Gestion d'annuaires unifiés

Lightweight Directory Access Protocol : Introduction

Luca SAIU

http://ageinghacker.net

Département Réseaux et Télécommunications
IUT de Villetaneuse, Université Paris 13

Décembre 2018

Sommaire

À propos de vous

- Connaissez-vous SQL ?
- Connaissez-vous LDAP ?
  Qu'est-ce qu'est un *annuaire* ?

À propos de vous

- Connaissez-vous SQL ?
- Connaissez-vous LDAP ?
  Qu'est-ce qu'est un *annuaire* ?

À propos de moi

- Luca SAIU
  - `http://ageinghacker.net`
  - Vous trouvez la page web officielle du cours en suivant le lien “*Teaching*” ;
  - Je suis facile à contacter (mais *n'utilisez pas l'ENT*).
  - Programmeur depuis 30 ans, spécialiste en langages de programmation
  - Utilisateur de GNU/Linux depuis 20 ans
  - Maintainer GNU
  - J'administre mon serveur personnel
    - Je croix en la puissance des interfaces *linguistiques* dans l'interface humain-machine

À propos de moi

- Luca SAIU
  - `http://ageinghacker.net`
  - Vous trouvez la page web officielle du cours en suivant le lien “*Teaching*” ;
  - Je suis facile à contacter (mais *n'utilisez pas l'ENT*).

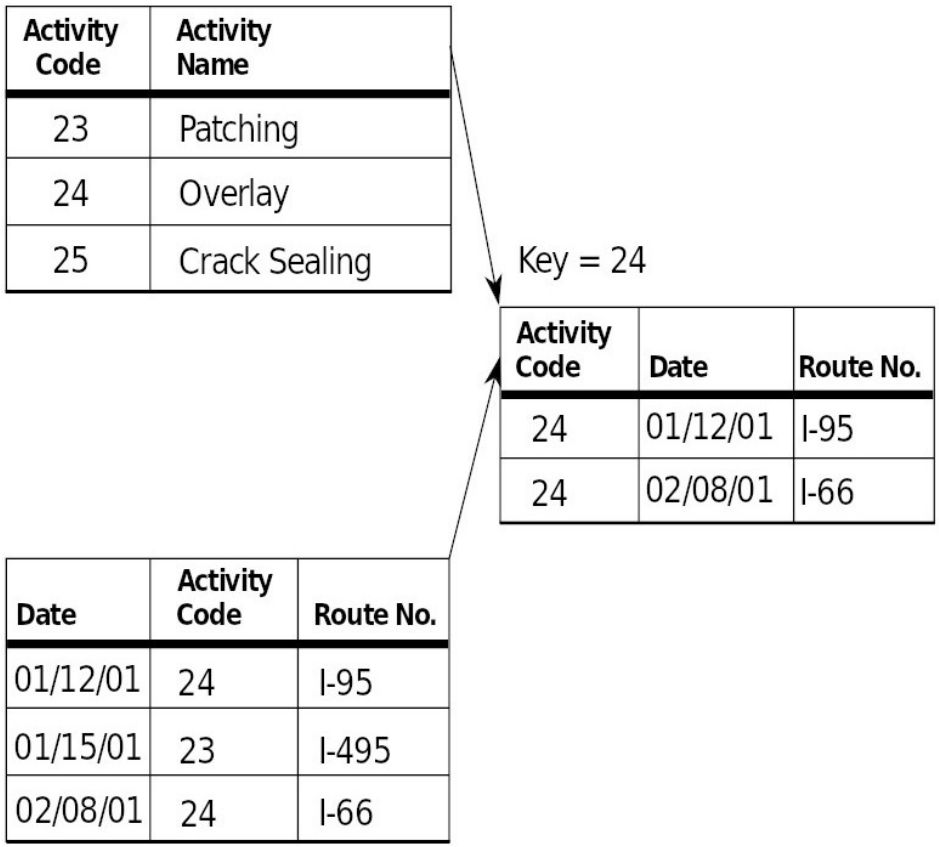
  - Programmeur depuis 30 ans, spécialiste en langages de programmation
  - Utilisateur de GNU/Linux depuis 20 ans
  - Maintainer GNU
  - J'administre mon serveur personnel
    - Je croix en la puissance des interfaces *linguistiques* dans l'interface humain-machine

