**Secure Sockets Layer (SSL) support in DB2 for Linux, UNIX, and Windows**

**Document Owner:** Luiz Andrade

**Role:** Senior Db2 Database Administrator

**Created at:** 18.01.2018

**Last changed at:** 09.02.2018

**Number of Pages:** 14

History of revision

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Authors** |
| 18/01/2018 | 0.1 | Draft | Luiz Andrade |
| 09/02/2018 | 0.2 | Conclusion | Luiz Andrade |

Contents

[1. Overview 5](#_Toc32328099)

[1.1 Objectives 5](#_Toc32328100)

[2. Server side SSL parameters 5](#_Toc32328101)

[2.1 Shows the server side SSL parameters you can set prior to DB2 V9.7 5](#_Toc32328102)

[2.2 Shows the server side SSL parameters you can set from DB2 V9.7 and above 6](#_Toc32328103)

[3. Client side SSL parameters 6](#_Toc32328104)

[3.1 Shows the client side SSL parameters you can set from DB2 V9.7 and newer releases 6](#_Toc32328105)

[4. SSL support for High Availability Disaster Recovery (HADR) systems 6](#_Toc32328106)

[5. Pre-configuration tasks on server 7](#_Toc32328107)

[6. Server setup 8](#_Toc32328108)

[6.1 Configure your system environment variable 8](#_Toc32328109)

[6.2 Make separate directory SSL 8](#_Toc32328110)

[6.3 Create Server key database 8](#_Toc32328111)

[6.4 Add certificate 8](#_Toc32328112)

[6.5 Extract certificate 8](#_Toc32328113)

[6.6 Verify files 8](#_Toc32328114)

[6.7 Set database manager configuration parameters 9](#_Toc32328115)

[6.8 Set DB2COMM 9](#_Toc32328116)

[6.9 Update DIAGLEVEL 9](#_Toc32328117)

[6.10 Stop and start DB2 9](#_Toc32328118)

[6.11 Validation in db2diag.log file 10](#_Toc32328119)

[6.12 Update DIAGLEVEL 10](#_Toc32328120)

[6.13 Alternative messages after db2start 10](#_Toc32328121)

[7. Client setup 10](#_Toc32328122)

[7.1 Make separate directory SSL 10](#_Toc32328123)

[7.2 Create the client key database 11](#_Toc32328124)

[7.3 Add the signer certificate sent from the server to the client key database. 11](#_Toc32328125)

[7.4 Set database manager configuration parameters 11](#_Toc32328126)

[7.5 Catalog the server 11](#_Toc32328127)

[7.6 Connect to server database 12](#_Toc32328128)

[8. SSL configuration is not enabled if the following is true 13](#_Toc32328129)

[8.1 SQL5043N error when configuration parameter set to null 13](#_Toc32328130)

[8.2 SQL5043N error for instance during db2start 13](#_Toc32328131)

[8.3 MAX\_CONNECTIONS greater than MAX\_COORDAGENTS 14](#_Toc32328132)

[8.4 db2diag.log file messages 14](#_Toc32328133)

[9. Conclusion 14](#_Toc32328134)

[10. Related topics 14](#_Toc32328135)

# Overview

Secure Sockets Layer (SSL) is a protocol that lets services communicate over a network without compromising security. It creates a secure connection between a client and a server. Any amount of data can then be sent securely over that connection. You should consider using SSL if, for example, you process credit cards through an online application, process sensitive data such as personal identification information, or need to comply with privacy standards.

You can use SSL to protect data in transit on all networks that use TCP/IP. Alternatively, you can think of an SSL connection as a secured TCP/IP connection.

The DB2 database system supports the use of Secure Sockets Layer (SSL). The IBM Data Server Driver for JDBC and SQLJ provides support for the SSL through the Java Secure Socket Extension (JSSE).

