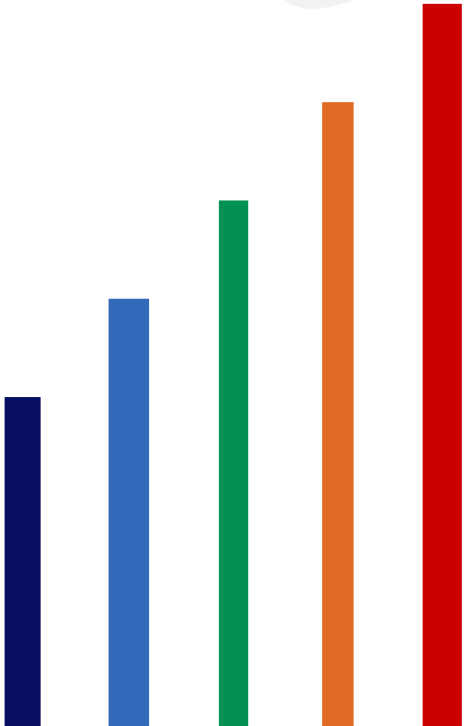
Vorteks
make IT work, make IT free

Feedback on OpenLDAP Password Policy usage in 2026 and possible evolutions

Table of contents



presentation

password policies

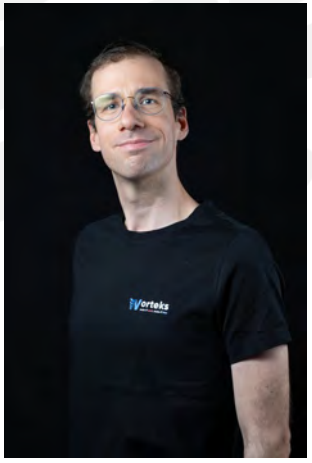
ppm

evolutions

LDAP 2026 CON TUEBINGEN

Presentation

David Coutadeur



Architect specialized in identity management

open-source enthusiast

~ 15 years of experience in IT

david.coutadeur@worteks.com

@dcoutadeur

david-coutadeur

LemonLDAP::NG
LTB-Project : OpenLDAP-LTB, SSP, SD
LSC
FusionIAM

Worteks

Open Source software experts and sovereign cloud providers
Training center

Actively contributing to numerous Open Source software like
LSC, LemonLDAP::NG, LDAP Tool Box, FusionIAM and OpenStack

Partners

Red Hat
BlueMind
ONLYOFFICE
Collabora Online
PROXMOX

Comprehensive offer

Heterogeneous and complex infrastructures, troubleshooting, cloud, mail, identity, authentication, security...

Worteks addresses a wide range of issues associated with your information system.

Customized solutions

Worteks publishes packaged solutions, entirely composed of Open Source bricks.

These solutions are available On Premise, SaaS or PaaS with our W'aaS offer.

V'Sweet

Collaborative platform

V'IDaaS

Identity and access management solution

V'Opla

Complex infrastructure deployment solution

Presentation

LTB-project

- Community around LDAP integration:
  - **OpenLDAP-LTB**: Debian / Red-Hat packages for OpenLDAP
  - LDAP monitoring modules
  - **Self Service Password**: Web interface to reset password
  - **Service-desk**: directory management for admins
  - **White Pages**: directory management for users
  - Various scripts helping LDAP integration and management
  - OpenLDAP overlays:
    - **ppm**: Password Policy Module

