DB2 QMF Data Service
Version 12 Release 1

Solution Configuration Guide

GC27-8887-00

DB2 QMF Data Service
Version 12 Release 1

Solution Configuration Guide

GC27-8887-00

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" at the end of this information.

This edition applies to Version 12 Release 1 of IBM DB2 Query Management Facility (QMF) Enterprise Edition, which is a feature of IBM DB2 12 for z/OS (5650-DB2) and IBM DB2 11 for z/OS (5615-DB2). It also applies to Version 12 Release 1 of IBM DB2 QMF for z/OS (5697-QM2), which is a stand-alone IBM DB2 for z/OS tool. This information applies to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview . . . 1
Virtual tables . . . 1

Chapter 2. The SQL solution . . . 3
Configuring Data Service with DB2 QMF for TSO and CICS . . . 3
Configuring access to data sources . . . 3

Chapter 3. Configuring access to data sources . . . 5
Configuring access to data in Adabas . . . 5
Configuring the server started task JCL . . . 5
Modifying the server configuration member . . . 5
Configuring access to data in relational database management systems (RDBMS) . . . 6
Modifying the server configuration member . . . 7
Verifying Coded Character Set Identifier (CCSID) values and definitions . . . 10
Configuring access to IBM DB2 for z/OS . . . 11
Configuring access to non-z/OS databases . . . 12
Configuring access to data in IBM IMS DB . . . 17
Configuring the server started task JCL . . . 17
Modifying the server configuration member . . . 17
Configuring IMS DB . . . 18
Configuring access to VSAM . . . 18
Configuring the server started task JCL . . . 18
Modifying the server configuration member . . . 18
Configuring VSAM . . . 19
Configuring access to sequential files . . . 19
Configuring the server started task JCL . . . 19
Modifying the server member . . . 19
Configuring sequential files . . . 19
Configuring access to SMF data for IT Operational Analytics . . . 19
Configuring System Management Facility (SMF) files . . . 19
Configuring SYSLOG files . . . 21

Notices . . . 23
Trademarks . . . 25
Terms and conditions for product documentation . . . 25
Privacy policy considerations . . . 26

Index . . . 27

Chapter 1. Overview

The QMF Data Service server supports a broad range of data sources, including mainframe relational/ non-relational databases and file structures, distributed databases running on Linux, UNIX, and Windows platforms, Cloud based relational and non-relational data, and NoSQL databases. IBM® DB2 QMF® Data Service solutions have a range of connectivity options for data consumers, including QMF Workstation/WebSphere, QMF Vision, and QMF for TSO/CICS.

Table 1. Partial list of supported data sources

Data support	Data source
Mainframe relational/non-relational databases and file structures	• IBM® DB2 • IBM® Information Management System (IMS/DB) • Native VSAM files • Sequential files • Software AG Adabas
Distributed databases running on Linux, UNIX, and Windows platforms	• IBM® DB2 • Apache Derby • IBM® Informix • Oracle • Microsoft SQL Server

Virtual tables

A virtual table enables data from multiple, disconnected sources to be virtually integrated into a single logical data source. You can use both mainframe and distributed data sources to build mappings and create virtual tables regardless of where the data is located and without having to copy or move the data.

Each data source provides a mechanism for defining data. For example, for VSAM and sequential file data, you use a COBOL copybook to store data definitions. When you create a virtual table, the data definitions determine how to create the mappings.

You create a virtual table only once. After you create a virtual table, you can use any interface to access the data. Virtual tables are used for SQL solutions.

Chapter 2. The SQL solution

To enable ANSI SQL access to mainframe data sources, configure IBM® DB2 QMF® Data Service.

Configuring a solution can include one or more of the following tasks:

- Configure the started task JCL by modifying the CQD1PROC member that is in the *hlq*.SCQDCNTL library.
- Configure the server member that is included in data set member *hlq*.CQDS.SCQDEXEC(CQDSIN00).
- Make definition changes in the data provider interface.

Before configuring the SQL solution, the Data Service server installation must be successfully completed.

You can also use the Data Service Studio to get SQL access to your data.

For information about configuring the SQL solution, see the following topics.

Configuring Data Service with DB2 QMF for TSO and CICS

Before using Data Service with DB2 QMF for TSO and CICS, verify that the configuration is complete. The instructions for setting up Data Service are described in the *Installing and Managing DB2 QMF for TSO and CICS* book.

Procedure

1. Ensure that the IBM® DB2 QMF® Data Service DB2 package, CQDHLI, has been bound to QMF, see QMF job in QMF1210.SDSQSAPE(DSQ1BPKQ).
2. For TSO QMF, ensure that the Data Service dataset CQD.SCQDLOAD has been allocated to all TSO users STEPLIB or ISPLLIB.
3. For QMF CICS ensure that the QMF1210.SDSQSAPE(DSQ1ECSQ) job was run to update the CICS region's CSD that includes the Data Service modules CQDHLI and CQDCLAPI.
4. For QMF CICS ensure that the Data Service load library, CQD.SCQDCLOD, has been allocated to the CICS DFHRPL.

Configuring access to data sources

The server supports access to many mainframe and distributed data sources. You can find detailed information for the specific data interface you want to use.

Before you begin

The server must be installed.

About this task

To configure a data source, see the following tasks:

- "Configuring access to data in Adabas" on page 5

- "Configuring access to data in relational database management systems (RDBMS)" on page 6
- "Configuring access to data in IBM IMS DB" on page 17
- "Configuring access to VSAM" on page 18
- "Configuring access to sequential files" on page 19

Chapter 3. Configuring access to data sources

Configure Data Service server to enable access to mainframe data sources.

