

Gestion des privilèges de mise à jour des sites web au CRI de l'Université de Rennes 1

Version 0.4 – 22 janvier 2004

Statut

Envoyé pour validation aux gestionnaires des sites web du CRI et aux étudiants du DESS MITIC chargé des développements.

Ce document est accessible sur le web :

- Au format HTML : <http://perso.univ-rennes1.fr/pascal.aubry/doc/web/> ;
- Au format PDF : <http://perso.univ-rennes1.fr/pascal.aubry/doc/web/web.pdf>.

Historique

Version 0.4 – 20 janvier 2004 (P. Aubry – IFSIC – Université de Rennes 1)

Références

- [1] Le projet ESUP-Portail, <http://www.esup-portail.org>

Table des matières

1	Introduction.....	2
2	Description fonctionnelle.....	3
2.1	Architecture.....	3
2.2	Consultation des pages (accès en lecture).....	3
2.3	Mise à jour des pages (accès en modification).....	4
2.4	Mise à jour des gestionnaires	4
3	Configuration	5
3.1	Sites et gestionnaires	5
3.2	Rédacteurs	5
3.3	Exemple.....	6
3.4	Serveur web de consultation	7
3.5	Serveur WebDAV de mise à jour.....	7
4	L'application web.....	8
5	Feuille de route.....	9
5.1	L'application web.....	9
5.2	Les fichiers de configuration de l'application.....	9
5.3	Les tests.....	9

1 Introduction

Les pages des sites web hébergés par le CRI sont accédées par :

- La machine ocean.univ-rennes1.fr, serveur web sur le port 80, qui sert les pages aux navigateurs des visiteurs ;
- La machine ebene.univ-rennes1.fr, serveur webDAV sur le port 8081, qui permet aux utilisateurs de gérer les pages des sites.

Dans les deux cas, un serveur Apache (muni de mod_dav pour WebDAV) est utilisé.

Le contrôle d'accès en lecture des pages (sur le port 80) est défini à l'aide de :

- La configuration d'Apache (le fichier httpd.conf), gérée par l'administrateur du serveur web ;
- Des fichiers .htaccess répartis dans l'arborescence des fichiers, gérés par les mainteneurs des sites, ce qui permet de déléguer la gestion des droits d'accès en lecture.

Le contrôle d'accès en modification des pages (sur le port 8081) est défini seulement par la configuration d'Apache, gérée par l'administrateur du site web. Les fichiers .htaccess ne peuvent être utilisés car ils le sont déjà pour contrôler l'accès en lecture au site web sur le port 80.

Lors d'une modification de la politique de mise à jour des pages, une intervention de l'administrateur du serveur webDAV est toujours nécessaire. L'objectif de ce document est de décrire une solution permettant de déléguer la politique de mise à jour des sites web aux administrateurs de ces sites.

