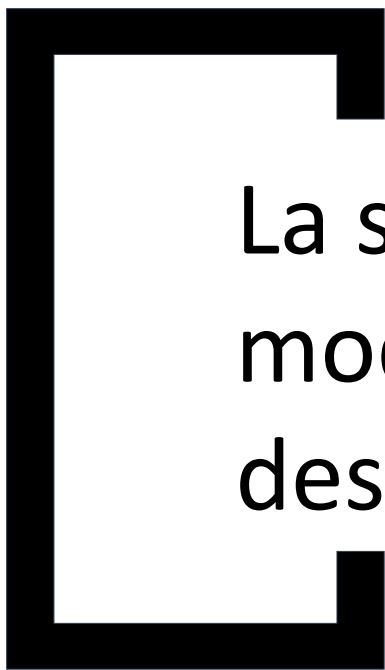




La suite logicielle FusionDirectory :
modernisez votre gestion des identités avec
des logiciels libres

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

A large, thick, black stylized bracket or 'C' shape that frames the text on the left side.

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 lesquelles 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 :

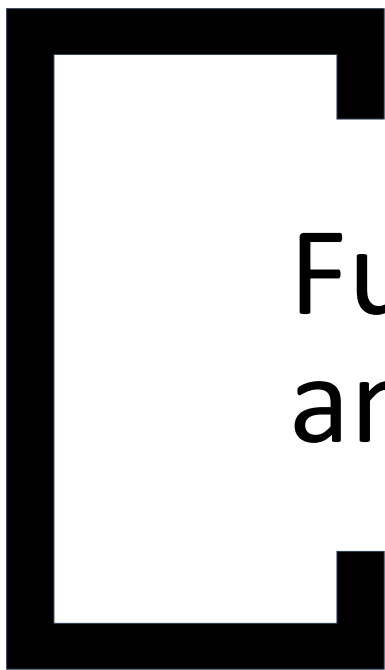
- Modéliser vos règles métier afin de les rendre dynamiques.
- Suivre les changements de statut, modifications.
- Surveillez et prévenir des changements non prévus.
- Automatiser votre gestion de groupes avec date de début et fin par utilisateurs.
- Archiver vos comptes pour éviter la réutilisation et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

FusionDirectory Integrator

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

Elles vous fournissent des fonctions 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

Utilisateurs									
< > Base Actions									
	Nom de famille	Prénom	Identifiant	Propriétés					Actions
☐	Administrator	System	fd-admin						
☐	carole	durieux	manager						
☐	paul	dufour	admin						
☐	peter	antoine	user						
4									

Filtre

Types

☒ Utilisateur
☐ Modèle

Onglet

☐ Unix
☐ Personnel
☐ Courriel
☐ Samba
☐ SSH
☐ Quota
☐ Ftp
☐ Freeradius
☐ SupAnn
☐ État SupAnn
☐ Carte multi service

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

Systèmes

<

<

🏠

🔄

🔗

Base

📄

Actions ▼

☐	Nom ▼	IP	MAC	Description	Service	Version	Actions
☐	demo-api	195.154.20.158	ff:ff:ff:ff:ee				
☐	demo-dev	195.154.20.159	ff:ff:ff:ff:fe				

🏠 2

🖥️ 0

🖨️ 0

📞 0

📱 0

📁 0

Filtre

Types

☒ Serveur

☒ Station de travail

☒ Terminal

☒ Imprimante

☒ Périphérique réseau

☒ Téléphone

☒ Téléphone portable

☐ Modèle

Onglet

☐ DNS

☐ Debconf

☐ FAI

☐ Inventaire

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

Utilisateur **Unix** Personnel Courriel Groupes et rôles SSH Références LDAP

Paramètres

Nom du modèle* clients

Informations personnelles

 Nom de famille* Prénom* Description Photo Browse... No file selected.

Compte utilisateur

Base /clients

Identifiant* %alps[1]|givenName%%alp|

Langue préférée

Méthode de mot de passe* ssha

Mot de passe %r[12]|%

Utilisateur **Unix** Personnel Courriel Groupes et rôles SSH Références LDAP

Ce compte a les paramètres Unix activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.

Retirer les paramètres Unix

Unix

Répertoire personnel* /srv/%uid%

Shell* /bin/bash

Groupe principal - automatique -

Statut

Forcer l'id d'utilisateur/groupe

Id d'utilisateur

Id de groupe

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

 **FUSION**
DIRECTORY

[Accueil](#) [Déconnexion](#)

Bienvenue dufour paul ! Connecté : admin

Utilisateurs et groupes
Départements
Utilisateurs
Groups and Roles
Groupes NIS
Mail Redirections

Supann
SupAnn Objects
SupAnn Structures

Workflow
Modèle de mail
Tasks Creation
Inscriptions
Public Forms
Invitations

Tableau de bord

Utilisateurs et groupes

 Départements

 Utilisateurs

 Groups and Roles

 Groupes NIS

 Mail Redirections

Supann

 SupAnn Objects

 SupAnn Structures

Workflow

 Modèle de mail

 Tasks Creation

 Inscriptions

 Public Forms

 Invitations

 **FUSION**
DIRECTORY

[Accueil](#) [Déconnexion](#)

Utilisateurs Connecté : admin

Utilisateurs et groupes
Départements
Utilisateurs
Groups and Roles
Groupes NIS
Mail Redirections

Supann
SupAnn Objects
SupAnn Structures

Workflow

Utilisateurs

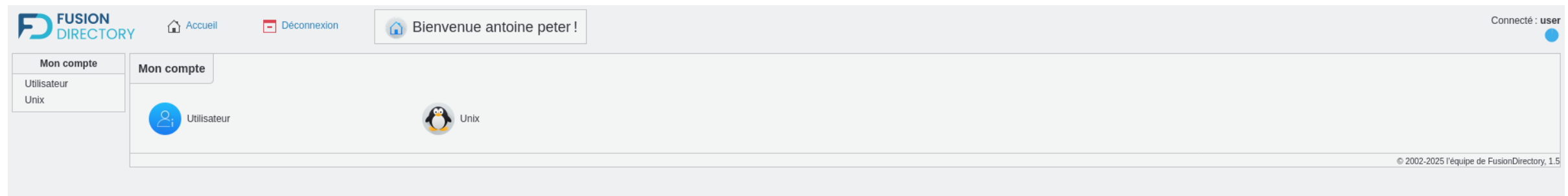
[Base /](#) [Actions](#)

