



Présentation des outils de gestion d'annuaire Microsoft Serveur et Client,
comparatif avec les protocole LDAP



Vs

LDAP et les solutions Libres



BTS SIO option SISR

Philippe JUNDT

Table des matières

I.	Présentation d'Active directory	1
II.	Le protocole LDAP	2
	Chaque entrée est constituée d'un ensemble d'attributs (paires clé/valeur) permettent de caractériser l'objet que l'entrée définit. Il existe deux types d'attributs :	4
A.	LDAP et RFC :	4
B.	LDAP et les similitudes avec ADDS :	5
C.	L'utilisation applicative de LDAP.....	7
III.	Comparatif LDAP et AD.....	8
A.	Différents niveau d'authentification.....	8
B.	Exemple de requêtes.....	8
C.	La syntaxe et les messages	9

Fiche de présentation

	BTS SIO Services Informatiques aux Organisations		
	Option	SISR	
	Session	2021	

Philippe JUNDT	Activité professionnelle N°	6
-----------------------	------------------------------------	----------

Nature de l'activité	Présentation des outils de gestion d'annuaire Microsoft Serveur et Client, comparatif avec les protocole LDAP
Contexte	
Objectifs	
Lieu de réalisation	

DESCRIPTION DE LA SOLUTION RETENUE	
Conditions initiales	Une entreprise souhaite s'assurer que les requêtes et les messages qui transitent sur son réseau sont sécurisées.
Conditions finales	Présenter le fonctionnement des solutions d'authentification Microsoft et de LDAP
Outils utilisés	

CONDITIONS DE REALISATION	
Matériels	Recherche sur internet, documentation des éditeurs de Software, site RFC
Logiciels	Microsoft Windows Serveur 2019 Solution Libre : FreeIPA, OpenLDAP
Contraintes	Recherche des solutions existantes pour un état des lieux Trouver des solutions pertinentes et efficace pour un parc informatique homogène Proposer des solutions qui permettent de réduire le risque de captation d'information par sniffing du réseau.

COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE	
	A3.3.3 , Gestion des identités et des habilitations A4.1.9 , Rédaction d'une documentation technique A5.1.2 , Recueil d'informations sur une configuration et ses éléments A5.2.1 , Exploitation des référentiels, normes et standards adoptés par le prestataire A5.2.3 , Repérage des compléments de formation ou d'auto-formation ... A5.2.4 , Étude d'une technologie, d'un composant, d'un outil ou d'une méthode

Présentation des outils de gestion d'annuaire Microsoft et l'ADDS solution Serveur et Client, comparatif avec les protocole LDAP

Contexte :

Présentation des éléments :

ADDS :

Active Directory Domain Services est un service Microsoft, il permet la mise en œuvre d'un domaine et d'un annuaire Active Directory AD. Ce service est à décomposer en sous unités : Unité d'organisation (Universelle, Globale, Locale), en Groupe, en Utilisateur, en Ordinateur, etc... L'intérêt est de permettre de contrôler les accès et de réaliser des authentifications pour un suivi des ressources et des accès. Il est possible de mettre en place des politiques de sécurité en s'appuyant uniquement sur l'ADDS et des GPO.

ADCS est un volet qui permet d'établir des certificats. Il n'est pas nécessairement associé à l'ADDS. ADCS permet aux systèmes d'informations d'intégrer davantage de sécurité en créant des clés et des certificats.

Pour aller plus loin l'ADDS permet d'intégrer à un domaine plusieurs serveurs et services. L'Active Directory peut servir de trame à une infrastructure. En effet un domaine peut se composer d'arbres, de forêts, de sous-domaines.

ADDS s'appuie sur différents protocoles, dont LDAP, le DNS et Kerberos.

I. Présentation d'Active directory

L'ADDS ou l'AD est un protocole propriétaire Microsoft.

