worteks

make IT work, make IT free

UNDERSTAND PASSWORD POLICY IN OPENLDAP AND DISCOVER TOOLS TO MANAGE IT

Pass the SALT 2020

$ ldapwhoami

Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot

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

KPTN
DonJon Legacy
Improcité

Password Policy standard

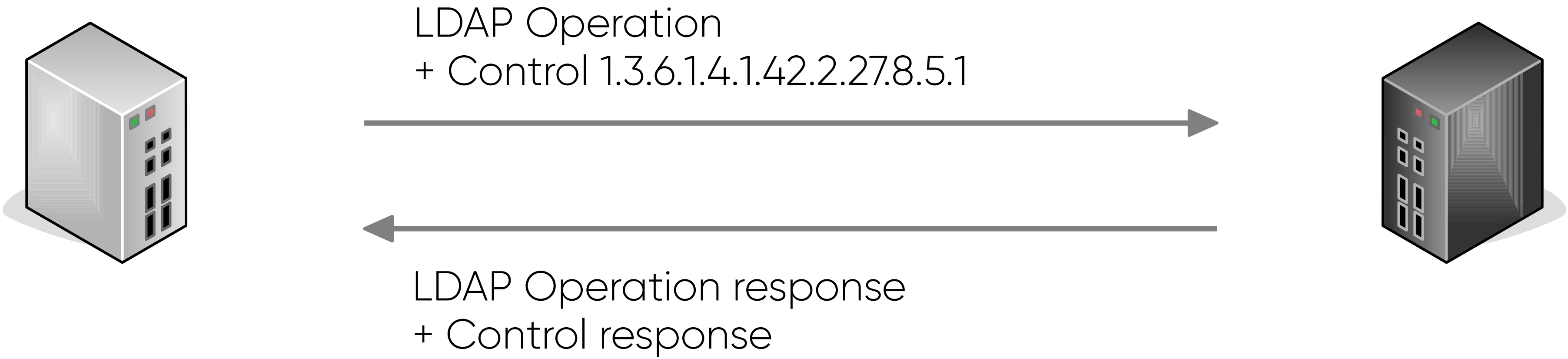
A draft with multiple versions

- Password policy for LDAP is an IETF draft: https://tools.ietf.org/html/draft-behera-ldap-password-policy
- First version published in 1999
- Last version (10) published in 2009, and now expired

Password policy content

- The specification covers:
  - LDAP control request and response
  - LDAP schema for password policy configuration
  - LDAP operationnal attributes for password policy status in user entries
  - How to process authentification and password modification requests

Client / Server



LDAP Operation
+ Control 1.3.6.1.4.1.42.2.27.8.5.1

LDAP Operation response
+ Control response

```
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 }
```

Authentication checks

- **Expiration**: do not allow authentication if password is expired, or manage authentication graces
- **Lock**: manage failures counter and do not allow authentication if password is locked
- **Force change**: allow authentication but force password change
- **Warnings**: time before expiration and graces remaining

Modification checks

- Password size
- Password minimal age
- Password history
- Password complexity (no details about complexity checks)

Password Policy in OpenLDAP

Overlay ppolicy

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

- Major changes between v9 and v10:
  - Maximum password size
  - Authentication delay
  - Idle time
  - Validity period

Overlay configuration

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

Password policy configuration

- Each password policy is represented as an LDAP entry using pwdPolicy objectClass
- Possibility to add pwdPolicyChecker objectClass to load a specific module to check password complexity
- LDAP Tool Box project ships an Open Source pwdChecker module named ppm: https://github.com/ltb-project/ppm

Password policy configuration

```
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
```

Password policy status in user entry

- Some opertionnal attributes are stored in user entry:
  - **pwdPolicySubentry**: active policy for this user
  - **pwdChangedTime**: last password change date
  - **pwdAccountLockedTime**: lock date. If the value is "000001010000Z", means account is locked permanently
  - **pwdFailureTime**: list of last failure dates
  - **pwdHistory**: history of old password
  - **pwdGraceUseTime**: list of grace dates
  - **pwdReset**: flag to request password change at next login