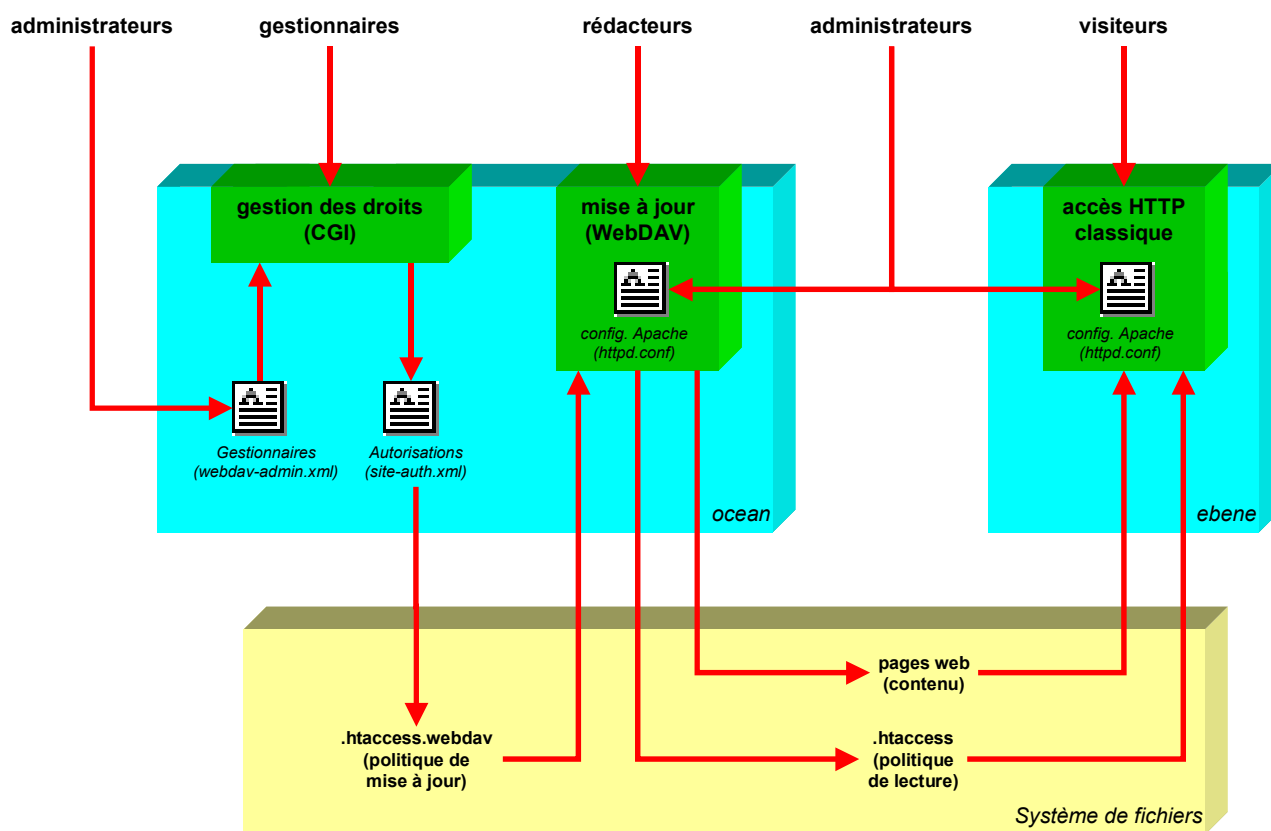
Note : la solution proposée n'est que provisoire : l'espace de stockage du projet ESUP-Portail [1] résoudra à terme tous les problèmes évoqués.

2 Description fonctionnelle

Nous faisons les hypothèses suivantes :

- Les pages d'un site sont modifiables par un ensemble de rédacteurs, sur la base de la structure du système de fichiers (toutes les pages d'un même répertoire sont modifiables par les mêmes rédacteurs) ;
- Un utilisateur rédacteur d'un ensemble de pages d'un site peut lire le contenu du site (dit autrement, les utilisateurs autorisés à lire l'ensemble des pages du site par le protocole WebDAV est l'union des rédacteurs de toutes les pages du site) ;
- Les rédacteurs d'un site sont gérés par les gestionnaires du site. Les gestionnaires d'un site sont automatiquement rédacteurs de toutes les pages du site.

2.1 Architecture



2.2 Consultation des pages (accès en lecture)

La consultation du contenu des pages se fait par le protocole HTTP sur le port 80 de la machine ebene (inchangé).

2.2.1 Contrôle d'accès en lecture

La politique de consultation des pages est définie par :

- La configuration d'Apache (le fichier httpd.conf sur ebene) pour la politique par défaut ;
- Des fichiers .htaccess répartis dans l'arborescence des fichiers.

2.2.2 Mise à jour du contrôle d'accès en lecture

La configuration d'Apache (le fichier httpd.conf) est gérée par l'administrateur du serveur web (directement sur ebene).

Les fichiers .htaccess sont gérés par les rédacteurs des sites à l'aide du protocole WebDAV (sur ocean comme les pages, cf plus bas).

2.3 Mise à jour des pages (accès en modification)

La mise à jour du contenu des pages se fait par le protocole HTTP sur le port 8081 de la machine ocean (inchangé).

2.3.1 Contrôle d'accès en modification

La politique de mise à jour des pages est définie par :

- La configuration d'Apache (le fichier httpd.conf sur ocean) pour la politique par défaut ;
- Les fichiers .htaccess.webdav répartis dans l'arborescence des fichiers.

2.3.2 Mise à jour du contrôle d'accès en modification

La configuration d'Apache (le fichier httpd.conf) est gérée par l'administrateur du serveur WebDAV (directement sur ocean).

