Link::Accounts

Olivier Thauvin

CNRS/LATMOS

ANF Les systèmes d'authentification dans la communauté ESR : étude, mise en œuvre et interfaçage dans un laboratoire de Mathématique
Angers, 22 - 26 septembre 2014

Progression

Moi...

le SA

Arrivé au Service d'Aéronomie fin 2000

Une formation clef

- Brevet de Technicien Agricole en Horticulture, option productions florales
- Brevet de Technicien Supérieur Agricole en Horticulture, option productions florales

Ah, au fait

J'y connais rien moi à l'informatique !

Moi...

le SA

Arrivé au Service d'Aéronomie fin 2000

Une formation clef

- Brevet de Technicien Agricole en Horticulture, option productions florales
- Brevet de Technicien Supérieur Agricole en Horticulture, option productions florales

Ah, au fait

J'y connais rien moi à l'informatique !

Tout change en 2009

Il y avait un déménagement

Déménagement dans un bâtiment neuf à Guyancourt :

- 2/3 du Service d'Aéronomie (100 personnes)
- 1/2 du CETP (100 personnes)

Il y avait une fusion

- le Service d'Aéronomie (150 personnes)
  - site de Verrières le Buisson (en déménagement)
  - site de Jussieu
- 1/2 du CETP (100 personnes)

Tout change en 2009

Il y avait un déménagement

Déménagement dans un bâtiment neuf à Guyancourt :

- 2/3 du Service d'Aéronomie (100 personnes)
- 1/2 du CETP (100 personnes)

Il y avait une fusion

- le Service d'Aéronomie (150 personnes)
  - site de Verrières le Buisson (en déménagement)
  - site de Jussieu
- 1/2 du CETP (100 personnes)

Et les comptes utilisateurs ?

Le Service d'Aéronomie

- Unix : 2 bases NIS (une par site)
- Windows : Néant absolu

CETP

- NIS : une base gérée à la main via des scripts obscurs
- un Active Directory

Et les comptes utilisateurs ?

Le Service d'Aéronomie

- Unix : 2 bases NIS (une par site)
- Windows : Néant absolu

CETP

- NIS : une base gérée à la main via des scripts obscurs
- un Active Directory

Problèmes :

Problèmes du design

- plusieurs créations de comptes
- informations non synchronisés
- comptes parfois incohérents entre bases

Fonctionnalités qui manquaient

- bases modifiables que par quelques admin
- informations non accessibles par les utilisateurs
- délégation impossible

Problèmes :

Problèmes du design

- plusieurs créations de comptes
- informations non synchronisés
- comptes parfois incohérents entre bases

Fonctionnalités qui manquaient

- bases modifiables que par quelques admin
- informations non accessibles par les utilisateurs
- délégation impossible

Progression

Ce qu'on veut :

Fonctionnalités primaires

- des bases synchrones
- un système modulable
- des automatismes
- virer NIS (en douceur), passer à LDAP

On voudrait aussi

- une interface WEB (simple)
- pouvoir déléguer
- garder les comptes utilisateurs détruits

Ce qu'on veut :

Fonctionnalités primaires

- des bases synchrones
- un système modulable
- des automatismes
- virer NIS (en douceur), passer à LDAP

On voudrait aussi

- une interface WEB (simple)
- pouvoir déléguer
- garder les comptes utilisateurs détruits

Link : :Accounts

Langage :

Ecrit en PERL :

- `PostgreSQL`
- `LDAP`, `KRB5`
- `Cracklib`
- `Catalyst` (Web)

Principe :

Une base centrale SQL contenant toutes les informations, les informations sont propagées aux autres bases.

Link : :Accounts

Langage :

Ecrit en PERL :

- `PostgreSQL`
- `LDAP`, `KRB5`
- `Cracklib`
- `Catalyst` (Web)

Principe :

Une base centrale SQL contenant toutes les informations, les informations sont propagées aux autres bases.

Fonctionnement

L'application comprends :

- des bases typées (LDAP, AD, Unix, . . .), le module uniformise les accès.
  - des objets typés (Users, Group) identifiés
    - des attributs

La synchronisation :

1. pour chaque base cible on liste les objets par type (User, Groups)
2. pour objets on synchronises les attributs commun entre les bases
3. on détruits les objets inexistants dans la base source

