ESUP Portail

Plugin Nuxeo Shibboleth

Atelier GED du 30/03/2011

Raymond Bourges – Université de Rennes 1

Configuration

- **bin/nuxeo.con**
  - nuxeo.templates=**custom**
- **templates/custom**
  - nxserver
    - bundles
      - nuxeo-platform-login-shibboleth-5.4.0.1-HF07.jar
      - nuxeo-platform-shibboleth-groups-web-5.4.0.1-HF07.jar
    - config
      - default-sql-directories-bundle.xml
      - ldap-config.xml
      - nuxeo.defaults
      - shibboleth-config.xml
      - shibboleth-groups-config.xml
      - userShib.xsd

Configuration

- **nuxeo.defaults**
  - nuxeo.template.includes=default,postgresql
- **shibboleth-config.xml**
  - <extension target="...PluggableAuthenticationService" point="chain">
    - <authenticationChain>
      <plugins>
      <plugin>BASIC_AUTH</plugin>
      <plugin>**SHIB_AUTH**</plugin>
  - <extension target="org.nuxeo.ecm.core.schema.TypeService" point="schema">
    - <schema name="user" src="**userShib.xsd**" override="true" />

Configuration

- **shibboleth-config.xml (suite)**
  - <extension target="...ShibbolethAuthenticationService" point="config">
    <config>
    <uidHeaders>
    <uidHeader idpUrl="https://ident-shib-test.univ-rennes1.fr/shibboleth">uid</uidHeader>
    <default>mail</default>
    </uidHeaders>
    <loginURL>http://sp-test3.univ-rennes1.fr/Shibboleth.sso/wayf</loginURL>
    <logoutURL>http://sp-test3.univ-rennes1.fr/Shibboleth.sso/Logout</logoutURL>
    <fieldMapping header="mail">email</fieldMapping>
    <fieldMapping header="sn">lastName</fieldMapping>
    <fieldMapping header="givenName">firstName</fieldMapping>
    <fieldMapping header="departmentNumber">company</fieldMapping>

Configuration

- **shibboleth-config.xml (suite)**
  - <extension target="...UserService" point="userManager">
    <userManager class="...**UserManagerWithComputedGroups**">
    <users>
    <anonymousUser id="Guest">
    <property name="firstName">Guest</property>
    <property name="lastName">User</property>
    <property name="email">foo@bidon.fr</property>

  - <extension target="...UserService" point="userManager">
    <userManager class="...UserManagerWithComputedGroups">
    <defaultAdministratorId>bourges</defaultAdministratorId>
    <defaultGroup>members</defaultGroup>

Configuration

- **userShib.xsd**
  - Ajout de nouveaux attributs
    - <?xml version="1.0"?>
      <xs:schema targetNamespace="http://www.nuxeo.org/ecm/schemas/user"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:nxs="http://www.nuxeo.org/ecm/schemas/user">
      <xs:include schemaLocation="base.xsd" />
      <xs:element name="username" type="xs:string" />
      .../...
      <xs:element name="**affiliation**" type="xs:string" />
  - À mapper sur des attributs Shibboleth
  - Utilisable dans des définitions de groupes Shibboleth
  - **Attention** de ne pas vider votre table users !

