Informatica

Informatica® Real-Time Alert Manager
3.1 HotFix1

Administrator Guide

Informatica Real-Time Alert Manager Administrator Guide
3.1 HotFix1
February 2012

Publication Date: 2022-04-25

Table of Contents

Preface

This guide describes how to install and administer Real-Time Alert Manager, set up and configure the software, create user accounts, optimize system performance, and how to back up and recover the Real-Time Alert Manager data store.

This guide is intended for administrators who installs, configures, and manages the Real-Time Alert Manager software.

Informatica Resources

Informatica Customer Portal

As an Informatica customer, you can access the Informatica Customer Portal site at http://mysupport.informatica.com. The site contains product information, user group information, newsletters, access to the Informatica customer support case management system (ATLAS), the Informatica How-To Library, the Informatica Knowledge Base, the Informatica Multimedia Knowledge Base, Informatica Product Documentation, and access to the Informatica user community.

Informatica Documentation

The Informatica Documentation team takes every effort to create accurate, usable documentation. If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com. We will use your feedback to improve our documentation. Let us know if we can contact you regarding your comments.

The Documentation team updates documentation as needed. To get the latest documentation for your product, navigate to Product Documentation from http://mysupport.informatica.com.

Informatica Web Site

You can access the Informatica corporate web site at http://www.informatica.com. The site contains information about Informatica, its background, upcoming events, and sales offices. You will also find product and partner information. The services area of the site includes important information about technical support, training and education, and implementation services.

Informatica How-To Library

As an Informatica customer, you can access the Informatica How-To Library at http://mysupport.informatica.com. The How-To Library is a collection of resources to help you learn more

about Informatica products and features. It includes articles and interactive demonstrations that provide solutions to common problems, compare features and behaviors, and guide you through performing specific real-world tasks.

Informatica Knowledge Base

As an Informatica customer, you can access the Informatica Knowledge Base at http://mysupport.informatica.com. Use the Knowledge Base to search for documented solutions to known technical issues about Informatica products. You can also find answers to frequently asked questions, technical white papers, and technical tips. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team through email at KB_Feedback@informatica.com.

Informatica Multimedia Knowledge Base

As an Informatica customer, you can access the Informatica Multimedia Knowledge Base at http://mysupport.informatica.com. The Multimedia Knowledge Base is a collection of instructional multimedia files that help you learn about common concepts and guide you through performing specific tasks. If you have questions, comments, or ideas about the Multimedia Knowledge Base, contact the Informatica Knowledge Base team through email at KB_Feedback@informatica.com.

Informatica Global Customer Support

You can contact a Customer Support Center by telephone or through the Online Support. Online Support requires a user name and password. You can request a user name and password at http://mysupport.informatica.com.

Use the following telephone numbers to contact Informatica Global Customer Support:

North America / South America	Europe / Middle East / Africa	Asia / Australia
Toll Free Brazil: 0800 891 0202 Mexico: 001 888 209 8853 North America: +1 877 463 2435 **Standard Rate** North America: +1 650 653 6332	**Toll Free** France: 00800 4632 4357 Germany: 00800 4632 4357 Israel: 00800 4632 4357 Italy: 800 915 985 Netherlands: 00800 4632 4357 Portugal: 800 208 360 Spain: 900 813 166 Switzerland: 00800 4632 4357 or 0800 463 200 United Kingdom: 00800 4632 4357 or 0800 023 4632 **Standard Rate** France: 0805 804632 Germany: 01805 702702 Netherlands: 030 6022 797	**Toll Free** Australia: 1 800 151 830 New Zealand: 1 800 151 830 Singapore: 001 800 4632 4357 **Standard Rate** India: +91 80 4112 5738

CHAPTER 1

Installation

This chapter includes the following topics:

Overview

RTAM is a web application that runs inside Apache Tomcat, Oracle WebLogic Server, IBM WebLogic Application Server, or JBoss. RTAM can be installed on its own server or within the same Tomcat or WebLogic Server as other Agent Logic products, such as RulePoint Installation Steps.

The following installation steps assume that you have reviewed and successfully set up a system environment that meets the recommended requirements as specified in Software Requirements (on page 16). Follow the steps below to install and configure RTAM:

1. Set up your Application Server
2. Deploy your Database Server
3. Define RTAM Authentication Mechanism
4. Test your RTAM Installation

RTAM System Requirements

Software Requirements

Software	Supported Versions
Database Server	- Oracle 11.1 - Oracle 10.2.0.1 - MySQL Enterprise Server 5.0.45 - Microsoft SQL Server 2008 R2 - IBM DB2 9.5.5 or IBM DB2 9.7
Web Application Server	- Apache Tomcat 5.0.28 **Tip:** Informatica provides a binary distribution of Tomcat. You can install this distribution, or you can use your own installation. **Important:** RTAM has not been certified with Tomcat 5.5 - Apache Tomcat 6.0.16 - Oracle WebLogic Server 10*g* - IBM WebSphere Application Server 7.0 - JBoss AS 4.0
Java Virtual Machine	- JRockit 1.5.0 (Oracle WebLogic) - JDK 1.5.0-21 - JDK 1.6 or later

Recommended Hardware Requirements

Recommended Hardware
x86/x64 (Intel, AMD-compatible) Xeon equivalent or better, 1.7-Ghz minimum CPU.
12-16 GB RAM
5-10 GB application disk space
1 GB (preferred) Ethernet network connection

Minimum Hardware Requirements

Minimum Hardware
x86/x64 (Intel, AMD-compatible) Xeon equivalent or better, 1.7-Ghz minimum CPU
2 GB RAM
1 GB application disk space
100 Mbps (Gigabit) Ethernet network connection

Supported Server Operating Systems

Supported Server Operating Systems
Microsoft Windows Server 2003 (32-bit and 64-bit)
Oracle Solaris 10 x86 (64-bit)
Red Hat Enterprise Linux AS Version 4 (32-bit and 64-bit)
SUSE Linux Enterprise Server 11 (32-bit and 64-bit)
IBM AIX Version 6.1 (64-bit),

Supported Client Operating Systems

Supported Client Operating Systems
Microsoft Windows 7 (32-bit and 64-bit)
Microsoft Windows XP Professional with Service Pack 2 or Service Pack 3 (32-bit)
Microsoft Windows 2008 R2 (32-bit and 64-bit)
Microsoft Windows 2003 (32-bit and 64-bit)

Supported JDBC Drivers

Real-Time Alert Manager supports the following JDBC drivers when connecting to a third-party database for Real-Time Alert Manager's data store:

JDBC Drivers
MySQL 5.1.6
Oracle thin client JDBC 10.2.0.1.0
jTDS version 1.2.2
IBM db2jcc version 3.58.82 (Supported with DB2 9.5.5 and 9.7.)

Supported Client Web Browsers

Supported Client Web Browsers
Internet Explorer, versions 6, 7, and 8
Mozilla Firefox, version 3.6

Recommended Screen Resolution

The recommended screen resolution for browsers is 1280 x 1024. The minimum screen resolution for browsers is 1024 x 768.

