



Programme de l'examen LPI 202 - v4.5



Table des matières

1 - Objectifs de l'examen LPI 202.....	2
1.1 - Sujet 207 : Serveur de nom de domaine.....	2
207.1 Configuration de base d'un serveur DNS (valeur : 3).....	2
207.2 Création et mise à jour des zones DNS (valeur : 3).....	2
207.3 Sécurisation d'un serveur DNS (valeur : 2).....	3
1.2 - <i>Topic 208: HTTP Services</i>	3
208.1 Configuration élémentaire d'Apache (valeur : 4).....	3
208.2 Configuration d'Apache pour HTTPS (valeur : 3).....	4
208.3 Mise en place du serveur mandataire squid (valeur : 2).....	4
208.4 Mise en place de Nginx en tant que serveur Web et proxy inverse (valeur : 2).....	5
1.3 - <i>Sujet 209 : Partage de fichiers</i>	5
209.1 Configuration d'un serveur SAMBA (valeur : 5).....	5
209.2 Configuration d'un serveur NFS (valeur : 3).....	6
1.4 - <i>Sujet 210 : Gestion des clients réseau</i>	6
210.1 Configuration DHCP (valeur : 2).....	6
210.2 Authentification PAM (valeur : 3).....	7
210.3 Clients LDAP (valeur : 2).....	7
210.4 Configuration d'un serveur OpenLDAP (valeur : 4).....	7
1.5 - <i>Sujet 211 : Services de courrier électronique</i>	8
211.1 Utilisation des serveurs de messagerie (valeur : 4).....	8
211.2 Gestion de la distribution des courriels (valeur : 2).....	8
211.3 Gestion des accès aux boîtes aux lettres (valeur: 2).....	9
1.6 - <i>Sujet 212 : Sécurité du système</i>	9
212.1 Configuration d'un routeur (valeur : 3).....	9
212.2 Gestion des serveurs FTP (valeur : 2).....	10
212.3 Shell sécurisé (SSH) (valeur : 4).....	10
212.4 Tâches de sécurité (valeur : 3).....	11
212.5 OpenVPN (valeur : 2).....	11

1 - Objectifs de l'examen LPI 202

1.1 - Sujet 207 : Serveur de nom de domaine

207.1 Configuration de base d'un serveur DNS (valeur : 3)

Valeur	3
Description	Les candidats doivent être en mesure de configurer BIND pour fonctionner comme serveur DNS avec autorité sur une zone ainsi qu'en tant que serveur DNS de cache récursif. Cet objectif inclut la gestion d'un serveur en cours d'exécution et la configuration de la journalisation.

Domaines de connaissance les plus importants :

- *Fichiers, termes et utilitaires de configuration de BIND 9.x*
- *Détermination de l'emplacement des fichiers de zone dans les fichiers de configuration de BIND*
- *Actualisation après modification des fichiers de configuration ou de zone*
- *Connaissance de base de dnsmasq, djbdns et PowerDNS comme serveurs de nom alternatifs*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- */etc/named.conf*
- */var/named/*
- *rndc*
- *named-checkconf*
- *kill*
- *host*
- *dig*

207.2 Création et mise à jour des zones DNS (valeur : 3)

Valeur	3
Description	Les candidats doivent être capables de créer des fichiers de zone pour une zone directe ou une zone inverse ainsi que la zone d'indices (hints) pour les serveurs racine. Cet objectif inclut la définition de bonnes valeurs pour les enregistrements, l'ajout d'hôtes dans une zone et l'ajout de zones au DNS. Un candidat doit aussi être capable de déléguer des zones à un autre serveur DNS.