Configuration

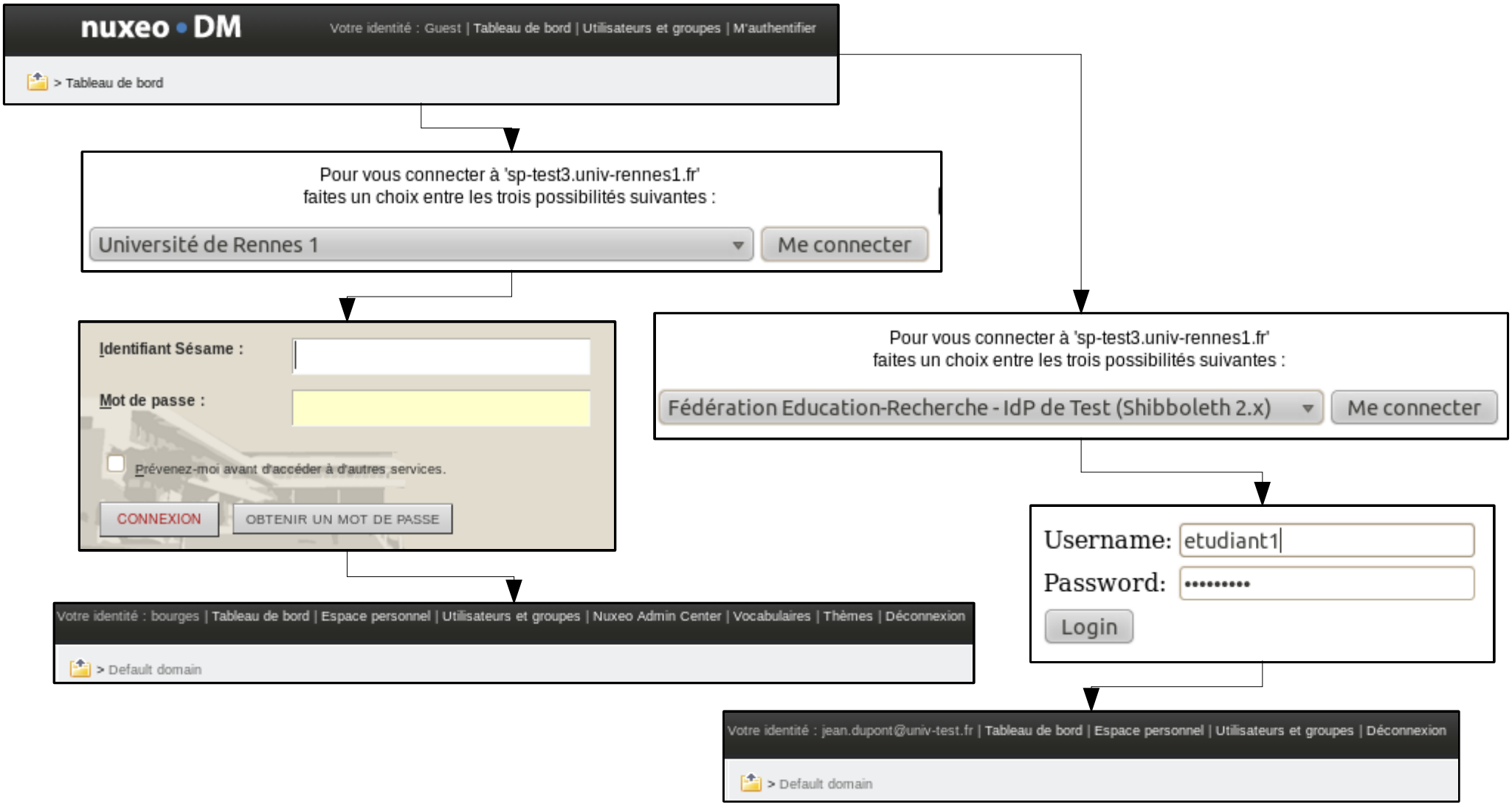
- **shibboleth-groups-config.xml**
  - <extension target="...ShibbolethGroupsService" point="config">
    <config>
    <parseString>:</parseString>
  - Le caractère : est utilisé faire apparaître le groupe dans arbre.
  - Ex : niv1:niv2:grp1
    - niv1
      - niv2
        - » grp1

Configuration

- **default-sql-directories-bundle.xml et ldap-config.xml**
  - Utilisation MultiDirectoryFactory
    - Pour utiliser LDAP **et** SQL
  - LDAP pour accéder aux comptes locaux
  - SQL pour stocker les informations obtenues au moment de la connexion Shibboleth

