
# 24 octobre 2023 - PARIS

# Des outils 100% Open Source pour gérer votre annuaire LDAP et votre Active Directory

Clément OUDOT

Vorteks
make IT work, make IT free

Clément OUDOT
Identity Solutions Manager

PRO :

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

PERSO :

- KPTN
- DonJon Legacy
- Improcité

# AGENDA DE LA CONFÉRENCE

- Introduction en chanson
- Annuaires LDAP / Active Directory
- Le projet LDAP Tool Box
  - Self Service Password
  - White Pages
  - Service Desk
- Le projet LDAP Synchronization Connector

Worteks

make IT work, make IT free

Infrastructures hétérogènes et complexes, troubleshooting, cloud, mail, identité, authentification, securité... **Worteks** intervient sur une multitude de problématiques associées à votre système d'information.

- Études, audit et conseil
- Expertise technique
- Support technique
- Transfert de compétences spécifique
- R&D et innovation

# Worteks

make IT work, make IT free

**Worteks** utilise son savoir-faire pour mettre à la disposition de ses clients des solutions packagées, intégralement composées des briques majeures de l'écosystème Open Source

**V'Sweet** — Portail d'applications collaboratif

**V'Opla** — Plateforme mutualisée de développement

**V'IDaaS** — Gestion des identités des accès

Ces solutions sont disponibles, au choix, **On Premise** ou en **SaaS** et en **PaaS** sur nos environnements

Worteks

make IT work, make IT free

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

# Introduction en chanson

# Arbre en panne – Francis CabreLDIF

On croyait savoir tout sur l'annuaire
Depuis toujours,
LDAP par cœur et les arborescences
Que l'on parcoure.
Des RFC et le schéma Supann,
Un standard qui circule dans des trames
Le protocole que l'on déploie
tous chez soi.

Les serveurs LDAP qui marchent sont là
Depuis toujours
Voilà qu'il arrive
Et que plus rien n'est mis à jour
Active Directory, c'est ça le drame
Est le premier service que l'on scanne
Le SI s'est ouvert par endroits
Depuis ça.

Pas besoin de phrases ni de longs discours
Ça casse tout dedans ça casse tout autour
Pourvu que jamais Active Directory
Ne devienne la norme que l'on suit
Les outils libres et open source
Sont là pour ça

# Annuaires LDAP / Active Directory

# Le protocole LDAP

→ Annuaire

- ensemble de données
- beaucoup d'enregistrements de petite taille
- souvent lus, rarement mis à jour
- recherches simples

→ **L**ightweight **D**irectory **A**ccess **P**rotocol

- issu de X.500, apparu à la fin des années 1980
- plus léger par rapport à X.500 DAP et DSP
- LDAP = protocole d'annuaire électronique (1993)
- standardisé dans plusieurs RFC (RFC 4511)
- LDAPv3 : 1998

# Le protocole LDAP

~~SQL~~

~~NoSQL~~

# Le protocole LDAP

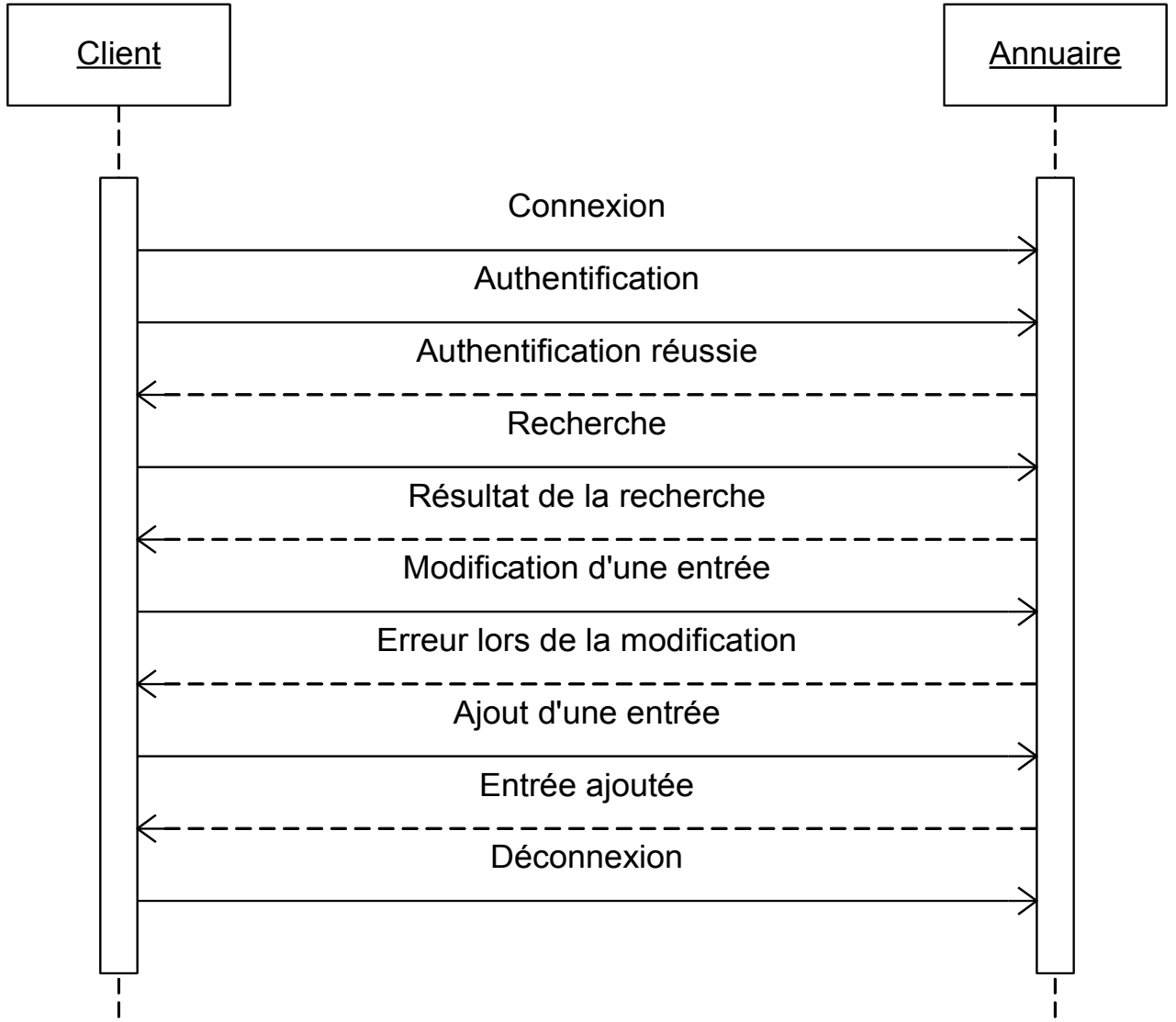
- la communication client serveur
  - au dessus de TCP / IP
  - l'encodage (LBER)