Domaines de connaissance les plus importants :

- *Fichiers, termes et utilitaires de configuration de BIND 9.x*
- *Utilitaires de requête sur les serveurs DNS*
- *Format, contenu et emplacement des fichiers de zone de BIND*
- *Différentes méthodes d'ajout de nouveaux hôtes dans les fichiers de zone, y compris dans les zones inversées*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- */var/named/*
- *syntaxe des fichiers de zone*
- *formats des enregistrements*
- *named-checkzone*
- *named-compilezone*

- *masterfile-format*
- *dig*
- *nslookup*
- *host*

207.3 Sécurisation d'un serveur DNS (valeur : 2)

Valeur	2
Description	Les candidats doivent être en mesure de configurer un serveur DNS afin qu'il s'exécute en tant qu'utilisateur non root et dans un environnement d'exécution restreint (chroot jail). Cet objectif inclut l'échange sécurisé de données entre des serveurs DNS.

Domaines de connaissance les plus importants :

- *Fichiers de configuration de BIND 9*
- *Configuration de BIND afin qu'il s'exécute dans un environnement restreint (chroot jail)*
- *Fractionnement de la configuration de BIND en utilisant l'instruction forwarders*
- *Configuration et utilisation des signatures de transaction (TSIG)*
- *Connaissance de base de DNSSEC et des outils basiques liés*
- *Connaissance de base de DANE et des enregistrements associés*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- */etc/named.conf*
- */etc/passwd*
- *DNSSEC*
- *dnssec-keygen*
- *dnssec-signzone*

1.2 - Topic 208: HTTP Services

208.1 Configuration élémentaire d'Apache (valeur : 4)

Valeur	4
Description	Les candidats doivent être en mesure d'installer et de configurer un serveur Web. Cet objectif inclut le contrôle de la charge et de la performance du serveur, la restriction d'accès aux utilisateurs, la configuration de la prise en charge via des modules des langages de scripts et le paramétrage de l'authentification utilisateur. La configuration des options du serveur pour restreindre l'accès aux ressources est également au programme. Les candidats doivent être en mesure de configurer un serveur Web avec des serveurs virtuels et de personnaliser les accès aux fichiers.

Domaines de connaissance les plus importants :

- *Fichiers, termes et utilitaires de configuration pour Apache 2.4*
- *Configuration et contenu des fichiers journaux Apache*
- *Méthodes et fichiers de restriction d'accès*
- *Configuration de mod_perl et de PHP*
- *Utilitaires et fichiers d'authentification utilisateur*
- *Configuration du nombre maximum de requêtes, des nombres minimums et maximums de serveurs et de clients*
- *Mise en place des serveurs virtuels (virtualhost) Apache 2.4, avec ou sans adresse IP dédiée*

- *Utilisation des déclarations de redirection dans la configuration d'Apache pour personnaliser l'accès aux fichiers*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- *journaux d'accès et d'erreurs*
- *.htaccess*
- *httpd.conf*
- *mod_auth_basic, mod_authz_host et mod_access_compat*
- *htpasswd*
- *AuthUserFile, AuthGroupFile*
- *apachectl, apache2ctl*
- *httpd, apache2*

208.2 Configuration d'Apache pour HTTPS (valeur : 3)

Valeur	3
Description	Les candidats doivent être en mesure de configurer un serveur web pour fournir un service HTTPS.

Domaines de connaissance les plus importants :

- *Fichiers de configuration, outils et utilitaires pour SSL*
- *Génération d'une clé privée et d'un CSR pour une autorité de certification commerciale*
- *Génération d'un certificat autosigné*
- *Installation de la clé et du certificat, y compris les autorités de certification intermédiaires*
- *Configuration des hôtes virtuels avec le module SNI*
- *Connaissance de base de aux problèmes liés à l'utilisation de SSL et des serveurs virtuels (virtual host)*
- *Problèmes de sécurité dans l'utilisation de SSL, désactivation des protocoles et des algorithmes de chiffrement non sécurisés*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- *Fichiers de configuration d'Apache2*
- */etc/ssl/, /etc/pki/*
- *openssl, CA.pl*
- *SSLEngine, SSLCertificateKeyFile, SSLCertificateFile*
- *SSLCACertificateFile, SSLCACertificatePath*
- *SSLProtocol, SSLCipherSuite, ServerTokens, ServerSignature, TraceEnable*

208.3 Mise en place du serveur mandataire squid (valeur : 2)

Valeur	2
Description	Les candidats doivent être en mesure d'installer et de configurer un serveur mandataire (proxy), y compris les règles d'accès, l'authentification et l'utilisation de ressource.

