Comment fonctionne un annuaire LDAP ?

- Qu’est-ce que le LDAP ?

Qu’est-ce que le LDAP ?

Le **LDAP** est un protocole utilisé pour communiquer avec un annuaire informatique. Son nom complet est *Lightweight Directory Access Protocol*, ce qui signifie « protocole léger d’accès à un annuaire ».

Dit comme cela, le LDAP peut sembler un peu compliqué. Pourtant, son idée principale est assez simple : il permet de ranger et de retrouver des informations sur des utilisateurs, des groupes, des ordinateurs et différents équipements d’un réseau.

On peut comparer un annuaire LDAP à un grand carnet d’adresses numérique. Au lieu d’y trouver uniquement des noms et des numéros de téléphone, on peut aussi y trouver des identifiants, des adresses électroniques, des services, des droits et des groupes.

Un carnet d’adresses pour les applications

Dans une organisation, les utilisateurs ont souvent besoin d’accéder à plusieurs services :

- leur messagerie ;
- le réseau Wi-Fi ;
- un serveur de fichiers ;
- une application interne ;
- un outil de support ;
- un logiciel de supervision.

Sans annuaire centralisé, chaque service peut avoir sa propre liste d’utilisateurs. Il faut alors créer plusieurs comptes pour une même personne.

Cette organisation devient vite difficile à gérer. Lorsqu’un nouvel employé arrive, il faut créer son compte partout. Lorsqu’il change de service, il faut modifier ses droits dans plusieurs applications. Lorsqu’il quitte l’organisation, il faut penser à désactiver tous ses accès.

Avec un annuaire LDAP, les informations principales peuvent être regroupées au même endroit. Les applications viennent ensuite consulter cet annuaire lorsqu’elles ont besoin de vérifier l’identité d’une personne ou de connaître ses groupes.

Une comparaison avec une bibliothèque

Pour comprendre le fonctionnement d’un annuaire LDAP, imaginons une bibliothèque.

Les livres ne sont pas rangés au hasard. Ils sont classés dans des rayons, puis organisés par thèmes. Grâce à cette organisation, il est plus facile de retrouver un livre précis.

Un annuaire LDAP fonctionne d’une manière comparable. Les informations sont rangées dans une arborescence :

- les utilisateurs peuvent être placés dans un rayon ;
- les groupes peuvent être placés dans un autre ;
- les ordinateurs peuvent être rangés dans une catégorie séparée ;
- les différents services de l’organisation peuvent avoir leur propre emplacement.

Cette organisation permet aux applications de retrouver rapidement les informations dont elles ont besoin.

Que trouve-t-on dans un annuaire LDAP ?

Un annuaire LDAP peut contenir beaucoup de types d’informations. On peut y enregistrer des personnes, des groupes, des ordinateurs, des imprimantes, des serveurs ou encore des services.

Pour un utilisateur, on peut par exemple enregistrer :

- son prénom ;
- son nom ;
- son identifiant ;
- son adresse électronique ;
- son numéro de téléphone ;
- son service ;
- son poste dans l’organisation ;
- les groupes auxquels il appartient.

On peut comparer cela à une fiche dans un carnet d’adresses. Chaque personne possède une fiche avec plusieurs informations.

Un exemple simplifié pourrait ressembler à ceci :

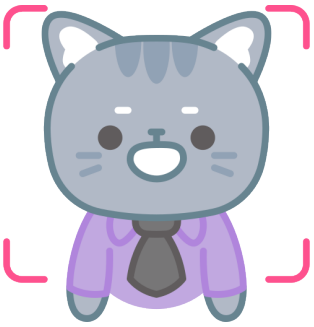
```
Prenom : Alice
Nom : Martin
Identifiant : alice
Adresse electronique : alice@exemple.fr
Service : Informatique
Groupes : Techniciens, Utilisateurs
```

Dans un véritable annuaire, ces informations sont enregistrées avec des noms d’attributs précis. Mais l’idée reste la même : chaque utilisateur possède une fiche qui peut être consultée par les applications autorisées.

Les utilisateurs et les groupes

Les groupes sont très utiles pour organiser les utilisateurs et gérer leurs droits.

