GL275: Enterprise Linux Networking Services

Days: 5

Prerequisites: Students should already be comfortable with basic Linux or Unix administration. Fundamentals such as the Linux filesystem, process management, and how to edit files will not be covered in class. A good understanding of network concepts, the TCP/IP protocol suite is also assumed. These skills are taught in the GL120 "Linux Fundamentals" and GL250 "Enterprise Linux Systems Administration" courses.

Audience: IT Professionals

Description: The GL275 is an expansive course that covers a wide range of network services useful to every organization. Special attention is paid to the concepts needed to implement these services securely, and to the trouble-shooting skills which will be necessary for real-world administration of these network services. Like all Guru Labs courses, the course material is designed to provide extensive hands-on experience. Topics include: Security with SELinux and Netfilter, DNS concepts and implementation with Bind; LDAP concepts and implementation using OpenLDAP; Web services with Apache; FTP with vsftpd; caching, filtering proxies with Squid; SMB/CIFS (Windows networking) with Samba; and e-mail concepts and implementation with Postfix combined with either Dovecot or Cyrus.

OUTLINE:

I. SECURING SERVICES

- Xinetd
- Xinetd Connection Limiting and Access Control
- Xinetd: Resource limits, redirection, logging
- TCP Wrappers
- The /etc/hosts.allow &a /etc/hosts.deny Files
- /etc/hosts.{allow,deny} Shortcuts
- Advanced TCP Wrappers
- SUSE Basic Firewall Configuration
- FirewallD
- Netfilter: Stateful Packet Filter Firewall
- Netfilter Concepts
- Using the iptables Command
- Netfilter Rule Syntax
- Targets
- Common match_specs
- Connection Tracking

LAB TASKS

- Securing xinetd Services
- Enforcing Security Policy with xinetd
- Securing Services with TCP Wrappers
- Securing Services with SuSEfirewall2
- Securing Services with Netfilter
- FirewallD
- Troubleshooting Practice

II. SELINUX AND LSM

- AppArmor
- SELinux Security Framework
- Choosing an SELinux Policy
- SELinux Commands
- SELinux Booleans
- SELinux Policy Tools

LAB TASKS

- Exploring AppArmor Modes
- SELinux File Contexts

GL275: Enterprise Linux Networking

Services

III. DNS CONCEPTS

- Naming Services
- DNS – A Better Way
- The Domain Name Space
- Delegation and Zones
- Server Roles
- Resolving Names
- Resolving IP Addresses
- Basic BIND Administration
- Configuring the Resolver
- Testing Resolution

LAB TASKS

- Configuring a Slave Name Server

IV. CONFIGURING BIND

- BIND Configuration Files
- named.conf Syntax
- named.conf Options Block
- Creating a Site-Wide Cache
- rndc Key Configuration
- Zones In named.conf
- Zone Database File Syntax
- SOA – Start of Authority
- A, AAAA, & PTR – Address & Pointer Records
- NS – Name Server
- TXT, CNAME, & MX – Text, Alias, & Mail Host
- SRV – SRV Service Records
- Abbreviations and Gotchas
- $GENERATE, $ORIGIN, and $INCLUDE

LAB TASKS

- Use rndc to Control named
- Configuring BIND Zone Files

V. CREATING DNS HIERARCHIES

- Subdomains and Delegation
- Subdomains
- Delegating Zones
- in-addr.arpa. Delegation
- Issues with in-addr.arpa.
- RFC2317 & in-addr.arpa.

LAB TASKS

- Create a Subdomain in an Existing Domain
- Subdomain Delegation

VI. ADVANCED BIND DNS FEATURES

- Address Match Lists & ACLs
- Split Namespace with Views
- Restricting Queries
- Restricting Zone Transfers
- Running BIND in a chroot
- Dynamic DNS Concepts
- Allowing Dynamic DNS Updates
- DDNS Administration with nsupdate
- Common Problems
- Common Problems
- Securing DNS With TSIG

LAB TASKS

- Configuring Dynamic DNS
- Securing BIND DNS

GL275: Enterprise Linux Networking

Services

VII. USING APACHE

- HTTP Operation
- Apache Architecture
- Dynamic Shared Objects
- Adding Modules to Apache
- Apache Configuration Files
- httpd.conf – Server Settings
- httpd.conf – Main Configuration
- HTTP Virtual Servers
- Virtual Hosting DNS Implications
- httpd.conf – VirtualHost Configuration
- Port and IP based Virtual Hosts
- Name-based Virtual Host
- Apache Logging
- Log Analysis
- The Webalizer

LAB TASKS

- Apache Architecture
- Apache Content
- Configuring Virtual Hosts

VIII. APACHE SECURITY

- Virtual Hosting Security Implications
- Delegating Administration
- Directory Protection
- Directory Protection with AllowOverride
- Common Uses for .htaccess
- Symmetric Encryption Algorithms
- Asymmetric Encryption Algorithms
- Digital Certificates
- TLS Using mod_ssl.so

LAB TASKS

- Using .htaccess Files
- Using TLS Certificates with Apache
- Use SNI and TLS with Virtual Hosts

IX. APACHE SERVER-SIDE SCRIPTING ADMINISTRATION

- Dynamic HTTP Content
- PHP: Hypertext Preprocessor
- Developer Tools for PHP
- Installing PHP
- Configuring PHP
- Securing PHP
- Security Related php.ini Configuration
- Java Servlets and JSP
- Apache's Tomcat
- Installing Java SDK
- Installing Tomcat Manually
- Using Tomcat with Apache

