IDENTITY DAYS

27 octobre 2022 - PARIS

@IdentityDays #identitydays2022

Merci à tous nos partenaires !

Microsoft

Vorteks
make IT work, make IT free

BeyondTrust

ermetic

Exakis Nelite
MagellanPartners

FUSION DIRECTORY

jumpcloud

KERBEROS CONSULTING

Kleverware

METSYS

okta

ONE IDENTITY by Quest

ManageEngine

SailPoint

semperis

SILVERFORT

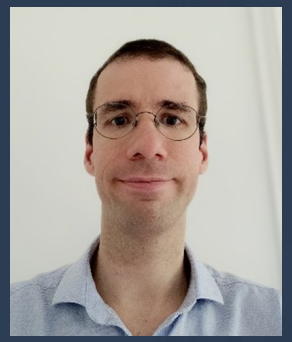
Systancia

La politique de mots de passe : de la théorie à la pratique avec OpenLDAP

David Coutadeur
Vorteks
make IT work, make IT free

David Coutadeur

Architecte en gestion d'identité



~ 10 ans d'ancienneté
Expert en gestion d'identité
Passionné d'open-source

david.coutadeur@worteks.com
@dcoutadeur

Ordre du jour

1. Présentation
2. LDAP et OpenLDAP
3. Introduction aux politiques de MdP
4. Etat des lieux des politiques de MdP
5. L'overlay password policy
6. Présentation de ppm
7. Fonctionnalités de ppm
8. Conclusion

Présentation

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

LDAP et OpenLDAP

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 :

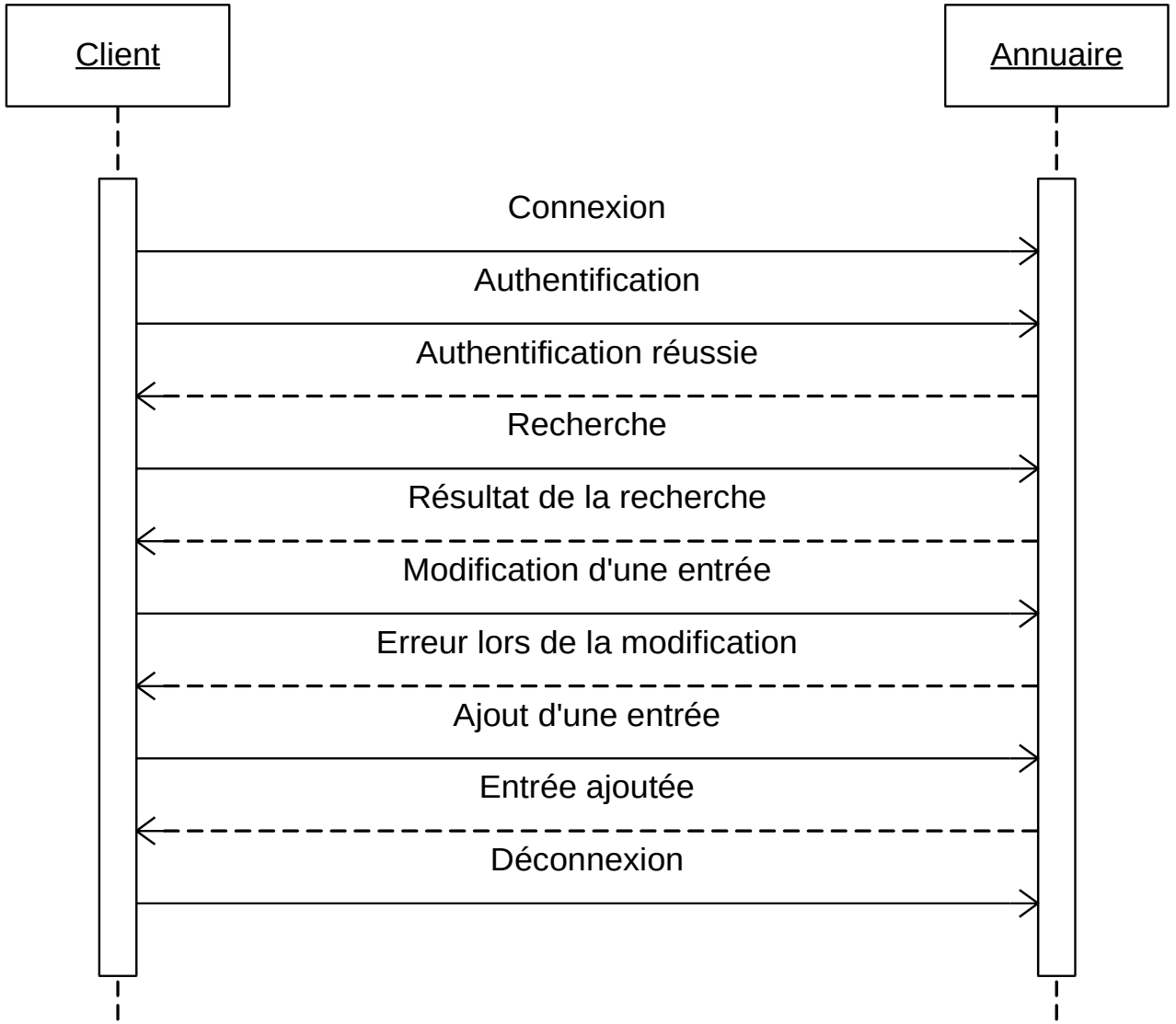
- la communication client serveur
  - au dessus de TCP / IP
  - l'encodage (LBER)

