Utilisation de WebDAV dans ESUP-Portail

JRES 2005 marseille

Thomas Bellembois Thomas.Bellembois@univ-rennes1.fr
Raymond Bourges Raymond.Bourges@univ-rennes1.fr
Yohan Colmant Yohan.Colmant@univ-valenciennes.fr

ESUP Portail

Plan

- Introduction
- Parlons WebDAV
  - Client
  - Serveur
- Conclusion

ESUP-Portail

- Consortium d'universités Françaises de promotion d'une solution Open Source d'espace numérique de travail
- 50 établissements ont choisi cette solution
- Pour en savoir plus
  - Site Web
    - http://esup-portail.org
  - Listes
    - http://listes.esup-portail.org/sympa
  - Espace développeurs
    - http://sourcesup.cru.fr/projects/esup

Démarche

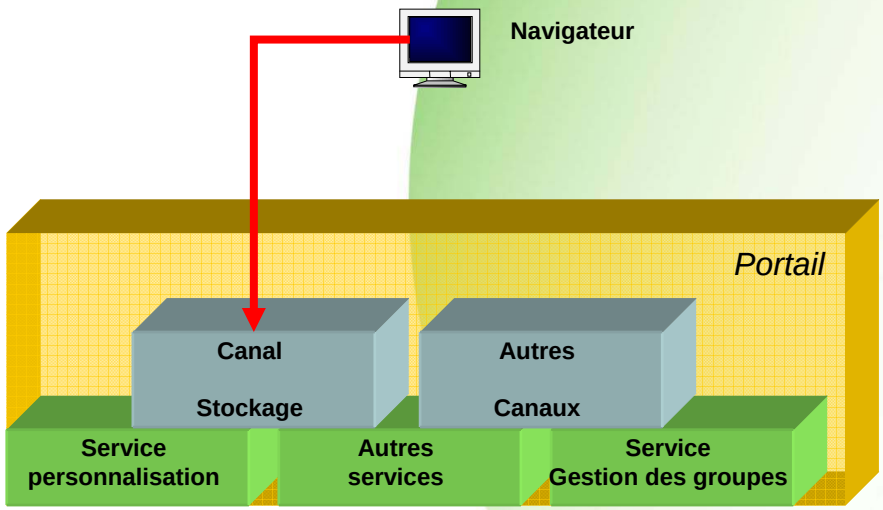
- Offrir un service de stockage
- Un client intégré au portail
  - Accès distant
  - Accès à toutes les ressources de stockage
  - Utiliser les fonctionnalités avancées du serveur de stockage ESUP
- Un serveur
  - Identification riche (notamment SSO)
  - Utilisation des groupes du portail
  - Gestion de la délégation des droits d'accès

Pourquoi WebDAV

- Naturellement bien adapté à des accès distants
- Accès possible depuis un client intégré au portail comme depuis les systèmes d'exploitation
- Pas forcément très performant (WebDAV ne remplace pas encore tous les autres systèmes de fichiers réseaux)
- Mais il est bien adapté à un grand nombre d'utilisateurs

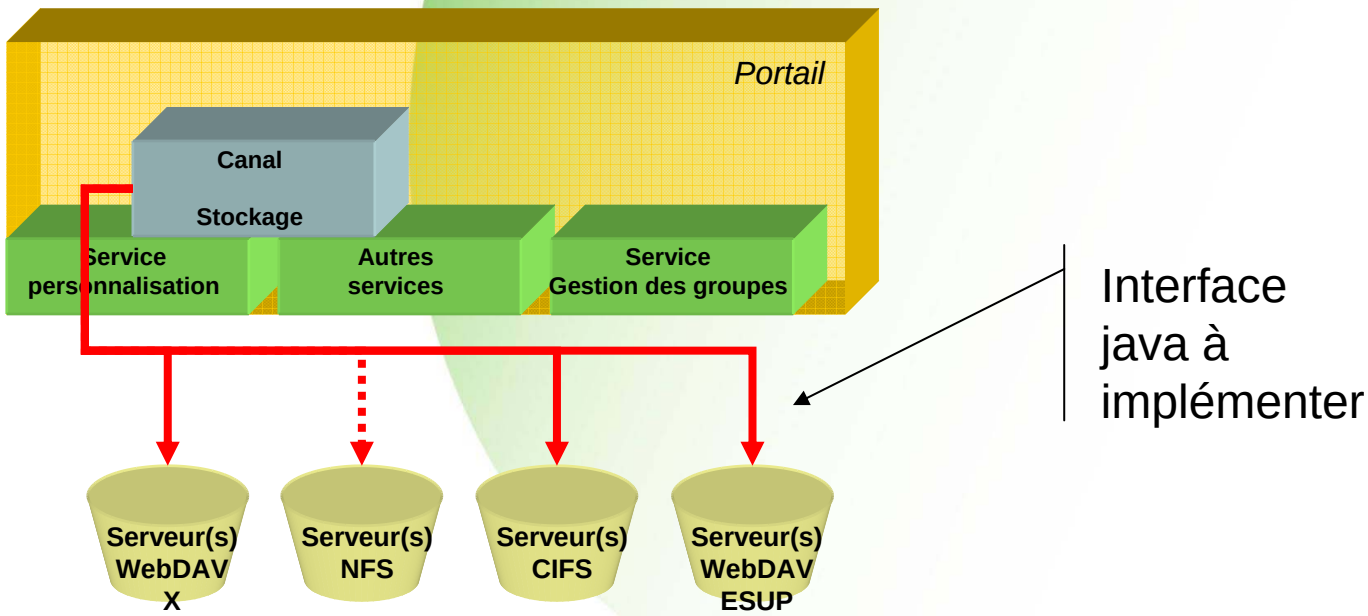
Bien comprendre la démarche

- Le portail (basé sur uPortal) et les canaux



Bien comprendre la démarche

- Canal permettant d'accéder à distance à toutes les ressources de stockage



Parlons WebDAV

Yohan

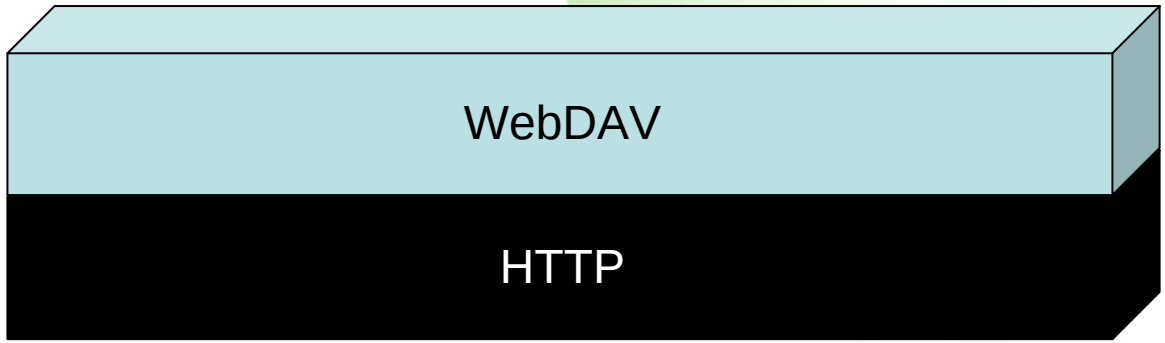
- Canal Stockage
  - Protocole WebDAV
  - Métadonnées
  - ACP

Thomas

- Serveur WebDAV ESUP
  - Authentification
  - Gestion des groupes
  - Quotas

Le protocole WebDAV

- Web-based Distributed Authoring and Versioning
  - Gestion de ressources distantes
    - Lecture et **écriture** à travers le WEB
  - Extension du protocole HTTP
    - Ajout de méthodes
      - MKCOL, COPY, MOVE, PROPFIND, PROPPATCH, LOCK
      - Utilisent XML comme format de requête et de réponse

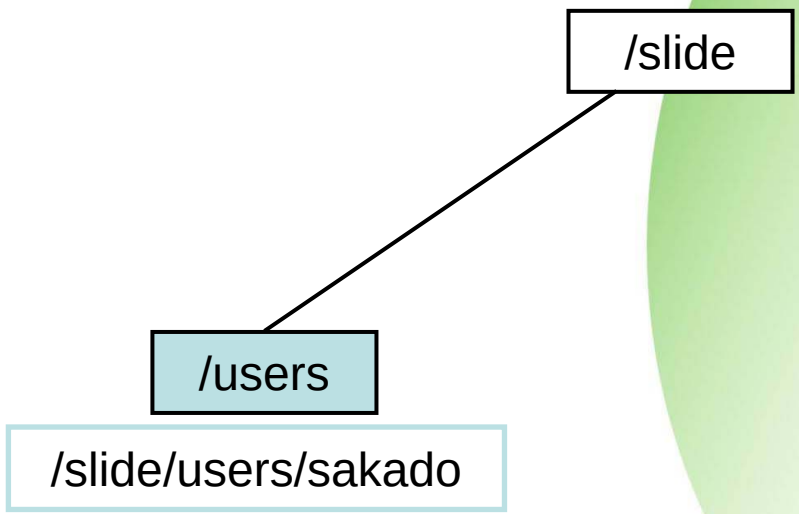


Le protocole WebDAV

- Ressources
  - Qu'est-ce qu'une ressource WebDAV ?
    - Tout objet pouvant être identifié par une URI
  - Tout est ressource dans WebDAV
    - Fichier, collection (répertoire), utilisateur, groupe
    - Les groupes sont des ressources qui référencent un ensemble d'utilisateurs et/ou d'autres groupes