L'Active Directory (AD) prend en charge à la fois Kerberos et LDAP – Microsoft AD est le système de services d'annuaire le plus répandu aujourd'hui. AD fournit l'authentification unique (SSO) et fonctionne en distantiel, notamment au travers des réseaux opérateurs FAI, des VPN, ou au Bureau.

Attention AD et Kerberos ne sont pas multiplateformes, tous les UNIX, notamment Linux doivent bénéficier de services complémentaires.

Aussi les entreprises ont recours à des logiciels de gestion d'accès pour centraliser les connexions réalisées à partir du parc de l'entreprise ou à partir des équipements à distances et multi-plateformes.

AD prend en charge LDAP, il peut s'intégrer à un système d'information et permettre d'avoir une vision globale des accès et de réaliser une gestion et une sécurisation en conséquent.

Il existe d'autres logiciels de gestion des annuaires : des services Red Hat et FreeIPA, Open LDAP, le serveur d'annuaire Apache

II. Le protocole LDAP

LDAP ou Lightweight Directory Access Protocol est un protocole multiplateforme utilisé pour l'authentification des services d'annuaires. Protocole d'accès aux annuaires léger et dit « L DAP », désigne aussi un protocole standard qui permet de gérer et d'accéder à des annuaires, des bases de données et d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP. Les informations sont en principe relatives aux utilisateurs, aux équipements informatiques d'une d'une entreprise.

Historique : Le protocole LDAP a été développé en 1993 par l'université du Michigan, pour supplanter le protocole DAP (intermédiaire pour l'accès au service d'annuaire X.500 de l'OSI), en l'intégrant à la suite TCP/IP.

C'est en 1995 que LDAP est devenu un annuaire natif (*standalone LDAP*), afin de ne plus servir uniquement à accéder à des annuaires de type X500. LDAP est devenu une version allégée du protocole DAP, d'où son nom de ***Lightweight Directory Access Protocol***.

LDAP permet de normaliser et définir une méthode d'accès aux données du serveur. C'est une normalisation pour encadrer l'accès aux identifiants ou informations qui doivent être récupérées par l'ordinateur client sur le serveur. La sécurisation et le stockage des informations sont indépendantes. La version exploitée actuellement est le LDAP version 3 normalisée par une RFC publiée par l'IETF RFC 1777 pour LDAP v.2 standard¹
RFC 2251 pour LDAP v.3 standard²

Pour faire simple LDAP assure la normalisation du langage de communication par les applications pour communiquer entre les serveurs de service d'annuaires. Les serveurs d'annuaire stockent les comptes et les mots de passe des utilisateurs et des ordinateurs et après authentification partagent ces informations avec d'autres entités du réseau.

Les avancées de LDAP sont qu'elle intègre dans sa version 3 un mécanisme de chiffrement SSL et d'authentification SASL qui sécurise l'accès aux informations stockées dans la base.

LDAP, comme active directory fonctionne par arborescence. Nous retrouvons des UO pour unité d'organisation, des groupes ou OU...

