Contents

[What is LDAP? 2](#_Toc332267698)

[LDAP Authentication 2](#_Toc332267699)

[LDAP Authorization 2](#_Toc332267700)

[Environment configuration 3](#_Toc332267701)

[Server side configuration 3](#_Toc332267702)

[Steps to deploy the ear 4](#_Toc332267703)

[SSL (Secure Socket Layer) 4](#_Toc332267704)

[Workbook Configuration on the local system 6](#_Toc332267705)

### What is LDAP?

LDAP is an [application protocol](http://en.wikipedia.org/wiki/Application_protocol) for accessing and maintaining distributed directory information services over an [Internet Protocol](http://en.wikipedia.org/wiki/Internet_Protocol) (IP) network.

### LDAP Authentication

To consume web service, User has to send his credentials with the request.

As part of this, VBA user sends his username/password in SOAP request header in specific format.

Before the request reaches to Web service, Soap handler reads the soap header and parse for user credentials and consult the Active Directory for user authentication. Right now RMC handles only INBOUND soap messages. Once the user is authenticated and authorized user will get response.

Here consulting AD(Active Directory) is implemented using LDAP(Light Weight Directory Access Protocol).

From VBA, User sends his credentials in below format.

***<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd/">***

***<wsse:UsernameToken>***

***<wsse:Username>NT ID</wsse:Username>***

***<wsse:Password>PASSWORD</wsse:Password>***

***</wsse:UsernameToken>***

***</wsse:Security>***

Usually, Developers are allowed to access Dev and QA environments.

Below files are required to read soap header and LDAP authentication.

1. *SecureLdapUserHandler* reads SOAP header and send user credentials to *LdapFactory*.
2. *LdapFactory* consults Active Directory for authentication.

### LDAP Authorization

Once the user is authenticated, User should exists under below groups in Active Directory according to the environment.

1. DEV\_CFGRatingMethodologyConfigurationRole
2. QA\_CFGRatingMethodologyConfigurationRole
3. PROD\_ CFGRatingMethodologyConfigurationRole

For this, We fetch all the groups for which user is added. Then based on environment We check user is added to that particular group or not.

When the VBA user sends his credentials as part of every request, LDAP code verifies that the user is authenticated and authorized then only he gets the response.

If User is not authenticated, a Soap fault message will be generated and send back to VBA user.

### Environment configuration

To read system properties and pass to the application We defined AppConfig.java. This file reads all system properties(from server side configuration too).

In RMC, We are maintaining 3 properties files respective to the environment. In this properties files we need to mention path for loggers and LDAP required properties.

1. rma\_DEV.properties
2. rma\_QA.properties
3. rma\_PROD.properties

### Server side configuration

Below are the steps prepared based on local server (Windows).

1. Place the following jar file at belowdirectory of Jboss application server installation

Path: *jbdevstudio\jboss-eap\jboss-as\common\lib*

File : *Jconn2.jar*

1. add below properties to the below mentioned file and path.

Path:  *jbdevstudio\jboss-eap\jboss-as\server\default\deploy*.

File: properties-service.xml

<attribute name="Properties">

**rma.property=DEV**

**rma.log.dir=C:/nas/CFG/rma/applogs**

</attribute>

For QA environment we can set **rma.property** to **QA**

For Production environment we can set **rma.property** to **PROD**

1. For data source configuration, add the **jdbc\_rmasybds-ds.xml** at below path.

Path: *jbdevstudio\jboss-eap\jboss-as\server\default\deploy* directory.

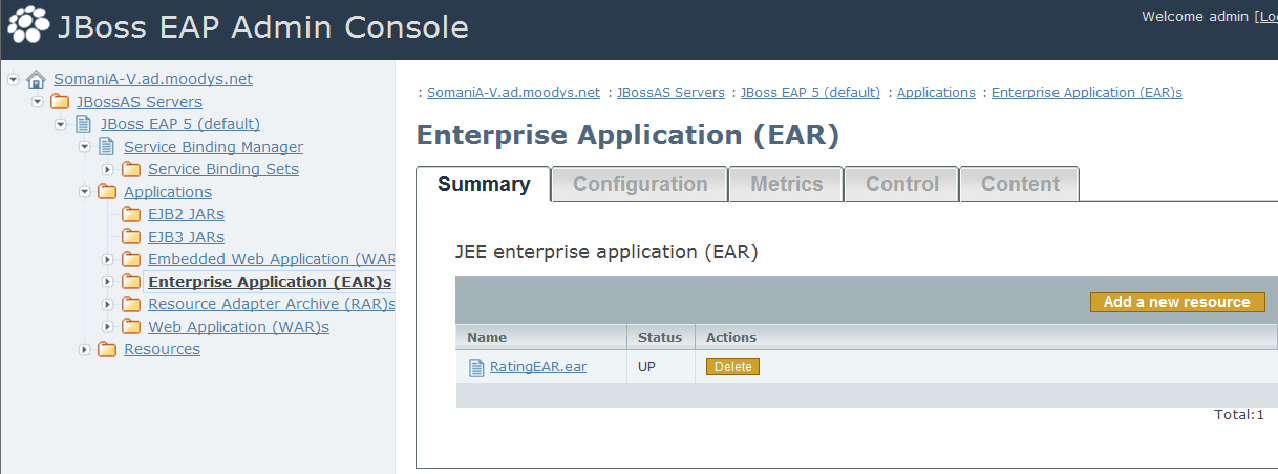
Please find attached data source file for the QA environment



