Pass the SALT | 2021 edition

The Free Software & Security CONFERENCE

July, 5 to 7 2021 VIRTUAL

Our Mission:

"Building bridges between Security communities and Free Software hackers!"

Hosting Identity in the Cloud with free softwares

worteks

make IT work, make IT free

Speaker

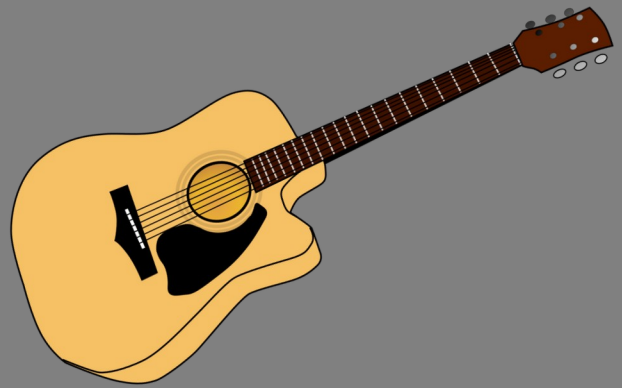
Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot

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

KPTN - https://kptn.org
DonJon Legacy
Improcité

Musical introduction



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

IAM

Identity and Access Management

- Identity Management:
  - Account creation and deletion (lifecycle management)
  - Provisioning into Information System
  - User self services (account edition, password change, ...)
  - Identity reconciliation
- Access Management:
  - Give permissions to users
  - Apply authorizations
  - Audit access

Identity Lifecycle

Account creation

Account deletion

Information update

IAM market

Figure 1. Magic Quadrant for Access Management, Worldwide

Source: Gartner (June 2018)

- Market hold by big closed source editors
- Mostly american companies
- Sofwares with many features but often complex to install and administrate
- Licence fee per user

Open Source

IAM in Open Source

- A lot of Open Source products already exist but:
  - They cover only a subset of IAM features
  - They don't integrate easily each others, even if they respect standard protocols
- The FusionIAM initiative has choosen some of these products and propose to ship them as a unified platform
- Free software and Open Source, backed by Worteks and Fusion Directory companies


USION
IAM


LSC
LDAP Synchronization Connector


LDAP
Tool
Box


FUSION
DIRECTORY


Open
LDAP


LemonLDAP::NG


OW2
USION
IAM


OW2
LSC
LDAP Synchronization Connector


OW2
LDAP
Tool
Box


OW2
FUSION
DIRECTORY


Open
LDAP


OW2
LemonLDAP::NG

Features

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

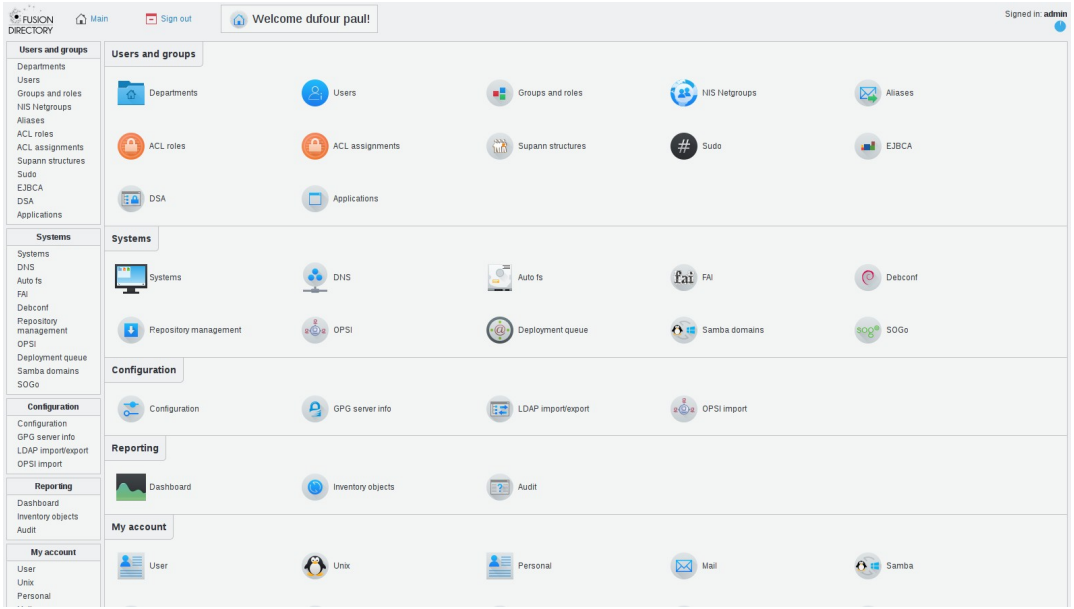
FusionIAM Directory Manager

FusionIAM Directory Server

- Users and groups
- Service accounts
- Password policies
- LDAP protocol available only for internal components
- Backup and restore scripts