RTAM Application Servers

This release of RTAM is certified on the following application servers:

"Apache Tomcat 5.0.28/6.0.16" on page 10

"RTAM on JBOSS 4.2.3" on page 13

"RTAM on Oracle WebLogic Server 10" on page 14

"RTAM on IBM WebSphere Application Server 7.0" on page 16

Apache Tomcat 5.0.28/6.0.16

To install RTAM in Tomcat, you must complete the following steps:

"Preparing Tomcat for Real-Time Alert Manager Installation" on page 10

"Set the Environment Variables" on page 12

"Installing RTAM on Tomcat" on page 12

Configure Security Authentication

Start Tomcat

Before You Begin

Before you begin installation, confirm the following details:

- Tomcat is installed properly.
- A minimum of 1 GB of free RAM is available for use by RTAM.
- For Tomcat, verify that the following directory exists:

  `%CATALINA_HOME%\temp`

  If it does not exist, you must create the temp directory.

Note: RTAM does not support the use of multiple instances of Tomcat, that is multiple CATALINA_BASE configurations.

Preparing Tomcat for Real-Time Alert Manager Installation

Assumes Tomcat is properly installed and running.

1. Open the `setenv.bat` command file (Windows) or `setenv.sh` script (Unix) located in the following directory: `%CATALINA_HOME%\bin`

   Note: If the setenv file does not exist, you must create it.
2. In `setenv`, edit the `CATALINA_OPTS` variable as follows:

Note: These configuration settings were formatted on multiple lines for legibility but actual file content must be in a single line with no carriage return.

Windows

```
CATALINA_OPTS= -server -Xms64m -Xmx2048m
-XX:MaxPermSize=256m
-XX:+HeapDumpOnOutOfMemoryError
-Djava.awt.headless=true
-Dfile.encoding=UTF-8
```

Unix

```
CATALINA_OPTS="-server -Xms64m -Xmx2048m
-XX:MaxPermSize=256m
-XX:+HeapDumpOnOutOfMemoryError
-Djava.awt.headless=true
-Dfile.encoding=UTF-8"
```

Note: In these examples, the Xmx memory setting is based on the minimum recommended amount of 2 GB (2048 MB) of free physical memory (RAM) installed on the server. Depending on your environment, application usage, and the amount of free RAM installed, you may need to increase this setting. For more information about how to increase the maximum amount of allocated memory, see the Apache Tomcat or Oracle WebLogic product documentation.

3. If you are using Tomcat 5.0.28 (not 6.0), complete the following steps:
   a. Create an `archive` folder in the following directory:

      ```
      %CATALINA_HOME%\common\endorsed
      ```

   b. Move `xercesImpl.jar` and `xml-apis.jar` from `endorsed` folder to the `archive` folder that you created.
4. Locate and open the server.xml file in the following directory:

   ```
   %CATALINA_HOME%\conf
   ```

5. In the server.xml file, locate the SSL Coyote HTTP/1.1 Connector section and add the following line:

   ```
   URIEncoding="UTF-8"
   ```

   For example, if you are using port 80 for the Tomcat 5.0 connector, the entry for the coyote HTTP/1.1 Connector would look like the following:

   ```
   <Connector port="80"
   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" redirectPort="8443" acceptCount="100"
   debug="0" connectionTimeout="20000"
   disableUploadTimeout="true"
   URIEncoding="UTF-8" />
   ```

   Note: The Tomcat Connector may be different for each version of Tomcat. Make sure to get the proper Connector for the version of Tomcat that you are using.

   If you are using the Tomcat 6.0 connector:

   ```
   <Connector port="8080" protocol="HTTP/1.1"
                  connectionTimeout="20000"
                  redirectPort="8443" URIEncoding="UTF-8" />
   ```

6. In the server.xml file, add the following text as the last context prior to the </Host> tag:

   ```
   <Context path="/RTAM" docBase="RTAM" reloadable="true">
       <Manager className="org.apache.catalina.session.
           PersistentManager" saveOnRestart="false"/>
   </Context>
   ```

7. (Optional) If you would like to be taken directly to the RTAM login page when you enter the URL for your Tomcat instance, see "Redirecting the Landing Page" on page xx.

Set the Environment Variables

Set CATALINA_HOME

Set the operating system environment variable CATALINA_HOME to the installation location of your Tomcat instance. For example: `CATALINA_HOME="C:\Program Files\jakarta-tomcat-5.0.28"`

Set JAVA_HOME

Set the operating system environment variable JAVA_HOME to the installation location of the JDK. For example: `JAVA_HOME="C:\Program Files\Java\jdk1.5.0_12"`

Installing RTAM on Tomcat

Assumes Tomcat is installed and running properly.

Informatica will provide you with a CEP_RTAM_[version].zip file that contains the RTAM software.

1. Stop Tomcat.
2. Extract the AL_RTAM_[version].zip file to the following location: `%CATALINA_HOME%\webapps`

   This directory is created: `%CATALINA_HOME%\webapps\RTAM`.

   Note: For Unix/Linux environments only: When installing RTAM on Unix or Linux environments take care to ensure that the "RTAM" webapp file structure is owned by the same user that will be running it. Alternately, if changing file/directory ownership is not desired you can set "world write" permissions recursively through the entire "RTAM" web application file structure. This is recommended because new directories are created the first time RTAM is started and, if they cannot be created, RTAM may fail to start properly.
3. Configure security authentication.

   Note: For Unix/Linux environments only: When installing RTAM on Unix or Linux environments take care to ensure that the "RTAM" webapp file structure is owned by the same user that will be running it. Alternately, if changing file/directory ownership is not desired one can set "world write" permissions recursively through the entire "RTAM" web application file structure. This is recommended because new directories are created the first time RTAM is started and, if they cannot be created, RTAM may fail to start properly.

   For security authentication, RTAM does not have to match how RulePoint authentication has been configured. However, if you choose to do so, you can connect to either of the following:

   - RulePoint's third-party MySQL or Oracle database using JDBC
   - A Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server
4. Change how GET parameters are interpreted by Tomcat .

   To change how GET parameters are interpreted by Tomcat, you have to set the `useBodyEncodingForURI` attribute on the `<Connector>` element in `%CATALINA_HOME%\conf\server.xml`to `true`. This will cause the Connector to use the request body's encoding for GET parameters.
5. Start Tomcat.

   The RTAM web application starts. Log into RTAM in your web browser.

Manage RTAM in Tomcat

You can manage the RTAM web application, including how to start and stop the RTAM web application, within Tomcat using the Tomcat Manager. For information about using the Tomcat Manager, see the following URLs:

`http://tomcat.apache.org/tomcat-5.5-doc/manager-howto.html`

-or-

`http://tomcat.apache.org/tomcat-6.0-doc/manager-howto.html`

Start RTAM at Boot

For Tomcat and RTAM to automatically startup at boot, Tomcat must be installed as a Service (Windows) or as a daemon (Unix within the rc*.d scripts). For more information about configuring Tomcat as a Service or daemon, see the following URL:

`http://tomcat.apache.org/tomcat-5.5-doc/setup.html`

-or-

`http://tomcat.apache.org/tomcat-6.0-doc/setup.html`

RTAM on JBOSS 4.2.3

This installation process assumes that you have properly installed the JBOSS server. Please consult the vendor's installation documentation if necessary. A minimum of 1 GB of free RAM is available for use by RTAM.