One URL: https://ltb-project.org

LDAP 2026 TUEBINGEN

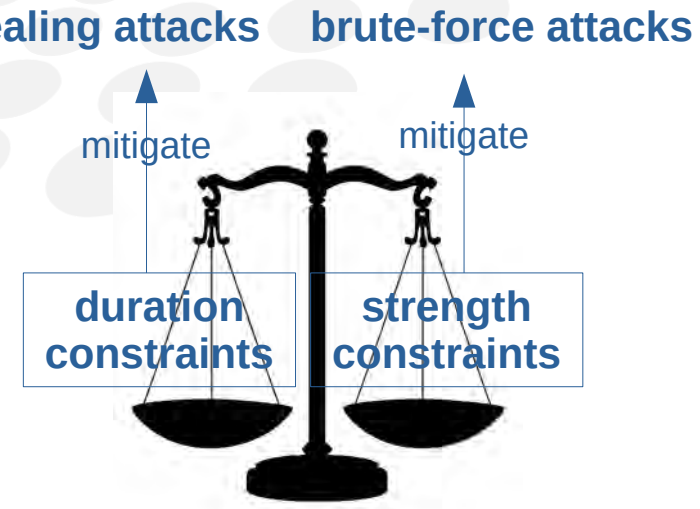
Password policies

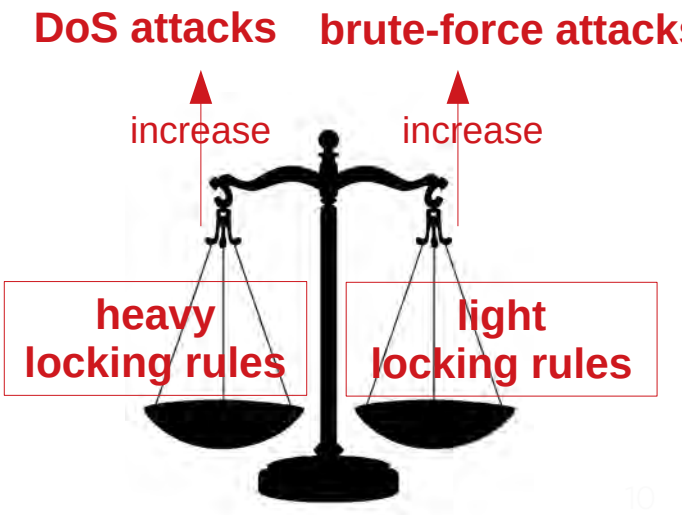
Password policies

What is a password policy?

set of rules about the user password

- **rules about strength**
  - length (minimum, maximum)
  - character classes (upper, lower, digit, special)
  - word blacklist
- **rules about password duration**
  - requirement to change the password after a delay (fixed or inactivity delay)
  - prohibition of password history reuse
  - prohibition to change password before a delay
- **locking rules**
  - locking after some bad authentications
  - locking because of unusual activity detection





Password policies

Normalizations

- No universal password policy!
- Recommandations / standards:
  - **NIST**, password guidelines, august 2024:
    - length (long passphrase) over complexity (too predictable)
    - no character classes required
    - no frequent change required
    - block common or compromised password
  - **IETF internet draft: "Password Policy for LDAP Directories"**

    draft-behera-ldap-password-policy (version 00: october 1999, version 11: february 2022), implemented into main directories:
    - OpenLDAP password policy overlay, SUN DS, Tivoli DS, Fedora DS, RH DS

Password policies

draft-behera-ldap-password-policy

- version 11, february 2022 (version 10 was released in 2009)
- Defines:
  - ☑ functional specifications of the password policy
  - ☑ LDAP schema for password policies and operationnal attributes
  - ☑ extended request and response controls
  - ☑ the way server should / must include ppolicy into LDAP operations (bind, modify,...)
  - ☑ the way clients should / must include ppolicy into LDAP operations (bind, modify,…)

Password policies

draft-behera-ldap-password-policy

- Does **not** define:
  - ☒ general considerations for managing policies (scope defined by SubtreeSpecification attribute, ppolicy overload)
  - ☒ replication and security considerations
  - ☒ the enforcement of password quality criteria, which are implementation specific
  - ☒ an automatic way to force password reset after a modification is performed by admin

