La suite logicielle FusionDirectory : modernisez votre gestion des identités avec des logiciels libres

AGENDA DE LA CONFÉRENCE

Benoit Mortier

- Fondateur et CEO de FusionDirectory
- Spécialiste de la gestion des identités avec des logiciels libres

- Présentation de la société FusionDirectory
- La suite logicielle FusionDirectory
- FusionDirectory
  - ✔ Améliorer la gestion quotidienne
- FusionDirectory API
  - ✔ Une API qui favorise l'extensibilité
- FusionDirectory Webservice
  - ✔ Améliorer le provisioning
- FusionDirectory Orchestrator
  - ✔ Automatiser et sécuriser
- Cas Concrets
- Pour découvrir la suite Logicielle FusionDirectory

Présentation de la société FusionDirectory

Présentation de la société FusionDirectory

- Éditeur de FusionDirectory
- Spécialiste de la gestion des identités pour l'enseignement et les services publics
- Expert sur les logiciels libres de gestion des identités
- Expert Enseignement Supérieur et Recherche, SupAnn, PARTAGE, workflow, applications métiers.
- Formations sur les logiciels libres de gestion des identités et les bonnes pratiques

La suite logicielle FusionDirectory

La suite logicielle FusionDirectory

La suite logicielle FusionDirectory est composée de plusieurs éléments

- FusionDirectory : Application de gestion des identités
- FusionDirectory Orchestrator : Orchestrateur en API REST
- FusionDirectory Orchestrator client : client qui donne les ordres a FusionDirectory Orchestrator
- FusionDirectory Integrator : librairies base niveau sur laquelles sont construits tout les outils

FusionDirectory : application de gestion des identités

- Gestion utilisateurs, groupes, rôles, politique de sécurité
- Gestion des systèmes de messagerie, cyrus, dovecot, zimbra
- Support complet de la norme SupAnn, Sinaps, PARTAGE de RENATER
- Contrôle d'accès fin pour délégation de tâches
- Modèles personnalisables pour l'approvisionnement des données
- Triggers sur action d'édition, modification, effacement, vérification
- Moteur de Workflow qui inclut cycle de vie, notifications, groupes automatiques, archive etc...
- Webservice REST
- Support CAS, LemonLDAP::NG, WebAuthn, Yubico

FusionDirectory Orchestrator

FusionDirectory Orchestrator, le moteur de workflow de la suite logicielle FusionDirectory vous aide à sécuriser et automatiser votre gestion des identités.

Il vous fournit une possibilité de :

- Modéliser vos règles métier afin de les rendre dynamiques.
- Suivre les changements de statut, modifications.
- Surveillez et prévenir des changements non prévus.
- Automatiser votre gestion de groupes avec date de début et fin par utilisateurs.
- Archiver vos comptes pour éviter la réutilisation et respecter le RPGD
- Et plus encore ...

FusionDirectory Integrator

FusionDirectory Integrator, sont nos librairies sur lesquelles sont basés tout nos outils.

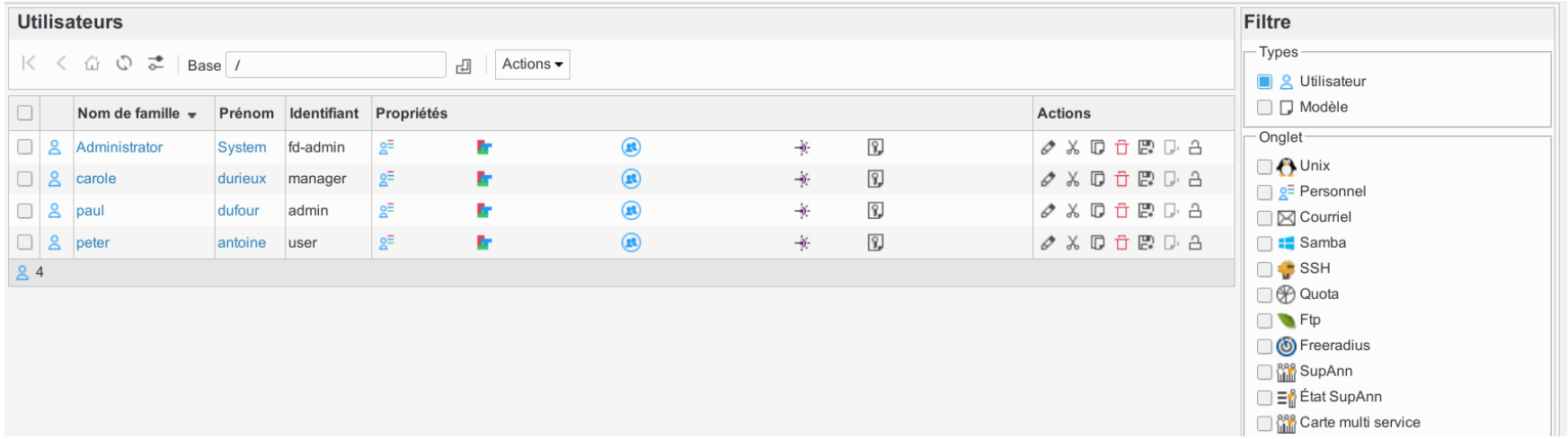
Elles vous fournissent des functions pour :

- Lire la configuration de FusionDirectory.
- Interagir avec OpenLDAP ses schémas et ses données.
- Manipuler les objets audits.
- Utiliser notre API REST.
- Et plus encore ...

FusionDirectory : améliorer la gestion quotidienne

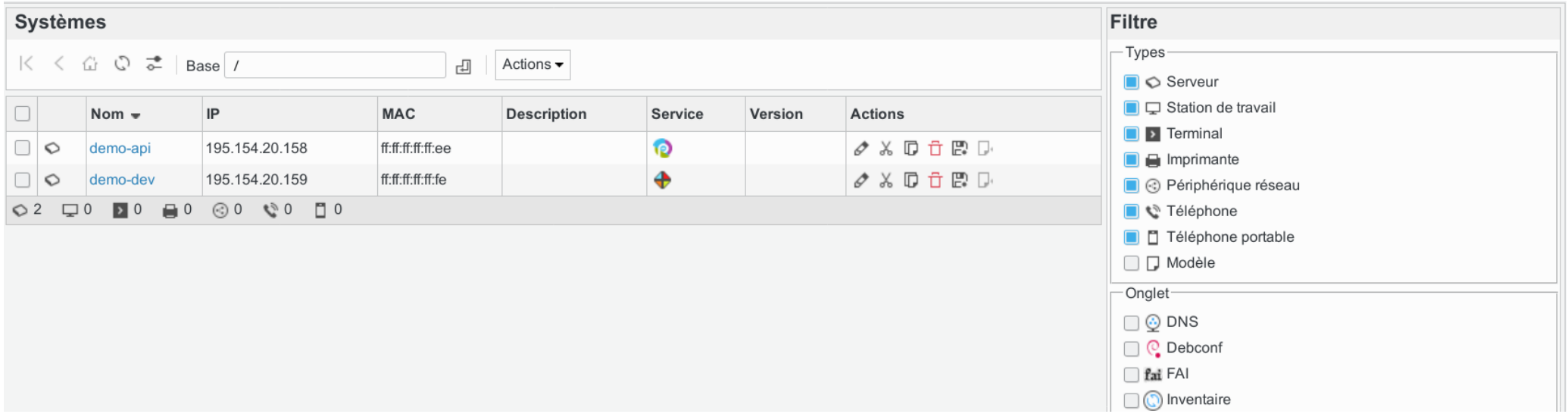
Utilisateurs, groupes, rôles

- Création d'utilisateurs, de groupes et de rôles
- Gestion de mot de passe standard ou basé sur ppolicy
- Modèles utilisateur, création des utilisateurs pré-configurés
- Importation et création en bloc avec prise en charge de modèles
- Snapshots, restaure les entrées après modification
- Copier coller pour la création facile de nouveaux utilisateurs, groupes



Systèmes et services

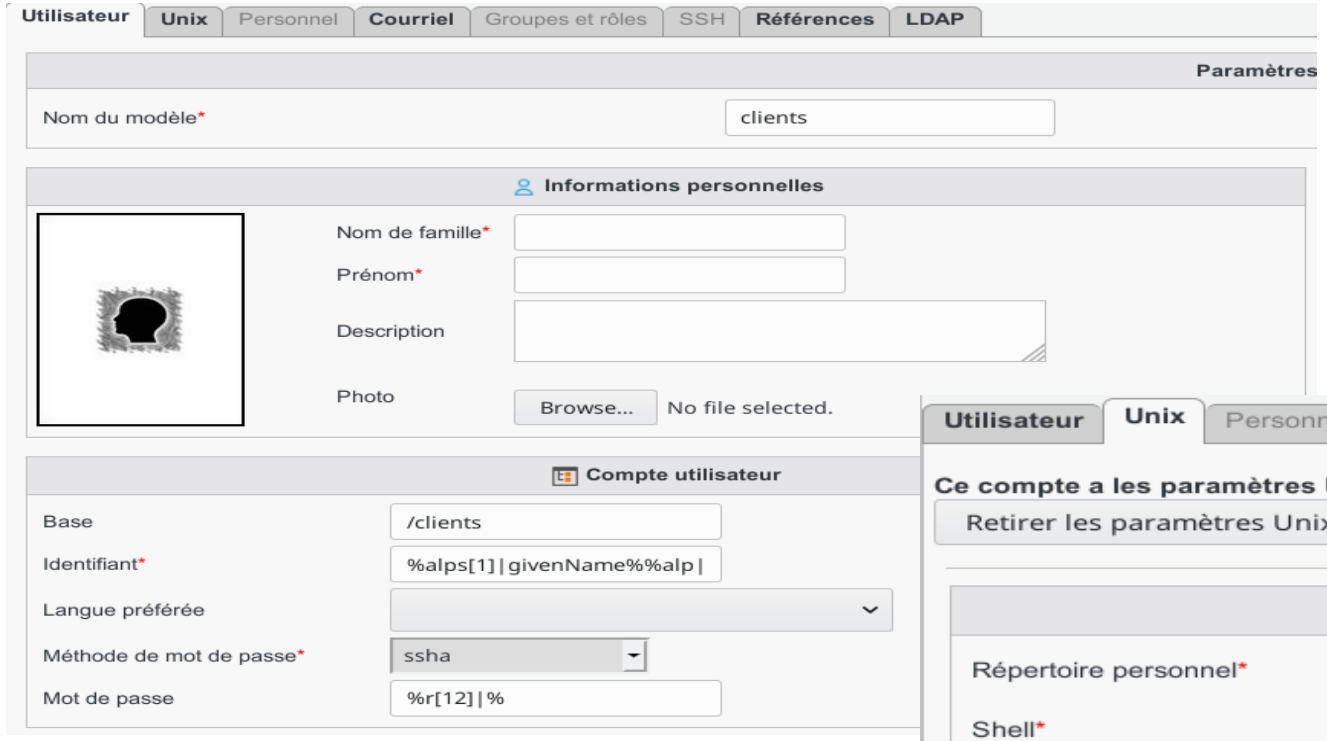
- Création de systèmes : serveurs, pc, terminaux, téléphone mobile, périphériques réseau
- Services réseaux : DHCP, DNS, Autofs, IPAM
- Outils de déploiement: FAI, OPSI, Debconf
- Services de messagerie : Cyrus, Dovecot, Zimbra, PARTAGE, SOGo