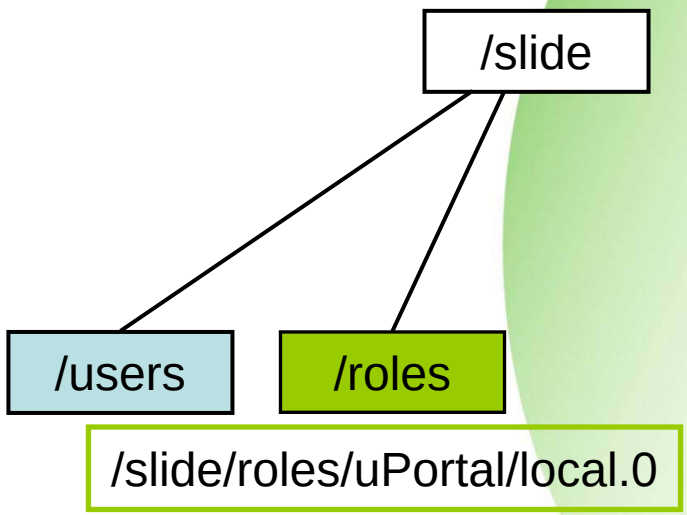
Le protocole WebDAV

- Arborescence du serveur WebDAV ESUP-Portail



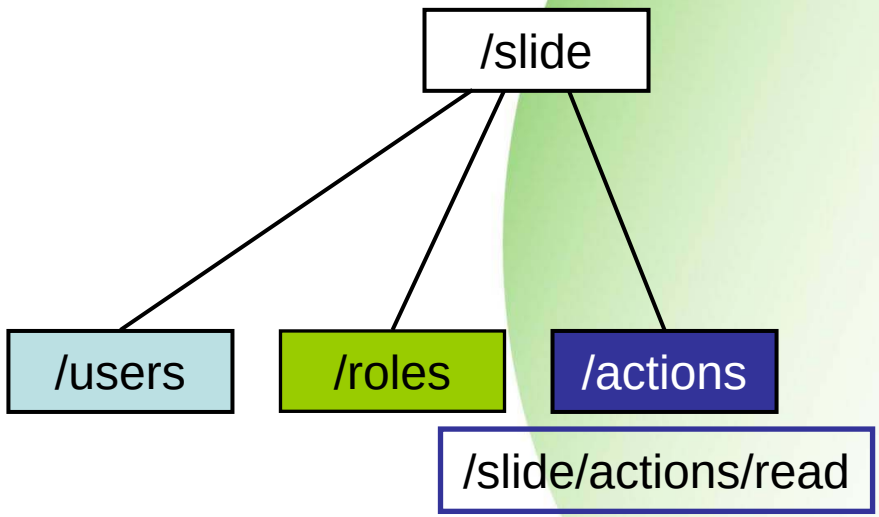
Le protocole WebDAV

- Arborescence du serveur WebDAV ESUP-Portail



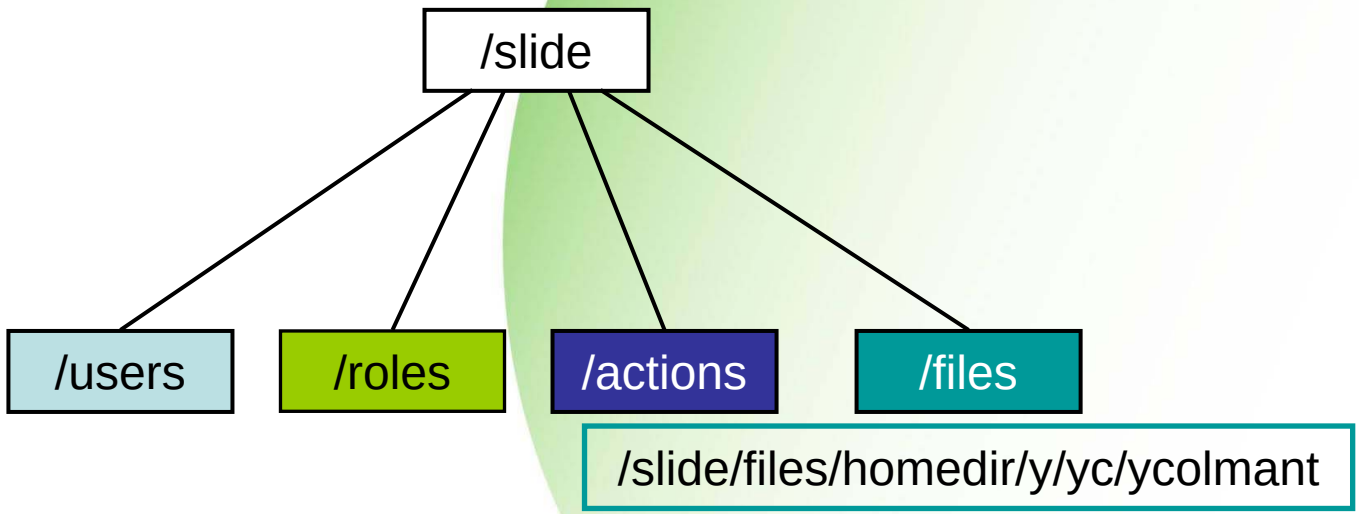
Le protocole WebDAV

- Arborescence du serveur WebDAV ESUP-Portail



Le protocole WebDAV

- Arborescence du serveur WebDAV ESUP-Portail

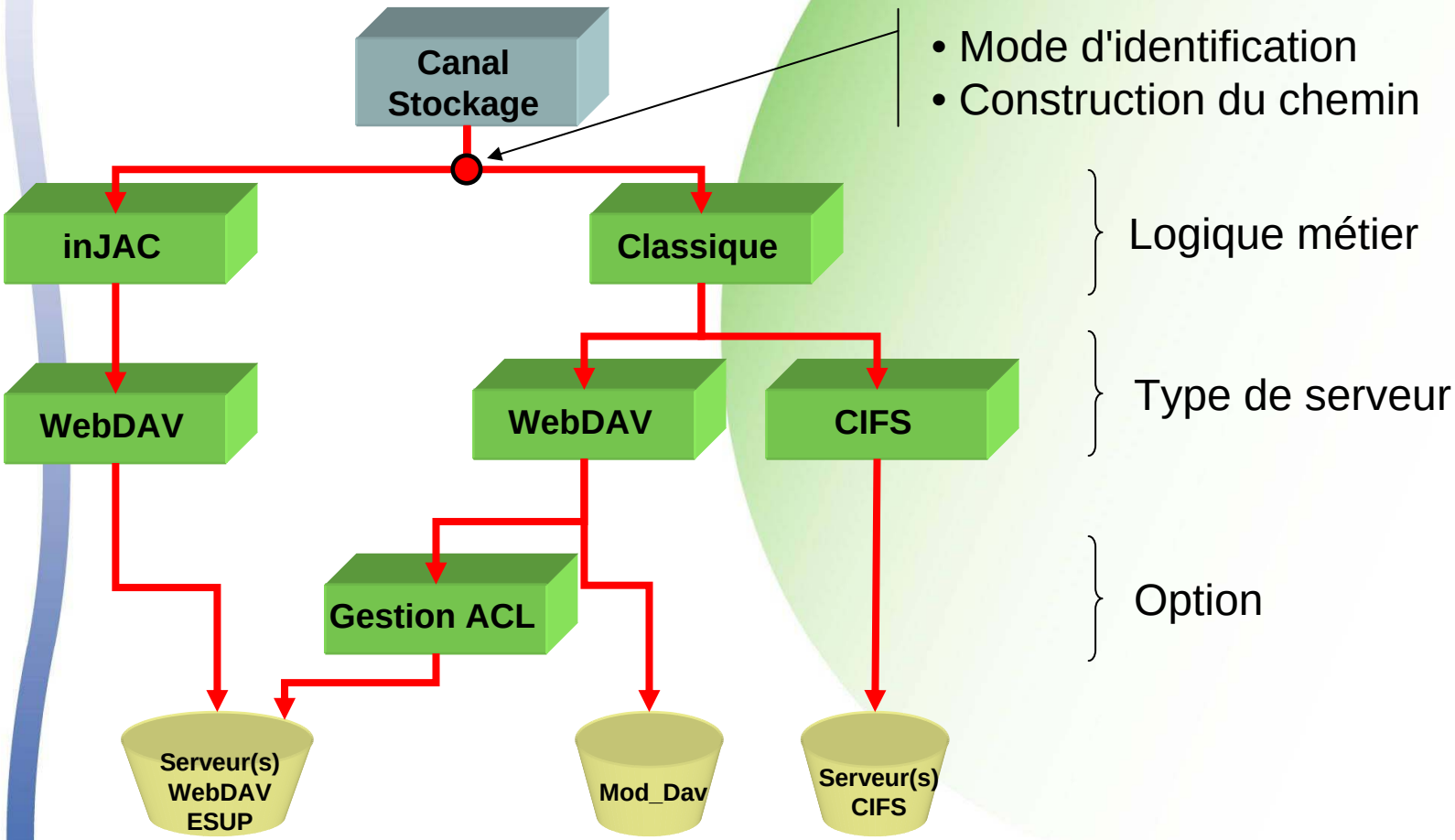


Le client : le canal stockage

- Généralités
  - Intégré à ESUP-Portail
  - Accès à des espaces personnels et/ou partagés
- Fonctionnalités
  - Gestion « classique » d'espaces de stockage
    - Dépôt/création de fichiers et dossiers
    - Gestion de documents (copier/couper/coller, etc.)
    - Partage de dossiers
  - Mode spécifique au référencement de documents inJAC
    - Gère toutes les étapes du *workflow*
    - Saisie de métadonnées