Before proceeding make sure you have set the JBOSS_HOME environment variable as specified in the JBoss documentation. The JBOSS_HOME environment variable gets set to the root directory of the jboss installation.

Installing RTAM on JBoss 4.2.3

Assumes JBoss 4.2.3 is installed and working properly.

1. In the `<JBOSS_HOME>/server` directory, create a new directory called informatica.

   A new directory `JBOSS_HOME>/server/informatica` is created.

2. Copy all of the contents from `<JBOSS_HOME>/server/minimal` into the new `<JBOSS_HOME>/server/informatica` directory.

3. Copy `jboss-web.deployer` from `<JBOSS_HOME>/server/default/deploy` to `<JBOSS_HOME>/server/informatica/deploy`.

4. Copy `login-config.xml` from `<JBOSS_HOME>/server/default/conf` to `<JBOSS_HOME>/server/informatica/conf`.

5. Copy the following .jar files from `<JBOSS_HOME>/server/default/lib` to `<JBOSS_HOME>/server/informatica/lib`:
   el-api.jar

   jboss.jar

   jboss-ejb3x.jar

   jboss-j2ee.jar

   jboss-management.jar

   jbosssx.jar

   jbossws-common.jar

   jbossws-framework.jar

   jbossws-jboss42.jar

   jbossws-spi.jar

   jnpserver.jar

   jsp-api.jar

log4j.jar

servlet-api.jar

6. Open the following file for editing : <JBOSS_HOME>/server/informatica/deploy/jboss-web.deployer/META-INF/jboss-service.xml. Delete the following <depends> statements:

```
<depends>jboss:service=TransactionManager</depends>
<depends>jboss.jca:service=CachedConnectionManager</depends>
```

7. Open the following file for editing: <JBOSS_HOME>/server/informatica/deploy/jboss-web.deployer/META-inf/jboss-service.xml. Paste the following <mbean> xml elements into the document.

```
<mbean code="org.jboss.security.plugins.SecurityConfig"
   name="jboss.security:service=SecurityConfig">
   <attribute name="LoginConfig">jboss.security:service=XMLLoginConfig</attribute>
</mbean>
<mbean code="org.jboss.security.auth.login.XMLLoginConfig"
   name="jboss.security:service=XMLLoginConfig">
   <attribute name="ConfigResource">login-config.xml</attribute>
</mbean>
<!-- JAAS security manager and realm mapping -->
<mbean code="org.jboss.security.plugins.JaasSecurityManagerService"
   name="jboss.security:service=JaasSecurityManager">
   <attribute name="ServerMode">true</attribute>
   <attribute
name="SecurityManagerClassName">org.jboss.security.plugins.JaasSecurityManager</
attribute>
   <attribute name="DefaultUnauthenticatedPrincipal">anonymous</attribute>
   <attribute name="DefaultCacheTimeout">1800</attribute>
   <attribute name="DefaultCacheResolution">60</attribute>
   <attribute name="DeepCopySubjectMode">false</attribute>
</mbean>
```

8. Open the following file for editing: `<JBOSS_HOME>/server/informatica/deploy/jboss-web.deployer/server.xml` and remove the following xml fragment for the `CachedConnectionValve`.

```
<Valve className="org.jboss.web.tomcat.service.jca.CachedConnectionValve"
cachedConnectionManagerObjectName="jboss.jca:service=CachedConnectionManager"
transactionManagerObjectName="jboss:service=TransactionManager"/>
```

9. On windows update `<JBOSS_HOME>/bin/run.bat` for the new memory and `permGen` settings. Find and edit the line below as follows:

```
set JAVA_OPTS=%JAVA_OPTS% -Xms512m -Xmx1024m -XX:PermSize=128m -XX:MaxPermSize=256m -
XX:+HeapDumpOnOutOfMemoryError
```

10. Copy the RTAM webapp to `<JBOSS_HOME>/server/informatica/deploy`. If the webapp is deployed as a folder. You will need to rename the folder to `RTAM.war`.

    The server is set up.

11. Start up the server

    Note: For Unix/Linux environments only: When installing RTAM on Unix or Linux environments take care to ensure that the "RTAM" webapp file structure is owned by the same user that will be running it. Alternately, if changing file/directory ownership is not desired one can set "world write" permissions recursively through the entire "RTAM" web application file structure. This is recommended because new directories are created the first time RTAM is started and, if they cannot be created, RTAM may fail to start properly.

RTAM on Oracle WebLogic Server 10

It is assumed that you have properly installed the WebLogic 10 server and that the system has at least 1 GB of RAM allocated for RTAM.

To install RTAM in WebLogic Server, you must complete the following steps:

- Create a New Domain in WebLogic Server

- Prepare WebLogic Server for RTAM Installation
- Install the RTAM Software
- Configure Security Authentication
- Deploy the RTAM Application

Before You Begin

Before you begin, confirm the following details:

- WebLogic Server is installed properly.
- A minimum of 1 GB of free RAM is available for use by RTAM.

Preparing WebLogic to Install RTAM

The WebLogic server is installed and you have created an Informatica domain for RTAM.

1. Open the `setDomainEnv.cmd` (Windows) or `setDomainEnv.sh` script (Unix) located in the following directory: `[WebLogicInstallDir]\user_projects\domains\informatica\bin`
2. In setDomainEnv, edit the MEM_ARGS variable as follows to provide an appropriate amount of application memory. For Windows: `set MEM_ARGS= -Xms256M -Xmx2048M` for Unix: `MEM_ARGS="-Xms256M -Xmx2048M"`

   Note: In these examples, the Xmx memory setting is based on the minimum recommended amount of 2 GB (2048 MB) of free physical memory (RAM) installed on the server. Depending on your environment, application use, and the amount of free RAM installed, you may need to increase this setting. For more information about how to increase the maximum amount of allocated memory, see the Apache Tomcat or BEA Weblogic product documentation.

Installing RTAM on WebLogic 10

Assumes WebLogic 10 is installed and running properly.

Informatica will provide you with a CEP_RTAM_[version].zip file that contains the RTAM software.

1. Stop the WebLogic Server.

   Tomcat is not running.
2. Extract the AL_RTAM_[version].zip file to the following location: `[WebLogicInstallDir]\user_projects\domains\informatica`

   Note: When extracting this file, be sure to enable the appropriate option in your uncompress utility to ensure that it preserves the folder structure.

   This directory is created: `[WebLogicInstallDir]\user_projects\domains\informatica\RTAM`
3. Configure Security Authentication

   Your RTAM security configuration does not have to match how RulePoint authentication has been configured. When RulePoint is configured using local authentication, you can choose to use RulePoint's third-party MySQL, SQL Server or Oracle database using JDBC or an external Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server for RTAM.