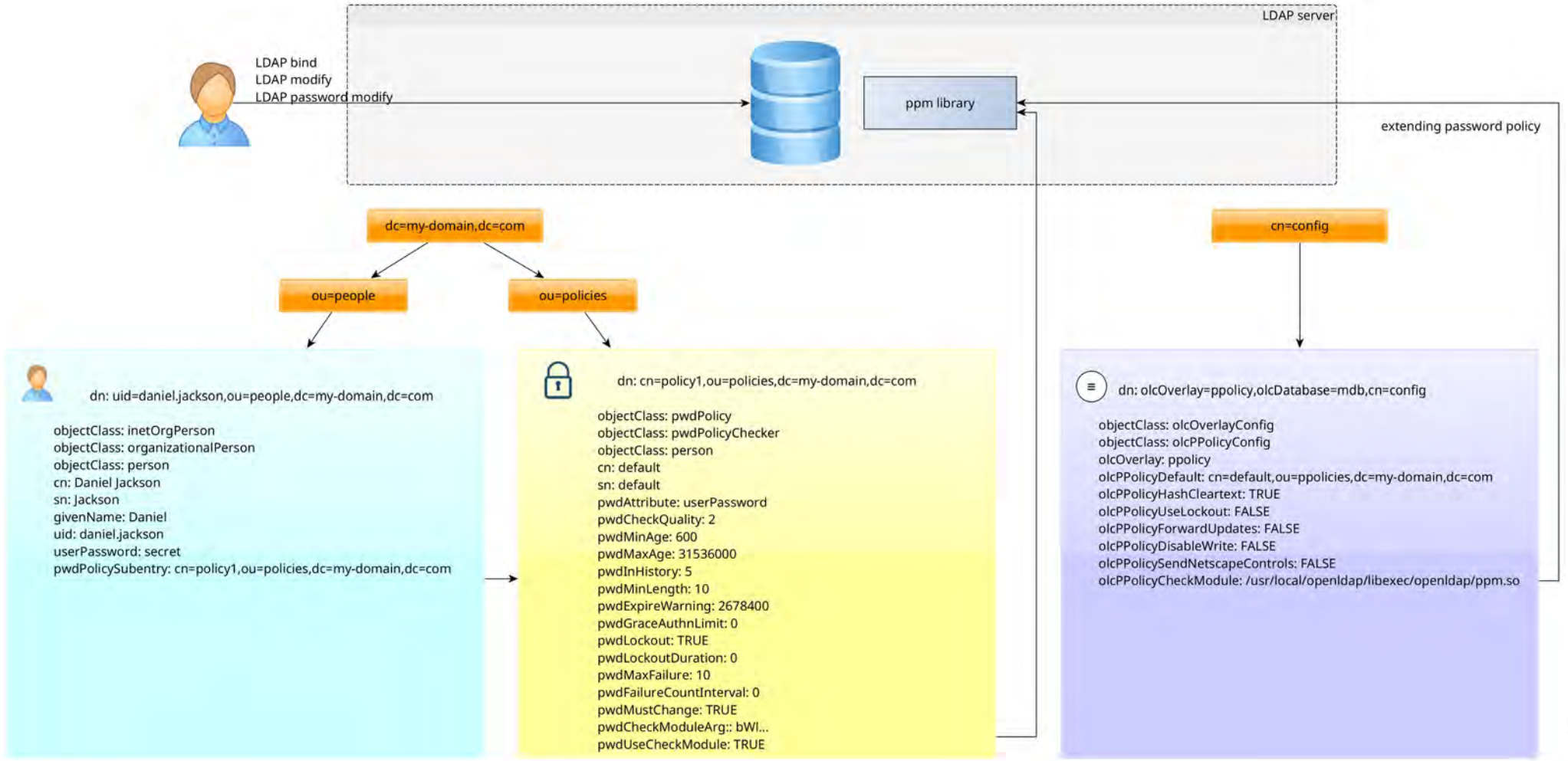
Password policies

Password policy overlay implements the IETF draft:

- ☑ the LDAP schema for password policies and operationnal attributes
- ☑ the extended request and response controls
- ☑ the server implementation
- ☑ the client implementation (ldapsearch, ldapmodify,…)
- ☑ protection against brute-force, based upon pwdMinDelay, pwdMaxDelay — New in 2.5!
- ☑ support of locking based upon pwdLastSuccess, pwdMaxIdle attributes — New in 2.6! New in 2.5!
- ☑ support of pwdMaxLength attribute — New in 2.5!
- ☑ support of pwdStartTime, pwdEndTime attributes — New in 2.5!
- ☑ password policies managed by scope in the DIT or by group — New in 2.7!

