

Configuring WebSphere Portal V6.1 with Multiple LDAP's and Multiple Realm's

Abstract :

This article contains step – by – step instructions for configuring Portal V6.1 with multiple federated ldap's and Multiple realms. Multiple Realms are used to create Virtual Portals for different ldap user population.

- A realm contains the entire user population of one virtual portal.
- Each virtual portal can have its own realm of users associated, but it is also possible that multiple virtual portals can share their user population by using the same realm in parallel.
- In order to be able to log in to a particular virtual portal, a user must be a member of the realm that is associated with that virtual portal.

System Info :

IDSLDAP 6.0 --- Windows 2000 server
Sun One Directory Server 5.2 – Windows 2003 server
WebSphere Portal Server V6.1 – AIX 5.3

NOTE : At this point WPV6.1 is installed Out of the box. And the example values given in the entire doc are based on the LDAP's IDS6.0 and Sun One Directory Server 5.2.

Adding First LDAP(IDS6.0) , Creating Realm1 and Make it Default :

1. Use a text editor to open the wkplc.properties file, located in the wp_profile_root/ConfigEngine/properties directory.
2. Enter a value for the following required parameters in the wkplc.properties file under the VMM Federated LDAP properties section :
 - federated.ldap.id=fed1
 - federated.ldap.host=manju.rtp.raleigh.ibm.com
 - federated.ldap.port=390
 - federated.ldap.bindDN=cn=root
 - federated.ldap.bindPassword=p0rtal4u
 - federated.ldap.ldapServerType=IDS6
 - federated.ldap.baseDN=dc=raleigh,dc=com
3. Save your changes to the wkplc.properties file.
4. Run the following task, from the wp_profile_root/ConfigEngine directory, to validate your LDAP server settings:
 - **Windows:** ConfigEngine.bat validate-federated-ldap -DWasPassword=password

- **Unix:** ./ConfigEngine.sh validate-federated-ldap -DWasPassword=password
 - **i5/OS:** ConfigEngine.sh validate-federated-ldap -DWasPassword=password
5. Run the following task to add a federated ldap :
 - **Windows:** ConfigEngine.bat wp-create-ldap -DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-create-ldap -DWasPassword=password
 - **i5/OS:** ConfigEngine.sh wp-create-ldap -DWasPassword=password
 6. Restart the server1 and WebSphere_Portal servers.
 7. To list the names and types of configured repositories run the following task. This task will list currently configured repositories ex: federated ldap repository, file based repository(out of box):
 - **Windows:** ConfigEngine.bat wp-query-repository -DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-query-repository -DWasPassword=password
 - **i5/OS:** ConfigEngine.sh wp-query-repository -DWasPassword=password
 8. Check that all defined attributes are available in the configured LDAP user registry. Run the following task :

NOTE: After running the following task, check the ConfigEngine/log/ConfigTrace.log file for missing attributes in portal. Then proceed to the following steps.

 - **Windows:** ConfigEngine.bat wp-validate-federated-ldap-attribute-config -DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-validate-federated-ldap-attribute-config -DWasPassword=password
 - **i5/OS:** ConfigEngine.sh wp-validate-federated-ldap-attribute-config -DWasPassword=password
 9. If an attribute is defined in WebSphere Portal but not in the LDAP server, you will need to perform one of the following tasks to resolve the mismatch.
 - Flag the attribute as unsupported for the LDAP server
 - Introduce an attribute mapping that maps the WebSphere Portal attribute to an attribute defined in the LDAP schema
 10. Run the following task : The task will create “**availableAttributes.html**” file in wp_profile_root/ConfigEngine/log dir.
 - **Windows:** ConfigEngine.bat wp-query-attribute-config -DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-query-attribute-config -DWasPassword=password
 - **i5/OS:** ConfigEngine.sh wp-query-attribute-config -DWasPassword=password

11. Open **availableAttributes.html** file and review the following output for the **PersonAccount** and **Group** entity type:
 - The following attributes are defined in WebSphere Portal but not in the LDAP server . Flag attributes that you do not plan to use in WebSphere Portal as unsupported. Map the attributes that you plan to use to the attributes that exist in the LDAP; you must also map the `uid`, `cn`, `firstName`, `sn`, `preferredLanguage`, and `ibm-primaryEmail` attributes.
 - The following attributes are flagged as required in the LDAP server but not in WebSphere Portal. This list contains all attributes that are defined as "MUST" in the LDAP server but not as required in WebSphere Portal. You should flag these attributes as required within WebSphere Portal.
 - The following attributes have a different type in WebSphere Portal and in the LDAP server. This list contains all attributes that WebSphere Portal might ignore because the data type within WebSphere Portal and within the LDAP server do not match.
12. Use a text editor to open the `wkplc.properties` file, located in the [wp_profile_root](#)/ConfigEngine/properties directory.
13. Enter a value for one of the following sets of parameters in the `wkplc.properties` file to correct any issues found in the config trace file:
 - **Federated Repository** : The following parameters are found under the VMM Federated repository properties heading:
 - `federated.ldap.attributes.nonSupported`
 - `federated.ldap.attributes.nonSupported.delete`
 - `federated.ldap.attributes.mapping.ldapName`
 - `federated.ldap.attributes.mapping.portalName`
 - `federated.ldap.attributes.mapping.entityTypes`

