LDAP

Lightweight Directory Access Protocol

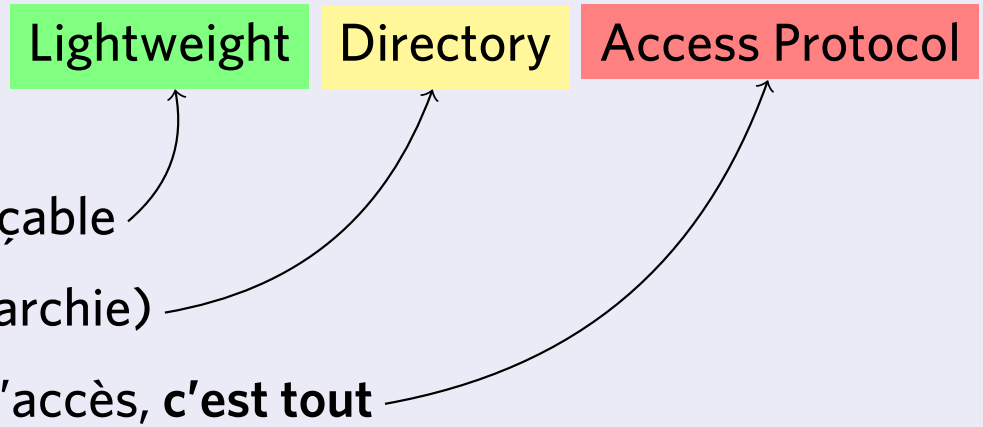
Antoine Lubineau

INP-net

18 décembre 2011

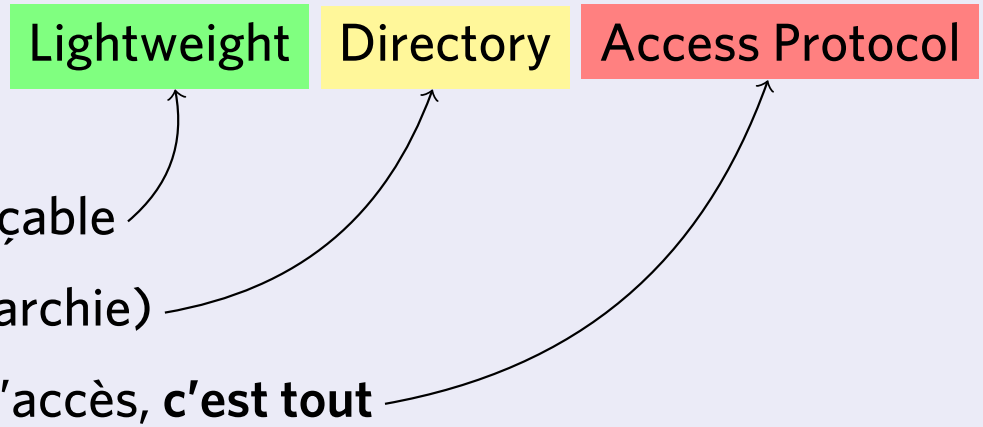
Introduction

Qu'est-ce que LDAP ?



Introduction

Qu'est-ce que LDAP ?



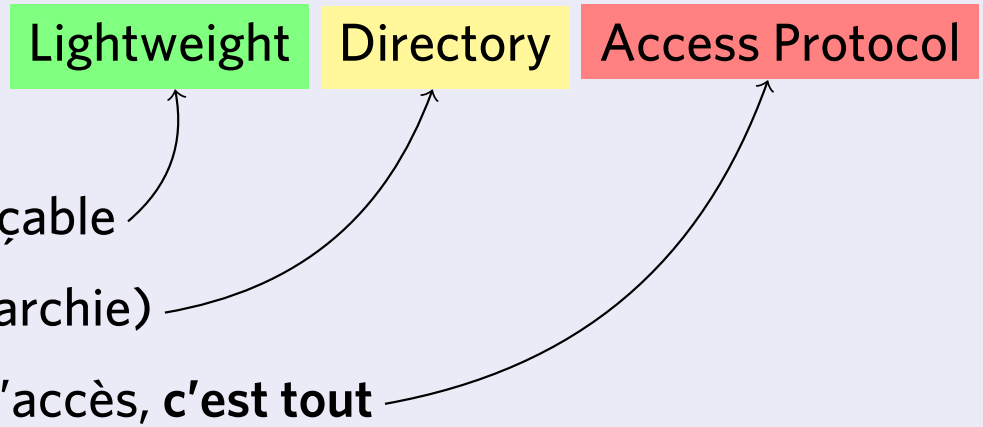
- simple, interfaçable
- annuaire (hiérarchie)
- un protocole d'accès, **c'est tout**

Pourquoi LDAP et pas autre chose ? (SQL ?)

