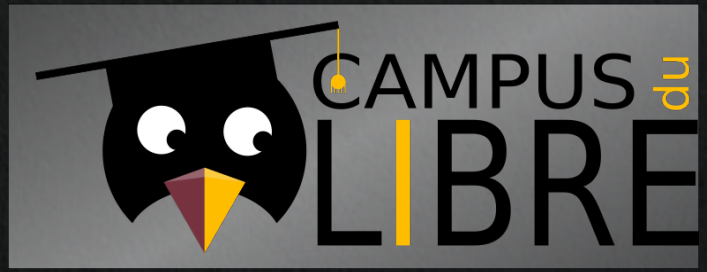
Vorteks

make IT work, make IT free

IAM : Gestion des identités et des accès avec du logiciel libre



26 novembre 2022

Présentation

Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot

LemonLDAP::NG
LDAP Tool Box
LDAP Synchronization Connector
FusionIAM
W'Sweet

KPTN
DonJon Legacy
Improcité
Les Amis Causent

Worteks

Service

Infrastructures hétérogènes et complexes, cloud, authentification, securité

- Etudes, audit et consulting
- Expertise technique
- Support technique
- Formation
- R&D et innovation

Édition

V'Sweet — Portail d'applications collaboratif

V'Opla — Plateforme mutualisée de développement

V'IDaaS — Gestion des identités des accès

Partenaires

Red Hat Advanced Business Partner Reseller

BlueMind

ONLYOFFICE

Collabora Online

On recrute !

https://www.worteks.com/rejoindre/

Introduction en musique

The Hacker

Some people call me the LDAP cowboy
Some call me Authentication man
Some people call me Single Sign On guy
Cause I speak of Identity in conferences

Cause I'm a hacker
A developer
I use servers
And containers
I put Identity in the Cloud

I'm a hacker
Software maker
Open Source
Community lover
My work is here for everyone

People talk about me, baby
Say I'm doin' security wrong
Well, don't you worry baby, don't worry
Cause I run services right here on localhost

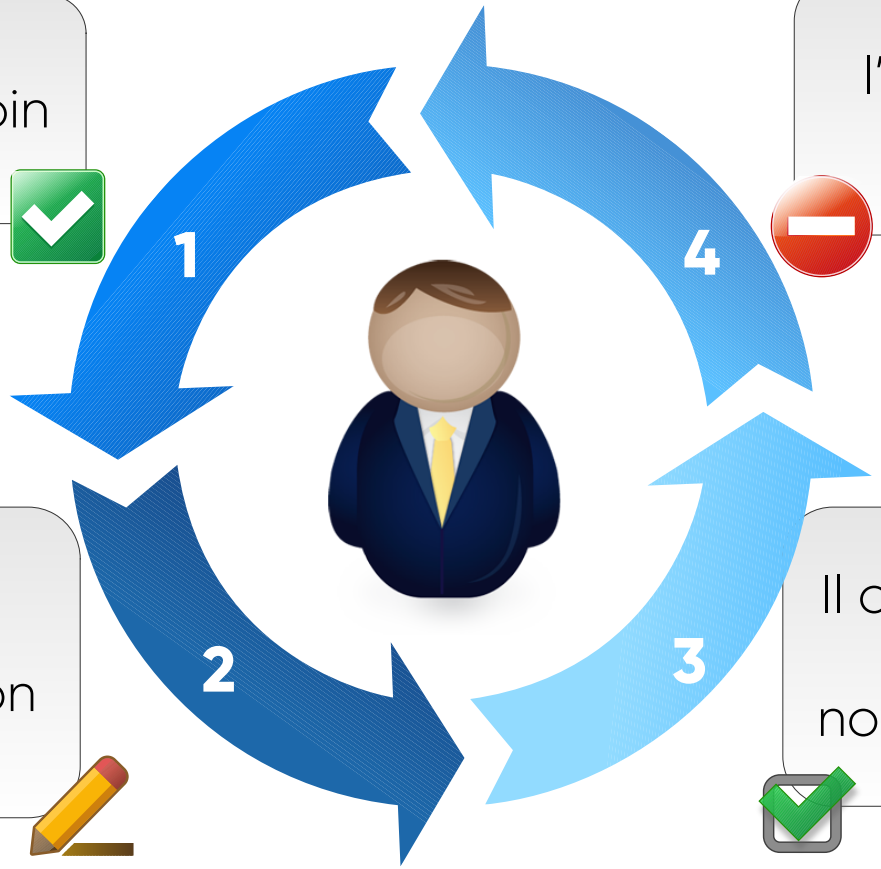
Cause I'm a hacker
Software maker
Open Source
Community lover
My work is here for everyone

