

Collection
Certifications

Préparation à la certification **LPIC-2**

LINUX

3^{ème} édition

EXAMENS LPI 201 et LPI 202

35 Travaux pratiques
127 Questions-réponses

OFFERT :
UN EXAMEN BLANC en ligne
avec réponses commentées et détaillées



Téléchargement
www.editions-eni.fr



Sébastien BOBILLIER
Philippe BANQUET

Les éléments à télécharger sont disponibles à l'adresse suivante :

<http://www.editions-eni.fr>

Saisissez la référence ENI du livre **CE3C2LIN** dans la zone de recherche et validez.

Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Descriptif

Chapitre 1	Introduction
A. La certification LPI	22
1. Intérêt de la certification	22
2. La certification LPI en quelques points	22
3. Le programme de la certification LPI	22
a. Niveau 1	22
b. Niveau 2	22
c. Niveau 3	23
4. Le passage d'examen	23
B. Contenu du livre	24
1. Les informations techniques	24
2. Les travaux pratiques	24
C. Préparation des travaux pratiques	25
1. Téléchargement des logiciels	25
2. Installation du serveur alpha	26
a. Éléments nécessaires	26
b. Création de la machine virtuelle	26
c. Personnalisation de la machine virtuelle	26
d. Démarrage de la machine virtuelle et installation du système	26
3. Installation du serveur beta	28
a. Éléments nécessaires	28
b. Création de la machine virtuelle	28
c. Personnalisation de la machine virtuelle	28
d. Démarrage de la machine virtuelle et installation du système	29
e. Personnalisation du système installé	30
4. Installation de la station de travail	30
a. Éléments nécessaires	30
b. Création de la machine virtuelle	30
c. Personnalisation de la machine virtuelle	31

d.	Démarrage de la machine virtuelle et installation du système	31
e.	Configuration de l'adresse IP de la station	31
5.	Ajout de périphériques supplémentaires à une machine existante	32
a.	Ajout de disque dur (SATA)	32
b.	Affectation du disque dur à la machine virtuelle	32
c.	Ajout de carte réseau	32
d.	Activation de la carte réseau sur la machine virtuelle	32

Chapitre 2

Gestion du stockage

A.	Gestion et configuration des systèmes de fichiers	35
1.	Gestion des systèmes de fichiers	35
a.	Les systèmes de fichiers courants	35
b.	Les systèmes de fichiers virtuels ou pseudo-filesystems	37
c.	Création des filesystems	38
d.	Vérification des filesystems	38
e.	Commandes spécialisées des filesystems ext	39
f.	Création de filesystems ext	39
g.	Affichage et modification des filesystems ext	39
h.	Dénomination des systèmes de fichiers	41
i.	Commandes spécialisées des filesystems XFS	42
2.	Gestion du swap	48
a.	Pourquoi le swap et en quelle quantité ?	48
b.	Optimisation du swap	49
3.	Montage des filesystems	51
a.	Montage et démontage	51
b.	Visualisation des filesystems montés	52
c.	Fichier fstab	52
d.	Automontage	54
4.	Protection des données stockées	56
a.	Protection au niveau fichier	56
b.	Protection au niveau disque ou partition	57
c.	Protection au niveau filesystem	58
5.	Gestion des disques durs	60
a.	Détermination des fichiers spéciaux	60
b.	Informations sur les périphériques de stockage	61
c.	Gestion des performances avec hdparm	63
d.	Gestion des défaillances matérielles	64

6.	Gestion des disques iSCSI	65
a.	Terminologie	65
b.	Paquetages iSCSI	66
c.	Linux client iSCSI	69
d.	Linux serveur iSCSI	74
B.	Sauvegardes	76
1.	Les utilitaires d'archivage	76
a.	La commande tar	76
b.	La commande cpio	77
2.	Les sauvegardes au niveau filesystem	79
a.	Sauvegardes de filesystems ext	79
b.	Sauvegardes de filesystems xfs	80
3.	Les logiciels de sauvegarde	82
a.	AMANDA	82
b.	Bacula	82
c.	BackupPC	82
d.	Les logiciels commerciaux	82
4.	Duplication et synchronisation de données	82
a.	Copie binaire avec dd	82
b.	Génération de fichiers ISO avec mkisofs	83
c.	Synchronisation de données avec rsync	84
C.	RAID	87
1.	Les principaux niveaux de RAID	87
a.	Le RAID 0	87
b.	Le RAID 1	87
c.	Le RAID 5	87
2.	Configuration du RAID	88
a.	Création du volume RAID	88
b.	Vérification d'un volume RAID	88
c.	Exploitation des volumes RAID	90
D.	Logical Volume Manager	90
1.	Architecture des volumes logiques	90
2.	Commandes LVM	91
a.	Création des éléments	91
b.	Diagnostics LVM	92
c.	Extension de volumes logiques	94
d.	Réduction de volumes logiques	95