Configuring access to data in Adabas

To access Adabas, you need to configure the started task JCL and the server configuration member.

Procedure

To configure and verify access to data in Adabas, perform the following tasks.

Configuring the server started task JCL

Make the ADALNKR module available.

Before you begin

All data sets that you add to the server started task JCL STEPLIB must be APF-authorized.

About this task

Note: You can skip this task if the ADALNKR module is in the z/OS linklist.

Procedure

1. Add the Adabas LOAD library to the server started task JCL. Uncomment the `ADALOAD` parameter and set it to the correct Adabas load library name.

   ```
   ADALOAD='ADABAS.LOAD'
   ```

2. Uncomment the reference to the LOAD library in the STEPLIB.

Modifying the server configuration member

Enable the Adabas parameters in the server configuration member.

About this task

The server configuration member is shipped in data set member *hlq*.SCQDEXEC(CQDSIN00) and copied to *hlq*.CQDS.SCQDEXEC(CQDSIN00) by the job in the CQDGNMP1 member for you to make your local modifications.

Procedure

1. In the CQDSIN00 member, locate the comment “ENABLE ADABAS DATABASE SERVER SUPPORT.”
2. Enable the Adabas parameters by changing `if DontDoThis` to `if DoThis`. Set the `ADABAS` parameter to `YES`.

   ```
   if DoThis then
     do
     "MODIFY PARM NAME(ADABAS)VALUE(YES)"
     "MODIFY PARM NAME(ADABASUBINFOSIZE)VALUE(256)"
     "MODIFY PARM NAME(ADABASAUTOCOMMITBIND)VALUE(YES)"
   ```

```
  "MODIFY PARM NAME(ACIMAPREDUCEADAB)VALUE(64000)"
  "MODIFY PARM NAME(ACIMAPREDUCEADAISN)VALUE(64000)"
end
```

The following table lists the parameters for configuring support for Adabas data stores:

Parameter	Description	Valid values
ACIMAPREDUCEADAB	Map Reduce Adabas Record Buffer Size - Allows Adabas Multi-Fetch used to read records via L1 commands. If the Adabas ADARUN limits are exceeded, an Adabas response code 53 is issued.	Buffer size in bytes. 64000 (default value)
ACIMAPREDUCEADAISN	Map Reduce Adabas ISN Buffer Size - When a Key Descriptor is used in a Search query, an Adabas S1 search is performed. The resulting internal sequence number (ISN) Record number list is divided up into separate Map Reduce threads.	Buffer size in bytes. 64000 (default value)
ADABAS	Activates support for Adabas data stores.	**NO** Support is not active. (default value) **Yes** Activate support.
ADABASAUTOCOMMITBIND	Activates support for the AUTOCOMMIT BIND option.	**YES** Activate support. (default value) **NO** Support is not active.
ADABASUBINFOSIZE	Specifies the total amount of space to allocate for user information and review information in the Adabas user block. Review the maximum user information size in the ADALNKR, and increase the value of this parameter to be equal to or greater than the maximum user information size.	256 KB (default value)

Configuring access to data in relational database management systems (RDBMS)

You can access data on IBM Big SQL, DB2 for z/OS, DB2 LUW (Linux, UNIX, and Windows), and Oracle.

Procedure

1. Enable the RDBMS access method in the DV configuration member. See "Modifying the server configuration member" on page 7.

2. Configure access to the database.
   - IBM DB2 for z/OS

     Configure DB2 to use the Distributed Relational Database Architecture (DRDA) access method.

     See "Configuring access to IBM DB2 for z/OS" on page 11.
   - Non-z/OS databases, including Big SQL, DB2 LUW, and Oracle.

     Configure the RDBMS to use the Distributed Relational Database Architecture (DRDA) access method.

     See "Configuring access to non-z/OS databases" on page 12.

Modifying the server configuration member

Enable the RDBMS access method in the server configuration member.

About this task

Configure the server to use Distributed Relational Database Architecture (DRDA) when accessing a RDBMS.

Modify the server configuration member in data set *hlq*.CQDS.SCQDEXEC(CQDSIN00).

Procedure

1. In the CQDSIN00 member, locate the section that contains the comment "ENABLE DRDA ACCESS TO RDBMS."
2. Enable the DRDA parameters by changing `if DontDoThis` to `if DoThis`. Set the `DRDASKIPZSERVICES` parameter to `YES`.

```
if DoThis then
  do
  "MODIFY PARM NAME(TRACEOEDRDARW)        VALUE(YES)"
  "MODIFY PARM NAME(CLIENTMUSTELECTDRDA)  VALUE(NO)"
  "MODIFY PARM NAME(DRDASKIPWLMSETUP)     VALUE(NO)"
  "MODIFY PARM NAME(DRDAFORLOGGINGTASK)   VALUE(NO)"
```

   The following table lists the parameters for configuring support for DRDA:

Parameter	Description	Valid values
CLIENTMUSTELECTDRDA	If set to YES, JDBC clients must explicitly opt in for DRDA to be used by setting the user parameter connection variable to 'DRDA'. **Note:** JDBC clients can always opt out of DRDA processing by setting the user parameter to 'NODRDA'. If set to NO, DRDA processing is used for access all configured RDBMSs.	**YES** **NO** Default value.