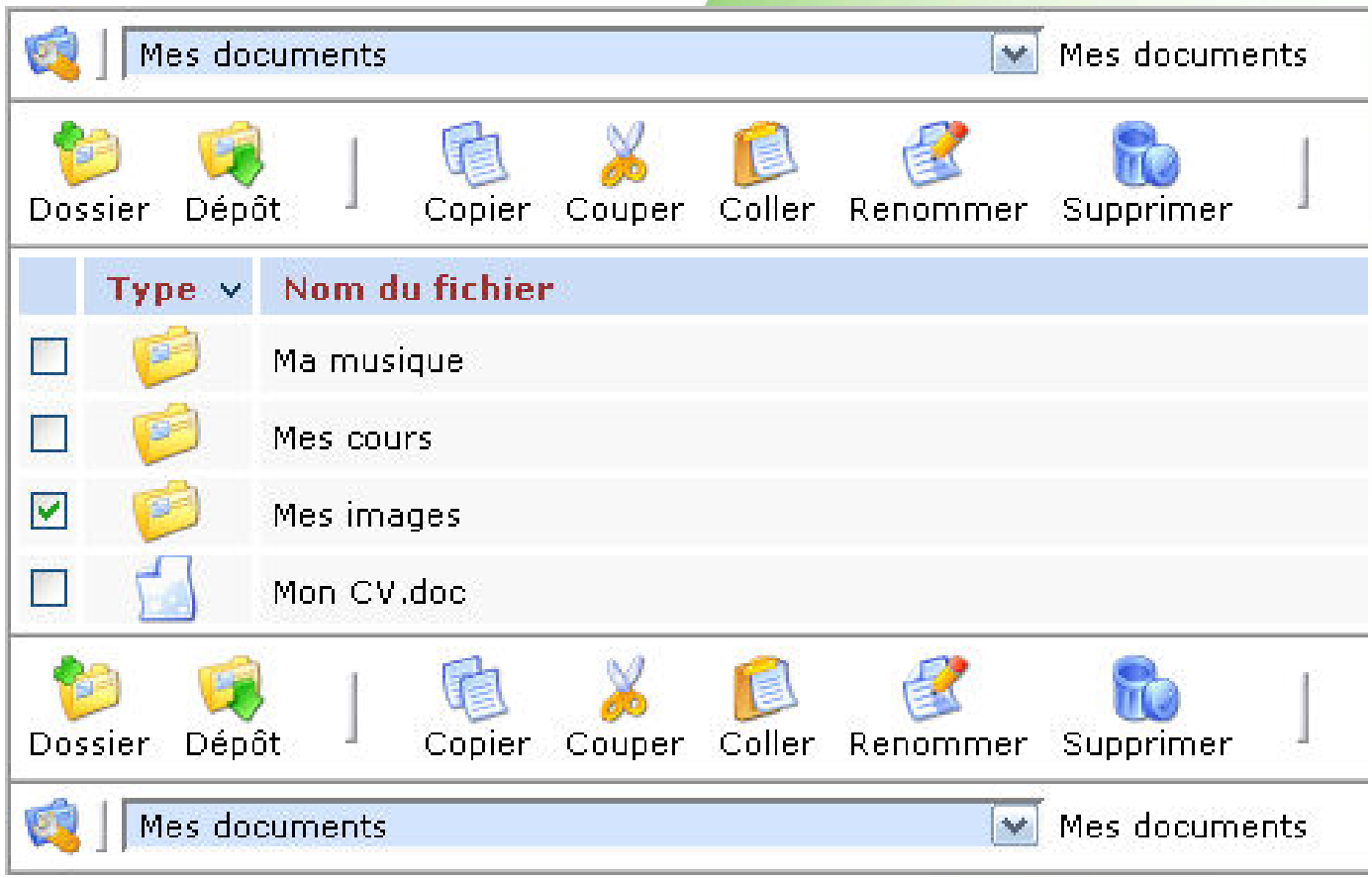
Le client : le canal stockage

- Conception modulaire

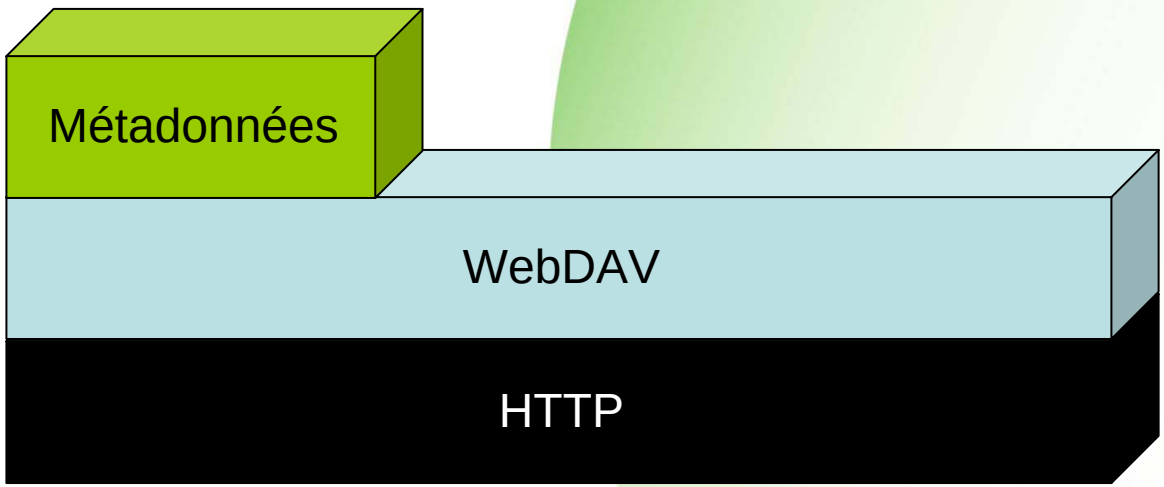


Le client : le canal stockage

- Interface du canal stockage



Les métadonnées



Les métadonnées

- Représentation de l'information relative aux ressources
  - Nom, date de création, …
- Méthodes WebDAV
  - PROPFIND pour l'interrogation
  - PROPPATCH pour la modification
- Concrètement
  - MD attachées aux ressources
    - Formalisme XML
    - Base de données

Les métadonnées

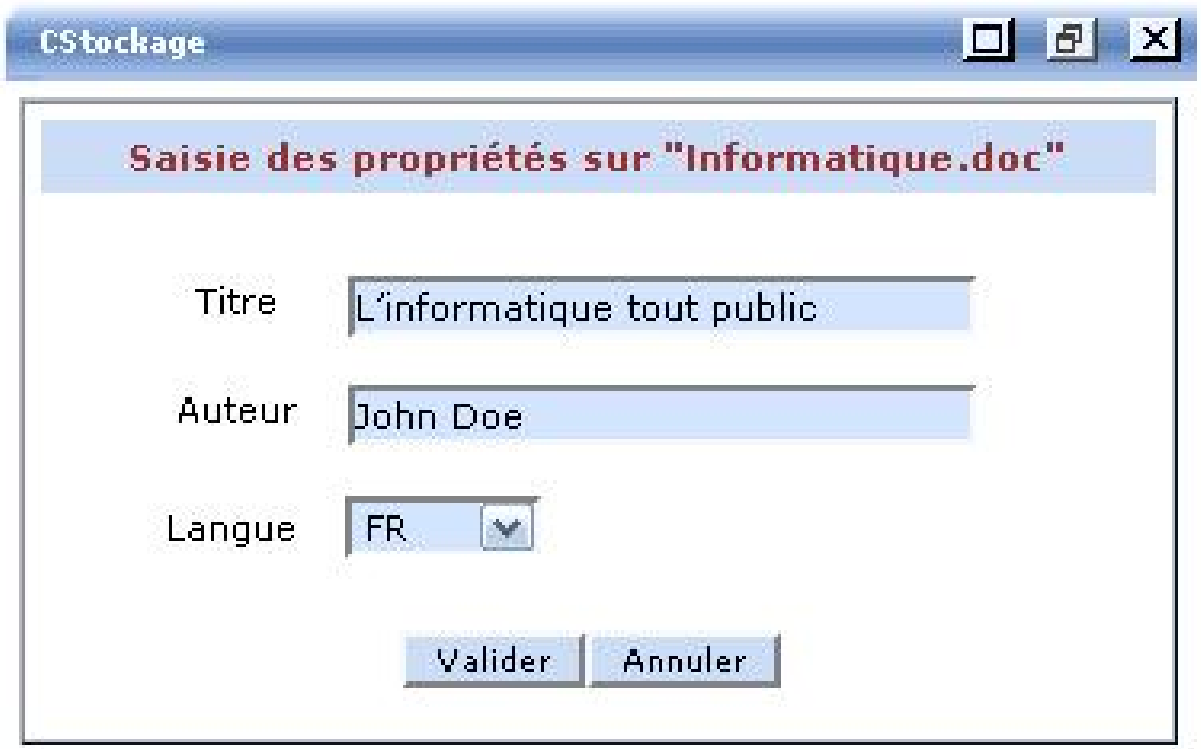
- MD vivante ou morte ?
  - Vivante : gérée par le serveur (Ex : taille de fichier)
  - Morte : fixée librement par le client
- MD protégée ou non protégée ?
  - Protégée : ne peut être modifiée par un PROPPATCH
- Exemple de requête/réponse sur la métadonnée `title`

```
<?xml version="1.0" ... ?>
<D:propfind xmlns:D="DAV:">
  <D:prop>
    <title/>
  </D:prop>
</D:propfind>
```