For example, the following values will flag `certificate` and `members` as unsupported attributes and will map `ibm-primaryEmail` to `mail` and `ibm-jobTitle` to `title` for both the `PersonAccount` and `Group` entityTypes:

```
federated.ldap.attributes.nonSupported=certificate, members
federated.ldap.attributes.nonSupported.delete=
```

```
federated.ldap.attributes.mapping.portalName=ibm-primaryEmail,
ibm-jobTitle
federated.ldap.attributes.mapping.ldapName=mail,title - Ex: IDS6
LDAP values. NOTE : Change these values according to
the LDAP Type.
federated.ldap.attributes.mapping.entityTypes=PersonAccount,
Group
```

14. Save your changes to the `wkplc.properties` file.
15. Run the following task to update the LDAP user registry configuration :

- **Windows:** ConfigEngine.bat wp-update-federated-ldap-attribute-config - DWasPassword=password
- **Unix:** ./ConfigEngine.sh wp-update-federated-ldap-attribute-config - DWasPassword=password
- **i5/OS:** ConfigEngine.sh wp-update-federated-ldap-attribute-config - DWasPassword=password

16. Restart the server1 and WebSphere_Portal servers.

17. **NOTE :** At this point the **File based Repository** (Out of box security configuration) is the **default repository**. Any New User or Group will be saved in the default repository. In order to create New user and group in LDAP repository instead of default file based repository perform the following step.

Perform the following steps to update the user registry where new users and groups are stored:

1. Use a text editor to open the wkplc.properties file, located in the [wp_profile_root](#)/ConfigEngine/properties directory.
2. Enter a value for the following required parameters in the wkplc.properties file under the VMM supported entity types configuration heading:
 - personAccountParent=cn=users,dc=raleigh,dc=com
 - groupParent=cn=groups,dc=raleigh,dc=com
 - personAccountRdnProperties=uid
 - groupRdnProperties=cn
3. Save your changes to the wkplc.properties file.
4. To update the Group and PersonAccount entity types with the corresponding default parent and relative distinguished name (RDN). Run the following task
 - **Windows:** ConfigEngine.bat wp-update-entitytypes - DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-update-entitytypes - DWasPassword=*password*
 - **i5/OS:** ConfigEngine.sh wp-update-entitytypes -DWasPassword=password
5. Restart the server1 and WebSphere_Portal servers.

NOTE : At this point your portal is configured with Federated LDAP security, configured with ldap attributes mapped with portal attributes. Portal configured with entity types for both User and Group entities such that any New User and Group Creation will be created/saved in LDAP Repository directly instead of default File Based Repository. Perform the following steps to verify the User /Group creation is done in LDAP.

6. Launch portal page in Web browser and create a New User :

7. Click OK in the following screen

The screenshot shows a web form titled "Edit My Profile" with a blue header. Below the header, there is a light blue banner with a speech bubble icon and the text "New user enrollment. Provide the information req". The form contains several input fields and a dropdown menu:

- * User ID:
- * Password:
- * Confirm Password:
- First Name:
- * Last Name:
- Email:
- Preferred language:

At the bottom of the form, there is a horizontal line, a small asterisk with the text "* Required Field", and two buttons: "OK" and "Cancel".

8. Login with this user /pwd and make sure you can login successfully.

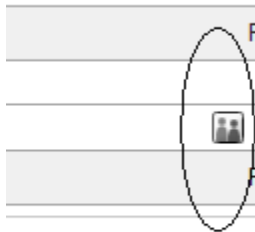
The screenshot shows the same "Edit My Profile" form, but now it displays a success message in a light blue banner: "EJPAT0010I: User created successfully". Below the banner, the text "Congratulations!" is displayed in a large, bold font. Underneath, there is a line of text: "You are now a member of this portal. Click the Log In button to enter this portal site." At the bottom, there are two buttons: "Log in" and "Cancel".

9. Now login as Portal Admin id /pwd and search for the user created above.

10. Login – Administrator – Users and Groups – Search for users – fedusr3 as shown in screen below.

The screenshot shows the 'Manage Users and Groups' portlet. At the top, there is a search bar with 'Users' selected in a dropdown menu. Below it, 'Search by' is set to 'uid' and the search text is 'fedusr3'. A 'Search' button is to the right. Below the search bar are two buttons: 'New Group' and 'New User'. A table below shows a single entry with 'ID' as 'fedusr3' and a 'Pag' column on the right.