Parameter	Description	Valid values
DRDASKIPWLMSETUP	If set to YES, WLM information is not collected and sent to DRDA during JDBC logon processing. If captured, the DRDA equivalent to SET_CLIENT_ID calls is issued after logon to establish these values on the DRDA connection. If not captured, the transmission that is used to set these WLM-related values is bypassed. If set to NO, the client user ID, application name, workstation name, and accounting token that were sent in the initial client buffer are collected and sent separately after logon processing to DRDA.	**YES** **NO** Default value.
DRDAFORLOGGINGTASK	If set to YES, DRDA processing is used for the CQD DB2 on z/OS logging subtask. If set to NO, SAF or RRSAF connections are used. **Note:** Passticket support must be enabled for the target DDF server. If passticket support is not configured, set the parameter to NO.	**YES** **NO** Default value.
TRACEOEDRDARW	If set to YES (recommended), TCP/IP communications via DRDA are traced. If set to NO, DRDA receive and send operations are not traced.	**YES** **NO** Default value.

3. Define DRDA RDBMSs by entering a definition statement. Provide your local environment values for all the parameters.
   - For DB2 for z/OS:

```
"DEFINE DATABASE TYPE(MEMBER)"          ,
                 "NAME(DSN1)"           ,
                 "LOCATION(DEV1DSN1)"   ,
                 "DDFSTATUS(ENABLE)"  ,
                 "PORT(443)"            ,
                 "IPADDR(127.0.0.1)"  ,
                 "CCSID(37)"            ,
                 "APPLNAME(DSN1LU)"     ,
                 "IDLETIME(110)"        ,
```

   - For DB2 for Linux, UNIX, or Windows:

```
"DEFINE DATABASE TYPE(LUW)"                  ,
               "NAME(UDB1)"                  ,
               "LOCATION(SAMPLE)"            ,
               "DDFSTATUS(ENABLE)"           ,
               "DOMAIN(your.domain.name)"    ,
               "PORT(50000)"                 ,
               "CCSID(37)"                   ,
```

- For Oracle:

```
"DEFINE DATABASE TYPE(ORACLE)"          ,
                "NAME(name)"            ,
                "LOCATION(location)"    ,
                "DDFSTATUS(ENABLE)" ,
                "DOMAIN(domain)"        ,
                "PORT(port)"            ,
                "CCSID(500)"            ,
```

The following table lists the parameters for defining DDF endpoints:

Parameter	Description	Valid values
APPLNAME	Application name. The APPLNAME used by the target endpoint for passticket generations. (*Optional*)	A valid value is 1 - 8 characters. If APPLNAME is not specified in the definition statement, no default value is provided and passticket access is disabled. **Note:** APPLNAME is not required when connecting from the JDBC driver.
CCSID	Specify the EBCDIC single-byte application CCSID (Coded Character Set Identifier) configured for this RDBMS subsystem on the RDBMS installation panel DSNTIPF, option 7. (*Optional*)	Refer to the RDBMS vendor documentation for a list of valid CCSID. **Note:** See "Verifying Coded Character Set Identifier (CCSID) values and definitions" on page 10.
DDFSTATUS	The DDF activation status can be altered online by using the ISPF 4-DB2 dialog panels. (*Required*)	**ENABLE** To make this DDF definition active within CQD. **DISABLE** DDF endpoint is not used.
IPADDR	Specify the dot-notation IPV4 address of the DDF endpoint. (*Optional*)	If this parameter is not specified, the value 127.0.0.1 (local host) is the default. For group director definitions, use the DVIPA IP address of the group director.

Parameter	Description	Valid values
LOCATION	For DB2: The DB2 location name. For LUW: The LUW database. For Oracle: The Oracle SSID as defined to the Oracle Database Provider (Gateway) (*Required*)	A valid value is a string 1 - 16 characters.
NAME	The database name as known to the server. (*Required*)	A valid value consists is 1 - 4 characters. Clients use this ID when they request access to a specific DB2 subsystem.
PORT	Specify the IP port number that is defined for DRDA access in this DDF endpoint. (*Optional*)	If this keyword is not entered, the default DRDA port number 443 is used.
TYPE	If this DDF endpoint is a DB2 group director, specify GROUP. If this DDF endpoint is a DB2 instance or group member for z/OS, specify MEMBER. If this DDF endpoint is a DB2 instance or group member for Linux, UNIX, or Windows, specify LUW. If this DDF endpoint is an Oracle instance, the parameter informs DRDA AR and supportive tooling that the remote server is an Oracle DB Provider which supports DRDA AS. The Oracle DRDA AS must be in z/OS simulation mode.	GROUP (DB2 for z/OS) MEMBER (DB2 for z/OS) LUW (Big SQL and DB2 LUW) ORACLE

Verifying Coded Character Set Identifier (CCSID) values and definitions

Verify that the Unicode translation of the CCSID used in the `DEFINE DATABASE` statement and the CCSID used by the target RDBMS are defined for your z/OS environment.

Procedure

1. You should identify the CCSID of the RDBMS. For example, Oracle may use *ccsid1*. In your `DEFINE DATABASE` statement in the configuration member for the RDBMS you have *ccsid2*. For this example, where Oracle is using *ccsid1*, you need to verify that you have *ccsid1-ccsid2* and *ccsid2-ccsid1* defined in your Unicode translation table on z/OS using the command **`D UNI,ALL`**.