- authentification centralisée

Introduction

Qu'est-ce que LDAP ?

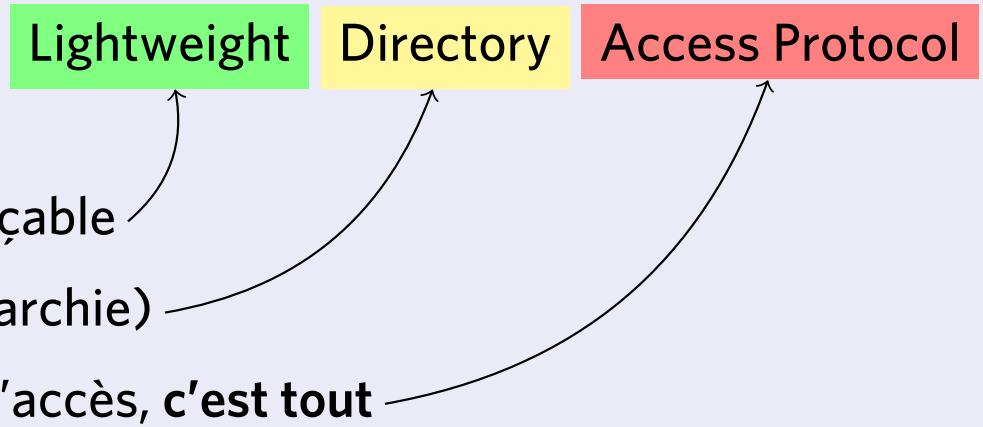


Pourquoi LDAP et pas autre chose ? (SQL ?)

- authentification centralisée
- structure hiérarchique réaliste

Introduction

Qu'est-ce que LDAP ?



- simple, interfaçable
- annuaire (hiérarchie)
- un protocole d'accès, **c'est tout**

Pourquoi LDAP et pas autre chose ? (SQL ?)

- authentification centralisée
- structure hiérarchique réaliste
- grandes performances en lecture

Introduction

Avantages de LDAP

- service d'annuaire très optimisé pour les lectures

Introduction

Avantages de LDAP

- service d'annuaire très optimisé pour les lectures
- service distribué de stockage d'information

Introduction

Avantages de LDAP

- service d'annuaire très optimisé pour les lectures
- service distribué de stockage d'information
- extensibilité des schémas standards

Introduction

Avantages de LDAP

- service d'annuaire très optimisé pour les lectures
- service distribué de stockage d'information
- extensibilité des schémas standards
- possibilités de recherche avancées

Introduction

Avantages de LDAP

- service d'annuaire très optimisé pour les lectures
- service distribué de stockage d'information
- extensibilité des schémas standards
- possibilités de recherche avancées
- réplication entre serveurs

Introduction

Avantages de LDAP

- service d'annuaire très optimisé pour les lectures
- service distribué de stockage d'information
- extensibilité des schémas standards
- possibilités de recherche avancées
- réplication entre serveurs

À faire sur une machine du réseau INP-net

```
$ ldapsearch -x uid=lubinea sn
```

- pas de *bind*
- filtre de recherche
- attribut demandé (facultatif)

Sommaire

Structure

- arbre n-aire organisé en :
  - racine basée sur le nommage DNS : `dc=etu-inpt,dc=fr` (DC : *domain component*)
  - organisations : `o=n7`, `o=a7`...
  - *organizational units* : `ou=groups`, `ou=aliases`...
  - nœuds dont la première composante du DN est souvent le CN *(common name)* ou l'UID

Structure

- arbre n-aire organisé en :
  - racine basée sur le nommage DNS : `dc=etu-inpt,dc=fr` (DC : *domain component*)
  - organisations : `o=n7`, `o=a7`...
  - *organizational units* : `ou=groups`, `ou=aliases`...
  - nœuds dont la première composante du DN est souvent le CN *(common name)* ou l'UID
- un nœud : un ensemble d'attributs dont :
  - un *Distinguished Name* (DN) **unique** = RDN *Relative DN* suivi du DN du parent
  - un ou des *objectClass* qui font référence aux schémas
  - un *common name* (CN) ou un UID
  - les attributs définis dans le schéma...

