SAP NetWeaver 2004s SPS 4

Security Guide

SAP Security Guide for IBM DB2 UDB for z/OS

Document Version 1.00 – October 24, 2005

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this documentation at the following Internet address:
`service.sap.com/securityguide`

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, *F2* or *ENTER*.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

SAP Security Guide for IBM DB2 UDB for z/OS

The following is meant to serve as reference material for security issues in an SAP on DB2 for z/OS environment. The target audience is advanced users. Only security **settings** are described in this documentation.

For more information about security in an SAP on IBM DB2 UDB for z/OS environment, see the following guides at **`service.sap.com/operationsnw2004s`**:

- *SAP Database Administration Guide for SAP NetWeaver on IBM DB2 UDB for z/OS*

  This guide is referred to here as *SAP DBA Guide for DB2.*
- *SAP Planning Guide for SAP NetWeaver on IBM DB2 UDB for z/OS*

  This guide is referred to here as *SAP Planning Guide for z/OS.*

1 General Information

This documentation describes the security settings needed in conjunction with using an SAP system on DB2 for z/OS.

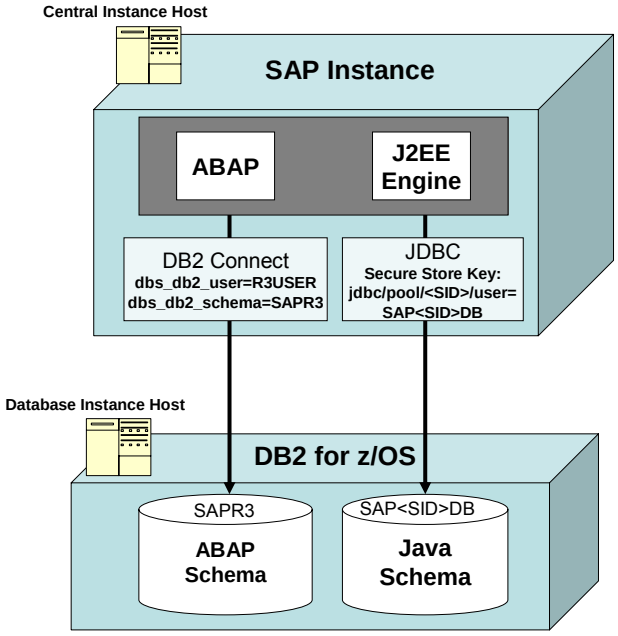
The following topics are covered:

- Connection Between Your SAP System and DB2 on z/OS
- Security Settings for z/OS
- Security Settings for DB2
- Security Settings for DB2 Connect (AIX, Linux and Windows)

2 Connection Between Your SAP System and DB2 on z/OS

This section is **not** a procedure. It is a description of the connection process from you SAP system to DB2 on z/OS.

The way your SAP system is connected to your database server depends on whether you are in an ABAP or Java environment:



ABAP Environment

`dbs_db2_user`, which is your DB Connect user, is specified when you install your database. `dbs_db2_user` is a member of the group `dbs_db2_schema`, which is the schema of the DB2 objects of the SAP system.

In this scenario, the environment variable `dbs_db2_user` is set to R3USER, and the `dbs_db2_schema` must be set to SAPR3.

When you log on to the database running on z/OS with R3USER, the following occurs:

1. RACF checks if the R3USER logon was correct.

   At this point, you are connected to the DB2 subsystem.

2. The R3USER is connected to DB on z/OS with the following command:

   `set current sqlid = SAPR3`

   RACF checks if the user ID R3USER is a member of the group SAPR3.

3. If yes, the ABAP schema is set to SAPR3.

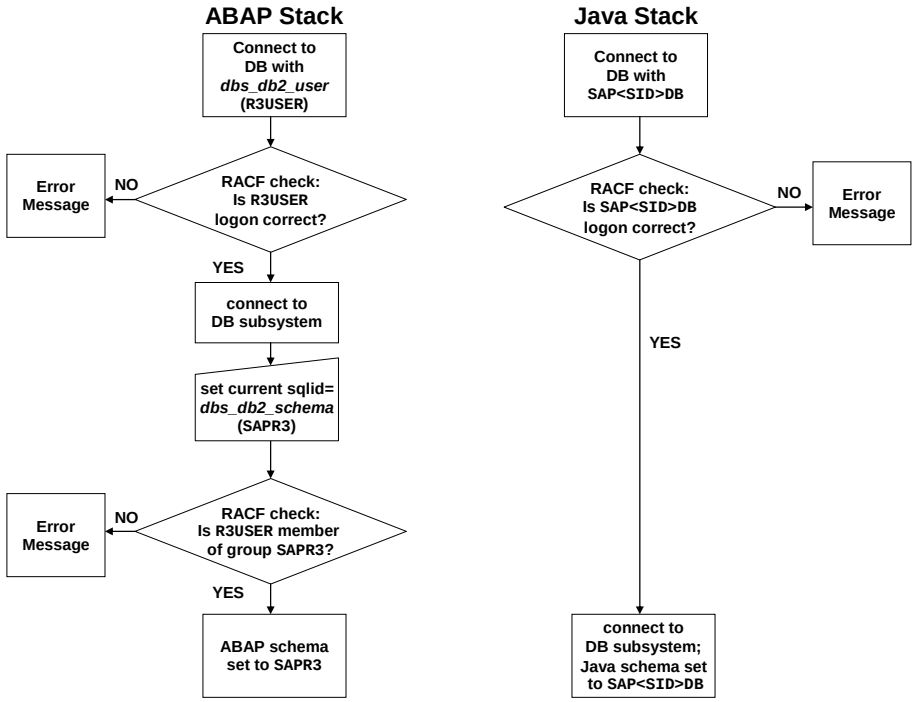
Java Environment

The user SAP<SID>DB exists and must not be created.

When you log on to the database running on z/OS with R3USER, the following occurs:

1. RACF checks if the SAP<SID>DB logon was correct.
2. If yes, then you are connected to the DB2 subsystem and the Java schema ist set to SAP<SID>DB.

The following graphic is a flow chart of both procedures:



3 Security Settings for z/OS

3.1 z/OS Security, Group IDs and User IDs

The following sections address topics related to the security of your SAP on DB2 system environment regarding:

- user IDs and authorization on z/OS and DB2
- physical security

The user IDs and group IDs mentioned in the following sections contain variable parts. The variable text that you need to replace with the valid value for your installation is enclosed in angle brackets (<>). The following variables are used:

Variable	Description
`<SCHEMA>`	The DB2 schema
`<SAPSID>, <sapsid>`	The SAP system identifier (in uppercase and lowercase letters) used for the SAP system that you plan to install. Refer to the SAP installation documentation for details on choosing the DB2 SAP system identifier. SAP requires that you use the name `<sapsid>adm` for the user that runs the SAP application server.
`<sapsid>adm`	The user ID used to run the SAP SCS instance

3.1.1 Overview

In the SAP client/server environment, you need to consider security from the presentation servers to the database server. This includes network, UNIX, Windows, SAP System, z/OS, and DB2 security:

UNIX-Style Security

Each UNIX-style system that runs SAP servers (application, update, message, and so on) has UNIX-style IDs and files that must be secured. To run SAP, the user ID `<sapsid>adm` is needed. In addition, `root` user access is needed to run the installation tool.

