



Vault Onboarding Program

Kickoff and Architectural Quickstart

COBRA Team | HashiCorp Customer Success



Agenda

- Welcome
- Customer Success
- Customer Support
- Vault Installation Planning
- Preparing for Success
- Next Steps



Code of Conduct



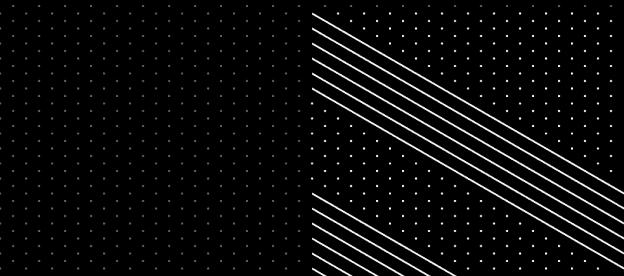
HashiCorp is dedicated to providing a harassment-free Vault Enterprise onboarding experience for everyone, regardless of gender, gender identity, sexual orientation, disability, physical appearance, body size, race, national origin, or religion. We value your attendance and do not wish anyone to feel uncomfortable or threatened at any time.

The bottom line is that we do not tolerate harassment of conference participants in any form. Harassment includes but is not limited to offensive verbal comments related to gender, gender identity, sexual orientation, disability, physical appearance, body size, race, national origin, religion; sexual or inappropriate images in public spaces; deliberate intimidation; stalking; trolling; sustained disruption of talks or other events; and unwelcome sexual attention. Participants asked to stop any harassing behavior are expected to comply immediately. If you are being harassed, notice that someone else is being harassed, or have any other concerns, please let the HashiCorp event representative know immediately or email customer.success@hashicorp.com.



-

HashiCorp Customer Success



HashiCorp Customers



FINANCIAL SERVICES



ENTERTAINMENT & TELCO



MANUFACTURING & LOGISTICS



SOFTWARE & TECHNOLOGY



INSURANCE & HEALTH





-

How We Engage





Customer Success Managers



Strategic Relationship Management

Engagement to ensure product & operational success including risk mitigation towards business outcomes



Customer Journey Delivery

Focus on solution value realization, driving organizational adoption and providing HashiCorp Best Practices



Trusted Advisor & Advocate

Proactive advisory services and program coordination across all functional areas within HashiCorp (Sales, Engineering, Support, Product, and more)





Solution Architecture Specialists



Product Experts

Subject matter expert on HashiCorp products as well as integration points with third-party platforms and tools.



Prescriptive Guide

High-value, prescriptive guidance on how to adopt HashiCorp products and consultation on the unique integration requirements of each customer.



Technical Advisors

Ongoing advisor on HashiCorp products and the integration with complimentary technologies. As customers evolve, providing highly relevant guidance based on the specific customer needs and value-based outcomes.



Keys to Success

Partnering to Drive Value Realization



Training Consumption

Ensure team members consume training resources in a timely fashion.



Use Case Guidance

Provide timely information on use case designs.



Project Team Participation

Inclusive of any stakeholder required for successful completion of onboarding.



Single Point of Contact

Main contact for decision making.



Escalation Process

Understanding of escalation process.



Change Control Process

Understanding of change control process.