Opérations LDAP

- StartTLS : pas utilisé ici
- Bind : authentification
- Recherche
- Comparaison
- Ajout
- Suppression
- Modification d'un nœud
- Modification du DN = déplacement
- Abandon
- Opérations étendues
- Unbind : fermeture de la *connexion*

Filtres LDAP

À compléter.

Configuration d'un serveur OpenLDAP

Configuration disponible dans le dépôt Mercurial INP-net `conf_ldap`.

Configuration d'un serveur OpenLDAP

Configuration disponible dans le dépôt Mercurial INP-net `conf_ldap`.

Schéma

`slapd.conf` et `inp-net.schema`.

Configuration d'un serveur OpenLDAP

Configuration disponible dans le dépôt Mercurial INP-net `conf_ldap`.

Schéma

`slapd.conf` et `inp-net.schema`.

Indexation du LDAP

`user-indexes.conf`.

Configuration d'un serveur OpenLDAP

Configuration disponible dans le dépôt Mercurial INP-net `conf_ldap`.

Schéma

`slapd.conf` et `inp-net.schema`.

Indexation du LDAP

`user-indexes.conf`.

ACL LDAP

`slapd.access`.

Configuration d'un serveur OpenLDAP

Configuration disponible dans le dépôt Mercurial INP-net `conf_ldap`.

Schéma

`slapd.conf` et `inp-net.schema`.

Indexation du LDAP

`user-indexes.conf`.

ACL LDAP

`slapd.access`.

Piège

Bien lire la documentation et **tester** avant de mettre en production.

Une requête sympathique

Trouver les machines d'une salle de TP

```
$ ldapsearch -x -h ldapmaster.enseeiht.fr \
  -b ou=hosts,dc=n7,dc=fr puppetclass=c201 cn
```

Une requête sympathique

Trouver les machines d'une salle de TP

```
$ ldapsearch -x -h ldapmaster.enseeiht.fr \
  -b ou=hosts,dc=n7,dc=fr puppetclass=c201 cn

# dragon.enseeiht.fr, hosts, n7.fr
dn : cn=dragon.enseeiht.fr,ou=hosts,dc=n7,dc=fr
cn : dragon.enseeiht.fr

# minotaure.enseeiht.fr, hosts, n7.fr
dn : cn=minotaure.enseeiht.fr,ou=hosts,dc=n7,dc=fr
cn : minotaure.enseeiht.fr

...
```

PHP

ldap.php?groupe=net7-n7 — affiche les membres d'un groupe n7

```php
<?php $conn = ldap_connect('discover');
ldap_set_option($conn, LDAP_OPT_PROTOCOL_VERSION, 3);
$search = ldap_search($conn, 'ou=groups,o=n7,' .
  'dc=etu-inpt,dc=fr', 'cn=' . $_GET['groupe']);
$values = ldap_get_values($conn,
  ldap_first_entry($conn, $search), 'memberUid');
for ($i=0; $i < $values['count']; $i++) {
  echo $values[$i] . '<br />';
}
ldap_close($conn); ?>
```

PHP

ldap.php?groupe=net7-n7 — affiche les membres d'un groupe n7

```php
<?php $conn = ldap_connect('discover');
ldap_set_option($conn, LDAP_OPT_PROTOCOL_VERSION, 3);
$search = ldap_search($conn, 'ou=groups,o=n7,' .
  'dc=etu-inpt,dc=fr', 'cn=' . $_GET['groupe']);
$values = ldap_get_values($conn,
  ldap_first_entry($conn, $search), 'memberUid');
for ($i=0; $i < $values['count']; $i++) {
  echo $values[$i] . '<br />';
}
ldap_close($conn); ?>
```

Documentation

http://www.php.net/manual/fr/ref.ldap.php

Python

Recherche simple avec le module ldap — Python 2

```
>>> import ldap
>>> conn = ldap.initialize('ldap://discover')
>>> conn.simple_bind_s()
(97, [])
>>> s = conn.search_s(base='ou=people,o=n7,dc=etu-inpt,dc=fr',
...                   scope=ldap.SCOPE_SUBTREE,
...                   filterstr='(!(loginShell=/bin/bash))',
...                   attrlist=['cn'])
>>> print s
plein de choses intéressantes
>>> conn.unbind_s()
```

