How to…

Configure UME for Multiple LDAP Data Sources

ENTERPRISE PORTAL 6.0

PUBLIC

VERSION 1.0

ASAP "How to…" Paper

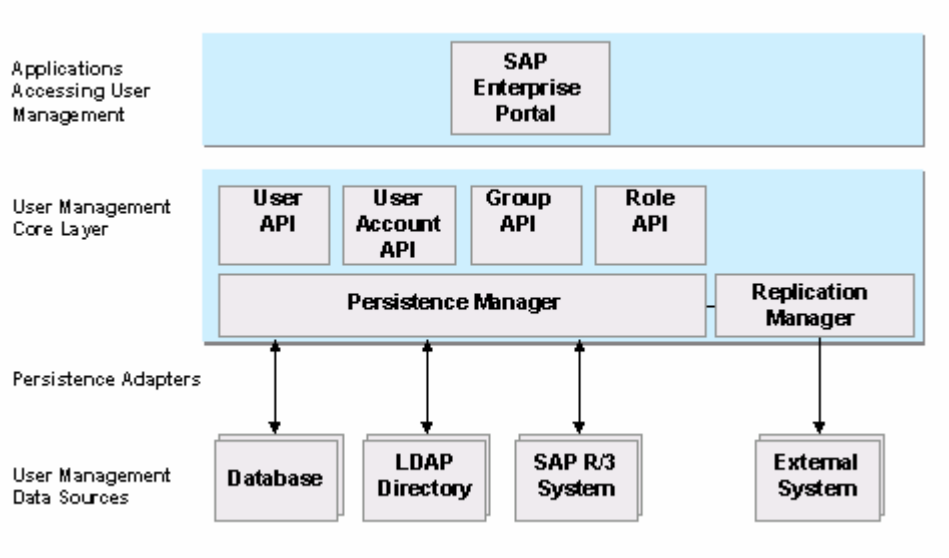
Applicable Releases: EP 6.0, SP 2

May 2004

1 Scenario

You need to authenticate against multiple LDAP directory servers with EP6.0. SAP's delivered configuration files do not properly address your enviromnent.

1.1 Overview of UME Architecture



UME user data is stored in one or more data sources. Each type of data source has its own persistence adapter. The persistence manager consults the persistence adapters when creating, reading, writing, and searching user management data.

Persistence adapters for the following types of repositories are available:

1. Database: See the Product Availability Matrix on SAP Service Marketplace (**`http://service.sap.com/pam60`**) for details on which databases are supported.
2. • Lightweight Directory Access Protocol (LDAP) directory: See the Product Availability Matrix on SAP Service Marketplace (**`http://service.sap.com/pam60`**) for details on which directories are supported.
3. SAP Systems based on Web Application Server 6.20

You can configure UME to use one or more of these persistence devices in parallel. Users can also be stored in several different physical LDAP directory servers, or in different branches of the same LDAP directory server.

This How To Guide shows you how to configure such devices using the XML configuration interfaces.

2 Prerequisites

Gather all of the connection information for each of the LDAP target systems you need to connect to. This information will include the server name (fully qualified), port, user to connect with (the full DN is required), the password for this user and the paths to both the user and groups definitions.

You will also need a text editor other than Notepad to edit the XML configuration files. Notepad adds an additional character to the end of the line which may cause problems with the XML parser used by the J2EE Engine. A great free XML editor is “Cooktop”.

3 Limitations

For most upto date general limitations in the UME please check SAP Note 673824.

Details about data source configuration can be found in the SAP NetWeaver 04 documentation on http://www.help.sap.com (Identity Management – User Management Engine).

3.1 Limitations of Multiple Data Sources

Since the number of data sources directly impacts the time for search operations inside the UME it is recommended to have **not more than 5 data sources.**

LDAP groups cannot span different LDAP data sources. LDAP groups can therefore only include users from the data source where they are read from.

