La base LDAP

Nicolas Dandrimont

Cr@ns

10 novembre 2009

Stockage de données ?

- Fichiers plats : gérable pour un serveur, pas pour 20
- Base de données classique (SGBDR) : Pratique pour le stockage de données, mais peu d'interfaçage avec les applications
- LDAP : le choix le plus simple : en UNIX, bien intégré, etc.

Stockage de données ?

- Fichiers plats : gérable pour un serveur, pas pour 20
- Base de données classique (SGBDR) : Pratique pour le stockage de données, mais peu d'interfaçage avec les applications
- LDAP : le choix le plus simple : en UNIX, bien intégré, etc.

Stockage de données ?

- Fichiers plats : gérable pour un serveur, pas pour 20
- Base de données classique (SGBDR) : Pratique pour le stockage de données, mais peu d'interfaçage avec les applications
- LDAP : le choix le plus simple : en UNIX, bien intégré, etc.

LDAP ?

- L : Lightweight
- D : Directory
- A : Access
- P : Protocol

LDAP ?

- L : Lightweight
- D : Directory
- A : Access
- P : Protocol

LDAP ?

- L : Lightweight
- D : Directory
- A : Access
- P : Protocol

LDAP ?

- L : Lightweight
- D : Directory
- A : Access
- P : Protocol

LDAP ?

- L : Lightweight
- D : Directory
- A : Access
- P : Protocol

Organisation de l'annuaire

Fortement hiérarchique, comme on le voit ici :

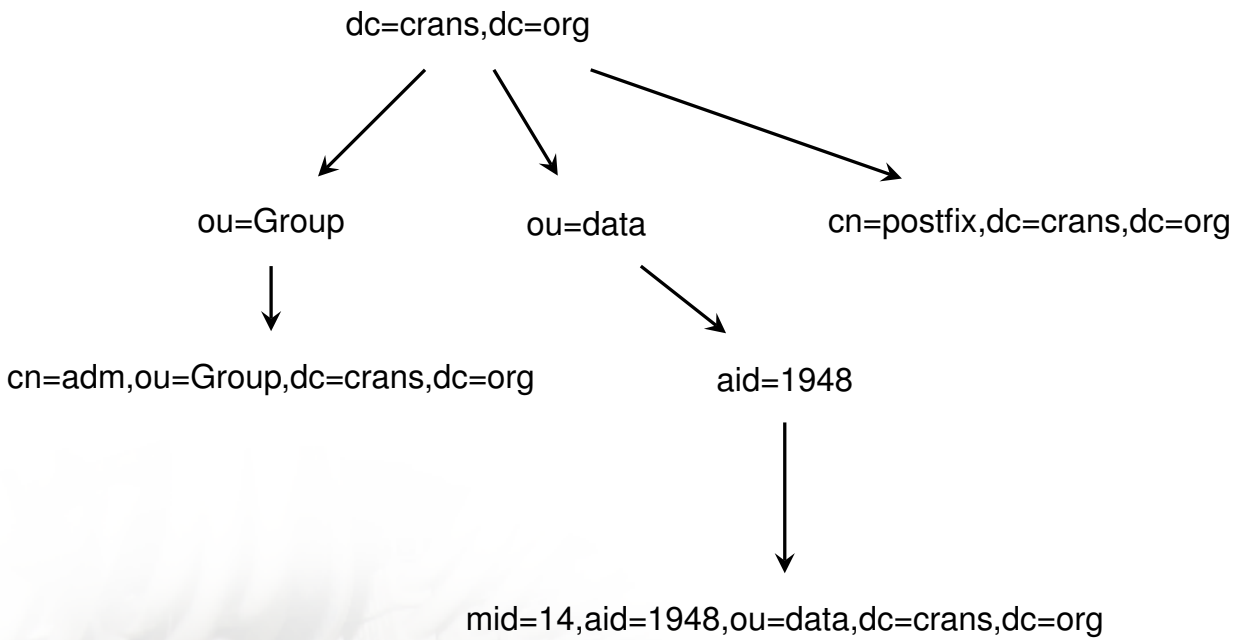

Schéma de la base

- Chaque objet a une ou plusieurs `objectClass`es
- Schéma : définition des attributs (champs) de chaque `objectClass`

```
objectclass ( 1.3.6.1.4.1.25368.3.2 NAME 'adherent' SUP proprio
   DESC 'Adhérent'
   MUST ( aid $ prenom $ tel $ mail )
   MAY ( carteEtudiant $ etudes $ postalAddress $ mailInvalide $ charteMA $
         adherentPayant ) )
```

