

31 mars, 1er et 2 avril 2009

WebSSO, synchronisation et contrôle des accès via LDAP

Clément Oudot -
Thomas Chemineau

LINAGORA

- Synchronisation d'identités
- WebSSO et contrôle des accès
- Démonstration



- Synchronisation d'identités
 - Présentation du projet LSC
 - Principes d'une synchronisation d'identités
 - Fonctionnalités de synchronisation de LSC





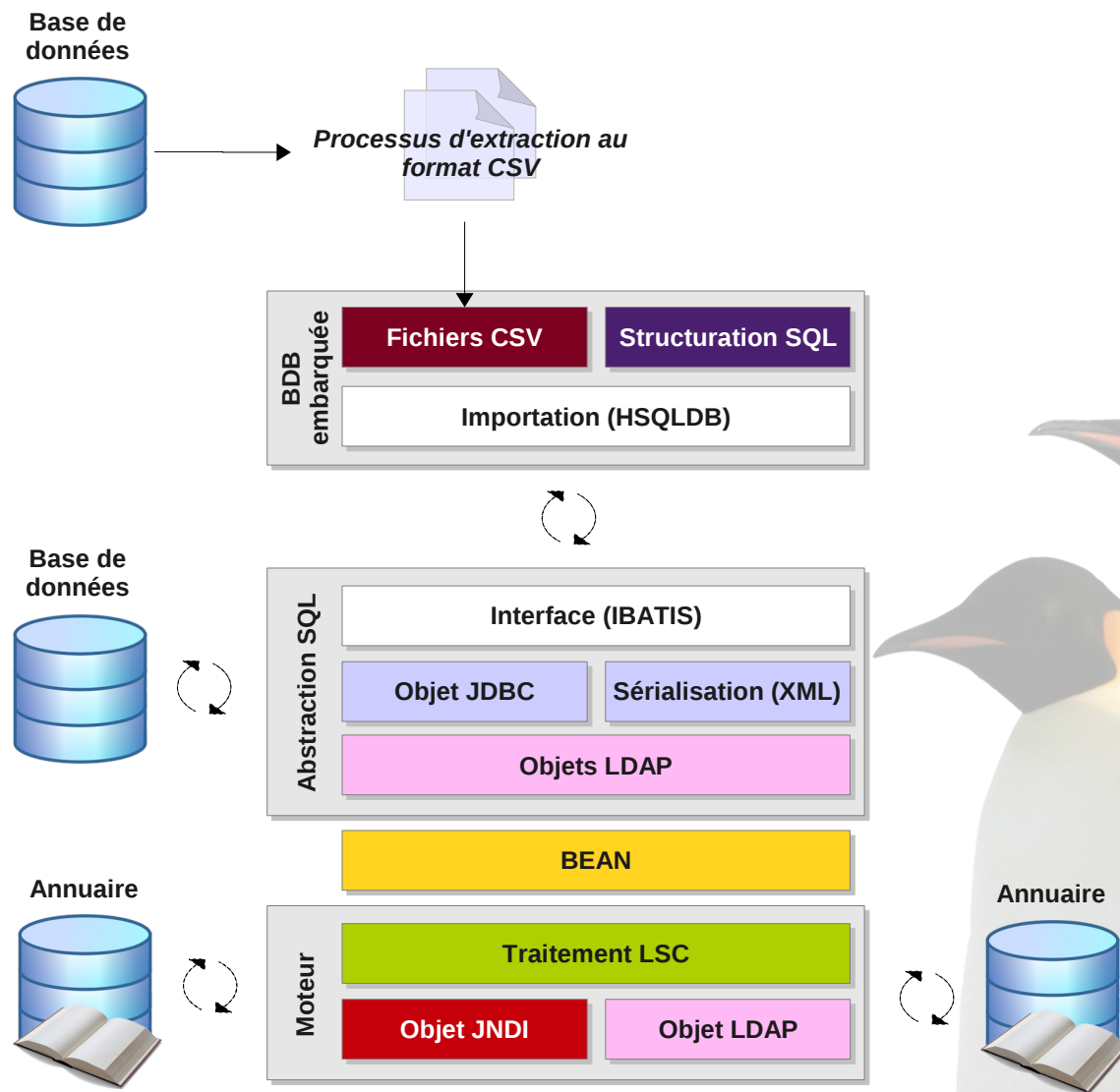
- Qu'est ce que LSC ?
 - Projet Open Source, licence BSD
 - Signifie LDAP Synchronisation Connector
 - Anciennement issu du projet InterLDAP
 - Couche applicative qui permet de synchroniser des référentiels de données divers vers un annuaire LDAP
 - Technologie : JAVA
- **Projet communautaire** : <http://lsc-project.org>