- 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)



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 LTS actuelle : OpenLDAP 2.5.13
- version « feature release » : OpenLDAP 2.6.3
- 3 développeurs principaux :
  - Howard Chu
  - Ondřej Kuzník
  - Quanah Gibson-Mount

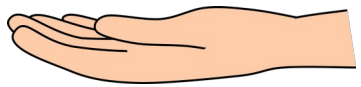
Présentation d'OpenLDAP

Caractéristiques

- OpenLDAP Public License, dérivée de la GNU GPL

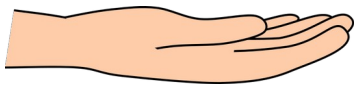
contient

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



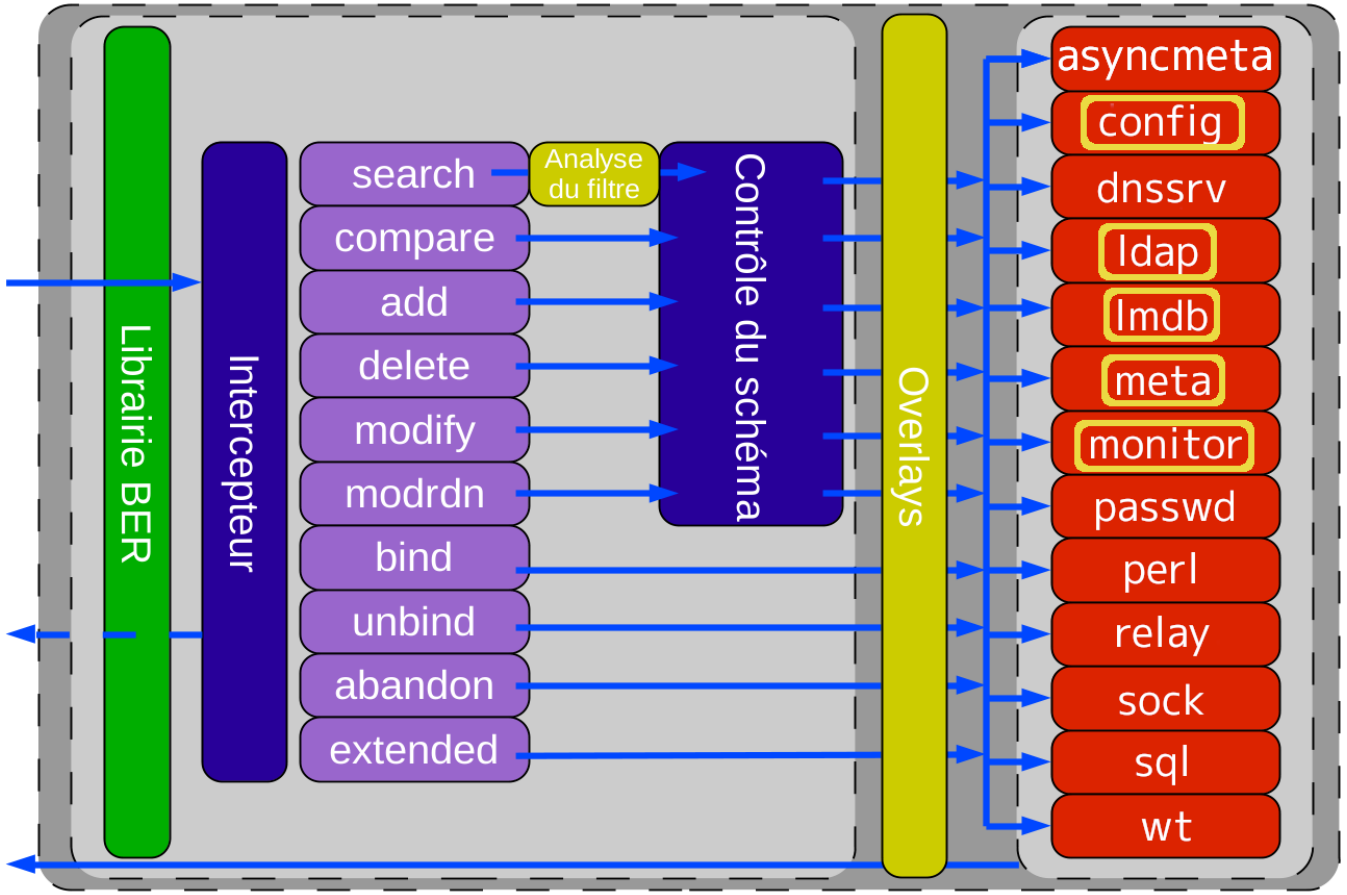
supporte

- 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

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

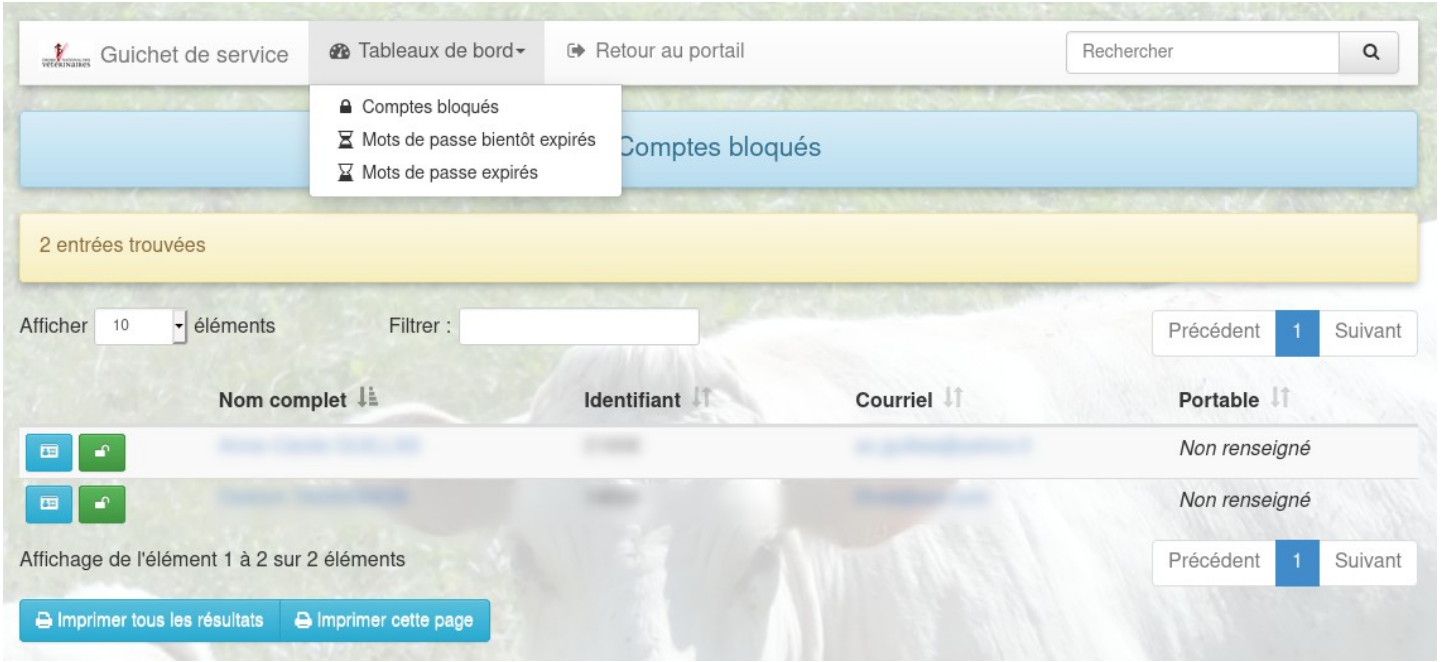
Services proposés par LDAP-toolbox

- **une base documentaire**
  - https://ltb-project-documentation.readthedocs.io
  - installation, configuration des paquets openldap-ltb
  - 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