Schéma de la base

- Chaque objet a une ou plusieurs `objectClass`es
- Schéma : définition des attributs (champs) de chaque `objectClass`

```
objectclass ( 1.3.6.1.4.1.25368.3.2 NAME 'adherent' SUP proprio
   DESC 'Adhérent'
   MUST ( aid $ prenom $ tel $ mail )
   MAY ( carteEtudiant $ etudes $ postalAddress $ mailInvalide $ charteMA $
         adherentPayant ) )
```

Schéma de la base

- Chaque objet a une ou plusieurs `objectClass`es
- Schéma : définition des attributs (champs) de chaque `objectClass`

```
objectclass ( 1.3.6.1.4.1.25368.3.2 NAME 'adherent' SUP proprio
   DESC 'Adhérent'
   MUST ( aid $ prenom $ tel $ mail )
   MAY ( carteEtudiant $ etudes $ postalAddress $ mailInvalide $ charteMA $
         adherentPayant ) )
```

Définition des attributs

- Chaque attribut a un nom, un type

```
attributetype ( 1.3.6.1.4.1.25368.2.10 NAME 'chbre'
    DESC 'Chambre adhérent'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{16} SINGLE-VALUE )
```

Définition des attributs

- Chaque attribut a un nom, un type

```
attributetype ( 1.3.6.1.4.1.25368.2.10 NAME 'chbre'
    DESC 'Chambre adhérent'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.44{16} SINGLE-VALUE )
```

Sécurité des données

- Réplication des changements automatique sur quelques réplicas (`sable`, `radius`, `ovh`, `vo` (base de tests, un peu morte...))
- Transit des données uniquement sur le vlan adm, ou à travers un tunnel SSL (pour `ragnarok`)
- Accès à seulement certains attributs...

Sécurité des données

- Réplication des changements automatique sur quelques réplicas (`sable`, `radius`, `ovh`, `vo` (base de tests, un peu morte...))
- Transit des données uniquement sur le vlan adm, ou à travers un tunnel SSL (pour `ragnarok`)
- Accès à seulement certains attributs...

Sécurité des données

- Réplication des changements automatique sur quelques réplicas (`sable`, `radius`, `ovh`, `vo` (base de tests, un peu morte...))
- Transit des données uniquement sur le vlan adm, ou à travers un tunnel SSL (pour `ragnarok`)
- Accès à seulement certains attributs...

Listes d'accès

- Accès à la base en lecture seule : attributs « publics » - connexion sous le dn `cn=readonly,dc=crans,dc=org`
- Accès tous ses propres attributs en lecture
- Accès à tous les attributs en lecture pour la réplication `cn=replica,dc=crans,dc=org`
- Accès en lecture/écriture à certains attributs pour certaines applications spécifiques... On en reparle plus tard :)

Listes d'accès

- Accès à la base en lecture seule : attributs « publics » - connexion sous le dn `cn=readonly,dc=crans,dc=org`
- Accès tous ses propres attributs en lecture
- Accès à tous les attributs en lecture pour la réplication `cn=replica,dc=crans,dc=org`
- Accès en lecture/écriture à certains attributs pour certaines applications spécifiques... On en reparle plus tard :)

Listes d'accès

- Accès à la base en lecture seule : attributs « publics » - connexion sous le dn `cn=readonly,dc=crans,dc=org`
- Accès tous ses propres attributs en lecture
- Accès à tous les attributs en lecture pour la réplication `cn=replica,dc=crans,dc=org`
- Accès en lecture/écriture à certains attributs pour certaines applications spécifiques... On en reparle plus tard :)

Listes d'accès

- Accès à la base en lecture seule : attributs « publics » - connexion sous le dn `cn=readonly,dc=crans,dc=org`
- Accès tous ses propres attributs en lecture
- Accès à tous les attributs en lecture pour la réplication `cn=replica,dc=crans,dc=org`
- Accès en lecture/écriture à certains attributs pour certaines applications spécifiques... On en reparle plus tard :)

whos prend deux heures ! C'est nul LDAP !

