i2b2: Security Baseline

UTHealth

The University of Texas
Health Science Center at Houston

Contents

Introduction

This document outlines the minimal recommended security configurations for i2b2 v1.6 and CentOS. This guide covers security configurations for the CentOS operating system, SSL configuration and procedures to encrypt the database configuration files for i2b2 v1.6. Prior to using this guide, ensure i2b2 v1.6 is running correctly in your environment and CentOS is up-to-date. This guide is intended for administrators with root privileges in CentOS. All codes presented in this document are prefixed with a "#" and is intended for CentOS 64-bit. Adjust the code accordingly if you are running CentOS 32-bit.

CentOS Security Configuration

Firewalls

The easiest way to configure the firewall in CentOS is through the GUI. The minimum port that should be open is *Secure WWW (HTTPS)*.

SELinux

Disable SELinux by opening a terminal and edit the SELinux configuration file /etc/selinux/config.

Edit: SELINUX=disabled

Restart the server for the changes to take effect.

SSL Configuration

Apache2

Apache2 is setup as a SSL proxy to JBoss and as a SSL web server for the i2b2 admin and i2b2 webclient.

SSL

To setup SSL, install mod_ssl and obtain a CA certificate.

1. Install mod_ssl:

```
# yum install mod_ssl
```

2. Edit the following in /etc/httpd/conf.d/ssl.conf to disable weak encryption:

```
SSLProtocol –all +SSLv3 +TLSv1
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
SSLCertificateFile <location of your CA cert>
SSLCertificateKeyFile <location of your private key>
```

3. Save the changes.

ProxyPass

ProxyPass is enabled to provide SSL support to JBoss through Apache2. ProxyPass is enabled in /etc/httpd/conf.d/ssl.conf for SSL connections and is enabled in /etc/httpd/conf.d/proxy_ajp.conf for non-SSL connections.

For SSL connections, add the following lines to the bottom of /etc/httpd/conf.d/ssl.conf:

```
ProxyPass /i2b2/ ajp://localhost:9009/i2b2/
ProxyPassReverse /i2b2/ ajp://localhost:9009/i2b2
```

For Non-SSL connections, add the following lines to the bottom of /etc/httpd/conf.d/proxy_ajp.conf:

```
ProxyPass /i2b2/ ajp://localhost:9009/i2b2/
ProxyPassReverse /i2b2/ ajp://localhost:9009/i2b2
```

Restart Apache2 for the changes to take effect (service httpd restart).

Database Configuration Files

There are several xml files that contain clear text username and passwords for the various i2b2 databases. There are database configuration files in /opt/jboss-4.2.2.GA/server/default/deploy/*-ds.xml and Spring Framework files in /opt/jboss-4.2.2.Ga/server/default/conf.

*Encrypting the Database Configuration Files in *-ds.xml*

The *-ds.xml database configuration files will be encrypted using the SecureIdentityLoginModule method. The examples below show configurations for pm-ds.xml, ont-ds.xml, crc-ds.xml, crc-jms-ds.xml, and work-ds.xml.

1. Encrypt the database password

```
# cd /opt/jboss-4.2.2.GA

# java -classpath lib/jboss-
common.jar:lib/jboss_jmx.jar:server/default/lib/jbosssx.jar:server/default/lib/jbossjca.jar
org.jboss.resource.security.SecureIdentityLoginModule <db_password>
```

