HCL SOFTWARE

HCL Digital Experience

Step-by-Step Guide

How to replace your HCL Portal´s LDAP

Author:

Fernanda de Sousa Gomes

HCL Digital Experience L2 Support

HCL Technologies

Contents

Before you start…

It is quite common to see a requirement to replace HCL Portal´s LDAP. This guide describes the steps required to have HCL Portal working properly with the new LDAP server. In this scenario, we are changing the LDAP´s hostname and the LDAP´s base DN.

If you are only changing the LDAP´s hostname and **not** the base DN, you should refer to the following article:

[How do I update the LDAP hostname being referenced by HCL Portal?]

This guide can be used for on-premises HCL Digital Experience deployments, being a stand-alone or cluster environments.

As any major change, it is **highly recommended** to have a complete **backup** of your system before starting. For more information about backup and restore in HCL Digital Experience:

https://help.hcltechsw.com/digital-experience/8.5/admin-system/i_wadm_c_bkup_restr_winlinux.html

For the scenario covered in this guide, consider the following:

Current LDAP Hostname:
`sds64020.hcl.com`
Current LDAP Base DNs:
`dc=hcl,dc=com`
`dc=nandavp,dc=hcl,dc=com`
Current Portal and WAS Administrator:
`uid=portaladmin,cn=users,dc=hcl,dc=com`
Current Portal Administrator Group:
`cn=portaladmins,cn=groups,dc=hcl,dc=com`
Current Virtual Portal Administrator:
`uid=vpadmin,cn=users,dc=nandavp,dc=hcl,dc=com`
Current Virtual Portal Administrator Group:
`cn=vpadmins,cn=groups,dc=nandavp,dc=hcl,dc=com`

New LDAP Hostname:
`sds64020b.hcl.com`
New LDAP Base DNs:
`dc=hcldev,dc=com`
`dc=nandavp,dc=hcldev,dc=com`
New Portal and WAS Administrator:
`uid=portaladmin,cn=users,dc=hcldev,dc=com`
New Portal Administrator Group:
`cn=portaladmins,cn=groups,dc=hcldev,dc=com`
New Virtual Portal Administrator:
`uid=vpadmin,cn=users,dc=nandavp,dc=hcldev,dc=com`
New Virtual Portal Administrator Group:
`cn=vpadmins,cn=groups,dc=nandavp,dc=hcl,dc=com`

1- Generating a complete XML export of system with the current LDAP

Generate a FULL XML Export from your BASE Portal and your Virtual Portals:

Reference:

https://support.hcltech.com/csm?id=kb_article&sysparm_article=KB0012516

Example to export your Base Portal:

```
<wp_profile>/PortalServer/bin/xmlaccess.sh -url http://hostname:10039/wps/config -in
<WebSphere>/PortalServer/doc/xml-samples/Export.xml -out FullExportBASE.xml -user
<admin> -password <password>
```

Example to export a Virtual Portal called “nandavp”:

```
<wp_profile>/PortalServer/bin/xmlaccess.sh -url
http://hostname:10039/wps/config/nandavp -in <WebSphere>/PortalServer /doc/xml-
samples/Export.xml -out FullExportVP.xml -user <admin> -password <password>
```

2- Listing all your Virtual Portals

If you have Virtual Portals, it is a good practice to list and keep their information, with this data and a complete XML export, you can quickly restore it if necessary:

Example:

```
<wp_profile>/ConfigEngine/ConfigEngine.sh list-all-virtual-portals -
DPortalAdminPwd=<password> -DWasPassword=<password>
```

Reference:

https://help.hcltechsw.com/digital-experience/8.5/admin-system/advp_cfgtsk_list.html?hl=list-all-virtual-portals

The output will show up in your `<wp_profile>/ConfigEngine/log/ConfigTrace.log`

This is the information you need to keep:

```
[wsadmin] ____________________________________________________
 [wsadmin] VirtualPortal:
 [wsadmin] Title:       nandavp
 [wsadmin] Description:
 [wsadmin] Realm:       NandaVPRealm
 [wsadmin] Object ID:   Z18_48L2G342O8LV60Q7H6EBBN0000
 [wsadmin] Hostname:    <cannot be retrieved>
 [wsadmin] Context:     nandavp
 [wsadmin] Short ID:    -9992
 [wsadmin] ____________________________________________________
```

