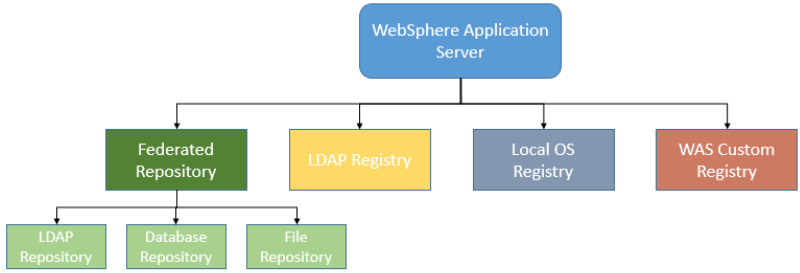
CHAPTER 17: SECURITY

Theory

WebSphere Application Server provides a strong security infrastructure that is usually complex and requires a high level understanding of different areas such as application, network infrastructure and user management. Therefore, WebSphere Application Server has different layers for security management:

- Physical security points out the areas where the environment is physically located.
- Network security contains areas to be protected against network based attacks.
- Operating system security means the security infrastructure of the operating system where WebSphere Application Server runs on.
- JVM security deals with security services between Java applications and operating system services.
- Java 2 security contains access control to system resources such as file system, threading and class loading.
- Java EE security API defines methods for applications to obtain user name and role.
- CSIv2 is a 3-tiered security protocol that provides message protection, interoperable authentication and delegation.
- WebSphere security provides variety of security services such as authentication, authorization, security auditing and so on, for applications running on WebSphere Application Server.

Authentication confirms a user's identity using user registries. WebSphere Application Server supports different types of user registries:



- Federated repository provides a single view for multiple user registries including all types of registries below and in addition to them database repository.
- Local operating system registry provides support to multiple operating systems like Windows, Linux, Solaris and AIX. This type of user registry should be used only for single server installation.

- LDAP registry provides authentication from a single LDAP tree. It is possible to configure high availability as long as all LDAP servers having the same user information.
- Custom registry allows you to implement Security Policy Index by using its user registry interface.

WebSphere Application Server uses different roles each of which has a set of typical user tasks. This helps to control the WebSphere Application Server environment in terms of security and management. In WebSphere, following administrative roles are defined:

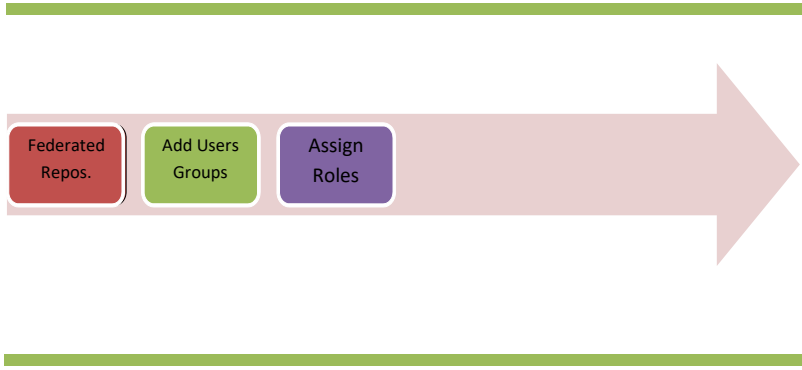
- Monitor gives you the least permissions that allow you to view configuration and current state.
- Configurator, in addition to monitor allows you to change configuration.
- Operator has same permissions as monitor and also able to change the runtime state.
- Administrator role is the super user of WebSphere Application Server.
- ISC admins role allows you to manage users and groups in a federated repository using administrative console.
- Deployer can both configuration and runtime operations.
- Admin security manager role permits users to assign administrator role.
- Auditor role, in addition to monitor role, can view and change only security auditing system.

AIM

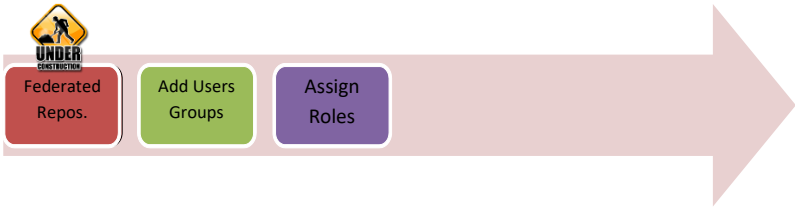
In this lab exercise, you will be able to configure the most common and important security settings of WebSphere Application Server in an enterprise environment. In order to achieve this goal, you need to complete following tasks:

1. Configure federated user repository
2. Add new users and groups
3. Assign users and groups to roles

Lab Exercise 17: SECURITY

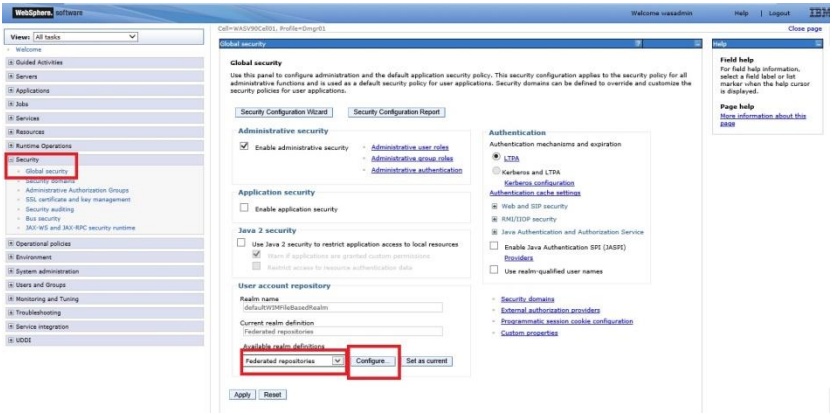


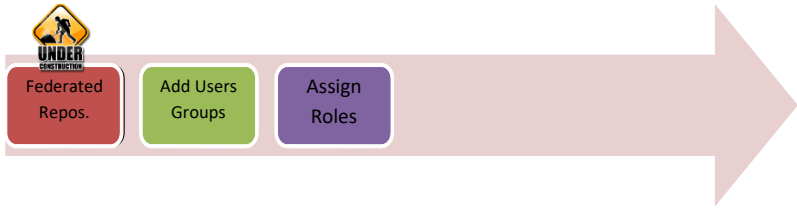
1. **Configure federated user repository**
2. **Add new users and groups**
3. **Assign users and groups to roles**



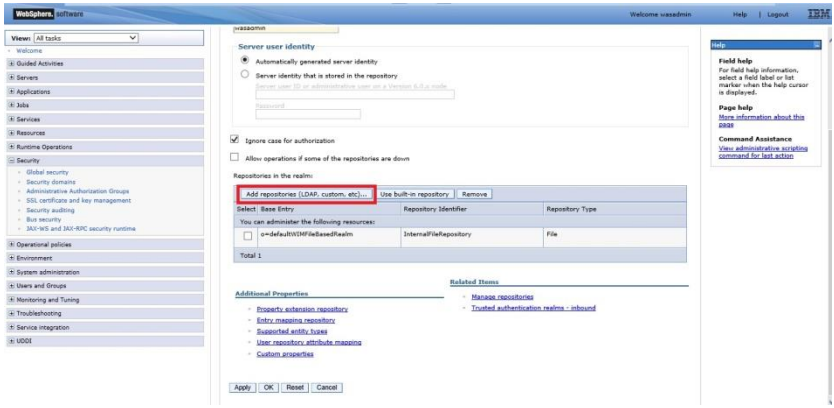
Task 1: Configure federated user repository

Step 1: Navigate to “Security>Global security”, select “Federated repositories” as “Available realm definitions” and then click “Configure”.

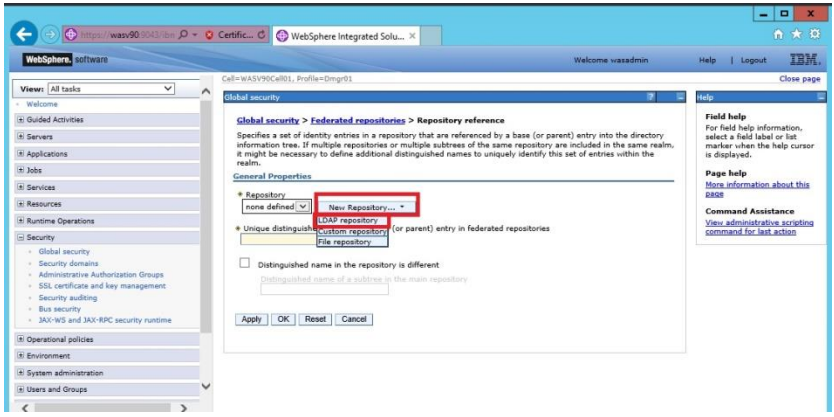


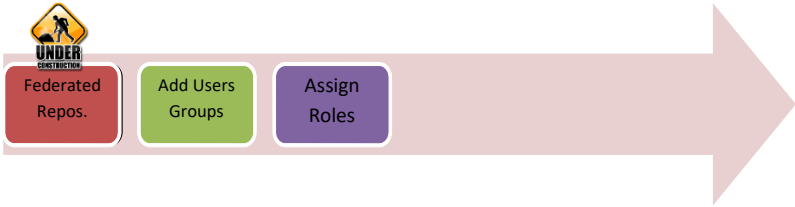


Step 2: Click on “Add repositories (LDAP, customer, etc)”.