		Nom de famille ▾	Prénom	Identifiant	Propriétés	Actions
☐		Administrator	System	fd-admin	  	     
☐		carole	durieux	manager	  	     
☐		paul	dufour	admin	  	     
☐		peter	antoine	user	  	     

4

Filtre
Types
☒ Utilisateur
☐ Modèle
Onglet
☐ Unix
☐ Personnel
☐ Courriel
☐ Samba
☐ OpenSSH
☐ Quota

Délégation : Vue de l'utilisateur user



FUSION DIRECTORY

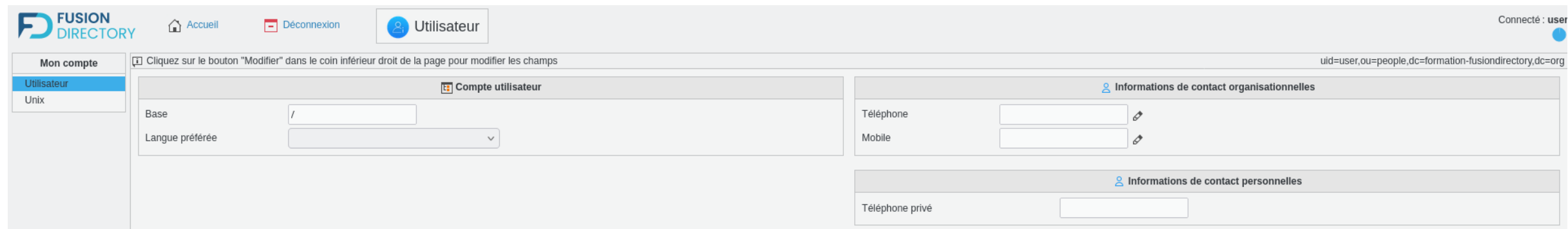
Accueil Déconnexion Bienvenue antoine peter ! Connecté : user

Mon compte

Utilisateur Unix

Utilisateur Unix

© 2002-2025 l'équipe de FusionDirectory, 1.5



FUSION DIRECTORY

Accueil Déconnexion Utilisateur Connecté : user

Mon compte

Utilisateur Unix

Cliquez sur le bouton "Modifier" dans le coin inférieur droit de la page pour modifier les champs uid=user,ou=people,dc=formation-fusiondirectory,dc=org

Compte utilisateur

Base /

Langue préférée

Informations de contact organisationnelles

Téléphone

Mobile

Informations de contact personnelles

Téléphone privé

Délégation : le système de de contrôle d'accès

FUSION
DIRECTORY

Accueil

Déconnexion

Acl Roles

Connecté : admin

Utilisateurs et groupes

cn=editowninfos,ou=acroles,dc=formation-fusiondirectory,dc=org

Acl Roles

Références

LDAP

Export

Éditer l'ACL pour "Utilisateur"

Toggle C

Toggle M

Toggle D

Toggle R

Toggle W

R+

W+

C+

C-

M+

M-

D+

D-

R+

R-

W+

W-

R+

R-

W+

W-

Objet: Utilisateur

☐ Create objects

☐ Move objects

☐ Remove objects

☒ Grant permission to owner

☐ Template hide main object creation button

Afficher/Cacher les paramètres avancés

L'objet au complet: ☐ read ☐ write

FUSION
DIRECTORY

Accueil

Déconnexion

Acl Roles

Connecté : admin

Utilisateurs et groupes

cn=editowninfos,ou=acroles,dc=formation-fusiondirectory,dc=org

Acl Roles

Références

LDAP

Export

Éditer l'ACL pour "Utilisateur"

Toggle C

Toggle M

Toggle D

Toggle R

Toggle W

R+

W+

C+

C-

M+

M-

D+

D-

R+

R-

W+

W-

R+

R-

W+

W-

Objet: Utilisateur

☐ Create objects

☐ Move objects

☐ Remove objects

☒ Grant permission to owner

☐ Template hide main object creation button

Afficher/Cacher les paramètres avancés

L'objet au complet: ☐ read ☐ write

hidden (cn)

☐ read ☐ write

Nom de famille de cet utilisateur (sn)

☐ read ☐ write

Prénom de cet utilisateur (givenName)

☐ read ☐ write

Les initiales de tout ou partie des noms de la personne, mais pas le(s) nom de famille (initials)

☐ read ☐ write

Une courte description de l'utilisateur (description)

☐ read ☐ write

L'avatar pour cet utilisateur (jpegPhoto)

☐ read ☐ write

Lieu (l)

☐ read ☐ write

Département (st)

☐ read ☐ write

Adresse postale professionnelle (postalAddress)

☐ read ☐ write

Numéro du bureau (roomNumber)

☐ read ☐ write

Numéro de téléphone professionnel (telephoneNumber)

☒ read ☒ write

Numéro de téléphone portable professionnel (mobile)

☒ read ☒ write

Numéro de bip professionnel (pager)

☐ read ☐ write

Numéro de fax professionnel (facsimileTelephoneNumber)

☐ read ☐ write

Site web personnel (labeledURI)

☐ read ☐ write

Identifiant de l'utilisateur (uid)

☐ read ☐ write

Langue préférée (preferredLanguage)

☒ read ☒ write

Mot de passe de l'utilisateur (userPassword)

☐ read ☐ write

Nom de l'utilisateur tel qu'il devrait apparaître. Utilisé par le carnet d'adresse Exchange. (displayName)

☐ read ☐ write

Adresse postale personnelle (homePostalAddress)

☐ read ☐ write

Numéro de téléphone privé (homePhone)

