

Collection  
**Certifications**

Préparation à la Certification **LPIC-3**

# LINUX

2<sup>ème</sup> édition

**EXAMEN LPI 300**

**30 Travaux pratiques**  
**168 Questions-réponses**

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



Téléchargement  
[www.editions-eni.fr](http://www.editions-eni.fr)



**Issam MEJRIR**

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

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

Saisissez la référence ENI du livre CE2C3LIN dans la zone de recherche et validez.

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

## Avant-propos

A. Introduction . . . . .	18
B. Les objectifs . . . . .	18
C. Contenu du livre . . . . .	19

## Chapitre 1

## Les annuaires X.500 et le protocole LDAP

A. Généralités sur les annuaires . . . . .	24
1. Définition des annuaires . . . . .	24
2. Qu'est-ce qu'un annuaire électronique ? . . . . .	25
3. À quoi sert un annuaire ? . . . . .	25
4. Quelles sont les particularités des annuaires ? . . . . .	26
B. Annuaires X.500 . . . . .	27
1. Le standard X.500 . . . . .	27
2. La normalisation X.500 . . . . .	28
3. Les composants d'un annuaire X.500. . . . .	29
4. Les points forts de X.500 . . . . .	30
5. Les points faibles de X.500 . . . . .	30
C. Introduction à LDAP. . . . .	31
1. Le protocole LDAP . . . . .	31
a. Le protocole . . . . .	31
b. Le standard LDAP . . . . .	32
c. Le modèle client-serveur . . . . .	33
2. Versions du protocole LDAP . . . . .	34
a. LDAP V1 . . . . .	34
b. LDAP V2. . . . .	34
c. LDAP V3. . . . .	35
3. Les modèles LDAP. . . . .	35
a. Le modèle d'information . . . . .	35
b. Le modèle de nommage . . . . .	40
c. Le modèle fonctionnel . . . . .	41
d. Le modèle de sécurité . . . . .	43
e. Le modèle de réplication . . . . .	43

<b>D. OpenLDAP et annuaires propriétaires</b> . . . . .	<b>44</b>
1. Le serveur OpenLDAP . . . . .	44
2. Les annuaires propriétaires . . . . .	45
<b>E. Validation des acquis : questions/réponses</b> . . . . .	<b>45</b>

## Chapitre 2

## Installation et configuration d'OpenLDAP

<b>A. Installation d'OpenLDAP à partir des sources</b> . . . . .	<b>50</b>
1. Pré-requis logiciels . . . . .	51
2. Installation de Berkeley DB . . . . .	52
3. Compilation et installation d'OpenLDAP . . . . .	53
4. Erreurs de compilation et dépannage . . . . .	54
<b>B. Installation d'OpenLDAP à partir des binaires</b> . . . . .	<b>55</b>
1. Choix d'une distribution GNU Linux . . . . .	55
2. Installation sous OpenSuse . . . . .	55
a. Installation des paquetages serveurs . . . . .	56
b. Installation des paquetages clients . . . . .	56
c. Organisation du répertoire d'installation . . . . .	56
<b>C. Clients et serveurs OpenLDAP</b> . . . . .	<b>57</b>
1. Les utilitaires clients . . . . .	57
2. Les utilitaires serveurs . . . . .	57
<b>D. Configuration du fichier slapd.conf</b> . . . . .	<b>58</b>
1. Sections du fichier de configuration slapd.conf . . . . .	58
2. Principales directives de configuration . . . . .	59
3. Première configuration de slapd.conf . . . . .	64
4. Démarrage du serveur slapd . . . . .	65
<b>E. Fichier de configuration client LDAP (ldap.conf)</b> . . . . .	<b>69</b>
1. Directives de ldap.conf . . . . .	69
2. Configuration d'un client LDAP . . . . .	70
<b>F. Validation des acquis : questions/réponses</b> . . . . .	<b>70</b>
<b>G. Travaux pratiques</b> . . . . .	<b>72</b>
1. Installation de Berkeley DB . . . . .	72
2. Installation d'OpenLDAP (sous Ubuntu 10.0.4 LTS) . . . . .	74
3. Peuplement de l'annuaire . . . . .	76

**Chapitre 3****Gestion des données et exploitation de l'annuaire**

<b>A. Peuplement de l'annuaire . . . . .</b>	<b>82</b>
1. Le format LDIF . . . . .	83
2. Le langage DSML . . . . .	84
3. Ajout des entrées dans l'annuaire . . . . .	91
4. Mise à jour des entrées de l'annuaire . . . . .	95
5. Recherche dans l'annuaire . . . . .	97
6. Les filtres de recherche . . . . .	100
7. Les modules Net::LDAP et Net::LDAP::LDIF . . . . .	105
a. Introduction au langage Perl . . . . .	105
b. Le module Net::LDAP . . . . .	105
c. Le module Net::LDAP::LDIF . . . . .	107
8. Les fonctions LDAP du langage PHP . . . . .	109
a. Introduction à PHP . . . . .	109
b. LDAP et PHP . . . . .	109
c. Fonctions LDAP de PHP . . . . .	110
<b>B. Indexation et sauvegarde des données . . . . .</b>	<b>115</b>
1. Indexation des données . . . . .	115
2. Sauvegarde des données . . . . .	117
<b>C. Clients graphiques pour la gestion des données . . . . .</b>	<b>120</b>
1. Le navigateur LDAP de la distribution Suse Linux Entreprise . . . . .	121
2. Le navigateur LDAP Phpldapadmin . . . . .	122
3. Apache Directory Studio . . . . .	123
<b>D. Validation des acquis : questions/réponses . . . . .</b>	<b>132</b>
<b>E. Travaux pratiques . . . . .</b>	<b>134</b>
1. Manipulation des fichiers LDIF . . . . .	134
2. Gestion des données de l'annuaire . . . . .	137
3. Recherches au sein de l'annuaire . . . . .	138
4. Le module Net::LDAP . . . . .	139
5. Apache Directory Studio . . . . .	139