3.	Exploitation des volumes logiques	96
a.	Données sur les volumes logiques	96
b.	Exploitation du snapshot LVM pour les sauvegardes	97
E.	Validation des acquis : questions/réponses	99
F.	Travaux pratiques	101
1.	Exploitation d'un espace de swap sur fichier	101
2.	Configuration d'un disque en RAID 0	105
3.	Création et exploitation d'un volume logique sur le disque RAID 0.	107
4.	Extension du volume logique	113
5.	Gestion d'un filesystem XFS.	116

Chapitre 3

Démarrage du système

A.	Le processus init et les niveaux d'exécution	129
1.	Les niveaux d'exécution	129
a.	Qu'est-ce qu'un niveau d'exécution ?	129
b.	Les niveaux d'exécution possibles	129
c.	Qui décide de ce qu'on met dans les différents niveaux ?	130
2.	Configuration du processus init.	130
a.	Le premier processus démarré sur le système	130
b.	Le fichier inittab	131
c.	Rappels sur le lancement des services.	132
d.	Liens entre les niveaux d'exécution et les services	133
e.	Gestion des niveaux d'exécution	133
f.	Commandes de gestion des liens de services.	134
g.	Script indépendant du niveau d'exécution : rc.local	135
3.	Utilisation des niveaux d'exécution	136
B.	Démarrage et chargement du noyau	136
1.	Le gestionnaire de démarrage GRUB.	136
a.	Configuration de GRUB 1	137
b.	Configuration de GRUB 2	138
c.	Le fonctionnement de GRUB	139
2.	Utilisation de GRUB 1 en mode interactif	139
a.	Édition des sections déjà présentes	139
b.	Chargement d'un noyau non listé	140
3.	Réinstallation de GRUB	140
a.	Réinstallation simple depuis un système actif.	140
b.	Réinstallation depuis un système non démarrable.	141

4.	Maintenance et mode single	142
a.	Passage en mode single planifié	142
b.	Ouverture d'un shell en cas d'échec au démarrage	142
5.	Les autres méthodes de chargement du noyau	142
a.	LILO	143
b.	ISOLINUX	144
c.	Démarrage PXE	144
C.	Validation des acquis : questions/réponses	145
D.	Travaux pratiques	147
1.	Création d'un niveau d'exécution sur mesure avec applications spécifiques	147
2.	Réinstallation de GRUB 1 après corruption	153

Chapitre 4

Gestion du réseau local

A.	Configuration du réseau	161
1.	Adressage IP	161
a.	Adressage IPv4 et notation CIDR	161
b.	Adressage IPv6	162
2.	Configuration universelle du réseau	163
a.	Détermination de l'interface réseau	163
b.	Affectation de l'adresse IP : ifconfig	164
c.	Configuration du client DNS : fichier /etc/resolv.conf	164
d.	Configuration de la passerelle par défaut : route	165
e.	Configuration du nom d'hôte : hostname	166
3.	Spécificités des distributions	166
a.	Configuration réseau dans /etc/network	166
b.	Configuration réseau dans /etc/sysconfig/network-scripts	167
4.	Autres commandes et fichiers de gestion du réseau	168
a.	Gestion des adresses MAC avec arp	168
b.	TCP Wrappers	169
5.	Configuration Wi-Fi	170
a.	Détermination de l'interface Wi-Fi	170
b.	Visualisation des réseaux disponibles	171
c.	Connexion à un réseau non sécurisé	172
B.	Diagnostic réseau	172
1.	Outils de diagnostic en couche réseau	172
a.	ping et ping6	172
b.	Indicateurs de la commande route	172
c.	traceroute	173

2.	Outils de diagnostic en couches transport et application	173
a.	netstat	173
b.	nc	174
3.	Diagnostics et informations en couche application	175
a.	lsof	175
b.	Journaux sur /var/log/syslog et /var/log/messages	175
4.	libpcap et les captures de paquets	176
a.	La bibliothèque libpcap	176
b.	tcpdump	176
c.	Wireshark	177
C.	Configuration automatique avec DHCP	178
1.	Le protocole DHCP	178
a.	Fonctionnement	179
b.	Le service DHCP sur les systèmes Linux	180
2.	Configuration du serveur	180
a.	Le fonctionnement général du serveur	180
b.	Les paramètres transmis aux clients	180
c.	Déclaration de plages d'adresses	181
d.	Paramètres spécifiques à une machine	181
e.	Serveurs à plusieurs interfaces	182
f.	Visualisation des baux DHCP	182
3.	Configuration du client	183
4.	Agent relais DHCP	184
a.	Principe du relais DHCP	184
b.	Configuration de l'agent de relais	184
D.	Validation des acquis : questions/réponses	185
E.	Travaux pratiques	187
1.	Configuration d'un serveur DHCP sur le serveur alpha	187
2.	Exploitation du service DHCP	190

Chapitre 5

Authentification des utilisateurs

A.	Évolution de l'authentification	197
1.	Les premiers systèmes Unix et le fichier passwd	197
a.	Mots de passe dans le fichier /etc/passwd	197
b.	Mots de passe dans le fichier /etc/shadow	197
2.	D'autres bases d'informations	197
3.	NSS	197
4.	Modules d'authentification	198