The Step By Step Solution

1) Ensure that the UM Configuration is set to "**Database Only**" or that the current UM configuration creates new users in the database.

a) Navigate the the UM Configuration UI (System Administration -> System Configuration -> UM Configuration) and select the ***"Data Sources"*** tab.

b) Choose "Database Only" or any "… Read Only" dataSource.

c) Save.

d) Restart J2EE Engine.

2) Create a new user ID in the portal and assign it to the **Super Administration** role. Log off and then log back on to the portal with this ID to ensure you can access the administrative function using the ID from the database. This ensures that you can logon and perform administration tasks even if the portal is unable to connect to an LDAP source.

- Follow the documentation for creating users (Administration Guide > Portal Platform > User Administration > User Management Administration Console) and assigning users to roles (Administration Guide > Portal Platform > User Administration > Role Assignment)

3) Establish the initial UM configuration.

a) Navigate the the UM Configuration UI (System Administration -> System Configuration -> UM Configuration) and select the ***"Data Sources"*** tab.

b) Choose the most appropriate DataSource configuration from the delivered list (e.g. iPlanet, Novell, MS ADS, etc.)

c) Complete UM configuration for the first LDAP data source using the User Management Configuration Tool.

d) Restart the J2EE Engine.

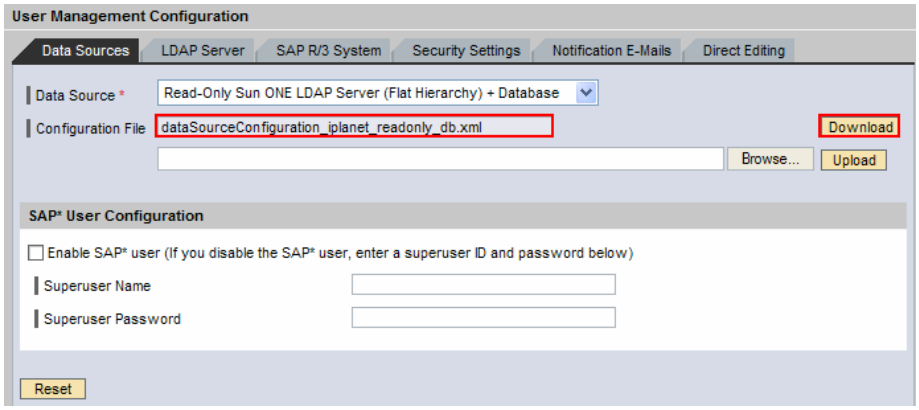
e) Logon to portal server with an LDAP user to test the connection. If there are problems, use the database user ID you created in step #2 to logon to the portal and resolve connectivity issues.

4) Capture information required for creating a new UM Configuration for Multiple LDAP sources.

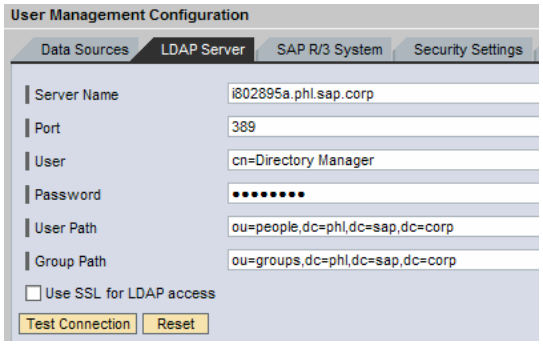
a) Log back on to the portal using an administrator ID.

b) Navigate back to the UM Configuration Tool and select the ***"Data Sources"*** tab.

c) Click "***Download***" to download a copy of the appropriate XML file. Save this file to your local filesystem for editing (suggested name: dataSourceConfiguration_multiLDAP_db.xml).