<b>Chapitre 4</b>	<b>Annuaire pages blanches</b>
<b>A. Qu'est-ce qu'un service pages blanches ?</b> . . . . .	<b>142</b>
1. L'annuaire pages blanches d'entreprise . . . . .	142
2. Que peut-on stocker dans un service pages blanches ? . . . . .	142
<b>B. Le schéma inetOrgPerson</b> . . . . .	<b>143</b>
1. Description de la classe d'objets inetOrgPerson . . . . .	145
2. Hiérarchie de la classe d'objets inetOrgPerson . . . . .	146
<b>C. Mise à jour de slapd.conf</b> . . . . .	<b>147</b>
1. Inclusion de schémas associés aux pages blanches . . . . .	147
2. Gestion des index . . . . .	148
<b>D. Insertion des données</b> . . . . .	<b>148</b>
1. Préparation d'un fichier LDIF . . . . .	148
2. Ajout des entrées . . . . .	150
3. Interrogation de l'annuaire . . . . .	150
<b>E. Validation des acquis : questions/réponses</b> . . . . .	<b>152</b>
<b>F. Travaux pratiques</b> . . . . .	<b>154</b>
1. Création d'un annuaire d'entreprise . . . . .	154
2. Attribution des comptes utilisateurs . . . . .	156
<b>Chapitre 5</b>	<b>Sécuriser l'annuaire</b>
<b>A. Généralités sur la sécurité informatique</b> . . . . .	<b>160</b>
1. Objectifs de la sécurité . . . . .	160
2. La disponibilité . . . . .	161
3. La confidentialité . . . . .	161
4. L'authentification . . . . .	161
5. L'intégrité des données . . . . .	161
<b>B. Le chiffrement SSL/TLS - StartTLS</b> . . . . .	<b>162</b>
1. La cryptographie . . . . .	162
2. Les algorithmes de chiffrement . . . . .	162
a. Le chiffrement symétrique . . . . .	162
b. Le chiffrement asymétrique . . . . .	163
3. Le chiffrement SSL-TLS . . . . .	163
a. Qu'est-ce qu'un certificat numérique ? . . . . .	164
b. Mise en place de chiffrement par SSL dans LDAP . . . . .	164

<b>C. Sécurité SASL</b> . . . . .	<b>166</b>
1. L'authentification . . . . .	166
2. Le protocole Kerberos . . . . .	166
a. Principe de fonctionnement du protocole . . . . .	167
b. Mise en place d'un serveur Kerberos . . . . .	168
<b>D. OpenLDAP et Kerberos</b> . . . . .	<b>170</b>
1. Authentification LDAP via SASL (Kerberos) . . . . .	170
2. Options SASL dans slapd.conf . . . . .	172
<b>E. Autres paramètres de sécurité</b> . . . . .	<b>173</b>
1. Protéger le mot de passe . . . . .	174
2. Gestion des mots de passe . . . . .	175
<b>F. Les listes de contrôle d'accès (ACL)</b> . . . . .	<b>177</b>
<b>G. Validation des acquis : questions/réponses</b> . . . . .	<b>179</b>
<b>H. Travaux pratiques</b> . . . . .	<b>181</b>
1. Mise en place de LDAPS . . . . .	181
2. Règles de contrôle d'accès (ACL) . . . . .	182
3. Mise en place d'une infrastructure Kerberos . . . . .	184

**Chapitre 6****Réplication LDAP**

<b>A. Concepts de réplication LDAP</b> . . . . .	<b>188</b>
1. Disponibilité de l'annuaire . . . . .	188
a. Assurer la disponibilité . . . . .	188
b. Augmenter les performances . . . . .	188
2. Politique de réplication . . . . .	189
a. Stratégies de réplication . . . . .	189
b. Types de réplication . . . . .	189
<b>B. Réplication basée sur slurpd</b> . . . . .	<b>190</b>
1. Le démon slurpd . . . . .	190
a. Installation de slurpd . . . . .	190
b. Étape de mise en œuvre d'une réplication slurpd . . . . .	191
2. Configuration du serveur maître et esclave . . . . .	191
a. Configuration du serveur maître . . . . .	191
b. Configuration du serveur esclave . . . . .	192
c. Les fichiers journaux de slurpd . . . . .	192
d. Diagnostic des fichiers journaux . . . . .	193

