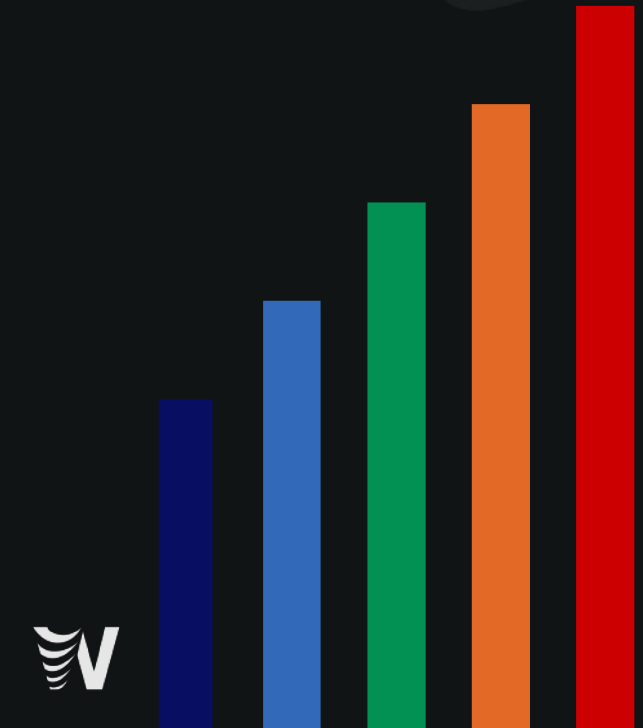
Worteks

make IT work, make IT free

IAM Open Source pour Active Directory

20 octobre 2025
Paris

Sommaire



Protocole LDAP et Active Directory

Les outils compatibles :

- LemonLDAP::NG
- LDAP Synchronization Connector
- LTB Self Service Password
- LTB White Pages
- LTB Service Desk

Qui a les droits Patrick BrueLDAP

On m'avait dit : "Te pose pas trop d'questions"
Active Directory comme annuaire il est bon
Il gère les groupes, les comptes et les mots de passe
On l'interroge pour savoir ce qu'il se passe

Qui a les droits, qui a les droits,
Qui a les droits d' faire ça
Dans le système d'information
On veut son mail et puis son nom

On m'avait dit les annuaires sont tous pareils
Le protocole LDAP tout le monde le respecte
Mais pour AD, il faut s'adapter
Changer son code pour pouvoir renseigner

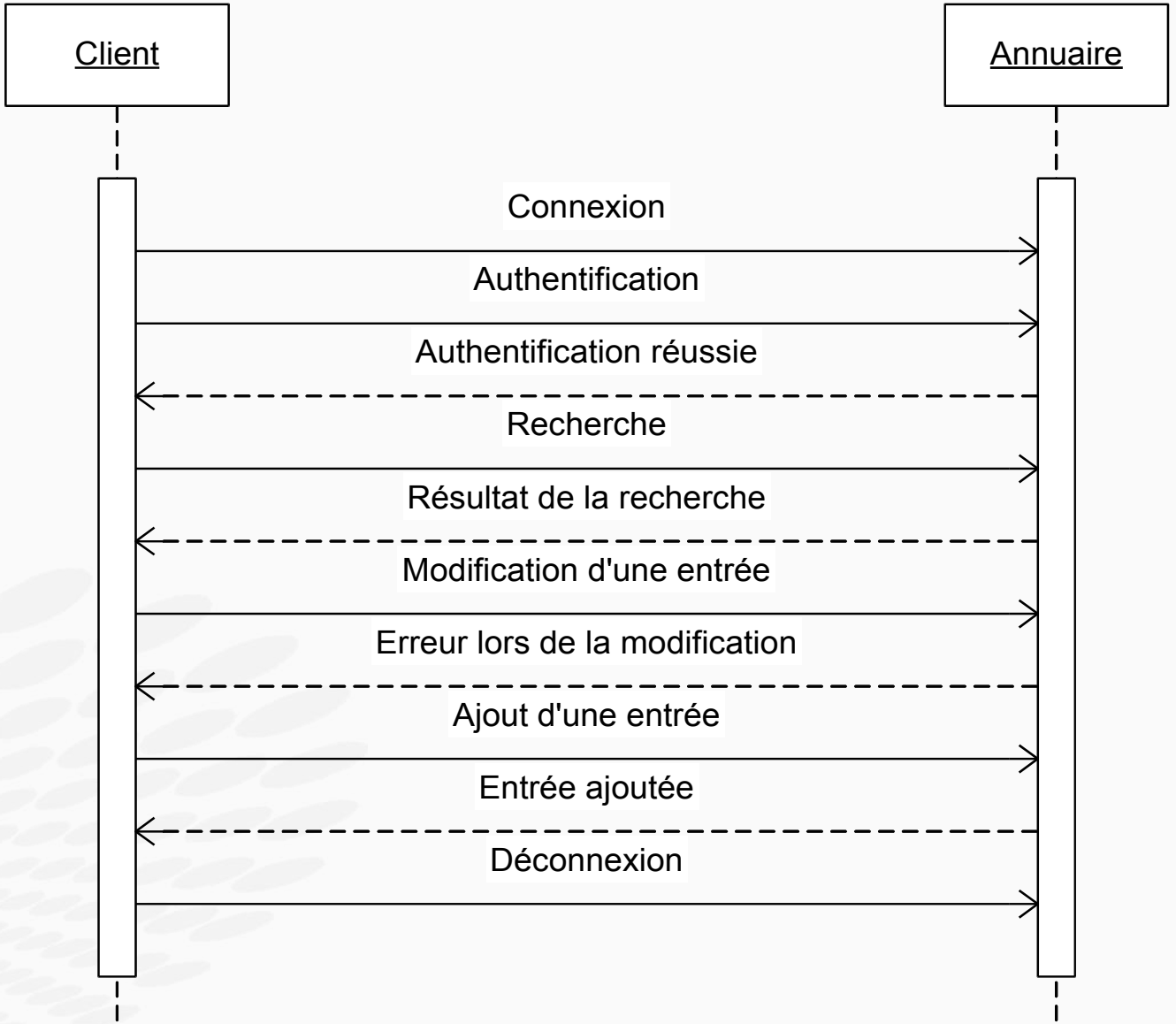
Qui a les droits, qui a les droits,
Qui a les droits d' faire ça
Dans le système d'information
On veut son mail et puis son nom

On passe sa vie à la merci,
d'Active Directory
Mais avec l'aide des logiciels libres
À l'administrer on y arrive

LDAP et AD

Le protocole LDAP

- Lightweight Directory Access Protocol
- Issu de X.500, apparu à la fin des années 1980
- LDAP v3 publié en 1998
- Définitions du modèle de données et des opérations : authentification, recherches, comparaisons, écritures...

