LibreOffice
The Document Foundation

ROME
CONFERENCE

Towards a single set of credentials across the whole TDF infrastructure

Guilhem Moulin

guilhem@libreoffice.org

ROME | 12 October 2017

The situation so far

- TDF’s infra team is maintaining a bunch of services (of various sizes)
- Each service manages its own authentication method and user database
- This is annoying:
  - For new contributors, who might need to create a gazilion accounts
  - For existing users, in case of a password or email change
  - For the admin team, who need to keep groups and roles up to date
- We need a central user/group database!

Lightweight Directory Access Protocol (1/2)

- Open standard
- Hierachical structure (tree), hence possibility to create namespaces

```
ou=WebSSO,dc=documentfoundation,dc=org
├── ou=users
│   ├── uid=guilhem
│   └── uid=test
└── ou=groups
    ├── cn=admin
    ├── cn=tdf-staff
    ├── cn=tdf-board
    └── ou=nextcloud
        ├── cn=user
        └── cn=admin
```

Lightweight Directory Access Protocol (2/2)

- Authentication can be delegated to the LDAP server itself
- Very fine-grained notion of ACLs
- Can provide LDAP internal audit log (OpenLDAP overlay)

Migrating isn’t easy

- We can’t just take user accounts and map them to a LDAP entry
  - Accounts `guilhem`, `gmoulin`, `guilhem.moulin` should be merged
  - Not all service use a username (login) as unique ID, some use email address
  - Users have multiple email accounts and aliases, for instance `@libreoffice.org`
- We can’t arbirtrarily decide to use a particular service as authoritative source for username and email address
- Instead we started with an empty DIT and kindly request you to populate it: `https://user.documentfoundation.org`. Please! Only 300 entries since November last year ☹

In the meantime

- We migrated *some* accounts to LDAP on services supporting dual auth method:
  - TestLink https://manual-test.libreoffice.org
  - SilverStripe's test instance https://newdesign.libreoffice.org
  - Wiki test instance https://wiki.documentfoundation.org
  - Etherpad-Lite https://pad.documentfoundation.org
  - NextCloud https://nextcloud.documentfoundation.org
- Furthermore Collabora's NextCloud instance (used for instance in ESC calls) has been bridged to our LDAP server since the start
- Less intrusive changes first!

Merging accounts (not ready)

- Manual merging is error prone and doesn’t scale
- We’ll need you to fill in the blanks ☺
  - All public services require email confirmation, so email addresses can be used to uniquely determine a user → need an interface to enter multiple addresses
  - Otherwise, you’ll be able to provide your username/password for each service, and on succesful auth the user panel will link the accounts internally
- Possibly ripe for abuse, but surely we can stay civil

The future: reduce attack surface

- Once *all* accounts have been migrated, we can get real SSO:
  - Replace the app’s login form with a redirection to the central auth portal `https://auth.documentfoundation.org` (and then back to the app)
  - Not all users are comfortable with password authentication; the `LemonLDAP::NG` portal supports Saml, Oauth2, etc.
  - `https://www.nginx.com/blog/nginx-plus-authenticate-users/` (or something more sophisticated like SAML)
- Custom portal `https://user.documentfoundation.org` will be shut down afterwards (was only needed for arbitrary usernames and account merging)
- Demo time! WebSSO for `https://wiki.documentfoundation.org` (SAML 2.0) and `https://pad.documentfoundation.org` (HTTPd protection)

Thanks!

https://user.documentfoundation.org