<b>C. Réplication basée sur Syncrepl</b> . . . . .	<b>193</b>
1. Le protocole LDAP Content Synchronization Protocol . . . . .	193
2. Modes de réplication Syncrepl . . . . .	193
a. Le mode maître/esclave (provider/consumer) . . . . .	194
b. Le mode miroir . . . . .	194
3. Configuration du Syncrepl Replication . . . . .	194
a. Configuration du mode provider/consumer . . . . .	194
b. Configuration du provider . . . . .	194
c. Configuration du consumer . . . . .	195
d. Configuration du mode miroir . . . . .	196
e. La réplication multimaître . . . . .	197
<b>D. Annuaires distribués</b> . . . . .	<b>197</b>
1. Distribution de l'annuaire . . . . .	197
2. Pourquoi un annuaire distribué ? . . . . .	198
3. Configuration des referrals . . . . .	198
4. Option de recherche dans un annuaire distribué . . . . .	199
<b>E. Validation des acquis : questions/réponses</b> . . . . .	<b>199</b>
<b>F. Travaux pratiques</b> . . . . .	<b>201</b>
1. Configuration d'une réplication en miroir . . . . .	201
2. Configuration d'une réplication multimaître . . . . .	203
3. Déploiement d'un annuaire distribué . . . . .	205

## Chapitre 7

## Migration de NIS vers LDAP

<b>A. Rappel sur le service NIS</b> . . . . .	<b>210</b>
<b>B. Authentification NIS</b> . . . . .	<b>210</b>
1. Générer une base NIS des utilisateurs et groupes . . . . .	211
2. Configurer le client NIS . . . . .	211
<b>C. Authentification LDAP</b> . . . . .	<b>212</b>
1. Introduction à PAM et NSS . . . . .	212
a. PAM (Pluggable Authentication Module) . . . . .	212
b. NSS (Name Service Switch) . . . . .	215
2. Le module pam_ldap.so . . . . .	216
3. Le module nss_ldap.so . . . . .	217
<b>D. Le schéma nis.schema</b> . . . . .	<b>217</b>
<b>E. Les outils de migration PADL (Migration Tools)</b> . . . . .	<b>220</b>
1. Migration des comptes utilisateurs (/etc/passwd) . . . . .	221
2. Migration des groupes (/etc/group) . . . . .	224

<b>F. Authentification client</b> . . . . .	<b>226</b>
1. Configuration de pam_ldap. . . . .	226
2. Configuration de nss_ldap . . . . .	226
<b>G. Test d'authentification</b> . . . . .	<b>227</b>
1. La configuration de nsswitch.conf . . . . .	227
2. Test de connexion d'un utilisateur LDAP. . . . .	229
<b>H. Implémentation d'une passerelle NIS-LDAP</b> . . . . .	<b>230</b>
1. La passerelle NIS/LDAP de PADL . . . . .	230
2. Le démon ypldapd de PADL . . . . .	231
a. Installation de ypldapd . . . . .	231
b. Configuration du démon ypldapd . . . . .	231
<b>I. Validation des acquis : questions/réponses</b> . . . . .	<b>232</b>
<b>J. Travaux pratiques</b> . . . . .	<b>233</b>
1. Migration des hôtes et restriction d'accès. . . . .	234
2. Migration des groupes réseau . . . . .	239
3. Authentification des clients Linux via LDAP . . . . .	242

## Chapitre 8

## Intégration des applications avec LDAP

<b>A. Intégration de SSH dans LDAP</b> . . . . .	<b>246</b>
1. Configuration de PAM. . . . .	246
2. Configuration de NSS . . . . .	247
a. Le fichier nsswitch.conf . . . . .	247
b. La commande getent . . . . .	248
<b>B. Intégration de FTP dans LDAP</b> . . . . .	<b>248</b>
1. Le serveur FTP ProFTPD. . . . .	248
2. Installation de ProFTPD . . . . .	248
3. Le module mod_ldap . . . . .	248
4. Configuration de ProFTPD . . . . .	249
<b>C. Intégration Apache avec LDAP</b> . . . . .	<b>250</b>
1. Modes d'authentification dans Apache . . . . .	250
a. Authentification Basic . . . . .	250
b. Authentification Digest . . . . .	251
2. L'authentification LDAP sous Apache . . . . .	252
a. Le module authnz_ldap . . . . .	252
b. Configuration d'Apache dans LDAP . . . . .	255

