worteks

make IT work, make IT free

OW2 con'21

Hosting Identity in the Cloud with OW2 free softwares

Speaker

Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot

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

KPTN
DonJon Legacy
Improcité

https://kptn.org

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

FusionIAM main features

- Authentication portal
- Application menu
- Second factor authentication (2FA)
- White pages
- Service desk
- Users/groups management
- CAS, SAML and OpenID Connect server
- Web services

Identity in the Cloud

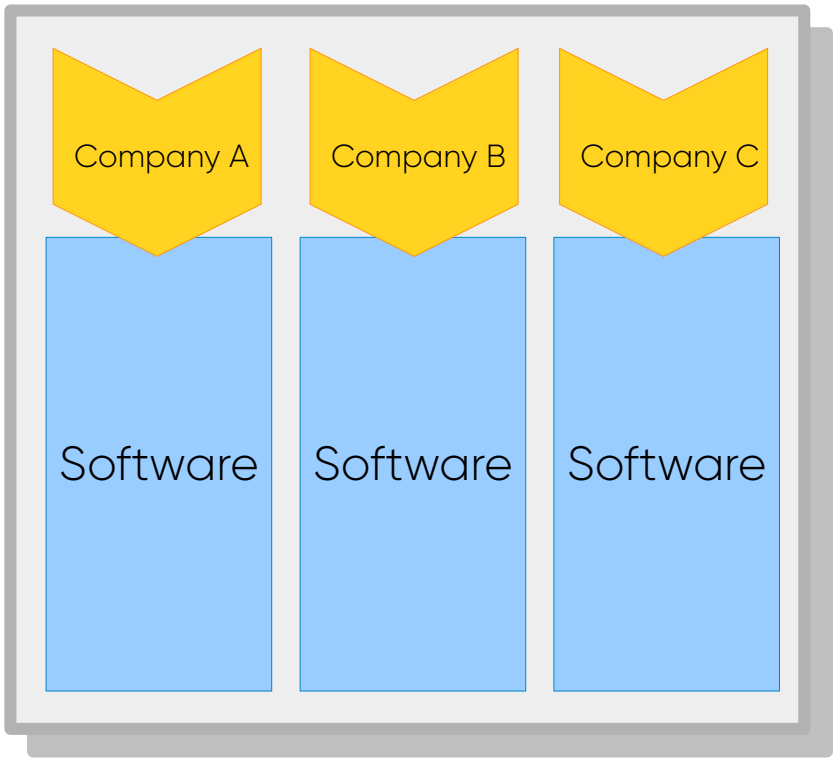
IDaaS

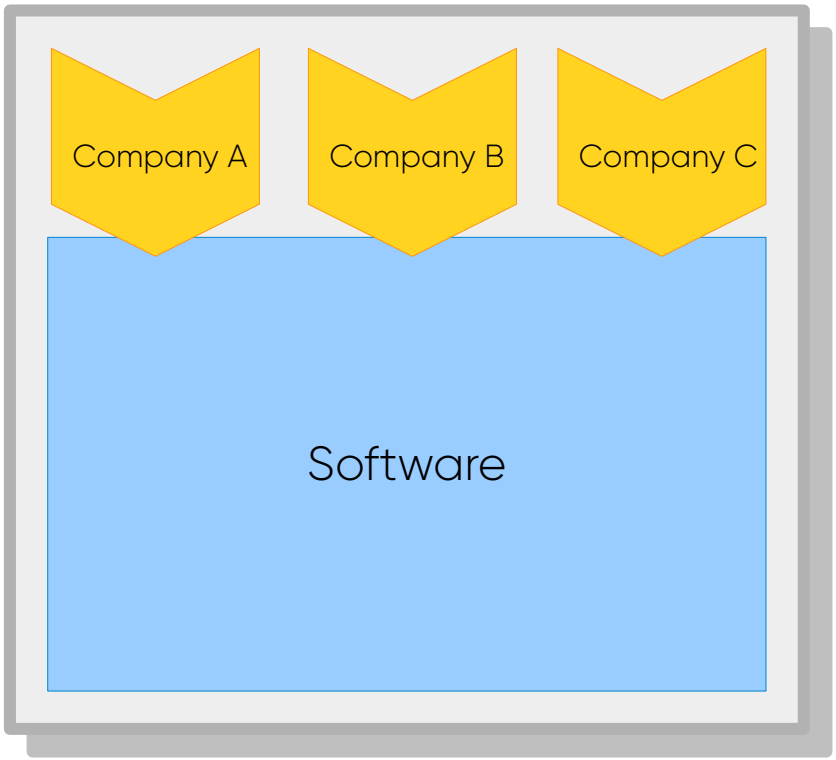
IDentity as a Service

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

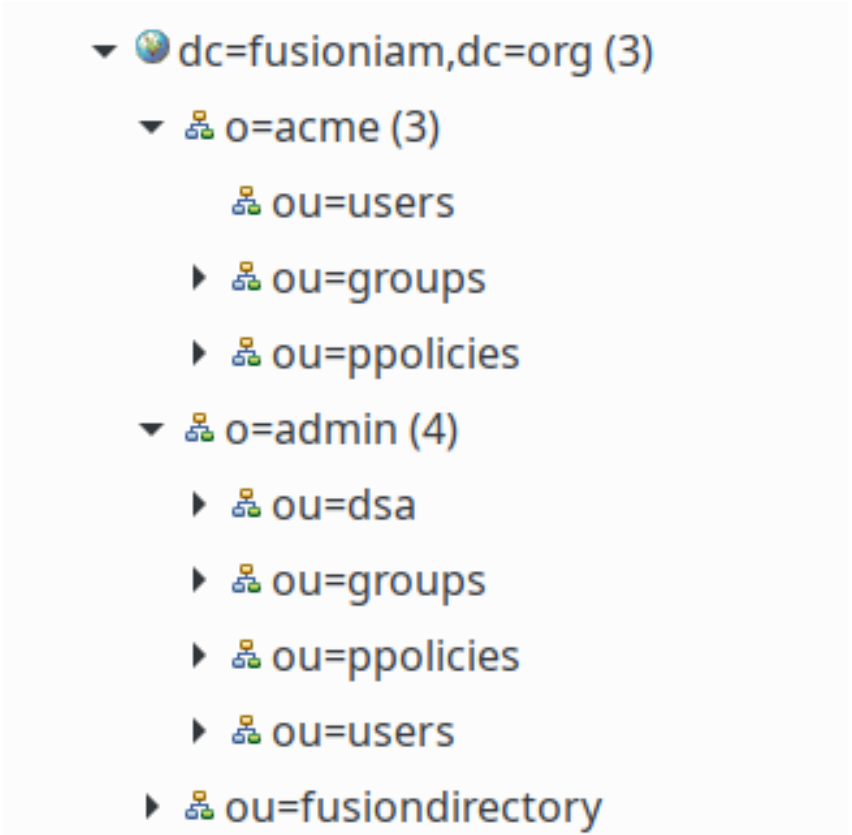
- Images build: **Podman** or **Docker**
- Software deployment and initial configuration: **Ansible**
- Images run: **Podman** or **Openshift**
- Images registry: OW2 **Gitlab** registry or **Openshift** registry
- Operating system: **CentOS**
- Configuration settings passed as environement variables

Containers

- Running software in containers:
  - Every data written in the container is lost when the container restarts, data should only be written in persistent storages
  - Routes need to be defined to allow communication to containers and between containers
  - All required files should be present in container image, and could 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
```

Run

- Run an image with podman:

```
podman run \
  -v ./ENVVAR:/ENVVAR \
  -p 33389:33389 \
  gitlab.ow2.org:4567/fusioniam/fusioniam/fusioniam-centos8-openldap-ltb:v0.1
```

- Systemd services also available

From POC to PROD

- POC:
  - Generic images available on OW2 Gitlab registry
  - Run with podman or systemd
- PROD:
  - Rebuild or derivate images
  - Store images in dedicated registry
  - Run with openshift

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

worteks

make IT work, make IT free

THANKS

info@worteks.com

@worteks_com

linkedin.com/company/worteks