LAB TASKS

- CGI Scripts in Apache
- Apache's Tomcat
- Using Tomcat with Apache
- Installing Applications with Apache and Tomcat

X. IMPLEMENTING AN FTP SERVER

- The FTP Protocol
- Active Mode FTP
- Passive Mode FTP
- ProFTPD
- Pure-FTPd
- vsftpd
- Configuring vsftpd
- Anonymous FTP with vsftpd

LAB TASKS

- Configuring vsftpd

GL275: Enterprise Linux Networking Services

XI. THE SQUID PROXY SERVER

- Squid Overview
- Squid File Layout
- Squid Access Control Lists
- Applying Squid ACLs
- Tuning Squid & Configuring Cache Hierarchies
- Bandwidth Metering
- Monitoring Squid
- Proxy Client Configuration

LAB TASKS

- Installing and Configuring Squid
- Squid Cache Manager CGI
- Proxy Auto Configuration
- Configure a Squid Proxy Cluster

XII. SQL FUNDAMENTALS AND MARIADB

- Popular SQL Databases
- SELECT Statements
- INSERT Statements
- UPDATE Statements
- DELETE Statements
- JOIN Clauses
- MariaDB
- MariaDB Installation and Security
- MariaDB User Account Management
- MariaDB Replication

LAB TASKS

- SQL with Sqlite3
- Installing and Securing MariaDB
- Creating a Database in MariaDB
- Create a Database Backed Application

XIII. LDAP CONCEPTS AND CLIENTS

- LDAP: History and Uses
- LDAP: Data Model Basics
- LDAP: Protocol Basics
- LDAP: Applications
- LDAP: Search Filters
- LDIF: LDAP Data Interchange Format
- OpenLDAP Client Tools
- Alternative LDAP Tools

LAB TASKS

- Querying LDAP

XIV. OPENLDAP SERVERS

- Popular LDAP Server Implementations
- OpenLDAP: Server Architecture
- OpenLDAP: Backends
- OpenLDAP: Replication
- Managing slapd
- OpenLDAP: Configuration Options
- OpenLDAP: Configuration Sections
- OpenLDAP: Global Parameters
- OpenLDAP: Database Parameters
- OpenLDAP Server Tools
- Native LDAP Authentication and Migration
- Enabling LDAP-based Login
- System Security Services Daemon (SSSD)

LAB TASKS

- Building An OpenLDAP Server
- Enabling TLS For An OpenLDAP Server
- Enabling LDAP-based Logins

GL275: Enterprise Linux Networking

Services

XV. SAMBA CONCEPTS AND CONFIGURATION

- Introducing Samba
- NetBIOS and NetBEUI
- Samba Daemons
- Accessing Windows/Samba Shares from Linux
- Samba Utilities
- Samba Configuration Files
- The smb.conf File
- Mapping Permissions and ACLs
- Mapping Linux Concepts
- Mapping Users
- Sharing Home Directories
- Sharing Printers
- Share Authentication
- Share-Level Access
- User-Level Access
- Samba Account Database
- User Share Restrictions

LAB TASKS

- Samba Share-Level Access
- Samba User-Level Access
- Samba Group Shares
- Handling Symbolic Links with Samba
- Samba Home Directory Shares

XVI. SMTP THEORY

- SMTP
- SMTP Terminology
- SMTP Architecture
- SMTP Commands
- SMTP Extensions
- SMTP AUTH
- SMTP STARTTLS
- SMTP Session

XVII. POSTFIX

- Postfix Features
- Postfix Architecture
- Postfix Components
- Postfix Configuration
- master.cf
- main.cf
- Postfix Map Types
- Postfix Pattern Matching
- Advanced Postfix Options
- Virtual Domains
- Postfix Mail Filtering
- Configuration Commands
- Management Commands
- Postfix Logging
- Logfile Analysis
- Postfix, Relaying and SMTP AUTH
- SMTP AUTH Server and Relay Control
- SMTP AUTH Clients
- Postfix / TLS
- TLS Server Configuration
- Postfix Client Configuration for TLS
- Other TLS Clients
- Ensuring TLS Security

LAB TASKS

- Configuring Postfix
- Postfix Virtual Host Configuration
- Postfix Network Configuration
- Postfix SMTP AUTH Configuration
- Postfix STARTTLS Configuration
- SUSE Postfix Configuration Cleanup

GL275: Enterprise Linux Networking Services

XVIII. MAIL SERVICES AND RETRIEVAL

- Filtering Email
- Procmail
- SpamAssassin
- Bogofilter
- amavisd-new Mail Filtering
- Accessing Email
- The IMAP4 Protocol
- Dovecot POP3/IMAP Server
- Cyrus IMAP/POP3 Server
- Cyrus IMAP MTA Integration
- Cyrus Mailbox Administration
- Fetchmail
- Roundcube Webmail
- Mailing Lists
- GNU Mailman
- Mailman Configuration

LAB TASKS

- Configuring Procmail & SpamAssassin
- Configuring Cyrus IMAP
- Dovecot TLS Configuration
- Configuring Roundcube
- Base Mailman Configuration
- Basic Mailing List
- Private Mailing List

XIX. NIS

- NIS Overview
- NIS Limitations and Advantages
- NIS Client Configuration
- NIS Troubleshooting Aids

LAB TASKS

- Using NIS for Centralized User Accounts
- Configuring NIS
- NIS Slave Server
- NIS Failover
- Troubleshooting Practice: NIS