

### Synthèse de l'intervention des 07 et 08 juillet 2010

Objet	Synthèse de l'intervention autour de l'ENT de l'IT SurdParis
Référence	ESUP-INTER-ITSP
Date de la première version	04 juillet 2010
Date de la dernière version	29 juillet 2010
Rédacteurs	<ul style="list-style-type: none"><li>Julien MARCHAL – Université de Nancy 2</li></ul>
Diffusion	<ul style="list-style-type: none"><li>Coordination technique ESUP-Portail</li><li>IT SurdParis</li></ul>

L'intervention sur place a permis d'avancer sur la perspective de passer l'ENT en version 3 mais aussi de réfléchir à l'architecture autour de ce projet. Voici la synthèse des 2 jours passés sur place.

#### Table des matières

<b>1. Version des logiciels actuellement en place.....</b>	<b>3</b>
<b>2. Articulation de brique logiciel.....</b>	<b>3</b>
<b>3. Intervention point par point .....</b>	<b>4</b>
Mise à jour de Horde.....	4
Récupération des sources .....	4
Configuration Apache.....	4
Script d'installation .....	6
Mise à jour de la base de données .....	7
Test .....	8
Cassification.....	9
Côté serveur imap.....	10
Explication autour de horde.....	11
Intégration de horde dans l'ent.....	12
Proposition d'architecture.....	12
Load Balancing Apache .....	16
Configuration pour le VirtualHost ent-dev.it-sudparis.eu .....	16

#### Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

<i>Configuration pour le VirtualHost ent1-dev.it-sudparis.eu</i> .....	18
<i>Au niveau tomcat</i> .....	19
<i>Gestionnaire du balancer</i> .....	20
Paramétrage JVM .....	20
Synchronisation .....	21
Monitoring .....	24
Syslog 26	
Statistiques .....	28

---

### **Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

## 1. Version des logiciels actuellement en place

Le portail actuellement en place est en version 2.6 DLM packagé par esup-portail.

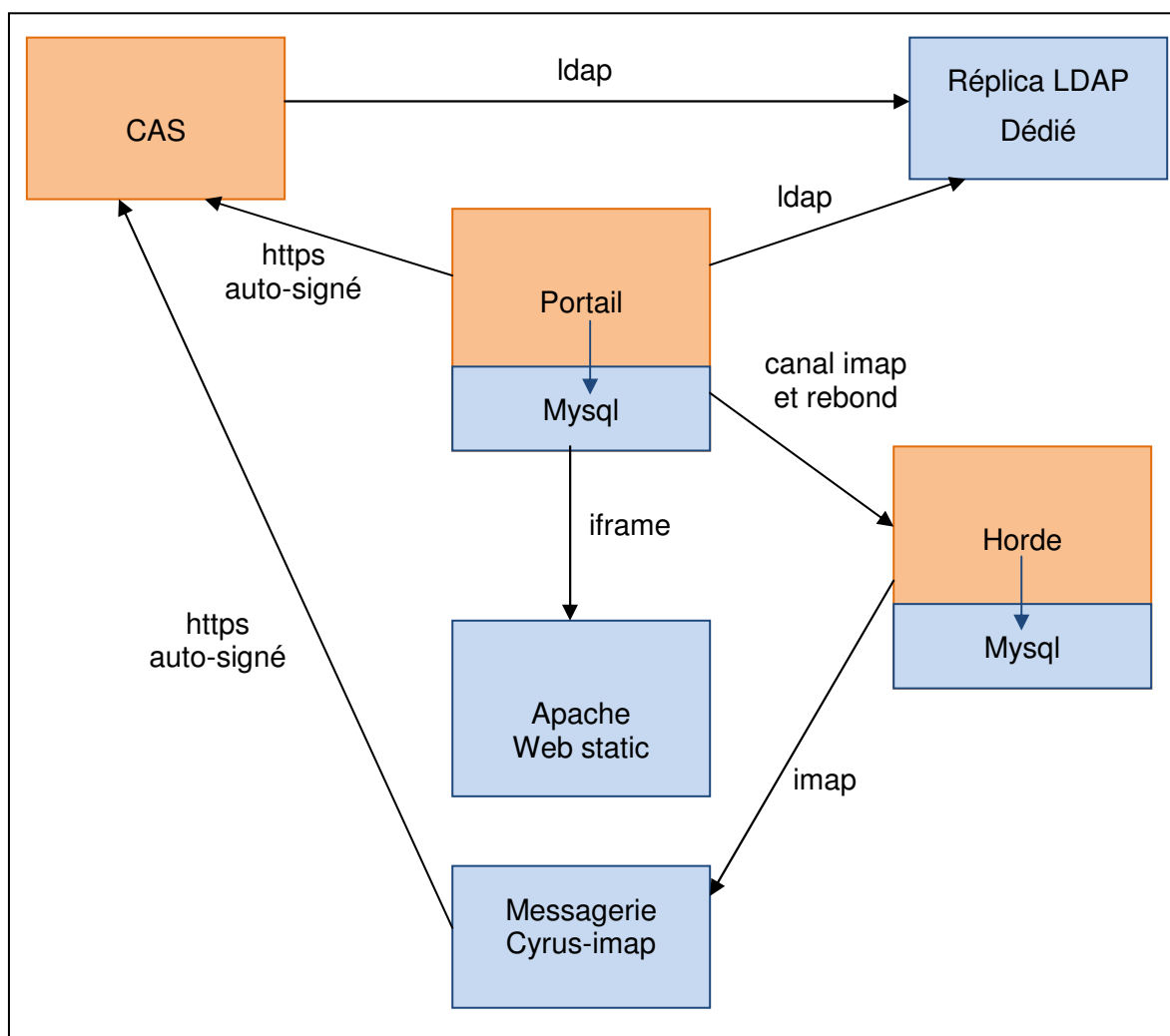
La version du serveur CAS utilisée est cas-toolbox-3.X.

Le tomcat hébergeant ces applications est en version 5.X

Le serveur LDAP utilisé comme référenciel est un openLdap.

Les accès HTTPS sont signés par des certificats générés localement.

