Db2 Connect – What's New and Best Practices

Christoph Theisen (ctheisen@rocketsoftware.com)

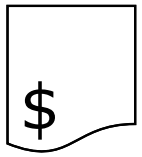
June 2024

Agenda

1. Quick overview
2. Db2 Connect license management
3. Db2 Connect Server (“Gateway”)
4. Db2 Clients and Data Server Drivers
5. TLS setup
6. Monitoring considerations
7. Important new features and changes
8. Summary

Db2 Connect – Did you know…

- Db2 Connect has three components:



Db2 Connect license (required)

IBM Db2 Client or Data Server Driver (required)

Db2 Connect Server ("Gateway" - optional)

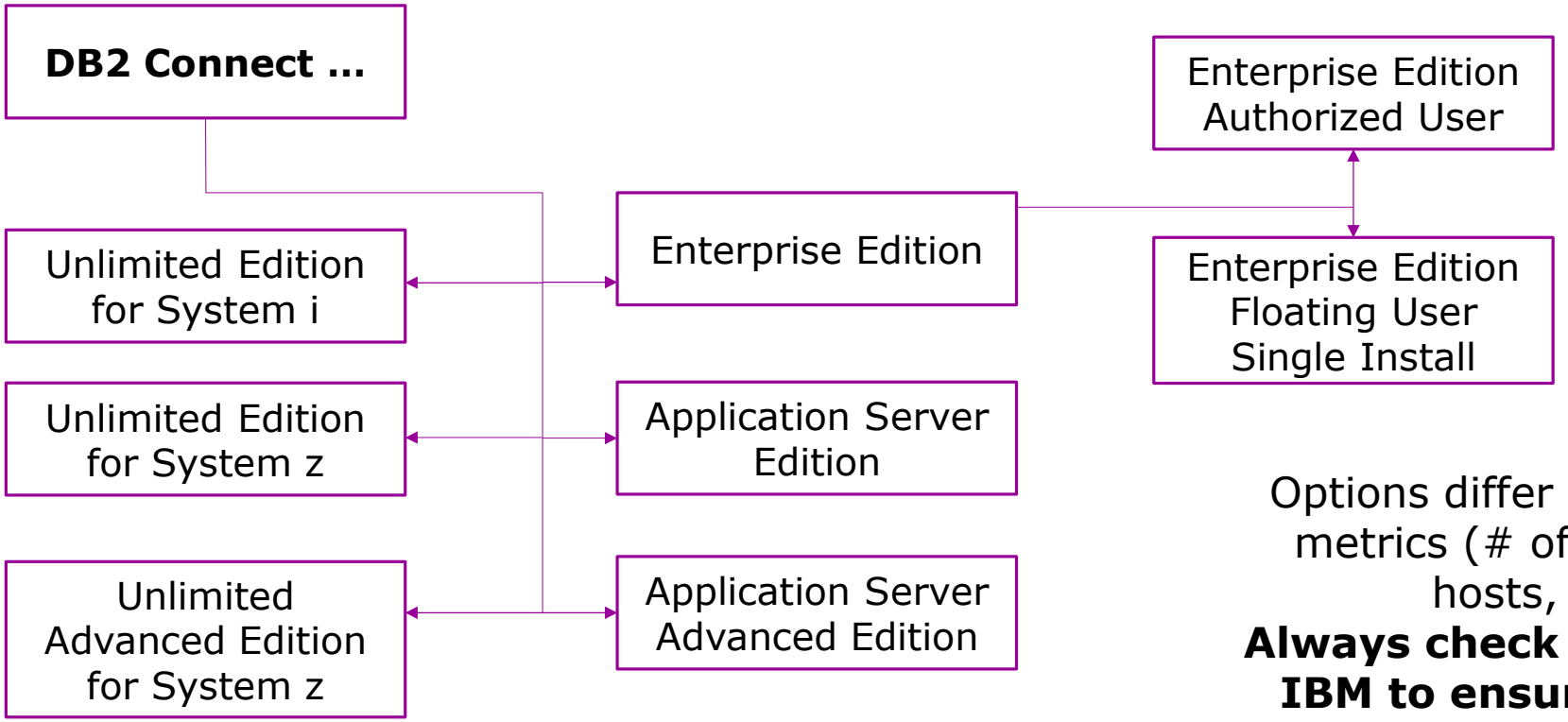
- Is relevant for IBM Mainframe users (IBM Z, IBM i)
- Often used as synonym for Db2 Clients or Db2 Data Server Drivers
- Is relevant when you use IBM Db2 Clients or Data Server Drivers for connectivity to Db2 on IBM Z or IBM i

IBM | Rocket software

Db2 Connect Licensing

- Several options from IBM exist
- **Almost no difference from technical perspective**
  - When license check is successful, connection is established
  - Features such as TLS/SSL encryption, MFA, etc. possible with any type of license
- License required when connecting from IBM Db2 Client, Db2 Data Server Driver, Db2 Connect Server (Gateway)
- No need for license
  - When calling Db2 for z/OS native REST services
  - For Db2 z/OS to Db2 z/OS connections
  - For connections to Db2 LUW server

Db2 Connect Licensing Options (as of 1H 2024)



Options differ in licensing metrics (# of users, #of hosts, # of PVUs)
Always check back with IBM to ensure you are correctly licensed