2. This will output the encrypted password.
3. Define the application policy in /opt/jboss-4.2.2.GA/server/default/conf/login-config.xml. The following lines are an example of configuring i2b2 with the demo data. Adjust the file accordingly based on your configuration. Add the following to the end of the file, replacing the password with the encrypted password that was obtained in step 2:

```
  <application-policy name="EncryptedPMBootStrapDS">
    <authentication>
      <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
        <module-option name="username">i2b2hive</module-option>
        <module-option name="password">encrypted_pw_here</module-option>
        <module-option
name="managedConnectionFactoryName">jboss.jca:name=PMBootStrapDS,service=LocalTxCM</module-
option>
      </login-module>
    </authentication>
  </application-policy>


  <application-policy name="EncryptedOntologyBootStrapDS">
    <authentication>
      <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
        <module-option name="username">i2b2hive</module-option>
        <module-option name="password">encrypted_pw_here</module-option>
        <module-option
name="managedConnectionFactoryName">jboss.jca:name=OntologyBootStrapDS,service=LocalTxCM</m
odule-option>
      </login-module>
    </authentication>
  </application-policy>


  <application-policy name="EncryptedOntologyDemoDS">
    <authentication>
      <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
```

```
        <module-option name="username">i2b2metadata</module-option>
        <module-option name="password">encrypted_pw_here</module-option>
        <module-option
name="managedConnectionFactoryName">jboss.jca:name=OntologyDemoDS,service=LocalTxCM</modul
e-option>
      </login-module>
    </authentication>
  </application-policy>


  <application-policy name="EncryptedQueryToolDemoDS">
    <authentication>
      <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
        <module-option name="username">i2b2demodata</module-option>
        <module-option name="password">encrypted_pw_here</module-option>
        <module-option
name="managedConnectionFactoryName">jboss.jca:name=QueryToolDemoDS,service=LocalTxCM</mod
ule-option>
      </login-module>
    </authentication>
  </application-policy>


         <application-policy name="EncryptedDefaultDS">
    <authentication>
      <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
        <module-option name="username">i2b2hive</module-option>
        <module-option name="password">encrypted_pw_here</module-option>
        <module-option
name="managedConnectionFactoryName">jboss.jca:name=DefaultDS,service=LocalTxCM</module-
option>
      </login-module>
    </authentication>
  </application-policy>


         <application-policy name="EncryptedWorkplaceBootStrapDS">
    <authentication>
      <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
        <module-option name="username">i2b2hive</module-option>
        <module-option name="password">encrypted_pw_here</module-option>
        <module-option
name="managedConnectionFactoryName">jboss.jca:name=WorkplaceBootStrapDS,service=LocalTxCM</
module-option>
      </login-module>
    </authentication>
  </application-policy>


  <application-policy name="EncryptedWorkplaceDemoDS">
    <authentication>
      <login-module code="org.jboss.resource.security.SecureIdentityLoginModule" flag="required">
        <module-option name="username">i2b2workdata</module-option>
        <module-option name="password">encrypted_pw_here</module-option>
        <module-option
name="managedConnectionFactoryName">jboss.jca:name=WorkplaceDemoDS,service=LocalTxCM</mod
ule-option>
      </login-module>
    </authentication>
  </application-policy>
```

4. Replace the username and password in each *-ds.xml file with the <security-domain> created in the login-conf.xml.

```
<!-- ##########################################################################
# pm-ds.xml
############################################################################-->
<datasources>
  <local-tx-datasource>
    <jndi-name>PMBootStrapDS</jndi-name>
      <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
      <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
      <security-domain>EncryptedPMBootStrapDS</security-domain>
    </local-tx-datasource>

</datasources>


<!-- ##########################################################################
# ont-ds.xml
############################################################################-->
<datasources>
    <local-tx-datasource>
    <jndi-name>OntologyBootStrapDS</jndi-name>

      <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
      <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
      <security-domain>EncryptedOntologyBootStrapDS</security-domain>
    </local-tx-datasource>

     <!-- sample oracle project data source   -->
 <local-tx-datasource>
    <jndi-name>OntologyDemoDS</jndi-name>
      <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
      <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
      <security-domain>EncryptedOntologyDemoDS</security-domain>
    </local-tx-datasource>

</datasources>


<!-- ##########################################################################
# crc-ds.xml
############################################################################-->
<datasources>
  <local-tx-datasource>
    <jndi-name>QueryToolDemoDS</jndi-name>
    <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
    <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
    <security-domain>EncryptedQueryToolDemoDS</security-domain>
    <idle-timeout-minutes>1</idle-timeout-minutes>
    <exception-sorter-class-
name>org.jboss.resource.adapter.jdbc.vendor.OracleExceptionSorter</exception-sorter-class-name>
    <metadata>
      <type-mapping>Oracle9i</type-mapping>
    </metadata>
  </local-tx-datasource>

</datasources>


<!-- ##########################################################################
```

```
# crc-jms-ds.xml
###########################################################################-->
<datasources>
  <local-tx-datasource>
    <jndi-name>DefaultDS</jndi-name>
    <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
    <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
    <security-domain>EncryptedDefaultDS</security-domain>
    <idle-timeout-minutes>1</idle-timeout-minutes>
    <exception-sorter-class-
name>org.jboss.resource.adapter.jdbc.vendor.OracleExceptionSorter</exception-sorter-class-name>
    <metadata>
      <type-mapping>Oracle9i</type-mapping>
    </metadata>
  </local-tx-datasource>

</datasources>


<!-- #########################################################################
# work-ds.xml
###########################################################################-->
<datasources>
  <local-tx-datasource>
    <jndi-name>WorkplaceBootStrapDS</jndi-name>
    <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
    <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
    <security-domain>EncryptedWorkplaceBootStrapDS</security-domain>
    <idle-timeout-minutes>1</idle-timeout-minutes>
    <exception-sorter-class-
name>org.jboss.resource.adapter.jdbc.vendor.OracleExceptionSorter</exception-sorter-class-name>
    <metadata>
      <type-mapping>Oracle9i</type-mapping>
    </metadata>
  </local-tx-datasource>

  <local-tx-datasource>
    <jndi-name>WorkplaceDemoDS</jndi-name>
    <connection-url>jdbc:oracle:thin:@localhost:1521:xe</connection-url>
    <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
    <security-domain>EncryptedWorkplaceDemoDS</security-domain>
    <idle-timeout-minutes>1</idle-timeout-minutes>
    <exception-sorter-class-
name>org.jboss.resource.adapter.jdbc.vendor.OracleExceptionSorter</exception-sorter-class-name>
    <metadata>
      <type-mapping>Oracle9i</type-mapping>
    </metadata>
  </local-tx-datasource>

</datasources>
```