11. Now Click on view membership as shown below:



12. you will get the following :

The screenshot shows the 'Manage Users and Groups' portlet with a warning message: 'EJPAL1010W: Sorry, no user or user group was found!'. Below the message, it displays 'Membership for: uid=fedusr3,cn=users,dc=raleigh,dc=com' and 'Groups that uid=fedusr3,cn=users,dc=raleigh,dc=com belongs to'. A table below has a header 'Group name' and the text 'There are no entries to display.' At the bottom, there are two buttons: 'Remove membership' and 'Cancel'.

13. This confirms that the user “fedusr3” is created in LDAP repository.

14. Create a New Group using Users and Groups portlet , search for it, and View Membership to verify it is created in LDAP Repository.

Adding the Realm1 Support (IDS LDAP) :

A realm is a group of users from one or more user registries that form a coherent group within IBM® WebSphere® Portal. Realms allow flexible user management with various configuration options. A realm must be mapped to a Virtual Portal to allow the defined users to log in to the Virtual Portal.

Before configuring realm support, you must add all LDAP user registries and/or database user registries, that you will use to create a single realm or multiple realms, to the federated repository. If you are going to create multiple realms, you must create all required base entries within your LDAP user registries and/or database user registries. All base entry names must be unique within the federated repository.

- 1) Start server1 and WebSphere_Portal servers before starting this task.
- 2) Use a text editor to open the wkplc.properties file, located in the [*wp_profile root*](#)/ConfigEngine/properties directory.
- 3) Enter a value for the following required parameters in the wkplc.properties file under the VMM realm configuration section:
 - a. realmName=IDSRealm1
 - b. addBaseEntry=dc=raleigh,dc=com
 - c. securityUse=active
 - d. delimiter=/
 - 4) Save your changes to the wkplc.properties file.
 - 5) Run the following task to add a new realm to the Virtual Member Manager configuration :
 - 6) **Windows:** ConfigEngine.bat wp-create-realm -DWasPassword=password
 - 7) **Unix:** ./ConfigEngine.sh wp-create-realm -DWasPassword=password
 - 8) **i5/OS:** ConfigEngine.sh wp-create-realm -DWasPassword=password
 - 9) Restart the server1 and WebSphere_Portal servers.

To update the default parents per entity type and realm.Run the following task:

1. Enter a value for the following required parameters in the wkplc.properties file under the VMM realm configuration heading and then save your changes:
 - realmName=IDSRealm1
 - realm.personAccountParent=cn=users,dc=raleigh,dc=com
 - realm.groupParent=cn=groups,cn=groups,dc=raleigh,dc=com
 - realm.orgContainerParent=dc=raleigh,dc=com
2. Run the task :
 - **Windows:** ConfigEngine.bat wp-modify-realm-defaultparents -DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-modify-realm-defaultparents -DWasPassword=password
 - **i5/OS:** ConfigEngine.sh wp-modify-realm-defaultparents -DWasPassword=password
3. Restart the server1 and WebSphere_Portal servers.

4. **NOTE : At this point the default File Based Realm is the default realm. So the WAS Admin and Portal Admin is File Based Repository users (Ex: This is same Admin id/pwd given while installing portal. Ex. : portaladmin/p0rtal4u).**
5. **NOTE : If planning to change the default realm from File Based Realm to IDS LDAP Realm just created above. Need to WAS Admin ID and Portal Admin ID before making IDS LDAP Realm Default. Follow the steps below to change the WAS Admin ID and Portal Admin ID's. Other wise skip the following steps.**
6. Update wkplc.properties file VMM Change admin users section.
 - newAdminId=uid=wpsadmin,cn=users,dc=raleigh,dc=com
 - newAdminPw=p0rtal4u
7. Run the following task to change the WAS Admin User :
 - **Windows:** ConfigEngine.bat wp-change-was-admin-user - DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-change-was-admin-user - DWasPassword=password
 - **i5/OS:** ConfigEngine.sh wp-change-was-admin-user - DWasPassword=password
8. Restart the server1 and WebSphere_Portal servers.
9. Launch WAS Admin Console and try to login as new WAS Admin ID as set in the step 14.
10. Update wkplc.properties file VMM Change admin users section.
 - newAdminId=uid=wpsadmin,cn=users,dc=raleigh,dc=com
 - newAdminPw=p0rtal4u
 - newAdminGroupId=cn=wpsadmins,cn=groups,dc=raleigh,dc=com
11. Run the following task to change the Portal Admin User :
 - **Windows:** ConfigEngine.bat wp-change-portal-admin-user - DWasPassword=password
 - **Unix:** ./ConfigEngine.sh wp-change-portal-admin-user - DWasPassword=password
 - **i5/OS:** ConfigEngine.sh wp-change-portal-admin-user - DWasPassword=password
12. Restart the server1 and WebSphere_Portal servers.
13. Launch Portal Page in Web browser. Login as New Portal Admin User id /pwd as set in Step 18.
14. Now you should see **Administration page** (as this user is the portal admin user now).
15. Logout and Login as Out of Box user id /pwd (original Portal admin id/pwd , from install) , you should **not see Administration page** , as this user is not Admin User anymore.
16. Set the realm created above Default :
17. Use a text editor to open the wkplc.properties file, located in the [wp_profile_root](#)/ConfigEngine/properties directory:

- realmName=IDSRealm1
- defaultRealmName=IDSRealm1

18. Save your changes to the wkplc.properties file.

19. Run the following task:

- **Windows:** ConfigEngine.bat wp-default-realm -DWasPassword=password
- **Unix:** ./ConfigEngine.sh wp-default-realm -DWasPassword=password
- **i5/OS:** ConfigEngine.sh wp-default-realm -DWasPassword=password

20. Restart the server1 and WebSphere_Portal servers.

Adding Second LDAP(Sun One Directory LDAP Server 5.2) and Creating Realm2 :

NOTE : Make sure that both the LDAP's have Unique base entries(base DN's) and Unique Users (especially the wpsadmin/wpsbind default portal admin id's doesn't exist in both LDAP's. If they exist in both ldap's one has to use Full User DN/pwd to login to WAS and Portal. Ex: uid=wpsadmin,cn=users,dc=raleigh,dc=com – IDS ldap user,

uid=wpsadmin,ou=people,dc=raleigh,dc=ibm,dc=com – Sun One Ldap User.)

- 1) Use a text editor to open the wkplc.properties file, located in the wp_profile_root/ConfigEngine/properties directory.
- 2) Enter a value for the following required parameters in the wkplc.properties file under the VMM Federated LDAP properties section :
 - a. federated.ldap.id=fed2
 - b. federated.ldap.host=dora1.rtp.raleigh.ibm.com
 - c. federated.ldap.port=395
 - d. federated.ldap.bindDN=cn=Directory Manager
 - e. federated.ldap.bindPassword=p0rtal4u
 - f. federated.ldap.ldapServerType=SUNONE
 - g. federated.ldap.baseDN=dc=raleigh,dc=ibm,dc=com
- 3) Save your changes to the wkplc.properties file.
- 4) Run the following task, from the wp_profile_root/ConfigEngine directory, to validate your LDAP server settings:
- 5) **Windows:** ConfigEngine.bat validate-federated-ldap -DWasPassword=password
- 6) **Unix:** ./ConfigEngine.sh validate-federated-ldap -DWasPassword=password
- 7) **i5/OS:** ConfigEngine.sh valdiate-federated-ldap -DWasPassword=password
- 8) Run the following task to add a federated ldap :
- 9) **Windows:** ConfigEngine.bat wp-create-ldap -DWasPassword=password
- 10) **Unix:** ./ConfigEngine.sh wp-create-ldap -DWasPassword=password
- 11) **i5/OS:** ConfigEngine.sh wp-create-ldap -DWasPassword=password

- 12) Restart the server1 and WebSphere_Portal servers.
- 13) Launch Portal Page in Web browser. And login successfully.
- 14) Should be able to search for portal users/groups for both repositories.

Adding the Realm2 Support (SUN ONE LDAP) :

- 1) Start server1 and WebSphere_Portal servers before starting this task.
- 2) Use a text editor to open the wkplc.properties file, located in the [wp_profile_root](#)/ConfigEngine/properties directory.
- 3) Enter a value for the following required parameters in the wkplc.properties file under the VMM realm configuration section:
 - a. realmName=SUNRealm2
 - b. addBaseEntry=dc=raleigh,dc=ibm,dc=com
 - c. securityUse=active
 - d. delimiter=/
- 4) Save your changes to the wkplc.properties file.
- 5) Run the following task to add a new realm to the Virtual Member Manager configuration :
- 6) **Windows:** ConfigEngine.bat wp-create-realm -DWasPassword=password
- 7) **Unix:** ./ConfigEngine.sh wp-create-realm -DWasPassword=password
- 8) **i5/OS:** ConfigEngine.sh wp-create-realm -DWasPassword=password
- 9) Restart the server1 and WebSphere_Portal servers.
- 10) Launch portal page in web browser and tried to login as Second Realm admin user id/pwd .Should be able to login to portal successfully.
- 11) Logout and to login as First Realm admin user id/pwd .Should be able to login to portal successfully.Search for users/groups belong to both realms and results should show both realms users and groups.