

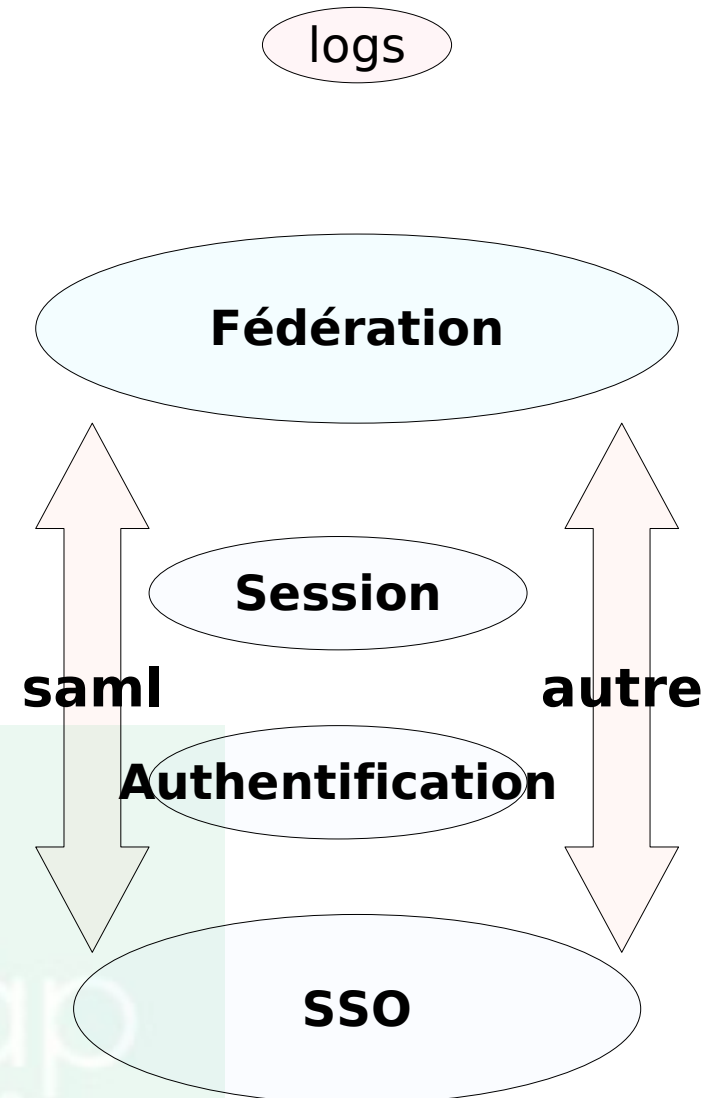