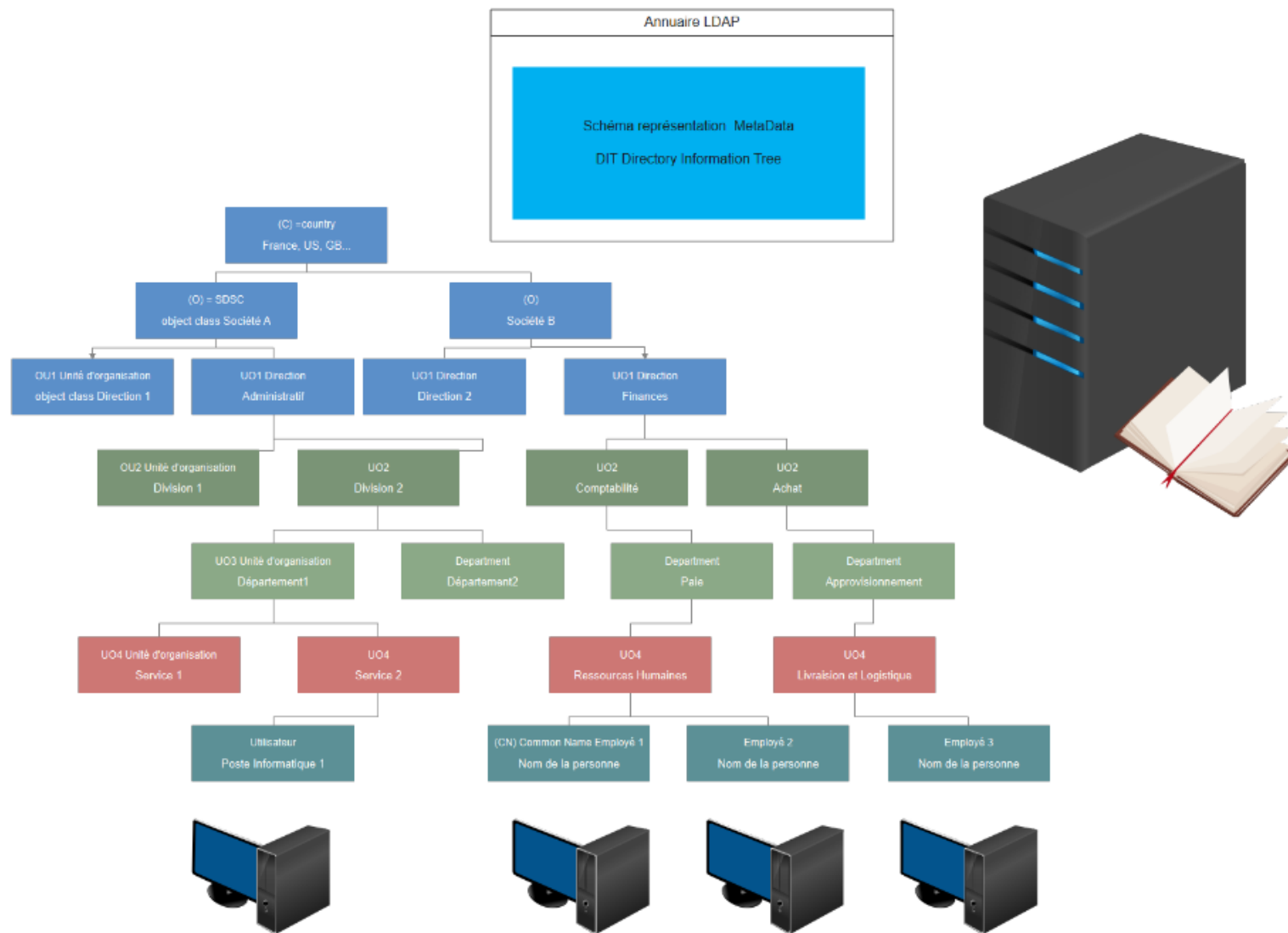
Cette arborescence d'information est hiérarchisée et standardisée, elle est appelée DIT (Directory Information Tree voir Schéma p3), dans laquelle les informations, appelées entrées ou (DES, *Directory Service Entry*), sont représentées sous forme de branches. Une branche située à la racine d'une ramification est appelée racine ou suffixe (*root entry*).

LDAP permet de réaliser des annuaires de personnel ou d'équipements (GLPI en est un exemple de service compatible)

Chaque entrée est composée d'un ensemble de paires clés/valeurs appelées **attributs**

¹ Site Internet Engineering Task Force IETF, : <https://www.ietf.org/rfc/rfc2251.txt>, dernière consultation le 14.03.2021

² Site Internet Engineering Task Force IETF, : <https://www.ietf.org/rfc/rfc2251.txt>, dernière consultation le 14.03.2021



Comme vu ci-dessus LDAP correspond à un annuaire normalisé, les entrées sont donc à coder en anglais.

