Configuration de CAS LDAP

Pré-requis

Avoir procédé à l'installation minimale de Nuxeo.

Avoir un serveur CAS et un annuaire fonctionnels.

Paramétrage de CAS

Récupération du plugin

Nuxeo fournit un plugin d'atuhentification CAS que vous pouvez récupérer ici : https://maven.nuxeo.org/nexus/index.html#nexus-search;quick~nuxeo-platform-login-cas2

> ⚠ Si vous souhaitez utiliser les fonctionnalités du mode Proxy de CAS, le plugin original vous retournera probablement une erreur. Nous proposons une version patchée de ce plugin que vous pourrez trouver ici.

Copiez le ensuite dans votre dossier templates/custom/bundles (se référer à la documentation sur l'utilisation des templates au besoin). Vous pouvez également choisir de créer un template spécifique "cas" pour y stocker le jar et le point d'extension associé.

Configuration du fichier esup-login-cas-config.xml

Éditez le fichier custom/config/esup-login-cas-config.xml comme suit avec vos propres paramètres :

```
<?xml version="1.0"?>
<component name="org.esup.ecm.login">

<!-- certains composants doivent être charges avant que ce fichier soit lu car ils contiennent des points
d'extension sur l'authentification qui peuvent
 eventuellement surcharger cette configuration, les composants appele dans les balises require dependent donc
de votre configuration -->
<require>org.nuxeo.ecm.platform.ui.web.auth.defaultConfig</require>
<require>org.nuxeo.ecm.platform.ui.web.auth.WebEngineConfig</require>
<require>org.nuxeo.ecm.platform.login.Cas2SSO</require>

<extension target="org.nuxeo.ecm.platform.ui.web.auth.service.PluggableAuthenticationService" point="
authenticators">
 <authenticationPlugin name="CAS2_AUTH">
    <loginModulePlugin>Trusting_LM</loginModulePlugin>
    <needStartingURLSaving>true</needStartingURLSaving>
    <parameters>
         <!-- variable contenant le ticket dans l'url -->
         <parameter name="ticketKey">ticket</parameter>

         <!-- si utilisation du mode proxy -->
         <parameter name="proxyKey">ticket</parameter>

         <parameter name="appURL">https://nuxeo.my-univ.fr/nuxeo/nxstartup.faces</parameter>

         <!-- URL de login du serveur CAS -->
         <parameter name="serviceLoginURL">https://sso.my-univ.fr/login</parameter>

         <!-- URL de validation du ticket du serveur CAS -->
         <parameter name="serviceValidateURL">https://sso.my-univ.fr/serviceValidate</parameter>

          <!-- Si utilisation de CAS en mode proxy -->
          <parameter name="proxyValidateURL">https://sso.my-univ.fr/proxyValidate</parameter>

          <!-- variable contenant le nom du service dans l'URL -->
          <parameter name="serviceKey">service</parameter>

           <!-- URL de logout de CAS -->
          <parameter name="logoutURL">https://sso.my-univ.fr/logout?service=http://nuxeo.my-univ.fr/nuxeo/<
/parameter>
     </parameters>
   </authenticationPlugin>

   <authenticationPlugin name="ANONYMOUS_AUTH_FOR_CAS2" enabled="true" class="org.nuxeo.ecm.platform.ui.web.
auth.cas2.AnonymousAuthenticatorForCAS2" >
        <loginModulePlugin>Trusting_LM</loginModulePlugin>
   </authenticationPlugin>
</extension>

<!-- chainage de l'authentification : on garde une authentification de type BASIC pour les acces particuliers
(RSS/cmis/contentAutomation)-->
<extension target="org.nuxeo.ecm.platform.ui.web.auth.service.PluggableAuthenticationService"
        point="chain">
        <authenticationChain>
            <plugins>
                <plugin>BASIC_AUTH</plugin>
                <plugin>CAS2_AUTH</plugin>
                <plugin>ANONYMOUS_AUTH_FOR_CAS2</plugin>
            </plugins>
        </authenticationChain>
</extension>
</component>
```