- Automatise les importations/exportations de données entre des référentiels de données et des annuaires LDAP
- Alimentation d'annuaire supportant une **base de données**, un **annuaire** ou un **fichier CSV** comme source d'alimentation
- Transformations spécifiques pour la gestion d'identités
- Optimisé pour la rapidité d'exécution pour permettre une synchronisation continue

- Deux niveaux d'information sur une identité :
 - L'existence d'une identité elle même
 - Les données spécifiques à chaque identité
- Opérations de synchronisation :
 - Création : report des nouvelles identités
 - Suppression : retrait des identités supprimées
 - Mise à jour : pour une identité existant de part et d'autre, recopie des données spécifiques

- Des critères de synchronisation
 - Type de la source (LDAP / base de données / CSV)
 - Identification de la population ciblée
 - Mapping et transformation des attributs sources – destination
 - Actions différentes selon les opérations (création / mise à jour / suppression)

- 3 niveaux de synchronisation :
 - Base de données vers annuaire LDAP
 - Fichier plat au format CSV vers annuaire LDAP
 - Annuaire vers annuaire (ex : LDAP vers AD)



- Les sources de synchronisation peuvent être de différentes natures (SGBD, LDAP)
- Différents formats d'entrées :
 - CSV : données injectées dans une base embarquée (HSQLDB)
 - LDIF : données injectées dans un annuaire embarqué (OpenDS)