I'm a hacker
A developer
I use servers
And containers
I put Identity in the Cloud

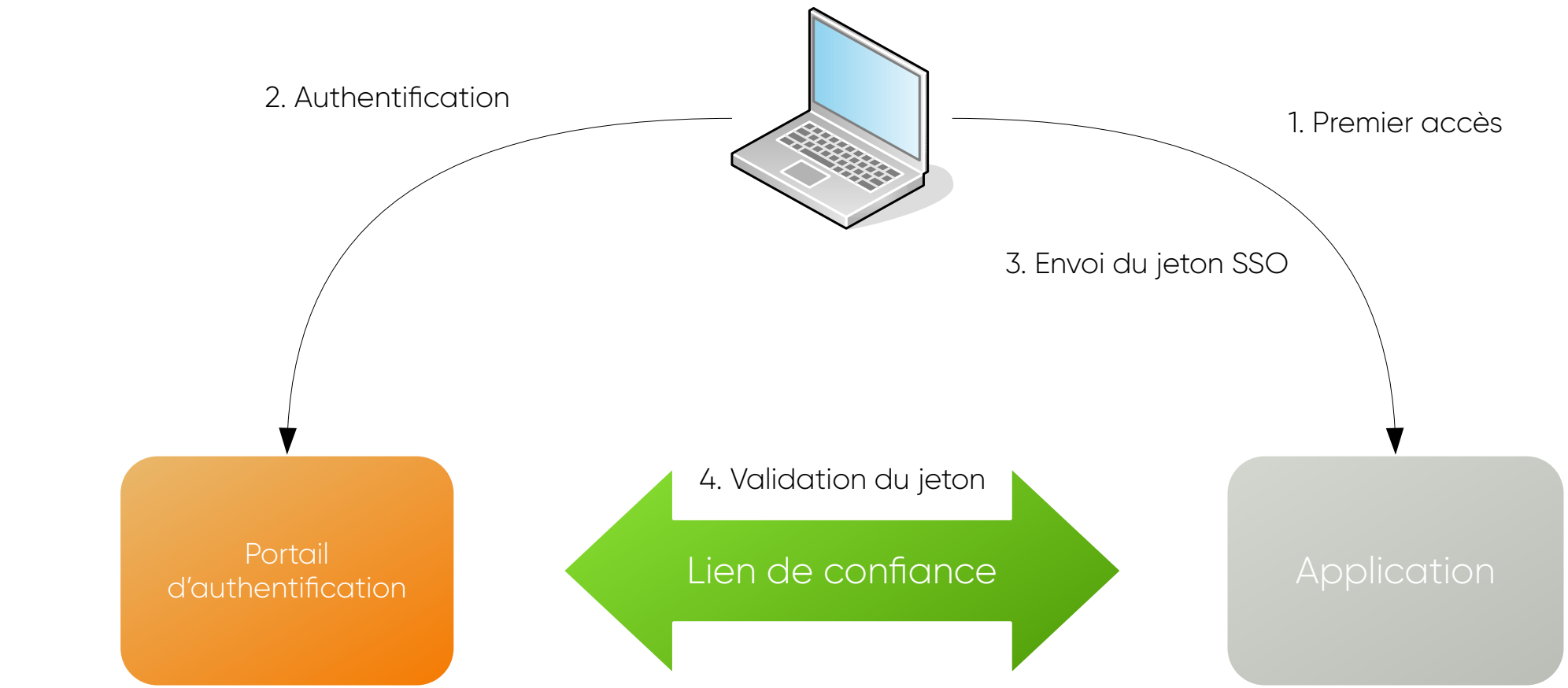
Gestion des Identités et des Accès

Cycle de vie de l'identité

1. Un nouvel embauché a besoin d'un compte
2. Il édite ses informations personnelles et son mot de passe
3. Il obtient une promotion nécessitant de nouveaux droits d'accès
4. Il quitte l'organisation, son compte est supprimé