5. Restart JBoss for the changes to take effect and ensure you have no errors.

Encrypting the Database Configuration Files in the Spring Framework

There are a few Spring bean configuration files that contain database usernames and passwords that will need to be encrypted using Jasypt. Jasypt is an open source product called Java Simplified Encryption (JASYPT) which allows decryption of encrypted text at run-time. Jasypt is used to encrypt the username/password of the Hive database located in the following Spring configuration files:

Directory	Bean ID
$JBOSS_HOME/server/default/conf/crcapp/CRCApplicationContext.xml	CRCDataSourceLookup
$JBOSS_HOME/server/default/conf/crcloader/CRCLoaderApplicationContext.xml	LoaderLookupDS

1. Download Jasypt from www.jasypt.org.
2. Unzip Jasypt:

```
# unzip jasypt-1.7-dist.zip
```

3. Change to the location where Jasypt was unzipped.

```
# cd jasypt-1.7/bin
```

4. Use Jasypt encryption tool to encrypt your database password.

```
# ./encrypt.sh input=”db_password” algorithm=PBEWithMD5AndTripleDES password=encryption_password
```

5. Jasypt will then output the encrypted password (+Sy2mi3vh/sDHWeFiHeqxSo3eewSY0XZ is the output in our example).
6. Move your credentials into a properties file. In this example, it is named *jasypt.properties*.

```
dataSource.username=i2b2hive
dataSource.password=ENC(+Sy2mi3vh/sDHWeFiHeqxSo3eewSY0XZ)
```

7. Edit $JBOSS_HOME/server/default/conf/crcapp/CRCApplicationContext.xml as below:

```
<bean id="propertyPlaceholderConfigurer"
class="org.jasypt.spring.properties.EncryptablePropertyPlaceholderConfigurer">
        <constructor-arg ref="configurationEncryptor" />
        <property name="location" value="jasypt.properties" />
</bean>

<bean id="configurationEncryptor" class="org.jasypt.encryption.pbe.StandardPBEStringEncryptor">
        <property name="config" ref="environmentVariablesConfiguration" />
</bean>

<bean id="environmentVariablesConfiguration"
class="org.jasypt.encryption.pbe.config.EnvironmentStringPBEConfig">
        <property name="algorithm" value="PBEWithMD5AndDES" />
        <property name="passwordEnvName" value="PBE_PASSWORD" />
        <property name="password" value="encryption_password" />
</bean>

 <bean id="CRCDataSourceLookup" class="org.apache.commons.dbcp.BasicDataSource" destroy-
method="close">
         <property name="driverClassName" value="oracle.jdbc.driver.OracleDriver"/>
         <property name="url" value="jdbc:oracle:thin:@localhost:1521:xe"/>
```

```
                <property name="username" value="${dataSource.username}"/>
                <property name="password" value="${dataSource.password}"/>
        </bean>
```

8. Repeat this process for LoaderLookupDS and any additional Spring configuration files.
9. Restart JBoss for your changes to take affect.

Revision History

Identify document changes	Ver	Date	Author
Initial Document	V1.0	4-28-11	J. Phan
Minor Updates	V1.1	10-7-11	J. Phan