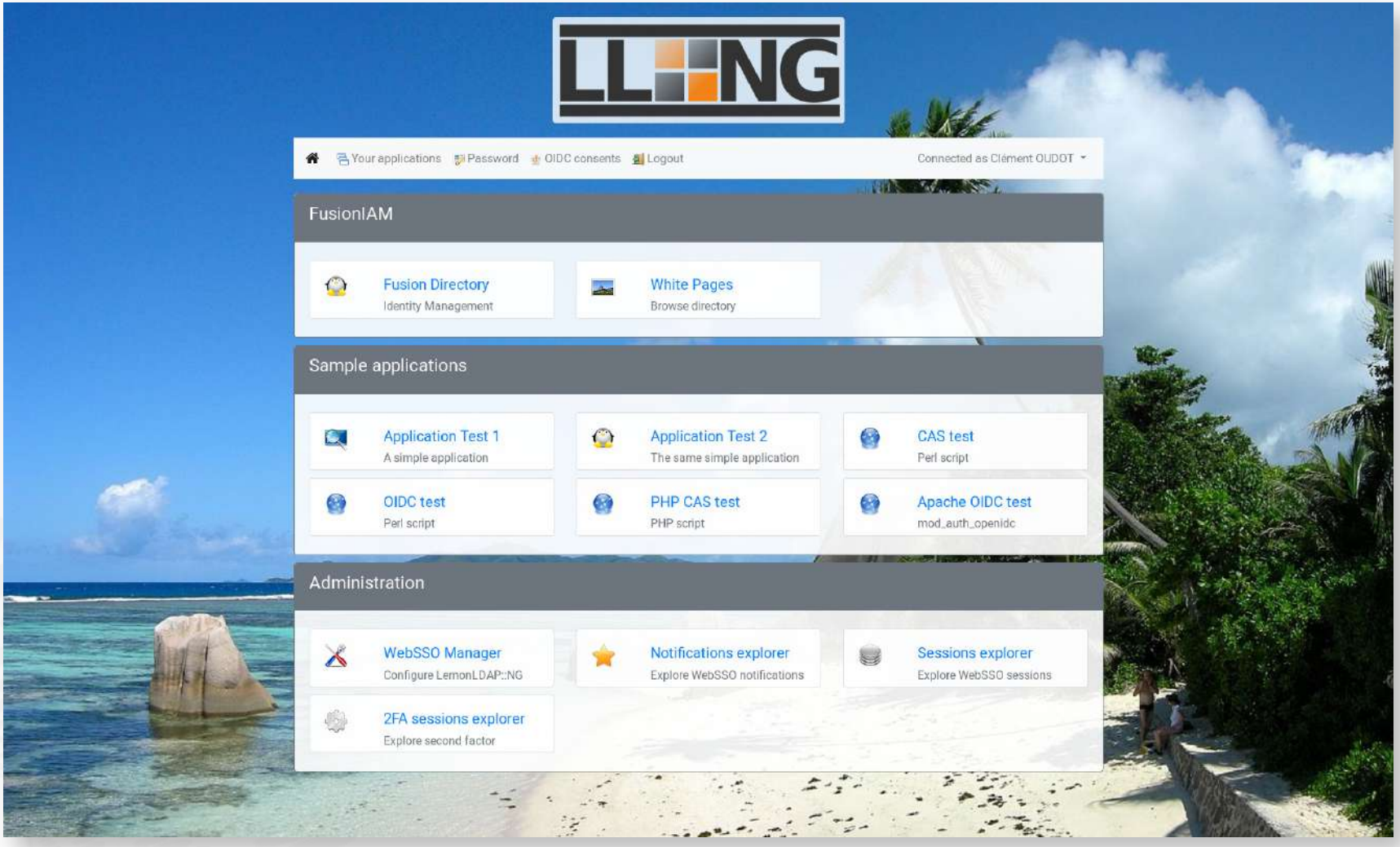

Client
Annuaire
Connexion
Authentification
Authentification réussie
Recherche
Résultat de la recherche
Modification d'une entrée
Erreur lors de la modification
Ajout d'une entrée
Entrée ajoutée
Déconnexion

Les particularités AD

- Active Directory est, entre autres, un serveur LDAP
- Mais il prend quelques libertés avec le standard :
  - Stockage du mot de passe dans unicodePwd (en écriture seule)
  - Pagination par défaut à 1000 entrées
  - Pagination des valeurs d'attribut (range)
  - Classes d'objet "user" et "group"
  - Attributs spéciaux userAccountControl, objectGuid, ObjectSid
  - Date = nb d'intervalles de 100ns depuis le 1er janvier 1601

