

IBM Rational Team Concert

How to integrate LDAP to work with Jazz team server



Goals

- To provide you an overview of Jazz™ team server authentication mechanism
- To provide you step by step guidance of how to integrate LDAP to work with Jazz team server

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.

Agenda

- Overview of Jazz team server authentication mechanism
- LDAP configuration steps with Jazz team server
- LDAP configuration demonstrations

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.

Overview of jazz team server: Authentication mechanism

- Jazz team server is a Java Enterprise Edition (Java EE) web Application
- Jazz team server application runs in a secure container and requires authentication
- A secure container is another term for "application server"
- WebSphere and Tomcat are the two supported application servers by Jazz
- Authentication is managed by container
- Jazz team server uses a set of predefined roles that can be assigned to users
- Jazz supports two authentication methods: FORM and BASIC

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.

Overview of the Jazz team server: authentication mechanism – authentication process

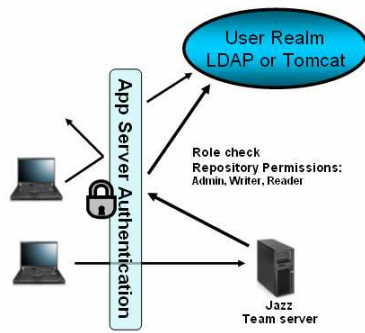


Figure 1: Container Managed Authentication for the Jazz Team Server

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.

Overview of the Jazz team server authentication mechanism: predefined repository roles

- Jazz team server application uses these pre-defined repository roles

Role Name	Description
JazzAdmins	Administrators of a Jazz Repository with full read-write access
JazzDatawarehouseAdmins	Administrators of a Jazz Repository with specific permissions to control the data warehouse on a Jazz Server
JazzUsers	Users with regular read-write access to the Jazz Repository
JazzGuests	Users with read-only access to the Jazz Repository.

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.

Overview of Jazz team server authentication mechanism: authentication methods

- Authentication methods supported by Jazz
 - Form: default method
 - Jazz team server web UI presents HTML form to collect user credentials first time user attempts to access a secured resource
 - Jazz redirects to custom page for failed login
 - Login "session" is established between the browser and the server; once authenticated, the server only needs to validate the session but does not need to re-authenticate credentials
 - Basic: method used by LDAP
 - The web browser itself presents a dialog to collect user credentials the first time the user attempts to access a secured resource
 - Credentials passed on every request from client to the server; on each request the server (WebSphere) validates credentials or (Tomcat) re-authenticates credentials

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 Server. 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.

LDAP configuration with Jazz team server

- LDAP configuration: four major steps:
 - Collect LDAP parameters and define LDAP groups for Mapping
 - Configure LDAP user registry from Jazz server setup page
 - Configure LDAP security realm from application server level
 - Import LDAP users into Jazz team server environment

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.

LDAP configuration with Jazz team server: Step 1 (1 of 2)

- LDAP parameters
 - **LDAP Registry Location**: the URL referencing your LDAP server, that is:
ldap://ldap.company.com:389
 - **User Name**: The user name to login to this LDAP server. Some LDAP servers do not require a login/password. In this case, the parameter will stay blank
 - **Password**: The password associated to the previous login
 - **Base User DN**: The search base indicates where in the hierarchy to begin the search the users. For example, "ou=[your organization], o=[your company]"
 - **User Property Names Mapping**: Indicates how to map Jazz user properties to your LDAP registry entry attributes. You will have to define these mapping:
 - `userId` =[LDAP user ID],
 - `name` =[LDAP user name],
 - `emailAddress` =[LDAP user email]
 - **Base Group DN**: This search base indicates where in the hierarchy to begin the search the group names
 - **Group Name Property**: LDAP Property to represent the name of the Jazz groups in the LDAP registry
 - **Group Member Property**: LDAP Property to represent the members of a group in the LDAP registry
- **Jazz to LDAP Group Mapping**

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.

LDAP configuration with Jazz team server: Step 1 (2 of 2)

- Define LDAP groups to map with Jazz roles
 - LDAP group for Jazz administrators
 - LDAP group for Jazz users
 - LDAP group for Jazz data warehouse administrator
 - LDAP group for Jazz guest

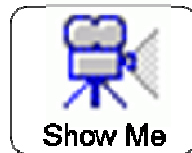
As mentioned in the previous slides, the Jazz team server application uses a set of predefined roles that can be assigned to users within the authentication operation. As part of step one of the LDAP configuration, you need to collect four LDAP groups to map with this set of predefined Jazz roles. The 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.

LDAP configuration with Jazz team server: Step 2

- Configure the LDAP user registry from the Jazz team server setup page
 - Login to Jazz team server setup page
 - Choose Fast Path or Custom Setup
 - Go to User Register Setup page
 - Fill in required parameters collected in step one

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.