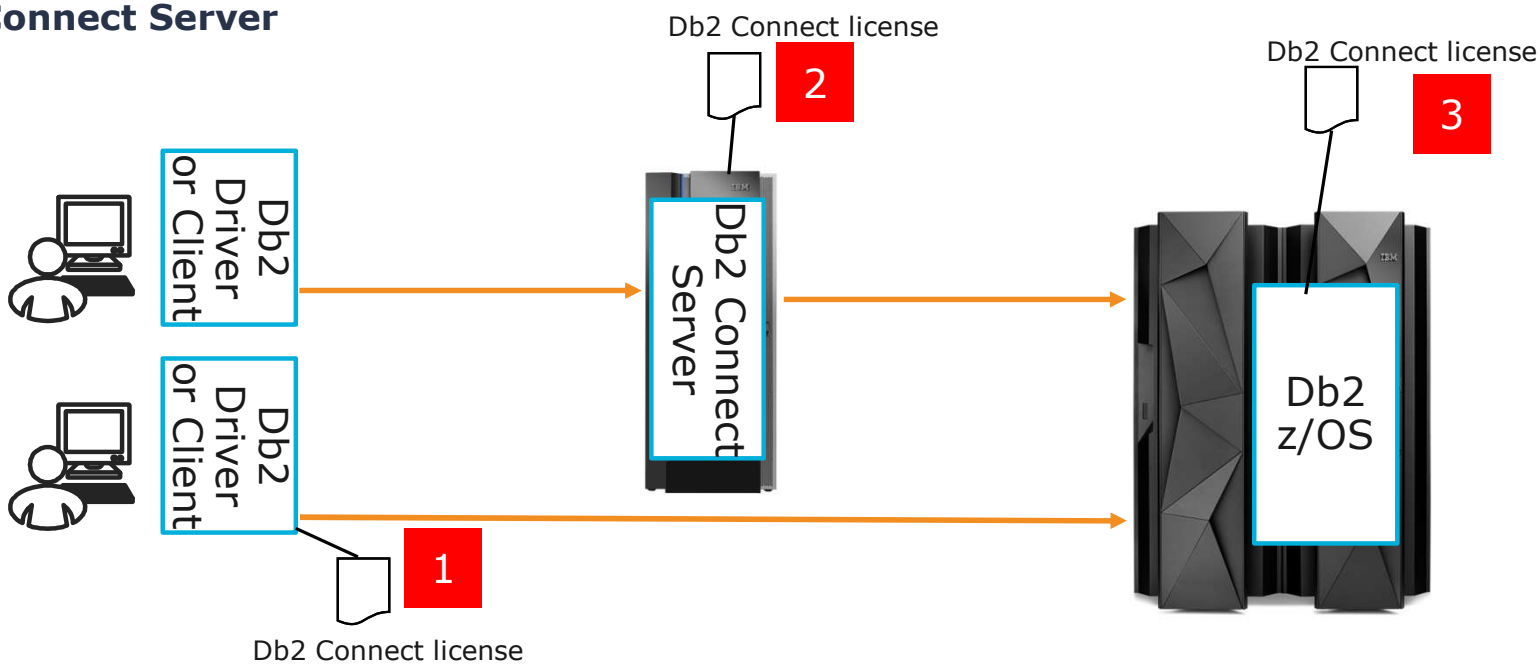
Db2 Connect License Management

Db2 Connect License Installation Options

1 **Distributed installation**

2 **Db2 Connect Server**

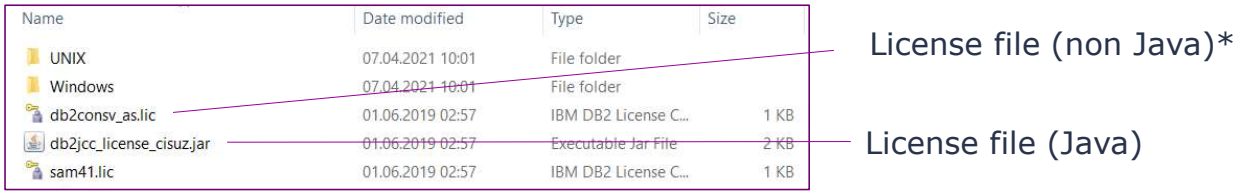
3 **Db2 z/OS Server**



Db2 Connect License – Distributed Installation

- **Applicable to all license types**

Db2 Connect License Activation Kit



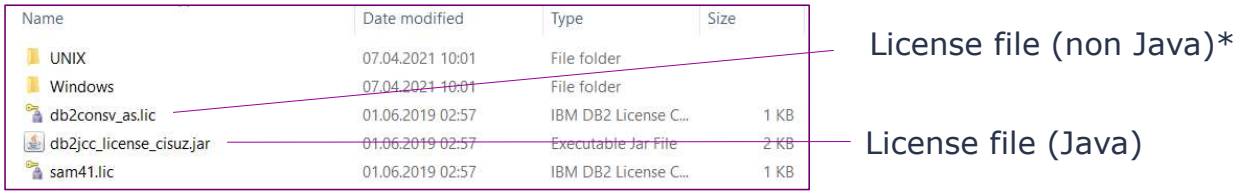
- Java clients: add db2jcc_license_cisuz.jar to classpath
- Non-Java clients: Copy license file to „license“ directory of Db2 Client or Data Server Driver installation path
- Db2 Client, Db2 Runtime Client: db2licm command

*File name depends on edition – example shows Application Server Edition

Db2 Connect License – Db2 Connect Server Option

- **Applicable to all license types**

Db2 Connect License Activation Kit



- Run db2licm command on Db2 Connect Server – this licenses all clients connecting through this server
- Primarily relevant for ODBC/CLI clients
- Could also be Java clients with Type 2 connectivity against DCS connection in the Db2 Connect Server

