

Vault Onboarding Program Closing Thoughts

COBRA Team | HashiCorp Customer Success



Agenda



Onboarding Program Recap

Look back at what we've accomplished the last 7 weeks



Production Readiness

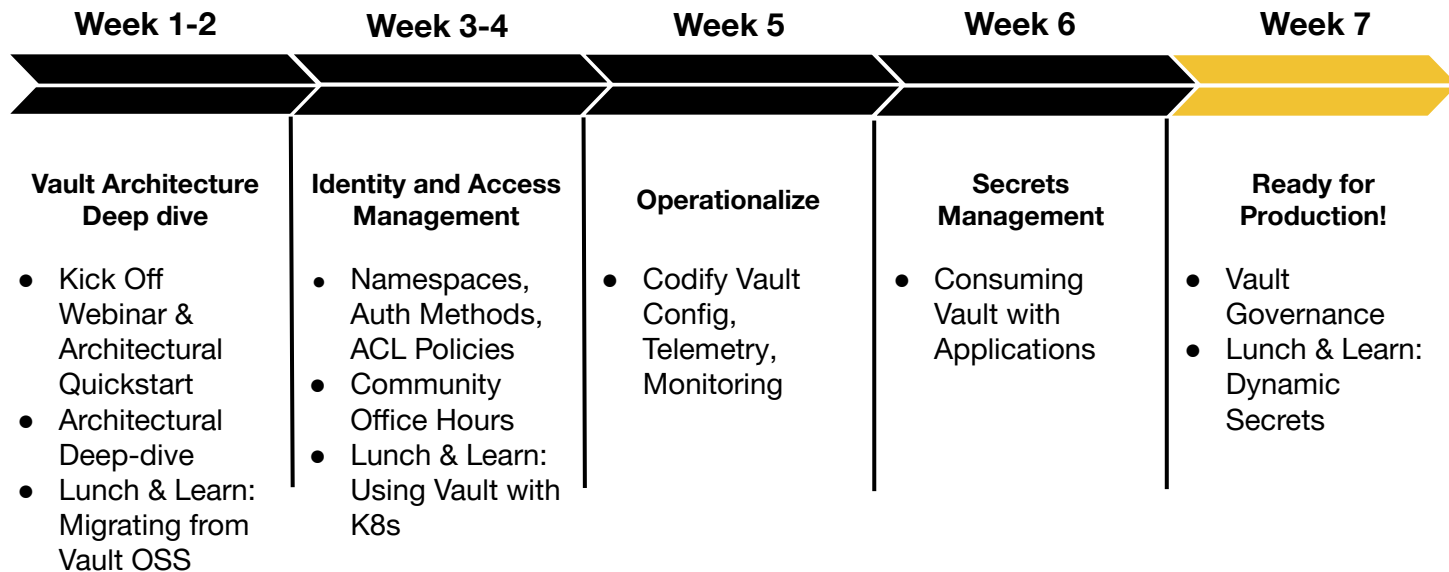
Vault Production Checkpoints



Exit Program Resources

Resources to support your post-program journey

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

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



Completed within 90 days



Vault Enterprise Production Readiness



Vault Production Readiness



Subscribe to release notifications:

<https://groups.google.com/g/hashicorp-announce>

☆ HashiCorp Announcements

[Join group](#)

1-30 of 282 < >

Welcome to the HashiCorp Announcement list!

On this list you will receive high-priority, low-volume announcements about HashiCorp products, including release information and security bulletins. Posting is reserved for HashiCorp staff only; for discussion about specific tools, please use the corresponding list.

As a reminder, if you wish to contact us regarding any security-sensitive matter, please responsibly disclose by emailing security@hashicorp.com. PGP information can be found at <https://www.hashicorp.com/security.html>.



	lu...@hashicorp.com	[ANN] Nomad 1.2.4, 1.1.10, and 1.0.16 Released — Nomad 1.2.4, 1.1.10, a...	Jan 19	☆
	jba...@hashicorp.com	Terraform CLI v1.1.3 Released — Today we release Terraform CLI v1.1.3. T...	Jan 6	☆
	meg...@hashicorp.com	Vault 1.9.2 released! — Hi folks, The Vault team is announcing the release ...	12/21/21	☆
	meg...@hashicorp.com	Vault 1.8.7 released! — Hi folks, The Vault team is announcing the release ...	12/21/21	☆
	meg...@hashicorp.com	Vault 1.7.8 released! — Hi folks, The Vault team is announcing the release ...	12/21/21	☆
	Krista LaFentes	Terraform CLI v1.1.1 released — Hello everyone! Today we released Terraf...	12/15/21	☆
	tgr...@hashicorp.com	Nomad 1.2.3 released — Nomad 1.2.3 Security Release Nomad 1.2.3 has b...	12/13/21	☆



Vault Production Readiness



Join security & vulnerability announcements list

<https://discuss.hashicorp.com/c/security/52>

HashiCorp | Discuss

Sign in



Now open: CFP & Registration for HashiTalks 2022. Sign up today to join us for 24-hours of knowledge-sharing: hashi.co/hashitalks-2022-discuss

