UNIRE – Administration

Objectifs :

- Installer un portail fonctionnant de façon autonome puis le brancher progressivement aux différents composants du système d'information : annuaire LDAP, serveur d'authentification CAS, frontal Apache.
- Se familiariser avec ESUP-Portail : gérer les préférences d'affichage, personnaliser l'environnement par défaut, gérer les groupes, les canaux et les fragments.

I. Préparation :

Créer un répertoire de travail `<REP_TRAVAIL>`. Toutes les installations se feront dans ce répertoire.
Créer une variable d'environnement Windows personnelle PATH :
`PATH=%JAVA_HOME%\bin;%ANT_HOME%\bin;%PATH%`

II. Installation du JDK :

Installer le Java Development Kit dans le répertoire `<REP_TRAVAIL>\JDK`

III. Installation de la distribution esupdev :

Décompresser l'archive `<ARCHIVE_ESUP>` dans le répertoire de travail. Un dossier `<VERSION_ESUP>` est automatiquement créé.

Editer le fichier `ant.bat` :
Modifier la variable `JAVA_HOME` pour qu'elle pointe vers `<REP_TRAVAIL>\JDK`
Modifier la variable `ESUPDEV` pour qu'elle pointe vers `<REP_TRAVAIL>\<VERSION_ESUP>`

Editer le fichier de configuration de la distribution `<VERSION_ESUP>.properties`.
Dans ce fichier sont regroupées toutes les options possibles de configuration de la distribution.

Section 'chemins file system' :
Modifier la variable `java_home` pour qu'elle pointe vers `<REP_TRAVAIL>/JDK`
Modifier la variable `esup.root` pour qu'elle pointe vers `<REP_TRAVAIL>/<VERSION_ESUP>`
Modifier la variable `esup.deploy` pour qu'elle pointe vers `${esup.root}/webapps`

Section 'paramètres LDAP' :

Modifier les variables nécessaires pour ne pas utiliser d'authentification LDAP, ne pas utiliser LDAP pour la récupération des attributs, ne pas utiliser LDAP pour la gestion des groupes.

Section 'accès DB pour la base uPortal' :
Modifier les variables nécessaires pour utiliser la base de données pour l'authentification, pour utiliser un pool de connexion Tomcat (JNDI), et pour utiliser MySQL.
Les paramètres de connexion sont les suivants :
Serveur : `<HOST_SERVEUR_SALLE>`
Base : `<BASE_PORTAIL>`
Login : `<BASE_PORTAIL_LOGIN>`
Password : `<BASE_PORTAIL_MDP>`

Une URL de connexion MySQL est de la forme :
`jdbc:mysql://host[:port]/database`

Section 'paramètres divers' :
Modifier les variables nécessaires pour utiliser un environnement ESUP, une navigation classique uPortal, un nom de portail personnalisé et un niveau de log INFO.

Ouvrir une fenêtre de commande MS-DOS et se placer à la racine du package :
`<REP_TRAVAIL>\<VERSION_ESUP>`
Faire un `'ant esup.init'`
Faire un `'ant esup.db.init'`
Faire un `'ant uportal.deploy'`

Démarrer le portail en lançant la commande `start-esup.bat`.
Tester le portail avec un navigateur en utilisant l'URL http://localhost:8080/uPortal (attention à la casse) et le compte local (auth locale) admin / admin.

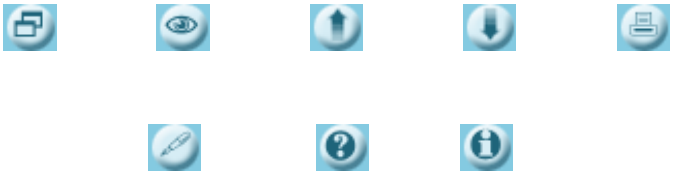
Remarques :
- *En cas de problème, toujours penser à regarder le fichier portal.log.*
- *A chaque init / deploy, les fichiers de configuration du portail sont modifiés. Il est intéressant de regarder ce qui s'y trouve et ce qui change lors de chacune des étapes.*
- *Dans la configuration actuelle, seuls les utilisateurs locaux au portail peuvent se connecter. Tester l'ajout d'un nouvel utilisateur à l'aide de la commande*

