Vault Enterprise Production Readiness

September 2022

HashiCorp

The HashiCorp Customer Success Team has created this document to augment the content presented in the Enterprise Onboarding Program. This guide is a starting point for reviewing your installation and environment and creation of a Vault runbook. This checklist is a collection of suggestions and best practices documents, please use it as a foundation to review your environment and adjust to your business needs, requirements and operating conditions. This document comes with no warranty.

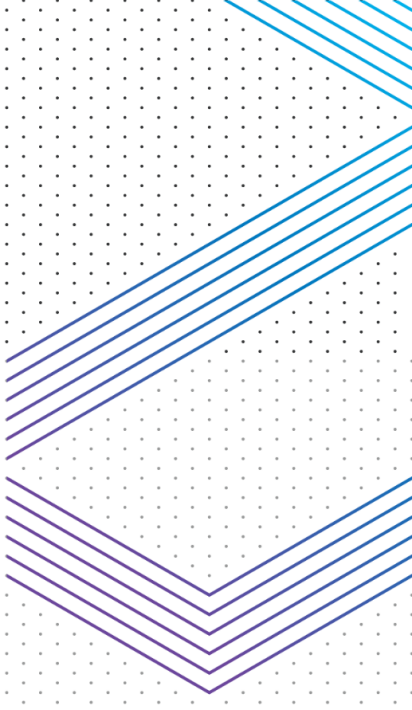
Architecture and Infrastructure
Is the cluster architecture aligned with the reference architecture? • Consul Storage Reference Architecture • Integrated Storage Reference Architecture • Are the nodes configured across multiple AZs / failure zones to provide resilience in accordance with your uptime 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?
Are the network ports that are opened aligned with the documentation and cluster configuration(I.E. 8200, 8021, and 8202)?
Are network and load balancer configurations and firewall openings understood, documented, and known not to change? Does the current documentation / runbook(s) include a topology diagram for all Vault cluster(s) and instances?
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? • Is the renewal reminder for TLS certificates a scalable process? I.E. more than a calendar entry in a single location? • Does the load balancer configuration follow best practices? Is TLS terminated on the Vault cluster?

Vault Operations and Infrastructure Security
Are servers provisioned via a build pipeline / infrastructure as code / using automation?
Can operators login to individual servers (SSH / console access / etc)?
Is the cluster running on a separate subnet or firewalled from other network resources?
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's key (if applicable) ● Generating root tokens
If a critical Vault CVE was published, how quickly could Vault be tested and upgraded? Does this meet security and operational requirements?
Have the production hardening recommendations been reviewed and implemented in the environment? Has the root token been disabled?
Is root token creation restricted and monitored?
Vault Initialization ● Was the recommended initialization ceremony followed? ● Have shamir/recovery keys been distributed to designated key holders? ● If not distributing shamir/recovery keys to key holders, what are the secure storage and handling processes for securing keys? ● Are keys signed with your PGP keys?
Is end-to-end TLS encryption being used for node communications (enabled by default) ● Are Consul and Vault communicating via TLS (if applicable)? ● Does Vault have the proper TLS certs for external communication? ● Does Consul have the proper TLS certs for external communication?
Have the Vault limitations been reviewed with Operations and Development teams?
Are Operations and Development teams aware to avoid the system default TTL of 768 hours?
Have the following items been validated and reviewed by the appropriate teams? ● How far back can access to a secret be audited? ● Who has access to audit logs? ● Who has access to server/application logs?

Are max lease TTL's being set?
Have rate limits and resource quotas been implemented? (Vault version 1.8.1 and above)
Is there an upgrade pattern and plan in place to stay within 2 major versions of the current release version?
Is the running version of Vault currently supported? N-2 window from latest release.
Have your operations and security teams subscribed to the release notifications group and/or the security and vulnerability announcements list?

Business Continuity
Are disaster recovery (DR) operations documented and tested? Is testing planned/scheduled on at least a semi-annual basis?
Have common DR failures been tested and procedures documented?
Has Vault operation been incorporated into the business continuity plan?
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?
Is monitoring and alerting in place?
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
Is replication WAL status being monitored?
Are multiple audit endpoints configured?
If a server is destroyed/lost, are logs and events available post-mortem?

Vault Policy and Configuration
Are policies documented, preferably managed via code, and audited occasionally?
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?
Is the use of “sudo” in capabilities understood and checked for?
When generating namespaces for teams are templated patterns being used to automate creation of Admin users, standard auth methods and secret engines.



USA Headquarters

101 Second St., Suite 700, San Francisco, CA, 94105
www.hashicorp.com