

A full Open Source Identity & Access Management solution



FOSDEM 2024

\$ ldapwhoami



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, a comprehensive offering

Heterogeneous and complex infrastructures, troubleshooting, cloud, email, identity, authentication, security... **Worteks** addresses numerous issues related to your information system.

Studies, audit, and consulting

Technical expertise

Technical support

Specific skills transfer

R&D and innovation

Custom solutions

Worteks leverages its expertise to provide its clients with packaged solutions, entirely composed of key components from the Open Source ecosystem

 **V'Sweet**

Collaborative applications portal

Shared development platform

 **V'Opla**

 **V'IDaaS**

Identity and access management

These solutions are available, either **On-Premise** or **SaaS** and **PaaS** models, on our environments, according to your preference



#jobcorner



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

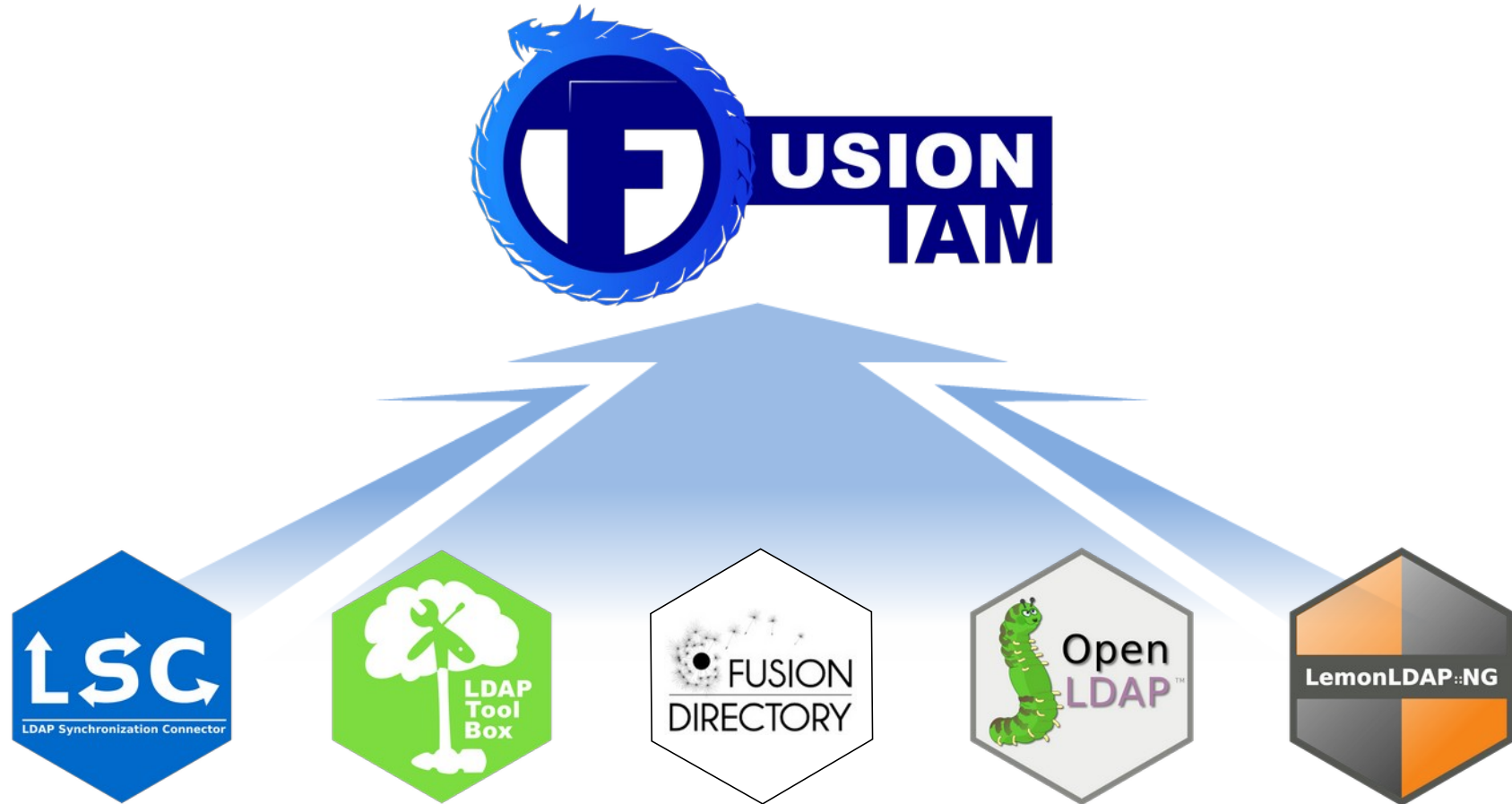


The FusionIAM project

History

- Founded in 2018 by Benoit MORTIER (Fusion Directory) and Clément OUDOT (Worteks)
- Goal: put together open source software to build a global IAM (Identity and Access Management) solution
- Project lead: Worteks (David COUTADEUR, Clément OUDOT)
- Official OW2 project : <https://gitlab.ow2.org/fusioniam>

