Mise en œuvre d’une infrastructure d’authentification centralisée

Jason SECULA

IUT Nancy-Charlemagne

Observatoire astronomique de Strasbourg

Plan

1 - Observatoire astronomique de Strasbourg

2 - Sujet du stage

3 - L’existant

4 - Travail réalisé

5 - Conclusion

Observatoire astronomique de Strasbourg

Sujet du stage

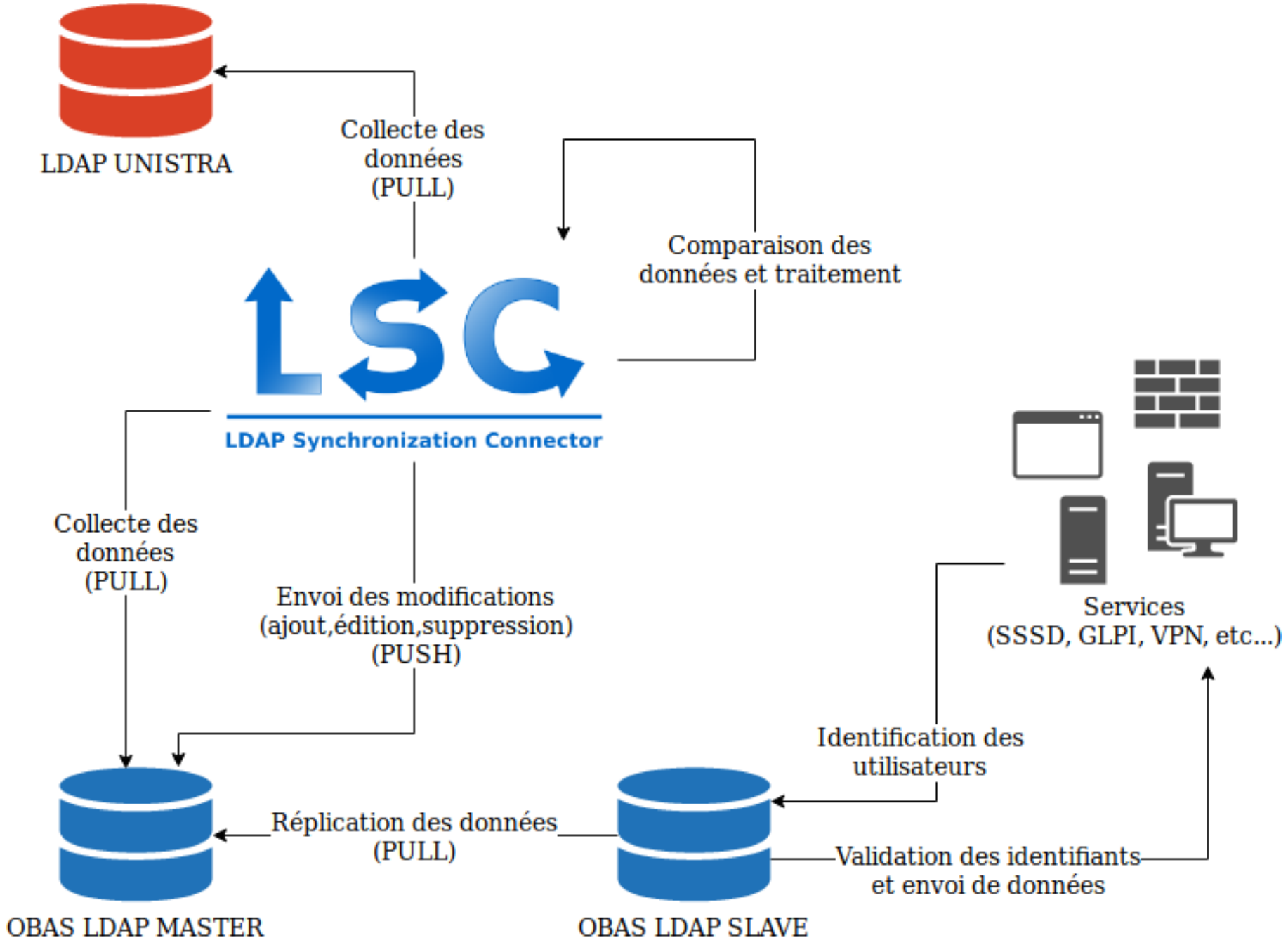
- **Contexte**
  - Plusieurs outils et services (réservation de salles, VPN, support)
  - Permettre aux usagers de s'authentifier avec les identifiants habituels
  - Création de compte manuelle en plus des utilisateurs de l'Unistra
- **Sujet**
  - Mise en œuvre d'une authentification LDAP centralisée
- **Objectifs**
  - Mise en place d'un annuaire LDAP
  - Synchroniser les utilisateurs de l'Université de Strasbourg
  - Authentifier des services et des postes avec un annuaire LDAP

