PUBLIC

Role-Based Security Concept for Database Users on IBM DB2 for Linux, UNIX, and Windows

Introduction

TABLE OF CONTENTS

SAP introduced a role-based security concept for database users on IBM Db2 for Linux, UNIX, and Windows 9.7 in SAP NetWeaver 7.0 or higher environments.

The role-based security concept for database users offers a solution for the following business scenarios:

- In an SAP system, you have default administrator users. With the role-based security concept, it is easier to create additional, individual administration users for all persons involved in monitoring and administration. As a result, it is possible to track the changes or activities of the individual administrators for security audits.
- The role-based concept provides different roles for monitoring or administration. These roles can be used to restrict the user privileges according to the organizational tasks. No individual person should have more privileges than required.
- In SAP Solution Manager, remote database connections are used to manage the databases in the landscape. The role-based security concept can add an additional security layer to protect business data.

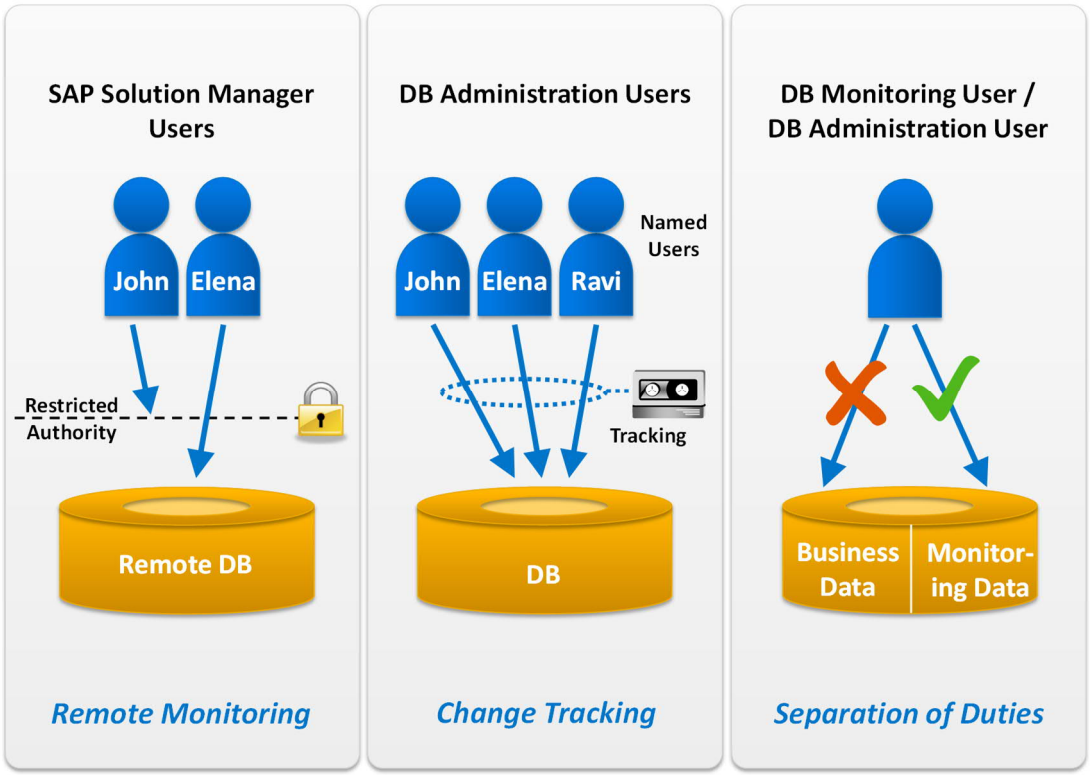
INTRODUCTION

During installation, the SAP installation tool creates users for connections, database administration, and SAP system administration. These users are initially created with maximum privileges. With security mechanisms from SAP, you can fine-tune the privileges of database administrators more easily. This is true for native database access as well as for a remote database access using SAP Solution Manager.
SAP Solution Manager is the recommended SAP tool to monitor the databases in your system landscape. In SAP Solution Manager, remote database connections are used to manage the databases. In the past, it was a complex task to create and organize database access and authorizations of database administrators carefully so that sensitive customer data is well protected. As of SAP Solution Manager 7.1 SP3 and SAP NetWeaver 7.0, this task has become easier with the following security mechanisms:

- The SAPTOOLS and SAPMON roles to restrict user privileges on the database according to organizational tasks
- The separation of duties to ensure that database administrators cannot read business data using a remote database connection
- The S_DBCON authorization object to restrict access to remote databases from the SAP Solution Manager system

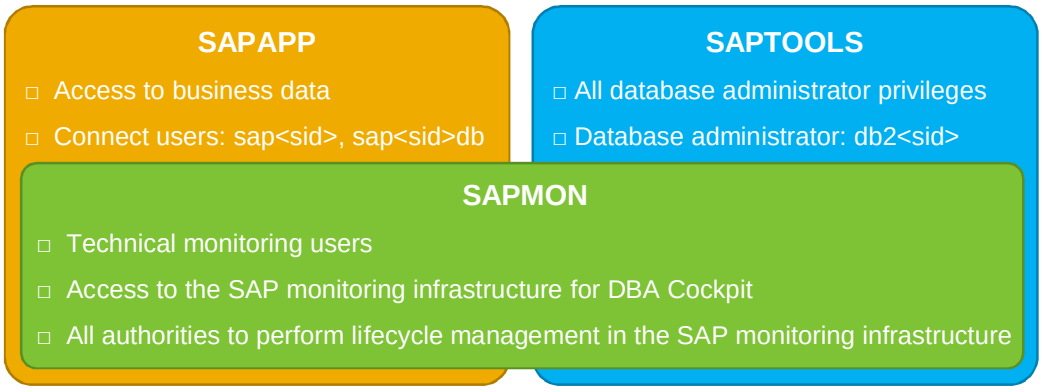
This is particularly relevant for the following use cases:

- **Restriction of user privileges**
  You identify database administration duties and provide each individual with their own user ID with an authority as minimal as possible to complete his or her daily task. You can reuse and adapt the default roles shipped by SAP to perform this task.
- **Change tracking**
  If you create individual users for all database administrators, this allows you to track the changes performed by database administrators on individual user account level.
- **Separation of duties**
  Optionally, you can decide to revoke the DATA ACCESS privilege from database monitoring and administrator users. This provides an additional security layer for your business data if needed.
- **Access protection to remote monitoring**
  With the S_DBCON authorization object, the user authorities on SAP Solution Manager for remote monitoring are restricted. Only database administrators with the authorizations of the S_DBCON authorization object are able to access remote databases. Access permissions can be granted for each user/database combination separately.



After an introduction of the database roles, the use cases are described below in more detail.

Database Roles for SAP Environments
No users should have more access privileges than what is needed to complete their daily task. To secure sensitive data and the system in general from potential damage, it is essential to identify database administration duties and to provide each individual with his or her own user ID and with an authority as minimal as possible to complete his or her daily task. It is also necessary to have a comprehensive hierarchy of users and separate duties among database/system administrators and security managers.
To support a clear-cut assignment of administration privileges, SAP has introduced a role-based security concept with user roles on the database layer. The privileges for the roles are pre-defined by SAP and can be used to restrict the privileges of database administrators.
SAP introduces three database roles: SAPAPP, SAPMON, and SAPTOOLS. The SAPAPP role is the role for business applications. By default, it is assigned to all connect users, including connect users of business applications. The role SAPMON is designed for monitoring. It has all privileges for the monitoring interfaces provided by IBM DB2 for LUW. In addition, users with this role hold all privileges to set up and maintain the monitoring infrastructure provided by SAP, especially the DBA Cockpit. For database administrators, the role SAPTOOLS has been introduced. It has the most powerful authorities to perform all administrative tasks.