Do not reinvent the wheel



Components

**FusionIAM
White Pages**

**FusionIAM
Access Manager**

**FusionIAM
Sync Connector**

**FusionIAM
Service Desk**

**FusionIAM
Directory Server**

**FusionIAM
Directory Manager**



Components and softwares

**FusionIAM
White Pages**



**FusionIAM
Access Manager**



**FusionIAM
Sync Connector**



**FusionIAM
Service Desk**



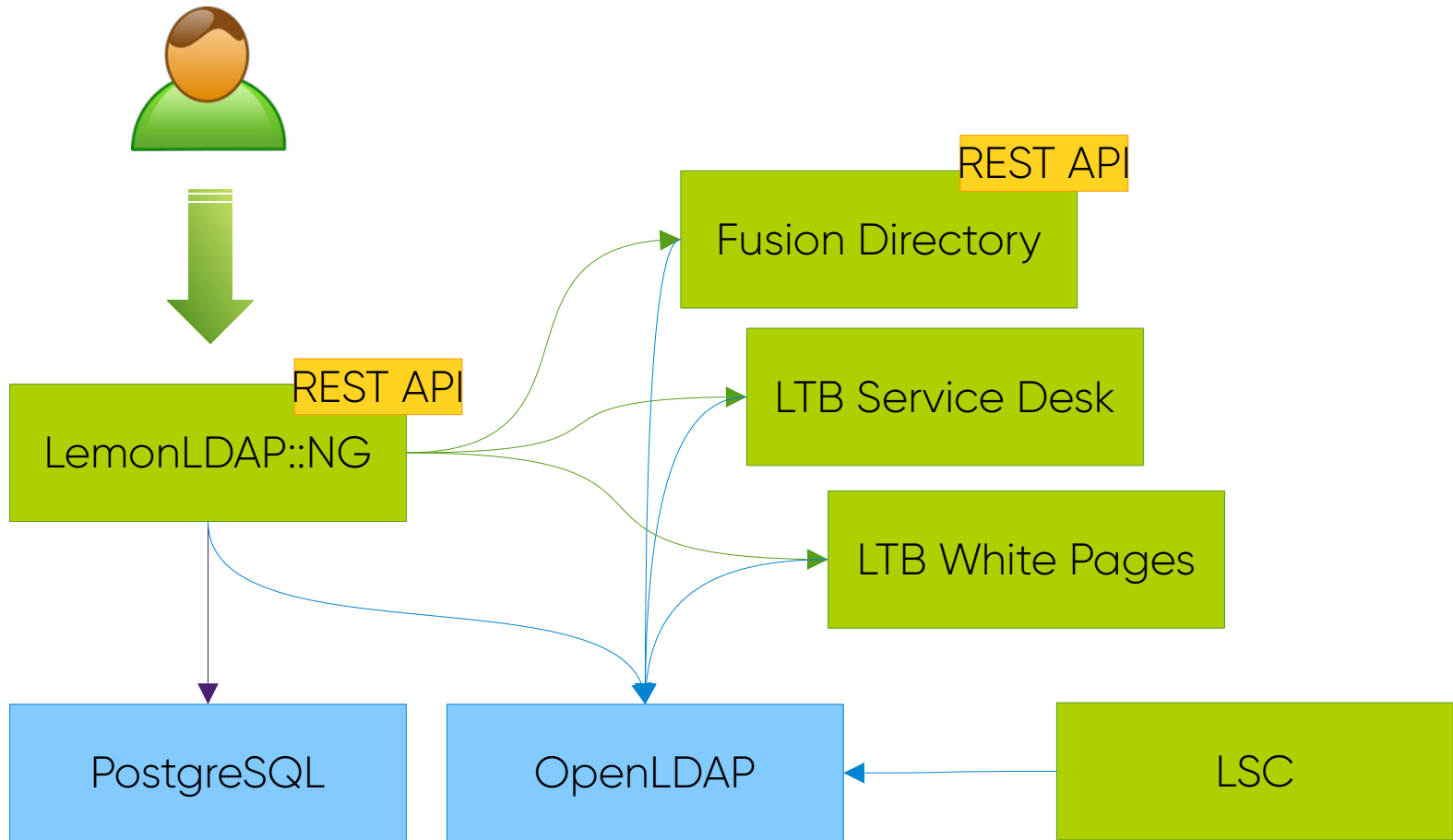
**FusionIAM
Directory Server**



**FusionIAM
Directory Manager**



Architecture



Zoom on selected softwares

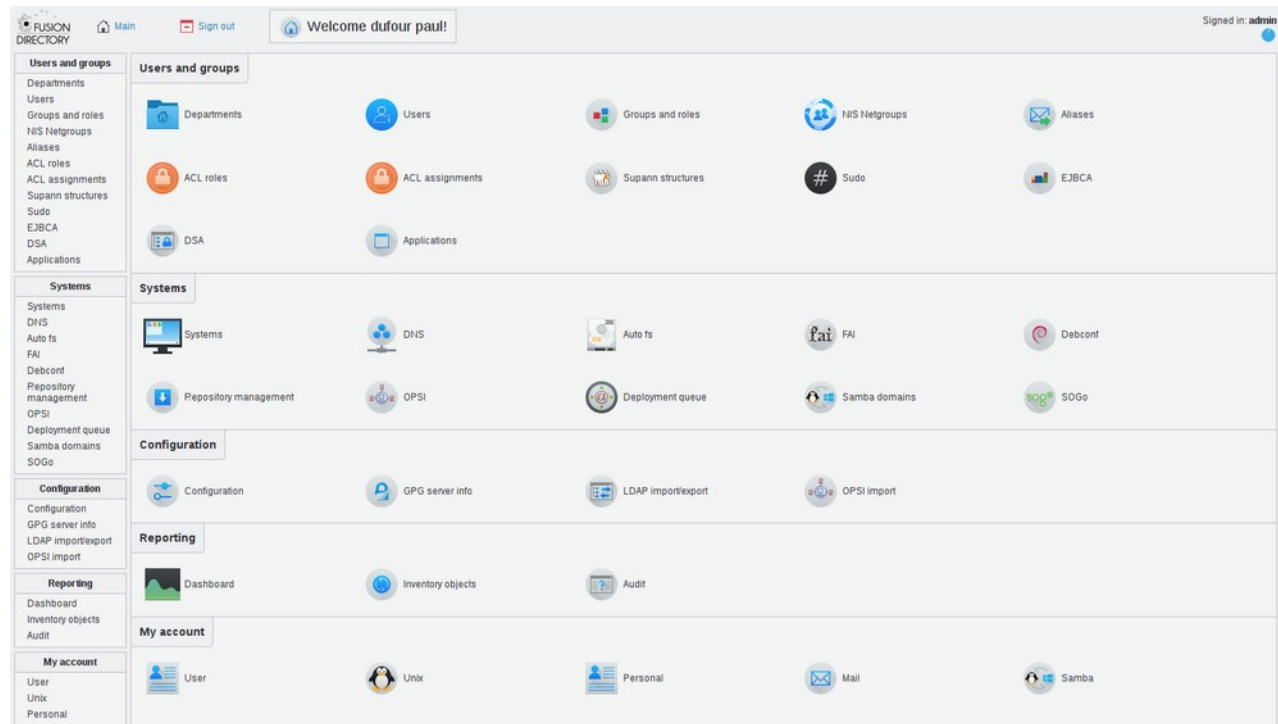
OpenLDAP

- Like Tina Turner said, it's simply the best (LDAP server)
- Many backends and overlays (password policy, dynamic groups...)
- Packaging and utilities provided by LDAP Tool Box Project



Fusion Directory

- Web UI for managing all LDAP objects
- Administration delegation
