LemonLDAP::NG 1.3
David Coutadeur

New features of LemonLDAP::NG 1.3
About the speaker
David Coutadeur

- LDAP engineer since 2010 in LINAGORA company, with experiences in SUN/Oracle to OpenLDAP migration
- Integrator for LinID solutions [http://linid.org](http://linid.org)
- Member of the LTB team [http://ltb-project.org](http://ltb-project.org)
- Member of the LSC team [http://lsc-project.org](http://lsc-project.org)
- Member of LemonLDAP::NG project core-team [http://lemonldap-ng.org](http://lemonldap-ng.org)
LemonLDAP::NG
Components

• LemonLDAP::NG main components:
  • **Portal**: authentication process, user interaction, application menu, password change form
  • **Manager**: configuration interface, sessions explorer
  • **Handler**: Apache agent, manage access authorizations

• Perl, only Perl, just Perl

• Relies on Apache and mod_perl
Follow the white request
What's new?

- FastCGI Portal
- Authentication/user modules:
  - Active Directory,
  - BrowserID,
  - WebID,
  - Google,
  - Facebook
- JSON file configuration backend
- Captcha
- Aliases for virtual hosts
- CLI LemonLDAP Manager
FastCGI Portal

- **CGI** interfaces applications to web servers
- **FastCGI** reduces overhead thanks to persistent processes, joined by a socket or TCP connexion
- LemonLDAP::NG CGIs can now be easily extended to FastCGI:
  - Manager (not so useful)
  - Portal
- Improves response time
- Scalability not tested yet (cgi farm servers)
Active Directory module

- Active Directory is a "special" LDAP directory
- AD module is nearly the same as LDAP
  - Specific default values for filters to match AD schema
  - Compatible password modification
  - Reset password on next logon workflow
Browser ID module

- Authentication database only
- **Mozilla Persona**: implementation of a distributed login system based on BrowserID protocol
- Similar to OpenID
- BrowserID based on email address / OpenID based on a complicated URL
- Cross-browser (if recent)
- Public key cryptography
- Involves users, Relying Parties, and Identity Providers
WebID module

• Invented by a community group at W3C

• **Public Key WebID** = URI that refers to a person
  → uniquely identifies a user by his relation to a public key

  e.g. `https://mywebsite.net/#dco`

• WebID protocol is based on these URIs and a client certificate

• You may already have one!
  By joining a social network site: Libre.fm, MyOpera, Twitter

• URI can be linked to other profiles, to create a linked web of trust

• FOAF sites: store Friend of a a friend datas
  can provision users module in LemonLDAP::NG
Google™ module

- Authentication and users databases
- Users log in with Google authentication process
- LemonLDAP uses OpenID protocol to trust the latter
- OpenID
  - decentralized authentication system based on URL, involving Providers, Relying parties and users,
  - user chooses what data he wants to be accessible for each RP
- Mail used as login name
- A few data available: country, email, firstname, language, lastname
Facebook module

- More than 1.1 billion users in the world
- Authentication and users databases
- OAuth2 as authorization protocol (no authentication)
- OAuth2
  - Based on access and refresh tokens exchanged between client application and resource server
  - Binding between LemonLDAP (client) and Facebook (resource server) is done by getting an application ID and a secret
JSON file configuration backend

- "JavaScript Object Notation"
- Generic data format allowing to represent structured information
- Configuration stored in a more readable way
- Can be shared by
  - any files sharing system (NFS, NAS, SAN,…)
  - SOAP configuration backend proxy
And much more...

- Captcha
  - Can be used
    - At user connection
    - In mail reset component
  - Extra control to ensure one is human
- Aliases for virtual hosts
  - Allows numerous vhosts creation owning same headers and same protection rules
- CLI LemonLDAP Manager
  - Tool to manage LemonLDAP configuration with the command line
What's next?

- Configuration and cache optimization
- Code refactoring with Moose/Mouse for a better OO code
- Handler modularization
  - compatibility with apache MPM-event or Nginx?
The end... almost
Thanks

• Thanks to:
  • OW2 Con organizers
  • LINAGORA company
  • LemonLDAP::NG and Perl community
• Stay in touch:
  • IRC: stryg #lemonldap-ng@freenode
Questions?