## 2. Articulation de brique logiciel



### Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

### 3. Intervention point par point

#### Mise à jour de Horde

Basé sur <http://www.esup-portail.org/display/PROJHORDE/Installation+de+Horde-webmail>

#### Récupération des sources

```
cd /var/www/html
wget http://ftp.horde.org/pub/horde-webmail/horde-webmail-1.2.6.tar.gz
tar xvfz /root/horde-webmail-1.2.6.tar.gz
ln -s horde-webmail-1.2.6 horde
```

#### Configuration Apache

```
/etc/httpd/conf.d/horde.conf
```

```
DocumentRoot /var/www/html/horde/
ErrorLog /var/logs/httpd/error-horde_log
```

```
SetEnvIf Request_URI \.gif$ display=gif
SetEnvIf Request_URI \.jpeg$ display=jpg
SetEnvIf Request_URI \.jpg$ display=jpg
SetEnvIf Request_URI \.png$ display=png
SetEnvIf Request_URI \.css$ display=css
SetEnvIf Request_URI \.js display=js
SetEnvIf Request_URI favicon\.ico$ display=check
```

```
#ne va pas loguer tout ce qui est extension gif, jpeg, jpg, png, css...
CustomLog /var/logs/httpd/access-horde_log combined env=!display
```

```
<Directory /var/www/html/horde/>
  Order deny,allow
  Deny from all
  Allow from all
  AcceptPathInfo On
```

```
<IfModule mod_dir.c>
  DirectoryIndex index.php
</IfModule>
```

---

#### Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
php_flag engine on
php_admin_flag safe_mode off
php_flag register_globals off
php_flag magic_quotes_gpc off
php_flag magic_quotes_runtime off
php_admin_flag register_argc_argv off
php_admin_flag allow_url_fopen on
php_value include_path "/var/www/html/horde/pear/php"
php_admin_value open_basedir "/var/www:/tmp:/var/"
php_admin_value memory_limit -1
php_flag session.use_trans_sid off
php_flag session.auto_start off
php_admin_value session.cache_limiter nocache
php_admin_value session.gc_maxlifetime 3600
php_admin_value session.cookie_domain "webmail-dev.it-sudparis.eu"
php_admin_value session.cookie_path "/"
php_admin_value session.save_path "/var/www/session-horde"
php_admin_flag file_uploads on
php_admin_value upload_tmp_dir "/tmp"
php_value upload_max_filesize 10M
php_flag log_errors on
php_admin_value error_reporting E_ALL
php_admin_value error_log /var/logs/http/error-php-horde_log
php_admin_value display_errors 0
Options Indexes FollowSymLinks
AllowOverride None
</Directory>

<Directory /var/www/html/horde/config>
    Order Deny,Allow
    Deny from all
</Directory>

# Deny access to files that are not served directly by the webserver
<DirectoryMatch
"^(/var/www/html/horde/(.*)?(config|lib|locale|po|scripts|templates)/(.*)?">
    Order Deny,Allow
    Deny from all
</DirectoryMatch>

# Deny access to the test.php files except from localhost
<LocationMatch "^(.*)?test.php">
    Order Deny,Allow
    Deny from all
    Allow from 159.X.X.X
</LocationMatch>
```

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

### **Script d'installation**

```
cd /var/www/html/horde/scripts
$ ./setup.php
```

```
What is the web root path on your web server for this installation, i.e. the
path of the address you use to access Horde Groupware Webmail Edition in your
browser? [/horde-webmail-1.2.6] /
```

Horde Groupware Webmail Edition Configuration Menu

- (0) Exit
- (1) Configure database settings
- (2) Create database or tables
- (3) Configure administrator settings
- (4) Update PEAR for a new or changed location
- (5) Update from an older Horde Groupware Webmail Edition version

Type your choice: 1

What database backend should we use? [false]

Type your choice: mysql

Request persistent connections? [0]

Type your choice: 1

Username to connect to the database as\* [] root

Password to connect with [] XXXXXX

How should we connect to the database? [unix]

Type your choice: unix

Location of UNIX socket [] /var/lib/mysql/mysql.sock

Database name to use\* [] horde\_db

Internally used charset\* [utf-8]

Use SSL to connect to the server? [0]

Type your choice: 0

Certification Authority to use for SSL connections []

Split reads to a different server? [false]

Type your choice: false

Writing main configuration file

Done configuring database settings.

Horde Groupware Webmail Edition Configuration Menu

Type your choice: 3

Specify an existing mail user who you want to give administrator permissions  
(optional): admin

Writing main configuration file

Done configuring administrator settings.

---

### **Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

Horde Groupware Webmail Edition Configuration Menu  
Type your choice: 0

Thank you for using Horde Groupware Webmail Edition!

### ***Mise à jour de la base de données***

En premier lieu il faut faire un dump de la base de production afin de la recharger dans une base de test. On peut ensuite passer les différentes étapes de migration.

Une fois la base de test prête

```
mysql> show tables;
```

```
+-----+  
| Tables_in_horde_db |  
+-----+  
| horde_alarms        |  
| horde_cache         |  
| horde_datatree      |  
| horde_datatree_attributes |  
| horde_datatree_seq  |  
| horde_prefs         |  
| kronolith_events   |  
| kronolith_storage  |  
| mnemo_memos        |  
| nag_tasks          |  
| turba_objects      |  
+-----+
```

```
$ cd /var/www/html/horde/scripts/upgrades  
$ mysql -u root -p horde_db < 3.1_to_3.2.mysql.sql
```

```
$ cd /var/www/html/horde/kronolith/scripts/upgrades  
$ mysql -u root -p horde_db < 2.1_to_2.2.sql  
$ mysql -u root -p horde_db < 2.1_to_2.2.sql  
$ php -d include_path="/var/www/html/horde" convert_datatree_shares_to_sql.php
```

```
$ cd /var/www/html/horde/mnemo/scripts/upgrades  
$ mysql -u root -p horde_db < 2.1_to_2.2.sql  
$ mysql -u root -p horde_db < 2.2_to_2.2.1.sql  
$ mysql -u root -p horde_db < 2.2.1_to_2.2.2.sql  
$ php -d include_path="/var/www/html/horde" convert_datatree_shares_to_sql.php
```

---

### ***Utilisation et diffusion de ce document***

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
$ cd /var/www/html/horde/nag/scripts/upgrades
$ mysql -u root -p horde_db < 2.1_to_2.2.sql
$ mysql -u root -p horde_db < 2.2_to_2.3.sql
$ mysql -u root -p horde_db < 2008-09-23_fix_group_uid.sql
$ php -d include_path="/var/www/html/horde-webmail"
convert_datatree_shares_to_sql.php
$ php -d include_path="/var/www/html/horde-webmail-1.2.6"
create_missing_add_histories_sql.php
```

```
$ cd /var/www/html/horde/turba/scripts/upgrades
$ mysql -u root -p horde_db < 2.1_to_2.2_add_sql_share_tables.sql
$ mysql -u root -p horde_db < 2.2.1_to_2.3.sql
$ php -d include_path="/var/www/html/horde" convert_datatree_shares_to_sql.php
$ export HORDE_DB_USER='root';
$ export HORDE_DB_PASS='XXXXXX';
$ php -d include_path="/var/www/html/horde" -d memory_limit=-1
2.1_to_2.2_sql_schema.php
```

```
$ cd /var/www/html/horde/ingo/scripts/sql
$ mysql -u root -p horde_db < ingo.sql
```

```
$ cd /var/www/html/horde/ingo/scripts/upgrades
$ ./convert_datatree_shares_to_sql.php
Do you want to keep your old datatree data or delete it?
Type your choice: 1
```

```
Data will be copied into the new tables, and WILL be deleted from the datatree.
Type your choice: y
Done.
```

```
$ vim /var/www/html/horde/conf/config/config.php
  > $conf['compress_pages'] = false;
$ mysql -u root -p horde_db -e 'select DISTINCT pref_uid from horde_prefs;' >
/tmp/user_horde
$ php -d include_path="/var/www/html/horde" -d memory_limit=-1
convert_imp_filters.php </tmp/user_horde
$ php -d include_path="/var/www/html/horde" -d memory_limit=-1
convert_prefs_to_sql.php </tmp/user_horde
```

## Test

Avant tout chose configurer le fichier horde/conf/server.php vers le serveur imap de l'établissement afin de valider que horde fonctionne correctement.