FusionIAM Directory Manager

- Web interface
- Authorization framework
- REST API
- Triggers

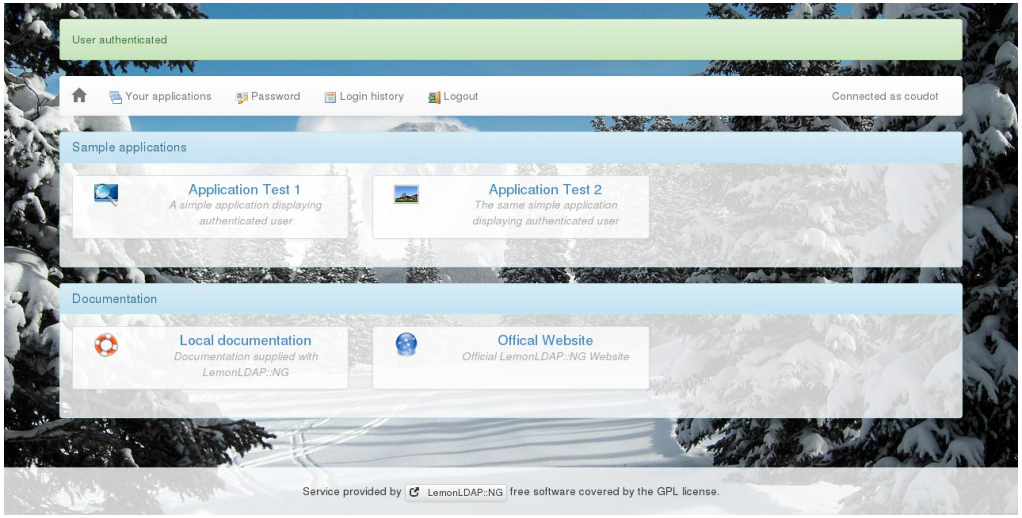


FusionIAM Sync Connector

- Command line synchronization engine
- Many connectors:
  - LDAP directories
  - Databases
  - REST API
  - Scripts

FusionIAM Access Manager

- SAML and OpenID Connect server
- Second factor (2FA)
- Application menu
- Password management
- Centralized access control

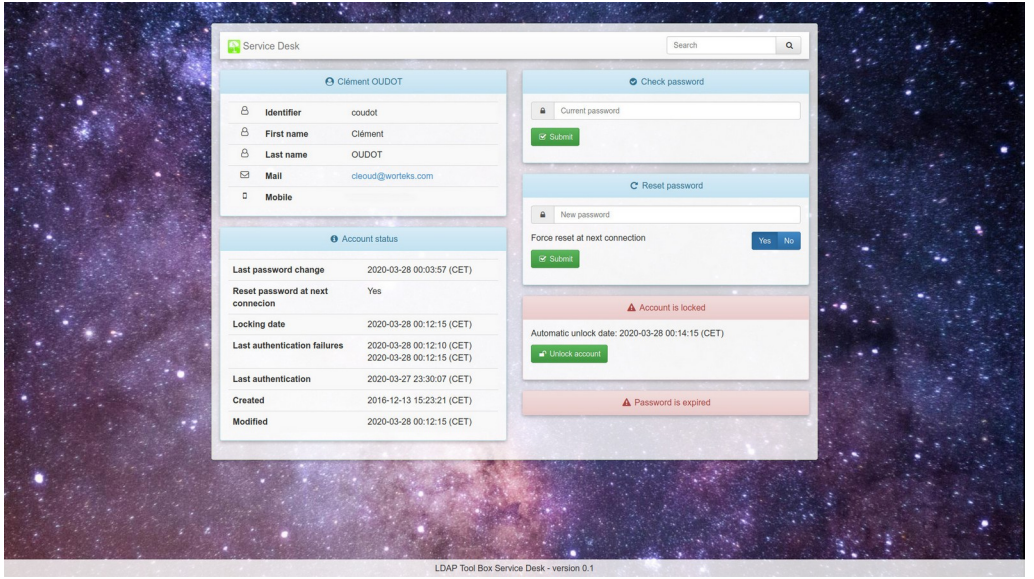


FusionIAM White Pages

- Browse user and groups
- Display photos
- Advanced search
- Export CSV and vCard

FusionIAM Service Desk

- Check and reset password
- Lock and unlock account
- Account information
- Dashboards