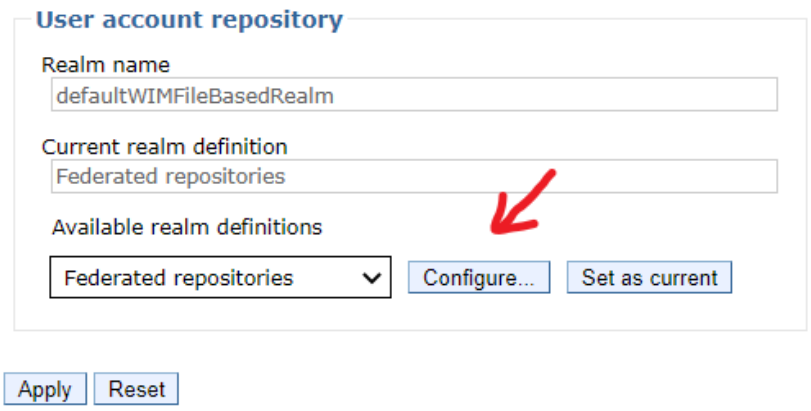
3- Adding the “InternalFileRepository” user repository

When you are replacing the LDAP, it is important that you have the out-of-the-box FileRegistry repository in place. We need to make sure that you will not lose the WAS and Portal Administration during this process, so before removing the old LDAP and adding the new one, we set the Portal and WAS Administrator ID to the out-of-the-box values located in the FileRegistry repository.

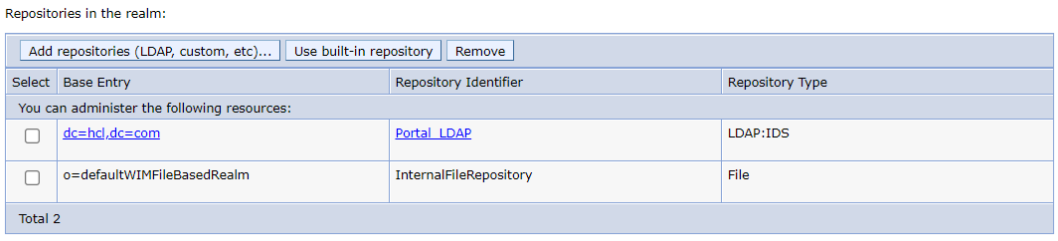
By default, Portal is configured with a Federated Repository with the **InternalFileRepository** user repository. Even after adding one or more User Repositories, such as a LDAP, the **InternalFileRepository** will remain there, unless you manually remove it.

If you are not sure you still have the **InternalFileRepository** in place, you can use the steps below to check:

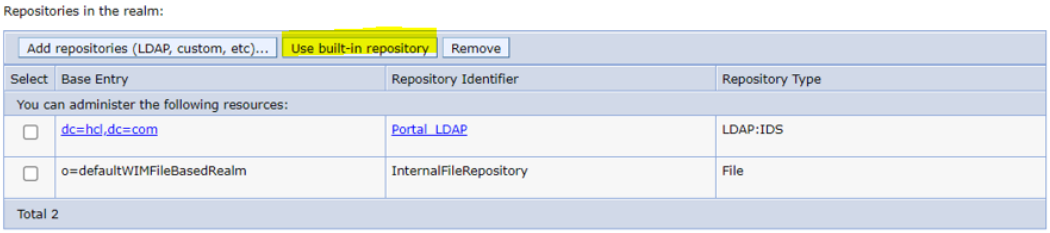
1- Access your WAS Admin Console using your current WAS Administrator user ID
2- Select: **Security >> Global Security**
3- Under **User Account Repository**, click on **Configure**:



4- The list of repositories in this realm is listed, if you see the “InternalFileRepository” in the list, it means, you are good to go and can continue with the next session:



5- If you no longer see the **InternalFileRepository** user repository, click on **Use built-in repository** to add it back.



a. Save the changes and synchronize your nodes, if cluster
b. Restart the server

4- Temporarily changing your admin user and group to your FileRegistry repository

Temporarily, before removing the current LDAP and adding the new one, we set the Portal and WAS Administrator ID to the out-of-the-box values located in the FileRegistry repository.

