IDENTITY DAYS

28 octobre 2021 - PARIS

@IdentityDays #identitydays2021

Merci à tous nos partenaires !

Microsoft

Vorteks
make IT work, make IT free

zscaler

onelogin

SailPoint

METSYS

Auth0

FUSION DIRECTORY

tenable

yubico

ManageEngine

WALLIX
CYBERSECURITY SIMPLIFIED

Exakis Nelite
Magellan Partners

Alphorm.com

Quel avenir pour OpenLDAP ?

David Coutadeur
Vorteks
make IT work, make IT free

David COUTADEUR

expert en gestion d'identité
~ 10 ans d'ancienneté
passionné d'open-source

Worteks
make IT work, make IT free

david.coutadeur@worteks.com
@dcoutadeur

Ordre du jour

1. Qu'est-ce que le LDAP ?
2. Paysage des annuaires
3. Présentation d'OpenLDAP
4. Comparatif des performances
5. Présentation de LDAP Tool Box
6. Les nouveautés d'OpenLDAP 2.5
7. Conclusion

Vorteks

make IT work, make IT free

Service

Infrastructures hétérogènes et complexes, cloud, authentification, securité

- Etudes, audit et consulting
- Expertise technique
- Support technique
- Formation
- R&D et innovation

Édition

V'Sweet — Portail d'applications collaboratif

V'Opla — Plateforme mutualisée de développement

V'IDaaS — Gestion des identités des accès

Partenaires

Red Hat Advanced Business Partner Reseller

BlueMind

ONLYOFFICE

Collabora Online

Qu’est ce que le LDAP ?

Qu'est-ce que le LDAP ?

- protocole d'annuaire
  annuaire = recueil d'informations, historiquement liées à l'identité

  - 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

Qu'est-ce que le LDAP ?

Le protocole définit :

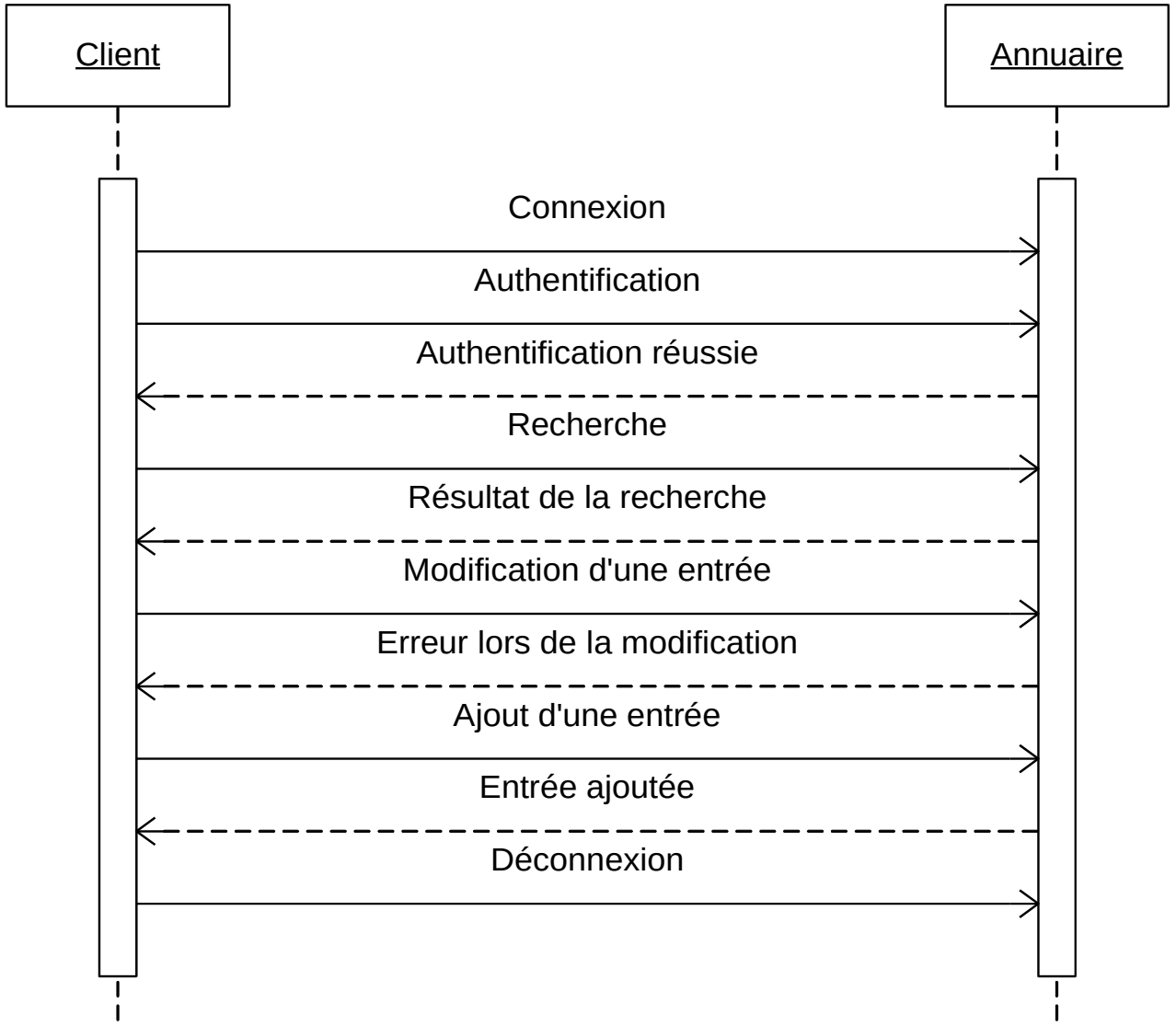
la communication client serveur
- au dessus de TCP / IP
- l'encodage (LBER)