Fonctionnement du SSO



You Only Log Once

IAM Open Source

Le marché IAM

- Marché détenu par des solutions propriétaires
- Solutions majoritairement américaines
- Produits riches et complexes
- Modèle de coût par utilisateur

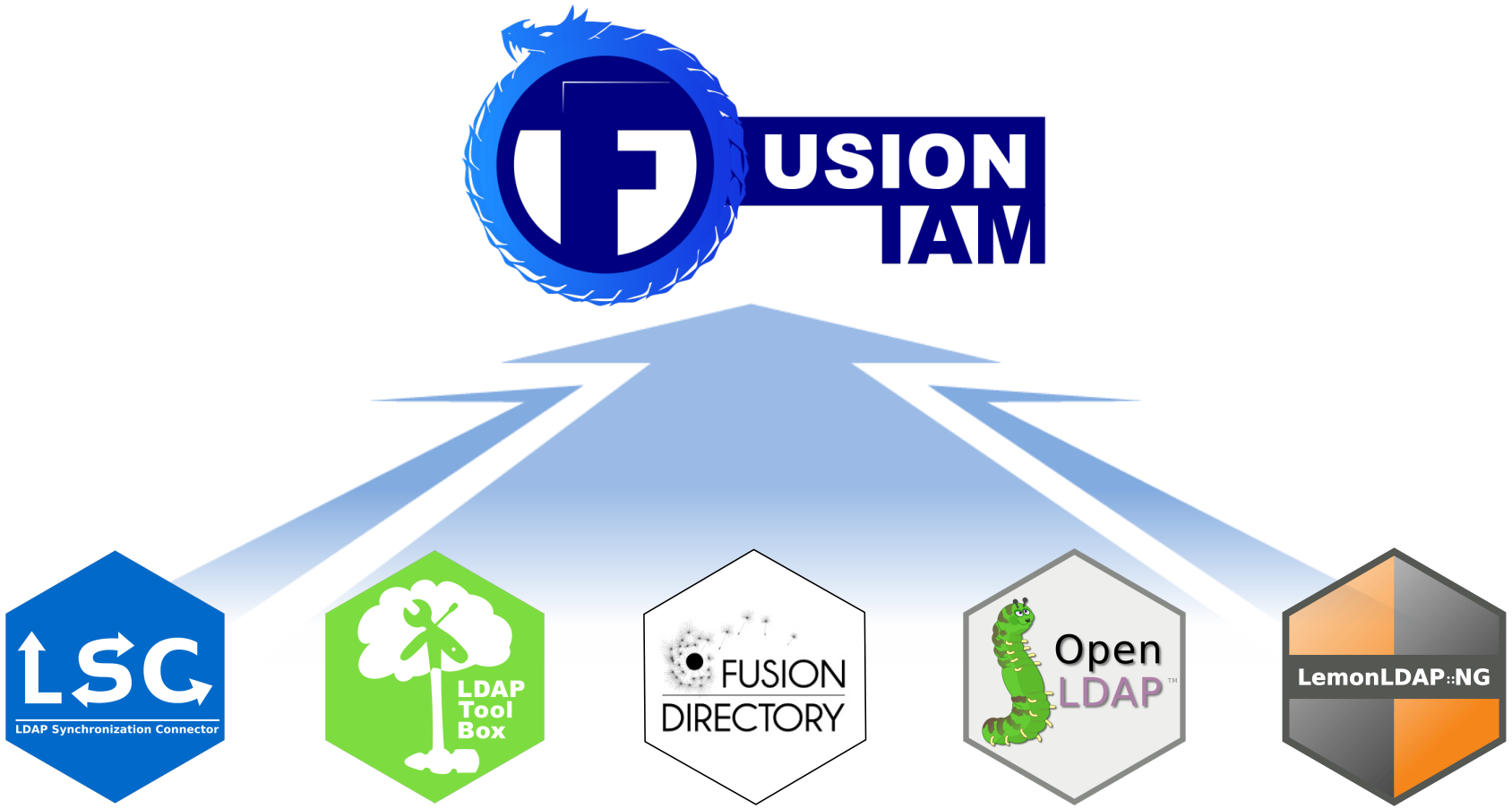
IAM Open Source ?