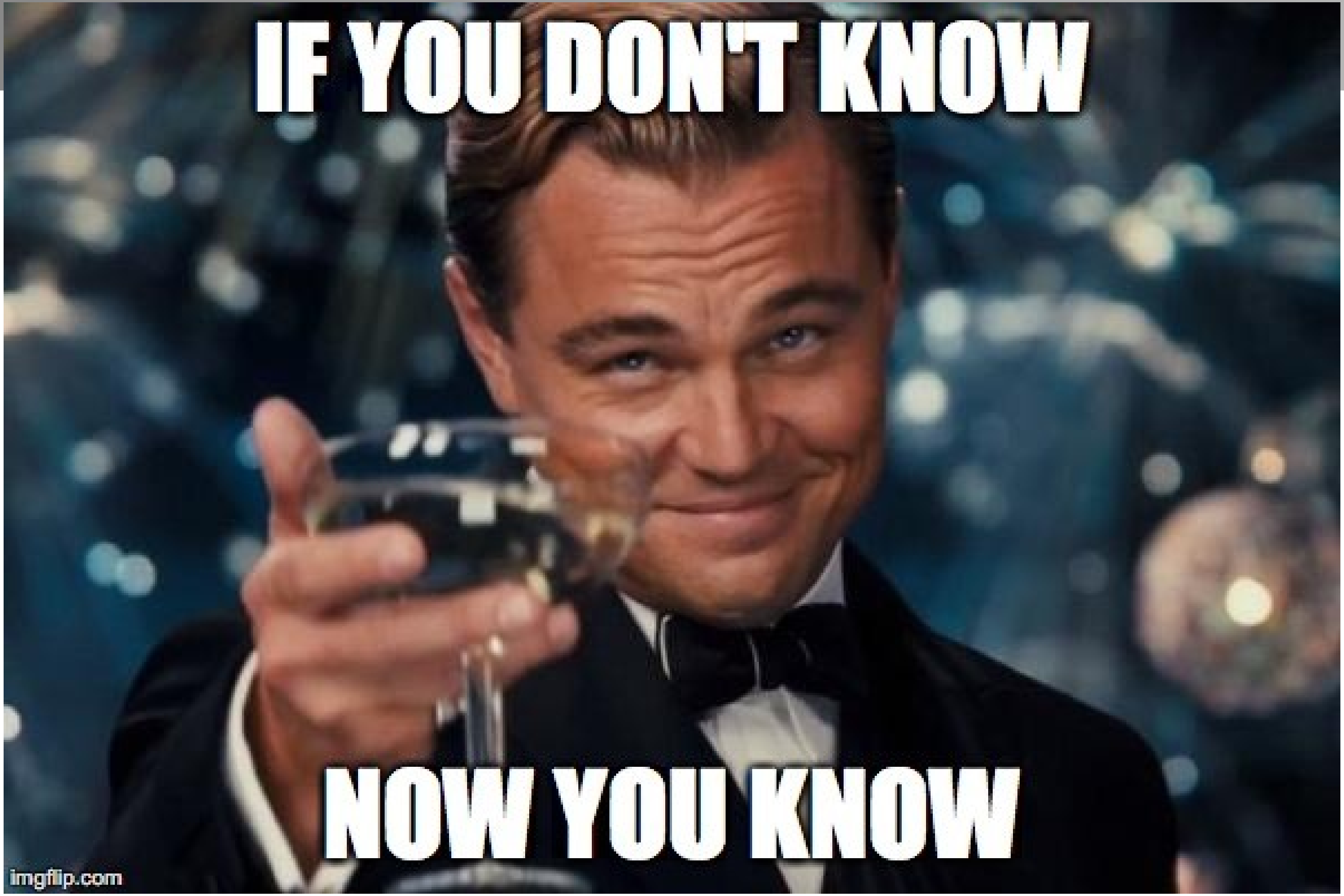
Overlay lastbind

- Specific overlay to remember last successful bind (operational attribute **authTimestamp**)
- Overlay configuration :

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

Things no one tells you

- **Account locking**: having a value in pwdAccountLockedTime of a user entry does not mean the user account is locked. Indeed, if current date is greater than lock date and lockout duration, the account is unlocked. The value will be erased at next authentication.
- **Password reset**: even if password reset is requested, authentication is allowed. OpenLDAP will just limit operations to the password modification, but this has no impact on applications just using OpenLDAP for authentication.