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

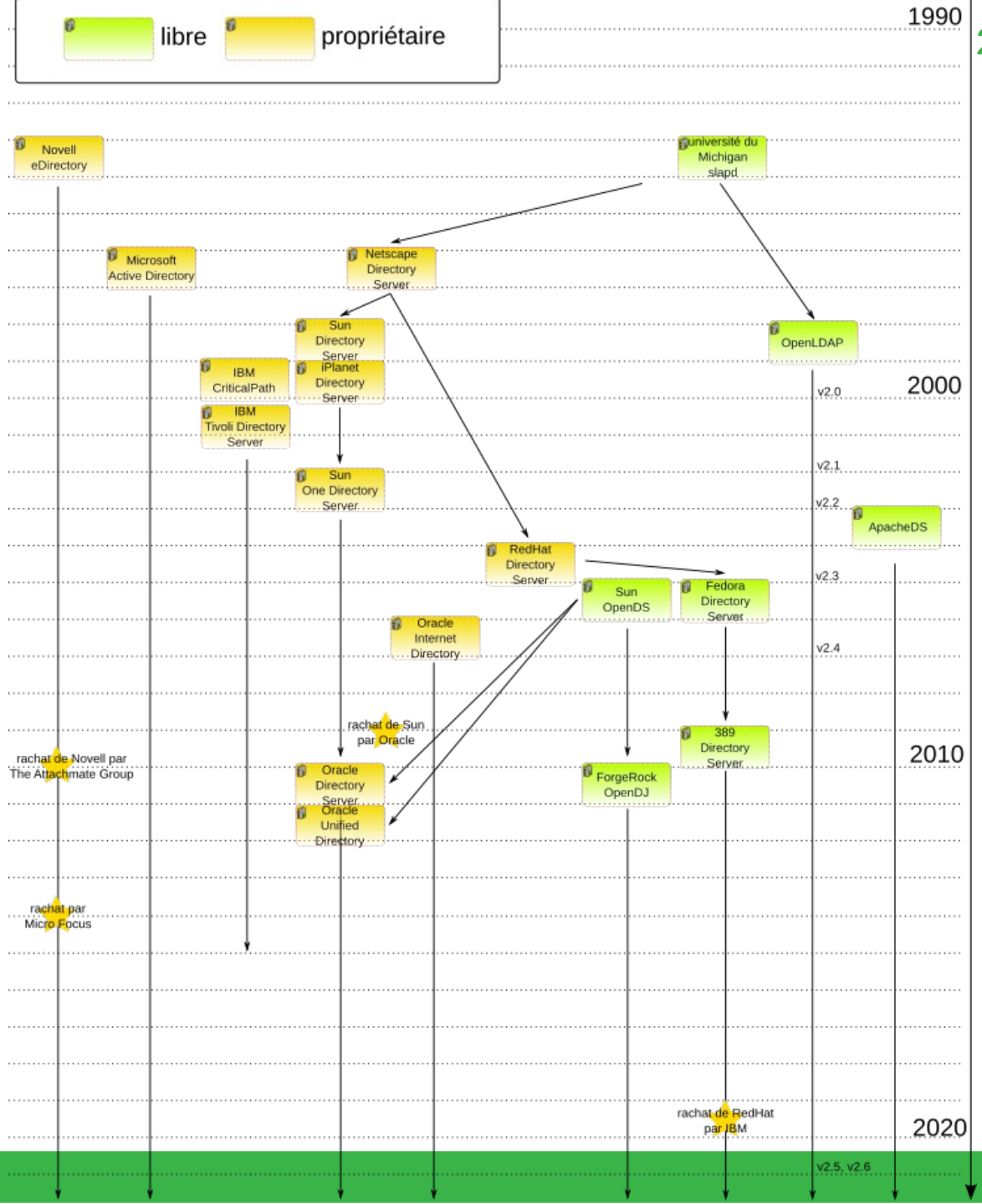
le modèle d'information (schéma)

le modèle de nommage (DIT)



Paysage des annuaires

Paysage des annuaires



Présentation d'OpenLDAP

Présentation d'OpenLDAP

Historique

- issu du serveur LDAP de l'université du Michigan, dont dérive également Netscape Directory Server
- projet initié en 1998 (OpenLDAP v1), avec support LDAPv2
- conforme LDAPv3 en 2000 (OpenLDAP v2)
- version stable actuelle : OpenLDAP 2.5 (avril 2021)
- version 2.6 en construction : prévue pour fin 2021
- 3 développeurs principaux :
  - Howard Chu
  - Ondřej Kuzník
  - Quanah Gibson-Mount

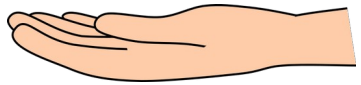
Présentation d'OpenLDAP

Caractéristiques

- OpenLDAP Public License, dérivée de la GNU GPL

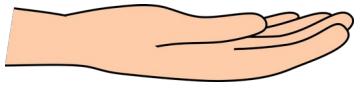
contient

- serveur LDAP
- bibliothèques de connexion
- commandes LDAP
- commandes de gestion du contenu
- API (C, C++, TCL, Java)



