INFORMATIQUE
TECHNIQUE

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

eni

Table des matières

Introduction

Chapitre 1
Généralités sur les annuaires

Chapitre 2
Présentation de la norme LDAP

Chapitre 3
Intégration à Active Directory

Chapitre 4
Introduction aux services AD LDS

Chapitre 5
Prérequis et installation des services AD LDS

Chapitre 6
Présentation des outils d'administration

Chapitre 7
Présentation des partitions d'annuaire

Chapitre 8
Gestion des instances

Chapitre 9
Gestion des objets AD LDS

Chapitre 10

Mise en place de l'authentification AD LDS

Chapitre 11
Sécurisation de l'AD LDS

Chapitre 12
Implémentation de la haute disponibilité

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.

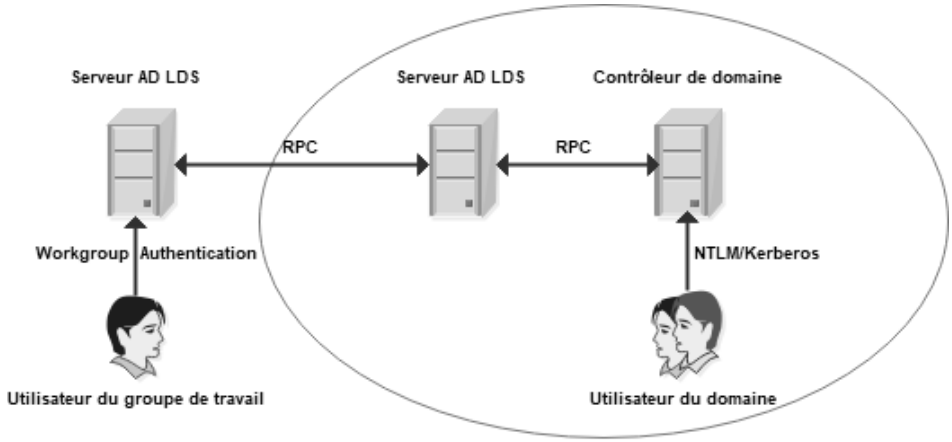
L'AD LDS peut être placé dans une DMZ ou un réseau isolé, ce qui permet à l'entreprise de ne pas exposer ses contrôleurs de domaine pour les besoins d'authentification des applications externes.

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 évènements	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

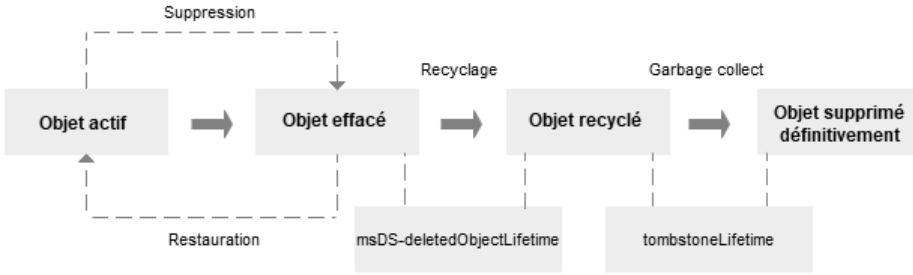
Depuis son lancement, il y a près de deux décennies, Microsoft n'a cessé d'améliorer les fonctionnalités de l'AD LDS et de l'enrichir de nouveautés.

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 cmdlts 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 évènements de modifications d'objets pour lesquels l'audit est activé ; les anciennes valeurs ainsi que les nouvelles sont conservées.