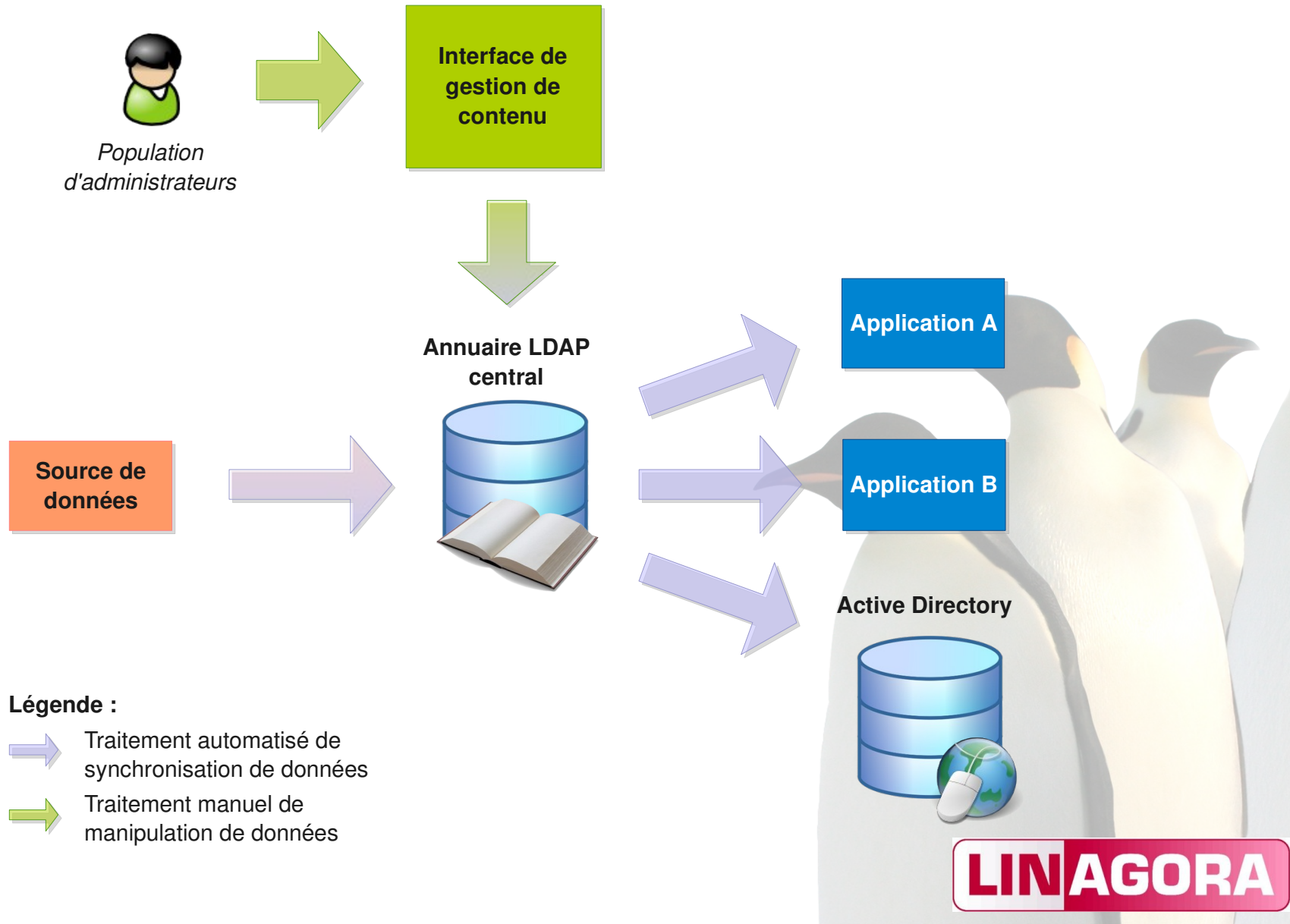


- Les synchronisations génèrent des rapports détaillés, sous différents formats :
 - CSV : les modifications apportées sur l'annuaire sont journalisées au format CSV
 - LDIF : les modifications apportées sur l'annuaire sont journalisées au format LDIF
- Différents niveaux de traçabilités et choix des opérations LDAP à tracer

- Des traitements simples, comme :
 - Concaténation de plusieurs attributs sources
 - Séparation des valeurs multiples d'un champ source vers un attribut LDAP multivalué cible
 - Suppression des caractères diacritiques
- Des traitements avancés, comme :
 - Tests d'existence des DN
 - Peuplement avancé des attributs
 - Prise en charge d'Active Directory

- Indispensable pour peupler les utilisateurs d'AD
- UserAccountControl permet de spécifier l'état d'un compte utilisateur, par exemple :
 - ACCOUNTDISABLE
 - PASSWORD_CANT_CHANGE
 - PASSWORD_EXPIRED
- Prise en charge de la synchronisation du mot de passe sur un flux SSL