Customer-Centric Communications



Making Communications Easy



Support



Email

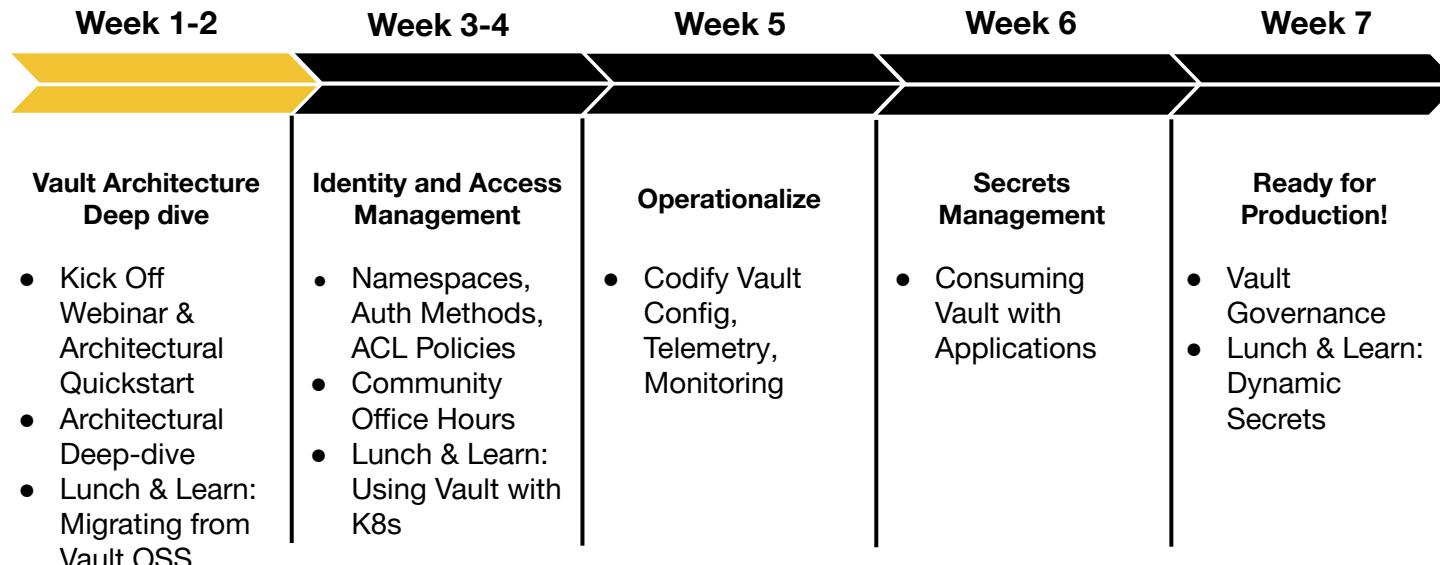


Webinars



Phone/Video

Vault Enterprise Path to Production





Onboarding Checklist

Our objective is to make you successful with our products and see value within 90 days



Vault Installed

- Vault Enterprise installed in your environment
- Basic configuration completed
- Telemetry and Monitoring in place
- Disaster Recovery replication in place



Vault Operational

- First use case (application) onboarded and consuming secrets stored in Vault
- A roadmap created for onboarding additional use cases



Completed within 90 days

COBRA Vault Onboarding Journey



- Week 1 - Kickoff - Program Intro & Architectural Quickstart
- [Week 2 - Webinar - Architectural Deep Dive](#)
- Week 3 - Lunch & Learn - Migrating from Vault OSS to Enterprise
 - Webinar - Auth Methods, Namespaces, Policies
- [Week 4 - Lunch & Learn - Using Vault with Kubernetes](#)
 - [Community Office Hours](#)
- Week 5 - Webinar - Vault Operations Basics & Best Practices
- [Week 6 - Webinar - Consuming Vault with your applications](#)
- Week 7 - Lunch & Learn - Dynamic Secrets
 - Webinar - Vault Governance



-

Customer Support

SLA, Contact Methods, Services, etc.





Contacting Support

There are two ways to contact our support team

1) **Support Portal:** Open a ticket through [our support portal](#)

- Once customer access is setup, authorized users can submit a ticket using the email address they provided us
- The portal provides faster routing via product and sub-product selection, the ability to send encrypted attachments, and set ticket priority

2) **Email Support:** Send an email to support@hashicorp.com

- All emailed support tickets default to “normal” priority - and cannot be changed

HashiCorp Support SLA



This info can also be accessed from our [Support SLA Page](#)

BRONZE

SILVER

GOLD

Hours of availability		N/A	9-5, Monday - Friday US LOCAL TIME EUROPEAN CENTRAL TIME AUSTRALIA EASTERN TIME	24 X 7 (SEV-1 URGENT)
SEVERITY 1	FIRST RESPONSE	N/A	4 business hours	60 minutes
	UPDATE FREQUENCY	N/A	8 business hours	4 hours
SEVERITY 2	FIRST RESPONSE	N/A	8 business hours	4 business hours
	UPDATE FREQUENCY	N/A	2 business days	8 business hours
SEVERITY 3	FIRST RESPONSE	N/A	24 business hours	8 business hours
	UPDATE FREQUENCY	N/A	5 business days	3 business days
SEVERITY 4	FIRST RESPONSE	24 business hours	24 business hours	24 business hours
	UPDATE FREQUENCY	Reasonable best effort	Reasonable best effort	Reasonable best effort
Technical contacts allowed		2	3	4



Severity Definitions

Sev-1 (Urgent)	A Sev-1 incident is an operational outage as defined below: Any error reported by customer where majority of the users for a particular part of the software are affected, the error has high visibility, there is no workaround , and it affects the customer's ability to perform its business .
Sev-2 (High)	Any error reported by customer where the majority of the users for a particular part of the software are affected, the error has high visibility, a workaround is available ; however, performance may be degraded or functions limited and it is affecting revenue .
Sev-3 (Normal)	Any error reported by customer where the majority of the users for a particular part of the software are affected, the error has high visibility, a workaround is available; however, performance may be degraded or functions limited and it is NOT affecting revenue.
Sev-4 (Low)	Any error reported by customer where a single user is severely affected or completely inoperable or a small percentage of users are moderately affected or partially inoperable and the error has limited business impact.