Python

Recherche simple avec le module ldap — Python 2

```
>>> import ldap
>>> conn = ldap.initialize('ldap://discover')
>>> conn.simple_bind_s()
(97, [])
>>> s = conn.search_s(base='ou=people,o=n7,dc=etu-inpt,dc=fr',
...                   scope=ldap.SCOPE_SUBTREE,
...                   filterstr='(!(loginShell=/bin/bash))',
...                   attrlist=['cn'])
>>> print s
plein de choses intéressantes
>>> conn.unbind_s()
```

Remarques

- `*_s` : opération synchrone
- Documentation sur `http://python-ldap.org/`

Ruby

Recherche simple avec la *gem* net-ldap

```
irb(main):001:0> require 'net/ldap'
=> true
irb(main):002:0> ldap = Net::LDAP.new
=> #<Net::LDAP:0x00000002466570 @host="127.0.0.1", @port=389,
@verbose=false, @auth={:method=>:anonymous}, @base="dc=com",
@encryption=nil, @open_connection=nil>
irb(main):003:0> ldap.host = 'discover'
=> "discover"
irb(main):004:0> ldap.search(:base => "dc=etu-inpt,dc=fr",
irb(main):005:1*                :filter => "cn=net7-n7")
=> [#<Net::LDAP::Entry:0x000000001290b20 ...
```

Ruby

Recherche simple avec la *gem* `net-ldap`

```
irb(main):001:0> require 'net/ldap'
=> true
irb(main):002:0> ldap = Net::LDAP.new
=> #<Net::LDAP:0x00000002466570 @host="127.0.0.1", @port=389,
@verbose=false, @auth={:method=>:anonymous}, @base="dc=com",
@encryption=nil, @open_connection=nil>
irb(main):003:0> ldap.host = 'discover'
=> "discover"
irb(main):004:0> ldap.search(:base => "dc=etu-inpt,dc=fr",
irb(main):005:1*                :filter => "cn=net7-n7")
=> [#<Net::LDAP::Entry:0x000000001290b20 ...
```

