

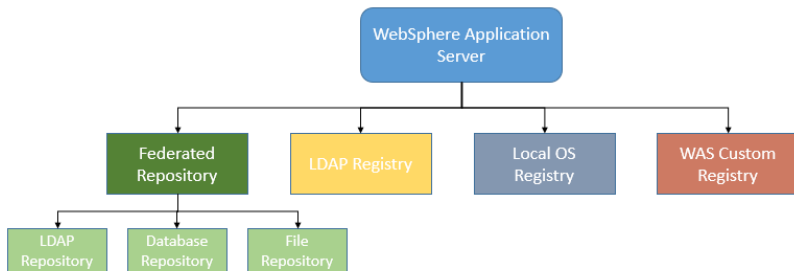
## CHAPTER 17: SECURITY

### 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:

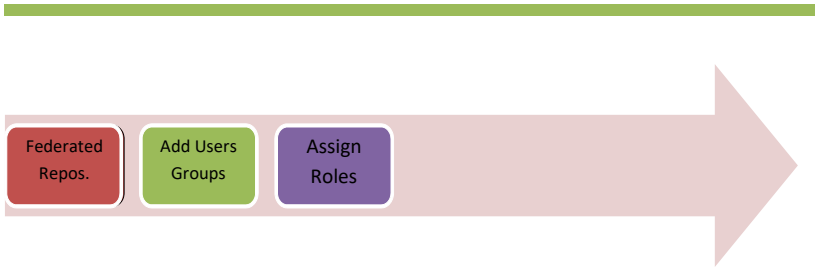
- Monitor gives you the least permissions that allow you to view configuration and current state.
- Configurator, in addition to monitor allows you to change configuration.
- Operator has same permissions as monitor and also able to change the runtime state.
- Administrator role is the super user of 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

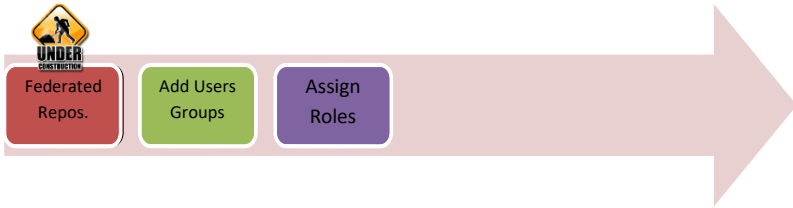
In this lab exercise, you will be able to configure the most common and important security settings of WebSphere Application Server in an enterprise environment. In order to achieve this goal, you need to complete following tasks:

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

## Lab Exercise 17: SECURITY



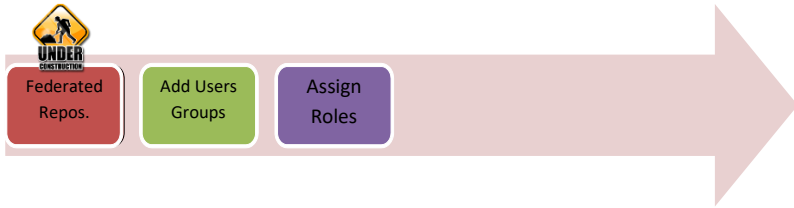
- 1. Configure federated user repository**
- 2. Add new users and groups**
- 3. Assign users and groups to roles**



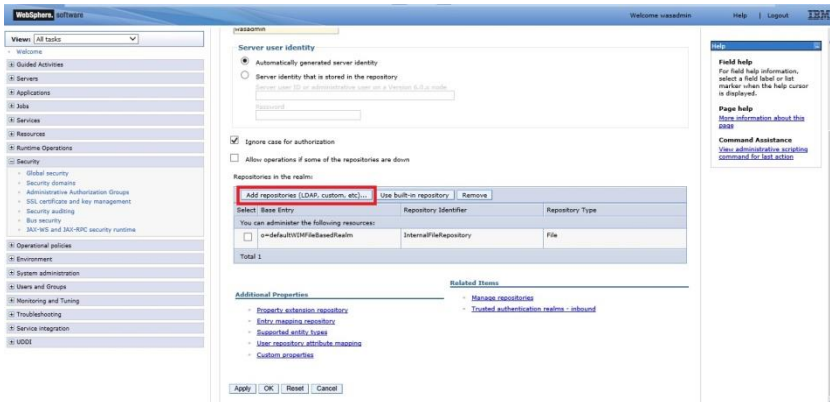
## Task 1: Configure federated user repository