B. PAM	199
1. Le principe	199
2. Les modules PAM	200
a. Les principaux modules PAM	200
b. Fonctionnement en piles de modules	201
3. Configuration de PAM	201
a. Structure des fichiers de configuration	201
b. Les types d'action de PAM	202
c. Les comportements des modules	203
C. LDAP	204
1. Généralités	204
a. Les annuaires	204
b. Structure et terminologie	205
c. Schéma	205
d. Le protocole LDAP	206
e. Désignation des objets	206
f. Authentification auprès d'un annuaire LDAP	207
g. Le format LDIF	207
2. Le serveur OpenLDAP	207
a. Gestion du service	208
b. Configuration	208
3. Les outils clients LDAP	209
a. Recherche d'informations avec ldapsearch	209
b. Ajout d'objets dans un annuaire avec ldapadd	211
c. Modification d'objets existants avec ldapmodify	212
d. Suppression d'objets avec ldapdelete	212
e. Modification de mot de passe avec ldappasswd	212
f. Allègement des syntaxes pour les utilitaires clients LDAP	213
g. Clients graphiques	214
D. Authentification par LDAP des systèmes Linux	215
1. Configuration NSS	215
a. Configuration de la bibliothèque NSS pour LDAP	215
b. Renseignement des sources de noms	215
c. Vérification des sources de noms	215
2. Configuration PAM	216
a. Identification des services nécessaires	216
b. Configuration des fichiers PAM	216
E. Validation des acquis : questions/réponses	217

F. Travaux pratiques	219
1. Création et alimentation d'un annuaire LDAP sur le serveur beta	219
2. Authentification du poste de travail par l'annuaire LDAP.	228

Chapitre 6

Partage de fichiers

A. Partage de données avec NFS	233
1. Partage de répertoires	233
a. Observation des partages actifs.	233
b. Partage ponctuel	234
c. Service NFS et partage permanent	234
d. Options de partage	234
2. Configuration des clients	235
a. Affichage des partages distants.	235
b. Montage d'un répertoire distant	235
3. Gestion des identités	236
a. Les droits du client	236
b. Le cas particulier du superutilisateur.	236
B. Partage de données avec Samba	236
1. Configuration générale	236
a. Les démons Samba	236
b. Les fichiers de configuration.	237
c. Configuration globale	238
2. Partage de répertoire	238
3. Gestion des identités	239
a. Algorithmes de hachage et stockage des mots de passe	239
b. Authentification auprès des serveurs Samba	240
c. Génération des mots de passe MD4	240
d. Synchronisation avec les mots de passe Linux.	240
e. Suppression ou désactivation d'un compte Samba.	240
4. Le client Samba	241
a. Exploitation ponctuelle de ressources avec smbclient.	241
b. Montage d'un partage SMB avec smbmount	242
c. Montage d'un partage CIFS.	243
C. Partage de fichiers avec FTP	243
1. Le protocole FTP	243
a. Historique	243
b. Paramètres techniques.	244
c. Modes FTP actif et FTP passif.	244

2. Les clients FTP	244
a. Les clients FTP graphiques.	244
b. Le client FTP en lignes de commande	244
3. Le serveur Pure-FTPd	245
a. Fonctionnement pour accès des utilisateurs à leurs répertoires personnels	245
b. Fonctionnement en accès anonyme	245
c. Options de fonctionnement	245
4. Le serveur vsftpd	246
D. Validation des acquis : questions/réponses	246
E. Travaux pratiques	248
1. Mise en place de partages Samba sur le serveur alpha	248
2. Mise en place de partages NFS sur le serveur beta	253
3. Configuration d'un serveur FTP sur le serveur alpha.	255

Chapitre 7**Résolution de noms DNS**

A. Généralités	261
1. Les débuts de la résolution de noms et l'apparition du DNS.	261
2. Concept de zones DNS	261
3. Mécanisme de la résolution de noms	262
4. Les enregistrements	264
a. Enregistrement de type A	264
b. Enregistrement de type AAAA	264
c. Enregistrement de type PTR	264
d. Enregistrement de type CNAME	265
e. Enregistrement de type MX	265
f. Enregistrement de type SOA	265
g. Enregistrement de type NS	265
5. DNS sur Linux	266
a. Le serveur DNS	266
b. Le client DNS.	266
B. Configuration de base du serveur	266
1. Fonctionnement du serveur BIND	266
a. Structure du fichier named.conf et principaux éléments de configuration	266
b. Les fichiers de définition de zone préinstallés	267
2. Serveur de cache	268
a. Configuration du serveur de cache	269
b. Redirection	269
3. Commande de pilotage rndc	269