Il faut adapter son code à AD

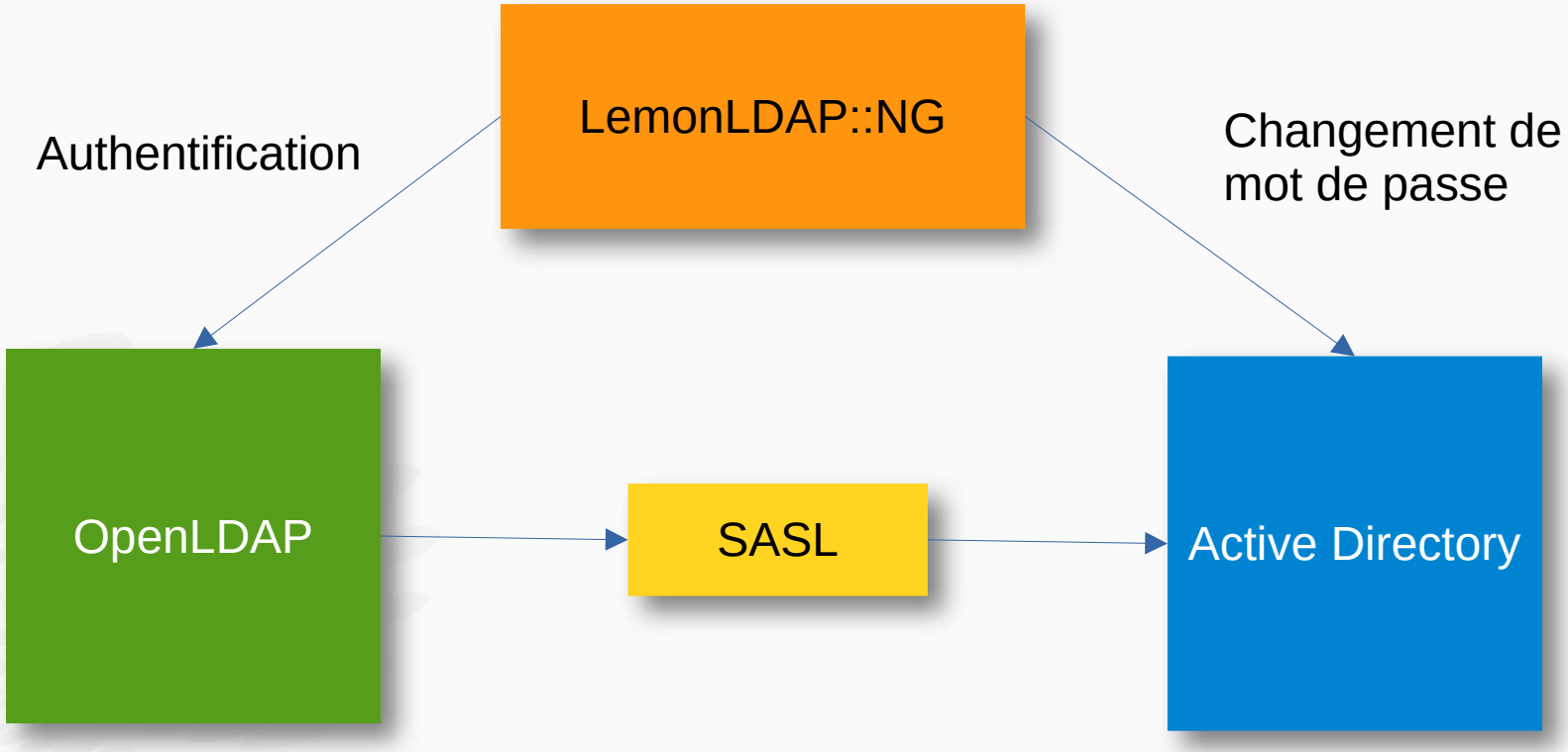
LemonLDAP::NG


LL NG
Your applications
Password
OIDC consents
Logout
Connected as Clément OUDOT
FusionIAM
Fusion Directory
Identity Management
White Pages
Browse directory
Sample applications
Application Test 1
A simple application
Application Test 2
The same simple application
CAS test
Perl script
OIDC test
Perl script
PHP CAS test
PHP script
Apache OIDC test
mod_auth_openidc
Administration
WebSSO Manager
Configure LemonLDAP::NG
Notifications explorer
Explore WebSSO notifications
Sessions explorer
Explore WebSSO sessions
2FA sessions explorer
Explore second factor