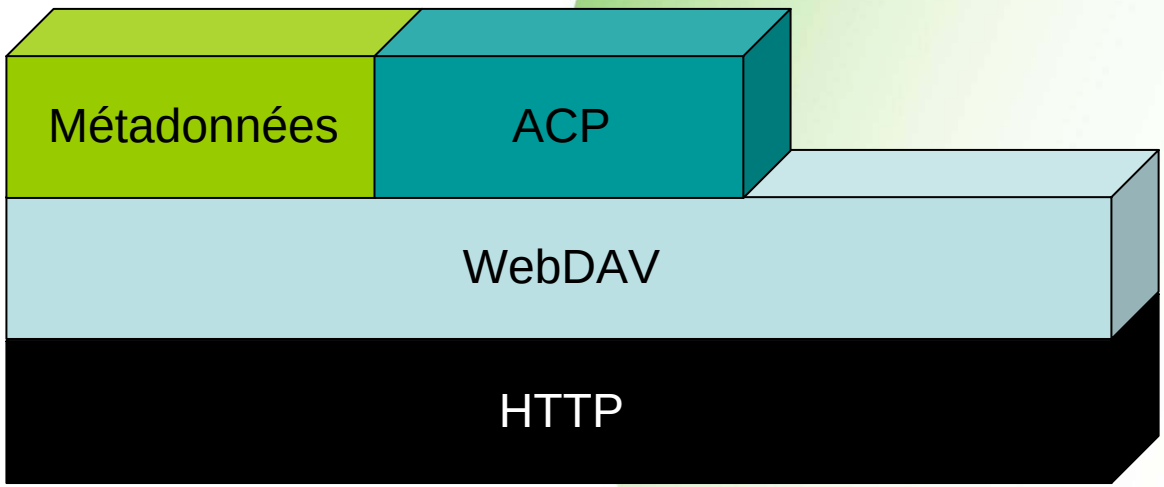
```
<?xml version="1.0" ... ?>
<multistatus xmlns="DAV:">
  <response>
    <href>/CV.doc</href>
    <propstat>
      <prop>
        <title>Mon CV</title>
      </prop>
    </propstat>
  </response>
</multistatus>
```

Les métadonnées

- Interface de saisie des métadonnées



Le contrôle d’accès



Le contrôle d'accès

- ACP (Access Control Protocol)
  - Extension du protocole WebDAV
  - Contrôle d'accès interopérable entre serveurs WebDAV
- Concrètement
  - ACL et ACE
    - ACE (Access Control Element) : associe des droits d'accès à un principal donné
    - ACL (Access Control List) = liste d'ACE
    - Une ACL par ressource
  - Une ACL est une MD particulière
  - Différents privilèges : read, write, read-acl, …

Le contrôle d'accès

- Exemple d'ACL sur le serveur WebDAV ESUP

```
<permissions>
    <permission subjectUri="/users/ycolmant"        actionUri="/actions/write" negative="false" />
    <permission subjectUri="/roles/uPortal/local.0" actionUri="/actions/read"  negative="false" />
    <permission subjectUri="all"                    actionUri="all"            negative="true" />
</permissions>
```

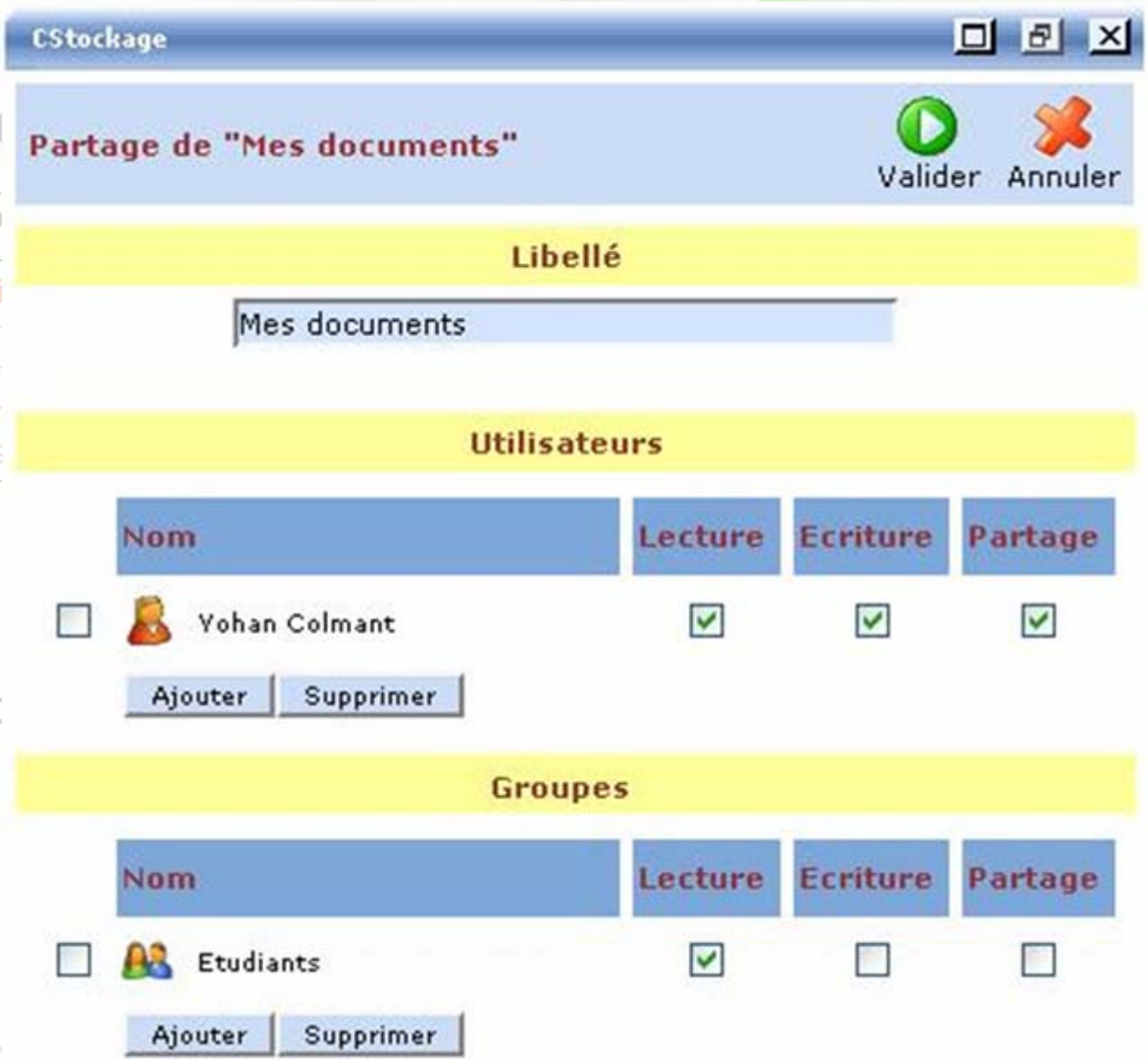
- Développements autour d'ACP
  - Partage de dossiers dans le canal stockage

Le contrôle d'accès

- Ex / ES

```
<permissi
    <pern                                   e="false" />
    <pern                                   e="false" />
    <pern                                   e="true" />
</permiss
```

- Dé
  - F je



Le contrôle d'accès

- Exemple d'ACL sur le serveur WebDAV ESUP

```
<permissions>
    <permission subjectUri="/users/ycolmant"        actionUri="/actions/write" negative="false" />
    <permission subjectUri="/roles/uPortal/local.0" actionUri="/actions/read"  negative="false" />
    <permission subjectUri="all"                    actionUri="all"            negative="true" />
</permissions>
```

- Développements autour d'ACP
  - Partage de dossiers dans le canal stockage
  - Gestion des droits relative aux documents inJAC