When SAP is installed on a UNIX-style system, the user ID `<sapsid>adm` is created by the SAP installation tool and does not need to be created during preparation.

SAP System Security

The SAP system has a security system that is used to grant user IDs access to transactions, data, and resources (such as printers).

z/OS Security

z/OS Security Server (RACF) or a similar security function protects resources and authorizes users in z/OS and UNIX System Services environments. Several user IDs need to be created (see z/OS Security [Page 10]).

DB2 Security

DB2 controls the access to database resources, such as tables and views. All transactions of a single SAP system use the same DB2 schema. An SAP ABAP application will change its SQLID to this DB2 schema when it accesses the database. However, an SAP Java application will not change its SQLID to this DB2 schema when it accesses the database. All DB2 objects that correspond to the SAP Java system use the DB2 schema of the Java Connect user. For more information, see Connection Between Your SAP System and DB2 on z/OS SAP Library.

Server and Network Physical Security

Physical security must be ensured in such a way that nobody can tamper with the z/OS, AIX, Linux, and Windows systems and the connections between them. We recommend that you separate your SAP system from your intranet by a firewall or the equivalent.

Connection between the SAP Application Server and DB2

SAP applications connect to DB2 via DB2 Connect and DDF (ABAP) or jdbc common client (jcc) and DDF (Java). DDF checks the user authorization at connect time using an RACF user (the DB Connect User ID) which is provided by the client at connect time.

For more information, see Connection Between Your SAP System and DB2 on z/OS SAP Library.

3.1.2 UNIX-Style Security

UNIX-style security (implemented on AIX, Linux and z/OS UNIX System Services) is implemented using UNIX-style user IDs (UID) and group IDs (GID). The UIDs and GIDs are numbers. The names of the groups and users are symbols that stand for the current GID and UID numbers. If two user names share the same UID number, they are the same user to a UNIX-style system. Keep the following in mind when adding or checking users and UIDs or GIDs:

- The UID number used by the `<sapsid>adm` user must not be assigned to any other user ID.
- The SAPSYS group must contain only SAP `<sapsid>adm` user IDs.
- The GID number used by the SAPSYS group must not be assigned to any other group.

In a UNIX environment, if you have several SAP application servers on different UNIX systems which share data (for example `/usr/sap/trans`), it is important for NFS that the UID and GID numbers match on all systems. In other words, `<sapsid>adm` must have the same UID on all systems, and SAPSYS must have the same GID on all systems. This can be implemented manually on each system, or by using the NIS (Network Information System) shared passwd and group files.

On z/OS, users and groups are defined by using the z/OS Security Server (RACF). The UNIX attributes of a user or group are specified in the OMVS segment. NIS is not supported on z/OS.

z/OS is no longer available as application server, however you may install your SAP SCS instance on this operating system.

3.1.3 z/OS Security

This section describes security setup using the z/OS Security Server (RACF). If you use a different security product, the following sections will give you an idea of the kind of security you must set up before using your product.

3.1.3.1 z/OS Group IDs

The following z/OS group IDs and user IDs need to be created as part of the preparation:

Group ID <SCHEMA>

A z/OS group ID <SCHEMA> must exist on z/OS, since <SCHEMA> is the creator of all SAP objects in the DB2 subsystem. The group ID <SCHEMA> must be defined as a DB2 secondary authorization ID of <sapsid>adm. This can be done after the DB2 subsystem setup is complete.

To define DB2 secondary authorization IDs, you have to change the default sign-on exit routine. This is described in the SAP NetWeaver installation documentation.

The group ID <SCHEMA> needs several DB2 privileges. The DB2 subsystem setup must be complete before the job can be run.

Special Considerations for MCOD

In an MCOD environment, you have to ensure that each group ID <SCHEMA> is either defined as a DB2 secondary authorization ID of <sapsid>adm or the DB Connect User IDs, or both.

Special Considerations for the J2EE Engine

For the J2EE Engine, the schema of the DB2 objects that belong to the Java system is identical to the J2EE Connect user sap<sapsid>db. Therefore, the concept of the secondary authorization ID does not apply to the Java stack. The primary authorization ID is always used.

Group ID SAPSYS

The group ID SAPSYS is a z/OS UNIX System Services group ID that must be defined to run the SAP SCS instance on z/OS. You define the group to RACF with an OMVS segment specifying the group ID (GID). In a heterogeneous environment with SAP systems on other UNIX platforms, the GID must be the same on all systems. This is important for NFS.

3.1.3.2 z/OS User IDs

The following sections describe the user IDs that you need to create as part of the installation preparation.

Setting the DB Connect User ID

DDF checks the user authorization at connect time using an RACF user (the DB Connect User ID).

For more information on how to define the DB Connect user on the client side for ABAP applications, see the *SAP DBA Guide for DB2*.

If you are using the RACF resource class DSNR for protecting access to DB2, then you need to give the DB Connect User the necessary authority so that it can access DB2 via DDF. This is done by giving the DB Connect user READ access to the `<db2subsystem>.DIST RACF` profile.

Java Applications

For Java applications, the DB Connect user must conform to the SAP naming convention: `sap<sapsid>db`.

The DB Connect user for Java applications is referred to in the SAP NetWeaver installation guides as the **Java Schema ID**.

See Also

For details on securing access to DB2 and setting up RACF protection, see “Controlling Access to a DB2 Subsystem” of the IBM documentation *DB2 UDB for z/OS V8 Administration Guide*, document number SC18-7413-00.

User ID to Install an SAP SCS Instance on z/OS

You need to create a z/OS user ID with superuser authorization to install an SAP SCS instance on z/OS.

Use this user ID whenever the SAP installation guide refers to the user ID `root`.