- Beaucoup de logiciels Open Source existent mais :
  - Ils ne couvrent qu'un sous-ensemble des fonctionnalités IAM
  - Ils ne s'intègrent pas facilement les uns les autres

- Le projet FusionIAM a fait le choix de certains composants Open Source et permet leur installation et configuration de façon unifiée

FusionIAM

Le projet FusionIAM



Composants

FusionIAM White Pages

FusionIAM Access Manager

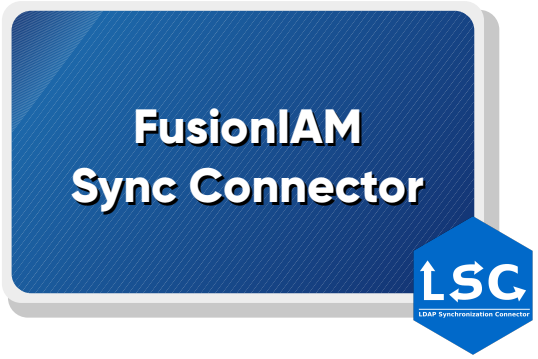
FusionIAM Sync Connector

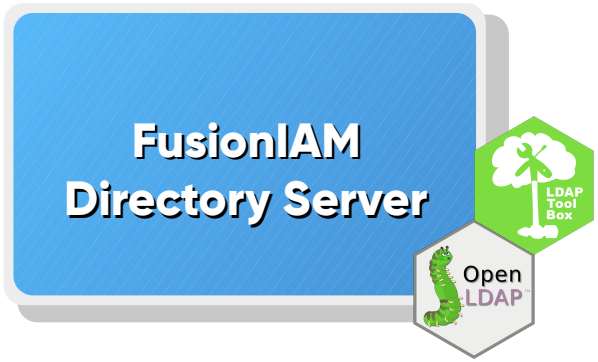
FusionIAM Service Desk

FusionIAM Directory Server

FusionIAM Directory Manager

Composants et logiciels



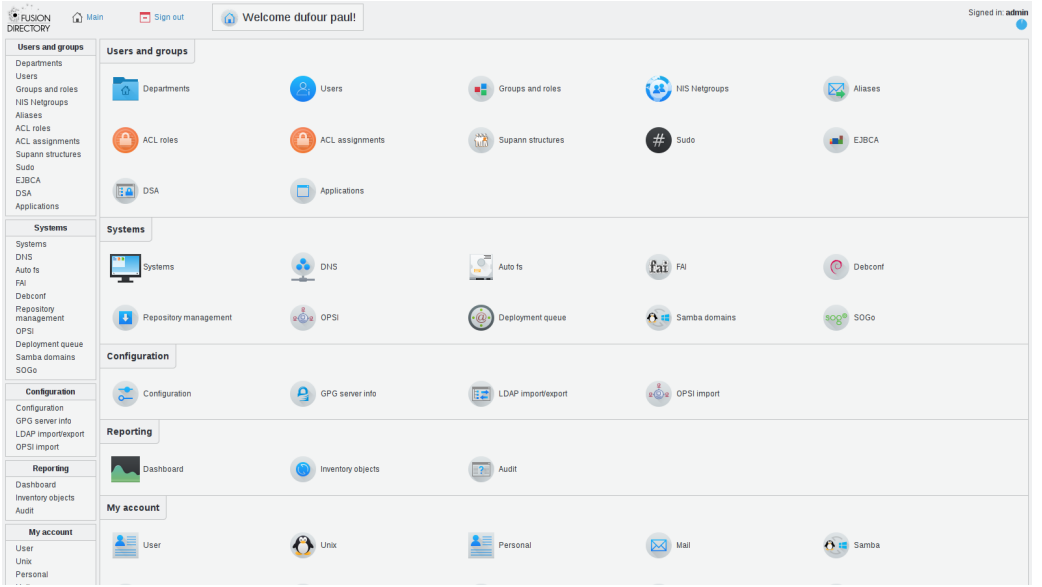


Directory Server (OpenLDAP)

