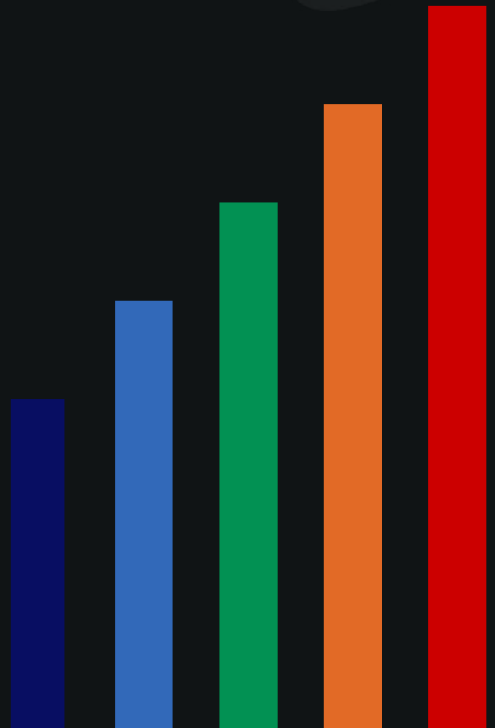
Worteks

make IT work, make IT free

Innovations et Roadmap IAM

20 octobre 2025
Paris

Sommaire



LL::NG

LTB

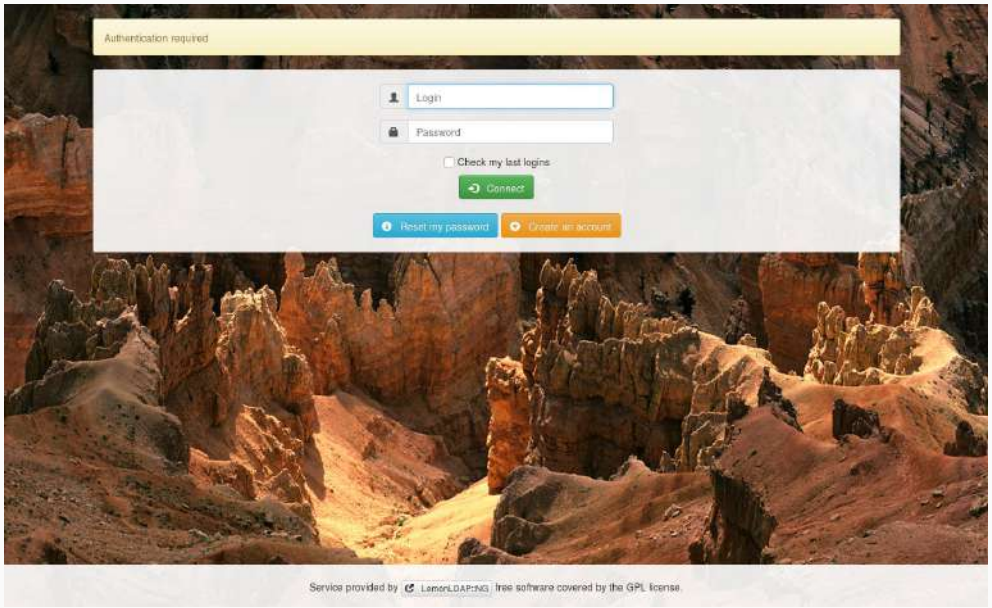
FusionIAM

Standards LDAP / OIDC

LemonLDAP::NG

LemonLDAP::NG : présentation

- Single Sign On
- logiciel libre, GPLv2, copyleft
- création en 2005 par la GN
- perl, javascript, css, html
- support des principaux protocoles:
  - CAS
  - SAML
  - OIDC



- Plusieurs références d’entreprises et organisations : jusqu’à 240 000 utilisateurs et 370 applications

