Overview: F5 TrainingPass

Subscription Training Services

Welcome to TrainingPass

Your company's business needs move very fast. Accordingly, F5 technology is leading the way in business transformation so that your applications are Available, Fast, and Secure. To keep up with technology shifts, F5 TrainingPass provides technical training content to address your business needs.

F5 TrainingPass Benefits

Technical operations content

TrainingPass courses provide a broad set of technical training content that covers key F5 infrastructure and security technologies with a focus on: Setup, Preventative Maintenance, Ongoing Operations, and Troubleshooting

TrainingPass delivers key technical content focused on the needs of operations teams. It is task-oriented approach helps the operations team members get the job done.

Grow your professional skills

Course catalog delivers leading edge content that maps to current business and technology needs to ensure your applications and solutions are Available, Fast and Secure.

Consume at your own time

All courses are provided online so that they can be accessed 24X7 to accommodate the shifting schedules of IT and DevOps professionals.

New classes are periodically added and content is refreshed to stay relevant with technology shifts. TrainingPass content contains videos, job aids, and targeted resources to optimize knowledge transfer. To learn more about TrainingPass please contact F5 Global Training:

North and South America
F5 Global Training Services
Seattle, WA
Phone: (206) 272-5555
Fax: (206) 272-5568
Toll-free: 1-888-88-BIGIP
E-mail: training@f5.com

Europe, Middle East, Africa
F5 Regional Training Services
United Kingdom - Chertsey Office
Phone: (+44) 0 1932 582 000
Fax: (+44) 0 1932 582 001
E-mail: emeatraining@f5.com

TrainingPass Current Catalog

Standalone BIG-IP Initial Setup Series

Mini-Lesson Title	Description
Overview of the BIG-IP Initial Setup Series	Learn about the process steps required to set up a standalone BIG-IP system.
Step 1: Configuring the Management Port	Gain administrative access to your BIG-IP by configuring the system's management interface.
Step 2: Licensing the BIG-IP System	Perform licensing tasks to activate your BIG-IP system software.
Step 3: Provisioning BIG-IP Product Modules	Specify the BIG-IP software to run on your system by allocating resources to licensed modules.
Step 4: Installing a Device Certificate	Install an appropriate device certificate to enable inter-system communication and mutual authentication.
Step 5: Configuring Platform and User Properties	Define general device and user administration settings.
Step 6: Configuring the BIG-IP Network	Integrate your BIG-IP system into your application delivery network by defining configuration objects such as VLANs and self IP addresses.
Step 7: Configuring NTP Servers	Configure the BIG-IP system to synchronize its clock with an NTP server.
Step 8: Configuring Device DNS settings	Configure DNS to resolve host names defined within your BIG-IP system’s configuration data

Implementing an Active-Standby HA Pair Series

Mini-Lesson Title	Description
Overview of the BIG-IP HA Feature	Provides an overview of the BIG-IP high availability feature and describes the overall flow of process steps.
Step 1: Configuring HA Communication Settings	Define and manage the self IPs that are used for ConfigSync operations, mirroring, and failover operations
Step 2: Establishing Device Trust	Create and manage the underlying device trust that allows BIG-IP systems to be placed in a device group for configuration synchronization and failover
Step 3: Establishing a Device Group	Create and manage a device group with two BIG-IP systems functioning in an active/standby configuration.
Step 4: Synchronizing Configuration Data	Perform the initial ConfigSync operation to synchronize traffic processing configuration data on the BIG-IP systems. Confirm resulting configuration data and HA status.

