Future Cert

LPIC-2: Linux Network Professional Certification

LPIC-2 Exam 202

LPIC-2 is the second certification in LPI's multi-level professional certification program. The LPIC-2 will validate your ability to administer small to medium–sized mixed networks. You must have an active LPIC-1 certification to receive LPIC-2 certification, but the LPIC-1 and LPIC-2 exams may be taken in any order.

To pass LPIC-2, you should be able to:

- Administer a small to medium-sized site
- Plan, implement, maintain, keep consistent, secure, and troubleshoot a small mixed (MS, Linux) network, including a:
  - LAN server (Samba, NFS, DNS, DHCP, client management)
  - Internet Gateway (firewall, VPN, SSH, web cache/proxy, mail)
  - Internet Server (web server and reverse proxy, FTP server)
- Supervise assistants
- Advise management on automation and purchases

TOPIC 207: DOMAIN NAME SERVER

207.1 Basic DNS server configuration (3)
Candidates should be able to configure BIND to function as a caching-only DNS server. This objective includes the ability to managing a running server and configuring logging.

Key knowledge areas:

- BIND 9.x configuration files, terms and utilities
- Defining the location of the BIND zone files in BIND configuration files
- Reloading modified configuration and zone files
- Awareness of dnsmasq, djbdns and PowerDNS as alternate name servers

207.2 Create and maintain DNS zones (3)
Candidates should be able to create a zone file for a forward or reverse zone and hints for root level servers. This objective includes setting appropriate values for records, adding hosts in zones and adding zones to the DNS. A candidate should also be able to delegate zones to another DNS server.

Key knowledge areas:

- BIND 9 configuration files, terms and utilities
- Utilities to request information from the DNS server
- Layout, content and file location of the BIND zone files
- Various methods to add a new host in the zone files, including reverse zones

207.3 Securing a DNS server (2)
Candidates should be able to configure a DNS server to run as a non-root user and run in a chroot jail. This objective includes secure exchange of data between DNS servers.

Key knowledge areas:

- BIND 9 configuration files
- Configuring BIND to run in a chroot jail
- Split configuration of BIND using the forwarders statement
- Configuring and using transaction signatures (TSIG)
- Awareness of DNSSEC and basic tools

TOPIC 208: WEB SERVICES

208.1 Implementing a web server (4)
Candidates should be able to install and configure a web server. This objective includes monitoring the server's load and performance, restricting client user access, configuring support for scripting languages as modules and setting up client user authentication. Also included is configuring server options to restrict usage of resources. Candidates should be able to configure a web server to use virtual hosts and customize file access.

Key knowledge areas:

- Apache 2.x configuration files, terms and utilities
- Apache log files configuration and content
- Access restriction methods and files
- mod_perl and PHP configuration
- Client user authentication files and utilities
- Configuration of maximum requests, minimum and maximum servers and clients
- Apache 2.x virtual host implementation (with and without dedicated IP addresses)
- Using redirect statements in Apache's configuration files to customize file access

208.2 Apache configuration for HTTPS (3)
Candidates should be able to configure a web server to provide HTTPS.

Key knowledge areas:

- SSL configuration files, tools and utilities
- Ability to generate a server private key and CSR for a commercial CA
- Ability to generate a self-signed Certificate from private CA
- Ability to install the key and Certificate
- Awareness of the issues with Virtual Hosting and use of SSL
- Security issues in SSL use

208.3 Implementing a proxy server (2)
Candidates should be able to install and configure a proxy server, including access policies, authentication and resource usage.

Key knowledge areas:

- Squid 3.x configuration files, terms and utilities
- Access restriction methods

Exam Objectives Version: Version 4.0 (last major update: November 1st, 2013, last minor formatting update: December 4th, 2014)

Exam Covered: LPIC-2 (LPI-202); Exam 2 of 2 to obtain LPIC-2 Linux Network Professional certification

Objectives Reflected in Published Exam: November 1st, 2013

Required Prerequisite: Successfully pass LPIC-1 101 and 102 exams, as well as LPI 201. The two LPIC-2 exams may be completed in any order, but candidates must pass both LPI-201 and LPI-202 in order to obtain the LPIC-2 certification.

About objective weights: Each objective is assigned a weighting value (x). The weights range roughly from 1 to 10 and indicate the relative importance of each objective. Objectives with higher weights will be covered in the exam with more questions.

- Client user authentication methods
- Layout and content of ACL in the Squid configuration files

208.4 Implementing Nginx as a web server and a reverse proxy (2)

Candidates should be able to install and configure a reverse proxy server, Nginx. Basic configuration of Nginx as a HTTP server is included.