The role SAPMON is included in the SAPAPP and SAPTOOLS roles. Since SAP ships DBA Cockpit as part of all SAP-NetWeaver-based systems and the applications require monitoring information, the role SAPAPP

includes role SAPMON. SAPMON is also included in the SAPTOOLS role because database administrators also do monitoring.

Note: The <sapsid>adm user is not assigned to any of the database roles discussed here. The <sapsid>adm user still belongs to the database group SYSCTRL, so administrators with this user can start and stop the database server.

Use Cases: Restriction of User Privileges and Change Tracking

During installation, the SAP installation tools create default users for connections, database administration, and SAP system administration. These operating system users are created with maximum privileges. By default, only two users are created for administration.

During installation, dedicated user GRANTs need to be performed. As a result, it is very challenging to create additional, individual, operating system user accounts for database administrators. This has very often resulted in one administration user being used by multiple persons. Such a situation increases the risk that some administrators have privileges that are above their organizational security clearance.

Sharing one administration user among several persons also causes problems during audits: If the same database user ID is used by multiple users, it is impossible to track database activities for security auditing on operating system level.

With the role-based security concept, you can create additional user accounts on your database server. With the roles, it is easier to assign the right authorizations to users for different use cases. For example, you can assign the SAPTOOLS role to your database administrators. Moreover, if you create an individual operating system user for each administrator, all database activities can then be tracked together with the correct user information.

Use Case: Separation of Duties

With the three roles, it has become easier to assign roles to users for different use cases and thus restrict user privileges. However, in some cases it might be necessary to protect business data even further. In the standard, database administrators hold the DATA ACCESS authority; they have read/write access to the data of all tables. The removal of the DATA ACCESS authority from all users is referred to as “separation of duties”.

Even after the removal of the DATA ACCESS authority from all users, connect users with the business application role SAPAPP still have access to business data. This is the case because SAP-NetWeaver-based systems use one single technical connect user to access the database from business applications. Hence this connect user with the SAPAPP role owns all tables with business data and therefore still has access to the data.

With activated separation of duties, the technical database monitoring role (SAPMON) and database administration role (SAPTOOLS) do not include permission to access business data. Users with these roles can only access the monitoring interfaces and performance history tables. Note that the SAPTOOLS role is assigned to db2<sid> user in the “separation of duties” scenario.

To enable separation of duties, you need an additional security administrator account on the database server. After the activation of separation of duties, the security administrator user can be used to grant DATA ACCESS authorities to database users again. Therefore keep the credentials of this user secret. This user account is not created by SAPINST, so you need to create the user manually. The database roles are a prerequisite for the separation of duties. The SAP default setup activates the database roles without separation of duties. For more information about the activation of separation of duties, see the *Activating Separation of Duties (Optional)* section.

If you want to work with separation of duties, you should also consider the following restrictions that apply in this scenario:

If performance tuning and administration users also need the possibility to perform EXPLAIN statements on tables that they cannot access, you need to assign the EXPLAIN authority to them. . Hence, you can perform a separation of duties without removing the EXPLAIN function from the user privileges of administrators.

With the “separation of duties” feature enabled, system administrators can**not** use the “Test Execute” function because they do not have a SELECT privilege for business tables. In addition, it is not possible to verify distribution statistics of all tables used by a problematic SQL statement. To enable these analysis functions, specific GRANTs are required. If you need the help of SAP support, a separation of duties might therefore increase message processing time. When SAP support needs to analyze the performance of SQL statements, they will have to ask you to grant them the required authorities before they can start working on your problem. Therefore, we recommend that you weigh the increased security level of the separation of duties against the lower flexibility and speed in support cases.

The separation of duties provides an additional security layer to restrict access to business data for database administrators. The separation of duties is optional, and you should consider the advantages and

disadvantages of this concept before its activation. For more information, see the *Deciding on the Optimal Authorization Setup for Your System Landscape* section.

Note: A system copy operation using the backup/restore method automatically assigns DATA ACCESS authority to the new instance owner. Therefore, after a system copy, activate the separation of duties again on the copied system.

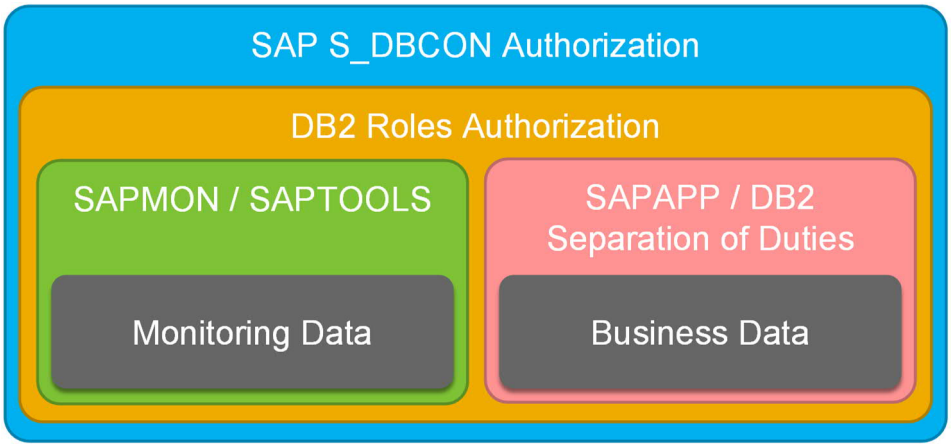
Use Case: Access Protection to Remote Monitoring

For the management of databases in an IT landscape, SAP provides remote monitoring capabilities with DBA Cockpit in SAP Solution Manager. When a system is connected to SAP Solution Manager, the setup of the DBA Cockpit monitoring infrastructure is always part of the setup wizard.

SAP Solution Manager 7.0 has only a very basic SAP authorization concept. It allows you to give a user in the SAP Solution Manager system either the monitoring authorities or the administration authorities for DBA Cockpit. Administration authorities always include monitoring capabilities. This is valid for all connected remote databases.

With SAP Solution Manager 7.1 SP3, a database-connection-specific assignment of SAP roles for DBA Cockpit was introduced (with the S_DBCON authorization object). You can use the SAP authorization object S_DBCON to manage the authorization for each database connection individually for each SAP user. For DBA Cockpit, you can decide for each user/database combination which authorizations you want to assign: for monitoring, for maintenance, or for extended maintenance. If no authorization is available for a database connection, the user is not allowed to connect to that specific database. There is only one remote database connection per monitored database. As a result, the S_DBCON authorization object gives you a high flexibility in user role assignment.

In addition to the S_DBCON authorization by SAP, there is also another layer for protecting remotely managed databases: the DB2 roles authorization.



Note: The S_DBCON authorization object only protects the databases from unauthorized accesses coming directly from the DBA Cockpit. It does not protect the databases from unauthorized accesses using native database connections. If you have users with development authorizations in your SAP Solution Manager system, these users could create their own code using the remote database connections. They still have all the authorizations that the database user has on the remote database.