Security ▾ Security-Vault ▾ | Latest Top

Topic	Replies	Views	Activity
HCSEC-2021-34 - Vault, Consul, Boundary, and Waypoint Affected By Denial of Service in Golang's net/http (CVE-2021-44716) Security security-vault, security-consul, security-waypoint, security-boundary	0	487	Dec '21
HCSEC-2021-33 - Vault's KV Secrets Engine With Integrated Storage Exposed to Authenticated Denial of Service Security security-vault	0	487	Dec '21
HCSEC-2021-30 - Vault's Templated ACL Policies Matched First-Created Alias Per Entity and Auth Backend Security security-vault	1	983	19d



Vault Production Readiness



- Architecture and Infrastructure
- Vault Operations and Infrastructure Security
- Business Continuity
- Vault Policy and Configuration



Vault Production Readiness



● Architecture and Infrastructure

- Is the cluster architecture aligned with the reference architecture?
 - [Consul Storage Reference Architecture](#)
 - [Integrated Storage Reference Architecture](#)
 - Are the nodes configured across multiple AZs / failure zones to provide resilience in accordance with your uptime requirements?
 - Are the [nodes sized appropriately \(RAM and CPU\)](#)?
 - Does the cluster have provisioned IOPS (Integrated Storage)?
- Is there less than 8 milliseconds of latency between Vault servers?



Vault Production Readiness



● Architecture and Infrastructure - continued

- Have high availability best practices been followed?
 - Has a process been identified and implemented to handle the lifecycle of the TLS certificates used on Vault Server listeners and load balancers?
 - How is DNS Implemented? Are appropriate TTL's configured that allow for failover that meet RTO Objectives
 - What is the validity period of TLS certificates? Is it rational?
 - Does the load balancer configuration follow [best practices](#), is TLS terminated on the Vault cluster?
 - Is the renewal reminder for TLS certificates a scalable process, i.e. more than a calendar entry in a single location?



Vault Production Readiness



● Vault Operations and Infrastructure Security

- Is root token creation restricted and monitored?
- Does the team managing Vault have runbooks and processes for all key administrative tasks?
 - Upgrading Vault
 - Executing DR failovers in Vault
 - Reissuing unseal/recovery key shares
 - Rotating Vault's master encryption key
 - Rotating any auto-unseal/seal-wrap mechanism key (if applicable)
 - Generating root tokens
- Have the [production hardening recommendations](#) been reviewed and implemented in the environment?
- Is the running version of Vault currently supported? N-2 window from [latest release](#)?



Vault Production Readiness



● Business Continuity

- Have runbooks been created and tested to validate the ability to meet the Recovery Time Objective?
 - Have [snapshots been enabled](#) in alignment with the desired Recovery Point Objective?
 - Has [recovery from a snapshot](#) been tested and the process documented?
 - Is there alerting in place if snapshots fail?
- Have alerts been created on the following parameters?
 - Disk space alerting on instance
 - Disk space alerting on audit points
 - Log monitoring/alerting for warn/errors
 - Draught/absence alerts on log outages/stoppages
 - RAM utilization alerting
 - CPU utilization alerting



Vault Production Readiness



● Vault Policy and Configuration

- Are policies least-privilege?
- Are policies tested in a negative fashion, ie, ensure that a token with this policy can do what it allows but also prevents more access than intended?



Content & Resources

COBRA Vault Onboarding Journey



- [Kickoff & Architectural Quickstart](#) - password: 8NVuDb
- [Webinar - Architectural Deep Dive](#) - password: fptjgznsmo
- [Webinar - Namespaces, Authentication, and Policies](#) - password: TbYyxt
- [Webinar - Operating Vault](#) - password: KX3rHv
- [Webinar - Consuming Vault](#) - password: 5B8rdK
- [Webinar - Vault Governance](#) - password: j4uTsP
- [Lunch and Learn - Migrating from OSS](#) - password: yTAK4u
- [Lunch and Learn - Dynamic Secrets](#) - password: FufQcR
- [Lunch and Learn - Using Vault with Kubernetes](#) - password: 6evnMW

[All program materials](#)



Additional Resources

- [Production Readiness Checklist](#)
- [HashiCorp Vault Adoption Guide](#)
- [How to Adopt a Producer-Consumer Model for Vault](#)
- [Running Vault in Production \(book\)](#)
- [HashiCorp Academy \(Training\)](#)





Additional Training Resources

Wanting to Learn More? A Topic Not Covered?

HashiCorp Developer Page

Self guided tutorials that include guidance on best practices and operating productions systems <https://developer.hashicorp.com/vault/tutorials>

Discuss for Vault - <https://discuss.hashicorp.com/c/vault>

Great place for best practices, finding similar configuration questions

HashiCorp Vault Certification

Even if you don't want the certification, the [Study Guide](#) is a relevant and useful curriculum to follow especially for folks new to Vault



Thank You

customer.success@hashicorp.com

www.hashicorp.com/customer-success