- REST API (not SCIM)
- Hooks/Triggers



LDAP Synchronization Connector

- Command Line Interface
- Many connectors:
 - LDAP Directories
 - Active Directory
 - Databases (SQL)
 - REST API
 - Scripts

```
Fichier Edition Affichage Signets Modules externes Configuration Aide
Janv. 18 16:53:30 - INFO - Starting sync for MySyncTask
Janv. 18 16:53:31 - INFO - # Adding new object mail=luke@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
Janv. 18 16:53:31 - INFO - # Adding new object mail=darth@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
# Wed Jan 18 16:53:31 CET 2023
dn: mail=darth@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: dvader
userPassword: changethis
mail: darth@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Darth Vader
sn: Vader

# Wed Jan 18 16:53:31 CET 2023
dn: mail=luke@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: lskywalker
userPassword: changethis
mail: luke@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Luke Skywalker
sn: Skywalker

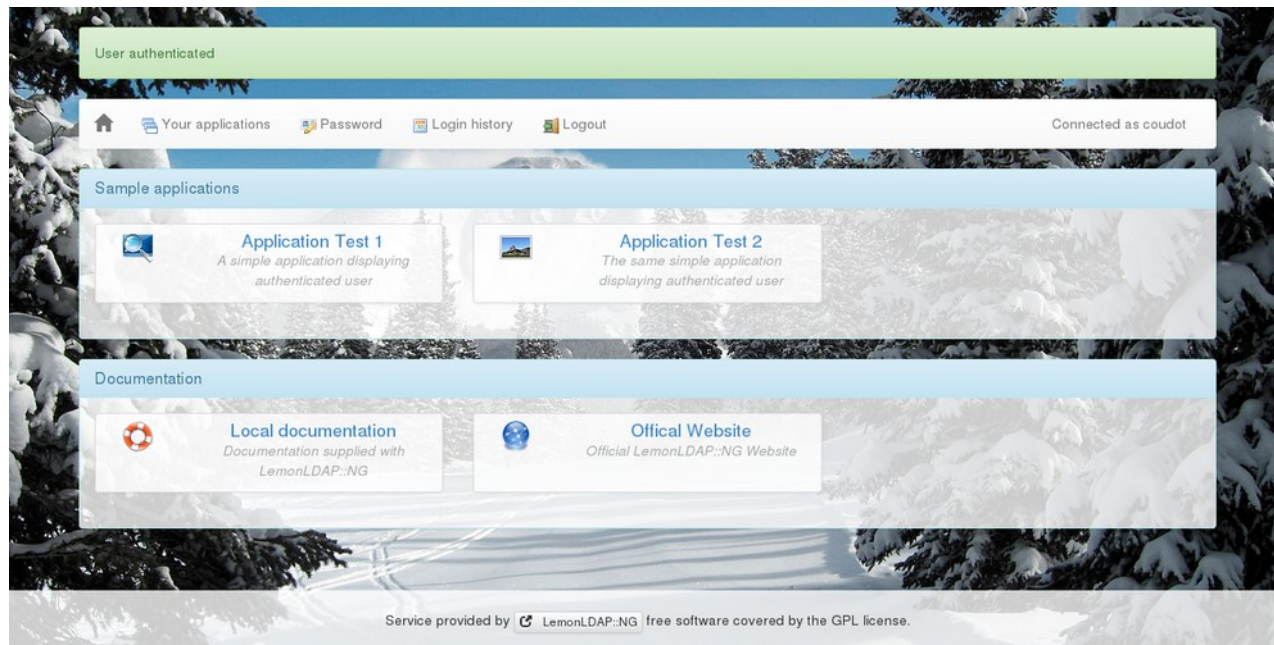
Janv. 18 16:53:31 - INFO - # Adding new object mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
# Wed Jan 18 16:53:31 CET 2023
dn: mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: lorgana
userPassword: changethis
mail: leia@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Leia Organa
sn: Organa

Janv. 18 16:53:31 - INFO - All entries: 3, to modify entries: 3, successfully modified entries: 3, errors: 0
Janv. 18 16:53:31 - INFO - Starting clean for MySyncTask
Janv. 18 16:53:31 - INFO - All entries: 3, to modify entries: 0, successfully modified entries: 0, errors: 0
clement@ader-worleks:~/Téléchargements/lsc-2.1.6/sample/hsqlDb$
```