`ant uportal.md5passwd -Dusername=newuser`
ainsi que la modification du mot de passe administrateur avec la commande
`ant uportal.md5passwd -Dusername=admin`

IV. Interface et navigation :

Démarrer le portail en lançant la commande `start-esup.bat`.
Se logger sur le portail avec un navigateur en utilisant l'URL http://localhost:8080/uPortal en tant qu'administrateur (auth locale) admin / admin.
Identifier les éléments : Onglets, Colonnes et Canaux.
Tester les options : retour à la page d'accueil, plan du site (les autres options seront vues plus en détail par la suite).

Enfin, observer les rôles des boutons suivants :



V. Préférences utilisateur :

Accéder aux préférences par le bouton 
Ajouter un onglet que l'on nommera « essai » et y ajouter deux colonnes.

Souscription d'un canal :
On va maintenant ajouter un canal dans l'une d'entre elles :
Cliquer sur « ajouter un canal »
Souscrire le canal « Person Attributes » disponible dans la catégorie « uPortal ».
Enfin choisissez l'emplacement du canal.

Déplacer maintenant le canal dans l'autre colonne.
Supprimer la colonne vide.

Remarques :

- *Le bouton*  *indique les endroits où peuvent être positionnés les éléments.*
- *Penser à enregistrer les préférences (*  *) avant de quitter (*  *) sinon elles seront perdues.*

Choix de la skin :
Tester le changement de skin du portail en cliquant sur « Skins »

Choix de la langue :
Cliquez sur « langues » et choisir allemand, suédois ou japonais on constate que le contenu du canal « Person Attributes » a changé.
Remarques :

- *Lorsqu'on remet la langue à « français » le texte apparaît en anglais. En effet, il n'y a pas de XSL correspondant à la langue française pour ce canal c'est donc la XSL par défaut qui est choisie.*
- *La personnalisation des fragments sera vue plus tard.*

VI. Branchement de l'authentification LDAP :

Section 'paramètres LDAP' :
Modifier les paramètres nécessaires pour utiliser une authentification LDAP.
Les paramètres de connexion sont les suivants :
Serveur : `<HOST_SERVEUR_SALLE>`

Port : <PORT_LDAP>
Base : <BASE_LDAP>
Bind : <BIND_LDAP>

Faire un 'ant esup.init'
Faire un 'ant uportal.deploy'

Fichiers de configuration impactés :
- security.properties
- ldap.properties

Tester l'authentification en utilisant le compte LDAP ensXX / ensXX (auth locale).

Remarques :
- *Avant la connexion, le portail ne connaissait pas l'utilisateur ensXX. Ce compte a été automatiquement créé car l'authentification a réussi et le portail fonctionne en mode autocréation.*
- *Ce nouveau compte hérite de toutes les propriétés et de tous les droits du compte 'demo'. Dans le cas particulier de la distribution ESUP, le compte demo a été privé de tous ses droits ce qui explique l'environnement vide du nouvel utilisateur.*
-

VII. Branchement de la récupération d'attributs LDAP :

Section 'paramètres LDAP' :
Modifier les paramètres nécessaires à la récupération d'attributs dans LDAP.

Faire un 'ant esup.init'
Faire un 'ant uportal.deploy'

Fichiers de configuration impactés :
- PersonDirs.xml

Vérifier que l'on récupère bien maintenant les informations de l'annuaire (plus de 'unrecognized person').

Remarques :
- *Par défaut, la récupération d'attributs a été configurée afin de correspondre à la norme Supann.*
- *Pour utiliser la récupération d'attributs avec un annuaire non compatible Supann ou pour personnaliser cette récupération, il est nécessaire d'étudier le fonctionnement du fichier PersonDirs.xml et d'en créer une version propre dans le répertoire Perso.*

VIII. Installation du serveur CAS :

Décompresser l'archive <ARCHIVE_CAS> dans le répertoire <REP_TRAVAIL>.

Editer le fichier de configuration :

`<REP_CAS>\properties\build.properties`.

Configurer une authentification de type simple LDAP en utilisant les mêmes paramètres pour le serveur LDAP que ceux du portail.