Define a user ID with the following attributes:

- The RACF Userid Profile should have an OMVS segment with a UID of 0 and its DEFAULT GROUP set to SAPSYS.

```
ALU (root-user) DFLTGRP(SAPSYS) OMVS(UID(0)) ...
```

- If the profile `BPX.DAEMON` of the RACF `FACILITY` class is defined on your system, allow READ access to `BPX.DAEMON` and READ access to `BPX.DAEMON.HFSCTL`.

```
PE BPX.DAEMON CLASS(FACILITY) ACCESS(READ) ID(root-user)
```

- READ access to the profile `BPX.SUPERUSER` of RACF's `FACILITY` class.

```
PE BPX.SUPERUSER CLASS(FACILITY) ACCESS(READ) ID(root-user)
```

- READ access to the profile BPX.FILEATTR.PROGCTL of RACF's FACILITY class.

```
PE BPX.FILEATTR.PROGCTL CLASS(FACILITY) ACCESS(READ) ID(root-user)
```

- READ access to the profile IRR.RADMIN of RACF's FACILITY class. If the profile did not previously exist, define it first. This profile authorizes the user to verify the other RACF settings. The SAP installation tool attempts to do such a RACF verification and will fail with RACF return code of 8 and reason code of 24 if this profile is not set up correctly.

```
PE IRR.RADMIN CLASS(FACILITY) ACCESS(READ) ID(root-user)
```

- READ access to the DB2 data set you specify as STEPLIB, that is, the load library <HLQ>.SDSNLOAD.

```
PE '<HLQ>.SDSNLOAD' ACCESS(READ) ID(root-user)
```

- Set the AUDITOR (or the SPECIAL) attribute for the user ID.

```
ALU (root-user) AUDITOR
```

  The attribute enables the SAP installation tool to verify the security setup of the installation user ID itself and that of <sapsid>adm. It verifies that the user ID <sapsid>adm exists and that the access permissions to RACF profiles are set as described in this section. If <sapsid>adm does not exist or the access permissions are insufficient, the installation utility generates error messages; these errors have to be corrected by the administrator.

Make sure that this user ID is also permitted to allocate up to 2 GB of storage. If you are using rlogin, the parameter MAXASSIZE applies. If you are using the z/OS UNIX shell via TSO log-on, the TSO REGION size must be set to 2 GB.

In particular, log on to this user ID to run the SAP installation tool; do not use the su command to switch to UID=0 because this will not grant you the required RACF authorization.

For further information on these security profiles, refer to "Defining Superuser Attributes for Users" in the IBM documentation *z/OS UNIX System Services Planning*.

Enhanced ASCII

The _BPXK_AUTOCVT variable controls the autoconversion, while the _TAG_REDIR_* variables control the tagging if standard input/output is redirected with <, > or |.

To enable enhanced ASCII support, include the following lines in the .profile file in the home directory of the <sapsid>adm user:

```
export _BPXK_AUTOCVT=ON
export _TAG_REDIR_IN=TXT
export _TAG_REDIR_OUT=TXT
export _TAG_REDIR_ERR=TXT
```

To enable enhanced ASCII support, include the following lines in the `.cshrc` file in the home directory of the `<sapsid>adm` user:

```
setenv _BPXK_AUTOCVT ON
setenv _TAG_REDIR_IN TXT
setenv _TAG_REDIR_OUT TXT
setenv _TAG_REDIR_ERR TXT
set _TAG_REDIR_IN=TXT
set _TAG_REDIR_OUT=TXT
set _TAG_REDIR_ERR=TXT
```

The "=" sign is required for **`export`** and **`set`** but is not valid for **`setenv`**.

User ID <sapsid>adm to Run the SAP SCS Instance on z/OS

The user ID `<sapsid>adm` – where `<sapsid>` is the SAP system identifier – is a z/OS UNIX System Services user ID. This user ID is needed to run the SAP SCS instance on z/OS.

Define the following attributes for this user ID:

- RACF definition with the OMVS segment specifying the UID and GID; as the GID, use the number you have specified for SAPSYS. In a heterogeneous environment with SAP application server instances on other UNIX platforms, the UID must not be 0 and the UID and GID must be the same on all systems. This is important for NFS.
- Home directory is `/u/<sapsid>adm`. The home directory may be shared with application servers on other UNIX systems.
- As the startup program, specify the C-shell: `/bin/csh` (see also "The C-shell, tcsh, and Korn shell" in *SAP Planning Guide for z/OS*).
- Optionally, specify maximum values for ASSIZEMAX, CPUTIMEMAX, PROCUSERMAX, FILEPROCMAX, and THREADSMAX. This is necessary if the system-wide settings are left at a lower value but the settings are increased for individual users. See "Specifying limits for individual users" in *SAP Planning Guide for z/OS*.
- If the `<sapsid>adm` user enters the z/OS UNIX shell via TSO log-on, the TSO region size must be set to 2 GB and the TIME parameter of the TSO logon procedure must be set to NOLIMIT.

- Since a user ID defined in RACF is always given in uppercase, but UNIX expects the user ID in lowercase, you must define a lowercase alias for the user ID in the file that was specified as USERIDALIASTABLE in parmlib member BPXPRMxx. See “Selecting the UNIX System Services parameters” in *SAP Planning Guide for z/OS*. If the file does not exist, create it. The following sample entry was created in USERIDALIASTABLE for the user ID <sapsid>adm of an SAP System with the system identifier C11:

  C11ADM c11adm

  The table is column-oriented. The uppercase user ID must start in column 1 and the lowercase alias in column 10. The in-storage copy of the table is regularly refreshed by the system. Using the OMVS operator command SET OMVS allows an immediate activation of the changes to that table.

  You can verify the definition using the command ID <sapsid>adm. The user name should appear in lowercase characters now.

- For the z/OS UNIX environment, the default language setting, LANG=C, and the default code page, IBM-1047, are to be used; the default is used if the environment variable LC_ALL is not set.
- READ, WRITE, EXECUTE (rwx) permissions to its home directory /u/<sapsid>adm, to /usr/sap/<SAPSID>, to /sapmnt/<SAPSID>, and to all of their subdirectories.
- READ access to the profile BPX.MAP of RACF's FACILITY class.

  ```
  PE BPX.MAP CLASS(FACILITY) ACCESS(READ) ID(<SAPSID>adm)
  ```

- READ access to the profile BPX.WLMSERVER of RACF's FACILITY class: WLM registration of the SAP SCS instance on z/OS can be enabled by setting the appropriate SAP profile parameter.

  ```
  PE BPX.WLMSERVER CLASS(FACILITY) ACCESS(READ) ID(<SAPSID>adm)
  ```

- READ access to the profile SUPERUSER.FILESYS.PFSCTL of RACF's UNIXPRIV class.

  ```
  PE SUPERUSER.FILESYS.PFSCTL CLASS(UNIXPRIV) ACCESS(READ)
  ID(<SAPSID>adm)
  ```

- READ access to the profile ERBSDS.SMFDATA of RACF's FACILITY class. This allows the operating system monitor saposcol to read the SMF records written by RMF.

  ```
  PE ERBSDS.SMFDATA CLASS(FACILITY) ACCESS(READ)
  ID(<SAPSID>adm)
  ```

- Define the profile BPX.SAFFASTPATH of RACF's FACILITY class. For performance reasons, this profile is strongly recommended. For further information, see *z/OS UNIX System Services Planning*, section "Establishing the FastPath support for system authorization facility (SAF)".

```
RDEFINE FACILITY BPX.SAFFASTPATH UACC(NONE)
```

- If the SAP SCS instance on z/OS is started as a started task, the user <sapsid>adm and group SAPSYS must be associated with the started task. This can be achieved by using the RACF STARTED class.