À propos de moi

- Luca SAIU
  - `http://ageinghacker.net`
  - Vous trouvez la page web officielle du cours en suivant le lien “*Teaching*” ;
  - Je suis facile à contacter (mais *n'utilisez pas l'ENT*).

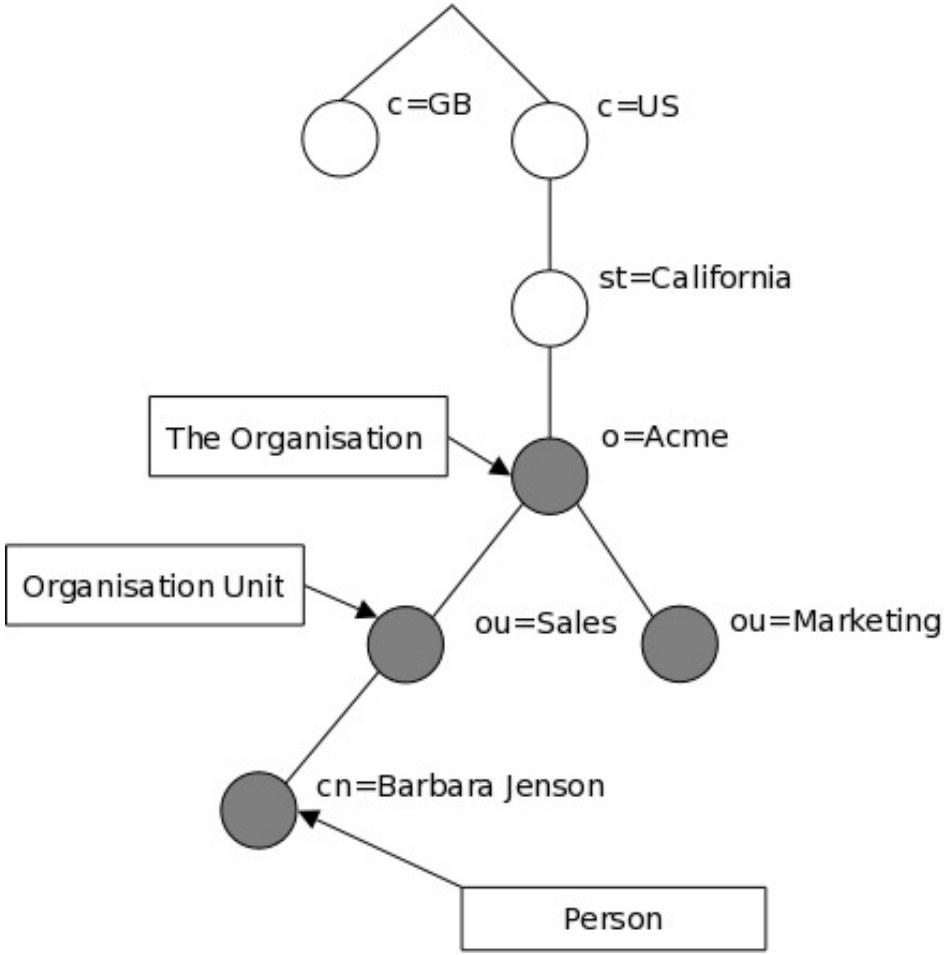
  - Programmeur depuis 30 ans, spécialiste en langages de programmation
  - Utilisateur de GNU/Linux depuis 20 ans
  - Maintainer GNU
  - J'administre mon serveur personnel
    - Je croix en la puissance des interfaces *linguistiques* dans l'interface humain-machine