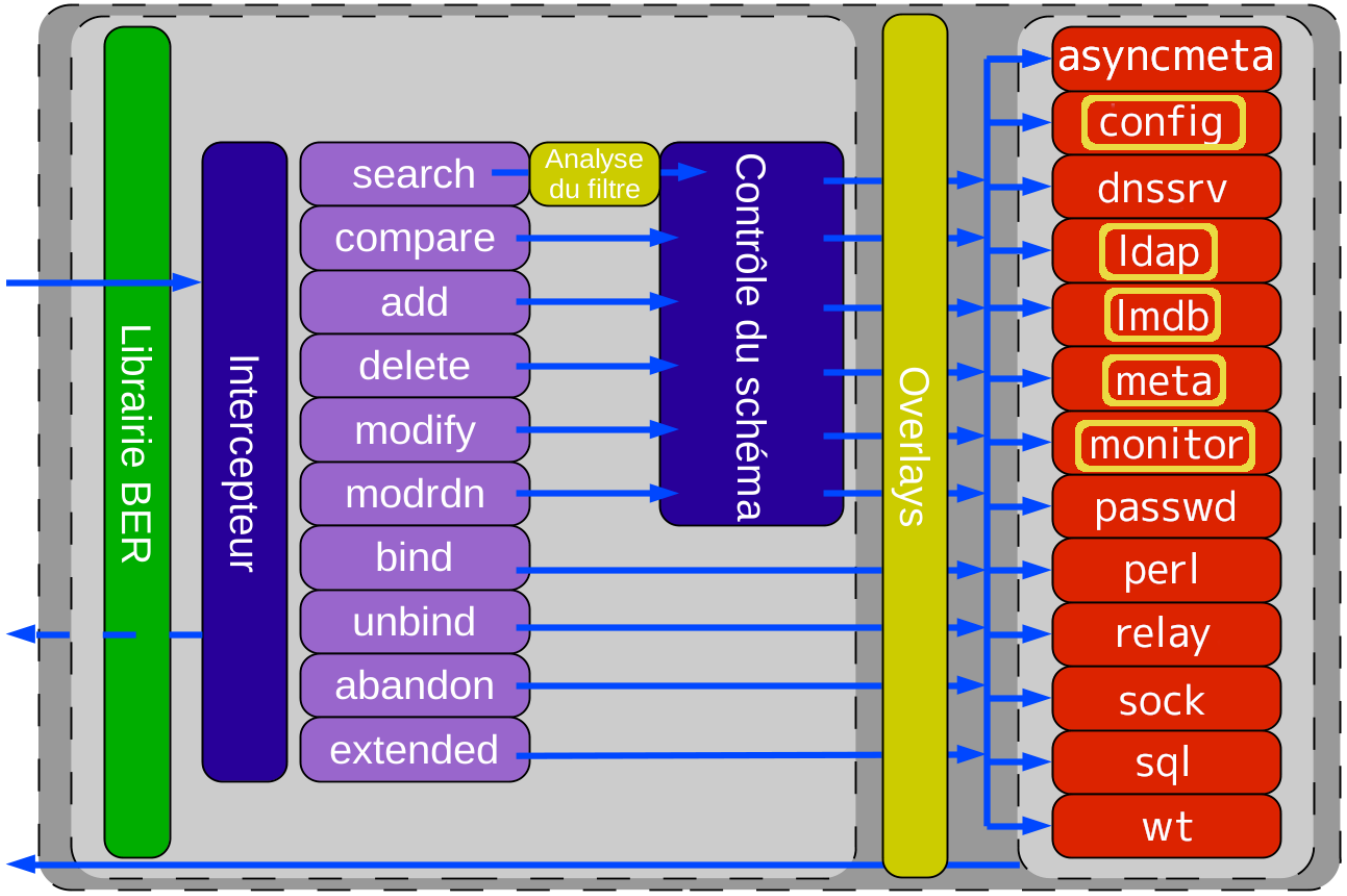
supporte

- LDAPv3
- réplication multi-maître, complète et différentielle
  - moteur syncrepl
  - Content Synchronization Operation (RFC 4533)
- délégation d'authentification SASL / GSSAPI
- internationalisation UTF-8 via Unicode



Présentation d'OpenLDAP

Fonctionnement



Backend = composant qui stocke ou traite des données en réponse à une requête ldap

Overlay = extension pour personnaliser le comportement des backends

Choix d'overlays : politique des mots de passe, listes dynamiques, intégrité référentielle

Comparatif des performances

Comparatif des performances

Critères pour retenir les concurrents

- annuaires LDAP natifs, généralistes
- maturité
- fonctionnalités
- activité de l'équipe de développement

389DS (C)
Red Hat

ApacheDS (java)
fondation Apache

OpenDJ (java)
Forgerock

OpenLDAP (C)
Symas

OUD (java)
Oracle

- Critères de performances :
  - temps de réponse en lecture
  - temps de réponse en écriture