User ID for Selected SAP System Installation Tasks

During the SAP system installation, a database administration user ID for job submission and for FTP access to z/OS is needed. The database administration user ID is needed for remote SAP application servers as well as for the SAP SCS instance on z/OS. It is only needed during the installation of the SAP system and must have the following attributes:

- DB2 SYSADM authority
- Authority to submit JCL jobs that invoke DB2 BINDs and GRANTs
- Authority to create and read data sets under its own High Level Qualifier (HLQ) on the default volume

If you have defined the RACF profile BPX.DAEMON of the RACF FACILITY class, you must add the FTP server user ID to this class profile. This enables the FTP daemon to submit the job on behalf of the user who requested the JCL submission service. For setting up a daemon, refer to "Setting Up for Daemons" in the IBM documentation *z/OS UNIX System Services Planning*.

User IDs for Selected SAP CCMS Functions

The Computer Center Management System (CCMS) functions that involve submitting jobs on z/OS, performing DB2 utilities, and viewing system console log output require a TSO user with the authorities necessary to perform these tasks. The TSO user ID must be the same as that of the SAP system user that is using the CCMS functions, and must not be more than seven characters long.

These TSO users are not necessary during SAP setup and can be created after successful SAP system installation.

For more information, see the *SAP DBA Guide for DB2*.

3.2 Security Considerations for NFS

The NFS server attribute `SECURITY(EXP,EXP,EXP)` means that normal UNIX-style security applies. If `SECURITY(SAF,SAF,SAF)` is specified, the command **`mvslogin`** must be executed and the z/OS password typed in before the files can be accessed.

SAF security is needed when installing the SAP SCS instance on z/OS to gain root authorization. It is not needed during normal SAP system operation. In fact, SAF security must not be used when running the high availability solution described in the IBM publication *High Availability for SAP on zSeries Using Autonomic Computing*, document number: SC33-8206.

Case 1

A customer's SAP file system is on z/OS and he would now like to install a dialog instance on AIX. To do this, the customer must do the following:

3. Invoke the SAP installation tool as the `root` user.
4. In order for the SAP installation tool to access the files, the customer must first issue the command **`mvslogin`** (thus obtaining UID=0 authorization on z/OS; a warning message about mismatching GID can be ignored).
5. During the installation, the SAP installation tool creates the AIX user ID `<sapsid>adm` and switches to that user ID, which leads to a permission error when accessing z/OS files.
6. The AIX user `<sapsid>adm` must now execute **`mvslogin`** to gain the appropriate authorization before the SAP installation tool is able to continue. In this case, the UID and GID of the AIX and the z/OS user ID must match.

Case 2

If, however, we assume that the shared files reside on an AIX file system and they are to be accessed from z/OS, security is controlled by the export file on AIX.

In this case, there is no need to perform a log-in with **`mvslogin`** before attempting to access the files; however, the UID and GID must match. Because the installation process runs under superuser authorization, the exported file systems must allow `root` access.

3.3 Security Considerations for SMB

Logon Considerations

To ensure that an application server can access shared resources without user intervention, SMB supports two different methods of user authentication without prompting the user for a password.

RACF DCE Segments for SMB Encrypted Password Support

To enable the SMB server to use encrypted passwords, you must set up the user ID `<sapsid>adm` and the SAP installation user ID `<root>` on z/OS for SMB encrypted password support.

Procedure

1. Activate the RACF class KEYSMSTR:

   SETROPTS CLASSACT(KEYSMSTR)

2. Define a DCE.PASSWORD.KEY entry in the class KEYSMSTR:

   RDEFINE KEYSMSTR DCE.PASSWORD.KEY
   SSIGNON(KEYMASKED(nnnnnnnnnnnnnnnn))

3. Define the RACF DCE segment for the user IDs <sapsid>adm and <root>:

   ALTUSER <sapsid>adm DCE

   ALTUSER <root> DCE

4. Log on as <sapsid>adm and enter the following z/OS UNIX System Services command:

   smbpw <login_password> <login_password>

   where <login_password> is the password of <sapsid>adm on Windows.

   This step must be repeated whenever the password is changed on Windows.

5. Log on as <root> and enter the following z/OS UNIX System Services command:

   smbpw <administrator_password> <administrator_password>

   where <administrator_password> is the password specified for the SAP installation user ID (<administrator>) that has administrator rights on Windows.

   This step must be repeated whenever the password is changed on Windows.

6. Enable the SMB server to use encrypted passwords by setting the following environment variable for the server process DFSKERN in file envar, which is normally located in /opt/dfslocal/home/dfskern:

   _IOE_SMB_CLEAR_PW=NOTALLOWED

Using Passthrough Authentication

Passthrough authentication permits the SMB server to use a domain controller to authenticate a client trying to log on to the SMB server. The SMB server will log on to the domain controller using the account name (user ID) and the challenge response from the client. If the logon to the domain controller is successful, the client is allowed to establish a session with the SMB server and the PC user ID will be mapped to a local (RACF) user ID. For detailed information, see APAR II13046.

For more information, see the IBM documentation *z/OS Distributed File Service SMB Administration*, "Chapter 7: Sharing Files, Logon considerations".

Mapping SMB User IDs to z/OS User IDs

ID mapping entries must be created in table smbidmap for the following user IDs:

- SAPService<SAPSID> must be mapped to <sapsid>adm.
- <sapsid>adm must be mapped to <sapsid>adm.
- The user ID <administrator> must be mapped to the user ID <root>.

Example of `smbidmap` table definitions:

```
SAPServiceEZ1
ez1adm

ez1adm
ez1adm

administrator
sup8
```

For detailed information on how to specify the entries in `smbidmap`, see the IBM documentation *z/OS Distributed File Service SMB Administration*, "Chapter 6: Mapping SMB user IDs to z/OS user IDs".

The following environment variable for DFSKERN must point to the mapping file:

`_IOE_SMB_IDMAP=<path_of_mapping_table>/smbidmap`

If `dfs` has already been started, enter the following command on z/OS to reload the user ID mapping table `smbidmap`:

`modify dfs,send dfskern,reload,smbmap`

4 Security Settings for DB2

4.1 Security Considerations for RTS and DSNACCOR

The following are security considerations for Real Time Statistics and DSNACCOR.