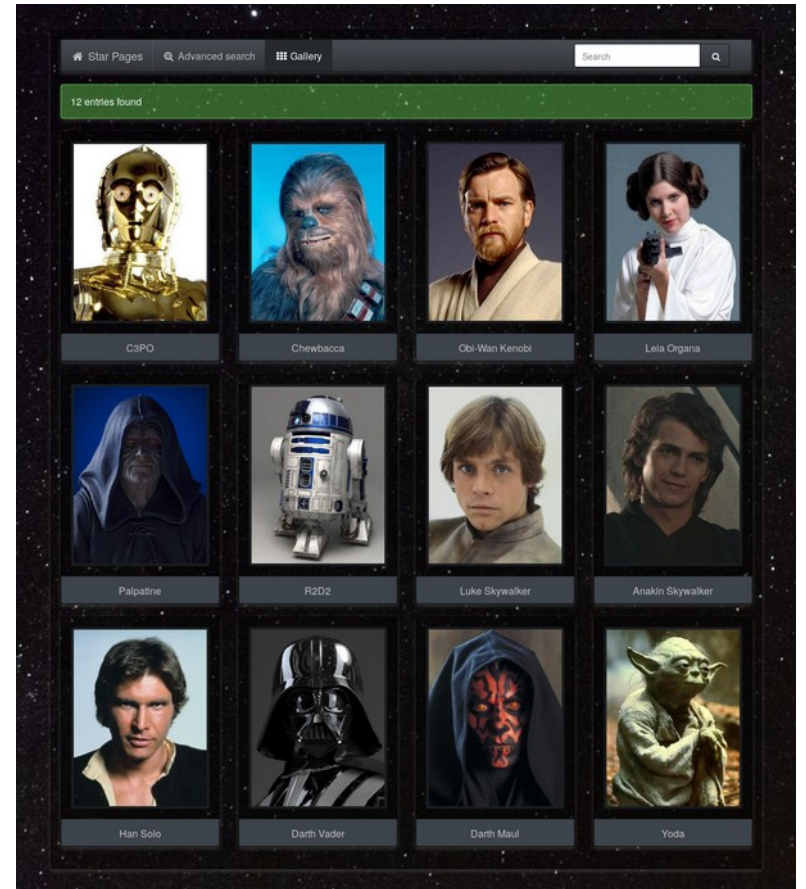
LemonLDAP:NG

- Web Single Sign On and access control
- CAS, SAML and OpenID Connect
- 2FA/MFA
- Application menu
- REST API