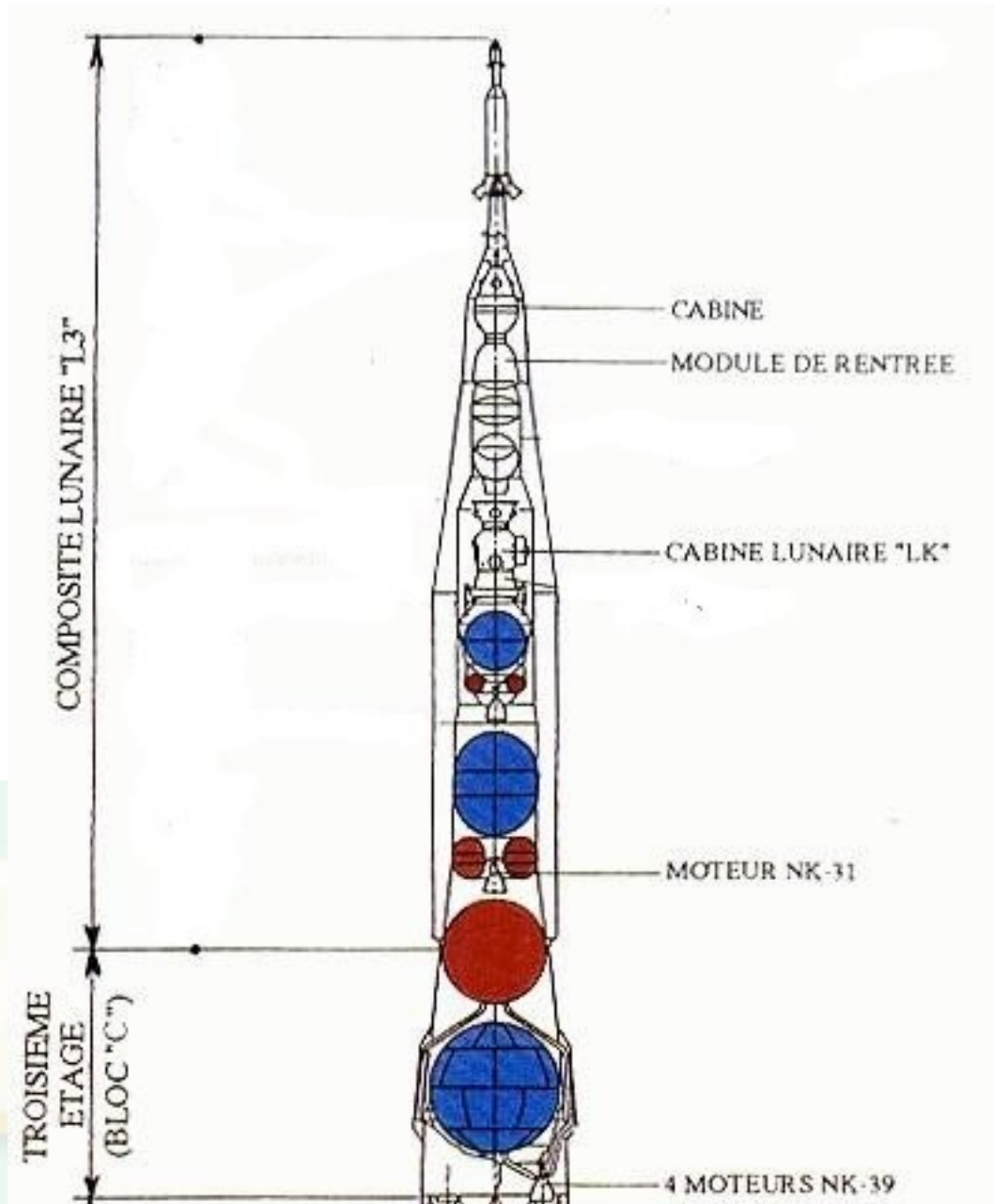
Autour de la gestion d'identité

