IDENTITY DAYS

29 octobre 2020

Politique des mots de passe des annuaires LDAP et outils de gestion

Clément OUDOT

worteks
make IT work, make IT free

AGENDA DE LA CONFÉRENCE

Clément OUDOT
Identity Solutions Manager

PRO :
- Worteks
- LemonLDAP::NG
- LDAP Tool Box
- LDAP Synchronization Connector
- FusionIAM
- W'Sweet

PERSO :
- KPTN
- DonJon Legacy
- Improcité

« Mot de passe protégé »
- Le standard LDAP "password policy"
- Implémentation dans OpenLDAP
- Les outils du projet LDAP Tool Box
  - Self Service Password
  - Service Desk

Mot de passe protégé

Sur l’air de Femme Libérée de Cookie Dingler

Souvent chiffré, mais parfois en clair
Un mot de passe mal géré ça peut coûter cher
Les attaquants ne font pas semblant
Quand ils s’en prennent à ton compte, c’est pas très marrant

Ne le laisse pas traîner
Il est si fragile
Un mot de passe à protéger tu sais c'est pas si facile
Ne le laisse pas traîner
Il est si fragile
Un mot de passe à protéger tu sais c'est pas si facile

Ta date naissance, le nom de ton chat
C’est pas comme si tu n’avais pas d’autre choix
Essaye un peu de faire un effort
Respecte les critères pour choisir un mot de passe fort

Ne le laisse pas traîner
Il est si fragile
Un mot de passe à protéger tu sais c'est pas si facile
Ne le laisse pas traîner
Il est si fragile
Un mot de passe à protéger tu sais c'est pas si facile

Des majuscules, des chiffres mais aussi
Des caractères spéciaux de la table ASCII
Un mot de passe complexe, c’est pas compliqué
Mais il faut bien l’apprendre pour ne pas l’oublier

Ne le laisse pas traîner
Il est si fragile
Un mot de passe à protéger tu sais c'est pas si facile
Ne le laisse pas traîner
Il est si fragile
Un mot de passe à protéger tu sais c'est pas si facile

IDENTITY DAYS

29 octobre 2020

Le standard LDAP “password policy”

Un standard encore en brouillon (draft)

La politique des mots de passe est spécifiée à l'IETF, mais sous forme de brouillon

→ https://tools.ietf.org/html/draft-behera-ldap-password-policy

Première version publiée en 1999

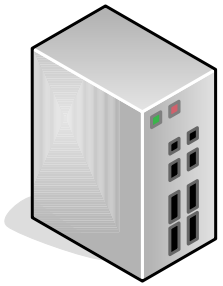
La dernière version (10), publiée en 2009, est maintenant expirée

Contenu du standard

Le standard porte sur :

- Le contrôle dans les requêtes et réponses LDAP
- Le schéma pour la configuration
- Les attributs opérationnels pour le statut de la politique pour chaque compte
- Le traitement des requêtes d'authentification et de changement de mot de passe

Dialogue Client / Serveur



Requête LDAP
+ Contrôle 1.3.6.1.4.1.42.2.27.8.5.1

Réponse LDAP
+ Contrôle

```
PasswordPolicyResponseValue ::= SEQUENCE {
        warning [0] CHOICE {
           timeBeforeExpiration [0] INTEGER (0 .. maxInt),
           graceAuthNsRemaining [1] INTEGER (0 .. maxInt) } OPTIONAL,
        error   [1] ENUMERATED {
           passwordExpired             (0),
           accountLocked               (1),
           changeAfterReset            (2),
           passwordModNotAllowed       (3),
           mustSupplyOldPassword       (4),
           insufficientPasswordQuality (5),
           passwordTooShort            (6),
           passwordTooYoung            (7),
           passwordInHistory           (8) } OPTIONAL }
```

Vérifications faites à l'authentification

- **Expiration** : refuser l'authentification si le mot de passe est expiré, ou gérer les grâces d'authentification
- **Verrouillage** : gérer le compteur d'authentification ratées, refuser l'authentification si le mot de passe est bloqué
- **Forcer le changement** : autoriser l'authentification mais forcer le changement de mot de passe
- **Alertes** : informer sur le temps avant expiration ou sur les grâces d'authentification restantes

