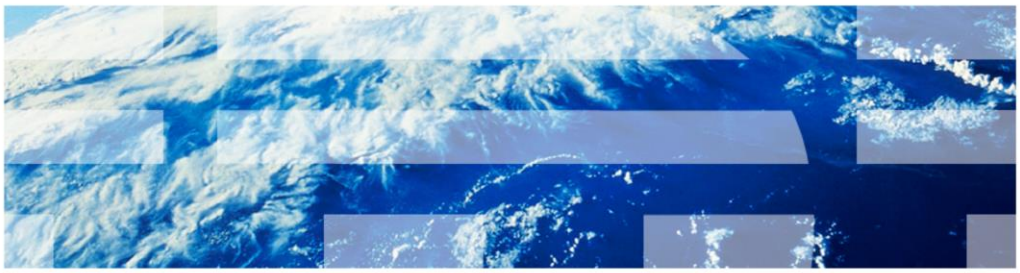
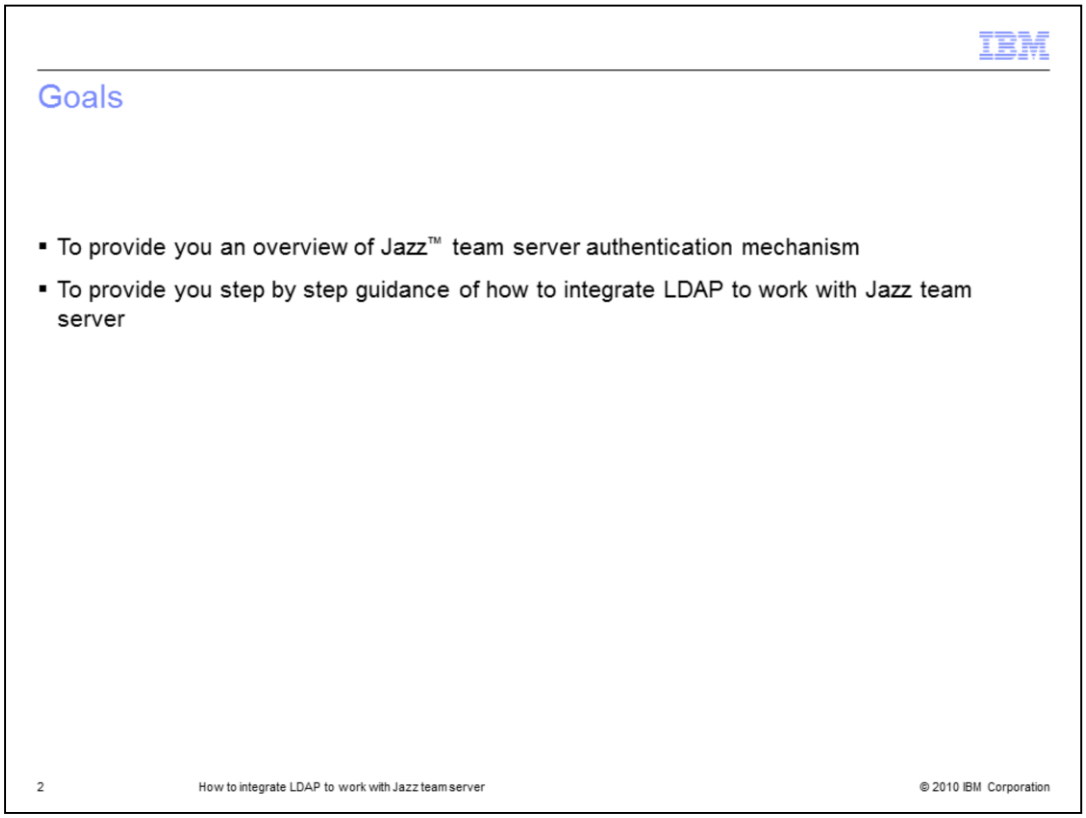
IBM Rational Team Concert

How to integrate LDAP to work with Jazz team server

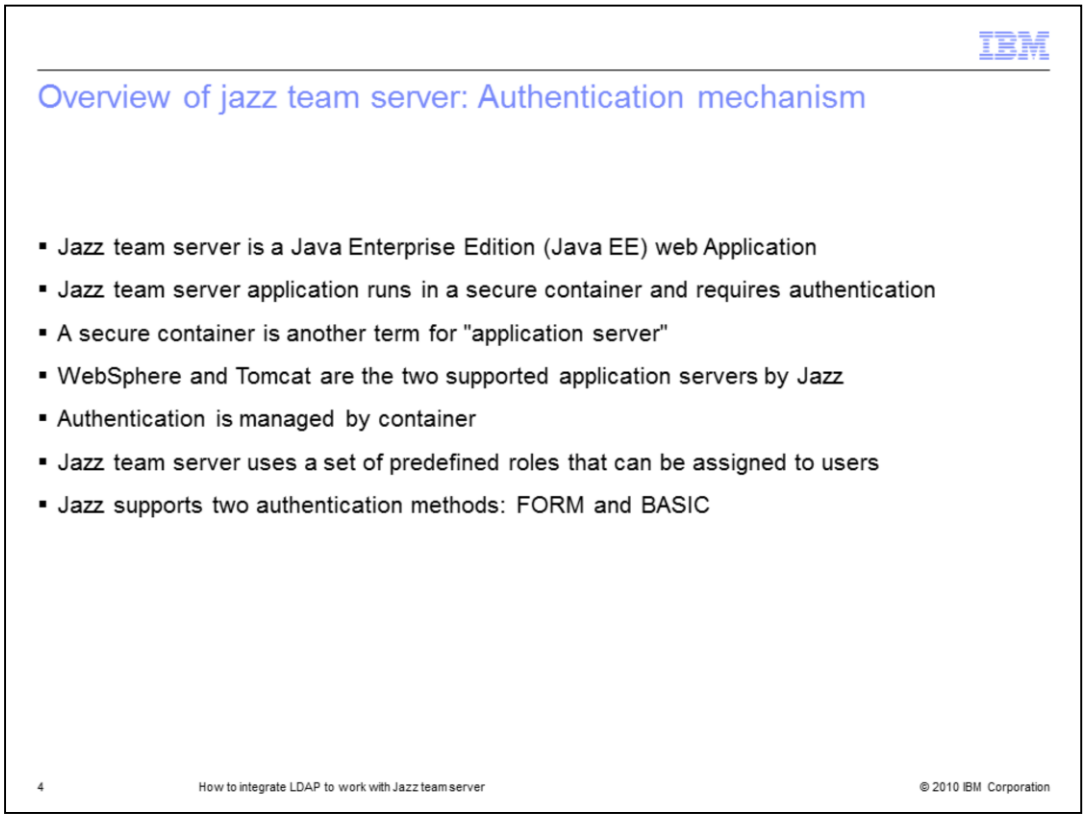


© 2010 IBM Corporation



Jazz team server that ships with Rational® Team Concert™ is packaged as a Java™ Enterprise Edition (Java EE) web Application, and as such runs within a supported Java EE application server (IBM WebSphere® Application Server or Apache Tomcat). The application uses Java EE authentication per the Java Servlet specification. The main goal of this module is to provide you step by step guidance of how to setup the LDAP configuration so that the Jazz team server can authenticate access by using the LDAP users credentials. In order to help you better understand the detailed LDAP configuration steps, you will be provided with an overview of the authentication mechanism that Jazz team server uses as well.

This slide covers the agenda. This module gives an overview of the Jazz team server authentication mechanism first, then it goes through the steps of configuring LDAP to work with the Jazz team server. It also includes four demonstrations that show you how to perform the LDAP configuration in detail.



The Jazz team server application runs in a secure container and requires authentication. The application also uses a set of predefined roles that can be assigned to users, for authorization to access specific URLs or to perform specific low-level operations (for example, read, write, administer). The "container" is another term for "application server", for example, WebSphere or Tomcat. The authentication itself is managed by the container.

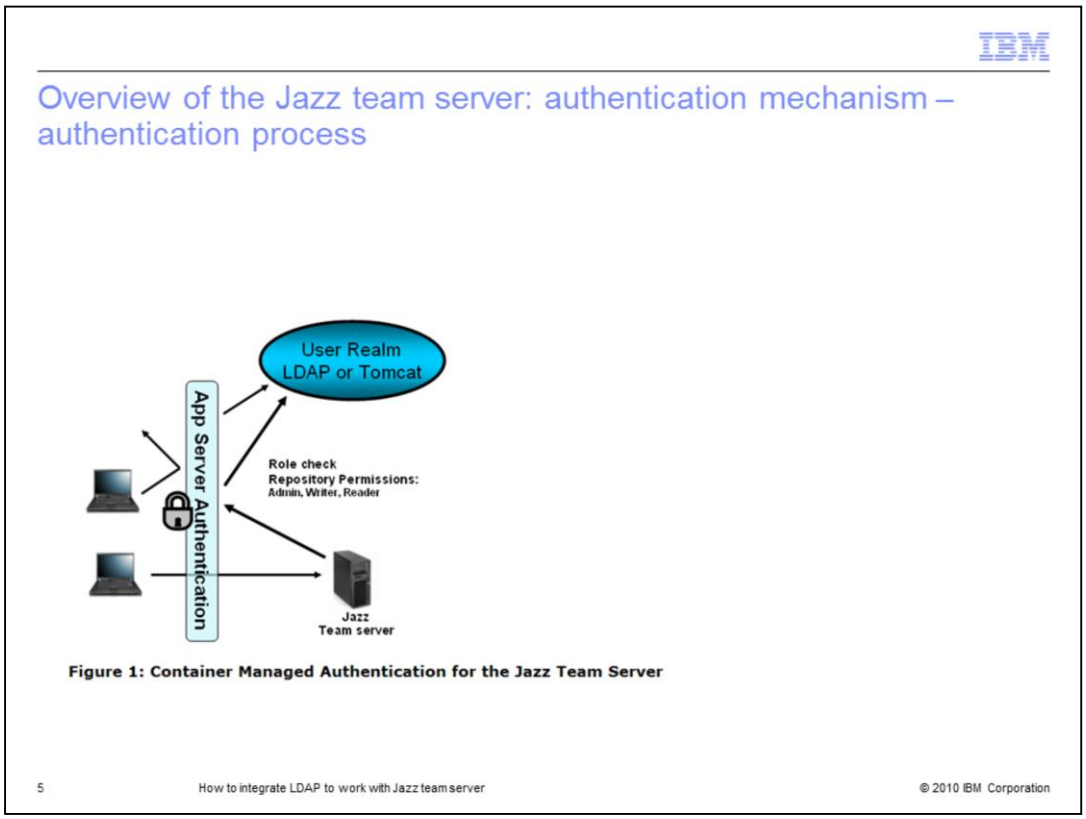
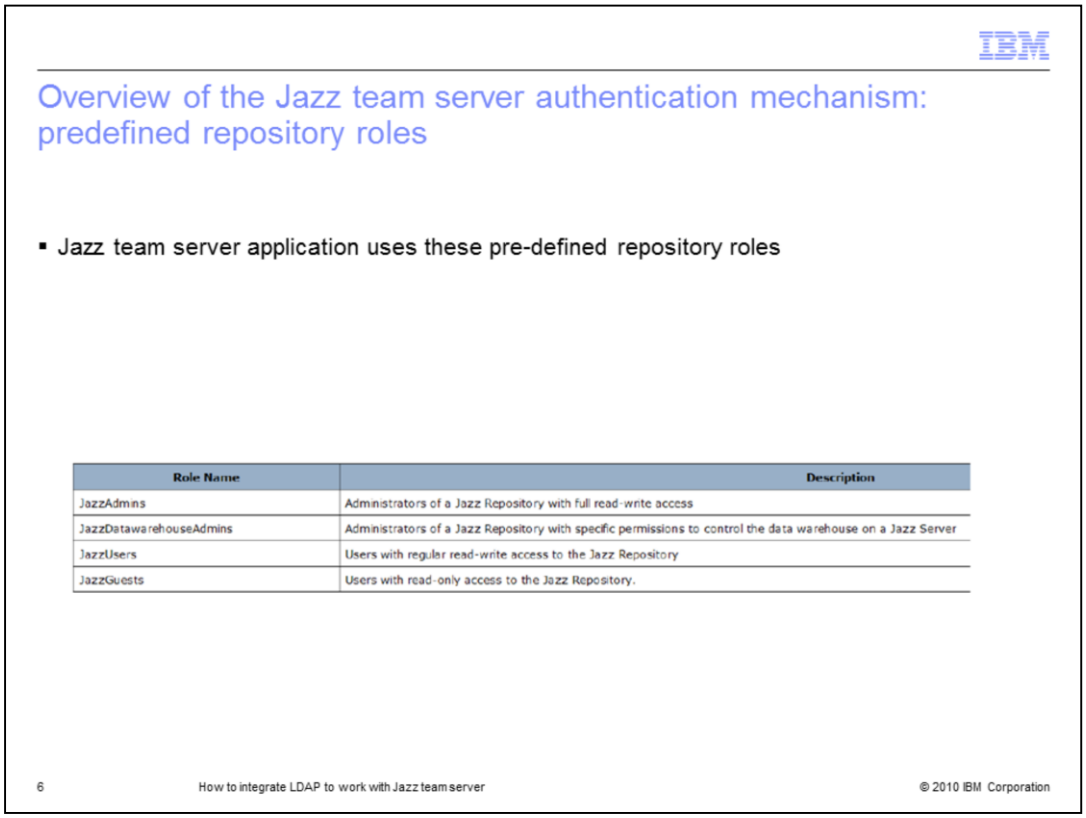
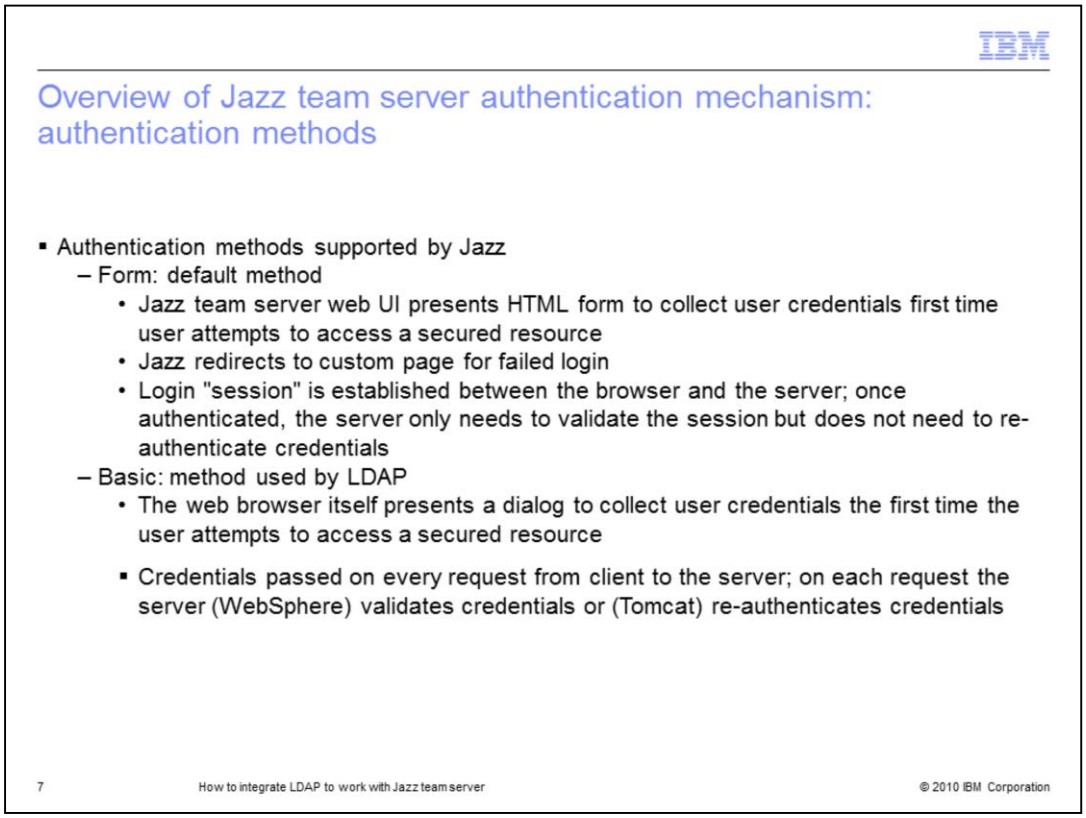


