Hello Friends,

Can someone assist for the cipher suites are inappropriate error? I am using talend 6.3 and trying to setup tibco connectivity via SSL.

Client cert and CA cert have been defined properly. The same certs works for other ETL tools. I have no clue on the below error.

Starting job jms_ssl_conneectivity_cert at 16:03 08/10/2018.

[INFO]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - TalendJob: 'jms_ssl_conneectivity_cert' - Start.
[statistics] connecting to socket on port 3454
[statistics] connected
[trace] connecting to socket on port 5069
[trace] connected
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_3 - Start to work.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_3 - Parameters:LIBRARY = "slf4j-api-1.4.2.jar" | HOTLIBS = [] | IMPORT = //import java.util.List; |
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_3 - Done.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_2 - Start to work.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_2 - Parameters:LIBRARY = "slf4j-simple-1.4.2.jar" | HOTLIBS = [] | IMPORT = //import java.util.List; |
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_2 - Done.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_1 - Start to work.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_1 - Parameters:LIBRARY = "tibcrypt-6.3.jar" | HOTLIBS = [] | IMPORT = //import java.util.List; |
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLibraryLoad_1 - Done.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLogRow_1 - Start to work.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tLogRow_1 - Parameters:BASIC_MODE = true | TABLE_PRINT = false | VERTICAL = false | FIELDSEPARATOR = "|" | PRINT_HEADER = false | PRINT_UNIQUE_NAME = false | PRINT_COLNAMES = false | USE_FIXED_LENGTH = false | PRINT_CONTENT_WITH_LOG4J = true |
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tJMSInput_1 - Start to work.
[DEBUG]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tJMSInput_1 - ParametersRIVER_JAR = "tibjms-6.3.jar" | CONTEXT_PROVIDER = "com.tibco.tibjms.naming.TibjmsInitialContextFactory" | SERVER_URL = "ssl://gtcpi-XXXXXXXXXXXXXroot.net:4243" | CONN_FACTORY_NAME = "CB_sslQueueConnectionFactory" | USER_IDENTITY = true | USER = "XXXXXXX" | PASS = 2669... | MSGTYPE = Queue | FROM = "XXXXXXXXXXXXXX.Request" | TIMEOUT = -1 | MAX_MSG = -1 | MSG_SELECTOR = "" | PROCESSING_MODE = RAW | ADVANCED_PROPERTIES = [{PROPERTY="java.naming.security.principal", VALUE="XXXXXXXXX"}, {PROPERTY="java.naming.security.credentials", VALUE="XXXXXXXX"}, {PROPERTY="com.tibco.tibjms.naming.security_protocol", VALUE="ssl"}, {PROPERTY="com.tibco.tibjms.naming.ssl_enable_verify_host", VALUE="false"}, {PROPERTY="com.tibco.ems.ssl.identity", VALUE="C:/Users/Desktop/Talend/TIBCO/certs/XXXXXXXXX.ca1.cert.p12"}, {PROPERTY="com.tibco.tibjms.naming.ssl_password", VALUE="XXXXXr"}, {PROPERTY="com.tibco.tibjms.naming.ssl_trusted_certs", VALUE="C:/Users/Desktop/Talend/TIBCO/certs/XXXXXXXXCAChain.pem"}, {PROPERTY="com.tibco.tibjms.naming.ssl_auth_only", VALUE="true"}, {PROPERTY="com.tibco.tibjms.ssl.identity_encoding", VALUE="PEM"}, {PROPERTY="com.tibco.tibjms.naming.ssl_trace", VALUE="true"}, {PROPERTY="com.tibco.tibjms.naming.ssl_debug_trace", VALUE="true"}, {PROPERTY="com.tibco.tibjms.naming.ssl_vendor", VALUE="j2se-default"}] |
2018-10-08 16:03:17.824 [33439459 main] [TIBCO EMS]: [J] [SSL] initializing security with vendor 'j2se-default'
2018-10-08 16:03:17.961 [33439459 main] [TIBCO EMS]: [J] [SSL] client version 6.3.0, security version 2.14.100.006, SSL initialized with vendor 'j2se'
2018-10-08 16:03:17.961 [33439459 main] [TIBCO EMS]: [J] [SSL] WARNING: server verification is disabled, will trust any server.
142 [main] INFO com.tibco.security.impl.ooOO - Initializing JSSE's crypto provider class com.sun.net.ssl.internal.ssl.Provider in default mode
2018-10-08 16:03:18.249 [33439459 main] [TIBCO EMS]: [J] [SSL] client identity not set, using empty identity.
Ignoring disabled cipher suite: SSL_RSA_WITH_DES_CBC_SHA