- Les objets de la base sont stockés dans des fichiers `BDB`
- La recherche dans ces fichiers est lente...
- ...mais on peut les indexer...
- ...ce qui *peut* ralentir le serveur lors des écritures
- Les attributs de recherche principaux sont indexés pour les recherches typiques

whos prend deux heures ! C'est nul LDAP !

- Les objets de la base sont stockés dans des fichiers `BDB`
- La recherche dans ces fichiers est lente...
- ...mais on peut les indexer...
- ...ce qui *peut* ralentir le serveur lors des écritures
- Les attributs de recherche principaux sont indexés pour les recherches typiques

whos prend deux heures ! C'est nul LDAP !

- Les objets de la base sont stockés dans des fichiers `BDB`
- La recherche dans ces fichiers est lente...
- ...mais on peut les indexer...
- ...ce qui *peut* ralentir le serveur lors des écritures
- Les attributs de recherche principaux sont indexés pour les recherches typiques

whos prend deux heures ! C'est nul LDAP !

- Les objets de la base sont stockés dans des fichiers `BDB`
- La recherche dans ces fichiers est lente...
- ...mais on peut les indexer...
- ...ce qui *peut* ralentir le serveur lors des écritures
- Les attributs de recherche principaux sont indexés pour les recherches typiques

whos prend deux heures ! C'est nul LDAP !

- Les objets de la base sont stockés dans des fichiers `BDB`
- La recherche dans ces fichiers est lente...
- ...mais on peut les indexer...
- ...ce qui *peut* ralentir le serveur lors des écritures
- Les attributs de recherche principaux sont indexés pour les recherches typiques

NIS, c'est quoi ?

- Sous UNIX, base de données d'informations système (Network Information Service)
- a.k.a. `yp` (yellow-pages) : `passwd`, `shadow`, `hosts`, ...
- Permet une recherche sur une base de données directement à partir de la libc

NIS, c'est quoi ?

- Sous UNIX, base de données d'informations système (Network Information Service)
- a.k.a. `yp` (yellow-pages) : `passwd`, `shadow`, `hosts`, ...
- Permet une recherche sur une base de données directement à partir de la libc

NIS, c'est quoi ?

- Sous UNIX, base de données d'informations système (Network Information Service)
- a.k.a.`yp` (yellow-pages) : `passwd`, `shadow`, `hosts`, ...
- Permet une recherche sur une base de données directement à partir de la libc

et PAM alors ?

- Sous Linux (un port pour *BSD existe), modules d'authentification « branchables » (Pluggable Authentication Modules)
- Permet d'identifier -quelque chose- (le plus souvent un utilisateur) à l'aide d'un mot de passe, d'une empreinte digitale, ...

et PAM alors ?

- Sous Linux (un port pour *BSD existe), modules d'authentification « branchables » (Pluggable Authentication Modules)
- Permet d'identifier -quelque chose- (le plus souvent un utilisateur) à l'aide d'un mot de passe, d'une empreinte digitale, ...

LDAP dans tout ça ?

- `libnss-ldap(d)` : mapper les recherches dans NIS à des recherches dans la base LDAP, sous Linux (à l'aide de NSS, système de modules pour NIS).
- `pam-ldap` : mapper les requêtes d'authentification PAM avec une authentification LDAP.
- Sous OpenBSD, utilisation de `login-ldap` pour l'authentification.
- Accès en `cn=readonly,dc=crans,dc=org`.

LDAP dans tout ça ?

- `libnss-ldap(d)` : mapper les recherches dans NIS à des recherches dans la base LDAP, sous Linux (à l'aide de NSS, système de modules pour NIS).
- `pam-ldap` : mapper les requêtes d'authentification PAM avec une authentification LDAP.
- Sous OpenBSD, utilisation de `login-ldap` pour l'authentification.
- Accès en `cn=readonly,dc=crans,dc=org`.

LDAP dans tout ça ?

- `libnss-ldap(d)` : mapper les recherches dans NIS à des recherches dans la base LDAP, sous Linux (à l'aide de NSS, système de modules pour NIS).
- `pam-ldap` : mapper les requêtes d'authentification PAM avec une authentification LDAP.
- Sous OpenBSD, utilisation de `login-ldap` pour l'authentification.
- Accès en `cn=readonly,dc=crans,dc=org`.