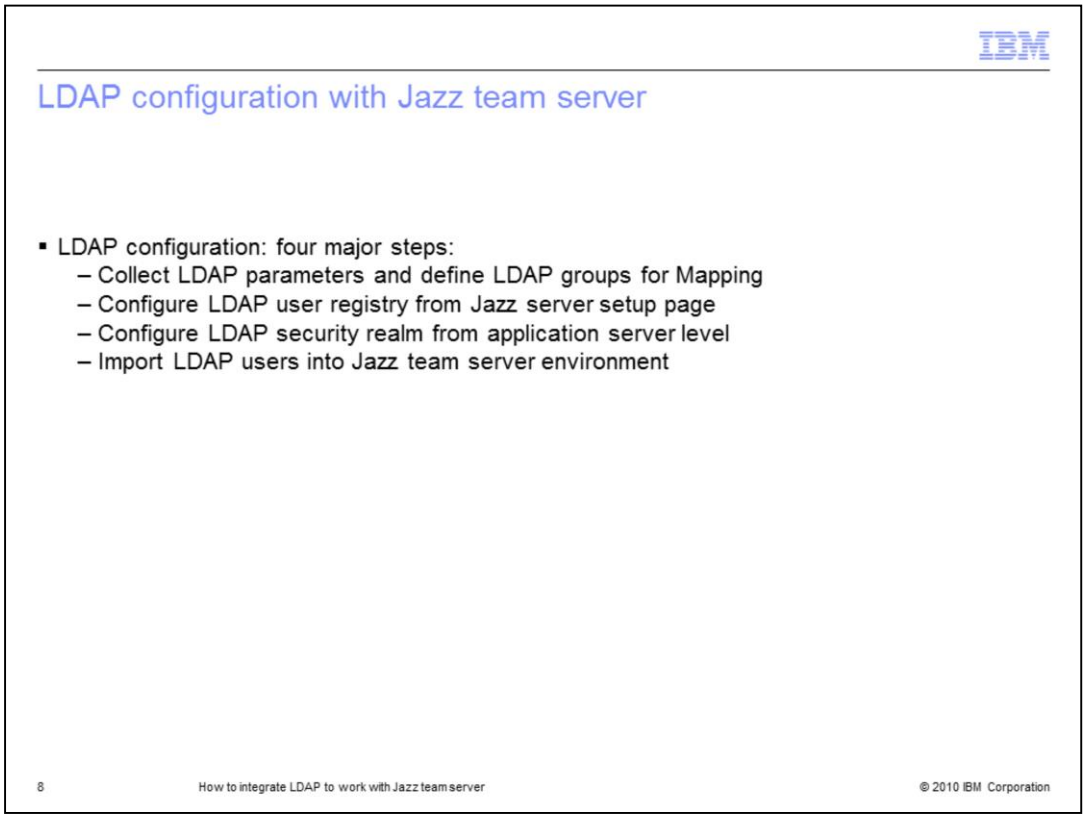
Figure 1 in this slide shows how authentication for the Jazz team server is managed within a container also known as Application server. If a user fails to authenticate by providing a valid user ID and password, then the container rejects the request without the request ever reaching the Jazz team server application. When you successfully authenticates, the container subsequently forwards the request to the application (the Jazz team server in this case) for processing. Within the operation that processes the request, the application checks that the user is assigned a role with requisite authority to perform the operation.



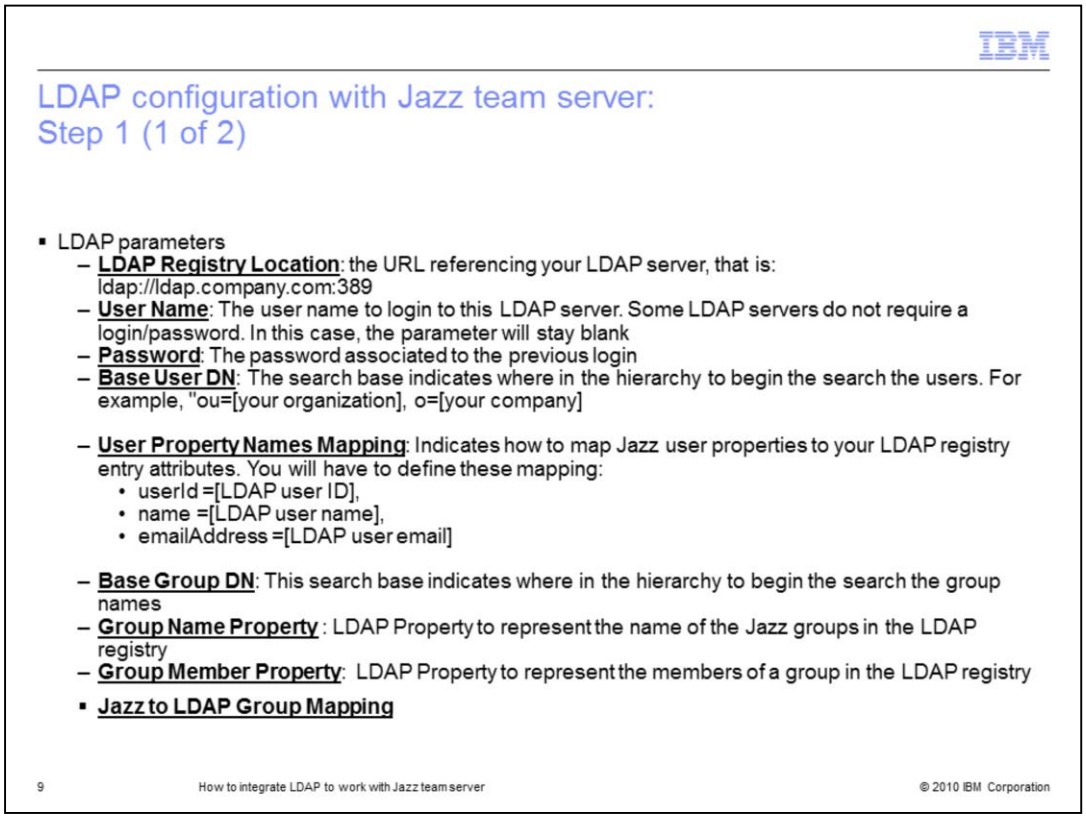
As mentioned in the previous slide, the Jazz team server application uses a set of predefined roles that can be assigned to users. Within the authentication operation, the application checks that the user is assigned one of the roles with requisite authority to perform the requested operation. This slide lists the four predefined roles with the Jazz team server application and their corresponding access type.



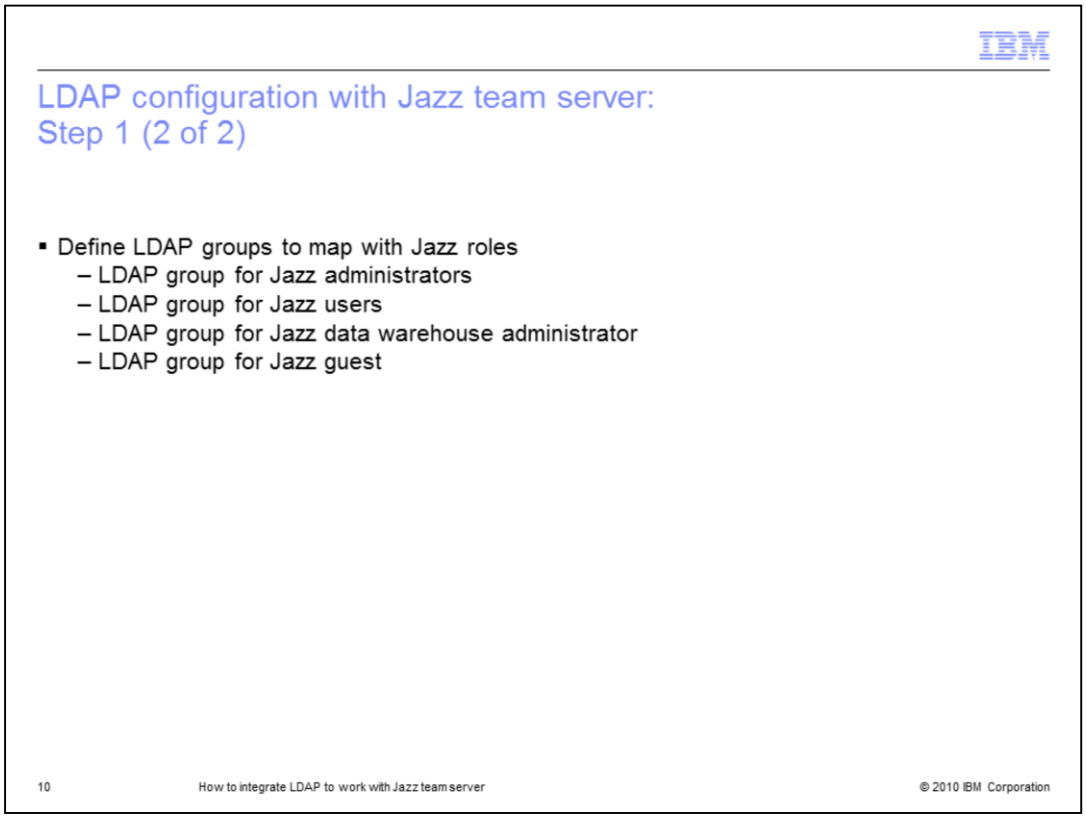
This slide introduces the two authentication methods supported by the Jazz team server application. FORM based authentication is the default method pre-configured in the Jazz Team Sever. LDAP uses the basic authentication method. Therefore, there is a list of configuration tasks you need to perform to setup LDAP to work with the Jazz team server, which will be discussed in the rest of the slides.



