CA GovernanceMinder

Installation Guide

12.6.1

CA Technologies Product References

- This document references the following CA Technologies products:
- CA GovernanceMinder
- CA IdentityMinder
- CA SiteMinder
- CA User Activity Reporting
- CA Service Desk Manager
- CA IAM Connector Server

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Installation Overview

This section contains the following topics:

Product Overview

CA GovernanceMinder complements CA Identity Lifecycle Management products with analytical and client tools for Role-Based Access Control (RBAC).

In RBAC, predefined roles codify common resource usage patterns. Often these roles bundle access rights related to specific business tasks and responsibilities. Users are assigned one or more of these roles based on their current duties, allowing access to only the resources they need.

CA GovernanceMinder supports implementation of RBAC in the enterprise in several ways:

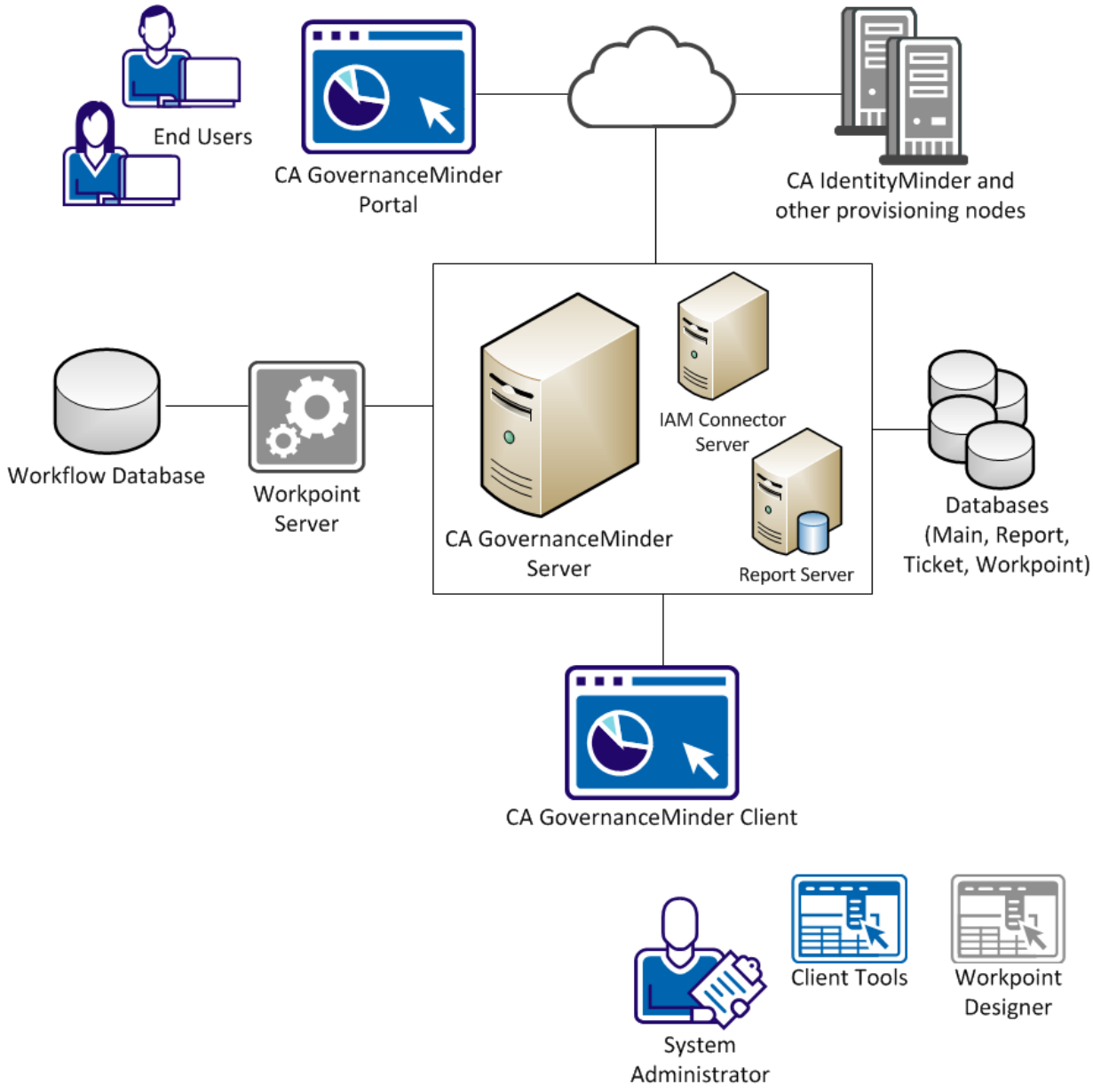
- **Role Discovery:** CA GovernanceMinder imports data from CA IdentityMinder and other provisioning nodes throughout the enterprise. Based on this data, CA GovernanceMinder provides powerful analytical tools that efficiently discover common usage patterns and construct an optimized role hierarchy that provides most users the resource access they need. The database and role hierarchy are constantly updated based on user, resource, and provisioning information from across the network.
- **Certification:** periodically, managers throughout the enterprise certify their workers' access privileges - by reviewing the roles assigned to them. Similarly, resource owners periodically review the users and roles that link to their resource. In some jurisdictions, these certifications are mandated by law. CA GovernanceMinder implements these certifications with a workflow.
- **Real-Time Provisioning Support:** provisioning nodes can query CA GovernanceMinder in real time using a set of web services. These web services suggest role profiles for users, and answer "what if" questions. In addition, CA GovernanceMinder can export changes to these nodes, creating account templates and other provisioning tools that reflect the best practices of the role hierarchy. In this way, the role hierarchy proactively controls the privileges assigned to users - realizing the promise of role-based access control.

Product Components

Every CA GovernanceMinder implementation includes the following functional components:

- The CA GovernanceMinder server supports data import, certifications, and the CA GovernanceMinder web portal and web services.
- CA GovernanceMinder client tools - let administrators manage data and develop the role hierarchy.
- The Workpoint server application and the Workpoint Designer client support certifications and other CA GovernanceMinder business processes that are implemented using Workpoint workflows.
- Databases - CA GovernanceMinder user, role, and resource databases, Workpoint processes, inbox data, and a reporting database.

The following diagram shows the interaction between these components.



The CA GovernanceMinder server application is the focal point of any CA GovernanceMinder implementation. It handles various functions and queries, including:

- Automatically importing data from CA IdentityMinder and other nodes, and support for web service calls
- Hosting the CA GovernanceMinder Web Portal
- Conducting certifications and other work flows through the CA GovernanceMinder Portal, using Workpoint processes and a management system

The Workpoint server application processes workflows such as certifications. Typically a dedicated instance of Workpoint server is installed together with the CA GovernanceMinder server, but an existing instance can be used.

The role engineer who administers CA GovernanceMinder uses a set of applications:

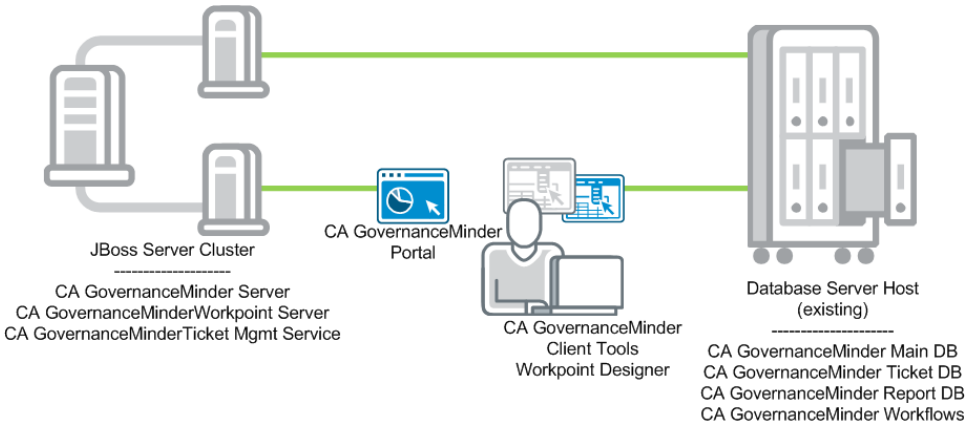
- The CA GovernanceMinder Client Tools manages data import and to define the role-based permissions hierarchy.
- The Workpoint Designer client loads and modifies Workpoint work flows.
- Additional management and configuration functions are exposed to administrators through the CA GovernanceMinder Portal.

JBoss Cluster Implementation

To help ensure availability and accommodate higher volumes of traffic, the CA GovernanceMinder and Workpoint server applications can be installed on a load-balanced JBoss server cluster of 64-bit Windows computers.

An existing database server hosts the CA GovernanceMinder databases.

You install the CA GovernanceMinder Client Tools and Workpoint Designer application on a separate Windows computer running a supported operating system, as shown in the following diagram:



More information:

JBoss/Windows Installation Worksheet (see page 61)

Chapter 2: System Requirements

This section contains the following topics:

Server Hardware Requirements

The following minimum hardware and software prerequisites apply to the production platforms that host the CA GovernanceMinder server and Workpoint server.

- **Processor**—Intel multicore processors with minimum 2.4 GHz. Four processors are required, configured as two dual-core processors or a single quad-core processor.
- **Memory**—8-GB RAM
- **Available disk space**—80 GB
- **Central database (RDBMS)**—For a list of supported databases, see the Platform Support Matrix available at CA Technologies Support Online.

  Note: You do not need to install this central database on the same computer as CA GovernanceMinder. For information about system prerequisites for your RDBMS, see the documentation for your product.

In addition, the CA GovernanceMinder server must have the following software installed:

- (Optional) **Active Directory**—An enterprise user store that is used to manage access to the CA GovernanceMinder portal

  If you are not using an enterprise user store, CA GovernanceMinder uses its own user store (the users database).

  Note: You do not need to install this user store on the same computer as CA GovernanceMinder. For information about system prerequisites, see the Active Directory product documentation. For supported versions, see the Platform Support Matrix available at CA Technologies Support Online.

- **Java Development Kit (JDK)**—CA GovernanceMinder 12.6.1 requires Oracle Java SE Development Kit 6u45 (1.6_45) as a prerequisite for the JBoss 5.1 application server that is installed with the product. For a list of supported JDKs, see the Platform Support Matrix available at CA Technologies Support Online.

  Add the pathname of this JDK instance to the JAVA_HOME and PATH variables in the System variables area in the Environment Variables window. If necessary, create the JAVA_HOME variable there.

  Note: When using a 64-bit JDK, and available memory is greater than 1400M (default), set the JVM maximum setting at 4 GB.

Database Requirements

CA GovernanceMinder creates database instances for user, role, and resource information, and Workflow data (for the Workpoint database). You can implement a database in the following two ways:

- A dedicated local RDBMS installed on the CA GovernanceMinder server.
- An existing RDBMS in the network.

Note: We recommend using Microsoft SQL Server for CA GovernanceMinder databases. During testing in CA Technologies labs, SQL Server provided the best performance.

For a list of supported databases, see the Platform Support Matrix available at CA Technologies Support Online. For information about system requirements for your RDBMS, see the documentation for your product.

Disk Space

To help ensure the best performance, the system that hosts the database must have sufficient disk space. Use the following guideline for determining the required disk space:

Set the disk space to 4 GB for every 100,000 links in a certification.

For example, if you have a certification that consists of 200,000 links, set the disk space to 8 GB.

Case Sensitive Requirements

The following case-sensitive states are applied to these databases:

- **eurekify_sdb**—case-sensitive
- **eurekify_ticket**—case-sensitive
- **WPDS (Workpoint)**—case-insensitive
- **Data Warehouse**—case-sensitive

Microsoft SQL Server

The following privileges and settings are required for Microsoft SQL Server:

- **User Account**—The CA GovernanceMinder database user must have the following privileges:
  - System Admin (SA)—Required during install if the installer is creating the database.
  - Dbo—Required during install if the database administrator manually created the database before install.
  - Datareader, Datawriter, BulkAdmin, DDLAdmin—minimum required privileges after installation.
- **Server Authentication mode**—"Mixed Authentication mode" only
- **Communications protocols**—TCP/IP and Named Pipes protocols enabled

Oracle Database

The following privileges and settings are required for Oracle Database:

- **Database**—The database must be defined either in a local tnsnames.ora file (under the Oracle Client installation), or in an Oracle directory server.
- **Encoding**—CA GovernanceMinder databases must use UTF-8 (AL32UTF8) encoding.
- **Database Sessions and Processes**—When an Oracle database server hosts CA GovernanceMinder databases, allot a minimum of 250 sessions and processes for CA GovernanceMinder activity on the database server.
- To increase the database sessions and process parameters (see page 16)
- **Schemas**—Empty, separate, schemas for SDB, ticketdb, and Workpoint (wpds), whose owners have the following roles and privileges:
  - Roles: CONNECT and RESOURCE. The CONNECT role provides the create session permission. The RESOURCE role provides several create system privileges, and provides for previous Oracle database compatibility releases.
  - System privileges:ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW, CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE, SELECT ANY DICTIONARY.