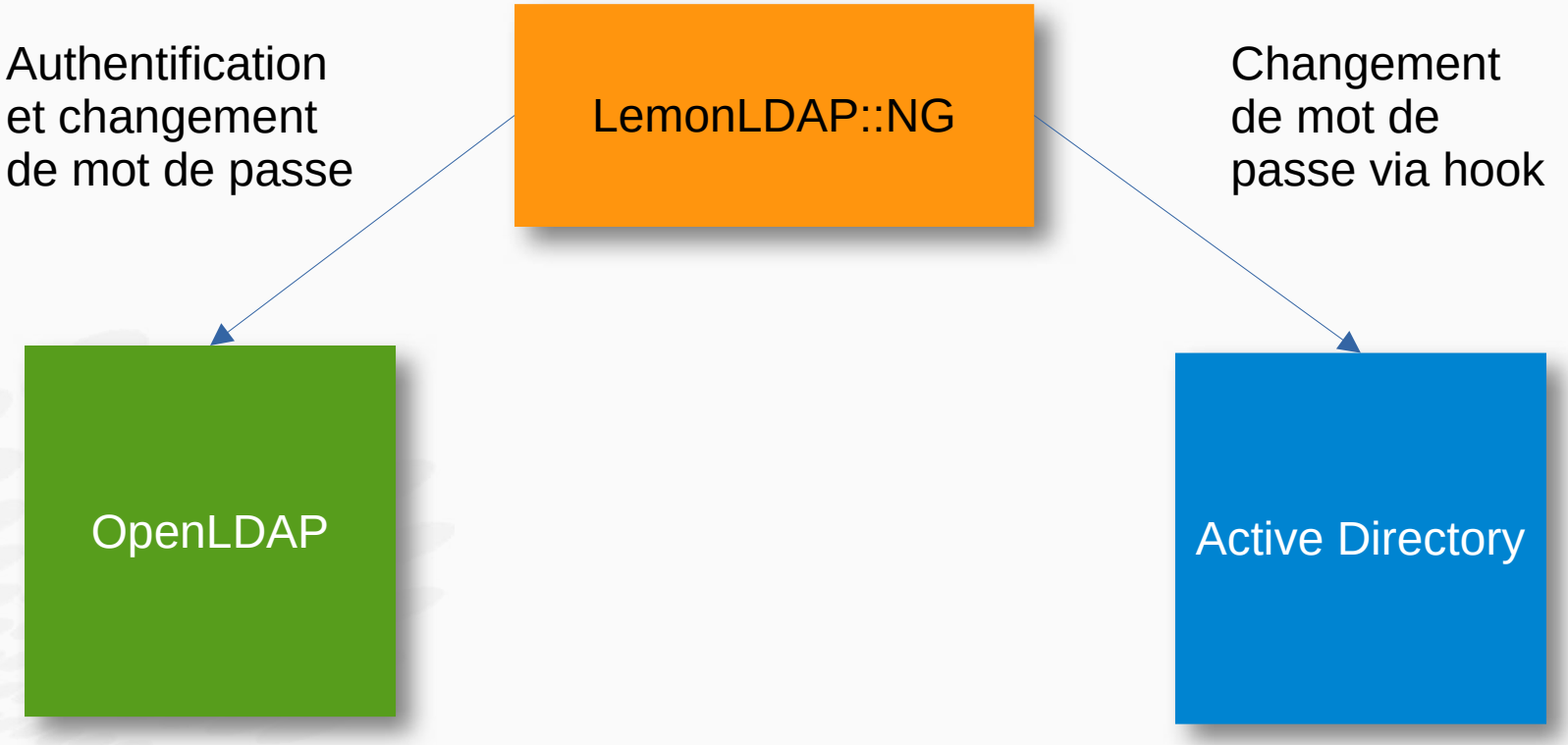
Authentification

- Modules dédiés à AD pour l'authentification (Auth), la récupération d'attributs (UserDB) et le changement de mot de passe (PasswordDB)
- Module d'authentification **Kerberos** pour l'authentification transparente
- Gestion des **groupes récursifs**
- Réinitialisation du mot de passe à la prochaine connexion
- Alerte d'expiration du mot de passe

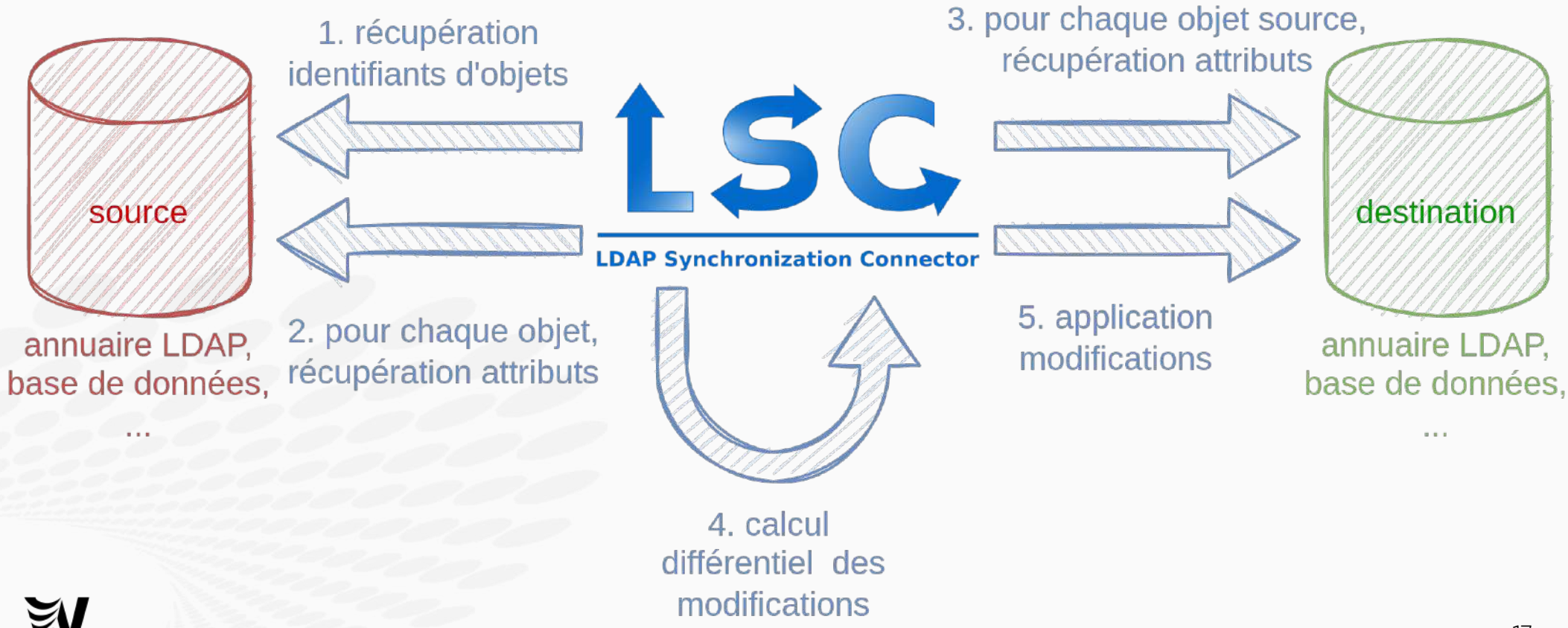
AD connecté via SASL



AD autonome


Authentification
et changement
de mot de passe
LemonLDAP::NG
Changement
de mot de
passe via hook
OpenLDAP
Active Directory

LDAP Synchronization Connector


1. récupération identifiants d'objets
3. pour chaque objet source, récupération attributs
source
LSC
LDAP Synchronization Connector
destination
annuaire LDAP, base de données, ...
2. pour chaque objet, récupération attributs
5. application modifications
annuaire LDAP, base de données, ...
4. calcul différentiel des modifications

Fonctions adaptées à AD

- Paramètre pageSize dans la connexion LDAP
- Possibilité de déclarer les attributs binaires (objectGuid, objectSid)
- Gestion du “range” par javascript dans le dataset des attributs
- Fonction pour l’encodage du mot de passe : getUnicodePwd
- Fonctions de manipulation de l’attribut userAccountControl : userAccountControlSet, userAccountControlCheck, userAccountControlToggle
- Fonctions de conversion de dates : unixTimestampToADTime, aDTimeToUnixTimestamp