Ignoring disabled cipher suite: SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
Ignoring disabled cipher suite: TLS_KRB5_WITH_DES_CBC_MD5
Ignoring disabled cipher suite: SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
Ignoring disabled cipher suite: SSL_DH_anon_WITH_DES_CBC_SHA
Ignoring disabled cipher suite: TLS_KRB5_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_KRB5_WITH_DES_CBC_SHA
Ignoring disabled cipher suite: TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5
Ignoring disabled cipher suite: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
Ignoring disabled cipher suite: SSL_DHE_RSA_WITH_DES_CBC_SHA
Ignoring disabled cipher suite: TLS_KRB5_WITH_3DES_EDE_CBC_MD5
Ignoring disabled cipher suite: SSL_DH_anon_WITH_RC4_128_MD5
Ignoring disabled cipher suite: SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: SSL_RSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDH_anon_WITH_RC4_128_SHA
Ignoring disabled cipher suite: SSL_DHE_DSS_WITH_DES_CBC_SHA
Ignoring disabled cipher suite: TLS_KRB5_EXPORT_WITH_RC4_40_SHA
Ignoring disabled cipher suite: SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
Ignoring disabled cipher suite: TLS_KRB5_WITH_RC4_128_SHA
Ignoring disabled cipher suite: SSL_RSA_EXPORT_WITH_RC4_40_MD5
Ignoring disabled cipher suite: TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA
Ignoring disabled cipher suite: TLS_KRB5_EXPORT_WITH_RC4_40_MD5
Ignoring disabled cipher suite: TLS_ECDH_ECDSA_WITH_RC4_128_SHA
Ignoring disabled cipher suite: TLS_KRB5_WITH_RC4_128_MD5
Ignoring disabled cipher suite: TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: SSL_RSA_WITH_RC4_128_SHA
Ignoring disabled cipher suite: TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDH_RSA_WITH_RC4_128_SHA
Ignoring disabled cipher suite: SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
Ignoring disabled cipher suite: SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDHE_RSA_WITH_RC4_128_SHA
Ignoring disabled cipher suite: SSL_RSA_WITH_RC4_128_MD5
Ignoring disabled cipher suite: TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: SSL_RSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
Ignoring disabled cipher suite: SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
trigger seeding of SecureRandom
done seeding SecureRandom
Exception in component tJMSInput_1
javax.naming.AuthenticationException: Not permitted: Failed to connect via SSL to [ssl://gtcpi-tibla01d.XXXXXXXXXXX:4243]: No appropriate protocol (protocol is disabled or cipher suites are inappropriate) [Root exception is javax.jms.JMSSecurityException: Failed to connect via SSL to [ssl://gtcpi-tibla01d.nam.nsroot.net:4243]: No appropriate protocol (protocol is disabled or cipher suites are inappropriate)]
at com.tibco.tibjms.naming.TibjmsContext.lookup(TibjmsContext.java:670)
at com.tibco.tibjms.naming.TibjmsContext.lookup(TibjmsContext.java:491)
at javax.naming.InitialContext.lookup(Unknown Source)
at test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert.tJMSInput_1Process(jms_ssl_conneectivity_cert.java:717)

at test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert.tLibraryLoad_1Process(jms_ssl_conneectivity_cert.java:1123)
at test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert.tLibraryLoad_2Process(jms_ssl_conneectivity_cert.java:1292)
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
main, handling exception: javax.net.ssl.SSLHandshakeException: No appropriate protocol (protocol is disabled or cipher suites are inappropriate)
main, SEND TLSv1.2 ALERT: fatal, description = handshake_failure
main, WRITE: TLSv1.2 Alert, length = 2
main, called closeSocket()
[FATAL]: test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert - tJMSInput_1 Not permitted: Failed to connect via SSL to [ssl://gtcpi-tibla01d.nam.nsroot.net:4243]: No appropriate protocol (protocol is disabled or cipher suites are inappropriate)
[statistics] disconnected
[trace] disconnected
at test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert.tLibraryLoad_3Process(jms_ssl_conneectivity_cert.java:1461)
at test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert.runJobInTOS(jms_ssl_conneectivity_cert.java:1721)
at test1.jms_ssl_conneectivity_cert_0_1.jms_ssl_conneectivity_cert.main(jms_ssl_conneectivity_cert.java:1548)
Caused by: javax.jms.JMSSecurityException: Failed to connect via SSL to [ssl://gtcpi-tibla01d.XXXXXXXXXXt:4243]: No appropriate protocol (protocol is disabled or cipher suites are inappropriate)
at com.tibco.tibjms.TibjmsxLinkSSL.connect(TibjmsxLinkSSL.java:427)
at com.tibco.tibjms.TibjmsConnection._create(TibjmsConnection.java:1308)
at com.tibco.tibjms.TibjmsConnection.<init>(TibjmsConnection.java:4185)
at com.tibco.tibjms.TibjmsQueueConnection.<init>(TibjmsQueueConnection.java:36)
at com.tibco.tibjms.TibjmsxCFImpl._createImpl(TibjmsxCFImpl.java:200)
at com.tibco.tibjms.TibjmsxCFImpl._createConnection(TibjmsxCFImpl.java:253)
at com.tibco.tibjms.TibjmsQueueConnectionFactory.createQueueConnection(TibjmsQueueConnectionFactory.java:87)
at com.tibco.tibjms.naming.TibjmsContext$Messenger.request(TibjmsContext.java:325)
at com.tibco.tibjms.naming.TibjmsContext.lookup(TibjmsContext.java:657)
... 8 more
Job jms_ssl_conneectivity_cert ended at 16:03 08/10/2018. [exit code=1]