

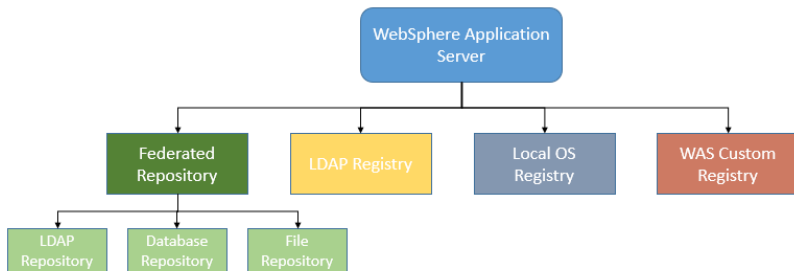
## CHAPTER 17: SECURITY

### 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.

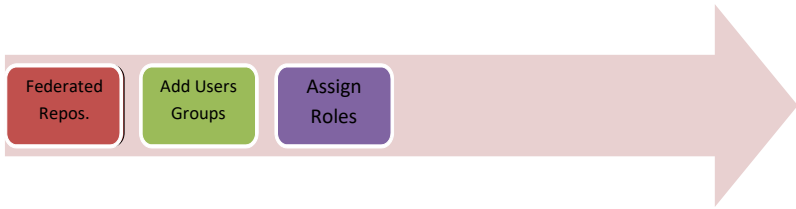
## AIM

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**



Federated  
Repos.

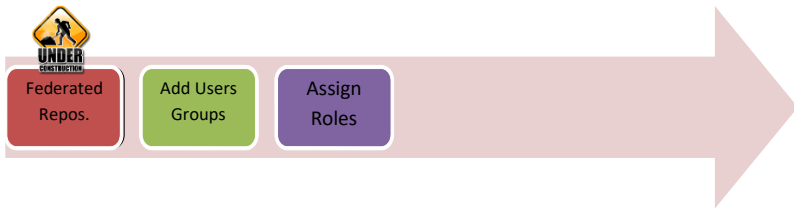
Add Users  
Groups

Assign  
Roles

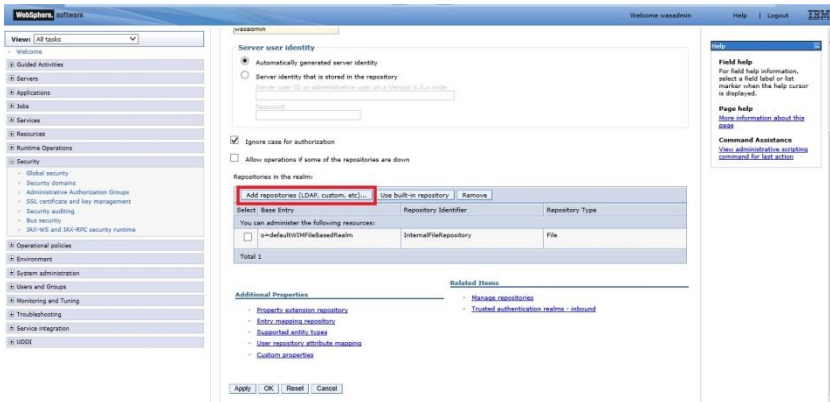
## Task 1: Configure federated user repository

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

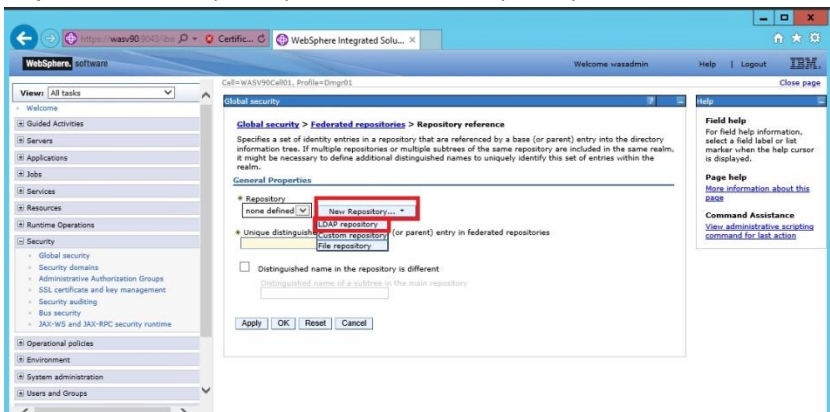
The screenshot displays the WebSphere Security Administration console. On the left, the navigation tree is visible with 'Global security' selected. The main content area shows the 'Global security' configuration page. The 'Administrative security' section has 'Enable administrative security' checked. The 'Application security' section has 'Enable application security' unchecked. The 'Java 2 security' section has 'Use Java 2 security to restrict application access to local resources' checked. The 'User account repository' section shows 'Available realm definitions' with 'Federated repositories' selected and the 'Configure' button highlighted. The right sidebar contains help links for field, page, and topic help.