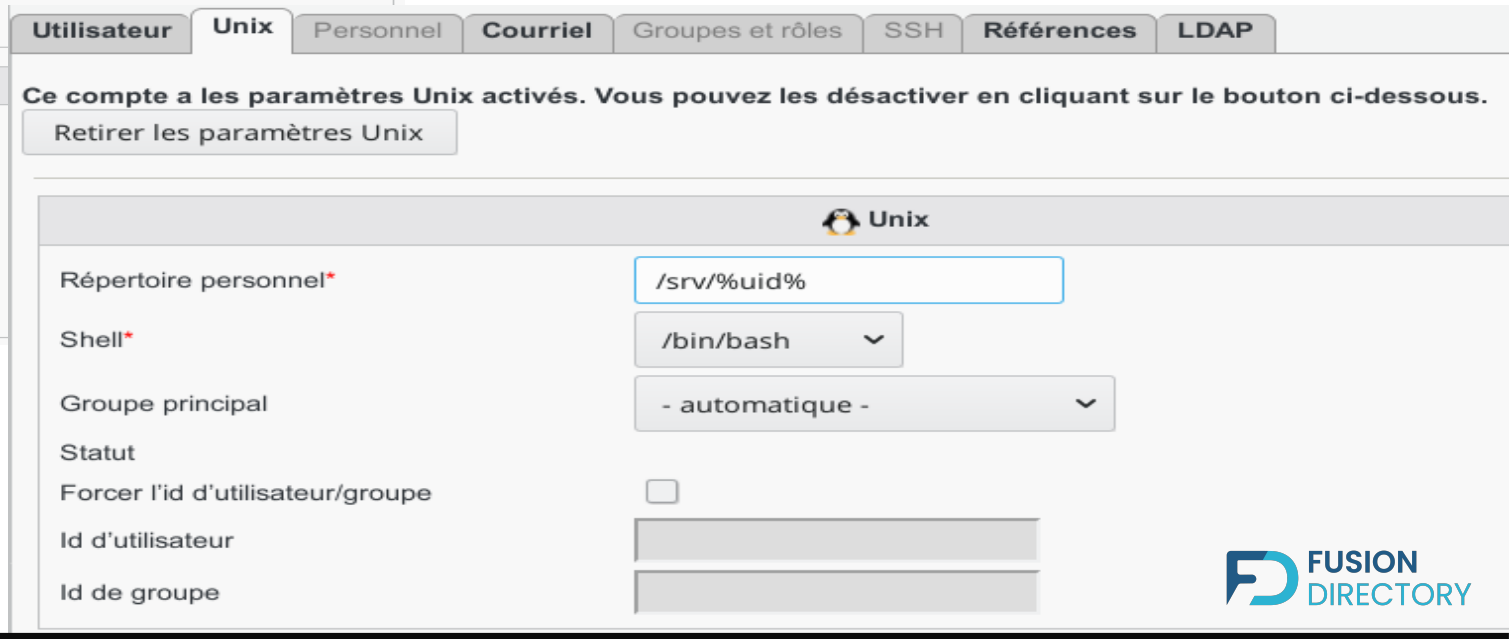


Modèles et macros

- Définissez précisément comment les attributs seront construits, majuscules, minuscules, première lettre d'un attribut + 4 lettres d'un autre attribut etc..
- Remplissez des attributs en fonction de la valeur d’autres attributs
- Générer des mots de passe aléatoires suivant un ensemble de règles
- Calculer la date et l'heure d'expiration du compte
- Et bien plus encore ...

Modèles et macros

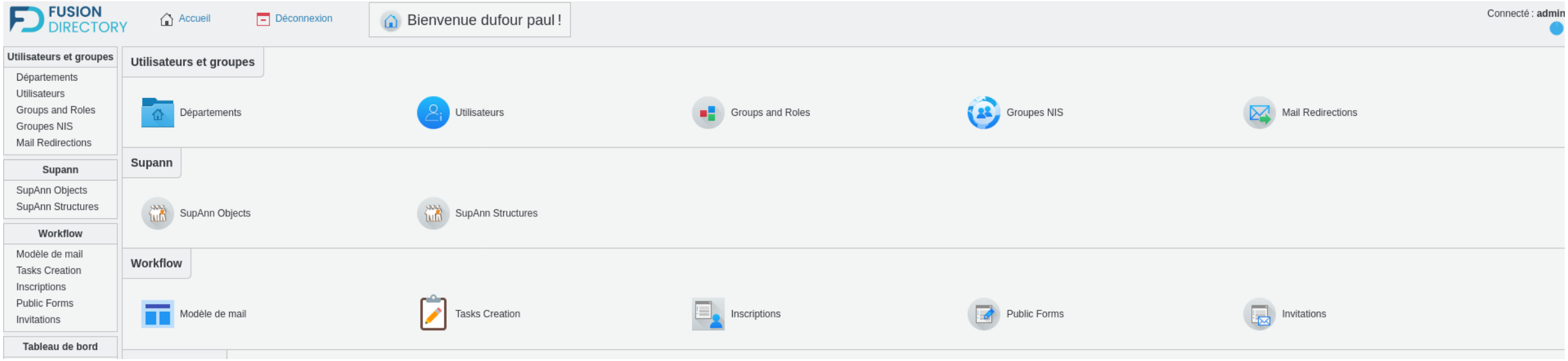


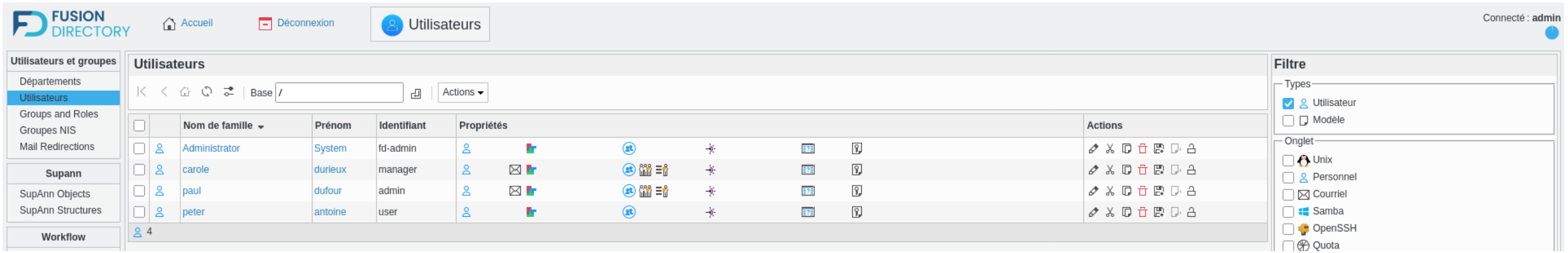


Délégation : le système de contrôle d’accès

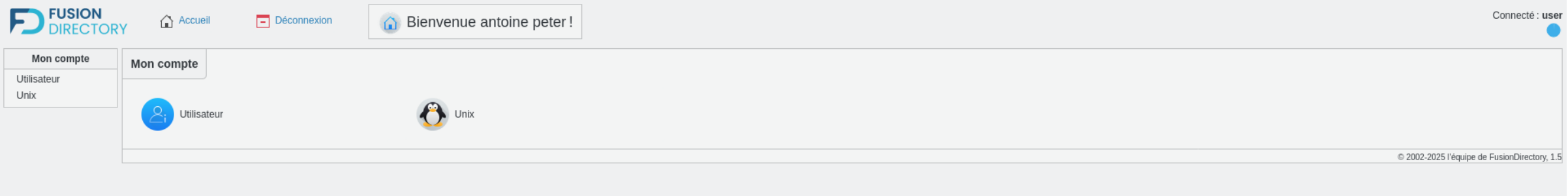
- Donner des droits sur le contenu de FusionDirectory à d'autres utilisateurs que l'administrateur
- Cacher les données non accessibles en ne montrant à l’utilisateur que ce qu’il est autorisé à voir
- Permettre à un chef de projet d'éditer les utilisateurs de son équipe.
- Avoir une vue en lecture seule