Configuration d'un annuaire LDAP

Définition de l'annuaire et paramétrage des recherche pour les utilisateurs

Éditez le fichier **custom/config/default-ldap-users-directory-bundle.xml** comme suit avec vos propres paramètres :

```
<?xml version="1.0"?>
<component name="org.esup.ecm.directory.ldap.storage.users">

  <require>org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory</require>
  <require>org.nuxeo.ecm.directory.sql.storage</require>

   <!-- configuration de la connexion : definition du serveur -->
  <extension target="org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory" point="servers">
    <server name="default">

      <!-- url du serveur -->
      <ldapUrl>ldap://ldap.my-univ.fr:389</ldapUrl>

      <!-- replicas eventuel pour tolerance de panne -->
      <!-- <ldapUrl>ldap://ldap2?my-univ.fr:389</ldapUrl> -->

      <!--utilisateur et mot de passe en cas de bind non anonyme -->
      <bindDn>cn=binduser,ou=admin,dc=my-univ,dc=fr</bindDn>
      <bindPassword>verySecret</bindPassword>

    </server>

 </extension>

 <extension target="org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory" point="directories">

    <!-- configuration du repertoire utilisateur, modifications par rapport aux versions 5.4.1 et anterieures
de nuxeo -->
    <directory name="userLdapDirectory">

     <!-- on s'appuie sur la connexion qu'on vient de définir -->
     <server>default</server>

     <!-- schema nuxeo utilisé : par defaut user -->
     <schema>user</schema>

      <!-- identifiant/mdp des personnes (dans nuxeo) -->
      <idField>username</idField>
      <passwordField>password</passwordField>

      <!-- branche ldap dans laquelle sont situes les utilisateurs -->
      <searchBaseDn>ou=people,dc=my-univ,dc=fr</searchBaseDn>

      <!-- ObjectClass a rechercher => ajouté au filtre de recherche -->
      <searchClass>person</searchClass>

      <!-- filtre de recherche personnalisé (ajouté au filtre par défaut) -->
      <searchFilter>(&amp;(!(eduPersonAffiliation=affiliate))(status=valide))</searchFilter>

      <!-- Portee de la recherche -->
      <searchScope>onelevel</searchScope>

      <!-- Type de recherches possibles :
               subinitial : toto => recherche sur toto*
               subfinal : toto => recherche sur *toto
               subany : toto => recherche sur *toto*
            Par defaut la recherche est en subinitial -->
      <substringMatchType>subinitial</substringMatchType>

     <!-- Si False avec un binddn ayant des acces en ecriture sur l'annuaire, proposera
      d'ajouter des utilisateurs dans l'annuaire -->
      <readOnly>true</readOnly>

     <!-- cache timeout en secondes -->
     <cacheTimeout>3600</cacheTimeout>

     <!-- nombre maximal d'entrees en cache -->
      <cacheMaxSize>1000</cacheMaxSize>
```

```
    <!-- utilisé pour éventuellement creer des utilisateurs depuis nuxeo ... -->
      <creationBaseDn>ou=people,dc=my-univ,dc=fr</creationBaseDn>
      <creationClass>top</creationClass>
      <creationClass>person</creationClass>
      <creationClass>organizationalPerson</creationClass>
      <creationClass>inetOrgPerson</creationClass>
      <rdnAttribute>uid</rdnAttribute>

    <!--Mapping entre le nom des champs dans le schema user de nuxeo et les attributs de l'annuaire -->
      <fieldMapping name="username">uid</fieldMapping>
      <fieldMapping name="firstName">givenName</fieldMapping>
      <fieldMapping name="lastName">sn</fieldMapping>
      <fieldMapping name="company">supannetablissement</fieldMapping>
      <fieldMapping name="email">mail</fieldMapping>

   <!-- reference aux groupes, cf. default-ldap-groups-directory-bundle.xml -->
      <references>
       <inverseReference field="groups" directory="groupLdapDirectory"  dualReferenceField="members" />
      </references>
    </directory>
  </extension>
</component>
```

⚠ Afin d'accélérer les requêtes LDAP (et donc la première connexion à Nuxeo), il est conseillé d'utiliser directement l'administrateur pour se connecter à l'annuaire (<*bindDn*>) et non un utilisateur avec droits restreints : ceci évite d'avoir à évaluer les ACLs lors des requêtes.