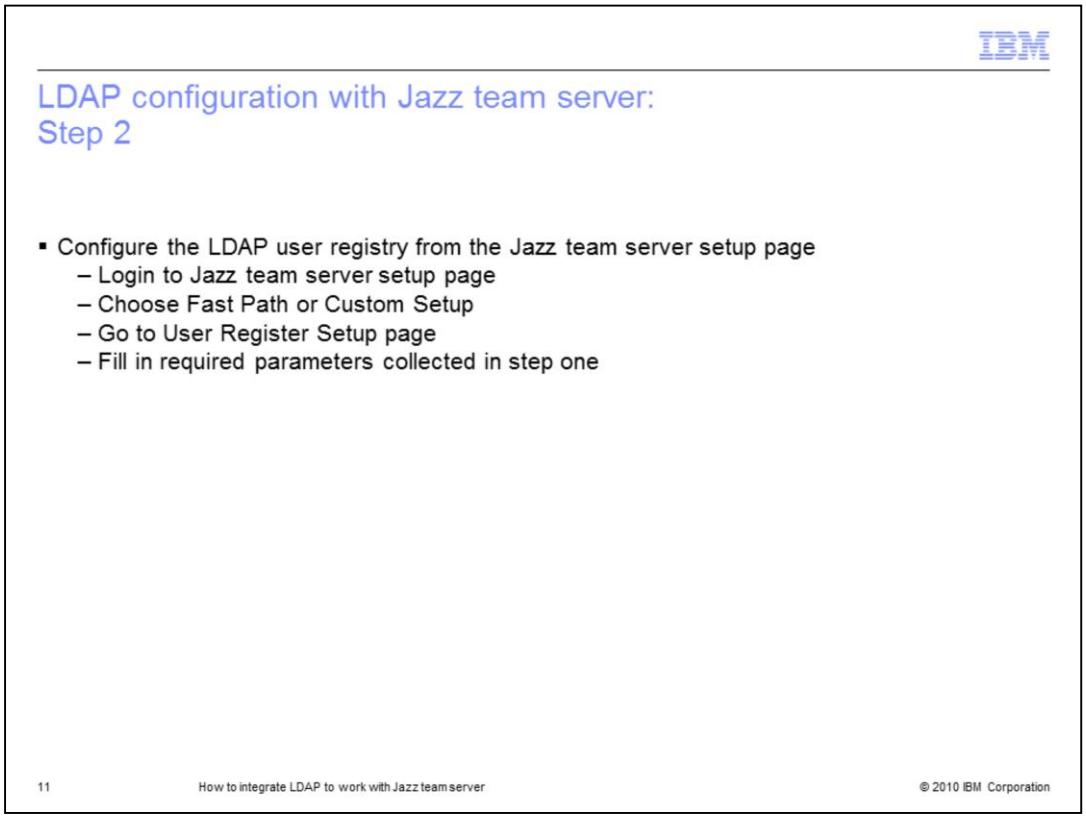
The Jazz server uses Java EE container managed authentication for login and system permissions. In order for application security to work, you must configure a realm with the application server where the Jazz server runs on. While file based realm is generally OK for testing, the LDAP realm is recommended for production deployment. A Realm is a "database" of usernames and passwords that identify valid users of a web application (or set of web applications), plus an enumeration of the list of roles associated with each valid user. In the next set of slides, the four major steps to configure LDAP to work with the Jazz team server are covered.



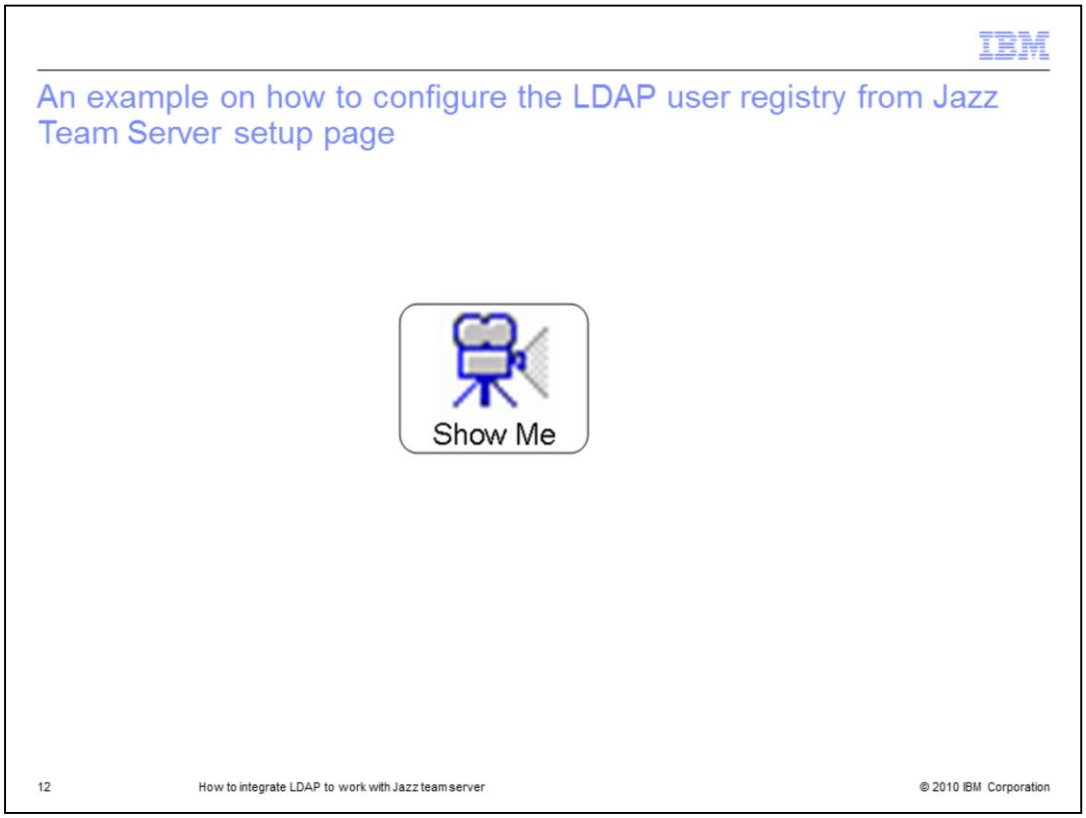
This slide covers step one which is collecting the LDAP parameters to prepare for the LDAP configurations. The list of parameters you need to collect are LDAP Registry Location, User Name, Password, Base User DN, User Property Names Mapping, Base Group DN, Group Name Property, Group Member Property and Jazz to LDAP Group Mapping. You will most likely collect these parameters from your LDAP server administrator.



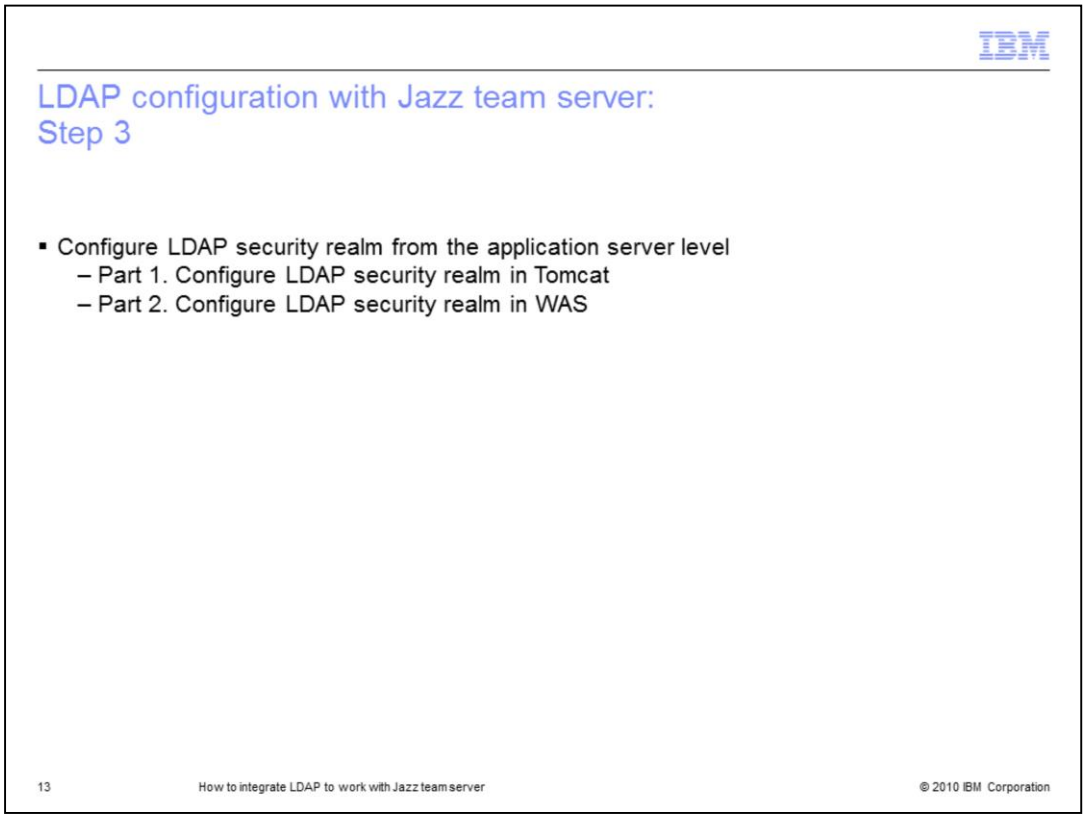
As mentioned in the previous slides, the Jazz team server application uses a set of predefined roles that can be assigned to users within the authentication operation. As part of step one of the LDAP configuration, you need to collect four LDAP groups to map with this set of predefined Jazz roles. The four LDAP Groups are Jazz admins, Jazz users, Jazz data warehouse administrator and Jazz guest. These LDAP groups need to be defined from your LDAP server level, most likely by your LDAP server administrator. One Jazz role can be mapped to multiple LDAP groups. The LDAP groups must be separated by a semi colon.



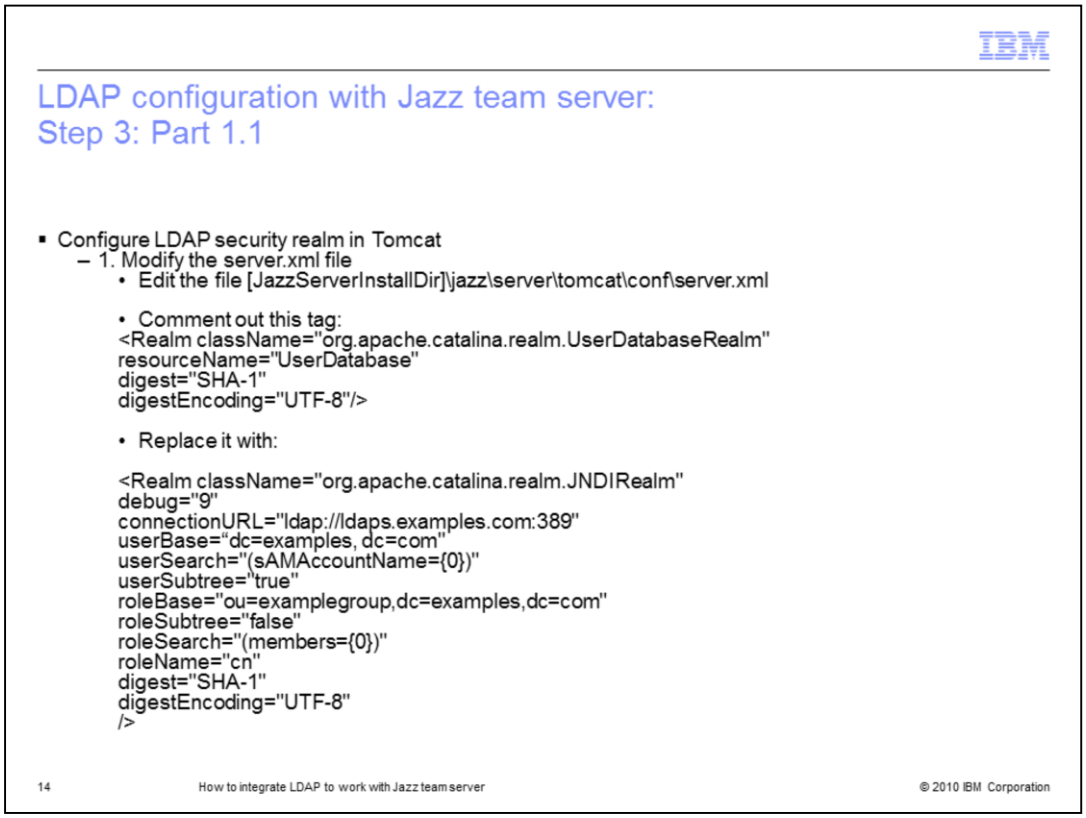
In step two, by using the information collected from step one, you need to configure the user registry to connect the Jazz team server with your LDAP registry. This slide concludes the major steps to complete the user registry configuration from your Jazz team server setup page. For details of how to perform the configuration, see demonstration module one on how to configure LDAP user registry from Jazz team server setup page. Refer to the demonstration in the next slide to see how to configure the LDAP user registry from the Jazz Team Server setup page.