- Etat de l'art.
- Les bonnes pratiques.
- Le tableau de bord

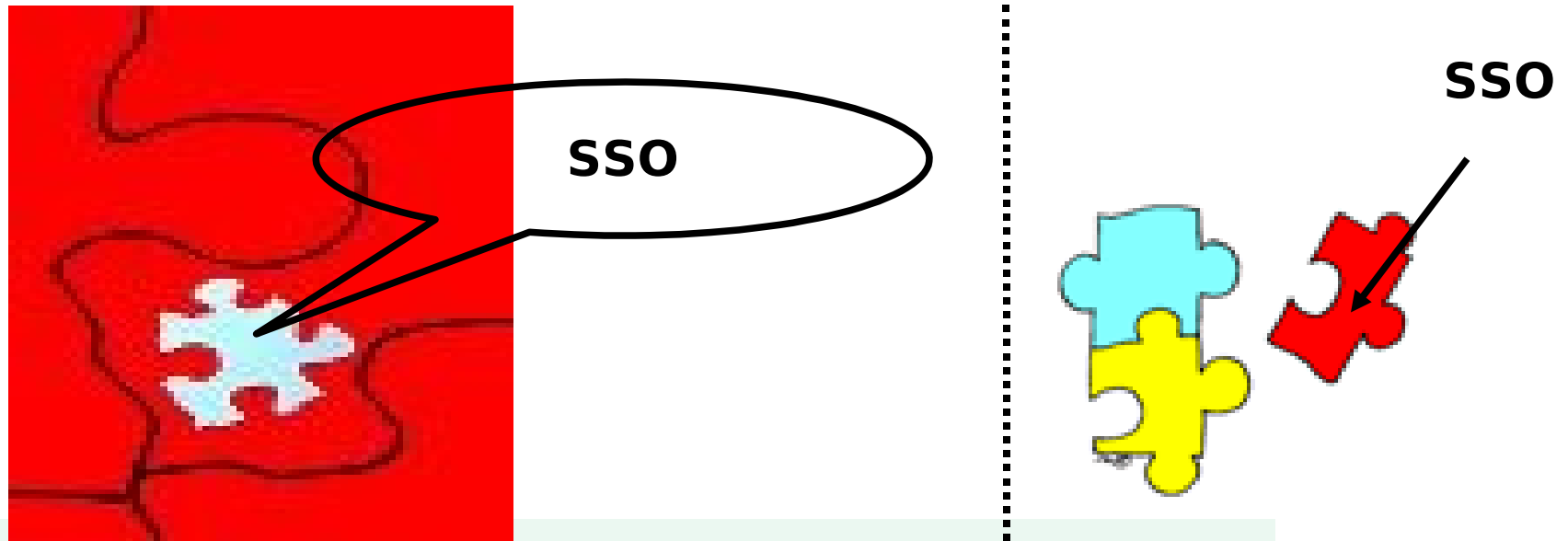


LemonLdap
Single Sign On Infrastructure

La Fusée Gestion d'identité



La gestion d'un projet SSO



Notre système d'identité en rêve

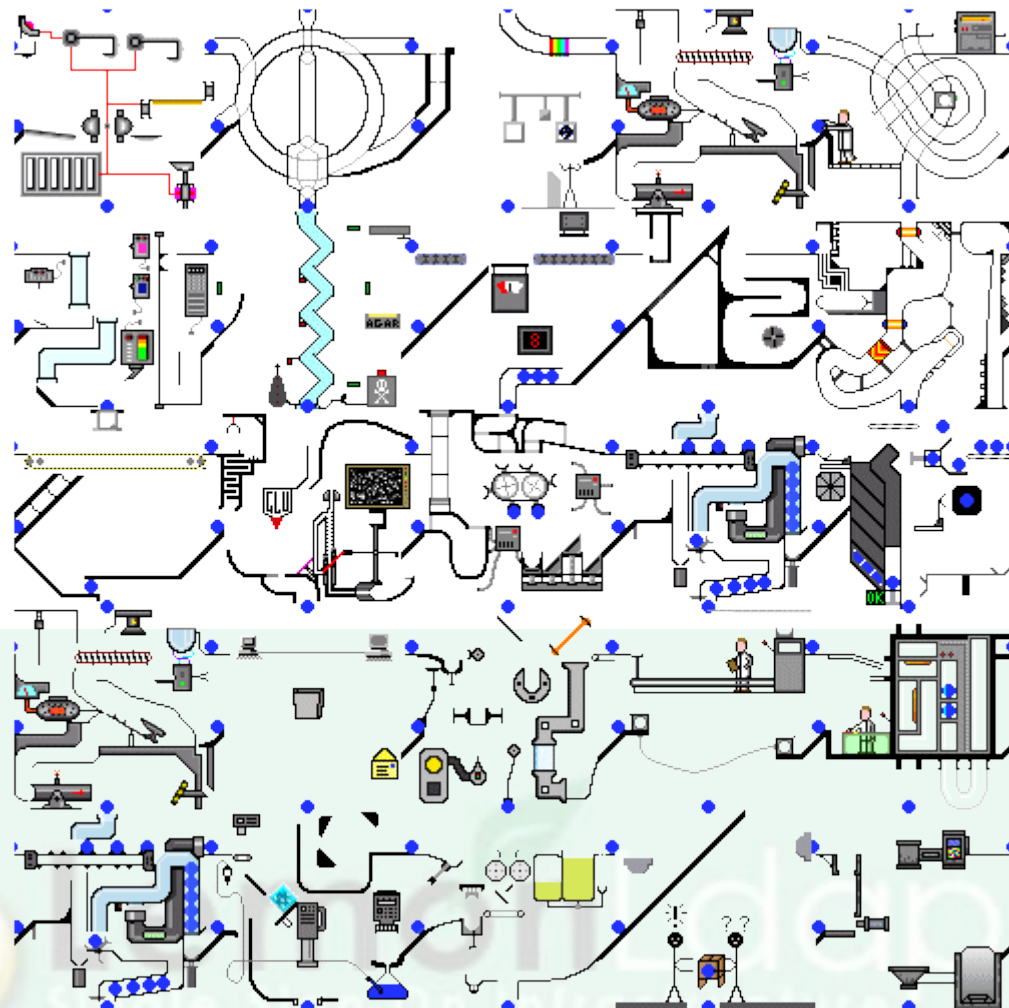


Tout ça pour moins de 300 €



LemonLdap
Single Sign On Infrastructure

La gestion d'identité en vrai



SSO : Single Sign ON Authentication unique

—————→ **Web**

JOSSO

BANDIT

CAS

OpenID

Interldap

Lemonldap

Sign and GO

OpenSSO

google account



LemonLdap
Single Sign On Infrastructure

Les Acteurs

- Liberty alliance
- WS*
- Shibboleth
- Netvibes
- google

SAML

web2

(le web2 ?? , le web3 ??? => paye des fonctionnaires :Bull DPS7/GCOS-COBOL)

Authentication server serveur d'authentification

- User / password
- Certificat client
- Certificat client + user/password
- Biometrie
- Smart card