Paramétrage de l'annuaire pour les groupes

Éditez le fichier **custom/config/default-ldap-groups-directory-bundle.xml** comme suit avec vos propres paramètres :

```
<?xml version="1.0"?>
<component name="org.esup.ecm.directory.ldap.storage.groups">
  <require>org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory</require>
  <require>org.nuxeo.ecm.directory.ldap.storage.users</require>
  <extension target="org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory" point="directories">

   <directory name="groupLdapDirectory">

        <!-- On utilise la connexion que l'on a definie dans default-ldap-users-bundle.xml -->
        <server>default</server>

        <!-- schema correspondant dans nuxeo, et identifiant des groupes (dans nuxeo pas dans l'annuaire !) -->
        <schema>group</schema>
        <idField>groupname</idField>

       <!-- branche dans laquelle sont les groupes -->
       <searchBaseDn>ou=groups,dc=my-univ,dc=fr</searchBaseDn>

       <!-- filtre de recherche -->
       <searchFilter>(objectClass=groupOfNames)</searchFilter>

      <!-- portee de la recherche -->
      <searchScope>subtree</searchScope>

      <!-- si readOnly a false et connexion a l'annuaire avec des droits d'ecriture, possibilite de creation de
groupes dans l'annuaire depuis nuxeo -->
      <readOnly>true</readOnly>

      <!-- cache en seconde -->
      <cacheTimeout>3600</cacheTimeout>

      <!-- nombre maximal d'entrees à mettre  en cache -->
      <cacheMaxSize>1000</cacheMaxSize>

     <!-- utilisé si création de groupes dans l'annuaire depuis nuxeo -->
      <creationBaseDn>ou=grouper,dc=u-bordeaux1,dc=fr</creationBaseDn>
      <creationClass>top</creationClass>
      <creationClass>groupOfUniqueNames</creationClass>
      <rdnAttribute>cn</rdnAttribute>

    <!-- mapping entre les attributs du schema groupe dans nuxeo et les attributs ldap -->
      <fieldMapping name="groupname">cn</fieldMapping>
      <!-- <fieldMapping name="description">description</fieldMapping>-->

      <references>
        <!-- LDAP reference resolve DNs embedded in uniqueMember attributes
         If the target directory has no specific filtering policy, it is most
        of the time not necessary to enable the 'forceDnConsistencyCheck' policy.
          Enabling this option will fetch each reference entry to ensure its
         existence in the target directory. -->
        <ldapReference field="members" directory="userLdapDirectory"
          forceDnConsistencyCheck="false"
         staticAttributeId="member"
         dynamicAttributeId="memberURL" />

        <ldapReference field="subGroups" directory="groupLdapDirectory"
          forceDnConsistencyCheck="false"
          staticAttributeId="member"
          dynamicAttributeId="memberURL" />
        <inverseReference field="parentGroups"
          directory="groupLdapDirectory" dualReferenceField="subGroups" />
      </references>
   </directory>
 </extension>
</component>
```

Paramétrage des utilisateurs / groupes virtuels (admins / members et guest)

Vous trouverez ici une explication sur le fonctionnement des groupes virtuels (notamment le groupe members) de nuxeo

Éditez le fichier **custom/config/default-virtual-groups-bundle.xml** comme suit avec vos propres paramètres :

```
<?xml version="1.0"?>
<component name="org.esup.ecm.platform.usermanager.VirtualGroups">
  <require>org.nuxeo.ecm.platform.usermanager.UserManagerImpl</require>
  <extension target="org.nuxeo.ecm.platform.usermanager.UserService" point="userManager">
    <userManager>
       <users>
     <!-- definition du repertoire utilisateur utilise -->
      <directory>userLdapDirectory</directory>

      <!-- configure l'utilisateur anonyme -->
            <anonymousUser id="invite">
               <property name="firstName">Invite</property>
               <property name="lastName">Anonyme</property>
            </anonymousUser>
        </users>

        <groups>
          <!-- definition du repertoire des groupes -->
          <directory>groupLdapDirectory</directory>
       </groups>

       <!-- uid ldap de l'administrateur -->
      <defaultAdministratorId>jeo</defaultAdministratorId>

      <!-- cn du groupe d'administrateurs -->
      <administratorsGroup>adminGroups</administratorsGroup>

    <!-- groupe par defaut, ne doit pas necessairement exister, dans lequel toute personne authentifiee est
placee -->
      <defaultGroup>members</defaultGroup>
    </userManager>
  </extension>
</component>
```