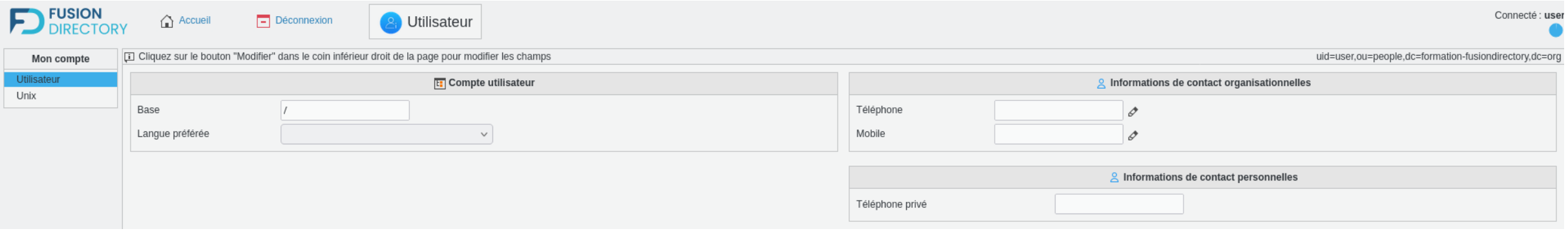
Délégation : Vue de l'utilisateur admin



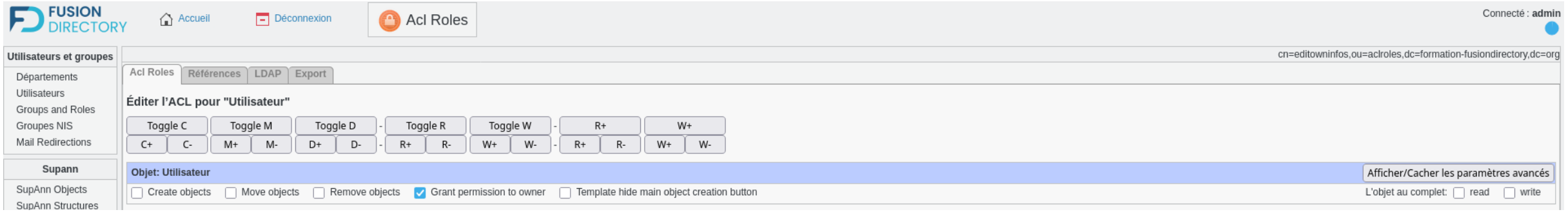


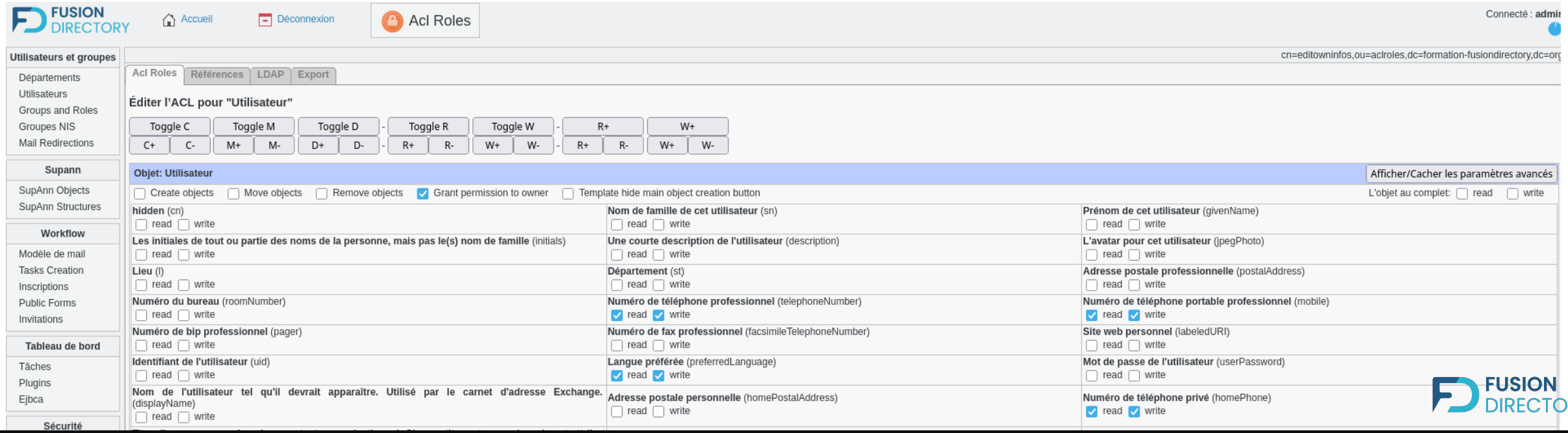
Délégation : Vue de l'utilisateur user





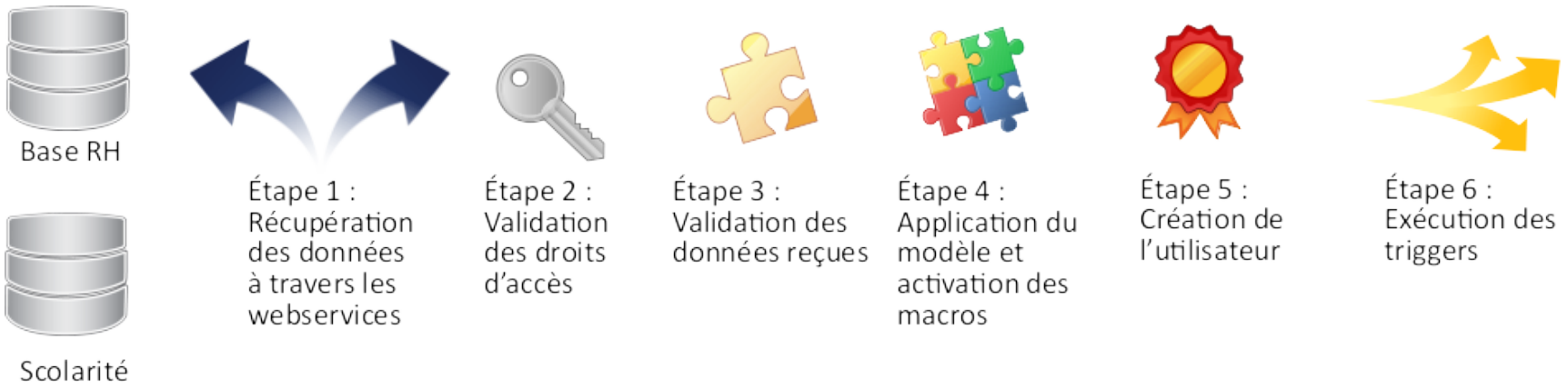
Délégation : le système de de contrôle d'accès





Le webservice REST

- Le webservice REST permet l'intégration de la gestion des identités avec des applications tierces de manière plus fluide
- L'utilisation des modèles permet de construire des process de provisionnement qui valident les données
- Le déclenchement des triggers permet des actions supplémentaires



Les triggers

- Il existe de nombreux cas où on désire déclencher des actions après la création, la modification ou la vérification de données
- Dans le cas de FusionDirectory, une liberté totale est laissée en ce qui concerne l'écriture des triggers
- Cela peut être utilisé pour appeler d'autres webservices ou déclencher des processus de synchronisation avec d'autres applicatifs

Étape 1 : Création du compte

Étape 2 : Exécution des triggers

Étape 3 : insertion dans ActiveDirectory

Norme SupAnn

Norme SupAnn

La norme SupAnn est la morme de l'enseignement supérieur recherche pour le stockage de données dans un annuaire.

La grande force de cette norme c'est que bien qu'elle soit initialement prévu pour l'enseignement, c'est une norme ouverte et qui formalise l'ensemble des problèmatiques de gestion des identités

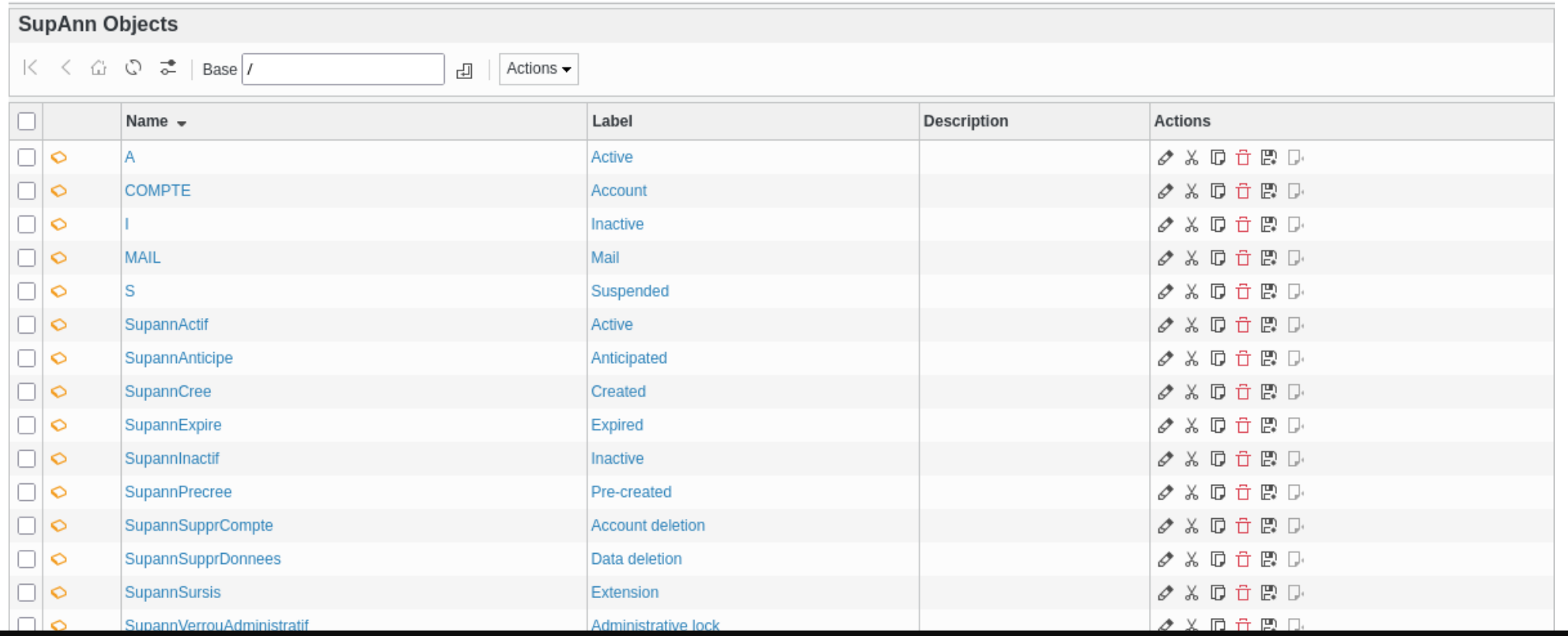
- Gestion des etablissements et des entités.
- Données administratives et techniques par rapport à un utilisateur.
- Gestion du cycle de vie du compte basée sur des ressources attribuables par utilisateur et permettant une gestion différenciée de chacune de ces ressources.
- Consentement utilisateur vis a vis de ses données et services.
- Code Population pour définir plus finement les différentes populations d'usagers.

Structures

Les structures dans la norme supann définissent les etablissement et les entités. Ce qui dans peut être traduit par site et services si on adopte un langage plus commun

SupAnn Objects

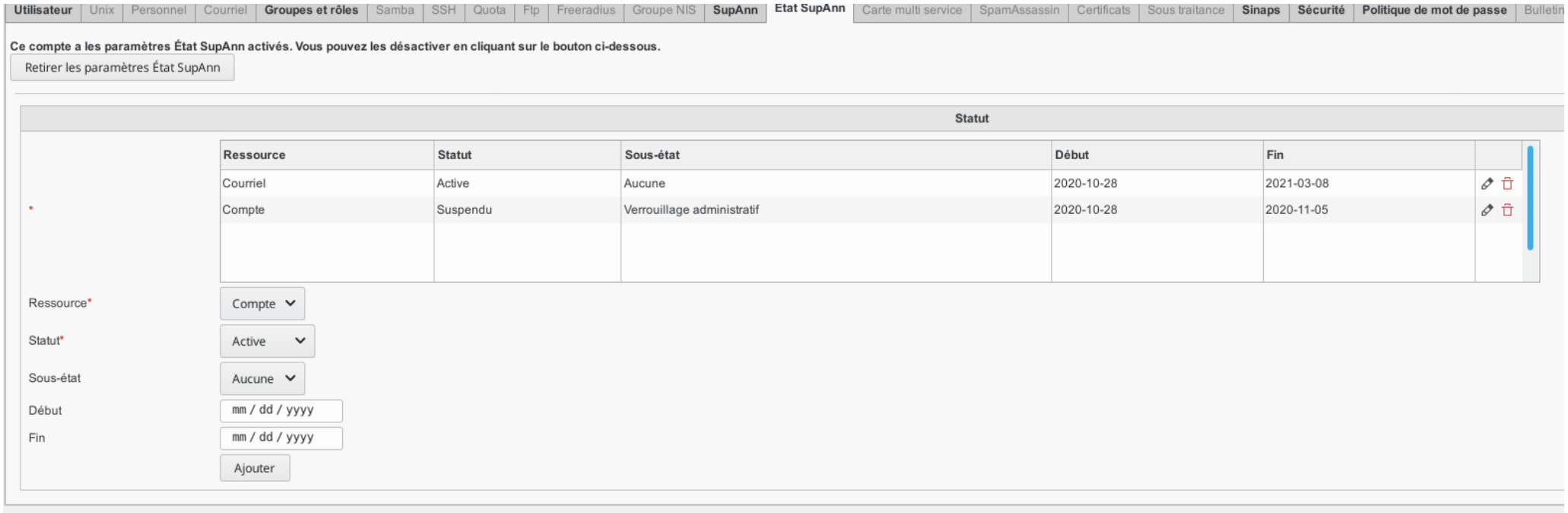
Supann Objects : concept de ressources avec état, sous état



Name	Label	Description	Actions
A	Active		
COMPTE	Account		
I	Inactive		
MAIL	Mail		
S	Suspended		
SupannActif	Active		
SupannAnticipe	Anticipated		
SupannCree	Created		
SupannExpire	Expired		
SupannInactif	Inactive		
SupannPrecree	Pre-created		
SupannSupprCompte	Account deletion		
SupannSupprDonnees	Data deletion		
SupannSursis	Extension		
SupannVerrouAdministratif	Administrative lock		