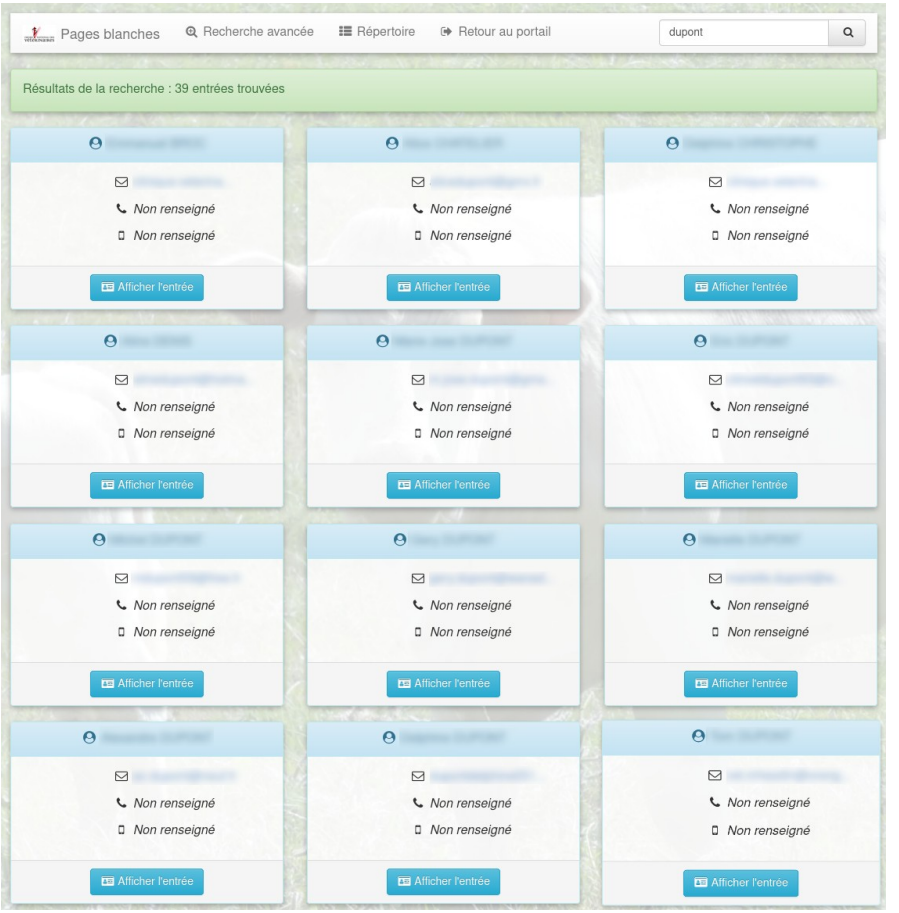
- **une interface web de gestion dédiée aux administrateurs : Service Desk**
  - tableaux de bord pour visualiser les comptes et leur statut (bloqués, expirés)
  - test d'un mot de passe
  - réinitialisation d'un mot de passe
  - blocage, déblocage d'un compte