- Grant the `EXECUTE` privilege for the procedure `DSNACCOR` to public.
- Grant the RACF group `<SCHEMA>` `SELECT` privileges on the RTS tables `SYSIBM.TABLESPACESTATS` and `SYSIBM.INDEXSPACESTATS`.

If your SAP system is installed with the schema SAPR3, the following SQL statements must be issued in SPUFI or similar tool:

```
GRANT SELECT, DELETE ON SYSIBM.TABLESPACESTATS TO SAPR3;

GRANT SELECT, DELETE ON SYSIBM.TABLESPACESTATS TO SAPR3;
```

For more information, see the SAP Database Administration Guide for DB2 at

`service.sap.com/instguidesNW04` → *Operations* → *SAP Database Administration Guide for DB2.*

4.2 Security Considerations for Stored Procedures

Up to release 6.20, JCL jobs were executed by logging on via FTP to the z/OS system as the SAP user that has scheduled the DBA action. For this reason, you had to have a TSO user that has the same name as the SAP user and needed to maintain your password in the JES Interface (*transaction DB2J*, button *Password*).

Stored Procedures are executed by different users depending on your application server setup:

1. For an SAP SCS instance on z/OS, it is the user who started the SAP system. Normally this is the `<sapsid>adm` user.
2. For application servers connecting via DB2 Connect, it is the user connecting to DB2. Normally, this is the DB Connect user. For more information, see Setting Up DB2 Connect User ID and Password SAP Library.

   In order to ensure a successful execution of the Stored Procedures, the executing user needs an OMVS segment.

Security Implications

Regarding point 1:

This poses no security threat because `<sapsid>adm` user already has an OMVS segment.

The main advantage is that you no longer need to maintain your TSO password in JES Interface (transaction DB2J, button *Password*).

Regarding point 2:

DB Connect user should have a password that does not expire (see Setting Up DB2 Connect User ID and Password SAP Library). Some companies' security policies may prohibit giving this user an OMVS segment. Therefore, the security model is maintainable in the JES Interface (transaction DB2J, button *Profile Parameters*):

- If you choose *DB2 Connect User*, the DB2 Connect User needs an OMVS segment. This is the most comfortable solution, because you do not need to maintain your TSO password in JES Interface (transaction DB2J, button *Password*) anymore. It is standard to secure SAP by placing database and application servers behind a firewall. If you adhere to this standard, the impact on security is limited.
- If you choose *Administrator*, then the old behavior is emulated, by performing a multiconnect to DB2 under the authority of the administrator. Each administrator has to have an SAP user with the same name as his TSO ID and has to maintain his own password. The DBA actions will be executed under the administrator's TSO user that has scheduled it.
- If you choose *User*, then you have to specify a user in the related input field that needs an OMVS segment and DB2 SYSCTRL authority. All DBA actions are executed under this user by performing a multiconnect to DB2 under this user's authority. The advantage is that only this user's password has to be maintained, and not all SAP administrators need an identically named TSO user to execute DBA actions.

Regarding Security Models with *DB2 Connect User* and *User*:

Security Models 1 and 3 are protected from uncontrolled JCL job execution by the SAP security system. In order to execute the relevant administrative transactions, you need operator profile `S_A.ADMIN` or `S_DB_DBADM`. Security Model 3 is the recommended option, because SAP support will be able to help you when logged on to your system without needing an identically named TSO user, which is often not possible due to company policies.

4.3 Installing Control Center Procedures Using WLM

This is a truncated version of the section “Installing Control Center Procedures Using WLM” in the *SAP DBA Guide for DB2*.

For more information, see the SAP Database Administration Guide for DB2 at

`service.sap.com/instguidesNW04` → *Operations* → *SAP Database Administration Guide for DB2.*

Stored Procedures for Submitting JCL and USS Commands

The stored procedures for submitting JCL and USS commands must be program-controlled because they use the `__login()` function for switching user identity. There are two ways to do this.

If you have defined `BPX.DAEMON` profile in the facility class in your environment (which is recommended), you either need to define programs from traditional libraries to program control or `BPX.DAEMON.HFSCTL` profile in the facility class.

We do not recommend you defining the `BPX.DAEMON.HFSCTL` profile in the facility class, because then programs that are loaded from MVS libraries are not checked for program control. This is because any MVS data set is considered to be secure and can execute nearly anything.

In our opinion, this poses a severe security risk. Therefore we describe the first option here, which is more work, but far more safe.

Procedure

To define programs from traditional libraries to program control, you need to:

1. Activate the RACF program control (both access control to load modules and program access to data sets).

   SETROPTS WHEN (PROGRAM)

2. The following members of SDSNLOAD need to be program-controlled:

   DSNX9WLM

   DSNX9SPA

   DSNARRS

   DSN3ID00

   DSNX9WLS

   DSNACCJS

   DSNACCJP

   DSNACCJQ

   DSNACCJF

   DSNACCUC

   DSNACCSS

   DSNACCSI

   DSNUTILS

   This can be done by defining discrete RACF PROGRAM class profiles as follows:

   RDEFINE PROGRAM member name ADDMEM ('datasetname'//NOPADCHK)

   UACC (READE)

   RDEFINE PROGRAM DSNX9WLM ADDMEM ('SGF1.SDSNLOAD'//NOPADCHK)

   UACC (READ)

3. Refresh the in-storage copy of the PROGRAM profile:

   SETROPTS WHEN(PROGRAM) REFRESH

   For more information on BPX.DAEMON and setting up program control, you can refer to the IBM documentation *z/OS UNIX System Services Planning*, GA22-7800-03.

Security Considerations for the Stored Procedures DSNACCJP and DSNACCJQ

The stored procedures DSNACCJP and DSNACCJQ use the Extended MCSconsole to issue JES commands to the console. These two stored procedures use the TSO/E user ID in the same way as an authorized TSO/E user can during a console session. The TSO/E user ID must be the same as your SAP user, and you have to maintain your password in transaction DB2J.

This means that the security administrator has to define a RACF user profile to control the console attributes of the EMCS console for the administrators TSO/E respective SAP user ID.

ADDUSER USER001 OPERPARM(AUTH(SYS))

This example defines the user ID USER001 as an EMCS console with console attributes defined by the OPERPARM keyword. Note that the example includes only the information about console attributes for USER001.

For complete information on the RACF ADDUSER command, refer to the IBM documentation *z/OS Security Server RACF Command Language Reference*, SA22-7687-03.

