Préparation à la Certification LPIC-2 : Exam 202

Présentation

Type d'Action (Article L. 6313-1) : Action d'acquisition, d'entretien ou de perfectionnement des connaissances.
Objectif : Préparer la Certification LPIC-2 - Exam 202.
Public : Administrateurs Linux.
Pré requis : Etre certifié(e) LPIC-1. Avoir réussi l'examen 201.
Méthode d'apprentissage : Alternance entre un scénario pédagogique clair et précis et des travaux pratiques basés sur des cas et exemples concrets.
Validation des acquis : Évaluations à l'aide de tests auto-correctifs.
Type d'apprentissage : **Apprentissage Accéléré**.
Durée : 35 heures.
Formateur : Certifié **LPI**.
Moyens pédagogiques : Support de cours en ligne téléchargeable au format PDF.
Ressources : Machines virtuelles : CentOS 6, CentOS 7.

Programme

Jour #1

- **Gestion des Serveurs de Base** - 3 heures.
  - Le serveur DNS
  - Préparation à l'Installation
  - Installation
  - Les fichiers de configuration
    - named.ca
    - named.conf
  - Les Sections de Zone
    - La Valeur Type

        - La Valeur File
        - Exemples de Sections de Zone
        - Sections de Zones de votre Machine
        - Les fichiers de zone
            - db.fenestros.loc.hosts
            - db.2.0.10.hosts
    - rndc
        - La clef rndc
        - Fichiers de Configuration
    - LAB #1 - Mise en place du serveur bind
    - Le Serveur DHCP
        - Introduction
        - Installation
        - Configuration de base
        - Le fichier dhcpd.conf
        - LAB #2 - Mise en place du serveur DHCP
    - Le Serveur FTP
        - Installation
        - Configuration de base
        - /etc/ftpusers
        - Serveur vsftpd Anonyme
            - Configuration
        - Serveur vsftpd et Utilisateurs Virtuels
            - Introduction
            - Configuration
    - LAB #3 - Mise en place du serveur FTP

- **Gestion du Serveur Apache** - 4 heures.
    - Présentation et Configuration d'Apache
        - Présentation d'Apache 2
        - Testez le serveur Apache
        - Configuration de l'environnement global
        - Configuration du serveur principal
        - Gestion de serveurs virtuels

- Modules Additionnels
  - Les Connections Sécurisées avec mod_ssl
- Validation des acquis
- **Commandes** : named, httpd, openssl.

Jour #2

- **Gestion du Serveur NGINX** - 2 heures.
  - Présentation et Configuration
    - Présentation
    - Testez le serveur
    - Configuration de base
  - Reverse Proxy
- **Gestion du Serveur OpenLDAP** - 5 heures.
  - Présentation
    - Qu’est-ce que LDAP ?
      - Le Protocole X.500
      - LDAP v3
    - Comment fonctionne LDAP ?
      - Le Modèle d'Information de LDAP
      - Les DN et les RDN
    - La Structure d’un annuaire LDAP
      - Les Attributs
        - Les Attributs Utilisateur
        - Les Attributs Opérationnels
        - Les Classes d'Objets
          - Les Types de Classe d'Objets
        - Les OID
        - Les Schémas de l'Annuaire
  - Installation du serveur LDAP
  - Configuration de Démarrage du serveur LDAP
  - Configuration du serveur LDAP
    - L'annuaire Local

- L''annuaire Local avec des Referrals
- L'annuaire local avec réplication

- Fichier(s) de Configuration
  - Le Fichier slapd.conf
    - Les Directives du Fichier slapd.conf
      - include
      - allow
      - referral
      - pidfile
      - argsfile
      - modulepath
      - moduleload
      - TLSCACertificateFile, TLSCertificateFile & TLSCertificateKeyFile
      - security
      - access to
      - database config
      - backend
      - suffix DN
      - checkpoint
      - rootdn <DN>
      - rootpw <mot de passe>
      - directory
      - index
      - replogfile <filename>
      - replica host <hostname>[:<port>] [bindmethod={ simple | kerberos | sasl }]
    - Autres Directives Utiles
      - loglevel
      - password-hash
      - schemacheck
      - idletimeout
      - sizelimit
      - timelimit
      - readonly <on | off>
      - lastmod <on | off>

