Training: F5
NGINX Bootcamp

TRANING TERMS

2025-08-13 | 3 days | Kraków / Virtual Classroom
2025-09-10 | 3 days | Warszawa / Virtual Classroom

TRAINING GOALS:

This training is a combination of an Administering NGINX for Web Services course, Configuring Load Balancing using NGINX course and Mitigating Vulnerabilities with NGINX App Protect course.

Administering NGINX for Web Services part learn how to administer, configure, and manage NGINX using recommended practices. Discover how to set up and control NGINX server contexts, and configure location context. Explore NGINX variables and their usage. Find out about NGINX logging methods, levels and severity of log entries, and how to set up error logging. Learn about proxy and reverse proxy concepts and discover how to map and use variables to convert requests from older locations to new locations. Further explore routing concepts and methods, including why and how to configure NGINX to use HTTPS/SSL to secure client and server connections and how to force the use of HTTPS. Finally, learn about the NGINX Plus API and Dashboard; configure systems to display their information via the Dashboard and control access to systems via the API.

Configuring Load Balancing using NGINX part begins with a general review of load balancing, and an introduction to load balancer configuration, selection algorithms, and weighting in NGINX. After you configure an upstream, you explore options for session persistence and enable extended status / live activity monitoring. You implement TCP/UDP load balancing with active health checks, and configure routing and IP sourcing. We demonstrate a highly available (HA) NGINX systems in case of node failure. By the end of the class, you will be able to deploy a high performing (ADC) application delivery controller using NGINX Plus and its features.

Mitigating Vulnerabilities with NGINX App Protect part gives participants a functional understanding of how to deploy and operate NGINX App Protect WAF to protect their web applications from the most common web application vulnerabilities and Layer 7 denial of service attacks.

Course Objectives

By the end of this course, students will be able to:

- Learn the basics of the NGINX Architecture, it's scaling features, processes and basic management commands
- Learn NGINX configuration files, structure and context hierarchy
- Configure servers to respond to requests based on server and location settings

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Discover how NGINX uses built-in and custom variables and their usage
- Configure NGINX to log Connection and Error details
- Learn about NGINX Reverse Proxy usage and tuning settings
- Learn about NGINX Request Routing and configure alias and rewrite operations
- Discover TLS/SSL concepts and configure NGINX to require secure protocols
- Discover the NGINX Plus Dashboard and API and use them to monitor and configure your servers
- Understand the fundamental principles of load balancing
- Explore load balancer configuration, including selection algorithms and weighting in NGINX
- Configure an upstream for load balancing
- Implement session persistence and enable extended status/live activity monitoring
- Set up TCP/UDP load balancing with active health checks
- Configure routing and IP sourcing
- Learn about highly available (HA) NGINX systems in case of node failure
- Deploy a high-performing application delivery controller (ADC) using NGINX Plus and its features
- Understand the importance of securing web applications
- Explore HTTP processing and its relevance to security
- Learn about common web application vulnerabilities in modern applications
- Familiarize yourself with web application security concepts and terminology
- Explore deployment options and use cases for NGINX App Protect
- Configure default policy settings and understand security event logging
- Gain insights into policy elements and their impact
- Fine-tune policies to meet specific security needs
- Work with multiple policies effectively
- Understand recommended practices for handling attack signatures and threat campaigns
- Define Behavioral Denial-of-Service (DoS) protection
- Connect DoS directives with the nginx.conf configuration

CONSPECT:

- Administering NGINX for Web Services
  - Understanding the NGINX Architecture
  - Configuring Contexts
  - Serving Content with Server Directives
  - Serving Content with Location Directives
  - Using Variables

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Managing NGINX Logging
- Proxying Requests
- Routing HTTP Requests
- Mapping Variables
- Encrypting Web Traffic and Restricting Access
- Monitoring and Managing Systems

- Configuring Load Balancing using NGINX
  - Set up http load balancing to backend servers
  - Describe load balancing migration scenarios
  - Configure and test the backup parameter
  - Use the NGINX live activity monitoring dashboard to monitor HTTP and TCP back-end servers
  - Understand and configure session persistence methods
  - Configure and test TCP load balancing and active health checks
  - Understand HA scenarios
- Mitigating Vulnerabilities with NGINX App Protect
  - An application-centered approach to security
  - Overview of HTTP processing
  - Exploiting web application vulnerabilities in a modern application
  - Web application security concepts and terminology
  - Deployment options and use cases for NGINX App Protect
  - Default policy configuration and settings
  - Security event logging
  - Understanding policy elements
  - Tuning policies for specific needs
  - Working with multiple policies
  - Recommended practices for attack signatures and threat campaigns
  - Defining Behavioral DoS protection
  - Connecting DoS directives and nginx.conf
  - Mitigating DoS

REQUIREMENTS:

The course assumes a basic understanding of networking, web servers, HTTP, load balancing, caching, proxying, and related concepts.

Hands on labs are performed in a Linux environment. You will need to be able to navigate the file system from the command line and edit configuration files using VI/VIM. Additional experience with

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Linux environments will be helpful.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by F5 Networks (course completion).

TRAINER:

Certified F5 Networks Trainer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007