**Contents**

[1 About This Document 1](#_Toc134612580)

[2 Prepare the deployable artifacts 1](#_Toc134612581)

[3 Deployment Procedure 3](#_Toc134612582)

## 1 About This Document

This document covers the deployment process for the rule engine applications in SIB environment.The first release involved installation of below applications.

|  |  |  |
| --- | --- | --- |
| **S.No** | **Application** | **Description** |
| 1 | Rule Engine UI | User interface for the Rule Engine with LDAP authentication. |
| 2 | Rule Engine API | API to perform functionalities of Rule Engine. |
| 3 | Rule Engine User Management API | API to manage user and roles. |
| 4 | Database | Database for Rule Engine and User Management |

## 2 Prepare the deployable artifacts

Prepare the binaries required for the deployment.

* RuleEngine.zip
  + [https://github.com/cognicx-it-solutions/Front\_end\_rule\_engine.git](about:blank) - branch: sib
  + In public/envconfig.js, mention the service URL of rule engine APIs for the targeted environment.
    - For UAT environment as below
    - const apiService = 'http://10.64.32.218:8081/rule/ruleEngine/'
    - const apiUserService = 'http://10.64.32.218:8081/userRule/'
  + run the command ‘npm run --save build’ to generate to UI build contents
  + Zip the contents of build folder to RuleEngine.zip
* rule.war
  + [https://github.com/cognicx-it-solutions/rule-engine-v2.git](about:blank) - branch: sib

The properties for the UAT and Prod environments are externalized out of the war in a predefined location in the UAT and Prod servers. It is referred inside the war from the corresponding locations. D:/RuleEngine/ruleengine-uat.properties, D:/RuleEngine/ruleengine-prod.properties.

* + - Build the war for the targeted environment using the command

mvn clean install –Puat / mvn clean install –Pprod

* + - Rename the war to rule.war
* userRule.war
  + [https://github.com/cognicx-it-solutions/rule\_Engine\_user\_management.git](about:blank) - branch: sib

The properties for the UAT and Prod environments are externalized out of the war in a predefined location in the UAT and Prod servers. It is referred inside the war from the corresponding locations. D:/RuleEngine/ruleengineuser-uat.properties, D:/RuleEngine/ruleengineuser-prod.properties.

* + - Build the war for the targeted environment using the command

mvn clean install –Puat / mvn clean install –Pprod

* + - Rename the war to userRule.war
* IVRrule\_ngdb\_script\_V1.sql, IVRrule\_ngdb\_script\_Metadata\_V1.sql – scripts available in setup folder in the git repository
* IVRrule\_engdb\_UM\_V1.sql, IVRrule\_engdb\_UM\_Metadata\_V1.sql - scripts available in setup folder in the git repository

## 3 Deployment Procedure

1. Install two instances of Tomcat10.0.27 (Tomcat10.0.27\_8080, Tomcat10.0.27\_8081) pointing to jdk18 under port 8080 and 8081 for the API (invocation of external app like CTI) and UI+API respectively.
2. Perform hardening steps in both instances of tomcat. (Refer the hardening document)
3. Create databases for the Rule Engine(rule\_Engine), Rule Engine User Management (user\_management) and setup corresponding users for the same.
4. Run the DBScripts which contains below
   1. New Tables
   2. New Stored Procedures
   3. Metadata insertion scripts
5. Place the rule.war, userRule.war in webapps-javaee folder of Tomcat10.0.27\_8080.
6. Place the RuleEngine folder extracted from RuleEngine.zip in the webapps folder, rule.war, userRule.war in webapps-javaee folder of Tomcat10.0.27\_8081.
7. Configure appropriate endpoints in the API service URLs of envconfig.js under Tomcat10.0.27/webapps/RuleEngine.
8. Start the Tomcat10.0.27\_8080, Tomcat10.0.27\_8081 services.
9. Create multipart file location folder ‘upload’ under Tomcat10.0.27/work/Catalina/localhost/rule.
10. Access Rule Engine UI via load balancer, login as the support\_uat and do any further setup.
11. Steps to import certificate for using LDAP over SSL

For communicating to LDAPS for user authentication in higher environments like UAT, we need to import the corresponding Ldap certificate in the JRE as below.

* Navigate to the JDK-install-dir/jre/bin directory. Use the JDK that was specified during the installation of the Repository.

Run the following command:

|  |
| --- |
| keytool -import -trustcacerts -alias alias -file certificate\_filename  -keystore cacerts\_filename |

* For the -alias option, you can assign any value.
* For the -file option, specify the fully qualified name of the LDAP server’s certificate. For example:

|  |
| --- |
| D:\LDAPS\SIB.cer |

* For the -keystore option, specify the fully qualified name of the cacerts file. The cacerts file is located in the JDK-install-dir/jre/lib/security directory. For example:

|  |
| --- |
| C:\Program Files\Java\jdk18\*\jre\lib\security\cacerts |

When prompted, enter the keystore password. The default password is changeit.

When prompted to trust this certificate, enter yes.

The following message appears:

|  |
| --- |
| Certificate was added to keystore |