Vérification faites à la modification du mot de passe

- Longueur minimale
- Âge minimal
- Présence dans l'historique
- Complexité

→ Le standard n'impose rien concernant la complexité

Implémentation dans OpenLDAP

Le logiciel OpenLDAP

- Serveur conforme au standard LDAPv3
- Licence compatible BSD (Logiciel Libre)
- Paquets Debian/Ubuntu/CentOS/RHEL disponibles dans le projet LDAP Tool Box

Overlay ppolicy

- OpenLDAP 2.4 : Behera draft v9
- OpenLDAP 2.5 : Behera draft v10 

- Principaux changements entre v9 et v10 :
  - Taille maximale du mot de passe
  - Délais d'authentification
  - Calcul du temps de non utilisation
  - Période de validité

Configuration de l'overlay

```
dn: olcOverlay=ppolicy,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcPPolicyConfig
olcOverlay: ppolicy
olcPPolicyHashCleartext: TRUE
olcPPolicyUseLockout: TRUE
olcPPolicyForwardUpdates: FALSE
```

Configuration des politiques

- Chaque politique est représentée par une entrée LDAP utilisant la classe d'objet **pwdPolicy**
- On peut ajouter la classe d'objet **pwdPolicyChecker** pour charge un module de vérification de la complexité
- Le projet LDAP Tool Box fournit un module nommé **ppm** :

→ https://github.com/ltb-project/ppm

Exemple d'entrée ppolicy

dn: cn=default,ou=ppolicy,dc=example,dc=com
objectClass: pwdPolicy
objectClass: pwdPolicyChecker
objectClass: device
objectClass: top
cn: default
pwdAttribute: userPassword
pwdCheckModule: ppm.so
pwdAllowUserChange: TRUE
pwdMustChange: TRUE
pwdSafeModify : FALSE
pwdCheckQuality: 2

pwdLockout: TRUE
pwdMaxFailure: 10
pwdFailureCountInterval: 30
pwdLockoutDuration: 600
pwdExpireWarning: 0
pwdMaxAge: 31536000
pwdMinAge: 600
pwdGraceAuthnLimit: 2
pwdMinLength: 8
pwdInHistory: 10

Attributs opérationnels pour le statut

- **pwdPolicySubentry** : politique active pour ce compte
- **pwdChangedTime** : date de dernier changement de mot de passe
- **pwdAccountLockedTime** : date de verrouillage. Si la valeur est "000001010000Z", cela signifie que le compte est bloqué pour une durée indéterminée
- **pwdFailureTime** : listes des dates d'authentification ratées
- **pwdHistory** : historique des mots de passe
- **pwdGraceUseTime** : liste des dates de grâce d'authentifcation
- **pwdReset** : forcer le changement à la prochaine connexion

Overlay lastbind

Overlay spécifique pour mémoriser la date de dernière authentification réussie (attribut opérationel **authTimestamp**)

dn: olcOverlay=lastbind,olcDatabase={1}mdb,cn=config
objectClass: top
objectClass: olcConfig
objectClass: olcLastBindConfig
objectClass: olcOverlayConfig
olcOverlay: lastbind
olcLastBindPrecision: 1

Ce que personne ne vous a jamais dit

Verrouillage de compte : avoir une valeur dans l'attribut **pwdAccountLockedTime** ne signifie pas que le compte est bloqué. Si la date courante est supérieure à la date de verrouillage à laquelle est ajoutée la durée de blocage, alors le compte n'est plus verrouillé. L'attribut sera supprimé à la prochaine authentification.

Réinitialisation du mot de passe : même si une réinitialisation du mot de passe est demandée, l'authentification est valide. OpenLDAP limite les opérations possibles ensuite pour n'autoriser que la modification du mot de passe. Cependant cela n'impacte pas les applications qui ne font qu'une requête d'authentification.

