

LemonLDAP++NG

LemonLDAP++NG 1.2



Clément OUDOT
RMML – 9 juillet 2012

LIN AGORA

- Le logiciel LemonLDAP::NG
- Les nouveautés de la version 1.2



Présentation



- Administrateur LDAP depuis 2003 à LINAGORA
- LinID Dream Team Manager <http://linid.org>
- Leader du projet LDAP Tool Box <http://ltb-project.org>
- Leader du projet LemonLDAP::NG <http://lemonldap-ng.org>

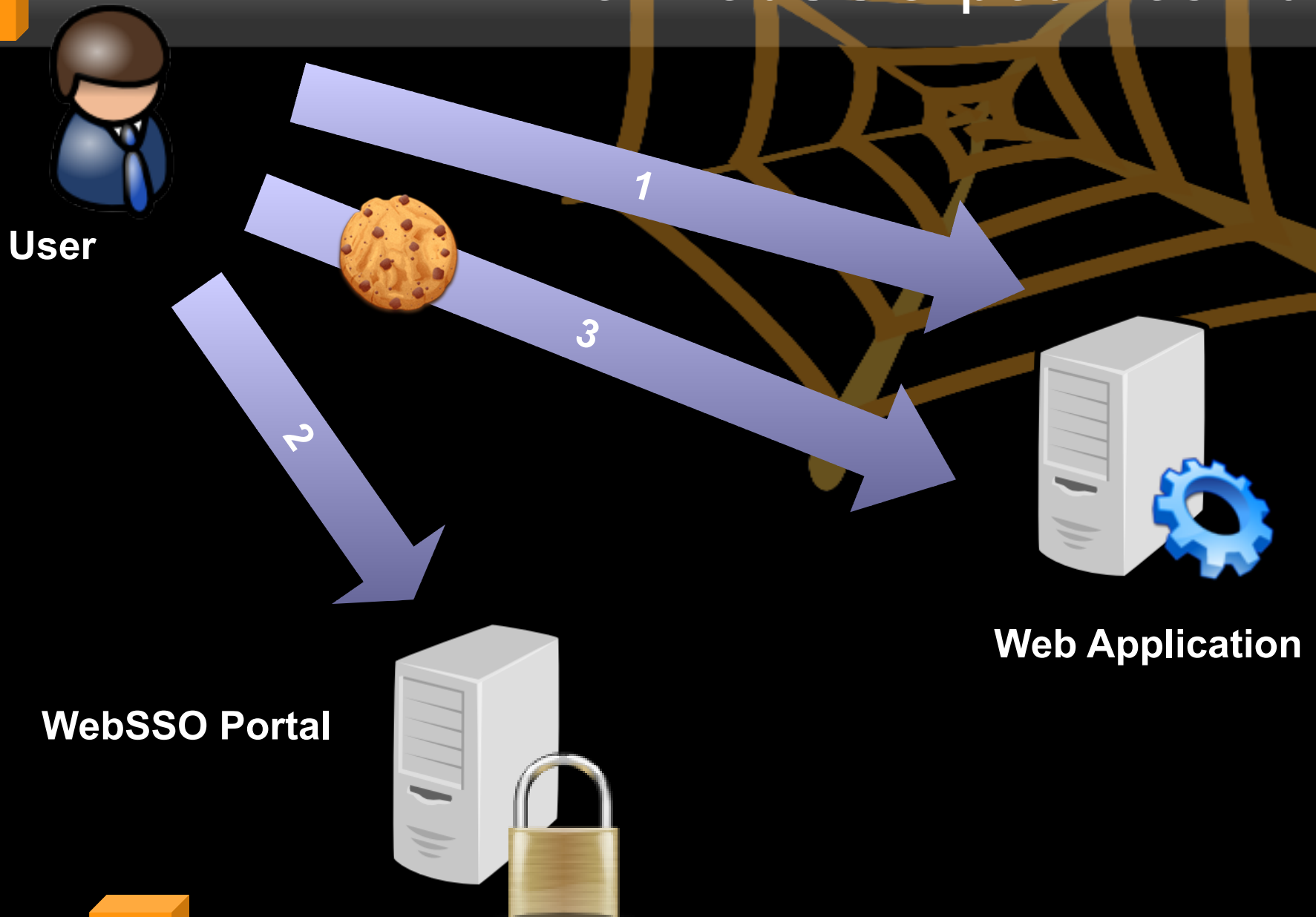
Le logiciel LemonLDAP:NG



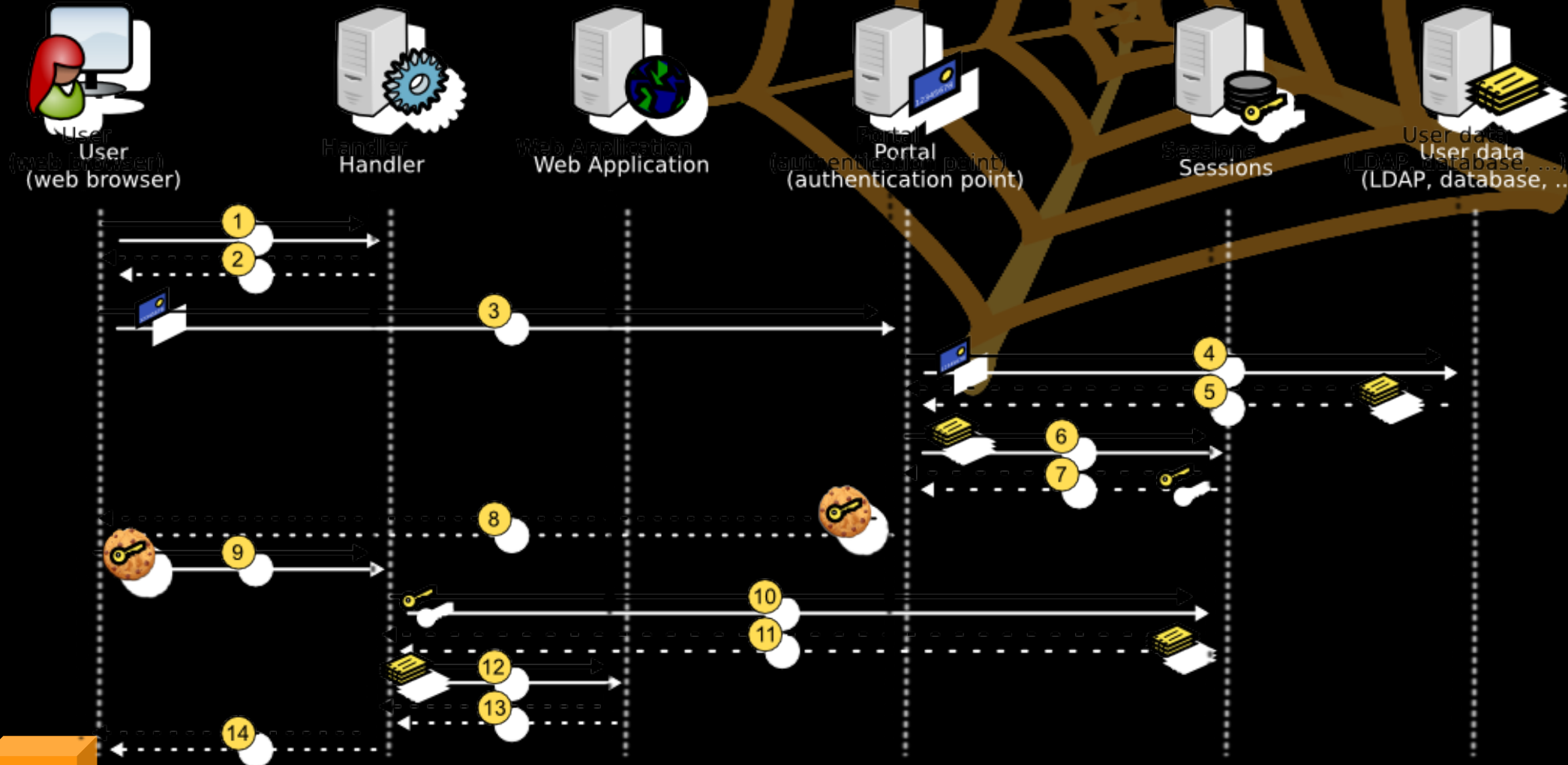
- Rayez les mentions inutiles ou complétez :
 - Logiciel libre
 - Écrit en Java
 - Single Sign On
 - Authentification LDAP
 - Fournisseur d'identité SAML 2.0
 - Made in Taiwan
 - Pas de concurrents sur le marché