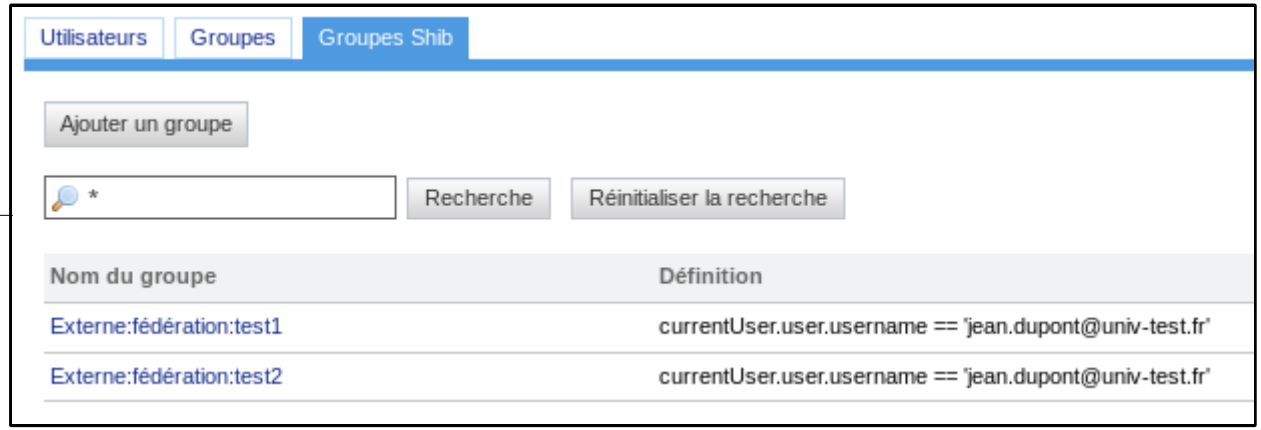
Fonctionnalités

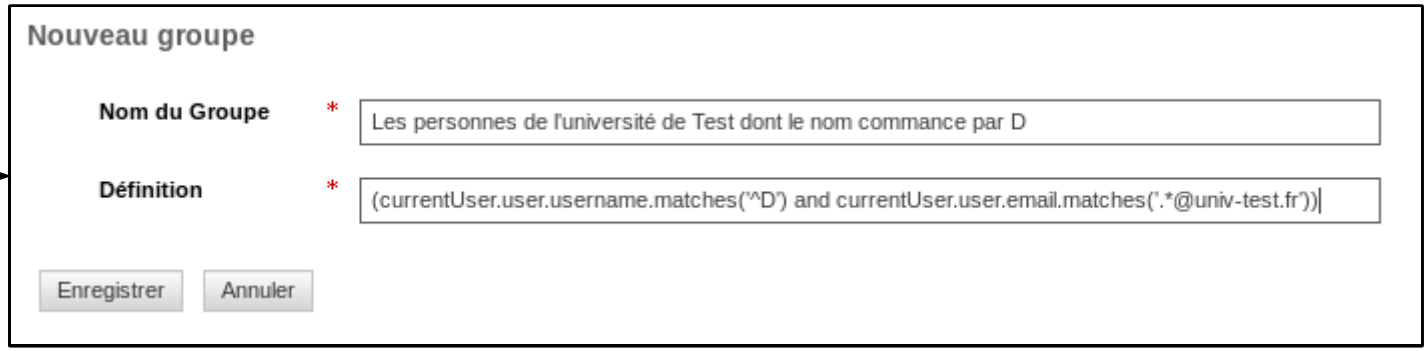
- **Identification**



Fonctionnalités

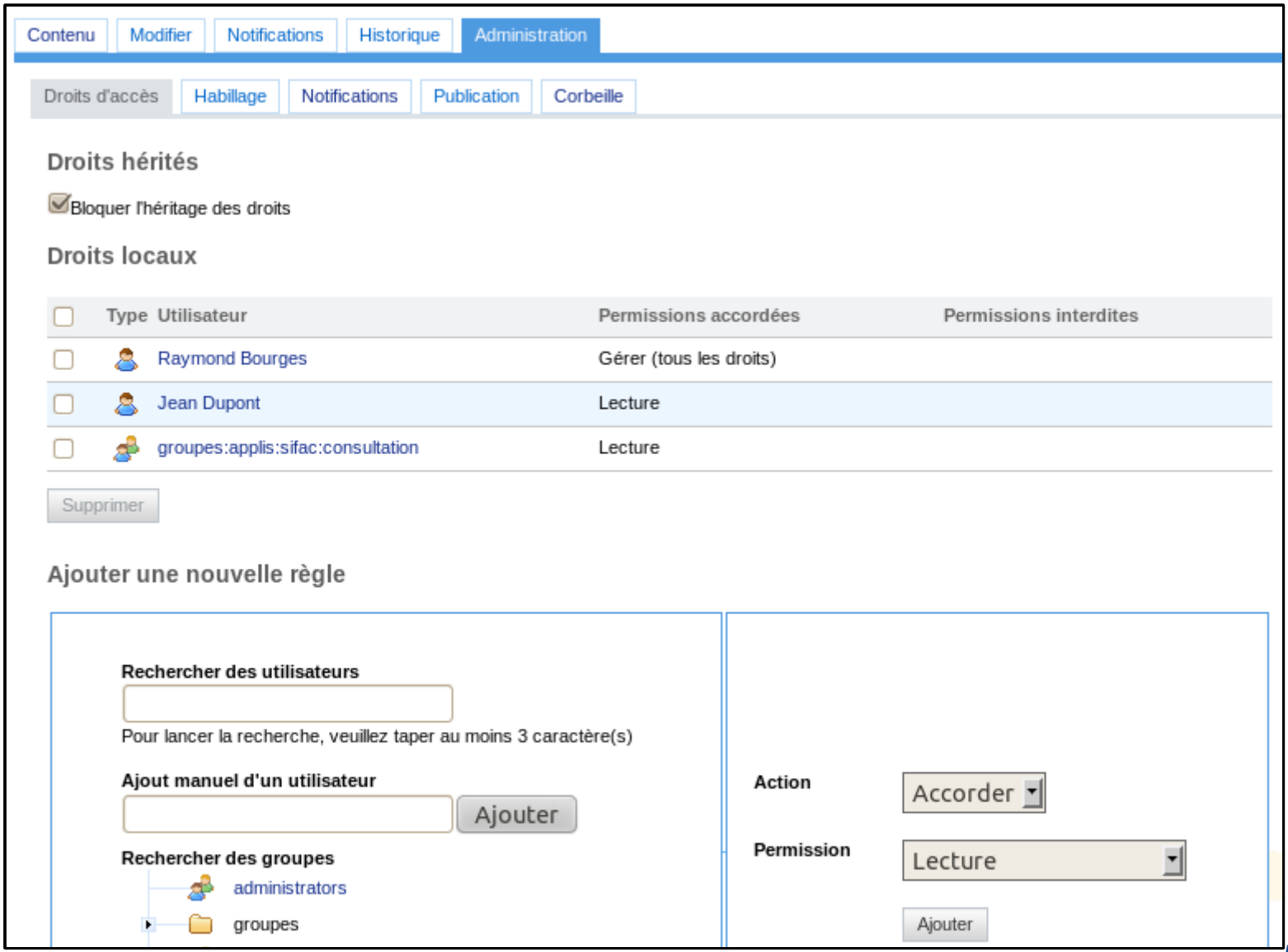
- **Définition des groupes Shibboleth**





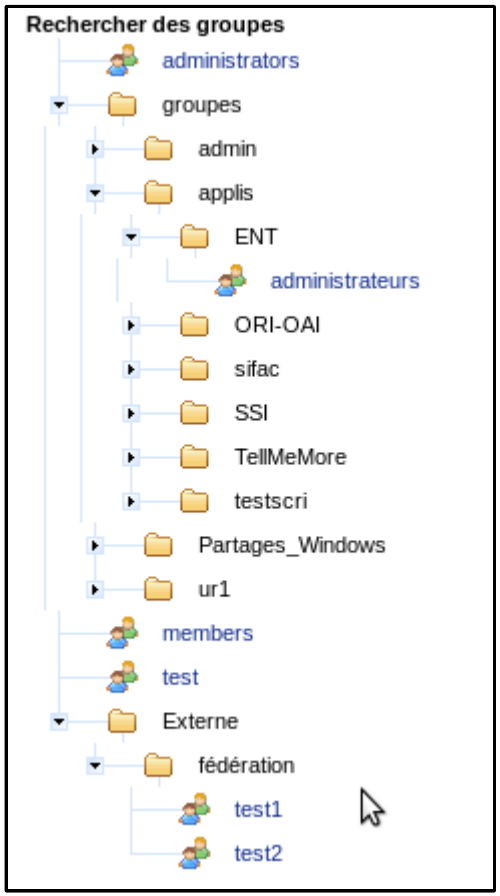
Fonctionnalités

- **Définition des ACL**



Fonctionnalités

- **Définition des ACL**
  - Sélection des groupes
    - Sous forme d'un arbre
    - Groupes Grouper
    - Groupes Shibboleth



Divers

- **Dysfonctionnements et questions**
  - java.io.FileNotFoundException:
    - nuxeo-platform-shibboleth-groups-web-5.4.0.1-HF07.jar.tmp/l10n/messages_en.properties
  - Faut-il permettre de saisir un user externe ?
    - Permettre de saisir un user sur une ACL avant une première connexion
      - Quel Identifiant utiliser ? Email ? EPPN ?
    - Si oui, on ne le voit pas dans la liste des ACE !
  - Erreur dans les recherches inverses entre LDAP et Shib
    - entry 'Externe:fédération:test2' cannot be found in 'ldapGroupDirectory'
  - Version de JUEL
    - Ne permet pas les méthodes matches
      - Passage nouvelle version et débranchement du contrôle ?
  - Les groupes externes apparaissent en fin de liste

Licence