SAP NetWeaver '04

Security Guide

Database Access Protection: Oracle Under Windows

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

Oracle Under Windows

The following list provides an overview of the sections that describe the measures to take on Windows when your database is Oracle:

1 Protecting the Database Standard Users

The table below shows the standard users for which you should change passwords, along with the method used.

Changing the Passwords for Oracle Standard Users

User	Type	Method used to change password
`<sapsid>adm`	Operating system user	Standard Windows method
`OPS$<domain>\<sapsid>adm` `OPS$<computer>\<sapsid>adm`	OPS$ user	OPS$ mechanism
`SAPService<SAPSID>`	Operating system user	Standard Windows method
`OPS$<domain>\SAPService<SAPSID>` `OPS$<computer>\SAPService<SAPSID>`	OPS$ user	OPS$ mechanism
SYS (/ as sysdba)	Database user	BRCONNECT (as of Web AS 6.10) SQLPLUS
`SYSTEM`	Database user	BRCONNECT (as of Web AS 6.10) SQLPLUS
`SAP<SAPSID>`	Database user (SAP System)	BRCONNECT (as of Web AS 6.10) SQLPLUS

With SAP releases prior to 4.6C the database user `SAPR3 was used instead of SAP<SAPSID>`.

Note that if you change the passwords for <sapsid>adm and SAPService<SAPSID>, you also have to change the passwords of all services and batch jobs started via the Windows Scheduler that use these users.

For more information about how to protect these users, see the following topics:

- The OPS$ Mechanism Under Windows [Page 6]
- Protecting the SAP Database User [Page 6]
- Encrypted Password for SAP Database User When Using BRCONNECT [Page 7]
- Changing Passwords for SAP Database Users Using BRCONNECT [Page 7]

1.1 The OPS$ Mechanism Under Windows

For the database, the SAP system is a single user, SAP<SAPSID>, whose password is stored in the table SAPUSER. Therefore, to access the database, the SAP system uses a mechanism called the OPS$ mechanism, which works as follows:

1. When the system accesses the database, it first logs on to the database as the user OPS$<operating_system_user>, for example, OPS$<sapsid>adm. (The OPS$ user that corresponds to the operating system user must be defined in the database and identified as *externally*.)

   

   SAP does not support changes of the Oracle parameter os_authent_prefix whose default value is OPS$.
2. It retrieves the password for SAP<SAPSID>from the SAPUSER table.
3. It then logs on to the database as the user SAP<SAPSID>.

1.2 Protecting the SAP Database User

To protect access to the SAPUSER table and the SAP database user SAPR3/SAP<SID>, note the following:

- Only define OPS$ users for the Windows users that are necessary for operating the SAP system. These are typically the users SAPService<SAPSID> and <sapsid>adm; however, you may assign them other names. (In this guide, we refer to SAPService<SAPSID> and <sapsid>adm.) For more information about creating OPS$ users under Windows, see **SAP Note 50088**.
- Change the passwords for SAP<SAPSID>and <sapsid>adm regularly.

  Consequently, after changing the password for SAP<SAPSID>in an SAP system that you use as an import system, test imports no longer work correctly. You could override this problem by assigning the corresponding OPS$ users in the import system for all of the export systems. However, we recommend that you keep OPS$ users to a minimum and accept the fact that test imports no longer work. For more information, see **SAP Note 27928**.

- With the Oracle network protocol SQL*Net, you can also use the file `sqlnet.ora` to restrict access to the database using IP addresses. In this file, you specify *invited* and *excluded* IP addresses.

  For example:

  ```
  tcp.validnode_checking = yes
  tcp.invited_nodes = (139.185.5.73, ...)
  ```

  or:

  ```
  tcp.excluded_nodes = (139.185.6.71, ...)
  ```

  In this way, you can make sure that only specific hosts (for example, only the application server host) can access the database.

See also:

Changing Passwords for SAP Database Users Using BRCONNECT [Page 7]

1.3 Encrypted Password for SAP Database User When Using BRCONNECT

By using BRCONNECT, you can have the password for SAP<SAPSID> encrypted before storing it in the database. To maintain compatibility, the following rules apply:

- If the old password was not encrypted, then the new password is not encrypted before being stored.
- If the old password was encrypted, then the new password is also stored encrypted.
- If the old password exists in both encrypted and non-encrypted form, then the new password is also stored in both forms.