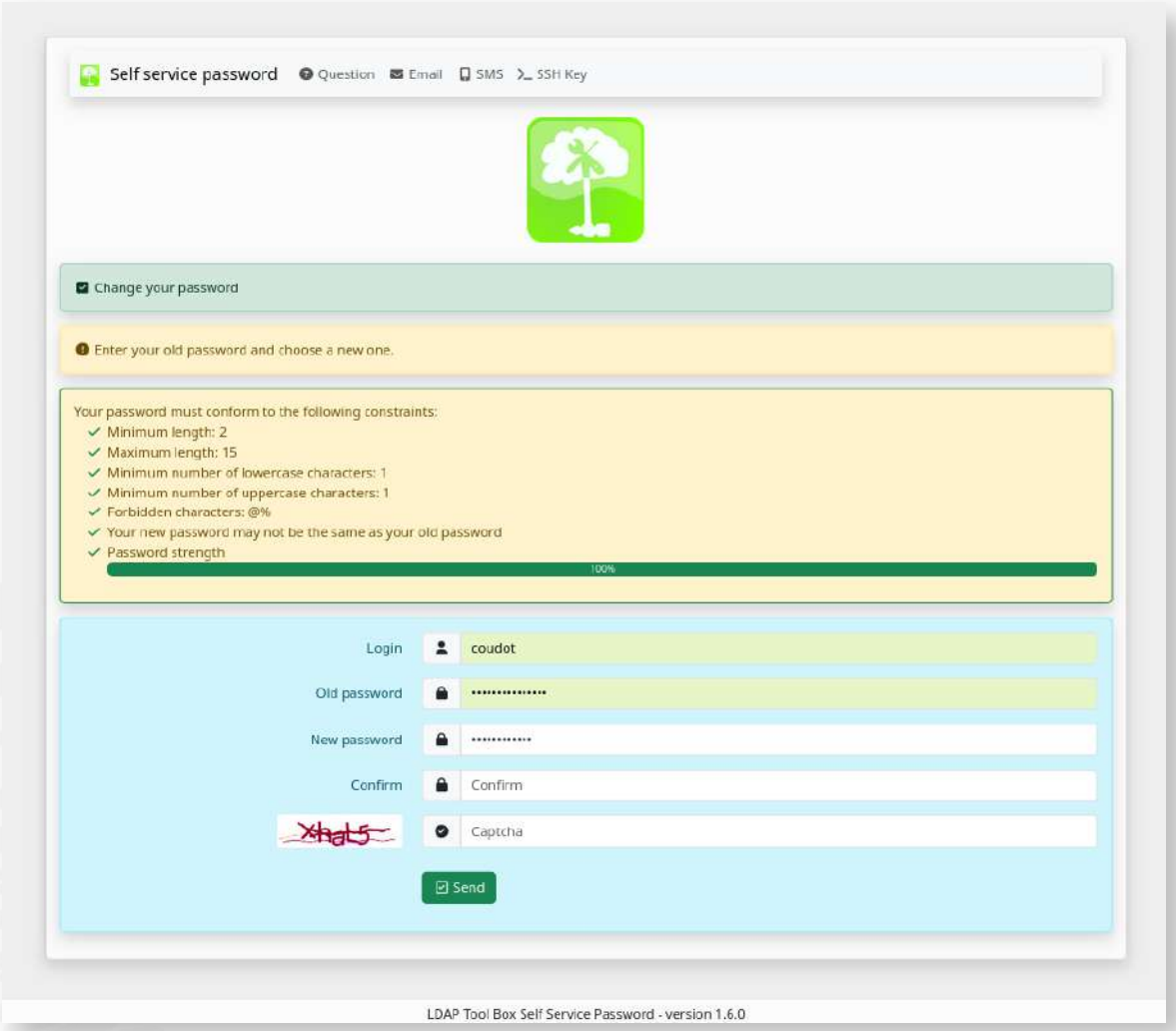
objectGuid → UUID ?

```
function readUUID(bytes) {
   var hex = new
java.lang.String(org.apache.commons.codec.binary.Hex.encodeHe
x(bytes));
   return hex.replace(/^(..)(..)(..)(..)(..)(..)(..)(..)(..)
(..)(..)(..)(..)(..)(..)(..)$/,"$4$3$2$1-$6$5-$8$7-$9$10-
$11$12$13$14$15$16").toUpperCase();
}
```

Quelques exemples d'usages

- Convertir les groupes dynamiques OpenLDAP dans des groupes statiques AD
- Synchroniser le statut de blocage des comptes entre OpenLDAP et AD
- Provisionner les comptes utilisateurs avec un mot de passe à changer à la prochaine connexion