*File name depends on edition – example shows Application Server Edition

Db2 Connect License – Db2 z/OS Server Option

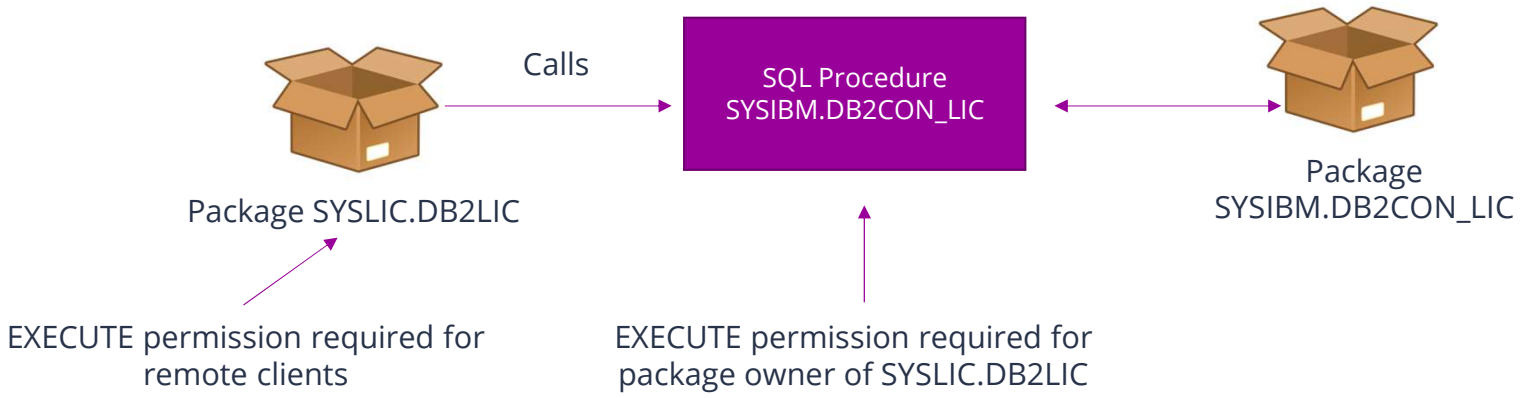
- **Db2 Connect Unlimited Edition only**

Db2 Connect License Unlimited Edition Activation Kit

- Activation kit contains „db2connectactivate" Java program
  - Installs server side license on Db2 for z/OS target system
  - Requires Java Runtime Environment on workstation
  - MFA, TLS, JDBC properties file supported
- Server side license contains version identifier (e.g. V11.5)
- Distributed installation on Clients / Db2 Connect Server still possible

Db2 Connect – More on server side licensing

- db2connectactivate adds objects to Db2 catalog
  - SQL Native stored procedure „SYSIBM.DB2CON_LIC“
  - Corresponding package „DB2CON_LIC“ in collection „SYSIBM“
  - Package „SYSLIC“ in collection „DB2LIC“
- Make sure packages are valid and operative



Db2 Connect – More on server side licensing

- SYSIBM.DB2CON_LIC contains Db2 Connect version of activation package (e.g. 10.5, 11.1, 11.5) in a „cryptic“ string
- Make sure that the highest possible version for your non-Java clients is installed
  - db2connectactivate with „-checkexisting“ tells which version is installed on Db2 for z/OS
  - Run db2connectactivate again when new (higher) version of Db2 Connect is deployed
  - No official alternative for license installation (no traditional batch job), but you can run db2connectactivate from z/OS USS
  - Not needed for fixpack installation
  - No version check for Java clients
  - No version check if client has a locally installed license

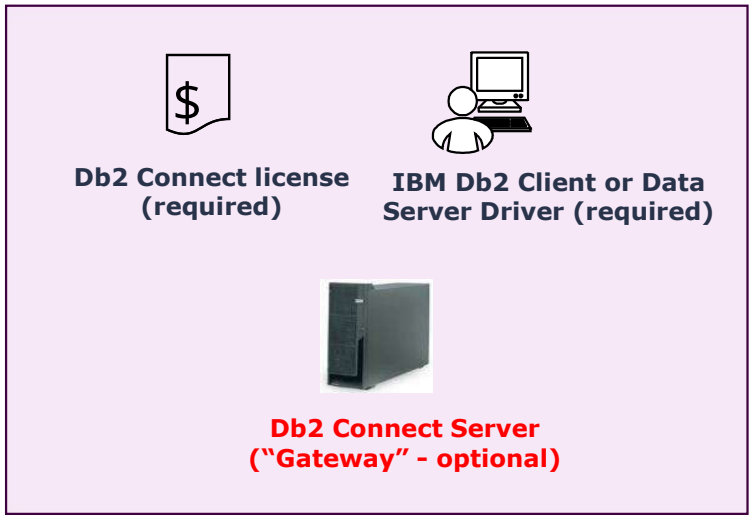
Db2 Connect License - Summary

- **Always check back with IBM for correct licensing**
  - Even „unlimited“ does not mean you are completely free
- **Server-side license is easiest option for „Unlimited“ users**
  - Do not touch catalog objects (stored procedure, packages) for server-side license
- **Tip for JDBC applications: useClientSideLicenseFirst property for Db2 data sources**
  - No license check on server side when license file is present in Java classpath
  - Saves network roundtrips to server and -805 errors on Db2 side if server-side license is not found
  - Requires JCC level 4.29 or higher (Db2 Connect 11.5.6 or higher)

Db2 Connect Server (“Gateway”)

Db2 Connect Server – a.k.a. Gateway

- **Not the same as "Db2 Connect" but optional component**
- Intermediate instance between Db2 Clients and Db2 Servers
- IBM recommends migration from Db2 Connect Servers to direct connections
- Some scenarios still require Db2 Connect Server
  - XA transactions with multi-transport model
  - Federation feature
  - Specific licensing model: Enterprise Edition with floating users



Important: Db2 Connect Server component is still supported, no end of marketing, no end of service announced yet

Db2 Connect Server – Why Migrate?