Modèle relationnel : tables ou relations



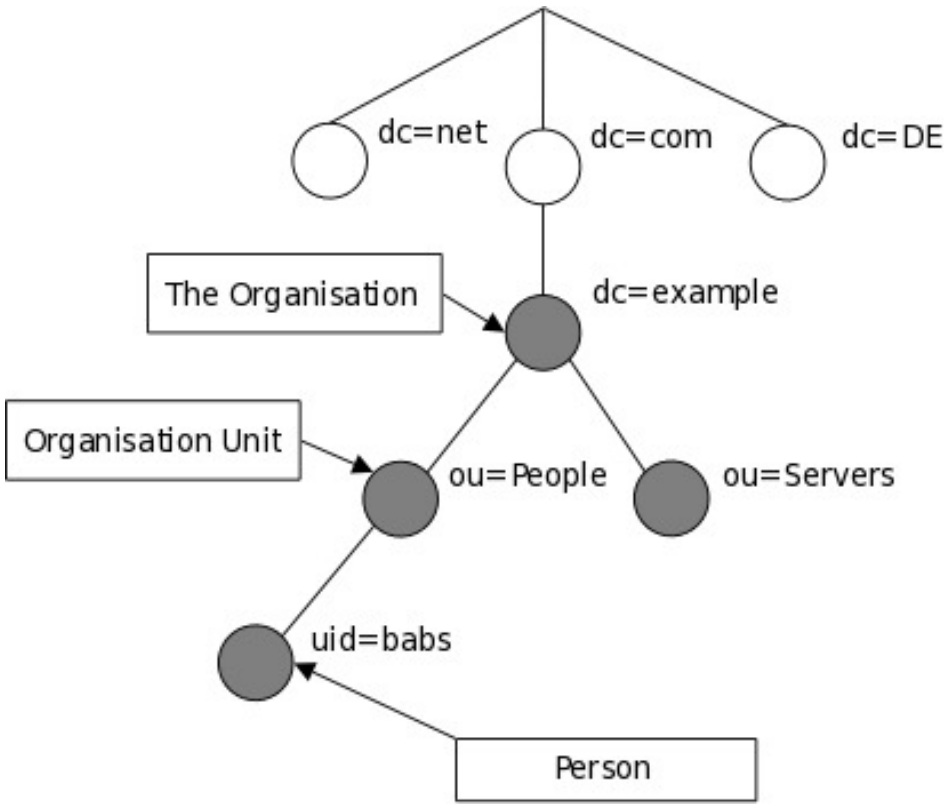
Modèle relationnel (par exemple, SQL—non LDAP) : tables, clés primaires, clés externes.

Modèle arborescent



Une vision hiérarchique (LDAP). Style traditionnel.

Modèle arborescent (style Internet)



Une vision hiérarchique (LDAP). Style Internet.

Les annuaires

LDAP : Introduction et histoire

Lightweight Directory Access Protocol

- Tim Howes, Steve Kille, Colin Robbins, Wengyik Yeong, ∼1993 (académie et industrie)
- À l'origine, une alternative (ou une interface) aux services d'annuaire X.500
  - X.500 est bâti sur ISO/OSI ;
  - LDAP sur la pile Internet, plus simple et performante.
- Lightweight : moins de trafique réseaux, efficace.
- Directory Access : spécialisé pour les annuaires.
  - à l'origine nommé « LDBP », *Lightweight Directory Browsing Protocol* : priorité aux performances en lecture et recherche ;
  - aujourd'hui l'écriture est aussi supportée, mais moins critique.
- Protocol : un protocole, niveau application (TCP ou UDP, port 389— ou 636 chiffré en SSL)
- Version actuelle LDAPv3 ∼1996, maintenant géré par l'IETF, un standard mature. Plein d'implémentations indépendantes.