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*



```
$ more /var/www/html/horde/conf/server.php
$servers['imap'] = array(
  'name' => 'IMAP IT SudParis Server',
  'server' => 'imap.it-sudparis.eu',
  'hordeauth' => true,
  'protocol' => 'imap/notls',
  'port' => 143,
  'maildomain' => 'it-sudparis.eu',
  'smtp host' => 'smtp.it-sudparis.eu',
  'smtp port' => 25,
  'realm' => '',
  'preferred' => '1',
  'quota' => array(
    'driver' => 'imap',
    'params' => array(
      'hostspec' => imap.it-sudparis.eu',
      'port' => 143
    )
  ),
  'login_tries' => 1
);
```

### **Cassification**

La cassification de horde se passe en 3 étapes :

1. Récupération des sources
2. Applications des patches
3. Configuration

```
$ cd /tmp
$ wget http://sourcesup.cru.fr/frs/download.php/3127/esup-horde-1.2.x-cas-1.3.tar.gz
$ tar -zxvf esup-horde-1.2.x-cas-1.3.tar.gz

$ cp esup-horde-1.2.x-cas-1.3/libs/casProxy.php /var/www/html/horde/
$ cp esup-horde-1.2.x-cas-1.3/libs/cas.php /var/www/html/horde/lib/Horde/Auth/
$ cd /var/www/html
$ patch -p 0 < /root/esup-horde-1.2.x-cas-1.3/patches/conf.xml.patch
$ patch -p 0 < /root/esup-horde-1.2.x-cas-1.3/patches/IMAP.php.patch
$ patch -p 0 < /root/esup-horde-1.2.x-cas-1.3/patches/timsieved.php.patch
```

---

### **Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
$ more /var/www/html/horde/config/conf.php
$conf['auth']['admins'] = array('admin', 'procacci', 'gaboret') ;
$conf['auth']['checkip'] = false;
$conf['auth']['checkbrowser'] = false;
$conf['auth']['alternate_login'] = false;
$conf['auth']['redirect_on_logout'] = false;
$conf['auth']['params']['hostspec'] = 'cas.it-sudparis.eu';
$conf['auth']['params']['hostport'] = 443;
$conf['auth']['params']['hostpath'] = 'cas';
$conf['auth']['params']['proxyback'] = 'https://webmail-dev.it-
sudparis.eu/casProxy.php';
$conf['auth']['params']['tmpdir'] = '/tmp/cas';
$conf['auth']['params']['authorisation'] = false;
$conf['auth']['params']['logout'] = true;
$conf['auth']['params']['debug'] = false;
$conf['auth']['params']['debug_file'] = '/var/log/phpCAS.log';
$conf['auth']['params']['handleLogout'] = true;
$conf['auth']['params']['handleLogoutHost'] = array('cas.it-sudparis.eu');
$conf['auth']['driver'] = 'cas';
```

Il serait intéressant de regarder l'authentification mixte :

<http://www.esup-portail.org/pages/viewpage.action?pageId=36732951>

Celle-ci a pour but de gérer 2 (ou plus) types d'authentification (CAS et LDAP par exemple) on définit ensuite une méthode qui permet de choisir le type d'authentification. Le but est de pouvoir faire une authentification LDAP pour les périphériques mobile par exemple.

### **Coté serveur imap**

```
$ more /etc/pam.d/imap
auth    sufficient    /lib/security/pam_cas.so -simap://imap.it-sudparis.eu -
f/etc/pam_cas.conf
auth    sufficient    /lib/security/pam_cas.so -simap://imap.it-sudparis.eu -
f/etc/pam_cas_dev.conf
auth    sufficient    /lib/security/pam_ldap.so
auth    include       system-auth
account sufficient    /lib/security/pam_ldap.so
account include       system-auth
```

```
$ more /etc/pam_cas_dev.conf
host casesup.int-evry.fr
port 80
uriValidate /proxyValidate
ssl off
debug off
trusted_ca /cert/notUseHere
```

Dans le cas du pam\_cas il est à mon sens inutile de faire du ssl (https) entre le pam\_cas et le cas d'où la directive (ssl off). Ceci qui simplifie les choses car on ne gère plus de certificat coté serveur imap.

---

### **Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

## Explication autour de horde

Horde se découpe en plusieurs modules :

- Imp : webmail
- Dimp : webmail dynamique (ajax)
- Mimp : webmail pour mobile (interface web adaptée)
- Ingo : gestion des filtres
- Kronolith : gestion de l'agenda
- Mnemo : gestion de note
- Nag : gestion de tâche
- Turba : gestion de carnet d'adresse

Chaque application remplit des fonctions différentes mais se configure de manière similaire. Tout ce situe dans le dossier config/ :

- conf.php : fichier de configuration global de l'application
- prefs.php : fichier de configuration des préférences utilisateurs
- hooks.php : ensemble de fonctions permettant de changer le comportement d'une préférence par programmation
- servers.php : spécifique à imp (dimp, mimp) pour la définition des serveurs IMAP
- backends.php : spécifique à ingo pour les backends de filtres
- sources.php : spécifique à turba pour la définition des sources de données

Il est intéressant de noter la structure de prefs.php par exemple la préférence représentant le nom complet

```
$_prefs['fullname'] = array(  
    'value' => '',  
    'locked' => false,  
    'shared' => true,  
    'type' => 'text',  
    'desc' => _("Your full name:")  
);
```

Si on veut modifier cette préférence placer en fin de fichier prefs uniquement ce qu'on écrase :

```
$_prefs['fullname']['locked'] = true;  
$_prefs['fullname']['hook'] = true;
```

Elle est maintenant configurée pour utiliser un hook, il faut donc définir dans le hooks.php

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
if (!function_exists('_prefs_hook_fullname')) {
    function _prefs_hook_fullname($user = null)
    {
        $user = Auth::getBareAuth();
        if (empty($user)) {
            return($user);
        }
        // Recuperation LDAP
        return($user);
    }
}
```

### **Intégration de horde dans l'ent**

On peut intégrer horde sous forme d'IFRAME dans l'ent.

Pour se faire on peut dériver de la page horde/services/portal/index.php

Les modifications consistent à enlever le bandeau du haut et à faire que tous les liens s'ouvrent dans une nouvelle fenêtre.