For the record, these are the information we will be using for step:

Temporary Portal and WAS Administrator User ID: `uid=wpsadmin,o=defaultWIMFileBasedRealm`
Temporary Password: `wpsadmin`
Temporary Portal Administrator User Group: `cn=wpsadmins,o=defaultWIMFileBasedRealm`

PS: If you no longer have your FileRegistry repository, or you are not sure you still have it, you can follow the steps to check or re-add it in Adding the "InternalFileRepository" user repository

Follow the steps below to complete this section:

1- Run the following task to replace the old HCL Portal administrative user with the temporary user:

```
./ConfigEngine.sh wp-change-portal-admin-user -DWasPassword=<WAS_password> -
DnewAdminId=uid=wpsadmin,o=defaultWIMFileBasedRealm -DnewAdminPw=wpsadmin -
DnewAdminGroupId=cn=wpsadmins,o=defaultWIMFileBasedRealm
```

Where, `<WAS_password>` is the password of the current WAS Administrator user.

2- Run the following task to replace the old WebSphere® Application Server administrative user with the temporary user:

```
./ConfigEngine.sh wp-change-was-admin-user -DWasPassword=<WAS_password> -
DnewAdminId=uid=wpsadmin,o=defaultWIMFileBasedRealm -DnewAdminPw=wpsadmin
```

Where, `<WAS_password>` is the password of your current WAS Administrator user, that is, the one located in your OLD LDAP.

3- Restart all WebSphere processes

5- Removing the OLD LDAP

Now that you have switched your Portal and WAS Administrators to your FileRegistry repository, it is time to remove your old LDAP:

1- Change to the wp_profile_root/ConfigEngine directory.

PS: Steps **2-10** are only required for those who have **multiple realms**, if it is not your case, skip those steps and go straight to step 11.

2- Run the following task to list the names and types of configured repositories:

```
./ConfigEngine.sh wp-query-realm -DWasPassword=wpsadmin
```

3- Check the ConfigEngine output and take note of your realm names, in this example, we have two:

```
[[wplc-query-realm] Realms : [defaultWIMFileBasedRealm, NandaVPRealm]
```

4- Edit your wkplc.properties with the following:

```
realmName=NandaVPRealm
```

5- Now, we need to list the base entries for this realm, take note, because they will be necessary for a later step:

```
./ConfigEngine.sh wp-query-realm-baseentry -DWasPassword=wpsadmin
```

The output includes the information you need to keep, example:

```
[wplc-query-realm-baseentry] Base entries for realm NandaVPRealm
propRealmBaseEntryList: [dc=hcl,dc=com, dc=nandavp,dc=hcl,dc=com,
o=defaultWIMFileBasedRealm]
```

6- Repeat steps 4 and 5 above, for the default realm `defaultWIMFileBasedRealm`:

```
realmName=defaultWIMFileBasedRealm
```

The output for the `defaultWIMFileBasedRealm` looks like this:

```
 [wplc-query-realm-baseentry] Base entries for realm defaultWIMFileBasedRealm
propRealmBaseEntryList: [o=defaultWIMFileBasedRealm, dc=nandavp,dc=hcl,dc=com]
```

Using the information we have captured above, we must perform the 2 actions below, otherwise, you wont be able to remove the old LDAP repository:

a. Temporarily remove the `NandaVPRealm` realm;
b. Temporarily remove the base-entry `dc=nandavp,dc=hcl,dc=com` from the `defaultWIMFileBasedRealm` realm;

7- Change your `wkplc.properties` with the following:

```
deleteRealmName=NandaVPRealm
```

8- Run the following task to remove the realm temporarily:

```
./ConfigEngine.sh wp-delete-realm -baseentry -DWasPassword=wpsadmin
```

9- Change your wkplc.properties with the following:

```
realmName=defaultWIMFileBasedRealm

deleteBaseEntry=dc=nandavp,dc=hcl,dc=com
```

10- Run the following task to remove base entry from the realm temporarily

```
./ConfigEngine.sh wp-delete-realm-baseentry -DWasPassword=wpsadmin
```

11- Run the following task to list the names and types of configured repositories:

```
./ConfigEngine.sh wp-query-repository -DWasPassword=wpsadmin
```

12- Check the ConfigEngine output for your current LDAP information, example:

```
[wplc-query-federated-repository] SDS_LDAP : {specificRepositoryType=IDS,
repositoryType=LDAP, host=sds64020.hcl.com} : [{certificateMapMode=EXACT_DN,
primaryServerQueryTimeInterval=15, supportAsyncMode=false,
supportTransactions=false, certificateFilter=,
adapterClassName=com.ibm.ws.wim.adapter.ldap.LdapAdapter,
searchTimeLimit=120000, isExtIdUnique=true, supportExternalName=false,
loginProperties=[uid],
baseEntries={dc=nandavp,dc=hcl,dc=com=dc=nandavp,dc=hcl,dc=com,
dc=hcl,dc=com=dc=hcl,dc=com}, sslConfiguration=, searchCountLimit=500,
supportPaging=false, returnToPrimaryServer=true, supportSorting=false,
id=SDS_LDAP, supportChangeLog=none, translateRDN=false, ldapServerType=IDS}]
```