3.	Apache et le Web SSO . . . . .	256
a.	Introduction à LemonLDAP::NG . . . . .	256
b.	Mode de fonctionnement . . . . .	257
c.	Installation. . . . .	258
d.	Configuration d'Apache . . . . .	258
e.	Configuration de l'authentification . . . . .	259
f.	Configuration de l'hôte virtuel. . . . .	259
<b>D.</b>	<b>Intégration Postfix avec LDAP . . . . .</b>	<b>260</b>
1.	Le serveur de messagerie Postfix . . . . .	260
2.	Postfix et LDAP. . . . .	260
3.	Configuration des clients de messagerie . . . . .	264
a.	Le client de messagerie Thunderbird . . . . .	264
b.	Le client de messagerie Outlook . . . . .	268
<b>E.</b>	<b>Intégration FreeRADIUS avec LDAP . . . . .</b>	<b>271</b>
1.	Le projet FreeRADIUS. . . . .	271
2.	Installation de FreeRADIUS. . . . .	272
3.	Le démon radiusd . . . . .	272
4.	Le fichier radiusd.conf . . . . .	273
5.	FreeRADIUS et LDAP. . . . .	275
6.	Paramètres du module rlm_ldap . . . . .	275
<b>F.</b>	<b>Migrer les utilisateurs Samba vers LDAP . . . . .</b>	<b>278</b>
1.	Rappel sur les services Samba . . . . .	278
2.	Authentification des utilisateurs Samba . . . . .	279
3.	Comptes utilisateurs dans un annuaire LDAP . . . . .	279
<b>G.</b>	<b>Intégration des comptes UNIX dans Active Directory . . . . .</b>	<b>286</b>
1.	Introduction à l'annuaire LDAP Active Directory. . . . .	286
2.	Création des objets dans Active Directory . . . . .	287
a.	Création de comptes utilisateurs . . . . .	287
b.	Création de comptes d'ordinateurs . . . . .	287
3.	Comptes UNIX dans Active Directory . . . . .	288
<b>H.</b>	<b>Intégration d'un serveur d'impression CUPS avec LDAP . . . . .</b>	<b>289</b>
1.	Rappel sur le serveur d'impression CUPS. . . . .	289
2.	Déclaration des imprimantes dans un annuaire LDAP . . . . .	291
<b>I.</b>	<b>Intégration d'un serveur DHCP avec LDAP . . . . .</b>	<b>291</b>
1.	Rappel sur DHCP . . . . .	291
2.	Paramètres de configuration du serveur DHCP. . . . .	292
3.	Configuration DHCP dans un annuaire LDAP . . . . .	294

J. Validation des acquis : questions/réponses	297
K. Travaux pratiques	299
1. Authentification via LDAP dans Apache	299
2. Authentification LDAP des utilisateurs FTP	301
3. Intégration du serveur d'impression CUPS avec LDAP	303
4. Configuration d'un serveur DHCP dans un annuaire LDAP	306

## Chapitre 9

## Optimisation OpenLDAP et surveillance système

A. Optimisation de l'annuaire	312
1. Optimisation du système	312
a. Réglage au niveau du système d'exploitation	313
b. Réglage au niveau OpenLDAP	313
c. Remplacement de slapd.conf par cn=config	314
d. Description de l'arbre cn=config	316
e. Installation de LinID OpenLDAP Manager	320
f. Intégrité et cohérence des données	325
g. Haute disponibilité par mécanismes de réplication	327
h. Supervision de l'annuaire LDAP	328
2. Optimisation de la base de données BDB	329
3. La sauvegarde	330
B. Surveillance des ressources système	331
1. Monitoring du CPU	331
2. Monitoring de la mémoire	334
3. Monitoring de l'espace de stockage	335
4. Monitoring du trafic réseau	337
a. Monitoring par netstat	337
b. Monitoring par ntop	337
C. Gestion des ressources	339
D. Validation des acquis : questions/réponses	340

<b>Chapitre 10</b>	<b>Samba et environnements hétérogènes</b>
<b>A. Quelques notions générales</b>	<b>344</b>
<b>B. Introduction à Samba</b>	<b>344</b>
1. Historique	345
2. Le protocole SMB	345
a. Définition	345
b. Les fonctionnalités du protocole SMB	345
c. Une connexion élémentaire SMB	346
3. Versions de Samba	346
<b>C. Les composants de Samba</b>	<b>348</b>
1. Les démons	348
2. Les utilitaires	348
a. Quelques utilitaires de gestion de domaine	349
b. Quelques utilitaires de gestion d'utilisateurs	351
c. Utilitaire de gestion de la configuration	351
<b>D. Les capacités de Samba</b>	<b>352</b>
1. Partage de fichiers et d'imprimantes	352
2. Contrôleur principal de domaine PDC	352
3. Contrôleur secondaire de domaine BDC	352
4. Serveur WINS	352
5. Authentification des clients	353
a. La gestion des comptes	353
b. Les modes d'authentification	353
<b>E. Validations des acquis : questions/réponses</b>	<b>354</b>
<b>Chapitre 11</b>	<b>Installation et configuration de Samba</b>
<b>A. Installation de la distribution Samba</b>	<b>358</b>
1. Installation à partir du code source	358
2. Installation binaire	358
<b>B. Configuration de Samba</b>	<b>359</b>
1. Le fichier smb.conf	359
2. Les directives de smb.conf	360
a. Les directives de la section [global]	360
b. Les directives des sections de partages	360
3. Mise en place d'un serveur de fichiers	361
a. Gestion des utilisateurs	361
b. Création de partages	362

c. Montages des ressources . . . . .	363
d. Impression . . . . .	363
e. smb.conf . . . . .	365
4. Configuration et mise en œuvre de SWAT . . . . .	367
a. Configuration de SWAT . . . . .	367
b. Démarrage de SWAT . . . . .	368
5. Test et validation de la configuration . . . . .	369
a. testparm . . . . .	369
b. Gestion des partages : smbclient . . . . .	370
c. Liste des ordinateurs . . . . .	371
<b>C. Validations des acquis : questions/réponses . . . . .</b>	<b>372</b>
<b>D. Travaux pratiques . . . . .</b>	<b>373</b>
1. Mise en place du serveur de fichiers Samba 3 . . . . .	373
2. Gestion des utilisateurs et des partages . . . . .	376

