IBM Workload Scheduler
SSO Configuration with LDAP

Summary

Single Sign-On (SSO) is a method of access control that allows a user to authenticate once and gain access to the resources of multiple applications sharing the same user registry.

This means that using SSO you can run queries on the plan or manage object definitions on the database accessing the engine without authenticating, automatically using the same credentials you used to log in to the Dynamic Workload Console.

The same is true when working with the Self-Service Catalog and Self-Service Dashboards apps from a mobile device. If the Dynamic Workload Console has been configured to use SSO, then these apps automatically use the same credentials used to log in to the Dynamic Workload Console.

Solution

WebSphere Administrative Console:

Jazz (Dynamic Workload Console "DWC") – 16316

http://hostname:16316/ibm/console

TWS (Workload Scheduler "Engine") – 31124

http://hostname:31124/ibm/console

Setup Realm Name

To enable SSO based on an LTPA token, the realm name for both DWC and Engine in WebSphere Application Server cells must be identical, which requires you to update the realm name.

Within WebSphere Administrative Console do the following steps for both DWC and Engine:

1. Log into the WebSphere Application Server Integrated Solutions Console as an administrator (ie. twsuser), expand Security, and select Global Security.
2. Click Configure... beside the Federated Repositories list.
3. Modify the Realm Name in the General Properties page to FQDN of the server (ie. twsserver.company.com), and click OK and save.
4. Recycle WebSphere

Export / Import LTPA Keys

To successfully decrypt the LTPA token from other parties, the WebSphere Application Server cells in the same SSO domain should share the same LTPA key. You can choose to export the LTAP key from any of the servers in the SSO domain. To do this:

Export Key

1. Log into the DWC WebSphere Application Server Integrated Solutions Console as an administrator, expand Security, and select Global Security.
2. Click LTPA in the Authentication section and then, in the Cross-cell single sign-on section, provide values for the following fields:
3. Password: Enter the password that you used for the key file that you exported.
4. Confirm password: Reenter the password; it must be same as the one you just entered.
5. Fully qualified key file name: Specify a fully qualified path on WebSphere Application Server for the file that will hold the exported keys. The LTPA key is encrypted with the password specified above.
6. Click Export keys.

Import Key

When the LTPA key is exported from one WebSphere Application Server cell, it should be imported to all other server cells in the same SSO domain. To import the LTPA key, perform the following steps on each server except for the server you exported the key from:

1. Log into the Engine WebSphere Application Server Integrated Solutions Console as an administrator, expand Security, and select Global Security.
2. Click LTPA in the Authentication section and then, in the Cross-cell single sign-on section, provide values for the following fields:
3. Password: Enter a secure password that you can remember. You will need to provide this password later, when you import the keys you are exporting.
4. Confirm password: Reenter the password; it must be same as the one you just entered.
5. Fully qualified key file name: Specify a valid path on WebSphere Application Server for the file that will hold the exported keys. LTPA key is encrypted with the password specified above.
6. Click Import keys.

Disable Automatic Key Generation

WebSphere Application Server provides the function to automatically generate the LTAP key via a schedule, increasing the security by refreshing the LTPA key in a single cell. However, when different WebSphere Application Server cells are involved in SSO, it is recommended to turn off the key generation; otherwise, once the LTPA key is refreshed, SSO between servers in different cells will break.

Follow these steps to disable automatic key generation:

1. Log into both the Engine and DWC WebSphere Application Server Integrated Solutions Console as an administrator, expand Security, and select Global Security.

2. Click LTPA in the Authentication section and then, in the Key generation section, click Key set groups.
3. Select NodeLTPAKeySetGroup in the table and, in the Key generation section, un-check the Automatically generate keys check box, if is already checked.
4. Click OK to save the changes.
5. Recycle both Engine and DWC WebSphere's

Create Temp Administrative User

We will be using the local file repository of WebSphere for the administrative user and LDAP for user authentication. We are able to remove the PAM repository in WebSphere. The Engine's WebSphere administrative user is tied to PAM instead of being in the local file repository.

Change the Administrative user to a temporary WebSphere local file repository user:

1. Log into the Engine's WebSphere Application Server Integrated Solutions Console as an administrator (ie. twsuser), expand Users and Groups, and select Manage Users.
2. Click Create
3. Enter the details of the user ID, and then click Create. (ie of user ID: tempuser)
    a. Do not add any mapped roles or groups to the user
4. expand Security, and select Global Security.
5. Click Configure... beside the Federated Repositories list.
6. Replace the existing user for Primary administrative user name to your new user id created in the previous step (ie. tempuser)
1. Replace the existing user and password for Server user identity with twsuser and its password
7. Recycle WebSphere

Remove PAM repository

1. Log into the Engine WebSphere Application Server Integrated Solutions Console as an administrator (ie. tempuser), expand Security, and select Global Security.
2. Click Configure... beside the Federated Repositories list.
3. Select the twaPAM Base Entry from the Repositories in the realm box, click Remove and Save
4. Recycle WebSphere

Create Administrative User

1. Log into the Engine's WebSphere Application Server Integrated Solutions Console as an administrator (ie. twsuser), expand Users and Groups, and select Manage Users.

2. Click Create
3. Enter the details of the IBM Workload Scheduler administrator user ID, and then click Create. (ie of user ID: twsuser)
    a. Do not add any mapped roles or groups to the user
4. Expand Security, and select Global Security.
5. Click Configure... beside the Federated Repositories list.
6. Replace the existing user for Primary administrative user name to your new user id created in the previous step (ie. twsuer)
7. Replace the existing user and password for Server user identity with twsuser and its password.
8. Recycle WebSphere

Configure LDAP

1. Log into the Engine and DWC WebSphere Application Server Integrated Solutions Console as an administrator (ie. tempuser), expand Security, and select Global Security.
2. Click Configure... beside the Federated Repositories list.
3. Click Manage repositories under Related Items
4. Select Add button and click LDAP repository
5. Fill in the following fields
    a. Directory type:
    b. Port (if different than default)
    c. Primary host name
    d. Bind distinguished name
    e. Bind password
6. Click OK and Save
7. Expand Security, and select Global Security.
8. Click Configure... beside the Federated Repositories list.
9. Under Repositories in the realm and select Add repositories (LDAP, custom, etc)
10. Fill in the following fields
    a. Repository
    b. Unique distinguished name of the base (or parent) entry in the federated repository
11. Click OK and select Save
12. Expand Security, and select Global Security.
13. Click Configure... beside the Federated Repositories list.
14. Select the LDAP Repository Identifier
15. Select Federated repositories entity types to LDAP object classes mapping

16. Click PersonAccount under Entity Type
17. In the Search filter textbox enter:
    (&(!(cn=<Administrative_User>))(ObjectCategory=User))
18. Restart WebSphere