        - Le Fichier /etc/openldap/ldap.conf
        - cn=config
        - Sécuriser l'Annuaire
            - Créer le Mot de Passe de l'Administrateur
            - Sécuriser avec SSL
        - Options de la ligne de commande de slapd
    - Création et maintenance de la base de données
        - Le format LDIF
        - Création d’une base de données en ligne
            - La commande ldapadd
            - Utilisation du client graphique luma
            - Le Directory Information Tree
            - Les alias
            - Les attributs
            - Les classes
            - Les schémas
            - Les referrals
            - La commande ldapsearch
            - La commande ldapmodify
            - La commande ldapdelete
        - Création d’une base de données hors ligne
            - La commande slapadd
        - Maintenance d’une base de données LDAP
            - La commande slapcat
            - La commande slapindex
            - La commande slapdn
            - La commande slaptest
            - La commande slapauth
    - LAB #1 - Replication de Serveurs OpenLDAP
        - Préparation
        - Replication
            - Configuration du serveur fournisseur
            - Configuration du serveur consommateur
            - Mise en place

- LAB #2 - Authentification Apache en utilisant OpenLDAP
- Validation des acquis
- **Commandes** : ldapadd, ldapsearch, ldapmodify, ldapdelete, slapcat, slapindex, slapdn, slaptest, slapauth.

Jour #3

- **Gestion du Serveur Samba** - 5 heures.
  - **Les Réseaux Microsoft**,
    - Types de Réseaux Microsoft,
    - Types de Clients Windows,
  - **Présentation de Samba3**,
    - Daemons Samba,
    - Commandes Samba,
  - **Installation de Samba**,
    - Configuration de base,
    - Démarrage manuel de Samba,
    - Configuration de Samba,
    - Gestion des comptes et des groupes,
    - Création du fichier smbpasswd,
    - Comprendre la structure du fichier de configuration smb.conf,
    - Sécurité = share,
    - Sécurité = user,
    - Tester Samba,
  - **Samba en tant que PDC**,
    - Introduction,
    - Création des comptes utilisateurs,
    - Création des comptes machines,
    - smbusers,
    - Mise en place de scripts de connexion,
    - Configuration d'un poste Windows XP,
    - Mise en place de stratégies par groupe d'utilisateurs,
  - **Samba en tant que serveur d’impression**,
    - Cups,

        - Protocoles,
        - Daemon,
        - cupsd.conf,
        - Filtres,
        - Backends,
        - Journaux,
        - Imprimantes,
        - Administration,
            - lpstat,
            - lpadmin,
            - accept, cupsenable,
            - Classe d'imprimantes,
            - Le fichier /etc/cups/printers.conf,
            - Le fichier /etc/cups/classes.conf,
            - cancel,
            - lpmove,
        - Configuration de samba,
            - Le fichier /etc/printcap,
            - Modifications au fichier /etc/samba/smb.conf,
            - Le partage print$,
    - **Samba en tant que serveur membre d'un domaine**,
        - Installation du Serveur Windows 2008,
        - Installation de samba,
        - Ajout du rôle Gestion des identités pour Unix au Serveur Windows 2008,
        - Obtenir un ticket Kerberos pour le serveur Linux,
        - Configuration de samba,
        - Mettre le serveur samba dans le domaine,
        - Modifier le fichier /etc/nsswitch.conf,
        - Vérifier les service winbind,
        - Terminer la configuration de samba,
        - Modifier PAM,
    - **Samba4**,
        - Présentation,
        - Installation,

        - Configuration de base,
        - Démarrage manuel de Samba,
        - Configuration de Samba,
        - Configurer le DNS,
        - Tester le DNS avec Samba,
        - Configurer Kerberos,
        - Tester Kerberos,
        - Créer un Partage.
    - Validation des acquis,
    - **Commandes** : NBTSTAT (Windows™), samba, smbd, nmbd, winbindd, findsmb, net, nmblookup, pdbedit, rpcclient, smbcacls, smbclient, smbcontrol, smbmount , smbpasswd, smbspool, smbstatus, smbtar, smbumount, swat, testparm, testprns, wbinfo, poledit.exe (Windows™), cups, lpadmin, accept, reject, cupsenable, cupsdisable, lpstat, cancel, lpmove, lpinfo, lppasswd, kinit, klist, winbind, getent.