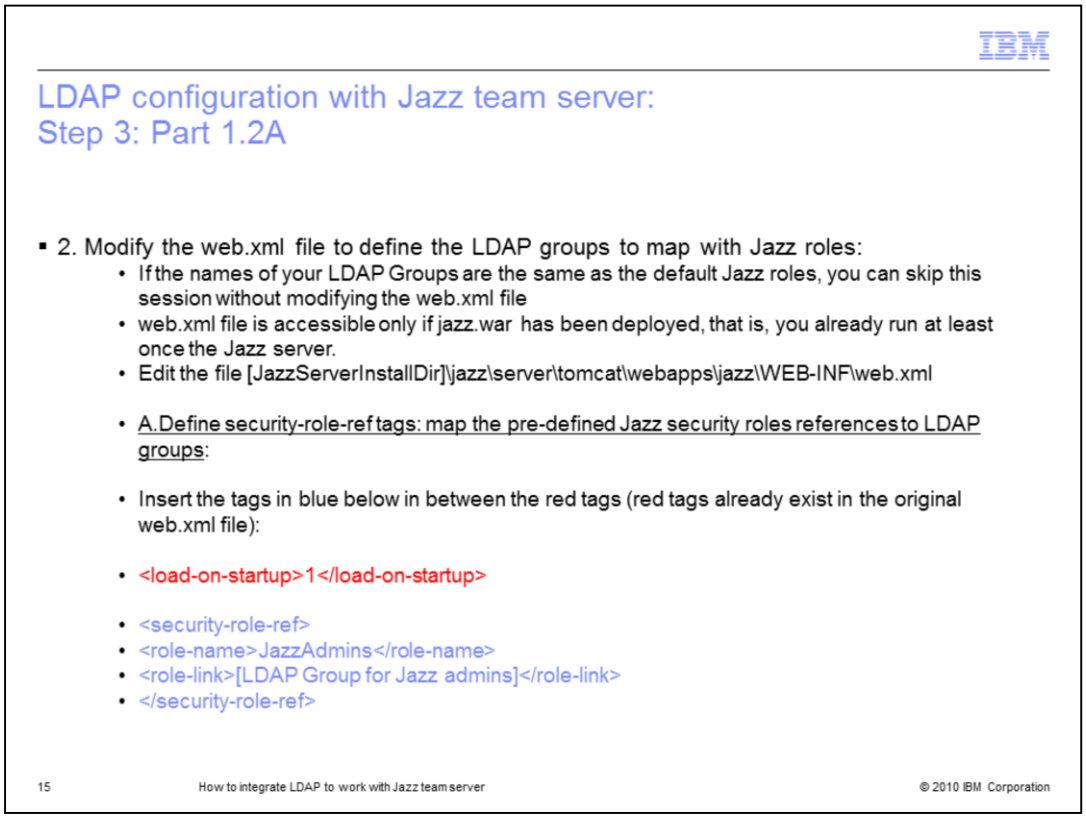
Here is an example on how to configure the LDAP user registry from the Jazz Team Server setup page. To watch a demonstration of this topic, pause this demonstration and click the “Show Me” Icon.



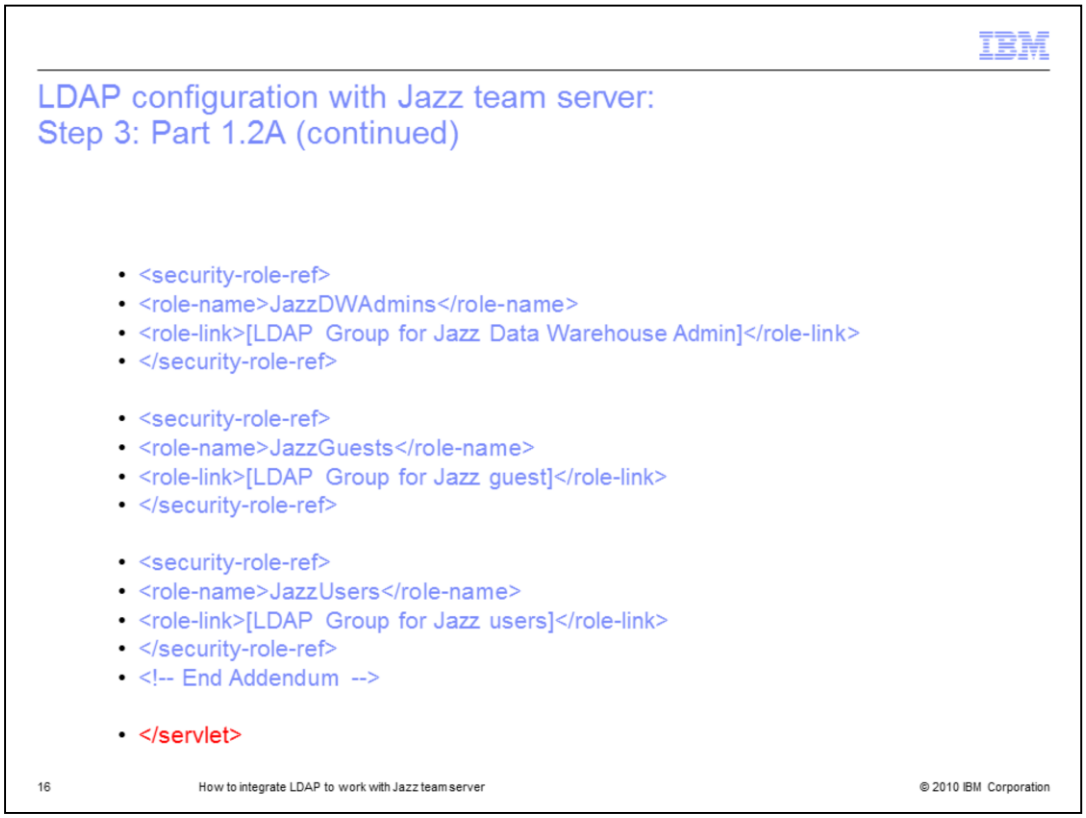
In step three, you need to setup security access from the Application server where the Jazz server runs on to enable connection between the Jazz server with the LDAP registry configured in Step 2. As mentioned earlier, the Jazz server runs within a supported Java EE application server including IBM WebSphere Application Server or Apache Tomcat. You will see the configuration steps in both of the application servers environment, based on a sample Microsoft® Active Directory built with a single forest and a single domain, with no organization unit. Therefore, steps three is divided into two parts. Part one shows you how to configure the LDAP security ream for the Jazz team server that runs in the Tomcat application server, while Part two shows the configuration steps using the IBM WebSphere Application Server.



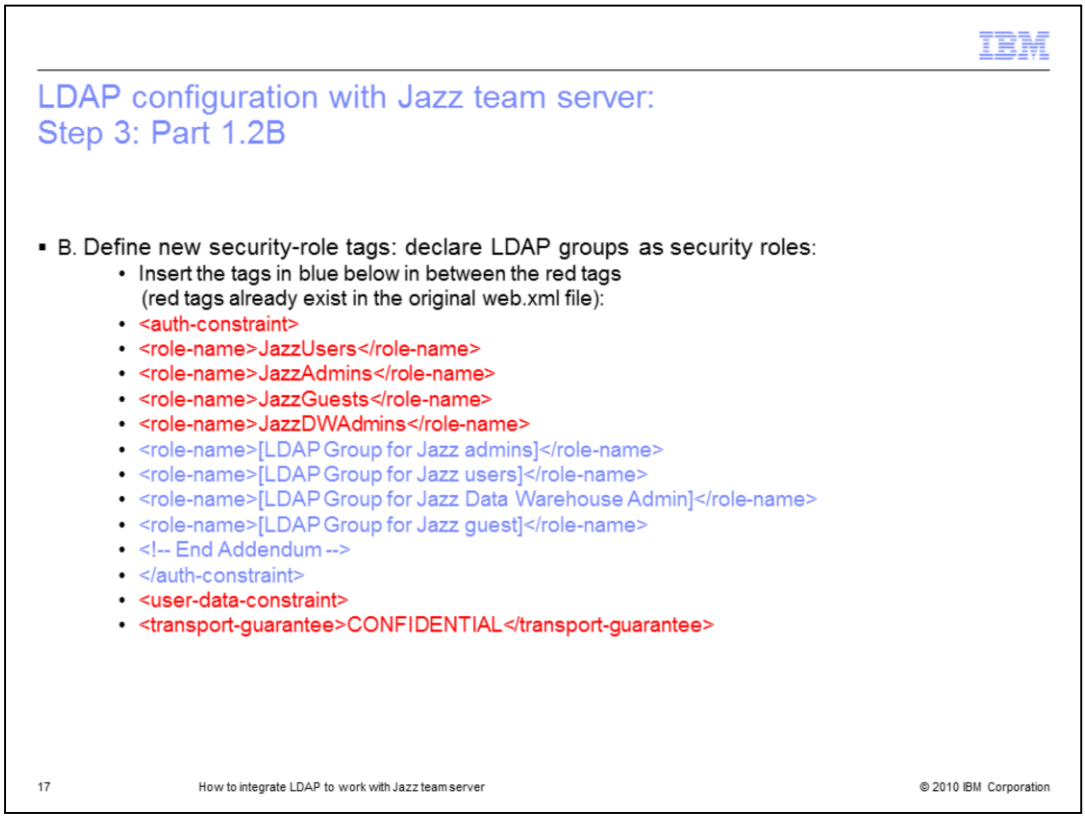
The following few slides show you what needs to be done to complete part one of step three on integrating LDAP security realm with the Jazz team server that runs in the Tomcat application server. In order to do so, you need to modify two files. The first one is server.xml under the tomcat directory shown above. This slide shows you what needs to be modified in the server.xml file.



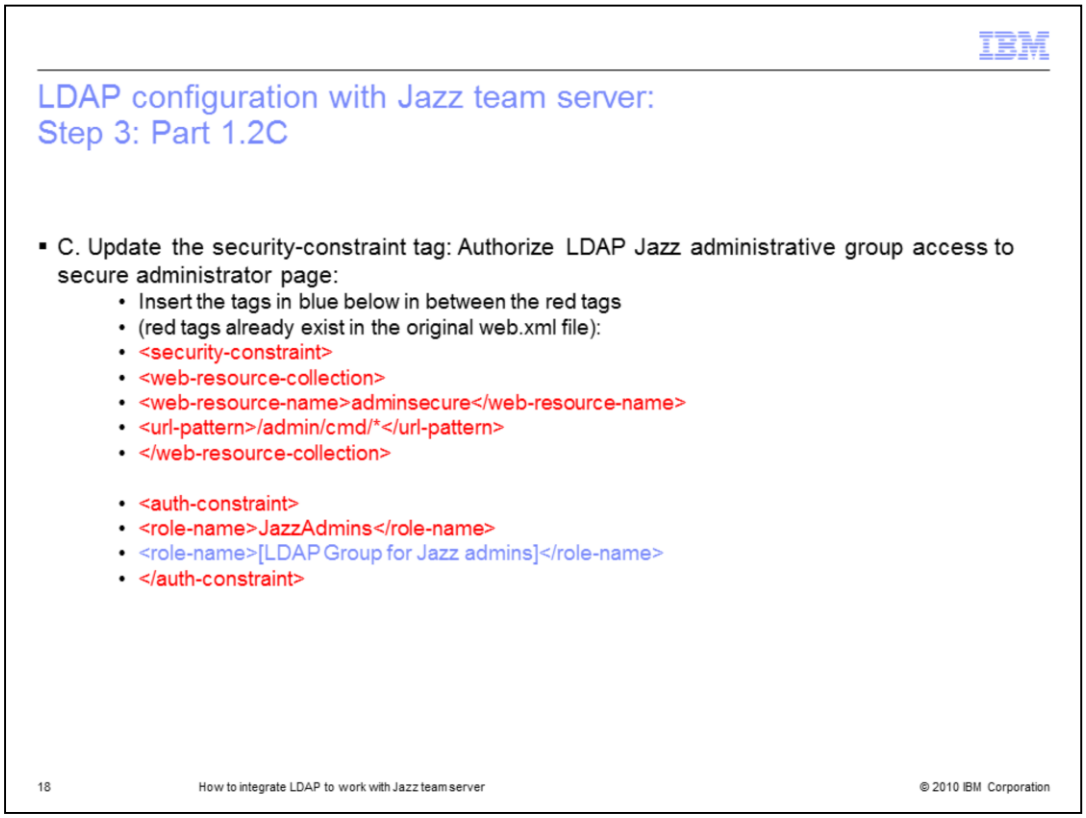
The second file you need to modify to configure the LDAP security realm for Jazz team server that runs in the Tomcat application server is the web.xml file located in the above file path. Note that if the names of your LDAP Groups are the same as the default Jazz roles, you can skip this session without modifying the web.xml file. And the web.xml file is accessible only if jazz.war has been deployed, that is, you already run at least once the Jazz server.