Procedure

Ensure that the user of DSNACCJP and JQ has READ access to a profile in the RACF OPERCMDS class named MVS.MCSOPER.console-name:

1. Issue the SETROPTS command to activate the OPERCMDS class:

   SETROPTS CLASSACT(OPERCMDS)

2. Issue the SETROPTS command to activate generic profiles for the class:

   SETROPTS GENERIC(OPERCMDS)

3. Issue RDEFINE to establish a profile for MVS.MCSOPER.*:

   RDEFINE OPERCMDS MVS.MCSOPER.* UACC(NONE)

4. Give the TSO/E user ID access to the class:

   PERMIT MVS.MCSOPER.* CLASS(OPERCMDS) ID(USER001) ACCESS(READ)

5. Issue the SETROPTS RACLIST command to refresh the OPERCMDS reserve class:

   SETROPTS RACLIST(OPERCMDS) REFRESH

The stored procedures DSNACCJP and DSNACCJQ issue the JES commands to cancel, purge or display a job. You will probably want to protect these JES commands:

1. Define the resource profile:

   ```
   RDEFINE OPERCMDS jesname.CANCEL.* UACC(NONE)
   RDEFINE OPERCMDS jesname.STOP.* UACC(NONE)
   RDEFINE OPERCMDS jesname.DISPLAY.* UACC(NONE)
   ```

2. Give UPDATE access to users:

   ```
   PERMIT jesname.CANCEL.* ID(USER001) ACCESS(UPDATE)
   PERMIT jesname.STOP.* ID(USER001) ACCESS(UPDATE)
   PERMIT jesname.DISPLAY.* ID(USER001) ACCESS(READ)
   SETROPTS RACLIST(OPERCMDS) REFRESH
   ```

Last but not least, to make sure that the related messages are always received by the EMCS console, provide the following command for the user employing DSNACCJQ and JP:

```
ALTUSER USER001 OPERPARM(ROUTCODE(ALL) AUTH(INFO))
```

For more information on RACF commands, refer to *z/OS Security Server RACF Command Language Reference*, SA22-7687-03.

For more information on the EMCS console, refer to *z/OS MVS Planning: Operations*, SA22-7601-03.

Security Considerations When Creating Stored Procedures

Procedure

1. Adapt a copy of members DSNTIJSG and DSNTIJCC of the SDSNSAMP data set according to the instructions in the headers. Ensure that the value of parameter WLM_ENVIRONMENT for each stored procedure matches the correct WLM application environment.
2. You have to grant SELECT and DELETE privileges on two RTS tables named SYSIBM, TABLESPACESTATS and SYSIBM.INDEXSPACESTATS to user <SCHEMA>. For example, if your SAP system is installed with schema SAPR3, the following SQL statements have to be added in member DSNTIJCC:

   ```
   GRANT SELECT, DELETE ON SYSIBM.TABLESPACESTATS TO SAPR3;
   GRANT SELECT, DELETE ON SYSIBM.INDEXSPACESTATS TO SAPR3;
   ```

3. You have to GRANT ALL privileges to PUBLIC on the global TEMP tables that are used by the Stored Procedures. This is not a security issue, because global TEMP tables are instantiated in the session, so their content is only visible from within the same session. Add the following SQL statements to member DSNTIJCC:

   ```
   GRANT ALL ON TABLE DSNACC.BP TBL to PUBLIC;
   GRANT ALL ON TABLE DSNACC.CMDMSG TBL to PUBLIC;
   GRANT ALL ON TABLE DSNACC.DBSTATUS TBL to PUBLIC;
   GRANT ALL ON TABLE DSNACC.DSLIST to PUBLIC;
   GRANT ALL ON TABLE DSNACC.DSNRECORDS to PUBLIC;
   ```

```
GRANT ALL ON TABLE DSNACC.IXTEMP TBL to PUBLIC;
GRANT ALL ON TABLE DSNACC.JFRECORDS to PUBLIC;
GRANT ALL ON TABLE DSNACC.JSRECORDS to PUBLIC;
GRANT ALL ON TABLE DSNACC.MO_SYSPRINT to PUBLIC;
GRANT ALL ON TABLE DSNACC.MO_TBL to PUBLIC;
GRANT ALL ON TABLE DSNACC.MO_TBL2 to PUBLIC;
GRANT ALL ON TABLE DSNACC.ST_TBL_IN to PUBLIC;
GRANT ALL ON TABLE DSNACC.ST_TBL_OUT to PUBLIC;
GRANT ALL ON TABLE DSNACC.THREAD_TBL to PUBLIC;
GRANT ALL ON TABLE DSNACC.TSTEMP_TBL to PUBLIC;
GRANT ALL ON TABLE DSNACC.UCRECORDS to PUBLIC;
GRANT ALL ON TABLE DSNACC.UTILITY_TBL to PUBLIC;
```

4. Run `DSNTIJSG` and `DSNTIJCC` on your DB2 subsystem

Many of the stored procedures require a TEMP database including tablespace. The SAP system creates the TEMP database automatically. It will not be dropped and is reused.

DSNACCMO is used by the SAP installation tool, so you must install it.

If the installation of the stored procedures were not successful, you will be notified by corresponding messages in the system log (Transaction SM21) due to unsuccessful stored procedure executions within transactions DB13, ST04, DB2 and DB2J.

Stored Procedures and Secondary Authorization IDs

Stored procedures do not recognize secondary authorization IDs by default. SAP always uses a secondary authorization ID because it issues `SET CURRENT SQLID=<SCHEMA>`. You need to activate a certain DB2 exit that is delivered with the example library in order to use a secondary authorization ID with Stored Procedures.

Procedure

1. Adapt a copy of member DSN3SATH of the SDSNSAMP data set by uncommenting the code marked with PQ51163 and PQ57756.
2. Run member DSNTIJEX of the SDSNSAMP dataset on your DB2 subsystem.

Recommendations

The following are errors which may occur and their solutions.

1. **Problem**

   You get the following RACF messages in z/OS system log:

   ```
   ICH420I PROGRAM ... FROM LIBRARY ... CAUSED THE
   ENVIRONMENT TO BECOME UNCONTROLLED.
   BPXP014I ENVIRONMENT MUST BE CONTROLLED FOR DAEMON (BPX.DAEMON)
   PROCESSING.
   ```

   Two Possible Causes and Solutions

   a. You did not define a separate WLM environment for the stored procedures DSNACCJS, JQ, JF, JP, and DSNACCUC

      To solve this problem, define a separate WLM environment as described above, and redefine the stored procedures with the correct specification of the new WLM environment as `WLM_ENVIRONMENT`.

   b. You missed one of the members of SDSNLOAD that need to be program-controlled.

      To solve this problem, have your system programmer execute the following RACF commands:

      ```
      RDEFINE PROGRAM member  ADDMEM('library'//NOPADCHK)
      UACC(READ)
      SETROPTS WHEN(PROGRAM) REFRESH
      ```

      "member" and "library" can be taken directly out of the RACF message.