2. If the entry is not present, you need to add the entry to your Unicode translation table and refresh. Please refer to the IBM z/OS documentation on how to add the entry.

   Note: As an alternative, the Unicode table can be appended within the server by using the following statement examples in the server configuration member:

   ```
   "DEFINE CONV SOURCE(ccsid1) TARGET(ccsid2) TECH(RE)"
   "DEFINE CONV SOURCE(ccsid2) TARGET(ccsid1) TECH(RE)"
   ```

Configuring access to IBM DB2 for z/OS

About this task

Before you issue DB2 requests, you must bind DRDA into packages within each DB2 subsystem.

Configuring the server started task JCL

If you use DB2 z/OS, add the DB2 load library to the server started task JCL.

Before you begin

All data sets that you add to the server started task JCL STEPLIB must be APF-authorized.

Procedure

Edit the JCL in the *hlq*.SCQDCNTL(CQD1PROC) member to add the name of the DB2 library to the DB2LIB parameter:

```
DB2LIB='DSNX10'
```

The DB2LIB must contain the DB2 interface modules, such as DSNALI and DSNHLI, and must be in uppercase and enclosed in quotation marks.

Configuring DB2 for Distributed Relational Database Architecture (DRDA)

If you are using a zIIP specialty engine, configure DB2 to use DRDA.

About this task

Before you can successfully issue DRDA requests, you must bind IBM® DB2 QMF® Data Service DBRMs into packages within each target DB2 subsystem.

Procedure

1. Set the DEFAULTDB2SUBSYS parameter in the server configuration member to a valid DB2 subsystem name.
2. Edit the CQDBINDD job that is supplied in the *hlq*.SCQDCNTL data set. Follow the instructions that are provided in the JCL.
3. Run the CQDBINDD job.

Configuring security

Configure security to provide user access to DB2.

Procedure

1. Assign users READ authority.
   - For DRDA, assign users READ authority to the *ssid*.DIST profile.
2. This step only applies to DB2 for z/OS. To grant users access to the DB2 subsystem and to enable passticket logon processing, you must define one RACF PTKTDATA resource for each unique DRDA APPLNAME. To define each PTKTDATA resource, customize and run the appropriate job.
   - CQDRADB2 is for IBM Resource Access Control Facility (RACF) security.
   - CQDA2DB2 is for CA ACF2 (Access Control Facility) security.
   - CQDTSDB2 is for CA Top Secret Security (TSS).

Configuring access to non-z/OS databases

You can configure access data on Big SQL, DB2 LUW (Linux, UNIX, and Windows), and Oracle.

About this task

Configure access to non-z/OS databases as follows.

Procedure

1. "Modifying the server configuration member" on page 7.
2. "Configuring Server Event Facility rules for Big SQL and LUW."
3. "Configuring Server Event Facility rules for Oracle DRDA" on page 14.

Configuring Server Event Facility rules for Big SQL and LUW

Configure Server Event Facility (SEF) rules to provide access to Big SQL and LUW Databases, including databases connected via IBM Federated Server.

Procedure

Auto-enable the SQL Rule SCQDXATH(CQDALUWG) to provide the logon credentials to each LUW instance. Global variables are used to define alternate authentication credential mapping for the SEF ATH Rule.

1. In the IBM DB2 QMF Data Service - Primary Option Menu, select option **E** for Rules Mgmt.
2. Select option **2** for SEF Rule Management.
3. Enter * to display all rules, or ATH to display only authentication rules.
4. Set Auto-Enable for the CQDALUWG rule member by entering A and ENTER.

Example

It is common for data centers to assign different user IDs for access to z/OS and for access to LUW. By default, the server will attempt to log on to LUW with the same user ID that was presented for logon to z/OS. A facility is needed in the server to optionally change a user's logon credentials when accessing DB2 on LUW.

A Server Event Facility (SEF) ATH Rule can be used to set these two parameters for logon to LUW:

```
ATH.AUDROTUS     LUW User ID
ATH.AUDROTPW     LUW Password
```

A SEF Rule could be coded to insert hard coded user IDs and passwords, even testing for different incoming IDs and specific LUW DBs. However, as an alternative to hard coding IDs and passwords in the SEF Rule, *hlq*.SCQDXATH(CQDALUWG) is provided to resolve LUW credentials from the Server Global Variables. Rule CQDALUWG should not be modified, except to toggle tracing of its execution. Server Global Variables for LUW are mapped as follows:

```
GLOBAL2.DRDA.ATH.grexx.GLOBAL.DEFAULT
GLOBAL2.DRDA.ATH.grexx.GLOBAL.userid
GLOBAL2.DRDA.ATH.grexx.ssid.GLOBAL.DEFAULT
GLOBAL2.DRDA.ATH.grexx.ssid.userid
```

Where:

- *grexx* is the name of the active SEF ATH rule, in this case CQDALUWG.
- *ssid* is the target LUW subsystem name in the *x*QD*y*IN00 `DEFINE DATABASE NAME(ssid)` statement.
- *userid* is the incoming z/OS user ID.