Serveur WebDAV - Introduction

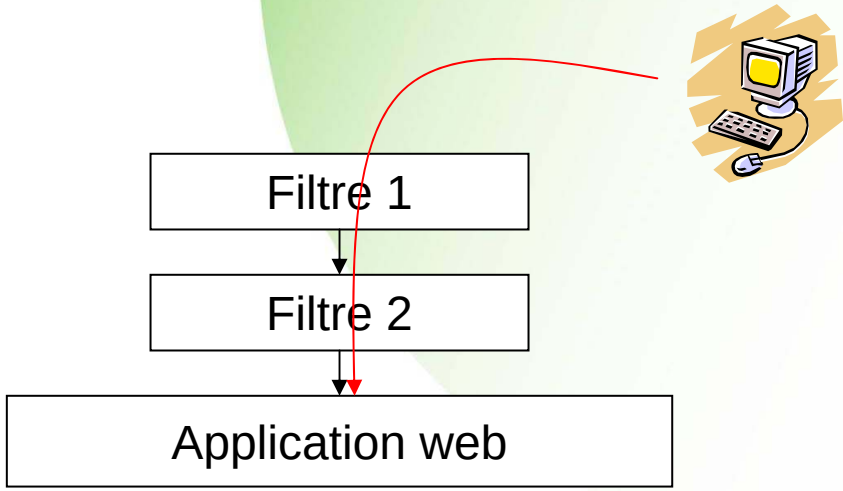
- Basé sur le serveur WebDAV Jakarta Slide
  - Conforme à la RFC WebDAV (2518)
  - Supporte ACP, la gestion de versions et les verrous
  - Différents supports possibles pour le stockage des données (notion de *stores*)
- Ajouts ESUP
  - Couche d'authentification multiple
  - Rattachement aux groupes du portail ESUP
  - Gestion des quotas
  - Gestion de la fédération d'identité (futur)

Serveur WebDAV - Authentification

- Par défaut dans Slide base d'utilisateurs interne (*Realm* Tomcat)
  - Peu flexible, difficilement administrable et dépendant de Tomcat
- Volonté d'ESUP
  - Couche d'authentification multiple (LDAP, SSO et *Trusted*)
  - Indépendante du conteneur d'applications

Serveur WebDAV - Authentification

- Idée : utilisation de filtres J2EE
  - Filtres d'interception
  - Prétraitement d'une requête HTTP provenant d'un client web vers une application web
  - Peuvent être cascadés



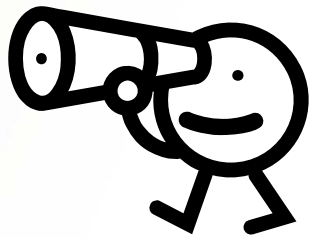
Serveur WebDAV - Authentification

4 filtres

- Filtre LDAP (ESUP)
- Filtre CAS (Université de Yale, JA-SIG)
- Filtre *Trusted* (ESUP)
  - Authentification depuis des serveurs de confiance
  - Mot de passe partagé et/ou utilisateurs autorisés

et

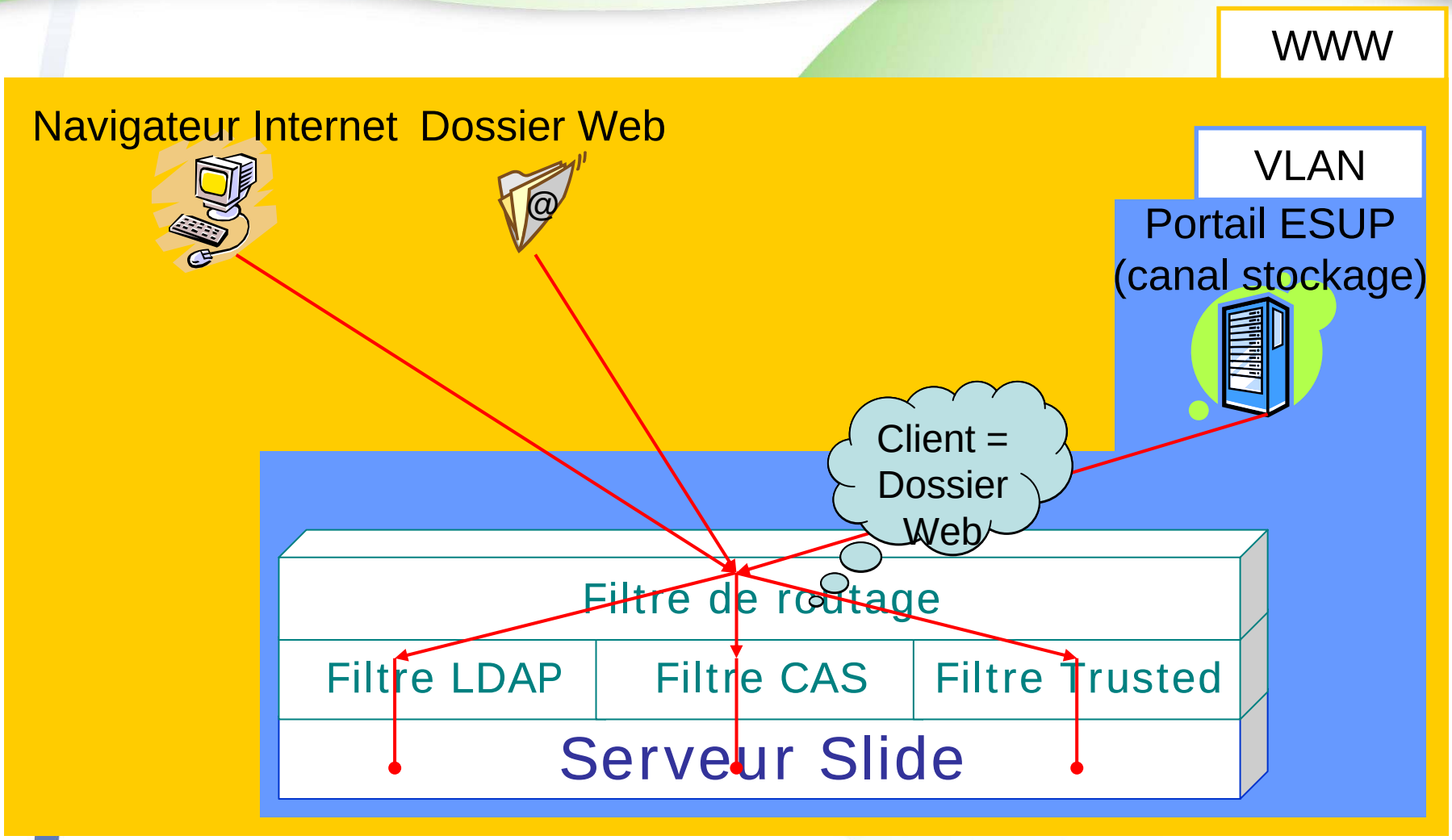
- Filtre de routage pour la sélection



Serveur WebDAV - Authentification

- Le filtre de routage
  - Dirige les requêtes vers le filtre approprié
  - Critères de sélection multiples
    - Adresse IP du client
    - Nom d'hôte destinataire
    - Agent client (navigateur web, application…)
    - …

Serveur WebDAV - Authentification



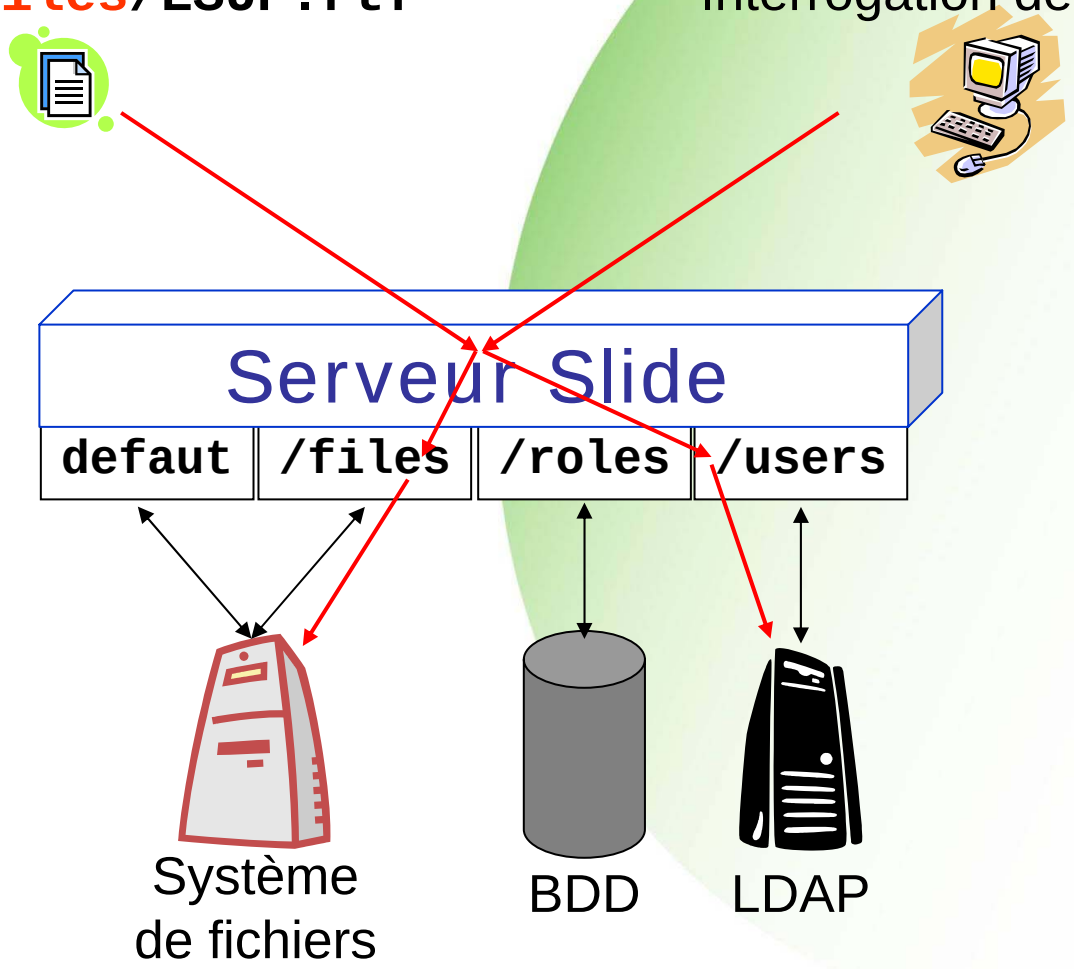
Serveur WebDAV - Notion de store

- Slide : différents supports possibles pour le stockage des données et MD (notion de *store*)
- Plus précisément
  - Définition d'un mode de stockage pour un *pattern* d'URL donné
  - Exemple
    - Ressources sous **`/files`** stockées sur un système de fichiers classique
    - Ressources sous **`/users`** stockées dans un LDAP
    - Ressources sous **`/roles`** stockées en BDD