C. Gestion de zones DNS	270
1. Gestion de zones locales	270
a. Création d'un fichier de zone directe	270
b. Création d'un fichier de zone inverse	271
c. Création d'enregistrements dans les fichiers de zone	272
d. Déclaration de zone principale dans le fichier named.conf	273
e. Prise en compte de la nouvelle configuration	273
2. Gestion de zones secondaires	273
a. Déclaration de la zone secondaire dans named.conf	273
b. Prise en compte de la nouvelle configuration	274
3. Délégation de zone	274
4. Outils de test	275
a. ping	275
b. nslookup	275
c. dig	276
d. host	277
e. time	278
D. Sécurisation du DNS	279
1. Limitation des clients	279
2. Utilisation d'un compte de service	279
a. Pourquoi un compte de service ?	279
b. Lancement de named avec un compte de service	279
3. BIND en mode chroot	280
a. Pourquoi enfermer le processus ?	280
b. Création de l'environnement nécessaire	280
c. Lancement du programme en mode chroot	281
4. Échange sécurisé entre serveurs	281
a. Génération du secret partagé	281
b. Déclaration du secret dans named.conf	282
c. Les deux serveurs doivent utiliser la clé	283
d. Tout service est refusé en l'absence de signature	283
E. Validation des acquis : questions/réponses	283
F. Travaux pratiques	285
1. Installation d'un serveur DNS	285
2. Configuration du serveur de cache	287
3. Création de zones personnalisées directes et inverses	289
4. Interrogation du serveur	292
5. Création d'un serveur secondaire	294

Chapitre 8

Serveurs web

A. Configuration de base d'un serveur Apache	301
1. Apache et les serveurs web	301
2. Fichier de configuration	301
a. Format du fichier de configuration	301
b. Les directives de conteneur	302
c. Validation de la syntaxe	303
d. Démarrage et arrêt du serveur	303
3. Les modules Apache	303
a. Chargement des modules	303
b. Visualisation des modules	304
c. Choix des modules	305
4. Gestion des ressources	306
B. Hôtes virtuels d'un serveur Apache	307
1. Configuration globale	307
a. Gestion des contenus	307
b. Organisation des sites virtuels	307
2. Configuration des hôtes virtuels	307
a. Hôtes virtuels sur adresse IP	308
b. Hôtes virtuels sur nom d'hôte	308
C. Restriction de l'accès utilisateur d'un serveur Apache	309
1. Restriction de l'accès aux pages web	309
a. Déclaration du répertoire à protéger	309
b. Directives d'authentification	310
2. Authentification locale	310
a. Création d'une base de comptes locale	310
b. Chargement des modules d'authentification	311
c. Configuration de l'authentification locale	311
3. Authentification par annuaire LDAP	312
a. Vérification de la disponibilité des informations de l'annuaire	312
b. Chargement des modules nécessaires	313
c. Configuration de l'authentification	313
4. Authentification simple par fichier .htaccess	313
D. Configuration d'Apache avec SSL	315
1. Cryptographie et certificats	315
a. Concepts cryptographiques	315
b. Les certificats numériques X509	315
c. Génération locale d'un certificat	316

2.	Configuration SSL d'un serveur Apache	317
a.	Chargement du module SSL	317
b.	Configuration des clés de serveur	317
c.	Gestion du fonctionnement SSL	318
d.	Authentification des clients par certificat	318
E.	Serveur proxy Apache.	318
1.	Les serveurs proxy	318
a.	Protection des clients	319
b.	Serveurs de cache	319
c.	Filtrages	319
d.	Inconvénients	319
2.	Le serveur proxy squid.	319
a.	Configuration de base	319
b.	Gestion des accès clients	321
F.	Configuration de base d'un serveur Nginx	323
1.	Nginx et les serveurs web	323
2.	Fichier de configuration	323
a.	Format du fichier de configuration	323
b.	Directives générales	324
c.	Règles de syntaxe	327
d.	Validation de la syntaxe	327
e.	Configuration par défaut de type Debian	328
f.	Démarrage et arrêt du serveur	328
3.	Les modules Nginx	329
a.	Chargement des modules	329
b.	Visualisation des modules	329
c.	Choix des modules	330
4.	Gestion des ressources	332
5.	Nginx et les expressions régulières	333
G.	Hôtes virtuels d'un serveur Nginx	338
1.	Configuration globale	338
2.	Configuration des hôtes virtuels	339
a.	Hôtes virtuels sur adresses IP/numéros de port	339
b.	Hôtes virtuels sur nom d'hôte	340
H.	Les filtres d'URI de Nginx : le bloc de type location.	341
1.	Définition d'un bloc location de sélection d'URI	342
a.	Syntaxe	342
b.	Priorité de sélection	342