LDAP : Introduction et histoire

Lightweight Directory Access Protocol

- Tim Howes, Steve Kille, Colin Robbins, Wengyik Yeong, ∼1993 (académie et industrie)
- À l'origine, une alternative (ou une interface) aux services d'annuaire X.500
  - X.500 est bâti sur ISO/OSI ;
  - LDAP sur la pile Internet, plus simple et performante.
- Lightweight : moins de trafique réseaux, efficace.
- Directory Access : spécialisé pour les annuaires.
  - à l'origine nommé « LDBP », *Lightweight Directory Browsing Protocol* : priorité aux performances en lecture et recherche ;
  - aujourd'hui l'écriture est aussi supportée, mais moins critique.
- Protocol : un protocole, niveau application (TCP ou UDP, port 389— ou 636 chiffré en SSL)
- Version actuelle LDAPv3 ∼1996, maintenant géré par l'IETF, un standard mature. Plein d'implémentations indépendantes.

LDAP : Introduction et histoire

Lightweight Directory Access Protocol

- Tim Howes, Steve Kille, Colin Robbins, Wengyik Yeong, ∼1993 (académie et industrie)
- À l'origine, une alternative (ou une interface) aux services d'annuaire X.500
  - X.500 est bâti sur ISO/OSI ;
  - LDAP sur la pile Internet, plus simple et performante.
- Lightweight : moins de trafique réseaux, efficace.
- Directory Access : spécialisé pour les annuaires.
  - à l'origine nommé « LDBP », *Lightweight Directory Browsing Protocol* : priorité aux performances en lecture et recherche ;
  - aujourd'hui l'écriture est aussi supportée, mais moins critique.
- Protocol : un protocole, niveau application (TCP ou UDP, port 389— ou 636 chiffré en SSL)
- Version actuelle LDAPv3 ∼1996, maintenant géré par l'IETF, un standard mature. Plein d'implémentations indépendantes.

LDAP : Introduction et histoire

Lightweight Directory Access Protocol

- Tim Howes, Steve Kille, Colin Robbins, Wengyik Yeong, ∼1993 (académie et industrie)
- À l'origine, une alternative (ou une interface) aux services d'annuaire X.500
  - X.500 est bâti sur ISO/OSI ;
  - LDAP sur la pile Internet, plus simple et performante.
- Lightweight : moins de trafique réseaux, efficace.
- Directory Access : spécialisé pour les annuaires.
  - à l'origine nommé « LDBP », *Lightweight Directory Browsing Protocol* : priorité aux performances en lecture et recherche ;
  - aujourd'hui l'écriture est aussi supportée, mais moins critique.
- Protocol : un protocole, niveau application (TCP ou UDP, port 389— ou 636 chiffré en SSL)
- Version actuelle LDAPv3 ∼1996, maintenant géré par l'IETF, un standard mature. Plein d'implémentations indépendantes.

LDAP : Introduction et histoire

Lightweight Directory Access Protocol

- Tim Howes, Steve Kille, Colin Robbins, Wengyik Yeong, ∼1993 (académie et industrie)
- À l'origine, une alternative (ou une interface) aux services d'annuaire X.500
  - X.500 est bâti sur ISO/OSI ;
  - LDAP sur la pile Internet, plus simple et performante.
- Lightweight : moins de trafique réseaux, efficace.
- Directory Access : spécialisé pour les annuaires.
  - à l'origine nommé « LDBP », *Lightweight Directory Browsing Protocol* : priorité aux performances en lecture et recherche ;
  - aujourd'hui l'écriture est aussi supportée, mais moins critique.
- Protocol : un protocole, niveau application (TCP ou UDP, port 389— ou 636 chiffré en SSL)
- Version actuelle LDAPv3 ∼1996, maintenant géré par l'IETF, un standard mature. Plein d'implémentations indépendantes.