### **Proposition d'architecture**

L'institut dispose de 4 machines :

- Cuzco : 16Go de mémoire
- Palenque : 16Go de mémoire
- Epidaure : 8Go de mémoire
- Baalbek : 8Go de mémoire

L'institut pratique la virtualisation légère avec openVZ, et souhaite répartir les services suivants sur ces machines :

- moodle : une instance de Moodle
- sql-moodle : un serveur mysql servant à Moodle
- ent-fr : un ENT en français
- sql-ent : un serveur mysql servant à l'ENT
- ent-en : un ENT en anglais
- webmail : un webmail horde/imp
- webmail-dev : un webmail horde/imp pour faire des tests
- web-static : Apache pour desservir les pages statiques
- frontal-http : va centraliser les requêtes http(s) et va faire la répartition de charge des ENT

---

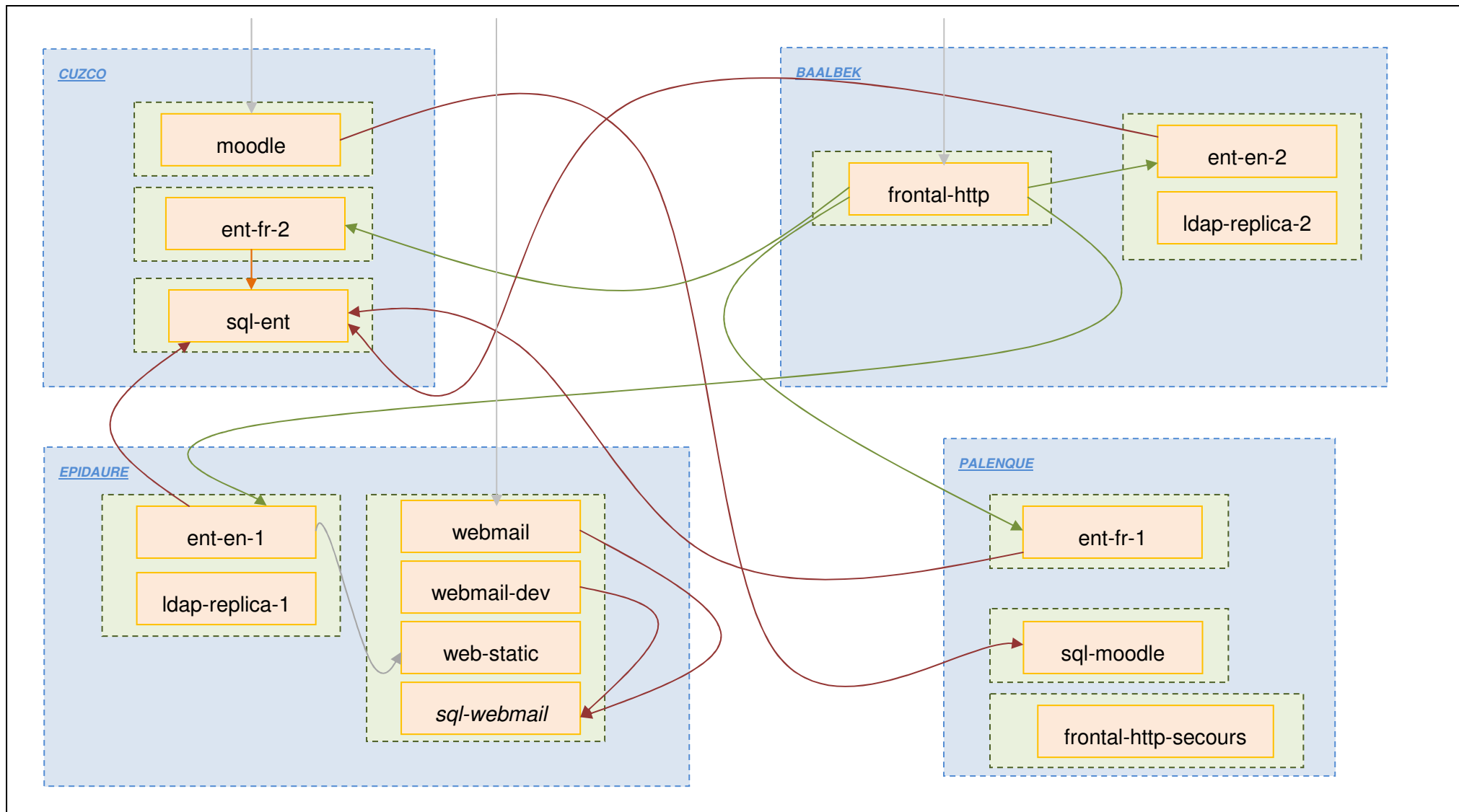
### **Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

---

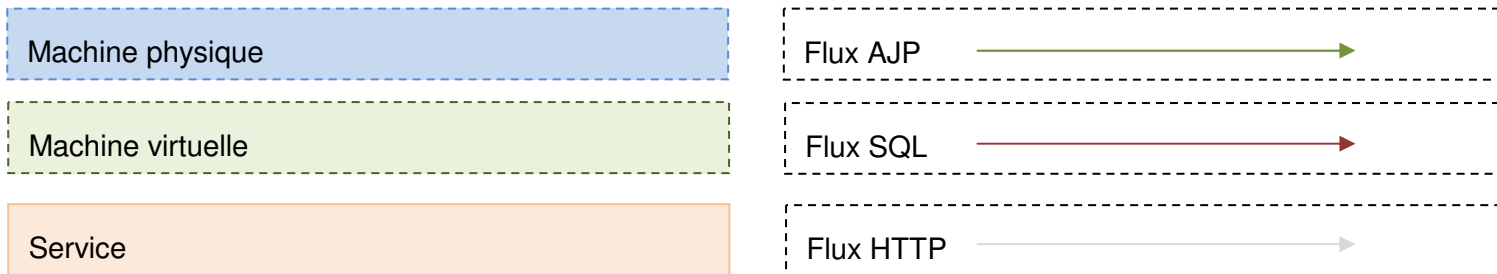
***Utilisation et diffusion de ce document***

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*



## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*



---

**Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

## Load Balancing Apache

Pour faire du load balancing devant les ENT il faut disposer d'un moteur http (apache). Apache doit avoir les modules suivants :

- mod\_proxy
- mod\_proxy\_ajp
- mod\_proxy\_balancer

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
```

Dans le cas de 2 serveurs ENT on va devoir définir les CNAME DNS suivant :

```
ent-dev.it-sudparis.eu (loadbalancer)
ent1-dev.it-sudparis.eu (accès direct ent1)
ent2-dev.it-sudparis.eu (accès direct ent2)
```

## Configuration pour le VirtualHost ent-dev.it-sudparis.eu

`$more /etc/httpd/conf.d/ent-dev_vhost.conf`

```
<VirtualHost 0.0.0.0:80>
  ServerName ent-dev.it-sudparis.eu
  include confN2.d/ent-dev.conf
</VirtualHost>
```

```
<VirtualHost 0.0.0.0:443>
  ServerName ent-dev.it-sudparis.eu
  include conf/genericSSL.conf
  include confN2.d/ent-dev.conf
</VirtualHost>
```

`$more /etc/httpd/conf.d/ent-dev.conf`

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"
\"SESSION_ROUTE=%{BALANCER_SESSION_ROUTE}e\"
\"ASSIGN_ROUTE=%{BALANCER_WORKER_ROUTE}e\"" balancedLogFormat
```

```
ErrorLog logs/error-ent-dev_log
```

```
CustomLog logs/access-ent-dev_log balancedLogFormat env=!display
```

