Bonita LDAP Configuration (for JOnAS)

This document is a HowTo describing necessary steps for install and configures Bonita with your LDAP directory. After this operation, you will use your own LDAP in order to control user's access to Bonita Workflow System. This configuration is specifically for JOnAS Application Server 3.3.5 version.

For the moment, Bonita's LDAP module offers two functionalities:

- Bonita User Authorization Access via LDAP.
- Users import from your LDAP directory to Bonita user's database.

Installation

- The EJB implementing this function is compiled and deployed with others bonita files (under ejb/hero/session repository).
- Ldap module for JOnAS application server needs *javax77.jar* and *mejb.jar* files, so you have to invoke the ldap config task with the command: *ant configLdap*, in order to copy and deploy these files into JOnAS directory.

Configuration

- As importLdap bean uses JMX, an LDAP resource in the JOnAS-realm.xml file is required
- The configuration of this resource is detailed in the JONAS documentation (you can also use JonasAdmin graphical tool to add the new ldap realm; defaults are provided)
- Notice that you must have one and only one LDAP resources in JOnAS, otherwise the ldapImport method will fail.
- The ldap base could be also your authentication base for both JOnAS and bonita. For JOnAS, see the documentation. For bonita you have to set the ldap resourceName for bonita context in $JONAS_ROOT/conf/server.xml and in $JONAS_ROOT/conf/jaas.config for bonita entries.
- Configuration example:

```
<jonas-ldaprealm>
  <ldaprealm name="ldaprlm_1"
        baseDN="ou=fr,o=Bull, c=fr"
        initialContextFactory="com.sun.jndi.ldap.LdapCtxFactory"
        providerUrl="ldap://serveur_host:389"
        securityAuthentication="simple"
        authenticationMode="bind"
        userPasswordAttribute="userPassword"
        userRolesAttribute="memberOf"
        roleNameAttribute="cn"
        userDN="ou=frec_users,ou=fr,o=Bull, c=fr"
        userSearchFilter="uid={0}"
        roleDN="ou=frec_groups,ou=fr,o=Bull, c=fr"
        roleSearchFilter="uniqueMember={0}"
        referral="follow" />
</jonas-ldaprealm>
```

What do this ldap Import?

This function is intended to search users under the *userDN* subtree with the *userSearchFilter* filter and then for each found user get the attribute value specified into the userSearchFilter and also get the mail attribute value (assuming that the attribute name for email in the ldap is: *mail*, otherwise change it in the bean code). No mapping attribute name for email has been yet introduced.

If the user doesn't exists in the bonita base, it is created by calling the userCreate() API with parameters: name, password (filled in with the name value) , mail. If it already exists, the email is updated (the user identifier in bonita db is the column-name: name). Remember also that all users in bonita db that no more exist in the ldap subtree (and only if the user is not involved in workflow projects) are removed. Previous operation except the default users of Bonita Workflow System: “admin”, “admin2”, “nobody”.

How you can use it?

- This function can be integrated into your administration module. See example provided under *src\main\client\hero\client\importLdap* to call the bean method.
- You can also simply invoke the ldap import with the command: *ant importLdap* –Duser=<uid> -Dpaswd=<password> from your $BONITA_HOME directory.

The user with the uid and password provided to the importLdap ant task has to be previously declared into the directory under the *userDN* subtree and has also to be member of the group Admin (under the *RoleDN* subtree)

Note: if the ldap server acts as your authentication base while the Bonita base is your user base, you have also to declare the user accessing the bonita admin console as member of the Admin group (under the *RoleDN* subtree)