Key knowledge areas:

- Nginx
- Reverse Proxy
- Basic Web Server

TOPIC 209: FILE SHARING

209.1 SAMBA Server Configuration (5)

Candidates should be able to set up a SAMBA server for various clients. This objective includes setting up Samba for login clients and setting up the workgroup in which a server participates and defining shared directories and printers. Also covered is a configuring a Linux client to use a Samba server. Troubleshooting installations is also tested.

Key knowledge areas:

- Samba 3 documentation
- Samba configuration files
- Samba tools and utilities
- Mounting Samba shares on Linux
- Samba daemons
- Mapping Windows usernames to Linux usernames
- User-Level and Share-Level security

209.2 NFS Server Configuration (3)

Candidates should be able to export filesystems using NFS. This objective includes access restrictions, mounting an NFS filesystem on a client and securing NFS.

Key knowledge areas:

- NFS version 3 configuration files
- NFS tools and utilities
- Access restrictions to certain hosts and/or subnets
- Mount options on server and client
- TCP Wrappers
- Awareness of NFSv4

TOPIC 210: NETWORK CLIENT MANAGEMENT

210.1 DHCP configuration (2)

Candidates should be able to configure a DHCP server. This objective includes setting default and per client options, adding static hosts and BOOTP hosts. Also included is configuring a DHCP relay agent and maintaining the DHCP server.

Key knowledge areas:

- DHCP configuration files, terms and utilities
- Subnet and dynamically-allocated range setup

210.2 PAM authentication (3)

The candidate should be able to configure PAM to support authentication using various available methods.

Key knowledge areas:

- PAM configuration files, terms and utilities
- passwd and shadow passwords

210.3 LDAP client usage (2)

Candidates should be able to perform queries and updates to an LDAP server. Also included is importing and adding items, as well as adding and managing users.

Key knowledge areas:

- LDAP utilities for data management and queries
- Change user passwords
- Querying the LDAP directory

210.4 Configuring an OpenLDAP server (4)

Candidates should be able to configure a basic OpenLDAP server including knowledge of LDIF format and essential access controls. An understanding of the role of SSSD in authentication and identity management is included.

Key knowledge areas:

- OpenLDAP
- Access Control
- Distinguished Names
- Changetype Operations
- Schemas and Whitepages
- Directories
- Object IDs, Attributes and Classes
- Awareness of System Security Services Daemon (SSSD)

TOPIC 212: SYSTEM SECURITY

212.1 Configuring a router (3)

Candidates should be able to configure a system to perform network address translation (NAT, IP masquerading) and state its significance in protecting a network. This objective includes configuring port redirection, managing filter rules and averting attacks.

Key knowledge areas:

- iptables configuration files, tools and utilities
- Tools, commands and utilities to manage routing tables.
- Private address ranges
- Port redirection and IP forwarding
- List and write filtering and rules that accept or block datagrams based on source or
- Destination protocol, port and address
- Save and reload filtering configurations
- Awareness of ip6tables and filtering

212.2 Securing FTP servers (2)

Candidates should be able to configure an FTP server for anonymous downloads and uploads. This objective includes precautions to be taken if anonymous uploads are permitted and configuring user access.

Key knowledge areas:

- Configuration files, tools and utilities for Pure-FTPd and vsftpd
- Awareness of ProFTPd
- Understanding of passive vs. active FTP connections

212.3 Secure shell (SSH) (4)

Candidates should be able to configure and secure an SSH daemon. This objective includes managing keys and configuring SSH for users. Candidates should also be able to forward an application protocol over SSH and manage the SSH login.

Key knowledge areas:

- OpenSSH configuration files, tools and utilities
- Login restrictions for the superuser and the normal users
- Managing and using server and client keys to login with and without password
- Usage of multiple connections from multiple hosts to guard against loss of connection to remote host following configuration changes

212.4 Security tasks (3)

Candidates should be able to receive security alerts from various sources, install, configure and run intrusion detection systems and apply security patches and bugfixes.

Key knowledge areas:

- Tools and utilities to scan and test ports on a server
- Locations and organizations that report security alerts as Bugtraq, CERT or other sources
- Tools and utilities to implement an intrusion detection system (IDS)
- Awareness of OpenVAS and Snort

212.5 OpenVPN (2)

Candidates should be able to configure a VPN (Virtual Private Network) and create secure point-to-point or site-to-site connections.

Key knowledge areas:

- OpenVPN