The last node of each Global Variable sets the LUW userID and password in the format:

```
userid:password;comment after the semicolon
```

For instance, using active SEF Rule CQDALUWG, a default LUW user ID and password could be set to `luwuser/luwpswd` by setting the subnode value of `GLOBAL2.DRDA.ATH.CQDALUWG.GLOBAL.DEFAULT` to:

```
luwuser:luwpswd;Global Default for any user
```

Similarly, a default LUW user ID and password for subsystem LUW1 could be set to `luw1user/luw1pswd` by setting the subnode value of `GLOBAL2.DRDA.ATH.CQDALUWG.LUW1.GLOBAL.DEFAULT` to:

```
luw1user:luw1pswd;Default for LUW subsystem named LUW1
```

Each user can be assigned unique credentials for `LUW1`. Assuming *ZOSUSER1* and *ZOSUSER2* are the z/OS user id:

```
GLOBAL2.DRDA.ATH.CQDALUWG.LUW1.ZOSUSER1
subnode value
luw1usera:pswda;LUW1 credentials for ZOSUSER1
GLOBAL2.DRDA.ATH.CQDALUWG.LUW1.ZOSUSER2
subnode value
luw1userb:pswdb;LUW1 credentials for ZOSUSER2
etc.
```

Each user can be assigned unique default credentials for `ALL LUWs`. Assuming *ZOSUSER1* and *ZOSUSER2* are the z/OS user id:

```
GLOBAL2.DRDA.ATH.CQDALUWG.GLOBAL.ZOSUSER1
subnode value
luw1usera:pswda;LUW credentials for ZOSUSER1
GLOBAL2.DRDA.ATH.CQDALUWG.GLOBAL.ZOSUSER2
subnode value
luw1userb:pswdb;LUW credentials for ZOSUSER2
etc.
```

Searches to resolve the LUW credentials follow the order:

```
GLOBAL2.DRDA.ATH.CQDALUWG.ssid.userid
GLOBAL2.DRDA.ATH.CQDALUWG.GLOBAL.userid
GLOBAL2.DRDA.ATH.CQDALUWG.ssid.GLOBAL.DEFAULT
GLOBAL2.DRDA.ATH.CQDALUWG.GLOBAL.DEFAULT
```

Global Variables are maintained between recycles of dvServer and between IPLs.

Configuring Server Event Facility rules for Oracle DRDA

Configure Server Event Facility (SEF) rules to provide access to Oracle databases via the Oracle Database Provider for DRDA.

Procedure

1. Auto-enable the SQL Rule SCQDXSQL(CQDSORAC) to allow Data Service Studio Meta discovery on Oracle databases.
   a. In the IBM DB2 QMF Data Service - Primary Option Menu, select option **E** for Rules Mgmt.
   b. Select option **2** for SEF Rule Management.
   c. Enter `*` to display all rules, or `SQL` to display only SQL rules.
   d. Set Auto-Enable for the CQDSORAC(CQD) rule member by entering `A` and `ENTER`.
2. Auto-enable the SEF ATH Rule SCQDXATH(CQDAODBG) to provide the logon credentials to each Oracle instance. Global variables are used to define alternate authentication credential mapping for the SEF ATH Rule.
   a. In the IBM DB2 QMF Data Service - Primary Option Menu, select option **E** for Rules Mgmt.
   b. Select option **2** for SEF Rule Management.
   c. Enter `*` to display all rules, or `ATH` to display only authentication rules.
   d. Set Auto-Enable for the CQDAODBG(CQD) rule member by entering `A` and `ENTER`.
3. Optional: Verify the CQD global variable setup for authentication rules:
   a. In the IBM DB2 QMF Data Service - Primary Option Menu, select option **E** for Rules Mgmt.
   b. Select option **1** for Display Global Variables.
   c. Enter `GLOBAL2` and press enter to display all GLOBAL2 Variables.
   d. If subnode DRDA does not exist, enter `S DRDA` in the COMMAND and press **Enter**.
   e. If subnode ATH does not exist, enter `S ATH` in the COMMAND and press **Enter**.
   f. If subnode CQDAODBG does not exist, enter `S CQDAODBG` in the COMMAND and press **Enter**.

Example

It is common for data centers to assign different user IDs for access z/OS and for access to Oracle AS. By default, the server will attempt to log on to Oracle with the same user ID that was presented for logon to z/OS. A facility is needed in the server to optionally change a user's logon credentials when accessing DB2 on Oracle.

A Server Event Facility (SEF) ATH Rule can be used to set these two parameters for logon to Oracle:

```
ATH.AUDROTUS     Oracle User ID
ATH.AUDROTPW     Oracle Password
```

A SEF Rule could be coded to insert hard coded User IDs and passwords, even testing for different incoming IDs and specific Oracle DBs. However, as an alternative to hard coding IDs and passwords in the SEF Rule,

hlq.SCQDXATH(CQDAODBG) is provided to resolve Oracle credentials from the Server Global Variables. Rule CQDAODBG should not be modified, except to toggle tracing of its execution. Server Global Variables for Oracle are mapped as follows:

```
GLOBAL2.DRDA.ATH.grexx.GLOBAL.DEFAULT
GLOBAL2.DRDA.ATH.grexx.GLOBAL.userid
GLOBAL2.DRDA.ATH.grexx.ssid.GLOBAL.DEFAULT
GLOBAL2.DRDA.ATH.grexx.ssid.userid
```

Where:

- *grexx* is the name of the active SEF ATH rule, in this case CQDAODBG.
- *ssid* is the target Oracle subsystem name in the *x*QD*y*IN00 `DEFINE DATABASE NAME(ssid)` statement.
- *userid* is the incoming z/OS user ID.