LemonLDAP::NG : innovations

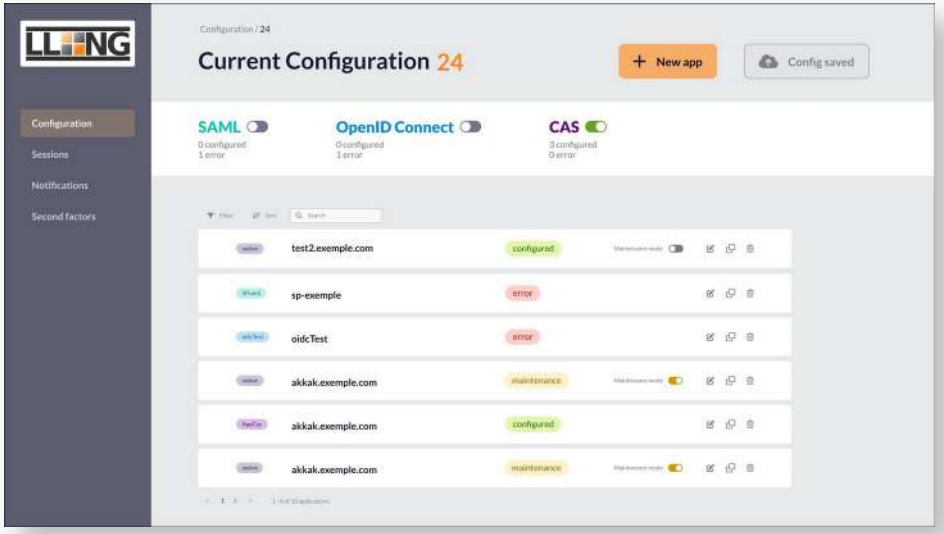
- **2.22.0 :**
  - affichage d’un message si le navigateur est déjà de confiance
  - ajout de points d’entrée (hooks) :
    - autour de la construction des jetons JWT (ID tokens)
    - lors de la validation de la redirect_uri
  - édition du nom du second facteur lors de l’enregistrement
  - politique de support :
    - retrait du support EL7
    - ajout du support EL10
    - deux versions LTS : 2.16 et 2.21, maintenues pour 5 ans
    - nouveaux dépôts communautaires pour les LTS 2.16 et 2.21

LemonLDAP::NG : innovations

- **2.22.0 :**
  - gestion de plusieurs clés OIDC / SAML
    - possible d'utiliser des clés EC pour un RP et RSA pour un autre
    - utilisation d'une clé dédiée pour le fournisseur JitsiMeet
  - ajout de statistiques sur l'outil de purge de sessions
    - nombre d'objets purgés (global, par backend)
    - temps de traitement (global, par backend)
  - option pour forcer le changement de mot de passe avant l'expiration (délai avant expiration)
  - plugin Webcron
  - nouveau panneau sur le portail pour gérer les sessions offline

LemonLDAP::NG : roadmap v3

- Refonte de l’interface du portail d’authentification
- Refonte de l’interface du Manager
- Meilleure gestion de l’encodage
- Flux d’authentification (continuation)



LTB

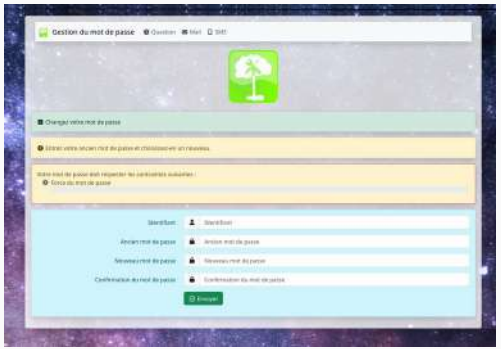
LTB : présentation

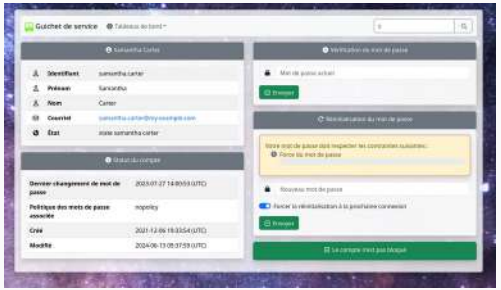
- Projet libre créé en 2009
- Regroupement d'outils dédiés à la gestion des annuaires LDAP
- Au début : paquets OpenLDAP et scripts de supervision
- Licence GPL
- Publié sur GitHub
- Projet OW2

https://ltb-project.org

LTB : présentation

- paquets OpenLDAP rpm et deb
- self-service-password
- service-desk
- white-pages
- documentation, base d’articles
- scripts de supervision