CLI, CLP, and .Net Data Provider client applications and applications that use the IBM Data Server Driver for JDBC and SQLJ (type 4 connections) support SSL.

The SSL communication will always be in Federal Information Process Standards(FIPS) mode.

Note: If you are configuring SSL on DB2 Versions V9.5 and earlier, then see the [Related topics](#_Related_topics) section for an article that describes a step-by-step procedure to setup SSL on Windows platform.

## Objectives

Give an overview and direction on how to proceed to implement a SSL support in Db2.

# Server side SSL parameters

Prior to DB2 V9.7, for DB2 data servers to recognize SSL support, the DB2COMM registry variable has to be set to include SSL, and the SSL configuration file SSLconfig.ini must be created in the instance directory under cfg (UNIX and Linux operating systems) or instance directory (Windows operating systems). The file shown in 2.1 stores the SSL parameters that are used to start SSL at the server.

## Shows the server side SSL parameters you can set prior to DB2 V9.7

| Name of SSL parameters | Nullable? | Description |
| --- | --- | --- |
| DB2\_SSL\_KEYSTORE\_FILE | NO | Fully Qualified file name of KeyStore that stores the Server Certificate |
| DB2\_SSL\_KEYSTORE\_PW | YES | Password of KeyStore that stores the Server Certificate |
| DB2\_SSL\_KEYSTORE\_LABEL | YES | Label of Server Certificate |
| DB2\_SSL\_LISTENER | NO | Service name/Port number for SSL Listener |

Starting from DB2 V9.7 and new versions, you don't need to create the SSL configuration file SSLconfig.ini. The SSL parameters mentioned previously in Table 1 are moved into the database manager configuration file, as shown in 2.2.

## Shows the server side SSL parameters you can set from DB2 V9.7 and above

| Name of SSL DBM configuration parameters | Nullable? | Description |
| --- | --- | --- |
| SSL\_SVR\_KEYDB | NO | Fully qualified path of the key file |
| SSL\_SVR\_STASH | NO | Fully qualified path of the stash file |
| SSL\_SVR\_LABEL | NO | Label of Server Certificate |
| SSL\_SVCENAME | NO | Service name/Port number for SSL Listener |

Note 1: DB2\_SSL\_KEYSTORE\_PW specifies the password to access the key database at the server side. But this has been replaced with SSL\_SVR\_STASH file. You will not add a DBM cfg parameter for the password. Instead, you will let GSKit encrypt the password and save it in a stash file and add a DBM cfg parameter SSL\_SVR\_STASH for the stash file. On the one hand, it avoids exposing the password in clear text. It also enables db2start to go without users’ intervention to supply the password. The stash file should be strongly protected by the file system.

Note 2: During instance startup, if DB2COMM is set to SSL, GSKit will use the stash file defined in the SSL\_SVR\_STASH DBM configuration file to access the key file. So SSL\_SVR\_KEYDB and SSL\_SVR\_STASH must be defined. If they are NULL (not specified), the instance will be started up without SSL protocol support.

# Client side SSL parameters

Starting from DB2 V9.7, you don't need to create a separate SSLClientconfig.ini file to define client-side settings for SSL. The SSL parameters are moved into the database manager configuration file, as shown in 3.1.

## Shows the client side SSL parameters you can set from DB2 V9.7 and newer releases

| Name of SSL DBM configuration parameters | Nullable? | Description |
| --- | --- | --- |
| ssl\_clnt\_keydb | NO | The fully qualified file path of the key file to be used for SSL connection at the client-side. |
| ssl\_clnt\_stash | NO | The fully qualified file path of the stash file to be used for SSL connections at the client-side |

# SSL support for High Availability Disaster Recovery (HADR) systems

SSL is supported between clients and the HADR primary server. Clients connecting to the HADR primary server using SSL are able to reroute to the HADR standby database using SSL. However, SSL is not supported between the HADR primary and standby servers.