Configurer le répertoire de déploiement pour qu'il soit le même que celui du portail :
`<REP_TRAVAIL>/<VERSION_ESUP>/webapps/cas`

Dans une fenêtre de commandes MS-DOS faire un `'ant deploy'`.

Création des certificats

Dans le répertoire `<REP_TRAVAIL>` créer un sous-répertoire `'cert'`.
Ouvrir une fenêtre de commandes MS-DOS et se placer dans ce répertoire.

Création du magasin contenant le couple clé privée / clé publique nécessaire au serveur Tomcat pour fonctionner en HTTPS :

```
<REP_TRAVAIL>\cert\keytool -genkey -alias tomcat -dname "CN=localhost" -keyalg RSA -storepass storepass -keystore server.keystore -keypass storepass
```

Exportation du certificat auto-signé :

```
<REP_TRAVAIL>\cert\keytool -export -alias tomcat -storepass storepass -file certificate.cert -keystore server.keystore
```

Ajout du certificat dans un magasin privé :

```
<REP_TRAVAIL>\cert\keytool -import -v -trustcacerts -alias tomcat -noprompt -file certificate.cert -keystore trust.keystore -storepass storepass
```

Remarques :

- *Les manipulations effectuées ici permettent de tester le fonctionnement du serveur CAS. Toutefois cette solution n'est pas celle préconisée en ce qui concerne la politique de certification.*
- *Il est impossible de faire fonctionner sur une machine deux services différents (deux Tomcat, un Apache et un Tomcat) si ils ne partagent pas le même certificat. Des outils sont disponibles afin de convertir des certificats générés par OpenSSL au format Java (keystores).*

Configuration Tomcat

Copier le fichier :
`<REP_TOMCAT>\conf\server.xml`
Dans :
`<REP_TRAVAIL>\<VERSION_ESUP>\Perso\Tomcat\conf`

Editer le fichier `server.xml` du répertoire `Perso`.

Ajouter un nouveau contexte :

```
<Context  path="/cas"
          docBase="<REP_TRAVAIL>/<VERSION_ESUP>/webapps/cas"
          crossContext="true"
          reloadable="false" />
```

Ajouter un connecteur HTTPS :

```
<Connector      port="8443"
                maxThreads="150"
                minSpareThreads="25"
                maxSpareThreads="75"
                enableLookups="false"
                disableUploadTimeout="true"
                acceptCount="100"
                debug="0"
                scheme="https"
                secure="true"
                clientAuth="false"
                sslProtocol="TLS"

     keystoreFile="<REP_TRAVAIL>/cert/server.keystore"
                keystorePass="storepass" />
```

Dans le fichier de configuration du portail, modifier les paramètres nécessaires pour faire confiance au certificat `<REP_TRAVAIL>/cert/trust.keystore`

Faire un `'ant esup.init'`
Faire un `'ant uportal.deploy'`

Tester le serveur CAS à l'URL suivante : https://localhost:8443/cas
Tester l'authentification avec un compte LDAP valide.

IX. Branchement de l'authentification CAS :

Section 'paramètres CAS'
Modifier les paramètres nécessaires à l'authentification CAS sans mode proxy.

Faire un `'ant esup.init'`
Faire un `'ant uportal.deploy'`

Branchement CAS en mode proxy

Section 'paramètres CAS'
Modifier les paramètres nécessaires pour faire fonctionne CAS en mode proxy.

Section 'paramètres divers'
Modifier les paramètres nécessaires pour passer les logs en mode debug.

Faire un `'ant esup.init'`
Faire un `'ant uportal.deploy'`

Fichiers de configuration impactés :
- security.properties

Vérifier dans le fichier de log que le portail fonctionne bien en mode proxy, le fichier doit contenir des lignes de cette forme :