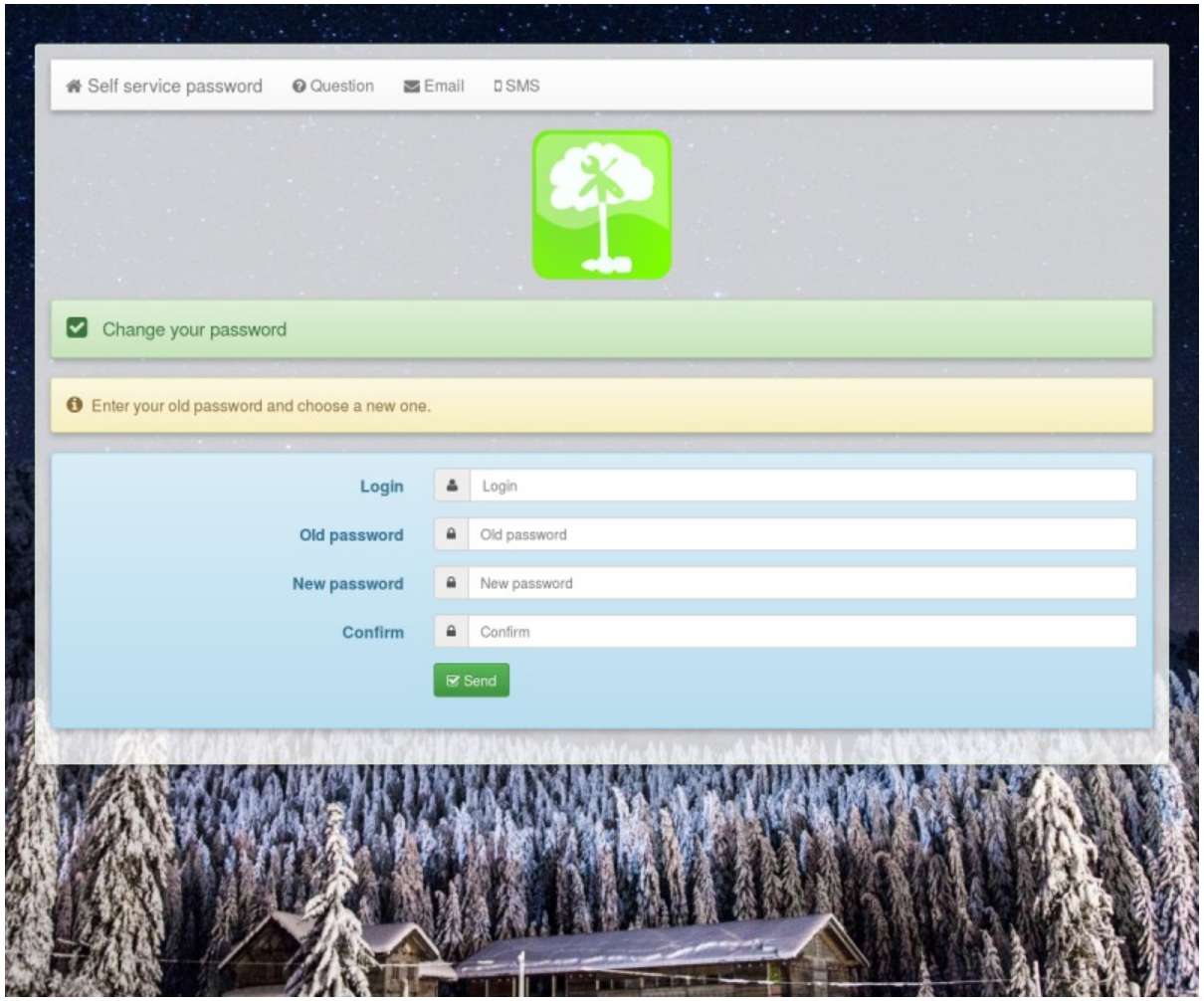
IDENTITY DAYS

29 octobre 2020

Les outils du projet LDAP Tool Box

Self Service Password

- Logiciel Libre (licence GPL)
- Destiné aux utilisateurs finaux
- Changement ou réinitialisation de mot de passe
- Utilisation d'un jeton par mail, SMS ou de questions de sécurité
- Modification de sa clé SSH
- Utilisation de la politique de l'annuaire ou d'une politique locale
- Fonctionne avec un annuaire LDAP standard et avec Active Directory