Clients connecting to the HADR primary database server is the same as clients connecting to a standard database server. Therefore SSL can be used between clients and the HADR primary server. However, between the HADR primary server and standby server, only TCPIP (either TCPIP4 or TCPIP6) can currently be used. They use the hostnames/ports defined in the DB CFG to communicate with each other. They listen on their own listener ports, which is different from the one in SVCENAME. Protocols set in DB2COMM are irrelevant.

# Pre-configuration tasks on server

The IBM Global Security Kit (GSKit) supports the use of the SSL protocol to protect DB2 client server communications over the network. GSKit is automatically included when you install the DB2 database system. In some situations, if you want to use SSL, you might need to install GSKit by yourself.

For information about the GSKit tool GSKCapiCmd, see the GSKCapiCmd User's Guide, available from the [Related topics](#_toc796) section.

For more information on IBM Global Security Kit (GSKit), refer to the [Related topics](#_toc796) section.

Before configuring SSL, ensure that the path to the IBM Global Security Kit (GSKit) libraries appears in the PATH environment variable on Windows platforms, and the LIBPATH, SHLIB\_PATH or LD\_LIBRARY\_PATH environment variables on Linux and UNIX platforms.

* On Windows 32-bit platforms, the GSKit libraries are located in C:\Program Files\IBM\GSK8\lib. In this case, the system PATH must include C:\Program Files\IBM\GSK8\lib.
* On Windows 64-bit platforms, the 64-bit GSKit libraries are located in C:\Program Files\IBM\GSK8\lib64, and the 32-bit GSKit libraries are located in C:\Program Files (x86)\IBM\GSK8\lib.
* On UNIX and Linux platforms, the GSKit libraries are located in sqllib/lib/gskit.

On non-Windows platforms, the DB2 database manager installs GSKit locally, and for a given instance, the GSKit libraries would be located in sqllib/lib/gskit or sqllib/lib64/gskit. It is unnecessary to have another copy of GSKit installed in a global location to bring up the instance. If a global copy of GSKit does exist, keep the version of the global GSKit at the same version of the local GSKit.

**Steps to configure SSL support on Linux/Unix**

# Server setup

Perform the following steps to configure the SSL on server side:

## Configure your system environment variable

|  |
| --- |
| export LD\_LIBRARY\_PATH=$LD\_LIBRARY\_PATH:/home/db2inst1/sqllib/gskit/bin  export PATH=$PATH:/home/db2inst1/sqllib/gskit/bin |

## Make separate directory SSL

Make a separate directory SSL under instance home directory to keep all SSL files separately

|  |
| --- |
| /home/db2inst1> mkdir SSL  /home/db2inst1> cd SSL  /home/db2inst1/SSL> pwd  /home/db2inst1/SSL |

## Create Server key database

Create a server key database and set up your digital certificates.

|  |
| --- |
| /home/db2inst1/SSL> gsk8capicmd\_64 -keydb -create -db "key.kdb" -pw "ssltest123456" -stash |

## Add certificate

Add a certificate for your server to your key database.

|  |
| --- |
| /home/db2inst1/SSL> gsk8capicmd\_64 -cert -create -db "key.kdb" -pw "ssltest123456" -label "SSLLabel" -dn "CN=oc6344180105.ibm.com,O=IBM,OU=GTS,L=Katowice,ST=SL,C=POLAND" |

## Extract certificate

Extract the certificate you just created to a file.

|  |
| --- |
| /home/db2inst1/SSL> gsk8capicmd\_64 -cert -extract -db "key.kdb" -pw  "ssltest123456" -label "SSLLabel" -target "key.arm" -format ascii -fips |

## Verify files

Verify the following files are created inside SSL directory.

|  |
| --- |
| /home/db2inst1/SSL> ls  key.arm, key.crl, key.kdb, key.rdb, key.sth |

## Set database manager configuration parameters

Log in to DB2 server as instance owner to set database manager configuration parameters on the server for SSL, as mentioned previously in 2.2.