Présentation de l'initiative LDAP Toolbox

Services proposés par LDAP-toolbox

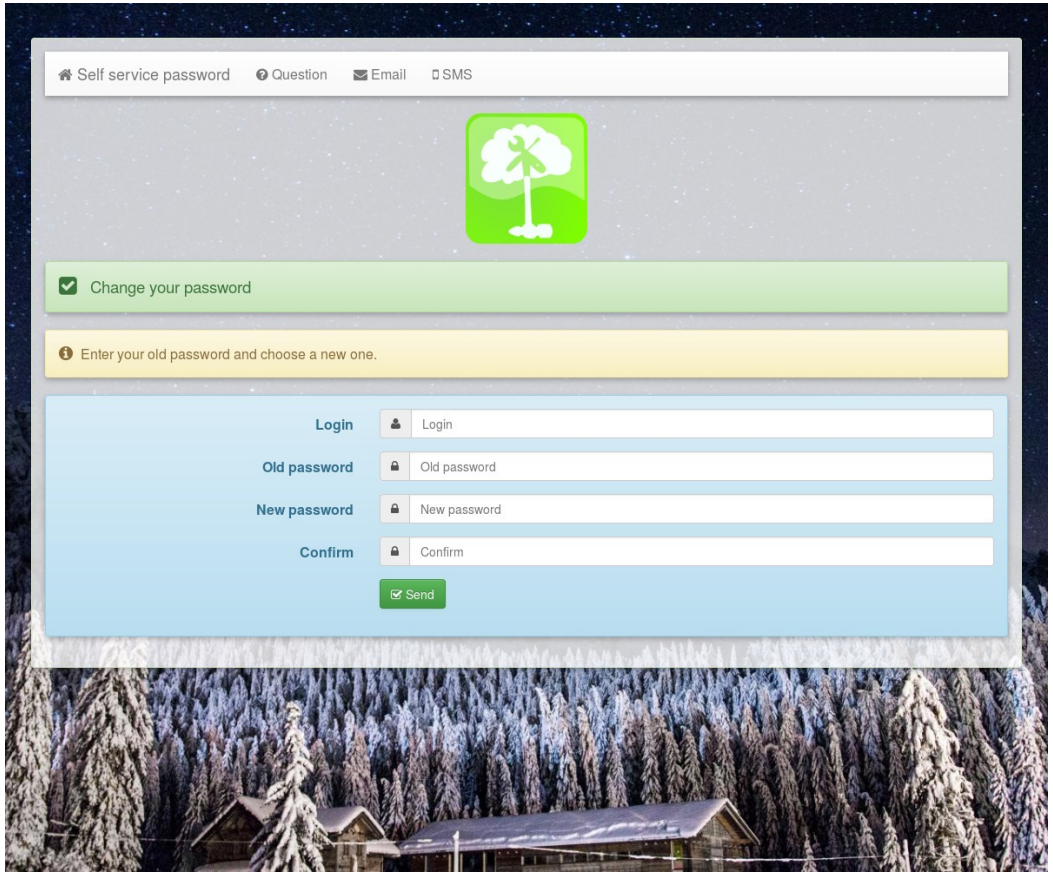
- **une interface web de gestion pour les utilisateurs : White Pages**
  - les informations principales sont affichées :
    - adresse mail
    - identité
    - téléphone
    - photo
  - récupération possible d'une identité au format vCard



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



Introduction aux politiques de MdP

Introduction aux politiques de MdP

« ensemble de règles visant à améliorer la sécurité, en encourageant les utilisateurs à recourir à des mots de passe relativement **robustes** et en les utilisant **correctement** »

Introduction aux politiques de MdP

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

- **Pas de norme universelle**
  - recommandations du NIST
  - recommandations de l'ANSSI
  - recommandations de la CNIL du 07/22 (tableau de correspondance / ANSSI)

- **Normes changeantes avec le temps**
  - Guide NIST de 2004 : utilisation de majuscules, minuscules, chiffres, avec obligation de changer périodiquement
  - Guide NIST de 2007 : 8 → 64 caractères, pas d'obligation d'imposer plusieurs classes de caractères, pas d'obligation de changement périodique

Introduction aux politiques de MdP

- **Recommandations ANSSI :**
- ***« Recommandations relatives à l'authentification multifacteur et aux mots de passe - v2.0 du 08/10/2021 »***

  - longueur ≥ 9 : faible, longueur ≥ 12 : moyen, longueur ≥ 15 : fort
  - pas de longueur maximale
  - plusieurs classes de caractères (à définir suivant le contexte)
  - pas de délai d'expiration pour les comptes non sensibles
  - délai d'expiration pour les comptes sensibles

Introduction aux politiques de MdP

- contrôle de la robustesse : règles de la politique, comparaison à une base de mots de passe fréquemment utilisée, interdiction de la réutilisation d'un ancien mot de passe, repérage des motifs basés sur les noms, prénoms,…
- stockage avec sel, hash Argon2 ou PBKDF2 recommandé
- privilégier l'authentification multi-facteurs : clé FIDO2 par exemple