The last node of each Global Variable sets the Oracle userID and password in the format:

```
userid:password;comment after the semicolon
```

For instance, using active SEF Rule CQDAODBG, a default Oracle user ID and password could be set to `orauser/orapswd` by setting the subnode value of `GLOBAL2.DRDA.ATH.CQDAODBG.GLOBAL.DEFAULT` to:

```
orauser:orapswd;Global Default for any user
```

Similarly, a default Oracle user ID and password for subsystem ORA1 could be set to `ora1user/ora1pswd` by setting the subnode value of `GLOBAL2.DRDA.ATH.CQDAODBG.ORA1.GLOBAL.DEFAULT` to:

```
ora1user:ora1pswd;Default for ORA subsystem named ORA1
```

Each user can be assigned unique credentials for `ORA1`. Assuming *ZOSUSER1* and *ZOSUSER2* are the z/OS user id:

```
GLOBAL2.DRDA.ATH.CQDAODBG.ORA1.ZOSUSER1
subnode value
ora1usera:pswda;ORA1 credentials for ZOSUSER1
GLOBAL2.DRDA.ATH.CQDAODBG.ORA1.ZOSUSER2
subnode value
ora1userb:pswdb;ORA1 credentials for ZOSUSER2
etc.
```

Each user can be assigned unique default credentials for `ALL Oracles`. Assuming *ZOSUSER1* and *ZOSUSER2* are the z/OS user id:

```
GLOBAL2.DRDA.ATH.CQDAODBG.GLOBAL.ZOSUSER1
subnode value
ora1usera:pswda;ORA credentials for ZOSUSER1
GLOBAL2.DRDA.ATH.CQDAODBG.GLOBAL.ZOSUSER2
subnode value
ora1userb:pswdb;ORA credentials for ZOSUSER2
etc.
```

Searches to resolve the Oracle credentials follow the order:

```
GLOBAL2.DRDA.ATH.CQDAODBG.ssid.userid
GLOBAL2.DRDA.ATH.CQDAODBG.GLOBAL.userid
GLOBAL2.DRDA.ATH.CQDAODBG.ssid.GLOBAL.DEFAULT
GLOBAL2.DRDA.ATH.CQDAODBG.GLOBAL.DEFAULT
```

The following is an example of Oracle Global Variables for the ATH rule CQDAODBG.

```
------------------------- Display Global Variables ------ Row 1 to 10 of 10

 Command ===> Scroll ===> CSR
 LCs: S Show Subnodes M Modify Value X Hex Browse
 D Remove Node and Subnodes P Drop Node B Browse

Global Prefix: GLOBAL2.DRDA.ATH.CQDAODBG

S Subnode Name Nodes Subnode Value
_-------------- ----- ------------------------------------------------------
 EXMP 0 TYPE(ORACLE) Oracle DRDA Provider Example NAME(EXMP)
 GLOBAL 2 TYPE(ORACLE) GLOBAL DEFAULT ATH USERID/PASSWORD

The following is example of Oracle Global Variables for SUBSYS NAME(EXMP) to
swap USERID to ALTUSER.

------------------------- Display Global Variables -------- Row 1 to 1 of 1
 Command ===> Scroll ===> CSR
 LCs: S Show Subnodes M Modify Value X Hex Browse
 D Remove Node and Subnodes P Drop Node B Browse

Global Prefix: GLOBAL2.DRDA.ATH.CQDAODBG.EXMP

S Subnode Name Nodes Subnode Value
_-------------- ----- ------------------------------------------------------
 USERID 0 ALTUSER:PASSWORD;USERID SWAP TO ALTUSER
```

Creating global variables

About this task

Procedure

Verify the CQD global variable setup for authentication rules:

1. In the IBM DB2 QMF Data Service - Primary Option Menu, select option **E** for Rules Mgmt.
2. Select option **1** for Display Global Variables.
3. Enter `GLOBAL2` and press enter to display all GLOBAL2 Variables.
4. If subnode DRDA does not exist, enter `S DRDA` in the COMMAND and press **Enter**.
5. If subnode ATH does not exist, enter `S ATH` in the COMMAND and press **Enter**.
6. If subnode CQDAODBG does not exist, enter `S CQDAODBG` in the COMMAND and press **Enter**.

Example

To create the Global Variable: `GLOBAL2.DRDA.ATH.CQDAODBG.GLOBAL.DEFAULT` and value of `myid:mypwd;my comment`:

1. In the IBM DB2 QMF Data Service - Primary Option Menu, select option **E** for Rules Mgmt.
2. Select option **1** for Display Global Variables.
3. Enter `GLOBAL2` and press enter to display all GLOBAL2 Variables.
4. If the next subnode (in this case, DRDA) does not exist, enter `S DRDA` in the COMMAND and press **Enter**.
5. Select the new subnode (DRDA) by entering `S` in the “S” column and **ENTER**.
6. Repeat steps 4 and 5 until all the subnodes are created except for the last node. For example, the Global Prefix shows `GLOBAL2.DRDA.ATH.CQDAODBG.GLOBAL`.

7. To create the last node (in this example, DEFAULT), only do step 4.
8. Locate the last node and enter the value by typing into the "Subnode Value" column. In this example: `myid:mypwd;my comment`.

   Note: Make sure that the Global Prefix value appended with the Subnode Name matches the search order as documented.

Configuring access to data in IBM IMS DB

To access IMS DB, you need to configure the server started task JCL and the server configuration member.

Before you begin

The server must already be installed.

About this task

Procedure

To configure and verify access to data in IMS DB, complete the following tasks.

Configuring the server started task JCL

Add `IMS.SDFSRESL` to the server started task JCL.