Domaines de connaissance les plus importants :

- *Fichiers, termes et utilitaires de configuration de Squid 3.x*
- *Méthodes de restriction d'accès*
- *Méthodes d'authentification utilisateur*

- *Format et contenu des ACL dans la configuration de Squid*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- *squid.conf*
- *acl*
- *http_access*

208.4 Mise en place de Nginx en tant que serveur Web et proxy inverse (valeur : 2)

Valeur	2
Description	Les candidats doivent être en mesure d'installer et de configurer un proxy inverse avec Nginx. La configuration élémentaire de Nginx en tant que serveur HTTP est incluse.

Domaines de connaissance les plus importants :

- *Nginx*
- *Proxy inverse*
- *Serveur Web*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- */etc/nginx/*
- *nginx*

1.3 - Sujet 209 : Partage de fichiers

209.1 Configuration d'un serveur SAMBA (valeur : 5)

Valeur	5
Description	Les candidats doivent être en mesure de paramétrer un serveur Samba pour différents clients. Cet objectif inclue la configuration de Samba comme serveur autonome ainsi que l'intégration en tant que membre d'un domaine Active Directory. De plus, la configuration de base CIFS et les partages d'imprimante sont couverts. La configuration d'un client Linux utilisateur du serveur Samba est aussi au programme. L'examen porte également sur la résolution de problème sur les installations.

Domaines de connaissance les plus importants :

- *Documentation de Samba 4*
- *Fichiers de configuration de Samba 4*
- *Outils et utilitaires Samba 4*
- *Montage des partages CIFS sous Linux*
- *Mise en correspondance des comptes utilisateur Windows avec les comptes utilisateurs Linux*
- *Sécurité aux niveaux utilisateur, partage et Active Directory*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- *smbd, nmbd, winbindd*
- *smbcontrol, smbstatus, testparm, smbpasswd, nmblookup*
- *samba-tool*
- *net*
- *smbclient*
- *mount.cifs*

- */etc/samba/*
- */var/log/samba/*

209.2 Configuration d'un serveur NFS (valeur : 3)

Valeur	3
Description	Les candidats doivent être en mesure d'exporter les systèmes de fichiers avec NFS. Cet objectif inclut les restrictions d'accès, le montage d'un système de fichiers NFS sur un client et la sécurisation du service NFS.

Domaines de connaissance les plus importants :

- *Fichiers de configuration NFS version 3*
- *Outils et utilitaires NFS*
- *Restrictions d'accès à certaines machines et/ou sous-réseaux*
- *Options de montage sur le serveur et les clients*
- *TCP Wrappers*
- *Connaissance de base de NFSv4*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- */etc/exports*
- *exportfs*
- *showmount*
- *nfsstat*
- */proc/mounts*
- */etc/fstab*
- *rpcinfo*
- *mountd*
- *portmapper*

1.4 - Sujet 210 : Gestion des clients réseau

210.1 Configuration DHCP (valeur : 2)

Valeur	2
Description	Les candidats doivent être en mesure de configurer un serveur DHCP. Cet objectif inclut le paramétrage des options par défaut et par client, l'ajout d'adresses statiques et l'ajout de postes clients BOOTP. La configuration d'agents relais DHCP et la maintenance des serveurs DHCP sont également au programme.

Domaines de connaissance les plus importants :

- *Fichiers, termes et utilitaires de configuration de DHCP*
- *Configuration de plages d'adresses par sous-réseaux et allouées dynamiquement*
- *Connaissance de base de DHCPv6 et des informations IPv6 aux routeurs (IPv6 Router Advertisements)*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- *dhcpd.conf*
- *dhcpd.leases*
- *Journaux DHCP dans syslog ou dans le journal systemd*

- *arp*
- *dhcpcd*
- *radvd*
- *radvd.conf*

210.2 Authentification PAM (valeur : 3)

Valeur 3

Description Les candidats doivent être en mesure de configurer PAM pour la prise en charge de l'authentification à partir des différentes méthodes disponibles. Cela inclut les fonctionnalités de base de SSSD.

