

Annuaire LDAP

2^e édition

Marcel Rizcallah

© Groupe Eyrolles, 2004
ISBN : 2-212-11504-0

EYROLLES



Table des matières

Avant-propos	1
Quel est l'objectif de cet ouvrage ?	4
La structure de l'ouvrage	4
À qui s'adresse cet ouvrage ?	5
Questions et réponses	6
Qu'est que LDAP ?	6
Qui est responsable du standard LDAP ?	6
Que peut m'apporter LDAP ?	6
Pourquoi LDAP est-il aussi important ?	7
Quelles différences y a-t-il entre LDAP et une base de données ?	7
Comment faire cohabiter un annuaire LDAP avec des applications existantes ?	7
Qu'est qu'un méta-annuaire ?	8
Qu'est-ce que la gestion des identités ?	8
Quel lien y a-t-il entre la gestion des identités et un annuaire LDAP ? ..	9
Qu'est-ce que la fédération des identités ?	9
PARTIE 1	
Les annuaires et leurs applications	11
CHAPITRE 1	
Généralités sur les annuaires et la gestion des identités ...	13
Introduction	13
Qu'est-ce qu'un annuaire ?	14
L'aspect dynamique	14
La flexibilité	15
La sécurité	15
La personnalisation	16

À quoi sert un annuaire ?	18
Localiser des ressources	18
Gérer un parc de ressources	20
Localiser des applications et gérer des droits d'accès	20
Recherche et navigation dans un annuaire	24
En résumé	24
Quelles sont les particularités des annuaires ?	25
Les annuaires sont plus sollicités en lecture qu'en écriture	25
Les annuaires ne sont pas destinés à gérer des transactions complexes	25
Les annuaires doivent pouvoir être sollicités à distance par tous, et à travers des débits réseau faibles	26
Les annuaires doivent pouvoir communiquer entre eux	27
Les informations gérées par un annuaire sont classées de façon hiérarchique	28
Les annuaires offrent un espace de noms homogènes	29
Les annuaires doivent pouvoir gérer les habilitations sur les données de l'annuaire lui-même	30
Les annuaires s'appuient sur des bases de données	33
Qu'est-ce que la gestion des identités ?	35
Le référentiel des identités	35
La gestion du contenu du référentiel des identités	36
L'identification et l'authentification électronique	36
La gestion des mots de passe	37
L'allocation et la désallocation automatisée de ressources	37
La gestion des droits d'accès aux applications	37
Le rôle des annuaires dans la gestion des identités	38
La fédération des identités	38
Introduction	38
Centralisation versus fédération	40
Quelques exemples d'applications	42
Comment fonctionne la fédération des identités ?	45
Les technologies et les standards	47
Enjeux et faisabilité de la gestion des identités et des annuaires	48
La gestion des identités et les annuaires dans l'entreprise	48
Ce que coûte la multiplicité de la gestion des identités et des annuaires ...	50
Les enjeux auxquels répond la gestion des identités et des annuaires à l'échelle de l'entreprise	53
Ce que coûte la mise en œuvre d'un annuaire d'entreprise	56
Quels apports et retour sur investissement ?	57
Pourquoi un standard comme LDAP ?	59

CHAPITRE 2

Historique des annuaires et introduction à LDAP	63
Naissance des annuaires	63
Les annuaires DNS	64
Les annuaires WHOIS	65
La normalisation X500	66
Généralités	66
Les composants d'un annuaire X500	67
Le chaînage des requêtes	69
Notions sur les modèles X500	72
Les points forts de X500	74
Les points faibles de X500	74
Les annuaires propriétaires	75
Les annuaires généralistes	75
Les annuaires de systèmes d'exploitation réseau	76
Les annuaires propres aux applications informatiques	77
Introduction à LDAP	79

CHAPITRE 3

Les annuaires LDAP et leurs applications	83
Introduction	83
Les réseaux et les systèmes d'exploitation	84
L'initiative DEN	84
Active Directory et Windows 2000/2003	87
Novell eDirectory Server et Netware	95
OpenLDAP et Linux	96
La sécurité des systèmes d'information	97
Les certificats X509 et les infrastructures à clés publiques	97
Les applications des certificats	97
L'identification unique (ou le Single Sign On)	101
La gestion des autorisations	104
Le commerce électronique	106
Les extranets	108
Les portails d'entreprise	111
Quelques exemples d'applications par secteur de marché	116
Les télécommunications	116
Les assurances	117
Les banques	118