4. Deploy the RTAM Application

   a. Start the WebLogic Server for the agentlogic domain:
   In Windows, click Start > Programs > BEA Products > User Projects > Informatica > Start Admin Server for Weblogic Server Domain.
   In Unix, run the `[WebLogicInstallDir]/user_projects/domains/agentlogic/startWebLogic.sh` script using the following command: `./startWebLogic.sh`.

   b. To log into the Administrator Console for that domain, see the following URL: http://[AdminServerConsole]:7001/console, and then complete the following fields using the username and password for your WebLogic Server: Username: [WebLogicUsername] , Password: [WebLogicPassword]

5. Deploy RTAM into the agentlogic domain using all of the default configuration settings except Deployment Order. If you are also installing RulePoint, the RTAM Deployment Order value should be set to a number lower than the RulePoint Deployment Order value.
   For example, if the RulePoint Deployment Order is set to 101, the RTAM Deployment Order should be set to 100, which is the default setting, so that RTAM deploys before RulePoint.

   Note: For Unix/Linux environments only: When installing RTAM on Unix or Linux environments take care to ensure that the "RTAM" webapp file structure is owned by the same user that will be running it. Alternately, if changing file/directory ownership is not desired one can set "world write" permissions recursively through the entire "RTAM" web application file structure. This is recommended because new directories are created the first time RTAM is started and if they cannot be created, RTAM may fail to start properly.

6. Start WebLogic 10

   The RTAM web application starts. Log into RTAM in your web browser.

Manage RTAM in WebLogic

You can manage the RTAM web application, including how to start and stop the RTAM web application, within the WebLogic Server using the Administration Console.

For information about using the Administration Console in WebLogic Server, see the following URL: https://docs.oracle.com/cd/E13222_01/wls/docs81/ConsoleHelp/console.html

Start RTAM at Boot

You can configure WebLogic Server and RTAM to automatically startup at boot using the WebLogic Server Node Manager. For information about using Node Manager in WebLogic Server, see the following URL: https://docs.oracle.com/cd/E13222_01/wls/docs81/adminguide/nodemgr.html

RTAM on IBM WebSphere Application Server 7.0

These instructions assume that you have properly installed WebSphere 7.0 with a minimum of 1 GB of RAM available for use by RTAM. We recommend that you use a staging environment outside of your production server to properly configure and repackage the RTAM zip file into a WAR file.

Deploying RTAM on WebSphere includes the following steps:

1. Use a Staging Environment to repackage RTAM.
2. Prepare WebSphere Application Server for RTAM Installation.
3. Install the RTAM WAR Application.
4. Configure RTAM Authentication.
5. Set Up the RTAM Database.

6. Configure RTAM for Optimization.
7. Start WebSphere.

Preparing WebSphere to Install WebSphere

1. Open the WebSphere application server administrative console. For example, if you are using the default installation, this will be at: `http://<server>:9060/ibm/console`
   Enter the administrator user ID and password.
2. Go to **Servers > Server Types > WebSphere** application servers. Click the server where you are installing RTAM. In the default install, this will be server1.
3. Under Server Infrastructure, select **Java** and **Process Management > Process Definition**.
4. Under Additional Properties, select Java Virtual Machine. Set the following JVM properties:
   Initial heap size: 256

   Maximum heap size: 1024

   Generic JVM arguments: -XX:PermSize=192m - XX:MaxPermSize=256m
5. Click **Apply** and then click **OK**.
6. Click **Save** to update the master configuration.

Installing the RTAM WAR on WebSphere

1. Open the WebSphere application server administrative console. If you are using the default installation, this will be at: `http://<server>:9060/ibm/` console. Enter the administrator user ID and password.
2. Create a new Enterprise Application server within WebSphere.
3. Using the remote file system browser option, browse and select the `RTAM.war` file created in the previous steps, then click **Next**,
4. Select **Fast Path** and click on **Next**.
   Directory to install application (example for Windows):

   ```
   e:\Program Files\IBM\WebSphere\AppServer\
   ```

   ```
   profiles\AppSrv01\installedApps\DVW2K8-WAS70Node01Cell
   ```

   Change Application Name to `rtam`
5. Select the RTAM web module and the appropriate virtual host (in the default installation, this will be default_host) and click **Next**.
6. Change the Context Root to /rtam and click **Next**,
7. Review the summary and click **Finish**.
8. Click **Save** to update the master configuration.
   You do not start RTAM at this time.
9. Configure RTAM Authentication for WebSphere

   If you want to use an authentication provider other than the RTAM database or any authentication method other than Form, you must configure RTAM authentication before starting the WebSphere application server.
10. Set Up the RTAM Database

    You must set up a database to be used with your RTAM application. If you do not set up a database, the RTAM application will not start.
11. Configure RTAM for Optimization

You can further configure RTAM to optimize its performance. To do so, you edit the properties in the rtam-config.properties configuration file. You can also configure the logging for RTAM using the log4j.xml file.

12. Start RTAM

    Open the WebSphere Application Server administrative console. If you are using the default installation, this will be at `http://<server>:9060/ibm/console`. Enter the administrator user ID and password. Then go to **Applications > WebSphere enterprise applications** and click **Start**.

Manage RTAM on WebSphere

You can manage the RTAM web application, including how to start and stop the RTAM web application, within the WebSphere application server using the WebSphere application server administrative console. If you are using the default installation, this will be at `http://<server>:9060/ibm/console`.

RTAM Database Servers

Before starting RTAM for the first time, you must create a MySQL 5.0.45, Oracle 11, Oracle 10.2.0, SQL Server 2008 or DB2 9.5.5 database named “rtam” and a rtam database user account. To create and set up this database, follow these steps:

- Create Database Admin and User Accounts
- Modify the Database Configuration Files
- Create the Database and Database tables

Create Database Admin and User Accounts

The RTAM database must be created using a database administrator account with the following privileges:

- Ability to create database objects
- Read/Write access

This account and its associated password are referred to in this guide as the [DBAdminUsername] and the [DBAdminPassword]. The RTAM database user account must have access to all of the tables in the RulePoint database as well as the following privileges for those tables:

- Select
- Write
- Update
- Delete

This account and its associated password are referred to in this guide as the [DBUsername] and the [DBPassword].

Note: Make sure to make note of the username and password for both of these accounts as they will be needed when setting up your database.

