

Configure Rational Change with 3rd Party LDAP Server

Release 5.3.2.2

Contents

1.	Introduction	3
2.	LDAP Server Supported version.....	3
3.	Enablement of LDAP Feature in Rational Change	3
I.	Access LDAP Configuration web interface.....	4
II.	Configure Primary Directory Server	5
III.	Configure Secondary Server	7
4.	Alternate way to configure Secondary DS.....	9
I.	Configuring Secure LDAP (SSL).....	11
II.	Migrate data from RDS to Change Server	11
5.	Troubleshoot:.....	13
6.	General Instruction:	13

1. Introduction

Rational Change 5.3.1 or above, requires IBM Rational Directory Server (RDS 5.x) to authenticate the users who wish to connect to Rational Change. From Change 5.3.2.2 onwards, it is possible to choose any 3rd party LDAP server for authentication. At present, Change 5.3.2.2 has been validated with "Apache DS" and "Active Directory" LDAP servers.

Change 5.3.2.2 works well with existing Rational Directory Server (RDS 5.x). As an alternative to RDS 5.x, it can be configured to use a 3rd party LDAP server. This document helps to understand the steps to configure Change with single or multiple DS(max 2).

This implementation provides an option to the customer (applicable for environment where number of users are more than 1500 having login issues with metagroup) to opt for RDS or this new LDAP implementation.

Pre-requisites

- Rational Change 5.3.2 or Rational Change 5.3.2.1

2. LDAP Server Supported version

- Apache DS version 2.0.0
- Active Directory Windows 2012

3. Enablement of LDAP Feature in Rational Change

- In Change server, open ../WEB-INF/wsconfig/pt.cfg file in text editor.
- Make below entry at the end of the file :-

```
[CCM_SYSTEM][LDAP_ENABLED]true[/LDAP_ENABLED]/[CCM_SYSTEM]
```

- Update its value to "true" to enable LDAP support.
- Save and exit.
- Restart the Change server.

Note: If the entry b) is not there or if the value is set to 'false' in "pt.cfg", then it uses RDS 5.x for authentication.

LDAP Configuration

Change 5.3.2.2 provides web interface to provide the LDAP configuration. To access this page, you need to enable the LDAP configuration in the "pt.cfg" file. (Point 3. c)

To configure Change with a LDAP server, **Change** administrator should get following details from the LDAP administrator.

Connection URL	The LDAP URL of the Server, For example ldap://winsyn2008:389
Service username	The complete DN (Distinguished Name) of the user who can perform the search on the users

	and groups.
Service password	Password for the service user
User search base	The location in the directory from which the LDAP search begins
User login attribute	The User Login Name for the user object in the LDAP server. For example, Active Directory: sAMAccountName Apache DS: uid
Filter	Additional search attribute to filter the user object to, For example, objectClass=Person
Search Sub-Tree	True/False, True if sub-tree search required false otherwise.
Group Name Attribute	This attribute holds the name of the group.
Group Member Attribute	A Groups, group member attribute contains user DN. For example – member or uniqueMember.
Group Object Value	Object class of the group.

I. Access LDAP Configuration web interface

Pre-requisites

- Enable LDAP as mentioned in section 3
- Navigate to the URL <http://change-server-hostname:server-port/change/admin>

This would prompt the Change LDAP Primary Directory Server configuration dialog as shown in the screenshot below:

Primary Directory Server	
* URL:	<input type="text"/>
* DS Admin:	<input type="text"/>
* Password:	<input type="text"/>
* User Login Attribute:	<input type="text"/>
* User Base Search:	<input type="text"/>
Filter:	<input type="text"/>
Search Sub-Tree:	<input type="checkbox"/>
* Group Name Attribute:	<input type="text"/>
* Group Member Attribute:	<input type="text"/>
* Group Object Value:	<input type="text"/>
<input type="button" value="connect"/> <input type="button" value="Test Connection"/>	
Configure Secondary DS	<input type="checkbox"/>

II. Configure Primary Directory Server

Example


Depending on the Users, Groups, Admin users present in the LDAP tree structure, fill the information into "IBM Rational Synergy LDAP Configuration" form.

Primary Directory Server	
* URL:	ldap://10.115.86.17:10389
* DS Admin:	uid=admin,ou=system
* Password:	●●●●●●
* User Login Attribute:	uid
* User Base Search:	ou=users,ou=system
Filter:	objectClass=*
Search Sub-Tree:	<input type="checkbox"/>
* Group Name Attribute:	cn
* Group Member Attribute:	uniqueMember
* Group Object Value:	groupOfUniqueNames
<input type="button" value="connect"/> <input type="button" value="Test Connection"/>	
Configure Secondary DS	<input type="checkbox"/>

- Click on 'Test Connection' to validate the LDAP configuration information.
- Once test is passed, it will show a message 'Connection Successful, successfully retrieved <N> users'.