L’existant

- **Actuellement**
  - Chaque service → +1 base de données utilisateurs
  - 1 serveur NIS qui distribue les données utilisateurs entre les postes
- **Après**
  - 1 serveur OpenLDAP maître et 1 serveur OpenLDAP esclave
  - Chaque service → Authentification LDAP
  - Les postes → Authentification LDAP

Travail réalisé

- Prise en main de OpenLDAP et création des annuaires
- Synchronisation des données de l’Unistra
- Sécurisation des annuaires
- Mise en place d’un site d’administration de l’annuaire
- Authentification des services, des postes et des serveurs
- Déploiement des configurations avec Ansible


LDAP UNISTRA
Collecte des
données
(PULL)
Comparaison des
données et traitement
LSC
LDAP Synchronization Connector
Collecte des
données
(PULL)
Envoi des modifications
(ajout,édition,suppression)
(PUSH)
Services
(SSSD, GLPI, VPN, etc...)
Identification des
utilisateurs
Réplication des données
(PULL)
Validation des identifiants
et envoi de données
OBAS LDAP MASTER
OBAS LDAP SLAVE

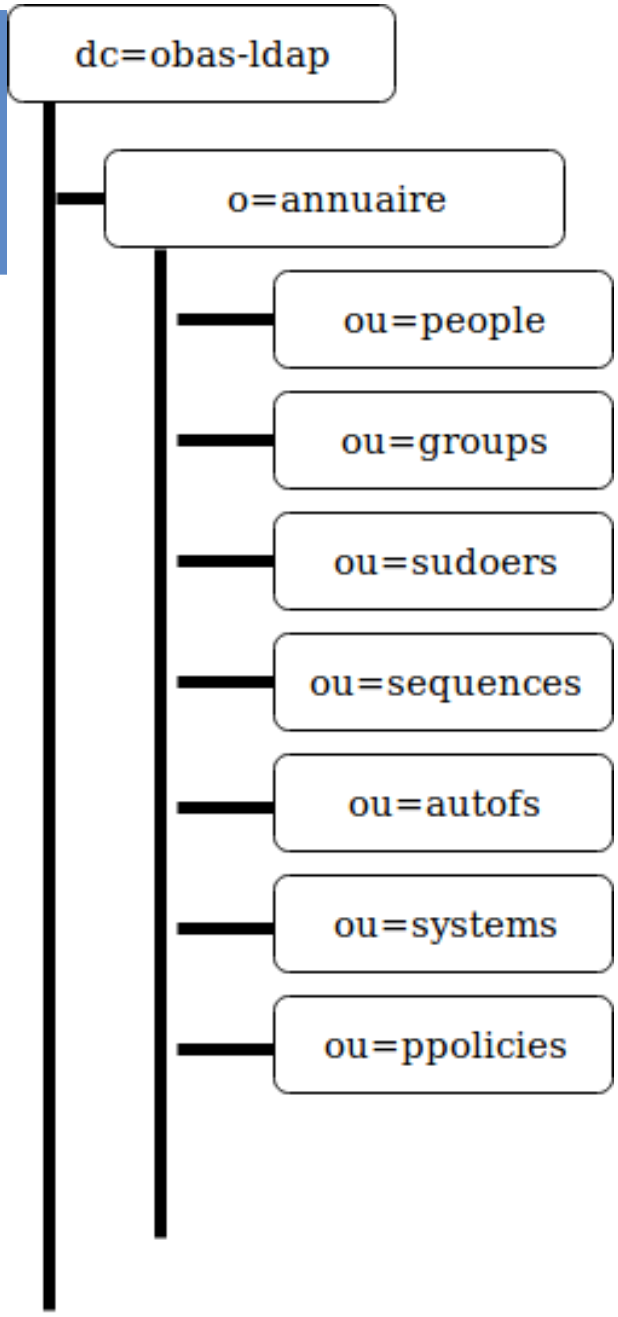
OpenLDAP

- **Outil libre écrit en C / 1998**
- **OpenLDAP Foundation**
- **Stocker des informations de n’importe quelle nature**
- **Structure arborescente**
- **LDAP Data Interchange Format (LDIF)**

OpenLDAP

