F5 Configuring Local Traffic Manager (LTM)

Duration: 3 Days **Course Code: WGAC-F5N-RG-BIG-LTM-CFG-3**

Overview:

This 3-day F5 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.

Target Audience:

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

Objectives:

- Back up the BIG-IP system configuration for safekeeping
- Configure virtual servers, pools, monitors, profiles, and persistence objects
- Test and verify application delivery through the BIG-IP system using local traffic statistics
- Configure priority group activation on a load balancing pool to allow servers to be activated only as needed to process traffic
- Compare and contrast member-based and node-based dynamic load balancing methods
- Configure connection limits to place a threshold on traffic volume to particular pool members and nodes
- Differentiate between cookie, SSL, SIP, universal, and destination address affinity persistence, and describe use cases for each
- Describe the three Match Across Services persistence options and use cases for each
- Configure health monitors to appropriately monitor application delivery through a BIG-IP system
- Configure different types of virtual services to support different types of traffic processing through a BIG-IP system
- Configure different types of SNATs to support routing of traffic through a BIG-IP system
- Configure VLAN tagging and trunking
- Restrict administrative and application traffic through the BIG-IP system using packet filters, port lockdown, and virtual server settings
- Configure SNMP alerts and traps in support of remote monitoring of the BIG-IP system
- Use iRules and local traffic policies appropriately to customize application delivery through the BIG-IP system
- Configure the BIG-IP to detect and mitigate some common attacks at the network and application layers using LTM features such as SYN check, eviction policies, iRules and Local Traffic Policies

Prerequisites:

Students are required to 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

Testing and Certification

EXAM 301A
BIG-IP LTM Specialist: Architect, Set up, Deploy

Prerequisites: Valid F5-CA, BIG-IP Certification

This is the first of two exams in the F5 Certified! Technology

very helpful for any student with limited BIG-IP administration and configuration experience.

- 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

Specialist, BIG-IP LTM certification and serves as a prerequisite to exam 301b. Candidates who pass this exam possess an understanding of underlying principles—from SSL-based VPN implementation to symmetric and asymmetric acceleration—and can draw on that insight to integrate BIG-IP LTM into existing networks as well as new implementations. Receiving the F5-CTS, BIG-IP LTM certification is a prerequisite for both the Cloud and Security Solutions Expert certification tracks

EXAM 301B
BIG-IP LTM Specialist: Maintain and Troubleshoot

Prerequisites: Valid F5-CA, BIG-IP Certification, valid passing score on Exam 301a

This is the second exam candidates are required to pass in order to receive the F5 Certified! Technology Specialist, BIG-IP LTM certification. Passing this exam validates their ability to design, implement, maintain, and troubleshoot advanced F5 product features to enhance the effectiveness of an Application Delivery Network. In addition, it shows that a candidate understands underlying principles—from SSL-based VPN implementation to symmetric and asymmetric acceleration—and can draw on that insight to integrate BIG-IP LTM into existing networks as well as new implementations. Receiving the F5-CTS, BIG-IP LTM certification is a prerequisite for both the Cloud and Security Solutions Expert certification tracks

Follow-on-Courses:

- WES_BIG-IP-APM, F5 Configuring BIG-IP APM: Access Policy Manager
- WES_BIG-IP-ASM, F5 Configuring BIG-IP ASM: Application Security Manager
- WES_BIG-IP-GTM, F5 Configuring BIG-IP DNS: Domain Name System (formerly GTM)

Content:

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 iRules

- 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
- Configuring 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

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo