HashiCorp Vault

Vault Onboarding Program Closing Thoughts

© HASHICORP

Vault Onboarding Program

A 7 week guided community environment
Assisting customers with onboarding and adoption

Vault Architecture Deep dive

- Kick Off & Architectural Quickstart
- Architectural Deep-dive
- Migrating from Vault OSS*

Identity and Access Management

- Namespaces, ACL Policies, Auth Methods
- Community Office Hours
- Using Vault with Kubernetes*

Operationalize

- Telemetry & Monitoring, DR Operations, Runbooks

Secrets Management

- How to consume Vault into applications
- Vault Dynamic Secrets*

Ready for Production!

- Vault Governance
- Exit Ramp & Operational Readiness Checklist (asynchronous)

© HASHICORP

Agenda

Onboarding Program Recap 01

Production Readiness 02

Content & Resources 03

© HASHICORP

01

Onboarding Program Recap

© HASHICORP

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

© HASHICORP

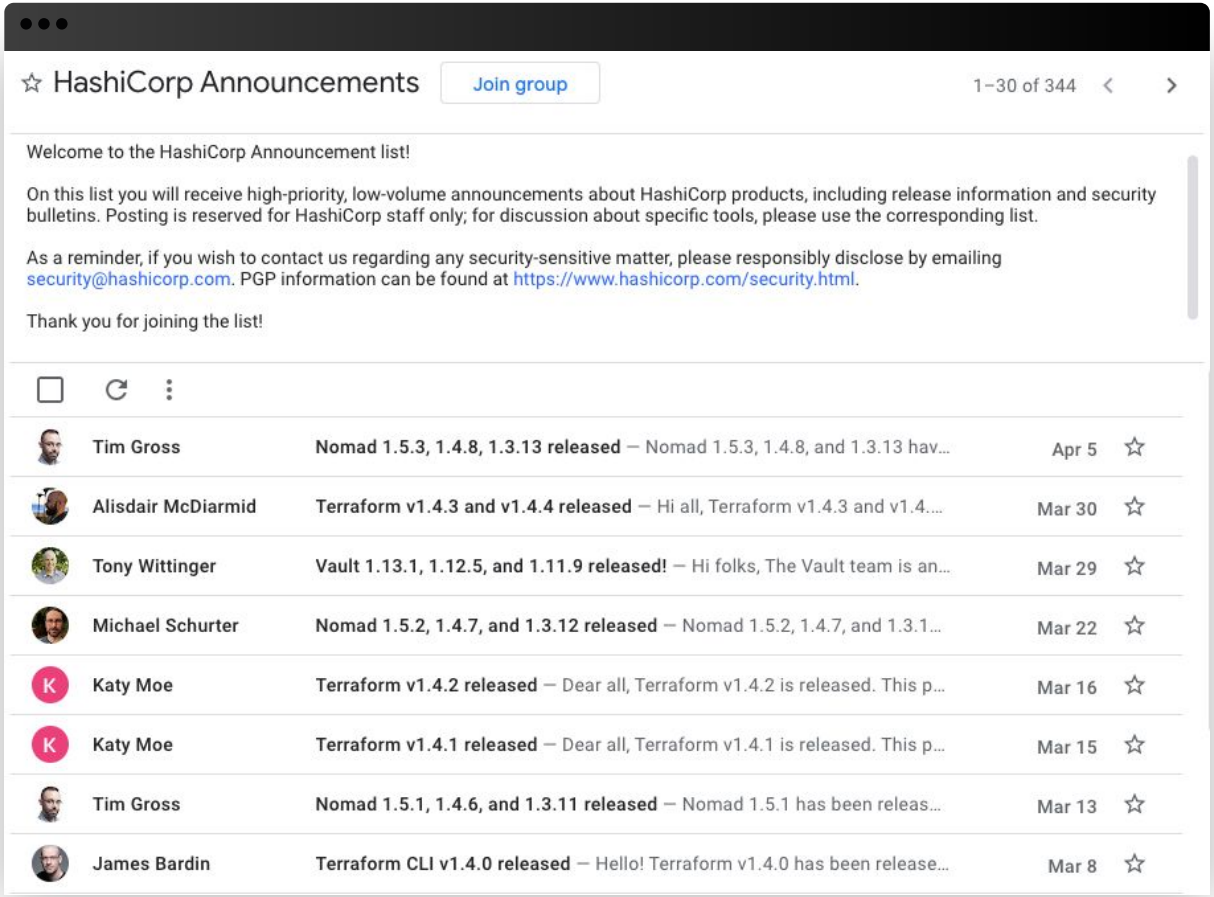
02

Production Readiness

© HASHICORP

Production Readiness

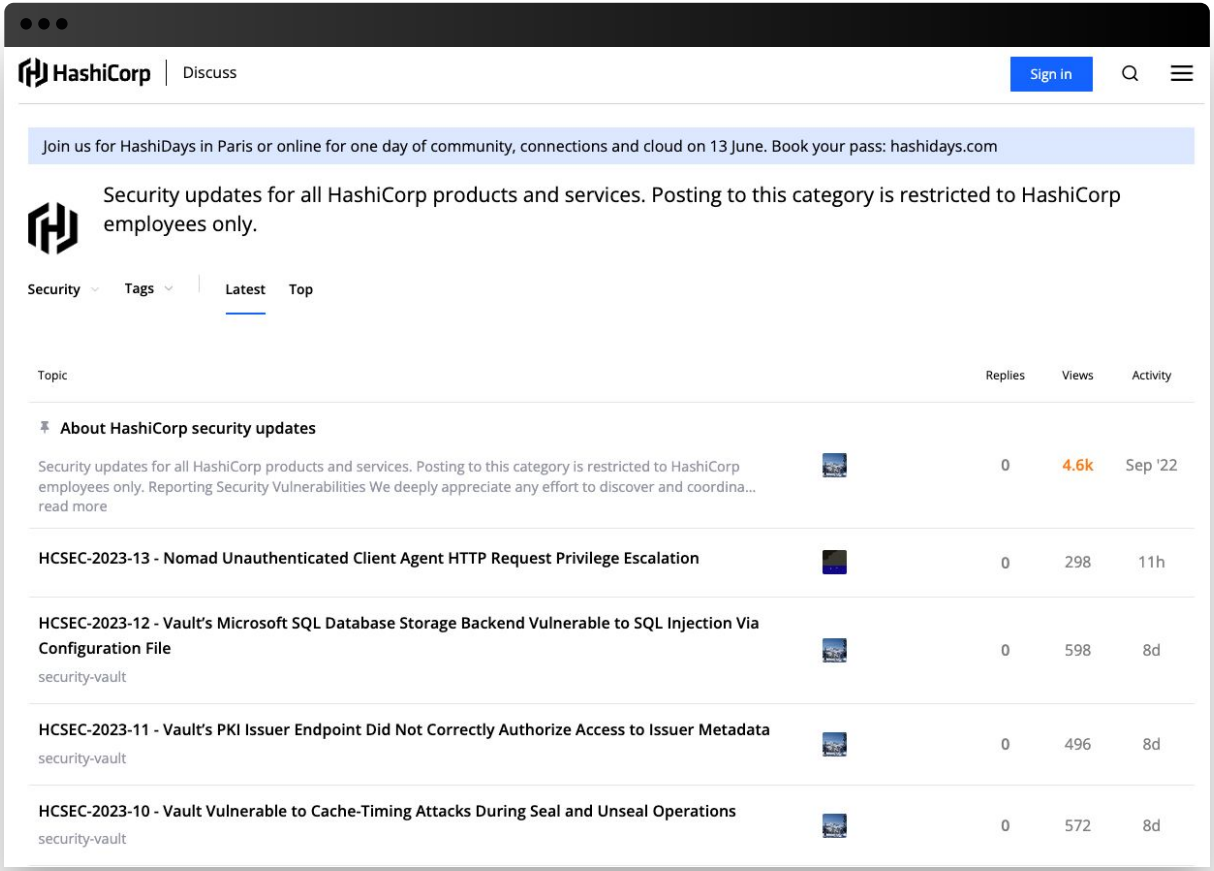
[Subscribe to release notifications]



© HASHICORP

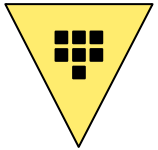
Production Readiness

[Join security & vulnerability announcements list]



© HASHICORP

Vault Production Readiness

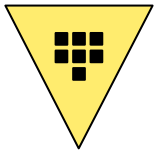


- Architecture & Infrastructure
- Vault Operations & Infrastructure Security
- Business Continuity
- Vault Policy & Configuration

© HASHICORP

Vault Production Readiness

Architecture & Infrastructure

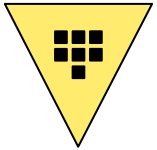


- Is the cluster architecture aligned with the reference architecture?