- les mécanismes de sécurité
  - authentification (simple, SASL,…)
  - chiffrement des flux
  - règles d'accès aux données

- les 9 opérations de base
  - bind, unbind, abandon, search, compare, add, modify, delete, modrdn

- le modèle d'information (schéma)

- le modèle de nommage (DIT)



# Active Directory  LDAP

Active Directory prend quelques libertés avec les standards :

- Stockage du mot de passe dans  l'attribut « unicodePwd »
- Mot de passe accessible en écriture uniquement (pas de lecture)
- Classe d'objet « user » insérée entre « organizationalPerson » et « inetOrgPerson »
- Format d'empreinte de temps (timestamp) : nombre d'intervalles de 100 nanosecondes depuis le premier janvier 1601
- Stockage des informations sur le statut du compte dans l'attribut « userAccountControl »

# Le projet LDAP Tool Box


- Projet libre créé en 2009
- Regroupement d'outils dédiés à la gestion des annuaires LDAP
- Au début principalement des paquets OpenLDAP et des scripts de supervision
- Licence GPL
- Publié sur GitHub
- Projet OW2

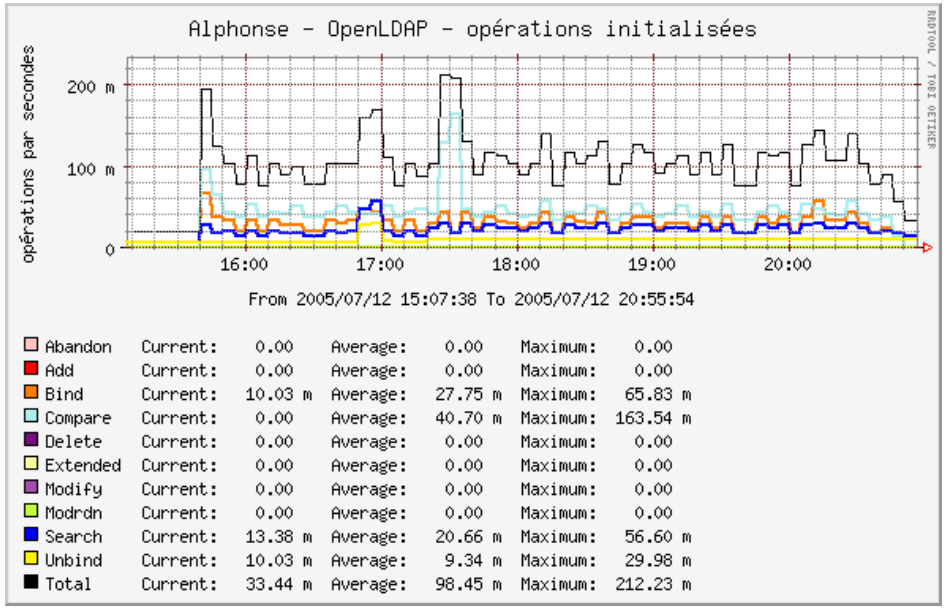
https://ltb-project.org

# OpenLDAP

- Paquets pour les familles de distributions Red Hat (RPM) et Debian (DEB)
- Utilitaire en ligne de commande nommé slapd-cli :
  - Arrêt et relance du service
  - Réindexation de la base
  - Sauvegarde et restauration des données
  - Sauvegarde et restauration de la configuration
  - Import de configurations et de données de démarrage (bootstrap)
  - Statut du service et de la réplication
- Modules et overlays complémentaires (ppm, explockout)

# Supervision

- Greffons Nagios et Cacti :
  - Temps de réponse des annuaires
  - Statut de la réplication
  - État de remplissage des bases
  - Statistiques sur les opérations