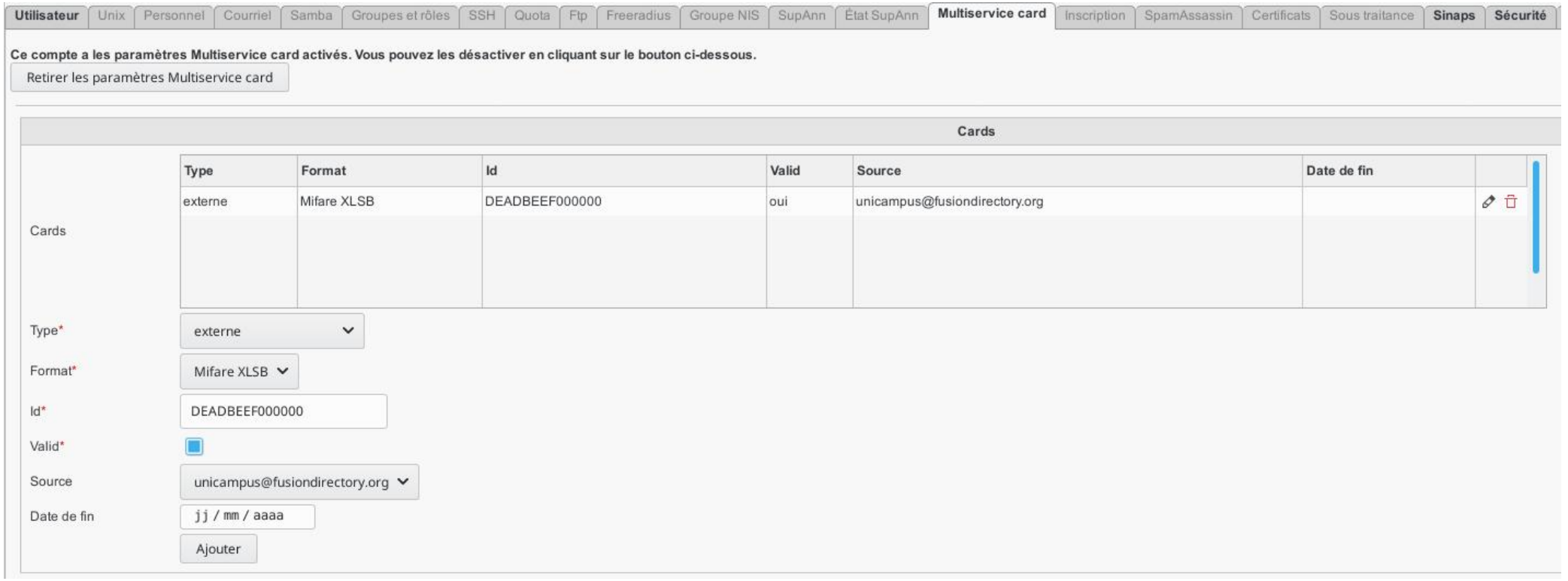
Cycle de vie

- Les ressources sont attribuables par utilisateur et permettent une gestion différenciée
- Des status et sous status permettent d'affiner l'etat d'une ressource.
- Une date de debut et une date de fin sur chaque ressource permettra de déclancher des actions preprogrammées



Carte Multi service

- On entend par carte multi-service, une carte combinant badge d'accès physique, carte de cantine, carte de bibliothèque, le tout sur un même support
- Le stockage de ces données dans la gestion des identités marque un tournant car jusqu'à présent seul le logiciel de création de carte possédait ces données



FusionDirectory API : favoriser l'extensibilité

L’api de FusionDirectory : simplePlugin

Lors des réflexions autour de la naissance de FusionDirectory, la question d’une API propre s’est imposée.

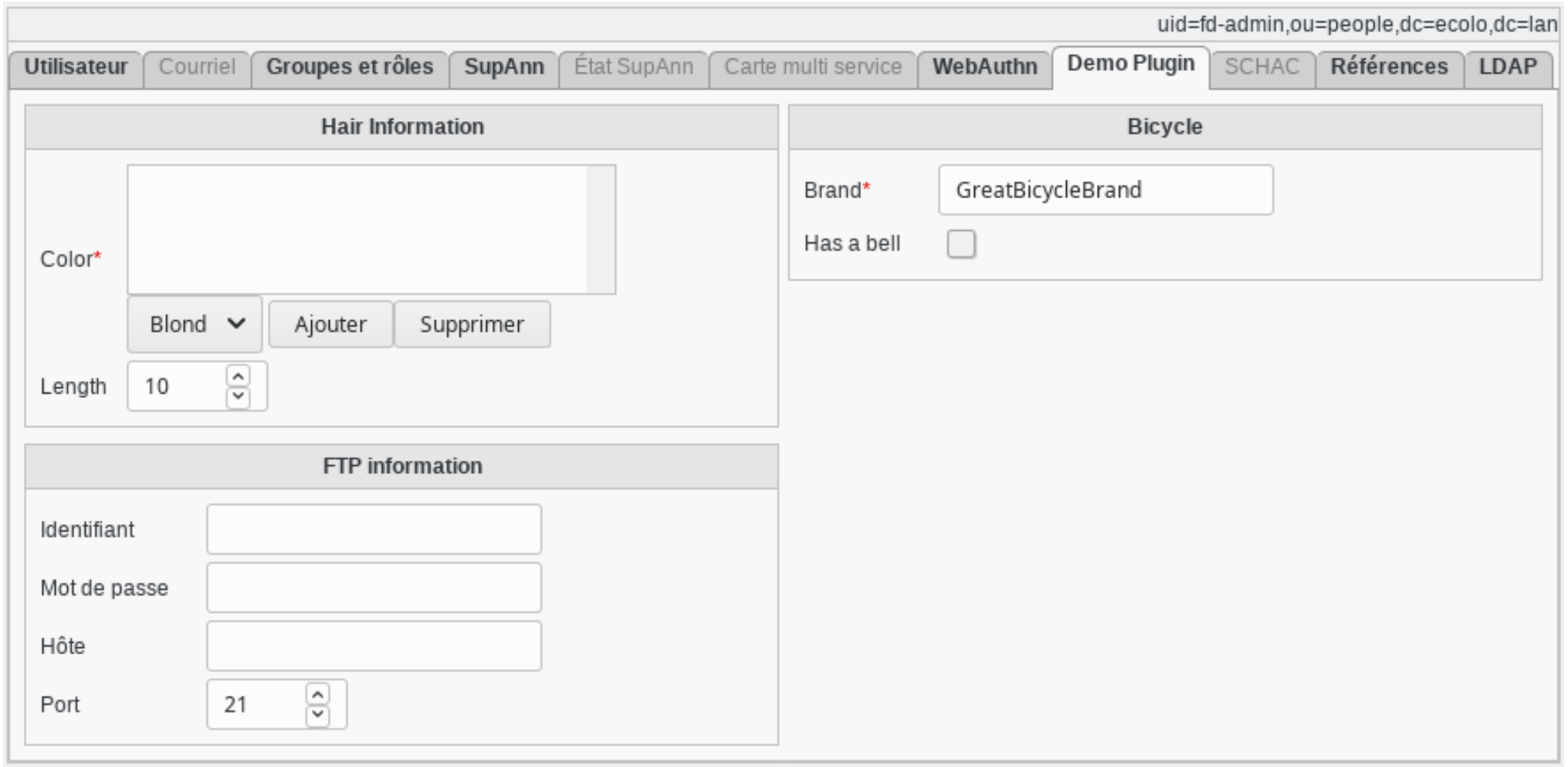
Parmi ses fonctionnalités les plus importantes on retrouve :

- Faciliter via une couche d’abstraction le stockage dans un annuaire LDAP
- Construire automatiquement l’interface graphique de manière simple et automatique
- Gérer automatiquement les acls de FusionDirectory sans écrire de code supplémentaire
- Fournir un ensemble d’attributs pour simplifier l’écriture de plugins gérant des données complexes

Plugin de demonstration : code

```php
<?php
// The main function : information about attributes
static function getAttributesInfo ()
{
  return [
    // Attributes are grouped by section
    'section1' => [
      'name'  => _('Hair Information'),
      'attrs' => [
        new SetAttribute(                    // This attribute is multi-valuated
          new SelectAttribute (
            _('Color'),                      // Label of the attribute
            _('Color of the hair'),          // Description
            'hairColor',                     // LDAP name
            TRUE,                            // Mandatory
            ['blond','black','brown'],       // [SelectAttribute] Choices
            '', // We don't set any default value, it will be the first one
            ['Blond','Black','Brown']        // [SelectAttribute] Output choices
          )
        ),
```

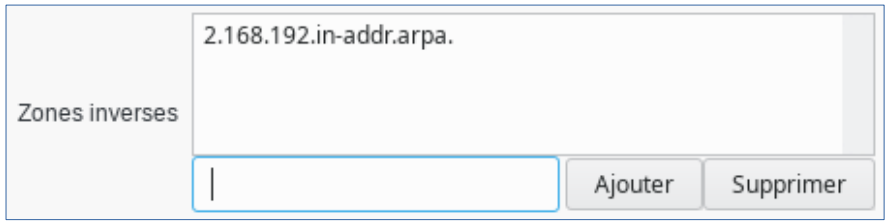
Plugin de demonstration : affichage



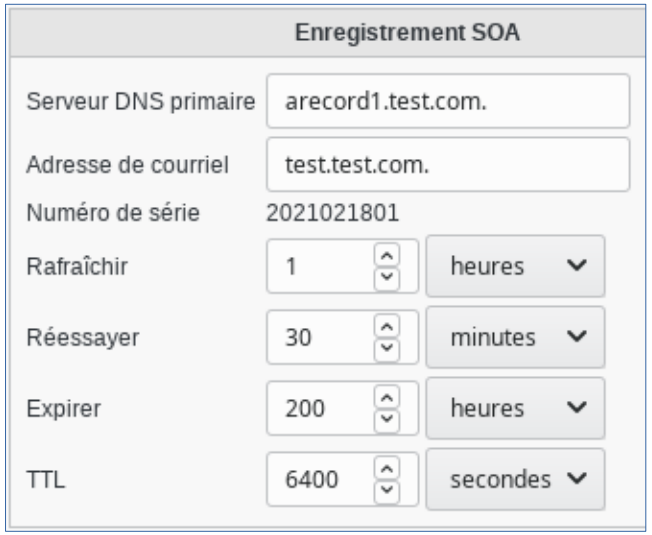
Attributs avancés

- Le SetAttribute englobe un attribut pour le rendre multivalué.
- Le CompositeAttribute permet de découper un seul attribut LDAP en plusieurs attributs dans l'interface.
- Un ObjectsAttribute permet de choisir des objets via une fenêtre de gestion.