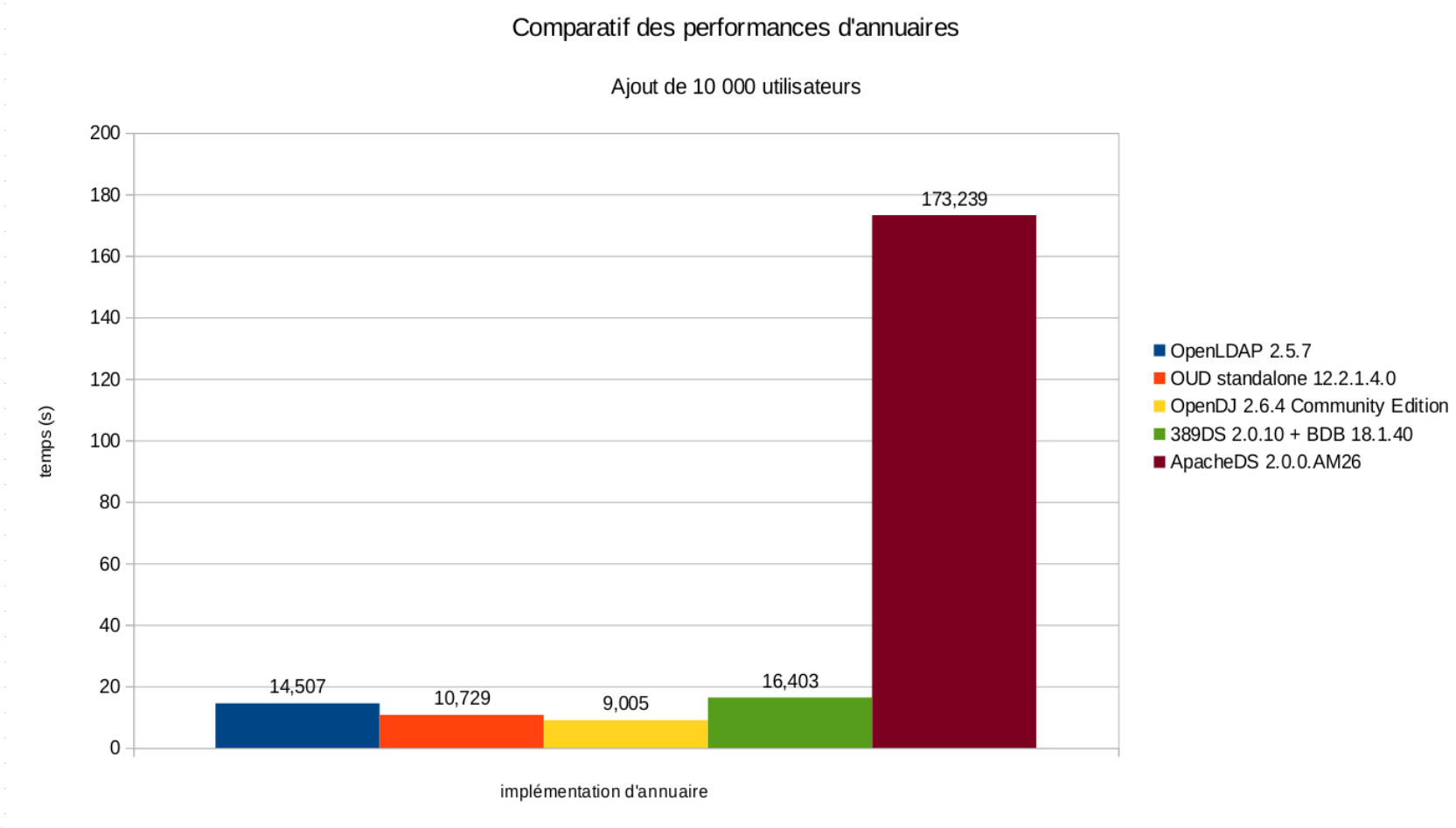
Comparatif des performances

Protocole de test

- conteneur LXC Debian 10
- machine :
  - Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz (4 coeurs, 8 threads)
  - 16 Go de RAM
  - disque SSD
- 4 tests :
  - **ajout de 10 000 utilisateurs**
    1 thread réalise un bind, ajoute successivement 10 000 utilisateurs (uid=userN), puis réalise un unbind
  - **10 000 recherches d'utilisateur**
    1 thread réalise un bind, 10 000 recherches successives (uid=userN), et un unbind
  - **8000 dumps de tout l'annuaire**
    8 threads réalisent en parallèle un bind, 1 000 recherches successives de tout l'annuaire (objectClass=*), et un unbind
  - **suppression de 10 000 utilisateurs**
    1 thread réalise un bind, supprime successivement les 10 000 utilisateurs précédemment ajoutés, puis réalise un unbind