## Chapitre 12

## Mise en place d'un domaine Samba

<b>A. Les domaines Windows NT . . . . .</b>	<b>380</b>
1. La notion de domaines Windows NT . . . . .	380
2. Windows NT Server . . . . .	381
3. Les services d'annuaires de Windows NT . . . . .	382
a. Le modèle utilisé jusqu'à Windows NT 4.0 . . . . .	382
b. L'Active Directory AD . . . . .	382
<b>B. Les comptes d'utilisateurs et d'ordinateurs . . . . .</b>	<b>383</b>
1. Les comptes d'utilisateurs . . . . .	383
a. Les comptes prédéfinis . . . . .	383
b. La protection des comptes utilisateur . . . . .	384
2. Les comptes d'ordinateurs . . . . .	385
<b>C. Jonction des stations Windows à Samba . . . . .</b>	<b>385</b>
1. Pré-requis des systèmes d'exploitation . . . . .	385
2. Configuration des stations Windows . . . . .	385
<b>D. Samba 3 en tant que PDC . . . . .</b>	<b>387</b>
1. Déploiement du domaine Samba . . . . .	387
a. Configuration . . . . .	387
b. Les partages spécifiques . . . . .	388
c. La gestion des comptes . . . . .	389

2.	Migration vers le PDC Samba 3	390
a.	Préparation des serveurs	390
b.	Importation des ressources.	392
c.	Prise de relais du serveur par Samba	392
<b>E.</b>	<b>Authentification Samba 3 / Winbind</b>	<b>394</b>
1.	Le démon winbindd	395
a.	Définition et fonctionnalités.	395
b.	Configuration et démarrage	395
2.	Ouverture de session sur un domaine Windows	397
<b>F.</b>	<b>Validations des acquis : questions/réponses.</b>	<b>397</b>
<b>G.</b>	<b>Travaux pratiques</b>	<b>399</b>
1.	Configuration de Samba en tant que PDC	399

## Chapitre 13

## Contrôleur de domaine Samba 4

<b>A.</b>	<b>Introduction à Samba 4</b>	<b>404</b>
<b>B.</b>	<b>Fonctionnalités de Samba 4 / Samba AD</b>	<b>404</b>
<b>C.</b>	<b>Installation et configuration sous CentOS 6.</b>	<b>405</b>
1.	Installation à partir des binaires.	405
2.	Installation à partir des paquets sources.	406
3.	Le répertoire /usr/local/samba	406
<b>D.</b>	<b>Les composants de Samba 4</b>	<b>407</b>
1.	Le serveur DNS	407
a.	La terminologie DNS	407
b.	Changement du backend DNS	408
2.	Le serveur Kerberos.	408
a.	L'authentification Kerberos	408
b.	La terminologie Kerberos	409
3.	Le serveur LDAP.	409
<b>E.</b>	<b>Samba 4 en tant que AD</b>	<b>409</b>
1.	Initialisation du domaine ou « provisioning Samba »	409
2.	Démarrage Samba AD.	410
3.	Tests de connectivité à Samba AD DC.	411
a.	Test de partages administratifs de Sysvol et Netlogon	411
b.	Test d'authentification	411
4.	Configuration et test du serveur DNS	411
a.	Serveur DNS interne à Samba AD	411
b.	Serveur de noms BIND	412

c. Tester les enregistrements DNS . . . . .	414
5. Configuration et test du serveur Kerberos . . . . .	415
a. Configuration du fichier krb5.conf . . . . .	415
b. Test du serveur Kerberos . . . . .	415
6. Configuration de la synchronisation NTP . . . . .	415
a. Configuration du côté contrôleurs de domaine . . . . .	416
b. Configuration du côté hôtes . . . . .	416
c. Test du serveur NTP . . . . .	416
<b>F. Administration en ligne de commande . . . . .</b>	<b>417</b>
1. Gestion des utilisateurs dans Samba 4 . . . . .	417
2. Gestion des groupes dans Samba 4 . . . . .	418
3. Administration du serveur DNS avec Samba AD . . . . .	419
<b>G. Administration par l'outil RSAT (Remote Server Administration Tools) de Windows 7 . . . . .</b>	<b>420</b>
1. Joindre un client Windows au domaine . . . . .	420
2. L'outil Remote Server Administration Tools (RSAT) . . . . .	422
3. Administration par RSAT . . . . .	423
<b>H. Validations des acquis : questions/réponses . . . . .</b>	<b>425</b>
<b>I. Travaux pratiques . . . . .</b>	<b>427</b>
1. Mise en place d'un serveur Samba AD . . . . .	427
2. Gestion des groupes et des utilisateurs en ligne de commande . . . . .	429
3. Gestion des enregistrements DNS . . . . .	432

