

Course 730: Essential Apache WebServer (3 days)

Course Description...

Geared for administrators that need to implement the Apache-2 Web Server with typical corporate functionality, this course is designed to quickly get your Apache-2 web server functional. Students will learn how to install, configure, maintain, and monitor the Apache-2 installation. Upon completion of this class, students will be comfortable with creating a secure web server, virtual hosts, CGI support, Intranets, Extranets, and adding modules for Java, Perl and PHP.

Upon completion of this course the administrator will be capable of installing, monitoring, and maintaining a secure corporate web server capable of hosting dynamic web pages for multiple virtual hosts.

Who should attend...

This course is geared for administrators that need to implement the Apache-2 Web Server with typical corporate functionality such as a secure web server, Extranet and Intranet capabilities, virtual hosting, and modules that interface with Perl, Java, PHP, and CGI for dynamic web pages.

Prerequisites...

Students should currently be working with UNIX System Administration (or the equivalent), and have knowledge of the vi editor.

Hands-On Learning

Throughout this course, students will be led through a series of progressively advanced topics, where each topic consists of lecture, group discussion, comprehensive hands-on lab exercises, and lab review.

This workshop is about 50% hands-on lab and 50% lecture. Multiple detailed lab exercises are laced throughout the course, designed to reinforce fundamental skills and concepts learned in the lessons. Because the lessons, labs and projects are presented in a building block fashion, students will gain a solid understanding of not only the core concepts, but also how all the pieces fit together in a complete solution.

See next page for a detailed course outline...



Course Outline...

UNIT 1 – Apache - Overview

- Terminology
- The Apache Software Foundation
- What is Apache?
- Overview of Apache Versions 1.3, 2.0, 2.2
- Obtaining the Software
- Apache Modules
- Important Files and Their Locations
- Default Settings
- The “/etc/httpd” Directory
- The /etc/httpd/htdocs directory
- Block Directives

UNIT 2 – Basic Installation

- A Development Tool
- Basic httpd.conf
- Seven Standard Directives
- Checking “httpd.conf” Syntax
- “apachectl” is a Script
- Controlling The “httpd” Daemon With “apachectl”
- Note on Web Browsers
- Adding web pages
- “DirectoryIndex” Directive
- “IndexOptions” Directive
- The “index.html” file

UNIT 3 – Basic Runtime Configuration

- Basic Security Suggestions
- Server Configuration Limits
- TimeOut
- KeepAlive
- MaxKeepAliveRequests
- KeepAliveTimeout
- LimitRequestBody
- LimitRequestFields
- LimitRequestFieldsize
- LimitRequestLine
- LimitXMLRequestBody
- Multiprocessing Modules
- The Prefork MPM
- StartServers
- MinSpareServers
- MaxSpareServers
- ServerLimit
- MaxClients
- MaxRequestsPerChild

UNIT 4 – Logging and Reporting

- Data Available to Apache
- Default Location of Logging files
- Error Logging
- Controlling The Level of Detail



- Access Logging
- Log Formatting
- Custom logs
- The “<Directory>” Block Directive
- The “<Location>” Block Directive
- On-Line Reports
- Miscellaneous Directives That Provide Information

UNIT 5 – Manual Pages and Custom Error Pages

- HTTP 1.1 Error Codes
- Customized Error Code Web Pages
- Error Page Locations
- Providing Online Manual Pages
- <Directory “var/www/manual”>
- Trailing Slash Issue
- Internationalization of Error Messages

UNIT 6 – Virtual Hosts

- Using Virtual Hosts
- Directives Used With Virtual Hosting
- The “NameVirtualHost” directive
- The <VirtualHost> Block Directive
- Directives Defining Locations For Your Logs and Web Pages
- Test Our Two New Virtual Hosts

UNIT 7 – Authentication

- Authentication with Apache
- Main Authentication Directives
- The “AuthName” Directive
- The “AuthGroupFile” Directive
- The “AuthUserFile” Directive
- The Require Directive
- The “htpasswd” Program
- Modifying Your Configuration to Require Basic Authentication
- The “AuthDigestFile” directive
- The “htdigest” program
- Modify Your Configuration to Use Digest Authentication

UNIT 8 – Authorization

- The “Allow from” Directive
- The “Deny from” Directive
- The “Order” Directive
- The “Satisfy” directive
- The “<Files>” Block Directive
- The “<Limit>” Block Directive
- Preventing DoS attacks

UNIT 9 – Secure Data Transmittal with HTTPS

- Creating a Secure Web Site
- Creating a Test Digital Certificate
- Create a “Private Key”
- Create a “Certificate Signing Request”
- Create a “Self Signed Certificate”
- Installing The Certificates



- Modifying "httpd.conf" to use SSL
- Testing Your Implementation

UNIT 10 – Performance and Monitoring

- Performance optimizations
- Load Balancing with mod_proxy
- Load Balancing with Netscaler
- Performance benchmarking
- Best Practices

UNIT 11 – CGI/mod_perl

- CGI 201
- "HTTP Headers"
- Modifying Apache to Use CGI
- Testing With "Shell Scripts"
- Using Perl with CGI
- Test Out a Perl Script Using CGI
- Using "mod_perl"
- Selecting a "PerlHandler"
- Additional Directives for "mod_perl"
- Test Your "cgi-perl" Script With a "mod_perl" Implementation

UNIT 12 – Common Modules

- mod_status
- mod_proxy
- mod_rewrite

Appendix - Directives

Please contact your ROI representative to discuss course tailoring!!!