Note: The S_DBCON authorization object checks must be enabled explicitly by setting the following parameter in the system default profile:

dbs/dba/ccms_security_level = 1

Setup Types

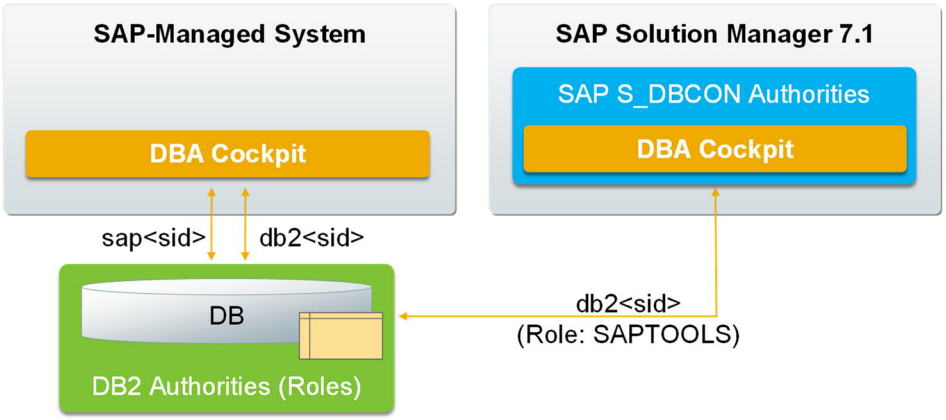
This section describes the setup types in remote monitoring scenarios. The DBA Cockpit uses a remote database connection for monitoring and administration of databases: the +++DB6ADM connection. Even if a database administrator logs on to a system and uses the locally installed DBA Cockpit of the system, this remote database connection is used to access the database.

SAP Default Setup: SAPTOOLS and S_DBCON

In the SAP default setup, database administrators who connect to databases for monitoring and administration get the SAPTOOLS authorizations. In addition, you can use the S_DBCON authorization object to assign the right monitoring or administration authorities for remote monitoring to different users on SAP Solution Manager 7.1.

This setup type is provided out-of-the-box. There is no need to change anything on the remote databases, and the setup of the managed systems is very simple.

This is the SAP default setup because it provides the most flexible solution for the assignment of authorizations to the various database administrators in your organization. With this setup, there are no restrictions for database administrators who want to perform remote database analysis using DBA Cockpit.



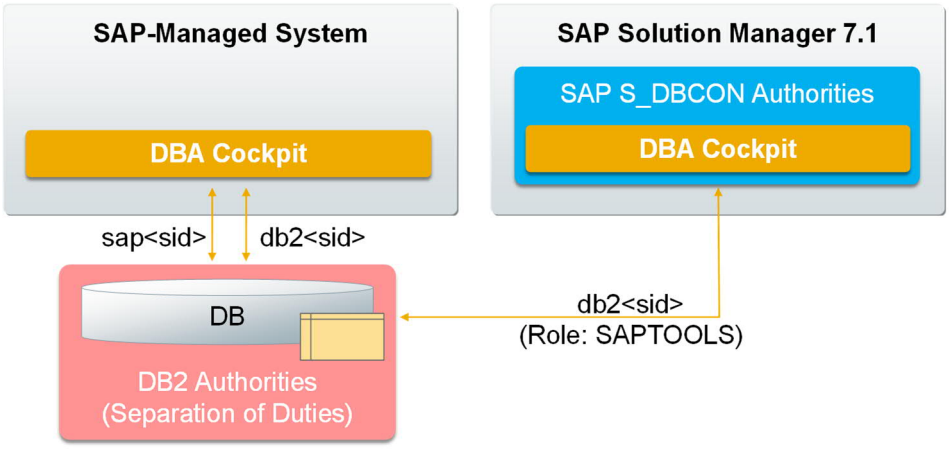
SAPMON and S_DBCON

In this setup, database administrators who connect to remote databases get the SAPMON authorizations. As a result, they can only use the pure monitoring functions in SAP Solution Manager. This applies to all users in the SAP Solution Manager system. In addition, you can restrict the monitoring authorizations even more with S_DBCON for each user. No user can use the administrative functions in DBA Cockpit in the SAP Solution Manager system for remote systems.

Separation of Duties, SAPTOOLS, and S_DBCON

In this setup, database administrators who connect to databases for monitoring and administration get the SAPTOOLS authorizations. This means that they have all authorizations required for both monitoring and administration. In addition, you can use the S_DBCON authorization object to fine-tune the monitoring or administration authorities for remote monitoring for different users in SAP Solution Manager 7.1.

Due to the use of separation of duties, no user in your SAP Solution Manager system can read business data using the remote database connection.



Note: With the “separation of duties” feature enabled, system administrators can**not** use the “Test Execute” function because they do not have a SELECT privilege for business tables. In addition, it is not possible to verify distribution statistics of all tables used by a problematic SQL statement. To enable these analysis functions, specific GRANTs are required. If you need the help of SAP support, a separation of duties might therefore

increase message processing time. When SAP support needs to analyze the performance of SQL statements, they will have to ask you to grant them the required authorities before they can start working on your problem. Therefore, we recommend that you weigh the increased security level of the separation of duties against the lower flexibility and speed in support cases.

Separation of Duties, SAPMON, and S_DBCON

In this setup, database administrators who connect to remote databases get the SAPMON authorizations. As a result, they can only use the pure monitoring functions in SAP Solution Manager. This applies to all users in the SAP Solution Manager system. In addition, you can restrict the monitoring authorizations even further with S_DBCON for each user. No user can use the administrative functions in DBA Cockpit in the SAP Solution Manager system.

Due to the use of separation of duties, no user in your SAP Solution Manager system can read business data using the remote database connection.

Note: With the “separation of duties” feature enabled, system administrators can**not** use the “Test Execute” function because they do not have a SELECT privilege for business tables. In addition, it is not possible to verify distribution statistics of all tables used by a problematic SQL statement. To enable these analysis functions, specific GRANTs are required. If you need the help of SAP support, a separation of duties might therefore increase message processing time. When SAP support needs to analyze the performance of SQL statements, they will have to ask you to grant them the required authorities before they can start working on your problem. Therefore, we recommend that you weigh the increased security level of the separation of duties against the lower flexibility and speed in support cases.

Support for Non-SAP-NetWeaver-Based Systems

For database systems running an application that is not based on SAP NetWeaver, we also support remote monitoring using SAP Solution Manager 7.1: You can use the *db6_update_db* script to create the SAPMON and SAPTOOLS database roles for such database systems. Note that in non-SAP-NetWeaver systems, the SAPAPP role is not created because this role is only needed for SAP NetWeaver connect users.

After you have executed the *db6_update_db* script, all authorizations are automatically granted to the SAPMON and SAPTOOLS roles only. In addition, after the *db6_update_db* script has run, no PUBLIC grants exist on the SAPTOOLS objects anymore.

In SAP-NetWeaver-based systems, users with the business application role SAPAPP still have access to business data because they are connect users with an SAPAPP role for SAP systems who own all database tables. For non-SAP-NetWeaver-based systems, a predefined separation of duties is not available because a separation of duties depends on the architecture of the application. You can manually enable a separation of duties using native DB2 commands, but you must align this with the application running on the database. All SAPTOOLS objects have specific GRANTS on the SAPMON and SAPTOOLS roles to ensure access authorizations in separation of duties scenarios.