LTB : innovations

- **paquets OpenLDAP-LTB**
  - nouveaux paquets pour Debian 13 et Red-Hat 10
  - OpenLDAP 2.6.10 (mai 2025) est maintenant la LTS
  - OpenLDAP 2.5.20 (mai 2025) est la dernière publication en 2.5

- **self-service-password**
  - 1.7.2 (janvier 2025)
  - 1.7.3 (mars 2025)

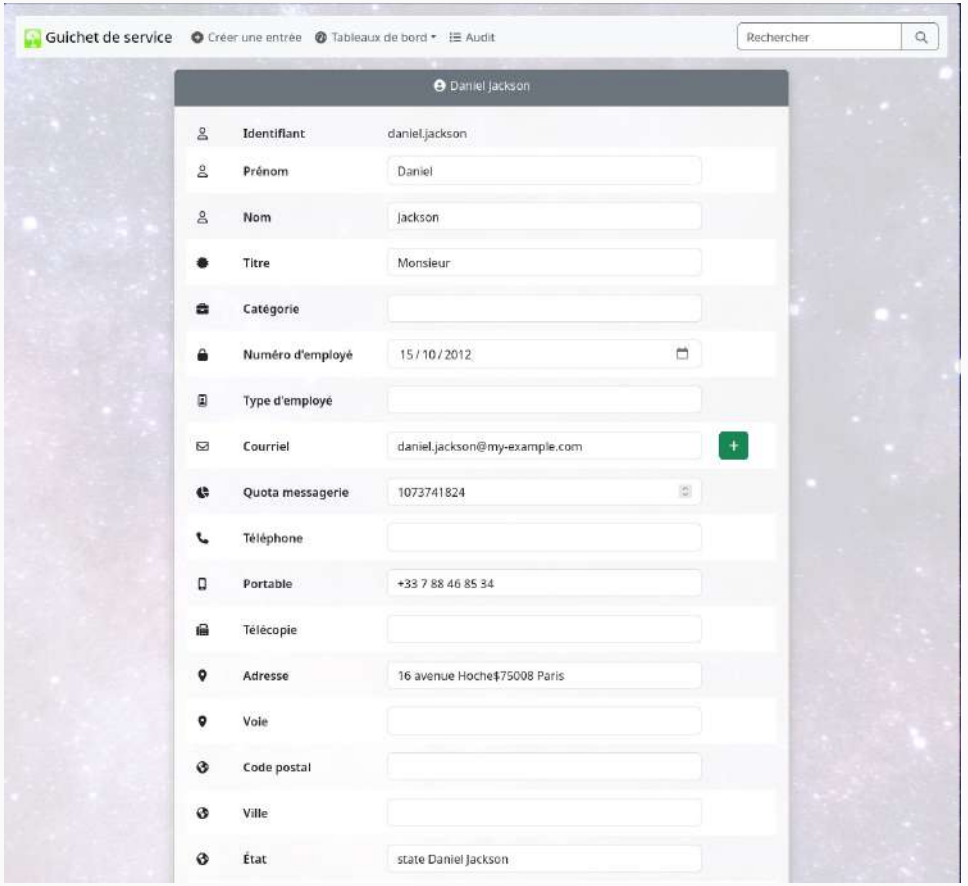
: corrections de bug

LTB : innovations

- **service-desk**
  - **0.7 (septembre 2025)**
    - nouvelles pages pour créer, modifier, renommer un compte
    - refactoring complet des tableaux (listes d'entrés) et de la pagination : système d'API côté serveur avec interrogation AJAX côté client
    - lors de l'édition, configuration des valeurs liées à un DN avec dn_link_label_attributes
    - dans les pages d'édition, remplacement des tableaux par le système grid/flex de bootstrap
    - personnalisation graphique par surcharge des templates souhaités dans un dossier de thème spécifique
    - traduction en Norvégien
    - gestion de la favicon