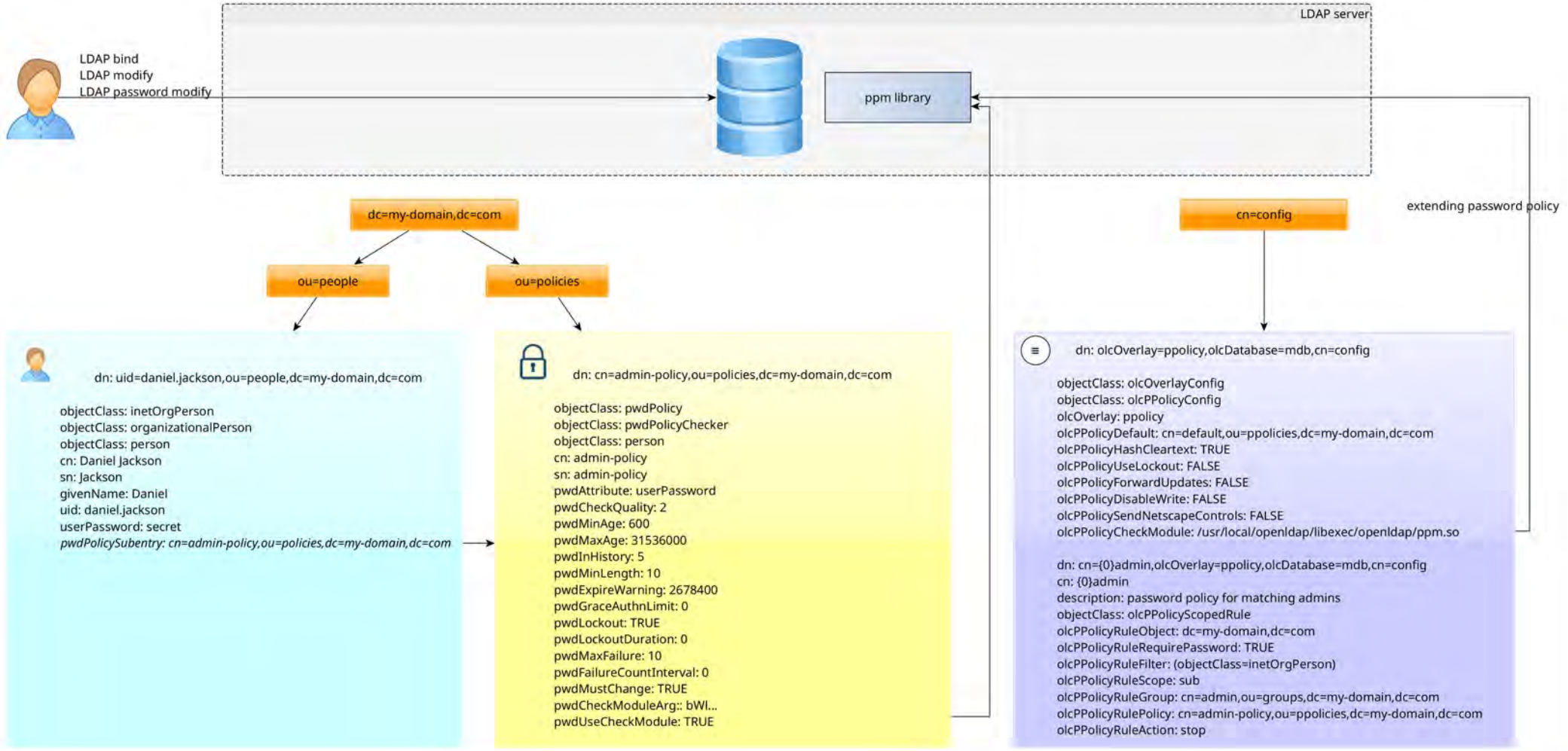
LDAP 2026 CON TUEBINGEN

Ppolicy implementation (2.6)



LDAP 2026 CON TUEBINGEN

Ppolicy implementation (2.7)



Ppolicy implementation

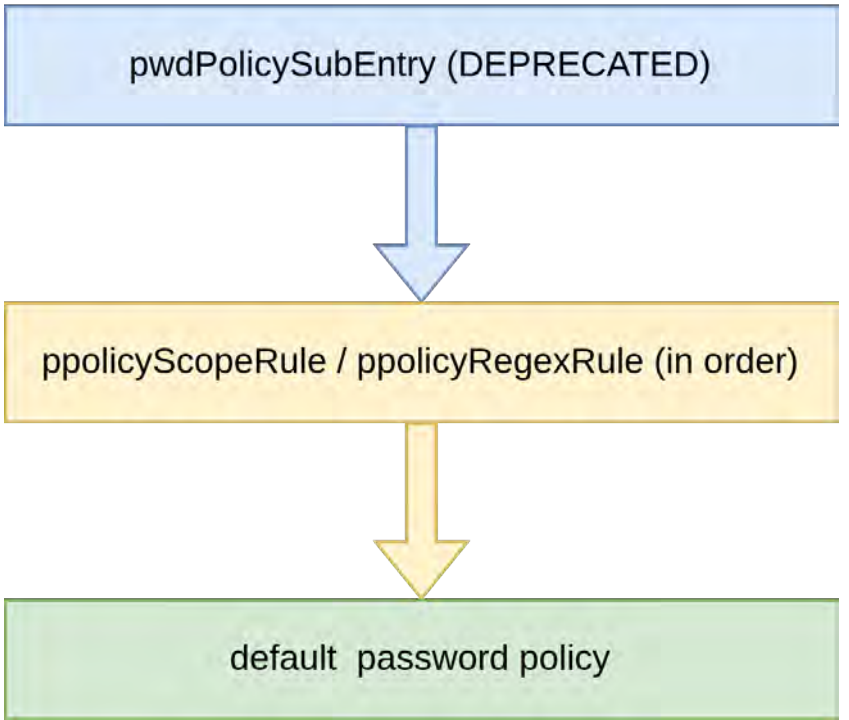
News in 2.7

- Ppolicy rules
  - list of rules
  - scope or regex rule
  - first match when rule=stop
  - default match when rule=continue