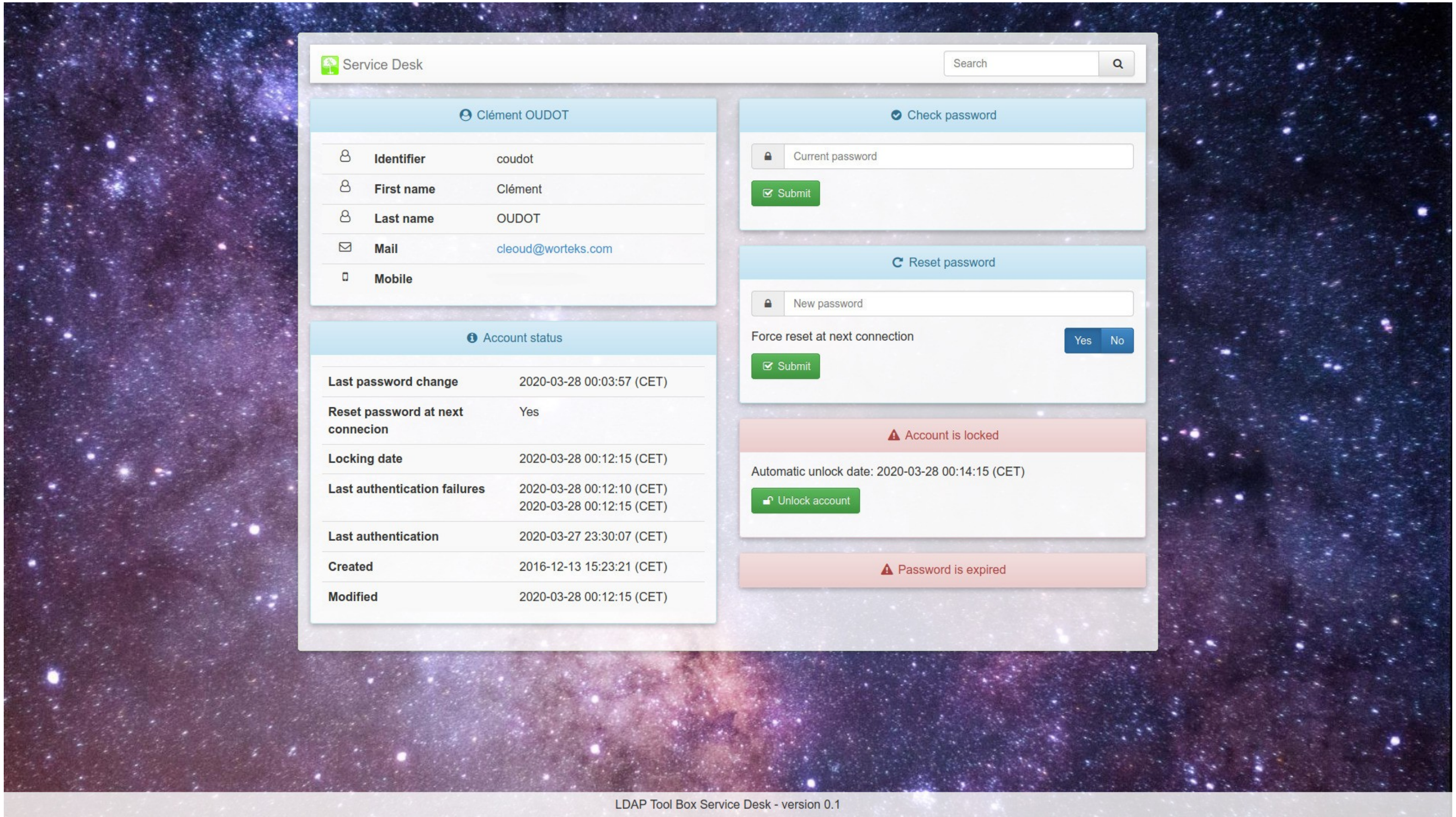

IF YOU DON'T KNOW
NOW YOU KNOW
imgflip.com

LDAP Tool Box Service Desk

Support your support

- User issues with authentication system is often linked to a lost password, expired password or locked account
- Support team does not have admin access to LDAP directory and do not know how password policy works
- Support team needs to know quickly the account status to give the correct answer to solve the user issue

LDAP Tool Box Service Desk



Service Desk

Search

Clément OUDOT

Identifier	coudot
First name	Clément
Last name	OUDOT
Mail	cleoud@worteks.com
Mobile	

Account status

Last password change	2020-03-28 00:03:57 (CET)
Reset password at next connecion	Yes
Locking date	2020-03-28 00:12:15 (CET)
Last authentication failures	2020-03-28 00:12:10 (CET) 2020-03-28 00:12:15 (CET)
Last authentication	2020-03-27 23:30:07 (CET)
Created	2016-12-13 15:23:21 (CET)
Modified	2020-03-28 00:12:15 (CET)

Check password

Current password

Submit

Reset password

New password

Force reset at next connection Yes No

Submit

Account is locked

Automatic unlock date: 2020-03-28 00:14:15 (CET)

Unlock account

Password is expired

LDAP Tool Box Service Desk - version 0.1

LDAP Tool Box Service Desk

- Main features:
  - Quick search for an account
  - View main attributes
  - View account and password status
  - Test current password
  - Reset password and force password change at next connection
  - Lock/Unlock account
  - Post hook

Want more?

Useful links

- OpenLDAP
  https://www.openldap.org/
- LDAP Tool Box
  https://ltb-project.org
- LDAP Tool Box Service Desk
  https://github.com/ltb-project/service-desk
- LDAP Tool Box ppm
  https://github.com/ltb-project/ppm

worteks

make IT work, make IT free

THANKS

✉ info@worteks.com

@worteks_com

in linkedin.com/company/worteks