La grande distribution	118
L'industrie	119
L'administration électronique	120
PARTIE 2	
Le standard LDAP	123
CHAPITRE 4	
Le standard LDAP et son modèle client-serveur	125
Naissance de LDAP	126
Le statut actuel du standard LDAP V3	127
Le modèle client-serveur	130
Le codage multilingue	133
CHAPITRE 5	
Les modèles de LDAP	135
Le modèle d'information	135
Les concepts	135
Le schéma de l'annuaire	136
Les OID	136
Les attributs	138
Les classes d'objets	146
L'entrée root DSE	157
La vérification du schéma de l'annuaire	158
Le modèle de désignation	158
Les concepts	158
L'organisation hiérarchique des données	160
Le nom des objets	161
Nom de domaine DNS et nom de domaine LDAP	164
Le modèle des services	166
Les différentes catégories de services	166
Description des services	167
Le renvoi de référence ou les referrals	177
Le filtre de recherche LDAP	180
Le modèle de sécurité	186
Généralités	186
L'authentification	187
La confidentialité des échanges	187

Le chiffrement des données	189
L'intégrité des données	190
La gestion des habilitations	190
CHAPITRE 6	
Les interfaces d'accès aux annuaires et les autres standards	193
L'interface de programmation en langage C	193
Le modèle client-serveur	194
La séquence des appels	195
La liste des fonctions de l'API C	196
Les kits de développement en C	198
Les autres interfaces de programmation	199
L'interface de développement en Java de l'IETF	199
L'interface de développement en Java de SUN : JNDI	200
L'interface de développement de Microsoft : ADSI	201
L'interface de développement .NET de Microsoft : system.DirectoryServices	202
Le format d'échange LDIF	202
Syntaxe des données LDIF	203
Syntaxe des commandes LDIF	205
Comment exporter ou importer des données au format LDIF ?	207
Le standard DSML	209
Qu'est-ce que DSML ?	209
À quoi sert DSML ?	211
Quelles sont les différences entre LDAP et DSML ?	212
Quels sont les outils qui supportent DSML ?	213
La norme DSML	215
La syntaxe URL de LDAP	221
Description de la syntaxe	222
L'identification et l'authentification	223
Quelques exemples	224
Les extensions du standard LDAP v3	227
La syntaxe des contrôles d'accès ou ACL	227
Tri des résultats d'une recherche par le serveur	227
Codage des langues dans les valeurs d'attributs	227
Données dynamiques dans un annuaire	228
Renvoi de référence (referrals)	228
Recherche de serveurs LDAP	228

Interface de programmation LDAP	229
LDAP sur UDP	229
Signature des données dans un annuaire LDAP	229
Réplication entre serveurs (LDUP)	229
La classe d'objet inetorgperson	230
Introduction aux standards de fédération des identités	230
Pourquoi la nécessité de tels standards ?	230
Introduction à SAML	231
PARTIE 3	
La conception et la réalisation	239
CHAPITRE 7	
La conception fonctionnelle	241
Présentation de la méthodologie	241
L'étape de cadrage	245
Les objectifs	245
Maîtrise d'œuvre et maîtrise d'ouvrage	246
Les points clés	247
Quelques exemples	250
L'élaboration du contenu	251
Les objectifs	251
Les points clés	251
La définition des attributs	253
La définition des classes d'objets	258
L'identification des acteurs	262
Les objectifs	262
Les utilisateurs	262
Les gestionnaires	264
Les administrateurs	265
La définition des droits d'accès	266
L'identification des contraintes réseau	268
La conception de l'arborescence (DIT)	269
La racine de l'arbre	269
Les bonnes raisons pour créer des branches dans l'annuaire	271
Quelques recommandations	277

Les processus de gestion de l'annuaire	280
Le partage des données entre différents acteurs	281
La gestion des conflits de mise à jour	286
CHAPITRE 8	
La conception technique	289
La conception de la gestion des habilitations	290
Rappel de la définition d'un ACL	290
Utilisation de groupes pour la gestion des habilitations	293
Utilisation de rôles pour la gestion des habilitations	294
Envoi des demandes à un administrateur	298
Utilisation de filtres dans les ACL	298
Désignation indirecte des objets auxquels la règle s'applique	299
La topologie de serveurs LDAP	300
Les partitions	300
Le renvoi de référence	303
La recherche dans un annuaire distribué sur plusieurs partitions	304
Identification dans un annuaire distribué sur plusieurs partitions	305
La réplication entre annuaires LDAP	306
La gestion de la disponibilité	306
L'optimisation des performances	307
Stratégies de réplication	308
Protéger le serveur d'annuaire par un firewall	315
CHAPITRE 9	
Études de cas	319
L'extranet de MyPizza	319
L'étape de cadrage	319
L'élaboration du contenu	321
Les acteurs	325
Les droits d'accès	327
L'identification des contraintes réseau	329
La définition de l'arborescence (DIT)	330
La gestion des habilitations	332
L'étude de cas Thomson	338
Les enjeux et objectifs du projet	339
Les différentes étapes du projet	339
Le système d'information existant	340