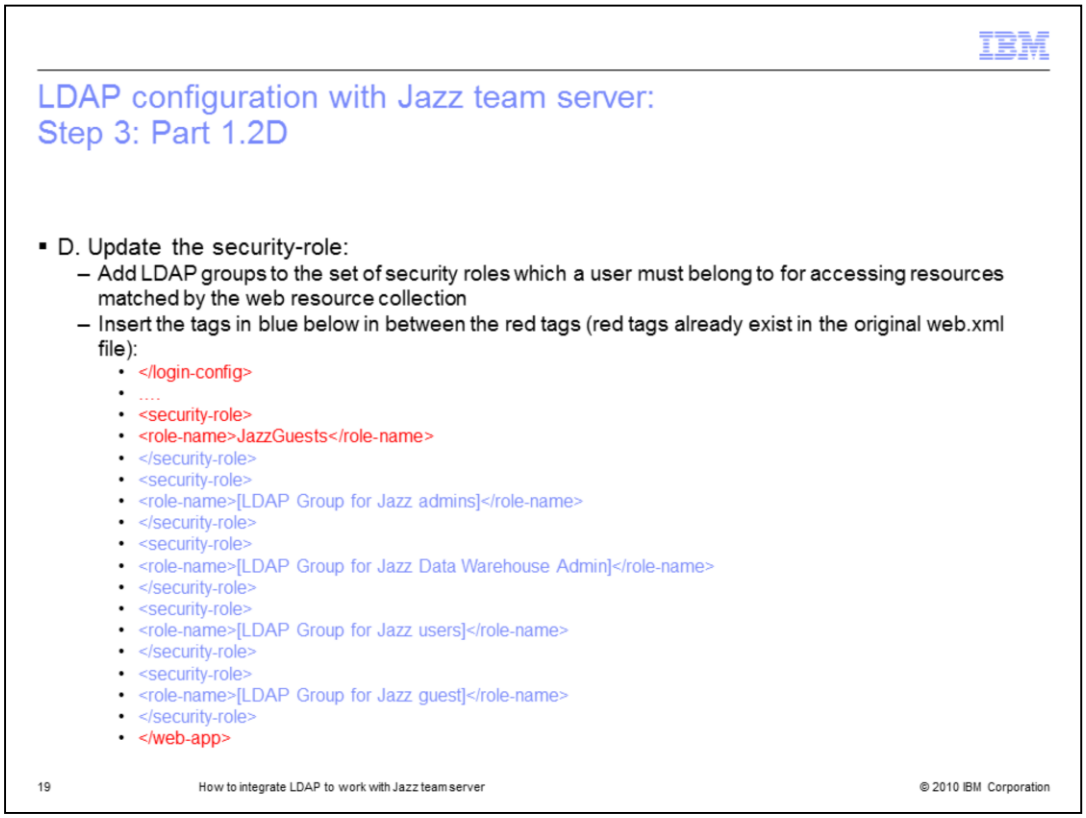
This slide continues to show you what needs to be modified to complete part A.



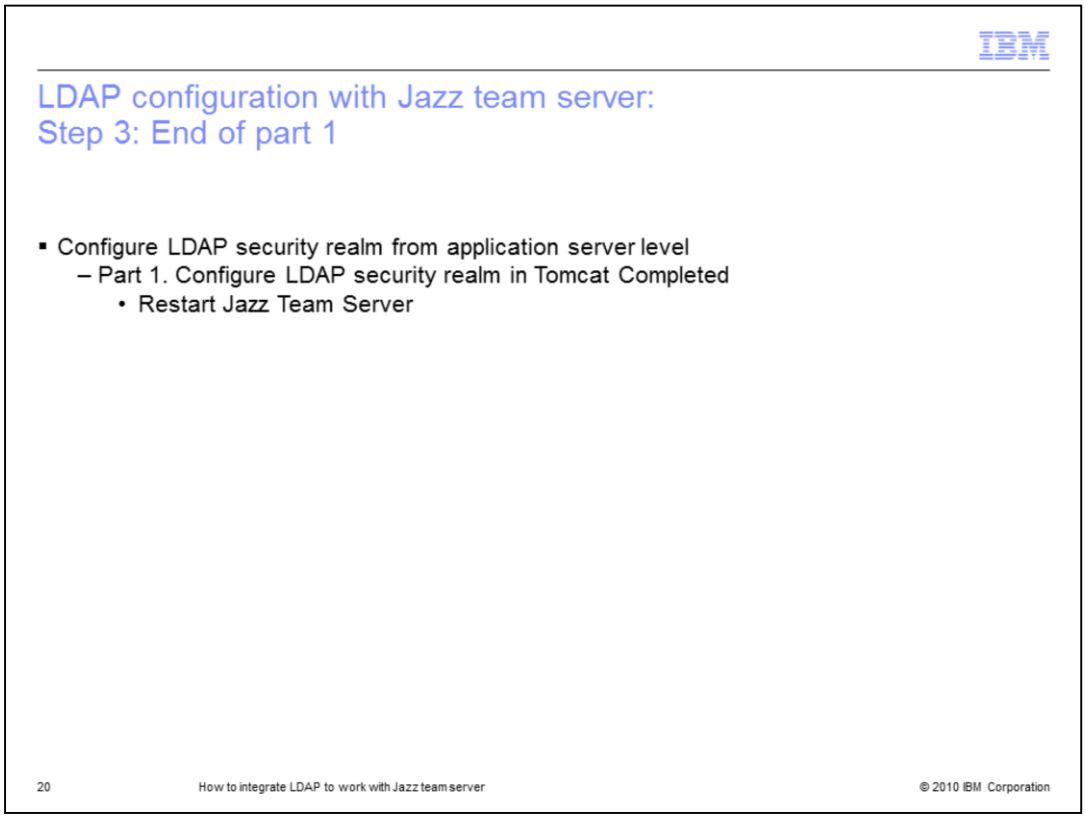
As mentioned earlier, there are four parts that need to be done to complete modifying the web.xml file. This slide shows you what needs to be modified to complete part B, which is to define new security-role tags. The purpose of doing so is to declare the LDAP groups as security roles.



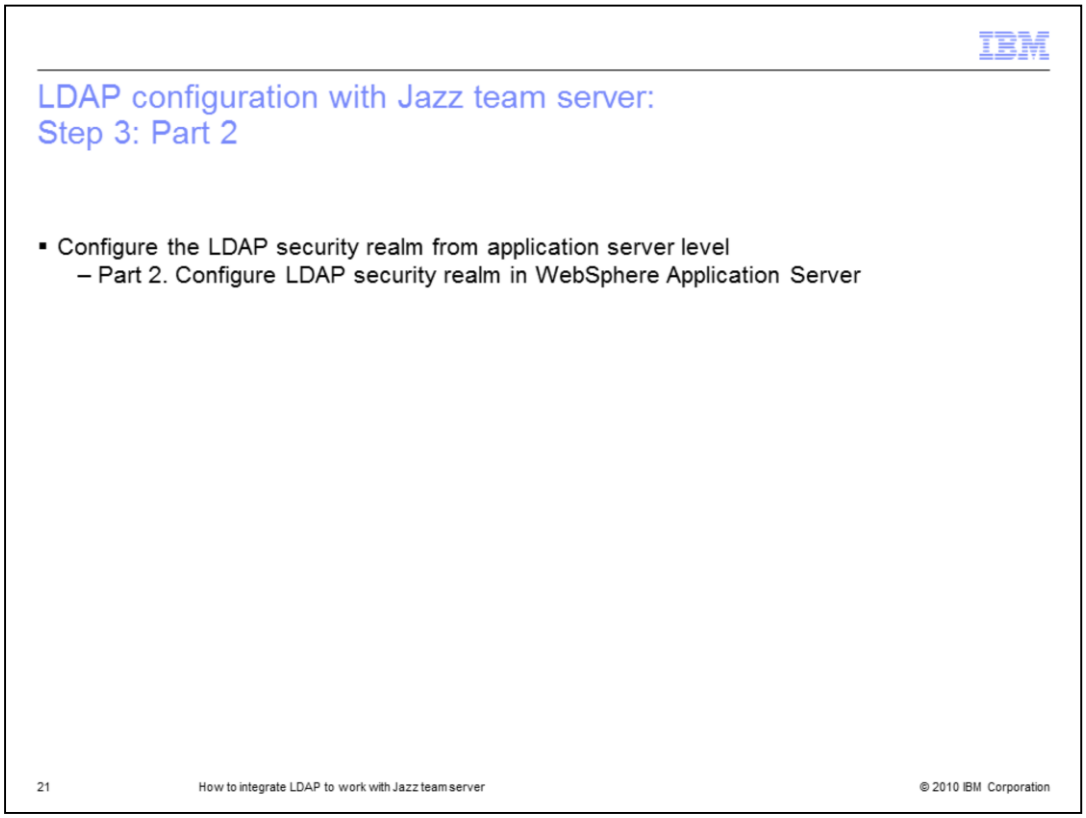
This slides shows you what needs to be modified in the web.xml file to complete part C, which is to update the security-constraint tag. The purpose of doing so is to authorize the LDAP Jazz administrator group access to the secure administrator page of your Jazz team server.



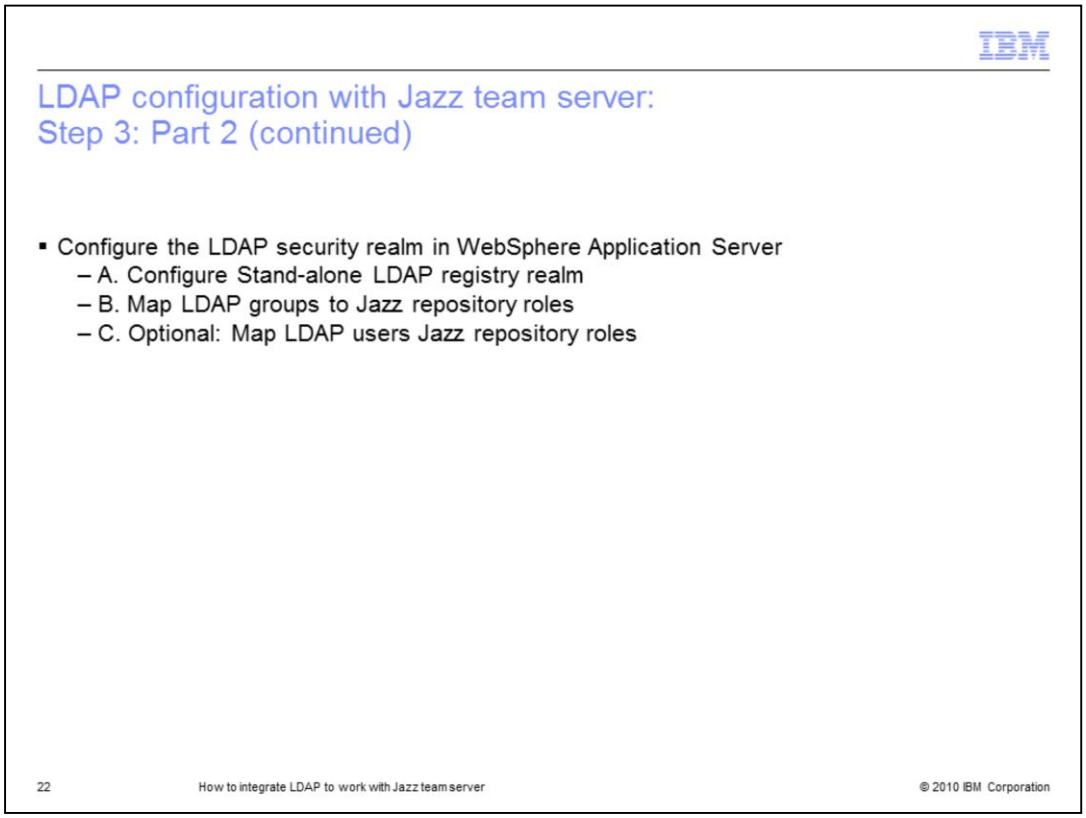
This slide shows you what needs to be modified in web.xml file to complete part four, which is to update the security-role. The purpose of doing so is to add the LDAP groups to the set of security roles which a user must belong to for accessing resources matched by the web resource collection.



This concludes part one on how to configure the LDAP security realm for the Jazz team server that runs in the Tomcat application server. You will need to restart your Jazz team server for all the changes you made to take effect. In the next section, you will see how to configure the LDAP security realm for the Jazz team server that runs in the IBM WebSphere Application Server. For audiences who are not interested in part two, you can move to step four to import LDAP users into the Jazz team server environment.