Voir aussi la conférence :

- « Authentification multi-facteurs et gestion du risque avec du logiciel 100 % libre »

Treat your passwords like your underwear

1. Don't share them with anyone

2. Change them regularly

3. Don't leave them on your desk

Etat des lieux des politiques de MdP

Etat des lieux des politiques de MdP

- **pas de spécification universelle**
  - AD, OpenDJ,... : implémentations spécifiques

- **IETF internet draft : "Password Policy for LDAP Directories"**
  - *draft-behera-ldap-password-policy* (version 00 : octobre 1999, version 11 : février 2022), implémenté dans plusieurs serveurs d'annuaire :
    - OpenLDAP password policy overlay
    - SUN Directory Server
    - Tivoli Directory Server
    - Fedora Directory Server
    - Red-Hat Directory Server

Etat des lieux des politiques de MdP

- version 11, février 2022, expire le 26 août 2022

- définit :
  - les spécifications fonctionnelles de la politique de mots de passe
  - le schéma LDAP et les attributs opérationnels pour supporter les politiques
  - le contrôle étendu « ppolicy » pour les requêtes et les réponses
  - la façon dont le serveur devrait / doit inclure la politique dans les opérations LDAP (bind, modify,…)
  - la façon dont les clients devraient / doivent inclure la politique dans les opérations LDAP (bind, modify,…)

Etat des lieux des politiques de MdP

- des considérations générales pour gérer les politiques (le scope défini par l'attribut SubtreeSpecification, la surcharge de politique)
- des considérations sur la réplication et la sécurité

- ne définit pas : (spécifique à chaque implémentation)
  - l'application des critères de politiques de mots de passe
  - une façon automatique de forcer la réinitialisation de mot de passe après qu'une modification ait été faite par un administrateur

L’overlay Password Policy

L’overlay password policy

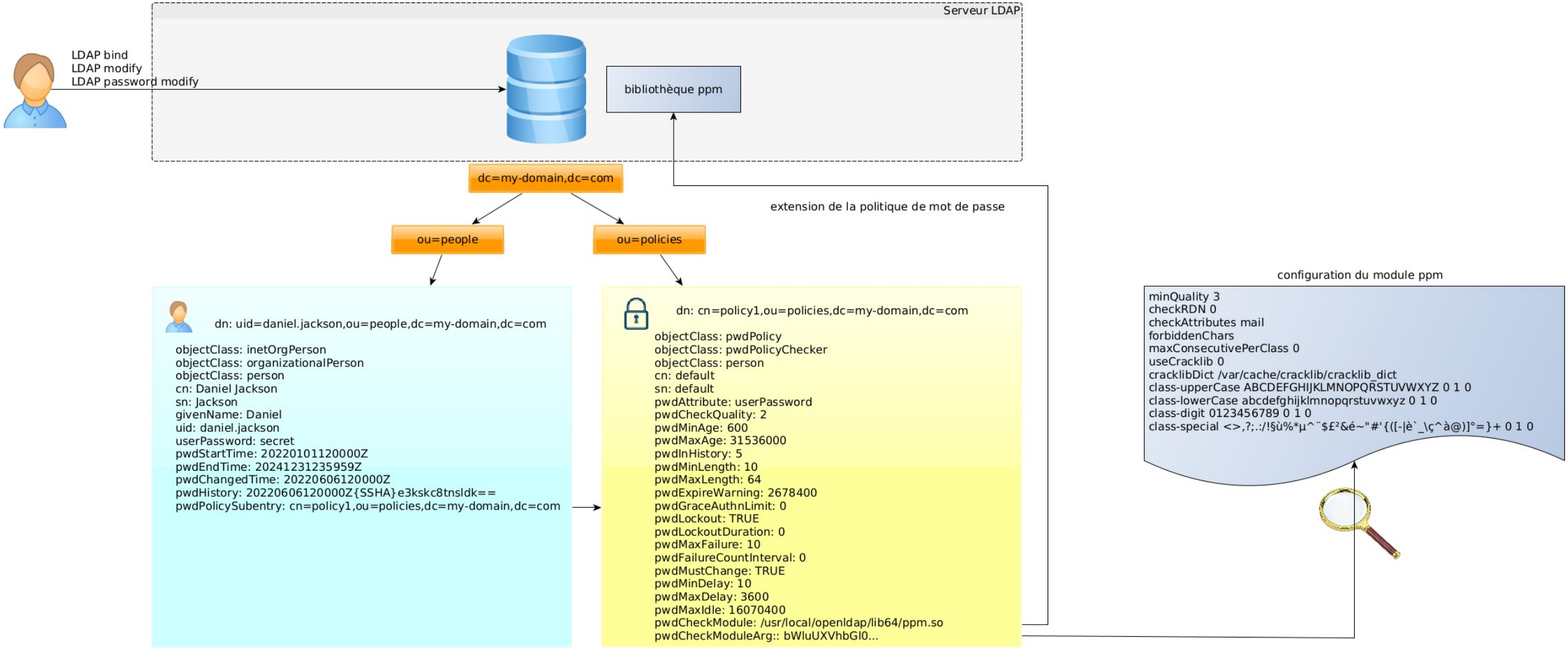
- OpenLDAP implémente le brouillon IETF :
  - ✅le schéma LDAP et les attributs opérationnels
  - ✅le contrôle étendu ppolicy pour les requêtes et réponses
  - ✅l’implémentation serveur
  - ✅l’implémentation cliente (ldapsearch, ldapmodify,...)