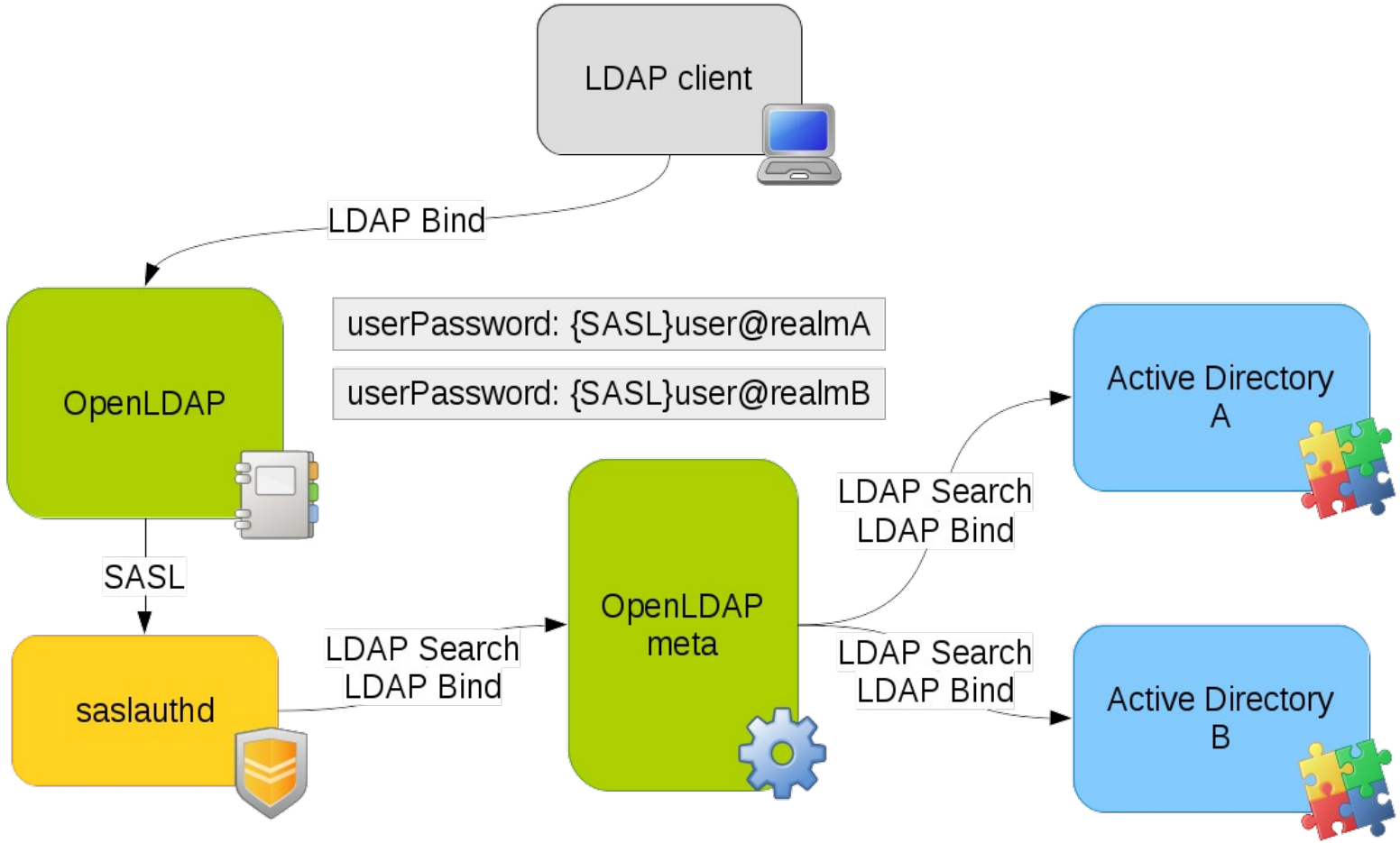

Nagios®

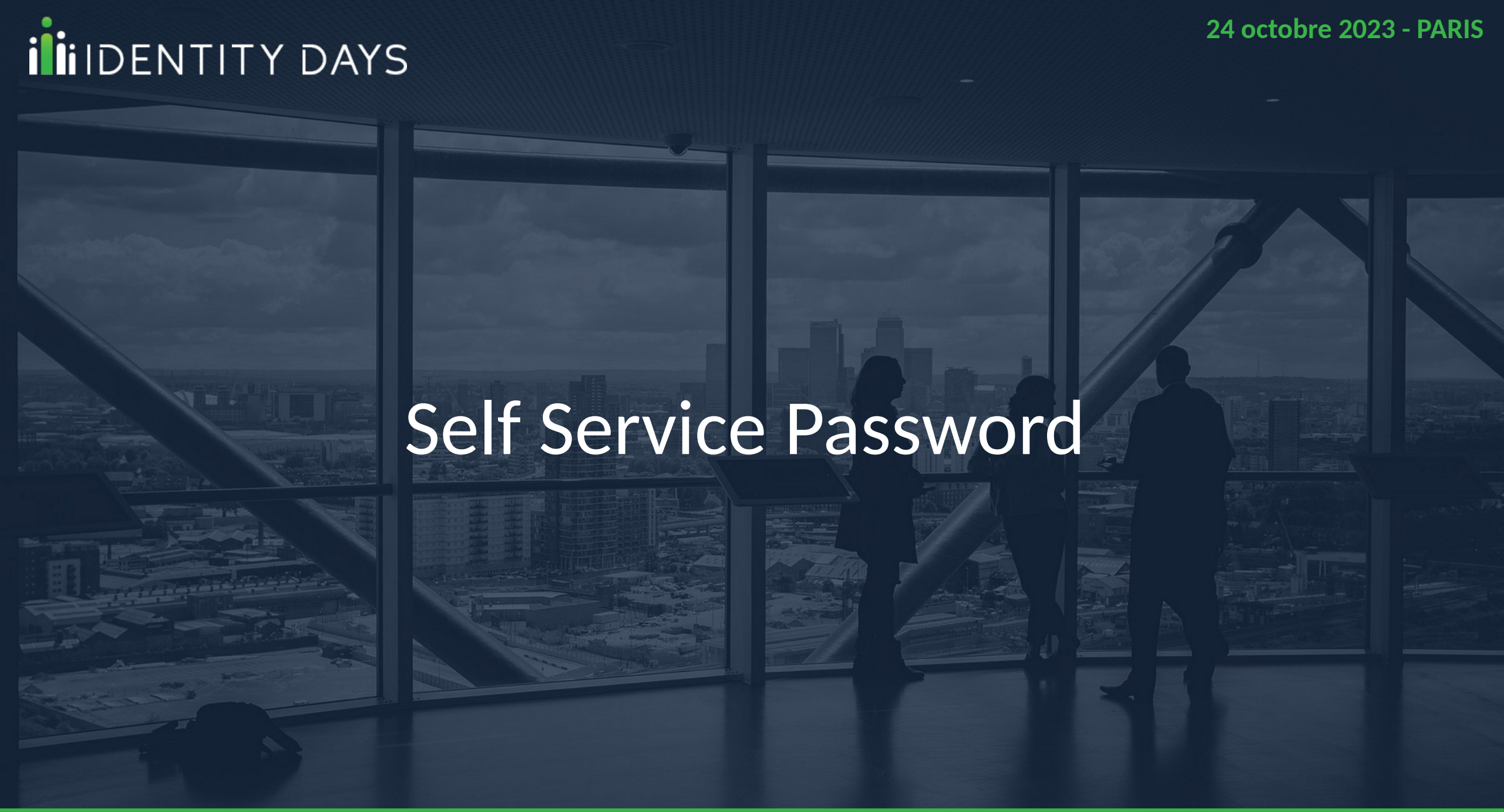
cacti

# Documentation

- Nombreuses ressources sur l'utilisation des outils fournis par le projet LDAP Tool Box
- Articles génériques sur l'usage d'OpenLDAP :
  - Migration de OpenLDAP 2.4 vers OpenLDAP 2.5
  - Authentification mutuelle SSL/TLS
  - Transfert d'authentification vers Active Directory à travers SASL

