Configuration de CAS LDAP dans Nuxeo 5.4.2

Cette version est en cours de validation. Nous vous recommandons l'Installation de Nuxeo 5.4.1

Pré-requis

Avoir effectué les opération définies dans Le template custom dans nuxeo 5.4.2

Avoir un serveur CAS et un annuaire fonctionnels.

Paramétrage de CAS

Opérations préliminaires

Nous allons créer un nouveau template pour l'utilisation de CAS avec Nuxeo. L'insertion de cas dans un template qui lui est propre à l'avantage de vous permettre de modifier rapidement la méthode d'authentification utilisée par Nuxeo.

Créez un dossier **esup-login-cas** dans le dossier nuxeo-dm-5.4.2-tomcat/templates. Puis déplacez-vous dans ce dossier

```
cd nuxeo-dm-5.4.2-tomcat/templates
mkdir esup-login-cas
cd esup-login-cas
```

Créez-y un fichier **nuxeo.defaults** et insérez y les valeurs ci-dessous :

```
esup-login-cas.target=nxserver
```

Créez-y également les dossiers suivants :

- **bundles** : Placez y le fichier nuxeo-platform-login-cas2-5.4.2.jar : *(Ce plugin contient le patch permettant d'utiliser un proxy CAS)*
- **config** : Créez y le fichier esup-login-cas-config.xml

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

Éditez le fichier **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 chargés avant que ce fichier soit
       lu car ils contiennent des points d'extension sur l'authentification -->
<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 accès 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>
```

Chargement de la configuration CAS au lancement de Nuxeo

Votre configuration CAS est maintenant complète. Toutefois il faut indiquer à Nuxeo qu'il doit également charger ce template. Éditez le fichier **nuxeo-dm-5.4.2-tomcat/templates/custom/nuxeo.defaults** et rajoutez le template esup-login-cas dans les dépendances du template default comme ci dessous :

```
nuxeo.template.includes=default,postgresql,esup-login-cas
```

Configuration d'un annuaire LDAP

Opérations préliminaires

Tout comme pour l'utilisation de CAS nous allons créer un nouveau template pour l'utilisation de LDAP avec Nuxeo.

Créez un dossier **esup-ldap** dans le dossier nuxeo-dm-5.4.2-tomcat/templates. Puis déplacez-vous dans ce dossier :

```
cd nuxeo-dm-5.4.2-tomcat/templates
mkdir esup-ldap
cd esup-ldap
```

Créez y un fichier **nuxeo.defaults** et insérez y la valeur suivante :

```
esup-ldap.target=nxserver
```

Créez y également le dossier suivant :

- **config**

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

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

```
<?xml version="1.0"?>
<component name="org.nuxeo.ecm.directory.ldap.storage.users">
  <implementation />
  <implementation />
  <require>org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory</require>
  <require>org.nuxeo.ecm.directory.sql.storage</require>
   <!-- configuration de la connexion -->
  <extension target="org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory" point="servers">
    <server name="default">
      <ldapUrl>ldap://ldap.my-univ.fr:389</ldapUrl>
      <!-- Optional servers from the same cluster for failover and load balancing -->
      <!-- <ldapUrl>ldap://server2:389</ldapUrl> -->
      <!--User to bind with-->
      <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, modification par rapport aux versions precedente de nuxeo -->
    <directory name="userLdapDirectory">
     <!-- on s'appuie sur la connexion qu'on vient de définir -->
     <server>default</server>
     <!-- schema nuxeo utilisé : user -->
     <schema>user</schema>
      <!-- identifiant/mdp des personnes (dans nuxeo) -->
      <idField>username</idField>
      <passwordField>password</passwordField>
      <!-- branche dans laquelle sont situés les utilisateurs -->
      <searchBaseDn>ou=people,dc=my-univ,dc=fr</searchBaseDn>
      <!-- ObjectClass à rechercher => ajouté au filtre de recherche -->
      <searchClass>person</searchClass>
      <!-- filtre de recherche personnalisé (ajouté au filter par défaut) -->
      <searchFilter>(&amp;(!(eduPersonAffiliation=affiliate))(status=valide))</searchFilter>
      <!-- Portee de la recherche -->
      <searchScope>onelevel</searchScope>
     <!-- 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>
```

Paramétrage de l'annuaire pour les groupes

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

```
<?xml version="1.0"?>
<component name="org.nuxeo.ecm.directory.ldap.storage.groups">
  <implementation />
  <implementation />
  <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 définie 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>

      <!--
       Trois types de recherches possibles :
       subinitial: suffixe votre recherche par * ex : test donnera test*
       subfinal  : prefixe votre recherche par * ex : test donnera *test
       subany    : prefixe et suffixe automatiquement votre recherche par * ex: test donnera *test*
      -->
      <substringMatchType>subany</substringMatchType>

      <!-- si readOnly a false et connexion a l'annuaire avec des droits d'écriture, possibilité de
       création 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

Créez et éditez le fichier **config/default-virtual-groups-bundle.xml** comme suit avec vos propres paramètres :

```
<?xml version="1.0"?>
<component name="org.nuxeo.ecm.platform.usermanager.VirtualGroups">
  <require>org.nuxeo.ecm.platform.usermanager.UserManagerImpl</require>
  <extension target="org.nuxeo.ecm.platform.usermanager.UserService" point="userManager">
    <userManager>
       <users>
     <!-- Changement par rapport aux versions precedentes de nuxeo -->
      <directory>userLdapDirectory</directory>
      <!-- configure l'utilisateur anonyme -->
            <anonymousUser id="invite">
                <property name="firstName">Invite</property>
                <property name="lastName">Anonyme</property>
            </anonymousUser>
        </users>
     <!-- a ajouter depuis 5.4.2 -->
      <groups>
        <directory>groupLdapDirectory</directory>
      </groups>
      <!-- uid ldap de l'administrateur -->
      <defaultAdministratorId>jeo</defaultAdministratorId>
      <!-- cn du groupe d'administrateurs -->
      <administratorsGroup>adminGroups</administratorsGroup>
      <defaultGroup>members</defaultGroup>
    </userManager>
  </extension>
</component>
```

Chargement de la configuration LDAP au lancement de Nuxeo

Votre configuration LDAP est maintenant complète. N'oubliez pas de mentionner à Nuxeo qu'il doit effectuer son chargement lors du démarrage.Éditez le fichier **nuxeo-dm-5.4.2-tomcat/templates/custom/nuxeo.defaults** et rajoutez le template esup-ldap dans les dépendances du template default comme ci dessous :

```
nuxeo.template.includes=default,postgresql,esup-login-cas,esup-ldap
```

Redémarrez votre instance de Nuxeo afin d'appliquer vos modifications.