Voici un petit mémo de Comment ça marche :

Chaque entrée est constituée d'un ensemble d'attributs (paires clé/valeur) permettant de caractériser l'objet que l'entrée définit. Il existe deux types d'attributs :

- **Les attributs normaux:** ceux-ci sont les attributs habituels (nom, prénom, ...) caractérisant l'objet
- **Les attributs opérationnels:** ceux-ci sont des attributs auxquels seul le serveur peut accéder afin de manipuler les données de l'annuaire (dates de modification, ...).

Une entrée est indexée par un **nom distinct** (**DN**, *distinguished name*) permettant d'identifier de manière unique un élément de l'arborescence.

Un DN se construit en prenant le nom de l'élément, appelé *Relative Distinguished Name* (*RDN*, c'est-à-dire le chemin de l'entrée par rapport à un de ses parents), et en lui ajoutant l'ensemble des nom des entrées parentes. Il s'agit d'utiliser une série de paires clé/valeur permettant de repérer une entrée de manière unique. Voici une série de clés généralement utilisées :

- **uid** (*userid*), il s'agit d'un identifiant unique obligatoire
- **cn** (*common name*), il s'agit du nom de la personne
- **givenname**, il s'agit du prénom de la personne
- **sn** (*surname*), il s'agit du surnom de la personne
- **o** (*organization*), il s'agit de l'entreprise de la personne
- **u** (*organizational unit*), il s'agit du service de l'entreprise dans laquelle la personne travaille
- **mail**, il s'agit de l'adresse de courrier électronique de la personne³

A. LDAP et RFC :

Selon la RFC : Protocole allégé d'accès à un annuaire (v3) ou LDAP "Lightweight Directory Access Protocol (v3)" a été normalisé en 1997.

Le modèle général adopté par ce protocole est celui de clients effectuant des opérations du protocole auprès de serveurs. Dans ce modèle, un client transmet à un serveur une demande du protocole décrivant l'opération à exécuter. Le serveur est alors responsable de l'exécution de l'opération(s) nécessaire dans l'annuaire. Sur l'accomplissement de l'opération(s), le serveur renvoie une réponse contenant tous les résultats ou erreurs au client demandeur.

En accord avec l'objectif de réduction des coûts associés à l'utilisation d'un annuaire, un des objectifs de ce protocole est de réduire au minimum la complexité des clients afin de faciliter le déploiement étendu des applications capables d'utiliser l'annuaire.⁴

Le protocole LDAP (Lightweight Directory Access Protocol) permet de gérer un annuaire, il fonctionne sur le principe des requêtes d'interrogations et de modification de base de données. L'AD est un annuaire LDAP.

³ Le protocole LDAP, comment ça marche : <https://www.commentcamarche.net/contents/525-le-protocole-ldap>, dernière consultation le 17 mars 2021

⁴ Traduction de la RFC LDAP, url : <http://abcedrfc.free.fr/rfc-vf/rfc2251.html>, dernière consultation le 14.03.2021

En principe LDAP communique sur le port 389, en TCP, depuis le serveur contrôleur du domaine.

Pour plus de sécurité LDAPS intègre des certificats SSL « LDAP over SSL » qui permet notamment d'intégrer du chiffrement dans les requêtes LDAP.

B. LDAP et les similitudes avec ADDS :

Un annuaire LDAP contient également des unités d'organisation qui forment l'arborescence générale. Ensuite, on trouve tous les différents types d'objets classiques : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, voir même serveurs et imprimantes.

Pour chaque objet, il stocke des attributs correspondant à la valeur d'un objet. Il est question d'attribut avec un nom relatif :

Nom différencié et nom différencié relatif

Un LDAPDN et un "RelativeLDAPDN" sont respectivement définis pour être la représentation d'un nom différencié et d'un nom différencié relatif après avoir encodé selon la spécification dans [4], tels que :

<distinguished-name> ::= <name>

<relative-distinguished-name> ::= <name-component>

ou <name> et <name-component> sont définis dans [4].