# Exemple : transfert d'authentification sur différents AD

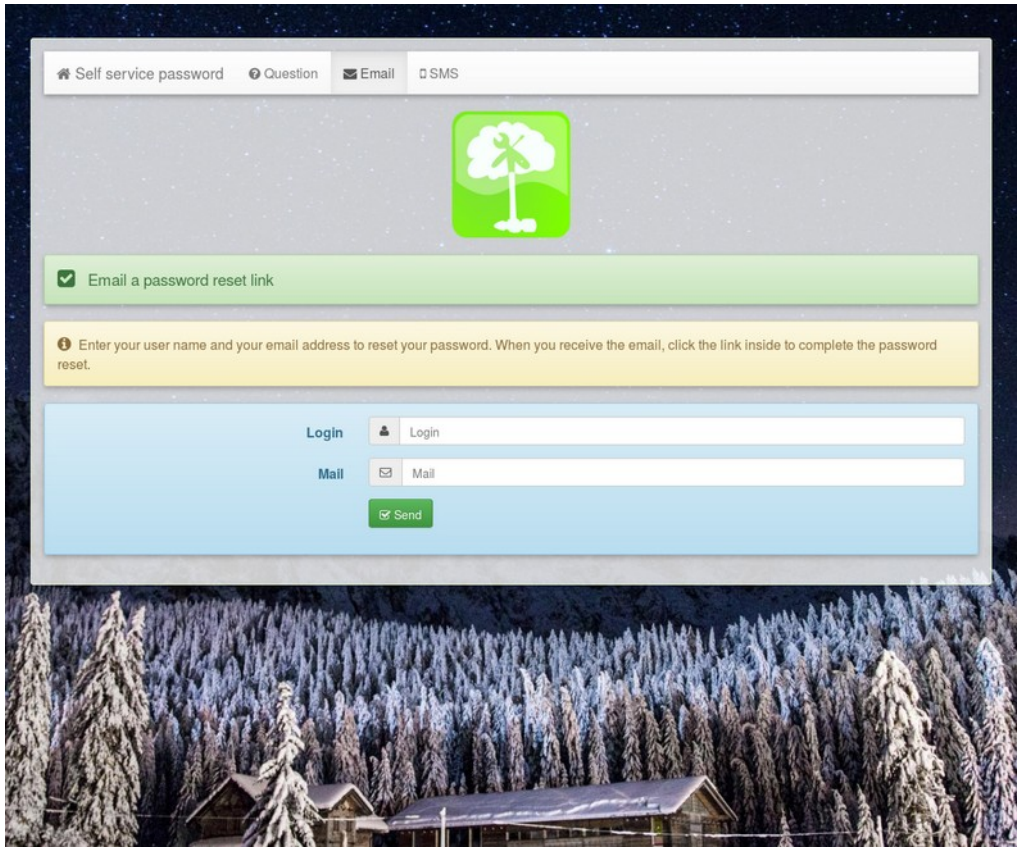




# Self Service Password

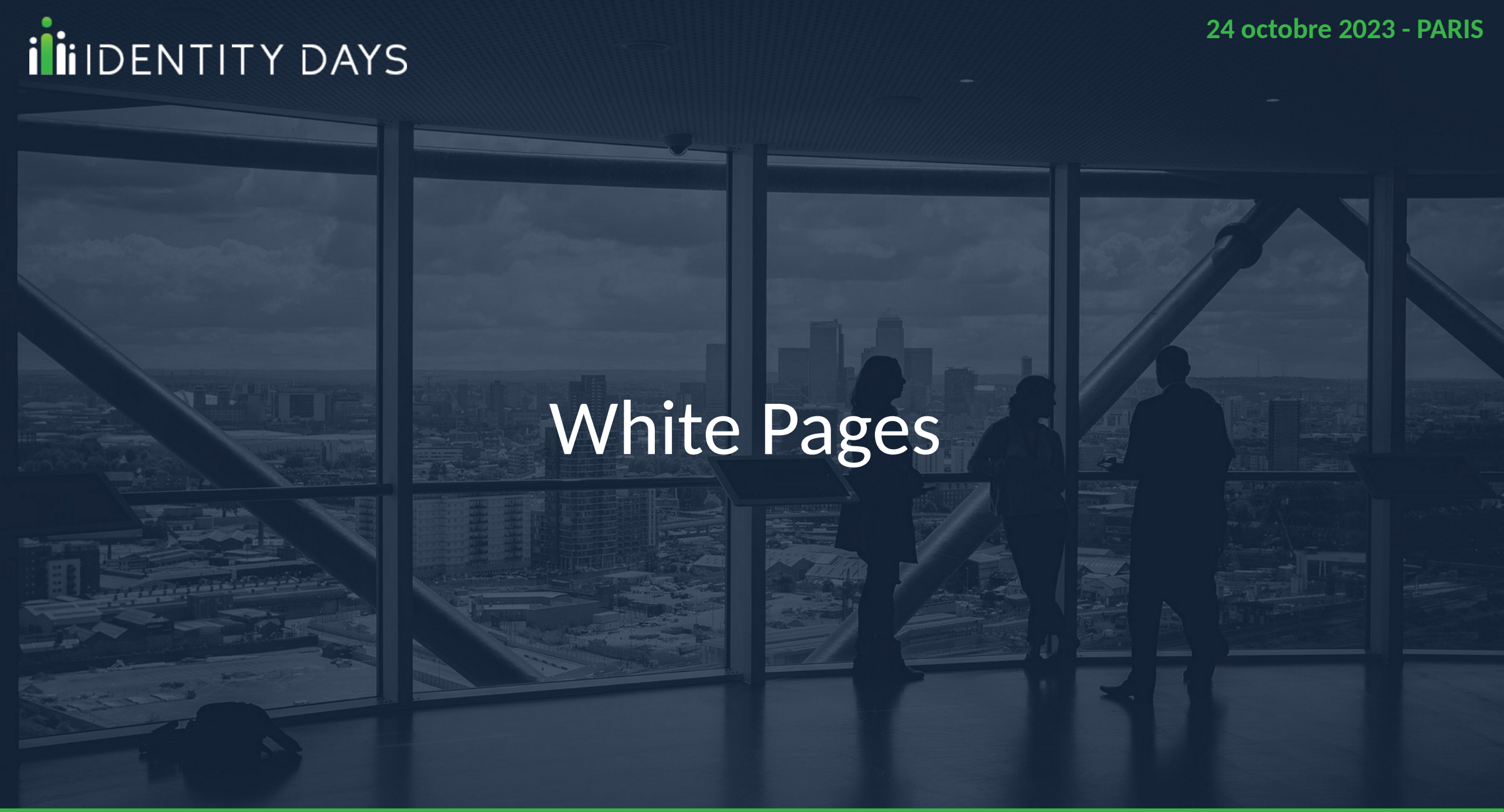
# Self Service Password

- Changement de mot de passe
- Réinitialisation de mot de passe par mail
- Réinitialisation de mot de passe par SMS
- Réinitialisation de mot de passe par questions/réponses
- Changement de clé SSH
- Pré/Post traitements