  - Consul Storage Reference Architecture
  - Integrated Storage Reference Architecture
  - Are the nodes configured across multiple AZs / failure zones to provide resilience in accordance with your uptime requirements?
  - Are the 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?

© HASHICORP

Vault Production Readiness

Vault Operations & Infrastructure Security

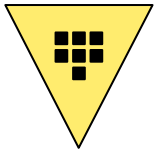


- Is root token creation restricted and monitored?
- Does the team managing Vault have runbooks and processes for all key administrative tasks?
  - Upgrading Vault
  - Executing DR failovers in Vault
  - Reissuing unseal/recovery key shares
  - Rotating Vault's master encryption key
  - Rotating any 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?

© HASHICORP

Vault Production Readiness

Business Continuity

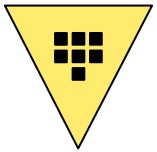


- Have runbooks been created and tested to validate the ability to meet the Recovery Time Objective?
  - Have snapshots been enabled in alignment with the desired Recovery Point Objective?
  - Has recovery from a snapshot been tested and the process documented?
  - Is there alerting in place if snapshots 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

© HASHICORP

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?

© HASHICORP

03

Content & Resources

© HASHICORP

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

© HASHICORP

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)

© HASHICORP

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

© HASHICORP

Thank you

customer.success@hashicorp.com

www.hashicorp.com/customer-success