### Steps to deploy the ear

Once the server is started follow the below steps to deploy.

1. Use the below admin console URL’s based on environment.
   1. Dev admin console URL: <https://rmcdev.ad.moodys.net:8543/RMC/>
   2. QA admin console URL: <https://rmcqa.ad.moodys.net:8543/RMC/>
2. Provide username/password to login.
3. Once the admin console is opened, deploy the ear from the below path.



**Dev Data source location in Unix Box : ftc-ldjbfrm208**

**/app/jboss/CFG/RMA/jboss-eap-5.1/jboss-as/server/rma/deploy**

### SSL (Secure Socket Layer)

Steps to be followed for SSL configuration in RMA

1. Generating **Key Store** with below command on the cmd

C:\Program Files\Java\jdk1.6.0\_27\bin>keytool -genkey -alias tomcat -keyalg RSA

The below details have to give for key store generation

Enter keystore password: Eg: rmatool

Re-enter new password: Eg : rmatool

What is your first and last name?

[Unknown]: Computer Name

What is the name of your organizational unit?

[Unknown]: TCS

What is the name of your organization?

[Unknown]: Moodys

What is the name of your City or Locality?

[Unknown]: Hyd

What is the name of your State or Province?

[Unknown]: AP

What is the two-letter country code for this unit?

[Unknown]: Ind

Is CN=Computer Name, OU=TCS, O=Moodys, L=Hyd, ST=AP, C=Ind correct?

[no]: Y

Enter key password for <tomcat>

(RETURN if same as keystore password): rmatool

Re-enter new password: rmatool

set path="C:\Program Files\Java\jdk1.6.0\_26\bin";%path%

1. Generating and Storing Certificate in Key Store

C:\Users\CharugaM>keytool -export -alias tomcat -keystore .keystore -storepass

rmatool -file server.cer

Certificate stored in file <server.cer>

1. Storing Certificate in Key Store

C:\Users\CharugaM>keytool -import -v -keystore client.truststore -storepass rmatool -file server.cer

Owner: CN= Computer Name, OU=TCS, O=Moodys, L=Hyd, ST=AP, C=Ind

Issuer: CN= Computer Name, OU=TCS, O=Moodys, L=Hyd, ST=AP, C=Ind

Serial number: 4fe02aa6

Valid from: Tue Jun 19 03:30:46 EDT 2012 until: Mon Sep 17 03:30:46 EDT 2012

Certificate fingerprints:

MD5: 0D:42:0D:FE:1E:6D:A7:9A:B5:76:4C:47:83:C5:23:69

SHA1: 3D:58:97:2E:0F:4D:6D:51:98:8A:44:70:7D:6A:DC:0E:B1:50:ED:9E

Trust this certificate? [no]: Y

Certificate was added to keystore

[Storing client.truststore]

1. Server.xml configuration for the accessing the WSDL’s with https

<Connector protocol="HTTP/1.1" SSLEnabled="true"

port="8443" address="${jboss.bind.address}"

scheme="https" secure="true" clientAuth="false"

keystoreFile="C:\Users\CharugaM\server.keystore"

keystoreType="jks"

keystorePass="rmatool" sslProtocol = "TLS" />

1. Web.xml configuration for the implementation of the SSL to the specific WAR/EAR

<security-constraint>

<web-resource-collection>

<web-resource-name>securedapp</web-resource-name>

<url-pattern>/\*</url-pattern>

</web-resource-collection>

<user-data-constraint>

<transport-guarantee>CONFIDENTIAL</transport-guarantee>

</user-data-constraint>

</security-constraint>

### Workbook Configuration on the local system

In RMC tool, To run the grid, OWC11.dll should be installed in the machine.

In the template, Backend sheet URL’s should point to by local computer name according to SSL.