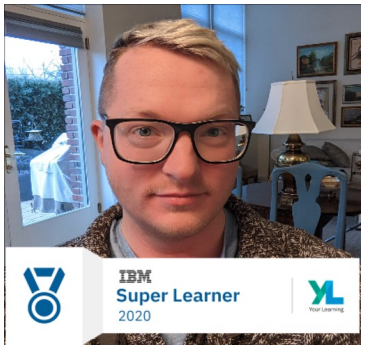
Securing JDBC Data Source



Kumaran Ayyakutti Nathan
J2C Support

James Stephen
J2C Development

Ajit Jariwala
SSL Security SME

Kyle Aure
J2C Development

Feb 23’2022

Agenda

- Minimum JDK support for TLSv1.2 and TLSv1.3
- Securing
  - DB2
  - Microsoft SQL
  - Oracle
- JDBC driver and FIPS
- Best Practice/Recommendations
- Demo – Showing traditional WebSphere Application Server (WSAS) configuration
- Question and Answer - Please post your questions in the chat

Minimum Java Level

Setup TLS on your system

- Identify Current Level of Java:
  - Run WAS_HOME/java/bin/java -version to find out the java versions
- Minimum Java version to support TLSv1.2
  - Java 6 – out of support
  - Java 7 – SR9 FP50
  - Java 7.1 – SR3 FP50
  - Java 8 – SR3 FP10

- Java 7/7.1 End Of support - July 2022 (WAS8.5.x) https://www.ibm.com/support/pages/node/6524282

- Minimum Java for TLSv1.3
  - Java 8 (8.0.6.25 and above) –for traditional WebSphere Application Server
  - WebSphere Liberty –openJ9 and JDK 11 or IBM Java 8 (8.0.6.25)

- To Verify Java SDK version shipped with IBM WebSphere Application Server fix packs: https://www.ibm.com/support/pages/node/317689

Engage vendor driver support team to confirm which version of driver supported with TLSv1.3

Securing DB2

Securing DB2

Required Custom Properties:

- **sslConnection**=true
- **sslVersion**=<version of protocol> (e.g., TLSv1.2)
- sslTrustStoreLocation=<trustStore location path>
- sslTrustStroePassword=<password>

- DB2 driver Versions and Downloads
- https://www.ibm.com/support/pages/db2-jdbc-driver-versions-and-downloads

To enable the custom property in the ISC admin console :
Click Data sources-> <data_source Name> -> WebSphere Application Server data source properties in the administrative console.

Securing DB2

Mutual Authentication enabled on Server side (Database Server)

- securityMechanism=18
- sslKeyStoreLocatoin=<keyStorelocation path>
- sslKeyStorePassword=<password>

Securing Microsoft SQL

Securing Microsoft SQL

Required Custom property :

- **sslProtocol=TLSv1.2**
- **encrypt=true** (Indicates if SSL (Secure Sockets Layer) encryption should be used for communication with the database. One of two ways to determine trust:
- **trustServerCertificate=true** (default is false)
  Determines if the JDBC driver validates the SSL certificate of the database. A value of false causes the JDBC driver to validate the SSL certificate, applied only when encrypt is true.

Download Microsoft JDBC Driver for SQL Server

- https://docs.microsoft.com/en-us/sql/connect/jdbc/download-microsoft-jdbc-driver-for-sql-server?view=sql-server-ver15

Securing Microsoft SQL

Custom property :

- trustStore=<trustStore path>
- trustStorePassword=<myPassword>
- hostNameInCertificate=<hostname>

- Host name is used to validate the SSL certificate of the database, this also applied only when encrypt is set to true. And trustServerCertificate is false.

- Default used by MS SQL driver as java layer CACERTS or you can define explicitly trustStorefile and password using driver custom properties.

- Microsoft JDBC Driver and TLSv12
  – At the minimum JDBC version 4.1 is needed (JDBC driver version 4.0 is already out of support)

Securing Oracle

Securing Oracle

- SSL connection using Oracle Thin Driver and Oracle Wallets The Following Oracle blog provides clear steps to establish an SSL connection over TLSv1.2 using the JDBC thin driver with either JKS files or a wallet.
  - https://blogs.oracle.com/dev2dev/ssl-connection-to-oracle-db-using-jdbc,-tlsv12,-jks-or-oracle-wallets
- Oracle Driver:
  - https://www.oracle.com/database/technologies/appdev/jdbc-downloads.html

Securing Oracle

Minimum requirement on WebSphere Application Server side.

1. Ensure that Java is current or as latest build as possible
2. You should have following jars in classpath for Oracle Wallet to work.
    - ojdbcdriver, oraclepki, osdt_core, and osdt_certin

Oracle JDBC driver specific properties

•The Oracle JDBC driver has added support for a new Custom Properties under connectionProperties.