- Annuaire LDAPv3 standard
- Stockages des comptes utilisateurs, groupes et comptes de services
- Politiques de mot de passe
- Scripts de sauvegarde et restauration

Directory Manager (Fusion Directory)

- Interface web de gestion des données
- Délégation et gestion des autorisations
- API REST
- Déclenchement de scripts (triggers)

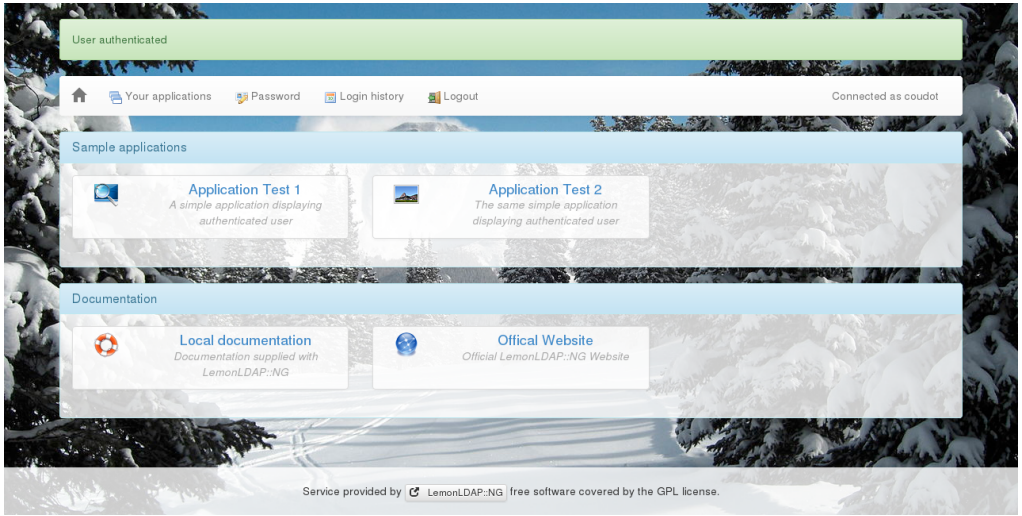


Sync Connector (LSC)

- Outil de synchronisation en ligne de commande
- Nombreux connecteurs :
  - Annuaires LDAP
  - Bases de données
  - API REST
  - Scripts

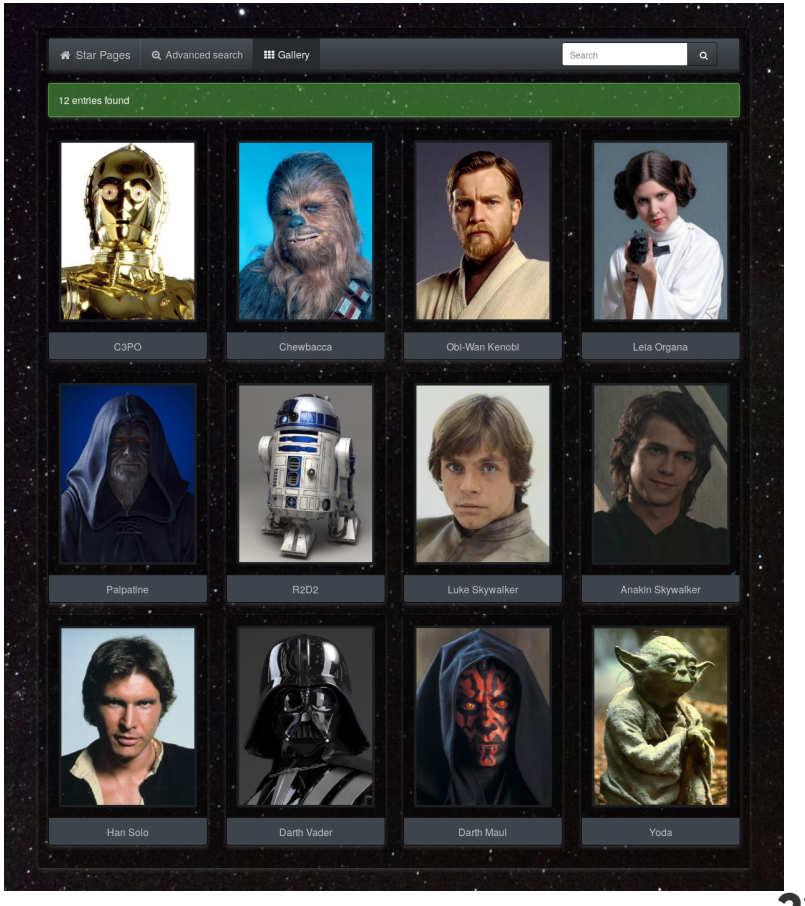
Access Manager (LemonLDAP::NG)