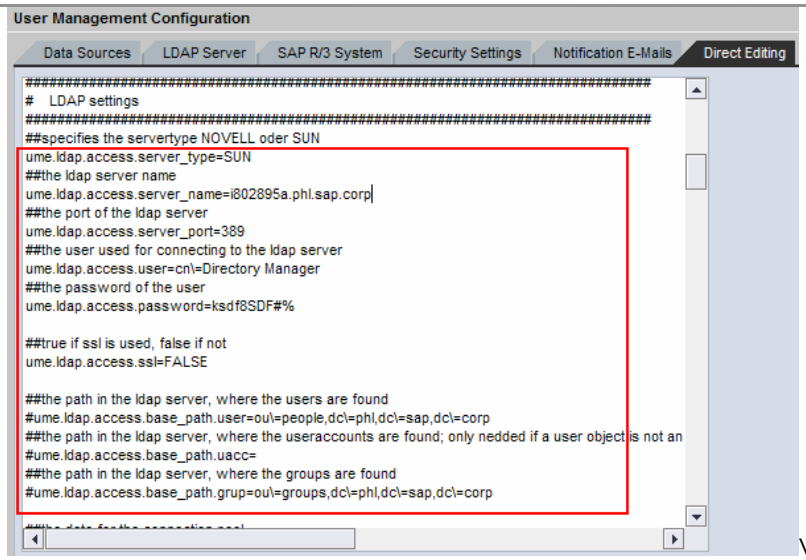


d) Navigate to "***LDAP Server***" tab and verify connection information to the LDAP server. Click "Test Connection" to ensure credentials are correct. Save the configuration before continuing to the next step.



e) Navigate to "***Direct Editing***" tab.

f) Scroll down to the LDAP Settings section and copy the contents to MS WordPad or other text editor (configuration document). This information will be used later. Be sure to capture the server name, port, user (the full DN is needed), the password (encrypted) and the path for both the users and groups. The LDAP Settings section will only contain values entered using the UM Configuration tool. Entering the password in the UI, will cause it to be encrypted in the sapum.properties configuration. This encrypted password can then be entered directly in the XML file (below).



g) Repeat steps d-e for each additional LDAP server you need to connect to. Enter the server name, host, ID, password, user, and group roots. Test the connection, then copy the information in the "Direct Editing" tab to the configuration document.

5) Create a new UM configuration file for multiple LDAP data sources.

a) Open the dataSourceConfiguration_multiLDAP_db.xml file (previously downloaded) using a text editor (other than Notepad) and locate the `<dataSource.../>` section for the "`CORP_LDAP`". Copy the entire section from `<dataSource...>` to `</dataSource>` to the clipboard.

b) For each additional LDAP server, paste the copy into the document after the original `</dataSource...>` ending tag for the CORP_LDAP source. Change the name of the data source for pasted copy to "CORP_LDAP_X" or some other value. This value becomes a data source identifier for UME and prefixes the principal Ids.

c) For each LDAP data source, locate the `<privateSection...>` within the `<dataSource...>` tag and enter the following lines if they are not present:

```
<ume.ldap.access.server_name>SERVER_HOSTNAME</ume.ldap.access.server_name>
<ume.ldap.access.server_port>SERVER_PORT</ume.ldap.access.server_port>
<ume.ldap.access.user>DS_USER_NAME</ume.ldap.access.user>
<ume.ldap.access.password>{encrypted}DS_PASSWORD</ume.ldap.access.password>
<ume.ldap.access.base_path.user>USER_ROOT_IN_DS</ume.ldap.access.base_path.user>
<ume.ldap.access.base_path.grup>GROUP_ROOT_IN_DS</ume.ldap.access.base_path.grup>
```

d) Update the properties for each datasource with the correct values obtained from the "Direct Editing" tab (now stored in the configuration document). An example is shown below:

```
<dataSource id="CORP_LDAP_2"
className="com.sap.security.core.persistence.datasource.imp.LDAPPersistence" isReadonly="true"
isPrimary="true">
...
<privateSection>
  <ume.ldap.access.server_name>i802895a.phl.sap.corp</ume.ldap.access.server_name>
  <ume.ldap.access.server_port>389</ume.ldap.access.server_port>
  <ume.ldap.access.user>cn=Directory Manager</ume.ldap.access.user>
  <ume.ldap.access.password>{encrypted}ksdf8SDF#%</ume.ldap.access.password>
  <ume.ldap.access.base_path.user>ou=people,dc=phl,dc=sap,dc=corp</ume.ldap.access.base_path.user>
  <ume.ldap.access.base_path.grup>ou=groups,dc=phl,dc=sap,dc=corp</ume.ldap.access.base_path.grup>
  <ume.ldap.access.server_type>SUN</ume.ldap.access.server_type>
   [more stuff]
</privateSection>
```