|  |
| --- |
| /home/db2inst1> db2 update dbm cfg using SSL\_SVR\_KEYDB /home/db2inst1/SSL/key.kdb  DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.  /home/db2inst1> db2 update dbm cfg using SSL\_SVR\_STASH /home/db2inst1/SSL/key.sth  DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.  /home/db2inst1> db2 update dbm cfg using SSL\_SVR\_LABEL SSLLabel  DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.  /home/db2inst1> db2 update dbm cfg using SSL\_SVCENAME 50050  DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully. |

Note: The value set to SSL\_SVCENAME should be the one which does not exist in your /etc/services file.

## Set DB2COMM

Set the DB2COMM registry variable.

|  |
| --- |
| /home/db2inst1> db2set DB2COMM=SSL,TCPIP  or  /home/db2inst1> db2set DB2COMM=SSL |

## Update DIAGLEVEL

Update DIAGLEVEL database manager configuration parameter to 4, this will be done just to monitor and check the procedure was successfully implemented.

|  |
| --- |
| /home/db2inst1> db2 update dbm cfg using DIAGLEVEL 4 |

## Stop and start DB2

Refresh your instance by running db2stop / db2start for above setting become effective.

|  |
| --- |
| /home/db2inst1> db2stop force  SQL1064N DB2STOP processing was successful.  /home/db2inst1> db2start  SQL1063N DB2START processing was successful. |

## Validation in db2diag.log file

The process was successfully done, if the messages are presented in db2diag.log file.

|  |
| --- |
| 2017-12-18-15.12.41.215231+060 I47526E399 LEVEL: Info  PID : 24977 TID : 140178609923840 PROC : db2sysc 0  INSTANCE: db2inst1 NODE : 000  HOSTNAME: oc6344180105.ibm.com  EDUID : 1 EDUNAME: db2sysc 0  FUNCTION: DB2 UDB, common communication, sqlcctcp\_start\_listen, probe:81  MESSAGE : DIA3000I "SSL" protocol support was successfully started.  2017-12-18-15.12.42.216077+060 I47926E353 LEVEL: Info  PID : 24977 TID : 140178609923840 PROC : db2sysc 0  INSTANCE: db2inst1 NODE : 000  HOSTNAME: oc6344180105.ibm.com  EDUID : 1 EDUNAME: db2sysc 0  FUNCTION: DB2 UDB, common communication, sqlccstrts, probe:984  MESSAGE : SSL is setup properly |

## Update DIAGLEVEL

Update DIAGLEVEL database manager configuration parameter to 3 again.

|  |
| --- |
| /home/db2inst1> db2 update dbm cfg using DIAGLEVEL 3 |

## Alternative messages after db2start

If this message appears after db2start, then there may be some problem with either, the system environment variables setting or the instance SSL server parameters settings.

|  |
| --- |
| /home/db2inst1> db2start  SQL5043N Support for one or more communications protocols failed to start successfully.  However, core database manager functionality started successfully.  SQL1063N DB2START processing was successful. |

# Client setup

Perform the following steps to configure the SSL on the client side.

## Make separate directory SSL

Make a separate directory SSL under instance home directory to keep all SSL files separately.

|  |
| --- |
| /home/db2inst2> mkdir SSL  /home/db2inst2> cd SSL  /home/db2inst2/SSL> pwd  /home/db2inst2/SSL |

Transfer the key.arm from the server and place it in the client /home/db2inst2/SSL.