LDAP : Introduction et histoire

Lightweight Directory Access Protocol

- Tim Howes, Steve Kille, Colin Robbins, Wengyik Yeong, ∼1993 (académie et industrie)
- À l'origine, une alternative (ou une interface) aux services d'annuaire X.500
  - X.500 est bâti sur ISO/OSI ;
  - LDAP sur la pile Internet, plus simple et performante.
- Lightweight : moins de trafique réseaux, efficace.
- Directory Access : spécialisé pour les annuaires.
  - à l'origine nommé « LDBP », *Lightweight Directory Browsing Protocol* : priorité aux performances en lecture et recherche ;
  - aujourd'hui l'écriture est aussi supportée, mais moins critique.
- Protocol : un protocole, niveau application (TCP ou UDP, port 389— ou 636 chiffré en SSL)
- Version actuelle LDAPv3 ∼1996, maintenant géré par l'IETF, un standard mature. Plein d'implémentations indépendantes.

LDAP : Protocole

- Protocole binaire : Basic Encoding Rules (BER), définies dans les RFCs, toujours utilisées dans les deux directions.
- Le client se connecte au serveur, et envoie des requêtes («opérations») ;
  - (Pas nécessaire d'attendre des réponses !)
- Le serveur envoie des réponses, en général sans contraintes d'ordre, ou envoie des unsolicited notifications ;

LDAP : Protocole

- Protocole binaire : Basic Encoding Rules (BER), définies dans les RFCs, toujours utilisées dans les deux directions.
- Le client se connecte au serveur, et envoie des requêtes («opérations») ;
  - (Pas nécessaire d'attendre des réponses !)
- Le serveur envoie des réponses, en général sans contraintes d'ordre, ou envoie des unsolicited notifications ;

LDAP : Protocole

- Protocole binaire : Basic Encoding Rules (BER), définies dans les RFCs, toujours utilisées dans les deux directions.
- Le client se connecte au serveur, et envoie des requêtes («opérations») ;
  - (Pas nécessaire d'attendre des réponses !)
- Le serveur envoie des réponses, en général sans contraintes d'ordre, ou envoie des unsolicited notifications ;

LDAP : Protocole

- Protocole binaire : Basic Encoding Rules (BER), définies dans les RFCs, toujours utilisées dans les deux directions.
- Le client se connecte au serveur, et envoie des requêtes («opérations») ;
  - (Pas nécessaire d'attendre des réponses !)
- Le serveur envoie des réponses, en général sans contraintes d'ordre, ou envoie des unsolicited notifications ;

LDAP : Opérations

Opérations (envoyées par le client au serveur) :

- StartTLS (commence une communication chiffrée) ;
- Bind (authentification : *parfois non indispensable*) ;
- Search ;
- Compare ;
- Add ;
- Delete ;
- Modify ;
- Modify Distinguished Name (déplacement ou renommage) ;
- Abandon (renonce à une requête précédente) ;
- Extended Operation ;
- Unbind (contre-intuitif : pas le contraire de Bind).

LDAP : Opérations : comportement

- Opérations individuellement atomiques, mais transactions (à la SQL) non supportées.
- Ordre des opérations exécutées sur le serveur indéfini, par défaut.
- Une réponse possible est un « referral » : une rédirection vers un autre serveur. Certains serveurs peuvent faire ils-mêmes du chaining (similaire aux appels DNS récursifs).

LDAP : Opérations : comportement

- Opérations individuellement atomiques, mais transactions (à la SQL) non supportées.
- Ordre des opérations exécutées sur le serveur indéfini, par défaut.
- Une réponse possible est un « referral » : une rédirection vers un autre serveur. Certains serveurs peuvent faire ils-mêmes du chaining (similaire aux appels DNS récursifs).

