HashiCorp
Vault

Vault Enterprise Academy ILT

Prerequisites

To attend the Vault Implementation training session there are a few prerequisites to ensure a successful experience.

- **Solid command line experience** : Most of the lab exercises are command line based. This course does not cover the basics of text based editing or command line basics. A good understanding of how to navigate the command line will ensure a good overall learning experience.

Class Agenda

Day 1

Vault Enterprise Architecture	Overview of Vault, Vault Workflow, Terminology, Server Architecture, and Intro to Replication
Vault Deployment Guidelines	Production Deployment Best Practices, Deployment Considerations, Deployment Security Model, and Consul Storage Security Model
Vault Configuration	Configuration Overview, Initialization, and Seal Key Overview
Lab 1- Deploy a Consul Cluster	Deploy a secure, production-quality Consul Enterprise cluster for use behind a Vault Enterprise cluster
Lab 2 - Deploy a Vault Cluster	Deploy a secure, production-quality Vault Enterprise cluster
Operations and Management	Management of Seal Keys and Root Tokens, Configuring Logging and Monitoring, API Endpoints for Operations
Lab 3 - Vault Operations	Learn about Vault operations including audit logs, root token management, and rekeying and rotating of Vault's keys. Then migrate a Vault cluster to the GCP Auto-Unseal option.

Day 2

Enterprise Replication	Replication Overview, Disaster Recovery Replication, Performance Replication
Lab 4 - Vault Replication	Learn How To Configure Disaster Recovery and Performance Replication Between Vault Clusters
Deployment Automation	Things to consider when looking at deployment automation
Incident Management	What to do when things go wrong, Troubleshooting and Prevention
Tokens	Authentication Workflow, Token Overview, Token Types, Token Lifecycle, Token Use Cases
Policies	Policy Overview, Tokens and Polices, Writing Polices, Associating Policies
Lab 5 - Vault Tokens and Policies	Learn How To configure and use Vault Tokens and Policies

Day 3

Authentication Methods	Authentication Overview, People Auth Methods, Machine Auth Methods
Lab 6A - LDAP Authentication Method	Learn How To configure and use Vault's LDAP authentication method
Lab 6B - AWS Authentication Method	Learn How To configure and use Vault's AWS authentication method
Lab 6C - AppRole Authentication Method	Learn How To configure and use Vault's AppRole authentication method
Lab 6D - Kubernetes Authentication Methods	Learn How To configure and use Vault's Kubernetes authentication method
Static Secrets	Secrets Engines Overview, Static Secrets
Lab 7 - Versioned Secrets	Learn How To use and manage versioned secrets stored in Vault's Key/Value Version 2 (KVv2) secrets engine

Day 3 Continued

Deploying Secrets with vault	Deploying Secrets Overview, Vault Agent
Lab 8 - Vault Agent	Learn How To configure and use Vault agent as a way of injecting secrets
Dynamic Secrets	Dynamic Secrets Overview, Databases, PKI, Cloud Credentials, Encryption Keys
Lab 9A - PKI Secrets Engine	Learn how to setup a vault server to generate dynamic PKI certificates
Lab 9B1 - AWS Secrets Engine	Learn How To dynamically generate short-lived AWS credentials with Vault
Lab 9B2 - Google Cloud Secrets Engine	Learn How To dynamically generate short-lived GCP credentials with Vault
Lab 9C - Database Secrets Engine	Migrate a Python web application from using static database credentials to credentials dynamically generated by Vault's Database secrets engine
Onboarding Applications and Users	Operational Readiness, Namespaces ,User/Service Onboarding, Vault Service Usage Patterns