Un groupe rassemble plusieurs personnes qui ont quelque chose en commun. Il peut s’agir du même service, du même métier ou du même niveau d’autorisation.



Une organisation pourrait par exemple posséder les groupes suivants :

- **Utilisateurs :** les personnes qui utilisent les services courants ;
- **Techniciens :** les personnes qui doivent accéder aux outils de support ;
- **Direction :** les personnes qui peuvent consulter certains documents ;
- **Administrateurs :** les personnes chargées de gérer les serveurs et les applications.

Au lieu de donner les droits à chaque personne une par une, on peut les attribuer à un groupe.

Imaginons qu’un logiciel soit réservé aux techniciens. L’administrateur n’a pas besoin d’ajouter chaque technicien manuellement dans le logiciel. Il peut demander au logiciel de vérifier si l’utilisateur appartient au groupe **Techniciens**.

On peut comparer ce fonctionnement à un système de badges dans un bâtiment :

- un badge classique permet d’entrer dans les espaces communs ;
- un badge de technicien permet d’entrer dans la salle informatique ;
- un badge d’administrateur permet d’ouvrir la salle des serveurs.

Le groupe auquel appartient l’utilisateur joue donc un peu le rôle de son badge.

Le LDAP peut vérifier votre identité

Un annuaire LDAP est souvent utilisé pour l’**authentification**. L’authentification consiste à vérifier l’identité d’une personne.

Lorsque vous vous connectez à une application, vous indiquez généralement un identifiant et un mot de passe. L’application peut demander à l’annuaire LDAP de vérifier ces informations.

Le déroulement ressemble à ceci :

1. Vous ouvrez une application.
2. Vous indiquez votre identifiant et votre mot de passe.
3. L’application recherche votre compte dans l’annuaire.
4. L’annuaire vérifie le mot de passe.
5. Il répond que la connexion est acceptée ou refusée.
6. L’application peut ensuite regarder les groupes auxquels vous appartenez.

Si les informations sont correctes, l’application vous laisse généralement entrer. Si le mot de passe est faux ou si le compte n’existe pas, la connexion est refusée.

Authentification et autorisation

Il ne faut pas confondre l’authentification et l’autorisation.

L’authentification répond à la question :

« Qui êtes-vous ? »

L’autorisation répond à une autre question :

« Qu’avez-vous le droit de faire ? »

Par exemple, le LDAP peut confirmer que vous êtes bien Alice. L’application peut ensuite vérifier que vous appartenez au groupe des techniciens.

Si vous êtes membre de ce groupe, vous pourrez peut-être consulter les tickets de support. En revanche, vous n’aurez pas forcément le droit de modifier la configuration du serveur.

Le LDAP fournit donc les informations sur l’utilisateur et ses groupes. C’est ensuite à chaque application de décider ce que cette personne peut faire.

Une organisation en forme d’arbre

Les informations d’un annuaire LDAP sont généralement organisées comme les branches d’un arbre.

Imaginons une organisation appelée **exemple.fr** :

```
exemple.fr
├── Utilisateurs
│   ├── Alice
│   └── Bob
├── Groupes
│   ├── Techniciens
│   │   ├── GLPI_TECH
│   │   └── Dossier_partagé_TECH
│   └── Administrateurs
│       ├── GLPI_ADMIN
│       └── Dossier_partagé_ADMIN
└── Ordinateurs
    ├── PC-001
    └── PC-002
```

Cette structure permet de comprendre où chaque information se trouve.

Dans une véritable configuration, les noms sont souvent écrits avec des abréviations. Le chemin d’Alice pourrait par exemple être écrit ainsi :

```
uid=alice,ou=Utilisateurs,dc=exemple,dc=fr
```

Cette ligne indique que l’utilisateur Alice se trouve dans la partie « Utilisateurs » de l’organisation « exemple.fr ».

Ce chemin peut être comparé à une adresse complète. Le nom Alice indique la personne recherchée, tandis que le reste du chemin indique où elle se trouve dans l’annuaire.

Le LDAP et Active Directory

Le LDAP est un protocole. Ce n’est donc pas un logiciel unique.

OpenLDAP est un logiciel libre qui permet de créer un annuaire LDAP. Il est très utilisé sur les serveurs Linux et dans les environnements auto-hébergés.

