



Expert
EXPERT

Les services AD LDS

Mise en œuvre
d'un annuaire **LDAP**
sur Windows Server 2019



+ QUIZ

Version en ligne

OFFERTE !

pendant 1 an

Marouane MAAMRI



Introduction

- 1. Introduction 11
- 2. Public visé 12
- 3. Structure du livre 12
- 4. Organisation des travaux pratiques 13

Chapitre 1
Généralités sur les annuaires

- 1. Introduction 17
- 2. Qu'est-ce qu'un annuaire ? 18
- 3. Différents types d'annuaires 20
- 4. Différences entre un annuaire et une base de données 22
- 5. Exemples d'annuaires d'entreprise 24
- 6. Domaines d'utilisation 27
- 7. Historique et normes 29
 - 7.1 Historique 29
 - 7.2 Norme X.500 31
- 8. Gestion des identités et des accès 34
 - 8.1 Gestion des identités 34
 - 8.1.1 Définition 34
 - 8.1.2 Attributs et identifiants 35
 - 8.1.3 Fournisseur d'identité 35
 - 8.1.4 Fédération d'identité 36
 - 8.2 Gestion des identités et des accès 37
 - 8.2.1 Cycle de vie des comptes utilisateurs 37
 - 8.2.2 Modèles de contrôle d'accès 39
- 9. Conclusion 41

2 _____ Les services AD LDS

Mise en œuvre d'un annuaire LDAP sur Windows Server 2019

Chapitre 2

Présentation de la norme LDAP

1. Introduction	43
2. Concepts LDAP.	44
3. Différence entre LDAPv2 et LDAPv3	47
4. Modèles LDAP	48
4.1 Le modèle d'information	48
4.2 Le modèle de nommage	52
4.2.1 La syntaxe de nom distinctif	53
4.2.2 Le service referral	54
4.3 Le modèle fonctionnel	55
4.3.1 La recherche	56
4.3.2 La comparaison.	57
4.3.3 La mise à jour	57
4.3.4 L'authentification.	58
4.3.5 Les contrôles et les opérations étendues	58
4.4 Le modèle de sécurité	59
4.4.1 L'authentification.	59
4.4.2 Le contrôle d'accès	61
4.4.3 L'intégrité de données	61
4.4.4 La politique des mots de passe.	61
4.5 Le modèle de réplication.	61
4.5.1 Principe	62
4.5.2 Modèles de réplication	62
5. Format d'échange LDIF	63
5.1 Syntaxe LDIF	64
5.2 Opérations LDIF.	65
6. Conclusion	66

Chapitre 3
Intégration à Active Directory

- 1. Introduction 67
- 2. Concepts fondamentaux 68
 - 2.1 Définition d'Active Directory 68
 - 2.2 Objets Active Directory 71
 - 2.3 Schéma Active Directory 72
 - 2.4 Niveau fonctionnel 74
 - 2.5 Catalogue global 75
- 3. Structure logique 78
 - 3.1 Arborescence et forêts 78
 - 3.2 Domaines 80
 - 3.3 Unités d'organisation 81
- 4. Structure physique 83
 - 4.1 Contrôleurs de domaine 83
 - 4.2 Sites 85
 - 4.3 Réplication 86
- 5. Présentation des maîtres d'opération 91
 - 5.1 Maître de schéma 92
 - 5.2 Maître d'attribution des noms de domaine 93
 - 5.3 Maître des identifiants relatifs 94
 - 5.4 Maître d'infrastructure 95
 - 5.5 Maître d'émulateur PDC 96
- 6. Système DNS et Active Directory 97
 - 6.1 Concepts fondamentaux 97
 - 6.2 Espace de noms DNS 98
 - 6.3 Types d'enregistrements DNS 100
 - 6.4 Zones DNS 101
 - 6.5 Délégation DNS 102
 - 6.6 Lien entre DNS et Active Directory 102

4 Les services AD LDS

Mise en œuvre d'un annuaire LDAP sur Windows Server 2019

7.	Déploiement de l'annuaire Active Directory	104
7.1	Ajout du rôle Service de Domaine Active Directory	104
7.2	Configuration du rôle Service de Domaine Active Directory	108
8.	Conclusion	110