- Rayez les mentions inutiles ou complétez :
 - Logiciel libre **GPLv2 / Perl Artistic License**
 - Écrit en ~~Java~~ **Perl**
 - Single Sign On **pour les applications Web**
 - Authentification LDAP, **SQL, SSL, Radius, etc.**
 - Fournisseur d'identité SAML 2.0, **OpenID et CAS**
 - Made in ~~Taiwan~~ **France**
 - ~~Pas de concurrents sur le marché~~ **OpenAM, ...**

Le WebSSO pour les nuls



Le WebSSO pour les dieux





Les points forts de LemonLDAP::NG

- Conception modulaire, philosophie CPAN
- Gestion des règles d'accès par expressions régulières
- Console d'administration Web
- Explorateur de sessions
- Internationalisation
- Portail d'applications et Self Service de mot de passe
- Déploiement en mono serveur ou en architecture distribuée
- Capture des déconnexions (Single Logout)

- Règles d'accès :
 - default → accept
 - ^/admin → \$groups =~ /admin/
 - ^/logout.php → logout_sso
- En-têtes HTTP :
 - Auth-User → \$uid
 - Auth-Name → uc(\$sn).", ".ucfirst(\$gn)

Interface d'administration

LemonLDAP::NG

Configuration management

Sessions explorer

Menu style

Configuration 177

- General Parameters
 - Portal
 - URL
 - Menu
 - Modules activation
 - Categories and applications
 - 1test
 - 2documentation
 - wiki
 - wikionline
 - Customization
 - Authentication modules
 - Issuer modules
 - Logs
 - Cookies
 - Sessions
 - Advanced parameters
 - Variables
 - Exported Variables
 - cn
 - login
 - mail
 - name
 - uid
 - Macros
 - Groups
 - Virtual Hosts
 - SAML 2 Service
 - SAML identity providers
 - SAML service providers

Available actions

Save Delete application

Edit key wikionline

Key	<input type="text" value="wikionline"/>	Display name	<input type="text" value="New site"/>
Address	<input type="text" value="http://lemonldap-ng.org"/>	Display mode	<input type="text" value="Automatic"/>
Description	<input type="text" value="This is a nice application"/>	Logo	<input type="text" value="bookmark.png"/>
<input type="button" value="Apply"/>			

Help

Categories and applications




Configuring the virtual hosts is not sufficient to display an application in the menu. Indeed, a virtual host can contain several applications (<http://vhost.example.com/appli1>, <http://vhost.example.com/appli2>).

In Manager, you can configure categories and applications in General Parameters > Portal > Menu > Categories and applications.

Portail d'applications

✔ Utilisateur authentifié

Connecté en tant que Clément OUDOT

 Vos applications  Mot de passe  Déconnexion

Applications de test



Application Test 1
This is a nice application



Application Test 2
This is a nice application



Application de test 3
Test du cross-domain

Documentation



New site
This is a nice application

Ce service est fourni par [LemonLDAP::NG](http://lemonldap-ng.org), logiciel libre protégé par la licence GPL.