## Chapitre 14

## La sécurité du système de fichiers Linux

<b>A. Rappel sur les systèmes de fichiers . . . . .</b>	<b>436</b>
1. Le système de fichiers ext2 . . . . .	436
a. Le super-bloc . . . . .	437
b. Les descripteurs de groupe . . . . .	439
c. Les tables bitmaps de blocs et d'inodes . . . . .	439
d. La table des inodes de groupe . . . . .	439
e. Les répertoires . . . . .	440
2. Le système de fichiers ext3 . . . . .	440
3. Les systèmes de fichiers ext4/btrfs . . . . .	441
<b>B. Les attributs des fichiers . . . . .</b>	<b>442</b>
1. Listes des attributs . . . . .	442
2. Les commandes de gestion d'attributs . . . . .	442

<b>C. Droits sur les fichiers et les répertoires</b> . . . . .	<b>443</b>
1. Les droits d'endossement . . . . .	444
2. Le sticky bit . . . . .	444
3. Les commandes de gestion des droits . . . . .	445
<b>D. Les ACL POSIX</b> . . . . .	<b>446</b>
1. Présentation . . . . .	446
2. Les commandes de gestion des ACL . . . . .	446
<b>E. Pré-requis d'un système de fichiers dans Samba 4</b> . . . . .	<b>447</b>
1. Permissions sur les partages . . . . .	448
2. Ajout des permissions NTFS . . . . .	449
<b>F. Validation des acquis : questions/réponses</b> . . . . .	<b>451</b>
<b>G. Travaux pratiques</b> . . . . .	<b>453</b>
1. Mise en place d'un système de fichiers supportant les ACL et les attributs étendus . . . . .	453
2. Création des partages et positionnement des ACL . . . . .	454

## Chapitre 15

## Dépannage de Samba

<b>A. Sauvegarde de Samba</b> . . . . .	<b>460</b>
1. Techniques de sauvegarde de Samba 3 . . . . .	460
a. BackupPC . . . . .	460
b. resync . . . . .	460
c. Amanda . . . . .	461
d. BOBS . . . . .	461
2. Sauvegarde et restauration de Samba 4 . . . . .	461
a. La sauvegarde . . . . .	461
b. La restauration . . . . .	462
<b>B. Journalisation</b> . . . . .	<b>463</b>
1. Définition . . . . .	463
2. Les options de journalisation . . . . .	463
a. Le fichier log . . . . .	464
b. Les niveaux de journalisation . . . . .	464
c. Taille maximale des fichiers . . . . .	465
d. L'horodatage . . . . .	465
e. L'utilisation de syslog . . . . .	465
3. Journalisation distincte de clients ou d'utilisateurs . . . . .	466

<b>C. Dépannage des services liés à Samba 3</b> .....	<b>466</b>
1. La configuration TCP/IP .....	466
2. Les démons du serveur Samba 3 .....	467
3. Les connexions SMB .....	468
4. L'exploration .....	469
a. Tester avec smbclient .....	469
b. Utilisation de nmblookup .....	470
5. Les services de noms .....	471
a. Le serveur DNS .....	471
b. Le serveur WINS .....	472
<b>D. Dépannage des services liés à Samba 4</b> .....	<b>472</b>
1. Démarrage Samba AD .....	472
2. Serveur DNS .....	473
3. Serveur Kerberos .....	473
4. Installer Python 2.6.5 pour Samba .....	473
5. Vérification des ports utilisés par Samba 4 .....	473
<b>E. Validation des acquis : questions/réponses</b> .....	<b>474</b>
Tableau des objectifs .....	477
Index .....	479

---

## Chapitre 5

---

A. Généralités sur la sécurité informatique . . . . .	160
B. Le chiffrement SSL/TLS - StartTLS . . . . .	162
C. Sécurité SASL . . . . .	166
D. OpenLDAP et Kerberos . . . . .	170
E. Autres paramètres de sécurité . . . . .	173
F. Les listes de contrôle d'accès (ACL) . . . . .	177
G. Validation des acquis : questions/réponses . . . . .	179
H. Travaux pratiques . . . . .	181

---

## Pré-requis

---

- Connaissances de base sur la sécurité informatique.
- Notions de base sur le chiffrement SSL.
- Connaissances élémentaires sur le protocole Kerberos.

---

## Objectifs

---

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

- Sécuriser l'accès à l'annuaire à l'aide des certificats électroniques.
- Configurer l'authentification SASL.
- Maîtriser l'authentification Kerberos.
- Mettre en place des ACL avancées.
- Restreindre l'accès aux mots de passe au sein de l'annuaire.
- Implémenter une politique de sécurité pour les mots de passe des utilisateurs de l'annuaire LDAP.

## A. Généralités sur la sécurité informatique

### 1. Objectifs de la sécurité

La sécurité des systèmes d'information est l'un des enjeux majeurs dans la vie de l'entreprise ainsi que dans sa résistance aux différents problèmes qu'elle peut rencontrer, tels que les attaques de l'extérieur, surtout lorsqu'une partie de son système d'information est relié à un réseau hostile comme Internet.

L'entreprise doit assurer aussi la confidentialité des informations et la documentation interne liée à ses employés ou à ses transactions avec le monde extérieur.

