LEMONLDAP::NG 2.0

FOSDEM 2019
LemonLDAP::NG Software
SSO Workflow

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

Authentication Portal

Trust link

Application
Main features

- Web Single Sign On
- Access control
- Applications portal
- Authentication modules choice and chain
- Password management, account creation
- Multi-factor authentication (MFA)
- Protection of Web applications and API/WebServices
- Graphical customisation
- Packages for Debian/Ubuntu/RHEL/CentOS
Portal with application menu
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::Cli(3) or Lemonldap::NG::Manager::Cli(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
How works the agent (Handler)
Protocols CAS, SAML and OpenID Connect
Main features

- LL::NG can act as client and as server
- Attributes sharing
- Manage authentication contexts and levels
- Autogeneration of public/private keys
- Access control per services
- Publication of configuration data (metadata)
- Multi-protocols gateway
- Single logout
New in LemonLDAP::NG 2.0
Second Factor Authentication (2FA)

- LemonLDAP::NG can use the following 2FA:
  - TOTP
  - U2F
  - TOTP or U2F
  - External
  - REST
  - Yubikey
Configuration backends

- Already existing backends:
  - JSON file
  - Database
  - LDAP
  - NoSQL (MongoDB)
  - SOAP

- New backends:
  - YAML file
  - REST
  - Local (no backend, only lemonldap-ng.ini file)
NodeJS Handler

- Native integration in Express application
- Rules and headers configured in Javascript
- https://github.com/LemonLDAPNG/node-lemonldap-ng-handler

```
npm install node-lemonldap-ng-handler
```
DevOps (SSO as a Service)

- Authentication managed by portal
- Access control and HTTP headers configuration set in a local JSON file
- Allow quick applications deployment without need to edit main SSO configuration
API / WebService protection

- New Handler "Service Token" installed between application and WebService
- Main Handler generates a token based on time, session_id, and virtual hosts
- The token is sent by application to WebService
- The Handler "Service Token" intercepts the token, validates it and applies access rules, and sends HTTP headers to WebService
API – Service Token

- Portal
- Web Service
- Session creation
- SSO cookie
- Session read
- Session read
- Handler
- HTTP headers
- Token
- Web Application
- HTTP headers
- Handler Service Token
Authentification modules

- New modules:
  - PAM
  - REST
  - Kerberos (GSSAPI)
  - CAS (attributes reading)
- Multi is replaced by Combination
- Custom module
Administration interface

- Configurations comparator: differences between two configurations are displayed in a tree
- Second factors administration (search, revoke)
- Sort sessions by creation date or modification date
• 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
Other new features

- A user can refresh rights without disconnect/reconnect
- REST services for configurations and sessions
- Select language before authentication
- New graphical theme built with Bootstrap 4
- Logo customization (used in graphical theme and sent mails)
- Log system choice (syslog, Apache, Log4Perl, Sentry...)
THANKS

Pour plus d’informations :

Email: info@worteks.com
Twitter: @worteks_com
LinkedIn: linkedin.com/company/worteks