Domaines de connaissance les plus importants :

- *Fichiers, termes et utilitaires de configuration de PAM*
- *Mots de passe *passwd* et *shadow**
- *Utilisation de *sssd* pour l'authentification LDAP*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- */etc/pam.d/*
- *pam.conf*
- *nsswitch.conf*
- *pam_unix, pam_cracklib, pam_limits, pam_listfile, pam_sss*
- *sssd.conf*

210.3 Clients LDAP (valeur : 2)

Valeur 2

Description Les candidats doivent être en mesure d'interroger et de mettre à jour les données d'un serveur LDAP. L'import et l'ajout d'éléments ainsi que l'ajout et la gestion des utilisateurs sont également au programme.

Domaines de connaissance les plus importants :

- *Utilitaires LDAP pour la gestion des données et les requêtes*
- *Modification des mots de passe utilisateurs*
- *Requêtes sur l'annuaire LDAP*

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- *ldapsearch*
- *ldappasswd*
- *ldapadd*
- *ldapdelete*

210.4 Configuration d'un serveur OpenLDAP (valeur : 4)

Valeur 4

Description Les candidats doivent être en mesure d'établir une configuration simple d'un serveur OpenLDAP, y compris la connaissance du format LDIF et l'essentiel des contrôles d'accès.

Domaines de connaissance les plus importants :

- *OpenLDAP*

- Configuration au sein de l'annuaire
- Contrôle d'accès
- DN (Distinguished Names)
- Opérations changetype
- Schémas et pages blanches
- Annuaire
- Identifiants objet (Object ID), attributs et classes

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- slapd
- slapd-config
- LDIF
- slapadd
- slapcat
- slapindex
- /var/lib/ldap/
- loglevel

1.5 - Sujet 211 : Services de courrier électronique

211.1 Utilisation des serveurs de messagerie (valeur : 4)

Valeur	4
Description	Les candidats doivent être en mesure de gérer un serveur de messagerie (e-mail), y compris la configuration des alias de courriel, la mise en place des quotas et la gestion des domaines virtuels. Cet objectif inclut la configuration de serveurs de relais internes et le contrôle des serveurs de messagerie.

Domaines de connaissance les plus importants :

- Fichiers de configuration de Postfix
- Configuration TLS de base pour postfix
- Connaissances de base du protocole SMTP
- Connaissance de base de sendmail et exim

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- Fichiers et commandes de configuration de Postfix
- /etc/postfix/
- /var/spool/postfix/
- Couche d'émulation des commandes sendmail
- /etc/aliases
- Journaux relatifs au courrier électronique dans /var/log

211.2 Gestion de la distribution des courriels (valeur : 2)

Valeur	2
Description	Les candidats doivent être en mesure de mettre en place des logiciels permettant de filtrer, trier et contrôler les courriels utilisateurs entrants.

Domaines de connaissance les plus importants :

- Compréhension des fonctionnalités, de la syntaxe et des opérateurs Sieve
- Utilisation de Sieve pour filtrer et trier les messages en fonction des expéditeurs, destinataires, entêtes et de la taille
- Connaissance de base de procmail

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- Opérateurs de condition et de comparaison
- keep, fileinto, redirect, reject, discard, stop
- Extension Dovecot vacation

211.3 Gestion des accès aux boîtes aux lettres (valeur: 2)

Valeur	2
Description	Les candidats doivent être en mesure d'installer et de configurer les services POP et IMAP.

