

**OPEN  
SOURCE  
EXPERIENCE**



**Des outils Open Source pour piloter votre  
Active Directory en mode Web**

# Ordre du jour



**1. Présentation**

**2. Le projet LDAP Tool Box**

**3. Itb-common**

**4. Self-Service-Password**

**5. Service-Desk**





# Présentation

# Présentation



David COUTADEUR

architecte en gestion d'identité

~12 ans d'expérience dans le domaine

passionné d'open-source



[david.coutadeur@worteks.com](mailto:david.coutadeur@worteks.com)



[@dcoutadeur@toot.aquilenet.fr](https://toot.aquilenet.fr/@dcoutadeur)



[www.linkedin.com/in/david-coutadeur-06571a1a4](https://www.linkedin.com/in/david-coutadeur-06571a1a4)



# Worteks

Société d'expertise, d'édition et d'hébergement Open Source

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

Partenaires



Membre fondateur



# 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





# Le projet LDAP Tool Box



# Le projet LDAP Tool Box

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



<https://ltb-project.org>



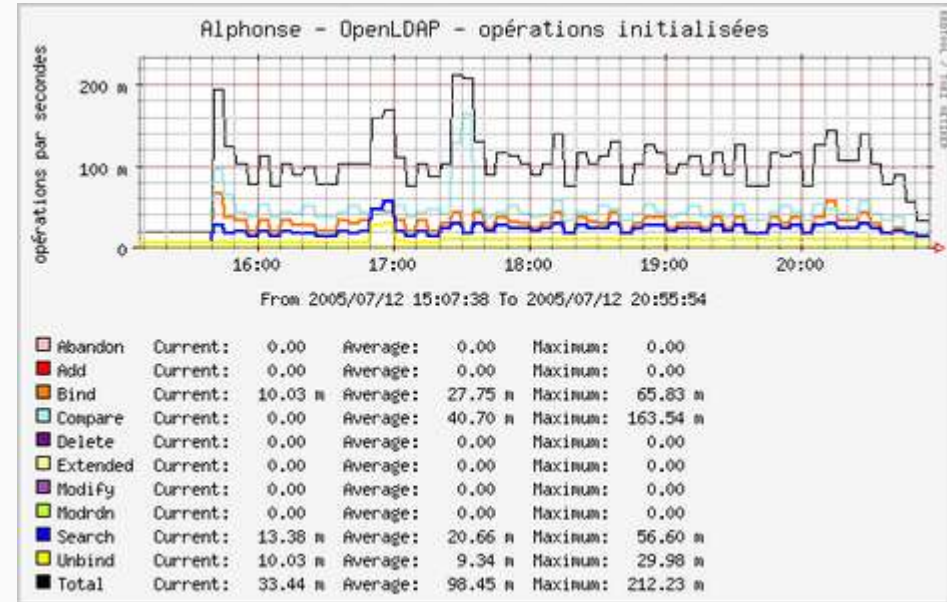
# OpenLDAP

- 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®**



# 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





**Itb-common**

# ltb-common

- Bibliothèque de développement commune à
  - self-service-password,
  - service-desk,
- Permet de mutualiser les fonctions :
  - LDAP
    - interface pour implémenter OpenLDAP et AD [NEW 0.3.0](#)
  - d'envoi de mail
  - de sélection de la langue du client
  - de changement et de vérification de mots de passe
  - de vérification des politiques de mots de passe [NEW 0.3.0](#)
  - de cache [NEW 0.3.0](#)