## Create the client key database

Create a client key database and set up a digital certificate.

|  |
| --- |
| /home/db2inst2/SSL> gsk8capicmd\_64 -keydb -create -db "keyclient.kdb" -pw "ssltest123456" -stash |

## Add the signer certificate sent from the server to the client key database.

|  |
| --- |
| /home/db2inst2/SSL> gsk8capicmd\_64 -cert -add -db "keyclient.kdb"  -pw "ssltest123456" -label "SSLLable" -file key.arm -format ascii -fips |

***Ps.: The “-label” must be the same as the certificate built in the server.***

## Set database manager configuration parameters

log in to DB2 client as the instance owner to set database manager configuration parameters for SSL as mentioned previously in 3.1.

|  |
| --- |
| /home/db2inst2> db2 update dbm cfg using SSL\_CLNT\_KEYDB /home/svtdbm12/SSL/keyclient.kdb  DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.  /home/db2inst2> db2 update dbm cfg using SSL\_CLNT\_STASH  /home/svtdbm12/SSL/keyclient.sth  DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully. |

## Catalog the server

Catalog the server with SSL port and SECURITY SSL option.

|  |  |
| --- | --- |
| /home/db2inst2> db2 catalog tcpip node SSLTEST remote oc6344180105.ibm.com server 50050 security ssl  DB20000I  The CATALOG TCPIP NODE command completed successfully.  DB21056W  Directory changes may not be effective until the directory cache is refreshed  [db2inst1@oc2468186123 SSL]$ db2 list node directory  Node Directory  Number of entries in the directory = 1  Node 1 entry:  Node name = SSLTEST  Comment =  Directory entry type = LOCAL  Protocol = TCPIP  Hostname = oc6344180105.ibm.com  Service name = 50050  Security type = SSL    /home/db2inst2> db2 catalog db SSLDB as SSLDBCLI at node SSLTEST  DB20000I  The CATALOG DATABASE command completed successfully.  DB21056W  Directory changes may not be effective until the directory cache is refreshed  [db2inst1@oc2468186123 SSL]$ db2 list db directory  System Database Directory  Number of entries in the directory = 1  Database 1 entry:  Database alias = SSLDBCLI  Database name = SSLDB  Node name = SSLTEST  Database release level = 10.00  Comment =  Directory entry type = Remote  Catalog database partition number = -1  Alternate server hostname =  Alternate server port number =    /home/db2inst2> db2 terminate  DB20000I  The TERMINATE command completed successfully. |  |

## Connect to server database

|  |
| --- |
| /home/db2inst2> db2 connect to SSLDBCLI user db2inst1  Enter current password for db2inst1:  Database Connection Information  Database server = DB2/LINUXX8664 10.5.8  SQL authorization ID = DB2INST1  Local database alias = SSLDBCLI |

# SSL configuration is not enabled if the following is true

* The ssl\_svr\_keydb configuration parameter is null (unset) instead of the fully qualified path of the key database file.
* The ssl\_svr\_stash configuration parameter is null (unset) instead of fully qualified path of the stash file.
* The ssl\_svcename is null (unset).

If TCP/IP and SSL are both enabled (the DB2COMM registry variable is set to 'TCPIP, SSL'), you must set ssl\_svcename to a different port than the port to which svcename is set. The svcename configuration parameter sets the port that the DB2 database system listens on for TCP/IP connections. If you set ssl\_svcename to the same port as svcename, neither TCP/IP or SSL will be enabled.

In HADR environments, do not set hadr\_local\_svc on the primary or standby database system to the same value as you set for ssl\_svcename. Also, do not set hadr\_local\_svc to the same value as svcename, or svcename plus one.

* When the DB2COMM registry variable is set to 'TCPIP, SSL', and if TCPIP support is not properly enabled, for example due to the svcename configuration parameter being set to null, the error SQL5043N is returned and SSL support is not enabled.