LDAP dans tout ça ?

- `libnss-ldap(d)` : mapper les recherches dans NIS à des recherches dans la base LDAP, sous Linux (à l'aide de NSS, système de modules pour NIS).
- `pam-ldap` : mapper les requêtes d'authentification PAM avec une authentification LDAP.
- Sous OpenBSD, utilisation de `login-ldap` pour l'authentification.
- Accès en `cn=readonly,dc=crans,dc=org`.

Postfix et LDAP

- Postfix va faire certaines requêtes directement dans la base LDAP
- Existence d'un utilisateur
- Conversion des alias
- Contournement de greylist
- Réécriture des entêtes
- Accès en `cn=postfix,dc=crans,dc=org`

Postfix et LDAP

- Postfix va faire certaines requêtes directement dans la base LDAP
- Existence d'un utilisateur
- Conversion des alias
- Contournement de greylist
- Réécriture des entêtes
- Accès en `cn=postfix,dc=crans,dc=org`

Postfix et LDAP

- Postfix va faire certaines requêtes directement dans la base LDAP
- Existence d'un utilisateur
- Conversion des alias
- Contournement de greylist
- Réécriture des entêtes
- Accès en `cn=postfix,dc=crans,dc=org`

Postfix et LDAP

- Postfix va faire certaines requêtes directement dans la base LDAP
- Existence d'un utilisateur
- Conversion des alias
- Contournement de greylist
- Réécriture des entêtes
- Accès en `cn=postfix,dc=crans,dc=org`

Postfix et LDAP

- Postfix va faire certaines requêtes directement dans la base LDAP
- Existence d'un utilisateur
- Conversion des alias
- Contournement de greylist
- Réécriture des entêtes
- Accès en `cn=postfix,dc=crans,dc=org`

Postfix et LDAP

- Postfix va faire certaines requêtes directement dans la base LDAP
- Existence d'un utilisateur
- Conversion des alias
- Contournement de greylist
- Réécriture des entêtes
- Accès en `cn=postfix,dc=crans,dc=org`

Dovecot et LDAP

- Le serveur POP/IMAP fait ses requêtes directement à la base LDAP
- Existence/Authentification d'un utilisateur
- ...
- Accès en `cn=dovecot,dc=crans,dc=org`

Dovecot et LDAP

- Le serveur POP/IMAP fait ses requêtes directement à la base LDAP
- Existence/Authentification d'un utilisateur
- ...
- Accès en `cn=dovecot,dc=crans,dc=org`

Dovecot et LDAP

- Le serveur POP/IMAP fait ses requêtes directement à la base LDAP
- Existence/Authentification d'un utilisateur
- ...
- Accès en `cn=dovecot,dc=crans,dc=org`

Dovecot et LDAP

- Le serveur POP/IMAP fait ses requêtes directement à la base LDAP
- Existence/Authentification d'un utilisateur
- ...
- Accès en `cn=dovecot,dc=crans,dc=org`

Accéder à la base simplement

- Il est pratique d'accéder aux informations de la base simplement
- Le protocole LDAP est limité (pas de jointures, ...)
- Les données doivent (devraient mieux) être vérifiées avant d'être insérées dans la base

Accéder à la base simplement

- Il est pratique d'accéder aux informations de la base simplement
- Le protocole LDAP est limité (pas de jointures, ...)
- Les données doivent (devraient mieux) être vérifiées avant d'être insérées dans la base

Accéder à la base simplement

- Il est pratique d'accéder aux informations de la base simplement
- Le protocole LDAP est limité (pas de jointures, ...)
- Les données doivent (devraient mieux) être vérifiées avant d'être insérées dans la base

Un accès haut-niveau

- Utilisation de Python (« pseudo-code qui s'exécute »), puissant et facile d'accès
- Abstraction totale du protocole LDAP à travers le modèle objet Python
- Recherches simplifiées dans la base, jointures, ...
- Vérification des données avant l'insertion dans la base de données