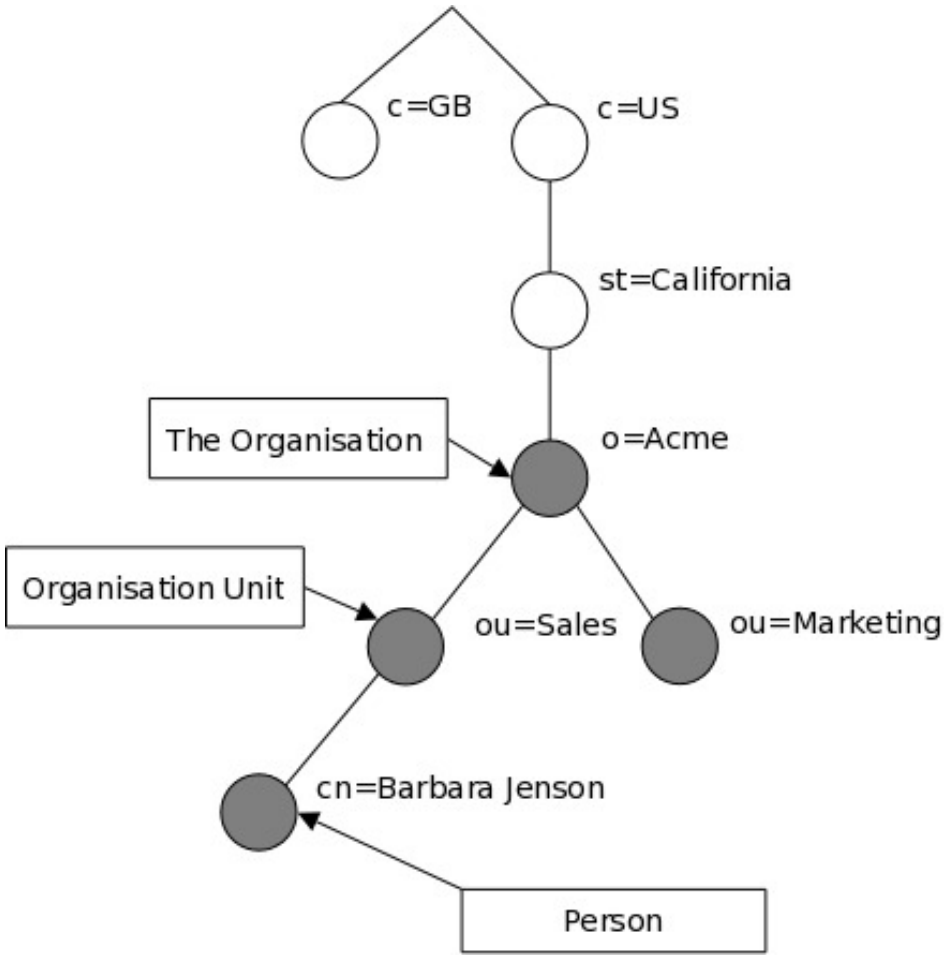
LDAP : Opérations : comportement

- Opérations individuellement atomiques, mais transactions (à la SQL) non supportées.
- Ordre des opérations exécutées sur le serveur indéfini, par défaut.
- Une réponse possible est un « referral » : une rédirection vers un autre serveur. Certains serveurs peuvent faire ils-mêmes du chaining (similaire aux appels DNS récursifs).

Structure d'un annuaire

- Une entrée est faite par un ensemble d'attributs.
- Un attribut a un nom et une ou *plusieurs* valeurs.
- Les attributs sont définis dans un schema.
- Toute entrée a un indentifiant unique : le Distinguished Name (DN), construit hiérarchiquement à partir de son Relative Distinguished Name (RDN : un ensemble d'attributs) suivi par le DN de l'*entrée parente*, si elle existe — on construit le nom à partir des feuilles vers la racine.
  Important : « RDN » **n'est pas** un nom d'attribut ! Il est déduit à partir du DN.
- Une entrée peux avoir un nombre arbitraire de fils, mais un seul parent (sauf la racine, qui n'a aucun parent). Le DN de la racine est le suffixe.