Hardening the BIG-IP System Series

Mini-Lesson Title	Description
Overview of Hardening the BIG-IP System	Learn the major activities associated with hardening a BIG-IP system, and why it is important to consider doing them.
Securing Management Access	Learn about securing management access to the BIG-IP system. Topics covered include limiting SSH access to the management and TMM switch interfaces using an SSH Allow List, disabling the system section of the LCD interface, and configuring a serial console timeout value.
Hardening TMOS: Securing Self IP Addresses with Port Lockdown	Learn how to use the Port Lockdown feature to protect self IP addresses by allowing connections only from those protocols and services you need to meet your network and administrative requirements.
Hardening TMOS: Securing SSH Administrative Traffic	Learn how to secure access to the BIG-IP system's command line interface through a variety of activities, including disabling SSH access entirely, limiting SSH access by IP address or IP address range (with an SSH IP Allow List), limiting command line access by administrative user, restricting the number of consecutive login attempts, allowing only SSHv2 access, and more.
Hardening TMOS: Securing HTTPS Administrative Traffic	Learn how to secure access to the BIG-IP system's graphical user interface (also called the Configuration utility) through a variety of activities, including disabling GUI access entirely, limiting GUI access by IP address or IP address range (with an HTTPD Allow List), restricting the number of concurrent connections to the Configuration utility, restricting SSL/TLS protocols used, and more.
Hardening TMOS: Securing NTP Services	Learn how to secure the NTP Server functions on the BIG-IP system to ignore unwanted NTP queries or to allow NTP queries only from particular network devices by their IP address or address range.
Hardening TMOS: Running BIG-IP in Appliance Mode	Learn how to limit administrative access to the BIG-IP system, including disabling Advanced shell (bash) and root user access, by running in Appliance Mode.
Hardening TMOS: Securing the Automatic Update Check and Phone Home Features	Learn how to secure two BIG-IP features - Automatic Update Check and Automatic Phone Home - that involve communication with the F5 downloads server and F5 API server.
Securing Administrative Access: Securing the Default System Maintenance Accounts	Learn how to secure the default system maintenance accounts, root and admin.
Securing Administrative Access: Restricting Command Line Access by User	Learn how to secure access to the BIG-IP system's command line interface administrative tools on an individual user basis.
Securing Administrative Access: Tracking User Access and Actions	Learn how to view and manage audit logs that keep track of user access to a BIG-IP system and the configuration actions they take while administering the system.
Securing Administrative Access: Enforcing a Secure Password Policy	Learn how to create a strong password policy for local BIG-IP users, a key task in helping to safeguard against unauthorized or malicious administrative access to your BIG-IP system.
Preventing BIG-IP Data Leakage: Securing Persistence Cookies	Learn how to encrypt persistence cookies to prevent leaking BIG-IP system information related to using a cookie persistence profile.
Preventing BIG-IP Data Leakage: Securing BIG-IP Generated HTTP Server Header Information	Learn how to secure the HTTP server header information provided in BIG-IP-generated responses such as those from an HTTP profile, an iRule or a local traffic policy.
Handling Evolving Threats: Subscribing to F5 Threat Intelligence	Learn how to access and subscribe to F5 security intelligence, an important and informative step in handling evolving threats to your application delivery environment.

Handling Evolving Threats: Getting Help If You Are Under Attack or Experiencing a Security Breach	Learn how to integrate regular expressions into application check monitors to make them more flexible and usable.

Monitoring Application Delivery Series

Mini-Lesson Title	Description
Overview of Monitoring Application Delivery Through the BIG-IP System	Begin exploring how to monitor the health and performance of applications delivered through a BIG-IP system. This high-level overview of the monitoring feature sets the stage for other episodes in the series which describe monitoring functions and monitor types in more detail.
Managing Monitors in a BIG-IP LTM Environment (Part 1 of 2)	Explore the different types of local traffic resources that can be monitored, learn about the local traffic resource hierarchy and how to interpret resource availability codes, discover the options for deploying a new local traffic monitor, including how to test the monitor before assigning it to a resource, and finally understand how monitoring is handled in a high-availability environment.
Managing Monitors in a BIG-IP LTM Environment (Part 2 of 2)	Learn how to manage the ongoing operation of monitors after they have been assigned to resources and are actively checking application health or performance. Explore how to check and interpret resource availability from the Configuration utility and TMSH, how to view monitor instances, use local traffic logs to see changes in availability, and view local traffic monitor statistics.
Monitoring an Alias Resource	Learn how to mark a resource's availability based on the availability of another dependent resource.
Monitoring a Path (Transparent Monitoring)	Learn how to monitor a path through network devices such as local ISP routers or firewall pools to check the path's availability rather than just the pool member's availability.
Managing Availability Requirements for Multiple Monitors	Learn when and how to use multiple monitors on a resource to check dependent resources or path availability, and how to configure monitor availability requirements in these situations.
Using the Manual Resume Feature	Control when the BIG-IP system starts sending traffic to a previously offline pool member after a monitor starts receiving successful check results again.
Using Advanced Monitor Timing Features: Up Interval, and Time Until Up	Explore advanced monitor timing features that allow you to control the frequency with which a monitor checks a resource while it is up as compared to when it is down, and control the waiting period between the time a monitor produces a successful check result on a resource that is down before marking that resource as up.
Using the Action on Service Down Feature	Control how the BIG-IP system responds to existing connections when a monitor marks a pool member down.
Using Regular Expressions in Application Check Monitors	Learn how to integrate regular expressions into application check monitors to make them more flexible and usable.