Configure IBM Rational Change to use Directory Server

Rational Change must be configured to use Directory Server (DS). DS is used to perform authentication and to store user data. Enter the details about your DS to establish a connection.

 Test Connection Success!!

- Click on 'connect'. If all fine then admin Change will redirected to Change Admin login page.

Note - Change allows you to have maximum two DS i.e. one Primary and One Secondary Server at a time.


III. Configure Secondary Server

Configuring Secondary Directory Server is optional. To configure secondary DS select Configure Secondary DS checkbox on the Primary Directory Server configuration page. If Primary DS connection is successful and 'Configure Secondary DS' was selected then on click of connect will redirect Change to Secondary DS configuration page.

Refer the screenshot below:

Configure IBM Rational Change to use Directory Server

Rational Change must be configured to use Directory Server (DS). DS is used to perform authentication and to store user data. Enter the details about your DS to establish a connection.

 Test Connection Success!!

Primary Directory Server	
* URL:	ldap://10.115.86.17:10389
* DS Admin:	uid=admin,ou=system
* Password:	●●●●●●
* User Login Attribute:	uid
* User Base Search:	ou=users,ou=system
Filter:	objectClass=*
Search Sub-Tree:	<input type="checkbox"/>
* Group Name Attribute:	cn
* Group Member Attribute:	uniqueMember
* Group Object Value:	groupOfUniqueNames
<input type="button" value="connect"/> <input type="button" value="Test Connection"/>	
Configure Secondary DS	<input checked="" type="checkbox"/>

Configure IBM Rational Change to use Directory Server

Rational Change must be configured to use Directory Server (DS). DS is used to perform authentication and to store user data. Enter the details about your DS to establish a connection.

Secondary Directory Server	
* URL:	ldap://10.115.86.17:10389
* DS Admin:	uid=admin,ou=system
* Password:	●●●●●●
* User Login Attribute:	uid
* User Base Search:	ou=users,ou=system
Filter:	objectClass=*
Search Sub-Tree:	<input type="checkbox"/>
* Group Name Attribute:	cn
* Group Member Attribute:	uniqueMember
* Group Object Value:	groupOfUniqueNames
<input type="button" value="connect"/> <input type="button" value="Test Connection"/>	

Steps to Configure Secondary DS

a) Enter all the mandatory fields as shown below:

Secondary Directory Server	
* URL:	ldap://10.115.86.26:10389
* DS Admin:	uid=admin,ou=system
* Password:	●●●●●●
* User Login Attribute:	uid
* User Base Search:	ou=users,ou=system
Filter:	objectClass=*
Search Sub-Tree:	<input type="checkbox"/>
* Group Name Attribute:	cn
* Group Member Attribute:	uniqueMember
* Group Object Value:	groupOfUniqueNames
<input type="button" value="connect"/> <input type="button" value="Test Connection"/>	

b) Click on test Connection Button to check if the connection is successful.

Possible actions are either 'Test Connection' or 'connect'. Test Connection will validate connection and show success/warning/error message on same screen. 'connect' will configure Change with given DS details and if successful then redirect Change to Admin login page.

Files created in backend: -

Primary DS :- ../WEB-INF/wsconfig/ldap_config.xml

Secondary DS :- ../WEB-INF/wsconfig/ldap_config1.xml

4. Alternate way to configure Secondary DS

There is also an alternate option to configure Secondary Directory Server if not configured earlier on the Primary Directory Server Configuration Page.

We can configure secondary DS when Change is running only with Primary DS.