c. Exemples de sélection	343
2. Bloc de location nommé	345
I. Restrictions de l'accès utilisateur d'un serveur Nginx	345
1. Contrôle par adresse IP	346
2. Contrôle par authentification	348
3. Contrôle par authentification locale	349
a. Choix de la portée de la restriction d'accès simple	349
b. Directives d'authentification	349
c. Création d'une base de comptes locale	350
4. Authentification par LDAP	351
a. Utilisation de PAM	351
b. Sous-requête	351
c. Module LDAP	351
J. Configuration de Nginx avec SSL	352
1. Configuration d'un serveur virtuel SSL	352
2. Optimisation d'un serveur SSL	354
K. Gestion des pages dynamiques avec un serveur Nginx	355
1. Les modules FastCGI	355
2. Configuration de FastCGI	355
L. Nginx en reverse proxy	356
1. Reverse proxy	356
2. Le module ngx_http_proxy	357
3. Déclaration du serveur cible	357
4. Sélection des demandes à rediriger	358
a. Sélection par un bloc location utilisant une expression régulière	358
b. Sélection par la directive try_files	358
c. Sélection par la directive fastcgi_pass	359
M. Répartition de charge avec un serveur Nginx	359
1. Le bloc upstream	359
2. Utilisation d'une grappe de serveurs	361
N. Validation des acquis : questions/réponses	361
O. Travaux pratiques	364
1. Configuration d'un serveur web avec deux sites virtuels	366
2. Contrôle d'accès par mot de passe sur un site en SSL	371
3. Mise en place d'un serveur proxy sur le serveur alpha	375
4. Mise en place d'un serveur Nginx sur le serveur alpha	378

Chapitre 9	Messagerie
A. Les MTA	395
1. Le protocole SMTP	395
2. Présentation de Sendmail.	396
3. Présentation d'Exim	396
4. Présentation de Postfix	396
B. Le serveur SMTP Postfix.	396
1. Configuration de Postfix	396
a. Gestion des identités	396
b. Gestion des alias	397
c. La commande postfix	397
d. Les fichiers de configuration	398
e. Vérification de la configuration active	399
2. Gestion de domaines virtuels	399
a. Définition des domaines virtuels	399
b. Gestion des identités pour les domaines virtuels	399
3. Gestion de quotas	400
C. Remise locale des messages	400
1. La commande mail	401
a. Envoi de courrier avec la commande mail	401
b. Lecture de courrier avec la commande mail	402
2. Formats mbox et maildir	403
a. Le format mbox	403
b. Le format maildir	403
c. Utilisation du format maildir par Postfix	403
3. procmail	404
a. Demander à Postfix d'utiliser procmail	404
b. Configurer procmail	404
4. Alternatives à la messagerie	405
a. write et wall	405
b. issue et issue.net	405
c. motd	405
D. Remise distante des messages	406
1. Fonctionnement conjoint de MTA, de MDA et de MUA	406
a. Le protocole POP3	406
b. Le protocole IMAP4	406

2. Serveurs Courier-IMAP et Courier-POP	406
a. Format de messages pour les services courrier	406
b. Configuration des services	406
c. Validation de l'authentification	407
3. Serveur Dovecot	408
a. Configuration de Dovecot	408
b. Visualisation de la configuration	408
E. Validation des acquis : questions/réponses	409
F. Travaux pratiques	411
1. Gestion des envois	411
2. Gestion des retraits	416

Chapitre 10**Protection des réseaux**

A. Routage et filtrage	425
1. Configuration d'un serveur Linux en tant que routeur	425
a. Activation du routage sur un serveur Linux	425
b. Consultation de la table de routage	425
c. Gestion des routes statiques	426
2. iptables.	427
a. Les tables	427
b. Les chaînes.	428
c. Les actions	428
d. Le traitement des règles	428
B. Administration d'un pare-feu avec les iptables.	429
1. Politiques.	429
a. Principe des politiques de pare-feu	429
b. Configuration d'une politique de base.	430
2. Filtrage de paquets	430
a. Politique et règles	430
b. Création de règles	430
c. Gestion des règles	431
d. Gestion des flux retour	432
3. Gestion du NAT	433
a. Rappel sur le principe du NAT.	433
b. Diagnostic de la configuration NAT d'un routeur.	434
c. Connexion d'un réseau privé à un réseau public	434

4.	Scripts de configuration des règles de filtrage	435
a.	Red Hat et les iptables	435
b.	Création de services personnalisés de pare-feu avec les iptables	435
C.	Détection des intrusions et des vulnérabilités	436
1.	Les systèmes IDS	436
a.	Les limitations des pare-feu	436
b.	Techniques d'analyse	436
c.	Sources d'information	437
2.	Snort	437
a.	Les composants	437
b.	Gestion des sources d'information	438
c.	Gestion des alertes	438
3.	OpenVAS	438
a.	Le serveur OpenVAS	438
b.	Les clients OpenVAS	438
c.	Récupération des vulnérabilités	439
D.	Validation des acquis : questions/réponses	439
E.	Travaux pratiques	441
1.	Restructuration du réseau local	441
2.	Configuration d'un routeur et pare-feu sur le serveur beta	447