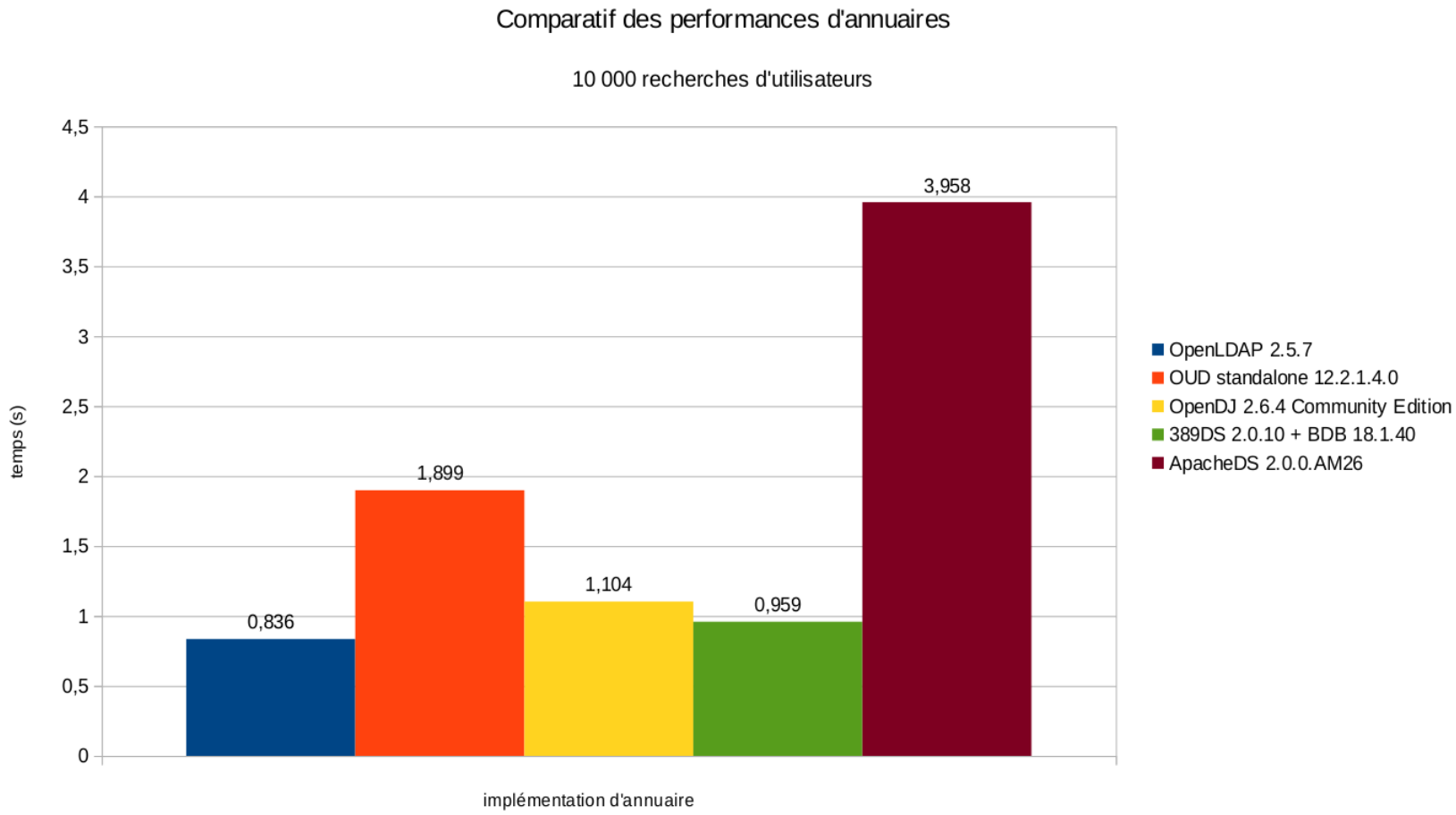
Comparatif des performances

Résultats



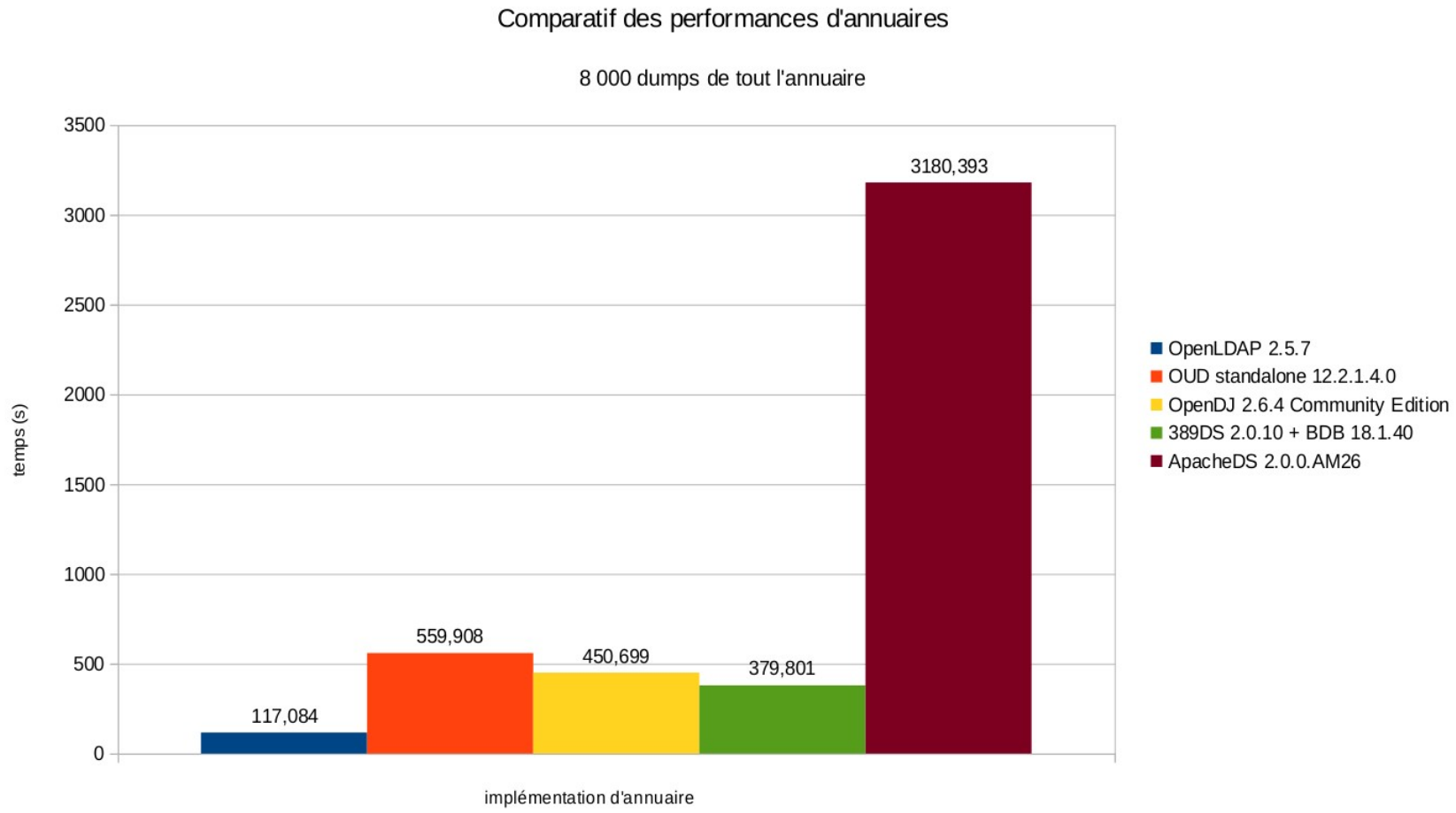
Comparatif des performances

Résultats



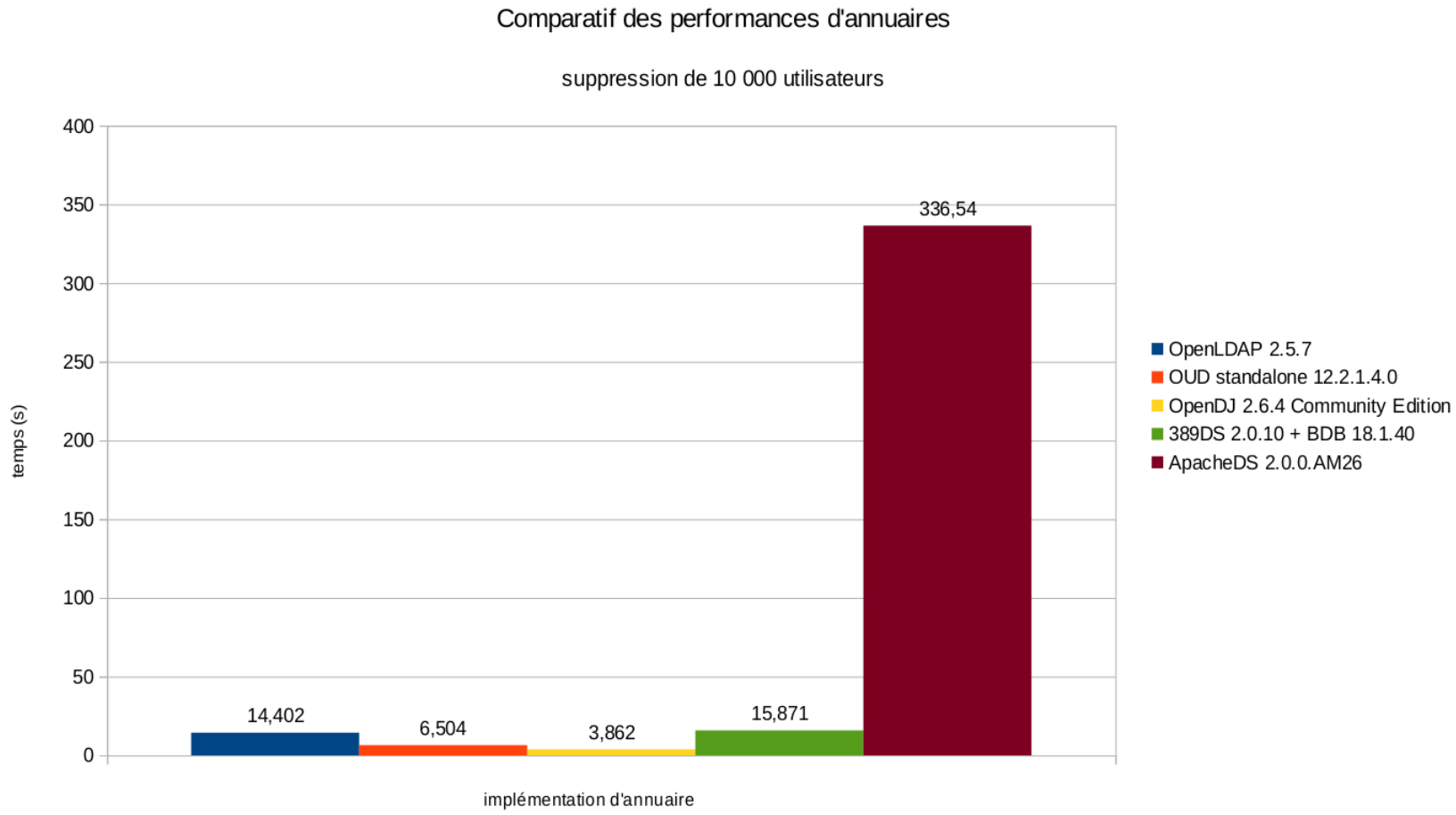
Comparatif des performances

Résultats



Comparatif des performances

Résultats



Présentation de LDAP Toolbox

Présentation de l'initiative LDAP Toolbox

- projet lancée en 2009

- supporté par OW2 : une association indépendante à but non lucratif visant à promouvoir une base de logiciels d'infrastructure open-source
- Community Award d'OW2 reçu en 2021 !