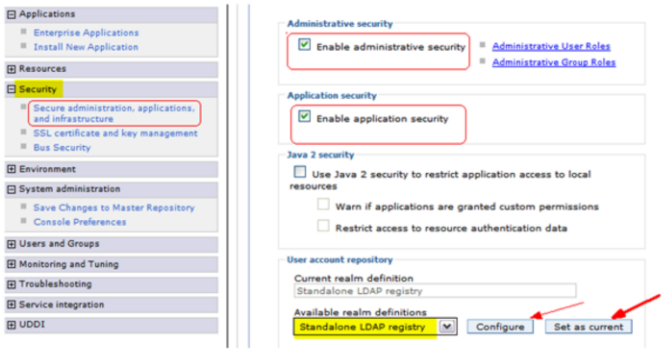
In the next few slides, you will see what needs to be done to configure the LDAP security realm that runs in the IBM WebSphere Application Server. It will include demonstration two to show you the detailed configuration steps based on a sample Windows® Active Directory LDAP server settings as well.



To configure the LDAP security realm for the Jazz team server that runs in the IBM WebSphere Application Server, you need to perform two major tasks from your WebSphere administrator Console, plus an optional one. You will see what needs to be done to complete these tasks in the next few slides.

LDAP configuration with Jazz team server: step 3: part 2.A

- A. Configure Stand-alone LDAP registry realm
  - From the WebSphere Application Server administrator Console, under secure administration, application and infrastructure page, ensure the administrative security and application security are enabled
  - From the same page, pick "Stand-alone LDAP registry" under available realm definitions box, click Set as current, then the Configure button



© 2010 IBM Corporation

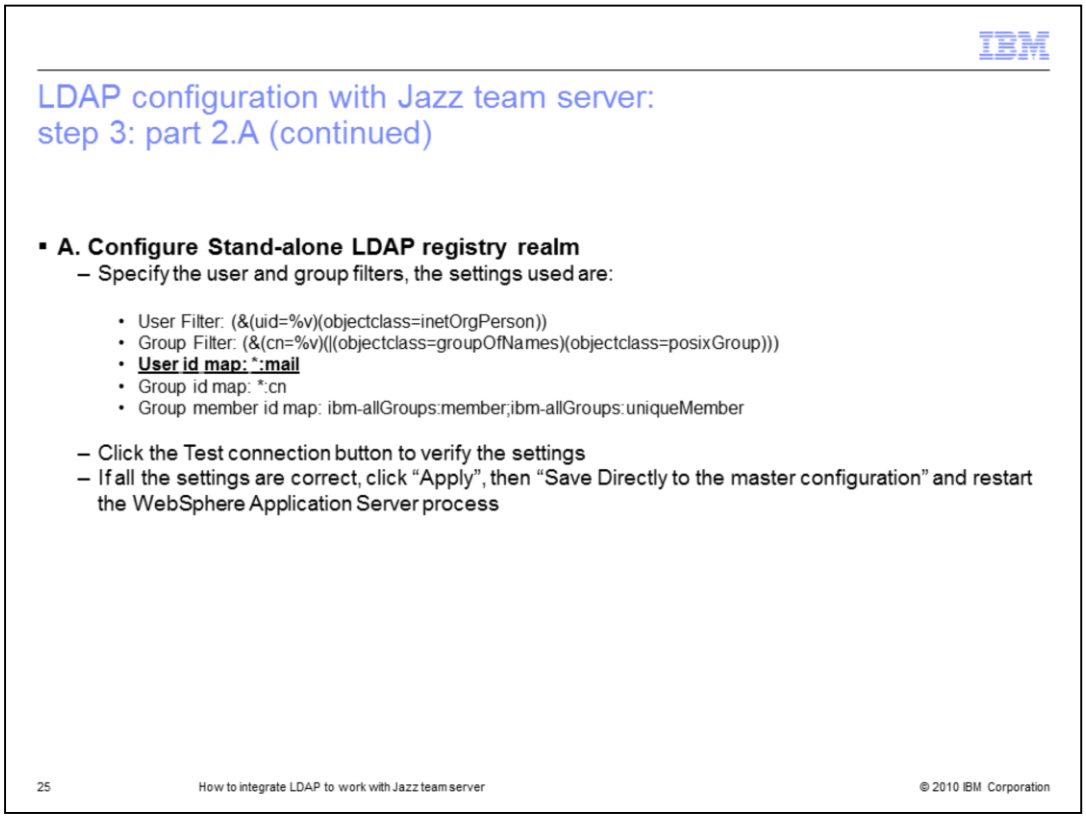
First, you need to configure the stand-alone LDAP registry realm. The next few slides show you what needs to be done to complete this task. Click the “set as current” button before going to the configuration page.

LDAP configuration with Jazz team server: step 3: part 2.A (continued)

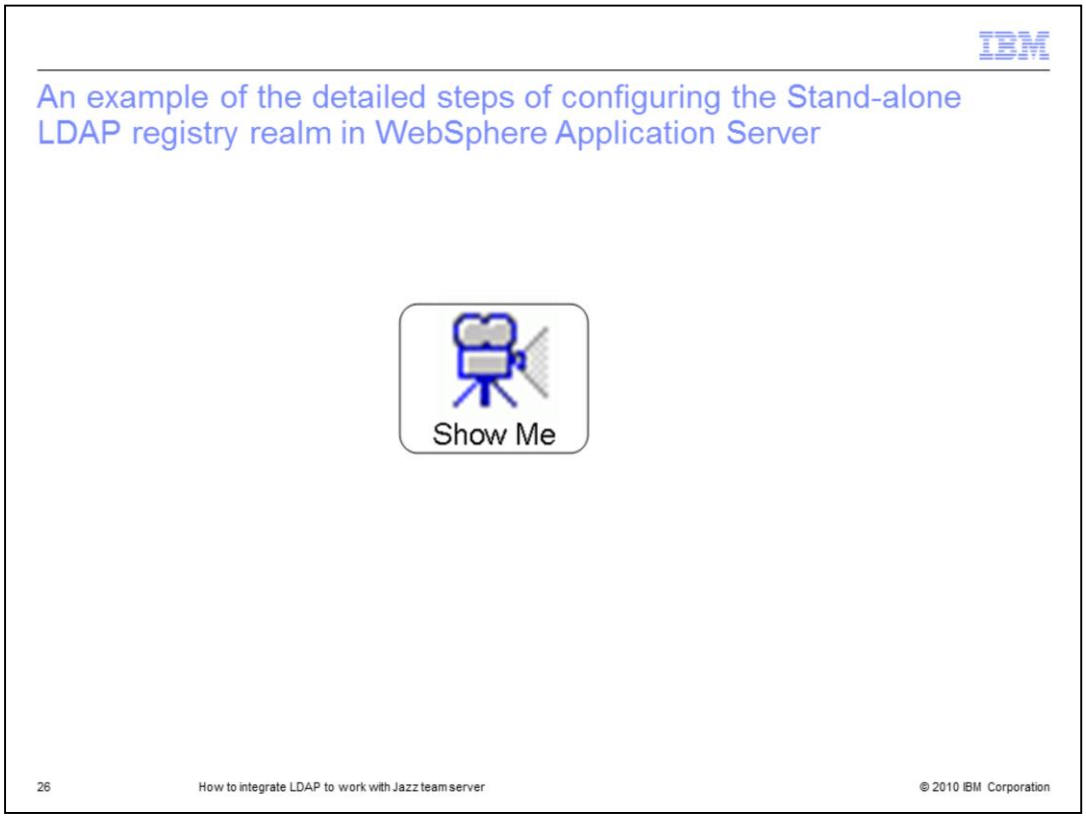
- A. Configure Stand-alone LDAP registry realm
  - Make sure these fields are set properly from the configuration page
    - Primary Administrative user name is set to the valid LDAP user, that is: **davesmith@examples.com**
    - Host is the correct LDAP host: **ldaps.examples.com** is used in this example
    - Port is the LDAP anonymous connection port. If SSL is enabled, the default port is 636, if SSL is not enabled, the default port is 389: **389** is used in this example
    - Base Distinguished Name (DN) is base user DN in the LDAP directory: **ou=examples.com** is used in this example
    - Select SSL enabled if the server requires SSL connection
  - Verify the LDAP server type, "**Custom**" is used in this example for the LDAP setting
  - Under Additional Properties, click advanced lightweight page

© 2010 IBM Corporation

From the configuration page, ensure the above underlined fields are filled in properly. Then go to the advanced LDAP user registry settings page.



From the advanced LDAP user registry setting page, these are just example settings that assumes that the uid is used to represent the user ID of a user in LDAP. cn is used to represent the name of a user in LDAP. The User ID map is important because this is the representation of the user that is passed to Jazz. This attribute must match the user ID that you created in the Jazz repository previously. Once the connection is established successfully, click "Apply" and save directly to the master configuration buttons. Restart your WebSphere Application server and log in with the administrator ID and password. Task A of configuring the LDAP realm for the Jazz team server in the WebSphere application server is now completed. Refer to the demonstration in the next slide to see an example of the detailed steps of configuring the stand-alone LDAP registry realm in WAS.



Here is an example of the detailed steps of configuring the Stand-alone LDAP registry realm in WebSphere Application Server. To watch a demonstration of this, pause this presentation and click the “Show Me” Icon.

LDAP configuration with Jazz team server
Step 3: Part 2.B

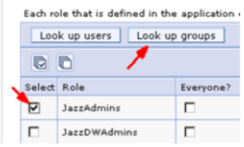
- **B. Map LDAP groups to Jazz Repository Roles**
  - From WebSphere Application Server administrator console, under Application, Enterprise Application, click jazz.war to open the Jazz team server application
  - From the application configuration page, click Security role to user/group mapping

© 2010 IBM Corporation

In this section you will see what needs to be done to complete task B which is to map LDAP groups to pre-defined Jazz repository roles. As mentioned earlier, there are four pre-defined Jazz roles within the Jazz team server to provide users/groups different types of access to resources in the application. These roles need to be mapped to your LDAP groups or users before they can get access to your Jazz team server environment. The next few slides show you how to map Jazz roles to LDAP groups.

LDAP configuration with Jazz team server
Step 3: Part 2.B (continued)

- **B. Map LDAP groups to Jazz Repository Roles**
  - From security role mapping page, select the jazz role you want to map LDAP group with
  - Click Look up groups button
  - Search for groups and move them to the selected list, click OK



Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
☐	JazzAdmins	☐	☐		cn=jazzadminswu,ou=memberlist,ou=ibmgroups,o=ibm.com
☐	JazzDWAdmins	☐	☐		cn=JazzDWAdminsSWU,ou=memberlist,ou=ibmgroups,o=ibm.com
☐	JazzUsers	☐	☐		cn=JazzUsersSWU,ou=memberlist,ou=ibmgroups,o=ibm.com
☐	JazzGuests	☐	☐		cn=JazzGuestsSWU,ou=memberlist,ou=ibmgroups,o=ibm.com

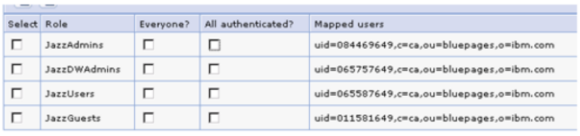
Figure 2: Jazz Roles with corresponding mapped LDAP roles

© 2010 IBM Corporation

After completing task B, you will see a screen similar to Figure 2, which shows an example of LDAP groups mapped to each pre-defined Jazz role. Members in these groups are now granted access to your Jazz team server with the type of access defined in jazz role the group is mapped to.