- Notifications par mail
- Compatible LDAP et Active Directory



# Self Service Password – Usage avancé

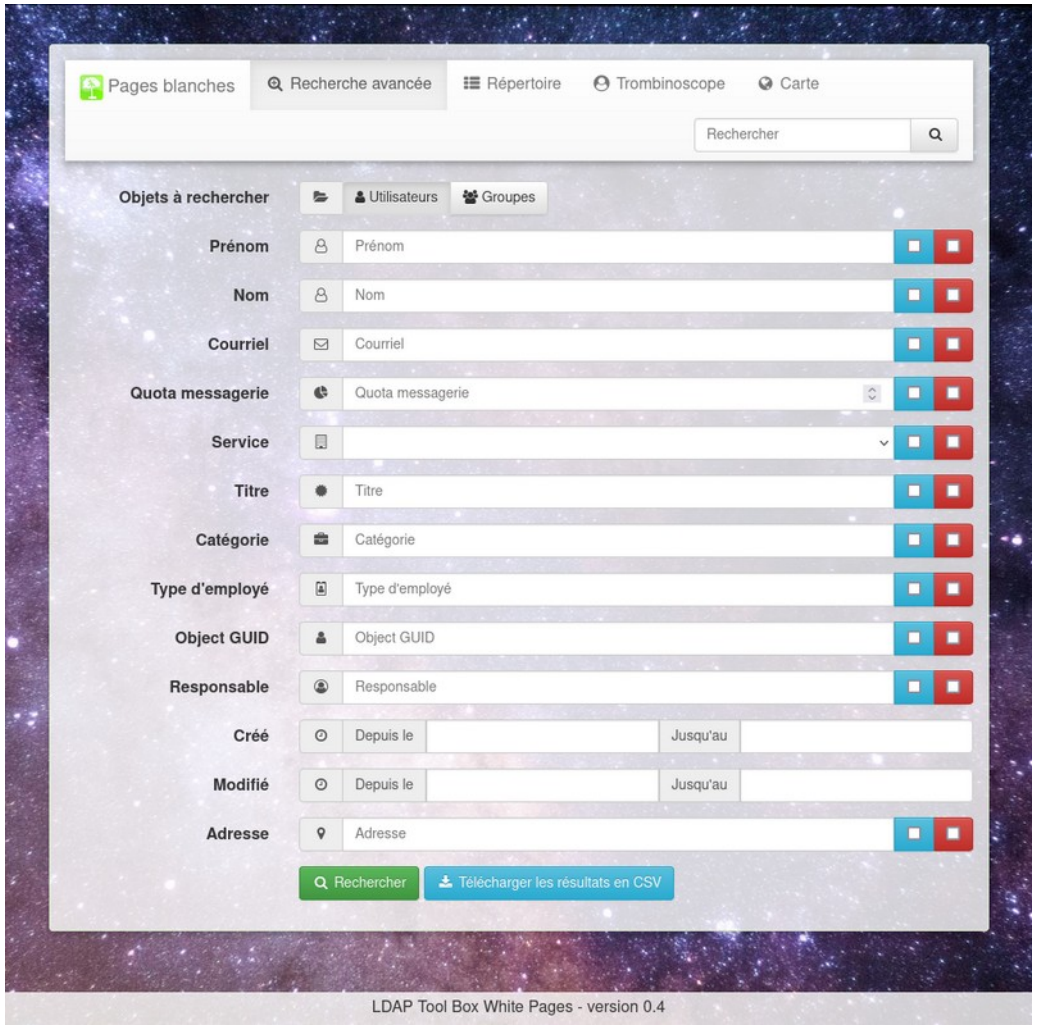
- API REST pour changement et réinitialisation du mot de passe
- Protection des attaques par force brute (rate limit)
- Multi tenants
- **Nouveau** – Fichier d'audit
- **Nouveau** – Modification de son mail et téléphone
- **Nouveau** – Modification de mots de passe secondaires (applicatifs)