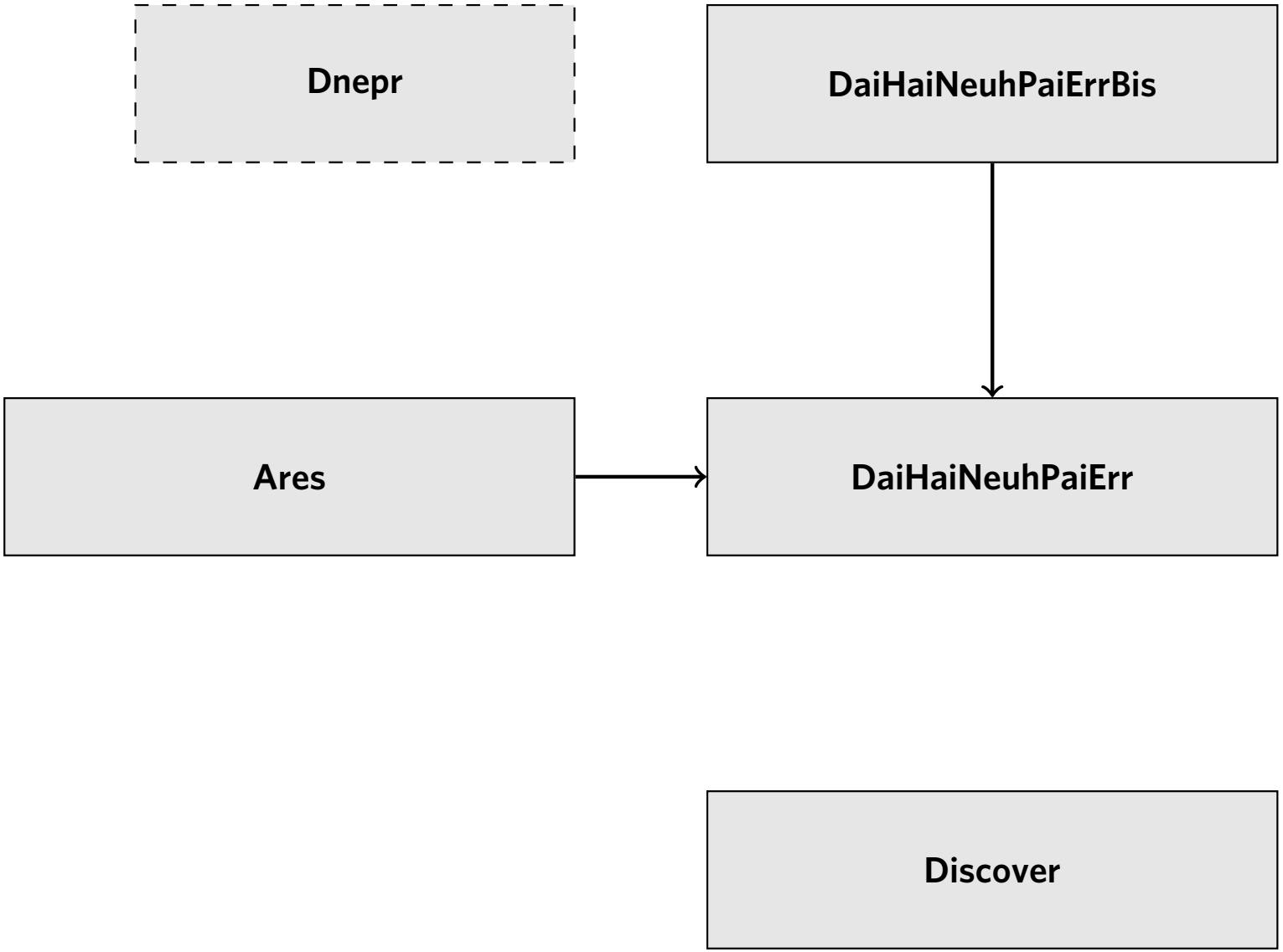
Remarque

La *gem* `ruby-ldap` ressemble un peu plus au module `ldap` de Python.

