Manuel d'installation de la v2

Une documentation d'installation plus complète avec utilisation de Git sera disponible prochainement ici

Nous décrivons ici une procédure pour l'installation de esup-activ 2.x

Préambule

esup-activ comprend 2 composants (comptex et esup-activ-bo) qui doivent être installés et configurés séparément. Ces 2 composants communiquent en SOAP. Il faut donc s'assurer que le flux réseau de comptex vers esup-activ-bo:port_tomcat est ouvert.

comptex : interfaces utilisateurs

esup-activ-bo : composant back-office exécutant les opérations d'activation de compte, de modification de mot de passe, ...

En raison de son caractère critique (accès privilégié à la base des utisateurs : LDAP, Kerberos, ...), nous recommandons d'installer ce module sur un serveur non accessible directement par les utilisateurs. On l'installera, par exemple, sur le serveur comportant les scripts de synchronisation et de création de comptes utilisateurs de votre SI.

Quelques définitions

- **Activation :** l'activation consiste à assigner un mot de passe à compte pour la première fois. On ne peut pas activer un compte plus d'une fois. L'application vérifie si l'attribut *ldap.attribute.shadowLastChange* existe. Si ce dernier n'existe pas, elle autorise l'activation du compte sinon elle renvoie un message d'erreur informant que le compte est déjà activé. À l'activation, l'application initialise *ldap.attribute.shadowLastChange* à la date courante. Il est prévu d'abandonner cet attribut au profit de *accountStatus* qui contiendra les états d'un compte ([vide], active, noaccess, disabled, deleted). On essayera de garder une compatibilité avec la procédure actuelle de *shadowLastChange*.
- **Réinitialisation** : procédure permettant aux utilisateurs de renseigner un nouveau mot de passe suite à un oubli de l'ancien. Cette procédure nécessite un code de réinitialisation qui est envoyé via différents canaux (SMS, mail perso, assistance, ...). Le taille du code et les types de canaux disponibles sont personnalisables.
- **changement de login** : cette procédure permet aux utilisateurs de choisir leur identifiant d'authentification. Cela suppose qu'on distingue l'identifiant applicatif (uid) de l'identifiant utilisateur (supannAliasLogin). Les SSO doivent être configurés en conséquence. Il faut, par exemple, que CAS utilise le supannAliasLogin comme identifiant utilisateur mais renvoie l'UID aux applications. Le login que peut choisir l'utilisateur peut être contrôlé. On peut, par exemple, limiter à une certaine combinaison des nom-prénom de l'utilisateur.

Installation

Pré-requis

- java 8 ou supérieur (validé java 8/11)
- tomcat 7 ou supérieur (validé tomcat 7/8.5)
- ant ou maven

Installation comptex

Voir https://github.com/UnivParis1/comptex/blob/master/README.md

Installation esup-activ-bo

- dézipper la dernière version disponible de esup-activ-bo
- éditer le fichier build.properties et renseigner les propriétés suivantes

```
-quick-start=true
+deploy.type=servlet
+deploy.home=/usr/local/activ/tomcat/webapps/esup-activ-bo #à adapter par rapport à votre installation de tomcat
```

- dans le dossier "properties" créer un lien symbolique config.properties -> config.sample.properties [esup-activ-fo# ln -s config.sample.properties properties/config.properties]
- renseigner les propriétés de properties/config.properties. Notamment,

```
ldap.host
ldap.dn.XXX
cas.XXX      # si utilisation de la fonctionnalité de consultation/modification des données utilisateur
authentication.type
kerberos.XXX #si utilisation de l'authentification kerberos
```

Pour déployer l'application : **ant deploy**

Pour tester, utilisez l'url http://xxxx/esup-activ-bo/xfire