Les fichiers .htaccess.webdav sont générés par les gestionnaires des sites web, à l'aide d'une application CGI.

Les utilisateurs autorisés à modifier les pages web d'un site sont enregistrés dans un fichier de configuration, au format XML (un fichier par site web). Grâce à l'application CGI, les gestionnaires des sites web peuvent :

- Mettre à jour le fichier de configuration (les utilisateurs autorisés à modifier les pages) ;
- Générer les fichiers .htaccess.webdav correspondant à la configuration.

2.4 Mise à jour des gestionnaires

Les gestionnaires des sites sont gérés par les administrateurs de l'application (qui est souvent la même personne physique que l'administrateur du serveur web), en éditant directement un fichier de configuration au format XML.

3 Configuration

Les fichiers de configuration sont stockés sur ocean (le serveur WebDAV), dans un répertoire dédié.

3.1 Sites et gestionnaires

Les sites, ainsi que leurs gestionnaires, sont décrits dans le fichier /data/htdocs/Webdav_admin/admin.xml, dont voici un exemple possible :

```
<admin>
  <def_site name="www.ifsic"
    root="/data/htdocs/Webdav_depot/www.ifsic">
    <manager>moigne</manager>
  </def_site>
  <def_site name="enseignant.ifsic"
    root="/data/htdocs/Webdav_depot/enseignant.ifsic">
    <manager>moigne</manager>
  </def_site>
  <def_site name="cri-perso"
    root="/data/htdocs/Webdav_depot/perso">
    <manager>defeo</manager>
    <manager>germes</manager>
  </def_site>
</admin>
```

3.2 Rédacteurs

Les rédacteurs d'un site web sont définis dans le fichier de configuration du site, situé dans le répertoire /data/htdocs/Webdav_admin/sites/xxx.xml (où xxx est le nom donné au site dans admin.xml).

Voici par exemple le contenu du fichier www.ifsic.xml, fichier de configuration du site www.ifsic :

```
<site name="www.ifsic">
  <def_group name="admin">
    <uid>paubry</uid>
    <uid>ayello</uid>
    <uid>diascorn</uid>
    <uid>krouilla</uid>
  </def_group>
  <def_group name="webmaster">
    <group>ifsic-admin</group>
    <uid>moigne</uid>
  </def_group>
  <def_group name="direction">
    <uid>ridoux</uid>
    <uid>perraude</uid>
    <uid>nebut</uid>
    <uid>moigne</uid>
  </def_group>
  <def_group name="dea">
    <uid>fbodin</uid>
    <uid>bmaret</uid>
  </def_group>
  <allow path="/">
    <group>webmaster</group>
  </allow>
  <allow path="/formation_initiale/cycle3/dea">
    <group>dea</group>
  </allow>
  <allow path="/relations/industrielles">
    <group>direction</group>
    <uid>kguerrie</uid>
  </allow>
</site>
```

Comme on le voit, il est possible de définir des groupes d'utilisateurs, ce qui permet de factoriser la configuration.

Note : les gestionnaires du site sont également considérés comme rédacteurs de tout le site.

3.3 Exemple

Les fichiers générés pour l'exemple donné ci-dessus seraient :

- /data/htdocs/Webdav_depot/www.ifsic/.htaccess.webdav ;
- /data/htdocs/Webdav_depot/www.ifsic/formation_intiale/cycle3/dea/.htaccess.webdav ;
- /data/htdocs/Webdav_depot/www.ifsic/relations/industrielles/.htaccess.webdav.

Le contenu des fichiers est donné ci-dessous.

/data/htdocs/Webdav_depot/www.ifsic/.htaccess.webdav :

```
<Limit GET POST OPTIONS PROPFIND >
  require user \
    paubry ayello diascorn krouilla moigne \
    ridoux perraude nebut fbodin bmaret kguerrie
</Limit>
<Limit PUT DELETE PATCH PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>
  require user \
    paubry ayello diascorn krouilla moigne
</Limit>
```

/data/htdocs/Webdav_depot/www.ifsic/formation_intiale/cycle3/dea/.htaccess.webdav :

```
<Limit GET POST OPTIONS PROPFIND >
  require user \
    paubry ayello diascorn krouilla moigne \
    ridoux perreaude nebut fbodin bmaret kguerrie
</Limit>
<Limit PUT DELETE PATCH PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>
  require user \
    fbodin bmaret moigne
</Limit>
```

