

Microsoft Active Directory

Avant propos.

esup-ecm a la possibilité de se connecter à un annuaire LDAP pour l'authentification et l'identification.

Le développement de cette possibilité s'est initialement naturellement concentré sur la compatibilité avec des annuaires LDAP type [SupAnn](#) .

Certains utilisateurs ont eu à installer esup-ecm sur un Microsoft Active Directory, un certain nombre de modifications sont à faire pour y parvenir, on tente ici de rassembler quelques notes autour de cela.

Nuxeo gère cette possibilité nativement, on donne ici donc les configurations Nuxeo qu'il faut faire pour cela.

N'hésitez pas à contribuer à cette page en la modifiant directement ou en y ajoutant des commentaires, cela afin d'obtenir une documentation complète, voire à permettre aux développeurs d'intégrer cette possibilité AD nativement dans esup-ecm.

Notes

Quelques notes pour pouvoir utiliser Active Directory de Microsoft avec esup-ecm.

On privilégiera cependant l'utilisation d'un annuaire ldap type Supann à celui d'un AD.

La particularité constatée de l'AD est que le full Domain Name d'un utilisateur ne comprend pas un uid=jtest mais un cn="Justin Test".

L'identifiant login étant un attribut particulier, le "sAMAccountName".

Objectifs

Avec les modifs données ci-dessous, on est censé pouvoir

- utiliser AD pour s'authentifier via le couple sAMAccountName / password
- utiliser AD pour récupérer les attributs d'un utilisateur
- la récupération des groupes est ici cependant désactiver (à étudier)

default-ldap-groups-directory-bundle.xml

on désactive la récupération des groupes -> on commente tout le fichier,

cf diff ci-dessous

```
Index: /opt/ori-oai/ori-oai-src/esup-ecm-svn/esup-ecm-config-plugin/src/main/resources/config/default-ldap-
groups-directory-bundle.xml
=====
--- /opt/ori-oai/ori-oai-src/esup-ecm-svn/esup-ecm-config-plugin/src/main/resources/config/default-ldap-groups-
directory-bundle.xml      (revision 628)
+++ /opt/ori-oai/ori-oai-src/esup-ecm-svn/esup-ecm-config-plugin/src/main/resources/config/default-ldap-groups-
directory-bundle.xml      (working copy)
@@ -10,66 +10,4 @@
<!-- the groups LDAP directory for users is required to make this bundle work -->
<require>org.nuxeo.ecm.directory.ldap.storage.users</require>

- <extension target="org.nuxeo.ecm.directory.ldap.LDAPDirectoryFactory"
-   point="directories">
-
-   <directory name="groupDirectory">
-
-     <!-- Reuse the default server configuration defined for userDirectory -->
-     <server>default</server>
-
-     <schema>group</schema>
-     <idField>groupname</idField>
-
-     <searchBaseDn><at:var at:name="ldapSearchBaseDn" /></searchBaseDn>
-     <searchFilter>(|(objectClass=groupOfNames)(objectClass=groupOfURLs))</searchFilter>
-     <searchScope>subtree</searchScope>
-
-     <readOnly>true</readOnly>
-
-     <!-- comment <cache* /> tags to disable the cache -->
-     <!-- cache timeout in seconds -->
-     <cacheTimeout>3600</cacheTimeout>
-
-   </directory>
- </extension>
```

```

-      <!-- maximum number of cached entries before global invalidation -->
-      <cacheMaxSize>1000</cacheMaxSize>
-
-      <creationBaseDn><at:name="ldapSearchBaseDn" /></creationBaseDn>
-      <creationClass>top</creationClass>
-      <creationClass>groupOfUniqueNames</creationClass>
-      <rdnAttribute>cn</rdnAttribute>
-
-      <fieldMapping name="groupname">cn</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="userDirectory"
-        forceDnConsistencyCheck="false"
-        staticAttributeId="member"
-        dynamicAttributeId="memberURL" />
-
-      <ldapReference field="subGroups" directory="groupDirectory"
-        forceDnConsistencyCheck="false"
-        staticAttributeId="uniqueMember"
-        dynamicAttributeId="memberURL" />
-
-      <inverseReference field="parentGroups"
-        directory="groupDirectory" dualReferenceField="subGroups" />
-
-      </references>
-
-    </directory>
-
-  </extension>
-
</component>