Chapitre 4

Introduction aux services AD LDS

1.	Introduction	113
2.	Présentation des services AD LDS	114
3.	Différences entre un AD LDS et un AD DS	117
4.	Historique des services AD LDS	118
4.1	AD LDS sous Windows Server 2008 et 2008 R2	118
4.2	AD LDS sous Windows Server 2012 et 2012 R2	120
5.	Scénarios métier et cas d'usage avec AD LDS	121
5.1	AD LDS et le serveur de transport Edge d'Exchange	121
5.2	AD LDS en tant qu'un annuaire téléphonique	122
5.3	AD LDS en tant qu'outil de consolidation de données	123
5.4	AD LDS en tant que service d'authentification web	125
6.	Architecture AD LDS	126
6.1	Interfaces	126
6.2	DSA	127
6.3	Database Layer	129
6.4	Moteur ESE	129
7.	Intégration de l'infrastructure AD LDS au système d'information	130
7.1	Organisation des données	130
7.2	Déploiement	132
8.	Conclusion	135

Chapitre 5

Prérequis et installation des services AD LDS

- 1. Introduction 137
- 2. Prérequis 138
 - 2.1 Mémoire 138
 - 2.2 Stockage 139
 - 2.3 Processeur 139
- 3. Éditions de Windows Server 2019 140
 - 3.1 Windows Server 2019 Essentials 140
 - 3.2 Windows Server 2019 Standard 140
 - 3.3 Windows Server 2019 Datacenter 141
- 4. Windows Server 2019 Core 141
- 5. Fichiers LDIF 142
- 6. Installation d'AD LDS 143
 - 6.1 Déploiement basé sur une nouvelle instance 144
 - 6.2 Déploiement basé sur une instance existante 159
 - 6.3 Déploiement en mode core 161
 - 6.3.1 Ajout du rôle AD LDS 161
 - 6.3.2 Ajout de l'instance 162
- 7. Vérification de l'installation et de l'initialisation des services AD LDS 164
- 8. Conclusion 166

Chapitre 6

Présentation des outils d'administration

- 1. Introduction 167
- 2. L'éditeur ADSI 169
- 3. L'outil LDP 172
- 4. L'outil Adamsync 180

6 Les services AD LDS

Mise en œuvre d'un annuaire LDAP sur Windows Server 2019

5. L'outil Csvde	181
6. L'outil Ldifde	184
7. L'outil DSACLs	184
8. Conclusion	187

Chapitre 7

Présentation des partitions d'annuaire

1. Introduction	189
2. L'entrée RootDSE	190
3. Les partitions d'annuaire	191
3.1 La partition de schéma	192
3.2 La partition de configuration	194
3.3 La partition d'application	196
3.3.1 Création d'une partition d'application avec LDP	197
3.3.2 Création d'une partition d'application avec Ntdsutil	199
4. Le fournisseur Active Directory	203
4.1 Les fournisseurs	203
4.2 Les PSDrives	204
4.2.1 Lister les PSDrive	204
4.2.2 Créer un PSDrive	205
4.2.3 Explorer les objets d'annuaire	205
4.2.4 Supprimer un PSDrive	207
5. Gestion de la base de données AD LDS	208
5.1 Présentation	208
5.2 Défragmentation de la base de données	210
5.2.1 Présentation	210
5.2.2 Procédure de défragmentation	210
6. Conclusion	212

Chapitre 8
Gestion des instances

- 1. Introduction 213
- 2. Réplication AD LDS 214
 - 2.1 Jeu de configuration 215
 - 2.2 Configuration de la réplication 216
- 3. Démarrage et arrêt d'une instance 225
 - 3.1 Démarrage et arrêt d'une instance
avec la console MMC services 225
 - 3.2 Démarrage et arrêt d'une instance en ligne de commande ... 227
- 4. Sauvegarde et restauration d'une instance 227
 - 4.1 Sauvegarde d'une instance 228
 - 4.1.1 L'outil « Sauvegarde de Windows Server » 228
 - 4.1.2 La commande Dsdbutil 229
 - 4.2 Restauration d'une instance 230
- 5. Conclusion 233