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



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





Federated  
Repos.

Add Users  
Groups

Assign  
Roles

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

The screenshot shows the 'Global security' console with the 'Federated repositories' section selected. The 'Repository reference' is 'New...'. The 'General Properties' section is expanded, showing the 'Repository identifier' as 'LDAP\_Federated' and the 'Repository adapter class name' as 'com.ibm.ws.siam.adapter.Map.LdapAdapter'. The 'LDAP server' section is also expanded, showing the 'Directory type' as 'Custom', the 'Primary host name' as 'ldap01.us.ibm.com', and the 'Port' as '389'. The 'Security' section is expanded, showing the 'Bind distinguished name' as 'cn=ldapadmin, cn=users, dc=us.ibm.com', the 'Bind password' as '\*\*\*\*\*', and the 'Certificate mapping' as 'EXACT\_OU'. The 'LDAP attribute for Kerberos principal name' is set to 'uid'. The 'Require SSL communications' checkbox is checked.

Global security > Federated repositories > Repository reference > New...

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

General Properties

Repository identifier  
LDAP\_Federated

Repository adapter class name  
com.ibm.ws.siam.adapter.Map.LdapAdapter

LDAP server

Directory type  
Custom

Primary host name  
ldap01.us.ibm.com

Port  
389

Fallover server used when primary is not available:

Default: Failover Host Name Port

Name Port

Add

Support referrals to other LDAP servers  
Ignore

Support for repository change tracking

Security

Bind distinguished name  
cn=ldapadmin, cn=users, dc=us.ibm.com

Bind password  
\*\*\*\*\*

Federated repository properties for login  
uid

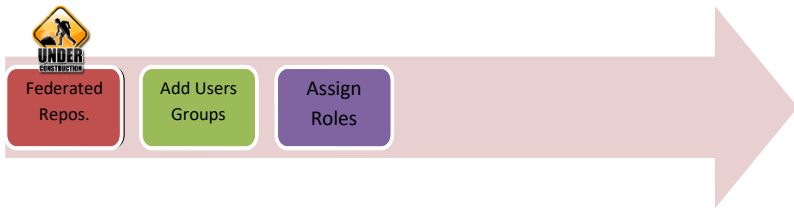
LDAP attribute for Kerberos principal name

Certificate mapping  
EXACT\_OU

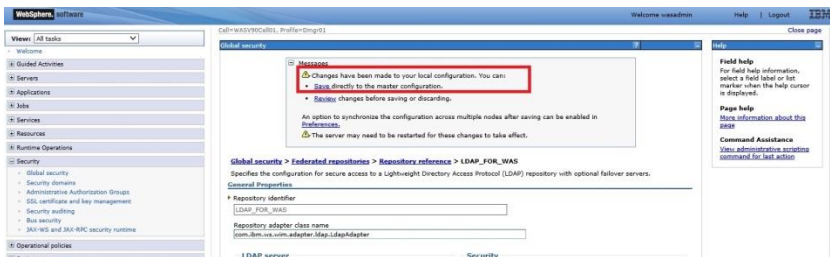
Certificate filter

Require SSL communications

Customized required



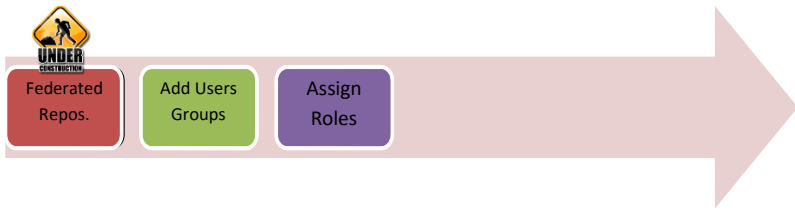
**Step 5:** Click “Save” to add new LDAP repository to the configuration.