Identity in the Cloud

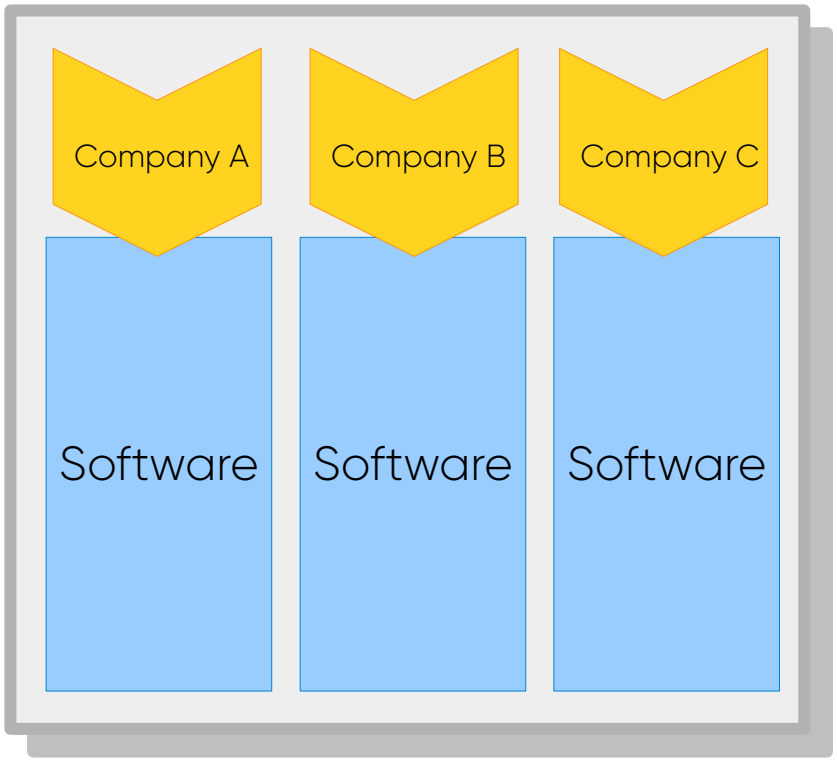
IDaaS

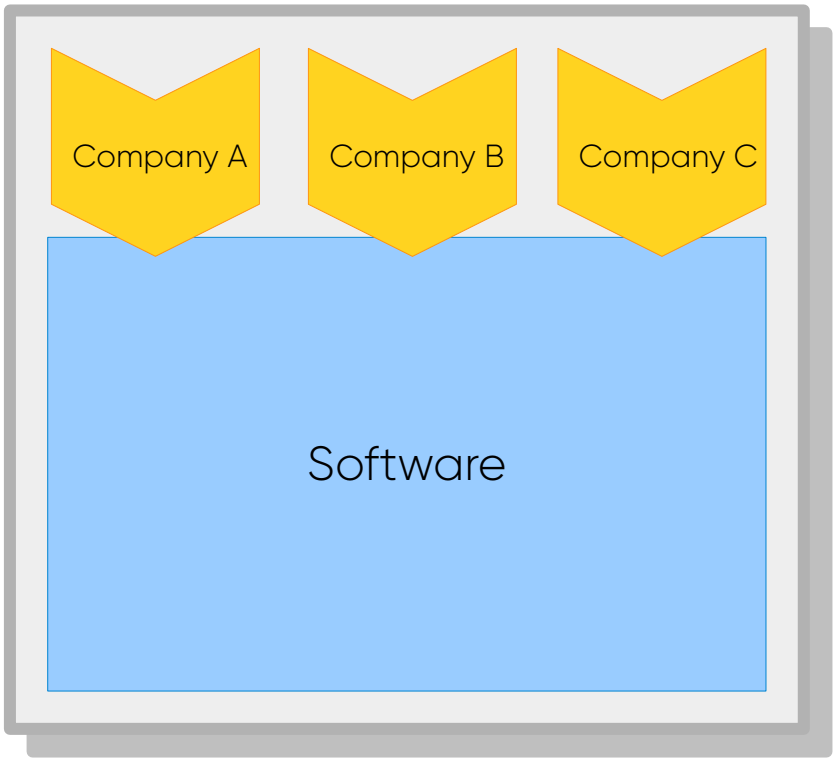
IDentity as a Service

Choosing the Cloud

- Benefits:
  - No installation or software updates
  - No infrastructure
  - Availability and scalability
- Drawbacks:
  - Data hosted by another company
  - Integration with internal information system is more difficult
  - Reversibility not always easy (read the contract)

