Hints for Special LDAP Server Products

Introduction

The Lightweight Directory Access Protocol (LDAP) enables a user to locate resources on a corporate intranet or on the public internet. Those resources can be files or devices as well as organizations and individuals. LDAP is smaller than the Directory Access Protocol (DAP) from which it was derived (hence "lightweight").

In EntireX, LDAP technology is used for authorization rules.

Hints for Microsoft Active Directory

To deploy the sagxds schema on Microsoft Active Directory, do not use the Microsoft Active Directory tools for editing the schema. Use the following step-by-step instructions:

1. Make a backup of the system state. Changes to the schema of Microsoft Active Directory are irreversible without a backup of the system state.
2. You must enable UPDATE schema.
    1. To make the Schema Master available, enter the following at a command prompt:

       ```
       regsvr32.exe schmmgmt.dll
       ```

    2. Enter: MMC.
    3. From Console menu item select: **add/remove snap-in**.
    4. Choose: **Add**.
    5. Choose: **Active Directory Schema** from **Action** menu item of Active Directory Schema, select: **Operations Master**.
    6. Choose "The schema may be modified on this domain controller".
3. Copy the following text to the file *sagxds.ldif*

```
# Add sag-value attribute

dn: CN=sag-value,CN=Schema,CN=Configuration,DC=<your domains name>
changetype: add
adminDisplayName: sag-value
attributeID: 1.2.276.0.12.2.1.2
attributeSyntax: 2.5.5.10
cn: sag-value
isSingleValued: FALSE
lDAPDisplayName: sag-value
distinguishedName: CN=sag-value,CN=Schema,CN=Configuration,DC=<your domains name>
objectCategory:
```

```
 CN=Attribute-Schema,CN=Schema,CN=Configuration,DC=<your domains name>
objectClass: attributeSchema
oMSyntax: 4
name: sag-value

# Add sag-key attribute
# Active Directory requires the naming attribute(RDN) to be a syntax of DirectoryString

dn: CN=sag-key,CN=Schema,CN=Configuration,DC=<your domains name>
changetype: add
adminDisplayName: sag-key
attributeID: 1.2.276.0.12.2.1.1
attributeSyntax: 2.5.5.12
cn: sag-key
isMemberOfPartialAttributeSet: TRUE
isSingleValued: TRUE
lDAPDisplayName: sag-key
distinguishedName: CN=sag-key,CN=Schema,CN=Configuration,DC=<your domains name>
objectCategory:
 CN=Attribute-Schema,CN=Schema,CN=Configuration,DC=<your domains name>
objectClass: attributeSchema
oMSyntax: 64
name: sag-key
searchFlags: 1

# Update the schema

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

# Add sag-xds class

dn: CN=sag-xds,CN=Schema,CN=Configuration,DC=<your domains name>
changetype: add
adminDescription: sag-xds
adminDisplayName: sag-xds
cn: sag-xds
defaultObjectCategory:
 CN=sag-xds,CN=Schema,CN=Configuration,DC=<your domains name>
governsID: 1.2.276.0.12.2.3.1
lDAPDisplayName: sag-xds
mayContain: sag-value
mustContain: sag-key
distinguishedName: CN=sag-xds,CN=Schema,CN=Configuration,DC=<your domains name>
objectCategory: CN=Class-Schema,CN=Schema,CN=Configuration,DC=<your domains name>
objectClass: classSchema
objectClassCategory: 1
possSuperiors: container
name: sag-xds
rDNAttID: sag-key
subClassOf: top

# Update the schema

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-

# Modify sag-xds class
# make sag-xds a possSuperior. This means a sag-xds class can contain other sag-xds classes.

dn: CN=sag-xds,CN=Schema,CN=Configuration,DC=<your domains name>
changetype: modify
add: possSuperiors
```

```
possSuperiors: sag-xds
-

# Update the schema

DN:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

4. Replace all instances of dc= <your domain name> with your domain name, i.e.dc=myunit,dc=mycompany,dc=com

5. Run it with the command:

   ```
   ldifde -s <your server> -b <account> <domain> <password> -i -f sagxds.ldif
   ```

6. Add containers which represent the base DN of the authorization rules. These containers determine the value of base DN in *xds.ini*. Example (for two containers):

   ```
   dn: CN=<your container 1>,DC=<your domain name>
   changetype: add
   cn: <your container 1>
   objectclass: container

   dn: CN=<your container2>,<your container 1>,DC=  <your domain name>
   changetype: add
   cn: <your container 2>
   objectclass: container
   ```

7. With the utilities for Microsoft Active Directory, set the permissions to read and to modify the containers.