Note: We recommend that your database administrator creates the empty schemas for you before you install CA GovernanceMinder. If you do not prepare empty schemas for the CA GovernanceMinder databases, the installation requires the credentials of an Oracle Database user with DBA privileges. The installation program then creates the schemas using the information you provide.

For more information:

Increase Database Sessions and Process Parameters (see page 16)

Increase Database Sessions and Process Parameters

Increase database sessions and process parameters from the default settings to reduce exceptions.

Follow these steps:

a. Connect to the database with the system account.

b. Run the following commands:

```
alter system set sessions=400 scope=spfile;

alter system set processes=400 scope=spfile;
```

c. Restart the entire database (all cluster instances).

Database sessions and process parameters are increased.

Client Tools Server Hardware Requirements

The following minimum requirements apply to the computer that hosts the CA GovernanceMinder Client Tools:

Note: Typically, you install the Client Tools on the same computer as the Workpoint Designer application. We recommend selecting a computer that satisfies the requirements of both packages.

- **Processor**—Intel Core2 Duo 2.4 GHz
- **Memory**—2-4 GB RAM
- **Central database (RDBMS)**—For a list of supported databases, see the Platform Support Matrix available at CA Technologies Support Online.

  Note: You do not need to install this central database on the same computer as the client tools. For information about system requirements for your RDBMS, see the documentation for your product.

In addition, the following software must be installed:

- **Supported web browser**—For a list of supported web browsers, see the Platform Support Matrix available at CA Technologies Support Online.
- **.NET Framework**—Version 1.1 or 2.0

- **Microsoft XML**—Version 6
- **Microsoft Visual C++ 2005 SP1 Redistributable Package**—x86 or x64 version, depending on the target computer.

  Install this package after you install the .NET framework. On 64-bit computers, run the assembly registration utility (regasm.exe) after you install the package.
- (Optional) **Microsoft SQL Native Client 2005**—Only required if you reference a remote SQL Server instance *or* if you have a local Microsoft SQL 2008 database.
- (Optional) **Oracle Client**—Only required if you reference a remote Oracle Database instance. CA GovernanceMinder uses the following Oracle Client components: Oracle Database Utilities, SQL *Plus, Oracle Objects for OLE, and Oracle Provider for OLE DB.
- (Optional) **Java Virtual Machine**—Version 1.6_23 (minimum)

  Only required if you are installing the Workpoint Designer client on the same computer as the client tools.

  Note: For detailed information about Workpoint software installation and requirements, see the Workpoint documentation at the following location:

  gm_install\Server\eurekify-jboss\Workpoint\WorkPointDesigner\docs
- **Java Development Kit (JDK)**—For a list of supported JDKs, see the Platform Support Matrix available at CA Technologies Support Online.

  This software and pathname configuration is required for the connector.

  On a Windows computer, add the pathname of this JDK instance to the PATH and JAVA_HOME environment variables. If necessary, create the JAVA_HOME variable.

JBoss Port Requirements

The JBoss Application Server that is installed with the CA GovernanceMinder server uses the following ports:

- 1098
- 1099
- 1577
- 4026
- 4444
- 4445
- 4446
- 5001
- 8009

- 8080
- 8083
- 8093
- 8094
- 9092

Chapter 3: Installation Prerequisites

Before you can install CA GovernanceMinder, verify that the preliminary requirements are met and that you have the necessary information available.

This section contains the following topics:

Verify Available Ports

This procedure describes how to verify that the required network communications ports for the product are available.

Follow these steps:

1. On the target server, issue the following command:

   ```
   netstat -a -o | findstr "1098 1099 1577 4026 4444 4445 4446 5001 8009 8080 8083 8093 8094 9092"
   ```

   The command checks for any activity on the listed ports. If no activity is found, the ports are available to CA GovernanceMinder.

2. If the command shows activity on one or more ports, issue the following command to identify the application using each port:

   ```
   netstat -a -o -b
   ```

3. Redirect traffic from other applications to free the ports for CA GovernanceMinder.

   You have verified that the required network communications ports for the product are available.

Create a Database

When you are installing CA GovernanceMinder, you may not want to provide database credentials during installation. Instead, manually create the database and then run the installer and provide the database information when prompted. To manually create a database, use the DBUtil tool.

Follow these steps:

1. Verify that a local instance of Microsoft SQL Server or Oracle is available.
2. Copy the CA-RCM-12.6.01-Core.zip file from the CA GovernanceMinder installation package to a temporary location, and extract the file.
3. Navigate to the DBUtil tool in a Command Prompt window.

   The DBUtil tool is located in the following directory where you extracted the installation package:

   \CA-RCM-12.6.01-Core\Utils&Conf\DB Utility
4. Enter one of the following commands:
   - Microsoft SQL Server: dbutil.bat -c_i2 -d alpha_rdb -h localhost -u sa -p capassword
   - Oracle: dbutil.bat -c_i2 -d db1 -h localhost -u i2db -p eurekify -su system -sp eurekify -ven oracle

   The CA GovernanceMinder database is created on the database server.

Prepare the Installation Package

The CA GovernanceMinder software is available as a zipped installation package. After you download the installation package, prepare the installation files before you install. Use this procedure to create the installation files from the installation package.

Note: In the following procedure, *RN* is the current release number for the product.

Follow these steps:

1. Create a temporary directory in a location that is accessible from the target system.
2. Download the installation package files to the temporary directory, and extract them.

3. Extract the following compressed files to yield the installation programs:

   - Extract the CA-RCM-*RN*-Installer.zip file to the current directory to yield the InstCARCM.exe installation program.

     Use this installation program to install the CA GovernanceMinder server components.

   - Extract the client tools ZIP file to yield the installation program. Select the client tools package appropriate to the processor of the target system, as follows:

     - For a 64-bit system, extract CA-RCM-*RN*-Client-Tools-x64.zip
     - For a 32-bit system, extract CA-RCM-*RN*-Client-Tools-x86.zip

     Use the appropriate installation program to install the CA GovernanceMinder client tools on the target system.

IBM WebSphere on Red Hat Enterprise Linux 6.2 Requirements

When you install the product on IBM WebSphere on Red Hat Enterprise Linux (RHEL) 6.2, consider the following prerequisites.

- **IBM WebSphere 7.0 Network Deployment Application Server**—Install the IBM WebSphere 7.0 Network Deployment Application Server.

  Important! When running the setup script, select the Cell (deployment manager and a managed node) option.

- **Java Development Kit (JDK)**—CA GovernanceMinder 12.6.1 requires Oracle Java SE Development Kit 6u45 (1.6_45) as a prerequisite for the JBoss 5.1 application server that is installed with the product. For a list of supported JDKs, see the Platform Support Matrix available at CA Technologies Support Online.

  Add the pathname of this JDK instance to the JAVA_HOME and PATH variables in the System variables area in the Environment Variables window. If necessary, create the JAVA_HOME variable there.

  Note: When using a 64-bit JDK, and available memory is greater than 1400M (default), set the JVM maximum setting at 4 GB.

- **RHEL 6.2**—Install RHEL 6.2 with these packages in this order:

  - glibc-2.12-1.25.el6.i686.rpm
  - libX11-1.3-2.el6.i686.rpm
  - libxcb-1.5-1.el6.i686.rpm
  - libXtst-1.0.99.2-3.el6.i686.rpm
  - libXau-1.0.5-1.el6.i686.rpm
  - libXi-1.3-3.el6.i686.rpm

- libXext-1.1-3.el6.i686.rpm
- nss-softokn-freebl-3.12.9-3.el6.i686.rpm
- dos2unix-3.1-37.el6.x86_64.rpm

- **Run Commands**—Run the following command to improve performance (Entropy):
  `rm /dev/random && mknod -m 644 /dev/random c 1 9`
- **Java Virtual Machine (JVM) 1.6.0**—Install JVM 1.6.0, and set the following java environment variables:
  - JAVA_HOME=/usr/java/jdk1.6.0_20/
  - PATH=$PATH:/usr/java/jdk1.6.0_20/bin

Install Workpoint Server on a Separate System

If you want to install a CA GovernanceMinder server on a system that references a Workpoint server on another system, run the installer twice. First run the installer on one server to install Workpoint. Then you install the CA GovernanceMinder server on a separate system and configure the server to reference the Workpoint server.

The installer also installs the CA GovernanceMinder server. However, this instance of the CA GovernanceMinder server is not used.

Follow these steps:

1. Verify that the database server which hosts CA GovernanceMinder databases is running.
2. Run *one* of the following installation programs:
   - **Windows:** InstCARCM.exe
   - **Linux:** InstCARCM.bin

   These installation programs are available in the installation package (see page 19) that you downloaded.

   The CA GovernanceMinder installer opens.
3. Select the language that you want for the CA GovernanceMinder Portal, which is a web-based interface for CA GovernanceMinder.

   Note: The language you that select affects only the Portal interface and not the installation or any other component. This selection does not affect this installation.
4. Complete the installer by providing the necessary information.
5. Review your installation choices, and click Install.

   The installer runs the customized installation package.
6. Click Done to close the installer.

7. Remove CA GovernanceMinder server files, as follows:
   a. Navigate to this directory:

      gm_install\Server\eurekify-jboss\server\eurekify\deploy

      Note: *gm_install* is the CA GovernanceMinder installation directory.

   b. Delete the following files:
      - eurekify.war folder and its entire content
      - viewer.war
      - reportdb-ds.xml

   The Workpoint server is installed and you can continue with the CA GovernanceMinder server installation.

More information:

Prepare the Installation Package (see page 19)
JBoss/Windows Installation Worksheet (see page 61)

View CA GovernanceMinder Installer Debugging Information

When CA GovernanceMinder installs from the installer, you can view CA GovernanceMinder installer debugging information in a console window.

To invoke the console window, hold down the CTRL key when launching the CA GovernanceMinder installer. A console window appears and displays CA GovernanceMinder installation information in parallel to the installer.

Chapter 4: Install CA GovernanceMinder on JBoss

This scenario describes how you install CA GovernanceMinder with JBoss 5.1 on Windows or Linux.

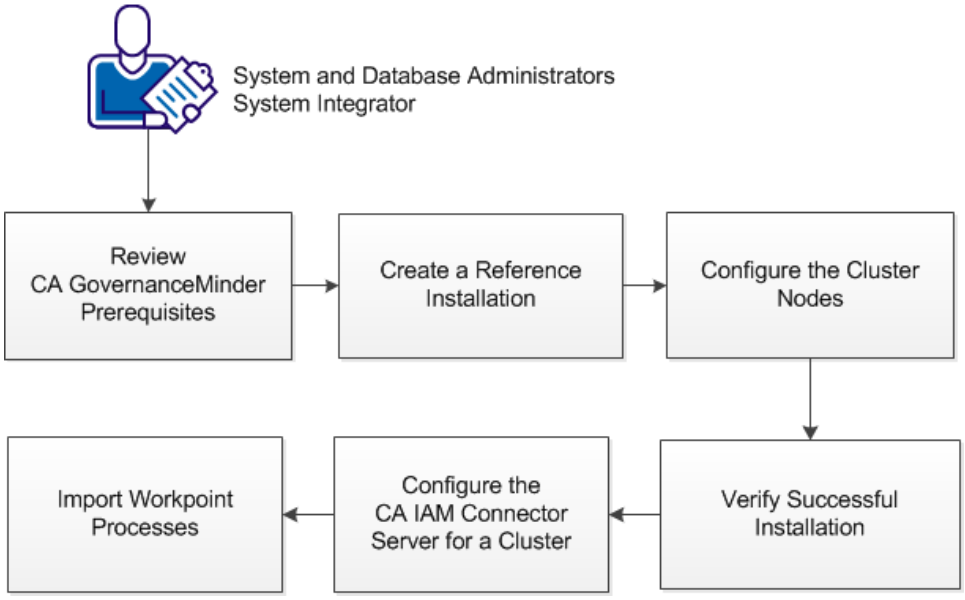
The target audience for this scenario is as follows:

- System and database administrators
- System integrators

This section contains the following topics:

How to Install CA GovernanceMinder on a JBoss Cluster

Run the installer on a single node to create a reference installation, then copy CA GovernanceMinder server components to other cluster nodes.



Follow these steps:

1. Review installation prerequisites. (see page 18)
2. Run the installer to create a reference installation (see page 24).
3. Configure the cluster nodes.
4. Verify successful installation.
5. Configure the CA IAM Connector Server for a Cluster.
6. Import Workpoint processes (see page 31).

Create a Reference Installation

Run the installer to create a reference installation on a single node.

Note: The installation worksheets (see page 61) list information you provide during installation. Use the worksheets during installation to avoid errors.

Follow these steps:

1. Verify that the designated CA GovernanceMinder database server host is running.

   Note: Host the database on a different computer than the cluster nodes.

2. Run one of the following installation programs:

   - Windows: InstCARCM.exe
   - Linux: InstCARCM.bin

   These installation programs are available in the installation package (see page 19) that you downloaded.

   The CA GovernanceMinder installer opens.

3. Select the language you want for the Portal, which is a web-based interface for CA GovernanceMinder.

   Note: The language you that select affects only the Portal interface and not the installation or any other component. This selection does not affect this installation.