L'overlay password policy

- Récemment implémenté (OpenLDAP ≥ 2.5) :
  - ✅ support de la protection contre les attaques par brute-force, basée sur les attributs pwdMinDelay et pwdMaxDelay
  - ✅ support du verrouillage basé sur les attributs pwdLastSuccess et pwdMaxIdle
  - ✅ support de la taille maximale (attribut pwdMaxLength)
  - ✅ support des dates de validité (attributs pwdStartTime et pwdEndTime)

- Pas encore implémenté
  - ☒ Politique de mots de passe gérée par « étendue » dans le DIT ou par groupe

L'overlay password policy



L'overlay password policy

- L'attribut *pwdCheckModule* stockant l'emplacement de la bibliothèque complémentaire évolue en version 2.6 d'OpenLDAP : il est maintenant défini dans la configuration et non plus dans la politique
  - empêche d'avoir plusieurs modules étendus de politiques
  - permet de meilleures performances car le module est chargé au démarrage

- L'attribut *pwdCheckModuleArg* permettant de transmettre les paramètres de la politique étendue est apparu avec la version 2.5 d'OpenLDAP
  - avant la version 2.5, ppm devait récupérer sa configuration en fichier plat

Présentation de ppm

Présentation de ppm

Architecture de ppm

- implémente les règles de robustesse intéressantes et populaires qui manquent à *slapo-ppolicy* → OK
- extensible → jusqu'à un certain point (plugin de 800 lignes en C)
- efficace → non critique (car appelé seulement en cas de changement de MdP)
- sécurisé → TODO (audit de code)

Présentation de ppm

ppm en bref

- code en C, bibliothèque dynamique (.so), ~ 800 lignes
- implémente des règles complémentaires de robustesse de mot de passe
- configuration dans l'attribut *pwdCheckModuleArg*, transmis par l'overlay ppolicy
- Code :
  - dépôt officiel : https://github.com/ltb-project/ppm
  - disponible dans les sources d'OpenLDAP (répertoire contrib/slapd-modules/ppm)
  - contient les sources pour compiler la librairie, l'exécutable de test vérifiant la force des mots de passe, la documentation

Présentation de ppm

ppm en bref

- packaging :
  - disponible dans les paquets openldap-ltb pour Debian, Red-Hat :
    - dans openldap-ltb pour les versions ≥ 2.5.13 et 2.6.3
    - dans openldap-ltb-contrib-overlays pour les versions inférieures
- Dernière version : v2.2, 17 mai 2022
- Licence : *OpenLDAP Public License*