An example on how to configure the LDAP user registry from 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.

LDAP configuration with Jazz team server: Step 3

- Configure LDAP security realm from the application server level
 - Part 1. Configure LDAP security realm in Tomcat
 - Part 2. Configure LDAP security realm in WAS

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 realm 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.

LDAP configuration with Jazz team server: Step 3: Part 1.1

- Configure LDAP security realm in Tomcat
 - 1. Modify the server.xml file
 - Edit the file [JazzServerInstallDir]\jazz\server\tomcat\conf\server.xml
 - Comment out this tag:
<Realm className="org.apache.catalina.realm.UserDatabaseRealm"
resourceName="UserDatabase"
digest="SHA-1"
digestEncoding="UTF-8"/>
 - Replace it with:

<Realm className="org.apache.catalina.realm.JNDIRealm"
debug="9"
connectionURL="ldap://ldaps.examples.com:389"
userBase="dc=examples, dc=com"
userSearch="(sAMAccountName={0})"
userSubtree="true"
roleBase="ou=examplegroup, dc=examples, dc=com"
roleSubtree="false"
roleSearch="(members={0})"
roleName="cn"
digest="SHA-1"
digestEncoding="UTF-8"
>

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.

LDAP configuration with Jazz team server: Step 3: Part 1.2A

- 2. Modify the web.xml file to define the LDAP groups to map with Jazz roles:
 - 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
 - web.xml file is accessible only if jazz.war has been deployed, that is, you already run at least once the Jazz server.
 - Edit the file [JazzServerInstallDir]\jazz\server\tomcat\webapps\jazz\WEB-INF\web.xml
 - A. Define security-role-ref tags: map the pre-defined Jazz security roles references to LDAP groups:
 - Insert the tags in blue below in between the red tags (red tags already exist in the original web.xml file):
 - `<load-on-startup>1</load-on-startup>`
 - `<security-role-ref>`
 - `<role-name>JazzAdmins</role-name>`
 - `<role-link>[LDAP Group for Jazz admins]</role-link>`
 - `</security-role-ref>`

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.

LDAP configuration with Jazz team server: Step 3: Part 1.2A (continued)

- `<security-role-ref>`
- `<role-name>JazzDWAdmins</role-name>`
- `<role-link>[LDAP Group for Jazz Data Warehouse Admin]</role-link>`
- `</security-role-ref>`

- `<security-role-ref>`
- `<role-name>JazzGuests</role-name>`
- `<role-link>[LDAP Group for Jazz guest]</role-link>`
- `</security-role-ref>`

- `<security-role-ref>`
- `<role-name>JazzUsers</role-name>`
- `<role-link>[LDAP Group for Jazz users]</role-link>`
- `</security-role-ref>`
- `<!-- End Addendum -->`

- `</servlet>`

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

LDAP configuration with Jazz team server: Step 3: Part 1.2B

- B. Define new security-role tags: declare LDAP groups as security roles:
 - Insert the tags in blue below in between the red tags
(red tags already exist in the original web.xml file):
 - `<auth-constraint>`
 - `<role-name>JazzUsers</role-name>`
 - `<role-name>JazzAdmins</role-name>`
 - `<role-name>JazzGuests</role-name>`
 - `<role-name>JazzDWAdmins</role-name>`
 - `<role-name>[LDAP Group for Jazz admins]</role-name>`
 - `<role-name>[LDAP Group for Jazz users]</role-name>`
 - `<role-name>[LDAP Group for Jazz Data Warehouse Admin]</role-name>`
 - `<role-name>[LDAP Group for Jazz guest]</role-name>`
 - `<!-- End Addendum -->`
 - `</auth-constraint>`
 - `<user-data-constraint>`
 - `<transport-guarantee>CONFIDENTIAL</transport-guarantee>`

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.

LDAP configuration with Jazz team server: Step 3: Part 1.2C

- C. Update the security-constraint tag: Authorize LDAP Jazz administrative group access to secure administrator page:
 - Insert the tags in blue below in between the red tags
 - (red tags already exist in the original web.xml file):
 - `<security-constraint>`
 - `<web-resource-collection>`
 - `<web-resource-name>adminsecure</web-resource-name>`
 - `<url-pattern>/admin/cmd/*</url-pattern>`
 - `</web-resource-collection>`

 - `<auth-constraint>`
 - `<role-name>JazzAdmins</role-name>`
 - `<role-name>[LDAP Group for Jazz admins]</role-name>`
 - `</auth-constraint>`

This slide 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.