13- Go to the `wp_profile_root/ConfigEngine/properties` directory.
14- Open the `wkplc.properties` file with a text editor.
15- Enter the following parameters in the `wkplc.properties` file under `VMM Delete federated repository` heading, example:

```
federated.delete.baseentry=dc=hcl,dc=com

federated.delete.id=SDS_LDAP
```

16- Save your changes to the `wkplc.properties` file.
17- Run the following task to delete the required repository:

```
./ConfigEngine.sh wp-delete-repository -DWasPassword=wpsadmin
```

18- Stop and restart the WAS processes to propagate the changes.

6- Adding the new LDAP

Here, we will be using ConfigWizard to add the new LDAP:

1- Start the ConfigWizard server:

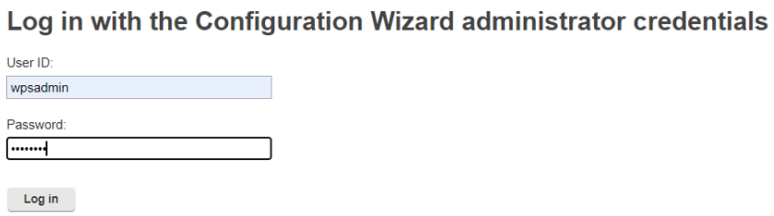
```
<WebSphere>/AppServer/profiles/cw_profile/bin/startServer.sh server1
```

2- Access the ConfigWizard GUI:

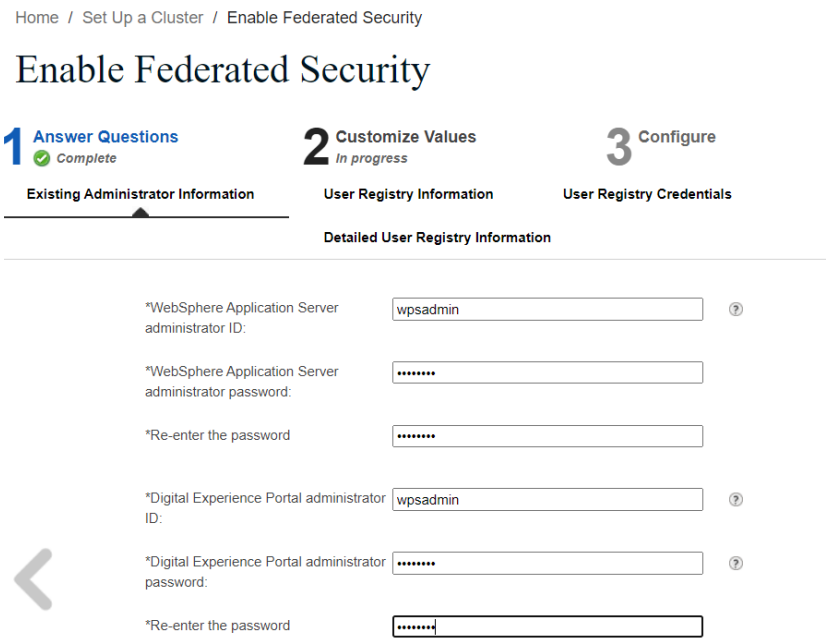
http:// your_server:10200/ibm/wizard/login.jsp

Note: If working with HCL Digital Experience 8.5 or 9 software level prior to CF18, the wizard address will be: *http://your_server:10200/ibm/wizard*. After installing CF18, the configuration wizard will automatically be adjusted to *http://your_server:10200/hcl/wizard*.

