



IDENTITY DAYS

7^{ème} édition

@IdentityDays
#identitydays2025

21 octobre 2025 - PARIS



Utilisation de workflow dans une gestion des identités libre en environnement critique

Benoit - Mortier

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
- Norme SupAnn
- Automatiser et sécuriser
- Pour découvrir la suite Logicielle FusionDirectory
- Références



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 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 ...



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 établissements 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						

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

Compte
Active
Aucune
mm / dd / yyyy
mm / dd / yyyy
Ajouter



Automatiser et sécuriser

Automatiser et sécuriser

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

Parmi les critères on retrouvait :

- 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.

Solution apportée

Developpement de nouvelles tâches FusionDirectory Orchestrator

- 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.
- Supann Objects : Sortie des ressources SupAnn du backend de config et creation d'objets à part entière
- Exporter : Exportation de données de manière automatisée avec choix fin.

Automatic groups

- Tache d'appartenance à des groupes en fonction de ressources supann

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

Audit + Syslog

- Tache de transformation des audit FusionDirectory en format syslog

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	Syslog Transformation
Temps de rétention en jours* 0	Enable Syslog Transformation ☒

```

Mon Apr 07 18:02:03 WEST
fd-audit-2025-04-07.log: plain text TEXT
<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=auditT
<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" res
<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=pe
  
```

Cycle de vie

- Ajout de changement d'état sur un groupe de ressources par regex dans le cycle de vie

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

SupAnn Objects

Supann Objects : Sortie des ressources SupAnn du backend de config et creation d'objets à part entière

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		     

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



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.
- Supann Objects : Sortie des ressources SupAnn du backend de config et creation d'objets à part entière
- Exporter : Exportation de données de manière automatisée avec choix fin.



Pour Découvrir la suite
logicielle FusionDirectory

Pour découvrir 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
Bonne journée et bonnes conférences.

21 octobre 2025 - PARIS

The logo consists of three stylized human figures of increasing height, colored green, white, and white from left to right.

iID IDENTITY DAYS



@IdentityDays
#identitydays2025