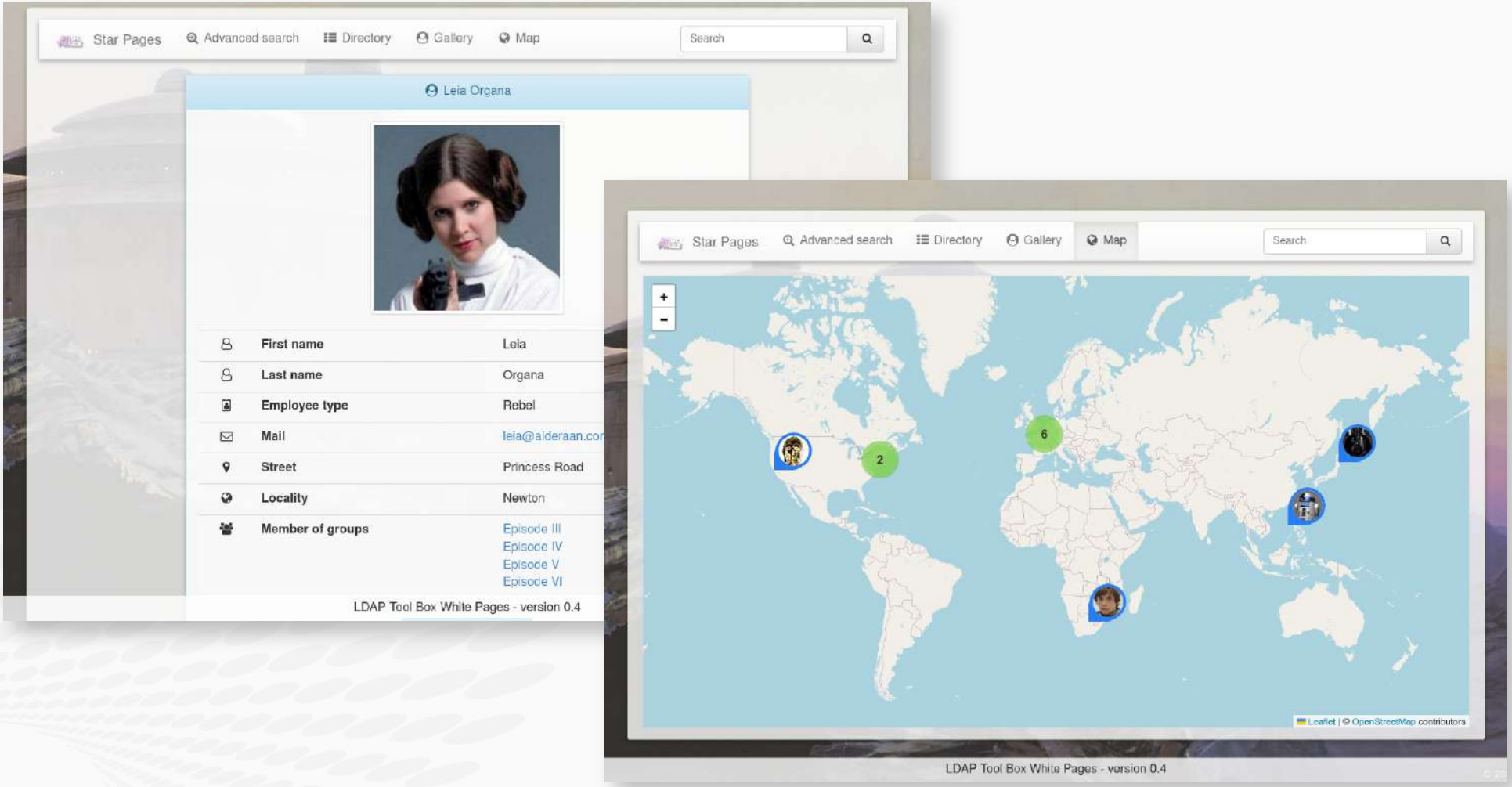
LTB
Self Service
Password


Self service password
Question
Email
SMS
SSH Key
Change your password
Enter your old password and choose a new one.
Your password must conform to the following constraints:
Minimum length: 2
Maximum length: 15
Minimum number of lowercase characters: 1
Minimum number of uppercase characters: 1
Forbidden characters: @%
Your new password may not be the same as your old password
Password strength
100%
Login
coudot
Old password
New password
Confirm
Captcha
Send
LDAP Tool Box Self Service Password - version 1.6.0

Le mode Active Directory

- Le paramètre “ad_mode” permet d’utiliser le format d’encodage pour unicodePwd, et donc l’écriture du mot de passe dans Active Directory
- Plusieurs options supplémentaires sont disponibles :
  - force_unlock : déverrouille le compte lors du changement de mot de passe
  - force_pwd_change : force le changement à la prochaine connexion
  - change_expired_password : autorise le changement d’un mot de passe expiré

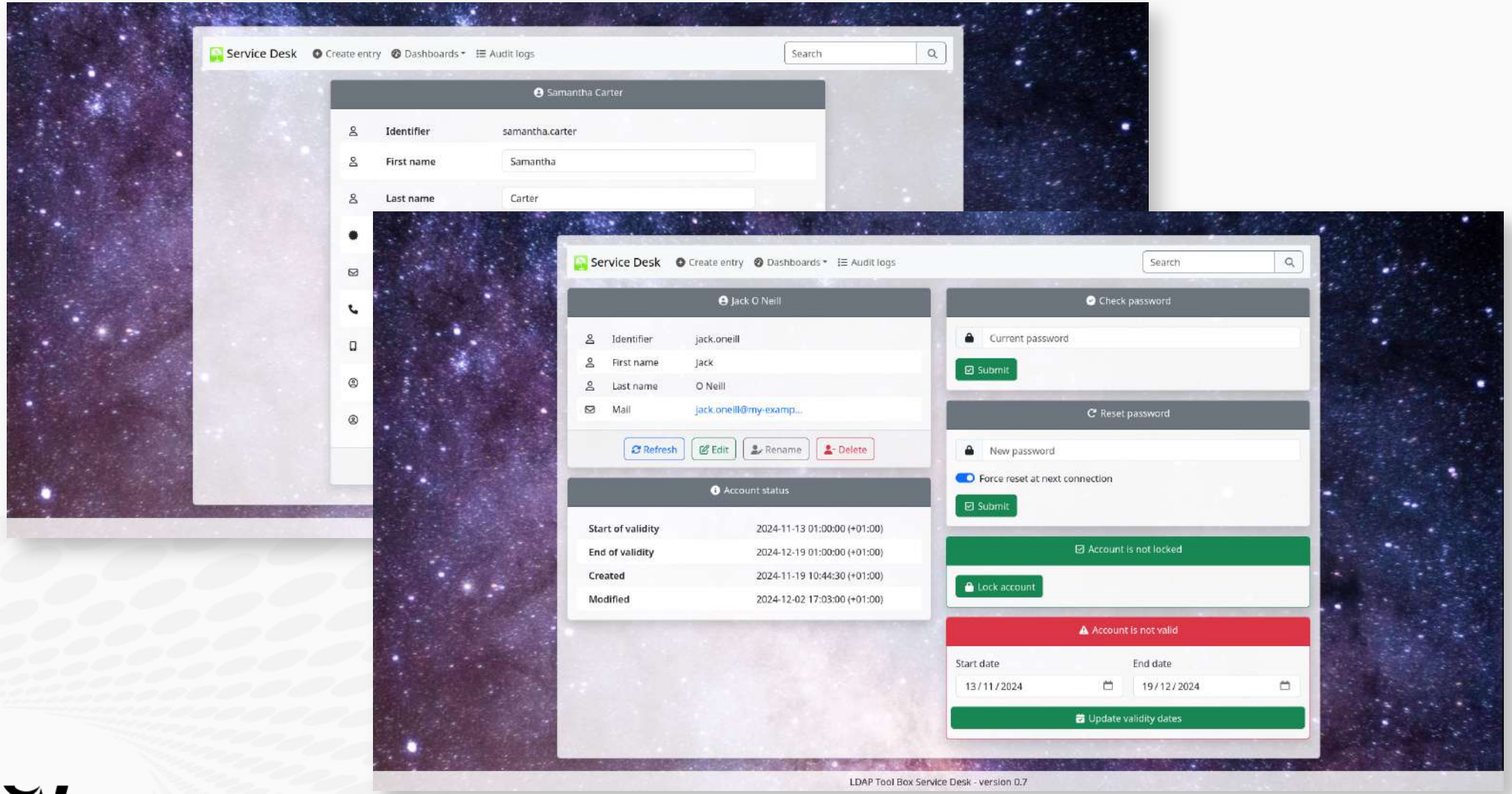
LTB
White Pages


Star Pages
Advanced search
Directory
Gallery
Map
Search
Leia Organa
First name
Leia
Last name
Organa
Employee type
Rebel
Mail
leia@alderaan.com
Street
Princess Road
Locality
Newton
Member of groups
Episode III
Episode IV
Episode V
Episode VI
LDAP Tool Box White Pages - version 0.4
Star Pages
Advanced search
Directory
Gallery
Map
Search
2
6
Leaflet | © OpenStreetMap contributors
LDAP Tool Box White Pages - version 0.4