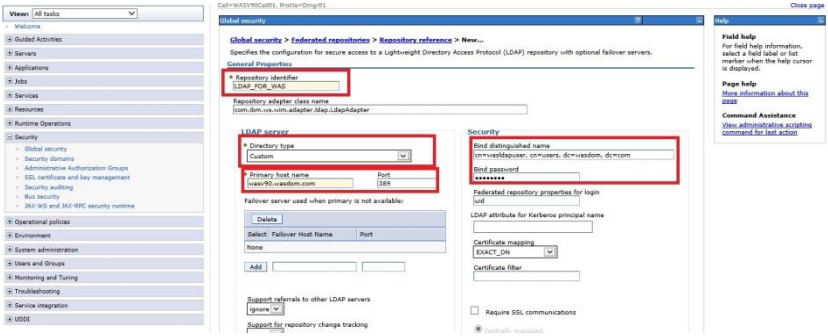


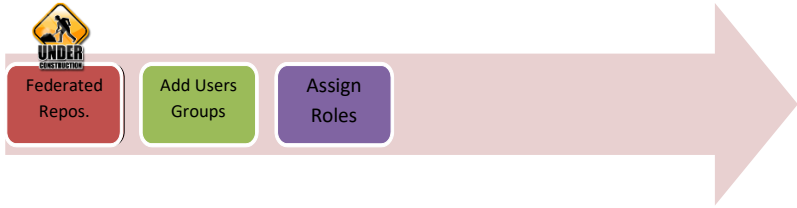
Step 3: Click “New Repository” and select “LDAP repository” from the list.





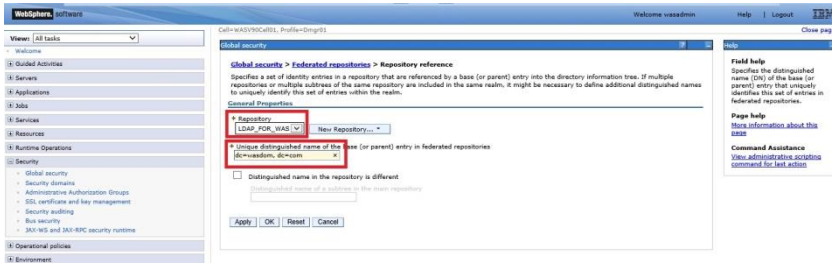
Step 4: We need to specify the configurations needed to connect and search users from LDAP server.

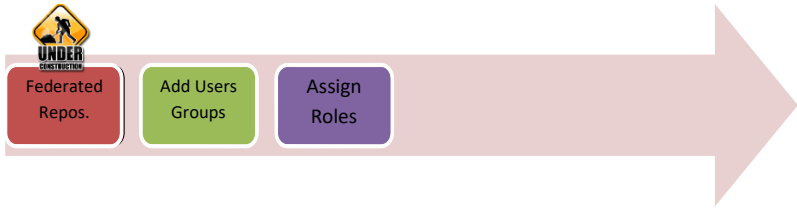




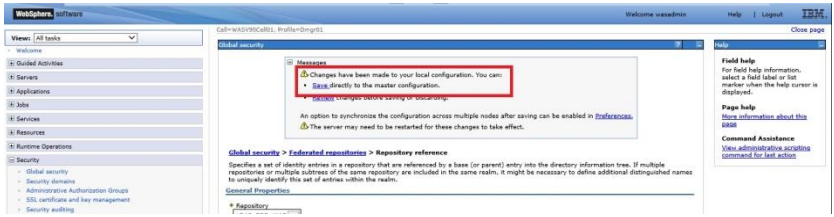
Step 5: Click “Save” to add new LDAP repository to the configuration.

Step 6: Enter unique distinguished name of the LDAP repository we defined in previous steps, then click “OK”.

