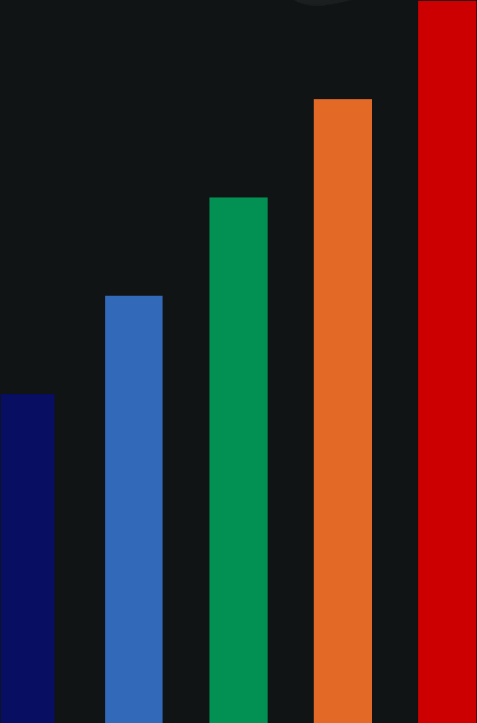




IAM Open Source pour OpenLDAP et AD

Sommaire



Protocole LDAP, OpenLDAP et Active Directory

Les outils compatibles :

LemonLDAP::NG

LDAP Synchronization Connector

LTB Self Service Password

LTB White Pages

LTB Service Desk





Clément OUDOT
Identity Solutions Manager
[Worteks](#)

 [@clementoudot](#)



LemonLDAP::NG
LDAP Tool Box
LDAP Synchronization Connector
FusionIAM



Worteks

Société d'expertise, d'édition et d'hébergement Open Source
Centre de formation certifié Qualiopi

Contribue activement à de nombreux logiciels libres comme LSC,
LemonLDAP::NG, LDAP Tool Box, FusionIAM et OpenStack

Partenaires



Worteks

Une offre Open Source globale.

Solution de déploiement d'infrastructure complexe

 **V'Opla**

Portail de travail collaboratif

 **V'Sweet**

Intégration, support et expertise

 **V'ise**

Hébergement souverain

 **V'aaS**

Solution de gestion des identités et des accès

 **V'IDaaS**



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

OpenLDAP et

Active Directory

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...



OpenLDAP

- Respect des standards
- Utilisable pour des annuaires de quelques entrées jusqu'à plusieurs millions
- Des fonctionnalités à la carte via les overlays :
 - Politique des mots de passe (ppolicy)
 - Groupes dynamiques (dynlist)
 - Unicité (unique), contraintes (constraint), réécriture (rwm), ...