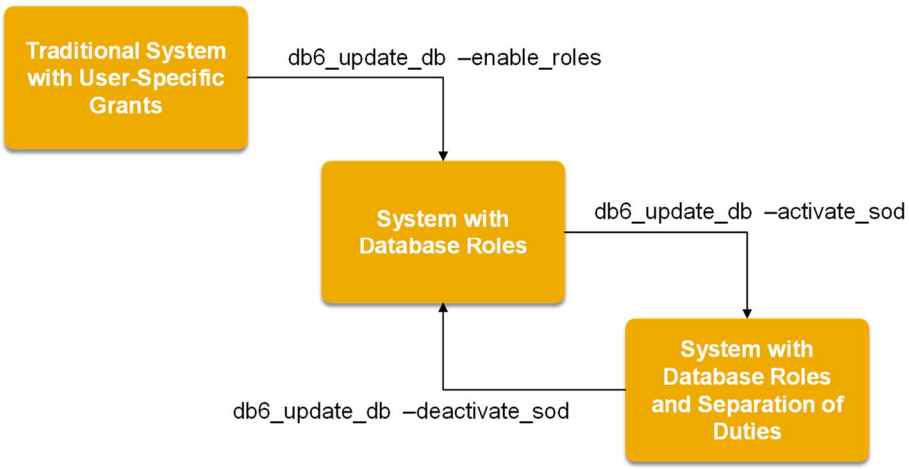
Deciding on the Optimal Authorization Setup for Your System Landscape

The following overview summarizes the pros and cons of the different authorization setups:

	SAPTOOLS, S_DBCON (SAP Default)	SAPMON, S_DBCON	SAPTOOLS, S_DBCON, Separation of Duties	SAPMON, S_DBCON, Separation of Duties
Easy setup of individual roles for all database administrators	+	+	+	+
Change tracking for all database administrators	+	+	+	+
Business users have full access to their data	+	+	+	+
Database administrators have access to monitoring data	+	+	+	+
Database administrators have no access to business data	−	−	+	+
Extended SQL analysis (Test execute, data distribution statistics)	+	+	−	−
No additional DB2 security administrator required	+	+	−	−

ACTIVATING THE ROLE-BASED SECURITY CONCEPT

The SAP role concept is available for SAP systems with at least SAP kernel 7.00 running on IBM DB2 for LUW V9.7 or higher. Depending on the release of your system, the role-based security concept is available after installation or needs to be enabled manually by running the *db6_update_db* script.



Activating the Role-Based Security Concept

Automatic Activation of the Role-Based Security Concept (as of SAP Enhancement Package 3 for SAP NetWeaver 7.0)

All new SAP system installations starting with Enhancement Package 3 for SAP NetWeaver 7.0 work with the role-based security concept. The installation tool SAPINST creates the roles automatically and does not assign any single user authorizations anymore. SAPINST also assigns the SAP default users to their appropriate database roles.

If you have performed an SAP system upgrade, you can also run the *db6_update_db* script to get the same default setup.

Activating the Role-Based Security Concept Manually
SAP provides the *db6_update_db.[sh|bat]* script to change the authorization concept manually for systems lower than SAP NetWeaver 7.0 EHP3 (see SAP Note 1365982). If you execute the db6_update_db script, it does not automatically change the authorization concept. It always enforces the concept for which the database is configured. This means that if you have a traditional system with user-specific authorizations, the *db6_update_db* script does not convert the authorization concept of the system into an authorization concept based on database roles. If you have a system configured for database roles, the *db6_update_db* script ensures that all SAP-specific authorizations are assigned based on database roles.
After a FixPack update or a DB2 version upgrade, the *db6_update_db* script can be used to repair the authorizations. It always enforces the database authorization concept that is currently active.

Procedure
To activate the role-based security concept for an existing database manually, call the *db6_update_db* script as follows:

UNIX:

```
db6_update_db.sh –d <dbsid> -enable_roles
```

Windows:

```
db6_update_db.bat –d <dbsid> -enable_roles
```

Note: The activation of the role-based security concept can be performed while the database is online.

Activating Separation of Duties (Optional)
You can activate the separation of duties as an optional step. The removal of DATA ACCESS authorities is never done by default by SAPINST. This is an explicit step that you must do manually.
To activate the separation of duties, you need to run the *db6_update_db* script. Since separation of duties requires enabled database roles, the *db6_update_db* script always activates the role-based security concept first. If the database roles have already been activated, the script still executes the commands for enabling the roles, but it does not produce any additional SQL GRANT statements. The script then contains only comments and some CONNECT statements.

Prerequisites
If you want to activate the separation of duties, you need a new user that will become SECADM during the activation. The user with SECADM role is required to remove the DATA ACCESS authorities.
The new user has to have an appropriate db2 environment set. To check the environment settings for the new user used for SECADM, logon as that user and connect to the database with user db2<sid>. If this works well, the settings are correct.

Procedure
To activate the separation of duties, call the *db6_update_db* script as follows:

Unix:

```
db6_update_db.sh –d <dbsid> -activate_sod <new_secadmusername>
```

Windows:

```
db6_update_db.bat –d <dbsid> -activate_sod <new_secadmusername>
```

Note: The activation of separation of duties can be performed while the database is online.

Deactivating the Separation of Duties
You can deactivate the separation of duties in the system and go back to a pure role-based security concept. Note that a deactivation of the role-based security concept is **not** possible.

Procedure
To deactivate the separation of duties, call the *db6_update_db* script as follows:

Unix:

```
db6_update_db.sh –d <dbsid> -deactivate_sod <new_secadmusername>
```

Windows:

```
db6_update_db.bat –d <dbsid> -deactivate_sod <new_secadmusername>
```

Note: The deactivation of separation of duties can be performed while the database is online.

Validating the Database Roles Authorities and Separation of Duties
In the following scenarios, authorizations are granted to PUBLIC or SECADM, which overrides the role-based security concept. In these cases, you need to run the *db6_update_db* script again to repair authority assignments.

Scenario: Registration of the db2sap Library
After all FixPack updates, run the *db6_update_db* script again. The script registers the db2sap library again. Up to IBM DB2 for LUW V9.7 FP6, this registration internally executes GRANT TO PUBLIC statements. The *db6_update_db* script repairs these PUBLIC grants and ensures your current security option.

Scenario: Creation of New Tablespace in DBA Cockpit
When you use DBA Cockpit to create a new tablespace, DBA Cockpit grants the USE authority of the tablespace to PUBLIC. The following SAP NetWeaver releases check for the role SAPAPP and if it exists, they grant the USE authority of the tablespace to the database role SAPAPP:

- SAP NetWeaver 7.0 Enhancement Package 2 SP 11
- SAP NetWeaver 7.0 Enhancement Package 3 SP 2
- SAP NetWeaver 7.3 SP 7

The *db6_update_db* script repairs these PUBLIC grants and ensures your current security option.

Scenario: System Copy
A system copy using the backup/restore method automatically assigns DATA ACCESS authority to the new instance owner. Therefore, after a system copy, activate the separation of duties again on the copied system using the *db6_update_db* script.

Validation Procedure
To verify whether the authorizations and the separation of duties are correctly set up, you can run the *db6_update_db* script with the *–enable_roles* or *–activate_sod* options. The *db6_update_db* script is implemented in a two-phase fashion. In the first phase, it generates an SQL command file. The second phase executes the SQL commands. You can make use of the script's behavior as follows: If the generated SQL file contains GRANT or REVOKE statements, there were some authorizations that the script has now repaired. If the SQL script contains only comments and some CONNECT statements, the authorizations and the separation of duties are correctly set up.
To verify the correct setup of the database roles, call the *db6_update_db* script as follows:

Unix:

```
db6_update_db.sh –d <dbsid> -enable_roles
```

Windows:

```
db6_update_db.bat –d <dbsid> -enable_roles
```

Note: The verification of the role-based security concept can be performed while the database is online.

To verify the separation of duties, call the *db6_update_db* script as follows:

Unix:

```
db6_update_db.sh –d <dbsid> -activate_sod <new_secadmusername>
```

Windows:

```
db6_update_db.bat –d <dbsid> -activate_sod <new_secadmusername>
```

Note: The verification of separation of duties can be performed while the database is online.

CREATING DATABASE USERS FOR SAP ROLES
This chapter describes the procedures for creating dedicated monitoring or administration users on the database server.

Creating an Administration User

1. Create an operating system user as a member of the DB2 for LUW SYSADM group.

   Note: The SAP default for the DB2 for LUW SYSADM group name is DB<DBSID>ADM.