Performance	➢ Less network hops required
Administration	➢ Less servers to maintain ➢ Less software components to maintain
Availability	➢ Elimination of potential point of failure ➢ Seamless automatic client reroute at transaction boundary in direct connections only
Security	➢ No end-to-end encryption with Db2 Connect Server ➢ Trusted Context: no propagation of client IP address
Future Readyness	➢ Db2 Connect Server is stabilized – do not expect significant new functionality being added

IBM | Rocket software

Db2 Connect Server – Migration Recommendations

Db2 Connect Server typically used for:

For migration to direct connections, consider:

Point of Control

- Use **Db2 profile tables** to control #of clients
- Wildcard support (e.g. for IP addresses)
- Preset of special registers and global variables

Connection Concentration

- #of DBATs is less critical than in the past
- **Connection pooling** in application servers and Db2 for z/OS itself
- Check settings for MAXDBAT, CONDBAT, CTHREAD

Sysplex Workload Balancing

- **Sysplex WLB** in Db2 Drivers and Clients since V9.5
- Seamless automatic client reroute enabled when Sysplex WLB is enabled

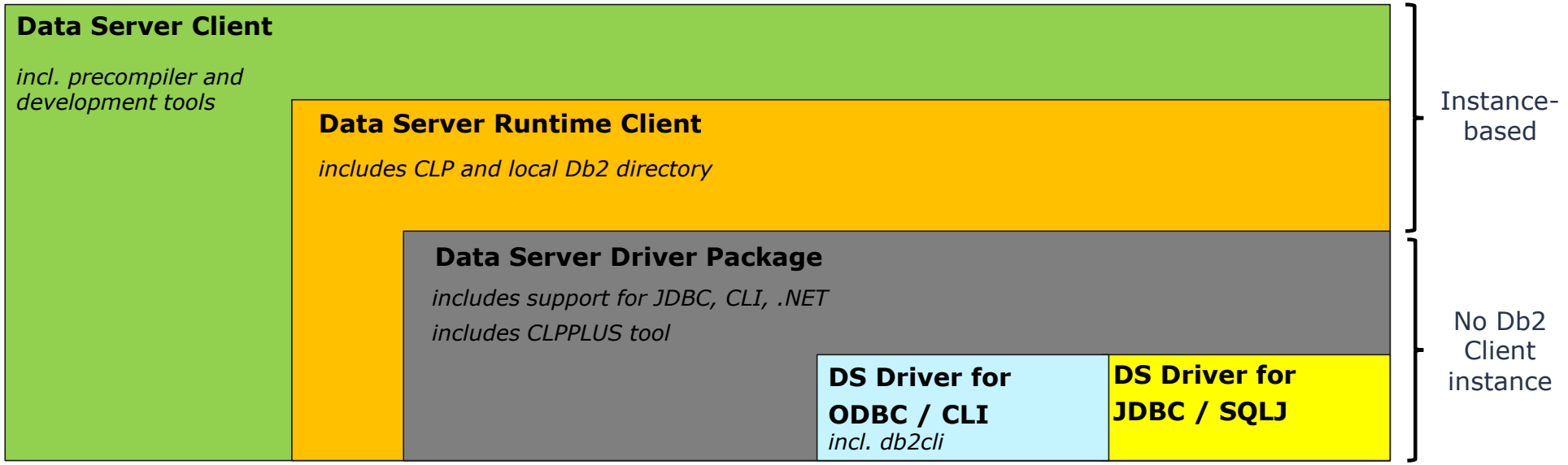
License Management

- Unlimited Edition allows server side license management
- License needs to be distributed to clients for non-Unlimited users

Db2 Clients and Data Server Drivers

Db2 Clients and Data Server Driver Options

- **Data Server Driver Package and Data Server Drivers** (JDBC/SQLJ and ODBC/CLI) have much smaller footprint than instance-based clients
- This should be sufficient for deployment of drivers + connection information to end users and application servers



Db2 Clients and DS Driver – Connection configuration options

	Db2 Client	Db2 Runtime Client	DS Driver Package	DS Driver for ODBC/CLI	DS Driver for JDBC and SQLJ (JDBC T4)
Local DB Directory	✓	✓	–	–	–
db2cli.ini (text file)	✓	✓	✓	✓	–
db2dsdriver.cfg (XML file)	✓	✓	✓	✓	–

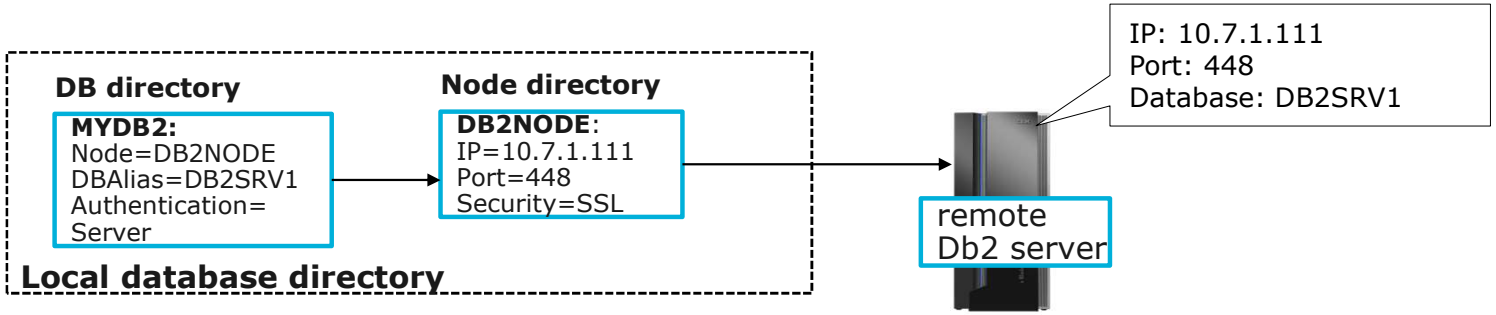
Recommended for client configuration to Db2 servers