LemonLDAP::NG 1.2





Mode démonstration

- Ce nouveau mode consiste dans un module d'authentification et d'utilisateurs « démo » (AuthDemo, UserDBDemo)
- Ces modules fournissent des comptes de test permettant d'ouvrir une session SSO
- Un des comptes de test possède les droits d'administration
- Ce mode est configuré par défaut lors de l'installation de LemonLDAP::NG

Mode démonstration



DOCTOR - WHO



Historique de connexion

- L'historique de connexion permet de conserver les dates des dernières authentifications réussies et des dernières authentifications ratées (avec la raison)
- L'historique est disponible aux administrateurs et peut être proposé aux utilisateurs :
 - Par un onglet dans le menu
 - Par un message affiché après l'authentification et avant la redirection vers l'application protégée



Insertion dynamique d'un menu sur les applications protégées

- Il est désormais possible d'insérer dynamiquement un menu dans les applications protégées
- Ce menu est pour l'instant très simple :
 - Un lien vers le portail des applications
 - Un lien pour se déconnecter
- Ce menu est ajouté à l'aide d'un Filtre Apache, totalement non intrusif sur l'application



Mode maintenance

- Ce mode permet de désactiver une application
- Le Handler LemonLDAP::NG renvoie un code HTTP 503
- Si cette application est déployée en cluster, tous les nœuds sont automatiquement configurés pour désactiver l'application
- Ce mode ne nécessite aucune intervention sur la configuration Apache

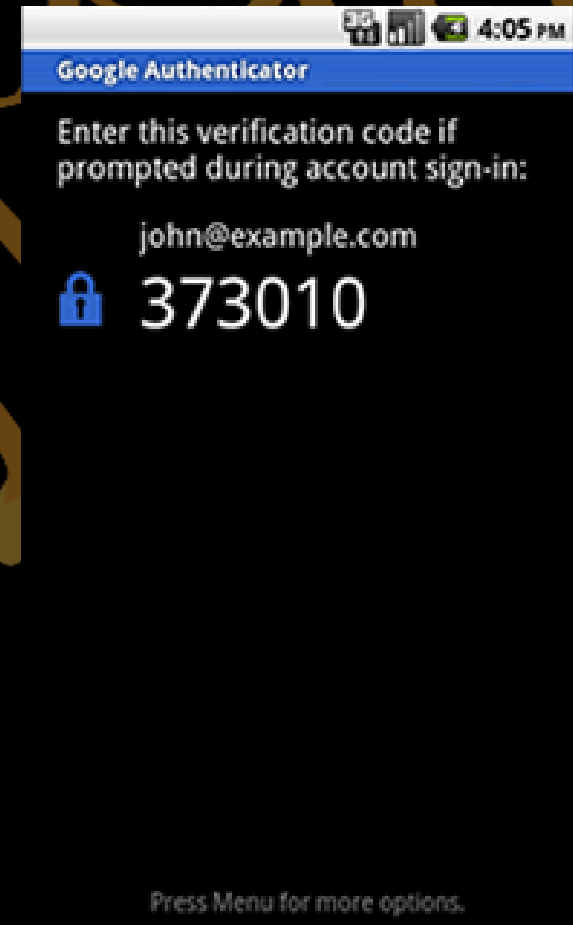


Règles unprotect et skip

- La règle « skip » est apparue, en renfort de la règle « unprotect » pour désactiver la protection de certaines parties d'une application :
 - Règle « skip » : la zone est déprotégée, les en-têtes sont supprimées pour tous les utilisateurs
 - Règle « unprotect » : la zone est déprotégée, les en-têtes sont supprimées pour les utilisateurs non authentifiés au SSO, mais conservées pour les utilisateurs possédant une session

Authentication Radius

- Possibilité d'utiliser un login/mot de passe pour s'authentifier sur Radius
- Compatibilité avec Google Authenticator en concaténant son mot de passe avec l'OTP dans le champ mot de passe



La fin est proche...