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*



```
<Location />
  Order deny,allow
  Allow from all
</Location>

<Location "/EsupMonitor">
  Order deny,allow
  Deny from all
  Allow from localhost RESEAU_ENT RESEAU_ADMIN
</Location>

<Location "/services">
  Order deny,allow
  Deny from all
  Allow from localhost RESEAU_ENT RESEAU_ADMIN
</Location>

<Location /manager>
  Order deny,allow
  Deny from all
  Allow from localhost RESEAU_ENT RESEAU_ADMIN
</Location>

<Location "/private">
  Order deny,allow
  Deny from all

  Allow from RESEAU_ADMIN
</Location>

<Location /balancer-manager>
  SetHandler balancer-manager
  Order Deny,Allow
  Deny from all
  Allow from RESEAU_ADMIN

  AuthName "Balancer Manager de ent-dev"
  AuthType CAS
  require user ADMINS
</Location>

<Proxy balancer://ent-dev-cluster>
  BalancerMember ajp://ent1-dev.it-sudparis.eu:8009 min=0 max=100 smax=50
  ttl=10 route=ent1-dev timeout=60
  BalancerMember ajp://ent2-dev.it-sudparis.eu:8009 min=0 max=100 smax=50
  ttl=10 route=ent2-dev timeout=60
</Proxy>
```

---

## **Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
ProxyPass /server-status !
ProxyPass /server-info !
ProxyPass /balancer-manager !
ProxyPass / balancer://ent-dev-cluster/ stickysession=JSESSIONID
```

```
ErrorDocument 503 "Red&eacute;marrage imm&eacute;diat de l'ENT. Patientez
quelques minutes."
```

### ***Configuration pour le VirtualHost ent1-dev.it-sudparis.eu***

\$more /etc/httpd/conf.d/ent1-dev\_vhost.conf

```
<VirtualHost 0.0.0.0:80>
  ServerName ent1-dev.it-sudparis.eu
  include confN2.d/ent1-dev.conf
</VirtualHost>
```

```
<VirtualHost 0.0.0.0:443>
  ServerName ent1-dev.it-sudparis.eu
  include conf/genericSSL.conf
  include confN2.d/ent1-dev.conf
</VirtualHost>
```

\$more /etc/httpd/conf.d/ent1-dev.conf

```
ErrorLog logs/error-ent1-dev_log
CustomLog logs/access-ent1-dev_log combined env=!display
```

```
<Location />
  Order deny,allow
  Allow from all
</Location>
```

```
<Location "/EsupMonitor">
  Order deny,allowz
  Deny from all
  Allow from localhost RESEAU_ENT RESEAU_ADMIN
</Location>
```

```
<Location "/services">
  Order deny,allow
  Deny from all
  Allow from localhost RESEAU_ENT RESEAU_ADMIN
</Location>
```

---

### ***Utilisation et diffusion de ce document***

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
<Location /manager>
  Order deny,allow
  Deny from all
  Allow from localhost RESEAU_ENT RESEAU_ADMIN
</Location>
```

```
<Location "/private">
  Order deny,allow
  Deny from all
  Allow from localhost RESEAU_ENT RESEAU_ADMIN
</Location>
```

```
ProxyPass / ajp:// ent1-dev.it-sudparis.eu:8009/ min=0 max=100 smax=50 ttl=10
route=ent1-dev timeout=60
```

```
ErrorDocument 503 "Red&eacute;marrage imm&eacute;diat de l'ENT. Patientez
quelques minutes."
```

Une configuration identique à ent1-dev devra être faite pour ent2-dev

### **Au niveau tomcat**

Afin que le load balancing soit complet il faut définir :

- le connecteur AJP
- la jvmroute

```
<Connector port="7009"
  protocol="AJP/1.3"
  redirectPort="8443"
  emptySessionPath="true"
  enableLookups="false"
  backlog="300"
  connectionTimeout="30000"
  maxThreads="500"/>
```

```
<Engine name="Catalina" defaultHost="localhost" jvmRoute="ent1-dev">
```

La jvmRoute va servir à suffixer le cookie de session JSESSIONID afin qu'apache sache vers quel ENT envoyer.

1. Première accès pas de cookie JSESSIONID
  2. Apache envoie vers ent1-dev
  3. Le tomcat de ent1-dev dépose un cookie JSESSIONID et se sert de sa jvmRoute :  
DEDFCA294E8CC195DF542665EF60C101.**ent1-dev**
  4. A la requête suivante on repasse par l'apache il regarde il y a un cookie JSESSIONID prend son suffixe (**ent1-dev**) et recherche si il a un membre du balancer dont la jvmRoute correspond si c'est le cas il renvoie vers ce membre.
- 

### **Utilisation et diffusion de ce document**

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

## Gestionnaire du balancer

Le module apache mod\_proxy\_balancer mets a disposition un handler balancer-manager dans les exemples de configuration celui-ci est mappé sur / balancer-manager

# Load Balancer Manager for ent.univ-nancy2.fr

Server Version: Apache  
Server Built: Apr 4 2010 17:22:45

## LoadBalancer Status for balancer://ent-cluster

StickySession Timeout FailoverAttempts Method  
JSESSIONID 0 3 byrequests

Worker URL	Route	RouteRedir	Factor	Set	Status	Elected To	From
<a href="#">ajp://ent1vm.univ-nancy2.fr:7009</a>	ent1		1	0	Ok	334661 4.4M	1.9G
<a href="#">ajp://ent2vm.univ-nancy2.fr:7009</a>	ent2		1	0	Ok	334534 680K	1.9G
<a href="#">ajp://ent3vm.univ-nancy2.fr:7009</a>	ent3		1	0	Ok	334455 537K	1.9G
<a href="#">ajp://ent4vm.univ-nancy2.fr:7009</a>	ent4		1	0	Ok	334448 485K	2.0G

## Edit worker settings for ajp://ent4vm.univ-nancy2.fr:7009

Load factor:

LB Set:

Route:

Route Redirect:

Status: Disabled:  | Enabled:

## Paramétrage JVM

La JVM des ENT doit être un minimum tuner. Pour ce faire on positionne une variable d'environnement JAVA\_OPTS. Ceci peut se faire dans un script env.sh par exemple.

Les directives intéressantes :

- -server : indique à la JVM qu'elle fonctionne en mode server
- -Xms256m : mémoire minimum alloué au démarrage (256 Mo)
- -Xmx1500m : mémoire maximum que la JVM va pouvoir s'allouer (1.5Go)
- -XX:+UseParallelGC : active la travaille parallèle du Garbage Collector

## Utilisation et diffusion de ce document

Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.