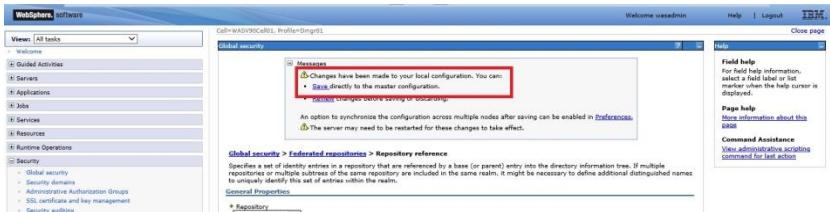
**Step 6:** Enter unique distinguished name of the LDAP repository we defined in previous steps, then click “OK”.



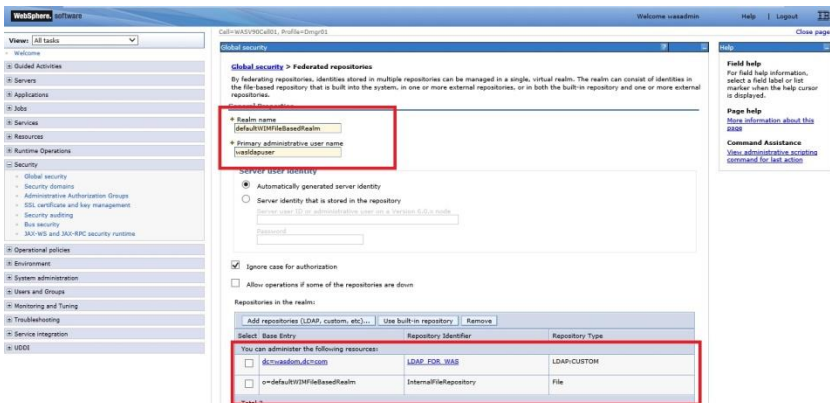


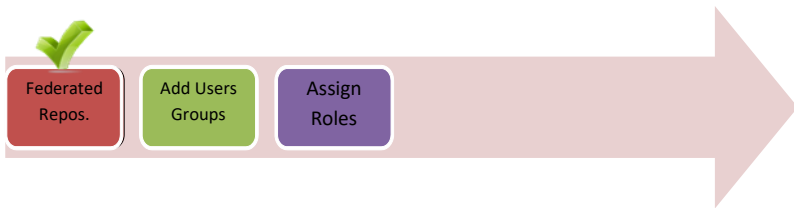


**Step 7:** Click “Save” to write changes to the master configuration file.



**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

WebSphere Software Security Configuration Wizard

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard | Security Configuration Report

**Administrative security**

☒ Enable administrative security

- Administrative user roles
- Administrative authentication

**Application security**

☒ Enable application security

**Java 2 security**

☒ Use Java 2 security to restrict application access to local resources

☒ Warn if applications are granted custom permissions

☐ Restrict access by resource authentication data

**User accessed repository**

Realm name: defaultRealm

Current realm definition: Federated repositories

Available realm definitions

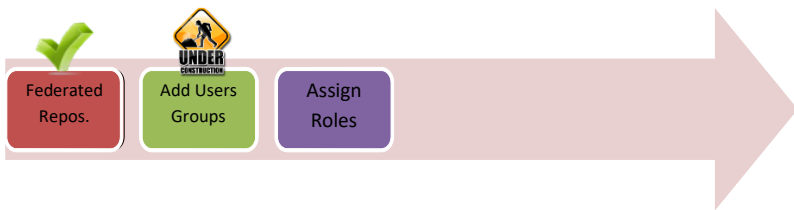
Federated repositories ☒ Configure... **Set as current**