- à l'origine :
  - fournir des didacticiels, des listes de diffusion et des scripts pour exploiter des annuaires LDAP

- aujourd'hui :
  - la base de code et de tutoriels s'est étendue
  - LTB-project propose des logiciels complets

Présentation de l'initiative LDAP Toolbox

Services proposés par LDAP-toolbox

des paquets communautaires pour OpenLDAP

- les paquets des principales distributions Linux sont souvent en retard dans les versions distribuées
- fourniture de paquets RPM et DEB à jour
- CLI pour configurer, administrer, superviser l'annuaire
- extensions (overlays) supplémentaires

des scripts d'exploitation

- notification d'expiration par mail, conversion LDIF, statistiques, nettoyage,...

Présentation de l'initiative LDAP Toolbox

Services proposés par LDAP-toolbox

une base documentaire

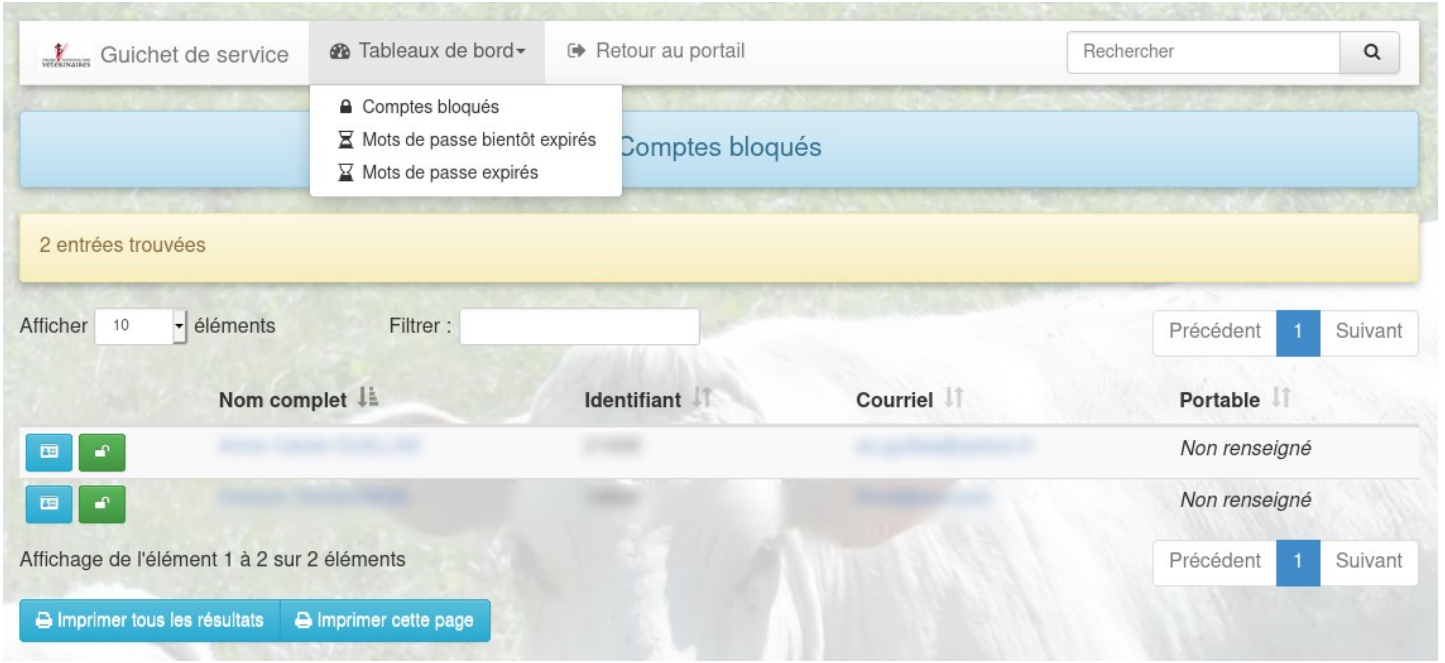
- migration en cours au format *reStructuredText* (sphinx)
  https://ltb-project-documentation.readthedocs.io
- installation, configuration des paquets
- supervision, statistiques LDAP avec Nagios® et Cacti
- documentation des applicatifs LTB
- tutoriels divers : migration d'annuaire, délégation d'authentification,...

Présentation de l'initiative LDAP Toolbox

Services proposés par LDAP-toolbox

une interface web de gestion dédiée aux administrateurs : Service Desk

- tableaux de bord pour visualiser les comptes et leur statut (bloqués, expirés)
- test d'un mot de passe
- réinitialisation d'un mot de passe
- blocage, déblocage d'un compte