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

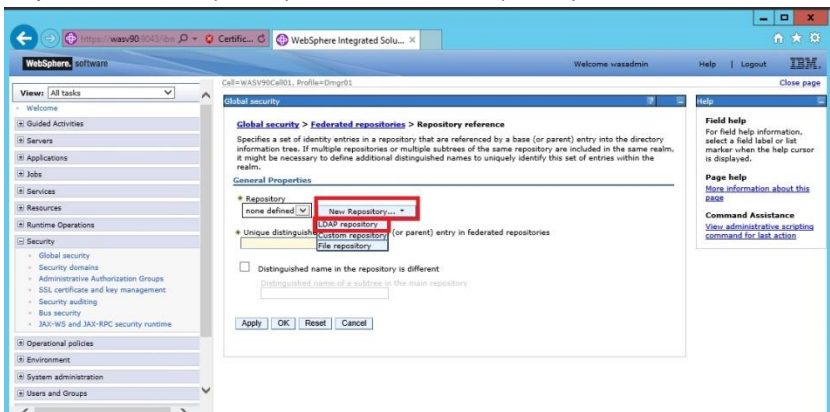
The screenshot shows the WebSphere Software Security Configuration page. The left sidebar contains a navigation tree with the following items: Overview, Guided Activities, Servers, Applications, Jobs, Services, Resources, Runtime Operations, Security (highlighted), Security domains, Administrative Authorization Groups, SSL certificates and key management, Security auditing, Bus security, JAX-WS and JAX-RPC security runtime, Operational policies, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and MBeans. The 'Security' item is highlighted, and its sub-items are visible: security domains, Administrative Authorization Groups, SSL certificates and key management, Security auditing, Bus security, JAX-WS and JAX-RPC security runtime, Operational policies, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and MBeans. The 'Global security' sub-item is also highlighted. The main content area shows the 'Global security' configuration page. The 'Available realm definitions' section is highlighted, showing 'Federated repositories' selected in the dropdown and the 'Configure' button highlighted. The 'Set as current' button is also visible.

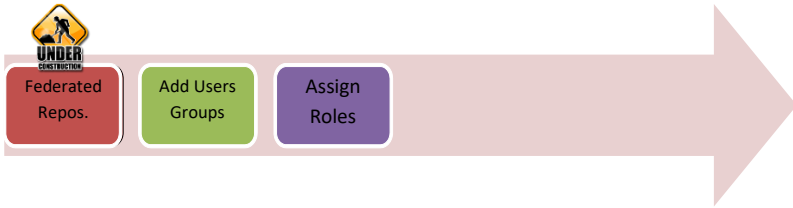


**Step 2:** Click on “Add repositories (LDAP, customer, etc)”.



**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.

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.us-east-1.amazonaws.com.adapter.LdapAdapter

**LDAP server**

Directory type: Custom

Primary host name: ldap01.us-east-1.amazonaws.com Port: 389

Fallover server used when primary is not available:

Default: Fallover host name Port

None

Add

Support referrals to other LDAP servers: ignore

Support for repository change tracking

**Security**

Bind distinguished name: cn=admin,dc=us-east-1,dc=com

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

Federated repository properties for login: OFF

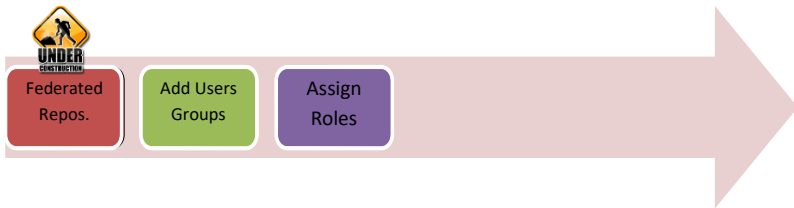
LDAP attribute for fallback principal name

Certificate mapping: EXACT\_OU

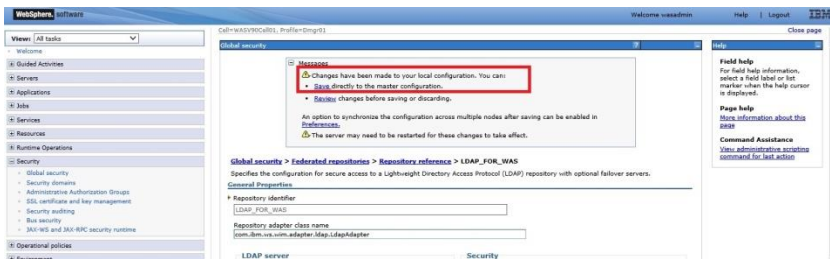
Certificate filter

Require SSL communications

Customly configured



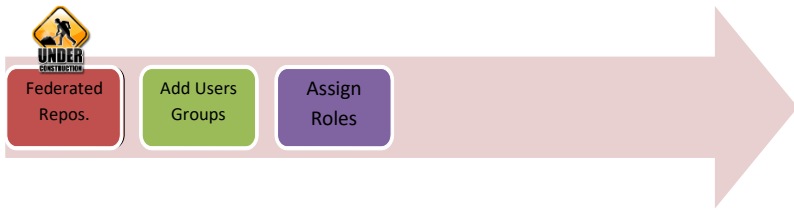
**Step 5:** Click “Save” to add new LDAP repository to the configuration.