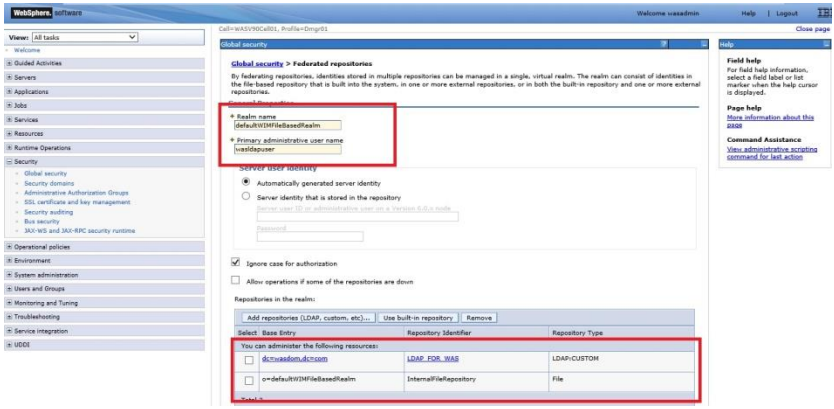


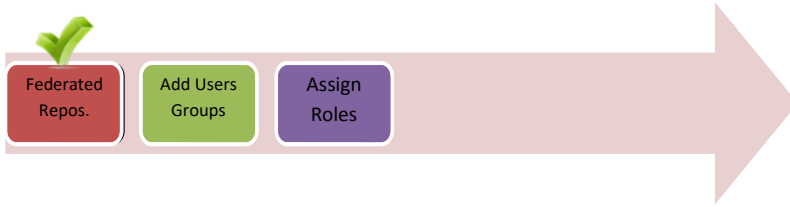


Step 7: Click “Save” to write changes to the master configuration file.

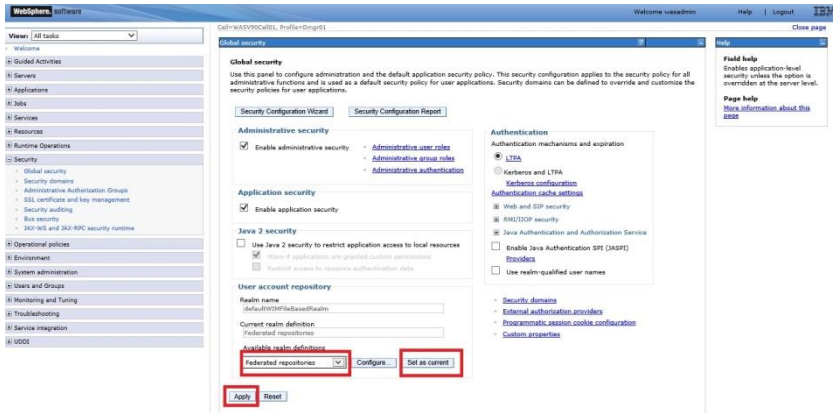


Step 8: Define the primary administrative user name and then click “OK”.

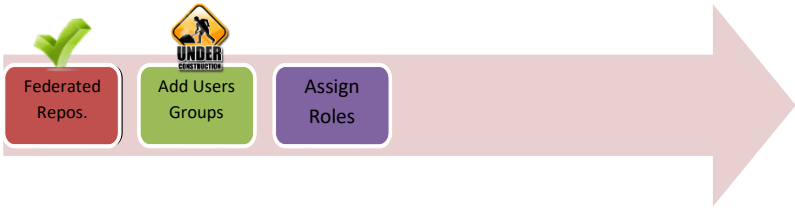




Step 9: Click on “Set as current” while “Federated repositories” is selected and click “Apply” to finish configuration.s

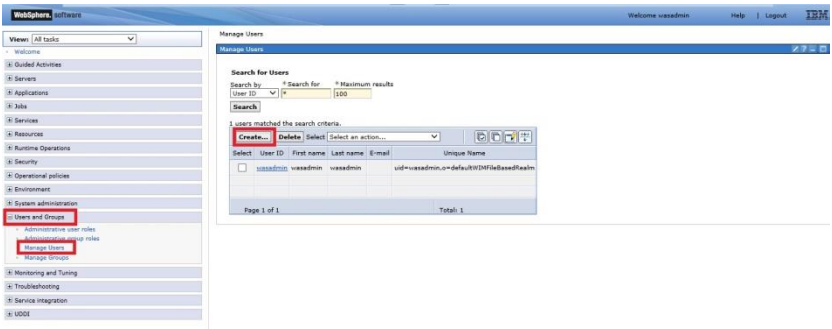


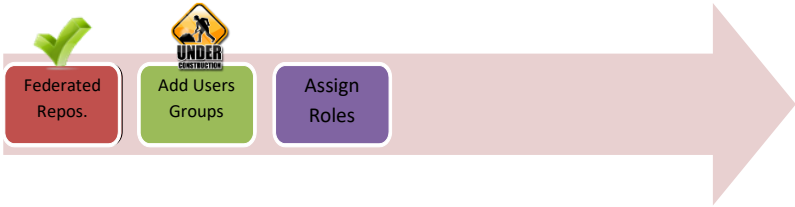
Task 1 is complete!