Configuration pour AD

- Les paramètres de connexion LDAP peuvent être adaptés pour Active Directory :
  - Pagination des résultats
  - Filtre de recherche des utilisateurs
  - Filtre de recherche des groupes
  - Liste des attributs à afficher
  - Attribut contenant la photo

LTB
Service Desk

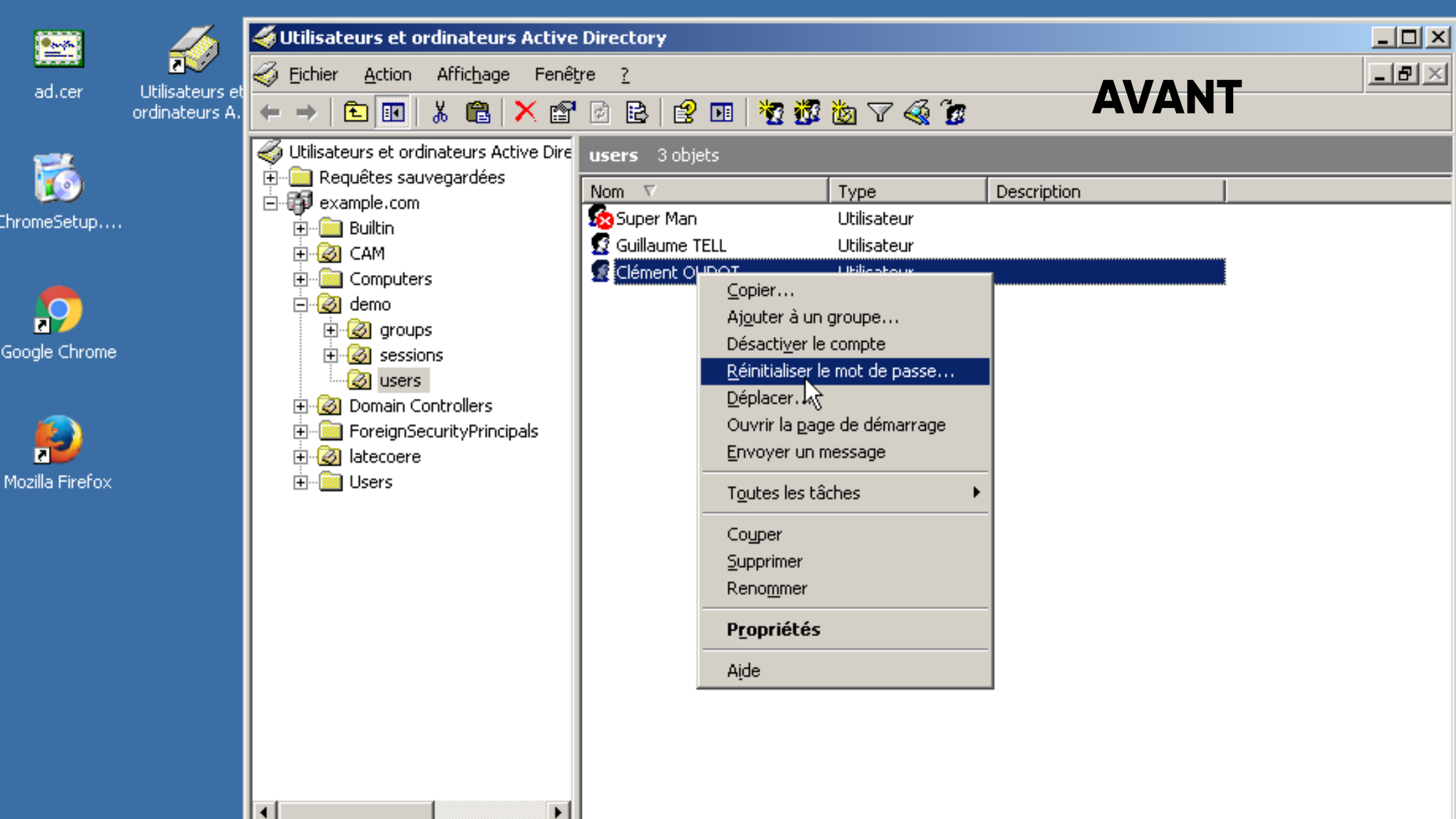

Service Desk
Create entry
Dashboards
Audit logs
Search
Samantha Carter
Identifier
samantha.carter
First name
Samantha
Last name
Carter
Service Desk
Create entry
Dashboards
Audit logs
Search
Jack O Neill
Identifier
jack.oneill
First name
Jack
Last name
O Neill
Mail
jack.oneill@my-examp...
Refresh
Edit
Rename
Delete
Account status
Start of validity
2024-11-13 01:00:00 (+01:00)
End of validity
2024-12-19 01:00:00 (+01:00)
Created
2024-11-19 10:44:30 (+01:00)
Modified
2024-12-02 17:03:00 (+01:00)
Check password
Current password
Submit
Reset password
New password
Force reset at next connection
Submit
Account is not locked
Lock account
Account is not valid
Start date
13 / 11 / 2024
End date
19 / 12 / 2024
Update validity dates
LDAP Tool Box Service Desk - version 0.7