Serveur WebDAV - Notion de store

Dépôt de **/files/ESUP.rtf**

Interrogation de **/users**



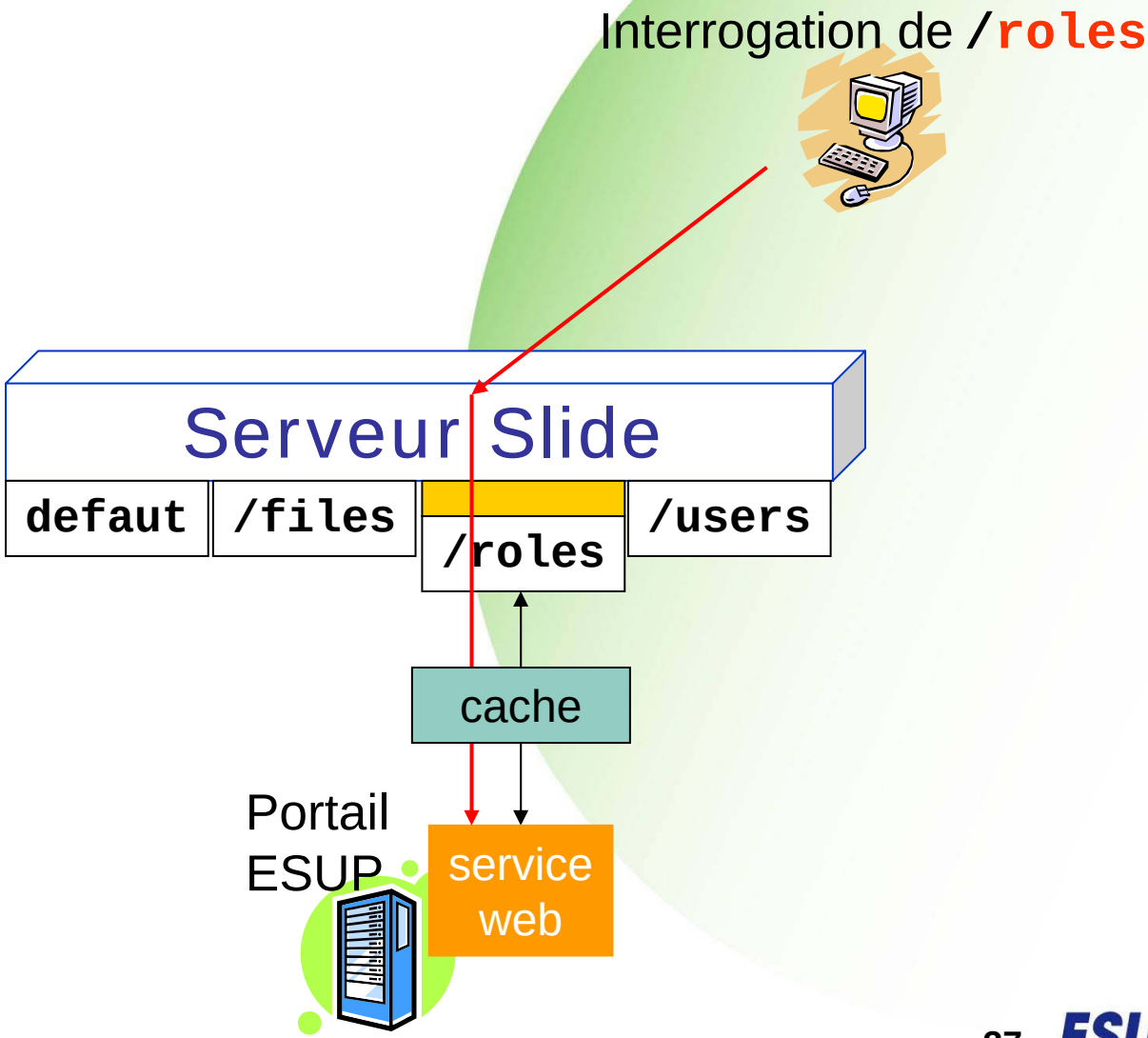
Serveur WebDAV - Les groupes

- De base dans Slide définition statique ou LDAP
- Visibles sous l'URL **`/roles`**
- Groupes du portail ESUP-Portail
  - Dynamiques et configurables (PAGS)
  - Interface de gestion et de sélection des groupes
- Volonté d'ESUP
  - Intégrer complètement les groupes du portail dans le serveur WebDAV

Serveur WebDAV - Les groupes

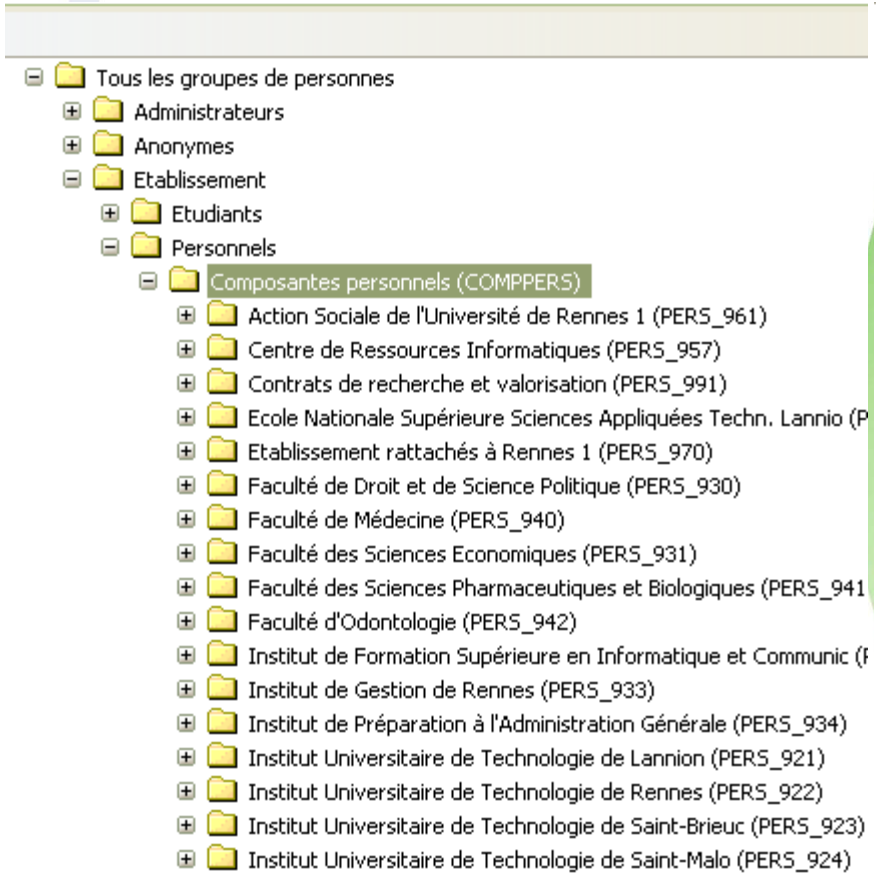
- Idée
  - Développer un *store* interrogeant dynamiquement le portail
- Plus précisément
  - Développement d'un service web exposant les groupes du portail
  - Développement d'un *store* de gestion de groupes connecté à ce service web