LDAP configuration with Jazz team server: Step 3: Part 1.2D

- D. Update the security-role:
 - Add LDAP groups to the set of security roles which a user must belong to for accessing resources matched by the web resource collection
 - Insert the tags in blue below in between the red tags (red tags already exist in the original web.xml file):
 - `</login-config>`
 - `....`
 - `<security-role>`
 - `<role-name>JazzGuests</role-name>`
 - `</security-role>`
 - `<security-role>`
 - `<role-name>[LDAP Group for Jazz admins]</role-name>`
 - `</security-role>`
 - `<security-role>`
 - `<role-name>[LDAP Group for Jazz Data Warehouse Admin]</role-name>`
 - `</security-role>`
 - `<security-role>`
 - `<role-name>[LDAP Group for Jazz users]</role-name>`
 - `</security-role>`
 - `<security-role>`
 - `<role-name>[LDAP Group for Jazz guest]</role-name>`
 - `</security-role>`
 - `</web-app>`

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.

LDAP configuration with Jazz team server: Step 3: End of part 1

- Configure LDAP security realm from application server level
 - Part 1. Configure LDAP security realm in Tomcat Completed
 - Restart Jazz Team Server

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.

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

- Configure the LDAP security realm from application server level
 - Part 2. Configure LDAP security realm in WebSphere Application Server

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.

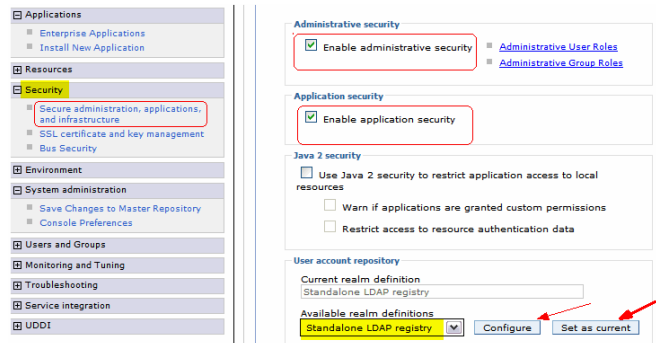
LDAP configuration with Jazz team server: Step 3: Part 2 (continued)

- Configure the LDAP security realm in WebSphere Application Server
 - A. Configure Stand-alone LDAP registry realm
 - B. Map LDAP groups to Jazz repository roles
 - C. Optional: Map LDAP users Jazz repository roles

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



23

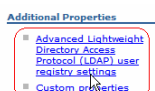
How to integrate LDAP to work with Jazz team server

© 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



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

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

▪ A. Configure Stand-alone LDAP registry realm

– Specify the user and group filters, the settings used are:

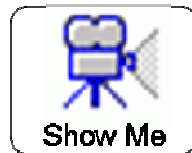
- User Filter: (&(uid=%v)(objectclass=inetOrgPerson))
- Group Filter: (&(cn=%v)(|(objectclass=groupOfNames)(objectclass=posixGroup)))
- **User id map: *.mail**
- Group id map: *.cn
- Group member id map: ibm-allGroups:member;ibm-allGroups:uniqueMember

– Click the Test connection button to verify the settings

– If all the settings are correct, click “Apply”, then “Save Directly to the master configuration” and restart the WebSphere Application Server process

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.

An example of the detailed steps of configuring the Stand-alone LDAP registry realm in WebSphere Application Server



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



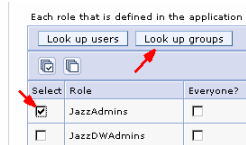
In this section you will see what needs to be done to complete task B which is to map LDAP groups to pre-defined Jazz repository roles. As mentioned earlier, there are four pre-defined Jazz roles within the Jazz team server to provide users/groups different types of access to resources in the application. 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
<input type="checkbox"/>	JazzAdmins	<input type="checkbox"/>	<input type="checkbox"/>		cn=jazzadmins,ou=memberlist,ou=ibmggroups,o=ibm.com
<input type="checkbox"/>	JazzDWAdmins	<input type="checkbox"/>	<input type="checkbox"/>		cn=JazzDWAdminsSWU,ou=memberlist,ou=ibmggroups,o=ibm.com
<input type="checkbox"/>	JazzUsers	<input type="checkbox"/>	<input type="checkbox"/>		cn=JazzUsersSWU,ou=memberlist,ou=ibmggroups,o=ibm.com
<input type="checkbox"/>	JazzGuests	<input type="checkbox"/>	<input type="checkbox"/>		cn=JazzGuestsSWU,ou=memberlist,ou=ibmggroups,o=ibm.com

Figure 2: Jazz Roles with corresponding mapped LDAP roles

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
<input type="checkbox"/>	JazzAdmins	<input type="checkbox"/>	<input type="checkbox"/>	uid=094469649,c=ca,ou=bluepages,o=ibm.com
<input type="checkbox"/>	JazzDWAdmins	<input type="checkbox"/>	<input type="checkbox"/>	uid=065757649,c=ca,ou=bluepages,o=ibm.com
<input type="checkbox"/>	JazzUsers	<input type="checkbox"/>	<input type="checkbox"/>	uid=065587649,c=ca,ou=bluepages,o=ibm.com
<input type="checkbox"/>	JazzGuests	<input type="checkbox"/>	<input type="checkbox"/>	uid=011581649,c=ca,ou=bluepages,o=ibm.com

Figure 1: Jazz roles with corresponding mapped LDAP users

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.



