SAP NetWeaver 2004s SPS 4

Security Guide

IBM DB2 UDB for UNIX and Windows under Windows

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

IBM DB2 UDB for UNIX and Windows under Windows

The following list provides an overview of the sections that describe the measures you take on Windows when your database is IBM DB2 Universal Database for UNIX and Windows:

Throughout this documentation the following conventions apply:
IBM DB2 Universal Database for UNIX and Windows is referred to *as DB2 UDB for UNIX and Windows* or *DB2*.

1 General Information

The following section provides information on:

- Database system groups
- Database authentication
- Password management
- Encryption key `DB2DB6EKEY`

Database System Groups

Depending on the SAP system release and the DB2 Admin Tools release, the following operating system groups apply to your installation:

Group	Operating System Group	User
`SYSADM_GROUP`	`db<dbsid>adm`	`db2<dbsid>`
`SYSCTRL_GROUP`	`db<dbsid>ctl`	`<sapsid>adm`
`SYSMAINT_GROUP`	`db<dbsid>mmt`	• ABAP database connect user • Java database connect user

If you want to find out which operating system group applies to your SAP system installation, you must check parameters `SYSADM_GROUP` and `SYSCTRL_GROUP`. To do so, log on to the database server as user `db2<dbsid>` and enter the following command: **`db2 get dbm cfg`**

Database Authentication

DB2 UDB for UNIX and Windows is always installed with one of the following database manager parameters:

- `Authentication = SERVER`

  The user ID and password provided on connect or attach are verified by DB2 using operating system services on the database server.

- `Authentication = SERVER_ENCRYPT`

  This parameter provides a higher level of security since passwords are send encrypted across the network. We recommend that you use this setting. It is supported by all currently supported database versions.

To authenticate a user, DB2 searches the Windows security databases in the following sequence:

1. It searches for the user in the local security database on the database server.

   

   The search for a user in a security database always starts at the database server.
2. If the user is not found, it searches in the security database of the Primary Domain Controller in the current domain.
3. If the user is still not found, it searches in the security databases of all trusted domains until either the user is located or all the security databases have been searched.

DB2 UDB for UNIX and Windows Version 8 provides a new registry variable that determines where DB2 searches for the following groups:

- `SYSADM_GROUP`
- `SYSCTRL_GROUP`
- `SYSMAINT_GROUP`

DB2 uses these Windows groups on the database server **only** if registry variable `DB2_GRP_LOOKUP` has been set to *LOCAL*.

To check whether registry variable `DB2_GRP_LOOKUP` has been set, log on to the database server as user `db2<dbsid>` and enter the following command:
`db2set DB2_GRP_LOOKUP`
To set `DB2_GRP_LOOKUP`, enter the following command:
`db2set DB2_GRP_LOOKUP=LOCAL`

Password Management

This section describes how you set passwords of SAP users that connect to the database in the **ABAP** stack. For information about how use set passwords of database connect users of the **Java** stack, see Security Aspects for the Database Connection [SAP Library], subsection *Using the Default DataSource*.

If the user is located in a security database, the user's password and its membership in a particular group are checked using only the information in the security database where the user is found. If the user is not found, access is refused.

Remote and local application servers normally connect to the database using the ABAP connect user (`sapr3` or `sap<sapsid>`). All SAP tables are created under the schema of these users. For special purposes, however (for example, taking database snapshots), SAP programs attach as user `<sapsid>adm`. The SAP programs must know the passwords of the ABAP connect user and of `<sapsid>adm`. Therefore, DB2 UDB for UNIX and Windows additionally maintains the passwords for the connect user and user `<sapsid>adm` in file `\\<%DSCDB6HOME%>\sapmnt\<SAPSID>\SYS\global\dscdb6.conf`.

DB2 UDB for UNIX and Windows provides functions to:

- Create password file `dscdb6.conf`

  This file can be recreated any time manually using the following command:

  `dscdb6up –create <connect_userpwd> <sapsid_adm_pwd>`

- Retrieve passwords

  This function is only used by SAP executables to connect or attach to the database.