3- Authenticate as the default “wpsadmin” user and password (if you didn’t change it)

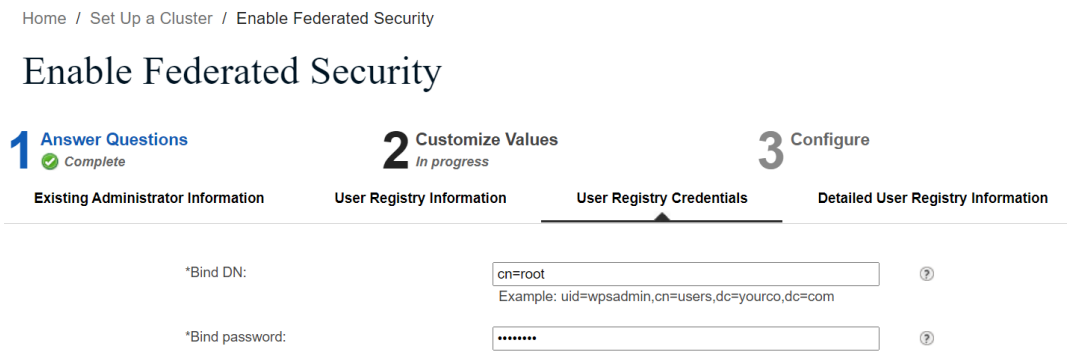


4- Click on **SET UP A CLUSTER** or **SET UP A STAND-ALONE SERVER** as appropriate
5- Select **ENABLE FEDERATED SECURITY**
6- The System Information panel will be displayed. Click **Next** to continue
7- Fill out the Security Settings Panel as appropriate. Click **Next**
8- Enter your ***current*** WAS and Portal Administrator information, in this case, the user from your InternalFileRepository and click **Next**:

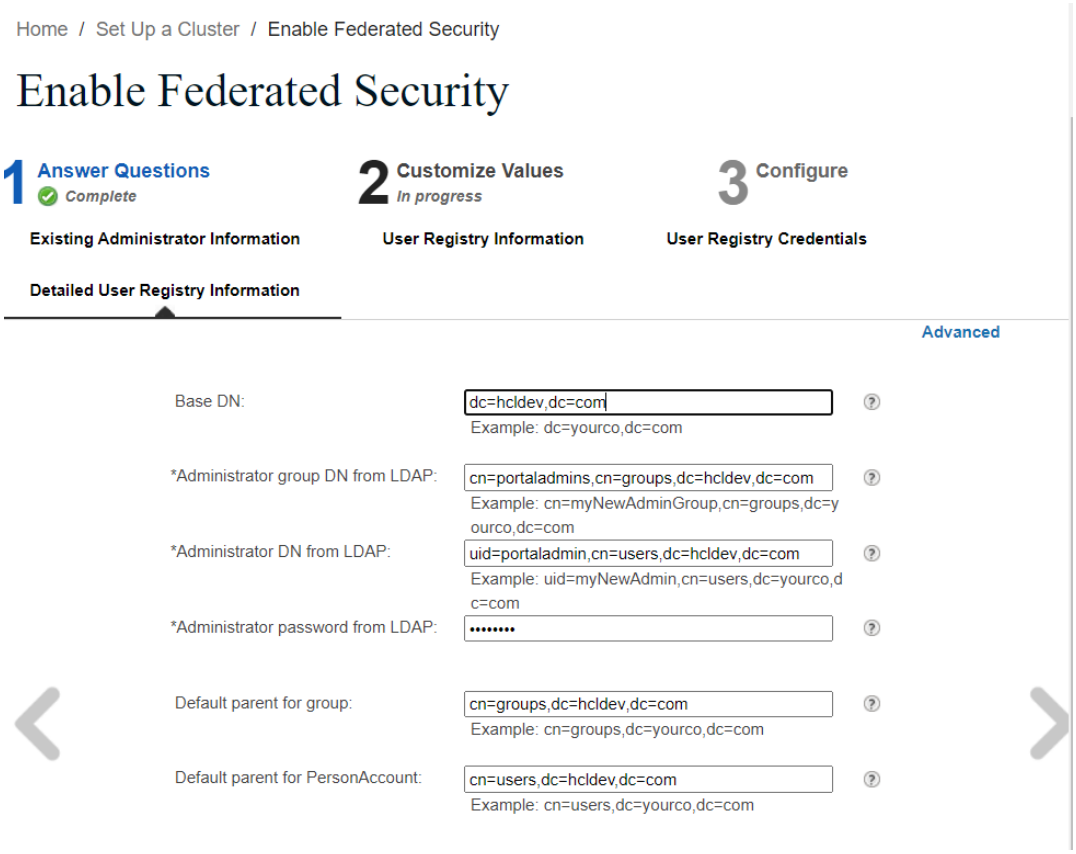


9- Now, enter your new LDAP information and click **Next**:

10- Enter your LDAP bind user and password, click **Next**:



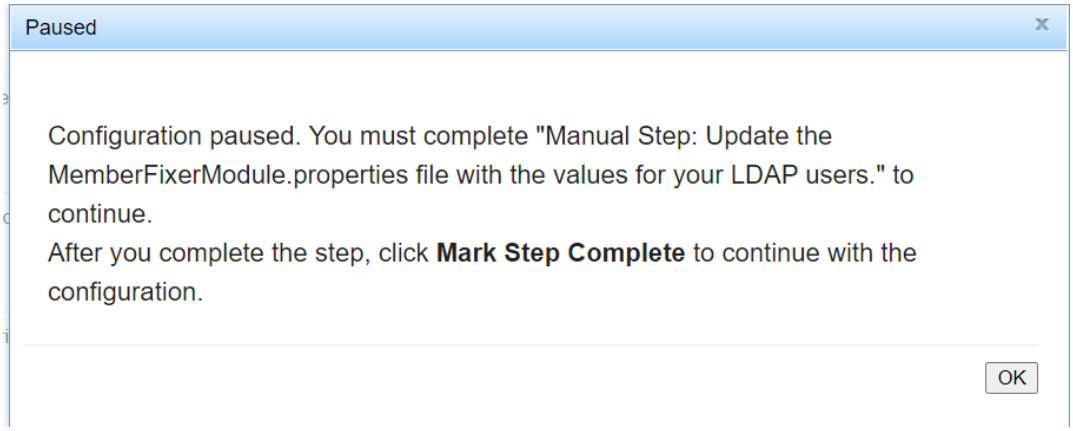
11- Enter information of your new LDAP Administrator user and group. Example:



12- Click **Next**.

13- Now, you are ready to start the configuration by clicking on **Start Configuration** and then, **OK**. This will start the configuration process automatically.

14- When it completes step 10, the configuration will pause:



15- Step 11 is marked as a “Manual Step”, manually follow the instructions for this step:

a. Edit `<wp_profile>/PortalServer/wcm/shared/app/config/wcmservices/MemberFixerModule.properties`

b. At the bottom of the file, add the line below. This change allows the member fixer tool to map the previous portal administrator ID to the new portal administrator ID. Use the full Distinguished Name (DN) for the user IDs entered in this line:

```
[old user DN] -> [new user DN]
```

```
#
# uid=user1,ou=websphere,c=au,o=ibm -> uid=user2,ou=tivoli,c=au,o=ibm
# cn=group1,dc=lotus,o=ibm -> cn=group2,dc=rational,o=ibm

# Configure part replacement of a distinguished names. This will
# change all of the distinguished name except the ID
#
# Example: To replace all DNs like cn=[ID],dc=websphere,o=ibm with cn=[ID],dc=tivoli,o=ibm
, use:
# cn=[ID],dc=websphere,o=ibm -> cn=[ID],dc=tivoli,o=ibm
#
# uid=[ID],ou=websphere,c=au,o=ibm -> uid=user2,ou=tivoli,c=au,o=ibm
# cn=[ID],dc=websphere,o=ibm -> cn=[ID],dc=tivoli,o=ibm
#uid=wpsadmin,o=defaultWIMFileBasedRealm -> uid=portaladmin,cn=users,dc=hcl,dc=com
uid=portaladmin,cn=users,dc=hcl,dc=com -> uid=portaladmin,cn=users,dc=hcldev,dc=com
```