2. Assign the SAPTOOLS database role to this user by executing the following DB2 command:

   ```
   GRANT ROLE SAPTOOLS TO USER <new_admin>
   ```

Creating a Monitoring User

1. Create an operating system user as a member of the DB2 for LUW SYSMON group.

   Note: The SAP default for the DB2 for LUW SYSMON group name is DB<DBSID>MON.

2. Assign the SAPMON database role to this user by executing the following DB2 command:

   ```
   GRANT ROLE SAPMON TO USER <new_admin>
   ```

ROLE AUTHORITIES IN DETAIL
This chapter describes which authorities the *db6_update_db* script automatically assigns to the SAPAPP, SAPMON and SAPTOOLS roles.

Grants to SAPMON Role
This table shows the authorities that are granted to the SAPMON role and revoked from PUBLIC or the possible connect users in the system (if they have these authorities).

Authority Type	Refers to	Authority
Database Authority	Database	CONNECT
Database Authority	Database	SQLADM
Database Authority	Database	EXPLAIN
Database Authority	Database	BINDADD
Database Authority	Database	CREATETAB
Database Authority	Database	CREATE_EXTERNAL_ROUTINE
Database Authority	Database	IMPLICIT_SCHEMA
Schema Authority	SAPTOOLS schema	CREATEIN
Schema Authority	SAPTOOLS schema	ALTERIN
Schema Authority	SAPTOOLS schema	DROPIN
Table Authority	Tables in SAPTOOLS	ALL PRIVILEGES
Index Authority	Indexes in SAPTOOLS schema	CONTROL
Routine Authority	Routines in SAPTOOLS schema	EXECUTE
Routine Authority	Routines in SYSPROC (MON%, WLM%, DB_GET%, DB_MEMBERS)	EXECUTE
Tablespace Authority	SAPTOOLS, SAPEVENTMON	Use of tablespace

The tablespace authorities for use of SAPTOOLS and SAPEVENTMON tablespaces are revoked from PUBLIC (if PUBLIC has these authorities).

Grants to SAPTOOLS role
This table shows the authorities that are granted to the SAPTOOLS role and revoked from PUBLIC or the possible connect users in the system (if PUBLIC or the connect users have these authorities).

Authority Type	Refers to	Authority
Database Authority	Database	DBADM
Database Authority	Database	WLMADM
Include role	SAPMON	

Grants to SAPAPP Role
This table shows the authorities that are granted to the SAPAPP role and revoked from PUBLIC or the possible connect users in the system (if PUBLIC or the connect users have these authorities).

Authority Type	Refers to	Authority
Database Authority	Database	LOAD
Tablespace Authority	SAP application tablespaces	Use of tablespace
Schema Authority	Connect user schema	CREATEIN
Include Role	SAPMON	

The tablespace authority for the SAP application tablespaces are revoked from PUBLIC (if PUBLIC has these authorities).

Note: The authorities that are granted to the SAPMON/SAPTOOLS/SAPAPP roles are also removed from the SAP connect users that were found on the respective system. Possible SAP connect users are the users that are table owners (TABOWNER) of a table named J2EE_CONFIG or E070 in the IBM DB2 for LUW system catalog.

Table Grants to SAPMON Role
This table shows the authorities that are granted to the SAPMON role and revoked from PUBLIC or the instance owner or the possible connect users in the system (if they have these authorities).

Table Name	Authority	Virtual Tables: Comment	Note
SVERS	Select	Not empty	System integration
CVERS	Select	Not empty	System integration

DBSTATC	Select	Not empty	Runstats control
TADB6	Select	Not empty	Dataclass maintenance
IADB6	Select	Not empty	Dataclass maintenance
LADB6	Select	Not empty	Dataclass maintenance
TSDB6	Select	Not empty	Dataclass maintenance
DDART	Select	Not empty	Dataclass maintenance
DARTT	Select	Not empty	Dataclass maintenance
DD07T	Select	Not empty	Table analysis
TRESC	Select	Not empty	Table analysis
DBDIFF	Update, Insert, Delete	Not empty	Required for EXPLAIN and DB2 V9.5 event monitor
DD06L	Select	Not empty	Table analysis
DB6TREORG	Select	Empty	Only in 6.40 up to 7.00 SP12
DB6IREORG	Select	Empty	Only in 6.40 up to 7.00 SP12
DD02L	Select	Not empty	Table analysis
DD03L	Select	Not empty	Table analysis
PATCHHIST	Select	Not empty	System history
PAT03	Select	Empty/not empty	System history
AVERS	Select	Not empty	System integration
PAT06	Select	Empty	System history
DB6CSTRACE	Select	Volatile	Cumulative SQL trace
RSDCUBE	Select	Not empty	Directory of InfoCubes / InfoProvider
RSDODSO	Select	Not empty	Directory of all DataStores

Table Grants to SAPTOOLS Role
This table shows the authorities that are granted to the SAPTOOLS role and revoked from PUBLIC or the instance owner or the possible connect users in the system (if the instance owner or the connect users have these authorities).

Table Name	Authority	Virtual Tables: Comment	Notes
DBSTATC	Update, Insert, Delete	Not empty	Runstats control
TADB6	Update, Insert, Delete	Not empty	Data class maintenance
IADB6	Update, Insert, Delete	Not empty	Data class maintenance
TSDB6	Update, Insert, Delete	Not empty	Data class maintenance
DDART	Update, Insert, Delete	Not empty	Data class maintenance
DARTT	Update, Insert, Delete	Not empty	Data class maintenance
DB6TREORG	Update, Insert, Delete	Empty	Only in 6.40 up to 7.00 SP12
DB6IREORG	Update, Insert, Delete	Empty	Only in 6.40 up to 7.00 SP12

Cleanup Activities of the *db6_update_db* Script
The following table authorities on SYSCAT objects may exist due to historical reasons. The *db6_update_db* script revokes them automatically during a cleanup step:

```
REVOKE SELECT ON SYSIBM.SYSTABLES FROM USER <CONNECTUSER>
REVOKE SELECT ON SYSIBM.SYSCOLUMNS FROM USER <CONNECTUSER>
REVOKE SELECT ON SYSIBM.SYSINDEXES FROM USER <CONNECTUSER>
REVOKE SELECT ON SYSIBM.SYSPLAN FROM USER <CONNECTUSER>
REVOKE SELECT ON SYSIBM.SYSVIEWS FROM USER <CONNECTUSER>
REVOKE UPDATE ON SYSIBM.INDEXES FROM USER <CONNECTUSER>
REVOKE UPDATE ON SYSIBM.TABLES FROM USER <CONNECTUSER>
REVOKE UPDATE ON SYSIBM.COLUMNS FROM USER <CONNECTUSER>
```

In addition, the script also revokes the following authorities automatically:

```
REVOKE DBADM FROM <SAPSID>ADM

REVOKE CREATE_NOT_FENCED_ROUTINE FROM USER <CONNECTUSER>
```

Remarks About Revoked Authorities

The CREATE_NOT_FENCED_ROUTINE routine is not required any more for the SAP connect user, since the *db6_update_db* script registers all required procedures stored in IBM DB2 for LUW and all user-defined functions (UDFs) from the db2sap library. The routine is also not required for SQL PL.

The CREATE_EXTERNAL_ROUTINE routine is also not needed any more. However, the *db6_update_db* script does not remove it to retain the possibility to support future scenarios like Java routines.

The role-based security concept only affects SAP-owned database objects such as SAP application tablespaces or tables, indexes or procedures in SAP-owned schemas. It does not apply to any default DB2 database objects delivered by IBM.

