

## F5-TRG-BIG-LTM-CFG-3

### Configuring BIG-IP LTM: Local Traffic Manager v.15.1

#### Overview

This course gives network professionals a functional understanding of BIG-IP Local Traffic Manager, introducing students to both commonly used and advanced BIG-IP LTM features and functionality. Incorporating lecture, extensive hands-on labs, and classroom discussion, the course helps students build the well-rounded skill set needed to manage BIG-IP LTM systems as part of a flexible and high performance application delivery network.

#### Course Length

3 days

#### Topics covered in this course Include

- BIG-IP initial setup (licensing, provisioning, and network configuration)
- A review of BIG-IP local traffic configuration objects
- Using dynamic load balancing methods
- Modifying traffic behavior with persistence (including SSL, SIP, universal, and destination address affinity persistence)
- Monitoring application health with Layer 3, Layer 4, and Layer 7 monitors (including transparent, scripted, and external monitors)
- Processing traffic with virtual servers (including network, forwarding, and reject virtual servers)
- Processing traffic with SNATs (including SNAT pools and SNATs as listeners)
- Modifying traffic behavior with profiles (including TCP profiles, advanced HTTP profile options, caching, compression, and OneConnect profiles)
- Advanced BIG-IP LTM configuration options (including VLAN tagging and trunking, SNMP features, packet filters, and route domains)
- Deploying application services with iApps
- Customizing application delivery with iRules and local traffic policies
- Securing application delivery using BIG-IP LTM



AUTHORIZED  
TRAINING CENTER

LIKE LIVING ORGANISMS, APPLICATIONS  
SHOULD ADAPT TO CHANGE

## Audience

This course is intended for system and network administrators responsible for installation, setup, configuration, and administration of the BIG-IP LTM system

## Prerequisites

Students must complete one of the following F5 prerequisites before attending this course:

- Administering BIG-IP instructor-led course
- F5 Certified BIG-IP Administrator

The following free web-based courses, although optional, will be very helpful for any student with limited BIG-IP administration and configuration experience. These courses are available at Learn F5:

- Getting Started with BIG-IP web-based training
- Getting Started with BIG-IP Local Traffic Manager (LTM) web-based training

The following general network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course:

- OSI model encapsulation
- Routing and switching
- Ethernet and ARP
- TCP/IP concepts
- IP addressing and subnetting
- NAT and private IP addressing
- Default gateway
- Network firewalls
- LAN vs. WAN

The following course-specific knowledge and experience is suggested before attending this course:

- Web application delivery
- HTTP, HTTPS, FTP and SSH protocols
- TLS/SSL



AUTHORIZED  
TRAINING CENTER

LIKE LIVING ORGANISMS, APPLICATIONS  
SHOULD ADAPT TO CHANGE

## Course Outline

- Chapter 1: Setting Up the BIG-IP System
  - Introducing the BIG-IP System
  - Initially Setting Up the BIG-IP System
  - Archiving the BIG-IP Configuration
  - Leveraging F5 Support Resources and Tools
- Chapter 2: Reviewing Local Traffic Configuration
  - Reviewing Nodes, Pools, and Virtual Servers
  - Reviewing Address Translation
  - Reviewing Routing Assumptions
  - Reviewing Application Health Monitoring
  - Reviewing Traffic Behavior Modification with Profiles
  - Reviewing the TMOS Shell (TMSH)
  - Reviewing Managing BIG-IP Configuration Data
- Chapter 3: Load Balancing Traffic with LTM
  - Exploring Load Balancing Options
  - Using Priority Group Activation and Fallback Host
  - Comparing Member and Node Load Balancing
- Chapter 4: Modifying Traffic Behavior with Persistence
  - Reviewing Persistence
  - Introducing Cookie Persistence
  - Specifying Default and Fallback Persistence
  - Introducing SSL Persistence
  - Introducing SIP Persistence
  - Introducing Universal Persistence
  - Introducing Destination Address Affinity Persistence
  - Using Match Across Options for Persistence
- Chapter 5: Monitoring Application Health
  - Differentiating Monitor Types
  - Customizing the HTTP Monitor
  - Monitoring an Alias Address and Port



- Monitoring a Path vs. Monitoring a Device
- Managing Multiple Monitors
- Using Application Check Monitors
- Using Manual Resume and Advanced Monitor Timer Settings
- Chapter 6: Processing Traffic with Virtual Servers
  - Understanding the Need for Other Virtual Server Types
  - Forwarding Traffic with a Virtual Server
  - Understanding Virtual Server Order of Precedence
  - Path Load Balancing
- Chapter 7: Processing Traffic with SNATs
  - Overview of SNATs
  - Using SNAT Pools
  - SNATs as Listeners
  - SNAT Specificity
  - VIP Bounceback
  - Additional SNAT Options
  - Network Packet Processing Review
- Chapter 8: Modifying Traffic Behavior with Profiles
  - Profiles Overview
  - TCP Express Optimization
  - TCP Profiles Overview
  - HTTP Profile Options
  - HTTP/2 Profile Options
  - OneConnect
  - Offloading HTTP Compression to BIG-IP
  - Web Acceleration Profile and HTTP Caching
  - Stream Profiles
  - F5 Acceleration Technologies
- Chapter 9: Selected Topics
  - VLAN, VLAN Tagging, and Trunking
  - Restricting Network Access
  - SNMP Features
  - Segmenting Network Traffic with Route Domains
- Chapter 10: Customizing Application Delivery with iRule



- Getting Started with iRules
- Understanding When iRules are Triggered
- Deploying iRules
- Constructing an iRule
- Testing and Debugging iRules
- Exploring iRules Documentation
- Chapter 11: Customizing Application Delivery with Local Traffic Policies
  - Getting Started with Local Traffic Policies
  - Configuration and Managing Policy Rules
- Chapter 12: Securing Application Delivery with LTM
  - Understanding Today's Threat Landscape
  - Integrating LTM Into Your Security Strategy
  - Defending Your Environment Against SYN Flood Attacks
  - Defending Your Environment Against Other Volumetric Attacks
  - Addressing Application Vulnerabilities with iRules and Local Traffic Policies
  - Detecting and Mitigating Other Common HTTP Threats
- Chapter 13: Final Lab Project
  - About the Final Lab Project
  - Possible Solution to Lab 13.1