Domaines de connaissance les plus importants :

- Configuration et administration de Dovecot en tant que serveur IMAP et POP3
- Configuration TLS de base pour Dovecot
- Connaissance de base de Courier

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- /etc/dovecot/
- dovecot.conf
- doveconf
- doveadm

1.6 - Sujet 212 : Sécurité du système

212.1 Configuration d'un routeur (valeur : 3)

Valeur	3
Description	Les candidats doivent être en mesure de configurer un système pour transférer des paquets IP et effectuer de la traduction d'adresse réseau (NAT, IP masquerading) ainsi que démontrer leur intérêt dans la protection d'un réseau. Cet objectif inclut la configuration de la redirection de ports, la gestion des règles de filtrage et la prévention des attaques.

Domaines de connaissance les plus importants :

- Fichiers, outils et utilitaires de configuration d'iptables et ip6tables
- Fichiers, outils et utilitaires de gestion des tables de routage.
- Plages d'adresses privées (IPv4), adresses locales uniques (Unique Local Addresses) ainsi que les adresses de lien local (Link Local Addresses) (IPv6)
- Redirection de ports et transmission IP (IP forwarding)
- Liste et écriture de règles et de filtres basés sur le protocole, l'adresse ou les ports source ou destination pour accepter ou bloquer des paquets IP
- Enregistrement et rechargement des configurations de filtrage

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- /proc/sys/net/ipv4/
- /proc/sys/net/ipv6/
- /etc/services
- iptables
- ip6tables

212.2 Gestion des serveurs FTP (valeur : 2)

Valeur	2
Description	Les candidats doivent être en mesure de configurer un serveur FTP pour le téléchargement et l'envoi de données anonymes. Cet objectif inclut les précautions à prendre dans le cas où les envois anonymes sont autorisés et la configuration des accès utilisateurs.

Domaines de connaissance les plus importants :

- Fichiers, outils et utilitaires de configuration de Pure-FTPd et vsftpd
- Connaissance de base de ProFTPd
- Compréhension des différences entre les connexions FTP passives et les connexions actives.

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- vsftpd.conf
- Options importantes de la ligne de commande de Pure-FTPd

212.3 Shell sécurisé (SSH) (valeur : 4)

Valeur	4
Description	Les candidats doivent être en mesure de configurer et de sécuriser un serveur SSH. Cet objectif inclut la gestion des clés et la configuration de SSH pour les utilisateurs. Les candidats devraient également être en mesure d'encapsuler un protocole applicatif sur SSH et de gérer les connexions SSH.

Domaines de connaissance les plus importants :

- Fichiers, outils et utilitaires de configuration d'OpenSSH
- Restrictions de connexions pour le superutilisateur et les utilisateurs normaux
- Gestion des clés serveur et client pour les connexions sans mot de passe
- Utilisation de multiples connexions à partir de multiples machines pour éviter les pertes de connexions distantes lors des changements de configuration

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- ssh
- sshd
- /etc/ssh/sshd_config
- /etc/ssh/
- Fichiers de clés privées et publiques
- PermitRootLogin, PubKeyAuthentication, AllowUsers, PasswordAuthentication, Protocol

212.4 Tâches de sécurité (valeur : 3)

Valeur

3

Description

Les candidats doivent être en mesure de recevoir les alertes de sécurité à partir de diverses sources, d'installer, configurer et exécuter des systèmes de détection d'intrusion et d'appliquer des correctifs de bogues ou de problèmes de sécurité.

Domaines de connaissance les plus importants :

- Outils et utilitaires permettant de balayer (scan) et de tester les ports sur un serveur
- Sites et organisations qui informent des alertes de sécurité comme Bugtraq, CERT ou d'autres sources
- Outils et utilitaires pour mettre en place un système de détection d'intrusion (IDS)
- Connaissance de base de OpenVAS et Snort

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- telnet
- nmap
- fail2ban
- nc
- iptables

212.5 OpenVPN (valeur : 2)

Valeur

2

Description

Les candidats doivent être en mesure de configurer un VPN (réseau privé virtuel) et de mettre en place des connexions de point à point ou de site à site sécurisées.

Domaines de connaissance les plus importants :

- OpenVPN

Liste partielle de termes, fichiers et utilitaires utilisés pour cet objectif :

- /etc/openvpn/
- openvpn