- -Djava.net.preferIPv4Stack=true : utilisation de la stack IPV4 en priorité
- -Dnetworkaddress.cache.ttl=3600 : temps de cache DNS de la JVM (3600 secondes)
- -Djava.awt.headless=true : désactive des fonctions graphiques (pas de display)
- -Dcom.sun.management.jmxremote : active la possibilité d'utilisé le JMX en more distant
- -Dorg.apache.catalina.loader.WebappClassLoader.ENABLE\_CLEAR\_REFERENCES : désactive des messages de log4j en lien avec tomcat
- -Dhttp.nonProxyHosts, -Dhttp.proxyHost, -Dhttp.proxyPort = les ENT doivent passer par un serveur proxy http pour faire des requêtes extérieurs
- 

Pointeurs :

- <http://blogs.sun.com/watt/resource/jvm-options-list.html>
- <http://java.sun.com/developer/technicalArticles/J2SE/jmx.html>
- <http://tomcat.apache.org/tomcat-6.0-doc/config/systemprops.html>
- [http://download.oracle.com/docs/cd/E17476\\_01/javase/1.4.2/docs/guide/net/properties.html](http://download.oracle.com/docs/cd/E17476_01/javase/1.4.2/docs/guide/net/properties.html)

```
export JAVA_OPTS="-server -Xms256m -Xmx1500m -XX:MaxPermSize=256m -
XX:+UseParallelGC"
export JAVA_OPTS="$JAVA_OPTS -Djava.net.preferIPv4Stack=true -
Dnetworkaddress.cache.ttl=3600"
export JAVA_OPTS="$JAVA_OPTS -Djava.awt.headless=true -
Dcom.sun.management.jmxremote"
export JAVA_OPTS="$JAVA_OPTS -
Dorg.apache.catalina.loader.WebappClassLoader.ENABLE_CLEAR_REFERENCES=false"
export JAVA_OPTS="$JAVA_OPTS -Dhttp.nonProxyHosts=*.univ.fr|*.univ.eu|localhost
-Dhttp.proxyHost=cache.univ.fr -Dhttp.proxyPort=8080"
export JAVA_OPTS="$JAVA_OPTS -Dhttp.agent=Java-ENT-Univ"
```

## Synchronisation

Lorsque l'on utilise plusieurs ENT en production il faut instaurer un mécanisme de synchronisation afin de ne pas avoir à faire les mises à jours sur toutes les instances des ENT.

Pour ce faire on établis le principe suivant un des ENT (ent1) est défini comme MAITRE, les autres sont défini comme ESCLAVE.

La synchronisation requière un utilisateur commun entre tous les ENT (« uportal » sur le MAITRE et sur le ESCLAVES) mais aussi un échange de clé afin que les ESCLAVES puissent ouvrir des connexions ssh (rsync) en tant que utilisateur uportal vers le MAITRE sans mot de passe.

Le MAITRE va donc contenir les éléments suivants :

- tomcat
- ant

---

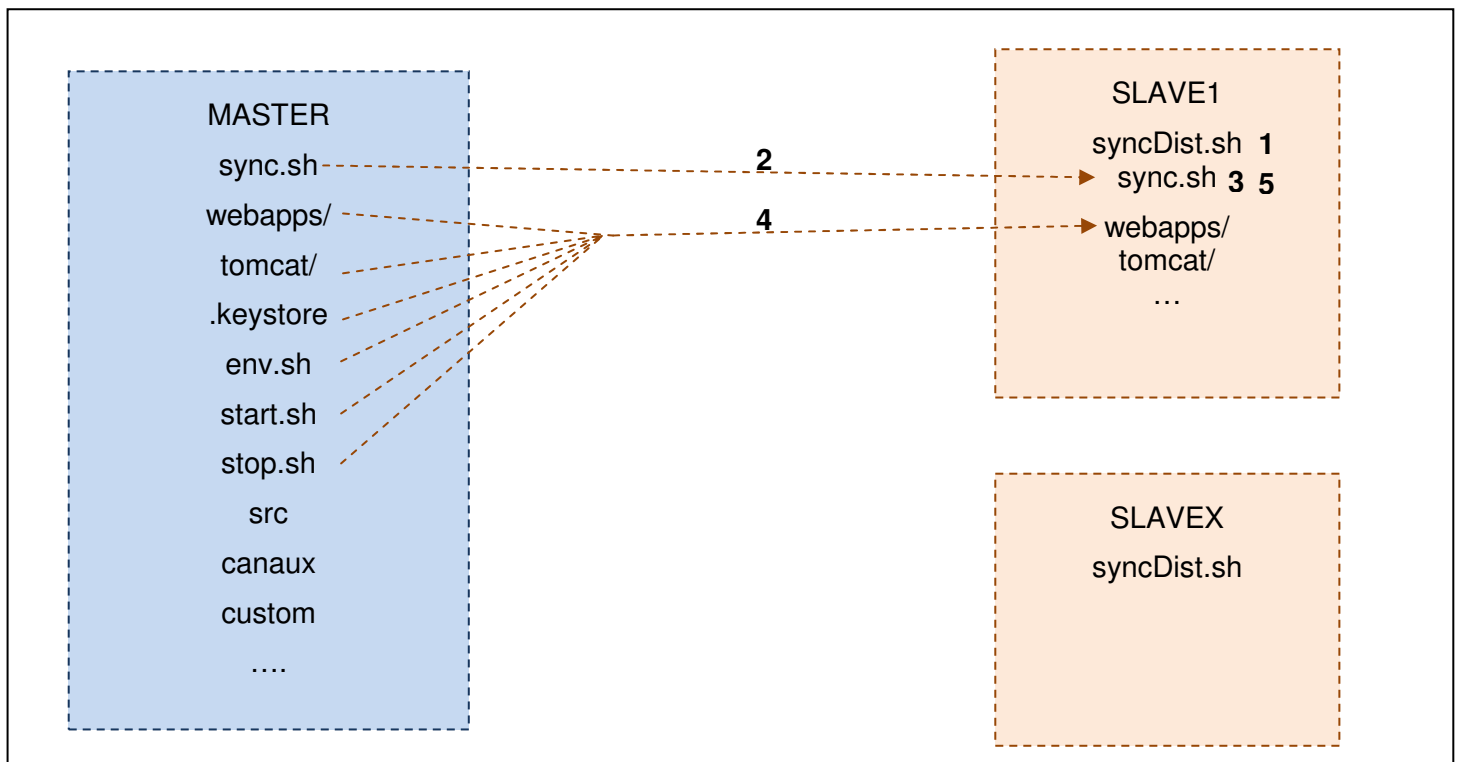
## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

- maven
- jdk
- le package d'installation esup
- vos customs

Les ESCLAVES quand a eux ne contiendrons que :

- tomcat
- jdk
- une copie du webapps du MASTER



Un ESCLAVE lors de sa première synchronisation ne détient qu'un script syncDist.sh (1) ce script va récupérer un script nommé sync.sh (2) sur le MAITRE, lance ce script (3) en donnant le nom logique de l'ESCLAVE (entX)

```
$ more syncDist.sh
```

```
#!/bin/sh
MASTER_HOST=ent1.it-sudparis.eu
SCRIPT_NAME=sync-up3-$RANDOM.sh
PORTAL_HOME=/home/uportal/up-3
TMP=/tmp
LOGICAL_NAME=ent2
```

### Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
/usr/bin/scp uportal@$MASTER_HOST:$PORTAL_HOME/sync.sh $TMP/$SCRIPT_NAME
```