APPENDIX

Sample Output of Generated SQL Script in “Enable Roles” Scenario

```
-- generated on Wed Nov 16 13:54:43 CET 2011
-- ****************************************************************************
--
-- This file was generated by db6_update_db.sh version 0023
-- by calling ./db6_update_db.sh -d D3D -enable_roles at Wed Nov 16 13:57:43 CET 2011
-- ****************************************************************************
--
-- This script introduces a role based security concept for the SAP system
-- environment. It creates the roles SAPTOOLS and SAPMON if they are not
-- already present and grants appropriate rights to these roles
--
--****************************************************************************
-- Connect to D3D
connect to D3D;
-- Create role SAPMON
CREATE ROLE SAPMON;
-- Create role SAPAPP
CREATE ROLE SAPAPP;
-- Create role SAPTOOLS
CREATE ROLE SAPTOOLS;
-- Assign connect users to role SAPAPP
GRANT ROLE SAPAPP TO USER SAPD3D;
-- Assign role SAPMON to role SAPAPP
GRANT ROLE SAPMON TO ROLE SAPAPP;
-- Assign role SAPMON to role SAPTOOLS
GRANT ROLE SAPMON TO ROLE SAPTOOLS;
-- Grant CONNECT to role SAPMON
GRANT CONNECT ON DATABASE TO ROLE SAPMON;
-- Grant SQLADM to role SAPMON
GRANT SQLADM ON DATABASE TO ROLE SAPMON;
-- Grant EXPLAIN to role SAPMON
GRANT EXPLAIN ON DATABASE TO ROLE SAPMON;
-- Grant BINDADD to role SAPMON
GRANT BINDADD ON DATABASE TO ROLE SAPMON;
-- Grant CREATETAB to role SAPMON
GRANT CREATETAB ON DATABASE TO ROLE SAPMON;
-- Grant IMPLICIT_SCHEMA to role SAPMON
GRANT IMPLICIT_SCHEMA ON DATABASE TO ROLE SAPMON;
-- Grant CREATE_EXTERNAL_ROUTINE to role SAPMON
GRANT CREATE_EXTERNAL_ROUTINE ON DATABASE TO ROLE SAPMON;
-- Revoke CREATE_NOT_FENCED_ROUTINE from possible Connectusers
REVOKE CREATE_NOT_FENCED_ROUTINE ON DATABASE FROM USER SAPD3D;
-- Revoke CREATE_NOT_FENCED_ROUTINE from PUBLIC
-- Revoke CONNECT from possible Connectusers
REVOKE CONNECT ON DATABASE FROM USER SAPD3D;
-- Revoke SQLADM from possible Connectusers
-- Revoke EXPLAIN from possible Connectusers
-- Revoke BINDADD from possible Connectusers
REVOKE BINDADD ON DATABASE FROM USER SAPD3D;
-- Revoke CREATETAB from possible Connectusers
REVOKE CREATETAB ON DATABASE FROM USER SAPD3D;
-- Revoke IMPLICIT_SCHEMA from possible Connectusers
REVOKE IMPLICIT_SCHEMA ON DATABASE FROM USER SAPD3D;
-- Revoke CREATE_EXTERNAL_ROUTINE from possible Connectusers
REVOKE CREATE_EXTERNAL_ROUTINE ON DATABASE FROM USER SAPD3D;
-- Revoke CONNECT from PUBLIC
-- Revoke SQLADM from PUBLIC
-- Revoke EXPLAIN from PUBLIC
-- Revoke BINDADD from PUBLIC
-- Revoke CREATETAB from PUBLIC
-- Revoke IMPLICIT_SCHEMA from PUBLIC
-- Revoke CREATE_EXTERNAL_ROUTINE from PUBLIC
-- grant LOAD to Role SAPAPP
GRANT LOAD ON DATABASE TO ROLE SAPAPP;
-- Revoke LOAD from possible Connectusers
REVOKE LOAD ON DATABASE FROM USER SAPD3D;
-- Grant use of SAP application tablespaces to SAPAPP role
GRANT USE OF TABLESPACE "D3D#BTABD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#BTABI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#CLUD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#CLUI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#DDICD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#DDICI" TO ROLE SAPAPP;
```

```
GRANT USE OF TABLESPACE "D3D#DIMD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#DIMI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#DOCUD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#DOCUI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#EL701D" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#EL701I" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#ES701D" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#ES701I" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#FACTD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#FACTI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#LOADD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#LOADI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#ODSD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#ODSI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#POOLD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#POOLI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#PROTD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#PROTI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#SOURCED" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#SOURCEI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#STABD" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#STABI" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#USER1D" TO ROLE SAPAPP;
GRANT USE OF TABLESPACE "D3D#USER1I" TO ROLE SAPAPP;
-- Grant use of SAPTOOLS and SAPEVENTMON tablespace to SAPMON role
-- Revoke use of all SAP tablespaces from public
REVOKE USE OF TABLESPACE "D3D#BTABD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#BTABI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#CLUD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#CLUI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#DDICD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#DDICI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#DIMD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#DIMI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#DOCUD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#DOCUI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#EL701D" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#EL701I" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#ES701D" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#ES701I" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#FACTD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#FACTI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#LOADD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#LOADI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#ODSD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#ODSI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#POOLD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#POOLI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#PROTD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#PROTI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#SOURCED" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#SOURCEI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#STABD" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#STABI" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#USER1D" FROM PUBLIC;
REVOKE USE OF TABLESPACE "D3D#USER1I" FROM PUBLIC;
-- Grant DBADM to role SAPTOOLS
GRANT DBADM ON DATABASE TO ROLE SAPTOOLS;
-- Grant WLMADM to role SAPTOOLS
GRANT WLMADM ON DATABASE TO ROLE SAPTOOLS;
-- Revoke DBADM from possible Connectusers
-- Revoke WLMADM from possible Connectusers
-- Revoke WLMADM from PUBLIC
-- Grant Table Authorities in SAPTOOLS Schema
-- Revoke Table Authorities in SAPTOOLS Schema from Connectusers
-- Revoke Table Authorities in SAPTOOLS Schema from PUBLIC
-- Grant Index Authorities in SAPTOOLS Schema
-- Revoke Index Authorities in SAPTOOLS Schema from Connectusers
-- Revoke Index Authorities in SAPTOOLS Schema from PUBLIC
-- Grant Routine Authorities in SAPTOOLS Schema
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.DB2SAP_SNAP_GET_DB TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.DB2SAP_SNAP_GET_DB_AP TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.DB2SAP_SNAP_GET_DYN_SQL TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.DB2SAP_SNAP_GET_DYN_SQL_AP TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.DB2SUPPORT_RETRIEVE TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.DISK_INFO TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.EXEC_CLP TO ROLE SAPMON;
```

```
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.EXEC_CMD TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.GET_EXPLAIN_DDL TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SAPTOOLS.MOUNT_INFO TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC PROCEDURE SAPTOOLS.DB2SUPPORT_STMT TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC PROCEDURE SAPTOOLS.INSPECT_TABLE_ROWCOMPESTIMATE TO ROLE SAPMON;
-- Revoke Routine Authorities in SAPTOOLS Schema from Connectusers
-- Revoke Routine Authorities for SAPTOOLS.* from Connectusers
-- Revoke Routine Authorities in SAPTOOLS Schema from PUBLIC
-- Revoke Routine Authorities for SAPTOOLS.* from PUBLIC
REVOKE EXECUTE ON FUNCTION SAPTOOLS.* FROM PUBLIC RESTRICT;
REVOKE EXECUTE ON PROCEDURE SAPTOOLS.* FROM PUBLIC RESTRICT;
-- Grant CREATEIN Authority for SAPTOOLS Schema to role SAPMON
GRANT CREATEIN ON SCHEMA SAPTOOLS TO ROLE SAPMON;
-- Grant ALTERIN Authority for SAPTOOLS Schema to role SAPMON
GRANT ALTERIN ON SCHEMA SAPTOOLS TO ROLE SAPMON;
-- Grant DROPIN Authority for SAPTOOLS Schema to role SAPMON
GRANT DROPIN ON SCHEMA SAPTOOLS TO ROLE SAPMON;
-- Revoke CREATEIN on schema SAPTOOLS from possible Connectusers
REVOKE CREATEIN ON SCHEMA SAPTOOLS FROM USER SAPD3D;
-- Revoke ALTERIN on schema SAPTOOLS from possible Connectusers
REVOKE ALTERIN ON SCHEMA SAPTOOLS FROM USER SAPD3D;
-- Revoke DROPIN on schema SAPTOOLS from possible Connectusers
REVOKE DROPIN ON SCHEMA SAPTOOLS FROM USER SAPD3D;
-- Revoke CREATEIN on SAPTOOLS schema from PUBLIC
REVOKE CREATEIN ON SCHEMA SAPTOOLS FROM PUBLIC;
-- Revoke ALTERIN on SAPTOOLS schema from PUBLIC