For the detailed procedure, see Changing Passwords for SAP Database Users Using BRCONNECT [Page 7]

1.4 Changing Password for Database Users Using BRCONNECT

Use

As of Release 6.10, you can use BRCONNECT to change the passwords for the database users SAP<SAPSID>, SYS, or SYSTEM.

You can also use BRCONNECT as of Release 6.10 to administer the database for older SAP systems.

Procedure

You can either change the passwords with BRCONNECT interactively or by using the command line.

Interactively

1. Start BRCONNECT with the command:

   brconnect [-u system/<system_password>] –f chpass –u <user_name>

2. Enter the new password twice for confirmation.

When you change the password interactively, on some platforms you can enter the new password hidden, as long as it is no longer than eight characters.

Using the command line

Enter the following command:

brconnect [-u system/<system_password>] –c –f chpass –u <user_name> –p <new_password>

Where:

- <system_password> is the password of the SYSTEM database user. You can use another user with DBA privileges.
- <user_name> is the database user for which the password should be changed (for example, SAP<SAPSID>).
- <new_password> is the new password for the user.

If you omit the -u option, then the logon occurs using SYSTEM with its default password.

Result

The password for the database user is changed.

For the user SAP<SAPSID>, the corresponding entry in the SAPUSER table is also updated. If no entry exists in the table, BRCONNECT creates one. In addition, the password for SAP<SAPSID>is encrypted. For more information see Encrypted Password for SAP Database User When Using BRCONNECT [Page 7].

2 Access Privileges for Database-Related Resources

Under Windows, you should protect all data files, all executable files, all Oracle files, and all SAP system files. To protect the Oracle files, assign the following access rights:

- Assign the local group SAP_<SAPSID>_LocalAdmin and the local user SYSTEM *Full Control* access rights for all Oracle files.
- Assign other groups and users no access rights for the Oracle files.

The table below shows the files and the corresponding access rights:

Setting Access Privileges for Oracle Directories and Files

Oracle Directories	Access Privilege	For User or Group
%ORACLE_HOME%	*Full Control*	SAP_<SAPSID>_LocalAdmin, SYSTEM
<drive>:\oracle\<dbsid>	*Full Control*	SAP_<SAPSID>_LocalAdmin, SYSTEM
<drive>:\usr\sap	*Full Control*	SAP_<SAPSID>_LocalAdmin, SYSTEM

Measures to take for the other files are included in Operating System Protection [SAP NetWeaver Security Guide].

3 Access Privileges for BR*Tools

If you use the DBA Planning Calendar, which uses the BR*Tools, then note the following:

- Assign <sapsid>adm and SAPService<SAPSID> to the local groups ORA_<DBSID>_DBA and ORA_<DBSID>_OPER. BRBACKUP then logs on using **connect / as sysoper**.

  The group ORA_<DBSID>_OPER (DB role: SYSOPER) is an administrator group that is restricted to operator operations. ORA_<DBSID>_OPER can start or shut down the database, perform backups, etc., but has no read or write authorizations.
- BRBACKUP and BRARCHIVE must also have full access to the SAP tables SDBAD, SDBAH and tables defined in the XDB interface. These access rights are contained in the DB role SAPDBA.
- BRCONNECT only executes from CCMS when the database is open. Appropriate database privileges are necessary for the following BRCONNECT operations:

  -f stats, -f next, -f cleanup, -f check
- BRCONNECT must have write permissions to the following tables:

  SDBAD, SDBAH, DBSTATC, DBSTATTORA, DBSTATHORA, DBSTATIORA, DBSTAIHORA, and other DBA* tables. These access rights are also contained in SAPDBA role.

4 Additional information on Oracle Under Windows

For general information about Windows operating system security, see **`www.microsoft.com/security`**

You can find additional information in the following SAP documentation:

Title of Documentation	Where to find?
Installation Guide: *SAP Web Application Server on Windows: Oracle*	SAP Service Marketplace at **`service.sap.com/instguides`** → *SAP Web Application Server* → *<Release>*
Installation Guide: *<SAP Component> on Windows: Oracle*	SAP Service Marketplace at **`service.sap.com/instguides`** → *<SAP Component>* → *<Release>*