Chapitre 11

Sécurisation du trafic

A.	OpenSSH	455
1.	Utilisations de OpenSSH.	455
2.	Gestion des authentifications	455
a.	Authentification par mot de passe	455
b.	Authentification par clés	456
c.	L'agent SSH	457
3.	Confidentialité des communications	458
a.	Session interactive avec SSH.	458
b.	Copie de fichiers avec SSH	459
c.	Utilisation d'applications dans des tunnels SSH	459
d.	Renvoi de sessions X11 via SSH.	460
B.	OpenVPN.	461
1.	Les modes de fonctionnement OpenVPN	461
a.	Authentification.	461
b.	Confidentialité	461

c. Fonctionnement réseau	461
2. Création d'un tunnel point-à-point	462
a. Gestion de l'authentification	462
b. Fichiers de configuration	462
c. Mise en œuvre du tunnel VPN	463
C. Validation des acquis : questions/réponses	464
D. Travaux pratiques	466
1. Gestion du réseau de test	466
2. Création d'un tunnel SSH entre la station de travail et le serveur beta	468
3. Création d'un tunnel VPN entre la station de travail et le serveur beta	471

Chapitre 12

Compilation des applications et du noyau Linux

A. Compilation des applications	479
1. Généralités	479
a. Principe de la compilation	479
b. Quand faut-il compiler ?	479
c. Rappels sur les utilitaires de décompression	479
2. Procédure de compilation GNU	480
a. Récupération des sources	480
b. Configuration de la compilation	480
c. Personnalisation des programmes compilés	481
d. Compilation	482
e. Les cibles de la commande make	483
f. Installation des binaires	483
g. Nettoyage des sources	483
h. Désinstallation d'un programme	484
3. Environnement des applications	484
a. Les bibliothèques	484
b. Visualisation des appels système	486
B. Compilation du noyau	487
1. Les composants du noyau	487
a. Le cœur de noyau	487
b. Les modules	487
c. Autour du noyau	489
d. Gestion des versions du noyau	489

2.	Procédure de compilation et d'exploitation	490
a.	Récupération des sources	490
b.	Génération du fichier de réponse	490
c.	Compilation du noyau et des modules	493
d.	Installation des modules	493
e.	Installation du noyau	494
f.	Création du ramdisk des modules	494
g.	Configuration du gestionnaire de démarrage	495
C.	Patch du noyau	495
1.	Ajout de patches	495
2.	Retrait de patches	497
D.	Validation des acquis : questions/réponses	497
E.	Travaux pratiques	499
1.	Compilation d'une application	499
2.	Compilation et installation d'un module de noyau	502
3.	Patcher une application	505
4.	Compilation et installation d'un nouveau noyau	507

Chapitre 13

Gestion et planification des ressources

A.	Gestion des ressources	515
1.	Types de ressources	515
2.	Sources d'information sur les ressources	515
a.	Les pseudo-systèmes de fichiers procfs et sysfs	515
b.	Les journaux du système	520
c.	Les commandes de suivi instantané	521
3.	Surveillance et suivi des ressources processeur	522
a.	Informations sur les ressources processeur	522
b.	Utilisation des ressources processeur	525
c.	Diagnostiquer une surutilisation du processeur	533
4.	Surveillance et suivi de la mémoire vive	535
a.	Informations sur la mémoire	535
b.	Utilisation de la mémoire	536
c.	Diagnostiquer une surconsommation de la mémoire	540
5.	Surveillance et suivi des ressources disques	541
a.	Informations sur les ressources disques	541
b.	Utilisation des ressources disques	552

6. Surveillance et suivi des ressources réseau	558
a. Informations sur les ressources réseau	558
b. Suivi et diagnostic des ressources réseau	560
B. Gestion prévisionnelle des ressources.	563
1. Le paquetage sysstat	563
a. La collecte d'informations avec sysstat	563
b. La commande sar	564
2. Le démon collectd	566
a. Installation	566
b. Configuration	567
c. Exploitation des données de collectd	569
3. Les solutions de supervision	571
C. Validation des acquis : questions/réponses	573
D. Travaux pratiques	574
1. Surveillance des ressources d'un serveur	574
2. Planification de charge	587
Tableau des objectifs	597
Index	601

Chapitre 5

A. Évolution de l'authentification	197
B. PAM	199
C. LDAP	204
D. Authentification par LDAP des systèmes Linux	215
E. Validation des acquis : questions/réponses	217
F. Travaux pratiques	219

Pré-requis

Les connaissances acquises lors de la certification LPI niveau 1, notamment :

- Connaître la structure du fichier `/etc/passwd`.
- Connaître l'existence et le principe du fichier `hosts`.

Objectifs

À la fin de ce chapitre, vous serez en mesure de :

- Interpréter une configuration NSS.
- Comprendre l'authentification modulaire PAM.
- Connaître les principaux modules PAM.
- Modifier la configuration PAM pour permettre un changement du mode d'authentification.
- Connaître le format de fichier LDIF.
- Interroger un annuaire LDAP.
- Gérer les mots de passe dans un annuaire OpenLDAP.
- Ajouter ou modifier des éléments d'un annuaire OpenLDAP.
- Configurer l'authentification d'un système Linux sur un annuaire OpenLDAP.