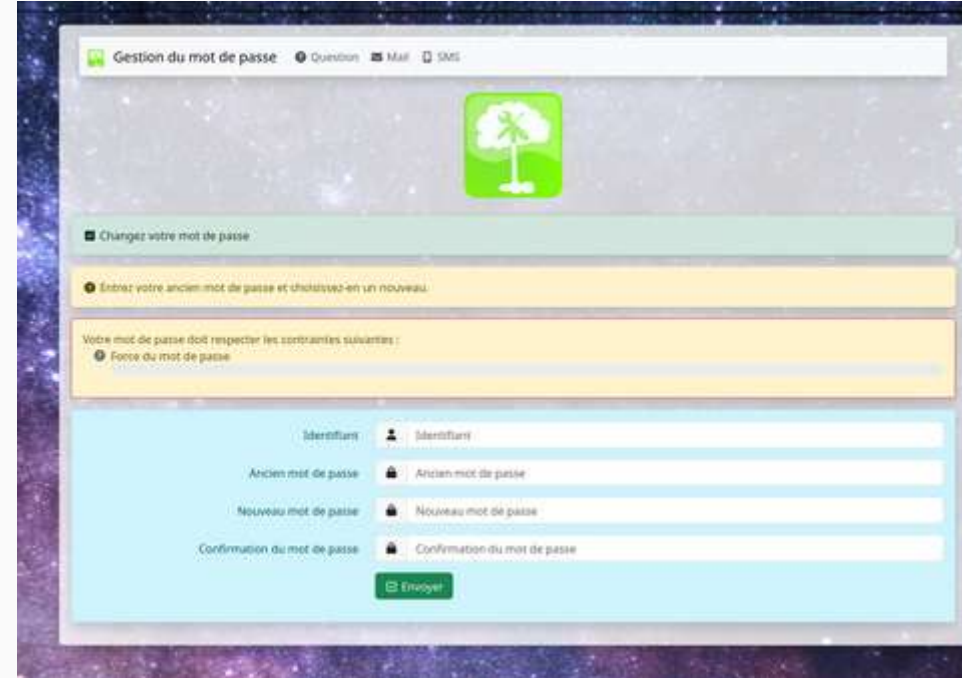




# Self-Service-Password

# Self-Service-Password

- Outil de changement de mot de passe
  - avec l'ancien mot de passe
  - par question / réponse
  - par mail
  - par SMS
- Changement de clé SSH
- Pré/Post traitements
- Notifications par mail
- Compatible LDAP et Active Directory



The screenshot shows a web interface for password management. At the top, there is a header with the title "Gestion du mot de passe" and navigation links for "Question", "Mail", and "SMS". Below the header is a green square icon with a white tree. A green button labeled "Changer votre mot de passe" is visible. Below this is a yellow box with the instruction "Entrez votre ancien mot de passe et choisissez-en un nouveau." Underneath, a yellow box lists password requirements: "Votre mot de passe doit respecter les contraintes suivantes:" and "Force du mot de passe". The main form area has a light blue background and contains several input fields: "Identifiant" (with a user icon), "Ancien mot de passe" (with a lock icon), "Nouveau mot de passe" (with a lock icon), and "Confirmation du mot de passe" (with a lock icon). A green "Envoyer" button is at the bottom right of the form.



# Self-Service-Password

- Compatibilité Active Directory
  - `$ad_mode = true` pour gérer le mot de passe unicodePwd
  - utilisation obligatoire d'une connexion TLS pour le chgt de MdP
  - Options de configuration spécifiques à AD :
    - `force_unlock` : déverrouillage automatique au chgt de MdP
    - `force_pwd_change` : forcer chgt de MdP à la prochaine connexion
    - `change_expired_password` : autorise le chgt d'un MdP expiré (il sera changé par le compte admin)



# Self-Service-Password

- API REST pour changement et réinitialisation du mot de passe
- Protection des attaques par force brute (rate limit)
- Multi tenants
- Gestion de l'entropie [NEW 1.6.0](#)
- champs de mots de passe personnalisés par applications [NEW 1.6.0](#)
- Système de Captcha (interne, FriendlyCaptcha, Recaptcha) [NEW 1.7.0](#)
- Nouveau système de cache pour : [NEW 1.7.0](#)
  - la gestion des sessions “longues” (envoi de mails, sms,...)
  - éviter le rejeu de formulaires