Creating RTAM Database and Tables in MySQL 5.0.45

1. Verify that the bin folder in the MySQL Server installation location folder is on the system path.

2. Open a command prompt and execute the commands as shown in the following example in the order shown, where [DBAdminUsername] and [DBAdminPassword] are the username and password for the database administrator account used to create the database, and [DBUsername] and [DBPassword] are the username and password for the RTAM database user account. For example,

```
[root@localhost]# mysql -uroot -prootpassword
mysql> create database rtam;
OR for UTF8 characters support;
mysql> create database rtam DEFAULT CHARACTER SET utf8;

mysql> grant all privileges on rtam.* to [DBUserName] identified by ['DBPassword']
with grant option;
mysql> exit;

[root@localhost]# cd [RTAMHome]\WEB-INF\db\sql\mysql

[root@localhost]# mysql -u[DBAdminUserName] -p[DBAdminPassword] rtam <tables-
default.sql

OR for UTF8 characters support;

[root@localhost]# mysql -u[DBAdminUserName] -p[DBAdminPassword] rtam <tables-utf8.sql
```

Creating RTAM Database and Tables in Oracle (11 or 10.2)

1. Start SQLPlus with the proper administrative privileges.
2. Open a command prompt and execute the commands as shown in the following example, in the order shown, where [TableSpaceName] is the name of your Oracle tablespace, [OracleTableSpaceDataDir] is the Oracle directory containing the table space, and [DBUsername] and [DBPassword] are the username and password for the database user account. For example,

```
CREATE TABLESPACE YourTableSpace DATAFILE 'c:\ORACLE\10.2\ORADATA
\YourTableSpace.DBF' SIZE 500M;

CREATE USER dbuser IDENTIFIED BY dbuserpassword DEFAULT TABLESPACE YourTableSpace
QUOTA UNLIMITED ON
     YourTableSpace;

GRANT CONNECT, RESOURCE TO dbusername;

REVOKE UNLIMITED TABLESPACE FROM dbusername;

GRANT CREATE SESSION, CREATE TABLE TO dbusername;

EXIT;
```

3. Test your connection to Oracle using the [DBUsername] and [DBPassword] using the following command:

```
[DBUsername]/[DBPassword]@[DBHostName]
```

4. If Oracle is installed to use UTF-8, read the `tables-UTF8.sql` file into Oracle using the following command:

```
[DBUsername]/[DBPassword]@[DBHostName] < [RTAMHome]\WEB-INF\db\sql\oracle10\tables-
UTF8.sql
```

   or If Oracle is installed to use non-UTF-8, read the `tables-default.sql` file into Oracle using the following command

```
[DBUsername]/[DBPassword]@[DBHostName] < [RTAMHome]\WEB-INF\db\sql\oracle10\tables-
default.sql
```

Creating RTAM Database and Tables in IBM DB2 9.5.5

Except for the parameters listed below, you can optimize the database settings and configuration based on your preferences or standard practices.

- CODESET for all tables should be UTF-8 and the Territory US.
- SYSTEM PAGE SIZE should be increased to 32KB.

1. On the operating system (OS), create a system user to own the tables, and be used by the RulePoint and RTAM applications to access the tables. For example, User Name: CEPUSER, Password:
2. Login into the operating system as the system user created in Step 1 above.
3. Connect to the DB2 server and create a database and table space for RTAM using the following command:

   ```
   CREATE DATABASE rtam AUTOMATIC STORAGE YES ON '[C:]\' DBPATH ON '[C:]\' USING
   CODESET UTF-8
   TERRITORY US COLLATE USING SYSTEM PAGESIZE 32768;
   ```

   Note: The file system storage locations and settings will need to be altered based on you environment. You may need to make additional changes to the internal database standards or change other database preferences. The key settings are that the code set is utf-8, and the system page size is 32768.
4. Connect to the RTAM database created in step 3 above and run the following RTAM script and read the tables-utf8.sql file into the DB2 server.

   ```
   [RTAMHome]\WEB-INF\db\sql\db2\tables-utf8.sql
   ```

Creating RTAM Database and Tables in Microsoft SQL Server 2008 R2

1. Login into the SQL Server Management Studio as an administrator.
2. Create a database user login account for RTAM.
   - Right-click **Security > Logins**
   - Select **New Login**
   - Enter new login name. For example, `dbuser`.
   - Select **SQL Server Authentication**

     Note: Leave the default database as Master for now. The default database will be changed shortly to the newly created database name.
   - Click **OK**.
3. Create the RTAM database
   - Right-click on **Databases**.
   - Select **New Database**.
   - Enter new login name. For example, `dbuser`.
   - Set the dbuser created in Step 2 above as owner.
   - Click **OK**.
4. Set the RTAM database as your default database.
   - Right click on the new user login created in Step 2 above.
   - Select **Properties**.
   - Change the default database to the one you just created in Step 3 above.

- Click **OK**

5. Test your database connection.

RTAM Authentication

When users log in to RTAM, the user's credential is authenticated using the authentication provider (whether local or external) and mechanism configured for this implementation. Every user authenticated is granted full access to the application.

By default, RTAM authenticates users using the RulePoint database as the provider and Form authentication as the mechanism. In addition, you can configure RTAM to authenticate using the RulePoint database as the provider with Basic authentication as the mechanism, or using an external authentication server as the provider and Basic, Form, or PKI for Public Key Infrastructure (X.509 client certificates) authentication as the mechanism.

Note: RTAM supports only standard LDAP constructs.

Options

The following table provides you with an overview of the possible choices for configuring authentication in RTAM:

Authentication options		
	Mechanism	
Provider	Basic	Form
RTAM database	X	X[1]
Lightweight Directory Access Protocol (LDAP) Server	X	X
Microsoft Active Directory (AD) via LDAP	X	X
X.509	n/a	n/a

1. Using the RulePoint database with Form authentication is the default configuration.

Note: RTAM does not support changing authentication providers after you have configured and begun using RTAM. To change authentication providers, you must drop the RTAM database and re-configure the external authentication server. Not all authentication mechanisms can be applied to all authentication provider directories, and supported options might also differ by container. For more information, see your authentication provider documentation.

Choose a Default Authentication Provider

RTAM supports three other authentication providers other than the default RTAM RulePoint database authentication and Form authentication as the mechanism. To change the default authentication, you can select one of three options

- If you are configuring RTAM to use LDAP, you must edit the contextConfigLocation property in the web.xml file located in the [RTAMHome]\WEB-INF\folder to read as follows:

```
<context-param>
        <param-name>contextConfigLocation</param-name>
        <param-value>
            /WEB-INF/classes/spring-context.xml
            /WEB-INF/classes/security-ldap.xml
        </param-value>
    </context-param>
```

- If you are configuring RTAM to use OpenLDAP, you must edit the contextConfigLocation property in the web.xml file that is located in the [RTAMHome]\WEB-INF\ folder to read as follows:

```
<context-param>
        <param-name>contextConfigLocation</param-name>
        <param-value>
            /WEB-INF/classes/spring-context.xml
            /WEB-INF/classes/security-openldap.xml
        </param-value>
    </context-param>
```

- If you are configuring RTAM to use X509, you must edit the contextConfigLocation property in the web.xml file that is located in the [RTAMHome]\WEB-INF\ folder to read as follows:

```
<context-param>
        <param-name>contextConfigLocation</param-name>
        <param-value>
            /WEB-INF/classes/spring-context.xml
            /WEB-INF/classes/security-X509.xml
        </param-value>
    </context-param>
```

Configure Authentication Provider

After selecting the authentication provider to use, you need to edit the rtam-config.properites file to identify the location and the relevant login credentials of the selected authentication provider . If you are configuring RTAM to use RulePoint for authentication, you must edit the RulePoint internal authentication setting in the rtam-config.properties file to match the login credentials provided by RulePoint to its security provider; and copy the appropriate jdbc driver for the RulePoint database into the [RTAMHome]\WEB-INF\lib\ folder. Provide the database credential to connect to the RulePoint database.