Note: The data in the "Direct Editing" tab escapes certain characters such as "=". Please make sure that the characters are NOT escaped when transferring to the XML configuration file. For instance the group root path (ume.ldap.access.base_path.grup) in the **sapum.properties** would be:

```
ume.ldap.access.base_path.grup=ou\=groups,dc\=phl,dc\=sap
```

In the XML configuration file it would be:

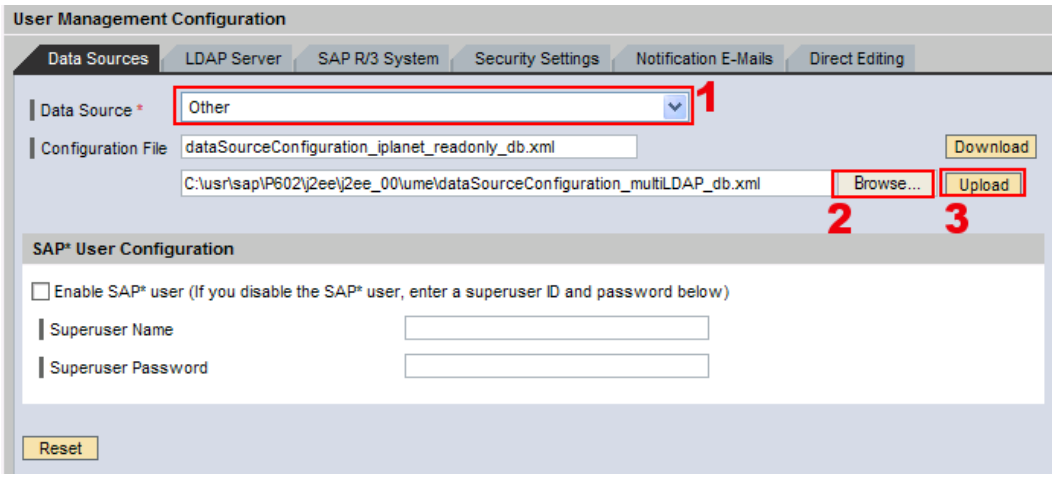
```
<ume.ldap.access.base_path.grup>ou=groups,dc=phl,dc=sap</ume.ldap.access.base_path.grup>
```

Failure to do so could cause problems in the startup of UME.

6) Upload the new UM Configuration file.

a) Navigate back to "Data Source" tab and choose "Other" for the data source.

b) Click "Upload" and navigate to the new configuration file - dataSourceConfiguration_multiLDAP_db.xml. Upload this to the server.



c) Click "Save" to save the new configuration.

d) Navigate to the "Direct Editing" tab.

e) Comment out all of the LDAP settings which begin with ume.ldap.access.* such as server name, passwords, etc. that are now manually configured in the XML file.

f) Click "Save" to save the properties. (You may also wish to make a copy of the new settings and save them to a file for recovery purposes).

g) Restart the J2EE engine.

7) Test the configuration.

a) Logon with a user from each LDAP server and verify that the authentication is working.

b) Logon with the database user to ensure everything is still working. Check the following operations:

i) Search for users – you should be able to search for users in each LDAP server

ii) Search for groups – you should see groups from each LDAP server as well as the database

iii) Peform role assignments with users from each DS.

8) Be happy.

4 Appendix

4.1 Troubleshooting

4.1.1 Logfiles

If you are having trouble logging in after making the configuration changes, consult the logfiles for user management to determine if there is a problem. The portal startup log may also indicate a problem trying to set up the connection pools to the various LDAP servers.

4.1.2 Unable to Save Role assignments

This error most commonly occurs because one or more of the LDAP data sources is misconfigured. If the connection cannot be established to one of the LDAP data sources, then role assignments are not saved into the UME persistence (database).