LDAPDN ::= LDAPString

RelativeLDAPDN ::= LDAPString⁵

Attention l'enveloppe message ou la requête du protocole correspond à un autre élément :

Pour les fonctions des échanges du protocole, toutes les opérations du protocole sont encapsulées sous enveloppe commune, le "LDAPMessage", qui est défini comme suit :

```
LDAPMessage ::= SEQUENCE {  
    messageID      MessageID,  
    protocolOp     CHOICE {  
        bindRequest      BindRequest,  
        bindResponse     BindResponse,  
        unbindRequest    UnbindRequest,  
        searchRequest    SearchRequest,  
        searchResEntry   SearchResultEntry,  
        searchResDone    SearchResultDone,  
        searchResRef     SearchResultReference,  
        modifyRequest    ModifyRequest,  
        modifyResponse   ModifyResponse,  
        addRequest       AddRequest,  
        addResponse      AddResponse,  
        delRequest       DelRequest,  
        delResponse      DelResponse,  
        modDNRequest     ModifyDNRequest,
```

⁵ RFC p7


```

modDNResponse ModifyDNResponse,
compareRequest CompareRequest,
compareResponse CompareResponse,
abandonRequest AbandonRequest,
extendedReq ExtendedRequest,
extendedResp ExtendedResponse },
controls [0] Controls OPTIONAL }

```

MessageID ::= INTEGER (0 .. maxInt)

maxInt INTEGER ::= 2147483647 -- (2³¹ - 1) --

La fonction du message LDAP est de fournir une enveloppe contenant les champs communs exigés dans tous les échanges du protocole. À cet instant les seuls champs communs sont l'identification de message et les commandes.

Si le serveur reçoit une PDU du client dans laquelle l'étiquette "LDAPMessage" SEQUENCE ne peut pas être identifiée, le "messageID" ne peut pas être analysé, l'étiquette du "protocolOp" n'est pas identifiée comme une demande, ou les structures ou les longueurs encodantes des champs données s'avèrent incorrectes, alors le serveur DOIT renvoyer la notification de déconnexion décrite dans la section 4.4.1, avec "resultCode protocolError", et fermer immédiatement la connexion. Dans les autres cas où le serveur ne peut pas analyser la demande reçue par le client, le serveur DOIT renvoyer une réponse appropriée à la demande, avec le "resultCode" réglé sur "protocolError".

Si le client reçoit une PDU du serveur qui ne peut pas être analysée, le client peut rejeter la PDU, ou peut fermer la connexion brutalement⁶.