This example is for the Oracle 11 or Oracle 10.2.0.1 database server:

```
auth.db.name=[SID]
auth.db.username=[RulePointDBuserName]
auth.db.password=[RulePointDBuserPassword]
auth.db.driver.class=oracle.jdbc.OracleDriver
auth.db.url_base=jdbc:oracle:thin:@[OracleServerName]:[port]:
[OracleInstanceName]
auth.db.url=${auth.db.url_base}${auth.db.name}
```

Note: For Oracle only the auth.db.name is left blank.

For MySQL 5.0.45, use the following database credential:

```
auth.db.name=[RulePointDBName]
auth.db.username=[RulePointDBuserName]
auth.db.password=[RulePointDBuserPassword]
auth.db.driver.class=com.mysql.jdbc.Driver
auth.db.url_base=jdbc:mysql://[HostName]:[port]/
auth.db.url=${auth.db.url_base}${auth.db.name}
```

For SQL Server 2008, use the following database credential:

```
auth.db.name=[RulePointDBName]
auth.db.username=[RulePointDBuserName]
auth.db.password=[RulePointDBuserPassword]
auth.db.driver.class=net.sourceforce.jtds.jdbc.Driver
auth.db.url_base=jdbc:jtds:sqlserver://[HostName]:[port]/auth.db.url=${auth.db.url_base}$
{auth.db.name}
```

For DB2 9.5.5, use the following database credential:

```
auth.db.name=[RulePointDBName]
auth.db.username=[RulePointDBuserName]
auth.db.password=[RulePointDBuserPassword]
auth.db.driver.class=com.ibm.db2.jcc.DB2Driver
auth.db.url_base=jdbc:db2://[hostname]:[port]/
auth.db.url=${auth.db.url_base}${auth.db.name}
```

Get the JDBC database driver file specified in the previous step and copy it to the following location:

```
[RTAMHome]\WEB-INF\lib\
```

If you are using the Microsoft Active Directory (standard LDAP) for authentication, the following sample configuration properties would be used.

```
ldap.provider.url=
ldap.user.search.base=
ldap.user.search.filter=sAMAccountName={0}
ldap.group.search.base=
ldap.role.default=ROLE_USER
ldap.role.search.subtree=true
ldap.role.prefix=ROLE_EXT_
ldap.role.convert.touppercase=true
ldap.user.default=
ldap.password.default=
ldap.group.search.filter=
ldap.group.role.attribute=memberOf
ldap.username.format={0}@
```

Note: Some of the properties listed above may not be required to connect to your authentication provider. For your specific configuration settings, please see your LDAP administrators for details.

If you are using open LDAP for authentication, the following sample configuration properties would be used.

```
ldap.provider.url=ldap://
ldap.user.search.base=
ldap.user.search.filter=(uid={0})
ldap.group.search.base=
ldap.group.search.filter=(&(objectClass=groupofuniquenames)(uniqueMember={0}))
ldap.group.role.attribute=
ldap.role.default=ROLE_USER
ldap.role.search.subtree=true
ldap.role.prefix=ROLE_EXT_
ldap.role.convert.touppercase=true
ldap.username.format={0}@
ldap.user.default=
ldap.password.default=
```

Some of the properties listed above may not be required to connect to your authentication provider. For your specific configuration settings, please see your LDAP administrators for details.

Configure the Group Resolver

RTAM 3.1 supports group addresses for both standard LDAP and open LDAP. The group resolver determines and resolves the individual names within the given group.

The standard LDAP group resolver is the default configuration. The properties are as follows:

```
ldapgroupresolver.url=ldap://ldapserver.mycompany.com:389
ldapgroupresolver.base=CN=Users,DC=mycompany,DC=com
ldapgroupresolver.userDn=user1@mycompany.com
ldapgroupresolver.userPwd=xXxXxXxXxX
ldapgroupresolver.baseFilter=
ldapgroupresolver.filter=(&(objectclass=person)
(memberOf=CN=%s,OU=Mailing List Groups,DC=mycompany,DC=com))
ldapgroupresolver.uidAttribute=sAMAccountName
ldapgroupresolver.escapeGroupIds=false
ldapgroupresolver.maxAge=3600000
```

The open LDAP group resolver is the default. The properties are as follows:

```
ldapgroupresolver.url=ldap://
ldapgroupresolver.base=
ldapgroupresolver.userDn=
ldapgroupresolver.userPwd=
ldapgroupresolver.baseFilter=
ldapgroupresolver.filter=(&(objectclass=person)(ou:dn:=%s))
ldapgroupresolver.uidAttribute=uid
ldapgroupresolver.escapeGroupIds=false
```

Assign Execute Permission for Linux or Solaris

If you are using Linux or Solaris, you must assign execute permissions before executing the StringUtil.sh script to encrypt your jdbc property values:

1. At a command prompt, change to the following directory:
   Tomcat in Unix

   ```
   $CATALINA_HOME/webapps/rtam/WEB-INF/db
   ```

   JBoss in Unix

   ```
   [JBOSSInstallDir]/[server]/informatica/deploy/RTAM.war
   ```

   WebLogic Server in Unix

   ```
   [WebLogicInstallDir]/user_projects/domains/informatica/RTAM/WEB-INF/db/
   ```

2. Add execute permissions for the StringUtil.sh script. This can be accomplished by typing either of the two following commands at the system prompt:

   ```
   # chmod u+x StringUtil.sh
   # chmod 744 StringUtil.sh
   ```

CHAPTER 2

RTAM Configuration

The configuration properties for RTAM are stored in the `rtam-config.properties` file. Editing this file enables administrators to tune RTAM system performance for their specific needs.

RTAM Configuration Properties

Core Alert Receiver Operations	
Property	**Description**
ingest.messageDurationMillis	This setting controls the length of time, in milliseconds, alert in the system are stored before being deleted. The default value is (604800000 ms), that is seven days. **Note:** This setting should be defined based on the volume of alerts that you expect to be ingested by the system. As a rule of thumb, you want to set the duration (life expectancy) of the incoming alerts low if you expect the system to ingest a high volume of alerts.
ingest.minExpirationCheckFrequency	This setting is the minimum time, in milliseconds, the system checks to delete alerts. The expiration check process operates mostly on volume: that is the number of alerts coming in. The system checks to keep database size down. But if the alert volume or rate is very low, this value guarantees the system checks at least this often.
ingest.doChannelCreation	This setting controls whether or not channels will be created for users, when alerts come in. This means if an alert arrives for a user with an associated channel that has not already been created by the user, then the system would automatically create the channel for the user and place it in their channel tree.

Core Alert Receiver Operations	
ingest.unknownRecipientLogCountInterval	This setting controls how many alerts for users that are not known to RTAM must appear, but there is an entry made in the log file indicating that the alerts were “dropped”, that is, not stored in the data store. By default, Alerts that arrive for users that do not exist, are cast-away.
ingest.groupRecipientsResolver	This setting is either NONE or LDAP. When sending alerts to the system, through RTAM or via the Send New Alert tab in RTAM, you can specify a group to receive alerts. To resolve group members address through LDAP, set this property to LDAP. To have the system ignore the associated group address, set this to NONE.