Chapitre 9
Gestion des objets AD LDS

- 1. Introduction 235
- 2. Les utilisateurs dans AD LDS 236
 - 2.1 Création d'utilisateur 236
 - 2.2 Suppression d'utilisateur 243
 - 2.3 Restauration d'utilisateur 245
 - 2.3.1 Augmentation du niveau fonctionnel 245
 - 2.3.2 Activation de la corbeille AD LDS 247
 - 2.3.3 Restauration d'utilisateur AD LDS 248
- 3. Les groupes dans AD LDS 252
 - 3.1 Rôles et privilèges 252
 - 3.2 Création de groupe 254
 - 3.3 Ajout et suppression de membres dans un groupe 256

8 **Les services AD LDS**

Mise en œuvre d'un annuaire LDAP sur Windows Server 2019

3.4	Suppression d'un groupe	258
3.5	Restauration d'un groupe	259
4.	Les conteneurs dans AD LDS	261
4.1	Conteneurs par défaut	261
4.2	Création de conteneurs	262
4.3	Protection de conteneurs contre les suppressions accidentelles	263
4.4	Gestion des listes de contrôle d'accès	265
5.	Conclusion	267

Chapitre 10

Mise en place de l'authentification AD LDS

1.	Introduction	269
2.	Authentification anonyme	270
3.	Authentification simple	274
3.1	Mécanisme d'authentification non authentifié	274
3.2	Mécanisme d'authentification par mot de passe	275
4.	Authentification SASL	277
5.	Authentification par l'intermédiaire d'un objet proxy	278
5.1	Présentation	278
5.2	Matrice des flux	279
5.3	Mise en place de l'authentification par l'intermédiaire d'un objet proxy	281
5.3.1	Préparation de l'instance AD LDS	282
5.3.2	Synchronisation des données	287
5.4	Démonstration	291
6.	Conclusion	293

Chapitre 11

Sécurisation de l'AD LDS

1. Introduction	295
2. Présentation des protocoles SSL/TLS	296
2.1 Intégration des protocoles SSL/TLS à LDAP	296
2.2 Terminologie utile à l'implémentation des protocoles SSL/TLS	297
2.2.1 La cryptographie	297
2.2.2 Le chiffrement symétrique	299
2.2.3 Le chiffrement asymétrique	299
2.2.4 La signature numérique	300
2.2.5 Le hachage	301
2.3 Principe de fonctionnement des protocoles SSL/TLS	303
3. Présentation de l'infrastructure à clé publique	305
3.1 Les composants d'une infrastructure à clé publique	305
3.2 Le principe de fonctionnement d'une infrastructure à clé publique	306
3.3 Les types d'autorité de certification	307
4. Implémentation du protocole LDAPS	309
4.1 Mise en place d'une autorité de certification d'entreprise	309
4.2 Implémentation du protocole LDAPS	325
4.2.1 Obtenir un certificat pour le service d'annuaire AD LDS	325
4.2.2 Inscrire le certificat	328
4.2.3 Lier le certificat avec les services AD LDS	330
4.2.4 Démonstration	333
5. Conclusion	334

Chapitre 12

Implémentation de la haute disponibilité

1. Introduction	335
2. Les risques d'une architecture centralisée	336
3. La haute disponibilité de l'annuaire AD LDS	337
3.1 Configuration de plusieurs serveurs AD LDS	338
3.2 Configuration de la mise en cache AD LDS	339
3.3 Mise en place d'une solution d'équilibrage de charge	339
4. L'équilibrage de charge	340
4.1 Algorithme d'équilibrage de charge	341
4.2 Solutions d'équilibrage de charge	342
4.2.1 Solution logicielle d'équilibrage de charge	342
4.2.2 Solution matérielle d'équilibrage de charge	343
4.2.3 Solution d'équilibrage de charge DNS	343
4.3 Considérations spécifiques à l'infrastructure AD LDS	344
5. La fonctionnalité NLB de Windows Server	345
5.1 Présentation	345
5.2 Configuration	347
5.3 Mise à niveau	350
6. La mise en place d'un NLB	351
6.1 Installer la fonctionnalité NLB	351
6.2 Créer un cluster NLB	353
6.3 Ajouter un nouvel hôte au cluster	358
6.4 Tester la tolérance aux pannes	359
7. Conclusion	360
Index	361

Chapitre 4

Introduction aux services AD LDS

1. Introduction

Depuis quelques années, nous assistons à l'apparition de nouveaux services d'annuaire qui font une certaine concurrence à l'annuaire Active Directory. De nombreuses entreprises ont déployé des solutions alternatives qui possèdent presque les mêmes fonctionnalités que l'Active Directory.