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



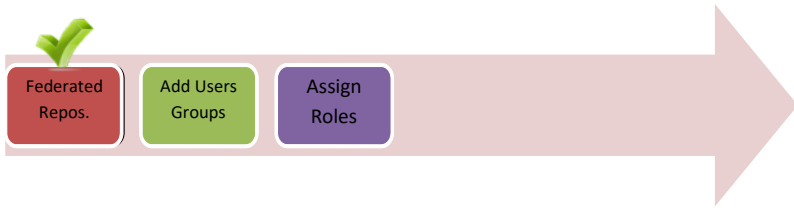




**Step 7:** Click “Save” to write changes to the master configuration file.

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

Select	Base Entry	Repository Identifier	Repository Type
<input type="checkbox"/>	ldap:realm:dc=com	LDAP_FOR_WAS	LDAP-CUSTOM
<input type="checkbox"/>	o=defaultIMRealm	InternalRepository	File



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

**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.

**Administrative security**

☒ Enable administrative security

- Administrative user roles
- Administrative audit rules
- 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:

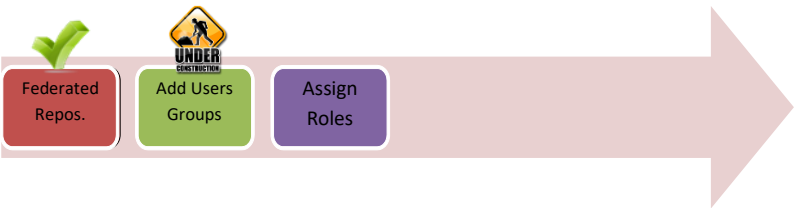
- ☒ Federated repositories
- ☐ Configure...
- ☐ Set as current

**Apply** **Reset**

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

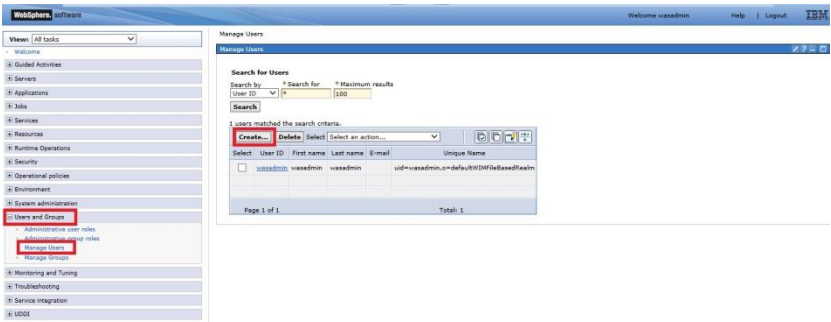
**Page help**  
Click information about this page

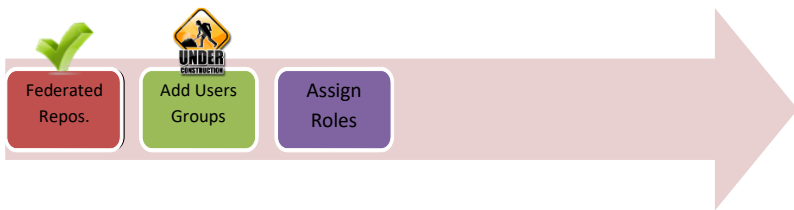
**Task 1 is complete!**



Task 2: Add new users and groups

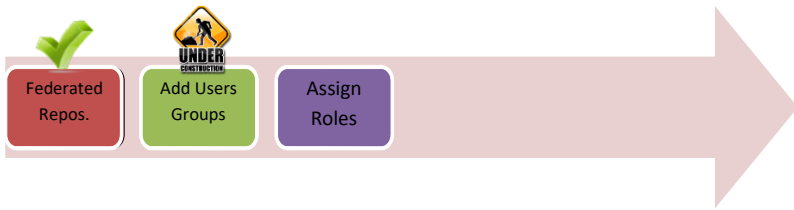
Step 1: Navigate “Users and Groups>Manage Users” and click “Create”.