•The method used with datasources is to set a Custom Property in the datasource as follows:
- Name: connectionProperties
- Value: propertyA=valueA;propertyB=valueB

Using Oracle JDBC driver specific properties through a datasource

Securing Oracle

Required Custom Property :

- oracle.net.ssl_version=1.2
- oracle.net.ssl_server_dn_match=false
- oracle.net.authentication_services=TCPS
- oracle.net.wallet_location={location};

Name: **connectionProperties**
Value:oracle.net.ssl_version=1.2;oracle.net.ssl_server_dn_match=false;oracle.net.authentication_services=TCPS;oracle.net.wallet_location=/work/security/oracle/;

Description: Set of properties that will be passed to the Oracle JDBC driver to be used when creating new connections. Type: java.lang.String
Example:
URL connection property
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=oracle)(PORT=1522))(CONNECT_DATA=(SERVICE_NAME=xe)))
Note: -This URL should match the corresponding entry in tnsnames.ora

Driver under FIPS enabled

What is FIPS?

- The **Federal Information Processing Standard Publication 140-2**, (**FIPS PUB 140-2**), is a U.S. government computer security standard used to approve cryptographic modules.
- **Microsoft SQL driver:**
- https://docs.microsoft.com/en-us/sql/connect/jdbc/fips-mode?view=sql-server-ver15

  - **fips** boolean ["true / false"] "false" For FIPS enabled JVM this property should be true Added in 6.1.4 (Stable release 6.2.2)
  - **fipsProvider** String null FIPS provider configured in JVM. For example, BCFIPS or SunPKCS11-NSS Added in 6.1.2 (Stable release 6.2.2), deprecated in 6.4.0
  - **trustStoreType** String JKS For FIPS mode set trust store type either PKCS12 or type defined by FIPS provider

Best Practice/Recommendations

Best Practice/Recommendations

Some drivers use SSLContext for the connection, which was hard coded TLS, but IBM JDK provided fix to override, some driver code might still require as workaround by setting these two properties. This workaround would be to use as last resources. **First and recommended best practice to use driver level SSL protocol properties for data source**.

Generic jvmarguments (JVM settings):

- -Dcom.ibm.jsse2.overrideDefaultTLS=true
- -Dcom.ibm.jsse2.overrideDefaultProtocol=TLSv12

Best Practice/Recommendations

IV84450: SSLCONTEXT.GETINSTANCE(TLS) BEHAVE LIKE ORACLE
https://www-01.ibm.com/support/docview.wss?uid=swg1IV84450

IV91348: SSLCONTEXT.GETINSTANCE BEHAVIOR LIKE ORACLE
https://www-01.ibm.com/support/docview.wss?uid=swg1IV91348

IV45696: PROVIDE SYSTEM PROPERTY TO ALLOW SETTING OF ENABLED PROTOCOLS WHEN DEFAULT SSLSERVERSOCKETFACTORY OR SSLSOCKETFACTORY IS USED
https://www-01.ibm.com/support/docview.wss?uid=swg1IV45696

After following this doc does not resolve SSL / TLS configuration issue for your specific driver, then we would recommend deep dive by enabling following trace and/or open a ticket with IBM Support

Best Practice/Recommendations

Deep dive by enabling trace:

- JDBC driver
- Microsoft SQL, DB2, Oracl, JDBC driver trace in WebSphere.
  https://www.ibm.com/docs/en/was/8.5.5?topic=problems-jdbc-trace-configuration

- Mustagher J2C
  - https://www.ibm.com/support/pages/node/89095

- Mustgather SSL/JSSE
  - https://www.ibm.com/support/pages/node/707663

Wrap up

Open Liberty

Useful Links

Why choose Liberty for Microservices
https://ibm.biz/6ReasonsWhyLiberty

Choosing the right Java runtime
https://ibm.biz/ChooseJavaRuntime

How to approach application modernization
https://ibm.biz/ModernizeJavaApps

Open Liberty Site
https://www.openliberty.io

Open Liberty Guides
https://www.openliberty.io/guides

© 2021 IBM Corporation

Liberty References

Read

Why choose Liberty for Microservices
ibm.biz/6ReasonsWhyLiberty

Choosing the right Java runtime
ibm.biz/ChooseJavaRuntime

How to approach application modernization
ibm.biz/ModernizeJavaApps

Watch

Explore the latest on WebSphere and Liberty
ibm.biz/LibertyTV

View our recent Expert TV episode all about Liberty ibm.biz/Liberty101

Learn more about Liberty in containers and Operator-based deployment
ibm.biz/LibertyContainerOperator

Experience

Try Liberty as a beginner
openliberty.io/guides/getting-started.html

Learn Liberty, MicroProfile, Containers, Kubernetes, Hands-on
openliberty.io/guides

Try dev mode in Containers
https://openliberty.io/guides/docker.html

Questions and Answers