LDAP configuration with Jazz team server: Step 3: Part 2.C

- **Optional: Map LDAP users Jazz Repository Roles**
  - From security role mapping page, select the jazz role you want to map LDAP users with
  - Click Look up users button
  - Search for users and move them to the selected list, click OK

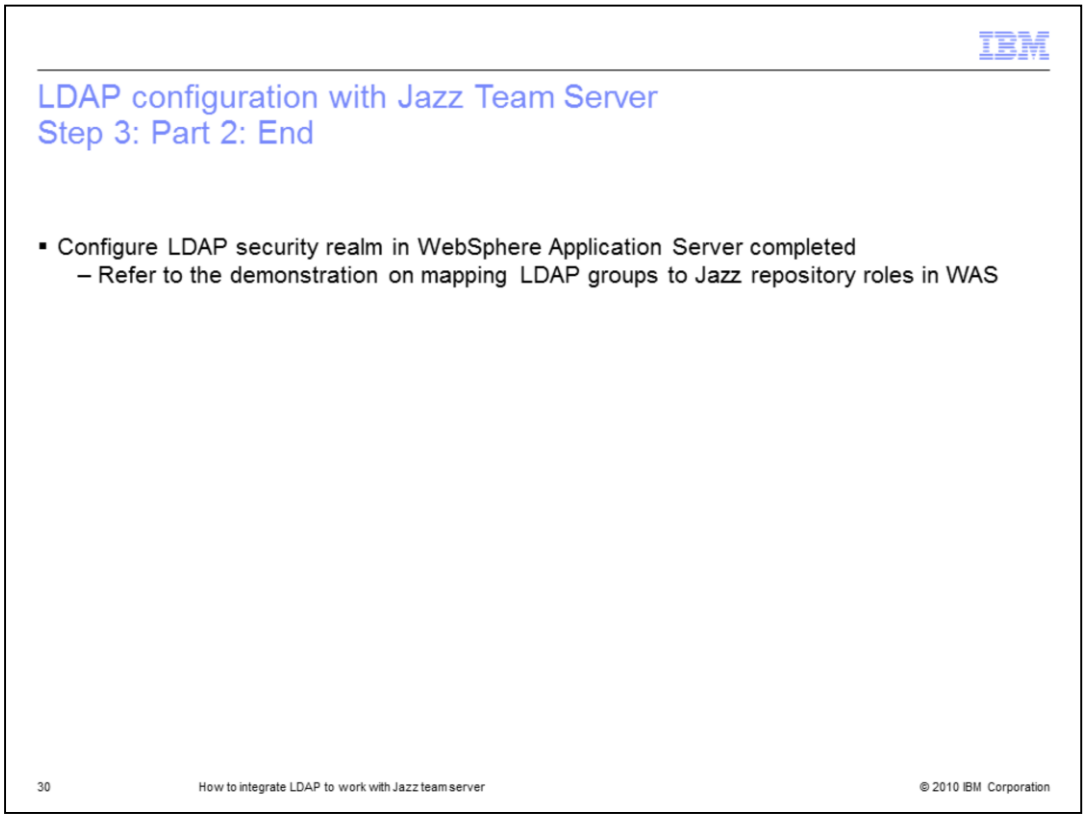


Select	Role	Everyone?	All authenticated?	Mapped users
☐	JazzAdmins	☐	☐	uid=084469649,c=ca,ou=bluepages,o=ibm.com
☐	JazzDWAdmins	☐	☐	uid=065757649,c=ca,ou=bluepages,o=ibm.com
☐	JazzUsers	☐	☐	uid=065587649,c=ca,ou=bluepages,o=ibm.com
☐	JazzGuests	☐	☐	uid=011581649,c=ca,ou=bluepages,o=ibm.com

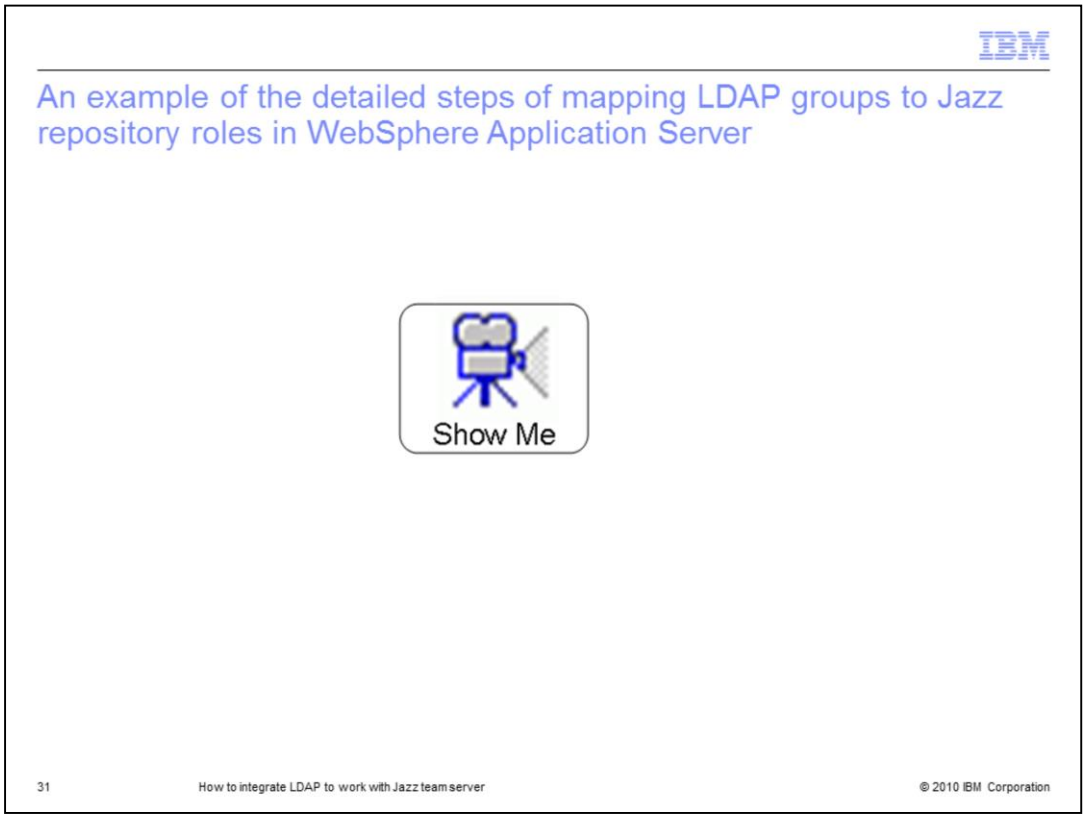
Figure 1: Jazz roles with corresponding mapped LDAP users

© 2010 IBM Corporation

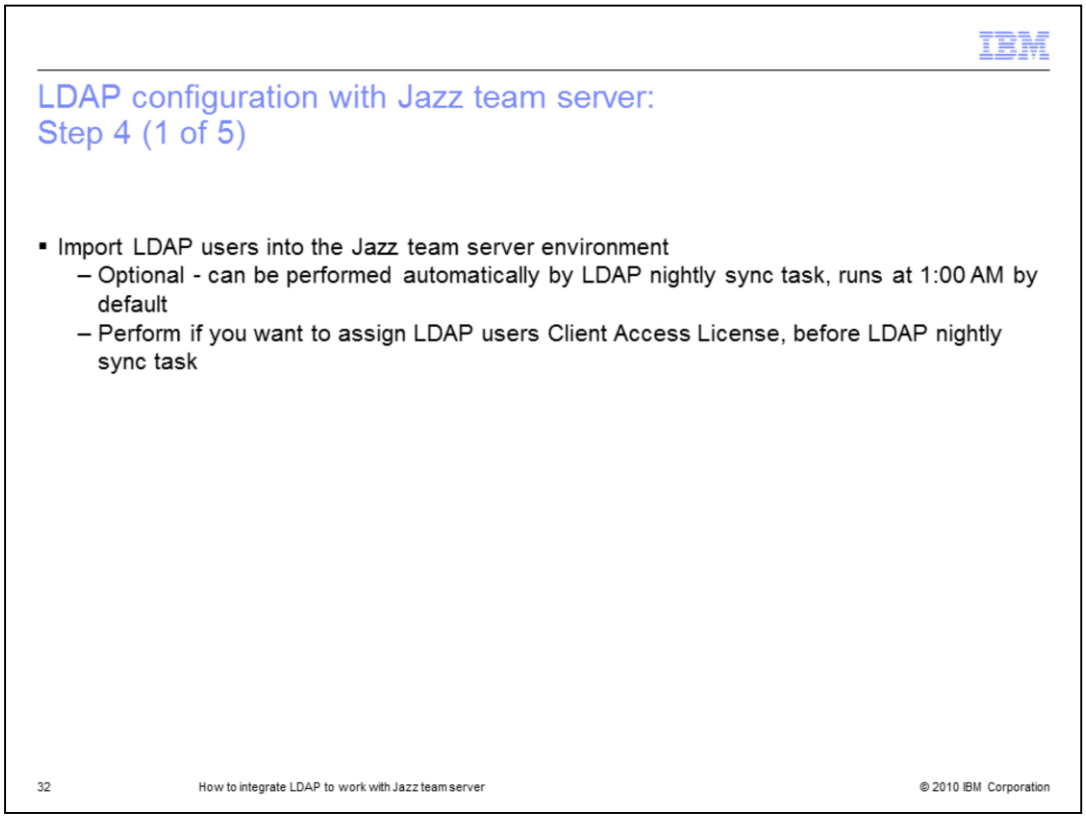
Instead of mapping LDAP groups, you can also map individual users to these pre-defined Jazz roles to provide them access to your Jazz team server. This slide shows you how to do so. After completing this task, you will see a screen similar to Figure 1, which shows an example of LDAP users mapped to each pre-defined Jazz role. These users are now granted access to your Jazz team server with the type of access defined in the jazz role they are mapped to.



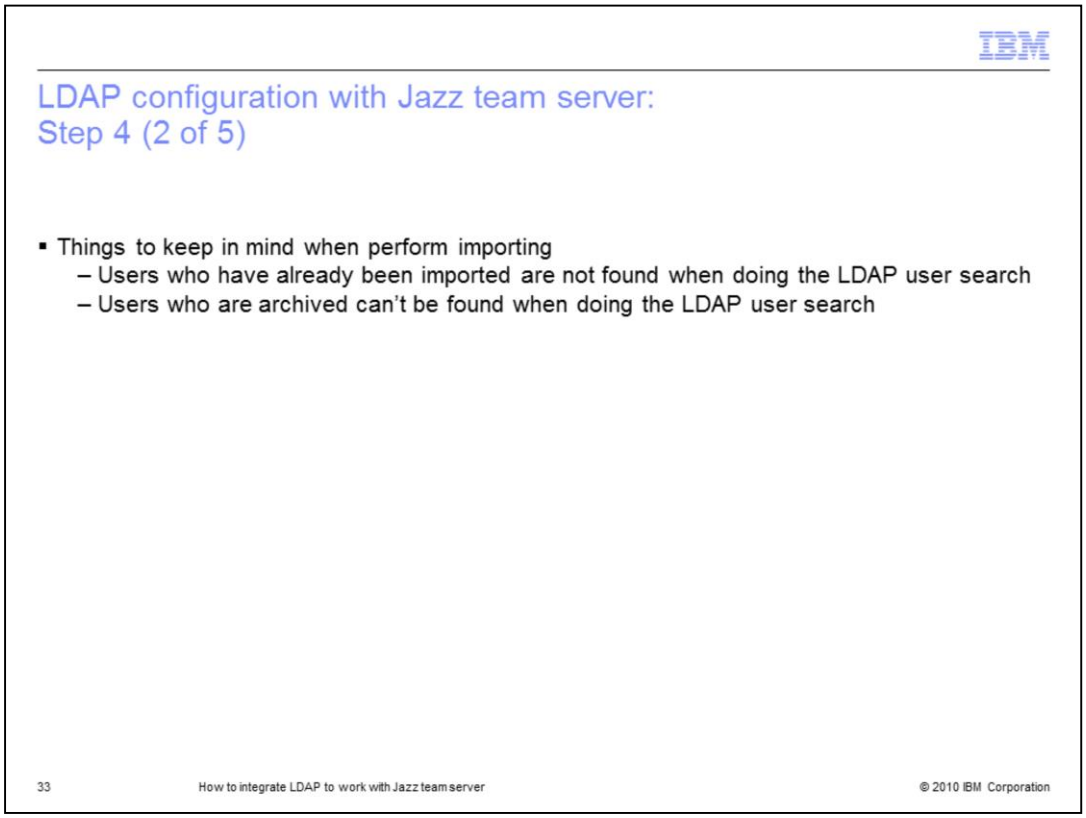
This concludes the configuration of the LDAP security realm in WebSphere Application Server. Refer to the demonstration in the next slide to see an example of the detailed steps of mapping LDAP groups to Jazz repository roles in WebSphere Application Server.



To watch a demonstration of this topic, pause this presentation and click the “Show Me” Icon.



The last step of LDAP configuration with the Jazz team server is to Import LDAP users into the Jazz team server environment. In the next few slides you will see how to import LDAP users into your Jazz team server environment manually. Note: this step can also be performed automatically by the LDAP nightly sync task which runs on your Jazz team server at 1:00 AM by default. The main reason you want to perform this step manually is because you want to assign LDAP users a client access license so they can perform their job with Rational Team Concert right away, before waiting for the LDAP nightly sync task runs.



Before you search LDAP users to import them, be aware of the two important points. First, users who have already been imported are not found when doing the LDAP user search. Second, users who are archived cannot be found when doing the LDAP user search. These are working as design features.