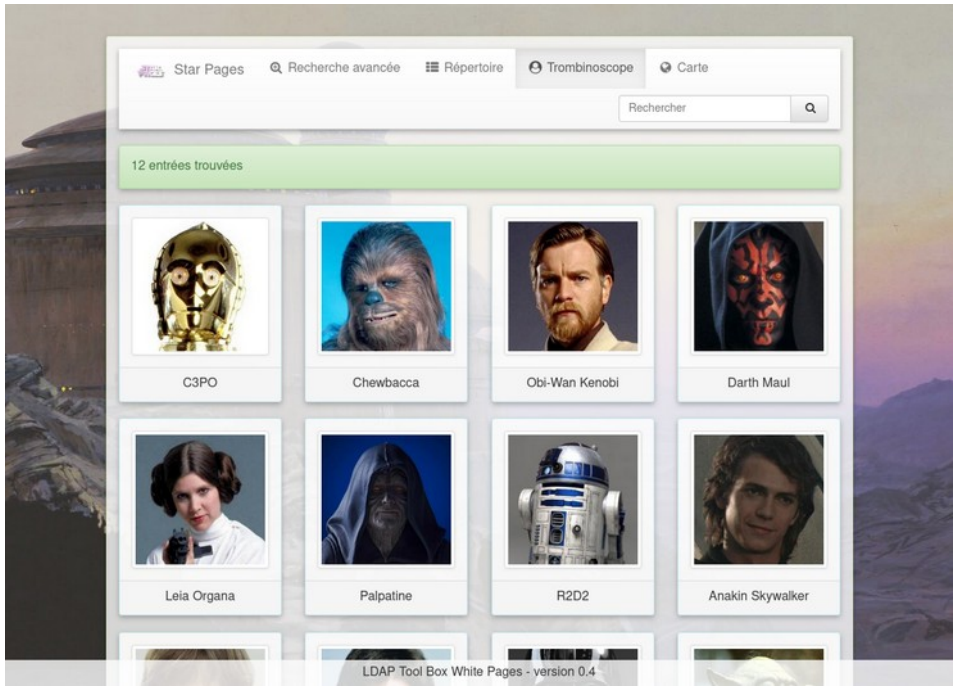
# White Pages

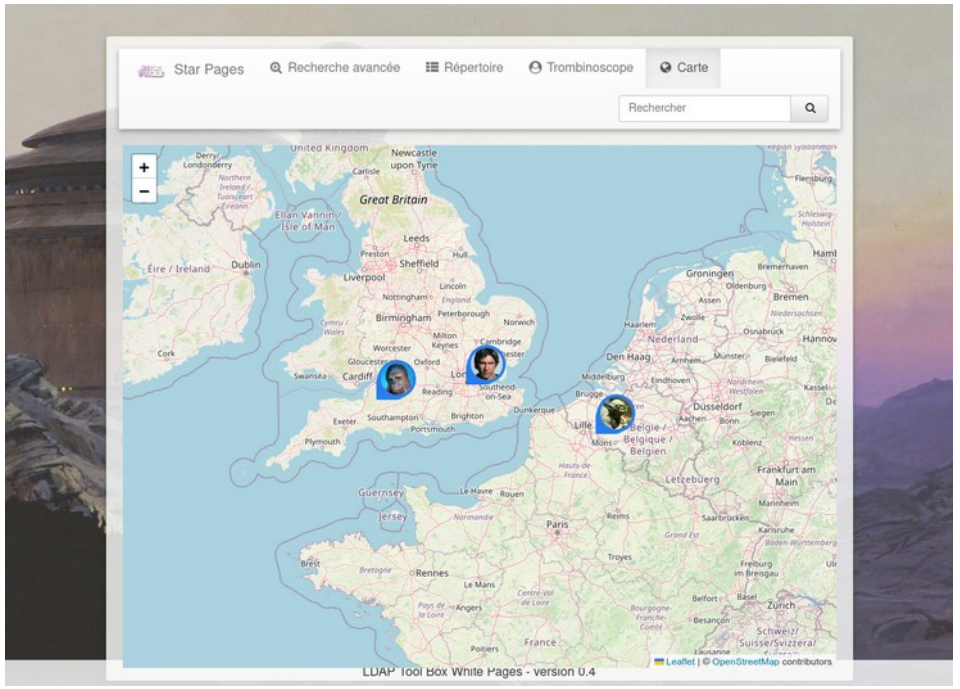
# White Pages

- Recherche simple
- Recherche avancée multi-critères
- Répertoire
- Trombinoscope
- **Nouveau** – Carte (OpenStreetMap)
- Export CSV
- Export vCard
- Compatible LDAP et Active Directory