Peu de temps après que Microsoft a publié la première version de l'Active Directory, des ingénieurs système, des développeurs d'applications et des professionnels de l'informatique lui ont demandé la possibilité de développer une version plus légère de ce service d'annuaire. Cette version devait permettre une prise en charge flexible des applications tierces, sans les dépendances que requièrent les services de domaine Active Directory.

Suite à ces sollicitations, Microsoft a lancé en 2003 un nouveau service d'annuaire, nommé ADAM (*Active Directory Application Mode*), basé lui aussi sur le protocole LDAP. L'idée est de fournir un système de stockage simple pour l'ensemble des informations relatives à l'authentification : mots de passe, groupes, droits utilisateur... et aussi d'apporter de la souplesse et des facilités aux développeurs d'applications.

Avec la sortie de Windows 2008, un changement de nom a été annoncé pour ADAM, qui a été rebaptisé AD LDS (*Active Directory Lightweight Directory Services*).

AD LDS a permis aux développeurs de stocker et de configurer librement les données de leurs applications sans avoir à se soucier de la gestion de l'authentification des utilisateurs et des groupes. Il représente un excellent produit de substitution aux systèmes de gestion de base de données grâce à son schéma extensible et ses règles de sécurité à granularité fine qui peuvent être implémentées sur les objets.

La documentation est très pauvre au sujet de l'AD LDS et les domaines d'utilisation sont inconnus. De ce fait, nombreux sont ceux qui se demandent pourquoi l'AD LDS n'a jamais été une priorité chez la communauté Microsoft.

Ce chapitre est organisé comme suit. Après cette introduction, la section Présentation des services AD LDS présente les concepts structuraux des services AD LDS. La section Différence entre un AD LDS et un AD DS correspond à l'ensemble des utilisations possibles du produit au sein d'une entreprise. La section Historique des services AD LDS décrit son architecture et les différents composants. La section Scénarios métier et cas d'usage avec AD LDS s'intéresse aux étapes de sa mise en place dans un système d'information.

2. Présentation des services AD LDS

L'AD LDS, le service d'annuaire numéro deux de Microsoft, permet de stocker des informations et fournit un moyen d'authentification centralisé aux applications de l'entreprise.

AD LDS est aussi un annuaire, mais sa particularité est d'être basé sur des instances indépendantes qui s'exécutent en tant que services Windows et qui peuvent être configurées de manière personnalisée pour chaque application. Il est également capable de contenir plusieurs informations comme :

- Utilisateurs
- Groupes
- Unités d'organisation

L'AD LDS ne stocke pas les entités de sécurité Windows mais peut les utiliser pour l'authentification et les contrôles d'accès.

Un annuaire AD LDS permet de distinguer trois types d'authentification :

- L'authentification AD LDS, qui consiste à authentifier les comptes locaux créés dans l'instance AD LDS. Ces comptes sont distincts de ceux utilisés pour se connecter au système d'exploitation ou au domaine AD DS. Si le serveur AD LDS est membre du domaine, les paramètres de stratégie de comptes (complexité du mot de passe, verrouillage...) sont appliqués via les GPO.
- L'authentification Windows connue sous le nom de SSPI (*Security Support Provider Interface*), qui permet d'authentifier les utilisateurs Windows du serveur AD LDS.
- L'authentification par l'intermédiaire d'un objet proxy, qui permet d'authentifier les utilisateurs des services de domaine Active Directory AD DS.

L'annuaire AD LDS permet aux utilisateurs de s'authentifier sur les services Microsoft et non Microsoft se trouvant dans un réseau local et/ou dans une société partenaire. Par exemple, la prise en charge de l'authentification par formulaire (FBA, ou *Forms-based Authentication*) permet à un site SharePoint d'authentifier les utilisateurs et de vérifier les informations des rôles.

AD LDS peut être utilisé en tant que magasin d'attributs personnalisé pour les applications tierces qui disposent d'une logique métier spécifique ou qui s'appuient sur un schéma particulier.