Fonctionnement

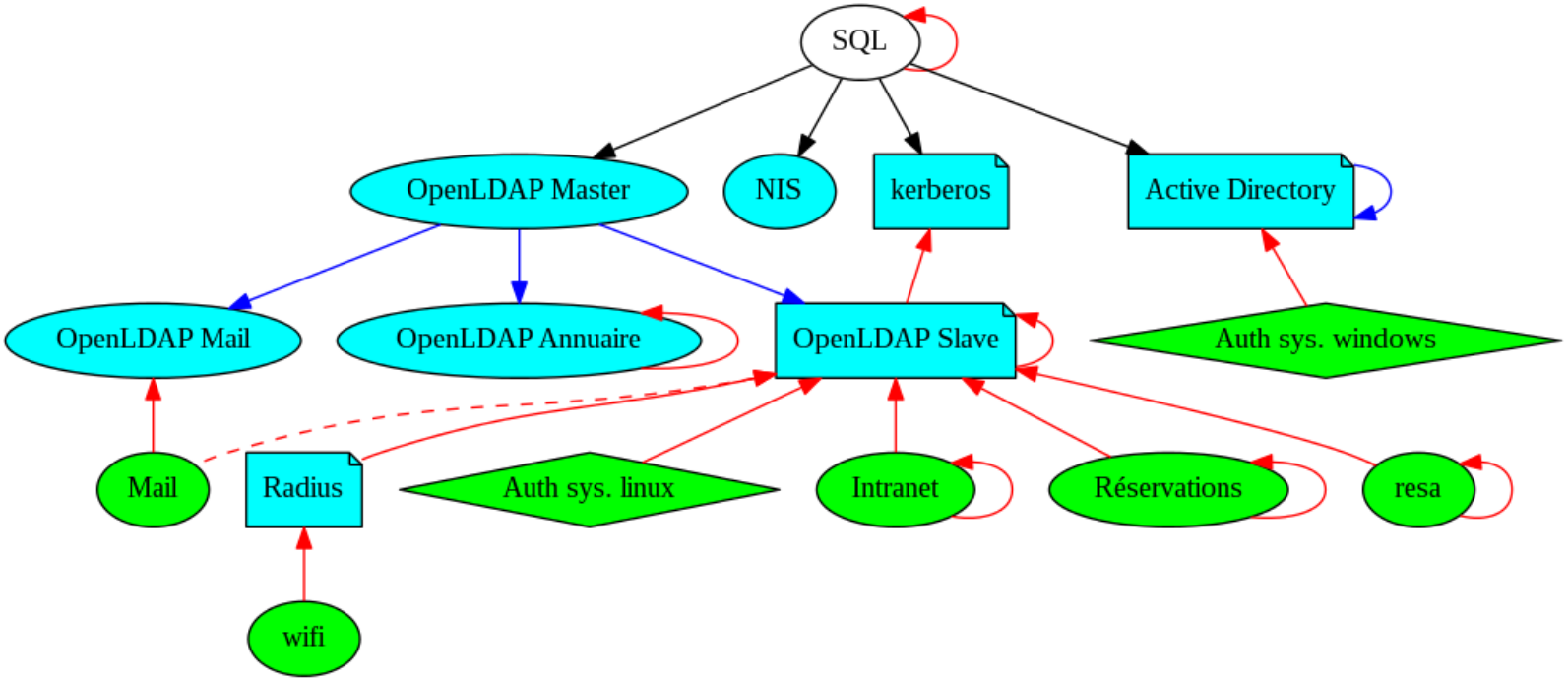
L'application comprends :

- des bases typées (LDAP, AD, Unix, . . .), le module uniformise les accès.
  - des objets typés (Users, Group) identifiés
    - des attributs

La synchronisation :

1. pour chaque base cible on liste les objets par type (User, Groups)
2. pour objets on synchronises les attributs commun entre les bases
3. on détruits les objets inexistants dans la base source

Notre architecture



Progression

Les mots de passe

Pas de mot de passe en clair !

- stockage local via crypt
- le mot de passe est propagé lors de la saisie

Chiffrement réversible

- création d'une clef asymétrique (protégé par mot de passe)
- chiffrement des mots de passe avec la clef publique

Les mots de passe

Pas de mot de passe en clair !

- stockage local via crypt
- le mot de passe est propagé lors de la saisie

Chiffrement réversible

- création d'une clef asymétrique (protégé par mot de passe)
- chiffrement des mots de passe avec la clef publique

Groupe typé

Des bases limitées

- On veut donner des droits en fonction des statuts
- mais les systèmes et applications n'ont que des groupes

Tout est groupe :

en interne :

- les données administratives sont des groupes
- les groupes sont « typés »

Groupe typé

Des bases limitées

- On veut donner des droits en fonction des statuts
- mais les systèmes et applications n'ont que des groupes

Tout est groupe :

en interne :

- les données administratives sont des groupes
- les groupes sont « typés »

Progression

La demo

C'est le moment où je tente une démo en ligne. . . et normallement ça marche pas !

Progression

Merci

https://forge.ipsl.jussieu.fr/link-accounts

Question ?

(c) Wikipédia

Licence

Cette œuvre est mise à disposition selon les termes de la Licence Creative Commons Attribution 3.0 non transposé.