LDAP configuration with Jazz team server: Step 4 (3 of 5)

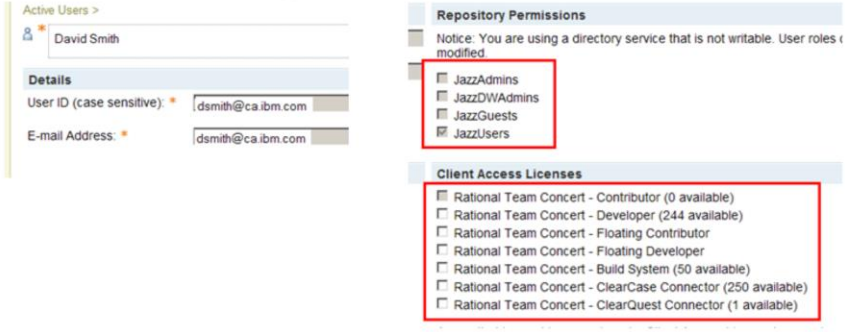
- **Import LDAP users into the Jazz team server environment**
  - Logon to your Jazz team server administrator page with administrator access
  - Under User Management, Active Users, click the “Import Users” button
  - Type in the User’s name, click Search
  - Select the user from the Matching Users list, click OK

© 2010 IBM Corporation

This slide shows you how to search for the LDAP user and then import it into your Jazz team server environment

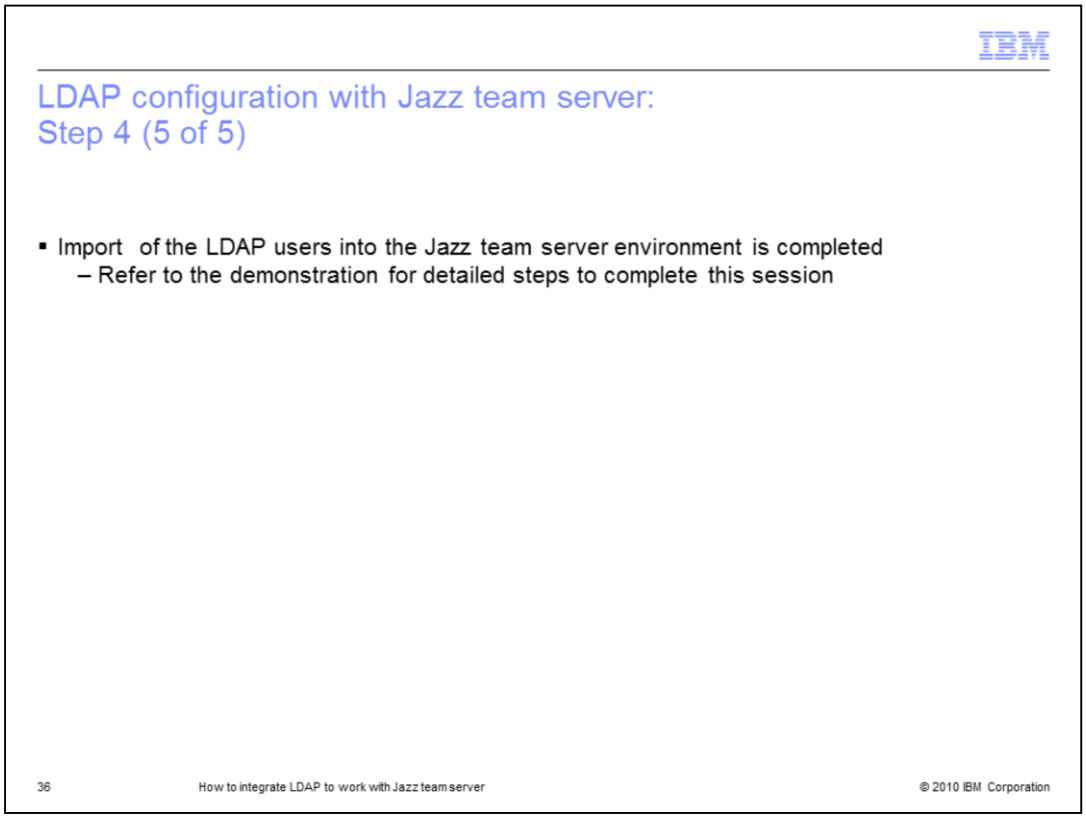
LDAP configuration with Jazz team server: Step 4 (4 of 5)

- **Assign Client Access Licenses**
  - Click the user name from the active user list
  - Ensure this user is assigned with one of the Jazz user role
  - Assign the proper client access license accordingly
  - Click Save to save the change

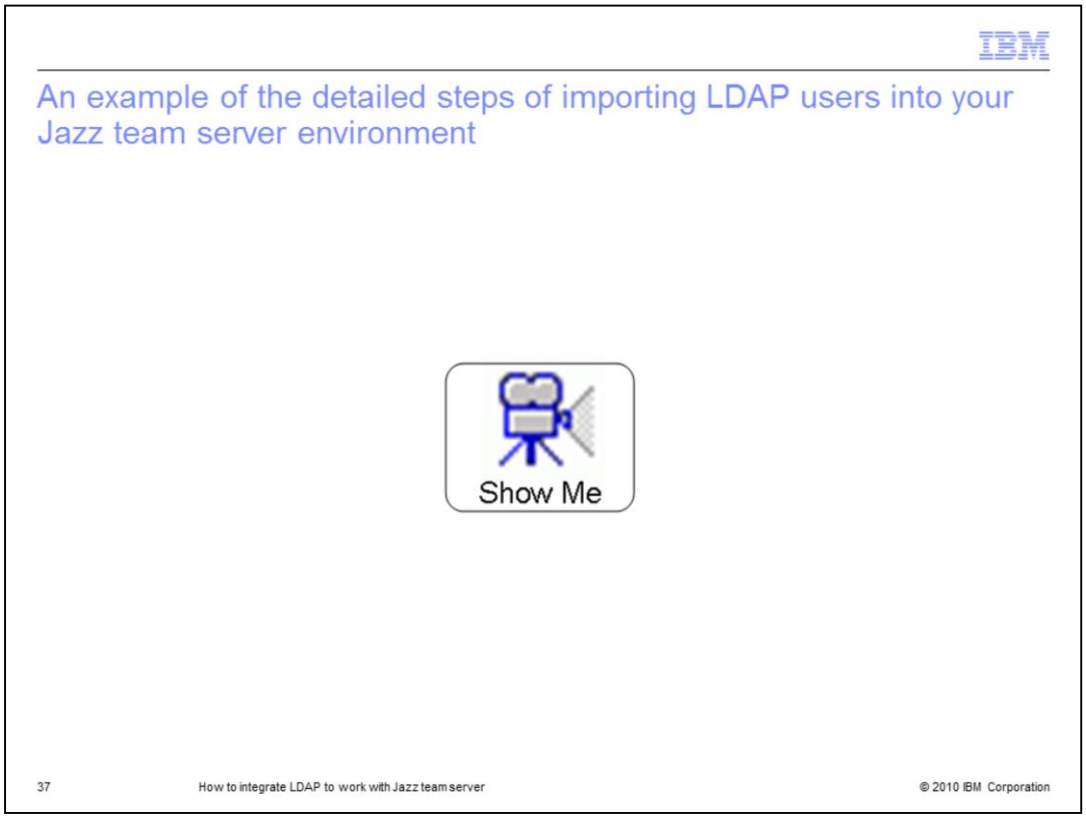


© 2010 IBM Corporation

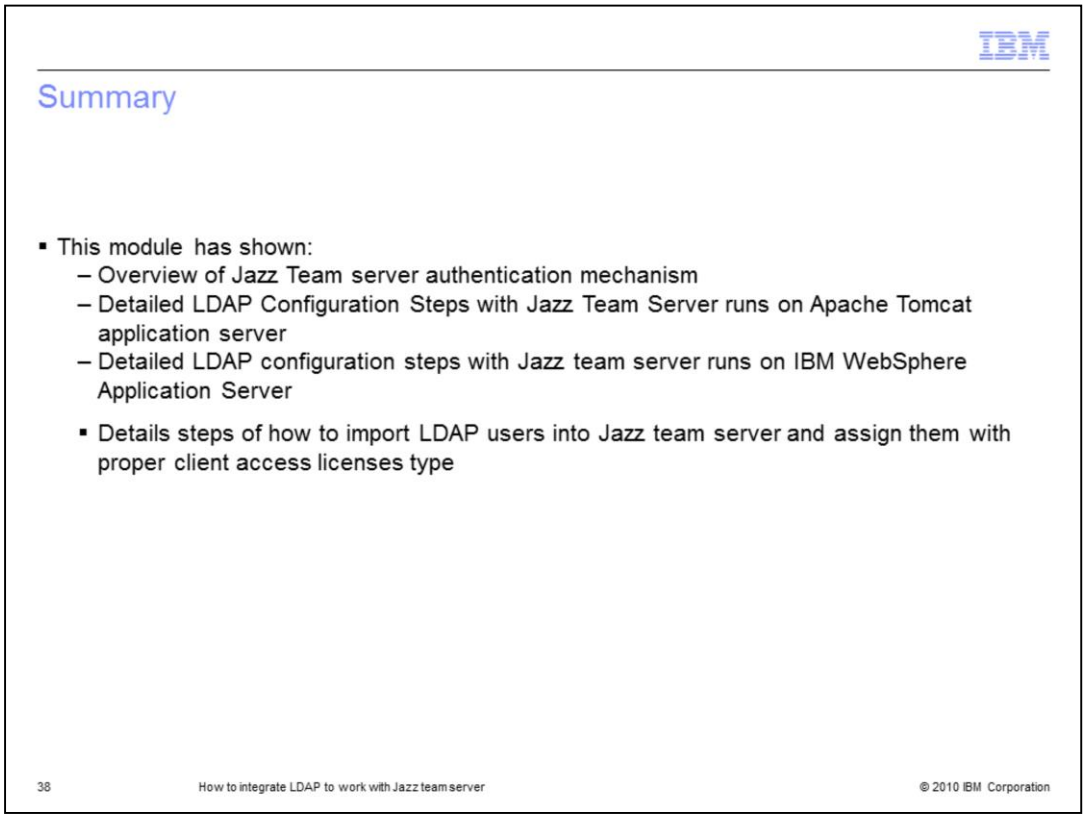
As mentioned earlier, the main purpose for manually importing LDAP users into your Jazz team server environment is to assign a client access license to the user. This slide shows you how to assign a client access license to an imported LDAP user.



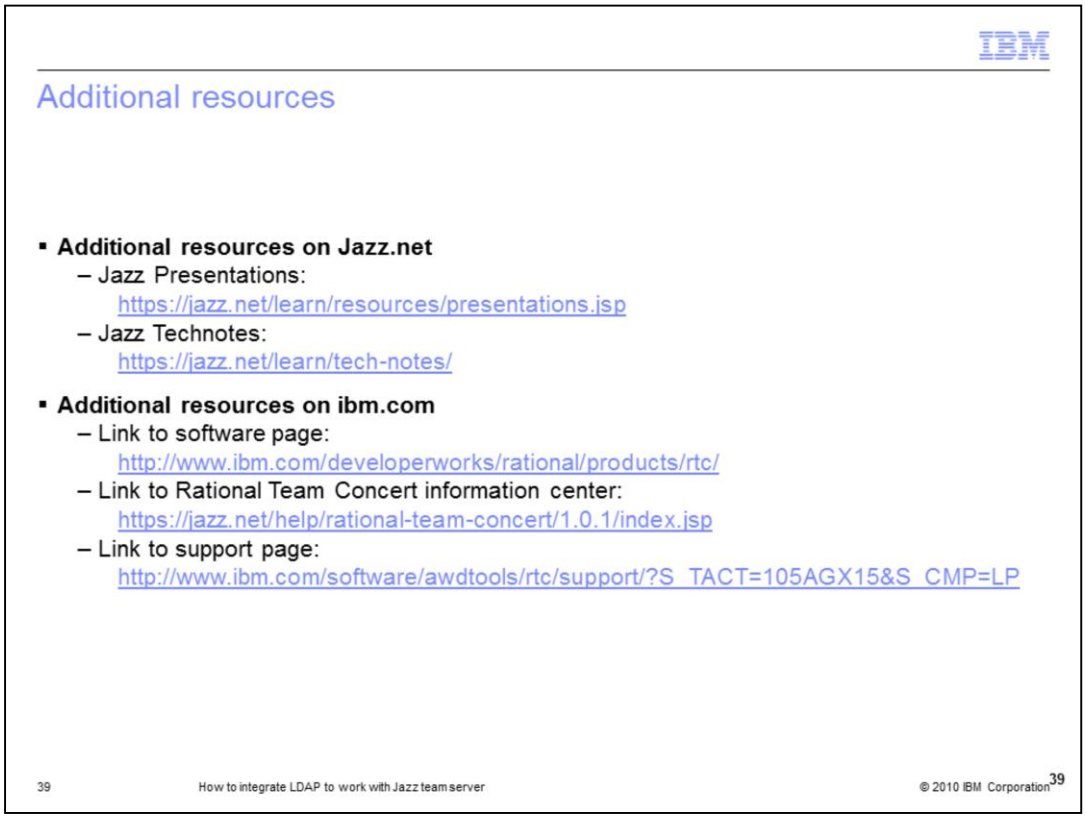
You now completed step four of the LDAP configuration with the Jazz team server by importing LDAP users into your Jazz team server environment. Refer to demonstration in the next slide to see how these steps are performed in detail. This is the end of LDAP configuration with the Jazz team server. Your Jazz team server should now be configured to authenticate access by using LDAP user credentials.



Here is an example of the detailed steps of importing LDAP users into your Jazz team server environment. To watch a demonstration of this, pause this presentation and click the “Show Me” Icon.



This concludes the LDAP configuration with the Jazz team server module. You should now have a better understanding of how Jazz team server authenticates access to its resources, in addition to the necessary steps to configure LDAP registry to work with your Jazz team server runs on Tomcat or WebSphere Application server.



Additional resources can be found on Jazz.net, Developerworks and the Rational Team Concert support page.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Jazz, Rational, Rational Team Concert, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
Java, and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2010. All rights reserved.

© 2010 IBM Corporation