Serveur WebDAV - Les groupes



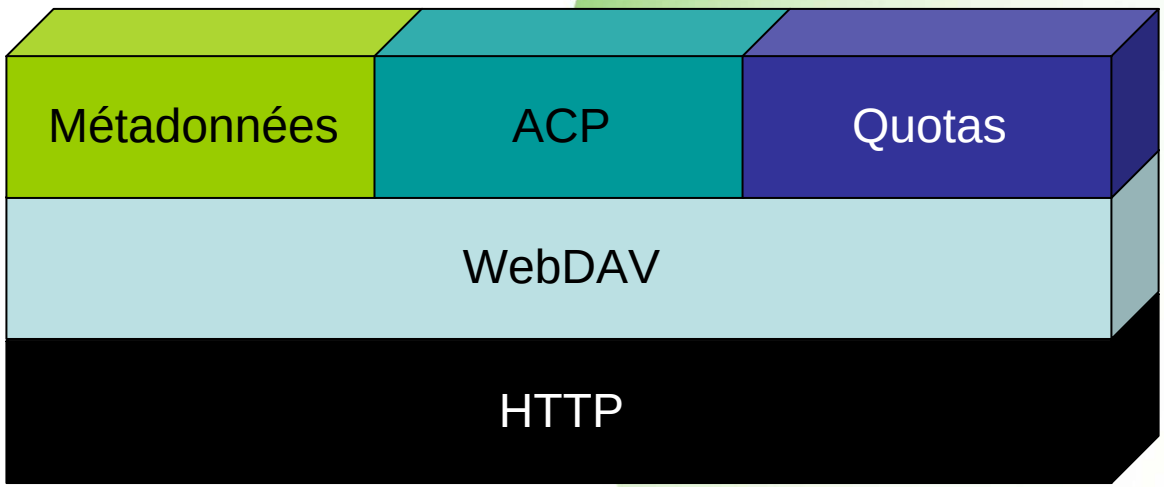
Serveur WebDAV - Les groupes

Serveur WebDAV : **`/roles`**



Portail : arborescence des groupes

Serveur WebDAV - Quotas



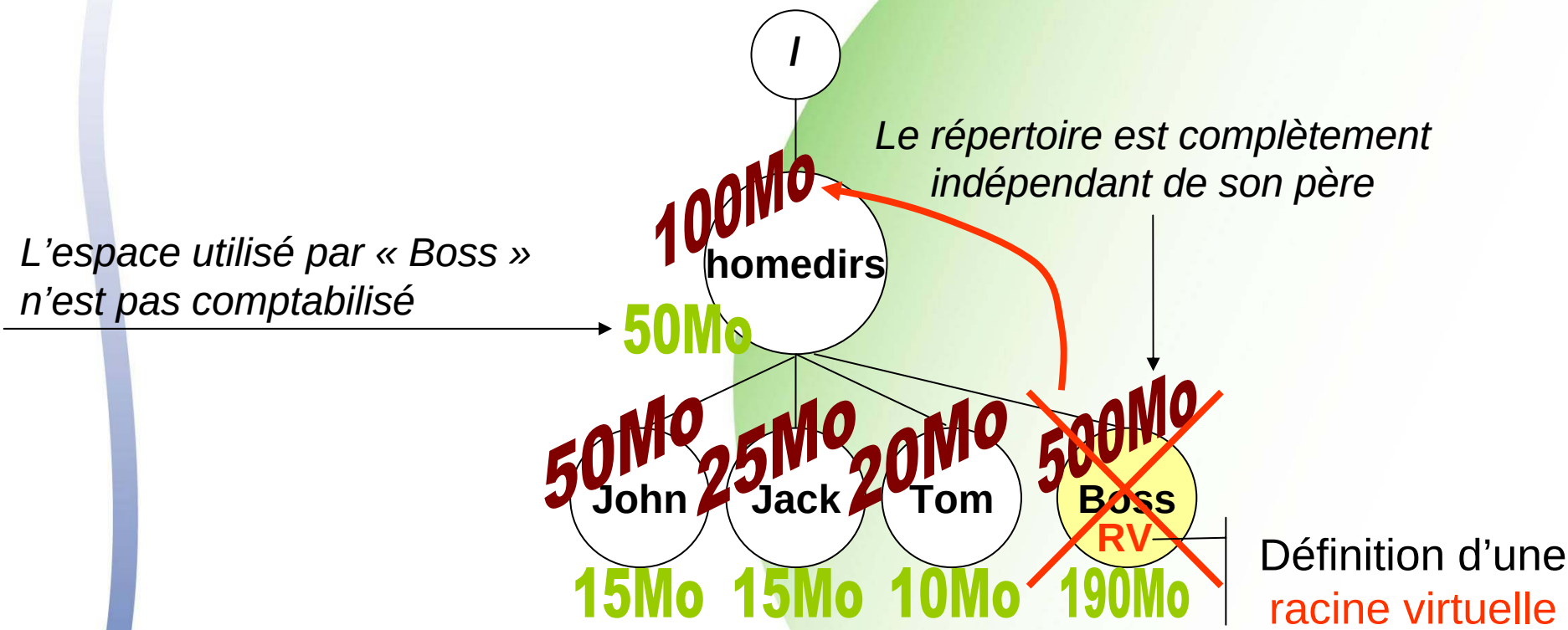
Serveur WebDAV - Quotas

- Draft qui spécifie
  - Deux nouvelles métadonnées vivantes et protégées définies sur les collections (répertoires)
    - **`DAV:quota-used-bytes`** : espace utilisé
    - **`DAV:quota-available-bytes`** : place restante
    - « quota » = la somme des deux
  - Dépassement de quota = erreur HTTP 507
- Slide 2.1 ne supporte pas les quotas

☞ *draft* peu flexible

  - Ne permet pas de casser les arborescences

Serveur WebDAV - Quotas



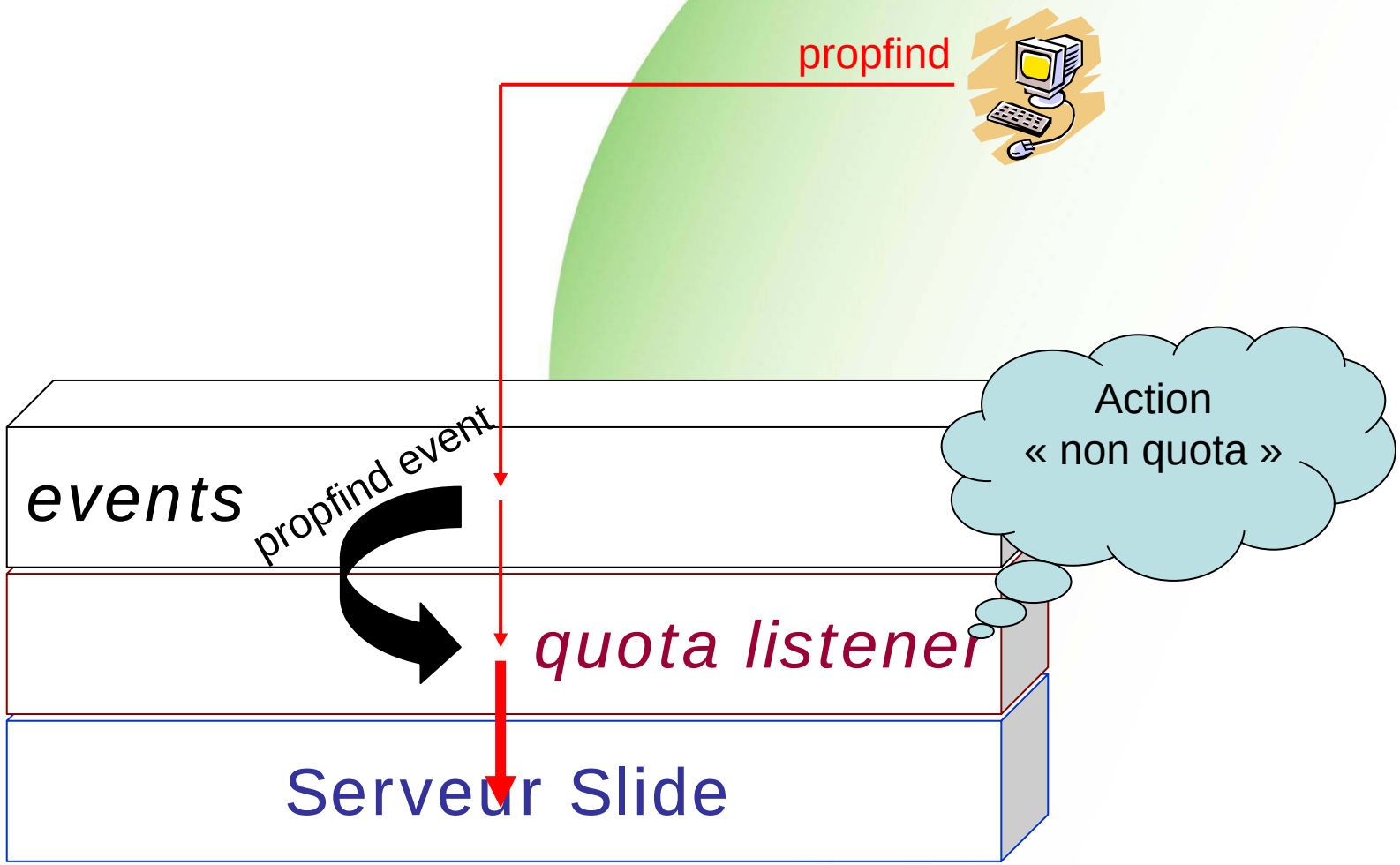
Serveur WebDAV - Quotas

- Définition d'une nouvelle métadonnée
  - **`ESUP:virtual-root`** : (booléen) racine virtuelle
  - Vivante et protégée
  - Indissociable des deux autres métadonnées

