F5 BIG-IP LTM Specialist: Maintain and Troubleshoot (Exam 301b)

This intermediate BIG-IP LTM Specialist: Maintain and Troubleshoot (exam 301B) training prepares network security admins to maintain and troubleshoot a flexible and high-performance application delivery system powered by F5's BIG-IP Local Traffic Manager. This course prepares you for one of two exams needed to earn F5's BIG-IP LTM Certified Technical Specialist certification.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Determining TCP Profiles — 158 min.

Data Buffering	17
TCP Profiles	21
Congestion and Packet Loss	8
Compression and Web Acceleration	8
Validation	9

Consolidating Configurations

Introduction	1
iRules Versus LTM Policies	7
Host VS Versus Network VS	7
Identify Redundant and Unused Objects	9
Identify Unnecessary Monitoring	11
Removing Functions From the LTM Device Configuration	5
Validation	11

Upgrading Big-IPs

Introduction	1
Performing a Clean Installation of the Big-IP	7
Using the TMSH Sys Software Install Options	9
Performing Additional Upgrade Steps	9
Installing Hotfixes	8
Copy A Config To A Previously Installed Boot Location/Slot	10

WEEK 2

151 min.

Rollback Steps For An Upgrade Attempt	5

Upgrading Big-IP HA Environments	6
Validation	7

Working With SNMP

Introduction	1
Simple Network Management Protocol (SNMP)	16
MIBs, OIDs, and SNMP Tools	16
Configuring SNMP Access On The Big-IP	9
Configuring SNMP Traps	3
Configuring Custom SNMP Alerts	5
Validation	4

Configuring Syslog and Email Alerting

Introduction	1
Logging Levels	12
Triggering Events	5
Configuring Email Alerts	15
Configuring Syslog	6
Validation	3

Working With iRules

Introduction	1
iRule Events and Commands	4
iRule Commands	6
iRule Logging	12
iRule Errors	4
iRule Traffic Steering	10

WEEK 3 **155 min.**

Validation	7

Using AVR On the Big-IP

Introduction	1
Enabling Application Visibility Reporting (AVR)	3
Using AVR With Profiles	14
Identifying Potential Latency Issues	5
Using Advanced Analytics Profile Filters	6
Tracing Application Traffic and Identifying Latency	6
Custom Analytics Widgets & Reporting	9
Validation	5

HTTP Headers and The SSL/TLS Handshake

Introduction	1
HTTP Status Code Refresher	3
Client HTTP Headers	5
Server HTTP Headers	7
Controlling HTTP Headers With Profiles	3
HTTP Methods	5
Decoding Post Data	7
The SSL/TLS Handshake Process	5
Browser Caching Behavior	8
Validation	8
Validation	1

Troubleshooting Applications and HTTPS

Introduction	1
Analyzing Causes of Problems	13
Protocol Analyzers and Other Tools	13

	SSL Handshake Failures (Tools and Handshake Process)	8
	Using Logs and SSLdump To Investigate SSL Handshake Failures	11
WEEK 4		**151 min.**
	Using OpenSSL To Investigation SSL Handshake Failures	3
	Decrypt SSL Traffic For Protocol Analysis	13
	Validation	12

Troubleshooting Slowness and Choosing Monitors

Introduction	1
Using Packet Captures To Troubleshoot Slowness	17
Identify Why Packet Drops Are Occurring	7
The bigd process and Monitor Timing	7
Choosing the Correct Monitor	5
Modifying Monitor Settings	6
Validation	6

Identifying LTM Device Issues

Introduction	1
Device Error Log Entries	12
End User Diagnostics (EUD)	10
Interpreting QKview Heuristic Results	6
Troubleshooting NTP Problems	9
Analyzing Logs For Other Problems	5
Validation	5

Managing High Availability and Failover

Introduction	1
Analyzing Performance Data To Identify A Resource Problem	8
Failover Event Categories	6
Serial Versus Network Failover	2
Identifying The Cause Of A Failover	9
WEEK 5	**22 min.**
Troubleshooting ConfigSync	13
Validation	9