- Serveur SAML et OpenID Connect
- Gestion 2FA/MFA
- Menu des applications
- Contrôle d'accès centralisé



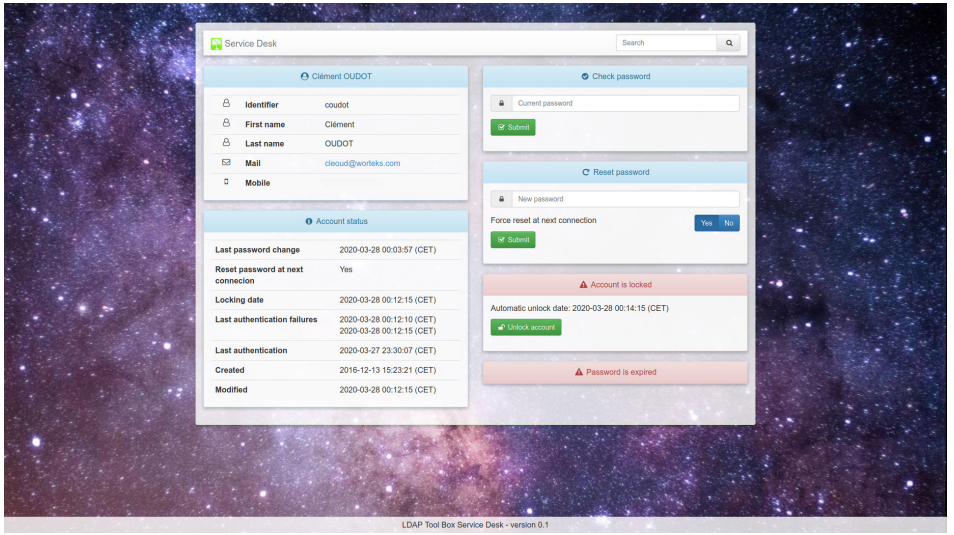
White Pages (LDAP Tool Box)

- Affichage des utilisateurs et des groupes
- Affichage des photos
- Recherche avancée
- Export CSV et vCard



Service Desk (LDAP Tool Box)

- Vérification et réinitialisation des mots de passe
- Blocage et déblocage des comptes
- Informations du compte
- Tableaux de bord