A. Évolution de l'authentification

1. Les premiers systèmes Unix et le fichier `passwd`

a. Mots de passe dans le fichier `/etc/passwd`

Depuis le début de leur existence, les systèmes Unix utilisent le fichier `/etc/passwd` comme base de comptes des utilisateurs. Ce fichier est utilisé naturellement pour les ouvertures de session sur le système. Comme son nom l'indique encore, il contenait en plus des identifiants utilisateurs leurs mots de passe chiffrés. Si des éléments logiciels autres que l'ouverture de session ont besoin des informations de compte (connexion ftp, ouverture de session distante, etc.), ils vont également consulter ce fichier. Dans cette situation originelle simple, on a affaire à une base de comptes unique et des applications multiples qui exploitent cette base de comptes. Toutes les applications doivent reconnaître le format de cette base d'information.

b. Mots de passe dans le fichier `/etc/shadow`

Avec l'évolution des techniques d'attaques des mots de passe, le besoin est venu de placer les mots de passe dans un fichier non accessible aux utilisateurs ordinaires. Ils sont alors stockés dans un fichier `/etc/shadow` fermé aux utilisateurs. Les paramètres d'authentification avec shadow sont gérés par un fichier `/etc/login.defs`. Les paramètres présents par défaut dans ce fichier sont en général satisfaisants.

Gestion des erreurs d'authentification dans le fichier `login.defs`

Parmi les nombreux paramètres du fichier `login.defs`, ceux concernant le login sont les plus fréquemment modifiés.

```
toto@ubuntu:~$ grep LOGIN /etc/login.defs
LOGIN_RETRIES      5
LOGIN_TIMEOUT      60
toto@ubuntu:~$
```

2. D'autres bases d'informations

Pour la consultation des éléments d'identification, la situation s'est compliquée quand il a fallu intégrer d'autres bases de comptes, différentes du fichier `passwd` et surtout plus complexes. Ces bases d'identités sont souvent centralisées, comme c'est le cas pour NIS (*Network Information Server*) ou LDAP (*Lightweight Directory Access Protocol*). La première solution envisagée fut naturellement de réécrire les programmes qui exploitaient initialement le fichier `/etc/passwd` afin qu'ils soient capables de consulter les bases centralisées sur le réseau. Cette méthode manquait cruellement de souplesse, puisqu'elle obligeait à reprendre beaucoup de programmes en profondeur à chaque fois qu'une modification était apportée au mode de stockage des bases centralisées.

3. NSS

NSS (*Name Service Switch*) est une première réponse à la multiplicité des bases d'information locales ou centralisées. NSS a pour objet de normaliser la résolution de noms au sein d'un système. NSS permet de résoudre un nom en une autre information associée, comme par exemple un nom d'utilisateur et son uid, un nom de groupe et son gid, ou encore un nom d'hôte et son adresse IP.

Dans un fonctionnement NSS, un fichier **/etc/nsswitch.conf** détermine pour différents types de résolutions la source d'information à privilégier, et les applications ayant besoin de ces informations vont consulter les sources dans l'ordre imposé par le fichier **nsswitch.conf**. La résolution s'appuie alors sur des bibliothèques NSS (**libnss_X.so** où X représente le service de résolution employé), et les applications n'ont pas besoin de connaître directement la méthode de résolution employée.

Format du fichier nsswitch.conf

résolution: source_1 source_n

nsswitch.conf : format du fichier	
<i>résolution</i>	Le type de résolution à effectuer.
<i>source_1</i>	Obligatoire. La première source de résolution à employer.
<i>source_n</i>	Facultatif. La ou les autres sources de résolution possibles à utiliser après la première.

Exemple de fichier nsswitch.conf

On voit dans cet exemple que les résolutions de type passwd, group et shadow feront leur résolution grâce à la bibliothèque libnss_compat.so, alors que la résolution de noms d'hôtes se fera par les bibliothèques libnss_files.so et libnss_dns.so. Ce qui veut dire que les éléments d'identification des utilisateurs seront trouvés dans les fichiers locaux de /etc, alors que la résolution de noms d'hôtes s'appuiera d'abord sur le fichier local (/etc/hosts) avant de se reporter sur un service dns.

```
passwd:          compat
group:          compat
shadow:        compat

hosts:          files dns
networks:       files

protocols:     db files
services:      db files
ethers:        db files
rpc:           db files

netgroup:      nis
```

☞ Sur un système Linux moderne, NSS n'est plus utilisé que pour des opérations d'identification, c'est-à-dire trouver des informations sur une identité. Tout ce qui relève de l'authentification est dévolu à un mécanisme plus élaboré : PAM.