⁶ RFC p9

C. L'utilisation applicative de LDAP

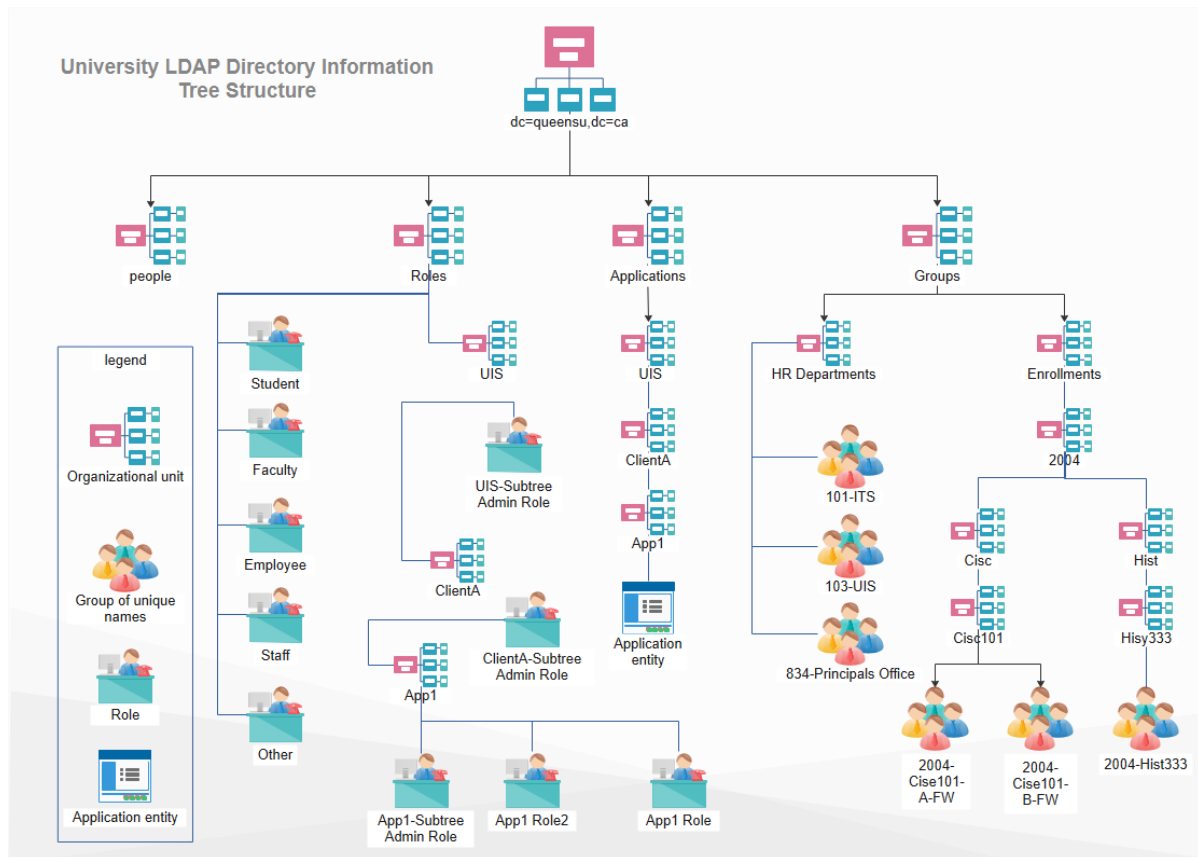


Figure 1 Source Edraw, LDAP et applicatif




III. Comparatif LDAP et AD

LDAP peut communiquer avec un AD, il s'agit d'un protocole générique et open source, compris par un grand nombre de services d'annuaires et de solutions de gestion des accès.

A. Différents niveaux d'authentification

LDAP version 3 propose en outre deux options d'authentification LDAP : simple et SASL (*Simple Authentication and Security Layer*).

Pour la forme simple :

anonyme	Non authentifié	Par nom ou mot de passe
		
Accorder l'anonymat au client pour l'accès aux services LDAP	Uniquement à des fins de journalisation ou d'administration, service sans accès aux clients	Accorde un accès au serveur en se basant sur les identifiants fournis – une simple authentification par nom/mot de passe n'est pas sécurisée et ne convient pas à une authentification dans les environnements sans protection de la confidentialité.

La forme SASL est une authentification qui lie le serveur LDAP à un autre mécanisme d'authentification. Similaire à l'authentification à double facteur (2FA pour two-factor authentication). Microsoft propose Kerberos. Pour LDAP le serveur utilise le protocole pour envoyer un message LDAP à l'autre service d'autorisation. Un processus s'enclenche pour authentifier et accorder l'accès ou pour aboutir sur un message :

- d'authentification réussie
- d'échec d'authentification.

Attention LDAP transmet par défaut les informations en texte clair, il faut se prémunir contre le sniffing de réseau. Il est possible d'implémenter un cryptage, comme le chiffrement par TLS pour garantir l'intégrité de l'information en transit qui sont le mot de passe et le nom de l'utilisateur.

Une requête LDAP est en principe normalisée comme vu dans la RFC v3 vu ci-haut. Une requête LDAP est une commande qui demande certaines informations à un service d'annuaire.