Isolation versus Multitenancy





Infrastructure stack

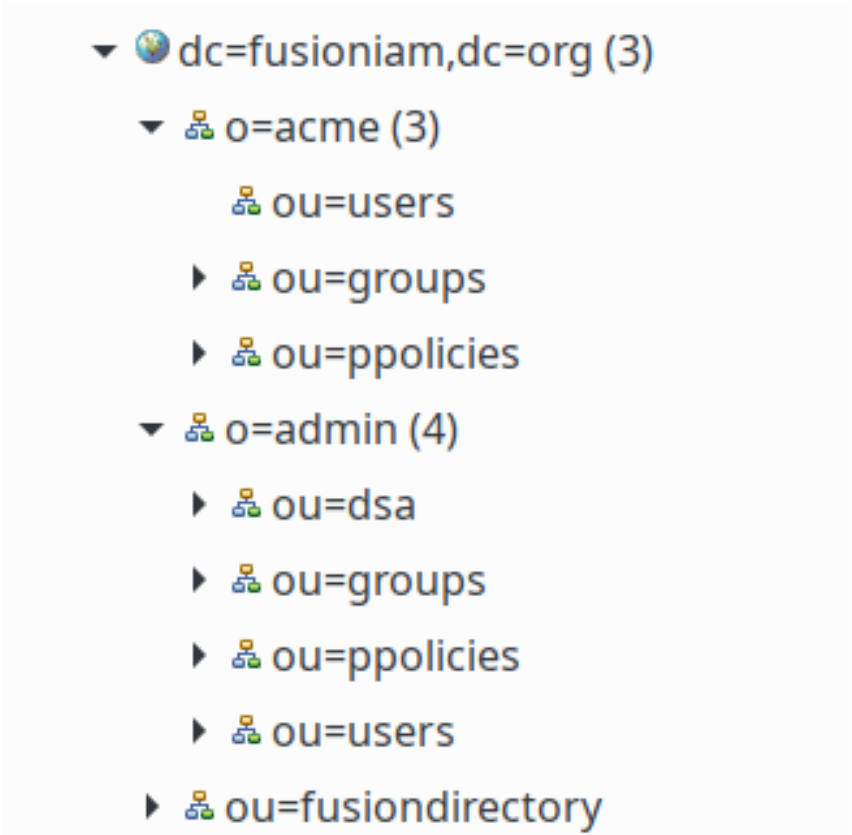
- Images build: **Podman** or **Docker**
- Software deployment and initial configuration: **Ansible**
- Images run: **Podman** or **Openshift**
- Images registry: OW2 **Gitlab** registry or **Openshift** registry
- Operating system: **CentOS**
- Configuration settings passed as environement variables

Containers

- Running software in containers:
  - Define volumes for all persistent data
  - Expose and map ports to allow communication to containers and between containers
  - All required files should be present in container image or mounted as volumes, and should only be modified when container starts
  - It should be possible to run several containers at the same time, for scalability

Data Model

- LDAP directory splitted in two main branches:
  - Customer: data than can be managed directlry by the customer (users, groups)
  - Admin: data dedicated to service hoster (technical and service accounts, security groups)



Ready to go?

Configuration

- Prepare configuration in ENVVAR file

```
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
```

- Prepare volumes

Run

- Launch every images:

```
podman run \
  --env-file=./run/ENVVAR.example \
  -v ./run/volumes/ldap-data:/usr/local/openldap/var/openldap-data \
  -v ./run/volumes/ldap-config:/usr/local/openldap/etc/openldap/slapd.d \
  --rm=true \
  -p 127.0.0.1:33389:33389 \
  --name=fusioniam-directory-server \
  --detach=true \
  --no-hosts \
  gitlab.ow2.org:4567/fusioniam/fusioniam/fusioniam-centos8-openldap-ltb:v0.1
```

- Start creating user and groups
- Connect applications

From POC to PROD

- POC:
  - Generic images available on OW2 Gitlab registry
  - Run with podman or systemd
  - Local reverse proxy
- PROD:
  - Optional: rebuild or derivate images
  - Optional: store images in a dedicated registry
  - Run with Kubernetes or Openshift
  - Configure Security Contexts
  - Frontal reverse proxy with valid SSL certificate

Useful links

- Main site:
  - https://fusioniam.org/
- Source code:
  - https://gitlab.ow2.org/fusioniam/fusioniam/-/tree/master
- Mailing lists:
  - https://mail.ow2.org/wws/subscribe/fusioniam-users
  - https://mail.ow2.org/wws/subscribe/fusioniam-dev
- IRC:
  - #fusioniam on libera.chat

worteks

make IT work, make IT free

THANKS

info@worteks.com

@worteks_com

linkedin.com/company/worteks