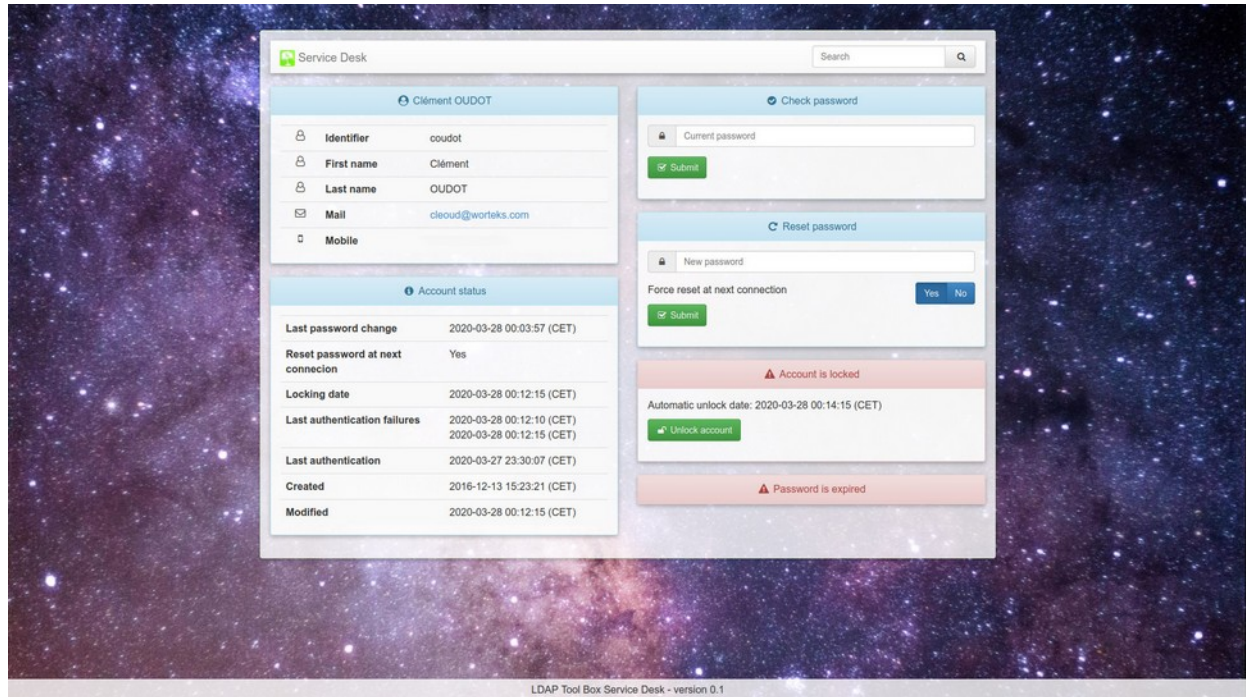
White Pages (LDAP Tool Box)

- Search for users and groups
- Quick and advanced search
- Export vCard and CSV
- Display people on a map (OpenStreetMap)



Service Desk (LDAP Tool Box)

- Check and reset passwords
- Lock and unlock accounts
- Comprehensive password policy status
- Dashboards