/data/htdocs/Webdav_depot/www.ifsic/rerelations/industrielles/.htaccess.webdav :

```
<Limit GET POST OPTIONS PROPFIND >
  require user \
    paubry ayello diascorn krouilla moigne \
    ridoux perreaude nebut fbodin bmaret kguerrie
</Limit>
<Limit PUT DELETE PATCH PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>
  require user \
    kguerrie moigne
</Limit>
```

3.4 Serveur web de consultation

La configuration de ce serveur, sur ebene est très classique.

Le contrôle d'accès se fait sur les fichiers .htaccess (directive par défaut) :

```
AccessFileName .htaccess
```

Les fichiers sont pris en compte grâce à la directive :

```
AllowOverride AuthConfig.
```

Les fichiers .htaccess et .htaccess.webdav ne sont ni visibles ni lisibles.

3.5 Serveur WebDAV de mise à jour

Le contrôle d'accès se fait sur les fichiers .htaccess.webdav :

```
AccessFileName .htaccess.webdav
```

Et les fichiers sont pris en compte grâce à la directive :

```
AllowOverride AuthConfig
```

Les fichiers .htaccess sont visibles, lisibles et modifiables.

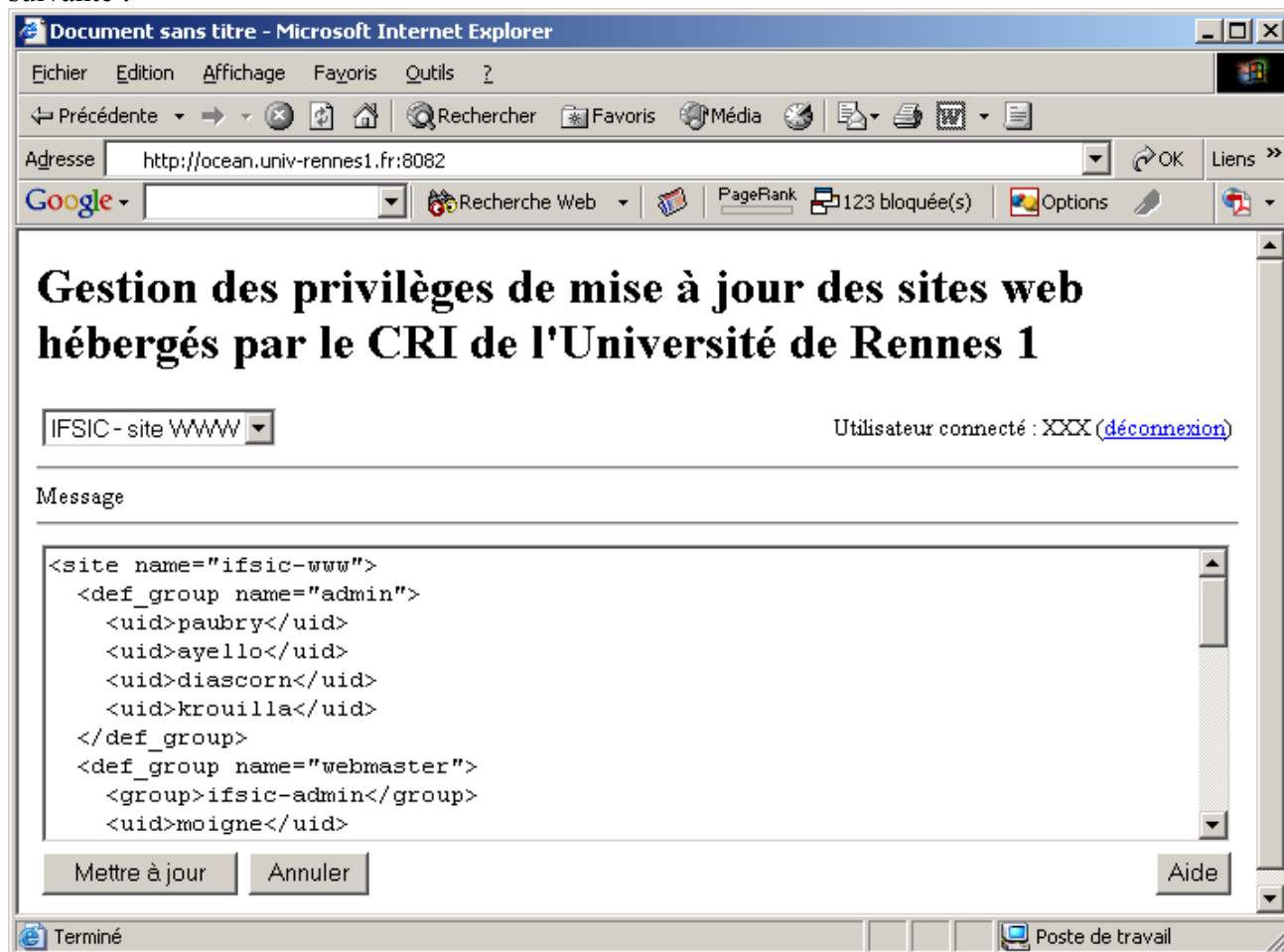
Les fichiers .htaccess.webdav ne sont ni visibles ni lisibles (en Apache 1.3, directive à inclure dans la configuration après la chargement de mod_access) :

```
<Files .htaccess.webdav>
  order allow,deny
  deny from all
</Files>
```