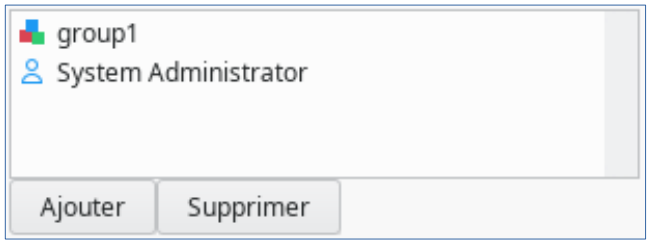
SetAttribute



CompositeAttribute



ObjectsAttribute



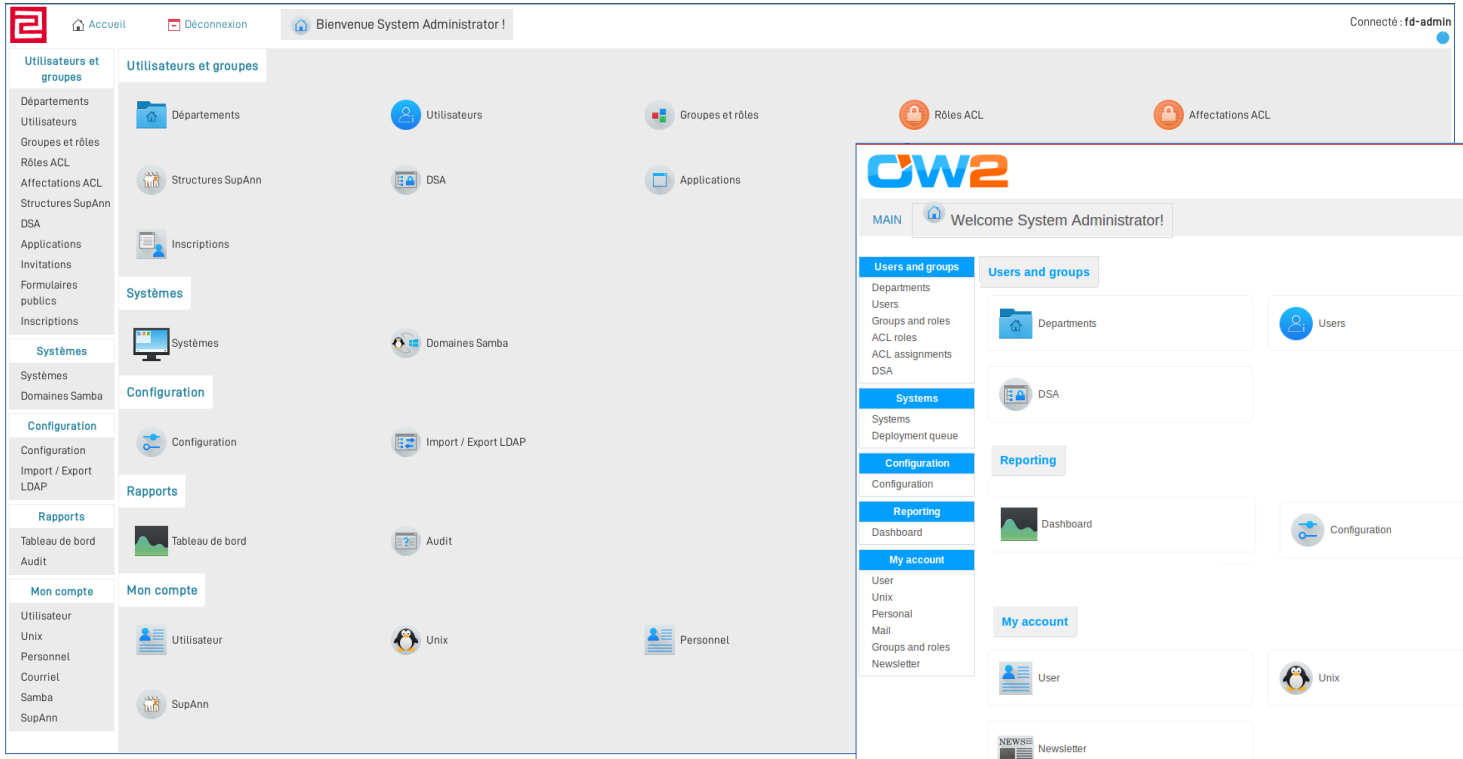
Clefs étrangères

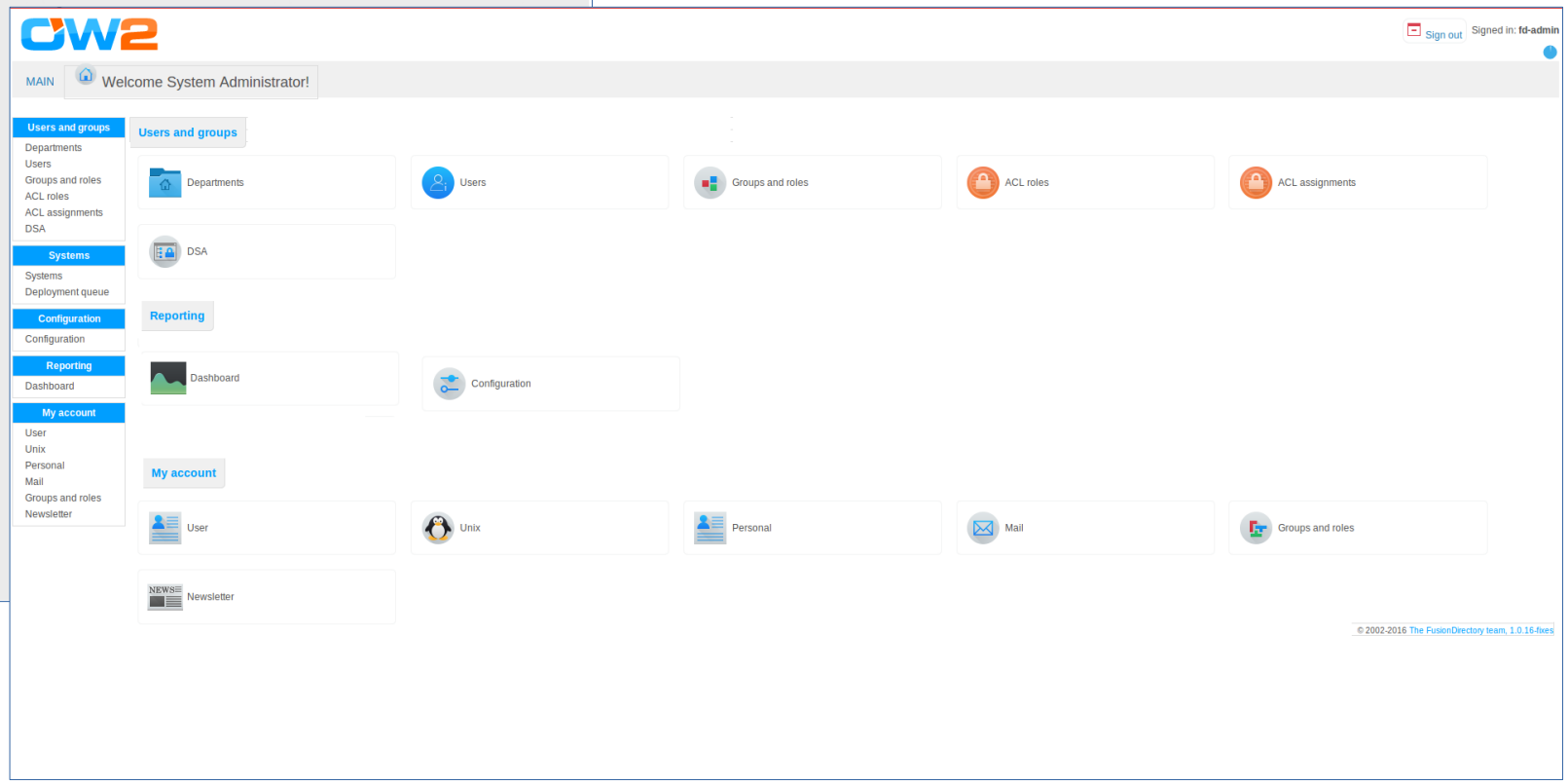
- La valeur de l'attribut sera mise à jour si l'objet référencé est modifié
- Le lien apparaîtra dans l'onglet références de l'objet référencé.

Thèmes de FusionDirectory

- FusionDirectory possède un système de thème permettant de personnaliser l'interface
- Un thème peut contenir des icônes, des fichiers CSS, et des templates smarty
- Pour tout fichier manquant dans un thème, le fichier du thème par défaut est utilisé en remplacement
- Pour les icônes, les normes freedesktop sont utilisées donc les thèmes d'icônes standards peuvent être utilisés
- Pour le CSS, le thème par défaut breezy possède des sources au format LESS, permettant de facilement générer des variations de couleurs, polices ou taille de texte
- Le fichier theme.css est vide par défaut et peut servir pour les petits ajouts

Thèmes de FusionDirectory

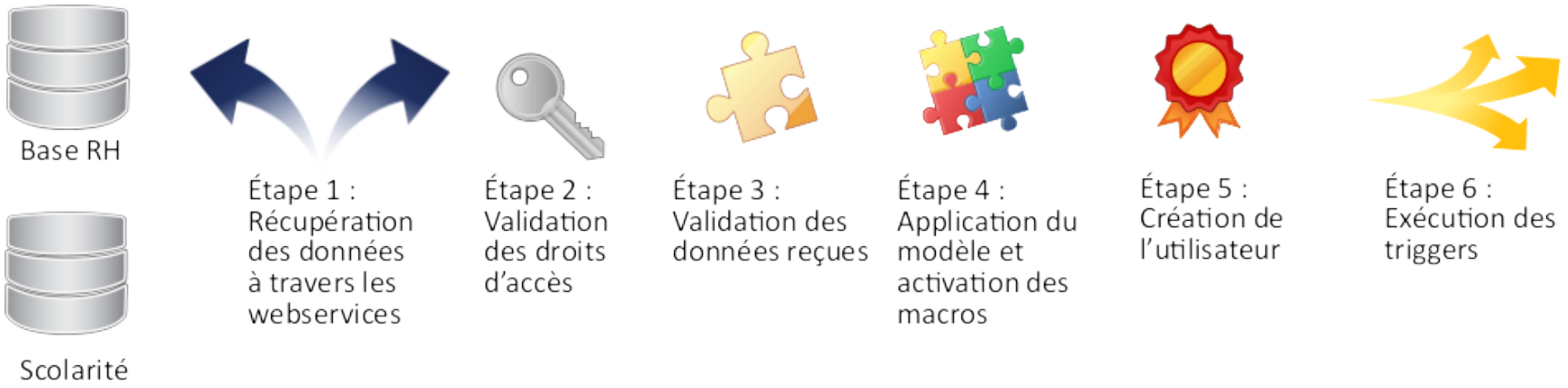




FusionDirectory Webservice : Améliorer le provisioning

Le webservice REST

- Le webservice REST permet l'intégration de la gestion des identités avec des applications tierces de manière plus fluide
- L'utilisation des modèles permet de construire des process de provisionnement qui valident les données
- Le déclenchement des triggers permet des actions supplémentaires



La spécification OpenAPI

- Le webservice REST propose un fichier au format OpenAPI qui liste les opérations disponibles
- Certains clients supportent directement ce format pour générer des requêtes
- La documentation officielle est générée depuis ce fichier et disponible sur https://rest-api.fusiondirectory.org/
- Le fichier est disponible depuis votre installation, les champs sont dynamiquement adaptés pour refléter votre configuration : https://<hote>/fusiondirectory/rest.php/v1/openapi.json

Exemples d’appels au webservice

GET /objects/user?base=ou=branche,dc=example,dc=com

- { "uid=login,ou=people,dc=example,dc=com": "login" }

GET /objects/user/uid=login,ou=people,dc=example,dc=com/posixAccount/uidNumber

- 1012

PUT /objects/user/uid=login,ou=people,dc=example,dc=com/posixAccount/uidNumber

1000

- uid=login,ou=people,dc=example,dc=com

Exemples d’appels au webservice

GET /types/user/mailAccount

```
{ "sections": {
      "main": {
         "name": "Mail account",
         "attrs": [
            "mail",
            "gosaMailServer",
            "gosaMailQuota"
         ]
      },
...
}
```

FusionDirectory Orchestrator : Automatiser et sécuriser

Situation actuelle

La gestion des identités nous permet d'organiser toutes les informations fonctionnelles de l'utilisateur.

Cependant, une multitude de problèmes subsistent.