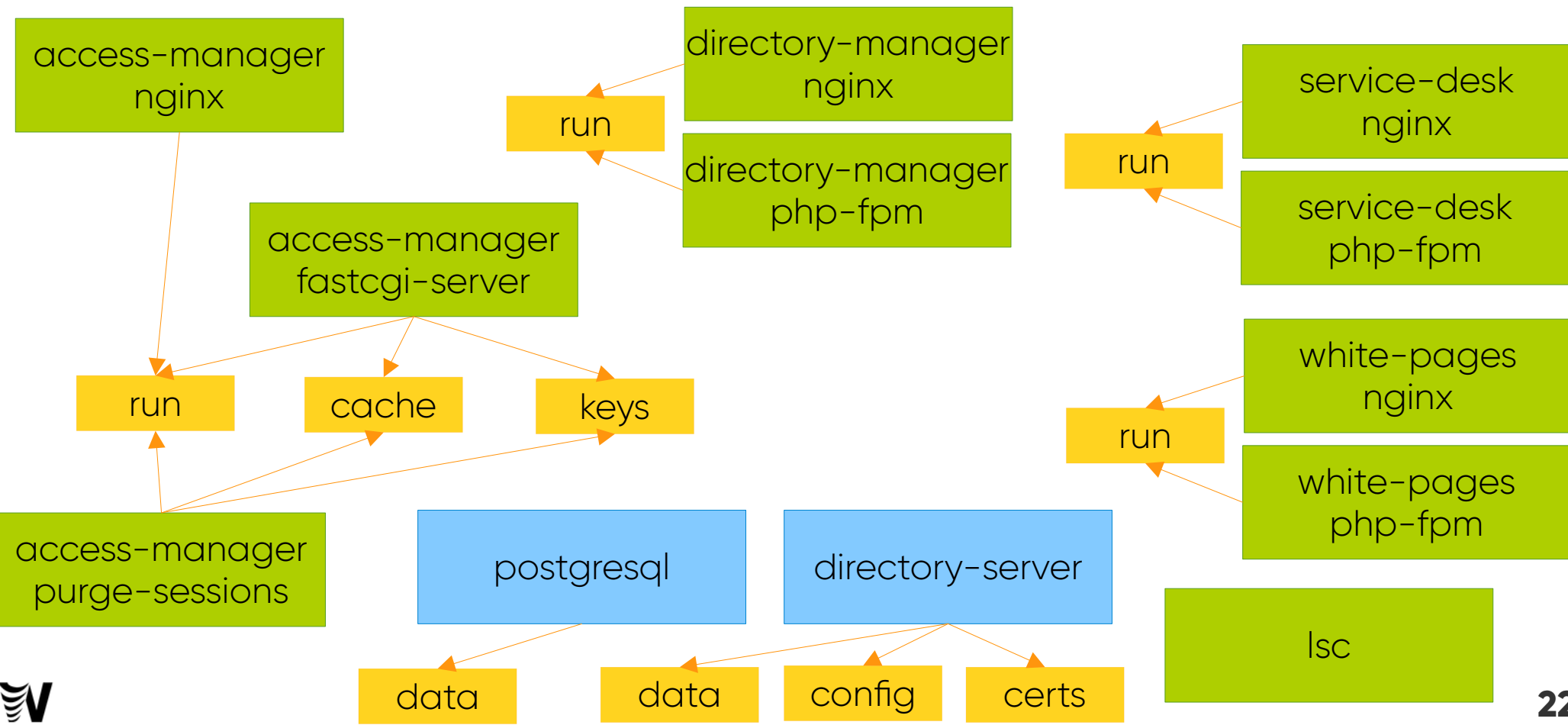
Moving to the Cloud



From packages to containers

- What we do for years:
 - Install separately all components through packages (Debian/Red Hat)
 - Configure all softwares to let them talk to each other
 - Apply graphical customization for all products (logo, background)
 - Follow releases and updates
- Cloud approach:
 - Containers with volumes
 - Global configuration through environment variables