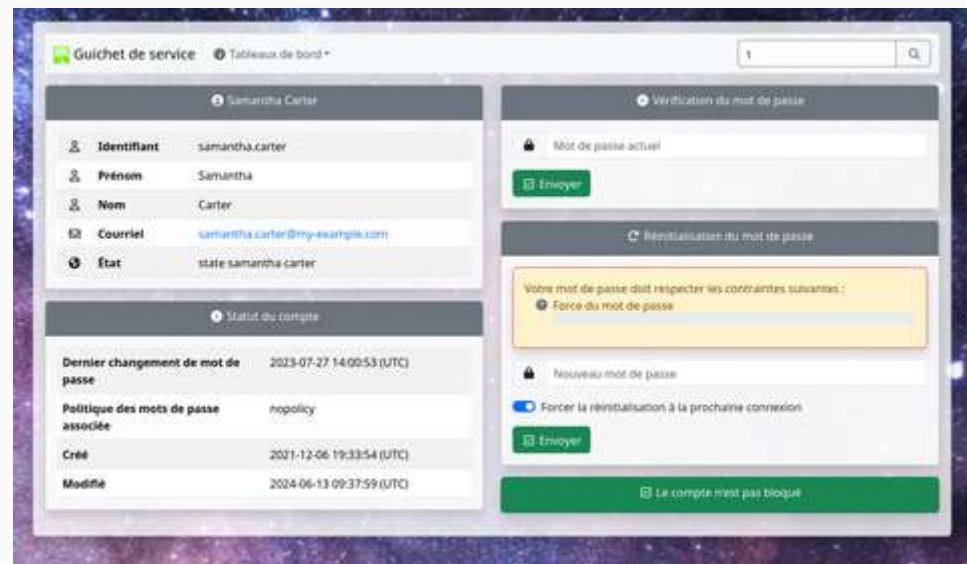




# Service-Desk

# Service-Desk

- Outil de gestion de comptes
  - visualisation attributs utilisateurs
  - statut des comptes
  - changement / vérification MdP
  - Blocage/déblocage
  - Pré/Post traitements
  - Audit
  - Notifications par mail



# Service-Desk

- support Active Directory [NEW 0.6.0](#)
  - modification du MdP (`unicodePwd`)
  - Verrouillage (`lockouttime`)
  - expiration (`pwdlastset` + `pwdMaxAge`)
  - désactivation (`userAccountControl`)
  - recherche paginée pour passer la limite par défaut de 1000 entrées
- affichage politique de MdP de l'annuaire associée à l'utilisateur [NEW 0.6.0](#)



# Service-Desk

- vérification du mot de passe aussi dans l'historique des anciens mots de passe [NEW 0.6.0](#)
- définition politique de MdP locale [NEW 0.6.0](#)
- le navigateur ne demande plus le stockage du nouveau MdP [NEW 0.6.0](#)
- bouton pour bloquer un compte, sans déblocage automatique par un changement de MdP [NEW 0.6.0](#)

The screenshot displays the 'Guichet de service' interface for user 'Daniel Jackson'. It features several panels:

- Profile Information:** Identifiant: daniel.jackson, Prénom: Daniel, Nom: Jackson, Courriel: daniel.jackson@my-example.com, État: state Daniel Jackson.
- Statut du compte:** A table showing password change history.

Statut du compte	Date
Dernier changement de mot de passe	2024-10-17 16:23:03 (UTC)
Politique des mots de passe associée	default
	2024-10-18 09:42:14 (UTC)
Créé	2021-12-06 19:33:54 (UTC)
Modifié	2024-10-18 09:49:19 (UTC)
Date d'expiration	2025-01-15 16:23:03 (UTC)
- Vérification du mot de passe:** A form for 'Mot de passe actuel' with an 'Envoyer' button.
- Réinitialisation du mot de passe:** A section with a list of password constraints:
  - ✗ Nombre minimum de caractères : 10
  - ✓ Nombre maximum de caractères : 20
  - ✗ Nombre minimum de minuscules : 1
  - ✗ Nombre minimum de majuscules : 1
  - ✗ Nombre minimum de chiffres : 1
  - ✗ Nombre minimum de classes de caractères : 3
  - ✓ Caractères interdits : @%
  - ✓ Votre nouveau mot de passe ne doit pas être identique à votre identifiant
  - ⓘ Votre nouveau mot de passe ne doit pas être connu d'une base publique de mots de passe compromis
  - ✓ Votre nouveau mot de passe ne doit pas avoir son seul caractère spécial en première ou dernière position.
  - ⊙ Force du mot de passe
- Nouveau mot de passe:** A form for 'Nouveau mot de passe' with a 'Forcer la réinitialisation à la prochaine connexion' checkbox and an 'Envoyer' button.
- Account Status:** A series of green status boxes: 'Le compte n'est pas verrouillé', 'Verrouiller le compte', 'Le compte est active', and 'Désactiver le compte'.





# Retrouvez-nous au stand B13

- Rencontrez nos experts, nos clients et nos partenaires
- Assistez à plusieurs mini-conférences
- Et bien d'autres surprises à découvrir sur place !





# Membre fondateur du groupement

---



Retrouvez les au stand B15 !



[www.worteks.com](http://www.worteks.com)

✉ [info@worteks.com](mailto:info@worteks.com)

☎ +33 1 84 20 86 47

🌐 [worteks\\_com](https://www.worteks.com)

📱 [worteks](#)

**Merci de votre attention**