2. **Problem**

   You find the following message in SAP system log (transaction SM21):

   ```
   Error executing stored procedure DSNACCJ? - MES_TXT: EMCS
   activation failed. Macro MCSOPER: RC=04,RSN=00
   ```

   where ? can be Q or P.

   Possible Causes and Solution

   a. As already descibed above, DSNACCJQ and JP use EMCS console. SDSF uses the same console, and if the user submitting the JCL job is at the same time in SDSF, DSNACCJQ and JP cannot execute.

      To solve this problem, leave SDSF while submitting JCL jobs from SAP.

   b. Another possible source for this error could be that your system programmer did not execute the following RACF command for the user ID submitting JCL jobs from SAP:

      ```
      ALTUSER userID OPERPARM(ROUTCODE(ALL) AUTH(INFO))
      ```

Security Considerations for Stored Procedure SAPCL

Starting with SAP NetWeaver 2004s, the stored procedure SAPCL is used to gather DB2 IFI performance data and provide it to the SAP system. In previous releases, `rfcoscol` provided this function.

SAPCL is accompanied by an alert router that is controlled by the stored procedure. SAPCL can also be used to monitor remote DB2 subsystems. For more information, see *SAP DBA Guide for DB2.*

This section describes the privileges that are necessary to install and run SAPCL.

SAPCL Installation

To install the stored procedure SAPCL, the files `sapdb2cl` and `DBRM.db2cldb` are used:

- `sapdb2cl` is the executable of the stored procedure
- `DBRM.db2cldb` is its database request module

The files reside in the USS directory on the host that is specified on the configuration panel of SAPCL. You can reach this panel in SAP transaction ST04 under *Checks/Settings -> SAP Collector Settings*. On the configuration panel, you can install and configure SAPCL. The user ID that is specified in transaction DB2J under *Profile Parameters* is used to perform the installation and configuration steps (for more information about installation and configuration options, see Security Considerations for Stored Procedures [Page 10].)

Permissions, Privileges and Authorizations

User ID Used to Install SAPCL

The user ID that is used to install SAPCL needs the following permission bits for the files `sapdb2cl` and `DBRM.db2cldb` in UNIX System Services:

- EXECUTE and READ permission for file `sapdb2cl`
- READ permission for file `DBRM.db2cldb`

DB Connect User ID

The DB Connect user ID requires the MONITOR1 and MONITOR2 privilege to collect trace data. The TRACE privilege to start the monitor trace needs to be granted to this user ID as well.

SAPCL Schema

The stored procedure SAPCL runs in the WLM application environment that is specified on the configuration panel of SAPCL. It must not be program-controlled.

The schema of the stored procedure, which is the schema of the SAP system in the local case, needs to be authorized to create the stored procedure in this WLM application environment. If it is generally prevented to create stored procedures in this WLM environment, the RACF group of the schema needs to be explicitly authorized.

The following example shows the RACF command that authorizes the RACF group of schema `SAPR3` to create stored procedures in the WLM application environment `D8T0CCA`:

```
PERMIT D8T0.WLMENV.D8T0CCA CLASS(DSNR) ID(SAPR3) ACCESS(READ)
```

User ID in DB2J

Moreover, to bind the packages of SAPCL, it is necessary that the user ID that is specified in transaction DB2J has BINDADD system privilege in DB2.

Link-Edit Step

To authorize the stored procedure SAPCL to be included in the DB2 load library that is used in the link-edit step, issue an **RALTER_RACF** command for SAPCL. In the following example, the load library `D8T0.V810.SDSNLOAD` is used.

```
RALTER PROGRAM SAPCL
ADDMEM('D8T0.V810.SDSNLOAD'//NOPADCHK) +
UACC(READ)
```

After link-editing new versions of SAPCL, it is necessary to refresh its WLM application environment. If you would like to perform this by pressing the button WLM refresh on the configuration panel, you need to permit access to the `WLM_REFRESH RACF` resource profile for the specified application environment.

For example, the `RACF RDEFINE` command for DB2 subsystem D8T0, WLM application environment D8T0CCA and the RACF group of schema `SAPR3` is as follows:

```
RDEFINE DSNR (D8T0.WLM_REFRESH.D8T0CCA)
PERMIT D8T0.WLM_REFRESH.D8T0CCA CLASS(DSNR) ID(SAPR3)
ACCESS(READ)
```

Additionally, in DB2 you need to grant EXECUTE authority on the WLM_REFRESH stored procedure to the authorization IDs or groups that refresh the application environment.

```
GRANT EXECUTE ON PROCEDURE SYSPROC.WLM_REFRESH TO SAPR3
```

Alternatively, you can issue the following z/OS command to refresh the application environment:

```
/V WLM,APPLENV=D8T0CCA,REFRESH
```

Granting Usage Privilege for SAPCL

To provide the DB2 Connect user ID the usage privileges for the stored procedure SAPCL, press the corresponding button on the configuration panel or invoke the operating system command `db2radm`:

```
 db2radm -m db2i -G only –S <SSID> -Q <SCHEMA> -O
<COLLECTION_FOR_SAPCL> -U <PLAN_FOR_SAPCL> -u <ADMIN_USER> -p
<ADMIN_PASSWORD>
```

Definitions of Variables

- <SSID> denotes the alias of the DB2 subsystem in DB2 Connect.
- <SCHEMA> stands for the schema/creator of SAPCL.
- <ADMIN_USER> is the user that grants the usage privilege of SAPCL. It is the owner of SAPCL or a user with SYSADM privileges.

See Also

For more details on RACF protection of stored procedures, see the IBM documentation *DB2 for z/OS Adminitration Guide* and *z/OS Security Server RACF Command Language Reference.*