☒ read ☒ write

Workflow

Modèle de mail

Tasks Creation

Inscriptions

Public Forms

Invitations

Tableau de bord

Tâches

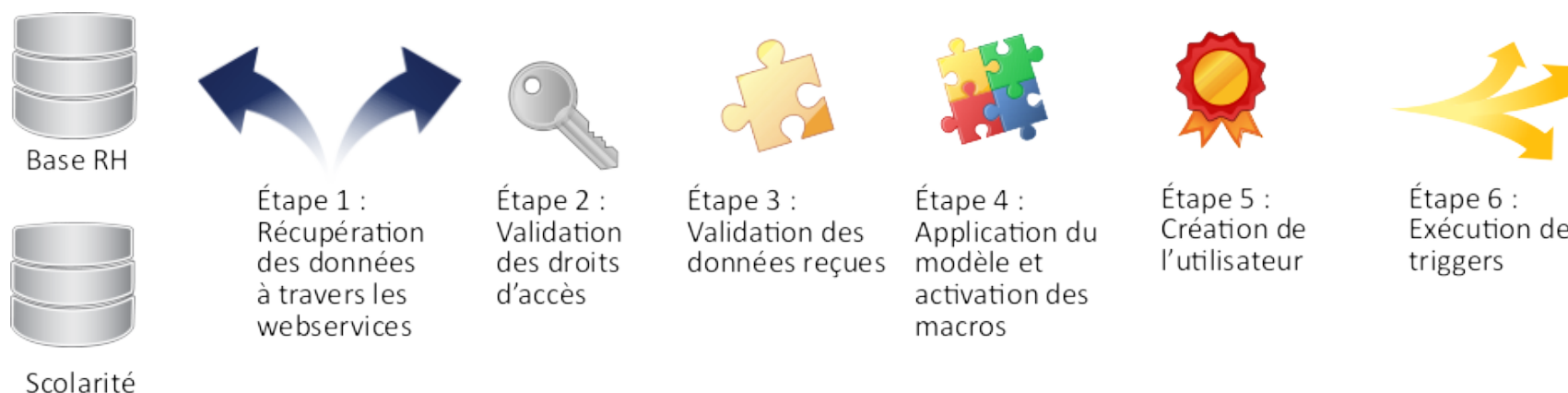
Plugins

Ejbca

Sécurité

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

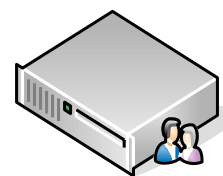
- Il existe de nombreux cas où on désire déclencher des actions après la création, la modification ou la vérification de données
- Dans le cas de FusionDirectory, une liberté totale est laissée en ce qui concerne l'écriture des triggers
- Cela peut être utilisé pour appeler d'autres webservices ou déclencher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

- Gestion des établissements 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 à vis de ses données et services.
- Code Population pour définir plus finement les différentes populations d'utilisateurs.

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

Structures SupAnn						
Actions ▾						
☐		Nom ▾	supannCodeEntite	Parent	Description	Actions
☐	🏠	DSI	54322	53056	Direction service informatique	
☐	🏠	nouvelle caledonie	53056		Université nouvelle caledonie	
☐	🏠	RH	54321	53056	service RH	
🏠 1 🏠 2						

SupAnn Objects

Supann Objects : concept de ressources avec état, sous état

SupAnn Objects					
Base / Actions					
☐		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'état d'une ressource.
- Une date de debut et une date de fin sur chaque ressource permettra de déclencher des actions preprogrammées

Utilisateur | Unix | Personnel | Courriel | **Groupes et rôles** | Samba | SSH | Quota | Ftp | Freeradius | Groupe NIS | **SupAnn** | **Etat SupAnn** | Carte multi service | SpamAssassin | Certificats | Sous traitance | Sinaps | Sécurité | Politique de mot de passe | Bulletin

Ce compte a les paramètres État SupAnn activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.

Retirer les paramètres État SupAnn

Statut						
	Ressource	Statut	Sous-état	Début	Fin	
*	Courriel	Active	Aucune	2020-10-28	2021-03-08	 
	Compte	Suspendu	Verrouillage administratif	2020-10-28	2020-11-05	 

Ressource*

Statut*

Sous-état

Début

Fin

Ajouter

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

Utilisateur

Unix

Personnel

Courriel

Samba

Groupes et rôles

SSH

Quota

Ftp

Freeradius

Groupe NIS

SupAnn

État SupAnn

Multiservice card

Inscription

SpamAssassin

Certificats

Sous traitance

Sinaps

Sécurité

Ce compte a les paramètres Multiservice card activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.

Retirer les paramètres Multiservice card

Cards

Type	Format	Id	Valid	Source	Date de fin	
externe	Mifare XLSB	DEADBEEF000000	oui	unicampus@fusiondirectory.org		 