**Apply** **Reset**

**Field help**  
Enables application-level security unless the option is overridden at the server level.

**Page help**  
Click information about this page

**Task 1 is complete!**

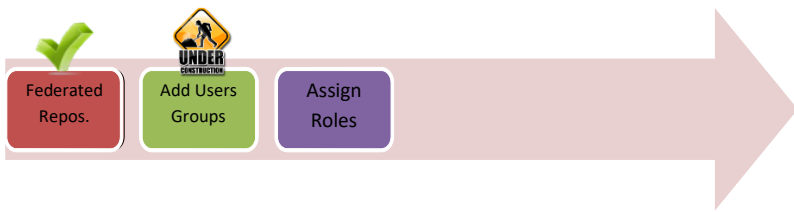


## Task 2: Add new users and groups

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

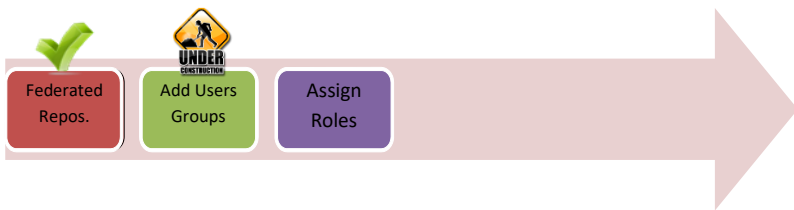
The screenshot shows the WebSphere software interface. On the left is a navigation pane with a tree view. The 'System administration' section is expanded, and 'Users and Groups' is selected. Within 'Users and Groups', 'Manage Users' is highlighted with a red box. The main content area displays the 'Manage Users' page. It includes a search bar with fields for 'Search by' (set to 'User ID'), 'Search for' (set to '\*'), and 'Maximum results' (set to '100'). Below the search bar, a message states '1 users matched the search criteria:'. A table lists the user details, with the first row highlighted. The table has columns for 'Select', 'User ID', 'First name', 'Last name', 'E-mail', and 'Unique Name'. The first row contains a checkbox, 'vvasadmin', 'vvasadmin', 'vvasadmin', 'vvasadmin@vvasadmin.com', and 'vvasadmin@vvasadmin.com'. At the bottom of the table, it says 'Page 1 of 1' and 'Total: 1'.

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	vvasadmin	vvasadmin	vvasadmin	vvasadmin@vvasadmin.com	vvasadmin@vvasadmin.com



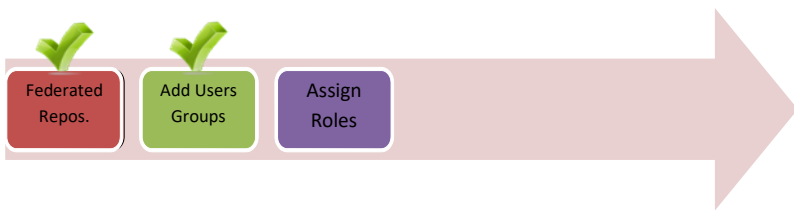
**Step 2:** Enter user information such as name, e-mail and password, then click “Create”.

**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”.



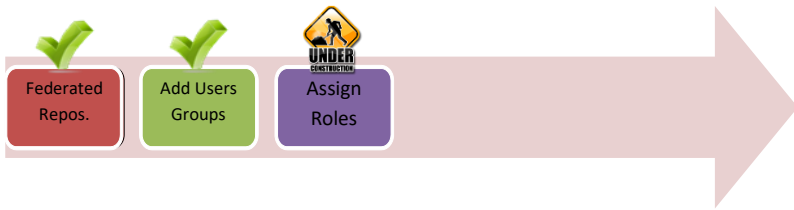
**Step 6:** Enter a group name and click “Create”.

The screenshot shows the WebSphere software interface. On the left is a navigation pane with a 'Views' dropdown set to 'All tasks'. The main area is titled 'Manage Groups'. A 'Create a Group' dialog box is open, with the 'Group name' field containing 'wasdomadmins' and the 'Create' button highlighted with a red box.

