

introduction to BIG IP F5

Day 1: BIG-IP F5 Overview & System Fundamentals

Objective: Understand BIG-IP's role in application delivery and become familiar with its core components.

Session 1: Introduction to Application Delivery Controllers (ADCs)

What is BIG-IP F5?

Use cases: Load balancing, security, acceleration

Licensing and BIG-IP modules (LTM, DNS, ASM, APM, etc.)

Session 2: BIG-IP System Architecture

TMM (Traffic Management Microkernel)

Configuration objects: nodes, pools, virtual servers

TMOS overview and key processes

Session 3: Initial Setup & Configuration

Lab: Accessing the system (GUI, CLI, SSH)

Network configuration (interfaces, VLANs, self IPs)

Device licensing and provisioning modules

Day 2: Local Traffic Manager (LTM) Essentials

Objective: Learn to configure LTM for intelligent traffic distribution and high availability.

Session 1: Virtual Servers, Pools, and Nodes

Understanding traffic flow

Health monitors and availability

Persistence and load balancing methods

Session 2: Profiles and iRules

TCP/HTTP profiles and optimization

SSL offloading and re-encryption

Writing and applying basic iRules

Session 3: SNATs, NATs, and Routing

Source Network Address Translation (SNAT)

Default gateway and routing logic
VLAN groups and traffic segmentation

Day 3: DNS (GTM) & High Availability

Objective: Explore DNS services and implement high availability in F5 environments.

Session 1: BIG-IP DNS (formerly GTM) Overview

Global Server Load Balancing (GSLB)
DNS zones, listeners, and wide IPs
Intelligent DNS resolution based on geolocation, latency

Session 2: Device Clustering and Sync-Failover

HA setup: Active/standby pairs
ConfigSync and failover groups
Manual vs. auto sync modes

Session 3: Upgrades and Backups

Software lifecycle and image management
UCS and SCF backups
Upgrade best practices

Lab Exercise: Set up DNS services and test failover scenarios

Day 4: Security, Access, and Application Protection (Optional ASM/APM Intro)

Objective: Introduce BIG-IP's security features and modules for application and access control.

Session 1: Application Security Manager (ASM) Basics

Web Application Firewall (WAF) concepts
Policies, learning modes, signatures
Logging and attack reporting

Session 2: Access Policy Manager (APM) Intro

Identity and access control
SSL VPN configuration
Visual policy editor

Session 3: Secure Configuration Best Practices

User authentication and RBAC

System hardening tips

Integration with external security tools

Day 5: Troubleshooting, Logging & Capstone Project

Objective: Build confidence in real-world F5 management, diagnostics, and hands-on configuration.

Session 1: Troubleshooting Tools and Logs

tcpdump and packet capture

Log locations and analytics

GUI tools: Statistics, analytics, and dashboards

Session 2: Advanced Diagnostics

Common issues: failed health checks, SSL issues, routing loops

Support tools: QKView, iHealth

Configuration review and validation

Session 3: Capstone Project

Design and deploy a full application delivery scenario

Configure virtual servers, pools, monitors, profiles

AL MAWRED TRAINING INSTITUTE