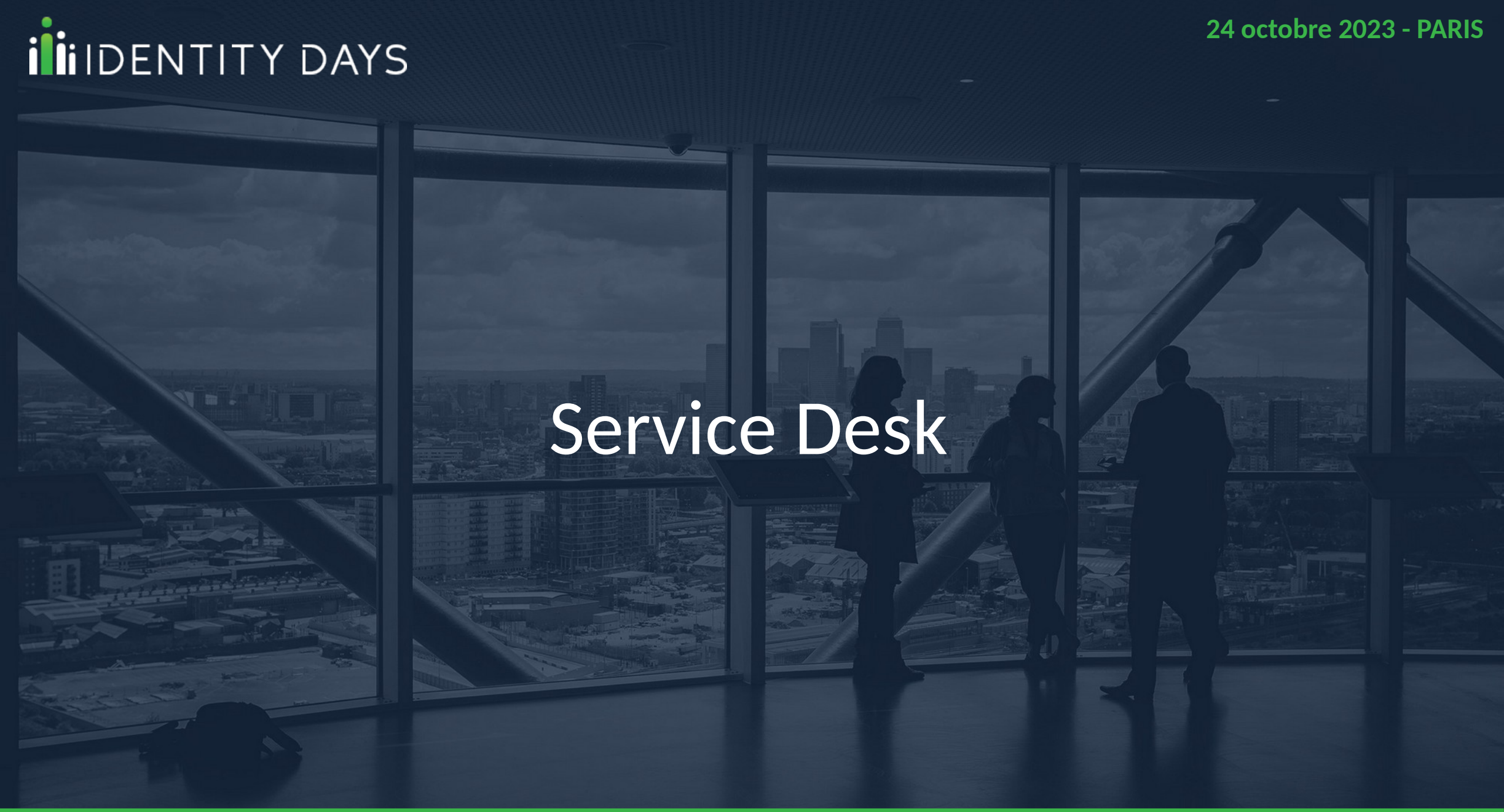


# Star Pages



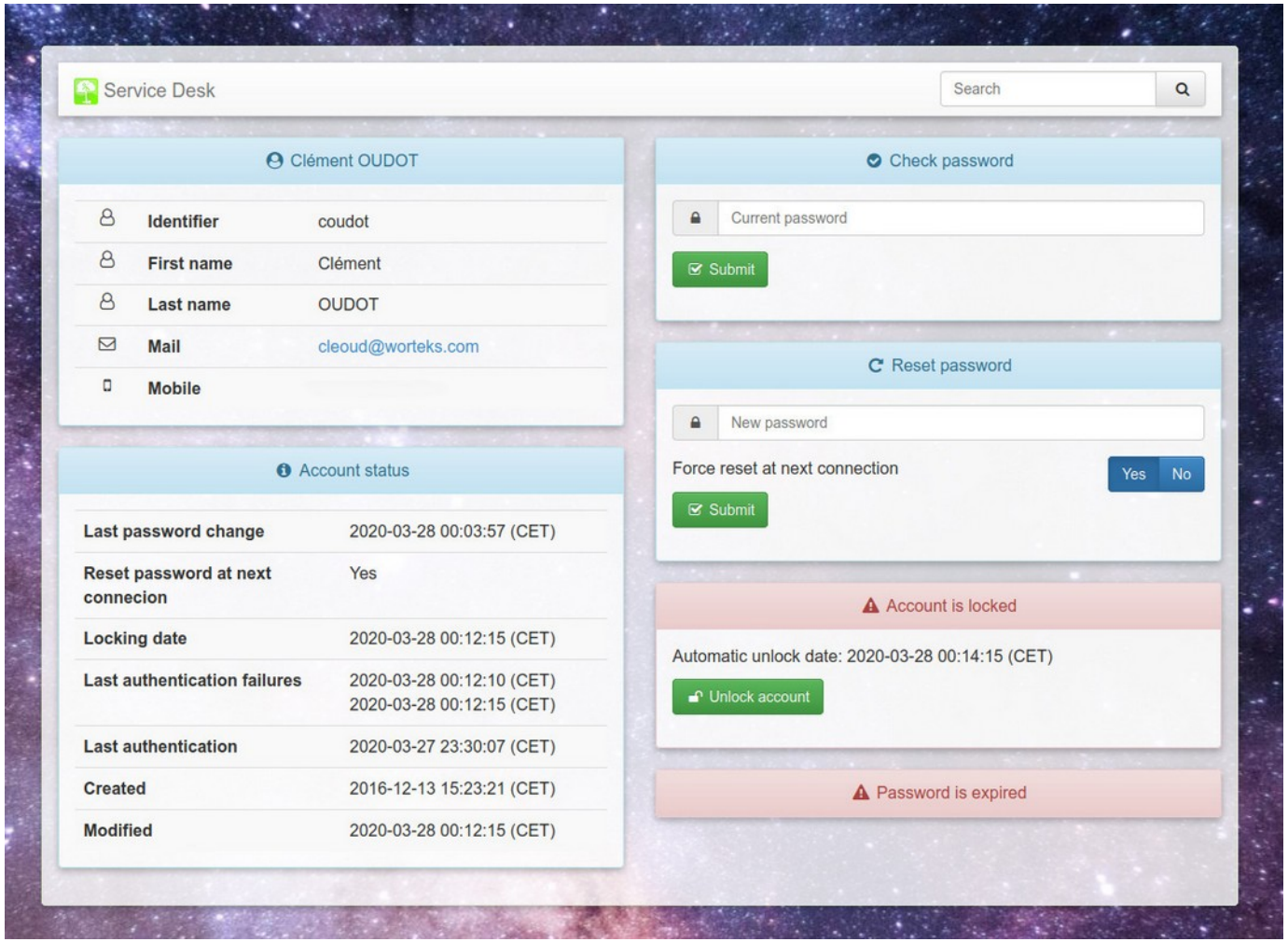

https://ltb-project.org/star-pages



# Service Desk

# Service Desk

- Vue des données principales
- Vue du statut du compte
- Blocage/déblocage
- Vérification du mot de passe
- Réinitialisation du mot de passe
- Pré/Post traitements
- **Nouveau** – Audit
- **Nouveau** – Notifications par mail
- **Compatible OpenLDAP uniquement**

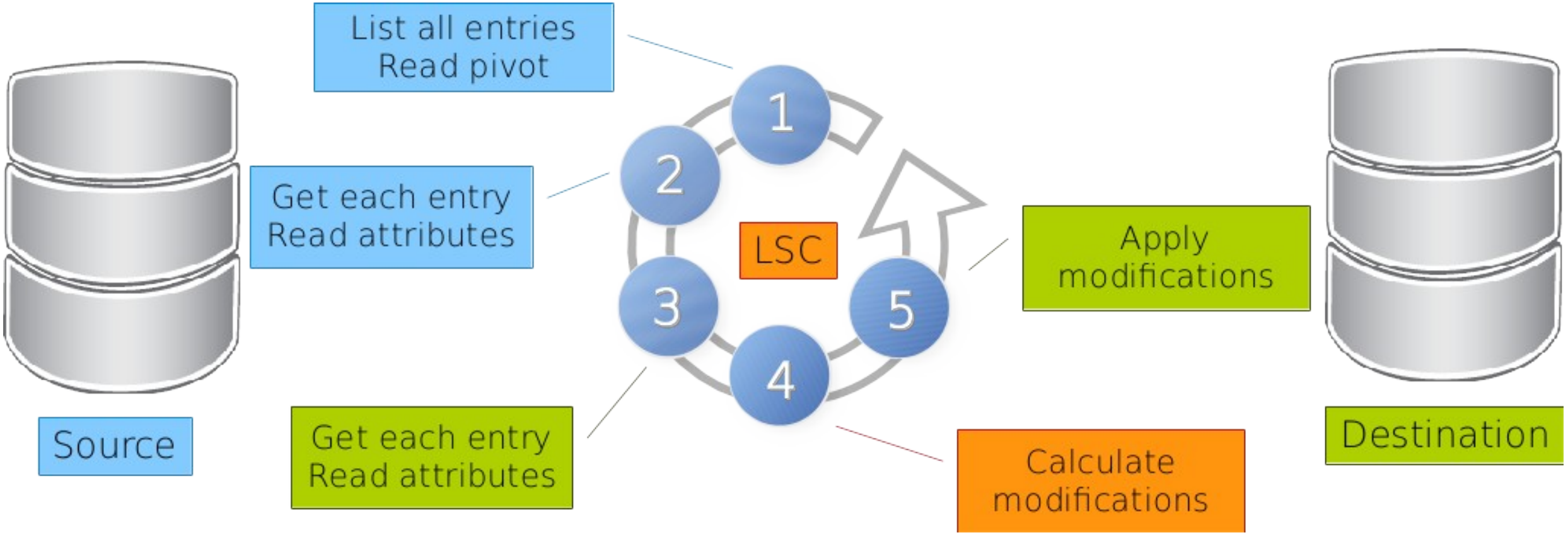


# Le projet LDAP Synchronization Connector


- Projet libre créé en 2008
- Utilitaire en java (ligne de commande)
- Moteur de synchronisation entre annuaires LDAP, Active Directory, bases de données et services Web
- Licence BSD
- Publié sur GitHub
- Projet OW2

https://lsc-project.org

# Principe général



# Exemples d'usage

- Alimentation de l'annuaire d'entreprise depuis la base de données RH
- Synchronisation des comptes et des groupes entre OpenLDAP et Active Directory
- Conversion des groupes dynamiques en groupes statiques
- Provisionning des comptes dans les applications SaaS (via REST API)

# Spécificités Active Directory

- Encodage du mot de passe (getUnicodePwd)
- Conversion des timestamps (aDTimeToUnixTimestamp, unixTimestampToADTime)
- Gestion des flags dans l'attribut userAccountControl (userAccountControlCheck, userAccountControlSet, userAccountControlToggle)
- Calculs sur les dates (getAccountExpires, getNumberOfWeeksSinceLastLogon)
- Support de la pagination sur les entrées (pageSize) et sur les attributs (range)

# Moteur de plugins

- Plugins officiels :
  - **Executable** : lancement de scripts pour chaque opération (ajout, modification …)
  - **Fusion Directory** : utilisation de l'API REST de Fusion Directory
  - **James** : utilisation de l'API REST de James (serveur mail)
  - **Microsoft Graph API**

- Plugins non officiels :
  - **Multi JDBC** : agrège plusieurs sources de données
  - **SCIM2** : Standard SCIM (Simple Cloud Identity Management)


IDENTITY DAYS
@IdentityDays
#identitydays2023