About this task

Note: You can omit this task if the IMS resident library (`SDFSRESL`) module is in the z/OS linklist.

Procedure

Modify the server started task JCL. If the IMS `SDFSRESL` is not already in the link pack area or linklist, add it to the STEPLIB.

Note: All data sets that you add to the server started task JCL STEPLIB must be APF-authorized.

Modifying the server configuration member

Enable the IMS DB parameters in the server configuration member.

About this task

The server configuration member is shipped in data set member *hlq*.SCQDEXEC(CQDSIN00) and copied to *hlq*.CQDS.SCQDEXEC(CQDSIN00) by the job in the CQDGNMP1 member for you to make your local modifications.

Procedure

1. In the CQDSIN00 member, locate the comment "ENABLE IMS CCTL/DBCT SUPPORT."
2. Enable the IMS DB parameters by changing `if DontDoThis` to `if DoThis`. Set the parameter DBCTL to `YES`.

```
if DoThis then
  do
  "MODIFY PARM NAME(DBCTL)              VALUE(YES)"
  "MODIFY PARM NAME(IMSID)              VALUE(IVP1)"
  "MODIFY PARM NAME(IMSDBNAME)          VALUE(IMSX10.SFDSRESL)"
              "MODIFY PARM NAME(IMSMINTHREADS)      VALUE(5)"
              "MODIFY PARM NAME(IMSMAXTHREADS)      VALUE(10)"
              "MODIFY PARM NAME(IMSNBABUFFERS)      VALUE(10)"
              "MODIFY PARM NAME(IMSFPBUFFERS)       VALUE(10)"
              "MODIFY PARM NAME(IMSFPOVERFLOW)      VALUE(10)"
              "MODIFY PARM NAME(TRACEIMSDLIEVENTS)  VALUE(NO)"
end
```

The following table lists the parameters for configuring support for IMS DB data stores:

Parameter	Description	Valid values
DBCTL	Initialize DBCTL support.	**YES** **NO** (default value)
IMSID	IMS SSID of the DBCTL region.	Four-character name
IMSDBNAME	The name of the data set for the IMS residence library.	Data set name
IMSMINTHREADS	Minimum number of threads.	Numeric value. Default is 5.
IMSMAXTHREADS	Maximum number of threads.	Numeric value. Default is 10.
IMSNBABUFFERS	Total number of NBA buffers.	Numeric value. Default is 10.
IMSFPBUFFERS	Fast path buffers per thread.	Numeric value. Default is 10.
IMSFPOVERFLOW	Fast path overflow buffers.	Numeric value. Default is 10.
TRACEIMSDLIEVENTS	Trace IMS DLI events.	**YES** **NO** (default value)

Configuring IMS DB

No modifications are required.

Configuring access to VSAM

No modifications are required to configure the SQL interface for native VSAM. However, you should verify that the server has access to VSAM.

About this task

To configure access to native VSAM, complete the following tasks:

Configuring the server started task JCL

No modifications are required.

Modifying the server configuration member

No modifications are required.

Configuring VSAM

No modifications are required.

Configuring access to sequential files

No modifications are needed to configure the SQL interface to access sequential files.

About this task

Configuring the server started task JCL

No modifications are required.

Modifying the server member

No modifications are required.

Configuring sequential files

No modifications are required.

Configuring access to SMF data for IT Operational Analytics

IT Operational Analytics (ITOA) allows you to retrieve, analyze, and report data for IT operations. System information can be logged using the IBM System Management Facility (SMF) and the native Data Service server logging feature. Logging allows you to collect various systems and operations-related information.

Before you begin

IBM APAR OA48933 provides real-time SMF support and is a requirement for the configuration of real-time SMF. Obtain and apply the fix for this APAR.

About this task

Virtual tables for SMF are provided in the *hlq*.SCQDSMAP data set.

There are two options to access the SMF data, real-time SMF (in memory) and SMF data sets.

To configure IT Operational Analytics, complete the tasks that follow.

Configuring System Management Facility (SMF) files

To configure SMF, you need to configure the server started task JCL, the server configuration member, and the server virtual table member.

Procedure

1. Configure the server started task JCL. Concatenate the *hlq*.SCQDSMAP data set to the `CQDMAPP DD` statement to add all maps for SMF.
2. Customize the server configuration member. To enable virtual table rule events, configure the `SEFVTBEVENTS` parameter in the CQDSIN00 member.

   ```
   "MODIFY PARM NAME(SEFVTBEVENTS) VALUE(YES)"
   ```

   Verify the VTB ruleset name:

```
"DEFINE RULESET NAME(VTB)"
       "RULETYPE(VTB)"
       "DSNAME('"||SHLQ2||".SCQDXVTB')"
```

If there were any changes to CQDSIN00, recycle the server started task.

3. To use real-time SMF, add the following statements to the CQDSIN00 member after the GLOBAL PRODUCT OPTIONS statement.

```
IF DoThis
  THEN DO
    "DEFINE SMF NAME(IFASMF.INMEM)",
    "BUFSIZE(500)",
    "TIME(0)"
END
```

4. Customize the Server Event Facility rule SCQDSMAP in the VTB ruleset using ISPF option SEF Rule Management with the SMF dump data set, the logstream data set or in-memory name. You can choose to activate all three options by customizing the rule.