- **Gestion du Serveur NFS** - 2 heures
    - Présentation
        - Les Services et Processus du Serveur NFSv3
        - Options d'un Partage NFS
        - Commandes de Base
    - Mise en Place
        - Configuration du Serveur sous RHEL/CentOS 6
        - Configuration du Serveur sous RHEL/CentOS 7
        - Configuration du Client sous RHEL/CentOS 6
        - Configuration du Client sous RHEL/CentOS 7
    - Surveillance du Serveur
        - La Commande rpcinfo
    - Validation des acquis,
    - **Commandes** : nfs, nfslock, portmap, exportfs, nfsstat, rpcinfo, showmount, mount.

Jour #4

- **Gestion du Serveur Mandataire Squid** - 3 heures.
    - Installation
    - Configuration
    - L'Extension squidGuard

    - LAB #1 - Mise en place du serveur squid avec squidguard
        - Créer une whitelist
        - Dansguardian
    - Validation des acquis,
    - **Commandes** : squid, squid3, squidGuard dansguardian.

- **Gestion du Serveur Postfix** - 4 heures.
    - Configuration de base de sendmail,
    - Installation & Configuration de postfix,
        - Installation de postfix,
        - Configuration de Base,
        - Dovecot,
    - Configurations Supplémentaires de postfix,
        - Définir les Aliases,
        - SMTP AUTH,
        - SSL,
    - Antispam et Antivirus,
        - SpamAssassin,
        - ClamAV,
    - Mandataires,
        - Présentation de MailScanner,
        - Configuration du couple MailScanner/Postfix,
    - Validation des acquis,
    - **Commandes** : chkconfig, sendmail, postfix, telnet, dovecot, newaliases, perl, saslauthd, spamassassin, clamav, clamd, rpm-build, MailScanner.

Jour #5

- **Sécurité**
    - LAB #1 - Utilisation de nmap et de netcat
        - nmap
            - Installation
            - Options de la commande
            - Utilisation

- Fichiers de Configuration
- Scripts

- netcat
  - Installation
  - Options de la commande
  - Utilisation

- LAB #2 - Mise en place du Système de Détection d'Intrusion Snort
  - Installation
  - Options de la commande
  - Utilisation de snort en mode “packet sniffer”
  - Utilisation de snort en mode “packet logger”
  - Journalisation
  - Utilisation de snort en mode “NIDS”
- LAB #3 - Utilisation du Chiffrement
  - Introduction à la cryptologie
  - Définitions
  - Algorithmes à clé secrète
    - Le Chiffrement Symétrique
  - Algorithmes à clef publique
    - Le Chiffrement Asymétrique
  - La Clef de Session
  - Fonctions de Hachage
  - Signature Numérique
    - Utilisation de GnuPG
      - Présentation
      - Installation
      - Utilisation
  - PKI
    - Certificats X509
- LAB #4 - Mise en place de SSH et SCP
  - SSH
    - Introduction
    - SSH-1
    - SSH-2

                - L'authentification par mot de passe
                - L'authentification par clef asymétrique
                - Installation
                - Options de la commande
                - Configuration
                - Serveur
                - Client
                - Utilisation
            - Tunnels SSH
            - SCP
                - Introduction
                - Utilisation
                - Mise en place des clefs
    - LAB #5 - Mise en place d'un VPN avec OpenVPN
        - Présentation
        - Architecture de test
        - Configuration commune au client et au serveur
        - Configuration du client
        - Configuration du serveur
        - Tests
            - Du client vers le serveur
            - Du serveur vers le client
    - LAB #6 - Configuration du Pare-feu Netfilter/iptables
        - Introduction
        - Configuration par Scripts sous RHEL/CentOS 6
    - LAB #7 - La Configuration par firewalld sous RHEL/CentOS 7
        - La Configuration de Base de firewalld
        - La Configuration Avancée de firewalld
        - Le mode Panic de firewalld
    - LAB #8 - Forcer l'utilisation des mots de passe complexe avec PAM
        - Utiliser des Mots de Passe Complexe
        - Bloquer un Compte après N Echecs de Connexion
        - Configuration
    - LAB #9 - Mise en place du Système de Prévention d'Intrusion Fail2Ban

        - Installation
        - Configuration
        - Le répertoire /etc/fail2ban
        - Le fichier fail2ban.conf
        - Le répertoire /etc/fail2ban/filter.d/
        - Le répertoire /etc/fail2ban/action.d/
        - Commandes
    - LAB #10 - Mise en place d'Openvas
        - Présentation
        - Installation
        - Configuration
        - Utilisation
        - Analyse des Résultat
    - **Commandes** : nmap, netcat, snort, nessus, ssh,iptables, openvpn.