## SQL5043N error when configuration parameter set to null

|  |  |
| --- | --- |
| /home/db2inst1> db2set -all  [i] DB2COMM=SSL,TCPIP  /home/db2inst1> db2 get dbm cfg | grep -i svcename  TCP/IP Service name       (SVCENAME) = |  |

## SQL5043N error for instance during db2start

Trying to start your instance will receive error SQL5043N.

|  |  |
| --- | --- |
| /home/db2inst1> db2start  SQL5043N  Support for one or more communications protocols failed to start successfully.  However, core database manager functionality started successfully. |  |

## MAX\_CONNECTIONS greater than MAX\_COORDAGENTS

DB2 connection concentrator is ON. To determine whether connection concentrator is ON, issue the GET DATABASE MANAGER CONFIGURATION command. If the configuration parameter MAX\_CONNECTIONS is set to a value greater than the value of MAX\_COORDAGENTS, connection concentrator is ON.

|  |
| --- |
| /home/db2inst1> db2 get dbm cfg | grep -i max  Max number of coordinating agents (MAX\_COORDAGENTS) = AUTOMATIC(100)  Max number of client connections   (MAX\_CONNECTIONS) = AUTOMATIC(1000) |

## db2diag.log file messages

If SSL\_CLNT\_KEYDB and SSL\_CLNT\_STASH NULL are not specified, the connection will fail with SQL30081N.

Messages in db2diag.log file

|  |
| --- |
| 2017-12-19-11.07.48.215335+060 I47526E399       LEVEL: Error  PID     : 1126574              TID  : 258         PROC : db2sysc  INSTANCE: db2inst1             NODE : 000  EDUID   : 258                  EDUNAME: db2sysc  FUNCTION: DB2 UDB, common communication, sqlcctcpconnmgr,  probe:110  MESSAGE : Disable SSL as Concentrator is ON |

Note: If DB2 Connect Concentrator is ON, the inbound request to the DB2 Connect server can not be SSL. However, the outbound request to the target database server can still be SSL. If DB2 Connect Concentrator is OFF, both the inbound and the outbound requests can be SSL.

# Conclusion

SSL is a valuable protocol for protecting your data as it moves through a network. Almost any Internet service can be protected with SSL. Using the configuration instructions and test case verification program described in this article, you can get started with securing your own DB2 data.

# Related topics

• [*"DB2 technical tip: Set up Secure Sockets Layer (SSL) for DB2 on Windows"*](https://www.ibm.com/developerworks/data/library/techarticle/dm-0806sogalad/index.html)

(developerWorks, Jun 2008) is a step-by-step guide to set up SSL on Windows.

• Read the GSKCapiCmd User's Guide *"*[*GSKCapiCmd User's Guide*](https://www.ibm.com/support/knowledgecenter/SSAL2T_8.2.0/com.ibm.cics.tx.doc/pdf/GSK_CapiCmd_UserGuide.pdf)*"* for more information about the GSKit tool.

• Refer to the *"*[*GSKit Installation*](https://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.swg.tivoli.gskit.install.doc/doc/c0055353.html)*"* for more information on IBM Global Security Kit (GSKit).

• See the [*IBM Global Security Kit*](https://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.swg.tivoli.gskit.install.doc/doc/c0055353.html) to get the resources you need to know more about IBM Global Security Kit Installation.

• Learn about [*GSKit return codes*](https://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.sec.doc/doc/r0054271.html) from the information center.

• Refer to the [*DB2 SSL - part numbers for the GSKit in Passport Advantage*](http://www-01.ibm.com/support/docview.wss?uid=swg21432998) for the appropriate GSKit version.

• [*DB2 SSL - How to download the "IBM DB2 Support Files for SSL Functionality" from Passport Advantage*](http://www-01.ibm.com/support/docview.wss?uid=swg21433407)

• Learn more about [*IBM Data Server Driver for JDBC and SQLJ support for SSL*](https://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_c0024688.html) and how the IBM Data Server Driver for JDBC and SQLJ provides support for the Secure Sockets Layer (SSL) through the Java Secure Socket Extension (JSSE).

• Refer to the [*DB2 JDBC Driver Versions and Downloads*](http://www-01.ibm.com/support/docview.wss?uid=swg21363866) to get the right driver for your environment.