Type*

externe

Format*

Mifare XLSB

Id*

DEADBEEF000000

Valid*

☐

Source

unicampus@fusiondirectory.org

Date de fin

jj / mm / aaaa

Ajouter



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 acs 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
// 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
                    )
                ),
            ],
        ],
    ],
    new SelectAttribute (
```

Plugin de demonstration : affichage

uid=fd-admin,ou=people,dc=ecolo,dc=lan

Utilisateur Courriel Groupes et rôles SupAnn État SupAnn Carte multi service WebAuthn **Demo Plugin** SCHAC Références LDAP

Hair Information		Bicycle	
Color*		Brand*	GreatBicycleBrand
	Blond Ajouter Supprimer	Has a bell	☐
Length	10		

FTP information	
Identifiant	
Mot de passe	
Hôte	
Port	21

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

Zones inverses

2.168.192.in-addr.arpa.

|

Ajouter Supprimer

CompositeAttribute

Enregistrement SOA

Serveur DNS primaire arecord1.test.com.

Adresse de courriel test.test.com.

Numéro de série 2021021801

Rafraîchir 1 heures

Réessayer 30 minutes

Expirer 200 heures

TTL 6400 secondes

ObjectsAttribute

group1

System Administrator

Ajouter Supprimer

Clefs étrangères

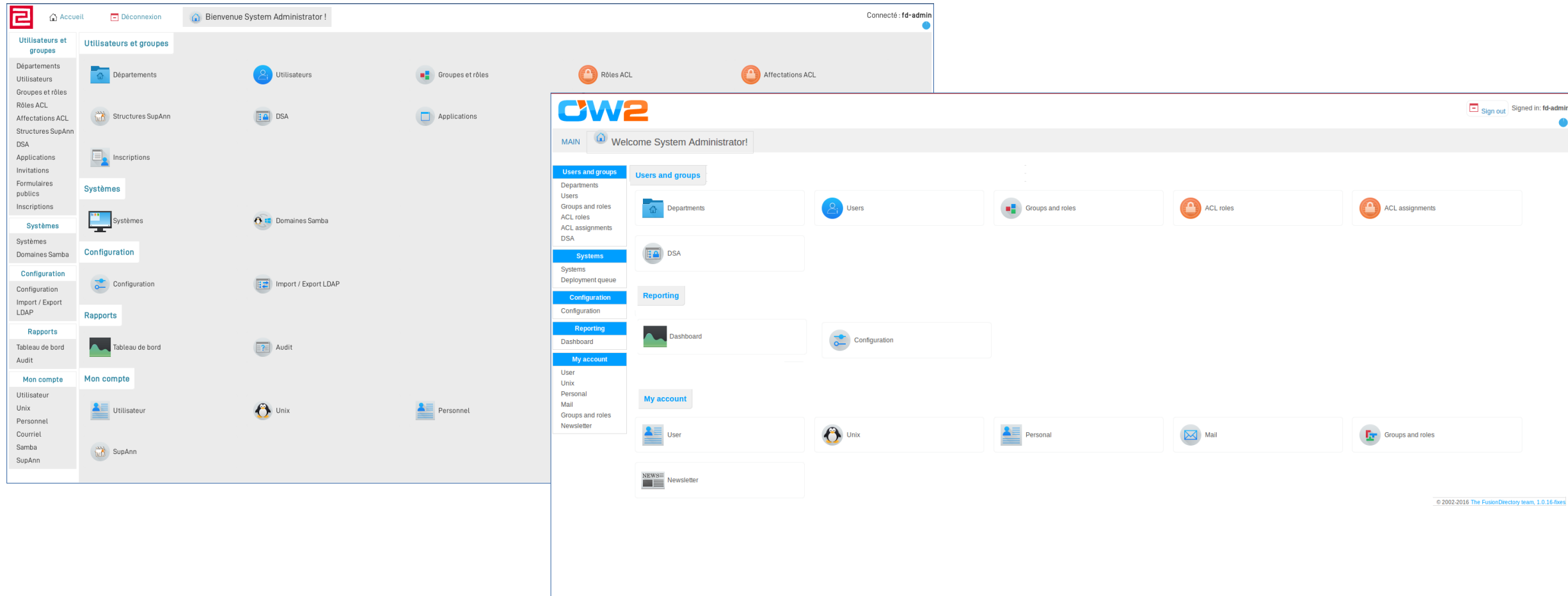
- La valeur de l'attribut sera mise à jour si l'objet référencé est modifié
- Le lien apparaîtra dans l'onglet références de l'objet référencé.

