



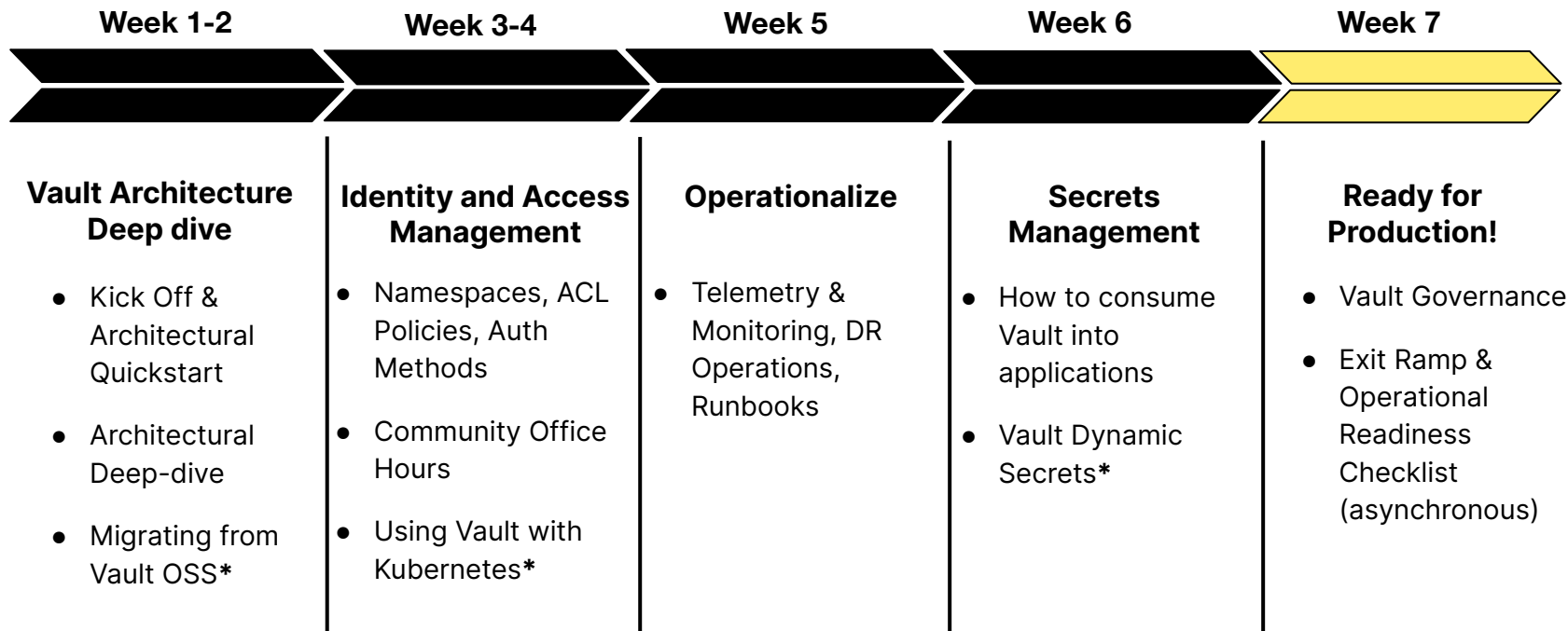
Vault Onboarding Program Closing Thoughts



Vault Onboarding Program

A 7 week guided community environment

Assisting customers with onboarding and adoption



Agenda

Onboarding Program Recap 01

Production Readiness 02

Content & Resources 03

01

Onboarding Program Recap

Onboarding Checklist



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

02



Production Readiness

Production Readiness

[Subscribe to release notifications](#)

☆ HashiCorp Announcements [Join group](#)









1-30 of 344 < >

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.