Passage au mode SaaS : W'IDaaS

IDaaS

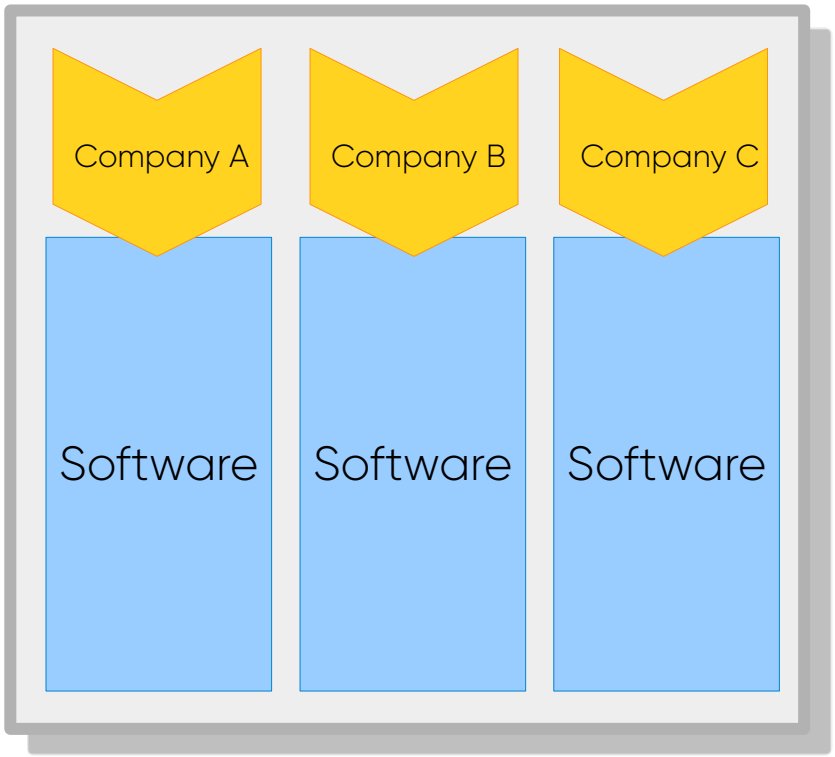
Identity as a Service

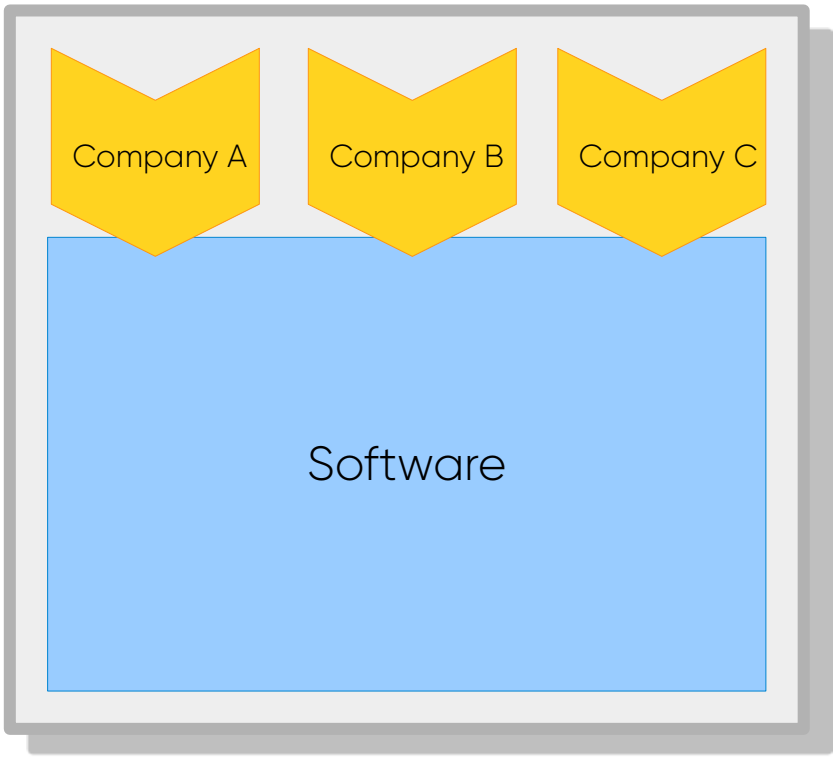
Avantages et inconvénients du Cloud

- Pas d'installation ou de mise à jour de logiciel
- Pas d'infrastructure
- Disponibilité et montée en charge

- Données hébergées par une autre société
- Moins d'intégration avec le SI interne
- Limitations des fonctionnalités