User Interface	
Property	**Description**
ui.refresh_rate	The time in milliseconds between when the UI calls back to the server to check for new alerts. Default is 10000 ms (10 seconds)
alerts.per.page	This property is for the number of alerts per page as indicated in the drop-down option menu.
priority.color.picker.colors	This property is for the number of default colors a user can select for high lighting the priority rows.
priority.colors	This is a comma delimited string of hex color values. The default value is: priority.colors=99FF99,00CC00,0000FF,FFFF00,FF9900,FF0000
languages.available	This property specifies the languages available using the language codes separated by commas. If no language choice should be available, give it no value at all. The default is en,kr.
userdefault.dateformat=EEE, d MMM yyyy	This property is the default date format that is used by the system.
userdefault.timeformat=HH:mm:ss Z	This property is the default time format for the every user.
userdefault.language=en	This property is the default language that is used by the system. It is English.
userdirectory.page.size	The page size (number of users) for the user directory. The default number is 15.

The JMS server information specifies where RTAM will go to look for new alerts or messages. The JMS broker or storage area is also used for the Send/Forward Alert to RTAM user. The jms.server.url and broker.url technically are almost always the same.

JMS Server	
Property	**Description**
jms.server.url	This is the address of the JMS server that alerts will be pulled from.

JMS Server	
broker.url	This value is to be left alone if using the embedded JMS server. If using an external JMS server, set this to the same value as the above jms.server.url.
jms.data.queue	This is the name of the JMS queue to pull alerts from.

The database connection points to the actual database responsible for storing all of the RTAM information. You either select the internal or embedded HSQL database, or set this to point to an external database.

Database Connection	
Database	**Configuration**
MySQL	hibernate.url=jdbc:mysql://localhost:3306/rtam? emulateLocators=true&useUnicode=true&characterEncoding=UTF-8 hibernate.user=rtamuser hibernate.password=ag3nt1 hibernate.driver=com.mysql.jdbc.Driver hibernate.dialect=org.hibernate.dialect.MySQL5Dialect hibernate.hbm2ddl.auto=validate
Oracle 11	hibernate.url=jdbc:oracle:thin:@localhost:1521:XE hibernate.user=rtamuser hibernate.password=ag3nt1 hibernate.driver=oracle.jdbc.OracleDriver hibernate.dialect=org.hibernate.dialect.Oracle11gDialect hibernate.hbm2ddl.auto=validate
Oracle 10	hibernate.url=jdbc:oracle:thin:@localhost:1521:XE hibernate.user=rtamuser hibernate.password=ag3nt1 hibernate.driver=oracle.jdbc.OracleDriver hibernate.dialect=org.hibernate.dialect.Oracle10gDialect hibernate.hbm2ddl.auto=validate

Database Connection	
SQL Server	hibernate.url=jdbc:jtds:sqlserver://localhost:[port]/dbname hibernate.user=rtamuser hibernate.password=ag3nt1 hibernate.driver=net.sourceforce.jtds.jdbc.Driver hibernate.dialect=org.hibernate.dialect.SQLServerDialect hibernate.hbm2ddl.auto=validate
DB2	hibernate.url=jdbc:db2://localhost:[port]/dbname hibernate.user=rtamuser hibernate.password=ag3nt1 hibernate.driver=com.ibm.db2.jcc.DB2Driver hibernate.dialect=org.hibernate.dialect.DB2Dialect hibernate.hbm2ddl.auto=validate

Database Tuning
The hibernate properties are for caching or pooling the settings that can be configured for improved performance. hibernate.c3p0.initialPoolSize=2 hibernate.c3p0.min_size=0 hibernate.c3p0.max_size=20 hibernate.c3p0.timeout=300 hibernate.jdbc.batch_size=50 hibernate.c3p0.max_statements=100 hibernate.c3p0.acquireIncrement=2 hibernate.c3p0.idleConnectionTestPeriod=300 **Note:** Please read both the C3PO and Hibernate documentation for guidance on best practices.

These properties represent the setup/configuration for the internal Lucene based indexing that allows RTAM to conduct rapid searching.

Search Indexing	
Property	**Description**
index.enabled	Set to true or false to enable or disable indexing of alerts (used for Search). The default is true.
index.batchsize	The number of alerts to index at one time for performance reasons. The default value is 100.

This section deals with RTAM internal and external authentication configuration settings. The default RTAM authentication configuration is internal set to the RulePoint database.

Internal Database Authentication	
Property	**Description**
auth.db.name	The name of the database you are using for authentication. The default is the rulepoint database.
auth.db.username	The default user name to connect for the authentication database. The default username is eesuser.
auth.db.password	The password for the default user name to connect to the authentication database. The default is password is ag3nt1.
auth.db.driverClass	This property is the default database driver class for connecting to the authentication server. The default is com.mysql.jdbc.Driver.
auth.db.url	Indicates the URL RulePoint database being used. This value should be set to the URL of your RulePoint database.

External Database Authentication (Standard /Open LDAP)	
Property	**Description**
ldap.provider.url	Indicates the URL of the LDAP provider being used. This value should be set to the URL of your LDAP provider. Typically, the LDAP provider URL consists of the three parts: - LDAP protocol prefix - ldap - LDAP server name - LDAP port - Typically 389 for non-SSL and 636 for SSL For example, ldap://ldapserver.mycompany.com:389
ldap.user.search.base	The distinguished name of the context(s) containing the users that you want to appear in RTAM. You can define any number of childless contexts, but you must define at least one. The default is CN=Users,DC=mycompany,DC=com
ldap.user.search.filter (optional)	This property is the LDAP record used to compare against the username typed into the login form. For example, john.doe is the value in John Doe's sAMAccountName field.
ldap.group.search.base (optional)	This property is similar to the user search filter except that this is searching within the security groups records, as opposed to the user records.
ldap.group.role.attribute	This property searches users LDAP record for the groups OU=Security Groups. For example, OU=Security Groups, CN=SG_rulepointusers.
ldap.role.default	This is used when an LDAP user is found that has no assigned role. This is the default user role that is assigned to them by the system.
ldap.role.search.subtree	This boolean property determines if the search should descend nodes of the trees looking for matching information. The default is true.
ldap.role.prefix	This property is to prefix for roles inside of the companies LDAP. For example, in RTAM we use ROLE_EXT_USER, ROLE_EXT_ADMIN, and so on. For example, ROLE_EXT_

External Database Authentication (Standard /Open LDAP)	
ldap.role.convert.touppercase	This property indicates to the LDAP connector to convert any role information it finds to upper case before doing the comparison. This is standard. The default setting is true.
ldap.username.format	This property indicates that the username format would be john.doe@informatica.com (or whatever domain is specified after the @). The default is {0}@.
ldap.user.default	This property is the default username to login for logging into LDAP. For example, user1@mycompany.
ldap.password.default	This property is the password for the default user. For example, xXxXxXxXxX.

RTAM 3.1 supports sending messages to groups. The resolver determines the individual members of the group to resolve the group address.

