SAP NetWeaver '04

Security Guide

Database Access Protection: IBM DB2 UDB for UNIX and Windows under UNIX

Document Version 1.00 – April 29, 2004

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 UNIX

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

Throughout this documentation the following naming 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 • sysadm	db2<dbsid>
SYSCTRL_GROUP	• db<dbsid>ctl • sysctrl	<sapsid>adm
SYSMAINT_GROUP	db<dbsid>mmt	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.

Password Management

Password management involves setting the passwords for the SAP users that connect to the database.

Remote and local application servers normally connect to the database using the 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 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 `/usr/sap/<SAPSID>/SYS/global/dscdb6.conf`. This file is accessible from all application servers using NFS or Windows shares. Passwords are stored encrypted. You should protect this file from unauthorized access.

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_user_pwd> <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>`

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 8].

2 Changing Passwords of the Database Standard Users

The following section provides information on the database standard users, whose passwords you need to change. The users are as follows:

Database Standard Users

User	Type	Method used to change password
`db2<dbsid>`	UNIX and database user	UNIX command **`passwd`**
`<sapsid>adm`	UNIX and database user	Program `dscdb6up`
Database connect user: • `sapr3` • `sap<sapsid>`	UNIX and database user	Program `dscdb6up`

Changing Passwords for User db2<dbsid>

This user is the DB2 instance owner. It is the DB2 system administrator and the SAP system database administrator. `db2<dbsid>` is authorized to execute database and database manager administration functions such as:

- Creating a database
- Creating or changing a tablespace
- Updating DB2 parameters
- Backing up or restoring the database

`db2<dbsid>` has the DB2 system administration authorities and belongs to group `SYSADM_GROUP`.

To change the password for user db2<dbsid>, log on as user db2<dbsid> and enter the **passwd** command at the UNIX prompt. Enter the old and new password.

If you use Network Information Service (NIS), you should also refer to the NIS guide and the operating system documentation. (Changing the password with an activated NIS may be different from changing it with the **passwd** command).
It is **not** necessary but recommended for the password to be the same on all hosts in your SAP system.

Changing Passwords for User <sapsid>adm

This user is the SAP system administrator. <sapsid>adm is authorized to start and stop the SAP system and the DB2 database manager. <sapsid>adm has the DB2 authorities DBADM **and** the ones belonging to group SYSCTRL_GROUP.

DB2-specific monitoring functions invoked by SAP system application server functions require SYSCTRL authority. The user belongs to group SYSCRTL_GROUP and the operating system group SAPSYS.

To change the password of user <sapsid>adm, use program dscdb6up.

For more information, 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/instguides** → *SAP Web Application Server* → *<Release>*

Changing Passwords of the Database Connect User

This user is the owner of all SAP System database objects (tables, indexes and views). All SAP System application server connections and accesses are performed under the connect user. The connect user belongs to group SYSMAINT_GROUP and to the operating system group SAPSYS. He is **only** created on the database server.

The user required at least the database authorizations CREATETAB, BINDADD, CONNECT, and IMPLICIT_SCHEMA. He also needs access to the SAP tablespaces belonging to his <SAPSID>. By default, tablespace access on SAP tablespaces is granted to PUBLIC, that is tablespaces can be accessed by all users that have CONNECT authorisations.

To change the password of the connect user (sapr3 or sap<sapsid>), use program dscdb6up.

For more information, 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/instguides** → *SAP Web Application Server* → *<Release>*.

3 Changing the Encryption Key DB2DB6EKEY

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.

The SAP profiles .dbenv_<hostname>.csh and .dbenv_<hostname>.sh contain the DB2DB6EKEY value. Both files must contain the same string value for DB2DB6EKEY.

To change variable DB2DB6EKEY, you must edit both files even if you only use the C-shell as login shell. This environment variable is set when <sapsid>adm or db2<dbsid> logs on. To activate your changes, log off and log on again as the same user who performed the changes.

Note the following:

- You can change DB2DB6EKEY at any time when your SAP system is stopped.
- You must regenerate the password file **immediately** after having altered DB2DB6EKEY. To do so, enter the following command:

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

See also:

For more information, 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/instguides** → *SAP Web Application Server* → *<Release>*.

4 Access Privileges for Database-Related Resources

The following section provides information on access privileges for DB2 or SAP system directories and files.

Some of the directories described in the following tables may not exist or remain empty depending on the set up of your SAP system and the archiving method (direct or indirect) you are using.
The access rights as described in the following table are automatically set in the installation procedures.

Access Privileges for DB2 Directories and Files

Directory or File	Access Privileges in Octal Form	Owner	Group
/db2/db2<dbsid>	755	db2<dbsid>	SYSADM_GROUP
/db2/<DBSID>/db2dump	755	db2<dbsid>	SYSADM_GROUP
/db2/<DBSID>/log_dir	755	db2<dbsid>	SYSADM_GROUP
/db2/<SAPSID>/sapdata*	755	db2<dbsid>	SYSADM_GROUP
/db2/<SAPSID>/sapdata*/ container	600	db2<dbsid>	SYSADM_GROUP
/db2/<DBSID>/saptemp1	755	db2<dbsid>	SYSADM_GROUP

SAP System Directory or File	Access Privileges in Octal Form	Owner	Group
<sapmnt>/exe	755	<sapsid>adm	sapsys
<sapmnt>/global	700 (lower than4.5B) 750 (greater than 4.5B)	<sapsid>adm	sapsys (lower than 4.5B) SYSADM_GROUP (greater than 4.5B)
<sapmnt>/profile	755	<sapsid>adm	sapsys
/usr/sap/trans	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/SYS	755	<sapsid>adm	sapsys
/usr/sap/<SAPSID>/<instance directory>	755	<sapsid>adm	sapsys

SAP System Directory or File	Access Privileges in Octal Form	Owner	Group
/usr/sap/<SAPSID>/SYS/exe/run/dscdb6up	4750	root	SYSCTRL_GROUP
/usr/sap/<SAPSID>/SYS/global/dscdb6.conf	600 (lower than 4.5B) 640 (greater than 4.5B)	<sid>adm	SYSADM_GROUP

We recommend that you restrict the UNIX file and directory access privileges according to the table above and as described in Setting Access Privileges for Files and Directories [Page 11].

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/instguides** → *SAP Web Application Server* → *<Release>*.

4.1 Setting Access Privileges for Files and Directories

Saving Current Settings

Before changing the access privileges, we advise you to save your current settings. To do so, log on to the database server as user db2<dbsid> and enter the following commands:

```
cd /db2/<SID>
ls -lR > db2_perm.txt

cd /usr/sap
ls -lR > sap_perm.txt

cd /sapmnt
ls -lR > sap_sw.txt
```

Setting Access Privileges

To change the access privileges for a file or directory, log on to the database server as user db2<dbsid> and enter the following command:

chmod <access privileges in octal> <file or directory>

```
chmod  755 /db2/<SID>
chmod  750 /db2/<SID>/log_dir
chmod 2755 /db2/<SID>/log_archive
.
.
.
```

Do **not** use chmod recursively. It is very easy to make unintended changes to authorizations when doing so.

5 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/instguides** → *SAP Web Application Server* → *<Release>*
Installation Guide: *SAP Web Application Server on UNIX – IBM DB2 Universal Database for UNIX and Windows*	SAP Service Marketplace at **service.sap.com/instguides** → *SAP Web Application Server* → *<Release>*
Installation Guide *<SAP Component> on UNIX- IBM DB2 Universal Database for UNIX and Windows*	SAP Service Marketplace at **service.sap.com/instguides** → *<SAP Component>* → *<Release>*