This info can also be accessed at the bottom of our [Support SLA Page](#)

Vault Enterprise Installation Planning





Vault Installation

What do we need to decide?

1

Cluster Storage

Vault Enterprise supports:

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

Migration to supported storage needs to be included in project planning if using other storage

2

Installation Location

Where will Vault be installed?

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

3

Vault Runtime

Vault supports installation in:

- **Physical & Virtual Machines**
- **Containers**
- **Kubernetes**



Cluster Storage

Integrated Storage vs. Consul

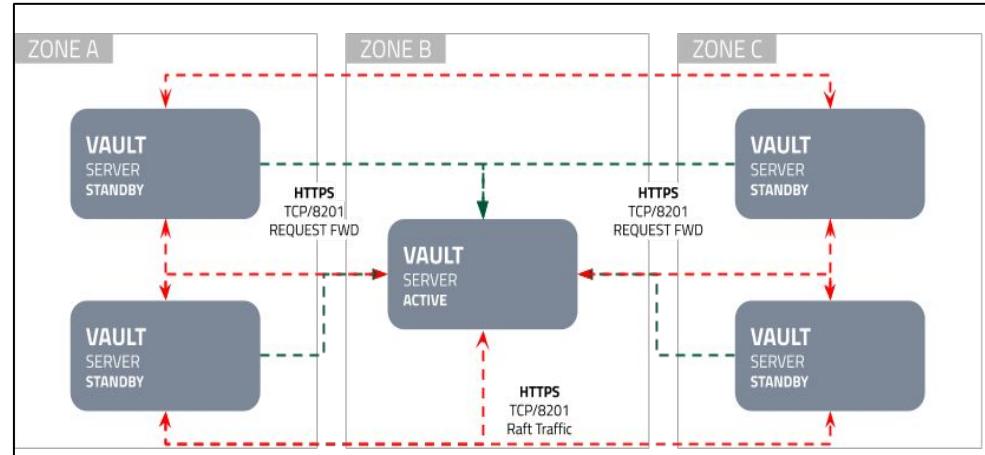
- Integrated storage eliminates the need for external storage; Vault is the only software needed to stand up a cluster
- Basic differences:
 - Consul - everything in memory (in memory database)
 - Integrated Storage - everything on disk
- Reference Architecture
 - [Consul Storage](#)
 - [Integrated Storage](#)

Recommended Solution - Integrated Storage



5 Vault Nodes

- Fault tolerant and scalable across multiple workloads
- N-2 resiliency Vault node level
- N-1 resiliency Availability Zone level



Installation Location & Runtime



- **Cloud Provider**
Terraform [starter code packs](#) for [AWS](#), [Azure](#), and [GCP](#) to kickstart installation
- **On-Premise Data Center**
- **Physical or Virtual Machine**
Recommended installation pattern for most deployments
- **Container**
[Vault Enterprise](#) image on Docker Hub
- **Kubernetes**
[Helm Chart](#) is recommended deployment pattern

Vault Runtime

Physical Hardware or Virtual Machine

- Recommended installation pattern
- The [**Vault security model**](#) is prescriptive around creating a robust system to prevent attempts to bypass its access controls
- Instance sizing recommendations listed in [**reference architecture**](#)

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

Kubernetes

- Kubernetes installation should be considered **only if all workloads and applications** that will access Vault are installed in Kubernetes
- VM installation is the preferred if any applications reside outside Kubernetes
- [**HashiCorp Developer - Vault & Kubernetes**](#)

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?

Next Steps



Upcoming Webinars



Architectural Deep Dive

Take a deep dive into best practices for architecting and deploying your Vault clusters including Enterprise DR and Replication best practices.

Migrating from Vault OSS to Enterprise

This Lunch & Learn (separate link) covers the best methods for upgrading an existing Vault OSS Cluster to Vault Enterprise

Auth Methods, Namespaces & Policy

Learn best practices for deploying Vault Namespaces, Authentication Methods, and Vault policy.

Action Items



- Identify your use case(s) and define your goals and project milestones with Vault Enterprise
- Share to customer.success@hashicorp.com
 - Authorized technical contacts for support
 - Stakeholders contact information (name and email addresses)
- Gather requirements and complete 3 critical decisions:
 - Cluster storage
 - Installation location
 - Cluster runtime

Q & A





Thank You

customer.success@hashicorp.com
www.hashicorp.com/customer-success