- Supann est une vue statique, mais comment la rendre dynamique ?
- Comment automatiser les changements sur les ressources en fonction des règles métier ?
- Comment suivre les changements sur les données d'une personne, d'un groupe de personnes ?
- Comment mettre en place des processus dynamiques, comme des envois de fiches de comptes, par exemple ?

La bonne gestion du cycle de vie

La création et la mise a jour des comptes est globalement bien géré

La désactivation est souvent mal conçue et dépend d'action semi-manuelle

La désactivation ne prend généralement pas en compte les différents actions nécessaire comme

- Archivage du home
- Désactivation et archivage de la boite de messagerie
- Assurance que tout les droits on bien été enlevés dans les applications externes non lapidifiés
- Archivage du compte numérique au regard de la RGPD
- Archivage du compte numérique au regard de la nom réutilisation de certaines données sensible, email, uid, samAccountName etc...

Problématiques

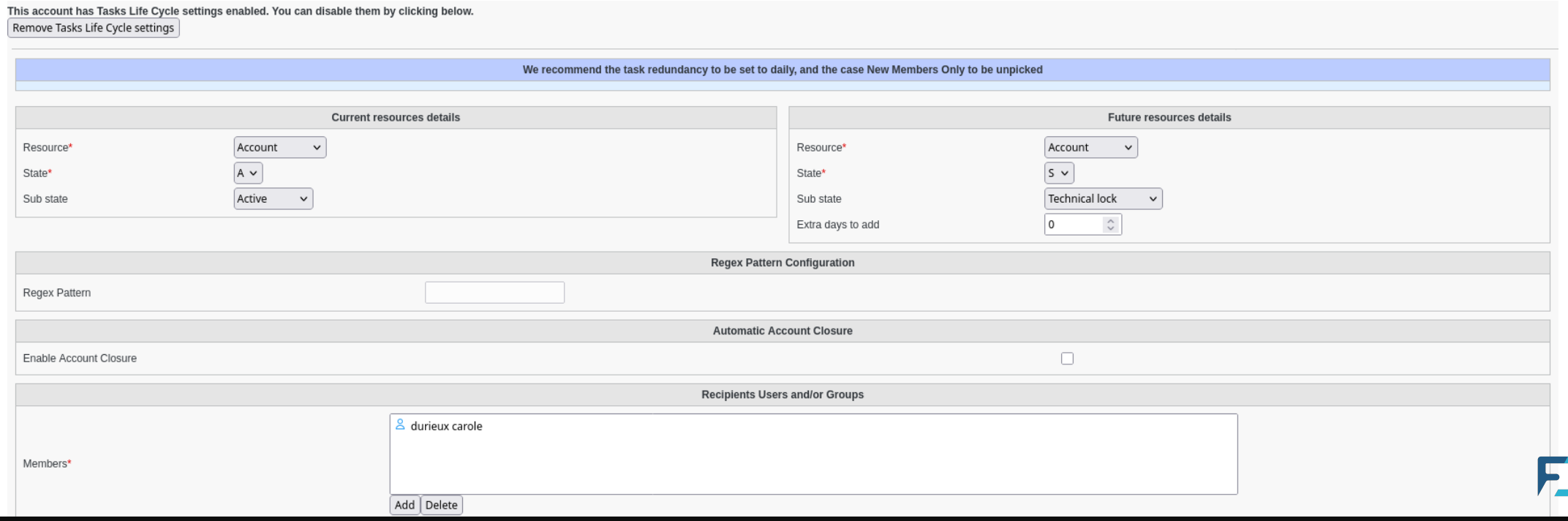
Jusqu'à présent, vous devez développer l’ensemble des interactions avec les données.

Cela implique de développer des scripts qui appellent les webservices de FusionDirectory afin d’automatiser le cycle de vie des comptes numériques, par exemple.

Il faut donc maintenir ce code sur le long terme et l’adapter à chaque changement, ce qui peut être lourd et couteux sur le long terme.

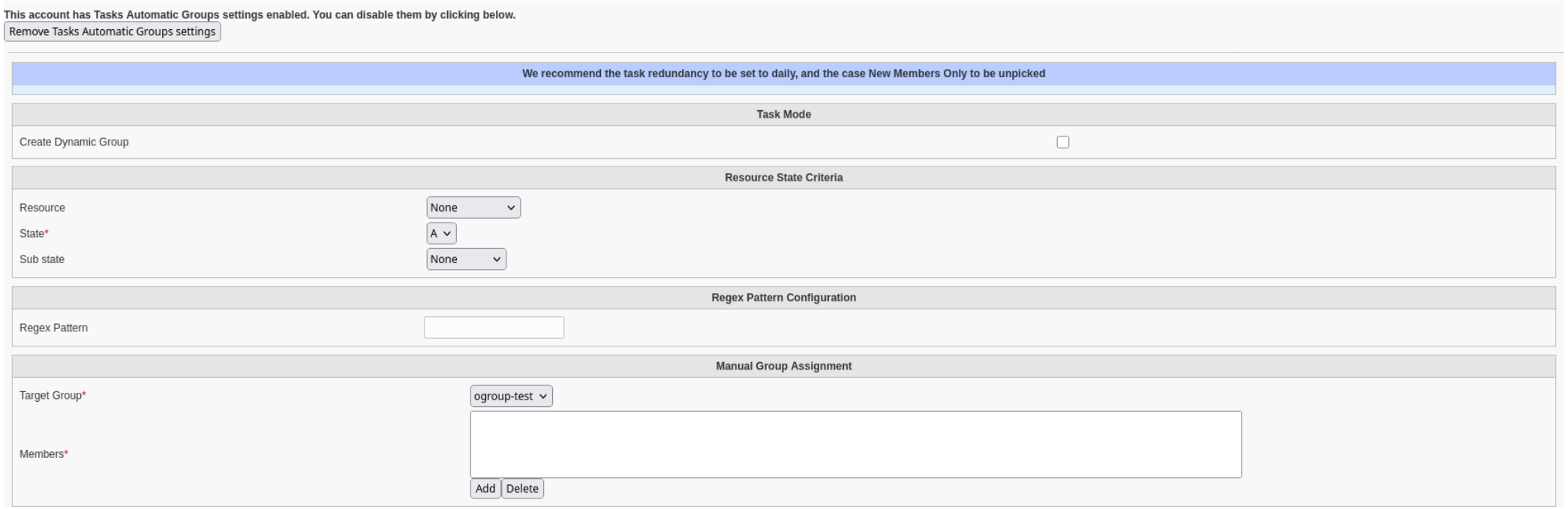
Cycle de vie

- Modélisation des règles métiers du cycle de vie
- Changement du statut des ressources supann sur une personne ou un groupe de personnes
- Fermeture automatique de compte sur base de calcul de ressources restantes.



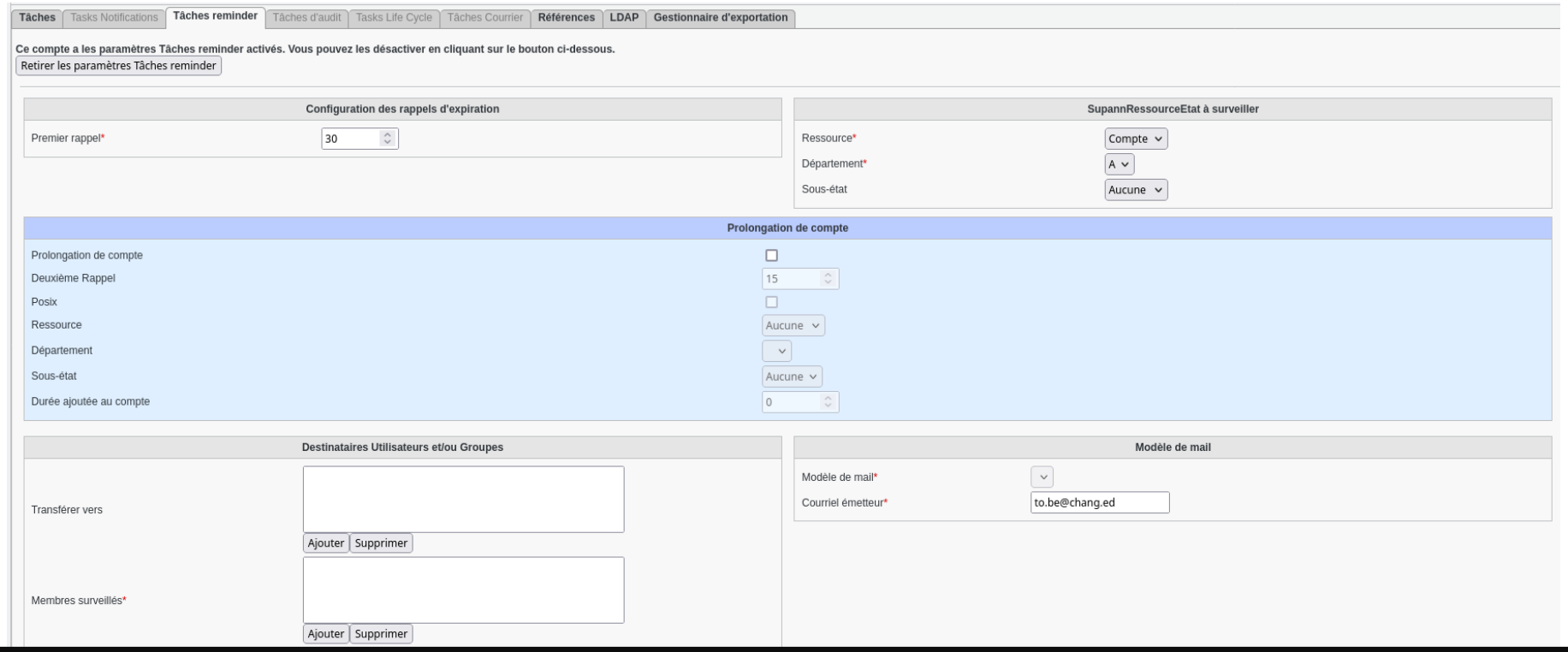
Automatic groups

- Tache d'appartenance à des groupes en fonction de ressources supann
- Création de groupe dynamiques OpenLDAP grâce aux ressources (dyngroups)