Upgrading a BIG-IP System Series

Mini-Lesson Title	Description
Overview of the BIG-IP Upgrade Process	Provides an overview of the upgrade process and the major goals of each phase.
Phase 1: Planning for a BIG-IP System Upgrade	Phase 1 of the upgrade is all about planning activities, such as selecting an appropriate upgrade path, identifying product- and configuration-specific upgrade considerations, reviewing release notes, and determining the impact of the upgrade in terms of deprecated features, changes in behavior, and resource and licensing requirements.
Phase 2: Preparing to Upgrade a BIG-IP System	Phase 2 is comprised of preparation activities, such as reactivating the BIG-IP system's license, verifying the configuration, uploading and verifying the upgrade software image, and backing up the BIG-IP system. These tasks make it possible to perform the upgrade and recover easily, if needed.
Phase 3: Installing an Upgrade on a BIG-IP System	Phase 3 is the actual upgrade execution, including ISO installation, booting to the new version, and testing activities. The planning and preparation phases are key to a seamless transition during the installation phase.
Phase 4: HA Considerations During an Upgrade	Phase 4 explores additional considerations when upgrading BIG-IP systems that are part of a high-availability configuration.

Using TCPDUMP on a BIG-IP System Series

Mini-Lesson Title	Description
Overview of Using TCPDUMP on a BIG-IP System	Learn about the general capabilities of the TCPDUMP utility on a BIG-IP system.
Interpreting TCPDUMP Output	Learn how to analyze simple TCPDUMP packet captures.
Understanding TCPDUMP Filters and Options	Learn about the most commonly used TCPDUMP filters and options.
Analyzing TCPDUMP Captures with Wireshark	Learn how to analyze some basic TPCDUMP captures using F5's Wireshark plugin.

Troubleshooting Device Service Clustering Series

Mini-Lesson Title	Description
Troubleshooting DSC Part 1: Verifying Device Service Clustering Requirements	Learn how to verify that the basic requirements for DSC are being met as part of your initial Troubleshooting DSC efforts.
Troubleshooting DSC Part 2: Troubleshooting ConfigSync	Learn how to examine status information that can be derived from the BIG-IP Configuration utility, tmsh commands, and log files that can be used to troubleshoot ConfigSync issues.
Troubleshooting DSC Part 3: General Diagnostic Commands	Learn how to run tmsh commands to check failover status, device trust status, and monitor the CMI communication channel.
Troubleshooting DSC Part 4: Resetting Device Trust	Learn how to remove devices from a group, reset device trust and add devices back to a device group.

Other TrainingPass Episodes

- Working with End User Diagnostics (EUD)
- Creating and Downloading a UCS Archive
- Customizing System Preferences
- Working with F5 Support: Opening a Case
- Working with F5 Support: Processing and Downloading Core Dump Files
- Working with F5 Support: Processing Local Log Files
- Working with F5 Support: Uploading Files
- Working with iHealth Part 1: Creating and Uploading a QKView
- Working with iHealth Part 2: Viewing Diagnostics and Status Information
- Working with iHealth Part 3: Troubleshooting
- Working with iHealth Part 4: Examining the BIG-IP Configuration
- Working with Single Configuration Files (SCF)