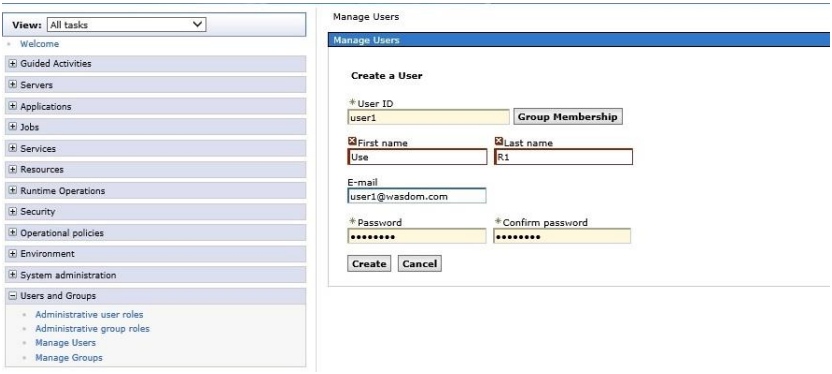
Task 2: Add new users and groups

Step 1: Navigate “Users and Groups>Manage Users” and click “Create”.

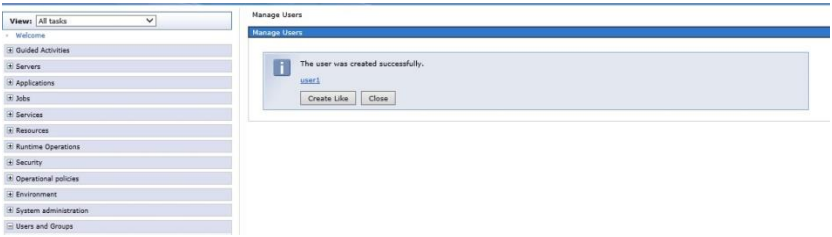


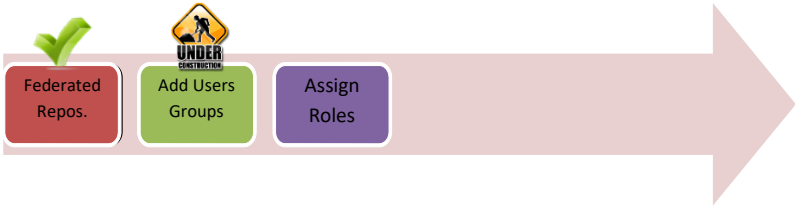


Step 2: Enter user information such as name, e-mail and password, then click "Create".

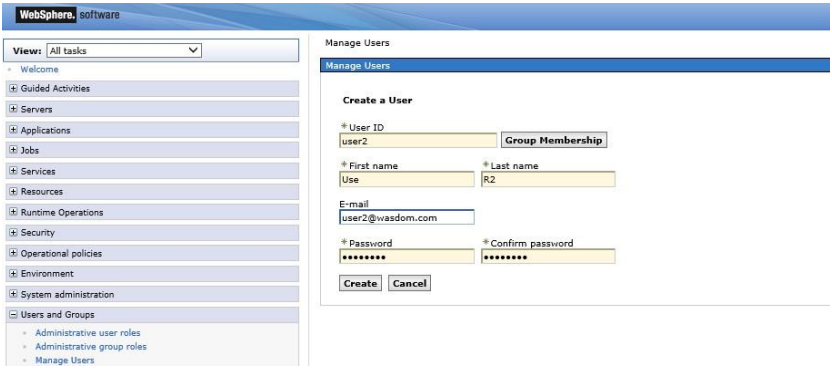


Step 3: You should be able to see the success message as below. Click "Create Like" to add another user.

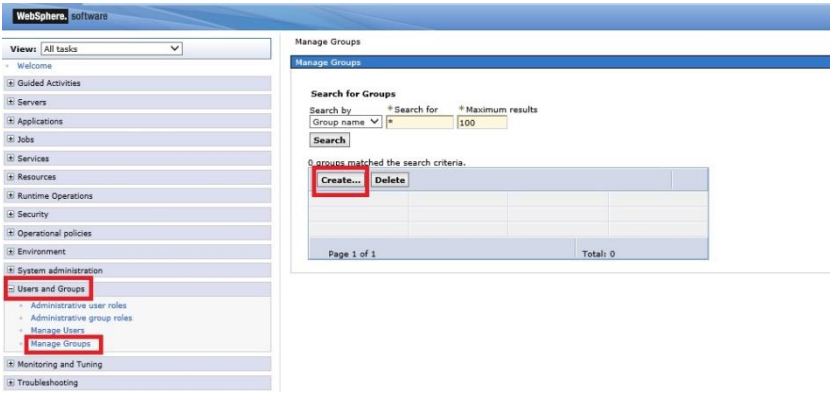


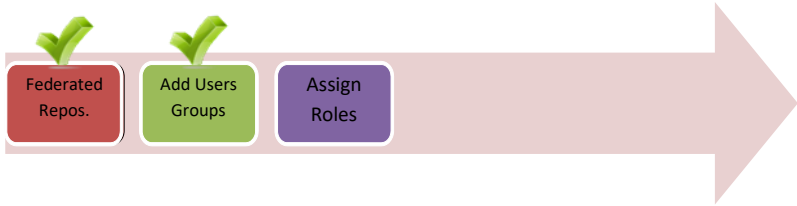


Step 4: Repeat the Step 2 and click “Create”.