Structure arborescente

- uid=bob,ou=people,o=annuaire,dc=obas-ldap
- cn=admins,ou=groups,o=annuaire,dc=obas-ldap



OpenLDAP

Le format LDIF

```
dn: uid=alice,ou=people,o=annuaire,dc=obas-ldap
uid: alice
uidNumber: 1003
gidNumber: 1003
cn: alice
loginShell: /bin/bash
homeDirectory: /home/alice
userPassword: {SSHA}VYeXUL7smgZ/u+JOqrUgVpNVEPXCRtfk
objectClass: inetOrgPerson
objectClass: posixAccount
```

Synchronisation LSC

LDAP Synchronization Connector

- **Outil libre écrit en Java**
- **Synchroniser des données entre plusieurs sources**
- **Configuration XML avec possibilité d’utiliser JavaScript**

Sécurisation des annuaires

- **Configuration de la communication LDAP over SSL (LDAPS)**

- **Ajout de listes d’accès déterminant les droits des utilisateurs**

- **Équilibrage de charge entre les deux annuaires avec HAProxy**

- **Supervision des annuaires via Zabbix avec un module LDAP**

Sécurisation des annuaires

- **Définition des droits d'accès**

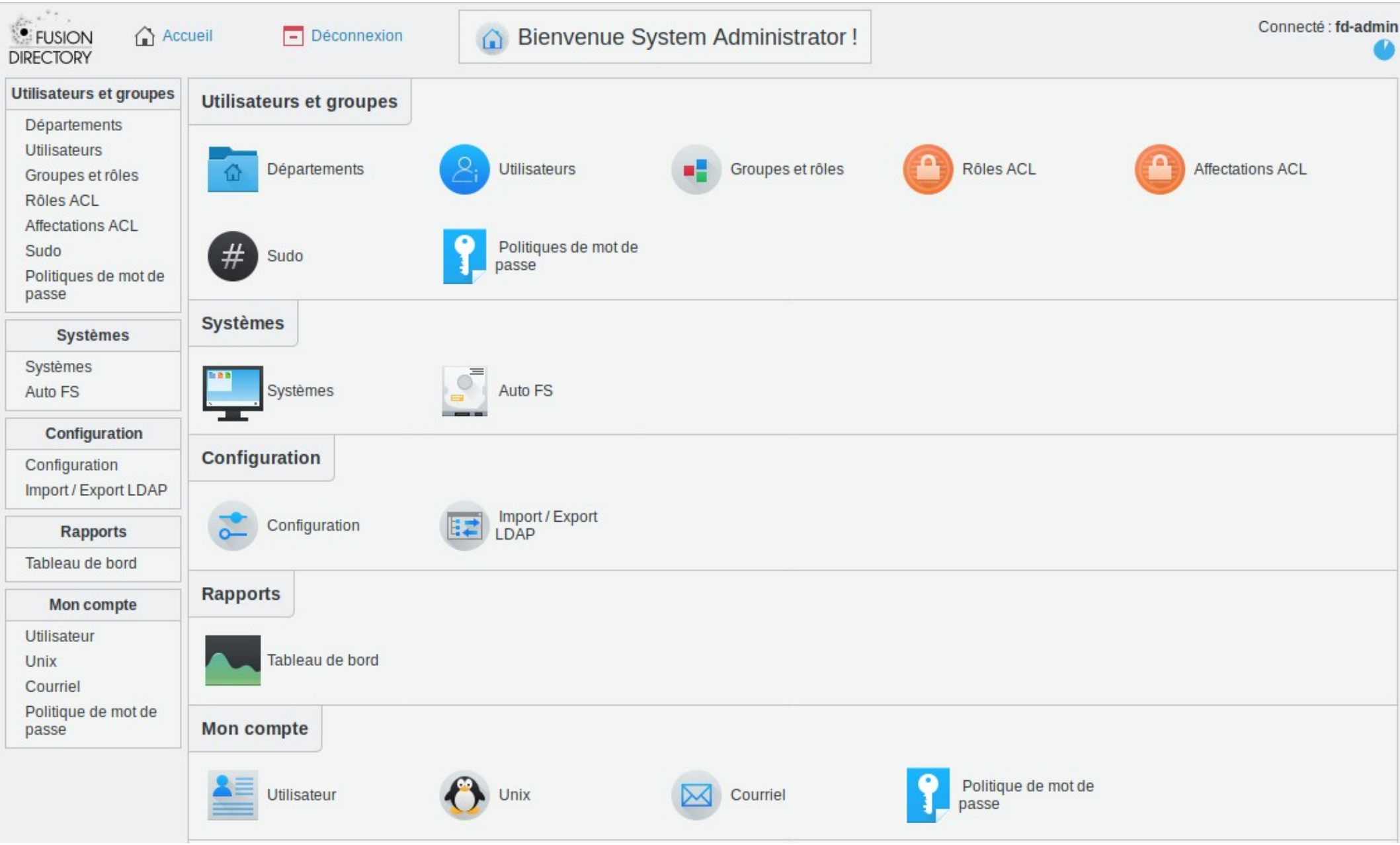
Ressources	cn=auth	cn=replicator	users	anonymous	*
Mot de passe perso	read	read	write	auth	none
Mot de passe autres utilisateurs	none	read	none	auth	none
dn.base dc=obas-ldap	read	read	read	auth	none
dn.subtree o=annuaire	read	read	read	auth	none