Structure d'un annuaire : figure



« Argot » de LDAP

- Directory Information Tree (DIT) : l'arborescence entière, représentée comme un *arbre inverti*.
- suffixe : La racine du DIT
- Branches (organisées de plusieurs façons possibles : par *ressources*, *rôles*, *pays*, *départements*, ... Des choix importants *à temps de conception*—Difficiles à changer après.
- Bind Name (nom d'utilisateur authentifié)

Noms d'attributs utiles :

- `dn` : Distinguished Name
- `dc` : Domain Component
- `objectclass` : le nom d'un ensemble d'attributs, définis dans un schema.
- ...(plein de noms définis dans des schemas standard !)
  - Par exemple `cn` pour « common name », `sn` pour « surname », `o` pour « organization », `ou` pour « organizational unit ». Mais vous pouvez aussi définir vos noms d'attributs non standard.

« Argot » de LDAP

- Directory Information Tree (DIT) : l'arborescence entière, représentée comme un *arbre inverti*.
- suffixe : La racine du DIT
- Branches (organisées de plusieurs façons possibles : par *ressources*, *rôles*, *pays*, *départements*, ... Des choix importants *à temps de conception*—Difficiles à changer après.
- Bind Name (nom d'utilisateur authentifié)

Noms d'attributs utiles :

- `dn` : Distinguished Name
- `dc` : Domain Component
- `objectclass` : le nom d'un ensemble d'attributs, définis dans un schema.
- ...(plein de noms définis dans des schemas standard !)
  - Par exemple `cn` pour « common name », `sn` pour « surname », `o` pour « organization », `ou` pour « organizational unit ». Mais vous pouvez aussi définir vos noms d'attributs non standard.

Le format LDIF

- LDAP Data Interchange Format : un format textuel, défini précisement dans le standard, qui convient aux humaines.
- Utilisé dans les applications, en entrée et sortie, pour representer les entrées.
- Souvent dans des fichiers, mais pas nécessairement
  - Heureusement nous utilisons Unix et en particulier GNU/Linux, et donc nous avons les pipes, les sockets, et des shells puissants comme Bash.

On commence toujours en donnant un `dn`, puis une (ou plusieurs) `objectclass` ; en suite les autres attributs, qui doivent être compatibles avec la classe ou les classes qu'on a spécifié.

Le format LDIF : exemple

```
# Un commentaire.
dn: dc=ageinghacker,dc=net
objectclass: dcObject
objectclass: Organization
o: "Mon entreprise"
dc: ageinghacker
```

Autres ressources I

Sur la page web du cours (suivez le lien « Teaching » dans la page principale de mon site web).
La page, préliminaire et écrite très rapidement, est encore crue, mas contient des informations utiles.
Je vais ajouter de l'autre matériel à la page.

La suite : OpenLDAP

Nous allons jouer avec OpenLDAP, une implémentation libre (et techniquement sophistiquée) de LDAPv3.

- Aujourd'hui je vais faire une démonstration sur mon portable.
  - Je vais utiliser LDAP comme utilisateur ordinaire, non `root`, pour simuler votre environnement au labo et avec les ordinateurs libre service.
- La prochaine fois, vous allez faire les mêmes chose au labo. **Le TP sera noté.**

La suite : OpenLDAP

Nous allons jouer avec OpenLDAP, une implémentation libre (et techniquement sophistiquée) de LDAPv3.

- Aujourd'hui je vais faire une démonstration sur mon portable.
  - Je vais utiliser LDAP comme utilisateur ordinaire, non `root`, pour simuler votre environnement au labo et avec les ordinateurs libre service.
- La prochaine fois, vous allez faire les mêmes chose au labo. **Le TP sera noté.**

La suite : OpenLDAP

Nous allons jouer avec OpenLDAP, une implémentation libre (et techniquement sophistiquée) de LDAPv3.