AD LDS offre plusieurs avantages pratiques touchant au fonctionnement quotidien de l'entreprise. Selon le métier et les besoins de chacun, AD LDS propose les fonctionnalités ci-après :

Pour les administrateurs : le schéma utilisé par l'AD LDS est indépendant et autonome, sa modification n'aura pas de conséquences sur l'environnement Active Directory.

Lors de la mise en place de l'authentification par l'intermédiaire d'un objet proxy, le mot de passe des comptes utilisateur du domaine n'est pas stocké dans l'annuaire AD LDS. Cela permettrait, en cas de vol/attaque du serveur, de sécuriser les informations de l'environnement Active Directory.

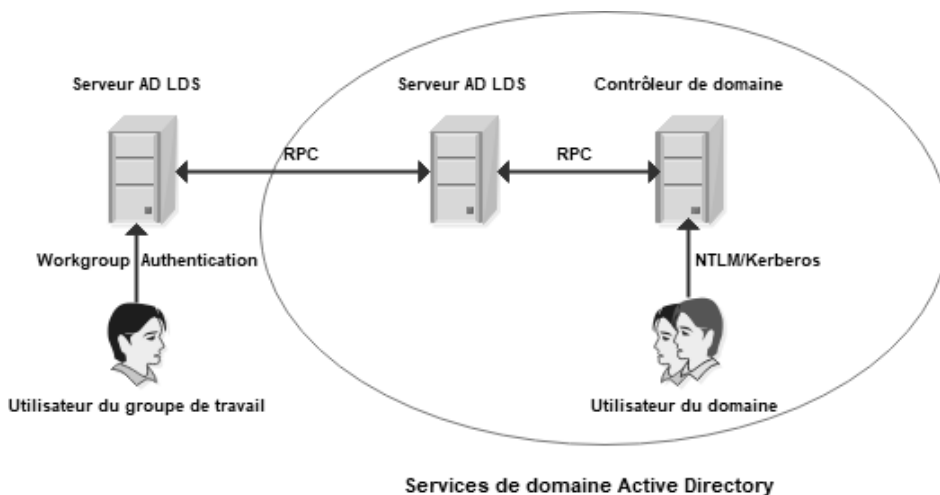
L'AD LDS peut être placé dans une DMZ ou un réseau isolé, ce qui permet à l'entreprise de ne pas exposer ses contrôleurs de domaine pour les besoins d'authentification des applications externes.

Les cmdlets PowerShell pour l'administration du serveur AD LDS sont identiques à celles utilisées avec Active Directory.

Pour les développeurs : AD LDS permet de maintenir une base de données complète des utilisateurs et de centraliser les accès au niveau des applications. Grâce à son schéma extensible, il est possible d'y stocker différents types d'informations, comme, par exemple, la photo des utilisateurs.

Les API standards basés sur le protocole LDAP permettent d'accéder à un panel de fonctionnalités de l'annuaire AD LDS.

Le schéma ci-dessous illustre la façon dont un serveur AD LDS fonctionne avec les services de domaine Active Directory :



Les services AD LDS prennent en charge simultanément deux types de comptes utilisateur : ceux du domaine et ceux du groupe de travail.

3. Différences entre un AD LDS et un AD DS

Les services AD DS et AD LDS partagent la même technologie et les mêmes concepts fondamentaux, mais il existe quelques différences des points de vue fonctionnel et technique.

AD DS et AD LDS reposent sur le système de réplication multimaître pour propager les modifications de données vers les autres serveurs membres. Ils supportent le chiffrement SSL/TLS (connexion LDAPS) ainsi que la délégation d'administration. Bien que les services AD DS et AD LDS puissent s'exécuter sur la même machine, Microsoft recommande d'installer le rôle AD LDS sur un serveur membre ou un serveur autonome.

À la différence d'AD DS, plusieurs instances d'AD LDS peuvent s'exécuter sur le même serveur. Chacune d'elles dispose d'un schéma d'annuaire indépendant et peut être installée ou supprimée sans redémarrage du serveur. Toutes ces instances doivent utiliser des ports TCP/IP distincts afin d'éviter les conflits.

Contrairement à AD DS, AD LDS ne peut stocker les objets représentant les ordinateurs ou les serveurs membres d'un domaine et il ne peut prendre en charge ni les stratégies de groupe (GPO) ni les relations d'approbation de domaines ou de forêts.