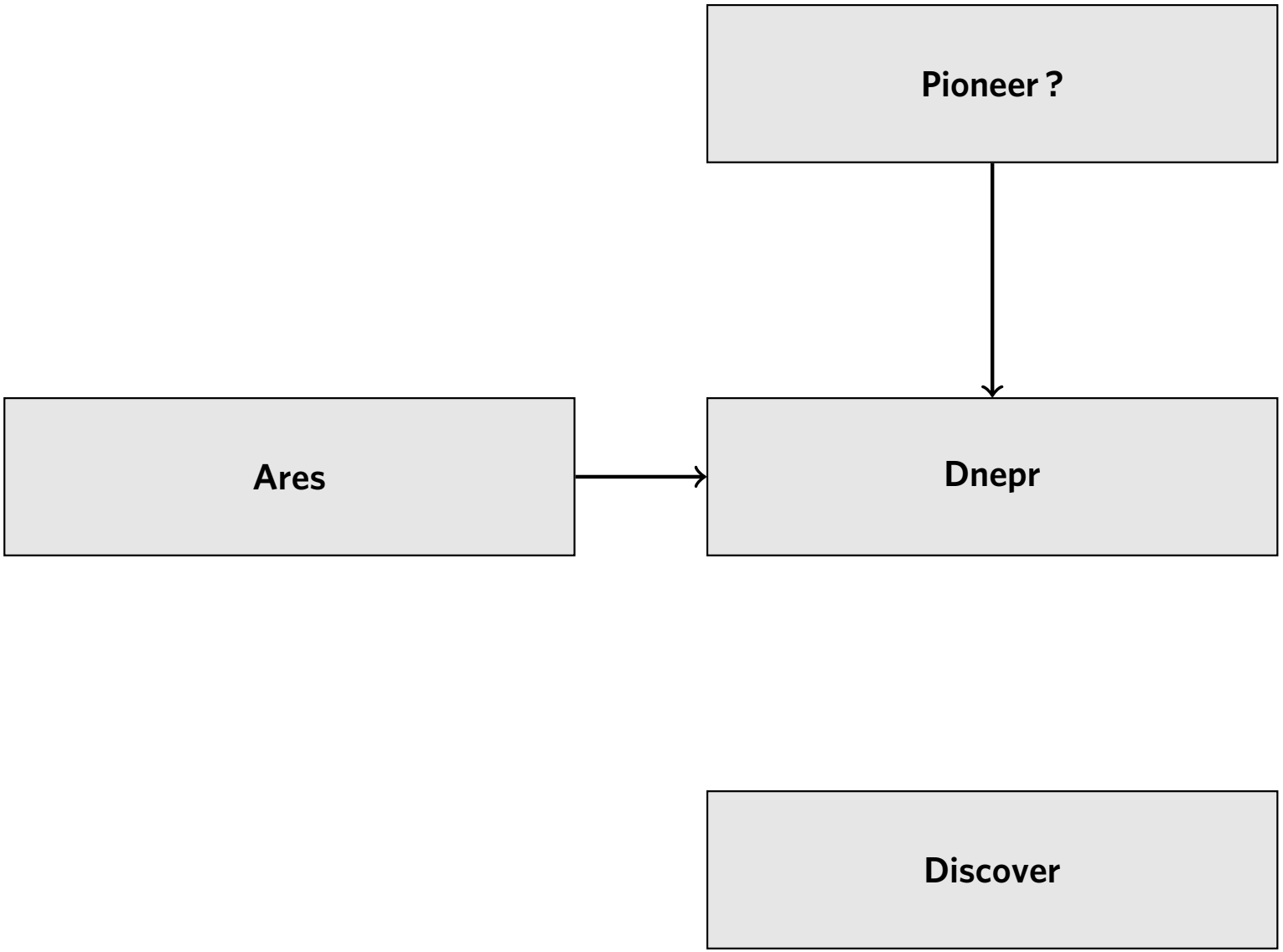
Perl

Voir `/clubs/n7/net7/private/scripts/generateClubsLinksOnDesktop.pl` : script de création de raccourcis pour les utilisateurs en fonction des dossiers auxquels ils ont accès.

Serveurs LDAP INP-net (configuration provisoire)



Serveurs LDAP INP-net (configuration stable)



Authentification avec PAM

PAM *(Pluggable authentication modules)* : API standardisée d'authentification.

/etc/pam.d/sshd

```
auth        required    pam_nologin.so
auth        required    pam_group.so use_first_pass
auth        sufficient  pam_ldap.so
auth        required    pam_env.so
auth        required    pam_unix.so use_first_pass
account     sufficient  pam_ldap.so
account     required    pam_unix.so
account     required    pam_time.so
password    required    pam_ldap.so
password    required    pam_unix.so
session     required    pam_unix_session.so
session     sufficient  pam_ldap.so
session     required    pam_limits.so
```

Authentification avec PAM

Exemple d'installation

`https://trac.inp-net.eu.org/wiki/InstallerUnServeur` et `http://wiki.debian.org/LDAP/PAM`.

Postfix

Serveur SMTP *(Simple Mail Transfer Protocol)* sur Galileo. Extraits de la configuration :

/etc/postfix/main.cf — alias utilisateurs

```
ldapuser_server_host = ldapmaster.bde.inp ldapslave.bde.inp
ldapuser_search_base = dc=etu-inpt,dc=fr
ldapuser_query_filter = (&(objectClass=qmailUser)(mail=%s))
ldapuser_result_attribute = mailForwardingAddress
ldapuser_bind = no
```

Postfix

Serveur SMTP *(Simple Mail Transfer Protocol)* sur Galileo. Extraits de la configuration :

/etc/postfix/main.cf — alias utilisateurs

```
ldapuser_server_host = ldapmaster.bde.inp ldapslave.bde.inp
ldapuser_search_base = dc=etu-inpt,dc=fr
ldapuser_query_filter = (&(objectClass=qmailUser)(mail=%s))
ldapuser_result_attribute = mailForwardingAddress
ldapuser_bind = no
```

/etc/postfix/main.cf — alias des clubs n7

```
ldapn7_domain = bde.enseeiht.fr
ldapn7_server_host = ldapmaster.bde.inp ldapslave.bde.inp
ldapn7_search_base = ou=aliases,o=n7,dc=etu-inpt,dc=fr
ldapn7_query_filter = (&(objectClass=nisMailAlias)(cn=%u))
ldapn7_result_attribute = rfc822MailMember
ldapn7_bind = no
```

ejabberd

Serveur Jabber `im.inpt.fr` sur Vega. Extrait de la configuration :

/etc/ejabberd/ejabberd.cfg

```
{auth_method, ldap}.
{ldap_servers, ["ldapmaster.bde.inp","ldapslave.bde.inp"]}.
{ldap_uidattr, "uid"}.
{ldap_base, "dc=etu-inpt,dc=fr"}.
```

ejabberd

Serveur Jabber `im.inpt.fr` sur Vega. Extrait de la configuration :

/etc/ejabberd/ejabberd.cfg

```
{auth_method, ldap}.
{ldap_servers, ["ldapmaster.bde.inp","ldapslave.bde.inp"]}.
{ldap_uidattr, "uid"}.
{ldap_base, "dc=etu-inpt,dc=fr"}.
```

Piège

L'ordre d'accès aux serveurs LDAP n'est pas spécifié… *hilarity ensues*.