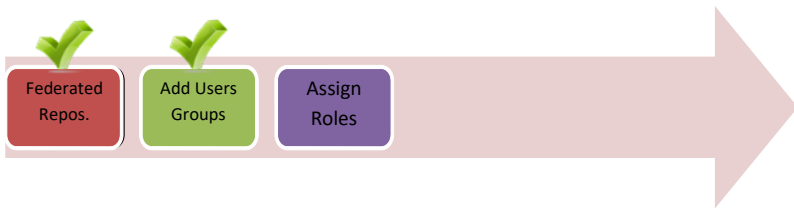
**Step 2:** Enter user information such as name, e-mail and password, then click “Create”.

**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”.

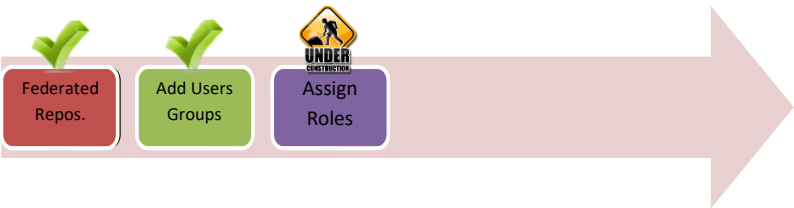
**Step 5:** Navigate to “Users and Groups>Manage Groups” and click “Create”.



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

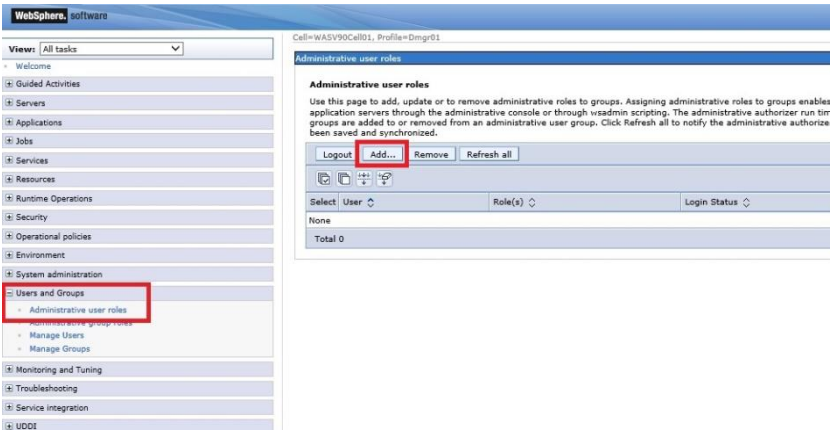
**Step 7:** You should get similar success message.

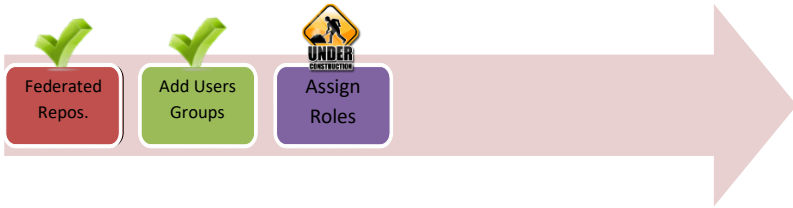
**Task 2 is complete!**



**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”.

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**

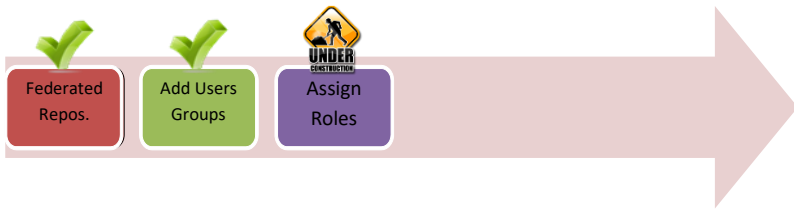
user2

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.  
• Changes have been made to your local configuration. You can:  
• [Save directly to the master configuration.](#)  
• [Revert](#) 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"/>	USBC1	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

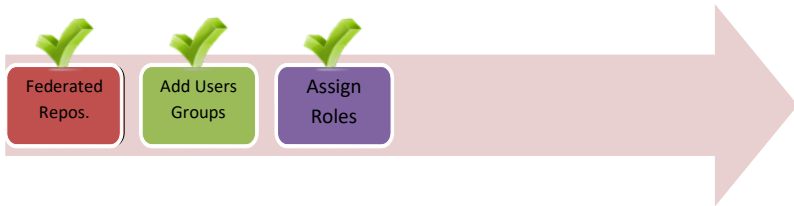
**Administrative group roles**

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