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
     <cas:authenticationSuccess>
          <cas:user>login</cas:user>
          <cas:proxyGrantingTicket>
               PGTIOU-49993-
          Hrjm0GXyi8kmgT3kbkj8MMDsFaSSi7dcobOtZqKuUQRlK2fSKP
          </cas:proxyGrantingTicket>
     </cas:authenticationSuccess>
 </cas:serviceResponse>
```

X. Utilisation d'un frontal Apache :

Section 'chemins file system' :
Modifier le paramètre pour faire confiance au certificat `<REP_TRAVAIL>/trust.keystore` (le certificat du serveur Apache frontal).

Section 'paramètres http et ports tcp liés à esup-portail' :
Modifier l'URI pour que celle-ci soit de la forme portalXX.

Section 'paramètres CAS' :
Modifier les paramètres nécessaires pour utiliser la machine `<HOST_SERVEUR_SALLE>/cas` comme serveur CAS. L'accès au portail (esup.host.http) doit refléter le passage par le frontal. Enfin les ports HTTP et HTTPS sont désormais standards (80 et 443).

Penser à supprimer les personnalisations de Tomcat afin de retrouver un fonctionnement normal.

Faire un `'ant esup.init'`
Faire un `'ant uportal.deploy'`

Accéder au portail en passant par une URL du type http://<HOST_SERVEUR_SALLE>/portalXX

Valider le fonctionnement proxy.

XI. Les Groupes :

Nous allons maintenant voir les 3 façons de créer des groupes uPortal.

Les groupes locaux :

Cette gestion n'est possible qu'à travers le portail
Se connecter au portail en administrateur et accéder au group manager.

Ajouter un groupe en cliquant sur  du groupe parent ou du root « Tous les groupes de personnes ».

Y ajouter un utilisateur en faisant une recherche : admin par exemple.

Penser à prendre en compte les modifications en cliquant sur 

Remarque :
Une fois créé il n'est pas possible de déplacer le groupe, on peut uniquement le supprimer.

Les groupes LDAP :

Il est fortement déconseillé d'utiliser cette création de groupe, nous allons cependant voir comment procéder sur un petit groupe.

Le mapping :
Nous allons d'abord devoir réaliser le mapping entre les attributs LDAP et les attributs uPortal.

Pour cela copier le fichier :
<REP_UPORTAL>\properties\PersonDirs.xml
Dans :
<REP_TRAVAIL>\<VERSION_ESUP>\Perso\uPortal\properties.

Si l'arborescence n'existe pas la créer.

Ouvrir la copie (Le fichier sera recopié au moment du esup.init).

Adapter les paramètres de connexion LDAP :

```
<url>ldap:// <REP_TRAVAIL>:<PORT_LDAP>/<BASE_LDAP></url>
    <logonid></logonid>
    <logonpassword></logonpassword>
    <uidquery>(uid={0})</uidquery>
    <usercontext></usercontext>
```

Faire correspondre les éléments suivants (LDAP)

```
<attribute>
        <name>n2atrtypepeople</name>
        <alias>typepeople</alias>
</attribute>
```

Remarques :

- *Le* « name » *est l'attribut source de données et l'* « alias » *est l'attribut uPortal*
- *Attention à la casse.*

LDAPGroupStoreConfig.xml

Copier le fichier :
<REP_UPORTAL>\properties\groups\LDAPGroupStoreConfig.xml
Dans :
<REP_TRAVAIL>\<VERSION_ESUP>\Perso\uPortal\properties\groups.

Ouvrir la copie.
Créer un groupe de ce type contenant un simple sous-groupe.

```
<LDAPGroupStore>
     <config>

     <url>ldap://<REP_TRAVAIL>:<PORT_LDAP>/<BASE_LDAP></url>
          <logonid></logonid>
          <logonpassword></logonpassword>
          <keyfield>uid</keyfield>
          <namefield>cn</namefield>
          <usercontext>ou=people</usercontext>
          <refresh-minutes>120</refresh-minutes>
     </config>
        <group name="LDAP Groups" key = "all">
          <description>groupe issu ldap pas bien</description>
          <group name="Personnel LDAP Groups" key="1">
                  <description>les personnels</description>
                  <entity-set>
                          <filter
string="n2atrtypepeople=PERS_EMP"/>
                  </entity-set>
          </group>