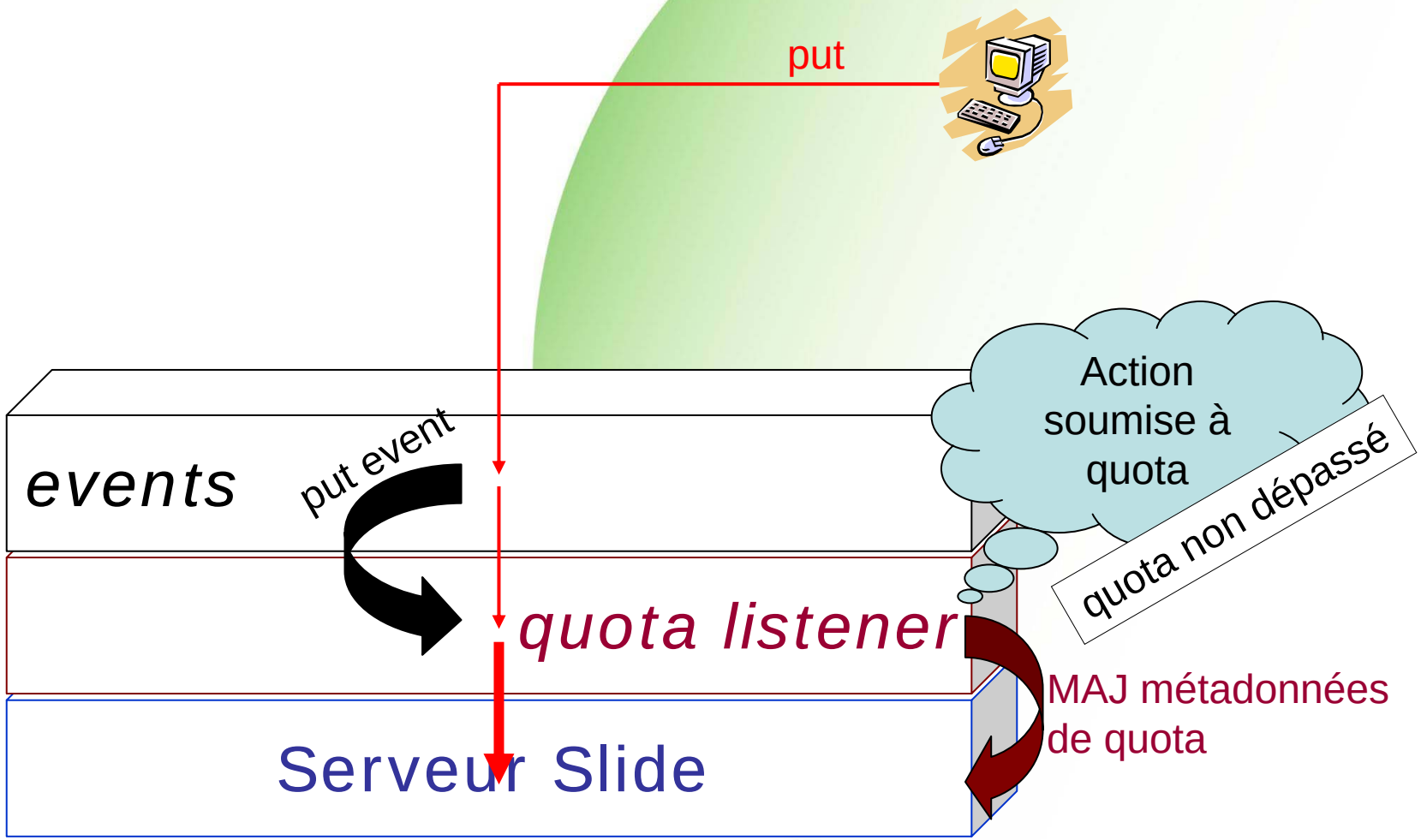
☞ reste l'implémentation dans Slide

- Utilisation de Java *event listeners*
  - Intégrés dans Slide
  - Un *event* (évènement) à chaque requête WebDAV
  - Un *listener* (écouteur d'évènements) de gestion de quotas qui intercepte les *events*

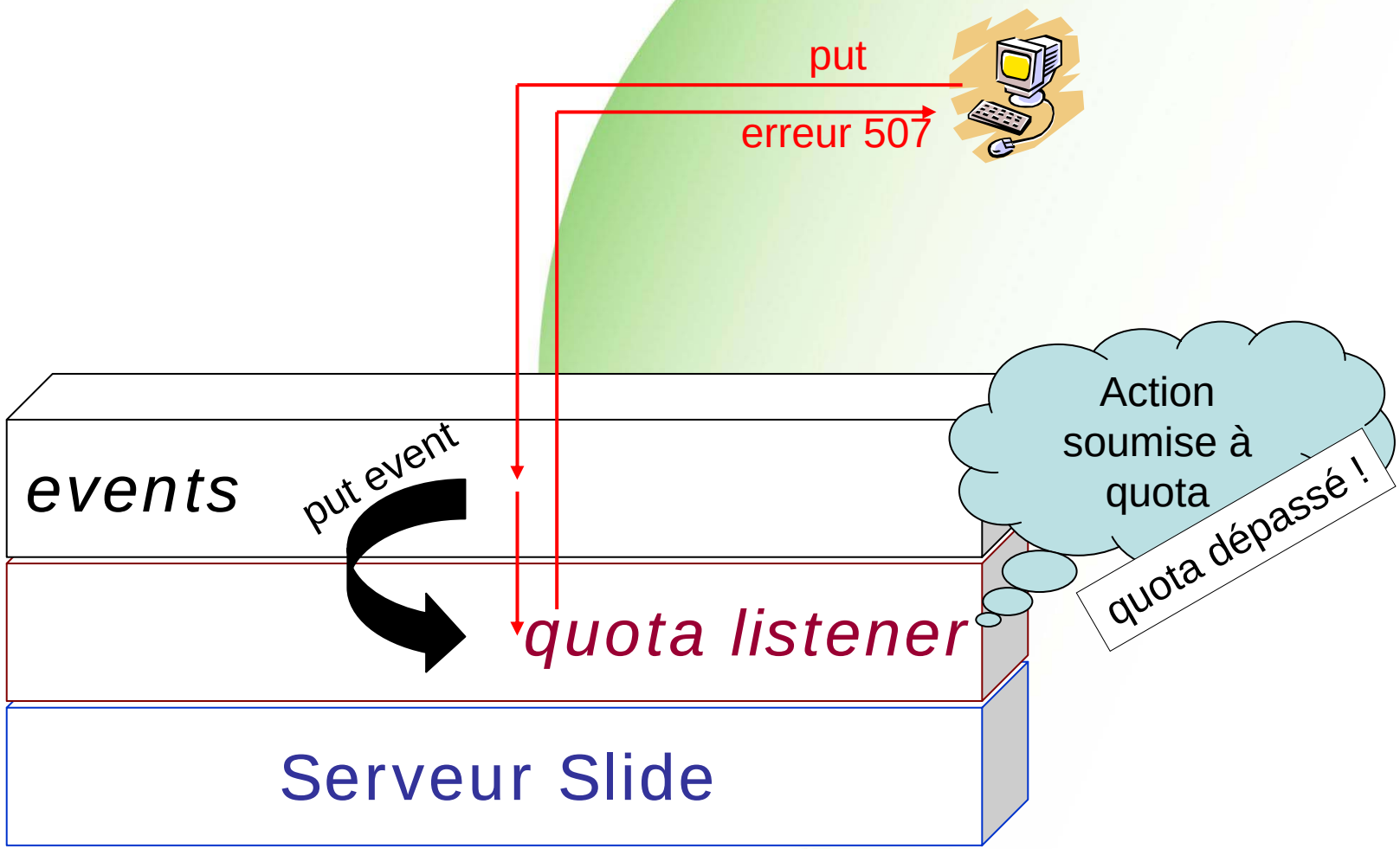
Serveur WebDAV - Quotas



Serveur WebDAV - Quotas



Serveur WebDAV - Quotas



Ex. de mise en application : inJAC

- Outil de référencement de ressources
  - Sur-ensemble du service de stockage
- Utilisation de WebDAV
  - Utilisation des métadonnées WebDAV pour
    - Stocker les métadonnées du document (Ex : Dublin Core, Lom)
    - Gérer le *workflow* sur le document
  - Utilisation de ACP pour
    - Gérer l'accès aux documents
    - Le moteur de rendu fait des accès WebDAV au serveur avec l'identité de l'utilisateur

Perspective : Shibboleth

- Shibboleth pour
  - Partager des ressources web entre établissements d'enseignement supérieur
  - Répondre à des besoins d'identification et d'autorisation inter établissements
- Objectif
  - Rendre compatible le serveur WebDAV ESUP dans sa version 5 avec Shibboleth
- Cf. Tutorial pour plus d'informations

Shibboleth et serveur WebDAV ESUP

- Principe de fonctionnement
  - Récupération des attributs de la personne via les mécanismes Shibboleth
  - Évaluation à la volée de l'appartenance de l'utilisateur au(x) groupe(s)
  - Possibilité d'autoriser des utilisateurs individuellement en utilisant l'EPPN (eduPersonPrincipalName)
  - Modification de l'interface du canal pour sélectionner ces groupes ou saisir les EPPN

Shibboleth et serveur WebDAV ESUP

- Écriture d'un *store* Shibboleth pour les groupes
  - Branché sur **`/roles/shib`**
  - Exemple d'un groupe :
    - **`/roles/shib/CRI_R1_R2`**
    - ((composante=957 et établissement=UR1) ou (composante=C32 et établissement=UHB))
- Écriture d'un *store* Shibboleth pour les utilisateurs
  - Branché sur **`/users/shib`**
  - Peut répondre avec un EPPN
    - Ex : bourges@univ-rennes1.fr
    - TargetedID si EPPN pas disponible

Conclusion

- ☺ Fonctionnellement riche
- ☹ De nombreux services mis en œu
  - Portail
  - SSO, LDAP
  - Shibboleth
- ☺ Expérience
  - Ex : Outil d'administration en version 2
- ☹ Produit est encore jeune
  - On aimerait une base installée plus importante, plus de développeurs, plus de retours d'expériences