**ИНТЕГРАЦИЯ Tomcat 9.0.0.M9 и JTLS**

Сначала следует ознакомиться с инструкцией *How\_to\_set\_gost\_tls\_tomcat.docx* в папке *Doc\WebServerIntegration\Tomcat*.

**Дополнительные сведения.**

В связи с серьезными изменениями, которым подвергся код *tomcat* (в частности, tomcat-coyote.jar, начиная примерно с версии 8.5), сделан адаптер *JCPTomcatAdapter*, расширяющий стандартный класс *JCPJSSEImplementation*, для обеспечения взаимодействия *tomcat* *9.0.0.M9* и *cpSSL*.

В tomcat'е появились два класса, предоставляющих несколько разные алгоритмы работы с *Connector*'ом tomcat'а (*lib\tomcat-coyote.jar\org\apache\tomcat\util\net\):*

*jsse/JSSEImplementation*

*openssl/OpenSSLImplementation*

По умолчанию, когда в *Connector*’е не задан параметр *sslImplementationName*, используется *OpenSSLImplementation*. Но *JSSEImplementation* ближе всего к старому *tomcat*.

[*https://tomcat.apache.org/tomcat-9.0-doc/config/http.html#SSL\_Support\_-\_SSLHostConfig*](https://tomcat.apache.org/tomcat-9.0-doc/config/http.html#SSL_Support_-_SSLHostConfig)

[*https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html*](https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html)

Класс *JCPJSSEImplementation* модуля *JCPTomcatAdapter* расширяет класс *JSSEImplementation*, обеспечивая корректное чтение параметров коннектора в новом формате (*Connector* -> *SSLHostConfig* -> *Certificate*) для *cpSSL* (некоторые параметры типа алгоритмов не используются).

Исходные коды адаптера приложены в виде *maven*-проекта *JCPTomcatAdapter*. Проект имеет несколько зависимостей - *tomcat-coyote, tomcat-juli, JCP, cpSSL*. Собирать проект следует с помощью *JDK* 8. Собранная библиотека *JCPTomcatAdapter* лежит в папке *Doc\WebServerIntegration\Tomcat9\JCPTomcatAdapter\target* проекта.

Для использования *JCPTomcatAdapter* готовую библиотеку следует положить в папку *{tomcat\_dir}\lib\ tomcat’*а, где *{tomcat\_dir} –* папка установленного веб-сервера*.* Соответственно, *JCP* и *cpSSL* должны быть установлены в эксплуатируемую веб-сервером JRE 8*.*

\*\*\*

Пример коннектора (*tomcat* 9.0.0.M9) с включенной аутентификацией клиента:

*<Connector*

*port="8443"*

*protocol="org.apache.coyote.http11.Http11NioProtocol"*

***sslImplementationName****="****ru.CryptoPro.ssl.tomcat.jsse.JCPJSSEImplementation****"*

*maxThreads="150"*

*secure="true"*

*scheme="https"*

*SSLEnabled="true" >*

*<SSLHostConfig*

*protocols="TLSv1"*

*sslProtocol="GostTLS"*

*truststoreFile="c:\tomcat9\test\_ca.store"*

*truststorePassword="1"*

*truststoreProvider="JCP"*

*truststoreType="CertStore"*

*certificateVerification="true" >*

*<Certificate*

*certificateKeystoreFile="c:\tomcat9\test\_ca.store"*

*certificateKeystorePassword="1"*

*certificateKeystoreProvider="JCP"*

*certificateKeystoreType="HDImageStore" />*

*</SSLHostConfig>*

*</Connector>*

Используется реализация *JCPJSSEImplementation* модуля *JCPTomcatAdapter*. Выбор ключевого контейнера сервера происходит по типу контейнера *certificateKeystoreType* и паролю для доступа к нему *certificateKeystorePassword*. Т.к. передается только информация о доверенном хранилище корневых сертификатов, то его пароль должен совпадать с паролем контейнера, который предполагается использовать в качестве серверного, т.е. *truststoreFile* совпадает с *certificateKeystoreFile*, *truststorePassword* - с *certificateKeystorePassword*.

*truststoreFile* - хранилище доверенных корневых сертификатов формата *CertStore* (JCP).

*truststorePassword* - пароль к нему.

*truststoreProvider* - провайдер для работы с хранилищем.

*truststoreType* - тип хранилища.

*certificateVerification* - параметр определяет, включена ли на сервере аутентификация клиента.

*certificateKeystoreFile* - хранилище доверенных корневых сертификатов формата *CertStore* (JCP).

*certificateKeystorePassword* - пароль к нему.

*certificateKeystoreProvider* - провайдер для работы с хранилищем.

*certificateKeystoreType* - тип хранилища.

В примере *c:\tomcat9\test\_ca.store* - это хранилище корневых сертификатов.