      </group>
</LDAPGroupStore>
```

Utiliser ce filtre qui contient un nombre d'utilisateurs restreint.

compositeGroupServices.xml

Copier le fichier :
<REP_UPORTAL>\properties\groups\compositeGroupServices.xml
Dans :
<REP_TRAVAIL>\<VERSION_ESUP>\Perso\uPortal\properties\groups.

Ouvrir la copie.

Décommenter alors la partie qui correspond au service LDAP :
`<service><name>ldap</name>` …

Lancer les commandes ant esup.init et ant uportal.deploy puis relancer le portail.
Le groupe nouvellement créé n'est pas rattaché à l'arborescence des groupes. Il vous faut alors l'ajouter comme un membre (c'est-à-dire avec une recherche) grâce au group manager du portail.

Il apparaît maintenant dans votre arborescence avec les utilisateurs qu'il contient. Vous constaterez peut être que l'affichage est long et comprendrez pourquoi cette méthodes n'est pas envisageable pour des groupes contenant beaucoup d'utilisateurs.

Les groupes PAGS :

L'appartenance à un groupe est calculée, à la connexion de l'utilisateur, suivant ses attributs uPortal de personne. On utilisera pour cela le mapping (vu précédemment). Par conséquent, ce service est incapable de lister les membres d'un groupe.

PAGSGroupStoreConfig.xml

Copier le fichier :
`<REP_UPORTAL>\properties\groups\PAGSGroupStoreConfig.xml`
Dans :
`<REP_TRAVAIL>\<VERSION_ESUP>\Perso\uPortal\properties\groups.`

Ouvrir la copie.

Créer deux groupes avec un XML ce type :

```
<Group-Store>
  <group>
    <group-key>TousPers</group-key>
    <group-name>LDAP Tout le personnel enseignant</group-name>
    <group-description>Tout le personnel enseignant de
l'etablissement issu de LDAP</group-description>
    <selection-test>
      <test-group>
        <test>
          <attribute-name>typepeople</attribute-name>
          <tester-
class>org.jasig.portal.groups.pags.testers.StringEqualsIgnoreC
aseTester</tester-class>
          <test-value>PERS_ENS</test-value>
        </test>
      </test-group>
    </selection-test>
  </group>
```