- Update passwords in file `dscdb6.conf` and in the operating system simultaneously

  You can perform this task using the following command:

  `dscdb6up <user> <password>`

All functions need the environment variables `DSDDB6HOME`, `DB2DB6EKEY`, `DB2INSTANCE` and `DB2DBDFT` to be set correctly.

In an exclusively Windows environment, the environment variable `DSCDB6HOME` contains the name of the database server. In a system environment where the database server operates under an operating system other than Windows, `DSCDB6HOME` should contain the name of a server where you can access the file `dscdb6.conf` with the above-mentioned path..

You should protect file `dscdb6.conf` from unauthorized access

Encryption Key DB2DB6EKEY

For all the `dscdb6.conf` accesses described in this guide, the environment variable `DB2DB6EKEY` is used to encrypt or decrypt the requested password.

For a 3.1I kernel, executables used environment variable `DB6EKEY` for encrypting and decrypting passwords. Any other kernel executables use `DB2DB6EKEY`. If both variables are set in the environment (`DB6EKEY` and `DB2DB6EKEY`), make sure that they are both set to the same string value.

In the following discussion, we refer to this variable as `DB2DB6EKEY`.

`DB2DB6EKEY` is set initially during installation to the string `<SAPSID><db_server_hostname>`. You can change this value at any time when your SAP system is stopped, but if you do, then you also need to recreate password file `dscdb6.conf`. For more information, see Changing the Encryption Key DB2DB6EKEY [Page 10].

2 Users and Groups

The tables below show the users and groups that are required when running a SAP system on Windows when your database is DB2 UDB for UNIX and Windows.

Standard Users under Windows

User	Function
<sapsid>adm	SAP system administrator
SAPService<SAPSID>	SAP service account
db2<dbsid>	Database administrator
ABAP connect user: • sapr3 • sap<sapsid>	
Java connect user sap<sapsid>db	User for SAP system database objects
db2as	Owner of administration server (for SAP releases greater than 4.6x)

DB2 Standard Groups under Windows

Group	Function
SAP_<SAPSID>_GlobalAdmin	Domain-level SAP system administration group
SAP_<SAPSID>_LocalAdmin	Local groups on an application server
SYSADM_GROUP	Database administrator group
SYSCTRL_GROUP	Database system control group
SYSMAINT_GROUP	Database maintenance group

The SAP system users and groups are explained in more detail below.

User: SAP System Administrator (<sapsid>adm)

This user administers the SAP system. It also performs the installation procedure.

User: SAP Service Account (SAPService<SAPSID>

The SAP service account user is a virtual user. The SAP system services are started with this user account but you do not log on to the Windows operating system with it. This user account must have the local user rights to *Log on as a service* and has to be a member of the local administrator group. The name of this user must be SAPService<SAPSID>.

Group: SAP_<SAPSID>_GlobalAdmin

This global group is a domain-level SAP system administration group for organizing the administrators for your SAP systems. The sole function of a global group is to gather users together at domain level so that they can be placed in the appropriate local groups. The members of this group are the domain users <sapsid>adm and SAPService<SAPSID>.

The group SAP_<SAPSID>_GlobalAdmin is used only when the SAP system belongs to a Windows domain. You do not need the group SAP_<SAPSID>_GlobalAdmin if you are installing locally.

Group: SAP_<SAPSID>_LocalAdmin

Only local groups are created and maintained on an application server. A local group can only be given permissions and rights to the system where it is located. If the system is part of the domain, the local group can contain users and global groups from the domain.

Working With or Without a Domain Controller

If you are working **with** a domain controller, then note the following:

- The members of the group SAP_<SAPSID>_LocalAdmin are the global group SAP_<SAPSID>_GlobalAdmin, and on the database server, the domain user db2<dbsid>.
- The DB2 admin and DB2 control groups are created on the domain controller.

If you are working **without** a domain controller, then note the following:

- The members of the group SAP_<SAPSID>_LocalAdmin are the users <sapsid>adm, SAPService<SAPSID> and db2<dbsid>.
- The DB2 admin and DB2 control groups are created locally.