4. Complete the installer by providing the necessary information.
5. Review your installation choices and click Install.

   The installer runs the customized installation package.

6. Click Done to close the installer.

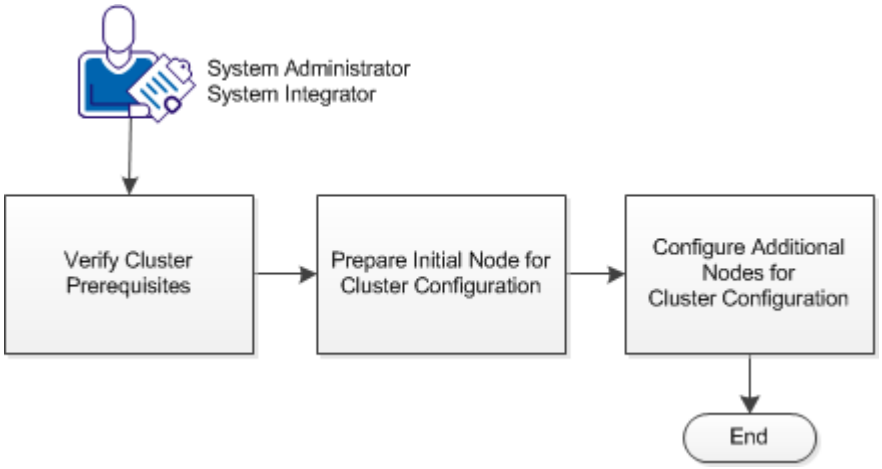
Next, you configure the cluster nodes.

More information:

Prepare the Installation Package (see page 19)

Configure the Cluster Nodes

The following diagram illustrates how to prepare and configure cluster nodes using the provided cluster script:



Follow these steps to prepare and configure CA GovernanceMinder cluster nodes:

1. Verify Cluster Prerequisites.
2. Prepare initial node for cluster configuration.
3. Configure additional nodes for cluster configuration.

Verify Cluster Prerequisites

This section lists cluster script software prerequisites.

Verify that all the prerequisites are installed before processing cluster components. Verify that they start with no errors and then stop them.

The software prerequisites are as follows:

- CA GovernanceMinder on Node 1
- Windows or Linux operating system
- JBoss 5.1 GA (5.1.0)

- CA GovernanceMinder cluster script (extracted into a temporary work folder on Node 1)

  Note: The script is in the Core.zip file at the following location:

  `CA-RCM-12.6.00-Core\Utils&Conf\Jboss Cluster`

- Apache Ant 1.7 or higher
- An ANT_HOME environment variable on the installation server.

  Set the ANT_HOME environment variable value to the ANT installation directory.

  Example:

  ANT_HOME="C:\ant 1.7.1"

Prepare Initial Node for Cluster Configuration

You prepare the initial cluster node by defining system components, permissions, and folders to work in a cluster configuration.

Follow these steps:

1. In the temporary folder where you extracted the cluster script, open the prepareCluster.properties file and set the following parameters:
   - CA GovernanceMinder installation directory

     Example: CA GovernanceMinder home (Windows)

     `rcm.installation.home=C:/Program Files/CA/RCM/Server`
   - JBoss 5.1 root directory

     Example: JBoss 5.1 root

     `jboss.5.1.home=C:/jboss-5.1.0.GA`
   - CA GovernanceMinder JBoss cluster operating system

     Set for Windows or Linux

     Example: For Linux

     `os.provider=linux`
   - CA GovernanceMinder database. Set for MSSQL or Oracle

     Example: For MSSQL

     `db.provider=mssql`
   - JBoss messaging database server name

     Example:

     `db.server.name=`*`your database computer name`*

- JBoss messaging database user login

  Example:

  `db.login.user=CA_GM_administrator`

- JBoss messaging database password login

  Example:

  `db.login.password=your database password`

- Database port

  Limits: 1433 MSSQL, port 1521 Oracle

  Example:

  `db.port=1433`

- Temporary files work folder

  Example:

  `work.dir=C:/temp/work`

- Cluster node names — a list of comma-separated host names and IP addresses

  Example:

  `cluster.nodes=nodeA, nodeB, 3.33.333.255`

- (Oracle) Oracle server service name

  Example:

  `oracle.service=ORCL`

2. Save and close the prepareCluster.properties file.
3. On the server where the Portal is installed, open a Command Prompt window and run the following file:

   Windows: prepareCluster.bat

   Linux: prepareCluster.sh

   This file prepares the downloaded JBoss 5.1 files to run in the cluster as Node 1.
4. Create a database and name it jboss_messaging.

   The nodes are prepared for cluster configuration. Repeat Steps 1-4 for preparing additional initial cluster nodes.

Configure Additional Nodes for Cluster Configuration

After configuring the initial node, you configure additional nodes for CA GovernanceMinder cluster configuration.

Configure additional CA GovernanceMinder cluster nodes using automatic or manual mode.

- Automatic
- Manual

Manual Cluster Node Configuration

Manually configure the CA GovernanceMinder cluster node. This mode is suggested for custom configurations.

Follow these steps:

1. Copy the JBoss 5.1 Home folder and all the contents from Node 1 to Node N, this server.
2. Locate and open for editing the following file in the JBoss home folder:

   Windows: eurikify.bat

   Linux: eurikify.sh
3. Assign the node to the following parameters:

   - jboss.messaging.ServerPeerID

   Defines the unique value (Node N) of this node in the cluster.

   - g

   Defines the unique cluster name.

   Example: Set the JBoss messaging peer ID and the network cluster name.

   From (default)

   ```
   run.bat -c %SERVER_NAME% -b %JBOSS_BIND_ADDRESS% -g CA_GM_Cluster -u 233.3.4.4
   -Djboss.messaging.ServerPeerID=1  %*
   ```

   To (assigned node number)

   ```
   run.bat -c %SERVER_NAME% -b %JBOSS_BIND_ADDRESS% -g CA_GM_Cluster -u 233.3.4.4
   -Djboss.messaging.ServerPeerID=2  %*
   ```
4. Save and close the file.

5. Open the server.xml file located in the following folder:

   JBoss 5.1 Home/server/all/deploy/jbossweb.sar/

   a. Locate and replace the following text:

      ```
      <Engine name="jboss.web" defaultHost="localhost">
      ```

      With

      ```
      <Engine name="jboss.web" defaultHost="localhost"
      jvmRoute="worker-node-name">
      ```

      Note: "*worker-node-name*" is the load balancer worker node name.

   b. Save and close the server.xml file.

   You have manually configured the CA GovernanceMinder cluster node.

Automatic Cluster Node Configuration

Automatically configure the CA GovernanceMinder cluster node. This mode configures multiple nodes using default parameters.

Follow these steps:

1. Locate and open the prepareCluster.properties file in the temporary work folder.
2. Locate the line containing the cluster.node.id=1 parameter, and set the cluster node property for this node.

   Example:

   For Node 4,

   ```
   cluster.node.id=4
   ```

   Note: The default node ID value is 1.
3. Open a Command Prompt window, and run the following file from the CA GovernanceMinder cluster work folder:

   Windows: prepareCluster.bat configure

   Linux: prepareCluster.sh configure

   This file configures JBoss 5.1 files to run as the designated node in the cluster.
4. Copy the JBoss 5.1 Home directory and all the contents from Node 1 to the next server in the cluster.
5. Repeat Steps 1-4 for each subsequent node in the cluster.

   You have automatically configured the CA GovernanceMinder cluster node.

Verify Successful Installation

When the installation is successful, you can access the CA GovernanceMinder Portal.

Follow these steps:

1. Open a Command Prompt window on Node 1, navigate to the JBoss home folder and run the following file:

   Windows: eurikify.bat

   Linux: eurikify.sh

   The CA GovernanceMinder and JBoss servers on Node 1 starts.

2. Review the logs and ensure Node 1 starts with no error messages.

   The CA GovernanceMinder cluster node log folder is:

   jboss.5.1home\server\all\log

   Note: *jboss.5.1home* is the CA GovernanceMinder cluster node home directory.

3. Log in using the default administration credentials:

   - **Username:** AD1\EAdmin
   - **Password:** eurekify

   Note: The password can be any password. It must be at least one character. The field must not be blank.

4. Stop the CA GovernanceMinder and JBoss servers on Node 1.

   You have verified the CA GovernanceMinder installation.

Next, you configure the CA IAM Connector Server for a cluster.

Configure the CA IAM Connector Server Connector Server for a Cluster

When installing the CA IAM Connector Server in a cluster environment, install the CA IAM Connector Server on one of the nodes, or on a dedicated node.

After installation, edit the following properties to reflect the location of the CA IAM Connector Server:

- jcs.ui.url=*IAMCS_hostname*

  The CA IAM Connector Serverhostname of the machine where the CA IAM Connector Server is installed.

- jcs.ui.enabled=true

- jcs.ui.username=*username*

  Default: admin

- jcs.ui.password=*IAMCS_password*

  The CA IAM Connector Server password is the one provided during installation.

Next, you import workpoint processes.

Import Workpoint Processes

To enable certifications and other business processes, import predefined workflow definitions into Workpoint.

Follow these steps:

1. Verify that the CA GovernanceMinder databases are running.
2. Log in to the Portal as an administrator.

   Your Portal home page appears.
3. Go to Administration, Settings.
4. Click Workpoint DB Administration.

   The Workpoint DB Administration screen appears.
5. Under Update Workpoint Processes, verify the CA GovernanceMinder Server Host Name, Port, and HTTPS setting.

   Note: In a clustered environment, enter the load balancer hostname instead of the server hostname, or localhost when no load balancer exists.
6. Click Update.

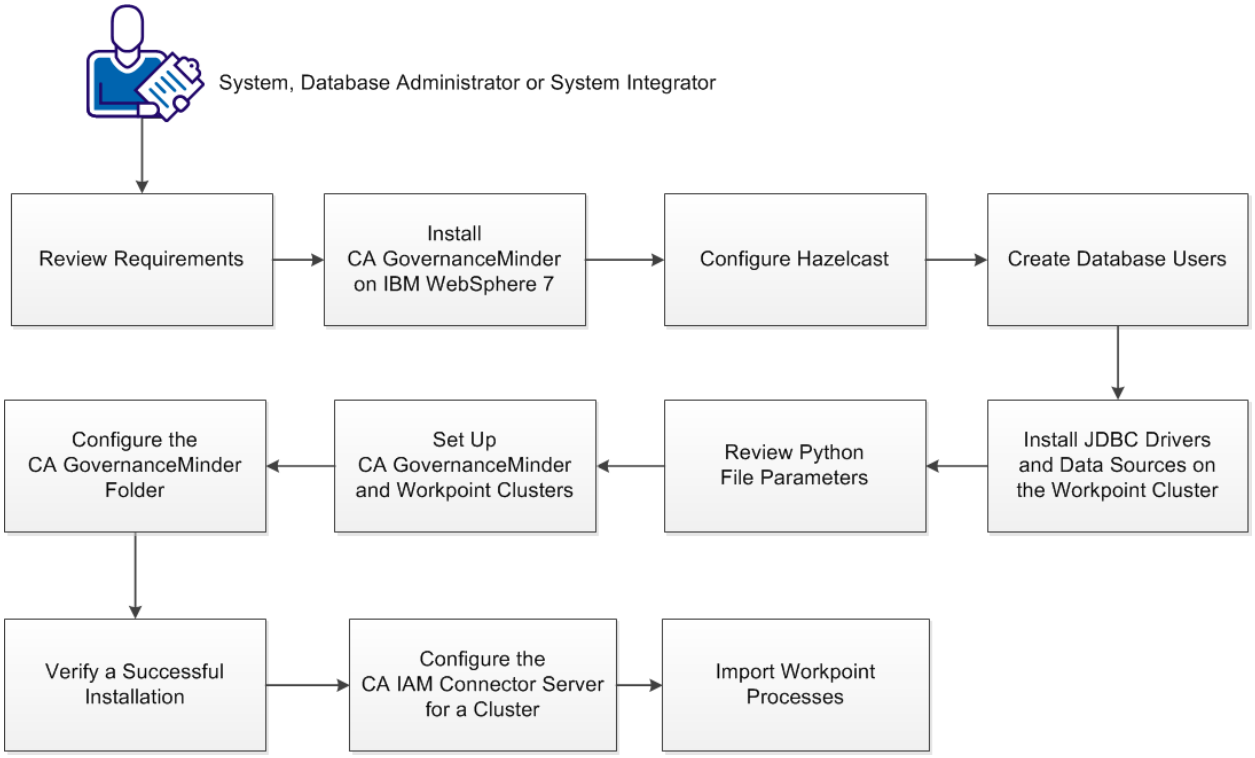
   The product populates the Workpoint database with Workpoint processes and related data.

Chapter 5: How to Install CA GovernanceMinder on an IBM WebSphere Cluster

As a system database administrator or system integrator, you install CA GovernanceMinder with IBM WebSphere Application Server (WAS) 7 on Red Hat Enterprise Linux (RHEL) 6.2.