- Clé USB

==> vérification sur un LDAP / Base de données



Autorisation

- Presence d'un attribut LDAP
- Valeur d'un attribut LDAP
- ➔ profil applicatif
- Exemple
 - Mefiappliddgi : ADONIS; 001
 - Mefiappliddgi : FICOBA; admin
- Groupes LDAP (unix groups)



LemonLdap
Single Sign On Infrastructure

Alors ?

- Sur la fédération d'identité :
- 2 gros acteurs :
 - Liberty Alliance (constructeurs/editeurs)
 - Shibboleth (Universitaire)
 - Aucun ne règle le problème du SSO (bas-niveau).
 - Très complexe (XML secure , vocabulaire, mise en oeuvre)
 - Avantage à Shibolet (Formations, plus de documentation, d'exemple)

===== > Même problème
qu'avec une PKI/IGC.

L'outsider : OpenID

- Simple
- Facile à installer
 - Client
 - Serveur
- Grosse part de marché



Pour commencer à s'amuser (cpan.org)

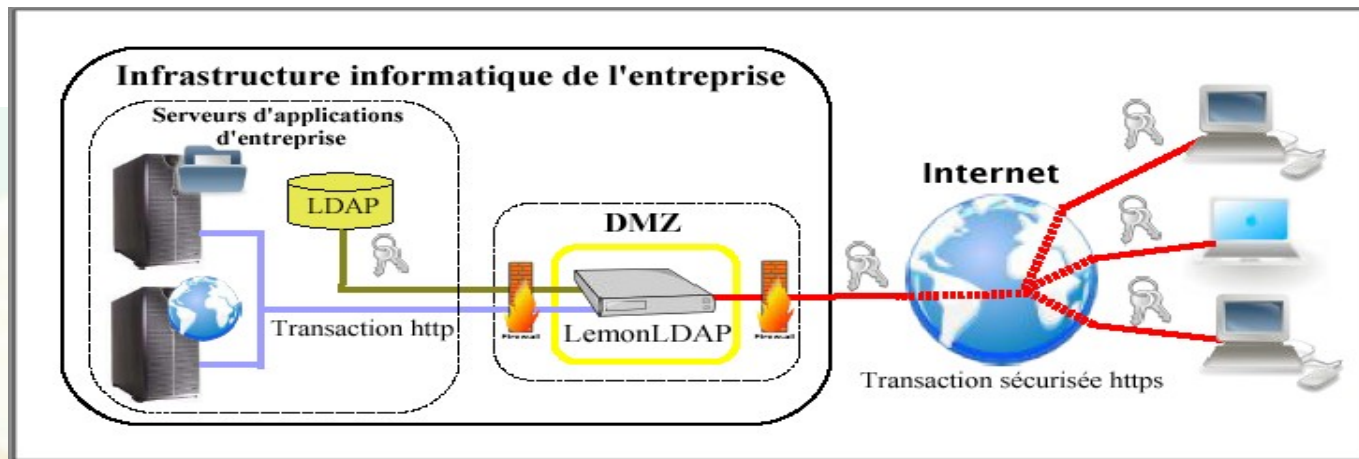
- Net-OpenID-Consumer
- Net-OpenID-Server