Fonctionnalités de ppm

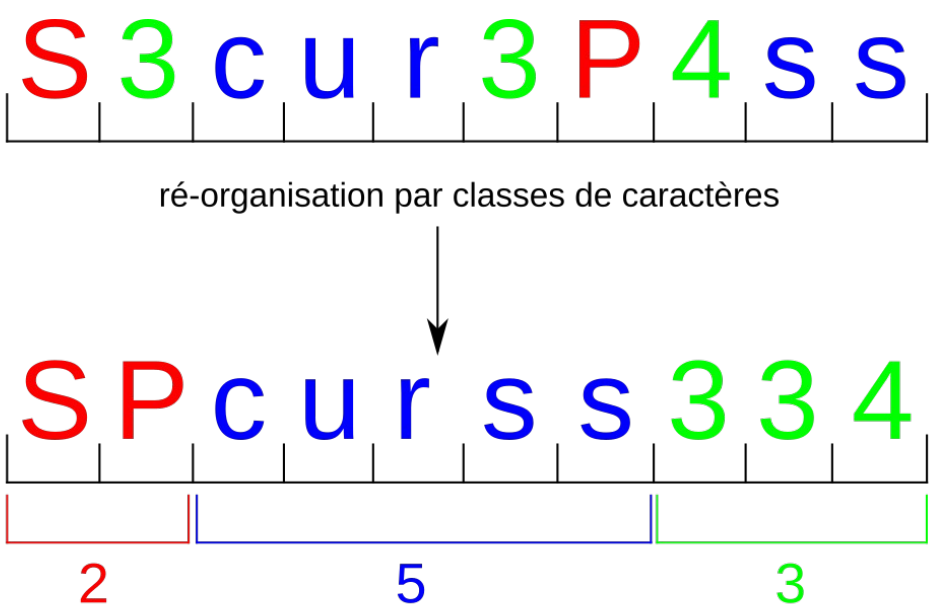
Fonctionnalités de ppm

Paramètres des classes de caractères

- définition des classes de caractères
- minQuality
- min (pour chaque classe)
- min_for_point (pour chaque classe)
- NEW max (pour chaque classe)

Exemple de politique :

```
minQuality 3
class-upperCase ABCDEFGHIJKLMNOPQRSTUVWXYZ 0 1 0
class-lowerCase abcdefghijklmnopqrstuvwxyz 0 1 0
Class-digit 0123456789 0 1 0
class-special <>,?;.:/!§ù%*µ^¨$£²&é~"#' 0 1 0
```



$qualité_{majuscules}$ = 1 si 2 >= $min\_for\_point_{majuscules}$, sinon 0
$qualité_{minuscules}$ = 1 si 5 >= $min\_for\_point_{minuscules}$, sinon 0
$qualité_{chiffres}$ = 1 si 3 >= $min\_for\_point_{chiffres}$, sinon 0

Critères :

$min_{majuscules} <= 2 <= max_{majuscules}$
$min_{minuscules} <= 5 <= max_{minuscules}$
$min_{chiffres} <= 3 <= max_{chiffres}$
$qualité_{majuscules} + qualité_{minuscules} + qualité_{chiffres} >= minQuality$

Fonctionnalités de ppm

Autres paramètres de robustesse

- checkRDN
- checkAttributes
- forbiddenChars
- maxConsecutivePerClass
- useCracklib
- cracklibDict

Exemple de politique :

```
checkRDN 1
checkAttributes mail
forbiddenChars ££
maxConsecutivePerClass 8
useCracklib 1
cracklibDict /var/cache/cracklib/cracklib_dict
```

Critère checkRDN :

dn: uid=daniel.jackson,ou=people,dc=my-domain,dc=com
- nouveau mot de passe : secret → OK
- nouveau mot de passe : daniel → KO

Conclusion

Conclusion

Avec l'overlay ppolicy + ppm, on peut implémenter toutes les recommandations actuelles

Axes d'amélioration

- Rejeter les modifications de mots de passe suivant le contexte :
  - ☑ attributs dans l'entrée LDAP
  - 

attributs liés à l'entrée LDAP (groupe,…)
  - 

environnement : @IP du client, date de requête,...
- Appliquer la politique à des groupes d'utilisateurs
  - 

fonctionnalité mentionnée dans les tickets de la 2.7

IDENTITY DAYS

27 octobre 2022 - PARIS

@IdentityDays #identitydays2022

Merci à tous nos partenaires !

Microsoft

Vorteks
make IT work, make IT free

BeyondTrust

ermetic

Exakis Nelite
MagellanPartners

FUSION DIRECTORY

jumpcloud

KERBEROS CONSULTING

Kleverware

METSYS

okta

ONE IDENTITY by Quest

ManageEngine

SailPoint

semperis

SILVERFORT

Systancia