```

default-ldap-users-directory-bundle.xml

On adapte ce fichier à l'utilisation de l'Active Directory Microsoft,

cf diff ci-dessous

```

Index: /opt/ori-oai/ori-oai-src/esup-ecm-svn/esup-ecm-config-plugin/src/main/resources/config/default-ldap-
users-directory-bundle.xml
=====
--- /opt/ori-oai/ori-oai-src/esup-ecm-svn/esup-ecm-config-plugin/src/main/resources/config/default-ldap-users-
directory-bundle.xml      (revision 628)
+++ /opt/ori-oai/ori-oai-src/esup-ecm-svn/esup-ecm-config-plugin/src/main/resources/config/default-ldap-users-
directory-bundle.xml      (working copy)
@@ -35,10 +35,11 @@
+
+      Only the authentication of users (bind) use the credentials entered
+      through the login form if any.-->
-      @begin.ldap.bind@
-      <bindDn>@ldap.bindDn</bindDn>
-      <bindPassword>@ldap.bindPassword</bindPassword>
-      @end.ldap.bind@
+
+      <bindDn>le sAMAccountName d'un "admin" dans l'AD</bindDn>
+      <bindPassword>son password</bindPassword>
+

```

```

    </server>

</extension>
@@ -52,8 +53,8 @@
    <idField>username</idField>
    <passwordField>password</passwordField>

    <searchBaseDn><at:var at:name="ldapSearchBaseDn" /></searchBaseDn>
-   <searchClass>person</searchClass>
+   <searchClass>User</searchClass>
    <!-- To additionally restricte entries you can add an
        arbitrary search filter such as the following:

@@ -63,7 +64,12 @@
    -->

    <!-- use subtree if the people branch is nested -->
-   <searchScope>onelevel</searchScope>
+   <searchScope>subtree</searchScope>
+
+   <!-- using 'subany', search will match toto. use 'subfinal' to
+       match toto and 'subinitial' to match toto. subinitial is the
+       default behaviour-->
+   <substringMatchType>subany</substringMatchType>

    <readOnly>true</readOnly>

@@ -74,26 +80,28 @@
    <!-- maximum number of cached entries before global invalidation -->
    <cacheMaxSize>1000</cacheMaxSize>

    <creationBaseDn><at:var at:name="ldapSearchBaseDn" /></creationBaseDn>
    <creationClass>top</creationClass>
    <creationClass>person</creationClass>
    <creationClass>organizationalPerson</creationClass>
    <creationClass>inetOrgPerson</creationClass>
-   <rdnAttribute>uid</rdnAttribute>
+   <rdnAttribute>SAMAccountName</rdnAttribute>

-   <fieldMapping name="username">uid</fieldMapping>
-   <fieldMapping name="firstName"><at:var at:name="ldapFirstName" /></fieldMapping>
-   <fieldMapping name="lastName"><at:var at:name="ldapLastName" /></fieldMapping>
-   <fieldMapping name="company"><at:var at:name="ldapCompagny" /></fieldMapping>
-   <fieldMapping name="email"><at:var at:name="ldapEmail" /></fieldMapping>
+   <fieldMapping name="username">SAMAccountName</fieldMapping>
+   <fieldMapping name="password">userPassword</fieldMapping>
+   <fieldMapping name="firstName">givenName</fieldMapping>
+   <fieldMapping name="lastName">sn</fieldMapping>
+   <fieldMapping name="company">compagny</fieldMapping>
+   <fieldMapping name="email">mail</fieldMapping>
+
+<!--
    <references>

        <inverseReference field="groups" directory="groupDirectory"
            dualReferenceField="members" />

    </references>
-
+-->
    </directory>

</extension>

```