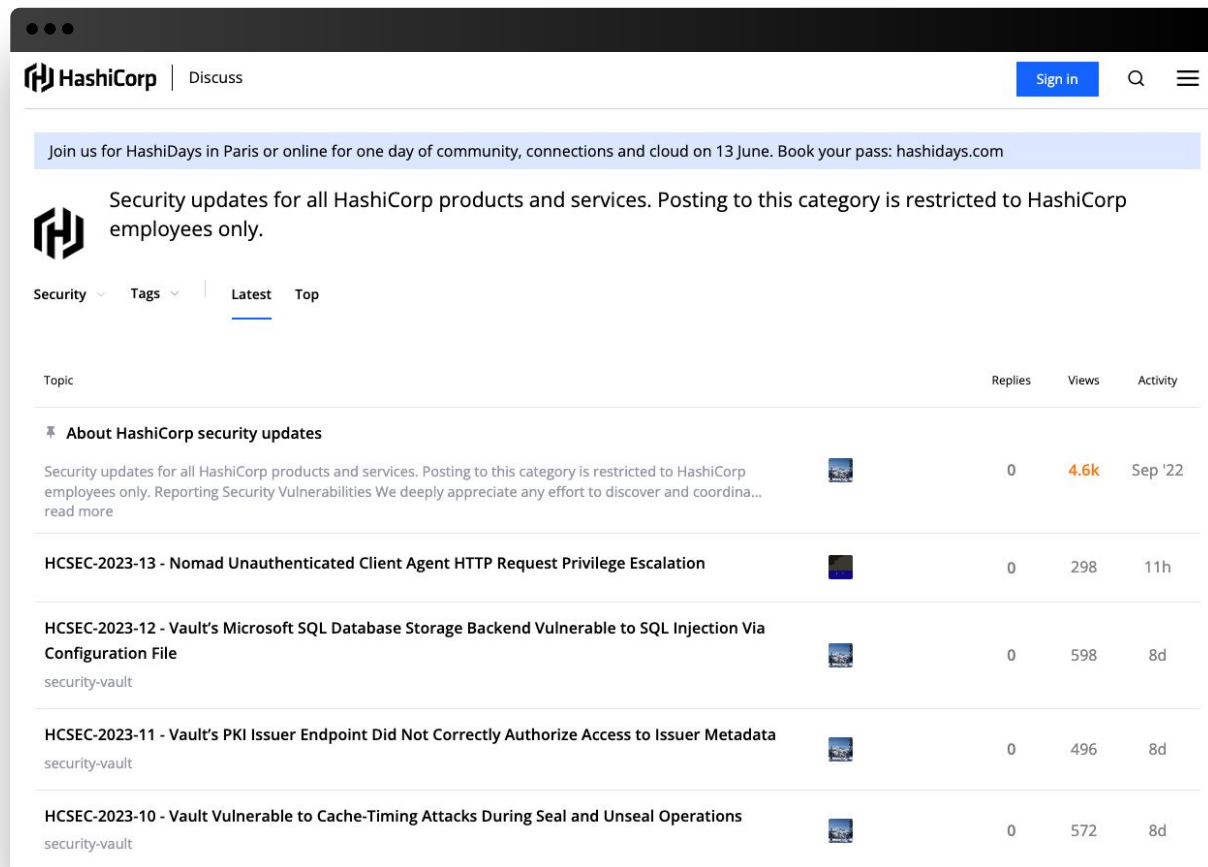
As a reminder, if you wish to contact us regarding any security-sensitive matter, please responsibly disclose by emailing security@hashicorp.com. PGP information can be found at <https://www.hashicorp.com/security.html>.

Thank you for joining the list!

	Tim Gross	Nomad 1.5.3, 1.4.8, 1.3.13 released — Nomad 1.5.3, 1.4.8, and 1.3.13 hav...	Apr 5	☆
	Alisdair McDiarmid	Terraform v1.4.3 and v1.4.4 released — Hi all, Terraform v1.4.3 and v1.4....	Mar 30	☆
	Tony Wittinger	Vault 1.13.1, 1.12.5, and 1.11.9 released! — Hi folks, The Vault team is an...	Mar 29	☆
	Michael Schurter	Nomad 1.5.2, 1.4.7, and 1.3.12 released — Nomad 1.5.2, 1.4.7, and 1.3.1...	Mar 22	☆
	Katy Moe	Terraform v1.4.2 released — Dear all, Terraform v1.4.2 is released. This p...	Mar 16	☆
	Katy Moe	Terraform v1.4.1 released — Dear all, Terraform v1.4.1 is released. This p...	Mar 15	☆
	Tim Gross	Nomad 1.5.1, 1.4.6, and 1.3.11 released — Nomad 1.5.1 has been releas...	Mar 13	☆
	James Bardin	Terraform CLI v1.4.0 released — Hello! Terraform v1.4.0 has been release...	Mar 8	☆