**Step 7:** You should get similar success message.

The screenshot shows the WebSphere software interface. On the left is a navigation pane with a 'Views' dropdown set to 'All tasks'. The main area is titled 'Manage Groups'. A success message is displayed: 'The group was created successfully. wasdomadmins'. The 'Create Like' and 'Close' buttons are visible.

**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”.

WebSphere software

Cell=WASV90Cell01, Profile=Dmgr01

**Administrative user roles**

Administrative user roles

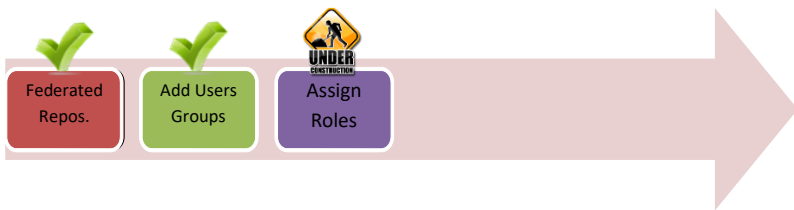
Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables application servers through the administrative console or through vsadmin scripting. The administrative authorizer run time groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer been saved and synchronized.

Logout Add... Remove Refresh all

Select User Role(s) Login Status

None

Total 0



**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”.

WebSphere<sup>®</sup> software

Cell=WASV90Cell01, Profile=Dmgr01

Administrative user roles

**Administrative user roles > User**

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to servers through the administrative console or through wsadmin scripting.

**Role(s)**

Admin Security Manager  
Administrator  
Auditor  
Configurator

**Search and Select Users**

Decide how many results to display, enter a search string (use \* for wildcard), and click Search. Select users from the Available the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string: \* Search

Maximum results to display: 20

**Available**

user2

**Mapped to role**

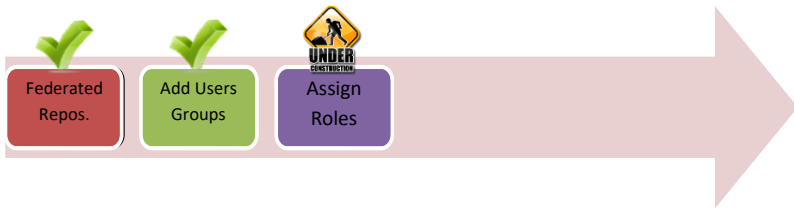
user2

Select All Deselect All

Select All Deselect All

OK Reset Cancel





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

Cell=WASV90Cell01\_Profile=Dmgr01

**Administrative user roles**

Messages  
These changes are effective immediately after saving and synchronizing the changes with the nodes.  
AD changes have been made to your local configuration. You can:  
• [Save](#) directly to the master configuration.  
• [Discard](#) changes before saving or discarding.  
An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

Administrative user roles  
Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through vsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Logout Add... Remove Refresh all

Select:	User	Role(s)	Login Status
<input type="checkbox"/>	USER1	Admin Security Manager	Not Active

Total 1

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

WebSphere software

Cell=WASV90Cell01\_Profile=Dmgr01

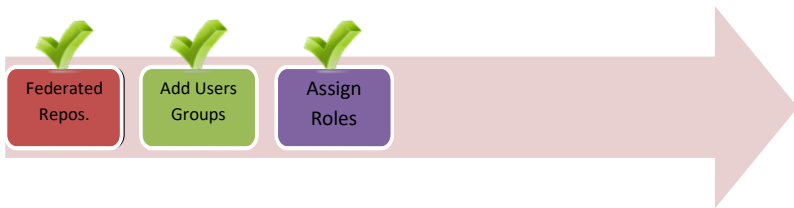
**Administrative group roles**

Administrative group roles  
Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through vsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Add... Remove Refresh all

Select:	Group	Role(s)
<input type="checkbox"/>	PRIMARYADMINID	Auditor
<input type="checkbox"/>	SERVERID	Auditor

Total 2



**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://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](http://www.ibm.com/developerworks/websphere/techjournal/1210_lansche/1210_lansche.html)

## INDEX

administrative roles .....	515
Authentication .....	514
Federated repository .....	515
LDAP registry.....	515
Local operating system registry .....	515
user registries .....	514