4.4 Grant Template

If you need to grant jobs, (for example, to change the plan name) adapt the following job template to suit your needs.

```
//DBGRANT  EXEC PGM=IKJEFT01
//STEPLIB DD DISP=SHR,DSN=<DB2_SDSNLOAD>
//SYSPRINT DD  SYSOUT=*
//SYSTSPRT DD  SYSOUT=*
//SYSIN    DD  *
//*DRDA only
GRANT EXECUTE ON PACKAGE "<COLLID>".* TO <CONNECTOR>;
//*End DRDA only
//*z/OS only
 GRANT EXECUTE ON PLAN <PLANNAME> TO <SIDADM>;
  GRANT TRACE,MONITOR1,MONITOR2 TO <SIDADM>;
  GRANT EXECUTE ON PACKAGE <PACKNAM6>.* TO <SCHEMA>;
  GRANT EXECUTE ON PACKAGE <PACKNAM8>.* TO <SCHEMA>;
//*End z/OS only
 GRANT EXECUTE ON PACKAGE DSNUTILS.* TO <SCHEMA>;
  GRANT EXECUTE ON PACKAGE DSNACC.* TO <SCHEMA>;
  GRANT SYSCTRL TO <SCHEMA>;
  GRANT ALL ON TABLE DSNACC.TSTEMP_TBL TO <SCHEMA>;
  GRANT ALL ON TABLE DSNACC.IXTEMP_TBL TO <SCHEMA>;
  GRANT CREATESG TO <SCHEMA>;
  GRANT CREATEDBA TO <SCHEMA>;
  GRANT DISPLAY TO <SCHEMA>;
  GRANT PACKADM ON COLLECTION <SCHEMA> TO <SCHEMA>;
```

```
GRANT ALTERIN, CREATEIN, DROPIN ON SCHEMA <SCHEMA> TO <SCHEMA>;
GRANT USE OF ALL BUFFERPOOLS TO <SCHEMA>;
GRANT INDEX ON TABLE SYSIBM.SYSTABLES TO <SCHEMA>;
GRANT INDEX ON TABLE SYSIBM.SYSTABLESPACE TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSCOPY TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSCOLAUTH TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSCOLUMNS TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSFOREIGNKEYS TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSINDEXES TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSINDEXPART TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSKEYS TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSRELS TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSSYNONYMS TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSTABAUTH TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSTABLEPART TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSTABLES TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSTABLESPACE TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSFIELDS TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSDATABASE TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSDBAUTH TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.MODESELECT TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.LUMODES TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.LULIST TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.USERNAMES TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.LUNAMES TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.LOCATIONS TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.IPNAMES TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSRESAUTH TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSSTOGROUP TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSVOLUMES TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSPKSYSTEM TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSPLSYSTEM TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSPACKAUTH TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSPACKDEP TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSPACKSTMT TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSPACKAGE TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSPACKLIST TO <SCHEMA>;
GRANT SELECT ON TABLE SYSIBM.SYSDBRM TO <SCHEMA>;
```

```
  GRANT SELECT ON TABLE SYSIBM.SYSPLAN TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSPLANAUTH TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSPLANDEP TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSSTMT TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSCOLDIST TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSCOLDISTSTATS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSCOLSTATS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSINDEXSTATS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSTABSTATS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSLOBSTATS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSDUMMY1 TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSCHECKDEP TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSCHECKS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSSTRINGS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSUSERAUTH TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSVIEWDEP TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSVIEWS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSVLTREE TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSVTREE TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSCONSTDEP TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSAUXRELS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSDATATYPES TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSROUTINES TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSPARMS TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSROUTINEAUTH TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSSCHEMAAUTH TO <SCHEMA>;
  GRANT SELECT ON TABLE SYSIBM.SYSTRIGGERS TO <SCHEMA>;
  GRANT UPDATE ON TABLE SYSIBM.SYSTABLES TO <SCHEMA>;
  GRANT UPDATE ON TABLE SYSIBM.SYSTABLESPACE TO <SCHEMA>;
  GRANT UPDATE ON TABLE SYSIBM.SYSTABSTATS TO <SCHEMA>;
  GRANT UPDATE ON TABLE SYSIBM.SYSINDEXES TO <SCHEMA>;
  GRANT UPDATE ON TABLE SYSIBM.SYSCOLUMNS TO <SCHEMA>;
  GRANT DELETE ON TABLE SYSIBM.SYSCOLDIST TO <SCHEMA>;
  GRANT ALL ON TABLE SYSIBM.SYSPRINT TO <SCHEMA>;
  GRANT SELECT, DELETE ON TABLE SYSIBM.TABLESPACESTATS TO <SCHEMA>;
  GRANT SELECT, DELETE ON TABLE SYSIBM.INDEXSPACESTATS TO <SCHEMA>;
/*
//SYSTSIN  DD  *
```

```
 DSN SYSTEM(<SUBSYSTEM_NAME> )
   RUN  PROGRAM(DSNTIAD) PLAN(<DB2_DSNTIAD_PLAN>) -
        LIB('<DB2_RUNLIB_LOAD>')
 END
/*
```

5 Security Settings for DB2 Connect

5.1 Changing the DB Connect User ID and Password After the Installation

DDF checks the user authorization at connect time using an RACF user ID (the DB Connect user ID).

<SCHEMA> defines the schema of the DB2 objects of the SAP system as specified by the environment variable `dbs_db2_schema`.

On the client side, the DB Connect user is specified by the following:

environment variable: `dbs_db2_user`

profile parameter: `dbs/db2/user`

You can change the `dbs_db2_user` by calling the command:

```
dbdb2pwd -create <connect_user_password>
```

as <sapsid>adm to create the encrypted password file **dbdb2pwd** in the respective global directory:

UNIX: **`/<sapmnt>/<SAPSID>/global`**

Windows: **`\\<SAPGLOBALHOST>\sapmnt\<SID>\global`**

Since the global directory is shared by all application servers of an SAP system, the password file is as well. Therefore, you only need to control the password file on **one** instance.

We strongly recommend that you create a DB Connect user in RACF without TSO segment and set the password without an expiration date. If the password expires, new processes cannot connect to the database, and the reconnect mechanism for all processes will no longer function until the password file is recreated with the new valid password.

We recommend that every SAP system uses a DB Connect user of its own. This ensures that if the password is supplied incorrectly for one system and the user is revoked by RACF, the effect does not propagate to other SAP systems which are running with the same DB Connect user.

5.2 DB2 Connect Configuration Using db2radm

This is a truncated version of the section “DB2 Connect Configuration Using db2radm” in the *SAP DBA Guide for DB2*.

For more information, see the *SAP DBA Guide for DB2* at

service.sap.com/instguidesNW04 → *Operations* → *SAP Database Administration Guide for DB2.*

The following command sets all necessary grants for the SAP system. The grantor is <user>. The grantee is specified by the environment variable dbs_db2_schema.

db2radm –m db2i –G only –u <user> -p <userpwd>

For a remote system (multiconnect), you can use the following:

db2radm –m db2i –G only –u <user> -p <userpwd> -s <ssid> -q <schema>

Here it is assumed that the remote database is cataloged with the alias <ssid>. The grantee (the schema of the remote system) is <schema>.

6 Additional Information on DB2 UDB for z/OS

For more information about DB2 UDB for z/OS, see:

- *SAP DBA Guide for DB2*
- *SAP Planning Guide for z/OS*

which you can find in the SAP Service Marketplace at **service.sap.com/instguidesNW04** → *Operations* → *SAP Web AS.*

For more information on the SAP Web AS installation on DB2 UDB for z/OS, see **service.sap.com/instguidesNW04** → *Installation.*