Service Desk

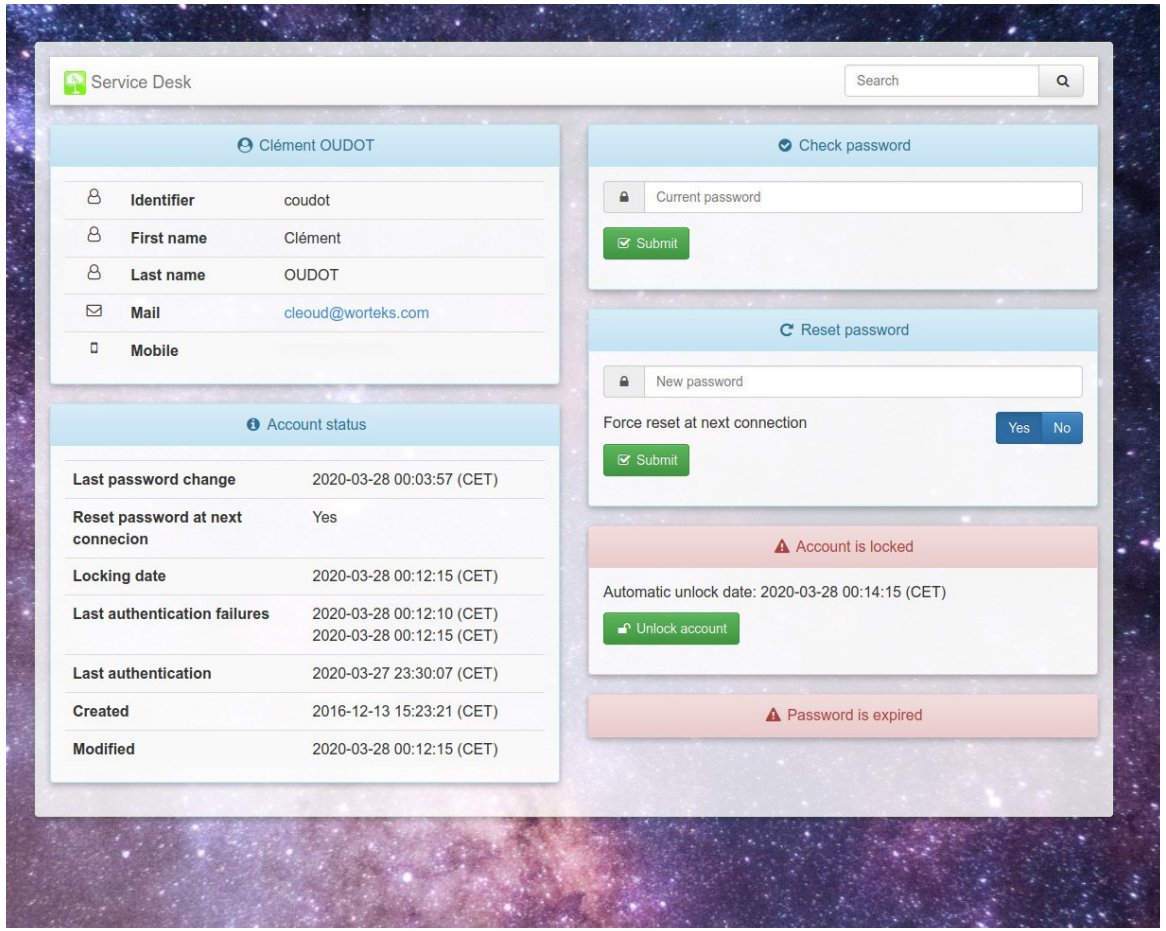
Les problèmes rencontrés par les utilisateurs avec le système d'authentification sont souvent liées à un mot de passe perdu, expiré ou bloqué

Les équipes de support ont rarement accès directement à l'annuaire LDAP et ne savent pas comment fonctionne la politique des mots de passe

Les équipes de support ont besoin d'un outil qui donne rapidement le statut d'un compte afin d'aider les utilisateurs

Service Desk

- Logiciel Libre (licence GPL)
- Destiné aux équipes de support
- Recherche d'un compte
- Affichage des attributs principaux
- Affichage du statut du compte
- Vérification du mot de passe courant
- Réinitialisation du mot de passe
- Verrouillage/déverrouillage



Pour aller plus loin

Quelques liens

OpenLDAP

→ https://www.openldap.org/

LDAP Tool Box

→ https://ltb-project.org

LDAP Tool Box Self Service Password

→ https://github.com/ltb-project/self-service-password

LDAP Tool Box Service Desk

→ https://github.com/ltb-project/service-desk

LDAP Tool Box ppm

→ https://github.com/ltb-project/ppm

IDENTITY DAYS

29 octobre 2020

Merci à tous nos partenaires

@IdentityDays #identitydays2020

Microsoft

Vorteks
make IT work, make IT free

ManageEngine

Auth0

METSYS

FUSION DIRECTORY

ALSID

SPIE

yubico

SailPoint

Systancia

Alphorm.com