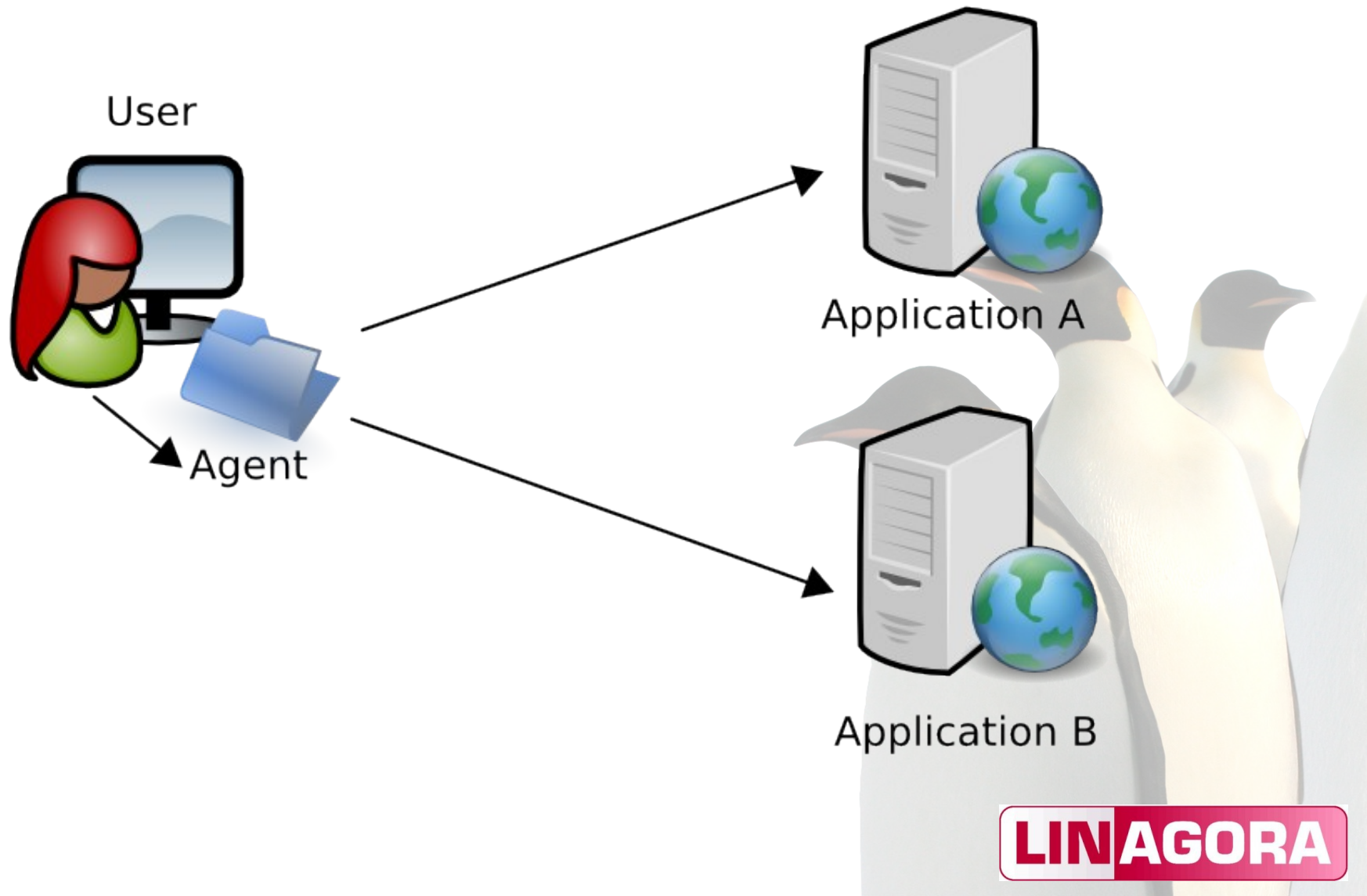


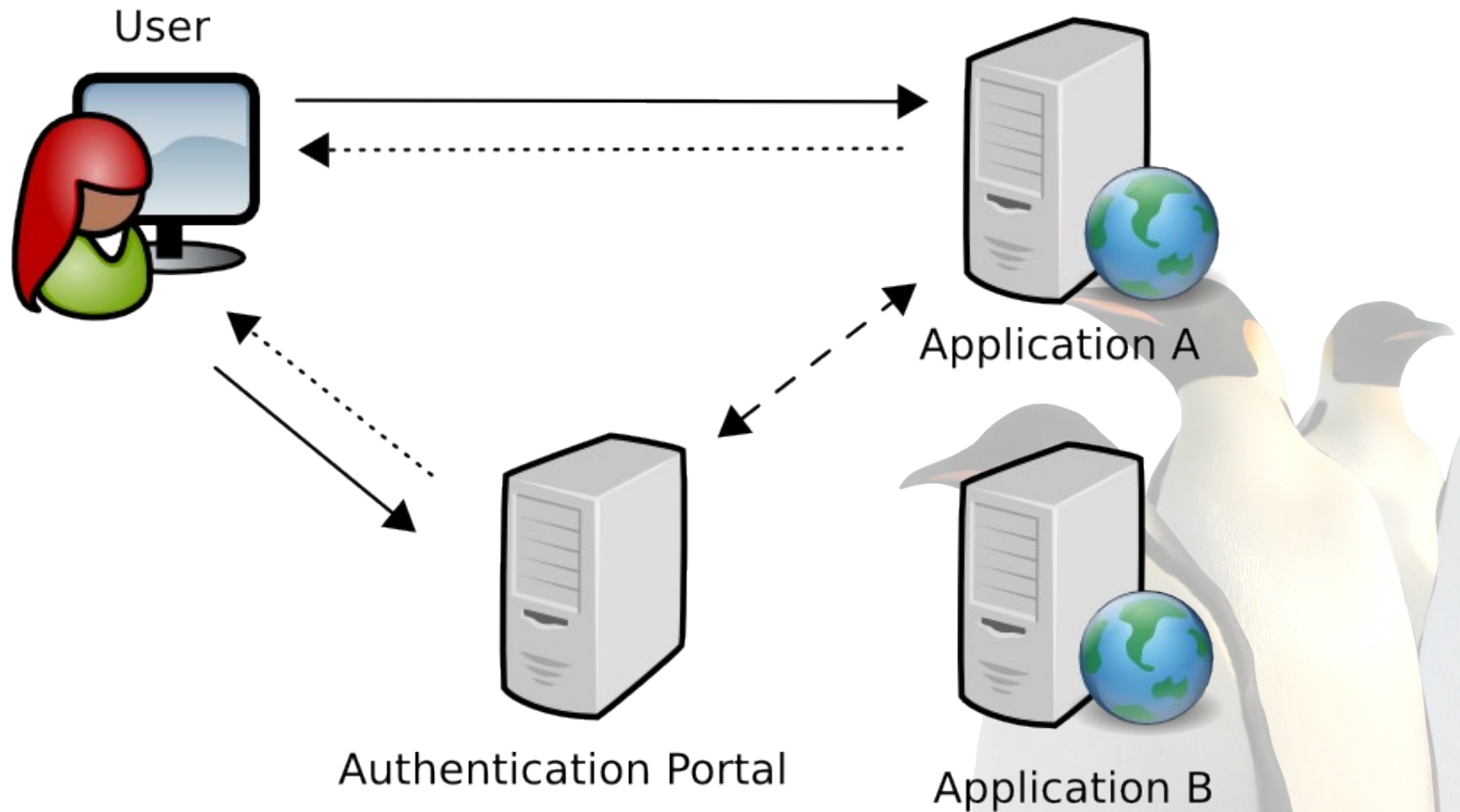