Configuration Options for Db2 Clients and Drivers

- **Non-Java:**
  - Up to 3 options (depending on Db2 Client/Driver) + connection string in application
  - Can be used in parallel (but not recommended)
  - Windows ODBC setup is separate step
- **Java:**
  - Java T4 uses connection string, so no configuration option required
  - JDBC Driver (db2jcc4.jar) needed, available in Db2 Clients, Db2 Data Server Driver package and Data Server Driver for JDBC and SQLJ package
  - Hint: db2jcc.jar ("old" JDBC 3 implementation) is deprecated
- **Db2 Connect licensing is a different topic**
  - Every license activation kit contains licenses for Java and Non-Java

Option 1 – Local database directory

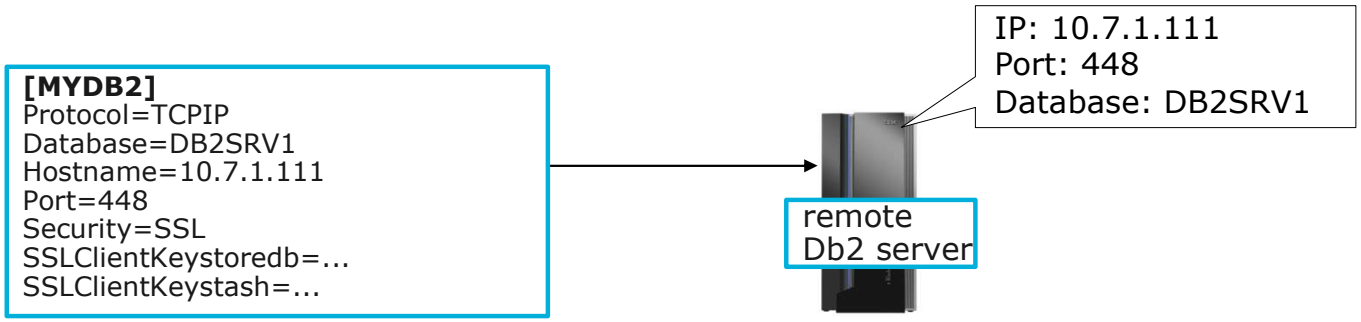
- **Applies to Db2 Clients, Db2 LUW Server and Db2 Connect Server**
- Connection information stored on Db2 instance base
- Managed via Db2 Command Processor (CLP, db2 catalog commands)



- Only limited number of configuration options available
- Consider other options for more sophisticated client configuration

Option 2 – db2cli.ini flat file

- **Applies to Db2 Clients, Db2 LUW Server and Db2 Connect Server, Data Server Driver Package, Data Server Driver for ODBC and CLI**
- Connection information stored in a text file (keyword/value)

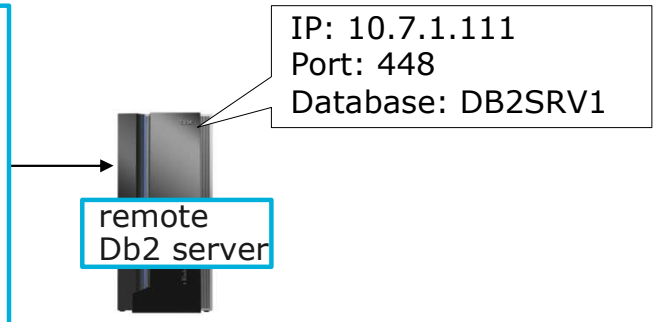


- Organized into sections (“Common” for all connections plus one section per connection)
- Several configuration keywords possible (e.g. “AutoCommit”, “current schema”)
- Manual editing (limited support in Db2 CLP)

Option 3 – db2dsdriver.cfg XML file

- **Applies to Db2 Clients, Db2 LUW Server and Db2 Connect Server, Data Server Driver Package, Data Server Driver for ODBC and CLI**
- Connection information plus additional options in XML file