Production Readiness

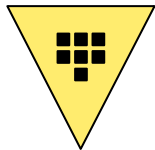
[Join security & vulnerability announcements list](#)



The screenshot shows the HashiCorp Discuss forum page. At the top, there's a navigation bar with the HashiCorp logo, a 'Discuss' link, a 'Sign in' button, and search/menus icons. Below the navigation bar is a blue banner for HashiDays in Paris. The main content area is titled 'Security updates for all HashiCorp products and services. Posting to this category is restricted to HashiCorp employees only.' Below this title are tabs for 'Security', 'Tags', 'Latest', and 'Top'. The 'Latest' tab is selected. The forum posts are listed in a table with columns for 'Topic', 'Replies', 'Views', and 'Activity'. The first post is 'About HashiCorp security updates' with 0 replies, 4.6k views, and activity from Sep '22. The subsequent posts are vulnerability announcements: 'HCSEC-2023-13 - Nomad Unauthenticated Client Agent HTTP Request Privilege Escalation' (0 replies, 298 views, 11h activity), 'HCSEC-2023-12 - Vault's Microsoft SQL Database Storage Backend Vulnerable to SQL Injection Via Configuration File' (0 replies, 598 views, 8d activity), 'HCSEC-2023-11 - Vault's PKI Issuer Endpoint Did Not Correctly Authorize Access to Issuer Metadata' (0 replies, 496 views, 8d activity), and 'HCSEC-2023-10 - Vault Vulnerable to Cache-Timing Attacks During Seal and Unseal Operations' (0 replies, 572 views, 8d activity).

Topic	Replies	Views	Activity
About HashiCorp security updates Security updates for all HashiCorp products and services. Posting to this category is restricted to HashiCorp employees only. Reporting Security Vulnerabilities We deeply appreciate any effort to discover and coordina... read more	0	4.6k	Sep '22
HCSEC-2023-13 - Nomad Unauthenticated Client Agent HTTP Request Privilege Escalation	0	298	11h
HCSEC-2023-12 - Vault's Microsoft SQL Database Storage Backend Vulnerable to SQL Injection Via Configuration File security-vault	0	598	8d
HCSEC-2023-11 - Vault's PKI Issuer Endpoint Did Not Correctly Authorize Access to Issuer Metadata security-vault	0	496	8d
HCSEC-2023-10 - Vault Vulnerable to Cache-Timing Attacks During Seal and Unseal Operations security-vault	0	572	8d

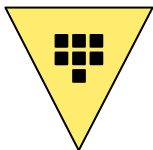
Vault Production Readiness



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

Vault Production Readiness

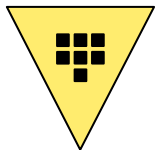
Architecture & Infrastructure



- 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?
- 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

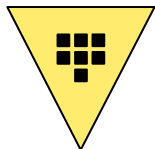
Vault Operations &
Infrastructure Security



- 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

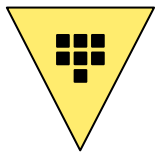
Business Continuity



- 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 & 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?

03



Content & Resources

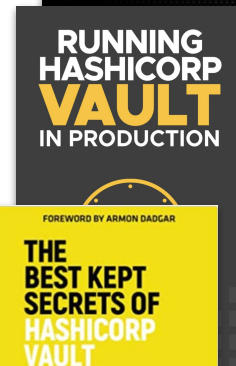
Vault Onboarding Journey Content

- [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](#)
- [Running Vault in Production \(book\)](#)
- [The Best Kept Secrets of Vault \(book\)](#)
- [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