```
/bin/sh $TMP/$SCRIPT_NAME $LOGICAL_NAME
```

```
/bin/rm $TMP/$SCRIPT_NAME
```

Une fois le syncDist.sh lancé on obtient le script sync.sh en local sur l'ESCLAVE. Ce script va récupérer (4) via rsync le tomcat, le webapps, ... il va ensuite appliquer un ensemble de sed afin d'adapter ce qui diffère entre le MAITRE et les ESCALVE (5)

```
$ more sync.sh
```

```
#!/bin/sh
```

```
PORTAL_HOME=/home/uportal/up-3
```

```
MASTER_HOST= ent1.it-sudparis.eu
```

```
MASTER_ID=ent1
```

```
LOCAL_ID=$1
```

```
if [ "$LOCAL_ID" = "" ]; then  
    echo "Il manque le parametre LOCAL_ID"  
    exit;  
fi
```

```
if [ ! -d $PORTAL_HOME ]; then  
    mkdir $PORTAL_HOME  
fi
```

```
rsync -e "ssh -x" --copy-links \  
uportal@$MASTER_HOST:$PORTAL_HOME/env.sh $PORTAL_HOME
```

```
rsync -e "ssh -x" --copy-links \  
uportal@$MASTER_HOST:$PORTAL_HOME/start.sh $PORTAL_HOME
```

```
rsync -e "ssh -x" --copy-links \  
uportal@$MASTER_HOST:$PORTAL_HOME/stop.sh $PORTAL_HOME
```

```
rsync -e "ssh -x" --recursive --links -H --exclude '*~' --delete \  
uportal@$MASTER_HOST:$PORTAL_HOME/web* $PORTAL_HOME/
```

```
rsync -e "ssh -x" --recursive --links -H --exclude '*~' \  
--exclude 'logs/*' -exclude 'work/*' --delete \  
uportal@$MASTER_HOST:$PORTAL_HOME/tomcat* $PORTAL_HOME/
```

```
rsync -e "ssh -x" --copy-links \  
uportal@\$MASTER\_HOST:\$PORTAL\_HOME/esup-portail.keystore \  
$PORTAL_HOME
```

```
# Adapte env.sh
```

```
/bin/sed -i \  
"s|TRUST_CERT=.*$|TRUST_CERT=$PORTAL_HOME/esup-portail.keystore|" \  
$PORTAL_HOME/env.sh
```

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
/bin/sed -i \  
"s|realhttp.host=$MASTER_ID|realhttp.host=$LOCAL_ID|" \  
$PORTAL_HOME/tomcat/webapps/manager/WEB-INF/web.xml
```

```
/bin/sed -i \  
"s|realhttp.host=$MASTER_ID|realhttp.host=$LOCAL_ID|" \  
$PORTAL_HOME/webapps/uPortal/WEB-INF/web.xml
```

```
/bin/sed -i \  
"s|jvm-route=$MASTER_ID|jvm-route=$LOCAL_ID|" \  
$PORTAL_HOME/tomcat/conf/server.xml
```

```
/bin/sed -i \  
"s|logicalName=$MASTER_ID|logicalName=$LOCAL_ID|" \  
$PORTAL_HOME/webapps/uPortal/WEB-INF/log4j.properties
```

```
# Adapte universality.xsl  
/bin/sed -i \  
"s|($MASTER_ID)|($LOCAL_ID)|g" \  
$PORTAL_HOME/webapps/uPortal/WEB-  
INF/classes/layout/theme/universality/messages.xml
```

```
# Adapte portal.properties  
/bin/sed -i \  
"s|org.esupportail.portal.logicalname=$MASTER_ID|org.esupportail.portal.logical  
name=$LOCAL_ID|" \  
$PORTAL_HOME/webapps/uPortal/WEB-INF/classes/properties/portal.properties
```

Ce script est sûrement à adapter au custom des établissements, le principe étant de trouver toute chaîne variant entre le MAITRE et les ESCALVES.

Il reste à positionner dans le crontab une synchronisation des ESCALVES dans la nuit et un redémarrage juste après.

## Monitoring

Le package esup mets à disposition une servlet EsupMonitor (<http://ent.it-sudparis.eu/EsupMonitor>).

Cette servlet donne des l'information en terme de mémoire, d'utilisateur connecté et d'utilisateur anonyme (guest pas encore connecté)

Elle est accessible avec différent paramètres (cf fichier CHANGELOG du package)

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*



```
20091109 : Amelioration de la servlet EsupMonitor :
/EsupMonitor : Display memory information and user connected (line mode)
/EsupMonitor?header=1 : Display headers for memory information and user
connected (line mode)
/EsupMonitor?xml=1 : Display memory information and user connected (xml mode)
/EsupMonitor?xml=full : Display memory information and user connected (xml
mode) full for list login use connected

/EsupMonitor?thread=1 : Display thread information (line mode)
/EsupMonitor?thread=1&header=1 : Display headers for thread information (line
mode)
/EsupMonitor?thread=1&xml=1 : Display thread information (xml mode)
/EsupMonitor?thread=1&xml=full : Display thread information (line mode) full
for list thread stack

/EsupMonitor?datasources=1 : Display datasources information (line mode) [must
have com.sun.management.jmxremote]
/EsupMonitor?datasources=1&header=1 : Display headers for datasources
information (line mode) [must have com.sun.management.jmxremote]
/EsupMonitor?datasources=1&xml=1 : Display datasources information (xml mode)
[must have com.sun.management.jmxremote]
```

Cette servlet peut être exploitée par plusieurs biais.

Le canal Info est distribué dans le package esup portail et permet d'afficher les informations suivantes :

### Informations ENT

	ENT1	ENT2	ENT3	ENT4
<b>Mémoire</b>				
Maximum (Mo)	1398	1398	1398	1398
Total (Mo)	709	789	765	726
Libre (Mo)	76	152	148	175
<b>Sessions</b>				
Total	135	134	140	124
Anonymes	12	14	15	9
Connectés	123	120	125	115
<b>Utilisateurs</b>				

Pour le configurer il suffit de prendre le fichier :

**update**/uPortal/uportal-impl/src/main/resources/properties/channels/org\_esup/CInfos/CInfos.xml

et de le recopier dans son custom en respectant l'arborescence :

### Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

---

**custom**/uPortal/uportal-impl/src/main/resources/properties/channels/org\_esup/CInfos/CInfos.xml

il suffit ensuite de configurer le fichier CInfos.xml

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<config>
  <server name="LOCAL" url="http://ent1-dev.it-sudparis.eu/EsupMonitor" />
  <server name="LOCAL" url="http://ent2-dev.it-sudparis.eu/EsupMonitor" />
  <server name="LOCAL" url="http://entX-dev.it-sudparis.eu/EsupMonitor" />
</config>
```

Un init deploy et un redémarrage du portail appliquera les modifications, ce canal est publier pour les administrateurs du portail.

Il est aussi envisageable de récupérer les informations dans un cacti par exemple (via un script qui fait un wget)

## Syslog

De base le portail log dans des fichiers locaux. Lorsque l'on utilise plusieurs ENT il faut centraliser ces logs sur un syslog. Pour ce faire il faut customiser le fichier :

**update**/uPortal/uportal-war/src/main/webapp/WEB-INF/log4j.properties

il faut donc le mettre dans

**custom**/uPortal/uportal-war/src/main/webapp/WEB-INF/log4j.properties