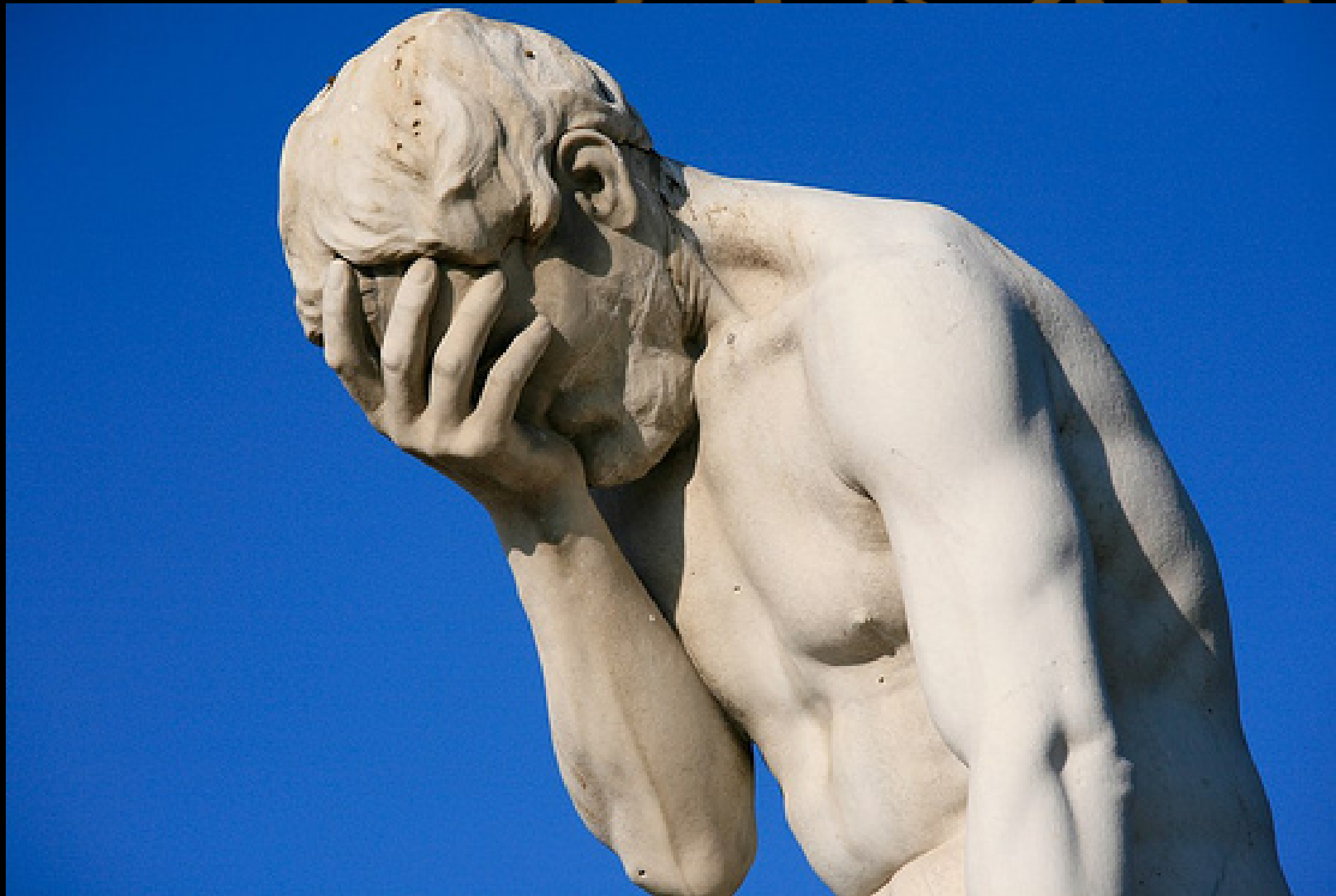


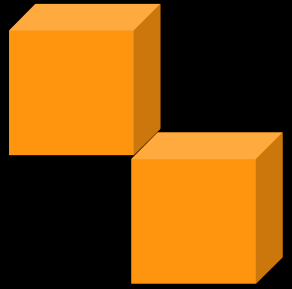
Merci



- Merci :
 - RMLL et les organisateurs de la session
 - Société LINAGORA
- Restons en contact :
 - Identica: @coudot
 - Twitter: @clementoudot @lemonldapng
 - IRC: KPTN #lemonldap-ng@freenode

Questions ?





LemonLDAP::NG



Merci de votre attention

LIN AGORA