The supplied script installs CA GovernanceMinder and WebSphere by automating various installation tasks. WebSphere is an application server that provides application delivery with operational efficiency, reliability, security, and control. Clustering increases computer processing power, load balancing, and provides application high availability.

The following diagram illustrates how to install CA GovernanceMinder and WebSphere with the supplied script:



Follow these steps:

1. Review requirements (see page 33).
2. Install CA GovernanceMinder on IBM WebSphere 7 (see page 34).
3. Configure Hazelcast (see page 36).
4. Create database users (see page 37).
5. Install JDBC drivers and data sources on the Workpoint cluster (see page 38).
6. Review Python file parameters (see page 41).
7. Set up CA GovernanceMinder and Workpoint clusters (see page 42).
8. Configure the CA GovernanceMinder folder (see page 42).

9. Verify a successful installation (see page 43).
10. Configure the CA IAM Connector Server for a cluster (see page 44).
11. Import Workpoint processes (see page 44).

Review Requirements

When you install the product on IBM WebSphere on Red Hat Enterprise Linux (RHEL) 6.2, consider the following requirements.

- **IBM WebSphere 7.0 Network Deployment Application Server**—Install the IBM WebSphere 7.0 Network Deployment Application Server.

  Important! When running the setup script, select the Cell (deployment manager and a managed node) option.

- **Java Development Kit (JDK)**—CA GovernanceMinder 12.6.1 requires Oracle Java SE Development Kit 6u45 (1.6_45). For a list of supported JDKs, see the Platform Support Matrix available at CA Technologies Support Online.

  Note: When using a 64-bit JDK, and available memory is greater than 1400M (default), set the JVM maximum setting at 4 GB

- **Verify that the following packages exist in this order:**
  - glibc-2.12-1.25.el6.i686.rpm
  - libX11-1.3-2.el6.i686.rpm
  - libxcb-1.5-1.el6.i686.rpm
  - libXtst-1.0.99.2-3.el6.i686.rpm
  - libXau-1.0.5-1.el6.i686.rpm
  - libXi-1.3-3.el6.i686.rpm
  - libXext-1.1-3.el6.i686.rpm
  - nss-softokn-freebl-3.12.9-3.el6.i686.rpm
  - dos2unix-3.1-37.el6.x86_64.rpm
- **Run Commands**—Run the following command to improve performance (Entropy):
  `rm /dev/random && mknod -m 644 /dev/random c 1 9`
- **Java Virtual Machine (JVM) 1.6.0**—Install JVM 1.6.0, and set the following java environment variables:
  - JAVA_HOME=/usr/java/jdk1.6.0_20/
  - PATH=$PATH:/usr/java/jdk1.6.0_20/bin

Note: For more information about installation prerequisites, see the *Installation Guide*.

Install CA GovernanceMinder on IBM WebSphere 7

This procedure describes how you install the CA GovernanceMinder server in a WebSphere environment. You must install the product as a root user on the same system where you have installed IBM WebSphere Network Deployment. The installer also installs and configures CA GovernanceMinder databases and data tables on a specified SQL or Oracle database server.

Follow these steps:

1. Verify that the SQL or Oracle server that is determined to host your databases is running.
2. Do the following:
   a. Download and install the latest Oracle JDK 1.6.X from the Oracle website.

      Note: We recommend that you download any Oracle JDK version above 1.6.23.

   b. Configure the Red Hat Enterprise Linux 6.2 Java alternatives.

      For example, run the following commands from the command prompt:

      ```
      /usr/sbin/alternatives --install  /usr/bin/java java
      /usr/java/jdk1.6.0_45/bin/java 1500
      ```

      ```
      /usr/sbin/alternatives --config java
      ```

      Note: In this example, the JDK installation root is as follows:

      ```
      /usr/java/jdk1.6.0_45
      ```

   c. Verify that the default Java command is now the Oracle JDK 6.45.

      From the command prompt, enter in the following command:

      ```
      java -version
      ```

      The Java version displays the following information:

      ```
      java version "1.6.0_45"
      ```

   d. Set the following java environment variables to the CA GovernanceMinder and IBM WebSphere cluster node installation:

      ```
      JAVA_HOME=JDK_6_install_root
      ```

      For example, add the following lines to the /root/.bashrc file:

      ```
      JAVA_HOME=/usr/java/jdk1.6.0_45
      ```

      ```
      export JAVA_HOME
      ```

      Note: You only set the environment variables on the node where you install CA GovernanceMinder, and not every node.

   You have configured Red Hat E Enterprise Linux 6.2 Java alternatives, verified default commands, and set Java environment variables.
3. Run the InstCARCM.bin installation program from the installation files.

   The CA GovernanceMinder installer opens.
4. Select the language that you want for the Portal, and click OK.

   Note: The language that you select affects the Portal interface only and not the installation or any other component.

5. Complete the installer by providing the necessary information. The following options are not self-explanatory:

   Application Server

   Specifies WebSphere: Prepare '.ear' installation files.

   Workpoint Server Host

   Specify *one* of the following server options:

   - This server - You install the Workpoint server on the CA GovernanceMinder server.
   - Remote server - Specify a remote Workpoint server.

6. Review your installation choices, and click Install.

   The installer runs the customized installation package.

7. When the installation completes, click Done to close the installer.

   You have installed CA GovernanceMinder and selected WebSphere as the application server in the Application Server step.

Next, you configure Hazelcast.

Configure Hazelcast

This procedure describes how to configure Hazelcast. Hazelcast is an open source clustering and highly scalable Java data distribution operating environment that CA GovernanceMinder uses.

For the CA GovernanceMinder cluster integration, edit the hazelcast.xml file to adjust the Hazelcast lock mechanism. The Hazelcast.xml file is located in the eurekify.war file.

Follow these steps:

1. Locate the hazelcast.xml file in the following folder:

   `eurekify.ear/eurekify.war/WEB-INF/classes`

   Note: Extract the eurekify.ear file before deploying to the cluster.

2. Open the hazelcast.xml file in an editor and locate the following group element:

   ```
   < group>
      <name>dev_RCM_WAS</name>
      <password>dev-pass</password>
   </group>
   ```

3. To match a unique name for your CA GovernanceMinder cluster, edit this element.

4. Locate the following element:

```
<tcp-ip enabled="true">
  <interface>127.0.0.1</interface>
</tcp-ip>
```

5. Add all your cluster member host names to the element as in Step 4.

   For example, the element would read as follows:

```
<tcp-ip enabled="true">
   <interface>Server1</interface>
   <interface>Server2</interface>
   <interface>Server3</interface>
   <interface>Server4</interface>
</tcp-ip>
```

6. Save the changes to the hazelcast.xml file and exit.

   You have configured the hazelcast.xml file to adjust the Hazelcast lock.

Next, you create database users to synchronize Java Messaging Service (JMS) topics.

Create Database Users

This procedure describes how to create database users to synchronize Java Messaging Service (JMS) topics.

Follow these steps:

1. Create the following database users:
   - gvmBus
   - wpBus
2. (Oracle only) Verify that the databases have the appropriate permissions by running the following SQL commands as user sys:

```
grant select on pending_trans$ to WPDS;
grant select on dba_2pc_pending to WPDS;
grant select on dba_pending_transactions to WPDS;
```

   - (if using an Oracle JDBC 10.2.0.3 or lower driver):

```
grant execute on dbms_system to WPDS;
```

   - (if using an Oracle JDBC 10.2.0.4 or higher driver):

```
grant execute on dbms_xa to WPDS;
```

3. (Oracle only) Restart the Oracle server.

   You have created database users to synchronize Java Messaging Service (JMS) topics.

Next, you install Server JDBC drivers and data sources on the Workpoint cluster.

Install JDBC Drivers and Data Sources on the Workpoint Cluster

This procedure describes how to install JDBC API support server cluster connections to the Microsoft and Oracle SQL database.

- **Microsoft:** (http://www.microsoft.com/en-us/download/default.aspx) XA data sources with Microsoft Distributed Transaction Coordinator (MS DTC) manage distributed transactions. To enable a specific user to participate in distributed transactions with the JDBC driver, assign the SqlJDBCXAUser role on the master database to the user that you create for the WDPDS database.
- **Oracle:** (http://www.oracle.com/technetwork/indexes/downloads/index.html) When an Oracle database server hosts CA GovernanceMinder databases, install JDBC drivers on the WebSphere Application Server. XA data sources manage distributed transactions. To enable a specific user to participate in distributed transactions with the JDBC driver, assign the SqlJDBCXAUser role on the master database to the user that you create for the WDPDS database.

Next, you review Python file parameters.

Install Microsoft SQL Server JDBC Drivers and Data Sources on the Workpoint Cluster

Valid on Microsoft SQL Server.

This procedure describes how you install Microsoft SQL Server JDBC drivers and data sources on the Workpoint cluster.

Java applications use the JDBC XA driver to establish concurrent connections to multiple databases through their associated resource managers.

Install the JDBC XA drivers on all SQL servers, and on the WebSphere application server.

Note the following:

- With a 32-bit SQL server, use the sqljdbc_xa.dll file in the x86 folder, even if the SQL server is installed on an x64 processor.
- With a 64-bit SQL server on the x64 processor, use the sqljdbc_xa.dll file in the x64 folder.
- With a 64-bit SQL server on an IA-64 processor, use the sqljdbc_xa.dll file in the IA64 folder.

Follow these steps:

1. Install the Microsoft SQL JDBC installer on the SQL server.

   Download the installer, Microsoft JDBC Driver for SQL (sqljdbc_4.0.2206.100_enu.exe), from the Microsoft Download Center.

2. Enable the XA transactions on the SQL server as follows:

   a. In the computer where you install the SQL server, browse to the Control Panel.

   b. Click Administrative Tools, Component Services.

   c. Right-click My Computer and click Properties.

   d. Click the MSDTC tab and click Security Configuration.

   e. Select Enable XA Transactions.

   f. Save the changes and restart the SQL server.

3. Copy and install drivers on other SQL cluster servers as follows:

   a. Locate the JDBC distributed transaction components under the \xa folder of the JDBC driver installation directory.

   b. Copy the file sqljdbc_xa.dll.

   c. Paste this file in the following directory of every SQL server computer that participates in distributed transactions:

      ```
      %SQL_SERVER_INSTALL%\Binn
      ```

   d. Execute the database script xa_install.sql on every SQL server instance that participates in distributed transactions. This script installs sqljdbc_xa.dll as an extended stored procedure.

      Note: When you run this script, log in as an administrator for the SQL Server instance.

4. Install the drivers on WebSphere as follows.
   a. In the original JDBC installation folder on the SQL server, locate the sqldbc.jar file in the following directory:

      `Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.2\enu`

   b. Copy this file to the WebSphere application server under the following directory:

      `WAS_install_root``/essentials/JDBC/`

      Note: *WAS_install_root* is the WebSphere Application Server installation directory.
5. To implement the new data source definitions, restart the WebSphere Application Server or the Deployment Manager service as required in your WebSphere environment.

   You have installed the Microsoft SQL Server JDBC drivers and data sources on the Workpoint cluster.

Install Oracle JDBC Drivers and Data Sources on the Workpoint Cluster

Valid on Oracle database.

This procedure describes how you install Oracle JDBC drivers and data sources on the Workpoint cluster.

Follow these steps:

1. Download the ojdbc14.jar file from the Oracle Download Center to the WebSphere application server, and place the file under the following directory:

   `WAS_install_root``/essentials/JDBC/`

   Note: *WAS_install_root* is the WebSphere application server installation directory.
2. In the WebSphere administration console, click Resources, JDBC, JDBC Providers and create a JDBC provider with the following settings:
   - The server provider:

     Name: ServerProvider

     Provider Type: Oracle JDBC Driver

     Implementation Type: data source

- The server XA provider:

  Name: ServerXAProvider

  Provider Type: Oracle JDBC Driver (XA)

  Implementation Type: XA data source

- Apply the following settings to both JDBC providers:

  Scope – Workpoint_cluster

  Database type – Oracle

  Class path – *WAS_install_root*/essentials/JDBC/ojdbc14.jar

3. Restart the WebSphere Application Server or the Deployment Manager service as required in your WebSphere environment.

   The new data source definitions are implemented.

   You have installed the Oracle JDBC drivers and data sources on the Workpoint cluster.

Review Python File Parameters

This procedure describes how you review the Python file to verify correct CA GovernanceMinder installation paths and data sources, and retain reusable memory. You download this file with the CA GovernanceMinder installation files. This file contains classes that can be used as reusable data sources and can construct dictionaries from other mappings or sequences of pairs.

Follow these steps:

1. Locate and open the dataSources.py file in the following folder:

   gm_install/rcm-websphere/WAS-Scripts

2. Change the passwords for the gvmBus and the wpBus users to the passwords set during the creation.
3. Save the dataSources.py file.

   You have reviewed the Python file.

Next, you set up the CA GovernanceMinder and Workpoint clusters.

Set Up CA GovernanceMinder and Workpoint Clusters

This procedure describes how you set up CA GovernanceMinder and Workpoint clusters on WebSphere.

Follow these steps:

1. Navigate to the following directory:

   gm_install\rcm-websphere\WAS-Scripts

2. Open a Command Prompt and enter the following command:

   ./DeployGVM.sh /opt/IBM/WebSphere/AppServer/bin

   This command instructs the installation script where to place the installation files.