De Brad Fitzpatrick (memcached)



Fonctions

- Authentification
- Autorisation
- Session (memcached)
- Passerelle https ↔ http



Single Sign-On Infrastructure

Lemonldap est apache



- Mod_proxy / mod_rewrite
- Mod_ssl



- Supervision : nagios / cacti
- Logs : apache

- Evolutif (scalability)



LemonLdap
Single Sign On Infrastructure

Evolutions

- Utilisateurs

- 200.000
- 500.000
- 6 000.000 (fin juin)

- Compatibilité

- CAS (client et serveur)
- Shibboleth
- OpenID (Client et serveur)
- Kerberos /NTLM

Bonnes pratiques

Notion de cluster 'lemonldap'

- Gestion de la configuration (rsync + monit)
- Fail over (openldap/memcached)
- Répartition de charge (apache)
- Statistiques (server-status)
- Logs

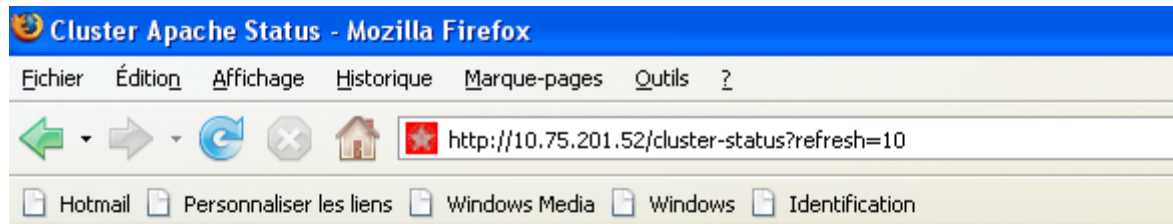
Openldap

- Mode multimaster
- Mode 'mirror' (openldap 2.4.n)
 - Promotion transparente d'un replicat en maitre .
 - Emulation du mode multimaster

Serveur de session

- Memcached
 - Simple , souple et puissant
 - Replication et répartition de charge
 - Utilisé par des très gros sites
 - Ruby on Rails

Supervision



Cluster Apache Status for oural Group

Lemonldap::Cluster::Status version: 0.01

Current Time: Wed Sep 12 10:03:36 2007

Number of Nodes: 8/8 : Status : NORMAL

Total Accesses: 241.098.971 - Total Traffic: 253.90 GB

CPU Usage: min: 0.000% max: 0.917% ave : 0.260% CPU load

258 requests currently being processed, 93 idle servers

Server	Address	Req	Idle	CPU	Accesses	Traffic
angara	10.75.15.206	64	31	0.917%	5070951	7.00GB
sylva	10.75.15.198	30	10	0.324%	6804728	14.50GB
istra	10.75.15.197	90	6	0.024%	99191774	116.60GB
oural	10.75.15.209	27	16	0.486%	7351228	15.40GB
belaya	10.75.15.100	27	14	0.321%	6888616	14.50GB
kama	10.75.15.121	7	4	0.000%	39053638	29.40GB
kolima	10.75.15.207	6	6	0.005%	38182938	23.90GB
sura	10.75.15.122	7	6	0.000%	38555098	32.60GB

article discussion modifier historique

Identification
https://pass.cp.finances.ader.gouv.fr/acct/secur/index.php?appli=1