```
dc=ecolo,dc=lan
  Onglet «Affectation ACL»
    • gosaAclEntry fait référence à notre dn
ogroup
  Onglet «Groupe d'objets»
    • member fait référence à notre dn
aprole
  Onglet «Rôle»
    • roleOccupant fait référence à notre dn
```

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

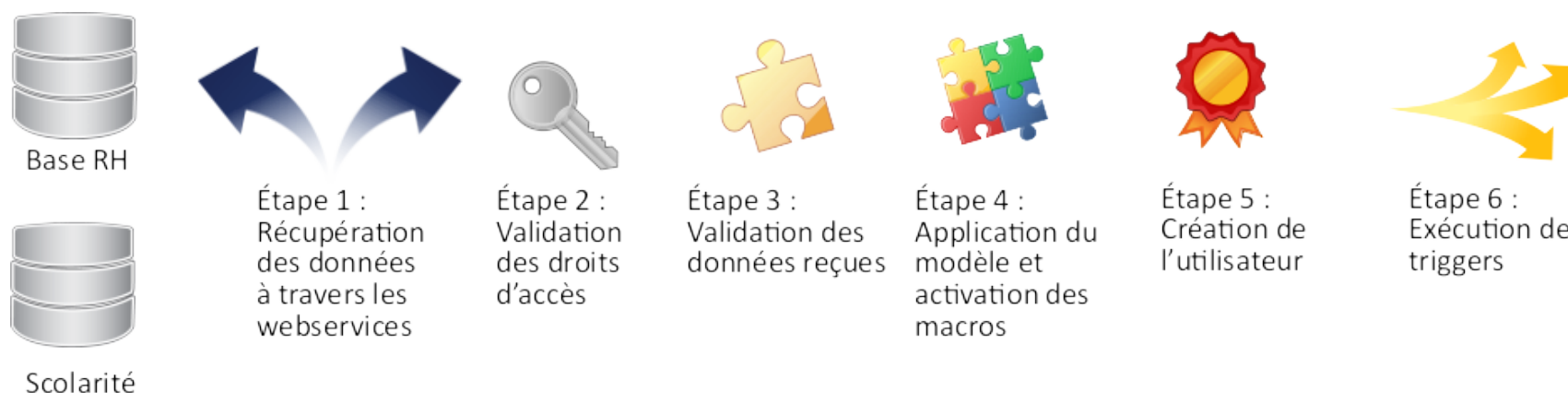




FusionDirectory Webservice : Améliorer le provisioning

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.

This account has Tasks Life Cycle settings enabled. You can disable them by clicking below.

[Remove Tasks Life Cycle settings](#)

We recommend the task redundancy to be set to daily, and the case New Members Only to be unpicked

Current resources details

Resource* Account

State* A

Sub state Active

Future resources details

Resource* Account

State* S

Sub state Technical lock

Extra days to add 0

Regex Pattern Configuration

Regex Pattern

Automatic Account Closure

Enable Account Closure ☐

Recipients Users and/or Groups

Members*

 durieux carole

[Add](#) [Delete](#)

Automatic groups

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

This account has Tasks Automatic Groups settings enabled. You can disable them by clicking below.

[Remove Tasks Automatic Groups settings](#)

We recommend the task redundancy to be set to daily, and the case New Members Only to be unpicked

Task Mode

Create Dynamic Group

☐

Resource State Criteria

Resource

None

State*

A

Sub state

None

Regex Pattern Configuration

Regex Pattern

Manual Group Assignment

Target Group*

ogroup-test

Members*

Add Delete

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.

Tâches Tasks Notifications Tâches reminder Tâches d'audit Tasks Life Cycle Tâches Courrier Références LDAP Gestionnaire d'exportation

Ce compte a les paramètres Tâches reminder activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.
Retirer les paramètres Tâches reminder

Configuration des rappels d'expiration	SupannRessourceEtat à surveiller
Premier rappel* 30	Ressource* Compte
	Département* A
	Sous-état Aucune

Prolongation de compte	
Prolongation de compte	☐
Deuxième Rappel	15
Posix	☐
Ressource	Aucune
Département	
Sous-état	Aucune
Durée ajoutée au compte	0

Destinataires Utilisateurs et/ou Groupes	Modèle de mail
Transférer vers	Modèle de mail*
	Courriel émetteur* to.be@chang.ed
Ajouter Supprimer	
Membres surveillés*	
Ajouter Supprimer	

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

Tâches Tasks Audit Tasks Life Cycle **Tasks Notifications** Tasks Reminder Tâches Courrier Références LDAP Gestionnaire d'exportation

Ce compte a les paramètres Tasks Notifications activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.
[Retirer les paramètres Tasks Notifications](#)

Modified attributes list to be notified	Add notification when the following Supann state is reached (supannRessourceEtat)
Attributes* supannRessourceEtat telephoneNumber ▼ Ajouter Supprimer	Ressource* Compte ▼ Département* S ▼ Sub state Verrouillage technique ▼
Destinataires Utilisateurs et/ou Groupes	Modèle de mail
Recipients* dufour paul durieux carole Ajouter Supprimer Monitored Members* antoine peter Ajouter Supprimer	Modèle de mail* envoi de compte numeriques ▼ Courriel émetteur* manager@demonstration.

Exporter

Exportation de données de manière automatisée avec choix fin.

This account has Tasks Extractor settings enabled. You can disable them by clicking below.
[Remove Tasks Extractor settings](#)

Members to Extract	Attributes to Extract
Selected Members*  supannactive Add Delete	Attributes* description givenName sn supannRessourceEtatDate ALL Add Delete
Extraction Settings	Email Notification
Format* CSV (Comma Separated Values)	Recipients*  adminZimbra adminZimbra Add Delete Sender email address* admin@zimbra.example.com

Archivage

- Tache d'archivage

Tasks	Tasks Reminder	Tasks Archive	Tasks Mail	Tasks Notifications	References	LDAP										
This account has Tasks Archive settings enabled. You can disable them by clicking below. Remove Tasks Archive settings																
SupAnn Resource Archiving Settings <table><tr><td>Resource*</td><td>rwcdm [fdArchiveTaskResource] Account ▾</td></tr><tr><td>State*</td><td>rwcdm [fdArchiveTaskState] I ▾</td></tr><tr><td>Sub state</td><td>rwcdm [fdArchiveTaskSubState] Archiving ▾</td></tr></table>			Resource*	rwcdm [fdArchiveTaskResource] Account ▾	State*	rwcdm [fdArchiveTaskState] I ▾	Sub state	rwcdm [fdArchiveTaskSubState] Archiving ▾	Recipients Users and/or Groups <table><tr><td>rwcdm [fdArchiveTaskMembers]</td></tr><tr><td>userA userA</td></tr><tr><td>rwcdm [fdArchiveTaskMembers]</td></tr><tr><td>Add Delete</td></tr></table>				rwcdm [fdArchiveTaskMembers]	userA userA	rwcdm [fdArchiveTaskMembers]	Add Delete
Resource*	rwcdm [fdArchiveTaskResource] Account ▾															
State*	rwcdm [fdArchiveTaskState] I ▾															
Sub state	rwcdm [fdArchiveTaskSubState] Archiving ▾															
rwcdm [fdArchiveTaskMembers]																
userA userA																
rwcdm [fdArchiveTaskMembers]																
Add Delete																

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.

Ce compte a les paramètres Tâches d'audit activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.

[Retirer les paramètres Tâches d'audit](#)

Planifier la conservation des audits

Temps de rétention en jours*

0

Syslog Transformation

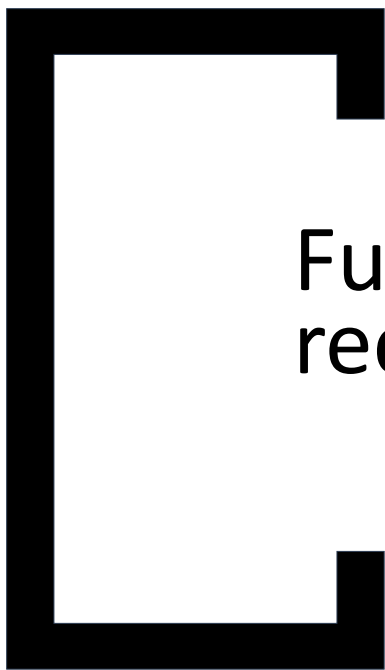
Enable Syslog Transformation