   You have set up CA GovernanceMinder and the Workpoint clusters on WebSphere.

Next, you configure the CA GovernanceMinder folder to configure and copy essential files to the cluster nodes.

Configure the CA GovernanceMinder Folder

This procedure describes how you configure the CA GovernanceMinder installation folder to set up and copy essential files to the cluster nodes.

Follow these steps:

1. Locate and copy the *GM_Install_Dir* folder to the WebSphere clustered node server.
2. Change the directory as follows:

   GM_Install_Dir\rcm-websphere\WAS-Scripts

3. Locate and run the setupEssentials.py file from the following folder:

   WAS_HOME\profiles*NODE_NAME*\bin\wsadmin.bat -lang jython -f setupEssentials.py

4. Repeat Steps 1, 2 and 3 for each cluster node.

   You have configured the CA GovernanceMinder installation folder to configure and copy essential files to the cluster nodes.

Next, verify a successful installation.

Verify a Successful Installation

This procedure describes how you verify a successful installation after you complete installing the product. When the CA GovernanceMinder installation is successful, you can access the CA GovernanceMinder Portal.

Follow these steps:

1. Select and start one server from the CA GovernanceMinder cluster, CA GovernanceMinder, and installed applications, including reports.
2. Review the started server logs and verify that no log errors exist.
3. Start all other servers in the CA GovernanceMinder cluster.
4. Review all the product cluster logs and verify that no errors exist in the logs.

   You can access the Portal after a successful installation.
5. Open a browser and enter the following URL:

   `http://serverhost:port/eurekify/portal/login`

   Note: *serverhost:port* is the network address and communications port of the CA GovernanceMinder server or load balancer. The WebSphere/AIX server default port is 9080.

   The CA GovernanceMinder Portal login page appears.
6. Log in using the following default administration credentials:
   - **Username:** AD1\EAdmin
   - **Password:** eurekify

   The Portal home page appears.
7. Set your Properties and Common properties URL setting under Administration, Settings.
8. Navigate to Reports, Configuration Reports, and select Configuration Properties.
9. Select ConfigWithRoles to verify that the report application is working.

   You have verified a successful installation.
10. (Upgrade only) Clear the browser cache or refresh the web page to replace old graphical elements.

Next, configure the CA IAM Connector Server for a cluster.

Configuring the CA IAM Connector Server for a Cluster

You configure the CA IAM Connector Server for a cluster after the installation completes. When you install the CA IAM Connector Server in a cluster environment, install the CA IAM Connector Server on one of the nodes, or on a dedicated node.

After the installation, edit the following properties to reflect the location of the CA IAM Connector Server:

- jcs.ui.url=*IAMCS_hostname*

  This name is the CA IAM Connector Serverhostname of the computer where the CA IAM Connector Server is installed.

- jcs.ui.enabled=true
- jcs.ui.username=*username*

  Default: admin

- jcs.ui.password=*IAMCS_password*

  The CA IAM Connector Server password is the one provided during the installation.

Next, you import the Workpoint processes to enable certification campaigns and other business processes.

Import Workpoint Processes

This procedure describes how you import Workpoint processes. To enable certification campaigns and other business processes, import predefined workflow processes into Workpoint.

Follow these steps:

1. Verify that the CA GovernanceMinder cluster is running.
2. Log in to the Portal as an administrator.

   The Portal home page appears.

3. Go to Administration, Settings, and click Workpoint DB Administration.

   The Workpoint DB Administration screen appears.

4. Under Update Workpoint Processes, verify the CA GovernanceMinder Server Host Name, Port, and HTTPS setting.

   Note: In a clustered environment, enter the CA GovernanceMinder (load balancer) name instead of the server hostname.

5. Click Update.

   The product populates the Workpoint database with predefined Workpoint processes and related data.

You have enabled certification campaigns and other business processes, and imported predefined workflow processes into Workpoint.

You have completed the CA GovernanceMinder on IBM WebSphere 7 installation process.

Chapter 6: SSL-Encrypted Communication

The portal is a web-based application that is available to client computers through supported application servers. To configure SSL for the HTTPS transport of the application server, you first create an SSL key file (which defines the security policy). You then configure the application server to use the file. Property settings and common properties must be edited for the secure server.

Note: For more information about how to configure your application server for SSL communication, see the documentation for your product.

Example: Create a Self-Signed Certificate (see page 47)

Example: How to Configure CA GovernanceMinder for SSL Communication (see page 46)

By default, JBoss is not installed with SSL support. This means that all communication between the application server and the Portal client is not encrypted. This example shows you how to configure JBoss version 5.1.0 to use a certificate to secure communication.

Note: For more information about configuring JBoss for SSL, see the JBoss Community Documentation Library.

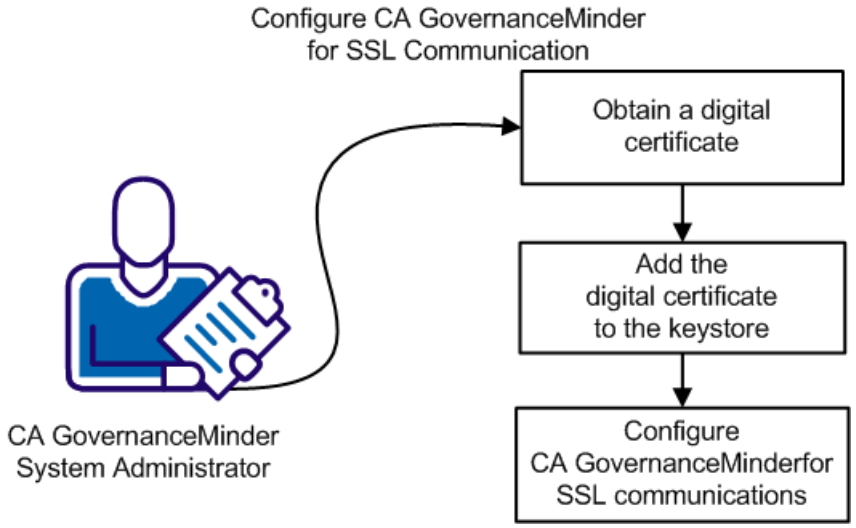
How to Configure CA GovernanceMinder for SSL Communication

Secure Sockets Layer (SSL) provides secure communications between applications. SSL helps ensure that communication between CA GovernanceMinder and endpoints have the following properties:

- **Authentication:** The participants in the communication are authenticated as being genuine.
- **Encryption:** Communication data is securely encrypted and delivered.

By default, the product is not installed with SSL support. This means that all communication between CA GovernanceMinder and the endpoints is not encrypted. You can configure the product to use SSL when working with endpoints.

The following diagram outlines the steps that are required to configure CA GovernanceMinder for SSL communication:



Follow these steps:

1. Obtain a digital certificate (see page 47).
2. Add the digital certificate to the keystore (see page 48).
3. Configure CA GovernanceMinder for SSL communication (see page 49).

Obtain a Digital Certificate

A digital certificate in specific syntax is required under certain circumstances.

Note: See the *Compatibility Matrix* for more information.

Follow these steps:

1. Access Microsoft Windows 2000 Server.

   Microsoft Windows 2000 Server contains a Certification Authority.
2. Create and manage digital certificates to users and computers.

   A digital certificate is obtained and ready to add to the keystore.

Example: Create a Self-Signed Certificate

This example shows you how to create a self-signed certificate.

Important! Regarding a self-signed certificate, trusting the issuer is problematic. In a production environment, use a certificate issued by a trusted Certificate Authority.

Follow these steps:

1. Open a Command Prompt window.
2. Enter the following command:

   `keytool -genkey -alias name -keyalg RSA -keystore server.keystore`

   -alias *name*

   Defines the alias to use for adding an entry to the keystore.

   -keyalg

   Specifies the algorithm to use to generate the key pair.

   The keytool utility starts.
3. Place your certificate in the following folder:

   gm_directory`\eurekify-jboss\server\eurekify\conf`
4. Complete the prompts as required and press Enter.

   A server.keystore file is created and positioned in the specified folder.

Add the Digital Certificate to the Keystore

Before you can configure CA GovernanceMinder to use SSL communication, you export and import the digital certificate to the keystore.

This procedure does the following:

- Describes how to configure CA GovernanceMinder to use SSL for secure communication using JBoss version 5.1.0 and JDK version 1.6_23.
- Assumes that you have created a digital certificate from the Certificate Authority named *digital_certificate_example*.

Follow these steps:

1. Stop JBoss if it is running. Do one of the following:
   - From the JBoss job windows, interrupt (Ctrl+C) the process.
   - Stop the JBoss Application Server service from the Services Panel.
2. Export and import the digital certificate as follows:
   a. On a system where the portal is installed, open a Command Prompt window and navigate to the following directory:

      ```
      C:\Program Files\Java\jdk1.6_23\bin
      ```

   b. To export, enter the following command:

      ```
      "%JAVA_HOME%\bin\keytool" -v -export -alias serverkeys -keystore "C:\Program Files\CA\RCM\Server\eurekify-jboss\server\eurekify\conf\server.keystore" -storepass password -file server_example.cer
      ```

   c. To import, enter the following command:

      ```
      "%JAVA_HOME%\bin\keytool" -v-import -keystore "%JAVA_HOME%\jre\lib\security\cacerts" -storepass password -file server_example.cer
      ```

3. Copy the *digital_certificate_example* file to the following JDK security folder:

   ```
   C:\Program Files\Java\jdk1.6_23\jre\lib\security
   ```

   The digital certificate is added to the keystore.

Configure CA GovernanceMinder for SSL Communication

After you add the users directory certificate to the keystore, you can configure CA GovernanceMinder to work with SSL by editing the JBoss run.bat file.

Follow these steps:

1. Edit the JBoss run.bat file (see page 49).
2. Edit the server.xml file (see page 50).
3. Set secure server properties (see page 51).

   JBoss is configured for SSL communication.

Edit the JBoss run.bat File

Edit the JBoss run.bat file for the correct certificate path and password.

Follow these steps:

1. Edit the JBoss run.bat file in the following folder:

   JBoss root\bin

2. Locate the following line in the run.bat file:

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000
   ```

3. Verify that you have the following correct path to the file and add the following:
   - set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.keyStore="C:/Program Files/Java/jdk1.6_23/jre/lib/security/*digital_certificate_example*"
   - set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.keyStorePassword=*password*
   - set JAVA_OPTS=%JAVA_OPTS% -Djavax.net.ssl.trustStore="C:/Program Files/Java/jdk1.6_23/jre/lib/security/*digital_certificate_example*"
4. Save the file and start JBoss.

   CA GovernanceMinder is configured for SSL communication.

Edit the server.xml File

Edit the server.xml file by activating and inactivating sections and adding properties for SSL.

Follow these steps:

1. Stop JBoss if it is running.
2. Locate the server.xml file in the following sar file and open it for editing:

   *gm_directory**Server*\eurekify-jboss\server\eurekify\deploy\jboss-web.sar

3. Locate the SSL <Connector port> tag in the following section:

   ```
   <!--
   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
              maxThreads="150" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS" /> -->
   ```

4. Remove the surrounding comment marks ("<!--" and "-->").

   You can now edit this tag.

5. Add the following properties to the <Connector port> tag:

   ```
   keystoreFile="${jboss.server.home.dir}/conf/server.keystore"
   keystorePass="newPassword"
   ```

   keystoreFile

   Specifies the full pathname of the keystore file.

   keystorePass

   Specifies the keystore password.

   The <Connector port> tag now appears as follows:

   ```
   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
       maxThreads="150" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS"

       keystoreFile="${jboss.server.home.dir}/conf/server.keystore"
       keystorePass="newPassword" />
   ```

6. Block default port 8080.

   a. Locate the following section

   ```
   <Connector protocol="HTTP/1.1" URIEncoding="UTF-8" port="8080"
   address=${jboss.bind.address}"

   connectionTimeout="20000" redirectPort="8443"  />
   ```

   b. Add the surrounding comment marks ("<!--" and "-->").

   Default port 8080 is blocked.

7. Save and close the server.xml file.
8. Start JBoss again.

   The server.xml file is edited.

Set Secure Server Properties

Setting secure server properties requires you to edit common properties and property settlings in the Portal. You enable the secure URI and delete the default port setting.

An edited secure server statisticalService.url property setting appears as follows:

```
https://localhost/eurekify/services/sageStatisticalService
```

Follow these steps:

1. Log in to the CA GovernanceMinder Portal as an administrator.
2. Go to Administration, Settings, Common Property Settings.

   The Common Properties Settings screen appears.
3. Edit the following Common Properties by making the URL secure and deleting the default port:
   - statisticalService.url
   - flowCampaignService.url
   - buildingBlockService.url
   - reportsService.url
   - campaignService.url
   - sageBrowsingService.url
4. Save the settings.

   The common properties are set for the secure server.
5. Go to Administration, Settings, Property Settings.
6. Edit the following Property Settings by making the URL secure and deleting the default port
   - integration.unicenter.servicedesk.webservice.url
   - portalExternalLink.certificationUrl
   - portalExternalLink.homeUrl
   - logout.landingPageUrl
   - resource.image.url
   - reports.baseUrl

- tms.workflow.url
- portalExternalLink.ticketQueueUrl
- sage.sageBaseUrl
- role.image.url
- sso.sajcsui.url

7. Save the settings.

   The property settings are set for the secure server.

Chapter 7: Installing Additional Components

This section contains the following topics:

Install Oracle Client Components

When an Oracle server hosts CA GovernanceMinder databases, you install Oracle Client components on computers that run CA GovernanceMinder Client Tools. These components support client interaction with databases on the Oracle server.

To install Oracle Client components

1. Download an Oracle Client installation package that is compatible with the target Oracle server from the Oracle website (http://www.oracle.com/technology/software/products/database/index.html) to the computer that hosts CA GovernanceMinder Client Tools.
2. Run the Oracle Client installer and install the following components:
   - Oracle Database Utilities
   - SQL*Plus
   - Oracle Windows Interfaces components:

     Oracle Objects for OLE

     Oracle Provider for OLE DB
3. Unzip the Oracle Client installer.

4. Create a tnsnames.ora file that defines the connection to the main CA GovernanceMinder database on the Oracle server.

   For example, the following code defines a TCP link to the rcm_sdb database on the XE database server.

   ```
   XE =
   (DESCRIPTION =
   (ADDRESS = (PROTOCOL = TCP)(HOST = ORAC01.com)(PORT = 1521))
   (CONNECT_DATA = (SERVER = DEDICATED)(SERVICE_NAME =rcm_sdb))
   )
   ```

5. Copy the tnsnames.ora file to the following directory:

   Oracle_home\network\admin

   Note: *Oracle_home* is the root directory for the Oracle Client package.

Install Client Tools

Use the Cient Tools to import and modify data, and analyze, construct and administer the role hierarchy. Install the Client Tools on a Windows computer that can communicate with the CA GovernanceMinder server and the database server.

Follow these steps:

1. On a Windows computer, run the .msi file you prepared earlier:

   - On a 64-bit computer, run CA-RCM-*rel#*-Client-Tools-x64.msi
   - On a 32-bit computer, run CA-RCM-*rel#*-Client-Tools-x86.msi

   The Client Tools installation wizard opens.

2. Complete the installer following the wizard prompts.

   If you selected to install additional components, the installation prompts you for the required files:

   - To install the UUID and IM Connector tools, locate the CA-RCM-*rel#*-Client-Tools-Open-Source.zip file.
   - To install the Online Help, locate the CA-RCM-*rel#*-Language-Files.zip file.

   The installer runs and installs the CA GovernanceMinder client tools on the computer.

3. (64-bit computers only) Run the Microsoft Assembly Registration Utility:
   a. Open a command line window and navigate to the following folder:

      ```
      C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727
      ```

   b. Enter the following commands:

      ```
      regasm.exe "C:\Program Files\CA\RCM\Client
      Tools\Software\Microsoft.Web.Services3.dll"
      regasm.exe "C:\Program Files\CA\RCM\Client Tools\Software\SageSOAP.dll"
      ```

   You have installed the Client Tools on a Windows computer that can communicate with the CA GovernanceMinder server and the database server.

More information:

Prepare the Installation Package (see page 19)

Configure Client Tools After Installation

After you install the Client Tools, configure them to connect to the CA GovernanceMinder database.

Follow these steps:

1. Verify that the database server is running.
2. If your installation also includes a CA GovernanceMinder server, verify that it too is running.
3. Run the Client Tools.
4. Click File, General Settings.

   The Settings dialog opens.
5. Close the dialog.
6. Do *one* of the following:
   - When your implementation includes a CA GovernanceMinder server, coordinate database interactions with CA GovernanceMinder server (see page 56).
   - When there is no CA GovernanceMinder server, configure a direct connection to the database server (see page 56).

   The Client Tools are configured and ready for use.

Coordinate the Client Connection to the Database with CA GovernanceMinder Server

When your implementation includes a CA GovernanceMinder server, configure the Client Tools to coordinate database interactions with the CA GovernanceMinder server. This coordination ensures data synchronization between the client and server interfaces.

Follow these steps:

1. Verify that the database server and CA GovernanceMinder server are running.
2. Run the client tools.

   The Enter Server Credentials dialog appears.
3. Click Cancel. Then click File, General Settings from the main menu.

   The Settings dialog appears.
4. Click the SQL Connectivity tab.
5. Select the Request SQL Credentials from a Server option.
6. Complete the address of the CA GovernanceMinder server URL, and click Apply.

   The Enter Server Credentials dialog appears.
7. In the SQL Server area, specify the user name and password that is defined for the CA GovernanceMinder database on the database server.
8. In the Web Server area, specify the user name and password of an administrator account on the CA GovernanceMinder portal.
9. Click OK.

   A message confirming SQL connectivity appears after a while. Changes that you make to databases using the client tools are synchronized with the CA GovernanceMinder portal.
10. Close the dialog.

    You have configured the Client Tools to coordinate database interactions with the CA GovernanceMinder server.

Configure Direct Client Connection to Databases

In implementations that **do not** include a CA GovernanceMinder server, configure your client applications to work directly with the database server.

Follow these steps:

1. Verify that the database server is running.

2. Run the Data Management application.

   The Enter Server Credentials dialog appears.

3. Click Cancel. Then click File, General Settings from the main menu.

   The Data Management Settings dialog appears.

4. Click the SQL Connectivity tab.

5. Select the Use Static SQL Credentials option.

6. Configure the following fields and options:

   SQL Server Type

   Specifies whether a Microsoft SQL Server or Oracle Server hosts CA GovernanceMinder databases.

   Server

   Defines the target on the database server:

   - For a Microsoft SQL Server, this field specifies the host name of the database server instance.
   - For an Oracle database server, this field specifies the Oracle service name, as defined in the tnsnames.ora file in the Oracle service directory.

   Database

   (Microsoft SQL Server only) Defines the main CA GovernanceMinder database.

   Username, Password

   Define the login credentials of the database user or schema owner.

   Windows Authentication

   (Microsoft SQL Server only) When the database user is mapped to a general Windows user account in the environment, specifies whether the Windows user is used to log in to the database server.

7. Click Apply.

   A message confirming SQL connectivity appears. The application is now connected to the database.

8. Close the dialog.

9. Repeat this procedure in the DNA application.

   The client applications are configured and ready for use.

Install Workpoint Designer

CA GovernanceMinder uses the Workpoint Business Process Management (BPM) solution to implement CA GovernanceMinder business workflows. For example, certifications are modeled as Workpoint processes, and the CA GovernanceMinder server is implemented as Workpoint jobs.

You can use the Workpoint Designer application to import and customize process workflows.

Note: We recommend that you use the workflow administration tools of the Portal to load and update Workpoint processes. Only experienced administrators should use Workpoint Designer to customize workflow behaviors.

The CA GovernanceMinder installer places a precompiled, customized Workpoint Designer package in the CA GovernanceMinder server installation directory. You can copy this package to run Workpoint Designer on another server.

This section describes how to install and configure Workpoint Designer to work with a CA GovernanceMinder server installation.

This section contains the following topics:

Install Workpoint Designer on JBoss

This procedure describes how to install and configure Workpoint Designer to work with a CA GovernanceMinder server on JBoss.

Follow these steps:

1. Locate the following directory on the server where you ran the CA GovernanceMinder installer:

   gm_install\Server\eurekify-jboss\Workpoint

   gm_install is the CA GovernanceMinder installation directory.

2. Copy the Workpoint Designer directory to a system that runs a supported version of Windows or Linux. Continue this procedure on that system.

3. (Remote) Define an ODBC Data Source that points to the CA GovernanceMinder Workpoint database.

4. Configure the Workpoint Designer as follows:

   a. In the Workpoint Designer directory, locate the workpoint-client.properties file in the following folder:

      \conf

   b. Locate and edit the following property:

      java.naming.provider.url—The host name and port information for the Workpoint server or the Workpoint cluster load balancer. For a JBoss cluster, the default port on the load balancer is 1100.

      Note: Edit the instance of this property that is under the JBOSS SETTINGS section of the file. Specify the full URL and port string. Do not specify a DNS hostname.

   c. Save and close the **workpoint-client.properties** file.

5. Verify the Workpoint Designer installation.

   Workpoint Designer is installed and configured to work with a JBoss installation.

Note: For detailed information about Workpoint Designer, see the Workpoint documentation at the following location:
gm_install\Server\eurekify-jboss\Workpoint\WorkPointDesigner\docs

Install Workpoint Designer to Work with WebSphere

This procedure describes how to install and configure Workpoint Designer to work with a CA GovernanceMinder server on WebSphere.

Follow these steps:

1. On the system where IBM WebSphere 7is installed, navigate to the following folder:

   WAS_home/opt/IBM/WebSphere/AppServer/essentials/Workpoint/

2. Copy and paste the following properties files:

   - Archive
   - GeneralMonitor
   - IdCheck
   - workpoint-client
   - workpoint-server

   in the following folder:

   WAS_home/opt/IBM/WebSphere/AppServer/essentials/Workpoint/WorkPointDesigner/conf

3. (Remote) Download and install the IBM Application Client for WebSphere Application Server.

4. (Remote) Define an ODBC Data Source that points to the CA GovernanceMinder Workpoint database.
5. Configure the Workpoint Designer as follows:
   a. In the Workpoint Designer directory, locate the workpoint-client.properties in the following folder:

      \conf

   b. Open the workpoint-client.properties file and make the following changes:
      - Under the J2EE Client Configuration header, change all lines in the JBoss SETTINGS section into remarks by adding the # character.
      - Remove the # character from all lines of the IBM WEBSPHERE SETTINGS section to make these lines active.
      - Save and exit.
   c. Locate the init.bat or initi.sh file located in the following directory:

      \bin

   d. Edit the **init.bat** or **init.sh** file by doing the following steps:
      - Add the *rem* keyword to all lines in the USE WITH JBoss section.
      - Remove the *rem* keyword from all lines in the USE WITH IBM WEBSPHERE section.
      - Set the JAVA_HOME and WAS_HOME properties to the WebSphere Application Server client application. Typically the values are as follows:

        Windows:

        SET JAVA_HOME=C:\PROGRA~1\IBM\WebSphere\AppClient\java\jre

        SET WAS_HOME=C:\PROGRA~1\IBM\WebSphere\AppClient

        Linux:

        SET JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/jre

        SET WAS_HOME=/opt/IBM/WebSphere/AppServer
      - Save and exit.
6. Run Workpoint Designer.

   Workpoint Designer is installed and configured to work with a WebSphere installation.

Appendix A: Installation Worksheets

The CA GovernanceMinder installation program requests information about previously installed software and the software that you are installing. Use the following worksheets to collect information about your system before installing CA GovernanceMinder. After you complete the worksheets, you can use them as you work through the installation prompts. You can print and complete the worksheets to record your selections.

This section contains the following topics:

JBoss/Windows Installation Worksheet

In a single Windows server installation, the CA GovernanceMinder server installation also installs a customized version of the JBoss Application Server. For clustered installations, a supported application server must already be configured and working. Record the following application server information you need during installation:

Field	Description	Your Response
Select SQL Options	Specifies the server host and supported database server type you want to install CA GovernanceMinder against. Can be either: ■ Microsoft SQL Server ■ Oracle **Note:** Verify that you complete the appropriate worksheet for your database server.	
Select the Application Server Environment	Specifies the supported application server where you want to install the CA GovernanceMinder server.	JBoss
Select the WorkPoint Server Host	Specifies the host name or IP address of the Workpoint server computer. **Default:** This server—the computer you are installing on.	

Field	Description	Your Response
Select a Destination Folder	Defines the location where the CA GovernanceMinder software files are installed. **Default:** C:\Program Files\CA\RCM\Server	
Select a Shortcut Folder	Defines the location where the CA GovernanceMinder installer creates product shortcuts. **Default:** Other—The Start menu of the user that executed the installer.	
Provisioning Options	Specifies which provisioning feature to install. Select from: ■ Standalone Connector Server ■ Connector Server Management UI **Note:** Provisioning option is **not** required.	

More information:

Microsoft SQL Server Worksheet (see page 64)
Oracle Database Worksheet (see page 65)

JBoss/Linux Installation Worksheet

In a single Linux server installation, the CA GovernanceMinder server installation also installs a customized version of the JBoss Application Server. For clustered installations, a supported application server must already be configured and working. Record the following application server information you need during installation:

Field	Description	Your Response
Select the SQL Server Type	Specifies the supported database server type you want to install CA GovernanceMinder against. Can be either: ■ Microsoft SQL Server ■ Oracle **Note:** Verify that you complete the appropriate worksheet for your database server.	
Select the Application Server Environment	Specifies the supported application server you want to install the CA GovernanceMinder server on.	JBoss
Select the WorkPoint Host	Specifies the host name or IP address of the Workpoint server computer. **Default:** This computer—the computer you are installing on.	
Where Would You Like to Install	Defines the location where the CA GovernanceMinder software files are installed. **Default:** /user home/CA/RCM/Server	
Where Would You Like to Create Product Icons	Defines the location where the CA GovernanceMinder installer creates product shortcuts. **Default:** Other—The Start menu of the user that executed the installer.	

More information:

Microsoft SQL Server Worksheet (see page 64)
Oracle Database Worksheet (see page 65)

Microsoft SQL Server Worksheet

A database server must already be configured and working with a supported RDBMS. Record the following database information you need during installation against an existing Microsoft SQL Server:

Field	Description	Your Response
Microsoft SQL Server Host	Defines the host name or IP address of the database server computer or cluster.	
Select Microsoft SQL Server Instance	Specifies a target SQL Server instance, by name or communications port. **Default:** Use default instance—uses an unnamed default instance and the standard port 1433.	
SQL Server Username	Defines the user ID of an SQL Server user with the system administrator privileges. **Note:** You can only use SQL login names to authenticate against the SQL Server.	
SQL Server Password	Defines the password of the SQL Server user with system administrator privileges.	

Important! We recommend that you use the default database names. CA GovernanceMinder database names cannot contain the hyphen (-) character.

RCM Database Name	Defines the name of the database that holds imported user, role, and resource information, CA GovernanceMinder portal settings, and other data. **Default:** eurekify_sdb	
RCM Ticket Database Schema Name	Defines the name of the schema for business processes data such as review and approval campaigns. User must have CONNECT and RESOURCE roles. **Default:** eurekify_ticketdb	
Workpoint Database	Defines the name of the database that holds the Workpoint work flows. **Default:** WPDS	
Report Database Name	(Optional) Defines the name of the database that holds the reporting information. **Default:** eurekify_reportdb	

Note: When you install CA GovernanceMinder on an AIX/WebSphere application server, you create two additional databases for CA GovernanceMinder and Workpoint cluster bus queues. For instructions, see the AIX installation notes in the CA GovernanceMinder support Knowledge Base section.

Oracle Database Worksheet

A database server must already be configured and working with a supported RDBMS. Record the following database information you need during installation against an existing Oracle Database Server:

Field	Description	Your Response
Oracle Server Host	Defines the host name or IP address of the database server computer or cluster.	
Select Service Name	Specifies the name that identifies your RDBMS on the system. **Default:** ORCL—the default service name for Oracle Database 10*g* or 11*g*.	
Specify Oracle Server port	Specifies the port used by the RDBMS you specified. **Default:** 1521—the default port for Oracle Database.	
	Important! We recommend that you use the default database names. CA GovernanceMinder database names cannot contain the hyphen (-) character.	
RCM Database Schema Name	Defines the name of the schema for imported user, role, and resource information, CA GovernanceMinder portal settings, and other data. User must have CONNECT and RESOURCE roles. **Default:** eurekify_sdb	
RCM Database Schema Password	Defines the password of the CA GovernanceMinder schema user.	

Field	Description	Your Response
RCM Ticket Database Schema Name	Defines the name of the schema for business processes data such as review and approval campaigns. User must have CONNECT and RESOURCE roles. **Default:** eurekify_ticketdb	
RCM Ticket Database Schema Password	Defines the password of the CA GovernanceMinder ticket schema user.	
Workpoint Database Schema Name	Defines the name of the schema for the Workpoint work flows. User must have CONNECT and RESOURCE roles. **Default:** WPDS	
Workpoint Database Schema Password	Defines the password of the Workpoint schema user.	

Note: We recommend that your database administrator creates the empty schemas for you before you install CA GovernanceMinder. If you do not prepare empty schemas for the CA GovernanceMinder databases, the installation requires the credentials of an Oracle Database user with DBA privileges. The installation program then creates the schemas using the information you provide.

Note: When you install CA GovernanceMinder on an AIX/WebSphere application server, you create these additional databases for CA GovernanceMinder and Workpoint cluster bus queues. See the AIX installation notes in the CA GovernanceMinder support Knowledge Base section.

Oracle DBA username	Defines the name of a DBA user you want to use to create the required CA GovernanceMinder schemas you supplied. **Note:** If you prepare the CA GovernanceMinder schemas in advance of running the installation program, you do not need to supply Oracle DBA credentials. **Default:** system	
Password	Defines the password of a DBA user you want to use to create the required CA GovernanceMinder schemas you supplied.	

Note: When you install CA GovernanceMinder on an AIX/WebSphere application server, you can work with either an Oracle 10*g* Database or an Oracle 11*g*R2 Database, but the installed driver is for the Oracle Database 10*g* Database.

Appendix B: Configure JBoss as a Windows Service

When you configure the JBoss application server as a web service, it automatically runs when the computer starts.

Follow these steps:

1. Browse to the JBoss community download website and download the jboss-native-2.0.9-windows-x86-ssl.zip file.
2. Copy and decompress the jboss-native-2.0.9-windows-x86-ssl.zip file to the following directory:

   gm_install\eurekify-jboss

   Note: *gm_install* is the CA GovernanceMinder installation directory.

   New directories and files are created.
3. Create a backup of the **service.bat** file in the following subdirectory:

   gm_install\eurekify-jboss
4. Edit the **service.bat** file in the *gm_install*\eurekify-jboss\bin subdirectory as follows:
   a. Search the file and replace the string **run.bat** with the string **eurekify.bat**.
   b. Locate and delete the following strings in the file:
      - > run.log
      - >> run.log
      - > shutdown.log
      - >> shutdown.log
      - 2>&1
   c. Save changes to the file.
5. Open a command line window from the Start menu and navigate to this directory:

   ...\jboss-native-2.0.9-windows-x86-ssl\bin
6. Enter **service install**.

   A confirmation message appears after the JBoss web application service is installed.
7. Open the Windows Control Panel, and double-click Administrative Tools, Services.

   The Services application window appears.
8. Locate and right-click the JBoss Application Server entry, and select Properties.

9. Change the Startup Type to Automatic, click OK and exit the Services application.
10. Restart the computer.
11. Verify CA GovernanceMinder log files to verify that the JBoss Application Server starts.

    The JBoss application server is configured as a Windows service.

This section contains the following topics:

JBoss Windows Service Fails to Start (see page 70)

JBoss Windows Service Fails to Start

When you implement JBoss as a Windows service, the JBoss service may not start when you restart Windows. There may be a conflict between existing DLL files and the new files you installed to implement the JBoss service. You can disable unnecessary DLLs.

Follow these steps:

1. Browse to the following directory:

   gm_install\eurekify-jboss\bin

   Note: *gm_install* is the CA GovernanceMinder installation directory.
2. Rename the **\native** subdirectory to **\native_bak**.
3. Restart the computer.
4. Verify CA GovernanceMinder log files to verify that the JBoss Application Server starts.

Appendix C: Configure JBoss as a Linux Daemon

When you configure the JBoss application daemon as a web service, it automatically launches when you restart the computer.

Follow these steps:

1. Copy the jboss_linux_service.sh file from the CA GovernanceMinder installation package, located in this directory;

   gm_install/eurekify-jboss/bin/

   To the following directory:

   /etc/init.d

   Note: *gm_install* is the CA GovernanceMinder installation directory.

2. Rename the file JBoss.
3. Open the jboss_linux_service.sh file for editing, and replace all instances of gm_install with the actual installation path.
4. Verify the file permissions.

Example: Configure JBoss as a Linux Daemon Script

This example shows you how to create a script to configure JBoss as a Linux daemon.

1. Copy and paste the following script in this directory:

   ```
   /etc/rc.d/init.d
   ```

2. As root (su - root) type vi /etc/rc.d/init.d/jboss and paste as follows:

   ```
   #! /bin/sh