Les applications à réaliser	341
Les choix techniques	342
La solution mise en œuvre	344
Le bilan	372
CHAPITRE 10	
Les outils	375
Vue d'ensemble	375
Les serveurs d'annuaire LDAP	377
Les annuaires dédiés aux systèmes d'exploitation	377
Les annuaires intégrés dans des logiciels	378
Les annuaires généralistes	379
Les méta-annuaires	383
Qu'est-ce qu'un méta-annuaire ?	383
Les différentes fonctions d'un méta-annuaire	384
La jointure des données	386
La transformation des données	388
Les connecteurs et la synchronisation des données	388
Le modèle de méta-annuaire basé sur la réplication des données	390
Le modèle de méta-annuaire basé sur un annuaire virtuel	391
Exemples de méta-annuaires	391
Les annuaires virtuels et les proxys LDAP	394
Le rôle d'un proxy LDAP	394
Exemples d'annuaires virtuels et de proxy LDAP	398
Les outils de e-provisionnement	399
Principales fonctionnalités	399
Exemples d'outils de e-provisionnement	401
Les outils de gestion des mots de passe	403
La réinitialisation du mot de passe	404
La synchronisation du mot de passe	404
Exemples d'outils de gestion des mots de passe	405
Les serveurs d'applications LDAP	405
Qu'est ce qu'un serveur d'applications ?	405
Exemples de logiciels	409
Les outils d'administration	412
Le rôle de l'administration dans le cycle de vie d'un annuaire LDAP ...	412
Exemples d'outils d'administration	413

Les outils de gestion du contenu d'annuaires	418
La gestion des entrées de l'annuaire	419
La gestion des groupes	423
L'analyse du contenu	424
Exemples d'outils de gestion de contenu	426
Les outils d'identification/authentification unique et de contrôle d'accès	427
L'identification et l'authentification	428
La gestion des autorisations	429
Exemple d'outils de SSO et de contrôle d'accès	431
Les outils de fédération des identités	432
Exemple d'outils de fédération d'identités	434
CHAPITRE 11	
La vie d'un annuaire d'entreprise	435
Les différentes étapes de la vie d'un annuaire	435
Les bonnes questions à se poser	436
Les acteurs	436
Favoriser la réutilisation de l'annuaire	437
Modifier le schéma	440
Tester et analyser les performances d'un annuaire	443
Optimiser les performances d'un annuaire	446
Modifier l'arborescence de l'arbre LDAP (DIT)	450
Synchroniser les données	452
Les étapes à suivre pour ajouter une nouvelle application	459
Le cadre légal	462
Droits et obligations	462
Impact sur les annuaires d'entreprise	465
PARTIE 4 467	
Exemples de code	467
CHAPITRE 12	
Exemples de code en C et C++	469
Le kit de développement LDAP en C	469
Où trouver ce kit ?	469
Un exemple simple	470

Exemple d'interrogation d'un annuaire LDAP à partir d'un téléphone mobile	474
Qu'est-ce SMS ?	474
Description de l'application	474
L'architecture technique	475
Principe de fonctionnement de l'application	476
Implémentation du code source	478
 CHAPITRE 13	
Exemples de mise en œuvre d'ADSI et de .NET	489
Le kit de développement ADSI	489
Qu'est-ce qu'ADSI ?	489
Où trouver le kit ADSI ?	491
Le modèle d'objets d'ADSI	491
Exemple de code avec ASP	496
L'énumération des unités organisationnelles	496
La liste des personnes dans une unité organisationnelle	498
La fiche d'une personne	500
L'authentification	502
La modification	503
Le framework .NET et l'accès aux annuaires	505
L'espace de nom (namespace) System.DirectoryServices dédié aux annuaires	506
Exemple de code C#.NET avec System.DirectoryServices	507
 CHAPITRE 14	
Exemples de mise en œuvre de JNDI	515
Le kit de développement JNDI	515
Qu'est-ce que JNDI ?	515
Où trouver le kit JNDI ?	515
Les concepts et les principes de l'interface JNDI	516
Un exemple simple	518
Exemple d'application avec JNDI	521
L'initialisation	521
La recherche	523
La comparaison	528
La mise à jour	528

CHAPITRE 15

Exemples de mise en œuvre de PHP	531
Le kit de développement LDAP en PHP	531
Qu'est-ce que PHP ?	531
Où trouver PHP et les fonctions d'accès à LDAP ?	532
Tester l'installation de PHP et des modules LDAP	533
Exemples de code avec PHP	534
La connexion	534
L'identification et l'authentification	534
La recherche	537
La suppression	540
La modification	542
La création	544

CHAPITRE 16

Installer et utiliser OpenLDAP	547
Introduction à OpenLDAP	547
Installation et mise en œuvre de OpenLDAP	548
Les différents modules de OpenLDAP	548
Installation de OpenLDAP	550
Configuration de OpenLDAP	550
Gestion des droits d'accès	556
Réplication du serveur OpenLDAP	559
Administration du serveur OpenLDAP	561
Lancement et arrêt de l'annuaire	561
Backup et restauration de l'annuaire	562

ANNEXE

Je monte un site Internet	563
Index	571