```
  <group>
    <group-key>TousEtud</group-key>
    <group-name>LDAP Tous les etudiants</group-name>
    <group-description>Tous les etudiants de l'etablissement
issu de LDAP</group-description>
    <selection-test>
      <test-group>
        <test>
          <attribute-name>typepeople</attribute-name>
          <tester-
class>org.jasig.portal.groups.pags.testers.StringEqualsIgnoreC
aseTester</tester-class>
          <test-value>APO_N2</test-value>
        </test>
      </test-group>
    </selection-test>
  </group>
</Group-Store>
```

compositeGroupServices.xml

Ouvrir le fichier :
`<REP_TRAVAIL>\<VERSION_ESUP>\Perso\uPortal\properties\groups\compositeGroupServices.xml`

Décommenter alors la partie qui correspond au service PAGS : `<service><name>pags</name>` …

Lancer les commandes ant esup.init et ant uportal.deploy puis relancer le portail.
Le groupe nouvellement créé n'est pas rattaché à l'arborescence des groupes. Il vous faut alors l'ajouter comme un membre (c'est-à-dire avec une recherche) grâce au group manager du portail.

Il apparaît maintenant dans votre arborescence en revanche les utilisateurs qu'il contient ne sont pas affiché. En effet, c'est au moment de la connexion de l'utilisateur ou lorsqu'il va chercher à accéder à une ressource protégée que le portail vérifiera son appartenance ou non au(x) groupe(s) autorisé(s).

Remarque :

Pour les groupes PAGS comme pour les groupes LDAP, il est possible de faire des groupes basés sir des tests plus fins. Ex : ((ou=100 ET cn=v) OU (ou=101 ET cn=w*)). Pour cela consulter la documentation en ligne (ou les commentaires de la présentation powerpoint).*

XII. Publication d'un canal :

Nous allons déployer un nouveau canal dans le portail afin de pouvoir le publier.

Décompresser l'archive `hello.zip` qui contient deux répertoires « virginia » et « edu » et le fichier `pubchan_CHello.xml`.

Copier le répertoire « virginia » dans :
`<REP_UPORTAL>\source\edu`

Copier le répertoire « edu » dans :
`<REP_UPORTAL>\webpages\stylesheets`
Faire un `'ant uportal.deploy'`

Remarque :

La méthode n'est pas propre mais le déploiement de canal n'est pas l'objet de cette formation. Nous verrons ce point dans la formation développement en décembre.

Le canal déployé doit maintenant être publié afin d'être mis à la disposition des utilisateurs.

Publication à travers le portail :

Sur le portail cliquer sur  puis sur « Publish a new channel »
Choisir le type « Custom »
Faire pointer le canal vers la classe :
`edu.virginia.uportal.channels.helloworld.CHelloWorld`
Il n'y a pas de paramètres (faire « next »)
Cocher le « Has about » ce qui indique que le canal possède un fichier de description qui sera accessible à l'utilisateur.
Enfin choisir une ou plusieurs catégorie(s) et un ou plusieurs groupe(s) pour ce nouveau canal.
Terminer par « finished ».

Vous pouvez alors souscrire le canal comme on l'a vu ci-dessus. Vous devez pouvoir saisir un nom et afficher « Hello »

Retourner sur le gestionnaire de canaux et cliquer sur « Modify a currently published channel »
Supprimer la publication que vous venez de faire.

Remarque :
Si on se déconnecte et on se reconnecte le message « `The <nom_channel> channel is no longer available. Please remove it from your layout !` *» apparaît à la place du canal.*

Publication par une directive ant :

Ouvrir le fichier `pubchan_CHello.xml` et le modifier à votre convenance.
Copier le fichier `pubchan_CHello.xml` dans le répertoire :
`<REP_TRAVAIL>\<VERSION_ESUP>\Perso\uPortal\properties\chanpub.`

Si l'arborescence n'existe pas la créer (Le fichier sera recopié au moment du esup.init `dans <REP_UPORTAL>\properties\chanpub)`.

Remarque :
C'est dans ce répertoire qu'apparaissent les fichiers des canaux à publier par défaut.

Lancer les commandes ant esup.init et ant uportal.deploy.
Lancer ensuite la commande :
`ant uportal.pubchan -Dchannel= pubchan_CHello.xml`
Relancer le portail.
Retourner sur le gestionnaire de canaux et cliquer sur « Modify a currently published channel ». Votre publication doit apparaître dans la liste.
Vous pouvez alors souscrire le canal comme on l'a vu ci-dessus.

XIII. Les Fragments :

Le portail permet la création d'ensembles définis de contenu associés à un ou plusieurs groupes. Ceci peut être très utile dans le cadre d'un déploiement au sein d'une université car les fragments permettent un affichage des canaux pertinents définis en fonction du public.

Fragments à travers le portail :

Accéder aux préférences par le bouton  et choisir « Fragments »
Créer un fragment pushed ou pulled
Modifier ensuite ses propriétés :

- y ajouter 2 canaux de la même manière que pour une souscription de canaux traditionnelle : « hello » et « Person Attributes » par exemple.
- Lier le fragment à un ou plusieurs groupe(s)

Remarque : Penser à enregistrer les préférences ( *) avant de quitter (*  *) sinon elles seront perdues.*

Déconnecter et reconnecter avec un utilisateur appartenant à un des groupes choisis.
Les fragments pushed apparaissent dans les onglets et les fragments pulled peuvent être souscrit de la même manière qu'un canal dans la catégorie « Fragments ».

Fragments par une directive ant :

Dans cette version seule la création de fragments pushed est possible (la nouvelle version de uPortal permettra cette opération).
Récupérer et adapter le fichier `frag.xml`.
Copier ce fichier dans :

`<REP_TRAVAIL>\<VERSION_ESUP>\Perso\uPortal\properties\al`

Si l'arborescence n'existe pas la créer (Le fichier sera recopié au moment du esup.init dans `<REP_UPORTAL>\properties\al)`.

Lancer les commandes ant esup.init et ant uportal.deploy

Lancer la commande :
ant uportal.pushfragment -DfragmentFile=properties/al/frag.xml

Relancer le portail et se connecter avec un utilisateur appartenant à un des groupes choisis : le fragment apparaît.

Remarque : Ces fragments n'apparaissent pas dans le gestionnaire de fragments et ne peuvent donc pas être supprimés ou modifiés.