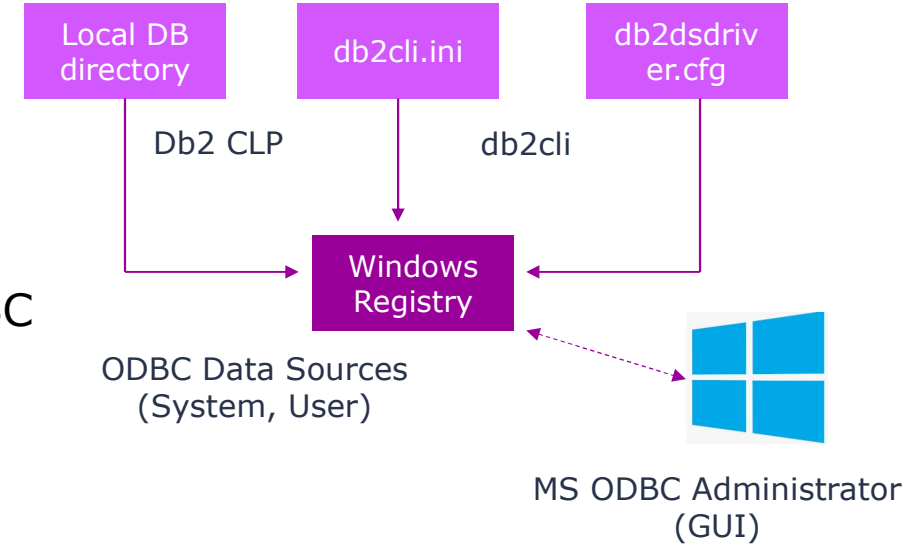
```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<configuration>
  <dsncollection>
    <dsn alias="MYDB2" host="10.7.1.111" name="DB2SRV1"
port="448">
    <parameter name="SecurityTransportMode" value="SSL">
    <parameter name="SSLClientKeystoredb" value="...">
    <parameter name="SSLClientKeystash" value="..."></dsn>
  </dsncollection>
  <databases>
    <database host="10.7.1.111" name="DB2SRV1" port="448"/>
  </databases></configuration
```



- Organized into sections similar to db2cli.ini
- Several configuration keywords + special register settings possible
- Manual editing (almost) not required, use db2cli utility program instea

ODBC Considerations (Windows)

- **For Windows ODBC, connections must be defined to Windows registry (regardless of configuration option)**
- Use Db2 CLP or db2cli program to register existing Db2 connections in Windows registry
- Use MS ODBC Administrator for verification of ODBC DSNs
- In most cases, no need for changes to ODBC connections in MS ODBC Administrator
- All changes in db2dsdriver.cfg / db2cli.ini reflected in ODBC DSN immediately
- ODBC on Linux requires separate ODBC driver manager but no "register" step



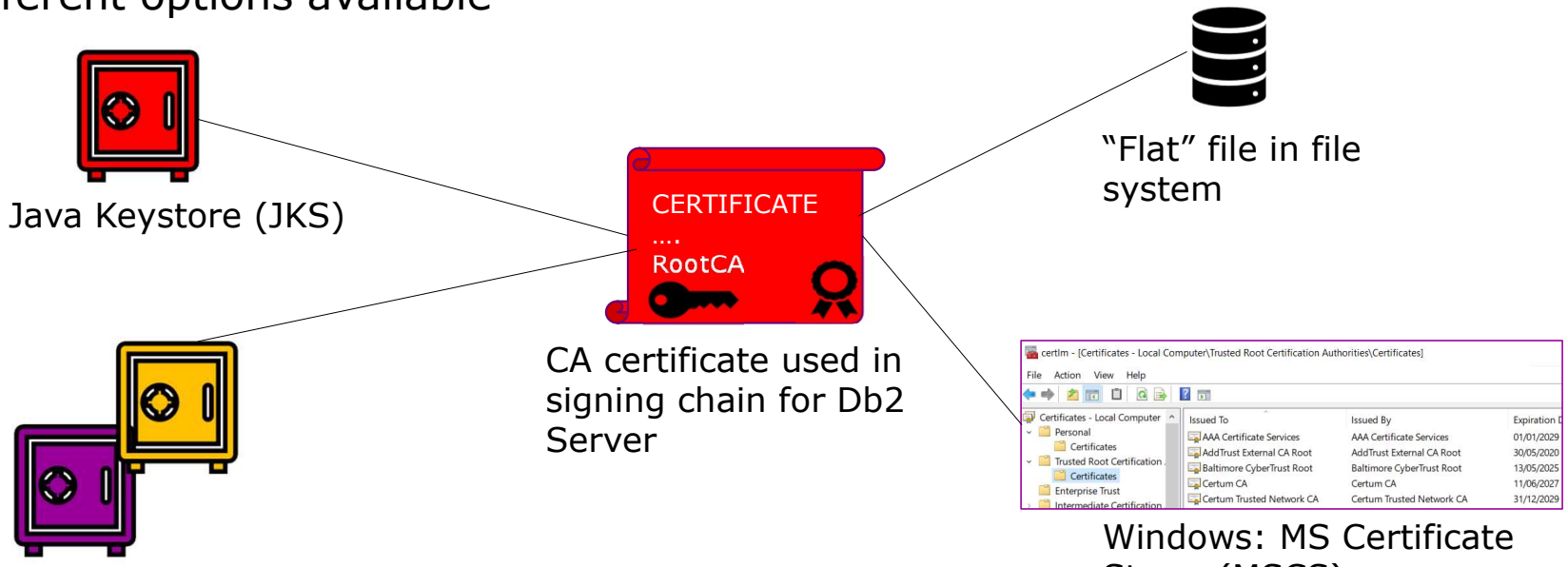
Db2 Client / Data Server Driver Recommendations

- **Data Server Driver Package is deployment option which should fit in most cases**
  - Small installation footprint, no instance needed
  - Contains JDBC, ODBC/CLI and more drivers
- **db2dsdriver.cfg is recommended option for client configuration**
  - Command line utility (db2cli) for maintenance and XML validation
  - Widest support of configuration keywords
  - Easy mass deployment (text file)
  - Supported in all non-Java (T4) deployment options
  - Automatic synchronization with Windows registry for ODBC data sources
- **Do not mix configuration information in local DB directory, db2cli.ini and db2dsdriver.cfg**
  - Technically possible, even for data source with same name
  - Precedence: local DB directory, then db2cli.ini, then db2dsdriver.cfg