```
Mon Apr 07 18:02:03 WEST
<local4.info>Apr 07 15:27:33 192.168.122.1 FusionDirectory-Audit: id="8591274230425578524" user="uid=fd-admin,ou=people,dc=example,dc=com" action="modify" objectType="plugin/tasks" object="cn=audit
<local4.info>Apr 07 15:27:33 192.168.122.1 FusionDirectory-Audit: id="4555288685039526012" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/tasksGranular" object="c
<local4.info>Apr 07 15:27:33 192.168.122.1 FusionDirectory-Audit: id="8673011557284582014" user="uid=fd-admin,ou=people,dc=example,dc=com" action="modify" objectType="plugin/auditTask" object="cn=au
<local4.info>Apr 07 15:57:35 192.168.122.1 FusionDirectory-Audit: id="8255461187111781893" user="uid=fd-admin,ou=people,dc=example,dc=com" action="security" objectType="logout" object="fd-admin" resu
<local4.info>Apr 07 16:31:46 192.168.122.1 FusionDirectory-Audit: id="2616429779211122843" user="uid=fd-admin,ou=people,dc=example,dc=com" action="security" objectType="login" object="fd-admin" resu
<local4.info>Apr 07 16:31:50 192.168.122.1 FusionDirectory-Audit: id="2860411961760233306" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/user" object="uid=fkslvt
<local4.info>Apr 07 16:31:50 192.168.122.1 FusionDirectory-Audit: id="2895780666398336477" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/posixGroup" object="cn=f
<local4.info>Apr 07 16:31:50 192.168.122.1 FusionDirectory-Audit: id="5970594206035570357" user="uid=fd-admin,ou=people,dc=example,dc=com" action="modify" objectType="plugin/posixGroup" object="cn=p
<local4.info>Apr 07 16:31:50 192.168.122.1 FusionDirectory-Audit: id="8744095969396848528" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/posixAccount" object="ui
