

HashiCorp Certified: Vault Operations Professional

OEM: Terraform • Duration: 5 Days (40 hrs) • Code: VA-PROF

COURSE MODULES & TOPICS

Section 1: Create a Working Vault Server Configuration Given a Scenario

- Enable and configure secret engines
- Practice production hardening
- Auto unseal Vault
- Implement integrated storage for Community and Enterprise Vault
- Enable and configure authentication methods
- Practice secure Vault initialization
- Regenerate a root token
- Rekey Vault and rotate encryption keys

Section 2: Monitor a Vault Environment

- Monitor and understand Vault telemetry
- Monitor and understand Vault audit logs
- Monitor and understand Vault operational logs

Section 3: Employ the Vault Security Model

- Describe secure introduction of Vault clients
- Describe the security implications of running Vault in Kubernetes

Section 4: Build Fault-Tolerant Vault Environments

- Configure a highly available (HA) cluster
- [Vault Enterprise] Enable and configure disaster recovery (DR) replication
- [Vault Enterprise] Promote a secondary cluster

Section 5: Understand the Hardware Security Module (HSM) Integration

- [Vault Enterprise] Describe the benefits of auto unsealing with HSM
- [Vault Enterprise] Describe the benefits and use cases of seal wrap (PKCS#11)

Section 6: Scale Vault for Performance

- Use batch tokens
- [Vault Enterprise] Describe the use cases of performance standby nodes
- [Vault Enterprise] Enable and configure performance replication
- [Vault Enterprise] Create a paths filter

Section 7: Configure Access Control

- Interpret Vault identity entities and groups
- Write, deploy, and troubleshoot ACL policies
- [Vault Enterprise] Understand Sentinel policies
- [Vault Enterprise] Define control groups and describe their basic workflow
- [Vault Enterprise] Describe and interpret multi-tenancy with namespaces

Section 8: Configure Vault Agent

- Securely configure auto-auth and token sink
- Configure templating