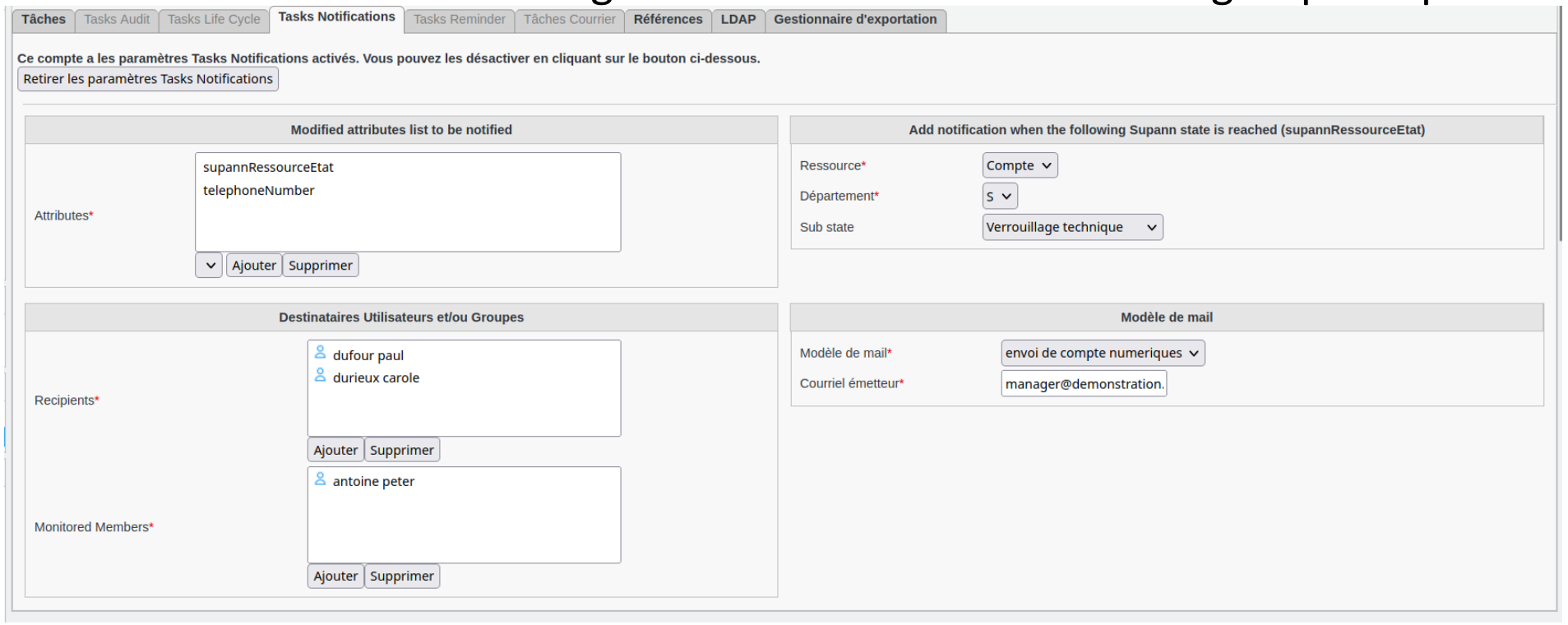
User-reminder : rappel d'expiration de compte

- Envoi d'un email x jours avant la date de fin de validité d'une ressource Supann
- Vérification de la validité d'un compte avec envoi de mail et attente de réaction de l'utilisateur qui doit cliquer sur un lien.



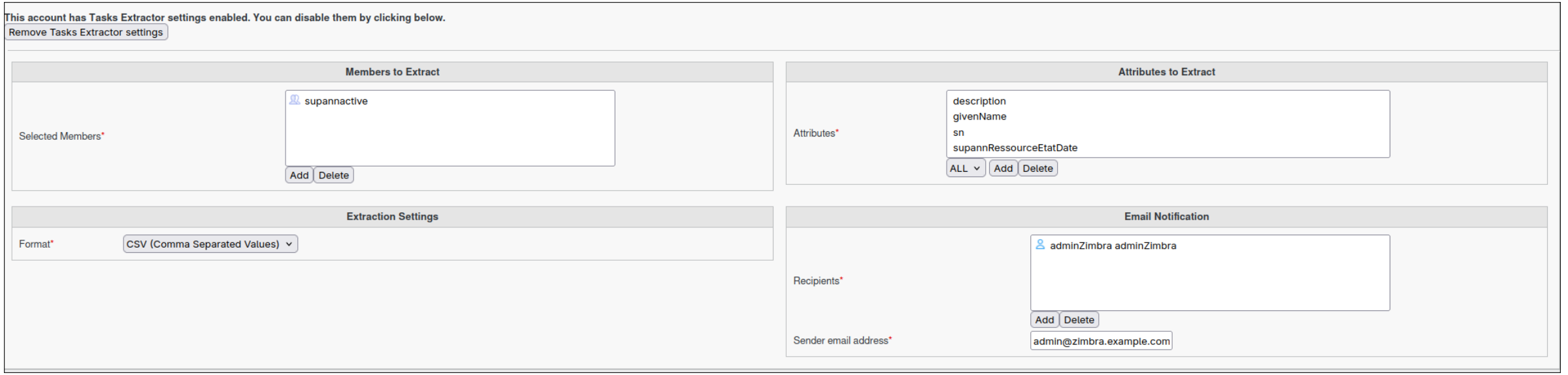
Notification

- Actions en fonction du changement du contenu d'un attribut d'une personne ou groupe de personnes
- Notification de suite au changement d'attributs sur un autre groupe de personnes



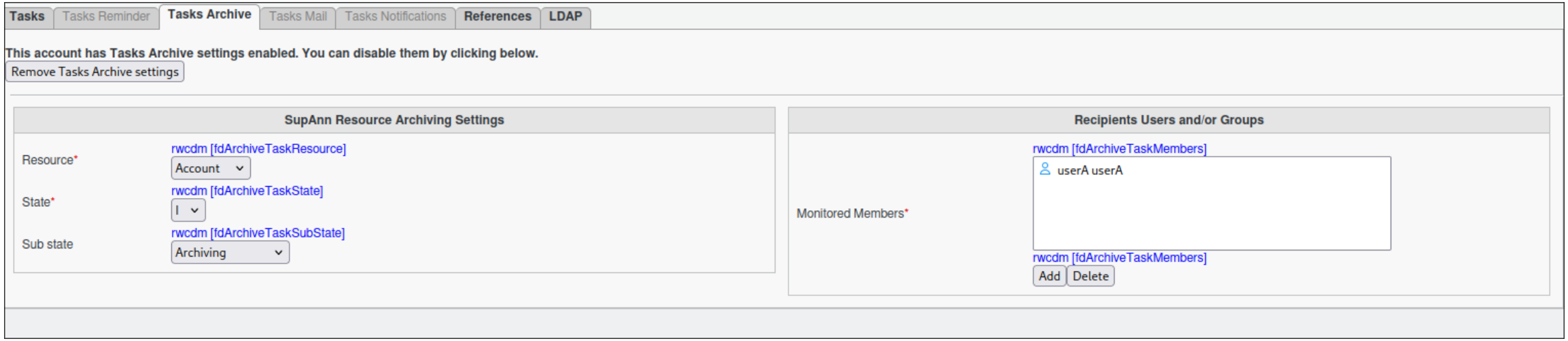
Exporter

Exportation de données de manière automatisée avec choix fin.



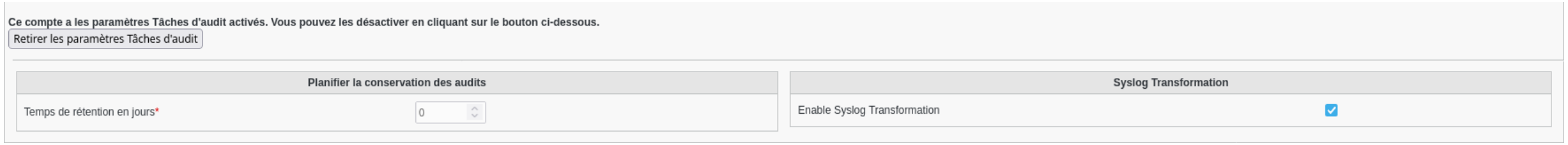
Archivage

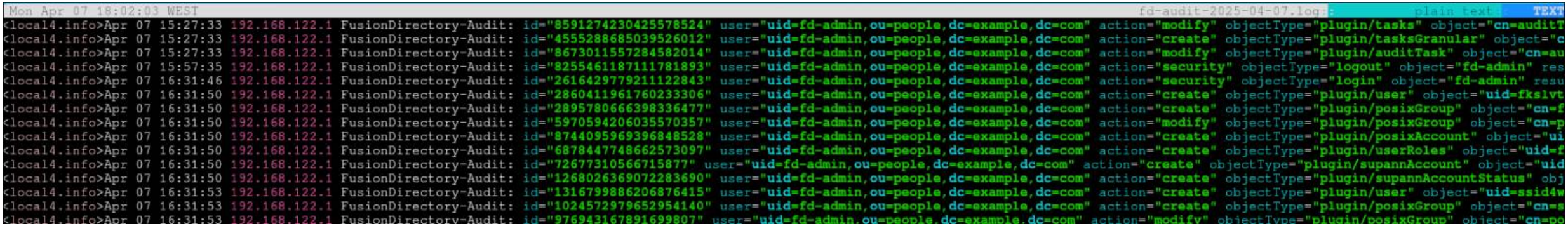
- Tache d’archivage



Audit + Syslog

- Tache de transformation des audit FusionDirectory en format syslog
- Suivi de la sécurité des accès en temps réels et agregation vers systeme de log centralisé.





Cas Concrets

FusionDirectory dans l’enseignement supérieur recherche

- Utiliser les webservices de FusionDirectory et les modèles afin de provisionner les utilisateurs par type dans toute leur complexité
- Utiliser les webservices de unicampus et FusionDirectory afin de propager les numéros de badges lors de leur création
- Utiliser les webservices de FusionDirectory afin d’archiver les comptes en fonction des statuts du cycle de vie

TELECOM SudParis

Application des modèles
- Mail
- SupAnn
- SupAnn cycle de vie
- SupAnn carte multi services

FUSION DIRECTORY

TELECOM SudParis

unicampus

Contrôle d'accès

Insertion du numéro de série du badge de l'utilisateur

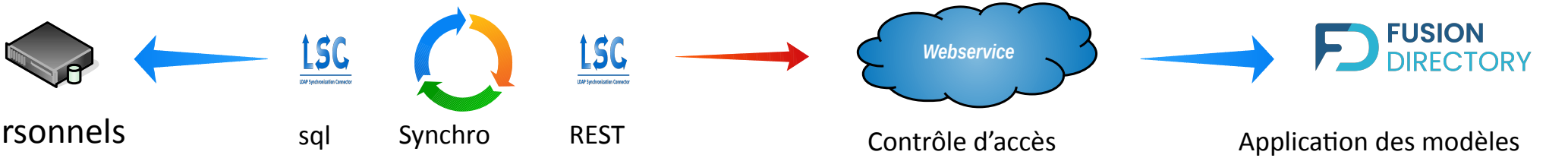
- SupAnn carte multi services

RENATER
CONNECTEUR DE SAVOIRS

- Utiliser les webservices de FusionDirectory et les modèles afin de provisionner les utilisateurs par type depuis les bases métiers
- Créer automatiquement les comptes et groupes utilisateurs dans samba 4
- Créer automatiquement les boites et groupes de messagerie dans PARTAGE de RENATER

FUSION DIRECTORY

RENATER
CONNECTEUR DE SAVOIRS



Personnels — sql — Synchro — REST — Contrôle d'accès

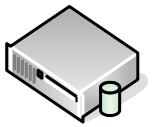
Application des modèles
- SupAnn
- SupAnn cycle de vie
- Samba 4
- Mail - Partage de Renater

- Utiliser les webservices de FusionDirectory et les modèles afin de provisionner les utilisateurs par type dans toute leur complexité
- Propager les mots de passe dans 3 ActiveDirectory différents
- Créer les fiches de contact utilisateurs Office 365