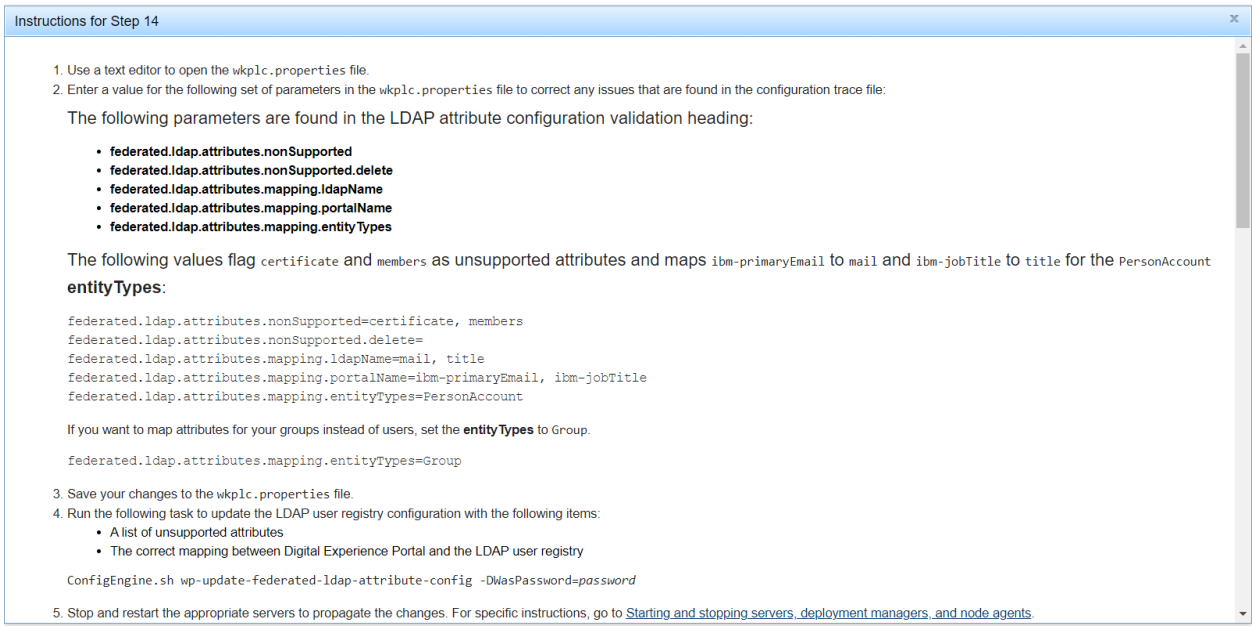
c. Save your changes.

PS: As you can see here, we are adding the OLD Portal Administrator ID as opposed to the “wpsadmin” user ID. This is because the “wpsadmin” was just a temporary change and you should not have any WCM data created with this user.

16- Once you are done, click on **Mark Step Complete** for this step.

17- Step 12 can take a while to complete, as it runs the MemberFixer tool. You can see its progress in the `<wp_profile>/logs/WebSphere_Portal/SystemOut.log`

18- The configuration will pause once again for step 14, click on **Instructions for step 14** and complete the steps as you see fit:



19- Once you are done, click on **Mark Step Complete** for this step, then click **Finished**.

Now, we must recreate the base entry and the realm that we have removed earlier:

20- Run the following task to list the names and types of configured repositories:

```
./ConfigEngine.sh wp-query-repository -DWasPassword=<password>
```

21- Check the ConfigEngine output for your current LDAP information, example:

```
[wplc-query-federated-repository] ************************************

[wplc-query-federated-repository] SDS_LDAP : {specificRepositoryType=IDS,
repositoryType=LDAP, host=sds64020.hcl.com} : [{certificateMapMode=EXACT_DN,
primaryServerQueryTimeInterval=15, supportAsyncMode=false,
supportTransactions=false, certificateFilter=,
adapterClassName=com.ibm.ws.wim.adapter.ldap.LdapAdapter,
searchTimeLimit=120000, isExtIdUnique=true, supportExternalName=false,
loginProperties=[uid], baseEntries={dc=hcldev,dc=com=dc=hcldev,dc=com},
sslConfiguration=, searchCountLimit=500, supportPaging=false,
returnToPrimaryServer=true, supportSorting=false, id=SDS_LDAP,
supportChangeLog=none, translateRDN=false, ldapServerType=IDS}]
```

22- Go to the `wp_profile_root/ConfigEngine/properties` directory.
23- Open the `wkplc.properties` file with a text editor.
24- Enter the following parameters in the `wkplc.properties` file:

```
id=SDS_LDAP

baseDN=dc=nandavp,dc=hcldev,dc=com

nameInRepository=dc=nandavp,dc=hcldev,dc=com
```

25- Save your changes to the `wkplc.properties` file.
26- Run the following task to create the baseentry:

```
./ConfigEngine.sh wp-create-base-entry -DWasPassword=<password>
```

27- Open the `wkplc.properties` file with a text editor.
28- Enter the following parameters in the `wkplc.properties` file

```
realmName=NandaVPRealm

addBaseEntry=dc=hcldev,dc=com

securityUse=active

delimiter=/
```

29- Run the following task to recreate the realm:

```
./ConfigEngine.sh wp-create-realm -DWasPassword=<password>
```

30- Now, you must add the 2nd base entry for your realm, change the `wkplc.properties`:

```
realmName=NandaVPRealm

addBaseEntry=dc=nandavp,dc=hcldev,dc=com
```

31- Run the following task to add more base entries to the realm configuration:

```
./ConfigEngine.sh wp-add-realm-baseentry -DWasPassword=<password>
```

