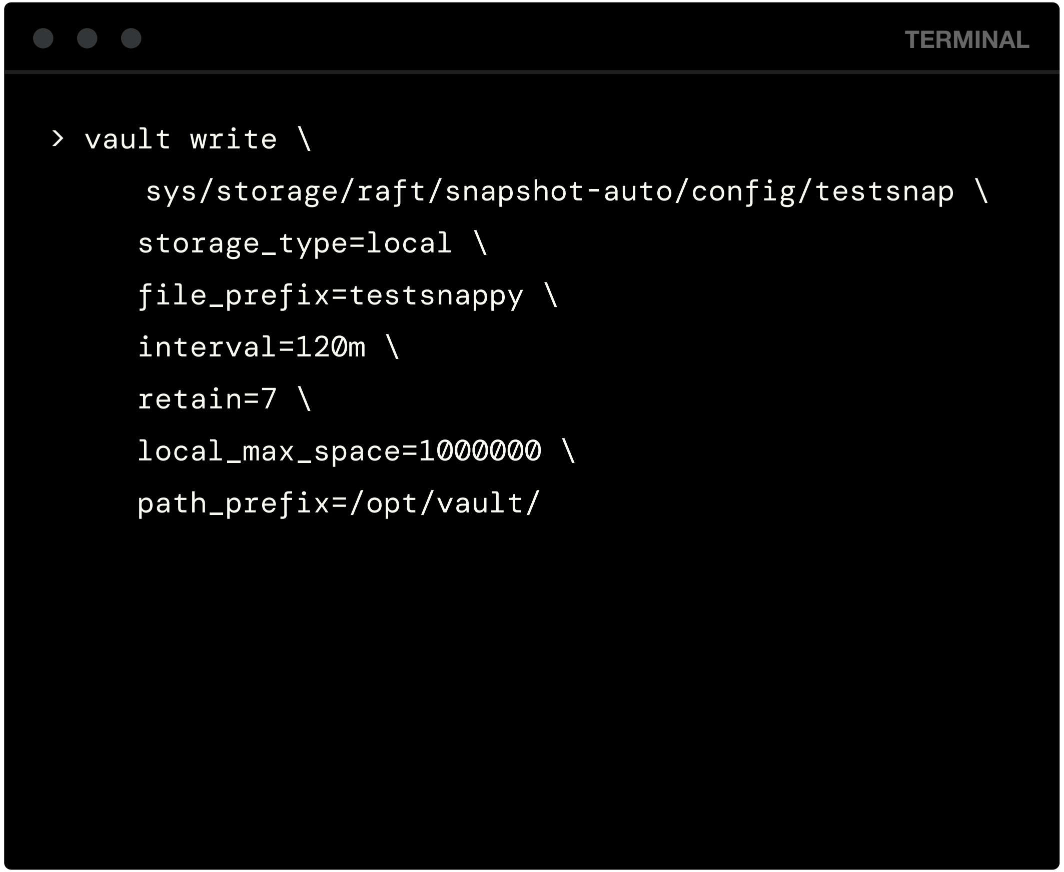
Critical items to have in place before production go-live

Backup

Automated Integrated Storage Snapshots, a Vault Enterprise feature takes periodic snapshots of Vault's data data

- Determine where snapshot files will be stored
- Configure based off your RPO/RTO requirements
- If snapshot is restored, the unseal keys that were valid at the time of the snapshot will be used to unseal

Automated Integrated Storage Snapshots



```
> vault write \
       sys/storage/raft/snapshot-auto/config/testsnap \
      storage_type=local \
      file_prefix=testsnappy \
      interval=120m \
      retain=7 \
      local_max_space=1000000 \
      path_prefix=/opt/vault/
```

Production Readiness

Critical items to have in place before production go-live.

Monitoring

Vault should be monitored closely to ensure the service remains healthy and available in production

- Telemetry - Export telemetry data to solution that can analyze and identify trends overtime
- Log Analytics - Capture app logs and system logs and perform analysis on the log files for useful signals
- Active Health Checks - Query health endpoints to get the health of nodes and route traffic to active node

Production Readiness

Critical items to have in place before production go-live.