Une entreprise qui offre des services à travers le réseau doit faire face à toute cause d'indisponibilité de son système d'information.

Dans le contexte d'un service critique (serveur Web, serveur LDAP, mail, base de données), une panne occasionnant un arrêt du service peut causer un tort considérable entraînant une perte de productivité, voire une perte de confiance du client.

Les solutions de sécurité qui seront mises en place doivent contribuer à satisfaire les critères suivants :

- La disponibilité.
- L'intégrité.
- La confidentialité.

Ce sont les critères DIC.

Un autre critère important doit aussi être pris en compte dans les communications entre un client et un serveur, l'authentification.

## 2. La disponibilité

La disponibilité d'une ressource signifie que celle-ci doit être accessible à tout instant, et doit également être utilisable avec des temps de réponse acceptables.

La disponibilité des services système et données est réalisée en assurant un dimensionnement approprié et une certaine redondance et par une gestion opérationnelle efficace des infrastructures, ressources et services.

Dans une entreprise, des solutions comme les tests de montée en charge sont généralement effectués pour évaluer le comportement des systèmes sous certaines conditions extrêmes et contribuer ainsi à mieux définir leur dimensionnement.

Il faut néanmoins mettre en place une politique de sauvegarde permettant de restituer des données en cas de défaillance matérielle ou logicielle.

Des solutions de haute disponibilité existent pour assurer la continuité de service. L'étude détaillée de ces solutions dépasse les objectifs de cet ouvrage.

## 3. La confidentialité

La confidentialité est le maintien du secret des informations. La confidentialité peut être vue comme la protection des données contre une divulgation non autorisée.

Deux opérations permettent d'assurer la confidentialité des données :

- Limiter leur accès par un mécanisme de contrôle d'accès (ACL).
- Transformer les données par des procédures de chiffrement afin qu'elles deviennent inintelligibles aux personnes ne possédant pas les moyens de les déchiffrer.

Le chiffrement contribue à assurer la confidentialité des données et à en augmenter la sécurité lors de leur transmission ou de leur stockage.

## 4. L'authentification

L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame.

Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a dotée.

Pour cela, l'identité devra produire une information spécifique telle que par exemple un mot de passe, un code ou une empreinte biométrique.

## 5. L'intégrité des données

Assurer l'intégrité de l'information est relatif au fait que des ressources de données, traitements, transactions ou services n'ont pas été modifiés, altérés ou détruits, tant de façon intentionnelle qu'accidentelle.

Lors de leur transfert, les données ne devraient pas être altérées par les protocoles de communication qui les véhiculent.

L'intégrité des données ne sera garantie que si elles sont protégées des écoutes actives qui peuvent modifier les données interceptées.

## B. Le chiffrement SSL/TLS - StartTLS

### 1. La cryptographie

La cryptographie a pour but d'assurer la confidentialité et l'intégrité des données.

La confidentialité est garantie par des algorithmes de chiffrement.

Le chiffrement est l'opération par laquelle on chiffre un message. C'est une opération de codage. Chiffrer ou crypter une information permet de la rendre incompréhensible en l'absence d'un décodeur particulier.

### 2. Les algorithmes de chiffrement

Les algorithmes de chiffrement sont divisés en deux grandes catégories :

- Le chiffrement symétrique.
- Le chiffrement asymétrique, dit à clé publique.

#### a. Le chiffrement symétrique

Dans le chiffrement symétrique, une seule clé, qui sert pour le chiffrement et le déchiffrement, est partagée entre toutes les personnes participant à un échange.

Pour chiffrer ou déchiffrer un texte, il faut définir une clé et un algorithme de chiffrement.

Chaque entité doit posséder autant de clés secrètes qu'elle a d'interlocuteur. Il faut donc disposer d'autant de paires différentes de clés qu'il y a de paires de correspondants.

Le tableau suivant liste quelques algorithmes de chiffrement symétriques :

Algorithme	Taille de clé (en bits)	Taille de bloc
3-DES	112,168	64
RC5	32, 64, 128	Jusqu'au 2048
AES	128, 192, 256	128
RC6	Jusqu'à 2048	128
Camelia	128, 192, 256	128
Serpent	128, 192, 256	128

- DES (*Data Encryption Standard*) : avec cet algorithme les données sont chiffrées par bloc de 64 bits avec une clé de 56 bits.
- 3DES (*Triple DES*) : on réalise trois niveaux de chiffrement ce qui donne une clé effective de chiffrement de 168 bits.
- RC5 est un algorithme propriétaire à clé symétrique développé par Ronald Rivest et diffusé par la société RSA Security Inc. Il utilise des clés de longueur variable pouvant aller jusqu'au 2048 bits.
- Camelia est un algorithme de chiffrement symétrique par bloc de 128 bits, conçu pour fonctionner avec des clés de 128, 192 et 256 bits. Il a été développé conjointement par la Nippon Telegraph And Telephone corporation et Mitsubishi Electric Corporation en 2000.

Depuis 2006, le code source de Camelia est disponible sous plusieurs licences libres telles que GPL, BSD, MPL et la licence OpenSSL.

- Serpent : est un algorithme de chiffrement par bloc, serpent a une taille de bloc de 128 bits et supporte des clés de 128, 192 ou 256 bits.