Transport Layer Security (TLS) setup

CA Certificate Options on Db2 Client Side

- **Db2 Client applications need access to a CA certificate file for validation of server certificate in TLS handshake (server authentication)**
- Different options available



TLS Setup - Recommendations

- **TLS (at least with Server authentication) is becoming a must-have**
- **CA certificate in flat file or Windows certificate store is preferred over traditional GSKit keydb**
  - No need for GSKit administration tools and "cryptic" keydb setup
- **Can also be leveraged by JDBC applications**
  - No need for Java keytool
  - For Windows certificate store: *com.ibm.security.capi.IBMCAC* security provider must be added to java.security file
- **TLS with Client authentication to Db2 for z/OS server requires password protected keystore for client credentials in addition to CA certificate**
  - Can be PKCS#12 file, GSKit keydb, Java Keystore, Windows certificate store

Monitoring Considerations

Client Information Fields

- **Always recommended that Db2 Client applications use client information fields to facilitate monitoring from the Db2 server side**
- **Most importantly**
  - Client End User
  - Client Workstation
  - Client Application Name (Transaction Name)
  - Client Accounting Information
- Better identification of individual applications
- More granular accounting and charge back
- Allows prioritization of distributed applications with z/OS WLM
- Better control with Db2 profile tables

Managing and Controlling Db2 Clients

Typical scenarios from Db2 for z/OS perspective

- Limit number of remote connections from specific sites (IP addresses, hostnames)
- Enforce certain standards for remote clients, e.g. assign specific NULLID-collection, APPLCOMPAT level, special register settings

Db2 Profile Tables

- Identify clients which are not compliant with company or site standards, e.g.
  - Unsupported data server driver versions (V11.1 and before)
  - Non-TLS connections
  - Cursor not closed
  - DGTT not dropped
  - LOB locator held
  - COMMIT inside stored procedure
  - KEEPDYNAMIC YES packages

Db2 Traces and Monitoring

Db2 Profile Tables - Example

Generate warning messages to z/OS syslog for non-TLS connection requests from JDBC clients:

SYSIBM.DSN_PROFILE_TABLE

All other identi-fication fields	LOCATION	PROF. ID	PROFILE_ ENABLED	REMARKS
NULL	*	61	Y	Non TLS warning

Non TLS request from **any** location triggers profile warning

SYSIBM.DSN_PROFILE_ATTRIBUTES

PROF.ID	KEYWORDS	ATTR.1	ATTR.2	ATTR.3
61	MONITOR JDBC CONNECTIONS FOR SECURITY	WARNING_ DIAGLEVEL3	5	1

enforces TLS

```
DSNT775I  !I9A2 DSNLTSEC SERVER DISTRIBUTED AGENT 724
WITH
        LUWID=GA0F3DFE.C9E8.DE318FA8B53B
        THREAD-INFO=SYSOPR:*:*:*:*:*:*:*
        PRDID=JCC04320
        FOR LOCATION=::10.xx.xx.xxx
        RECEIVED MONITOR JDBC CONNECTIONS FOR SECURITY
        WARNING DUE TO PROFILE ID=61
        OCCURRED 1 TIME(S)
```

Note: “MONITOR …FOR SECURITY” is new with Db2 13, requires APAR PH48764/PH53182

Db2 Traces for Remote Clients

3 relatively new trace records for monitoring of remote clients (Db2 12 and Db2 13):

IFCID 365 Remote Location Stats

IFCID 411 Remote Application Stats

IFCID 412 Remote User Stats

- Trace collection starts with activation of specific statistics trace classes
- Collects information such as
  - Product-Id
  - Profile activity
  - DBAT Connection pooling blockers
  - #active connections, queued connections, …
  - Authentication mechanism used
  - #commits, #rollbacks, #aborts, …
- in aggregated form per remote IP address, client transaction, client userid

Important new features and changes

TLS Hostname Validation

- **Db2 Clients can enforce that Db2 Server's IP address or DNS name matches IP address or DNS name on server certificate**
- Default is "Off" (no validation)
- Requires at least V11.5.6 of Db2 Clients or Drivers
- Supported for JDBC and Non-JDBC applications
  - Equivalent db2dsdriver.cfg keyword is "SSLClientHostnameValidation"

```
db2ds.setServerName("db2server1.mycompany.com");
db2ds.setPortNumber(448);
db2ds.setSslClientHostnameValidation("BASIC");
```

Requires matching "Subject Alternative Name" ("db2server1.mycompany.com") on server certificate

Otherwise TLS handshake fails

TLS V1.3 Support

- **TLS V1.3 is the latest and (currently) most secure TLS version**
- Supported since V11.5.8 of Db2 LUW and Db2 Clients/Drivers
- Non-Java Clients: enabled by default – toleration of downlevel clients possible
  - Set configuration keyword “TLSVersion” in db2dsdriver.cfg to “TLSV13” to enforce TLS V1.3

```
<dsn alias="DSACSSLSRV1" host="10.xx.xxx.xx" name="SS01DSAC" port="xxxx">
   <parameter name="SecurityTransportMode" value="SSL"/>
   <parameter name="SSLServerCertificate" value="e:\certs\ss01\serverauth\SS01CANEW.crt"/>
   <parameter name="TLSVersion" value="TLSV13"/>
</dsn>
```

- **Java Clients: TLS V1.3 support depends on JRE (e.g. IBM Java 8.0.6.25 or higher, Oracle JDK 8u261 or higher)**
  - Set JDBC property “sslVersion” to “TLSv1.3” to enforce TLS 1.3

```
//enforce TLS 13 for Db2 Datasource
db2ds.setSslVersion("TLSv1.3");
```