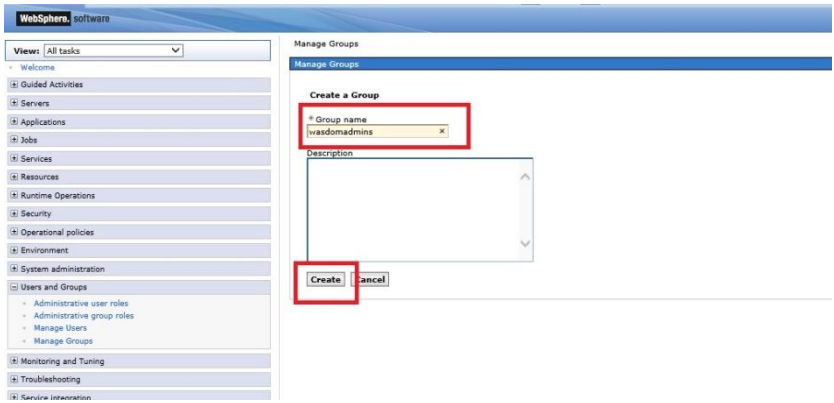


Step 5: Navigate to “Users and Groups>Manage Groups” and click “Create”.

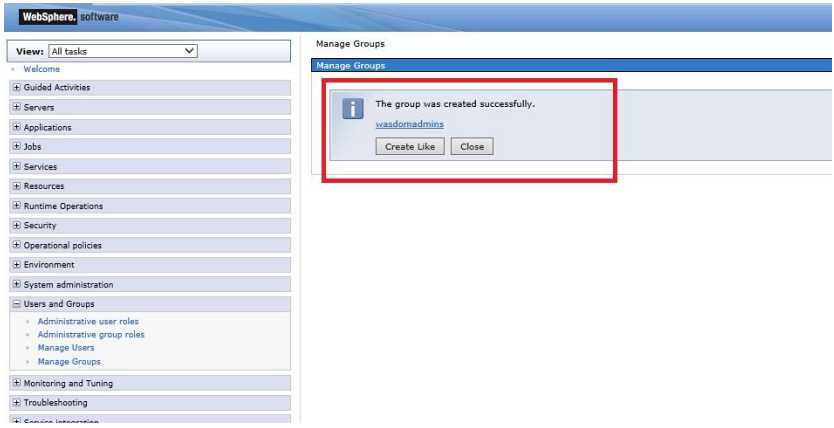




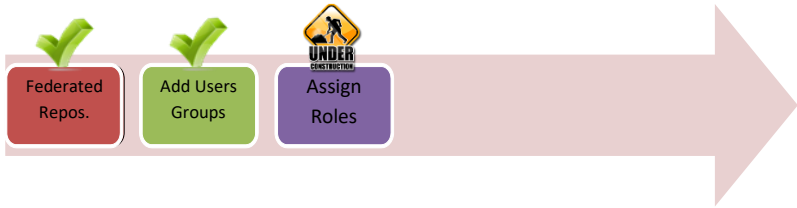
Step 6: Enter a group name and click “Create”.



Step 7: You should get similar success message.