4 L'application web

Toutes les pages de l'application, à l'exception de la page d'accueil, renvoient le navigateur vers la page d'accueil si l'utilisateur n'est pas authentifié.

Les utilisateurs non authentifiés se voient proposer un lien qui force l'authentification par Single Sign-On (CAS). Après passage par le serveur d'authentification, l'utilisateur est redirigé vers la page suivante :



A partir de cette page, les gestionnaires peuvent mettre à jour les privilèges de mise à jour.

Note : le menu des sites web dont les gestionnaires peuvent modifier les privilèges est construit dynamiquement.

5 Feuille de route

5.1 L'application web

L'application est accessible à l'URL <http://webdav-gestion.cri.univ-rennes1.fr:8090>. Le dépôt des pages se fait à l'aide du protocole WebDAV à l'URL <http://ocean.univ-rennes1.fr:8081/webdav-gestion>, avec authentification Sésame. Pour le moment, seul l'utilisateur paubry peut déposer des pages, Pascal doit transmettre à Sylvain la liste des uid des étudiants du projet.

L'authentification se fait sur le serveur CAS <https://sso-cas.univ-rennes1.fr:443>.

Une documentation sur le développement d'applications PHP sur les serveurs du CRI est disponible sur <http://php.univ-rennes1.fr>.

5.2 Les fichiers de configuration de l'application

Tous les fichiers de configuration de l'application sont situés sur le système de fichiers du serveur web dans /data/htdocs/Webdav_admin/. Dans ce répertoire, le fichier admin.xml (maintenu par les administrateurs du serveur web) appartient à root. Les fichiers de configuration des sites sont situés dans un sous-répertoire sites, qui appartient à apache (ces fichiers doivent pouvoir être modifiés par l'application web).

La première version du fichier admin.xml :

```
<admin>
  <def_site name="www.ifsic"
    root="/data/htdocs/Webdav_depot/www.ifsic">
    <manager>moigne</manager>
  </def_site>
  <def_site name="enseignant.ifsic"
    root="/data/htdocs/Webdav_depot/enseignant.ifsic">
    <manager>moigne</manager>
  </def_site>
  <def_site name="cri-perso"
    root="/data/htdocs/Webdav_depot/perso">
    <manager>defeo</manager>
    <manager>germes</manager>
  </def_site>
</admin>
```

5.3 Les tests

Le serveur <http://www-test.ifsic.univ-rennes1.fr> servira à la fois :

- Aux tests de l'application web, en générant par exemple des fichiers .htaccess.test dans la hiérarchie du site ;
- A la mise au point du nouveau look du serveur web de l'IFSIC.

Le dépôt des pages sur ce site se fait à l'aide du protocole WebDAV à l'URL <http://ocean.univ-rennes1.fr:8081/www.ifsic>.

A terme, ce serveur sera utilisé pour héberger le serveur web de l'IFSIC (www-test.ifsic sera renommé www.ifsic).