Resolver Configuration (Standard / open LDAP)	
Property	**Description**
ldapgroupresolver.url	Indicates the group URL of the LDAP provider being used. This value should be set to the URL of your LDAP provider. For example, ldap:// ldapserver.mycompany.com:389.
ldapgroupresolver.base	The distinguished name of the context(s) containing the groups that you want to appear in RTAM. For example, CN=Users,DC=mycompany,DC=com
ldapgroupresolver.userDn	This property is the user DN from which the LDAP search will be executed . For example, user1@mycompany.com.
ldapgroupresolver.userPwd	This property is the password for the default group resolver. For example, xXxXxXxXxX.
ldapgroupresolver.baseFilter	This property is the LDAP group resolver record used to compare against the group name typed into the login form.
ldapgroupresolver.filter (optional)	This property is the LDAP record used by the resolver to compare against the username typed into the login form. For example, (&(objectclass=person) (memberOf=CN=%s,OU=Mailing List Groups,DC=mycompany,DC=com)).
ldapgroupresolver.uidAttribute	This property searches group resolver record for the groups OU=Security Groups. For example, OU=Security Groups, CN=SG_rulepointusers. For example, AMAccountName.
ldapgroupresolver.escapeGroupIds	This property indicates if you want the resolver to escape the IDs of groups. The default is false.
ldapgroupresolver.maxAge	The default MaxAge for the group resolver is 3600000.

Encrypting the Configuration Property Values

You can encrypt the values in the RTAM configuration properties file.

1. Locate the rtam-config.properties file.
2. For each property value that you want to encrypt, navigate to the `[rtamHome]` directory and execute the StringUtil.bat or StringUtil.sh file.

   `StringUtil <value>`, where *value* is the password string to encrypt. For example, `StringUtil rtam50`, where `rtam50` is your unencrypted password.
3. Copy the output from the StringUtil.bat or StringUtil.sh execution.
4. In the rtam-config.properties file, replace the unencrypted value with the output from the StringUtil.bat or StringUtil.sh execution.

   For example, `db.password = +eN+TZKSK14lbWtOONiS5dcYihXkx2sCCQ5Z`
5. After inserting the encrypted passwords, modify the database configuration files for the specific databases.

If you do not want to encrypt the configuration property values,

1. Find and edit the `[rtamHome]\WEBINF\classes\spring-context.xml` file.

   Find the definition for the propertyConfigurer bean, and change its definition from:

   ```
   <bean id="propertyConfigurer"
   class="com.agentlogic.rtam.common.StringUtilConfigu
   rer"> <property name="location"><bean
   class="org.springframework.core.io.ClassPathResourc
   e"> <constructor-arg><value>rtamconfig.
   properties</value></constructor-arg>
   </bean>
   </property>
   </bean>
   ```

   to:

   ```
   <context:property-placeholder
   location="classpath:rtam-config.properties" />
   ```
2. Find and edit the `[rtamHome]\WEBINF\classes\hibernate.xml` file.

   Find the definition for the propertyConfigurer bean, and change its definition from:

   ```
   <bean id="propertyConfigurer"
   class="com.agentlogic.rtam.common.StringUtilConfigu
   rer"> <property name="location"><bean
   class="org.springframework.core.io.ClassPathResourc
   e"> <constructor-arg>
   <value>rtam-config.properties</value>
   </constructor-arg></bean> </property>
   </bean>
   ```

   to:

   ```
   <context:property-placeholder
   location="classpath:rtam-config.properties" />
   ```

CHAPTER 3

RTAM Logging

RTAM logs messages using log4j, which is a framework for logging application debugging messages. You configure this framework to control where and in what format RTAM logs messages.

With log4j, it is possible to enable logging at runtime without modifying the application binary. The log4j package is designed so that these statements can remain in shipped code without incurring a heavy performance cost. Logging behavior can be controlled by editing a configuration file without touching the application binary. You configure log4j for RTAM using the log4j.xml file.

For information about configuring log4j for Tomcat, see the following URLs:

- Main documentation page: `http://logging.apache.org/log4j/docs/documentation.html`
- Short introduction to log4j: `http://logging.apache.org/log4j/docs/manual.html`
- log4j Wiki page: `http://wiki.apache.org/logging-log4j/Log4JProjectPages`

For detailed log4j documentation for WebLogic Server, see the following URL: `http://e-docs.bea.com/wls/docs100/logging/config_logs.html`

log4j.properties File

The log4j.xml configuration file resides in the following location:

```
[RTAMHome]\WEB-INF\log4j.xml
```

Default Loggers

The following is a list of the default loggers currently defined for RTAM:

```
### set log levels - for more verbose logging change 'warn' to 'debug' ###
log4j.rootLogger=warn, stdout, file
log4j.logger.com.agentlogic.rtam=warn
log4j.logger.org.apache.activemq=ERROR

### direct log messages to stdout ###
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.Target=System.out
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%d{ABSOLUTE} %5p %c{1}:%L - %m%n

### direct messages to file rtamApplication.log ###
log4j.appender.file=org.apache.log4j.RollingFileAppender
log4j.appender.file.File=${log.dir}rtam.log
log4j.appender.file.layout=org.apache.log4j.PatternLayout
log4j.appender.file.layout.ConversionPattern=%d{ABSOLUTE} %5p %c{1}:%L - %m%n
log4j.appender.file.encoding=UTF-8
```

For any of these loggers, the logging level can be set according to the specified value.

Log Level

You can set the following five log levels in the log4j.xml file:

- FATAL: logs only fatal errors

- ERROR: logs all errors
- WARN: logs warnings, and all errors
- INFO: logs information, warnings, and all errors
- DEBUG: logs debug information, and all other levels

The `rtam.log` File

RTAM processing, warning, and error messages are logged to the rtam.log file. In Tomcat for example, the rtam.log file resides in the following location: `[RTAMHome]\WEB-INF\system\logs\rtam.log`

Note: You must be a system administrator with file system access to view this file.

In this location, you can also view older versions of the rtam.log file that contain the history of past execution of RTAM.

Web Container Log Files

RTAM warning and error messages may also be logged in Tomcat or WebLogic Server log files or consoles.

Tomcat Log Files

In Tomcat on Windows, these messages are logged to the following file: `$CATALINA_HOME\logs\catalina.out`

In Tomcat on Unix, these messages are logged to the following file: `$CATALINA_HOME/logs/catalina.out`

For information about Tomcat log files, see the following URL:

- http://tomcat.apache.org/tomcat-5.5-doc/index.html

-or-

- http://tomcat.apache.org/tomcat-6.0-doc/index.html

WebLogic Server Log Files

In WebLogic Server, these messages are logged to the following files:

```
[WebLogicInstallDir]\user_projects\domains\informatica\ servers\AdminServer\logs
\AdminServer.log
[WebLogicInstallDir]\user_projects\domains\informatica\ servers\AdminServer\logs
\informatica.log
```

For information about log files in WebLogic Server, see the following URL:

`http://e-docs.bea.com/wls/docs100/logging/index.html`

JBOSS Server Log Files

In the JBOSS Server, these messages are logged to the following files:

```
[JBOSSInstallDir]\server\informatica\log\wrapper.log
[JBOSSInstallDir]\server\informatica\log\server.log
```

INDEX

I