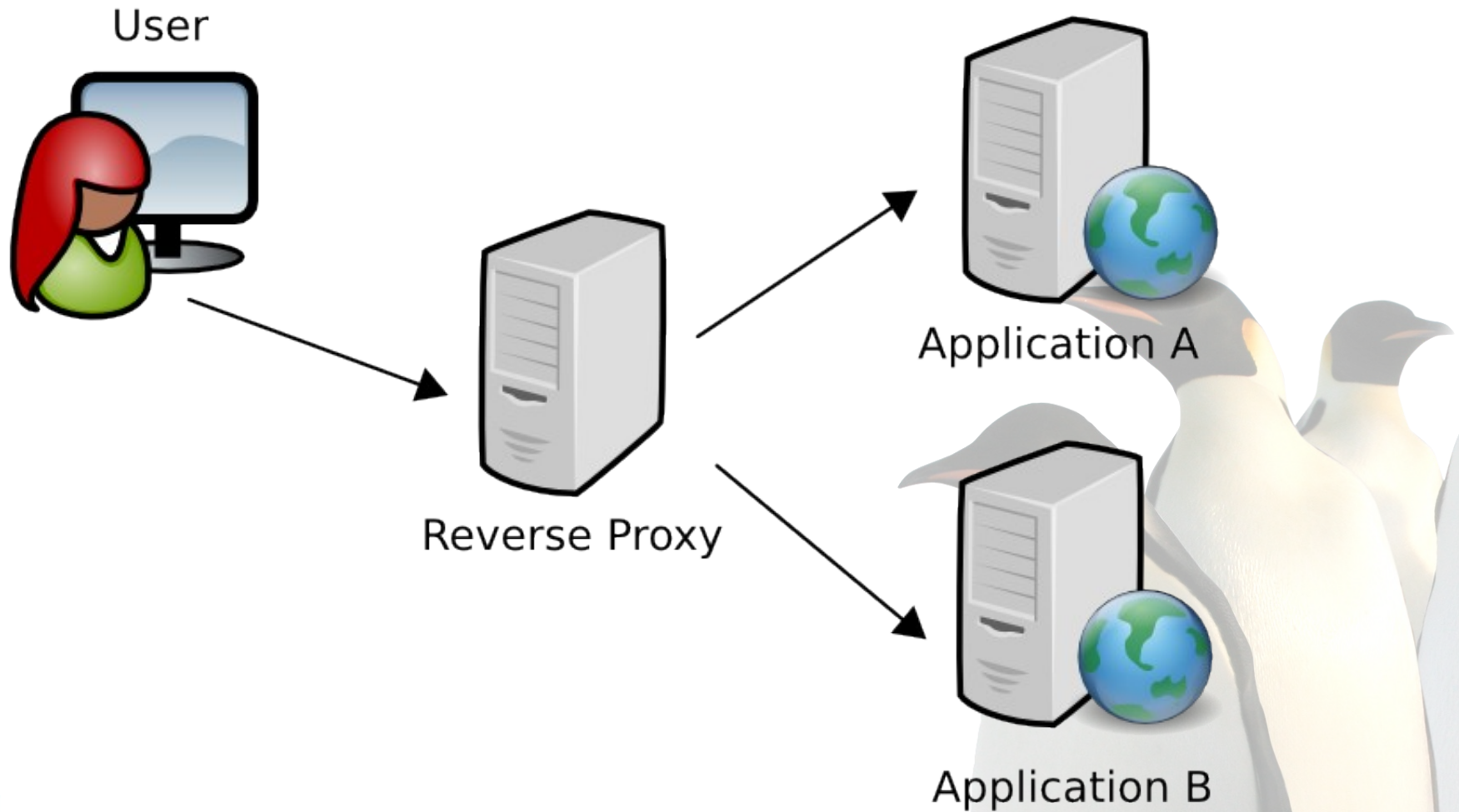
- WebSSO et gestion des accès
 - Concepts et définition du WebSSO
 - Présentation de LemonLDAP::NG
 - X-domain et Liberty Alliance