LTB : innovations

- **service-desk**
  - **0.7.1 (septembre 2025)**
    - attributes_static_list : attributs dont la liste de valeurs est fixée en dur
    - attributes_list : attributs dont la liste de valeurs est fixée par une recherche LDAP



- **white-pages**
  - pas de version récente

LTB : roadmap

- **self-service-password (en construction)**
  - option pour déverrouiller le compte lors d’un changement de mot de passe
  - construction du DN de l’utilisateur à partir de son identifiant, afin de changer son MdP sans compte de service
  - injection des paramètres de configuration automatiquement dans les templates
  - envoi des mails avec un template HTML

LTB : roadmap

- **service-desk (en construction)**
  - optimisation : amélioration des performances pour l'affichage des listes de comptes verrouillés, mots de passe expirés,…
    - 30 000 comptes => environ 30 secondes
  - ajout de la notion d'attribut obligatoire / facultatif
  - gestion du mot de passe Samba
  - ajout du panneau de recherche avancé de white-pages
  - système de plugins, appelés pour certains points d'entrée, par exemple l'affichage ou l'édition d'une valeur, et permettant l'ajout d'éléments graphiques à certains endroits
  - workflow de création de compte
  - gestion de l'appartenance aux groupes
  - gestion des politiques de mots de passe

LTB : roadmap

- **white-pages (en construction)**
  - intégrer les développements de service-desk dans white-pages (via ltb-common ?)
    - système de tableaux en ajax avec pagination
  - vérificateur de syntaxe pendant l’édition (selon le type d’attribut)
  - système de tooltip pendant l’édition
  - amélioration des performances pour le rendu des photos
  - affichage de l’arborescence organisationnelle