Below are the steps to be followed:

1. Login to Change Admin Page.
2. Navigate to System Administration
3. Click on Configure Secondary DS Tab.
4. Refer screenshot below:

The screenshot shows the 'Configure Secondary DS' window in the IBM Rational Change System Administration tool. The window has a title bar with 'IBM Rational Change' and a menu bar with 'Home', 'System Administration', 'User Management', 'Lifecycle Editor', 'Report Builder', 'Help', and 'Exit'. Below the menu bar is a navigation bar with 'System Administration' and several tabs: 'General', 'Server', 'Search', 'Integrations', 'Listbox Manager', 'Package Installer', and 'Configure Secondary DS'. The main content area is divided into two sections:

- Secondary Directory Server:** A form with the following fields:
 - * URL: [Text Input]
 - * DS Admin: [Text Input]
 - * Password: [Text Input]
 - * User Login Attribute: [Text Input]
 - * User Base Search: [Text Input]
 - Filter: [Text Input]
 - * Search Sub-Tree:
 - * Group Name Attribute: [Text Input]
 - * Group Member Attribute: [Text Input]
 - * Group Object Value: [Text Input]
- Information:** A text box containing the following text:
 - Below points should be considered before/after Secondary DS Configuration.
 - * This option will be available when RDS is disabled and Rational Change was configured with Primary DS only (only 1 DS).
 - * Once Secondary DS is configured this option will disappear from System Administration.
 - * Secondary DS Connection configured from here will be in effect only after Rational Change restart.

At the bottom of the form, there are two buttons: 'Test Connection' and 'Connect'.

5. Enter all the mandatory fields.
6. Click on 'Test Connection' button, it will validate data.
7. If all the details are correct, then a Connection Successful message will appear at the left side bottom of the page.
8. Clicking 'connect' button will configure Secondary DS.
9. This will create ldap_config.xml in ../WEB-INF/wsconfig/
10. For changes to take effect restart the Change server.

Note - If Connection was successful then 'Configure Secondary DS' menu will disappear from Admin

How to update the password in the LDAP configuration

There are two ways an administrator can use to modify the password or any other configuration related values in the Change server.

- Delete the ldap_config.xml and ldap_config1.xml file and restart the server. This will allow the user to access the LDAP configuration page again and provide all the configuration values.
- Navigate to the URL: <http://change-server-hostname:server-port/change/admin>
- Administrator can manually edit the ldap_config.xml file to update the password in plain text format and restart the server. Once you restart the server, it will automatically encrypt the password.
- If password needs to be updated in file manually then follow below :-
 - Update new password in password tag
 - Change password tag from 'password' to 'password-unencrypted'
 - Once Change server will restart, Change will decrypt it again and update 'password- unencrypted' tag to 'password'

I. Configuring Secure LDAP (SSL)

This section describes how to configure Change server to use the LDAPS protocol for secure network communication between the Change server and LDAP Server. Configuring Change to communicate using the LDAPS protocol involves two steps:

1. Get the SSL certificate from the LDAP server: Customer can use any LDAP UI (For example Apache Directory studio) to download the certificate from the server or need contact the LDAP administrator to get the SSL certificate. The certificate should be either in 'X509 Certificate EDR' or 'X509 Certificate PEM' format.
2. Import the certificate into Change Server: Use the keytool to import the certificate to Synergy Server JRE and restart Change services.

```
C:> cd %CCM_HOME%/jre/bin
C:> keytool -import -alias ldapkey -file ldap.cer -
keystore ../lib/security/cacerts
Enter keystore password: changeit
Owner: CN=my_server, OU=Unknown, O=Unknown, L=Unknown,
ST=Unknown, C=Unknown
Issuer: CN=my_server, OU=Unknown, O=Unknown, L=Unknown,
ST=Unknown, C=Unknown
Serial number: 49d2466b
Valid from: 3/31/09 9:35 AM until: 6/29/09 9:35 AM
Certificate fingerprints:
MD5: F6:3F:8C:0C:DB:22:0C:51:0B:B3:4B:41:40:27
SHA1: CE:6C:B6:99:48:94:4D:0A:7B:88:EE:CF:F7:68:B4
Trust this certificate? [no]: y
Certificate was added to keystore
```

Note: The default password of the JRE keystore is "changeit"

Once proper certificate is imported, Change has to be configured with proper ldaps URL in connection window as mentioned in Configuration step 2.