FreeRADIUS

Serveur d'authentification 802.1X *(Remote Authentication Dial-In User Service)* sur Atlas (provisoirement Discover). Extrait de la configuration :

/etc/raddb/modules/ldap

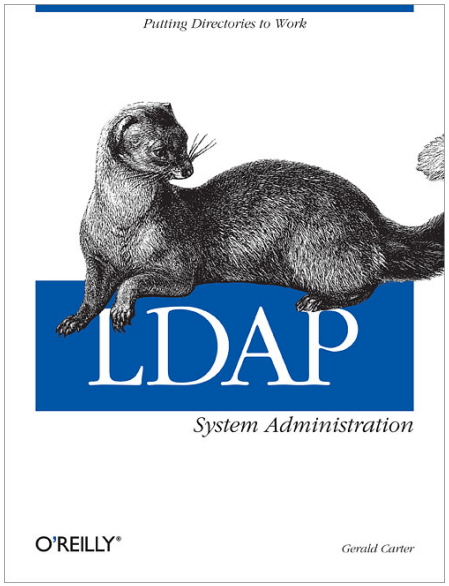
```
ldap {
  server = "ldapmaster.bde.inp"
  identity = "uid=client-consult,ou=scripts," \
    "ou=inp-net,o=inp,dc=etu-inpt,dc=fr"
  password = "********************"
  basedn = "dc=etu-inpt,dc=fr"
  filter = "(uid=%{%{Stripped-User-Name} :-%{User-Name}})"
  base_filter = "(objectclass=Eleve)"
  access_attr = "inscritAE"
  dictionary_mapping = ${confdir}/ldap.attrmap
}
```

ORM Django du portail BDE

À compléter.

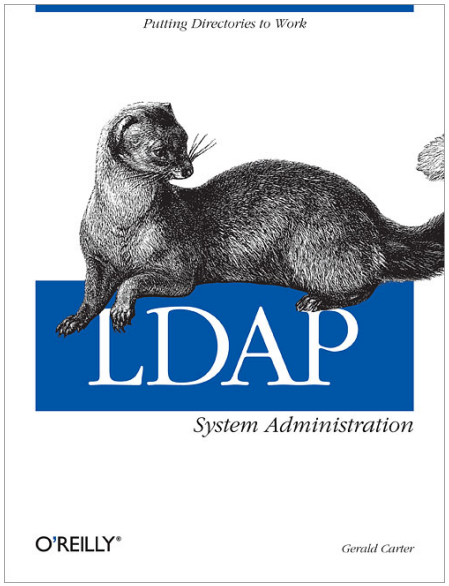
Références

- Carter (Gerald), *LDAP System Administration*, O'Reilly, 2003. Disponible sur l'étagère.



Références

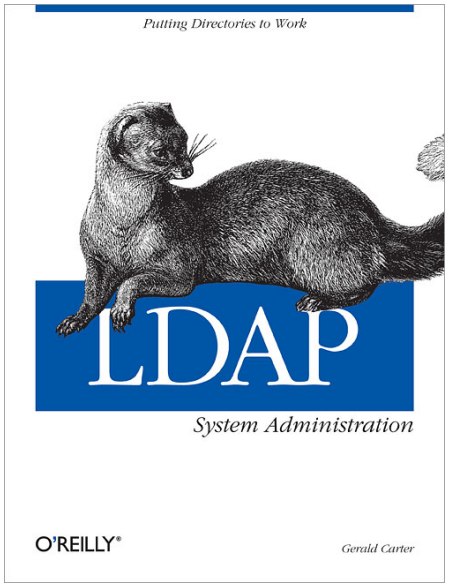
- Carter (Gerald), *LDAP System Administration*, O'Reilly, 2003. Disponible sur l'étagère.



- Le manuel d'OpenLDAP : `http://www.openldap.org/doc/admin24/`

Références

- Carter (Gerald), *LDAP System Administration*, O'Reilly, 2003. Disponible sur l'étagère.



- Le manuel d'OpenLDAP : `http://www.openldap.org/doc/admin24/`
- Les RFC 4510 à 4519 : `http://www.rfc-editor.org/`

C'est fini !

Questions ?