32- Repeat steps **31-32** to add all the base entries required for this realm.
33- Enter a value for the following parameters in the `wkplc.properties` file in the VMM realm configuration section:

```
realmName=NandaVPRealm

realm.personAccountParent=cn=users,dc=nandavp,dc=hcldev,dc=com

realm.groupParent=cn=groups,dc=nandavp,dc=hcldev,dc=com

realm.orgContainerParent=dc=nandavp,dc=hcldev,dc=com
```

34- Run the following task to update the default parents per entity type and realm:

```
./ConfigEngine.sh wp-modify-realm-defaultparents -DWasPassword=<password>
```

35- Restart all WebSphere processes

7- Running CleanupUsers to clear up the old LDAP entries

The article below describes this process very well, you can follow the steps as described there:

https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0069350

8- Re-importing the Full XML Export

In this section, we will manually update the Full XML Export with the new user DN information and re-import it.

1- Create a backup of the full XML Export `FullExportBASE.xml` that was generated on step 1 and save it as `FullExportBASE_Changed.xml`.

2- Edit the `FullExportBASE_Changed.xml`, find **all** entries that contains your OLD DN information and replace them with your NEW DN information, for example:

   Find: `dc=hcl,dc=com` and replace with: `dc=hcldev,dc=com`

3- Now, we will prevent the portlets from being redeployed, since this is not necessary and would take a long time to complete. Find and replace these entries:

   Find: `<url>` and replace with: `<!--url>`

   Find: `</url>` and replace with: `</url-->`

   The result for **all** entries containing a <url> tag should be like this, in **blue**:

```
<web-app action="update" active="true" domain="rel" objectid="Z1_0000000000000A0BR2B300IG4" removable="true" uid="login.war.webmod">
    <!--url>file://localhost/$archive_root$/login.war.webmod/login.war</url-->
    <context-root>/wps/PA_Login_Portlet_App</context-root>
    <display-name>PA_Login_Portlet_App</display-name>
```

4- Now, import the changed XML file into your BASE Portal, for example:

```
<wp_profile>/PortalServer/bin/xmlaccess.sh -url
http://hostname:10039/wps/config -in FullExportBASE_Changed.xml -out
resultBASE.xml -user <portal_admin> -password <password>
```

5- Repeat steps **1-4** for you Virtual Portal and import the XML as the example below:

```
<wp_profile>/PortalServer/bin/xmlaccess.sh -url
http://hostname:10039/wps/config/nandavp -in FullExportVP_Changed.xml -out
resultVP.xml -user <admin> -password <password>
```

9- Running MemberFixer with treatallUsersAsMissing

Use the **treatAllUsersAsMissing** parameter to indicate to WCM that all users won't exist in the current repository and nonexistent handling should take place.

Note: Use this parameter with care and make sure to create a backup repository before proceeding.

Reference:

https://help.hcltechsw.com/digital-experience/8.5/wcm/wcm_admin_member-fixer.html

This is an example of running MemberFixer against an specific WCM Library (`-Dlibrary="MyLibrary"`):

```
./ConfigEngine.sh run-wcm-admin-task-member-fixer -DPortalAdminId=username -
DPortalAdminPwd=password -DWasUserId=username -DWasPassword=password -
Dlibrary="MyLibrary" -Dfix=true -DtreatAllUsersAsMissing=true
```

If you prefer to run against all Web Content Libraries, this is how you do it:

```
./ConfigEngine.sh run-wcm-admin-task-member-fixer -DPortalAdminId=username -
DPortalAdminPwd=password -DWasUserId=username -DWasPassword=password -
DallLibraries=true -Dfix=true -DtreatAllUsersAsMissing=true
```

For Virtual Portals, you must add the `-DVirtualPortalContext` or `-DVirtualPortalHostName`, for example:

```
./ConfigEngine.sh run-wcm-admin-task-member-fixer -DPortalAdminId=username -
DPortalAdminPwd=password -DWasUserId=username -DWasPassword=password -
Dlibrary="MyLibrary" -Dfix=true -DVirtualPortalContext=nandavp
```

Optional: Once MemberFixer completes it´s execution, confirm that all items have been properly handled generating a report (-Dfix=false):

```
./ConfigEngine.sh run-wcm-admin-task-member-fixer -DPortalAdminId=username -
DPortalAdminPwd=password -DWasUserId=username -DWasPassword=password -
Dlibrary="MyLibrary" -Dfix=false
```

Done. You have completed the steps to change your Portal LDAP hostname and Base DN.