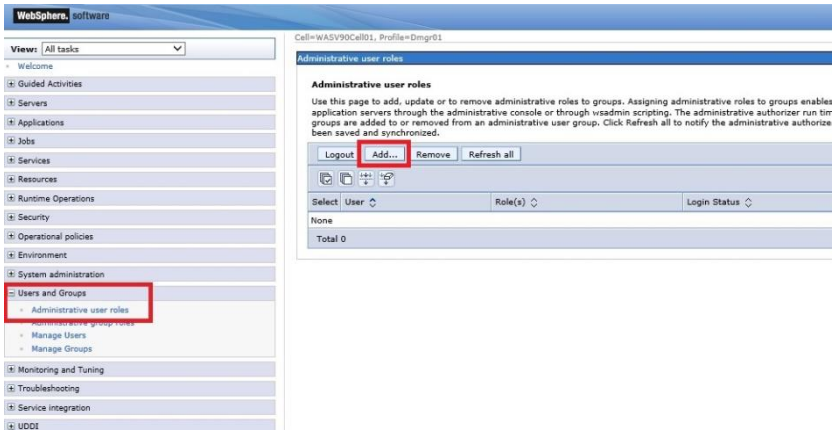


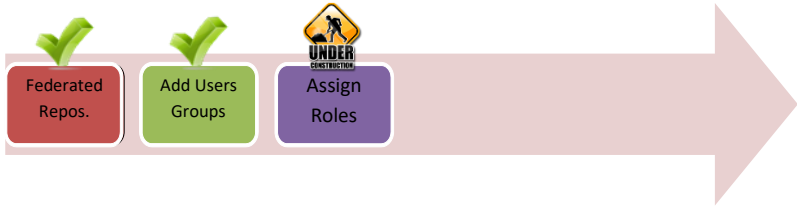
Task 2 is complete!



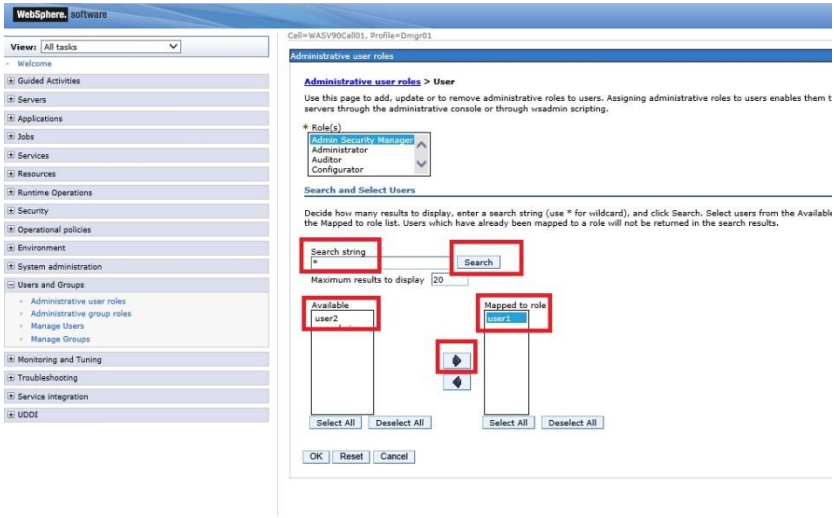
Task 3: Assign users and groups to roles

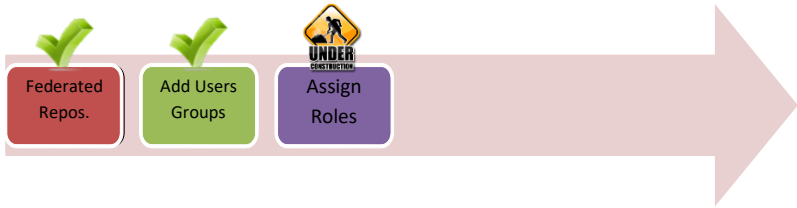
Step 1: Navigate to “Users and Groups>Administrative user roles” and click “Add”.



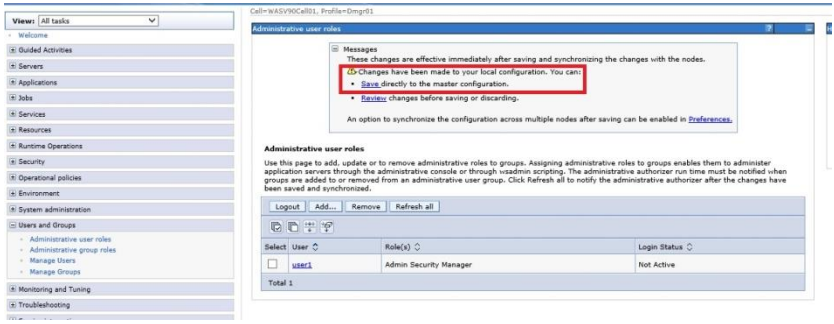


Step 2: Select the role from the list (e.g. Admin Security Manager), search the user you want to assign the role, from the results in “Available” list, highlight the user and send it to “Mapped to role” by clicking on right arrow. When ready, click “OK”.