Encryption Algorithm (Change of Default)

- **JDBC Driver with level 4.33 or above requires encrypted userid and password by default – applies to Db2 LUW / Db2 Connect V11.5.9**
- Changes were made to default values for JDBC driver configuration properties

Old defaults (11.5.8 and earlier)

```
// clear text UID and PW
securityMechanism=3
// 56-bit DES (weak) in case UID and PW should be
// encrypted
encryptionAlgorithm=1
```

New defaults (11.5.9)

```
// encrypted UID and PW
securityMechanism=9
// 256-bit AES (strong)
encryptionAlgorithm=2
```

Important: AES encryption requires ICSF on the z/OS side, otherwise connection will fail

```
DSNL511I  !DSAC DSNLIENO TCP/IP CONVERSATION FAILED 952
           TO LOCATION ::FFFF:10.15.xx.xx
           IPADDR=::FFFF:10.15.xx.xx PORT=52082
           SOCKET=RECV RETURN CODE=1121 REASON CODE=74520442
DSNL045I  !DSAC DSNLCICF ICSF CSNFPKE FUNCTION FAILED 953
WITH RETCODE='0000000C'X AND RSNCODE='00002B34'X
```

Encryption Algorithm (Change of Default), cont.

- **Solution: Configure and start ICSF on the z/OS LPAR**
- Workaround 1: explicitly set securityMechanism to clear text

```
//enforce clear text for UID and PW
db2ds.setSecurityMechanism(DB2BaseDataSource.CLEAR_TEXT_PASSWORD_SECURITY);
```

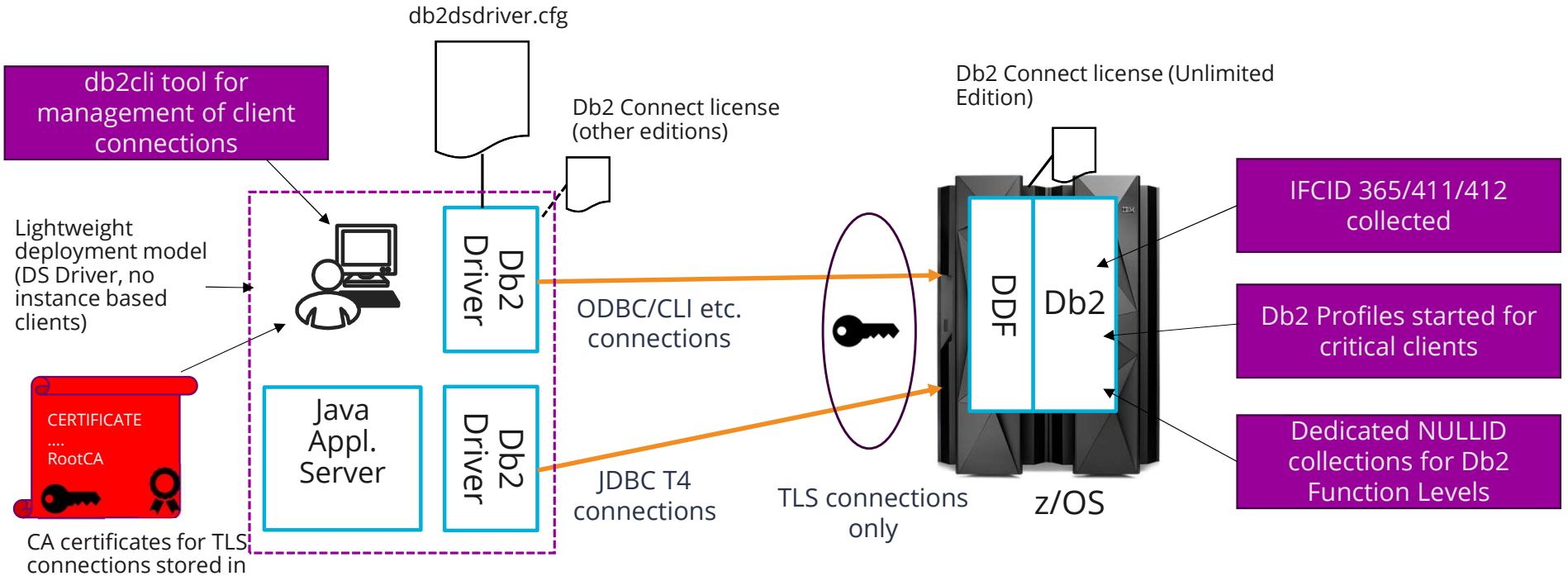
- Workaround 2: explicitly set encryptionAlgorithm to DES

```
//enforce DES encryption
db2ds.setEncryptionAlgorithm(1);
db2ds.setSecurityMechanism(DB2BaseDataSource.ENCRYPTED_USER_AND_PASSWORD_SECURITY);
```

- Note: encryptionAlgorithm cannot be set when clear text password is in effect
- Affects JDBC and SQLJ only
- See this blog for more information: https://community.ibm.com/community/user/datamanagement/blogs/paul-mcwilliams1/2023/11/16/ibm-data-server-driver-jdbc-v433-more-secure?CommunityKey=621c2a2a-01f9-4b57-992f-36ed7432e3bb

Summary

The “All-In-One Picture”




```
con.setClientInfo(name:"ClientUser", value:"JDBC_SampleUser");
con.setClientInfo(name:"ApplicationName", value:"JDBC_SampleApplication");
con.setClientInfo(name:"ClientAccountingInformation", value:"MyAccounting_1");
```

Client Information fields set by client applications

Thank you.

rocketsoftware.com
ctheisen@rocketsoftware.com