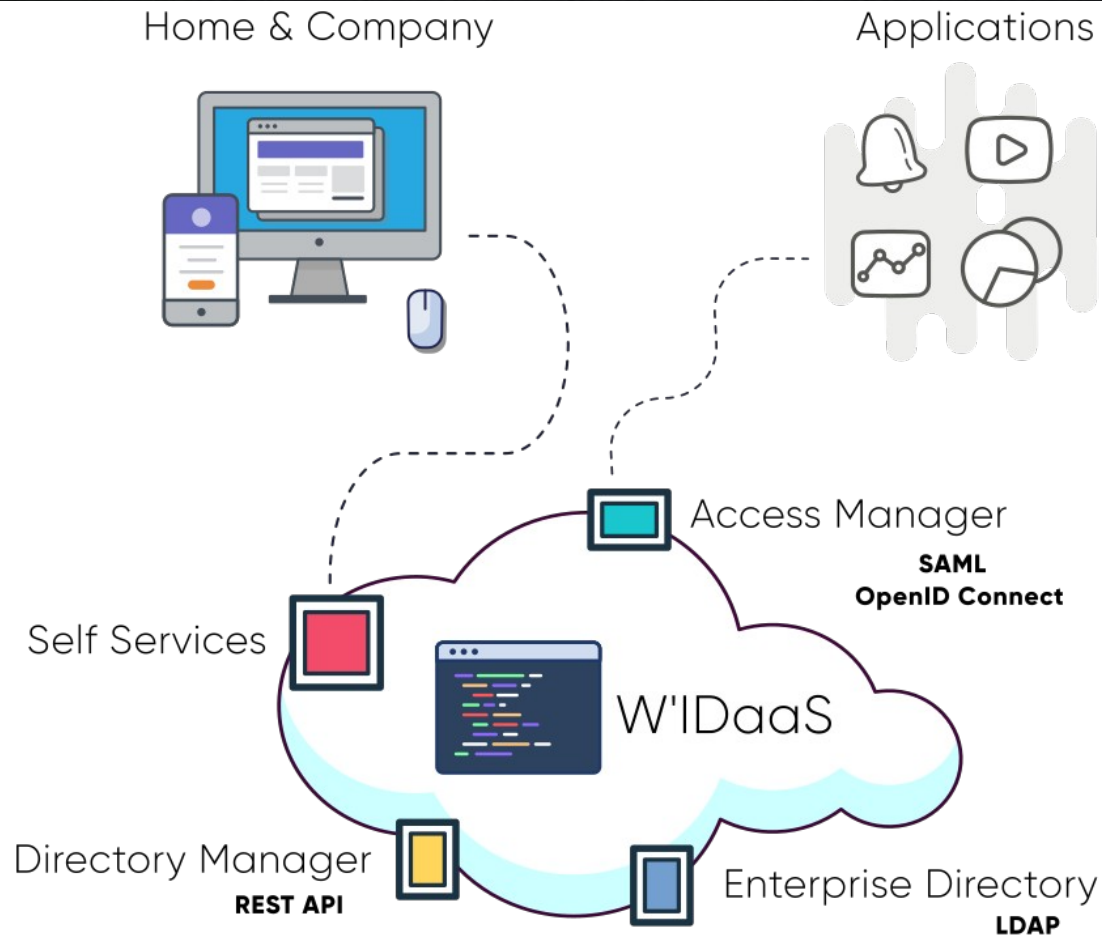
Pods and volumes



How to run FusionIAM

- All images available at:
https://gitlab.ow2.org/fusioniam/fusioniam/container_registry
- Run it with docker, podman or even docker-compose:
`docker-compose up -d`
- Use the local Makefile:
`make runall`
- Preparation:
 - Create volumes
 - Populate ENVVAR

W'IDaaS – 100% Open Source IDaaS



Demo effect



<https://auth.ow2.widaas.cloud/>





Thank you



info@worteks.com



[@worteks_com@mastodon.social](https://mstdn.social/@worteks_com)



[@worteks_com](https://twitter.com/worteks_com)



[linkedin.com/company/worteks](https://www.linkedin.com/company/worteks)

www.worteks.com