Un accès haut-niveau

- Utilisation de Python (« pseudo-code qui s'exécute »), puissant et facile d'accès
- Abstraction totale du protocole LDAP à travers le modèle objet Python
- Recherches simplifiées dans la base, jointures, ...
- Vérification des données avant l'insertion dans la base de données

Un accès haut-niveau

- Utilisation de Python (« pseudo-code qui s'exécute »), puissant et facile d'accès
- Abstraction totale du protocole LDAP à travers le modèle objet Python
- Recherches simplifiées dans la base, jointures, ...
- Vérification des données avant l'insertion dans la base de données

Un accès haut-niveau

- Utilisation de Python (« pseudo-code qui s'exécute »), puissant et facile d'accès
- Abstraction totale du protocole LDAP à travers le modèle objet Python
- Recherches simplifiées dans la base, jointures, ...
- Vérification des données avant l'insertion dans la base de données

Rassurez-vous...

Je ne vais pas vous lire le code de gest_crans.py !

Utilisation de IPython

- Sur `zamok`
- En utilisant `ldap_crans` (la base de test n'est pas accessible, attention à ne pas faire du caca)
- ... demo !

Utilisation de IPython

- Sur `zamok`
- En utilisant `ldap_crans` (la base de test n'est pas accessible, attention à ne pas faire du caca)
- ... demo !

Utilisation de IPython

- Sur `zamok`
- En utilisant `ldap_crans` (la base de test n'est pas accessible, attention à ne pas faire du caca)
- ... demo !

Des pages web...

- Tout d'abord le tutorial de Python... Part de très bas et vient toucher du doigt la programmation orientée objet. Très bonne lecture pour débuter
- `http ://www.python.org/doc/2.5.2/tut/tut.html`
- La documentation de `http ://www.python.org/` est très fournie.
- ...et est générée à partir de la documentation intégrée au code source, accessible via `help(objet)`

Des pages web...

- Tout d'abord le tutorial de Python... Part de très bas et vient toucher du doigt la programmation orientée objet. Très bonne lecture pour débuter
- `http ://www.python.org/doc/2.5.2/tut/tut.html`
- La documentation de `http ://www.python.org/` est très fournie.
- ...et est générée à partir de la documentation intégrée au code source, accessible via `help(objet)`

Des pages web...

- Tout d'abord le tutorial de Python... Part de très bas et vient toucher du doigt la programmation orientée objet. Très bonne lecture pour débuter
- `http://www.python.org/doc/2.5.2/tut/tut.html`
- La documentation de `http://www.python.org/` est très fournie.
- ...et est générée à partir de la documentation intégrée au code source, accessible via

```
help(objet)
```

Des pages web...

- Tout d'abord le tutorial de Python... Part de très bas et vient toucher du doigt la programmation orientée objet. Très bonne lecture pour débuter
- `http://www.python.org/doc/2.5.2/tut/tut.html`
- La documentation de `http://www.python.org/` est très fournie.
- ...et est générée à partir de la documentation intégrée au code source, accessible via

```
help(objet)
```

...et des livres

- *Programming Python*, volumineux, mais sous windows, et ne va pas au fond des choses
- *Python Cookbook*, une série d'études de cas, intéressant pour résoudre un problème
- *Python in a Nutshell*, couvre la bibliothèque standard avec quelques exemples d'utilisation
- ...sont disponibles au 2B

...et des livres

- *Programming Python*, volumineux, mais sous windows, et ne va pas au fond des choses
- *Python Cookbook*, une série d'études de cas, intéressant pour résoudre un problème
- *Python in a Nutshell*, couvre la bibliothèque standard avec quelques exemples d'utilisation
- ...sont disponibles au 2B

...et des livres

- *Programming Python*, volumineux, mais sous windows, et ne va pas au fond des choses
- *Python Cookbook*, une série d'études de cas, intéressant pour résoudre un problème
- *Python in a Nutshell*, couvre la bibliothèque standard avec quelques exemples d'utilisation
- ...sont disponibles au 2B

...et des livres

- *Programming Python*, volumineux, mais sous windows, et ne va pas au fond des choses
- *Python Cookbook*, une série d'études de cas, intéressant pour résoudre un problème
- *Python in a Nutshell*, couvre la bibliothèque standard avec quelques exemples d'utilisation
- ...sont disponibles au 2B

Encore des questions ?