- Rehash feature
  - rehash user password at bind
  - defined in a password policy:

```
pwdRehashOnBind=TRUE
pwdDefaultHash={ARGON2}
```

Precedence of ppolicy assignment

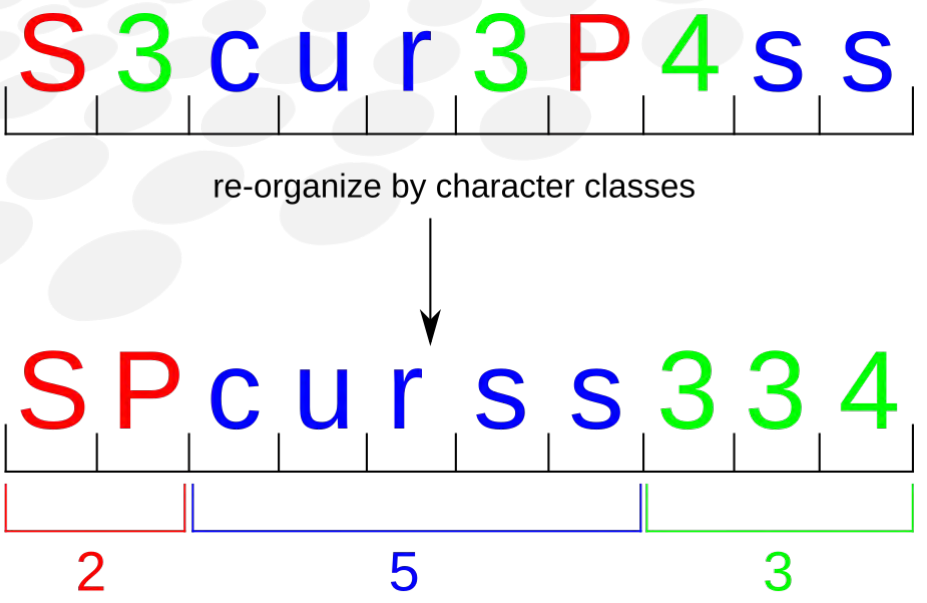


LDAP 2026 CON TUEBINGEN

ppm

LDAP 2026 CON TUEBINGEN

ppm



Character classes parameters

- definition of character classes
- minQuality
- min_for_point (for each character class)
- min (for each character class)

$quality_{uppercase}$ = 1 if 2 >= $min_for_point_{uppercase}$, else 0
$quality_{lowercase}$ = 1 if 5 >= $min_for_point_{lowercase}$, else 0
$quality_{digit}$ = 1 if 3 >= $min_for_point_{digit}$, else 0

Policy example:

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

Criteria:

2 >= $min_{uppercase}$

5 >= $min_{lowercase}$

3 >= min_{digit}

$quality_{uppercase}$ + $quality_{lowercase}$ + $quality_{digit}$ >= minQuality

ppm

Other strength parameters

- maxLength
- checkRDN
- forbiddenChars
- maxConsecutivePerClass
- useCracklib
- cracklibDict

CheckRDN criteria:

dn: uid=daniel.jackson,ou=people,dc=my-domain,dc=com

- new password: secret → OK
- new password: daniel → KO

Policy example:

```
maxLength 12
checkRDN 1
forbiddenChars ££
maxConsecutivePerClass 8
useCracklib 1
cracklibDict /var/cache/cracklib/cracklib_dict
```

LDAP 2026 CON TUEBINGEN

Evolutions

Evolutions

List for Santa

- Fix replication issues for operational attributes, like pwdLastSuccess
  - Issue when huge authentication trafic (lastBindPrecision)
  - Replication slave → master (doc about updateRef + chain overlay?)
- new parameter for account disabling: pwdAccountDisabled
  - pwdAccountLockedTime exists for temporary of permanent locking
  - most of the time, it allows automatic unlock, from user or admin
  - pwdAccountDisabled would be more restrictive
  - proposition of IETF ppolicy draft evolution for standardization of the schema
  - can also be achieved with custom schema and some ACL

Evolutions

List for Santa

- Write a standard for strength policy rules
- Reject password changes according to context criteria:
  - attributes in LDAP entry
  - attributes linked to LDAP entry (group,…)
  - environment: client IP address range, date and time of request
- Reject password with insufficient entropy (external library / API for entropy check?)

Worteks
make IT work, make IT free

LDAP 2026 CON TUEBINGEN

Thank you for your attention

www.worteks.com

info@worteks.com
+33 1 84 20 86 47
worteks_com
worteks