Isolation / multi-tenants

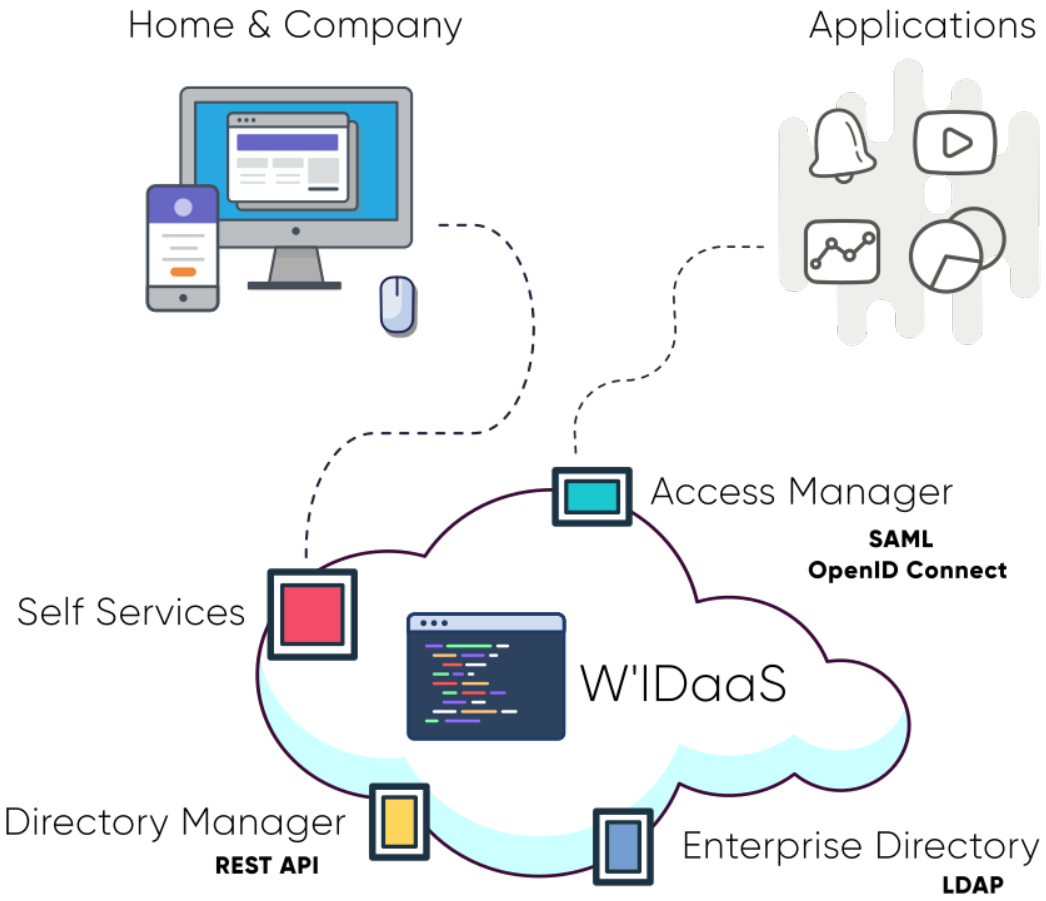




W'IDaaS

- 100 % basé sur le code Open Source de FusionIAM
- Hébergement et infogérance par Worteks
- Données stockées en France
- Utilisation des protocoles standards
- API REST pour les gestion des comptes et des applications

W'IDaaS


Home & Company
Applications
Access Manager
SAML
OpenID Connect
Self Services
W'IDaaS
Directory Manager
REST API
Enterprise Directory
LDAP

Déployer et tester le service

1) Préparer sa configuration (ENVVAR)
2) Installer podman
3) Cloner le dépôt
4) Lancer les conteneurs

```
ACCCONFIGROOTPW=secret
ACCDATAROOTPW=secret
ADMIN_LDAP_PASSWORD=secret
CUSTOMERID=acme
FUSIONDIRECTORY_LDAP_PASSWORD=secret
FUSIONDIRECTORY_LDAP_USERNAME=fd
LSC_LDAP_PASSWORD=secret
LSC_LDAP_USERNAME=lsc
SERVICEDESK_LDAP_PASSWORD=secret
SERVICEDESK_LDAP_USERNAME=sd
WHITEPAGES_LDAP_PASSWORD=secret
WHITEPAGES_LDAP_USERNAME=wp
```

```
$ git clone https://gitlab.ow2.org/fusioniam/fusioniam.git
$ fusioniam/run/start-all.sh
```

Merci