Newcastle University - LDAPPCNG Provisioning to the Active Directory

At Newcastle we have been provisioning groups from our Grouper deployment into the Active Directory using LDAPPC for a number of use cases such as delegating access control to the University's wireless network, and managing access to PC cluster room. We have now tested and are ready to put into place the use of LDAPPCNG for the provisioning of these groups. This page has been created to complement the main LDAPPCNG documentation, and documents our set-up for provisioning to the AD, including using a custom subject identifier for searching subjects and filtering groups to be provisioned.

ldappc.properties

This specific settings we enabled in this file for provisioning to the AD were setting the Group objectClass and allowing the provisioner to handle groups with a large number of members, this can be done with the following 2 settings.

```
# Group objectClass for Active Directory# Group objectClass for Active Directory


groupObjectClass=group


# handle Active Directory groups with a large (>1500) number of members


edu.vt.middleware.ldap.searchResultHandlers=edu.internet2.middleware.ldappc.util.QuotedDnResultHandler,edu.vt.
middleware.ldap.handler.FqdnSearchResultHandler,edu.internet2.middleware.ldappc.util.RangeSearchResultHandler
```

The rest of this file depends on an individuals infrastructure set-up.

Using custom subject identifier

Within our deployment of Grouper we identify users with the following scope, subject@ncl.ac.uk, and assign group memberships with this identifier, yet in the Active Directory people are identified with just their user name without @ncl.ac.uk.

This caused problems when we initially attempted to provision groups and memberships into the active directory, the groups were successfully provisioned, yet users were not being provisioned. This was due to LDAPPCNG provisioning the user with the identifier "testsubject@ncl.ac.uk", and trying to match this user against a users sAMAccountName attribute in the DN for members which was set to "testsubject", and therefore returning a subject not found error.

In order to be able to identify a user by both the scoped and un-scoped user name, we created a custom subject identifier in our sources.xml file named SAMA.

```
<init-param>
<!-- col which identifies the row, perhaps not subjectId -->
<param-name>subjectIdentifierCol0</param-name>
<param-value>loginname</param-value>
</init-param>
<init-param>
<param-name>subjectIdentifierCol1</param-name>
<param-value>SAMA</param-value>
</init-param>
<init-param>
<param-name>subjectAttributeCol0</param-name>
<param-value>SAMA</param-value>
</init-param>
<init-param>
<param-name>subjectAttributeName0</param-name>
<param-value>SAMA</param-value>
</init-param>
```

So we are now able to identify a subject by both identifiers, testsubject@ncl.ac.uk and testsubject.

In order for LDAPPCNG to provision subjects using the correct identifier, the MemberDataConnector and the SpmlDataConnector in the ldappc-resolver.xml file had to be amended to the following;

```
 <resolver:DataConnector id="MemberDataConnector" xsi:type="grouper:MemberDataConnector">
    <grouper:Attribute id="groups" />
    <grouper:Attribute id="SAMA" source="jdbc" />
  </resolver:DataConnector>

<resolver:DataConnector id="SpmlDataConnector" provider="ldap-provider" xsi:type="ldappc:SPMLDataConnector"
    scope="subTree" base="${peopleOU}" returnData="identifier">
    <resolver:Dependency ref="MemberDataConnector" />
<ldappc:FilterTemplate>(sAMAccountName=${SAMA.get(0)})</ldappc:FilterTemplate>
  </resolver:DataConnector>
```

This allows us to find subjects within the active directory using the SAMA attribute and provision the necessary groups and memberships.

Filtering groups to be provisioned

The defining of which groups need to be provisioned is done within the ldappc-resolver.xml file. In this example we only want groups that are located in "Applications:Filestores:ISS" to be provisioned into the AD. To do this you define GroupFilters in the GroupDataConnector and StemDataConnector.

```
<resolver:DataConnector id="GroupDataConnector" xsi:type="grouper:GroupDataConnector">
<grouper:GroupFilter xsi:type="grouper:StemName" name="Applications:Filestores:ISS" scope="SUB" />
<grouper:Attribute id="members" />
<grouper:Attribute id="groups" />
</resolver:DataConnector>


<resolver:DataConnector id="StemDataConnector" xsi:type="grouper:StemDataConnector">
<grouper:GroupFilter xsi:type="grouper:StemName" name="Applications:Filestores:ISS" scope="SUB" />
</resolver:DataConnector>
```

More details on filtering groups is documented here.

See Also

Newcastle University Intro Page