```
log4j.rootCategory=@esup.log.level@, R
```

```
# http://www.ja-sig.org/wiki/display/UPC/Quieting+Whirlycache
```

```
log4j.logger.com.whirlycott.cache=WARN, R
```

```
# la ligne suivante permet de ne pas loguer les ouvertures fermeture de session
```

```
log4j.logger.org.jasig.portal.jndi.JNDIManager=WARN, R
```

```
# la ligne suivante permet de ne pas loguer les caches de XSLT et SSL
```

```
log4j.logger.org.jasig.portal.utils.XSLT=WARN, R
```

```
#evite les logs info de spring
```

```
log4j.logger.org.springframework=ERROR, R
```

```
#evite les logs webProxy
```

```
log4j.category.org.jasig.portal.channels.webproxy=ERROR, R
```

```
log4j.logger.org.jasig.portal.layout.dlm.FragmentDefinition=WARN, R
```

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
log4j.logger.org.jasig.portal.layout.dlm.PLFIntegrator=WARN, R
log4j.logger.org.jasig.resourceserver.utils.cache.ConfigurablePageCachingFilter
=ERROR, R

log4j.logger.org.jasig.portal.properties.PropertiesManager=ERROR, R
log4j.logger.org.jasig.portal.jndi.JndiManagerImpl=WARN, R
log4j.logger.org.jasig.portal.ChannelManager=WARN, R
log4j.logger.org.hibernate.cfg.AnnotationBinder=WARN, R
log4j.logger.org.hibernate.cfg.SettingsFactory=WARN, R
log4j.logger.org.jasig.portal.tools.checks.InitializingCheckRunner=WARN, R
log4j.logger.org.jasig.portal.layout.dlm.LegacyConfigurationLoader=WARN, R
log4j.logger.org.jasig.resourceserver.utils.cache.ConfigurablePageCachingFiltre=
=ERROR, R
log4j.logger.net.sf.ehcache.constructs.web.filter.CachingFilter=ERROR, R
log4j.logger.org.hibernate=WARN, R
log4j.logger.org.jasig.portal.channels.CGenericXSLT=WARN, R
log4j.logger.org.jasig.portal.portlet.session.PortletSessionExpirationManager=>
ARN, R

#evite les logs webProxy
log4j.category.org.jasig.portal.channels.webproxy=ERROR, R

#Silence an erroneous WARN level log message from Hibernate
log4j.logger.org.hibernate.engine.loading.LoadContexts=ERROR, R
log4j.additivity.org.hibernate.engine.loading.LoadContexts=false

@log_debug_StaticRenderingPipeline@log4j.logger.org.jasig.portal.rendering.Stat
icRenderingPipeline=DEBUG, R
#log4j.logger.org.esupportail.portal.layout.dlm.processing.AuthorisationCheck=D
EBUG, R
#log4j.additivity.org.esupportail.portal.layout.dlm.processing.AuthorisationChe
ck=false

log4j.logger.org.jasig.services.persondir.support.web.RequestAttributeSourceFil
ter=ERROR, R

log4j.appender.R=org.apache.log4j.net.SyslogAppender
log4j.appender.R.SyslogHost=ent1-dev.it-sudparis.eu
log4j.appender.R.Facility=LOCAL5
log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern=@esup.host.logicalName@\t%5p [%t]
[%c] - %m%n

log4j.category.org.esupportail.portal.events.handlers=INFO, stats
log4j.additivity.org.esupportail.portal.events.handlers=false
log4j.category.org.esupportail.portal.services.stats=INFO, stats
log4j.additivity.org.esupportail.portal.services.stats=false
```

---

## Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*

```
log4j.appender.stats=org.apache.log4j.net.SyslogAppender
log4j.appender.stats.SyslogHost= ent1-dev.it-sudparis.eu
log4j.appender.stats.Facility=LOCAL6
log4j.appender.stats.layout=org.apache.log4j.PatternLayout
log4j.appender.stats.layout.ConversionPattern=%d{ISO8601}\t@esup.host.logicalName@\t%m%n
```

Il est intéressant de remonter aussi les logs de statistique sur le MAITRE car on pourra par la suite lancer le package esup-indicateur afin de générer des statistique humainement visible.

### Statistiques

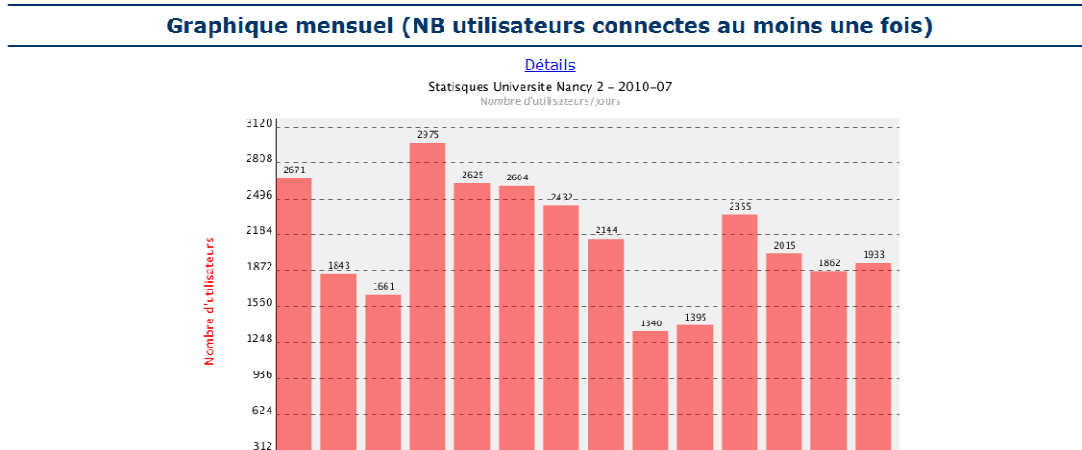
Le portail logs par défaut un fichier de statistique. On peut trouver dans le fichier log4j.properties sa localisation.

Le package esup-indicateur est totalement découplé du portail.

<http://www.esup-portail.org/display/PROJINDIC/Indicateurs+Esup>

Il permet de prendre ce fichier statistique et d'en faire des pages HTML et des graphiques :

Statistiques- Université Nancy 2 - 2010-07					
	Nombre maximum d'utilisateurs possibles	Nombre d'utilisateurs ayant ouvert au moins une fois une session	Nombre d'utilisateurs ayant ouvert au moins 5 sessions dans le mois	Nombre de sessions ouvertes dans la période	Temps moyen d'une session pour la période, en minutes
Global	20672	8544	2358	47312	17
<a href="#">Détails</a>					



La documentation de ce package est assez fournie pour ne pas la redétailler.

Sur le principe ce package prend le fichier statistique l'agrège dans un fichier XML puis le retransforme en fichier HTML et en graphique (SVG => PNG)

### Utilisation et diffusion de ce document

*Il est de la responsabilité de chacun des destinataires de ce document de ne pas le rediffuser en dehors du cadre pour lequel il a été écrit.*