UNIVERSITÉ DE NAMUR

Personnels

Étudiants



Contrôle d'accès

FUSION DIRECTORY

Création d'utilisateurs
Création Fiche Office 365

Synchronisation mot de passe

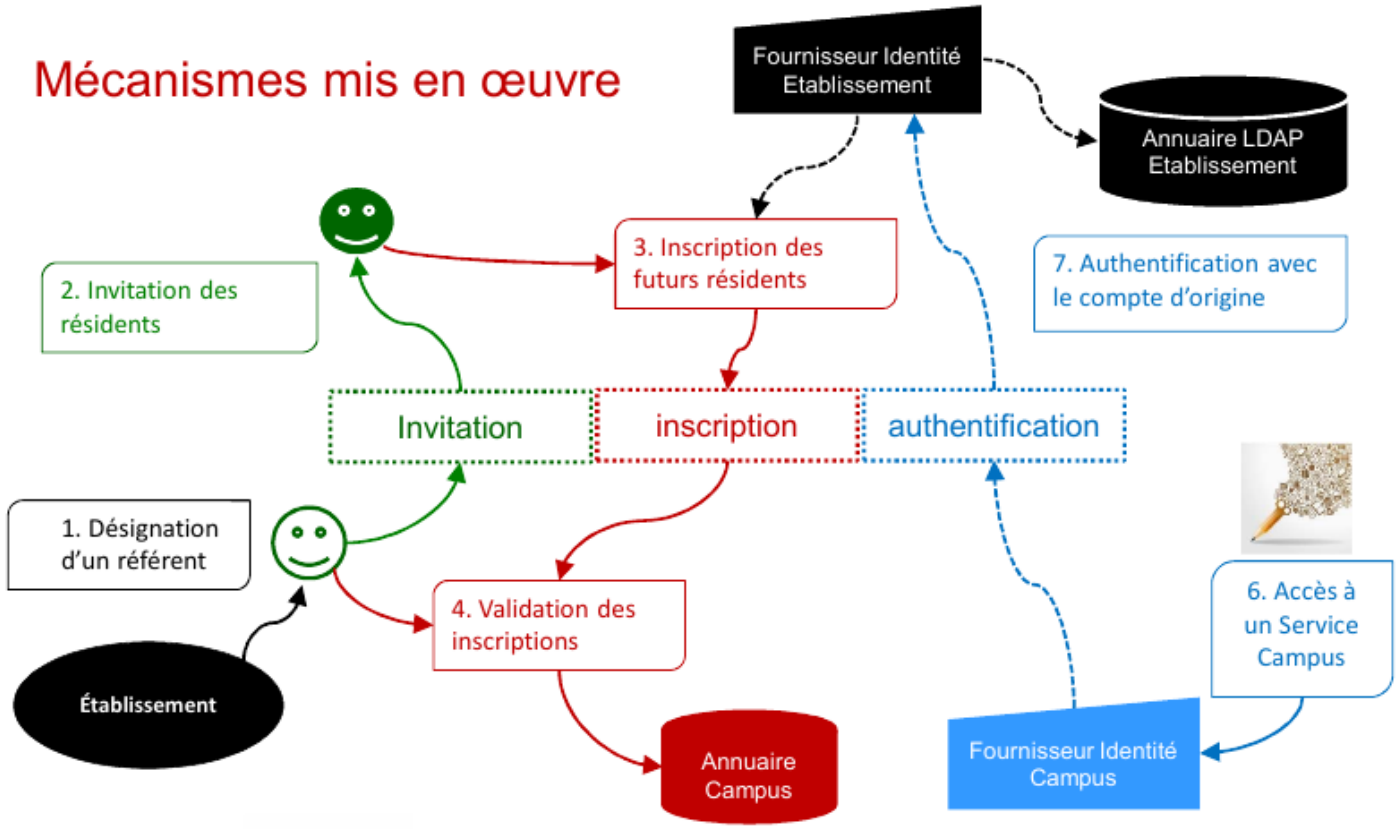
FUSION DIRECTORY

CAMPUS CONDORCET
Paris–Aubervilliers

- Nouveaux campus comprenant des personnels et étudiants de 11 etablissements
- Garder le lien d'affiliation avec son université d’origine
- Ne pas créer de nouvelle identité pour les utilisateurs
- Respecter la RGPD
- Déployer un système d'inscription et d'invitation
- Utiliser les standards de l'enseignement supérieur recherche et de la fédération européenne Edugain

CAMPUS CONDORCET
Paris–Aubervilliers

Mécanismes mis en œuvre

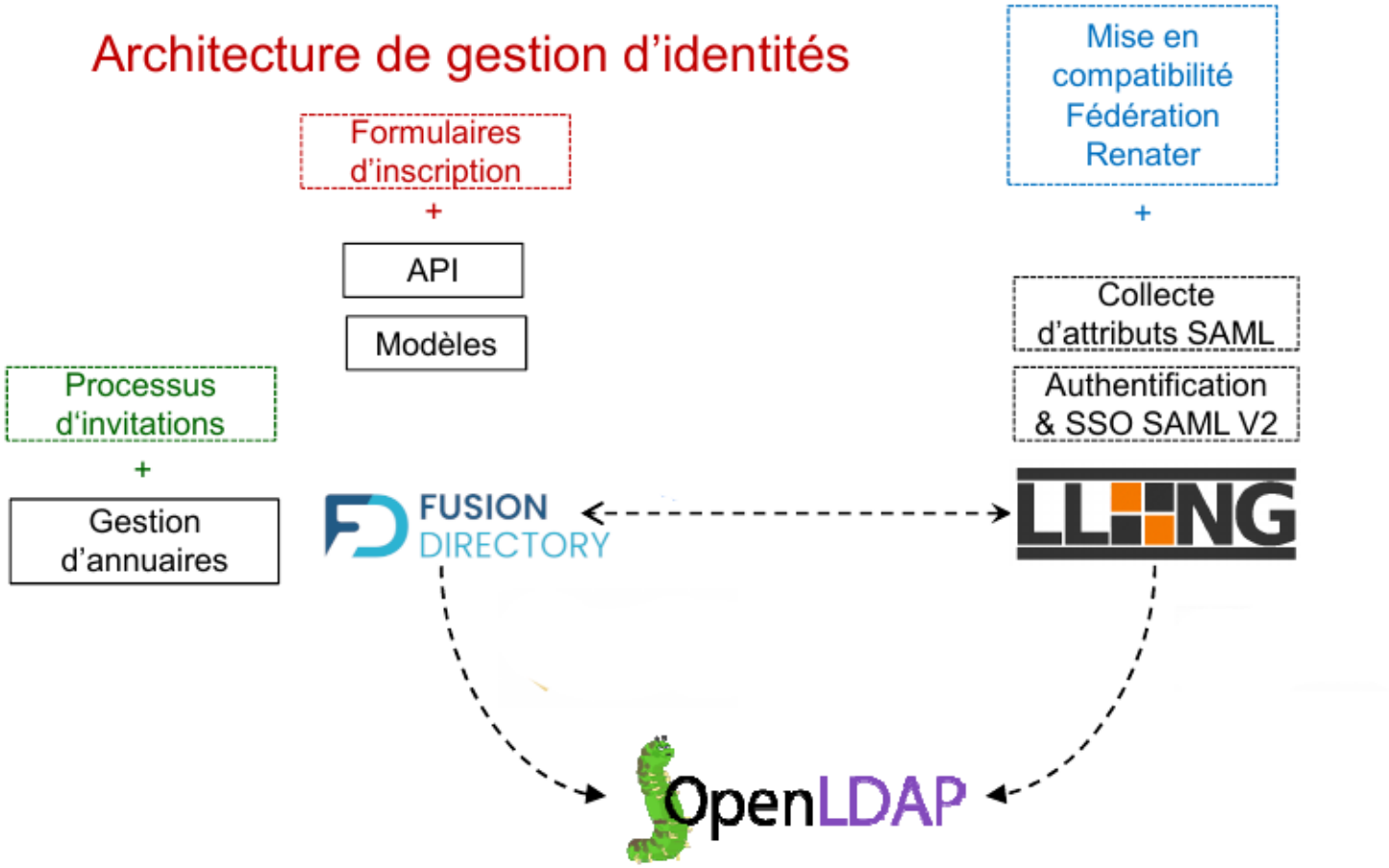


L'ECOLE DES HAUTES ETUDES EN SCIENCES SOCIALES
CéSoR Centre d'études en sciences sociales du religieux

CAMPUS CONDORCET
Paris–Aubervilliers

CAMPUS CONDORCET
Paris–Aubervilliers

Architecture de gestion d'identités



FusionDirectory dans les services publics

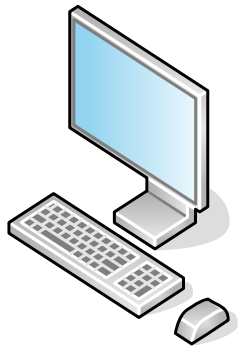
La demande etait de remplacer un logiciel métier existant par FusionDirectory.

- Accès par des chefs de projet avec peu d’expertise informatique.
- Segmentation forte entre les projets, le chef de projet A ne peut pas voir/lire des informations du projet B.
- Suivi de la sécurité des accès en temps réels et agragation vers systeme de log centralisé.
- Fermeture automatique de compte sur base de calcul de ressources restantes.
- Exportation de données de manière automatisée avec choix fin.

FusionDirectory dans les entreprises

- Synchronisation des utilisateurs & Groupes de OpenLDAP vers Samba 4
- FusionDirectory est utilisé pour les créations,modifications, suppression d'utilisateurs et de groupes
- FusionDirectory lance LSC grâce à ses triggers lors d'une création,modification d'un utilisateur ou d'un groupe et propage les modifications vers Samba 4

saluc SA



Utilisateurs

FUSION DIRECTORY

Trigger

LSC
LDAP Synchronization Connector

OpenLDAP
http://www.OpenLDAP.org

SAMBA

EVIDEN

- Utilisation de FusionDirectory dans leurs projets clients

- Utilisation de FusionDirectory dans la branche it de thyssenkrupp pour la gestion des identites.

- Utilisation de FusionDirectory dans les laboratoires d’orange Bretagne pour la gestion des identités

FusionDirectory dans les partis politiques

- Décision politique de migrer vers le Libre
- Démontrer qu'il est possible de fonctionner en environnement "full libre »
- Gérer les identités et le déploiement des systèmes avec la même interface
- Permettre à l'ensemble des membres et sympathisants d'accéder aux applications nécessaires à la vie du parti
- Allonger la vie des pc portables qui auraient été déclassés après 5 ans
- Déployer des pc portables prêt à l'emploi en 20 min

Démonstration

Demonstration

- Automatic groups : création de groupes basé sur des ressources ou des groupes dynamiques.
- Audit + syslog : Suivi de la sécurité des accès en temps réels et agregation vers systeme de log centralisé.
- Cycle de vie : Fermeture automatique de compte sur base de calcul de ressources restantes.
- Exporter : Exportation de données de manière automatisée avec choix fin.

Afin de vous familiariser avec la suite logicielle FusionDirectory.

Afin de vous familiariser avec la suite logicielle FusionDirectory.

FusionDirectory : https://www.fusiondirectory.org/

Présentations : https://www.fusiondirectory.org/presentations-autour-du-logiciel-fusiondirectory/

Fonctionalités : https://www.fusiondirectory.org/benefices-et-fonctionalites/

Documentation : https://www.fusiondirectory.org/documentation/

Forge logicielle : https://gitlab.fusiondirectory.org/

Webinaires : https://www.fusiondirectory.org/webinaires/

Chaine Youtube : https://www.fusiondirectory.org/chaine-youtube/

Démonstration personnalisée

Vous désirez en découvrir plus sur FusionDirectory ?

Vous aimeriez avoir une démonstration plus complète de certaines fonctionnalités ?

Demandez une démonstration personnalisée de FusionDirectory :

https://www.fusiondirectory.org/demande-de-demonstration/

Merci d’avoir assisté à ma présentation

OSSIR

https://infosec.exchange/@ossir
https://bsky.app/profile/ossir.infosec.exchange.ap.brid.gy