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



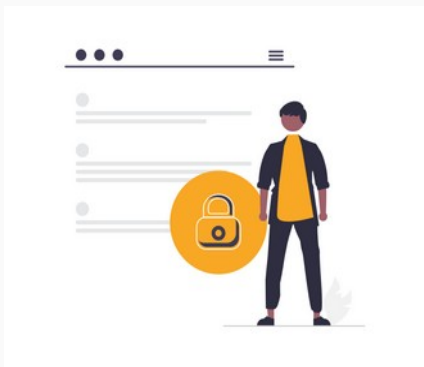


Il faut adapter son code à AD

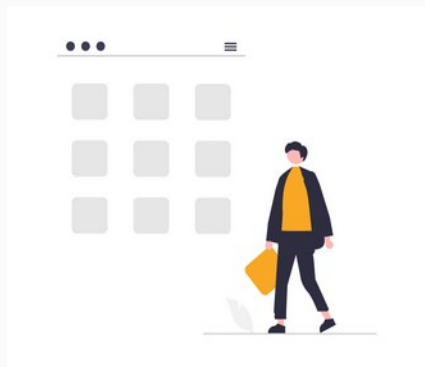
LemonLDAP::NG



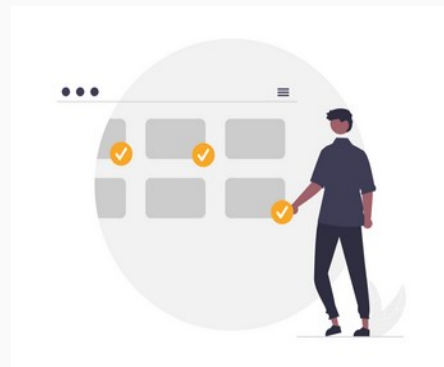
Fonctionnalités



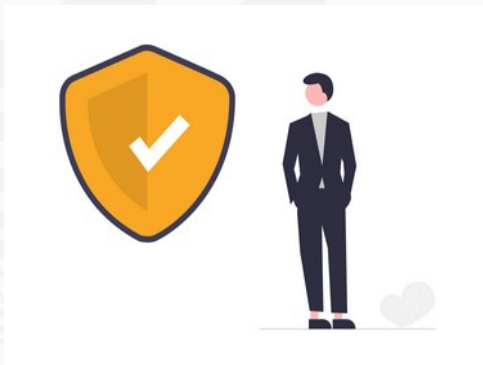
SSO & Contrôle d'accès



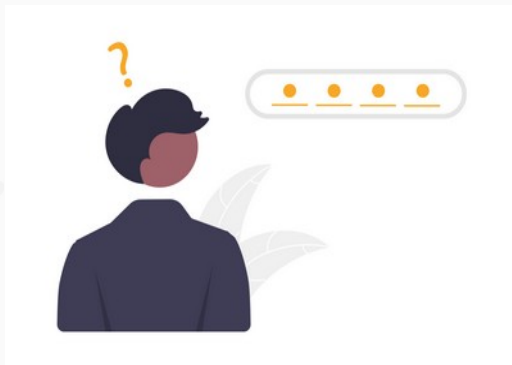
Menu des applications



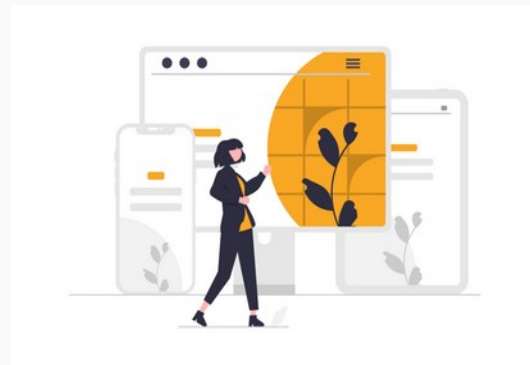
CAS / SAML / OIDC



Second facteurs (2FA)



Gestion du mot de passe



Personnalisation graphique



[Home](#) [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



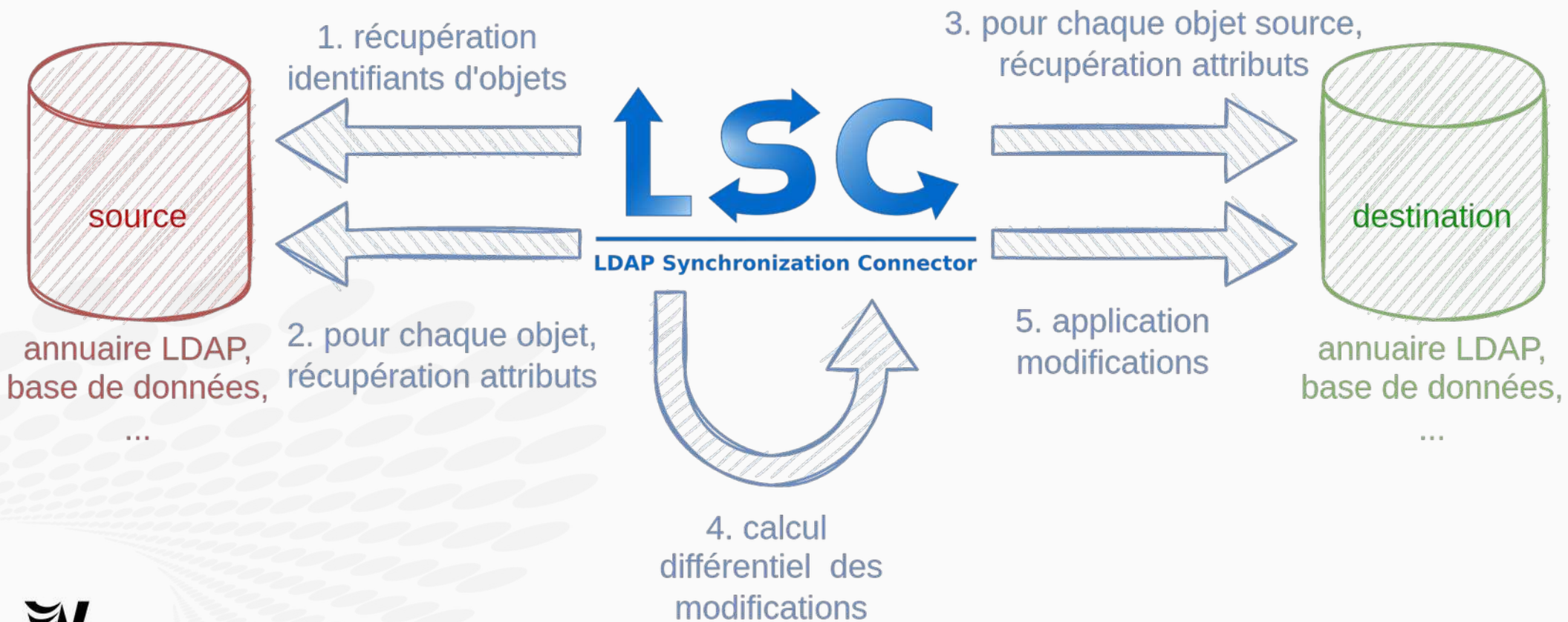
Sessions explorer
Explore WebSSO sessions



2FA sessions explorer
Explore second factor

LDAP Synchronization Connector





LTB Self Service Password



Fonctionnalités

- Changement du mot de passe
- Réinitialisation via mail
- Réinitialisation via SMS
- Réinitialisation via questions/réponses
- Changement de sa clé SSH
- Modification de mots de passe secondaires
- Hook : propagation du mot de passe à d'autres systèmes





☒ Change your password

1 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



Confirm



Captcha



Send

LTB

White Pages



Fonctionnalités

- Recherche simple et avancée
- Répertoire
- Trombinoscope
- Vue sur un plan (OpenStreetMap)
- Modification de sa fiche



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



LDAP Tool Box White Pages - version 0.4

LTB Service Desk



Fonctionnalités

- Gestion du mot de passe et du statut du compte
- Tableaux de bord (comptes expirés, bloqués, inactifs etc.)
- Création de comptes
- Modification, renommage, suppression de comptes
- Hooks par script externe ou fonction PHP
- Toutes les fonctionnalités sont activables/désactivables par configuration



Service Desk Create entry Dashboards Audit logs Search

Samantha Carter

Identifier samantha.carter

First name Samantha

Last name Carter

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)

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

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

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

AVANT

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage Fenêtre ?

← → [Icones]

Utilisateurs et ordinateurs Active Directory

- 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	Utilisateur	

Context menu for 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

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)

APRÈS

oudot



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

Stand 1C25

**OPEN
SOURCE
EXPERIENCE**