<local4.info>Apr 07 16:31:50 192.168.122.1 FusionDirectory-Audit: id="6878447748662573097" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/userRoles" object="uid=f
<local4.info>Apr 07 16:31:50 192.168.122.1 FusionDirectory-Audit: id="72677310566715877" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/supannAccount" object="uid
<local4.info>Apr 07 16:31:50 192.168.122.1 FusionDirectory-Audit: id="1268026369072283690" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/supannAccountStatus" obj
<local4.info>Apr 07 16:31:53 192.168.122.1 FusionDirectory-Audit: id="1316799886206876415" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/user" object="uid=ssid4w
<local4.info>Apr 07 16:31:53 192.168.122.1 FusionDirectory-Audit: id="1024572979652954140" user="uid=fd-admin,ou=people,dc=example,dc=com" action="create" objectType="plugin/posixGroup" object="cn=s
<local4.info>Apr 07 16:31:53 192.168.122.1 FusionDirectory-Audit: id="976943167891699807" user="uid=fd-admin,ou=people,dc=example,dc=com" action="modify" objectType="plugin/posixGroup" object="cn=ps
```



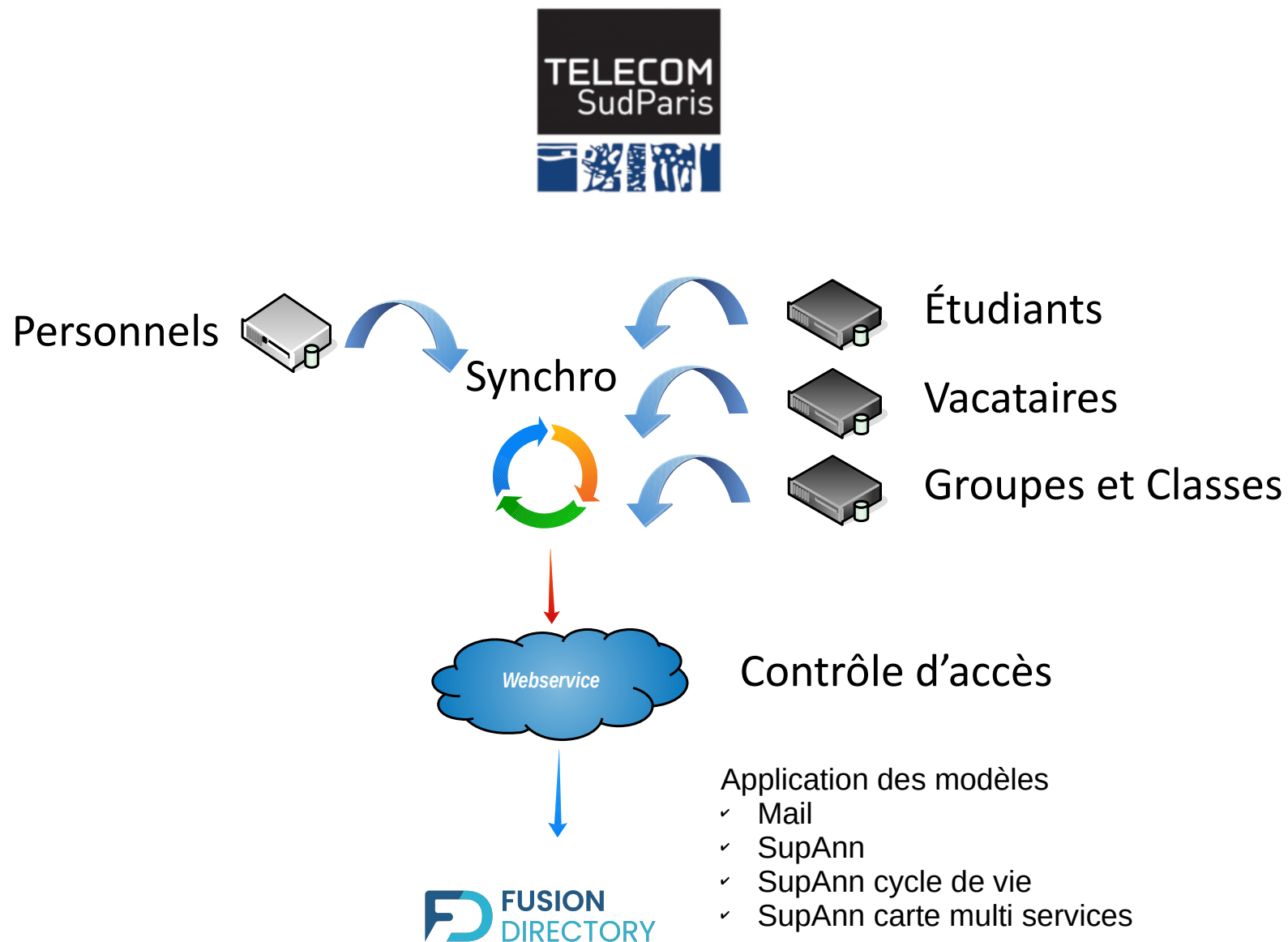
Cas Concrets

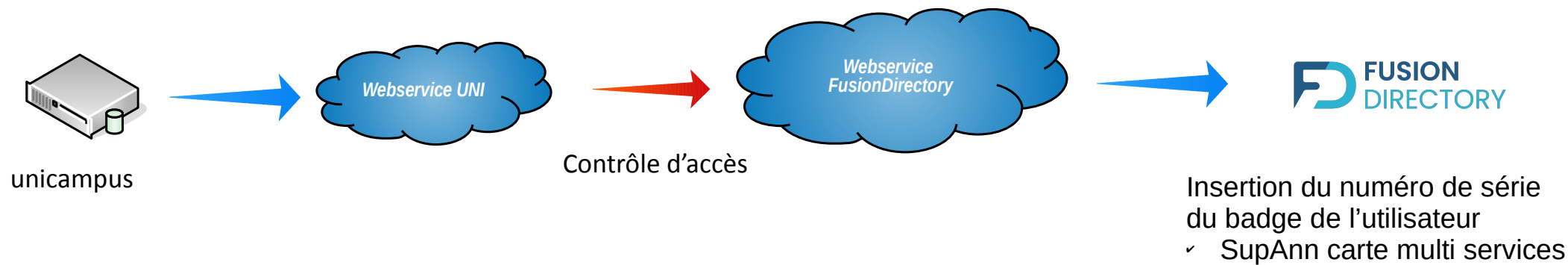


FusionDirectory dans l'enseignement supérieur recherche



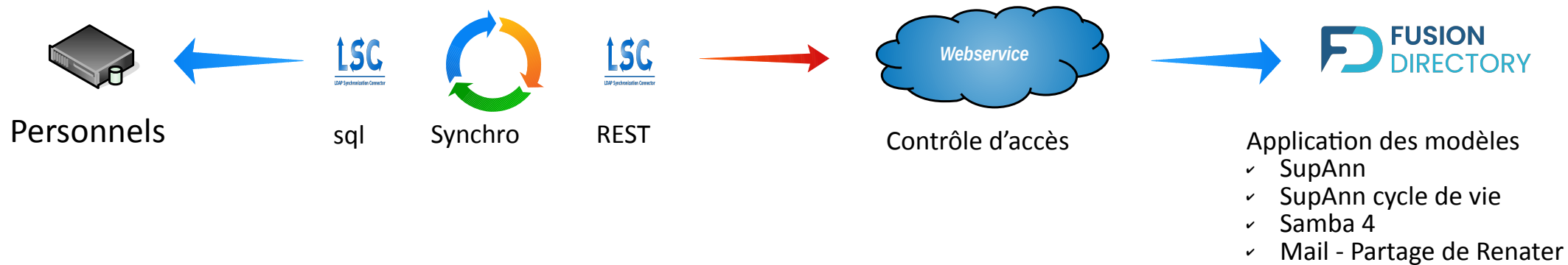
- Utiliser les webservices de FusionDirectory et les modèles afin de provisionner les utilisateurs par type dans toute leur complexité
- Utiliser les webservices de unicampus et FusionDirectory afin de propager les numéros de badges lors de leur création