   The VTB rule can select from a GDG data set, any SMF dump dataset, logstream data set or the in-memory stream.

   a. In the IBM DB2 QMF Data Service - Primary Option Menu, select option **E** for Rules Mgmt.
   b. Select option **2** for SEF Rule Management.
   c. Enter VTB for Display Only the Ruleset Named.
   d. Select the SCQDSMAP member by entering S and ENTER.
   e. Edit the SMF data set as follows:

      Note: If you do not have GDG, leave GDGBASE as it is.

```
when PHASE = "INIT" then
    do
/*--------------------------------------------------------------------*/
/*    Create the required global variables.                           */
/*    Rather than modifying the default values in this rule           */
/*    we recommend that you use the Global Variable application       */
/*    or another SEF rule to set the values for your site.            */
/*--+----1----+----2----+----3----+----4----+----5----+----6----+----*/
      /* Set up the required global variables */
      if SDBVALUE("GLOBAL2.SMFTBL2.GDGBASE","E") = "N" then
        GLOBAL2.SMFTBL2.GDGBASE = "HLQ.SMF.DUMP.DSN"
          < === point to your raw smf dataset
      if SDBVALUE("GLOBAL2.SMFTBL2.DEFAULT","E") = "N" then
        GLOBAL2.SMFTBL2.DEFAULT = "HLQ.SMF.DUMP.DSN(+0)"
          < === point to your raw smf dataset
    end   /* End of INIT phase code */
```

   f. Enable the rule by entering E and ENTER. Set this to Auto-enable by using A and ENTER.
   g. Check to make sure the Global Variable is created with the raw SMF data set: Navigate one screen back on the ISPF panel or start over by going to option **E** (Rules Mgmt) and **1** (Global Variables). In this Global Variable display, select the following:
      1) Change Global Prefix to GLOBAL2.
      2) Select SMFTBL2 by entering S next to the SMFTBL2 data set.
      3) GDGBASE and DEFAULT should have its corresponding SMF dump data set name if used.
      4) IM should have its corresponding SMF in-memory name if used.
      5) LOG should have its corresponding SMF logstream name if used.

Note:

VTB rules and global variables may be used to reference a GDG data set, any SMF dump data set, logstream data set or the in-memory stream. For example:

```
GLOBAL2.SMFGBL2.YESTERDAY = "RSPROD.DEV1.SMFDUMP(-1)"

GLOBAL2.SMFGBL2.M2 = "RSPROD.DEV1.SMFDUMP(-2)"

GLOBAL2.SMFGBL2.M3 = "RSPROD.DEV1.SMFDUMP(-3)"

GLOBAL2.SMFGBL2.M4 = "RSPROD.DEV1.SMFDUMP(-4)"

GLOBAL2.SMFGBL2.M5 = "RSPROD.DEV1.SMFDUMP(-5)"

GLOBAL2.SMFGBL2.IM = "IFASMF.INMEM"

GLOBAL2.SMFGBL2.IM2 = "IFASMF.INMEM2"

GLOBAL2.SMFGBL2.LOG = "LOGSTREAM.dataset.name"
```

5. Enable the virtual table rule CQDSMFT3 to support the ability to pass a dynamic data set name for SMF tables. This REXX program is invoked by the SEF every time a table with the prefix 'SMF_' is found in the SQL statement. At invocation, this rule looks for an SMF map name, double underscore "__", and then the data set name for the SMF tables. The table name in the SQL statement must be of the form:

   `BaseMapName__DataSetName`

   Where `DataSetName` contains underscores instead of periods.

   For example, `SELECT * FROM SMF_03000__DATA_SET_NAME` would translate into an SQL Query of `SELECT * FROM SMF_03000` and access the data set `DATA.SET.NAME`.
6. In the Studio:
   a. On the **Server** tab, expand **SQL** > **Data** > **Virtual Tables**.
   b. Right-click on any SMF data set.
   c. Select **Generate Query** to run the query.

Configuring SYSLOG files

To configure SYSLOG files, you need to configure the server configuration member and the server virtual table member.

Procedure

1. Customize the server configuration member. To enable virtual table rule events, configure the `SEFVTBEVENTS` parameter in the CQDSIN00 member.

   `"MODIFY PARM NAME(SEFVTBEVENTS) VALUE(YES)"`
2. Customize the virtual table rule CQDYSLOG with the System Logging data set name.

Notices

This information was developed for products and services offered in the US. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as shown below.

© (*your company name*) (*year*).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. (*enter the year or years*).

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions:

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM®.

Commercial use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Index

A

Adabas
  server configuration 5
analytics
  configure 19
ANSI SQL data access 3

C

Coded Character Set Identifier (CCSID)
  verifying 10
Configuring
  DB2 for Distributed Relational Database Architecture (DRDA) 11
  server started task JCL 11
CQDDFDIV member 3
creating
  system data sets 3

D

data access
  configure access 3
DB2
  configure the started task 11
Distributed Relational Database Architecture (DRDA)
  configuring access 7

I

IBM DB2 for z/OS
  configure access to data 11
IBM® DB2 QMF® Data Service
  overview 1
IMS DB
  configure access to data 17
IMS DBconfiguring 18

J

JCL
  configure started task 18
  configuring 5
  started task 5

L

links
  non-IBM Web sites 25

N

notices
  legal 23

S

Security
  configure 12
sequential files
  configuring access 19
server event facility (SEF)
  configure 12, 14
SYSLOG
  configuring 21
system data sets
  creating 3

V

VSAM
  access to VSAM data 18

Product Number: 5650-DB2
5615-DB2
5697-QM2

Printed in USA

GC27-8887-00