- SSO signifie « Single Sign On », qui peut se traduire en français par « authentification unique ».
- Le SSO regroupe plusieurs fonctionnalités :
 - Couple identifiant/mot de passe unique
 - Transmission transparente des informations de session aux applications
 - Gestion des profils applicatifs, c'est-à-dire qui accède à quoi









```
GET http://www.linagora.com HTTP/1.1
Accept: text/html
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.7.6)
```

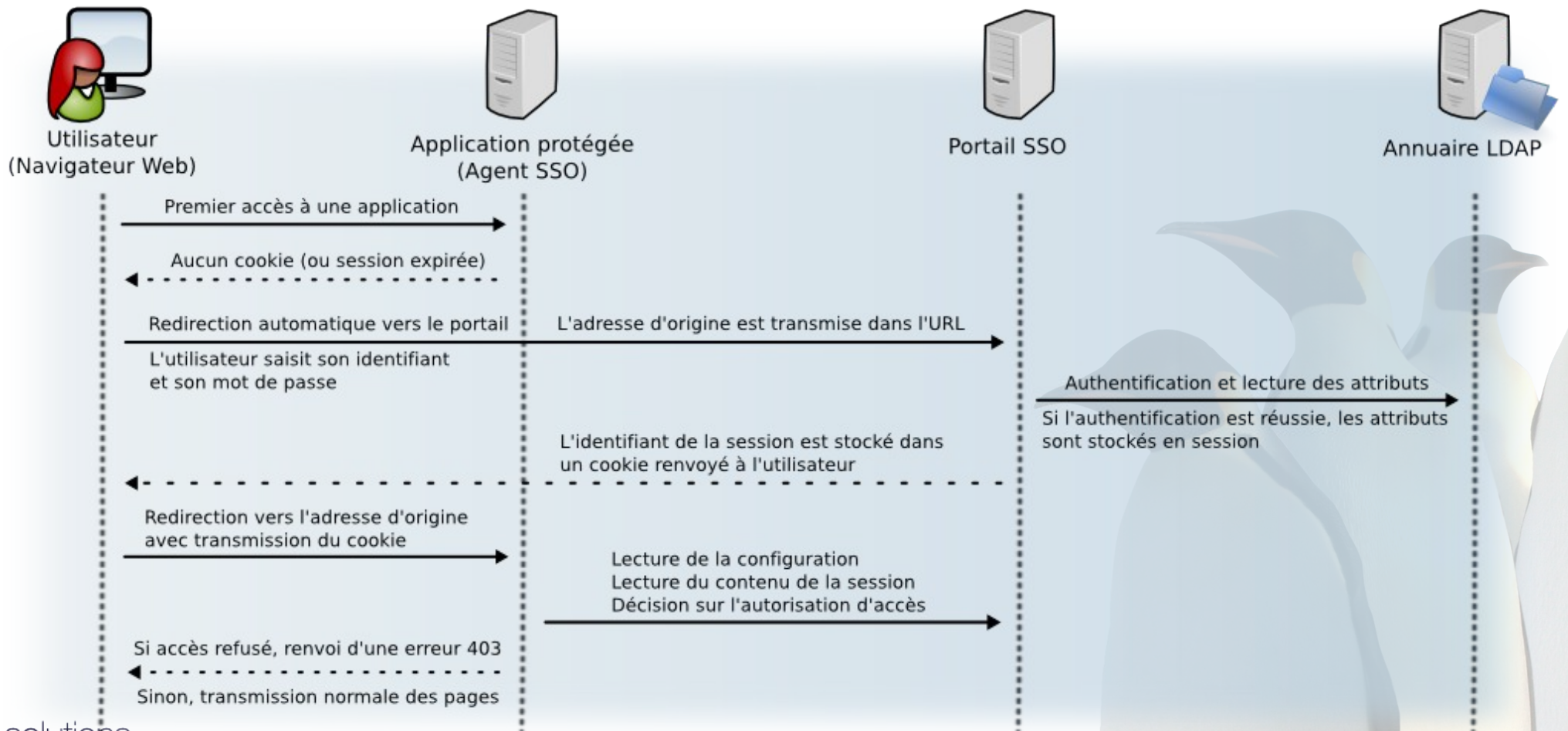
```
HTTP/1.1 200 OK
Date: Thu, 13 Mar 2008 15:05:29 GMT
Server: Apache
Content-Length: 264
Content-Type: text/html; charset=iso-8859-1

<?xml version="1.0" encoding="iso-8859-1" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="fr" xml:lang="fr" dir="ltr">
<head>
<title>Linagora, integrateur de reference sur le marche des logiciels libres</title>

...
</html>
```

- LemonLDAP est un ensemble de scripts et de modules Perl utilisés à travers mod_perl et le serveur HTTP Apache
- LemonLDAP et LemonLDAP::NG sont des logiciels libres, les projets sont hébergés chez OW2 : <http://lemonldap.objectweb.org>
- LemonLDAP a été créé par Eric German, du Ministère des Finances
- La version ::NG a été écrite par Xavier Guimard, de la Gendarmerie Nationale

- Le principe général est d'utiliser un annuaire LDAP pour :
 - authentifier l'utilisateur (vérification du mot de passe)
 - effectuer un contrôle d'accès (selon les attributs LDAP de l'utilisateur)
 - approvisionner les applications (par transmissions des attributs LDAP dans les entêtes HTTP)
- LemonLDAP::NG a été choisi pour le projet FederID (<http://www.federid.org>)