4. Modules d'authentification

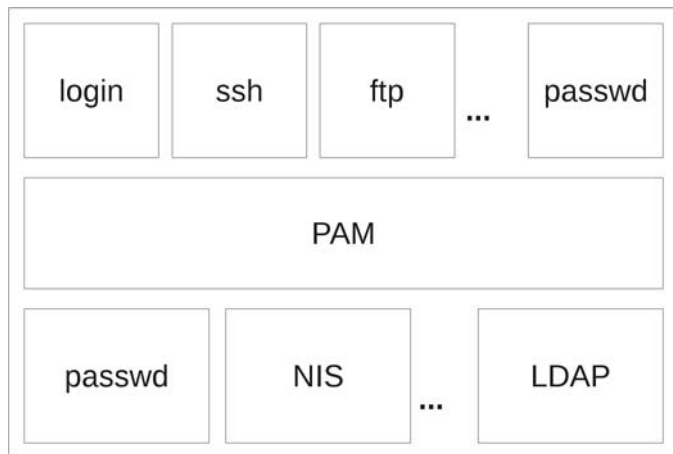
Si NSS représente déjà un progrès par rapport aux fichiers statiques utilisés dans les premiers temps, la révolution viendra avec PAM (*Pluggable Authentication Module*). PAM est un mécanisme complémentaire de NSS qui assure une authentification sur mesure par l'exécution de modules au choix de l'administrateur.

Lors d'une ouverture de session Linux, l'utilisateur va présenter un identifiant et un mot de passe. Grâce à la résolution NSS, on en déduira les identifiants uid/gid, ainsi que les autres paramètres nécessaires (date d'expiration, etc.). PAM de son côté va en fonction de sa configuration exécuter des modules pour assurer l'authentification mais aussi éventuellement pour effectuer certaines tâches liées à l'ouverture de session, comme la définition de variables par exemple.

B. PAM

1. Le principe

PAM se positionne en interface entre les applications et les méthodes d'authentification.



Le principal objectif de PAM est de proposer une couche d'abstraction entre les applications et les méthodes d'authentification. Ainsi, une application qui se veut souple et évolutive quant aux méthodes d'authentification qu'elle emploie n'aura d'autre besoin que d'être compatible avec PAM. Cela signifie qu'elle devra être capable de s'adresser à la couche d'authentification PAM, et le reste ne la regarde pas. En parallèle, les procédés d'authentification quels qu'ils soient, doivent être exploitables par la mécanique PAM.

Une application demande à PAM si un utilisateur peut se connecter. PAM en fonction de sa configuration, appelle des modules fonctionnels qui vont exploiter une méthode d'authentification. Si le résultat est positif (l'utilisateur a fourni les bons éléments d'authentification), PAM renvoie l'autorisation de connexion à l'application.

PAM a un autre avantage. Nous venons de voir que la demande d'authentification entraînait le chargement de modules. Il se trouve que le nombre de ces modules n'est pas limité et qu'ils peuvent être cumulés. Il est donc tout à fait possible de demander une double authentification selon deux méthodes différentes. De plus, on peut profiter de la séquence d'authentification sous PAM pour provoquer le chargement de bibliothèques sans rapport avec l'authentification. De nombreuses actions peuvent donc être gérées dès l'authentification réussie.

En résumé : lors de la demande d'authentification, des modules PAM sont chargés en fonction d'un fichier de configuration, et ces modules provoquent certaines actions, relevant de l'authentification proprement dite ou d'autres actions.

2. Les modules PAM

a. Les principaux modules PAM

Les modules PAM, appelés lors des opérations d'authentification sont nombreux et d'usages variés. Certains d'entre eux sont néanmoins rencontrés très fréquemment et leur existence est à connaître. D'autres sont plus ou moins fréquents selon les distributions, mais connaître leur fonctionnement et leurs objectifs permet de mieux comprendre la mécanique et la philosophie de PAM.

Ces modules sont dans des fichiers dont l'emplacement normalisé est `/lib/security`.

Principaux modules PAM	
<code>pam_securetty.so</code>	Interdit le login par le compte root excepté sur les terminaux listés dans <code>/etc/securetty</code> .
<code>pam_nologin.so</code>	Si le fichier <code>/etc/nologin</code> existe, affiche son contenu à toute tentative d'ouverture de session et interdit le login à tout autre que root.
<code>pam_env.so</code>	Déclare des variables d'environnement lues dans <code>/etc/environnement</code> ou dans le fichier donné en référence par le paramètre « <code>envfile=</code> ».
<code>pam_unix.so</code>	Permet l'authentification par la méthode traditionnelle des fichiers <code>/etc/passwd</code> et <code>/etc/shadow</code> .
<code>pam_deny.so</code>	Voie de garage. Est généralement exécuté si aucun autre module n'est exécuté avec succès.
<code>pam_permit.so</code>	Renvoie un retour positif inconditionnellement.
<code>pam_limits.so</code>	Affecte certaines limitations fonctionnelles à des utilisateurs ou des groupes en fonction des données du fichier <code>/etc/security/limits.conf</code> .
<code>pam_cracklib.so</code>	S'assure que le mot de passe employé présente un niveau de sécurité suffisant.
<code>pam_selinux.so</code>	Si <code>selinux</code> est activé sur le système, ce module va s'assurer que le shell sera bien exécuté dans le contexte de sécurité adéquat.
<code>pam_lastlog.so</code>	Affiche les informations sur la dernière ouverture de session réussie.
<code>pam_mail.so</code>	Vérifie la présence de nouveaux mails pour un utilisateur (messagerie interne).