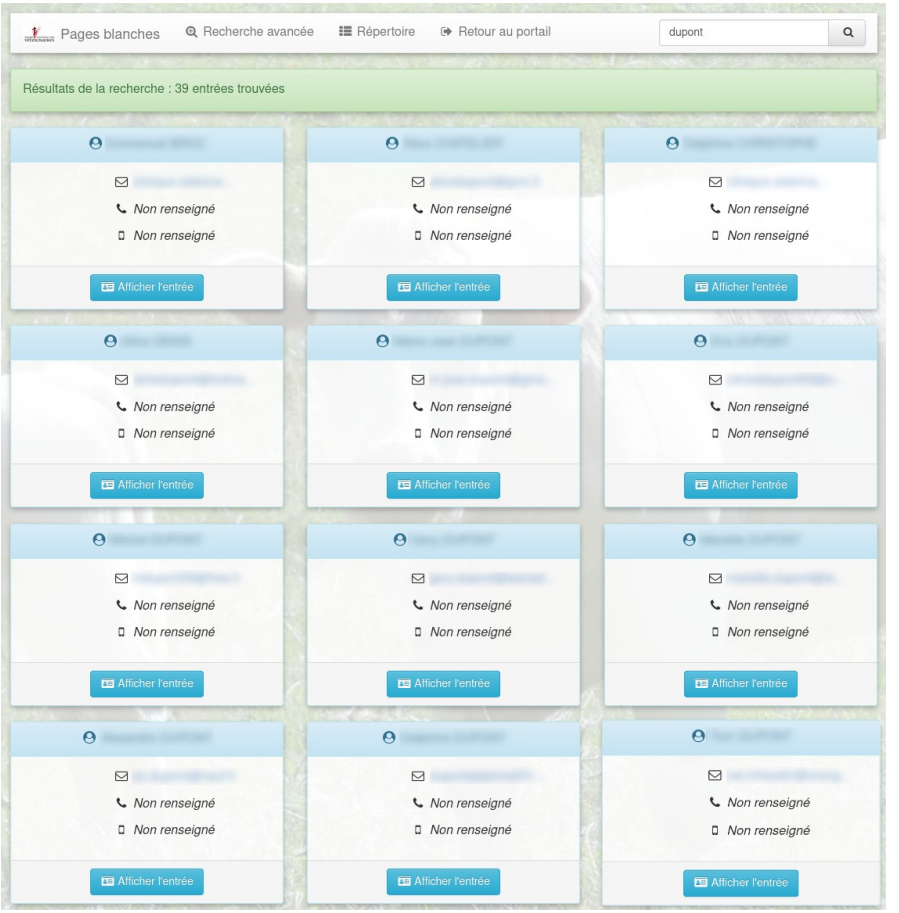


Présentation de l'initiative LDAP Toolbox

Services proposés par LDAP-toolbox

une interface web de gestion pour les utilisateurs : White Pages

- les informations principales sont affichées :
  - adresse mail
  - identité
  - téléphone
  - photo
- récupération possible d'une identité au format vCard

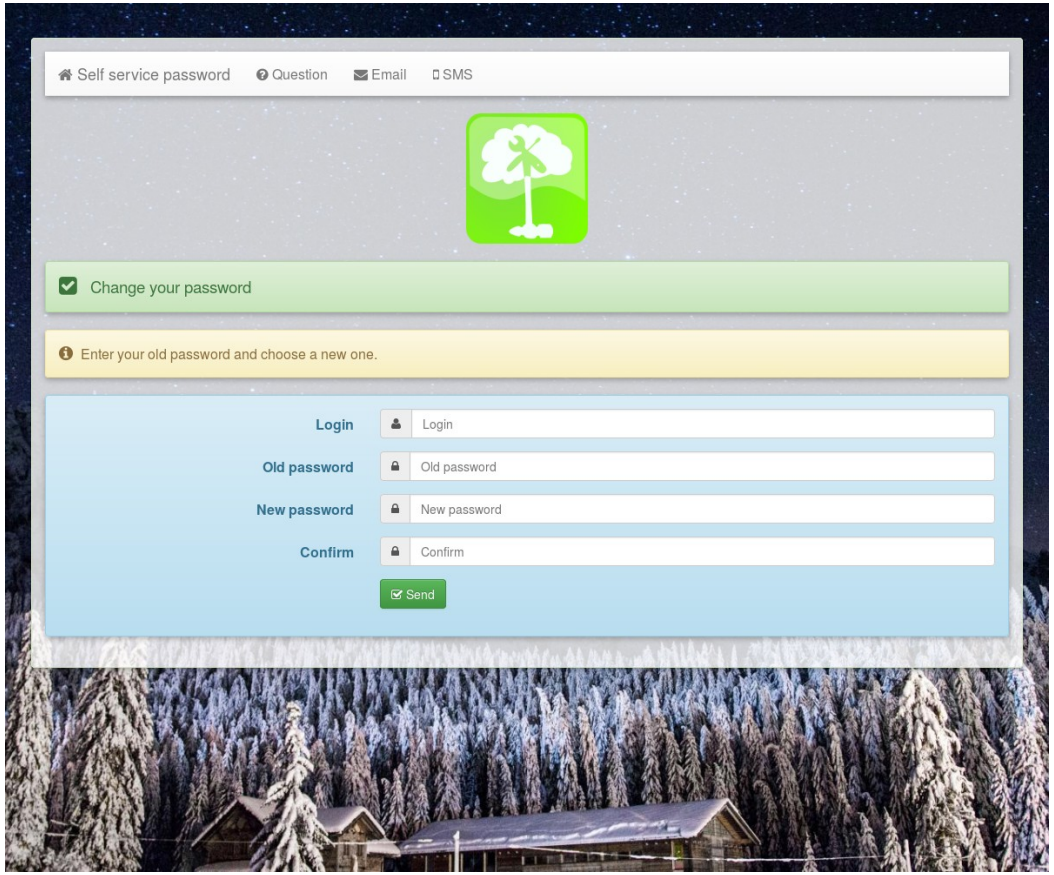


Présentation de l'initiative LDAP Toolbox

Services proposés par LDAP-toolbox

une interface web de self-service-password

- réinitialisation du mot de passe en autonomie par l'utilisateur :
  - par connaissance du mot de passe actuel
  - par une vérification du mail
  - par une vérification par SMS
  - par une vérification par question / réponses
  - support des politiques de mots de passe

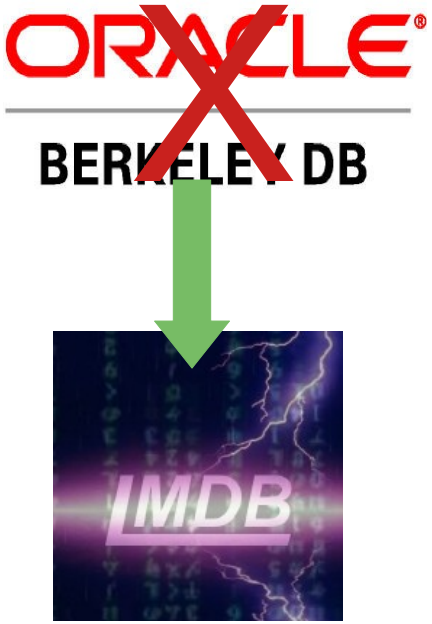


Les nouveautés d'OpenLDAP 2.5

Les nouveautés d'OpenLDAP 2.5

Changements généraux

- pour surtout des raisons de compatibilité de licence, mais aussi de performances :
  - abandon définitif de BerkeleyDB (backend bdb et hdb)
  - remplacé par lmdb
    - base de données clé-valeur
    - arbre B+
    - mappée en mémoire
    - copie sur écriture