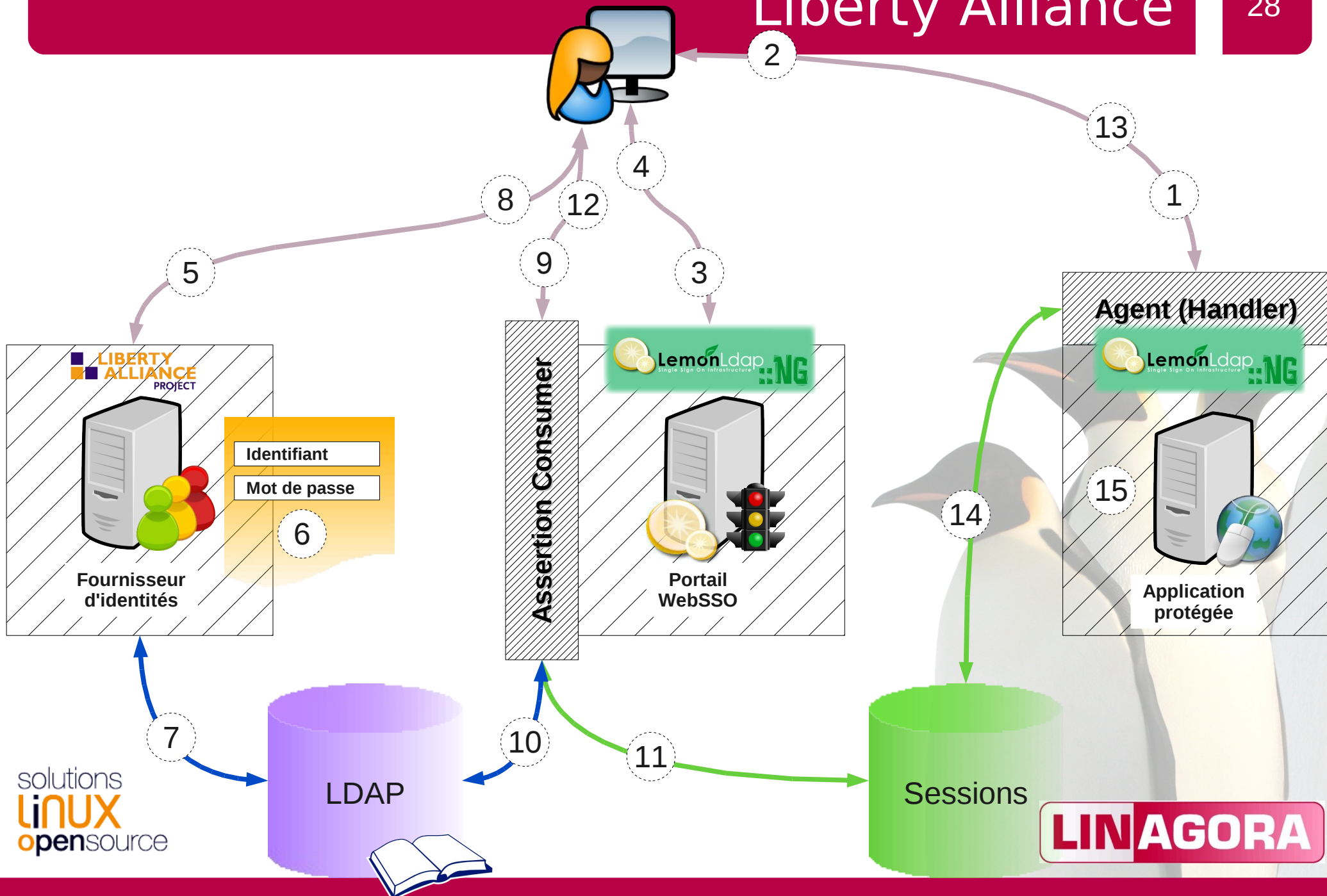


- Pré-requis :
 - Accès au code source et possibilité de le modifier
 - disposer d'un langage permettant la lecture des en-têtes HTTP
- Désactiver le formulaire d'authentification local
- Lire les en-têtes HTTP, en particulier celle fournissant l'identité de l'utilisateur

- Utilisation du Manager pour créer un nouvel hôte virtuel dans la configuration LemonLDAP::NG :
 - Nom de l'hôte virtuel
 - Règles d'accès
 - Informations transmises
- Configuration du serveur Apache2 :
 - Ajout d'un hôte virtuel ou reprise de l'existant
 - Ajout des paramètres d'appel du Handler

- Un domaine est constitué d'un nom (linagora, yahoo, google, ...) et d'une extension, appelée aussi suffixe (fr, de, com, net, ...).
- La spécification des cookies précise qu'un cookie doit être déclaré sur un domaine et envoyé à aucun autre. Les navigateurs refusent d'ailleurs de transmettre un cookie à un domaine différent de celui qui l'a émis.
- Certaines applications sont parfois réparties sur plusieurs domaines, elles utilisent alors des mécanismes dits de « cross-domain ».

- Plusieurs solutions techniques permettent de faire du cross-domain, la plus répandue consiste à faire transiter le numéro de session dans l'URL.
- L'architecture cross-domain suppose généralement l'existence d'un serveur maître unique, réalisant l'authentification et la mise en session des informations, et de un ou plusieurs esclaves, utilisant le numéro de session transmis pour retrouver les informations.



Passons à la pratique !



Merci de votre attention

**Retrouvez-nous
sur notre stand B25 !**