-- Revoke DROPIN on SAPTOOLS schema from PUBLIC
-- Grant Execute on SYSPROC functions / procedures to role SAPMON
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.DB_GET_CFG TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_FORMAT_LOCK_NAME TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_FORMAT_XML_COMPONENT_TIMES_BY_ROW TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_FORMAT_XML_METRICS_BY_ROW TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_FORMAT_XML_TIMES_BY_ROW TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_FORMAT_XML_WAIT_TIMES_BY_ROW TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_ACTIVITY_DETAILS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_APPLICATION_HANDLE TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_APPLICATION_ID TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_APPL_LOCKWAIT TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_BUFFERPOOL TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_CONNECTION TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_CONNECTION_DETAILS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_CONTAINER TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_EXTENT_MOVEMENT_STATUS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_FCM TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_FCM_CONNECTION_LIST TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_INDEX TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_LOCKS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_PKG_CACHE_STMT TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_PKG_CACHE_STMT_DETAILS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_SERVICE_SUBCLASS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_SERVICE_SUBCLASS_DETAILS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_TABLE TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_TABLESPACE TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_UNIT_OF_WORK TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_UNIT_OF_WORK_DETAILS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_WORKLOAD TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.MON_GET_WORKLOAD_DETAILS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_ACTIVITY_DETAILS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_CONN_ENV TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_QUEUE_STATS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_SERVICE_CLASS_AGENTS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_SERVICE_CLASS_AGENTS_V97 TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_SERVICE_CLASS_WORKLOAD_OCCURRENCES TO ROLE
SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_SERVICE_CLASS_WORKLOAD_OCCURRENCES_V97 TO ROLE
SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_SERVICE_SUBCLASS_STATS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_SERVICE_SUBCLASS_STATS_V97 TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_SERVICE_SUPERCLASS_STATS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_WORKLOAD_OCCURRENCE_ACTIVITIES TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_WORKLOAD_OCCURRENCE_ACTIVITIES_V97 TO ROLE
SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_WORKLOAD_STATS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_WORKLOAD_STATS_V97 TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC FUNCTION SYSPROC.WLM_GET_WORK_ACTION_SET_STATS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC PROCEDURE SYSPROC.WLM_CANCEL_ACTIVITY TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC PROCEDURE SYSPROC.WLM_CAPTURE_ACTIVITY_IN_PROGRESS TO ROLE SAPMON;
```

```
GRANT EXECUTE ON SPECIFIC PROCEDURE SYSPROC.WLM_COLLECT_STATS TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC PROCEDURE SYSPROC.WLM_COLLECT_STATS_WAIT TO ROLE SAPMON;
GRANT EXECUTE ON SPECIFIC PROCEDURE SYSPROC.WLM_SET_CONN_ENV TO ROLE SAPMON;
-- Revoke Execute on SYSPROC Stored Procedures from Connectusers
-- Revoke Execute on SYSPROC Stored Procedures from PUBLIC
-- Grant SELECT on SAP Basis tables to ROLE SAPMON
GRANT SELECT ON TABLE SAPD3D."AVERS" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."CVERS" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DARTT" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DB6CSTRACE" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DB6IREORG" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DB6TREORG" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DBSTATC" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DD02L" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DD03L" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DD06L" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DD07T" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."DDART" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."IADB6" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."PAT03" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."PAT06" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."PATCHHIST" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."SVERS" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."TADB6" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."TRESC" TO ROLE SAPMON;
GRANT SELECT ON TABLE SAPD3D."TSDB6" TO ROLE SAPMON;
-- Grant INSERT on SAP Basis tables to ROLE SAPMON
GRANT INSERT ON TABLE SAPD3D."DBDIFF" TO ROLE SAPMON;
-- Grant UPDATE on SAP Basis tables to ROLE SAPMON
GRANT UPDATE  ON TABLE SAPD3D."DBDIFF" TO ROLE SAPMON;
-- Grant DELETE on SAP Basis tables to ROLE SAPMON
GRANT DELETE ON TABLE SAPD3D."DBDIFF" TO ROLE SAPMON;
-- Grant SELECT on SAP Basis tables to ROLE SAPTOOLS
GRANT SELECT ON TABLE SAPD3D."AVERS" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."CVERS" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."DB6CSTRACE" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."DD02L" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."DD03L" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."DD06L" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."DD07T" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."PAT03" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."PAT06" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."PATCHHIST" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."SVERS" TO ROLE SAPTOOLS;
GRANT SELECT ON TABLE SAPD3D."TRESC" TO ROLE SAPTOOLS;
-- Grant INSERT on SAP Basis tables to ROLE SAPTOOLS
GRANT INSERT ON TABLE SAPD3D."DARTT" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."DB6IREORG" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."DB6TREORG" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."DBDIFF" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."DBSTATC" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."DDART" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."IADB6" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."TADB6" TO ROLE SAPTOOLS;
GRANT INSERT ON TABLE SAPD3D."TSDB6" TO ROLE SAPTOOLS;
-- Grant UPDATE on SAP Basis tables to ROLE SAPTOOLS
GRANT UPDATE ON TABLE SAPD3D."DARTT" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."DB6IREORG" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."DB6TREORG" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."DBDIFF" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."DBSTATC" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."DDART" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."IADB6" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."TADB6" TO ROLE SAPTOOLS;
GRANT UPDATE ON TABLE SAPD3D."TSDB6" TO ROLE SAPTOOLS;
-- Grant DELETE on SAP Basis tables to ROLE SAPTOOLS
GRANT DELETE ON TABLE SAPD3D."DARTT" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."DB6IREORG" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."DB6TREORG" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."DBDIFF" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."DBSTATC" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."DDART" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."IADB6" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."TADB6" TO ROLE SAPTOOLS;
GRANT DELETE ON TABLE SAPD3D."TSDB6" TO ROLE SAPTOOLS;
-- revoke SELECT on SAP Basis tables from PUBLIC
REVOKE SELECT ON TABLE SAPD3D."AVERS" FROM PUBLIC;
```

```
REVOKE SELECT ON TABLE SAPD3D."CVERS" FROM PUBLIC;
REVOKE SELECT ON TABLE SAPD3D."PAT03" FROM PUBLIC;
REVOKE SELECT ON TABLE SAPD3D."PAT06" FROM PUBLIC;
REVOKE SELECT ON TABLE SAPD3D."PATCHHIST" FROM PUBLIC;
-- revoke INSERT on SAP Basis tables from PUBLIC
-- revoke UPDATE on SAP Basis tables from PUBLIC
-- revoke DELETE on SAP Basis tables from PUBLIC
-- revoke SELECT privileges from SYSIBM objects
REVOKE SELECT ON TABLE SYSIBM."SYSCOLUMNS" FROM user SAPD3D;
REVOKE SELECT ON TABLE SYSIBM."SYSINDEXES" FROM user SAPD3D;
REVOKE SELECT ON TABLE SYSIBM."SYSPLAN" FROM user SAPD3D;
REVOKE SELECT ON TABLE SYSIBM."SYSTABLES" FROM user SAPD3D;
REVOKE SELECT ON TABLE SYSIBM."SYSVIEWS" FROM user SAPD3D;
-- revoke UPDATE privileges from SYSCAT objects
REVOKE UPDATE ON TABLE SYSCAT."COLUMNS" FROM user SAPD3D;
REVOKE UPDATE ON TABLE SYSCAT."INDEXES" FROM user SAPD3D;
REVOKE UPDATE ON TABLE SYSCAT."TABLES" FROM user SAPD3D;
-- Revoke DBADM from user sidadm
REVOKE DBADM ON DATABASE from user D3DADM;

-- Terminate connection to D3D
terminate;

-- Done
```

