HashiCorp Vault

Vault Installation Planning & Architecture

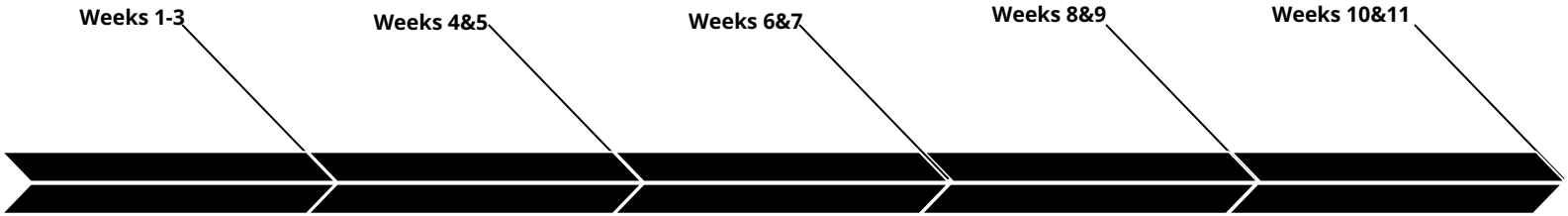
October 2021

Copyright © 2021 HashiCorp

Agenda

- Vault Installation Planning
- Vault Architecture
- Preparing for Success

Vault Enterprise Path to Production



Vault cluster deployed

- Kick Off Webinar
- Architectural Deep Dive Workshop
- Terraform starter code modules
- Office Hours
- Schedule Success Planning Session

Identity & Access Management configured

- Auth Methods, Namespaces, Policies Workshop
- Office Hours
- 1:1 Success Planning

Telemetry & Disaster Recovery instantiated

- Telemetry & Monitoring and DR Operations Workshop
- HCDiag & Vault Metrics Lunch & Learn
- Office Hours
- 1:1 Success Planning

Secrets Management

- How to consume Vault into applications Workshop
- Dynamic Secrets Lunch & Learn
- Office Hours
- 1:1 Success Planning

Vault Ready for Production!

- Success Plan Reviews
- Exit Ramp & Operational Readiness Workshop

Vault Installation

What do we need to decide?

1

Cluster Storage Technology

Vault Enterprise supports two storage backends.

- **Integrated Storage**
- **Consul Storage**

These are the 2 supported enterprise storage backends. If using non-supported backends with a Vault OSS cluster then migration to one of theses backends should be included in the project plan.

2

Installation Location

Where will Vault be installed:

- **On-Premise Data Center**
- **Cloud Provider**

Vault supports installation in:

- **Physical and Virtual Machines**
- **Containers**
- **Kubernetes**

© 2021 HashiCorp

Cluster Storage

Integrated Storage vs. Consul

Integrated storage eliminates the need for external storage; therefore, Vault is the only software you need to stand up a cluster.

The fundamental difference between Vault's integrated storage and Consul is that Consul KV stores everything in memory while integrated storage stores everything on disk.

Reference Architecture - Consul Storage

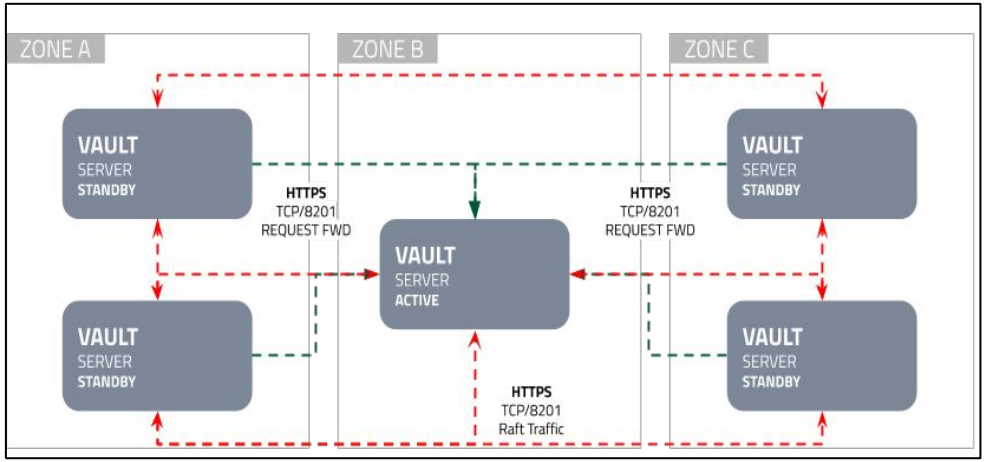
© 2021 HashiCorp

Recommended Solution - Integrated Storage

5 Vault Servers

This design is fault tolerant and scalable across multiple workloads. This solution has an n-2 at the node level for Vault and an n-1 at the Availability Zone level and as such is considered the most resilient of all architectures for a single Vault cluster with integrated storage backend.

Reference Architecture - Integrated Storage



© 2021 HashiCorp

Installation Location

Physical or Virtual Machine

This is the recommended installation pattern for the vast majority of customers. The Vault security model is prescriptive around creating a robust system to prevent attempts to bypass it's access controls.

Instance sizing recommendations are listed in the reference architecture.

The Terraform Registry has published starter code packs for the AWS, Azure, and GCP to kickstart installation.

Container

Vault can be installed into a container that has persistent storage and provisioned IOPS.

Instance sizing recommendations are the same as when installing on VMs.

The Vault Enterprise image on Docker Hub is available if using a container deployment pattern.

Kubernetes

HashiCorp has an officially supported Helm Chart for Vault that is the recommended way to install Vault on Kubernetes.

Kubernetes installation should be considered only if all workloads and applications that will access Vault are installed exclusively in Kubernetes. If any applications or workloads reside elsewhere the VM installation is the preferred deployment pattern for Vault.

HashiCorp Learn - Vault and Kubernetes

© 2021 HashiCorp

Preparing for Success

Use Cases

- Vault will be used for Secrets Management
  - How is this solved for currently?
  - What is the key driver for the change?

- How will Vault be accessed/interacted with?
  - Sporadic access? Continuous access?
  - API? CLI? UI?

- What is the rollout plan?
  - What is the first use case that will be brought onboard?
  - Is a managed service being created?

Auth Methods

Human & Machine implementations for authenticating to Vault.

AppRole	Kerberos
AliCloud	Kubernetes
AWS	LDAP
Azure	Oracle Cloud
Cloud Foundry	Okta
Github	RADIUS
Google Cloud	TLS Certificates
OIDC	Username & Password

+ Custom Plugins

Secret Engines

Custom logic for handling secrets

Active Directory	Key/Value
AliCloud	Nomad
AWS KMS	OpenLDAP
Azure Key Vault	PKI
K8S CSI Provider	SSH
Consul	Terraform Cloud
Cubbyhole	TLS Certificates
Databases	TOTP
Secrets Manager for GCP	Transform
Key Management	Transit
KMIP	Venafi

+ Custom Plugins

Architecture

- Where will Vault be deployed?
- Where will the users be accessing this Vault from?
- What are the target Disaster Recovery RPO and RTO?
- Are there any noteworthy regulatory constraints in the environment that need to be considered?

Success Metrics

- What are the short term goals for the rollout of Vault?
  - What are the must-haves?
  - What metrics are being used to gauge the success of this project?

- What are the longer term goals for the rollout of Vault?
  - Are there particular features that are planned to be adopted?
  - Are there particular business problems that Vault is going to solve?

Thank you

The Customer Success Team
www.hashicorp.com/customer-success