- backends shell, perl et SQL dépréciés
- les options « **-h** hostname » et « **-p** port » des clients sont maintenant dépréciées au profit de **-H** qui combine les deux

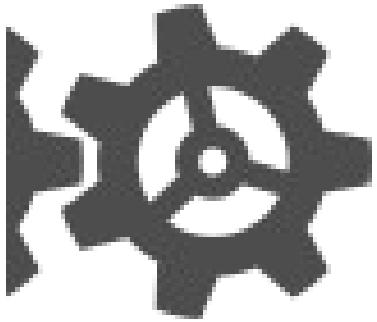
nouvelles dépendances :

- OpenSSL ≥ 1.1.1
- Cyrus SASL ≥ 2.1.27
- libevent (pour lload)

Les nouveautés d'OpenLDAP 2.5

Changements de configuration

- configuration « **cn=config** » devient recommandée
- configuration « **slapd.conf** » toujours valable en 2.5 et dans la future 2.6

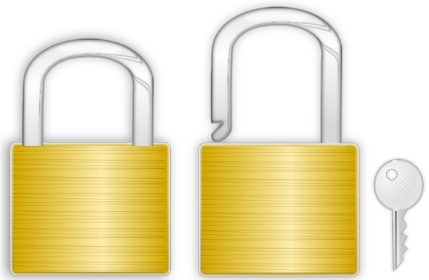


- OpenLDAP 2.5 **rétro-compatible** avec une configuration 2.4
  - certains attributs de configuration ont évolué
  - anciens noms reconnus par rétro-compatibilité
  - migration conseillée, par exemple :

olcMirrorMode: TRUE → olcMultiProvider: TRUE

Les nouveautés d'OpenLDAP 2.5

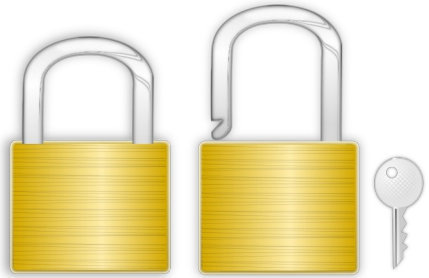
Changements de la politique de mots de passe



- implémentation du nouveau draft 10 de la ppolicy
  https://datatracker.ietf.org/doc/html/draft-behera-ldap-password-policy-10
  - protection contre les attaques par brute-force → pwdMinDelay, pwdMaxDelay
  - verrouillage après inactivité → pwdLastSuccess, pwdMaxIdle
  - longueur maximale du mot de passe → pwdMaxLength
  - dates de validité du compte → pwdStartTime, pwdEndTime
  - extension des fonctionnalités de la politique avec une librairie externe → pwdCheckModule, pwdCheckModuleArg
  - gestion des politiques de mots de passe
    - par étendue dans le DIT
    - par groupe
  - ticket ITS#9343 programmé pour la 2.7.0

Les nouveautés d'OpenLDAP 2.5

Changements de la politique de mots de passe



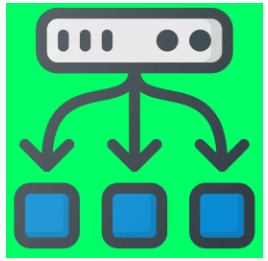
- schéma ppolicy maintenant inclus dans l'overlay
- attributs marqués « NO-USER-MODIFICATION » ne peuvent plus être écrits sans le control RELAX :

pwdChangedTime
pwdAccountLockedTime → revert en 2.5.8 et 2.6
pwdFailureTime
pwdHistory
pwdGraceUseTime
pwdPolicySubentry → revert en 2.5.8 et 2.6
pwdStartTime / pwdEndTime → revert en 2.5.8 et 2.6
pwdLastSuccess
pwdAccountTmpLockoutEnd

Les nouveautés d'OpenLDAP 2.5

Nouveaux backends

lload : load-balancer



- répartiteur de charge (roundrobin, poids, latence), qui comprend le LDAP
- peut répartir la charge selon le contenu des requêtes LDAP

- mode standalone ou module de slapd (recommandé)

- manquent :
  - plus de méthodes de répartition de charge
  - sticky-sessions (prévues en 2.6)

wt : wiredTiger (expérimental)

- base NoSQL (utilisée par MongoDB)

Les nouveautés d'OpenLDAP 2.5

Changements sur les overlays

dynlist
- constitution de groupes dynamiques
- remplace memberOf, qui devient déprécié

lastbind
- intégré en grande partie dans ppolicy

argon2, pw-pbkdf2, pw-sha2
- argon2, pbkdf2 : recommandé
- sha2 : non recommandé
- argon2 intégré directement dans le core

ppm
- extension de la politique de mots de passe

totp
- support du « Time-base One Time Password »

variant
- partage d'attributs entre plusieurs entrées

vc
- bind sans impact sur la session LDAP en cours

Les nouveautés d'OpenLDAP 2.5

Nouveautés des paquets OpenLDAP-LTB

- paquets fournis à partir de la version 2.5.7 : Debian 10 et 11, CentOS 7 et 8
- nouvelle version de slapd-cli
  - affichage de la version de slapd dans la commande status
  - correction de checksync lors de multiples suffixes
  - renommage du service slapd en slapd-ltb
  - modèles de configurations pour slapd (en fichier plat et cn=config) et lload (fichier plat)
  - modèles d'échantillons de données à importer
  - suppression de bdb, hdb, slurpd, init.d, correction de 2 tickets de sécurité

Les nouveautés d'OpenLDAP 2.5

Nouveautés des paquets OpenLDAP-LTB

- compilation de tous les backends et overlays comme modules
  - permet de les activer / désactiver selon le besoin
  - maintenant obligatoire de charger au moins quelques modules de base : lmdb, argon2
- installation d'une configuration « cn=config » par défaut en cas de nouvelle installation
- fourniture d'un paquet **openldap-ltb-contrib-overlays** contenant :

• autogroup • lastbind • noopsrch • nssov • pw-pbkdf2	• pw-sha2 • smbk5pwd • ppm • variant • vc

Conclusion

Conclusion

OpenLDAP a encore de beaux jours devant lui !

- communauté très active
  - nouveau cycle de releases, sorties plus rapides
- produit robuste (backend de stockage, réplication)
- nombreuses fonctionnalités
- très bonnes performances face à la concurrence
- effort sur la documentation à faire…
- nouveau load-balancer prometteur

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com