- Utiliser les webservices de FusionDirectory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







- 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

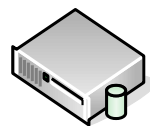




- Utiliser les webservice de FusionDirectory et les modèles afin de provisionner les utilisateurs par type dans toute leur complexité
- Propager les mots de passe dans 3 ActiveDirectory différents
- Créer les fiches de contact utilisateurs Office 365



Personnels
Étudiants



Contrôle d'accès



Création d'utilisateurs
Création Fiche Office 365



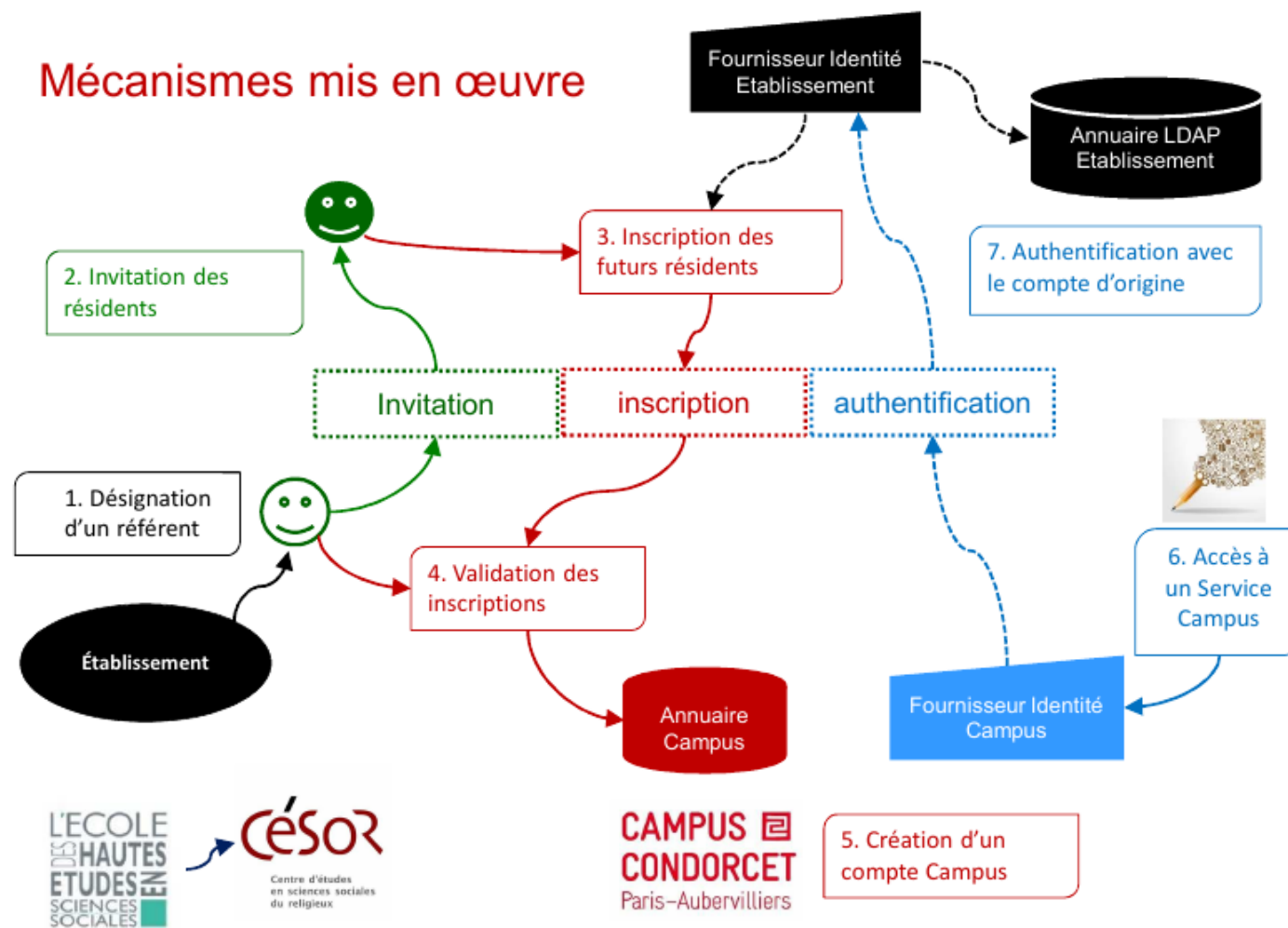
Synchronisation mot de passe



- Nouveaux campus comprenant des personnels et étudiants de 11 établissements
- 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

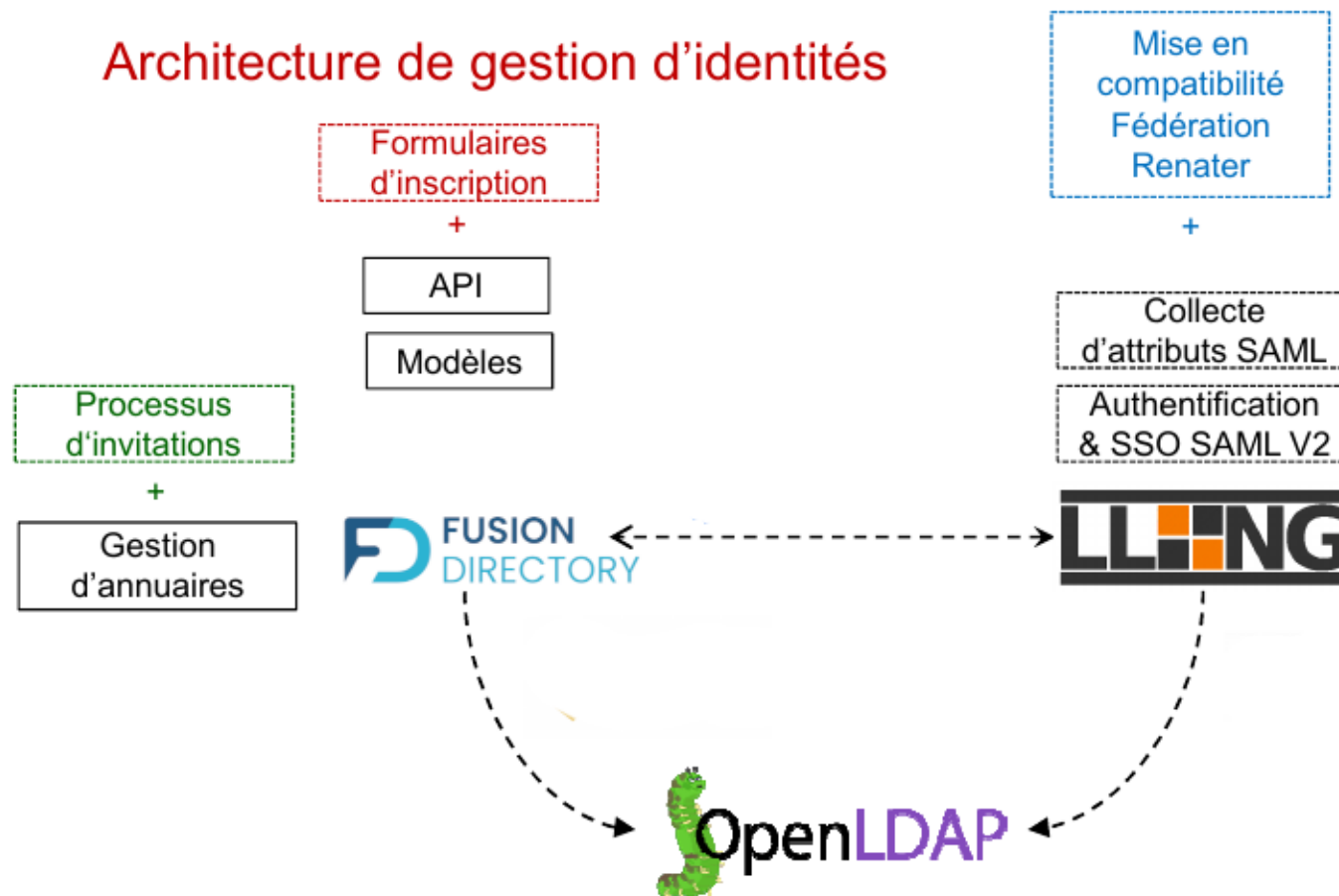
Mécanismes mis en œuvre



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.

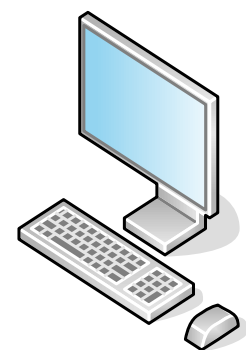
- Accès par des chefs de projet avec peu d'expertise informatique.
- Segmentation forte entre les projets, le chef de projet A ne peut pas voir/lire des informations du projet B.
- Suivi de la sécurité des accès en temps réels et agragation vers systeme de log centralisé.
- Fermeture automatique de compte 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



Utilisateurs



EVIDEN

- Utilisation de FusionDirectory dans leurs projets clients



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



- 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/>

Fonctionnalités : <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



<https://infosec.exchange/@ossir>

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