Apache and Secure Web Server Administration

Course Duration: 24 Hours (3 Days)

Overview

The Apache and Secure Web Server Administration course is a comprehensive program designed to equip learners with the skills and knowledge necessary to install, configure, maintain, and secure Apache web servers. This course covers a wide range of topics from initial installation to advanced configuration and performance tuning. Module 1 begins with various installation methods, including using package managers on Linux distributions like Red Hat and Debian, installing on Windows, and compiling from source. It provides practical guidance on managing the server lifecycle, choosing the correct version of Apache, and optimizing the installation process. Module 2 through Module 11 delve into adding modules, logging, virtual hosts, security, SSL, dynamic content, error handling, and performance, respectively. By completing Apache training courses like this one, learners will gain hands-on experience with the apache web server course, enabling them to build and manage robust, secure web servers effectively. Through this curriculum, participants will become proficient in Apache administration, which is an essential skill set for IT professionals working with web technologies.

Audience Profile

The Apache and Secure Web Server Administration course is designed for IT professionals responsible for managing web server environments.

- System Administrators
- Network Administrators
- Technical Support Specialists
- Web Developers
- IT Security Specialists
- DevOps Engineers
- Infrastructure Architects
- Site Reliability Engineers (SREs)
- IT Managers overseeing web server operations
- Professionals looking to enhance their web server management skills
- Technical Consultants providing web server solutions
- Cloud Engineers managing web server deployments on cloud platforms

Course Syllabus

Module 1: Installation

- Web Servers and Their Components
- Apache Web Server and Architecture

- Apache Core and Its Modules
- Concurrency in Apache
- Lab: Installing Apache
- Starting, Stopping, and Restarting Apache
- Lab: Apache Tarball-Based Installation
- Lab: Apache Installation from Debian Packages
- Lab: Apache on Windows
- Choosing the Right Apache Version
- Starting Apache at Boot
- Apache Configuration File
- Lab: Uninstalling Apache
- Upgrading Using config.nice
- Locating Apache Files

Module 2: Adding Common Modules

- Generic Third-Party Modules
- Lab: Installing mod_dav on a Unix System
- Lab: Installing mod_perl on a Unix System
- Lab: Installing mod_php on a Unix System
- Lab: Installing mod_ssl
- Finding Modules Using Modules.Apache.Org
- Apache mod_security Module
- Lab: Installing mod_security

Module 3: Logging

- Enhancing Log Detail
- Lab: Configuring Access Logs
- Improving Error Logging
- Lab: Configuring Error Logs
- Logging POST Contents
- Lab: POST Request Logging
- Logging a Proxy Client's IP Address
- Logging Client MAC Addresses
- Logging Cookies
- Lab: Excluding Image Requests from Logs
- Lab: Rotating Log Files at a Specific Time
- Lab: Rotating Logs on the First of the Month
- Logging Hostnames Instead of IP Addresses

Module 4: Virtual Hosts

- Setting Up Name-Based Virtual Hosts
- Lab: Name-Based Virtual Hosts
- Lab: Setting a Default Name-Based Virtual Host
- Lab: Setting Up Address-Based Virtual Hosts
- Lab: Creating a Default Address-Based Virtual Host
- Lab: Mass Virtual Hosting with mod_vhost_alias
- Mass Virtual Hosting Using Rewrite Rules
- Lab: Logging for Each Virtual Host
- Splitting Up a Log File
- Lab: Port-Based Virtual Hosts
- Lab: Displaying the Same Content on Multiple Addresses
- Defining Virtual Hosts in a Database

Module 5: Aliases, Redirecting, and Rewriting

- Lab: Mapping a URL to a Directory
- Creating a New URL for Existing Content
- Redirecting to Another Location
- Lab: Using the Redirect Directive
- Lab: Using the RedirectMatch Directive

Module 6: Security

- Using System Account Information for Web Authentication
- Setting Up Single-Use Passwords
- Expiring Passwords
- Managing .htpasswd Files
- Lab: Setting Up Basic HTTP Authentication in Apache
- Creating Password Files for Digest Authentication
- Relaxing Security in a Subdirectory

Module 7: SSL

- SSL and Its Components
- Apache mod_ssl Module
- Lab: Installing SSL Using mod_ssl
- Lab: Generating Self-Signed SSL Certificates
- Generating a Trusted CA
- Authenticating with Client Certificates

Module 8: Dynamic Content

- Dynamic Content in Apache
- CGI Scripts
- Enabling CGI Scripts in Non-Script Aliased Directories
- Lab: Using CGI Scripts
- Lab: Enabling CGI Scripts in Apache Configuration
- Testing CGI Setup
- Invoking a CGI Program for Specific Content Types

Module 9: Error Handling

- Error Handling in Apache
- Lab: Handling a Missing Host Field
- Lab: Customizing Error Messages
- Providing Error Documents in Multiple Languages
- Lab: Redirecting Invalid URLs to Another Page

Module 10: Proxies

- Proxying in Apache
- Lab: Creating a Proxy Server in Apache
- Lab: Securing Your Proxy Server
- Lab: Preventing Your Proxy Server from Being Used as an Open Mail Relay

Module 11: Performance

- Determining Memory Requirements
- Lab: Benchmarking Apache with ab
- Lab: Tuning Keep-Alive Settings
- Lab: Monitoring Site Activity
- Lab: Avoiding DNS Lookups
- Optimizing Symbolic Links