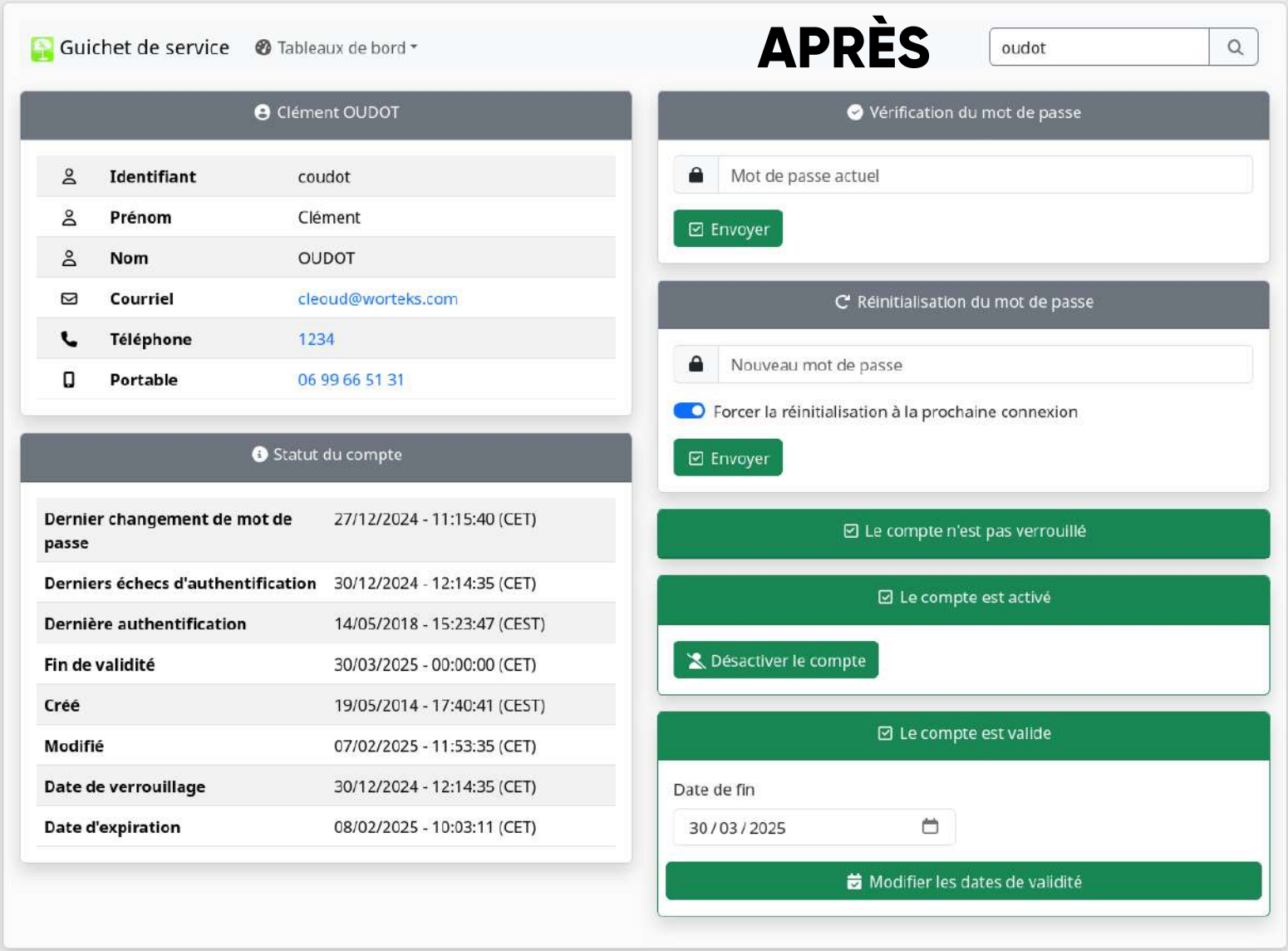
Un support AD avancé

- Module PHP dans la bibliothèque ltb-common : Ltb/Directory/ActiveDirectory.php

=> Aucun code spécifique OpenLDAP ou AD dans Service Desk !

- Variable de configuration “ldap_type” pour indiquer si on utilise OpenLDAP ou Active Directory
- Type “ad_date” pour gérer les dates AD
- Gestion du statut activé/désactivé (indépendant du statut bloqué/débloqué)


ad.cer
Utilisateurs et ordinateurs A.
ChromeSetup....
Google Chrome
Mozilla Firefox
Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage Fenêtre ?
AVANT
Utilisateurs et ordinateurs Active Dire
Requêtes sauvegardées
example.com
Builtin
CAM
Computers
demo
groups
sessions
users
Domain Controllers
ForeignSecurityPrincipals
latecoere
Users
users 3 objets
Nom
Type
Description
Super Man
Utilisateur
Guillaume TELL
Utilisateur
Clément OUDOT
Copier...
Ajouter à un groupe...
Désactiver le compte
Réinitialiser le mot de passe...
Déplacer...
Ouvrir la page de démarrage
Envoyer un message
Toutes les tâches
Couper
Supprimer
Renommer
Propriétés
Aide


Guichet de service
Tableaux de bord
APRÈS
oudot
Clément OUDOT
Identifiant coudot
Prénom Clément
Nom OUDOT
Courriel cleoud@worteks.com
Téléphone 1234
Portable 06 99 66 51 31
Statut du compte
Dernier changement de mot de passe 27/12/2024 - 11:15:40 (CET)
Derniers échecs d'authentification 30/12/2024 - 12:14:35 (CET)
Dernière authentification 14/05/2018 - 15:23:47 (CEST)
Fin de validité 30/03/2025 - 00:00:00 (CET)
Créé 19/05/2014 - 17:40:41 (CEST)
Modifié 07/02/2025 - 11:53:35 (CET)
Date de verrouillage 30/12/2024 - 12:14:35 (CET)
Date d'expiration 08/02/2025 - 10:03:11 (CET)
Vérification du mot de passe
Mot de passe actuel
Envoyer
Réinitialisation du mot de passe
Nouveau mot de passe
Forcer la réinitialisation à la prochaine connexion
Envoyer
Le compte n'est pas verrouillé
Le compte est activé
Désactiver le compte
Le compte est valide
Date de fin
30 / 03 / 2025
Modifier les dates de validité

www.worteks.com

info@worteks.com
+33 1 84 20 86 47
worteks_com
worteks