Active Directory est la solution d’annuaire proposée par Microsoft. Un annuaire Active Directory utilise notamment le LDAP, mais il s’appuie aussi sur d’autres technologies, comme Kerberos, le DNS et les stratégies de groupe.

On peut comparer le LDAP à une langue commune. Plusieurs logiciels peuvent parler cette langue, même s’ils ne proposent pas exactement les mêmes fonctions.

Le LDAP dans la vie quotidienne

Vous utilisez peut-être déjà un annuaire LDAP sans le savoir.

Dans une entreprise ou une école, un annuaire peut servir à :

- ouvrir une session sur un ordinateur ;
- se connecter au réseau Wi-Fi ;
- accéder à une application ;
- retrouver les coordonnées d’un collègue ;
- déterminer les droits d’un utilisateur ;
- gérer les comptes d’un grand nombre de personnes.

Le LDAP est particulièrement pratique lorsqu’il faut gérer beaucoup d’utilisateurs et plusieurs services différents.

Lorsqu’une nouvelle personne arrive, son compte peut être créé dans l’annuaire puis ajouté aux groupes nécessaires.

Lorsqu’elle change de service, il suffit souvent de modifier ses groupes.

Lorsqu’elle quitte l’organisation, son compte peut être désactivé dans l’annuaire. Les applications qui utilisent cet annuaire peuvent alors refuser ses prochaines connexions.

La sécurité d’un annuaire LDAP

Un annuaire LDAP peut contenir des informations importantes. Il faut donc éviter de le laisser accessible à n’importe qui.

Les échanges entre les applications et le serveur doivent être protégés, surtout lorsqu’ils contiennent des mots de passe. Une connexion chiffrée permet d’éviter qu’un mot de passe soit lu pendant son transport sur le réseau.

Il faut également limiter les droits des applications. Une application qui a seulement besoin de consulter les utilisateurs ne devrait pas pouvoir supprimer des comptes.

Quelques bonnes pratiques sont importantes :

- utiliser une connexion sécurisée ;
- limiter les droits des comptes techniques ;
- éviter de partager les mots de passe ;
- désactiver les comptes inutilisés ;
- effectuer des sauvegardes régulières ;
- tester la restauration des sauvegardes ;
- surveiller les connexions inhabituelles.

La sécurité ne dépend pas uniquement du mot de passe. Il faut aussi vérifier que les utilisateurs ne reçoivent pas plus de droits que nécessaire.

Les avantages du LDAP

- **Les comptes sont centralisés :** les informations sont regroupées au même endroit.
- **L’administration est simplifiée :** il est plus facile de créer, modifier ou désactiver un utilisateur.
- **Les groupes facilitent la gestion des droits :** les autorisations peuvent être organisées par métier ou par service.
- **Les applications peuvent partager les mêmes informations :** il n’est pas nécessaire de recréer chaque utilisateur partout.
- **La structure est claire :** les informations sont rangées dans une arborescence.

Les limites du LDAP

Le LDAP est très utile, mais il ne répond pas à tous les besoins.

Un annuaire est surtout conçu pour consulter rapidement des informations sur les utilisateurs et les équipements. Il n’est pas forcément adapté pour gérer des commandes, des factures, des articles ou de gros historiques de données.

Une mauvaise organisation peut également rendre l’annuaire difficile à maintenir. Il faut donc réfléchir à sa structure avant de créer beaucoup de comptes et de groupes.

Enfin, une panne de l’annuaire peut perturber plusieurs applications en même temps. Il est donc important de prévoir des sauvegardes et une solution de restauration.

Pour résumer

Le LDAP est un protocole qui permet aux applications de communiquer avec un annuaire informatique.

Un annuaire LDAP peut contenir des utilisateurs, des groupes, des ordinateurs et différentes informations utiles à une organisation.

Il peut notamment servir à :

- centraliser les comptes ;
- vérifier l’identité des utilisateurs ;
- organiser les personnes en groupes ;
- faciliter la gestion des droits ;
- permettre à plusieurs applications de partager les mêmes informations.

Pour le dire simplement, un annuaire LDAP est à la fois un carnet d’adresses et un gardien. Il peut dire qui est une personne, à quel groupe elle appartient et quelles informations les applications peuvent consulter.