II. Migrate data from RDS to Change Server

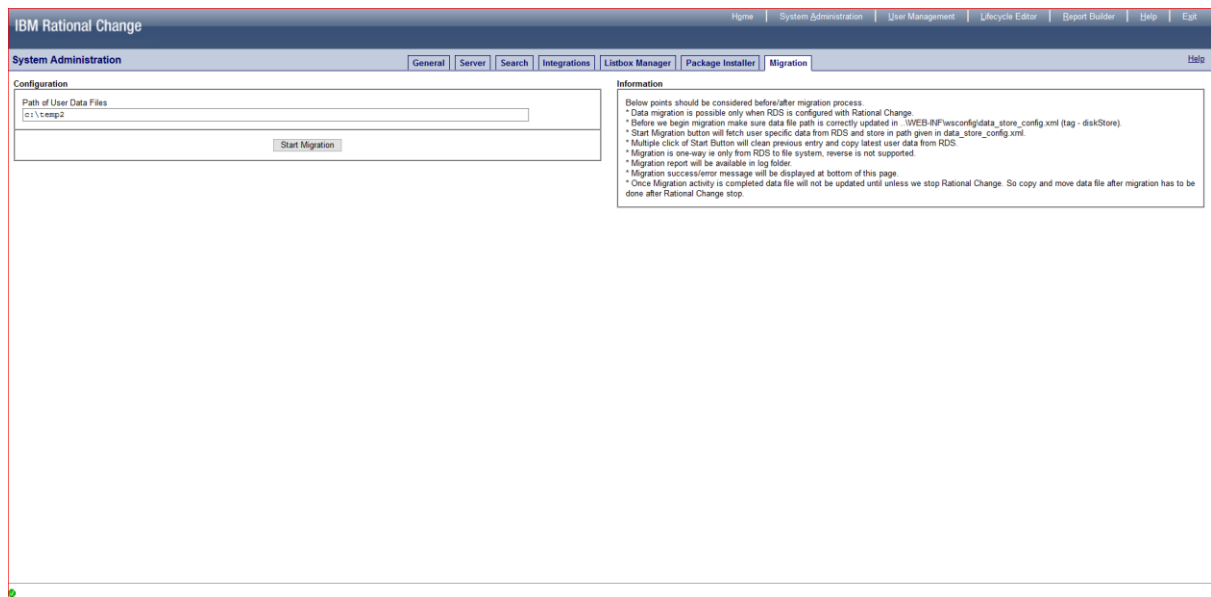
- With Change release 5.3.2.2 it is possible to store user preference data in Change server instead of RDS.
- Location of file system is mentioned in diskStore tag in data_store_config.xml available in ../WEB-INF/wsconfig/.

- Change allows to migrate user data from RDS in flat files.

Note: - Before we start Migration make sure dataStore folder has write permission.

Steps to Migrate

- Enable RDS as mentioned in point 3
- Login to Change Admin page.
- Navigate to Admin → System Administration → Migration Tab.
- Validate correct path for the user data file is shown in the “Path of User Data Files”.



Note - Data migration is possible only when RDS is configured with Rational Change.

Before we begin migration make sure data file path is correctly updated in ..\WEB-INF\wsconfig\data_store_config.xml (tag - diskStore).

- **Restart Change after updating the data file path in the data_store_config.xml file.**
Clicking “Start Migration” button will fetch user specific data from RDS and store in path given in data_store_config.xml.
Multiple click of “Start Migration” Button will clean previous entry and copy latest user data from RDS.
- If it is required to update data store location, update in data_store_config.xml -
<diskStore path="\$CHANGE_HOME/.. /RDSData"/>
- Migration is one-way i.e. only from RDS to file system, reverse is not supported.
- Migration report will be available in log folder.
- Migration success/error message will be displayed at bottom left of the page.
- Once Migration activity is completed data file will not be updated until unless we

restart Rational Change server.

- Copy and move data files after migration must be done after Rational Change stop.
- If user preference count are more than 1500 in RDS then it is possible that all user preference data will not be migrated. To get all user preference from RDS update **maxSizeLimit** flag in RDS :- ../RDS_5.1.1.2/apacheds_1.5.5/conf/server.xml

```
<ldapServer id="ldapServer"
    allowAnonymousAccess="false"
    saslHost="ldap.example.com"
    saslPrincipal="ldap/ldap.example.com@EXAMPLE.COM"
    searchBaseDn="ou=people,dc=telelogic,dc=com"
    maxTimeLimit="15000"
    maxSizeLimit="1500">
```

5. Troubleshoot:

- I. Based on number of users in DS, during Change server startup it calculates duplicate users in Change. This process may take more time than usual to boot Change. Because of this if server startup throws FAILED message then increase timeout in Jetty. Update flag JETTY_START_TIMEOUT (to 180) in Jetty/bin/jetty.sh
- II. LDAP_ENABLED flag in pt.cfg was introduced 5.3.2.2 onwards to support third party ldap support in Rational Change. If Change is running on 5.3.2.2 after enabling this flag as true and later planning to revert back to prior version of Rational Change, in this case if we proceed with uninstall 5.3.2.2 package it is mandatory to disable this flag back to false after uninstall or before uninstall package.

6. General Instruction:

- I. Users are not be allowed to change password in User Interface (Settings->Password)