Serpent est souvent considéré comme l'un des systèmes de chiffrement les plus sûrs actuellement disponibles.

## b. Le chiffrement asymétrique

Dans le chiffrement asymétrique, il existe deux clés, une clé publique et une clé privée. Ces deux clés sont générées ensemble par un logiciel (exemple OpenSSL, GNUTLS) et elles dépendent mathématiquement l'une de l'autre.

La clé publique peut être publiée sans risque, mais la clé privée doit être soigneusement gardée secrète par son propriétaire.

La clé publique sert habituellement à crypter un message et la clé privée à le décrypter, mais l'inverse est également possible.

La cryptographie à clés publiques présente plusieurs avantages :

- Elle diminue le nombre de clés nécessaire à la communication entre un nombre important de personnes.
- Elle permet la signature d'un document numérique.
- Elle permet l'authentification mutuelle de deux composants.
- Les principaux algorithmes de chiffrement à clé publique, dont le nom est celui de leur inventeur, utilisent le plus souvent des clés de longueur variant de 512 à 1024 bits, citons par exemple :
  - RSA (*Rivest, Shamir, Adelman*) qui est basé sur la factorisation des nombres premiers.
  - El Gamal, basé sur la difficulté de résoudre le problème de logarithme discret.

 *La sécurité du processus de chiffrement repose en grande partie sur la sécurité et la confidentialité des clés utilisées, sur la robustesse des algorithmes et sur la sécurité des plates-formes matérielles et logicielles qui les supportent.*

## 3. Le chiffrement SSL-TLS

Le protocole cryptographique SSL (*Secure Sockets Layers*) a été créé par la société Netscape en collaboration avec d'autres acteurs dont MasterCard et Bank of America pour prendre en charge des échanges sécurisés et authentifiés entre un client et un serveur. SSL peut être utilisé pour toute application reposant sur TCP, à l'instar de LDAP.

TLS (*Transport Layer Security*), le véritable nom pour SSLv3.1 décrit dans la RFC 2246, est la couche cryptographique qui se glisse entre TCP et LDAP pour sécuriser des échanges sur un lien non sûr.

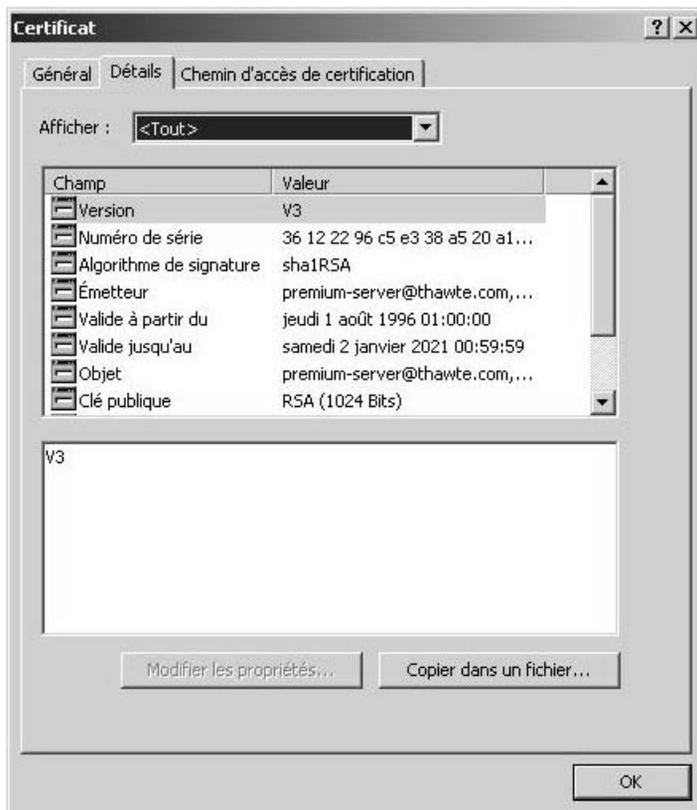
SSL permet de chiffrer les communications entre deux machines et d'assurer la confidentialité des données, l'authentification de l'utilisateur et du serveur, ainsi que l'intégrité des données par signatures électroniques à travers les certificats numériques et la mise en œuvre du chiffrement asymétrique.

Dans ce chapitre on s'intéresse particulièrement à la sécurisation du protocole LDAP et la configuration d'OpenLDAP à l'aide des certificats.

### a. Qu'est-ce qu'un certificat numérique ?

Un certificat numérique ou certificat électronique constitue la carte d'identité numérique d'une entité (personne morale ou physique) ou d'une ressource informatique à laquelle il appartient. Il contient entre autres l'identification de son propriétaire, la clé publique qui lui est attribuée ainsi que l'identification de l'organisme qui l'a délivrée.

Propriétés d'un certificat dans Internet Explorer :



### b. Mise en place de chiffrement par SSL dans LDAP

Pour mettre en place le chiffrement des échanges avec LDAP, il faut générer un certificat pour le serveur.

Pour créer ce certificat, il existe plusieurs façons :

- Créer un certificat auto-signé : ce type de certificat ne garantira pas l'identité de la source, mais permettra le chiffrement des échanges.