Sample Output of Generated SQL Script in “Activate Separation of Duties” Scenario

```
-- generated on Wed Nov 16 13:57:43 CET 2011

--*************************************************************************
--
-- This file was generated by db6_update_db.sh version 0023
-- by calling ./db6_update_db.sh -d D3D –activate_sod db2sadm at Wed Nov 16 13:57:43 CET 2011
--*************************************************************************
--
-- Dependant on your system configuration it enables db2 features:
--
--  run db2updv8, db2updv9, db2updv95 or db2updv97 if necessary
--  enable autoresize on DMS table spaces
--  create 16k bufferpool if necessary
--  create SYSTOOLSPACE table space if not exists
--  create SYSTOOLSTMPSPACE table spaces if not exists
--  set db2 registry DB2_WORKLOAD=SAP
--  enable AUTORUNSTATS if not set already
--  rebind packages
--
--*************************************************************************

-- Connect to D3D
connect to D3D;
-- Connect to database as db2<sid>
connect to D3D user db2d3d;
-- Grant new SECADM
grant secadm on database to user db2sadm;
-- Revoke DATAACCESS from db2sadm if required
-- Disconnect/reconnect as new SECADM
disconnect D3D;
-- Disconnect/reconnect as new SECADM
connect to D3D user db2sadm;
-- Assign Instance Owner to role SAPTOOLS
GRANT ROLE SAPTOOLS TO USER db2d3d;
-- Revoke DATAACCESS from all users if required
REVOKE DATAACCESS ON DATABASE FROM USER DB2D3D;
REVOKE DATAACCESS ON DATABASE FROM USER D3DADM;
-- Revoke SELECT on SAP Basis tables from Instance Owner
REVOKE SELECT ON TABLE SAPD3D."CVERS" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."DARTT" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."DB6IREORG" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."DBSTATC" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."DD02L" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."DD03L" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."DD06L" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."DDART" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."IADB6" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."SVERS" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."TADB6" FROM db2d3d;
REVOKE SELECT ON TABLE SAPD3D."TRESC" FROM db2d3d;
```

```
REVOKE SELECT ON TABLE SAPD3D."TSDB6" FROM db2d3d;
-- Revoke INSERT on SAP Basis tables from Instance Owner
REVOKE INSERT ON TABLE SAPD3D."DARTT" FROM db2d3d;
REVOKE INSERT ON TABLE SAPD3D."DB6IREORG" FROM db2d3d;
REVOKE INSERT ON TABLE SAPD3D."DB6TREORG" FROM db2d3d;
REVOKE INSERT ON TABLE SAPD3D."DBSTATC" FROM db2d3d;
REVOKE INSERT ON TABLE SAPD3D."DDART" FROM db2d3d;
REVOKE INSERT ON TABLE SAPD3D."IADB6" FROM db2d3d;
REVOKE INSERT ON TABLE SAPD3D."TADB6" FROM db2d3d;
REVOKE INSERT ON TABLE SAPD3D."TSDB6" FROM db2d3d;
-- Revoke UPDATE on SAP Basis tables from Instance Owner
REVOKE UPDATE ON TABLE SAPD3D."DARTT" FROM db2d3d;
REVOKE UPDATE ON TABLE SAPD3D."DB6IREORG" FROM db2d3d;
REVOKE UPDATE ON TABLE SAPD3D."DB6TREORG" FROM db2d3d;
REVOKE UPDATE ON TABLE SAPD3D."DBSTATC" FROM db2d3d;
REVOKE UPDATE ON TABLE SAPD3D."DDART" FROM db2d3d;
REVOKE UPDATE ON TABLE SAPD3D."IADB6" FROM db2d3d;
REVOKE UPDATE ON TABLE SAPD3D."TADB6" FROM db2d3d;
REVOKE UPDATE ON TABLE SAPD3D."TSDB6" FROM db2d3d;
-- Revoke DELETE on SAP Basis tables from Instance Owner
REVOKE DELETE ON TABLE SAPD3D."DARTT" FROM db2d3d;
REVOKE DELETE ON TABLE SAPD3D."DB6IREORG" FROM db2d3d;
REVOKE DELETE ON TABLE SAPD3D."DB6TREORG" FROM db2d3d;
REVOKE DELETE ON TABLE SAPD3D."DBSTATC" FROM db2d3d;
REVOKE DELETE ON TABLE SAPD3D."DDART" FROM db2d3d;
REVOKE DELETE ON TABLE SAPD3D."IADB6" FROM db2d3d;
REVOKE DELETE ON TABLE SAPD3D."TADB6" FROM db2d3d;
REVOKE DELETE ON TABLE SAPD3D."TSDB6" FROM db2d3d;

-- Terminate connection to D3D
terminate;

-- Done
```

Sample Output of Generated SQL Script in “Deactivate Separation of Duties” Scenario

```
-- generated on Wed Nov 16 15:50:00 CET 2011

--*********************************************************************
--
-- This file was generated by db6_update_db.sh version 0023
-- by calling ./db6_update_db.sh -d D3D –deactivate_sod db2sadm at Wed Nov 16 15:50:00 CET 2011
--*********************************************************************
--
-- Dependant on your system configuration it enables db2 features:
--
--  run db2updv8, db2updv9, db2updv95 or db2updv97 if necessary
--  enable autoresize on DMS table spaces
--  create 16k bufferpool if necessary
--  create SYSTOOLSPACE table space if not exists
--  create SYSTOOLSTMPSPACE table spaces if not exists
--  set db2 registry DB2_WORKLOAD=SAP
--  enable AUTORUNSTATS if not set already
--  rebind packages
--
--*********************************************************************

-- Connect to D3D
connect to D3D;
-- Connect to database as db2sadm
connect to D3D user db2sadm;
-- Grant SECADM to db2<sid> again
GRANT SECADM ON DATABASE TO USER db2d3d;
-- Grant DATAACCESS to db2<sid> again
GRANT DATAACCESS ON DATABASE TO USER db2d3d;
-- Revoke SAPTOOLS from db2<sid> again
REVOKE SAPTOOLS FROM USER db2d3d;
-- Disconnect/reconnect as db2<sid>
disconnect D3D;
-- Disconnect/reconnect as db2<sid>
connect to D3D user db2d3d;
-- Revoke SECADM from db2sadm again
REVOKE SECADM ON DATABASE FROM db2sadm;
-- Grant DATAACCESS to <sid>adm and connectuser
GRANT DATAACCESS ON DATABASE TO USER DB2SADM;
GRANT DATAACCESS ON DATABASE TO USER D3DADM;
```

```
-- Terminate connection to D3D
terminate;

-- Done
```

www.sap.com/contactsap

THE BEST RUN SAP®