Authentication on web applications with LemonLDAP::NG
Speaker

Clément OUDOT
Identity Solutions Manager
Worteks

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

KPTN - https://kptn.org
DonJon Legacy
Improcité
**Service**

- Complex infrastructures, cloud, mail, authentication, security
- Studies, audit & consulting
- Technical expertise
- Support
- Training
- R&D and innovation

**Edition**

- V'Sweet Collaborative portal
- V'Opla Common development platform
- V'IDaas Identity and Access Management

**Partners**

- Red Hat
- BlueMind
- ONLYOFFICE
- Collabora Online
All we need is you!

https://www.worteks.com/rejoindre/
Imagine SSOng

Imagine there are no passwords
Or maybe just only one
A single secured form
To access our applications
Imagine all the users
Loving security
Imagine some protocols
Made by clever people
CAS, OpenID or SAML
Even WS Federation
Imagine authentication
Interoperability

Imagine applications
No more storing passwords
Relying on a token
Even for authorizations
Imagine all developers
Loving security
You may say
I'm a hacker
But I'm not the only one
I hope one day
You will log in
Using the Single Sign On

© John Lennon
SSO Workflow

1. First access
2. Authentication
3. Send SSO Token
4. Validate SSO token

Authentication Portal

Trust link

Application
History

- Project creation: 2003
- Protocols CAS, SAML and OpenID: 2006
- Protocol OpenID Connect: 2010
- Second factors (2FA) Version 2.0: 2016
- Fork – version NG: 2018
Main features

- SSO & Access Control
- Application menu
- CAS / SAML / OIDC
- Second Factor (2FA)
- Password management
- Graphical customization
Command Line Interface

root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli info

Num : 88
Author : clement
Author IP: localhost
Date : Tue Dec 18 09:57:58 2018
Log : Edited by lnConfigEditor

root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli help
Usage: /usr/share/lemonldap-ng/bin/lemonldap-ng-cli <options> action <parameters>

Available actions:
- help : print this
- info : get current configuration info
- update-cache : force configuration cache to be updated
- get <keys> : get values of parameters
- set <key> <value> : set parameter(s) value(s)
- addKey <key> <subkey> <value> : add or set a subkey in a parameter
- delKey <key> <subkey> : delete subkey of a parameter

See Lemonldap::NG::Common::Cll(3) or Lemonldap::NG::Manager::Cll(3) for more

root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli set ldapServer 'ldap://ldap.example.com'
Free Software

- License GPL
- OW2 project
- Forge: https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng
- Site: https://lemonldap-ng.org
- OW2 Community Award in 2014
- SSO component of FusionIAM project: https://fusioniam.org/
Component roles

Portal

- Application menu
- CAS SAML OpenID Connect
- Self Services
- SOAP/REST server
- Session management

Manager

- Configurations
- Sessions
- Notifications
- Second factors

Handler

- Access Control
- SSOaaS
- Web Service Token
- Custom
Web application

Portal

Authentication

Session creation

Sessions

Session read

Web Application

Handler

SSO cookie

HTTP headers
CAS

- Created by University of Yale
- Central Authentication Service
- Proxy mode since v2.0
- Attributes sharing since v3.0
- https://www.apereo.org/projects/cas
CAS

First access

Redirection for authentication

Service Ticket

Service ticket validation

Access to identity

CAS client

CAS server
SAML

- Created by OASIS organization
- Security Assertion Markup Language
- Version 1.0 in 2002
- Version 1.1 in 2003
- Version 2.0 in 2005 merging SAML, Shibboleth and ID-FF (Liberty Alliance)
SAML

First access
IDP choice

Authentication request

Authentication response

Signature verification
Read assertion

Service Provider (SP)

Authentication response

Authentication response

Identity Provider (IDP)
OpenID Connect

• Created in 2014
• Presented at RMLL in 2015
• Based on OAuth 2.0, REST, JSON, JWT, JOSE
• Adapted to web browser and native mobile applications
• Attributes sharing through UserInfo endpoint
OpenID Connect

First access
OP choice

Authentication request

JWT

Signature verification
Read JWT

Get UserInfo

Relying Party (RP)

OpenID Provider (OP)
Second Factor Authentication (2FA)

- LemonLDAP::NG can use the following 2FA:
  - TOTP
  - WebAuthn
  - Mail
  - External (SMS)
  - REST
  - Yubikey
  - Radius
RENATER / eduGAIN

- Support of RENATER / eduGAIN via SAML2:
  - Service Provider
  - Identity Provider
- Call to Identity Provider selection page (WAYF) via SAML Discovery Protocol
- Metadata bulk import script
Plugin engine

- Portal code was fully rewritten, and it now allows to write plugins

- Plugin examples, provided by default:
  - Auto Signin: direct authentication for some IP
  - Brute Force: protect against brute-force attacks
  - Stay Connected: "remember me" button
  - Public Pages: create static pages using portal skin

- Write a custom plugin:
  https://lemonldap-ng.org/documentation/latest/plugincustom
Password Policy

• A local password policy can now be configured (minimal size, type of characters, ...)

• A graphical form shows which criteria are filled
Documentation and Website

- Documentation was rewritten with Sphinx (reStructuredText)
- Website rebuilt as static pages with Templer
Keep informed about LL::NG

- Register to lemonldap-ng-announces mailing list
  https://mail.ow2.org/wws/subscribe/lemonldap-ng-announces

- Follow project updates
  https://projects.ow2.org/bin/view/lemonldap-ng/

- Social networks:
  - Twitter: https://twitter.com/lemonldapng/
  - Facebook: https://www.facebook.com/lemonldapng/
Thank you