Supervision



graphs

setting

Graphs -> Tree Mode

Presets: Last 2 Days From: 2007-09-10 13:00 To: 2007-09-12 13:00

Tree: Architecture Annuaire-> Leaf: CPU Usage

- navigation
- Accueil
 - Modifications récentes
 - Aide
 - Annuaire
 - Messagerie

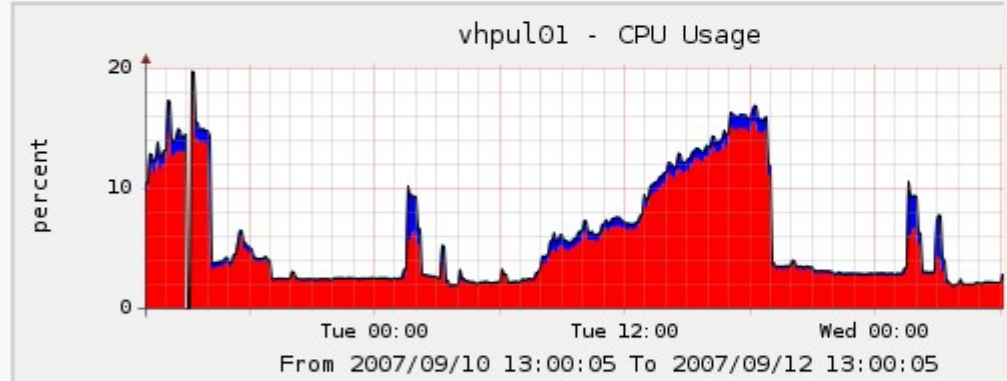
rechercher

Consulter

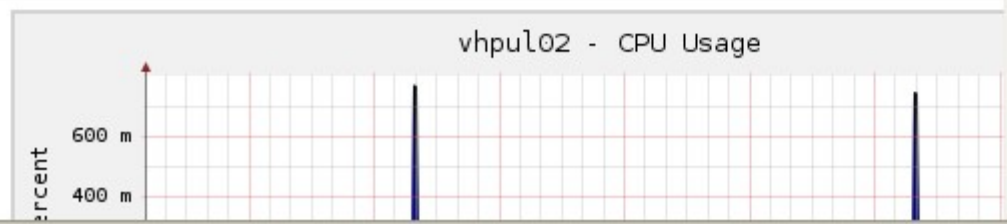
Rechercher

- boîte à outils
- Pages liées
 - Suivi des liens
 - Copier sur le serveur
 - Pages spéciales
 - Version imprimable
 - Lien permanent
 - Print as PDF