If all SAP system servers are domain controllers, then the local group exists at domain level and only has to be defined once for all domain controllers.

- With DB2 UDB for UNIX and Windows Version 8, you have to set DB2 registry variable DB2_GRP_LOOKUP to *LOCAL*.

3 Assigning Environment Variables

The following table lists the values of the environment variables as they are assigned in the installation procedures.

Environment Variables for DB2 UDB for UNIX and Windows

Environment Variable	Value
DB2INSTANCE	DB2<DBSID>
DB2DBDFT	<DBSID>
DSCDB6HOME	<database server name>
DB2DB6EKEY	<SAPSID><database server name> (default)

We recommend that you keep these values with the exception of DB2DB6EKEY.

You can change the value of DB2DB6EKEY at any time when the SAP system is down. However, changing the value of DB2DB6EKEY is difficult and must be executed on every server in the SAP system where a dialog process is running (all servers with the same <SAPSID>).

4 Changing the Environment Variable DB2DB6EKEY

Use

The environment variable DB2DB6EKEY contains the key used to encrypt the passwords for <sapsid>adm and the connect user that are stored in file dscdb6.conf. For all SAP application servers that use the same dscdb6.conf file to connect to the database, you must set DB2DB6EKEY to the same string value in the environment of the <sapsid>adm user. The same value should be set in the environment of user db2<dbsid> on the database server. In addition, you should protect file dscdb6.conf from unauthorized access.

Procedure

1. Stop all SAP services SAP<SAPSID>_<Instance_ID>.
2. Perform the following steps for all <sapsid>adm users on each application server of your SAP system and for user db2<dbsid> on the database server:
   a. Change the value of variable DB2DB6EKEY in your user environment.
   b. If your current user is <sapsid>adm, execute program ntenv2reg. If there are serveral SAP systems, select the correct SAP service name.
   c. Log off and log on again.

3. On the server %DSCDB6HOME% only:

   Log on as user <sapsid>adm an recreate file dscdb6.conf using the following command:

   dscdb6up –create <connect user pwd> <sapsid_adm pwd>

4. Restart your SAP services and your SAP system.

5 Access Privileges for Database-Related Resources

We recommend that you restrict the file and directory access privileges as shown in the table below.

Access Privileges for DB2 UDB Directories and Files

Directory	Access Privilege	Owner	For User or Group
<drive>:\Program Files\IBM\sqllib	*Full Control*	Administrator	Administrator, SYSTEM, SAP_<SAPSID>_LocalAdmin
<drive>:\ Program Files\IBM\sqllib\ db2<dbsid>	*Full Control*	Administrator	Administrator, SYSTEM, SAP_<SAPSID>_LocalAdmin
<drive>:\db2<dbsid>	*Full Control*	Administrator	SAP_<SAPSID>_LocalAdmin, SYSTEM
<drive>:\db2	*Full Control*	Administrator	Everyone
<drive>:\db2\<DBSID>	*Full Control*	Administrator	SAP_<SAPSID>_LocalAdmin, SYSTEM
<drive>:\db2\<SAPSID>\ sapdata*	*Full Control*	Administrator	db2<dbsid>, SYSTEM

See also:

For information on access privileges for Admin Tool-related directories and files, see the documentation *Database Administration Guide: SAP on IBM DB2 Universal Database for UNIX and Windows* that is available in SAP Service Marketplace at **service.sap.com/instguidesnw04** → *Operations* → *SAP Web AS*.

6 Additional Information on DB2 UDB for UNIX and Windows

You can find additional information in the following SAP documentation:

Title of documentation	Location
Database Administration Guide: *SAP on IBM DB2 Universal Database for UNIX and Windows*	SAP Service Marketplace at **service.sap.com/instguidesNW2004s**
Installation Guide: *SAP NetWeaver 2004s <Stack> <Platform/OS>:IBM DB2 Universal Database for UNIX and Windows*	SAP Service Marketplace at **service.sap.com/instguidesNW2004s**