Une autre différence est qu'AD DS dépend totalement des services DNS, ce qui n'est pas le cas pour AD LDS. Cela a du sens, car AD DS utilise les mécanismes DNS pour maintenir la hiérarchie des domaines.

Le tableau ci-dessous récapitule les points communs et les différences qui existent entre AD DS et AD LDS :

Caractéristiques	AD DS	AD LDS
Notion de domaine et forêt	Oui	Non
Notion de site	Oui	Oui
Exécution en tant que service	Oui	Oui
Relation d'approbation	Oui	Non
DNS requis	Oui	Non
Notion de schéma	Oui	Oui

Caractéristiques	AD DS	AD LDS
Catalogue global	Oui	Non
Rôle FSMO	Oui	Non
Prise en charge des services AD FS	Oui	Non
Journalisation des événements	Oui	Oui
GPO	Oui	Non
Audit	Oui	Oui
Console utilisateur et ordinateurs Active Directory	Oui	Non
API LDAP	Oui	Oui
Serveur en multi-instance	Non	Oui
Prise en charge du protocole Kerberos	Oui	Non
Liste de contrôle d'accès (ACL)	Oui	Oui

4. Historique des services AD LDS

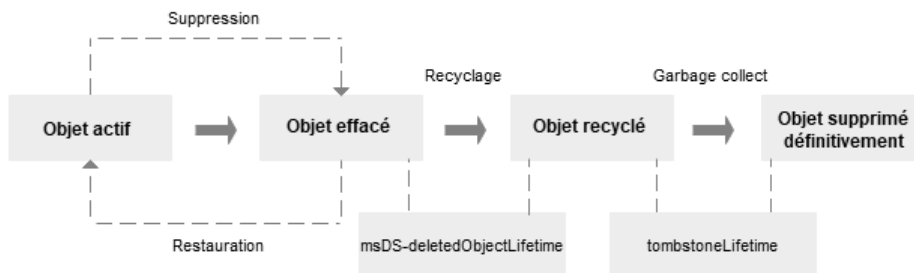
Depuis son lancement, il y a près de deux décennies, Microsoft n'a cessé d'améliorer les fonctionnalités de l'AD LDS et de l'enrichir de nouveautés.

AD LDS est étroitement lié au développement des systèmes d'exploitation Windows. Les sections suivantes présentent les principales nouveautés apportées par Windows Server 2008 et 2012.

4.1 AD LDS sous Windows Server 2008 et 2008 R2

Certes, Windows Server 2008 n'est plus supporté par Microsoft, mais il est utile de rappeler les débuts des services AD LDS. Dans Windows Server 2008, AD LDS peut être installé dans un mode appelé mode core ou minimal, c'est-à-dire sans interface graphique de gestion (GUI, pour *Graphical User Interface*). Le but est de réduire la surface d'attaque du serveur et de supprimer les programmes qui pourraient être exploités par une personne mal attentionnée.

Les services AD LDS utilisent la fonctionnalité de Corbeille AD apparue avec Windows Server 2008, laquelle permet de restaurer, en cas de suppression accidentelle, les objets d'annuaire.



Lorsqu'un objet AD LDS est supprimé, il est déplacé dans le conteneur « CN=Deleted Objects ». L'attribut « msDS-deletedObjectLifetime » indique la durée maximale pendant laquelle un objet supprimé pourra être restauré, tandis que l'attribut « tombstoneLifetime » détermine la durée de vie maximale de l'objet avant sa suppression définitive.

Les services AD LDS peuvent être administrés via des applets de commandes PowerShell incluses dans le module Active Directory. Ces cmdlets sont organisées en deux parties : la première vous permet de gérer les objets de l'annuaire d'une manière générale (utilisateurs, groupes, conteneurs...), et la seconde, appelée Fournisseur Active Directory, permet de représenter la base de données AD LDS sous forme d'une arborescence de fichiers.

Les services AD LDS permettent l'ajout des fichiers de configuration LDIF personnalisés durant le processus d'installation.

Les services AD LDS implémentent la même stratégie d'audit des services de domaine Active Directory. Une sous-catégorie nommée Directory Services Changes est ajoutée. Elle permet de journaliser les événements de modifications d'objets pour lesquels l'audit est activé ; les anciennes valeurs ainsi que les nouvelles sont conservées.