- Aujourd'hui je vais faire une démonstration sur mon portable.
  - Je vais utiliser LDAP comme utilisateur ordinaire, non `root`, pour simuler votre environnement au labo et avec les ordinateurs libre service.
- La prochaine fois, vous allez faire les mêmes chose au labo. **Le TP sera noté.**

La suite : OpenLDAP

Nous allons jouer avec OpenLDAP, une implémentation libre (et techniquement sophistiquée) de LDAPv3.

- Aujourd'hui je vais faire une démonstration sur mon portable.
  - Je vais utiliser LDAP comme utilisateur ordinaire, non `root`, pour simuler votre environnement au labo et avec les ordinateurs libre service.
- La prochaine fois, vous allez faire les mêmes chose au labo. **Le TP sera noté.**

La suite : OpenLDAP

OpenLDAP contient un serveur `slapd`, extensible avec des modules, et plusieurs clients à ligne de commande—plus ou moins un par opération : `ldapsearch`, `ldapadd`, `ldapcompare`, `ldapdelete`, …

Demo

[Demo]

Bibliography I


Crocker (Ed.), D. and Overell, P. (2005). Augmented BNF for Syntax Specifications : ABNF. RFC 4234 (Draft Standard). Obsoleted by RFC 5234. (Une expliquation de la meta-syntaxe utilisée dans les autres RFCs. C'est officiellement remplacé par un autre RFC, mais il s'agit du document directement cité par les RFCs décrivant LDAP ; et c'est lisible).


Harrison (Ed.), R. (2006). Lightweight Directory Access Protocol (LDAP) : Authentication Methods and Security Mechanisms. RFC 4513 (Proposed Standard).


Legg (Ed.), S. (2006). Lightweight Directory Access Protocol (LDAP) : Syntaxes and Matching Rules. RFC 4517 (Proposed Standard).

Bibliography II

- Saiu, L. (2018). La page web de mes cours. http://ageinghacker.net/teaching
  La page web officielle du cours contient des pointeurs à des ressources web, et une copie des mes transparents.
- Sciberras (Ed.), A. (2006). Lightweight Directory Access Protocol (LDAP) : Schema for User Applications. RFC 4519 (Proposed Standard).
- Sermersheim (Ed.), J. (2006). Lightweight Directory Access Protocol (LDAP) : The Protocol. RFC 4511 (Proposed Standard).
- Smith (Ed.), M. and Howes, T. (2006a). Lightweight Directory Access Protocol (LDAP) : String Representation of Search Filters. RFC 4515 (Proposed Standard).

Bibliography III

- Smith (Ed.), M. and Howes, T. (2006b). Lightweight Directory Access Protocol (LDAP) : Uniform Resource Locator. RFC 4516 (Proposed Standard).
- Zeilenga, K. (2006). Lightweight Directory Access Protocol (LDAP) : Internationalized String Preparation. RFC 4518 (Proposed Standard).
- Zeilenga (Ed.), K. (2006a). Lightweight Directory Access Protocol (LDAP) : Directory Information Models. RFC 4512 (Proposed Standard).
- Zeilenga (Ed.), K. (2006b). Lightweight Directory Access Protocol (LDAP) : String Representation of Distinguished Names. RFC 4514 (Proposed Standard).

Bibliography IV


Zeilenga (Ed.), K. (2006c). Lightweight Directory Access Protocol (LDAP) : Technical Specification Road Map. RFC 4510 (Proposed Standard).

Image credits and licenses

- Les deux arbres :
  `http://www.openldap.org/doc/admin24/`
  Copyright © 1998-2012, The OpenLDAP Foundation,
  Copyright © 1992-1996, Regents of the University of Michigan, Released under the OpenLDAP Public License as per the document's preface.
- Image tables, modèle relationnel :
  `https://commons.wikimedia.org/wiki/File:Relational_Model.svg`
  Public domain, prepared by an officer or employee of the US government.