Training: F5
NGINX Bootcamp

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.

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.

Administering NGINX for Web Services is critical for all levels of NGINX product users, from beginner to experienced, because this course teaches the concepts and practices that form the foundation for learning about other products in the NGINX family.

NGINX Load Balancing 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 course gives participants a functional understanding of how to deploy and operate NGINX App Protect (WAF and DoS) to protect their web applications

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

from the most common web application vulnerabilities and Layer 7 denial of service attacks.

Audience

Administering NGINX for Web Services Configuring Load Balancing using NGINX are essential for all NGINX product users. The target audience for Mitigating Vulnerabilities with NGINX App Protect is personae new to DevOps and SecOps, along with anyone in DevOps where exposure to app security knowledge is limited.

CONSPECT:

- Getting Started with NGINX
- Understanding the NGINX Architecture
- Configuring Contexts
- Serving Content with Server Directives
- Serving Content with Location Directives
- Using Variables
- Managing NGINX Logging
- Proxying Requests
- Routing HTTP Requests
- Mapping Variables
- Encrypting Web Traffic and Restricting Access
- Monitoring and Managing Systems
- HTTP load balancing to backend servers
- Load balancing migration scenarios
- Configuring and testing the backup parameter
- Using the NGINX live activity monitoring dashboard to monitor HTTP and TCP backend servers
- Session persistence methods
- TCP load balancing
- Active health checks
- High Availability (HA) scenarios
- Overview of HTTP Communication
- Overview of Web Application Vulnerabilities
- Applying Security Concepts and Enabling NGINX App Protect
- Logging Security Events in NGINX App Protect
- Setting Policy
- Policy tuning and working with multiple policies

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Updating Attack Signatures and Threat Campaigns
- Mitigating Denial of Service Attacks
- Troubleshooting

REQUIREMENTS:

Before taking this course, make sure you have completed one of the following:

- Administering NGINX for Web Services

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 Linux environments will be helpful.

Difficulty level



CERTIFICATE:

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

This course helps prepare participants for the F5 Certified Administrator, NGINX (F5-CA, NGINX) certification. The certification requires candidates to pass four exams: NGINX Management (F5CAN1); NGINX Configuration: Knowledge (F5CAN2); NGINX Configuration: Demonstrate (F5CAN3); and NGINX Troubleshoot (F5CAN4).

More information: https://education.f5.com/learning-path/view/24

TRAINER:

Certified F5 Networks Trainer

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310