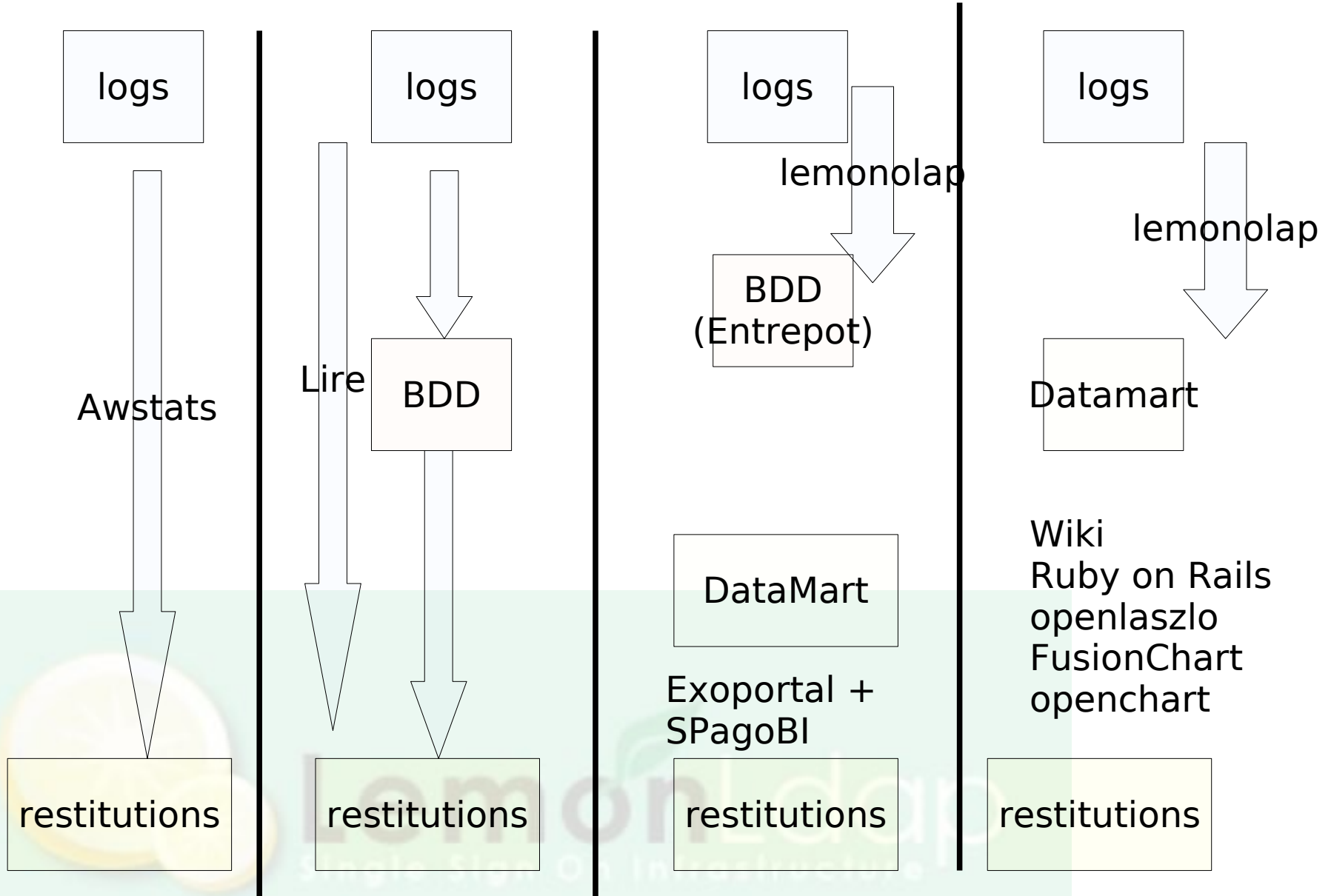
- [-] Architecture Annuaire
 - [-] CPU Usage
 - [-] Load Average
 - [-] Memory Usage
 - [-] Network Traffic
 - [-] QOS LDAP
 - [-] LDAP Operations - Proxys
 - [-] LDAP Operations - Password Storage
 - [-] LDAP Operations - Annuaire
 - [-] Connexions etablies
- [+] Architecture Annuaire (Qualification)
- [+] Architecture Brique
 - Authentication Copernic
 - Authentication Lyon
- [+] Architecture PDFEDIT
- [+] Autres
- [+] Blades Vauban
- [+] IAM
- [+] Messagerie
- [+] Reseau Paris
- [+] Reseau-DGCP-Lyon



	Current	Average	Maximum
System	7.80	5.27	18.35
User	591.18 m	585.64 m	6.46
Nice	0.00	290.36 u	51.67 m
Total	8.39	5.83	19.70



Les logs



Médiawiki

Nagios
cacti

Requeteur

Subversion

Restitutions

Plannification
GDT/scrum

Ruby on rails

Base documentaire

Conclusion

- On peut s'amuser avec le SSO.
- Permet de valider la portabilité d'une application
- Mediawiki => aller plus loin avec les Extensions
 - Mixer dans une même page des infos 'ROR' avec des infos pures wiki
- Merci

german.eric@gmail.com