LDAP : Préambule

Une bonne et une mauvaise nouvelle

La mauvaise nouvelle

- Je ne suis pas un spécialiste ldap
- xxx m'a dit qu'il serait bien d'animer une discussion sur ldap (sujet réclamé)

La bonne nouvelle

- Présence de spécialistes dans la salle

Donc

→ C'est le moment de poser des questions !

→ Merci de corriger toutes les erreurs présentes

LDAP

De nombreuses présentations ont déjà été faites dans la cadre de mathrice

Mettre en avant les interrogations (Retour du sondage envoyé par mail)

Le sésame : Authentification centralisée (diminuer le nombre de mots de passe / le nombre de système d'authentification.)

Ldap : Le bla bla

Protocole d'accès à des données en mode connecté

Permet d'avoir un référentiel unique en ”ldapifiant” les applications clientes.

DN : Chemin absolu

RDN : Chemin relatif, sorte d'index d'un ou plusieurs éléments

ACL : Incluses dans slapd.conf pour Openldap

Ldap : ...

Mode connecté

- Authentification anonyme, simple (mot de passe en clair), sur SSL/TLS ou SASL

Possibilité de distribuer son arbre via des referals.

→ Fait penser au DNS... (ex : u-picardie.fr : nserver: gip.u-picardie.fr [193.49.184.17]...)

Ldap : Les RFCs

RFC 2251-2256 : ”Authentification Methode for LDAP”

RFC 2830 : ”LDAP : Extension for TLD”

RFC 3377 : ”LDAP : Technical specifications”

...

LDAP vs Base de données

Ldap n'est qu'un protocole

Il est optimisé pour la consultation

Aucun verrou pour l'integrité des données

→ Y-a-t'il d'autres arguments pour différencier LDAP d'une base de données ?

LDAP : Le schéma ?

Comment bien définir l'arbre de son annuaire ?

- Quel schéma pour un labo ?
- Intérêt d'un schéma large vs profond ?
- Comment valider le schéma choisi ? (outils, process.)
- Avoir un schéma sans RDN multivalué semble crucial, non ?
- Comment faire quelque chose de compatible avec les annuaires univ, cnrs ou mathrice ?

Ldap : le fichier ldif

LDIF : LDAP Interchange Format

- Fichier résultat d'un ”cat” d'un ldap
- Simple fichier édité pour injection de données
- Ldapmodify utilise des fichiers à syntaxe proche

Ldap : Quel serveur ?

Openldap → Y-a-t'il plus léger ? (cf personnes ayant quelques expériences avec autre chose ?)

Apache Directory Server | Open Directory d'Apple | Critical Path Directory Server | Meta Directory Server | 389 Directory Server | Red Hat Directory Server | OpenLDAP | Novell eDirectory | Sun Directory Server Enterprise Edition | OpenDS a Sun Open | Source Directory Server | IBM SecureWay Directory | IBM Tivoli Directory Server | IBM Lotus Domino | Active Directory de Microsoft | Siemens DirX | View500 | Oracle Internet Directory | tinyldap | Mandriva Directory Server

Ldap : Où mettre le serveur ?

Le serveur est un point central

Où le placer ?

- En DMZ ?
- En Interne ....

Ldap : Openldap

Le serveur slapd ← slapd.conf : Contient le schéma utilisé et les ACL

Le module de réplication : slurpd maintenant remplacé par syncrepl

Les outils d'intéraction : ldapadd, ldapmodify, ldapdelete

OpenLdap : Les ACL

* : Correspond à tout utilisateur

self : L'actuel utilisateur

anonymous : Connexion non authentifiée

users : Connexion authentifiée

Expression régulière

OpenLdap : Les ACL

Niveau d'accès

- Write
- Read
- Search
- Compare
- Auth
- none

ACL en ”allow, deny”

→ ACL les plus restrictives à mettre avant dans slapd.conf

Openldap : Saisie d'entrée

Via fichier ldif

Via ligne de commande

Via éditeur graphique

Via phpLDAPadmin

...

Ldap : En pratique

Mise en pratique longue ou pas ?
  Que faut-il au minimum ?

Quelques exemples de manipulation courrante
  (ldapadd...modify..) ?

Extraction vers l'annuaire des maths ?

Les interrogations

Angoisse du ”château de carte”

→ Dans la conception du schéma, des ACLs

→ Dans la centralisation : Quelle stratégie de réplication ?

A partir de combien de services ”ldapifiés” l'investissement ldap est ”rentable” ?

Ldap avec windows et linux

Quel frontend d'authentification ? (Directement ldap ou samba ?)

LDAP peut-il être contrôleur principal de domaine (en utilisant le service d'annuaire de samba)

ou

Est-il plus judicieux qu'ldap gère le DNS et donc les noms de machine/ip comme bind 9 l'annuaire 389 DS ?

Quid de Kerberos ?

LDAP : Tous les oublis

Ldap : quelques liens

http://www.alvestrand.no/objectid → Tous les oid normalisés

http://www.dsml.org -> un ldif xmlisé pour la description d'un ldap

Kit de développement :

- www.microsoft.com/adsi
- java.sun.com/products/jndi

Le slideshow du TP de Poitiers

The end

Merci.