B. Exemple de requêtes

Voici un exemple, avec une référence au groupe, auquel appartient un utilisateur :

```
(&(objectClass=user)(sAMAccountName=yourUserName)
(memberof=CN=YourGroup,OU=Users,DC=YourDomain,DC=com))
```

```
(&(objectClass=user)(sAMAccountName=yourUserName)
(memberof=CN=YourGroup,OU=Users,DC=YourDomain,DC=com))
```

LDAP permet de réaliser un ensemble de fonctions ou procédure, pour effectuer des requêtes sur les données :

Opération	Description
Abandon	Abandonne l'opération précédemment envoyées au serveur
Add	Ajoute une entrée au répertoire
Bind	Initie une nouvelle session sur le serveur LDAP
Compare	Compare les entrées d'un répertoire selon des critères
Delete	Supprime une entrée d'un répertoire
Extended	Effectue des opérations étendues
Rename	Modifie le nom d'une entrée
Search	Recherche des entrées d'un répertoire
Unbind	Termine une session sur le serveur LDAP

C. La syntaxe et les messages

Ces données ou messages sont échangées selon le format LDIF :

LDAP fournit un format d'échange (**LDIF**, *Lightweight Data Interchange Format*) permettant d'importer et d'exporter les données d'un annuaire avec un simple fichier texte. La majorité des serveurs LDAP supportent ce format, ce qui permet une grande interopérabilité entre eux.

La syntaxe de ce format est la suivante :

```
[<id>] dn: <distinguished name> <attribut> : <valeur> <attribut> : <valeur> ...
```

Dans ce fichier, *id* est facultatif, il s'agit d'un entier positif permettant d'identifier l'entrée dans la base de données.

- chaque nouvelle entrée doit être séparée de la définition de l'entrée précédente à l'aide d'un saut de ligne (ligne vide)
- Il est possible de définir un attribut sur plusieurs lignes en commençant les lignes suivantes par un espace ou un tabulation
- Il est possible de définir plusieurs valeurs pour un attribut en répétant la chaîne *nom:valeur* sur des lignes séparées

- lorsque la valeur contient un caractère spécial (non imprimable, un espace ou :), l'attribut doit être suivi de :: puis de la valeur encodée en base64

Finalement les requêtes LDAP sont souvent liées à des interfaces et s'exécutent en arrière-plan.

LDAP est un protocole et Active Directory est un service ou rôle lié à un serveur. LDAP authentifie Active Directory, qui est un ensemble de directives pour envoyer et recevoir des informations (comme des noms d'utilisateurs et des mots de passe) vers et depuis Active Directory.

Sitographie :

Protocole allégé d'accès à un annuaire (v3), LDAP "Lightweight Directory Access Protocol (v3)"
<http://abcdnrfc.free.fr/rfc-vf/rfc2251.html>

Renforcement de la sécurité de l'authentification LDAP sur SSL/TLS à l'aide de l'entrée de Registre LDAPEnforceChannelBinding (microsoft.com)
<https://support.microsoft.com/fr-fr/topic/renforcement-de-la-s%C3%A9curit%C3%A9-de-l-authentification-ldap-sur-ssl-tls-%C3%A0-l-aide-de-l-entr%C3%A9e-de-registre-ldapenforcechannelbinding-e9ecfa27-5e57-8519-6ba3-d2c06b21812e>

Un annuaire Active Directory, pourquoi ? | IT-Connect (it-connect.fr)
<https://www.it-connect.fr/chapitres/un-annuaire-active-directory-pourquoi/>

Tutoriel Active Directory - Activation du LDAP sur SSL [Étape par étape] (techexpert.tips)
<https://techexpert.tips/fr/windows-fr/activer-le-ldap-active-du-repertoire-par-dessus-la-fonction-ssl/>

Afficher et définir la stratégie LDAP (Lightweight Directory Access Protocol) avec Ntdsutil - Windows Server | Microsoft Docs
<https://docs.microsoft.com/fr-fr/troubleshoot/windows-server/identity/view-set-ldap-policy-using-ntdsutil>

Comment activer la signature LDAP - Windows Server | Microsoft Docs
<https://docs.microsoft.com/fr-fr/troubleshoot/windows-server/identity/enable-ldap-signing-in-windows-server>

La différence entre Active Directory et LDAP (varonis.fr)
<https://blog.varonis.fr/difference-entre-active-directory-et-ldap/>

Annexes