olcAccess: {1}to dn.subtree="cn=replicator,o=annuaire,dc=obas-ldap" by dn.exact="cn=replicator,o=annuaire,dc=obas-ldap" read by anonymous auth by * none

olcAccess: {2}to attrs=userPassword by self write by dn.exact="cn=replicator,o=annuaire,dc=obas-ldap" read by anonymous auth by * none

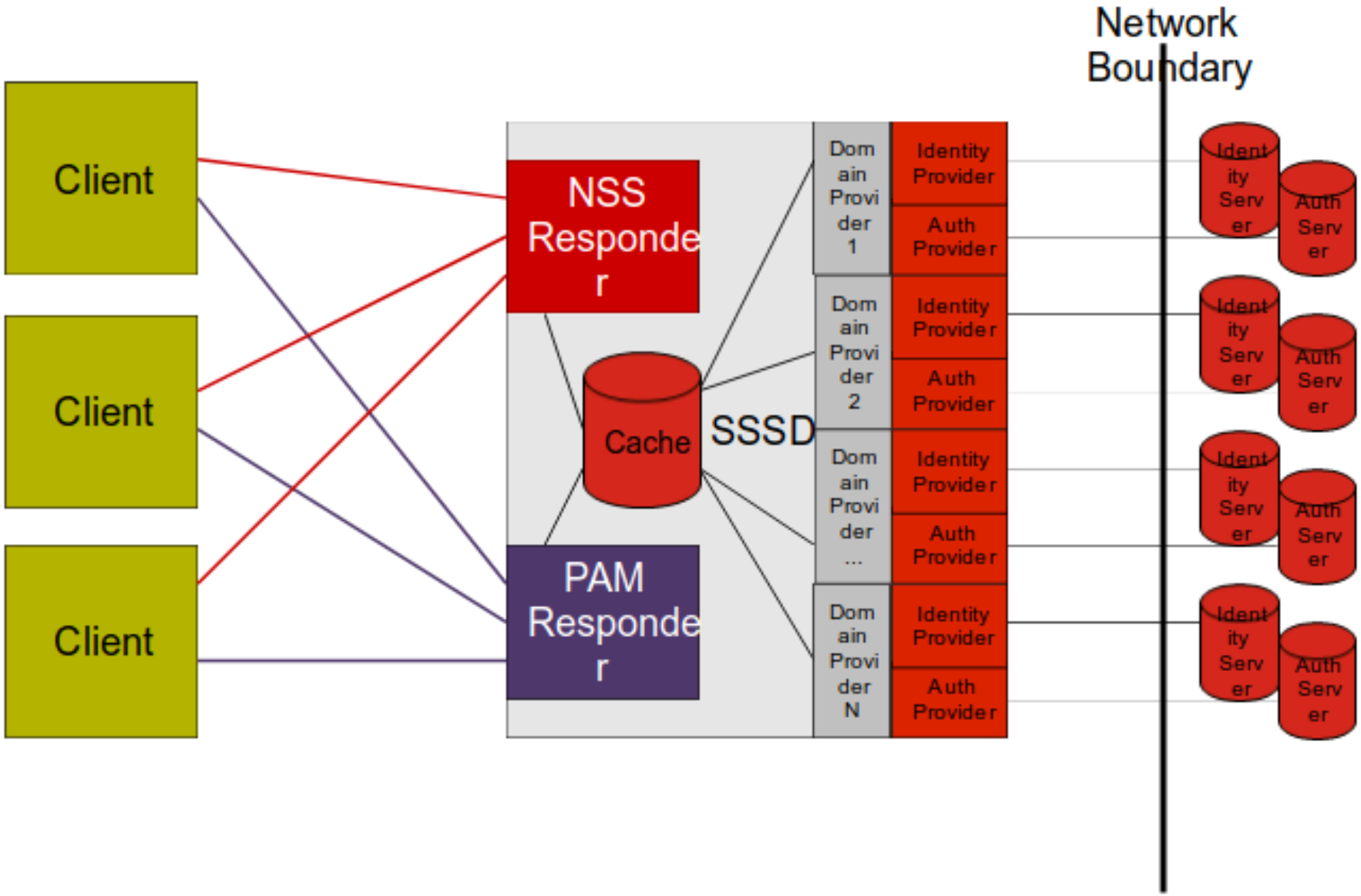
FusionDirectory

- **Outil libre écrit en PHP**
- **Permet d’administrer les données d’un serveur LDAP via une interface web**
- **Simple d’utilisation**
- **Beaucoup de plugins**


FUSION DIRECTORY
Accueil
Déconnexion
Bienvenue System Administrator !
Connecté : fd-admin
Utilisateurs et groupes
Départements
Utilisateurs
Groupes et rôles
Rôles ACL
Affectations ACL
Sudo
Politiques de mot de passe
Systèmes
Systèmes
Auto FS
Configuration
Configuration
Import / Export LDAP
Rapports
Tableau de bord
Mon compte
Utilisateur
Unix
Courriel
Politique de mot de passe

System Security Services Daemon

- **Outil libre écrit en C**
- **FreeIPA, RedHat**
- **Simplifier l’administration des accès de plusieurs postes**
- **Système de cache**


Network Boundary
Client
Client
Client
NSS Responder
PAM Responder
Cache
SSSD
Domain Provider 1
Domain Provider 2
Domain Provider ...
Domain Provider N
Identity Provider
Auth Provider
Identity Server
Auth Server

Ansible

- **Outil libre écrit en Python, PowerShell et Ruby / 2012**
- **RedHat et Ansible**
- **Configurer et gérer des ordinateurs à distance**
- **SSH / sans agent**
- **Format YAML**

Ansible

Extrait de playbook

```
- hosts: astromas
 tasks:
        - name: Install packages
          apt:
                name: "{{item}}"
          with_items:
                - sssd
                - sssd-tools
        - name: Send configuration files
          copy:
                src: "./files/{{item.file}}"
                dest: "{{ item.dest }}"
          with_items:
                - { file: sssd.conf, dest: /etc/sssd/sssd.conf, mode: '0600' }
                - { file: nsswitch.conf, dest: /etc/nsswitch.conf, mode: '0644' }
```

Conclusion et perspectives

- **Acquisition de nouvelles compétences (LDAP, Ansible)**
- **Développement de nouvelles méthodes de travail**
- **Découverte des enjeux d’une solution d’authentification centralisée**