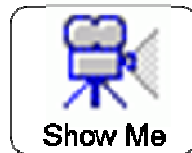
LDAP configuration with Jazz Team Server

Step 3: Part 2: End

- Configure LDAP security realm in WebSphere Application Server completed
 - Refer to the demonstration on mapping LDAP groups to Jazz repository roles in WAS

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.

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.

LDAP configuration with Jazz team server: Step 4 (1 of 5)

- Import LDAP users into the Jazz team server environment
 - Optional - can be performed automatically by LDAP nightly sync task, runs at 1:00 AM by default
 - Perform if you want to assign LDAP users Client Access License, before LDAP nightly sync task

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.

LDAP configuration with Jazz team server: Step 4 (2 of 5)

- Things to keep in mind when perform importing
 - Users who have already been imported are not found when doing the LDAP user search
 - Users who are archived can't be found when doing the LDAP user search

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



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

The screenshot shows the 'Active Users' management interface. On the left, under 'Active Users >', a user named 'David Smith' is selected. Below this, the 'Details' section shows the 'User ID (case sensitive):' as 'dsmith@ca.ibm.com' and the 'E-mail Address:' as 'dsmith@ca.ibm.com'. On the right, the 'Repository Permissions' section has a notice: 'Notice: You are using a directory service that is not writable. User roles cannot be modified.' Below this, three roles are listed: 'JazzAdmins', 'JazzDWAdmins', and 'JazzGuests', all with unchecked checkboxes. The 'JazzUsers' role is checked. Below the permissions, the 'Client Access Licenses' section lists several Rational Team Concert licenses with their available counts. The 'JazzUsers' role and the 'Client Access Licenses' list are highlighted with red boxes.

Active Users >

David Smith

Details

User ID (case sensitive): * dsmith@ca.ibm.com

E-mail Address: * dsmith@ca.ibm.com

Repository Permissions

Notice: You are using a directory service that is not writable. User roles cannot be modified.

- ☐ JazzAdmins
- ☐ JazzDWAdmins
- ☐ JazzGuests
- ☒ JazzUsers

Client Access Licenses

- ☐ Rational Team Concert - Contributor (0 available)
- ☐ Rational Team Concert - Developer (244 available)
- ☐ Rational Team Concert - Floating Contributor
- ☐ Rational Team Concert - Floating Developer
- ☐ Rational Team Concert - Build System (50 available)
- ☐ Rational Team Concert - ClearCase Connector (250 available)
- ☐ Rational Team Concert - ClearQuest Connector (1 available)

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.

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

- Import of the LDAP users into the Jazz team server environment is completed
 - Refer to the demonstration for detailed steps to complete this session

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.

An example of the detailed steps of importing LDAP users into your Jazz team server environment



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.

Summary

- This module has shown:
 - Overview of Jazz Team server authentication mechanism
 - Detailed LDAP Configuration Steps with Jazz Team Server runs on Apache Tomcat application server
 - Detailed LDAP configuration steps with Jazz team server runs on IBM WebSphere Application Server
- Details steps of how to import LDAP users into Jazz team server and assign them with proper client access licenses type

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

- **Additional resources on Jazz.net**

- Jazz Presentations:
<https://jazz.net/learn/resources/presentations.jsp>
- Jazz Technotes:
<https://jazz.net/learn/tech-notes/>

- **Additional resources on ibm.com**

- Link to software page: <http://www.ibm.com/developerworks/rational/products/rtc/>
- Link to Rational Team Concert information center:
<https://jazz.net/help/rational-team-concert/1.0.1/index.jsp>
- Link to support page:
http://www.ibm.com/software/awdtools/rtc/support/?S_TACT=105AGX15&S_CMP=LP

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

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_JazzRTCLDAPConfiguration.ppt

This module is also available in PDF format at: [../JazzRTCLDAPConfiguration.pdf](http://JazzRTCLDAPConfiguration.pdf)

You can help improve the quality of IBM Education Assistant content by providing feedback.



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](http://www.ibm.com/legal/copytrade.shtml)" 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.