Auditing

Vault sends audit information to a SIEM system or logging backend

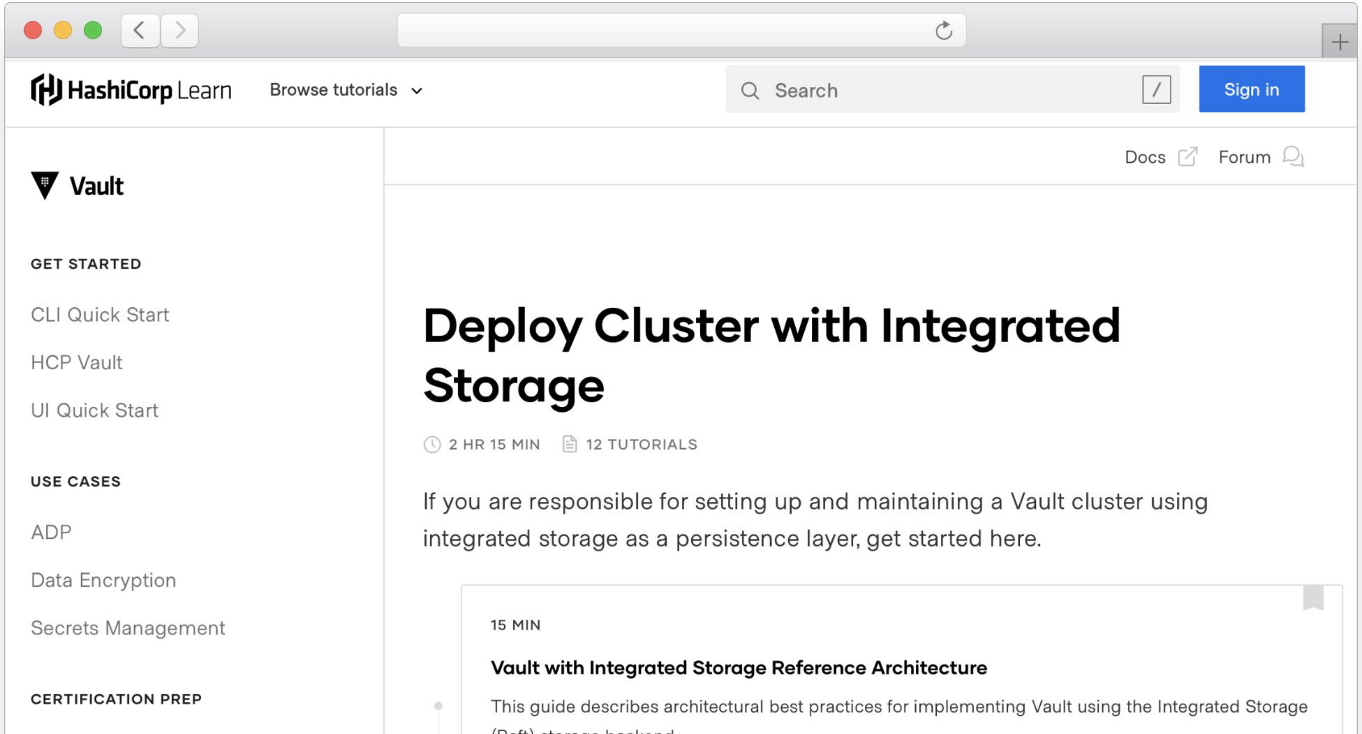
- Determine audit devices that will be used
- Vault will not respond if the audit device is unavailable, use multiple audit devices to ensure Vault remains available
- Sensitive fields are HMAC, Selectively determine if any HMAC fields need to be exposed

05

Next Steps

Learn

Step-by-step guides to accelerate deployment of Vault



Deploy Cluster with Integrated Storage

2 HR 15 MIN 12 TUTORIALS

If you are responsible for setting up and maintaining a Vault cluster using integrated storage as a persistence layer, get started here.

15 MIN

Vault with Integrated Storage Reference Architecture

This guide describes architectural best practices for implementing Vault using the Integrated Storage (Raft) storage backend.

Resources

- Vault Internal Architecture
- Vault Security Model
- Vault Reference Architecture
- Vault Redundancy Zones (1.11.0+)
- Terraform Starter Code
- Disaster Recovery Replication Setup
- Performance Replication Setup
- Vault Eventual Consistency and Controls

Need Additional Help?

Customer Success

Contact our Customer Success Management team with any questions. We will help coordinate the right resources for you to get your questions answered.

customer.success@hashicorp.com

Technical Support

Something not working quite right? Engage with HashiCorp Technical Support by opening a ticket for your issue at support.hashicorp.com.

Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

discuss.hashicorp.com

Up Next…

- Webinar: Vault Namespaces, Authentication Methods, and Policy Basics

Q & A

Thank You

customer.success@hashicorp.com
www.hashicorp.com