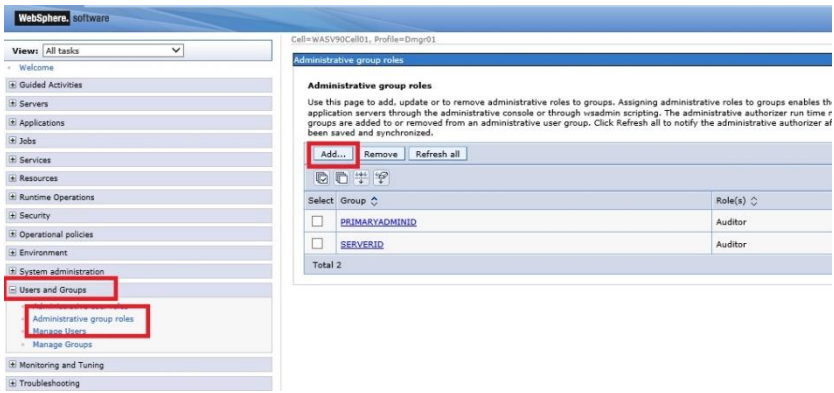


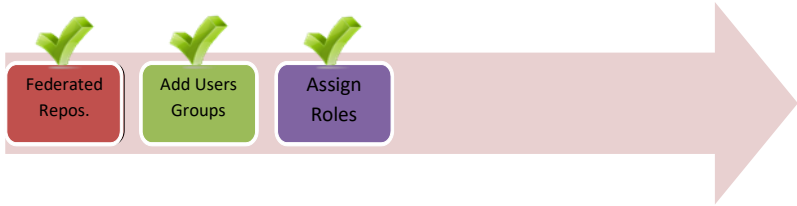


Step 3: Click “Save” to write changes to the master file.

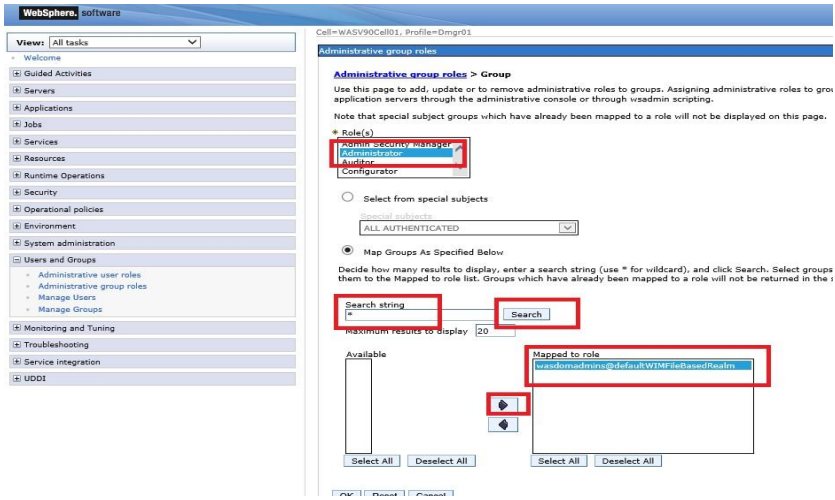


Step 4: Navigate to “Users and Groups>Administrative group roles” and click “Add”.

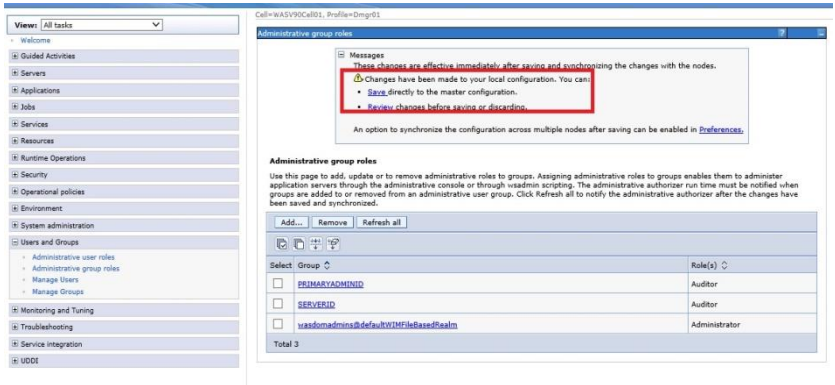




Step 5: Select the role (e.g. Administrator) and map the group you want to assign this role with similar way described in Step 2, then click “OK”.



Step 6: Click “Save” to write changes directly to the master configuration file.



Task 3 is complete!

SUMMARY

WebSphere Application Server provides a strong security infrastructure in different layers that are physical, network, operating system, JVM and so on. As part of authentication, WebSphere Application Server supports different types of user registries. It is also possible to use more than one user registry by using federated repositories. There are different roles are defined that are task oriented and using roles make easier management of user security.

REFERENCES

- http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/welc6topsecuring.html?lang=en
- http://publib.boulder.ibm.com/infocenter/discover/v8r5m0/index.jsp?topic=/com.ibm.discovery.es.ad.doc/security/iiysawasglobal.htm
- http://www.ibm.com/developerworks/websphere/techjournal/1210_lansche/1210_lansche.html

INDEX