       start(){
               echo "Starting jboss.."
               su -l root -c ' gm_install/eurekify-jboss/bin/eurekify.sh  >
       /dev/null 2> /dev/null &'
       }

       stop(){
               echo "Stopping jboss.."
               su -l root -c ' gm_install/eurekify-jboss/bin/shutdown.sh -S &'
       }
       restart(){
               stop
       # give stuff some time to stop before we restart
               sleep 60
       # protect against any services that cannot stop before we restart (warning
       this kills all Java instances running as 'jboss' user)
               su -l root -c 'killall java'
               start
       }

       case "$1" in
         start)
               start
               ;;
         stop)
               stop
               ;;
         restart)
               restart
               ;;
         *)
               echo "Usage: jboss {start|stop|restart}"
               exit 1
       esac
       exit 0
   ```

3. Change the permissions of the file with the following command:

   ```
   chmod 0755 /etc/init.d/jboss
   ```

4. Create links that you use to identify JBoss start and stop run levels.

   For example, (create as root):

   ```
   ln -s /etc/rc.d/init.d/jboss /etc/rc3.d/S84jboss
   ln -s /etc/rc.d/init.d/jboss /etc/rc5.d/S84jboss
   ln -s /etc/rc.d/init.d/jboss /etc/rc4.d/S84jboss
   ln -s /etc/rc.d/init.d/jboss /etc/rc6.d/K15jboss
   ln -s /etc/rc.d/init.d/jboss /etc/rc0.d/K15jboss
   ln -s /etc/rc.d/init.d/jboss /etc/rc1.d/K15jboss
   ln -s /etc/rc.d/init.d/jboss /etc/rc2.d/K15jboss
   ```

5. Test the script by running it with the following commands:

   ```
   Run JBoss:
   /etc/init.d/jboss start
   ```

   The CA GovernanceMinder server becomes available in a few moments.

   ```
   Stop JBoss:
   /etc/init.d/jboss stop
   ```

   You have configured the JBoss application daemon as a web service, and it automatically launches when you restart the computer.

Chapter 8: Installing CA GovernanceMinder and Oracle RAC

This scenario describes how to install CA GovernanceMinder with Oracle Real Application Clusters (RAC).

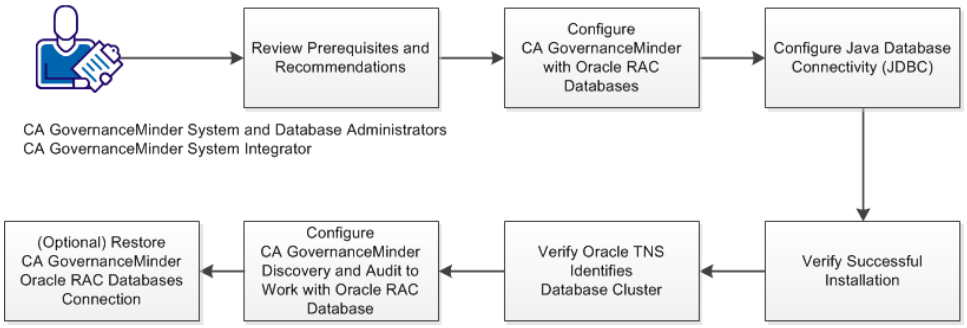
This scenario targets the following CA GovernanceMinder users:

- System and database administrators
- System integrators

How to Install CA GovernanceMinder and Oracle RAC

You configure CA GovernanceMinder to function in an Oracle RAC environment. Oracle RAC provides clustering and high availability software for Oracle database environments.

The following diagram illustrates how to install CA GovernanceMinder with Oracle RAC databases:



Follow these steps to install CA GovernanceMinder with Oracle RAC databases:

1. Review prerequisites and recommendations.
2. Configure CA GovernanceMinder with Oracle RAC databases.
3. Configure Java Database Connectivity (JDBC).
4. Verify successful installation.
5. Verify Oracle TNS Identifies Database Cluster.
6. Integrate CA GovernanceMinder Discovery and Audit with Oracle RAC databases.
7. (Optional) Restore CA GovernanceMinder Oracle RAC databases connection.

Review CA GovernanceMinder and Oracle RAC Prerequisites

This section lists CA GovernanceMinder and Oracle RAC prerequisites.

- CA GovernanceMinder databases must use UTF-8 (AL32UTF8) encoding.
- We recommend enabling 400 connections for each CA GovernanceMinder server that is connected to the same database, even if they are connected to different schemas.
- We recommend that you expand the CA GovernanceMinder cache memory limits to support considerable CA GovernanceMinder configurations. The default setting limits the memory cache to 500,000 elements. We recommend that you reset the CA GovernanceMinder cache limits to 900,000 elements.

Configure CA GovernanceMinder with Oracle RAC Databases

You configure CA GovernanceMinder with Oracle RAC databases by adding roles, establishing communication, and defining parameters.

Follow these steps:

1. Create a CA GovernanceMinder database user (schema). This user must have the following permissions and settings:
   - Roles: CONNECT, RESOURCE
   - System Privileges: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW, CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE, SELECT ANY DICTIONARY

   The CONNECT role provides the create session permission. The RESOURCE role provides several create system privileges, and provides for previous Oracle database compatibility releases.

2. Edit the tnsnames.ora file for the database cluster from the database server.

   You modify the tnsnames.ora file by adding your cluster address and port. The Oracle client uses the tnsnames.ora file to connect to the Oracle server. Do the following:

   a. Locate the tnsnames.ora file in the Oracle home directory. The tnsnames.ora file is located in the following folder:
   Oracle_home/NETWORK/ADMIN

   b. Locate the instances that define your clustered service and add your cluster address and port.

      Example:

```
RCMDB1 =
   (DESCRIPTION =
     (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode1-vip)(PORT = 1521))
     (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode2-vip)(PORT = 1521))
     (LOAD_BALANCE = yes)
     (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = RCMDB1
   )
)
```

      In this example, your Oracle RAC cluster and port have been defined.

   c. Save and close the file.

      The tnsnames.ora file is edited.

3. Update the hosts file to define current cluster nodes.

   You define the IP addresses and the Oracle RAC host names. Do the following:

   a. Locate the hosts file in the following folder:

      gm_install/Windows/System32/drivers/etc

   b. Define the IP addresses and the Oracle RAC host names.

   c. Save and close the file.

      You have updated the hosts file to define the current cluster nodes.

      Example: In this example, in the # RAC VIRTUAL INTERFACES section, IP address 10.0.0.82 is defined as rac1-vip.localdomain, and IP address 10.0.0.83 is defined as rac2-vip.localdomain.

      ```
      ##########################################
      # Do not remove the following line, or various programs
      # that require network functionality will fail.
      127.0.0.1       localhost.localdomain localhost
      10.0.0.39       ca_gm_linux46.localdomain   ca_gm_linux46
      # RAC VIRTUAL INTERFACES
      10.0.0.82       rac1-vip.localdomain    rac1-vip
      10.0.0.83       rac2-vip.localdomain    rac2-vip
      # RAC PUBLIC INTERFACES
      10.0.0.182      rac1.localdomain        rac1
      10.0.0.183      rac2.localdomain        rac2
      ##########################################
      ```

4. Edit the eurekify.properties file to define the database host name as the CA GovernanceMinder SDB database. The SDB contains CA GovernanceMinder Master and Model data.

   Important! When you upgrade from CA GovernanceMinder 12.5 SPx with Oracle RAC, edit this property file after the upgrade process completes.

   a. Locate the eurekify.properties file in the following folder:

      gm_install/Program Files/CA/RCM/Server/eurekify-jboss/conf/

      Note: *gm_install* is the CA GovernanceMinder installation directory.

b. Add the following property:

```
sdb.host=RCMDB1
```

Note: *RCMDB1* is the Oracle RAC database service name as defined above.

c. Save and close the file.

You have edited the eurekify.properties file to define the database host name as the CA GovernanceMinder SDB database.

Note: Update this property file in each node when you configure CA GovernanceMinder to work in a cluster.

5. Run the CA GovernanceMinder installer, and in the database parameters section, define the following database parameters:

- **Oracle Server Host** - The IP address of one of the cluster nodes.
- **Oracle Service name** - Cluster Database service name (not the nodes).

Example:

```
Specify Oracle SQL Server Information

Oracle Server Host (DEFAULT: rcmlinux46.localdomain): rac1

Oracle Service Name (DEFAULT: ORCL): RCMDB1

Specify Oracle Server port (DEFAULT: 1521):1521
```

Note: For more information, refer to the *CA GovernanceMinder Installation Guide*.

6. Increase the database sessions and processes parameters from the default setting to reduce exceptions.

a. Connect to the database with the system account.

b. Run the following commands:

```
alter system set sessions=400 scope=spfile;

alter system set processes=400 scope=spfile;
```

c. Restart the entire database (all cluster instances).

Database sessions and process parameters are increased.

You have configured CA GovernanceMinder with Oracle RAC databases. You now configure JDBC connectivity.

Configure Java Database Connectivity (JDBC)

You configure the JDBC to connect to a database and increase default cache settings. JDBC, an API for the Java programming language, defines how a client accesses a database by providing querying methods and updating database data.

Follow these steps:

1. Backup the eurekify-ds.xml and wp-ds.xml files from the following folder:

   gm_install/CA/RCM/Server/eurekify-jboss/server/eurekify/deploy/

2. Update JDBC URL values to define Oracle RAC database cluster rac1-vip and rac2-vip. Do the following:

   a. Locate the following elements in both files:

      ```
      <connection-url>jdbc:oracle:thin:@rac:1521/RCMDB1</connection-url>
      ```

   b. Replace with the following text that defines the JDBC URL to Oracle RAC cluster rac1-vip and rac2-vip databases:

      ```
      <connection-url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
      (ADDRESS=(PROTOCOL=TCP)(HOST=rac1-vip.localdomain) (PORT=1521))
      (ADDRESS=(PROTOCOL=TCP)(HOST=rac2-vip.localdomain) (PORT=1521))
      (CONNECT_DATA=(SERVICE_NAME=RCMDB1)))</connection-url>
      ```

   c. Save and close the files.

      The JDBC URL values define Oracle RAC database cluster rac1-vip and rac2-vip.

3. Reset the CA GovernanceMinder cache limits, as follows:

   a. Edit the **ehcache-sageDal.xml** file on the CA GovernanceMinder server:

      - For JBoss, this file is found in the following location:

        jboss_install\server\all\farm\eurekfiy.war\WEB-INF\classes\

      - For WebSphere, this file is located in the eurekify.ear file found in the following location:

        /eurekify.war/WEB-INF/classes

   b. In the **defaultCache** entry, change the following attribute:

      maxElementsInMemory

      Defines the maximum number of elements stored in cache memory.

      We recommend that you set this field using the following formula:

      maxElementsInMemory = total number of entities * 3

      For example, if you have one universe with 500,000 users and 500,000 roles, set maxElementsInMemory to 3,000,000 elements.

      If you have two universes, each with 500,000 users and 500,000 roles, set maxElementsInMemory to 6,000,000 elements.

   c. Save and close the file.

      The CA GovernanceMinder cache limits are reset.

      You have configured the JDBC. You now verify a successful CA GovernanceMinder installation.

Verify a Successful Installation

Verify a successful CA GovernanceMinder Windows or Linux installation.

You can access the CA GovernanceMinder portal when you have successfully installed CA GovernanceMinder on a JBoss cluster.

Follow these steps:

1. Select one server from the CA GovernanceMinder cluster and start it.
2. Review the started server logs and verify no log errors exist.
3. Start all other servers in the CA GovernanceMinder cluster.
4. Review all CA GovernanceMinder cluster logs and verify that no errors exist in the logs.

   When the installation is successful, you can access the CA GovernanceMinder portal.

5. Open a browser and enter the following URL:

   `http://serverhost:port/eurekify/portal/login`

   Note: *serverhost:port* is the network address and communications port of the CA GovernanceMinder server or load balancer. The JBoss/Windows server default port is 8080.

6. Log in using the default administration credentials:

   - **Username:** AD1\EAdmin
   - **Password:** eurekify

   Note: The password can be any password. It must be at least one character. The field must not be blank.

7. Set your Property and Common Property URL settings under Administration, Settings.

8. (Linux only) Update Workpoint DB administration to the load balancer server.

9. Navigate to Reports, Configuration Reports, select Configuration Properties and select ConfigWithRoles. This action verifies that the report application is working.

10. (Upgrade only) Clear the browser cache or refresh the web page to replace old graphical elements.

Verify Oracle TNS Identifies Database Cluster

You verify that the Oracle TNS entries in the tnsnames.ora file identify your Oracle RAC database structure. Oracle Transparent Network Substrate (TNS) provides a network platform of different protocols to function as a homogeneous network. The tnsnames.ora file is a configuration file that defines database addresses by establishing connections to them.

Follow these steps:

1. Locate the tnsnames.ora file on the computer hosting the CA GovernanceMinder Discovery and Audit tool.

   The tnsnames.ora file is located in the following folder:

   Oracle_home/NETWORK/ADMIN

2. Open the tnsnames.ora file and verify that the existence of TNS entries identifies your database cluster.

   Example:

```
RCMDB1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.localdomain)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.localdomain)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = RCMDB1)
    )
  )
```

3. Save and close the file.

   You have verified that the Oracle TNS entries in the tnsnames.ora file identify your Oracle RAC database structure. You now install and configure CA GovernanceMinder Discovery and Audit tools to work with Oracle RAC databases.

Integrate CA GovernanceMinder Discovery and Audit with Oracle RAC Databases

You integrate the CA GovernanceMinder Discovery and Audit tool with Oracle RAC databases to import and modify data, analyze, construct and administer the role hierarchy.

Follow these steps:

1. Run the CA GovernanceMinder Client Tools installer and open the application.

   The CA GovernanceMinder Client Tools installer, CA-RCM-*RN*-Client-Tools-x86.zip, is located in the folder where you downloaded the installation package files when you installed CA GovernanceMinder.

   Note: *RN* is the current release number for the product.

   The CA Role and Compliance Manager - Discover and Audit window appears.

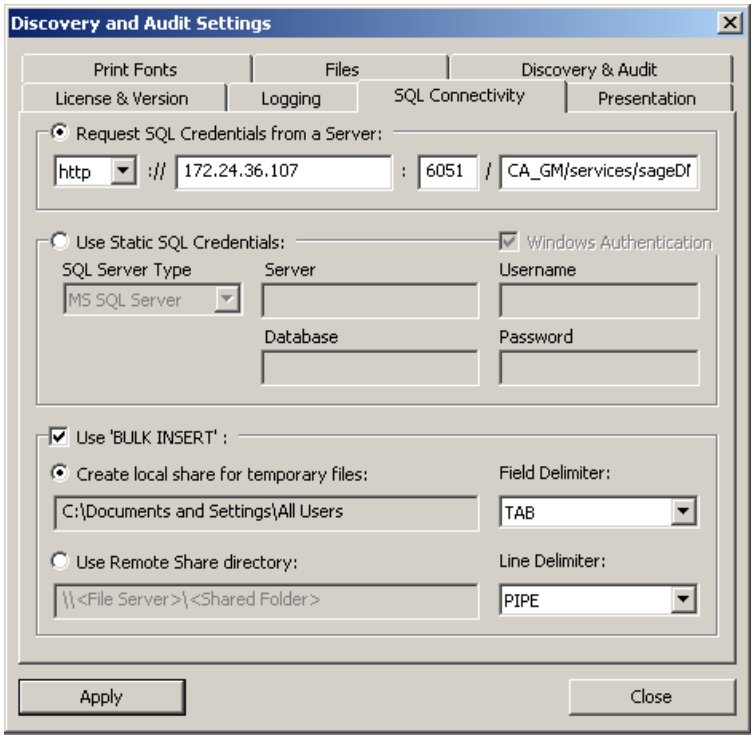
2. Navigate to File, General Settings.

   The Discovery and Audit Settings window appears.

3. In the SQL Connectivity tab, select Request SQL Credentials from a Server.

   This option connects the SQL database through the CA GovernanceMinder server.

   The following graphic displays the Request SQL Credentials from a Server option that is selected with an example server host IP address and port number displayed:



4. Enter in the CA GovernanceMinder server host name and the CA GovernanceMinder Server port number and click Apply.

   The Enter Server Credentials window appears.

5. In the SQL Server section, enter in the user name and password.

6. In the Web Server section, enter in the CA GovernanceMinder Portal administrator and password, and click OK.

7. In the Discovery and Audit Settings window, click Close.

   The CA GovernanceMinder Discovery and Audit tool is integrated to connect with Oracle RAC databases to manage data.

(Optional) Restore CA GovernanceMinder-Oracle RAC Databases Connection

You restore the connection between CA GovernanceMinder and Oracle RAC databases after a failure. Connection failures can occur when you connect to the SQL database through the CA GovernanceMinder server.

Follow these steps:

1. Edit the tnsnames.ora file for the database cluster from the database server. Do the following:
   a. Locate the tnsnames.ora file in the Oracle home directory.
   b. Locate the instances that represent your clustered service and verify your cluster address and port.

      Example:

      ```
      RCMDB1 =
         (DESCRIPTION =
           (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode1-vip)(PORT = 1521))
           (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode2-vip)(PORT = 1521))
           (LOAD_BALANCE = yes)
           (CONNECT_DATA =
            (SERVER = DEDICATED)
            (SERVICE_NAME = RCMDB1
         )
      )
      ```

   c. Save and close the file.

      The tnsnames.ora file is edited, and the Oracle client-server connection is restored.

2. Edit the eurekify.properties file to define the database host name as the CA GovernanceMinder SDB database. The SDB contains CA GovernanceMinder Master and Model data.

   Do the following:

   a. Locate the eurekify.properties file in the following folder:

      gm_install/Program Files/CA\RCM/Server/eurekify-jboss/conf

   b. Add the following property to define the database host name as the CA GovernanceMinder SDB database:

      sdb.host=*RCMDB1*

      Note: *RCMDB1* is the Oracle RAC database host name.

   c. Save and close the file.

      The eurekify.properties file is edited to define the database host name as the CA GovernanceMinder SDB database.

3. On the CA GovernanceMinder installation computer, open Oracle SQL Developer or similar program for working with SQL in Oracle databases.

4. Connect to the eurekify_sdb database, and insert the following text:

   ```
   insert into SAGE_PREFERENCES
   (LoginID, PrefGroup, Name, Value)
   values
   ('eurekify.properties', 'eurekify.properties.dynamic', 'sdb.host', 'RCMDB1');
   ```

5. In the Query menu, select Execute to run the SQL query.

   The CA GovernanceMinder and Oracle RAC databases connection is restored.