IBM - Boundary (HashiCorp)

Course Number: 8H504G

Duration: 3 days

Course Description

Boundary Enterprise is a comprehensive 3-day instructor-led course that teaches participants how to design, deploy, secure, operate, and scale HashiCorp Boundary Enterprise. Through a combination of expert-led instruction and hands-on labs, attendees learn Zero Trust access principles, platform administration, credential management, Vault integration, observability, and enterprise-scale automation. Designed for SREs, DevOps engineers, security teams, and platform operators, the course provides practical skills and proven best practices for implementing secure identity-based access across modern infrastructure.

Skills Gained

After completion of this course, learners will be able to:

1. Design, deploy, and operate HashiCorp Boundary Enterprise using proven enterprise architecture patterns and best practices.
2. Configure secure access through authentication, identity provider integration, scopes, projects, and role-based access controls (RBAC).
3. Manage targets, host catalogs, credentials, and connection workflows to deliver secure infrastructure access.
4. Implement advanced security capabilities, including credential injection, credential brokering, dynamic secrets with Vault, and session monitoring.
5. Monitor, scale, automate, and troubleshoot Boundary deployments to meet enterprise security, availability, and compliance requirements.

Who Can Benefit

- Site Reliability Engineers (SREs)
- DevOps Engineers
- Platform Engineers
- Cloud Engineers and Cloud Architects
- Systems Administrators
- Infrastructure Engineers
- Security Engineers

Prerequisites

Recommended Prerequisites

- Basic experience using a command-line interface (CLI) in Linux, macOS, or Windows.
- Foundational understanding of cloud and infrastructure concepts, including servers, networking, and environments.
- Familiarity with identity and access management concepts such as users, groups, authentication, and authorization.
- Basic knowledge of Terraform and Infrastructure as Code (IaC).
- Understanding of security concepts such as least privilege and Zero Trust principles.

Nice-to-Have

- Experience with HashiCorp Vault.
- Experience administering cloud infrastructure (AWS, Azure, or GCP).
- Familiarity with RBAC, IAM, or PAM solutions.
- Experience with DevOps, platform engineering, or security operations practices.

Course Details

Outline

Day 1: Foundations

- Boundary introduction, architecture, and core concepts
- Zero Trust security model and identity-based access
- Scopes, projects, roles, and access management
- Connection workflows (UI, CLI, API)
- Identity provider (IdP) integration
- Host discovery and resource management labs

Day 2: Deployment & Administration

- Deploying and configuring Boundary Enterprise
- Platform architecture, HA, and disaster recovery
- Authentication, RBAC, users, groups, and projects
- Managing targets, host catalogs, and host sets
- Platform operations, monitoring, and observability
- Session recording and lifecycle management

Day 3: Advanced Operations & Enterprise Features

- Credential management and credential brokering
- Credential injection and secretless access
- Vault integration for dynamic secrets
- Client agents and advanced connectivity workflows
- Multi-hop and transparent sessions
- Security hardening, compliance, and enterprise automation with Terraform