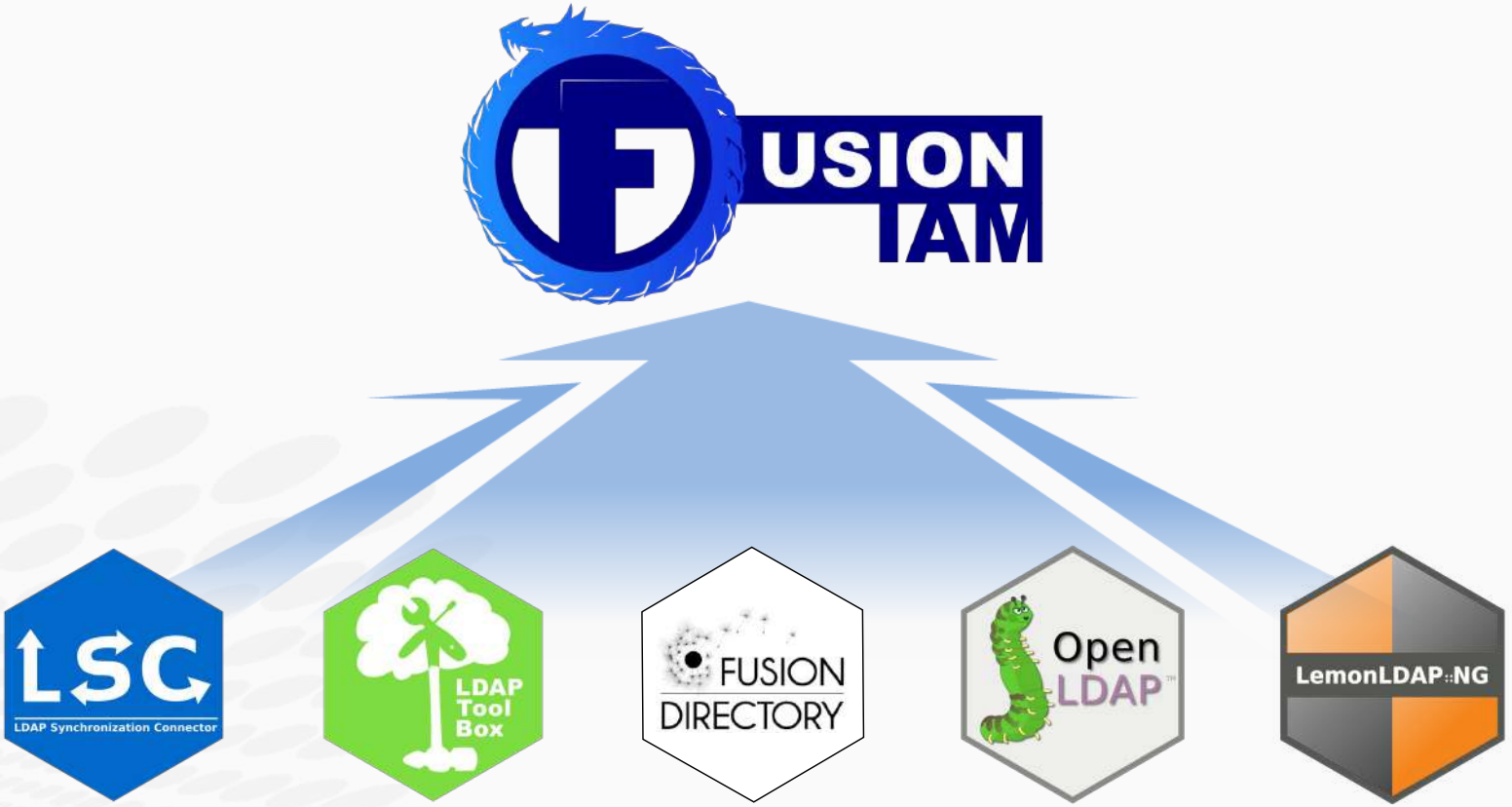
FusionIAM

FusionIAM : présentation

- Projet libre créé en 2018
- But : regrouper des logiciels open-source pour construire une offre globale d'identité en SAAS
- basé sur des images Docker
- Licence GPL
- Projet OW2

https://www.fusioniam.org/

FusionIAM : présentation



FusionIAM : innovations

- Montée de version des différents composants :
  - OpenLDAP 2.6
  - LemonLDAP::NG 2.21.2
  - Service-desk 0.7
  - Fusiondirectory 1.5
- Montée de version de l'image de base RockyLinux de 9 à 10
- Ajout d'une image LSC pour synchroniser l'annuaire LDAP
- Accès à l'API de Fusiondirectory (authentification Basic)
- Ajout du plugin invitations sur FusionDirectory (pour l'enregistrement de comptes)

FusionIAM : innovations

Ajout de méthodes de configuration supplémentaires sur LL::NG :

- fichier `lemonldap-ng.ini`
- dossier `conf-override` (peuplé par variables d'environnements) 
- fichiers `llng_config_*.yaml` dans l'image 
- configuration en base (éditable via l'interface Manager)

FusionIAM : roadmap

- **Version 1.0 (en construction)**
  - système de mise à jour de FusionIAM
    - migration automatique des bases de données
    - migration des paramètres, configurations,…
    - sous la forme d’une image docker dédiée ?
  - documentation complète à écrire :
    - pour un usage docker / podman / docker-compose
    - pour un usage Kubernetes / Openshift
  - développer thème graphique homogène à tous les composants

FusionIAM : roadmap

- **Version ?**
  - disposer de tableaux de bords avec des métriques (grafana)
  - système de notification par mail des évènements principaux :
    - mot de passe sur le point d’expirer
    - compte inactif
    - mot de passe changé
    - connexion depuis un nouvel emplacement

Veille active sur les standards

LDAP

- Draft sur de nouvelles syntaxes : https://datatracker.ietf.org/doc/draft-codere-ldapsyntax/
  - Dates, durées
  - Nombres flottans, entiers
  - Langue, URI, jeton...

OpenID Connect

- Groupe de travail IPSIE: https://openid.net/wg/ipsie/ :
  - Interoperability Profiling for Secure Identity in the Enterprise
  - OpenID Connect + SAML + SCIM + …
- AuthZEN : https://openid.net/specs/authorization-api-1_0-01.html
- Native SSO for Mobile Apps : https://openid.net/specs/openid-connect-native-sso-1_0.html

Worteks

make IT work, make IT free

www.worteks.com

info@worteks.com

+33 1 84 20 86 47

worteks_com

worteks

Merci pour votre attention