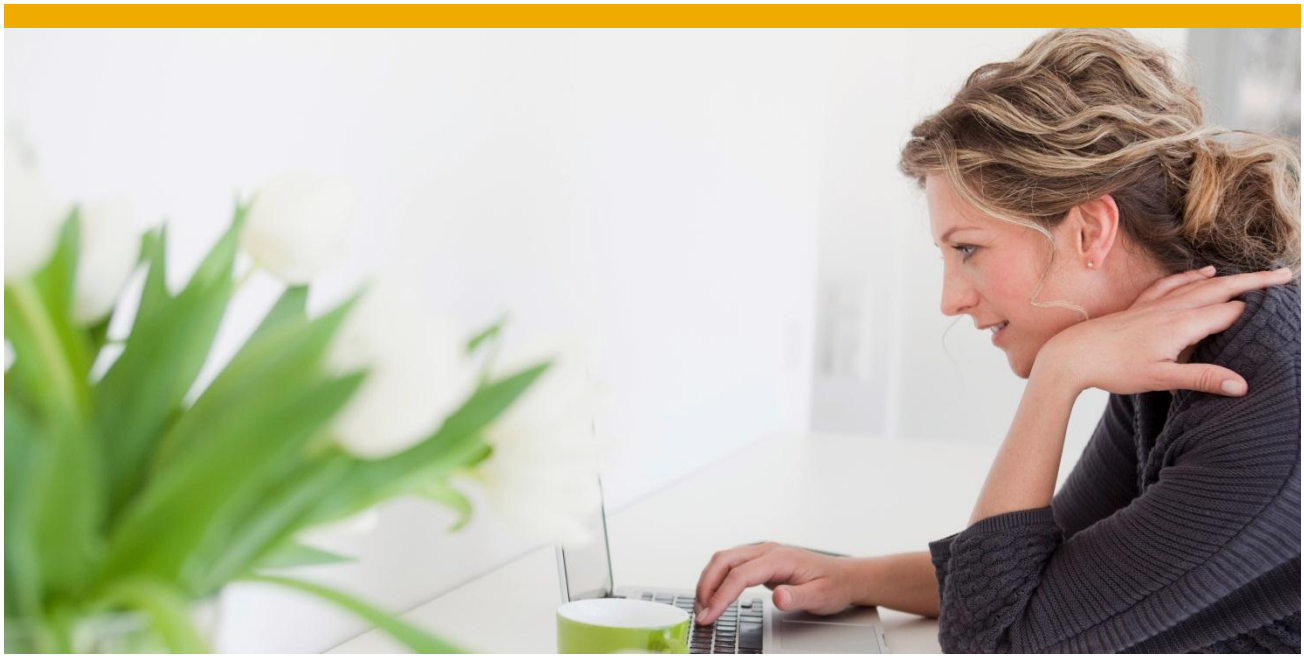


Database Security for Oracle

White Paper: Oracle Database Administration

February 2012

TABLE OF CONTENTS

INTRODUCTION

The security issues in the two-user concept (`ora<sid>`, `<sid>adm` (UNIX) or `<SID>ADM`, `SAPSERVICE<SID>` (Windows)) made it necessary to consider a global solution in the area of database security. This document is intended to explain the overall context and the improvements made in this area.

REQUIREMENTS OF THE DBA TOOLS

Secure Store Connect

Previously the connection of the SAP system (application server ABAP) and of SAP tools that use the ABAP database interface (R3trans, R3load, and so on) to the database via SQLNet (using the database alias name, for example, TNS) worked as follows. An OPS$ connection (with the database user `OPS$<SID>ADM`) that was authorized by the operating system user `<sid>adm` was created first ("connect /@TNS"). This permitted access only to the single table OPS$<SID>ADM.SAPUSER. It contains the encrypted password for the actual database connection of the SAP database user (default name SAPSR3).

As of Release 11g, OPS$ remote connect (using the TNS alias name) is no longer supported by future Oracle versions. As of kernel release 7.20, SAP has therefore introduced a new method of securely storing the database password and for connecting to the database: "Secure Storage in File System" (SSFS). The encrypted password for the SAP database user is then no longer stored in the database, but in the file system.

With the implementation of kernel 7.20 (11/2011) as a downward-compatible kernel (DCK for 7.x), the new method is available in all 7.x systems (as of SAP 7.00).

We recommend that you use the new method for security reasons.

For backwards compatibility, the conventional connect method continues to be supported up to Version 11.2 for all SAP systems that have Oracle.

All SAP systems as of Kernel 7.20, which use future Oracle versions after 11g, can only be operated with the new method.

For more information, see SAP Notes 1622837 and 1639578.

Database User OPS$<SID>ADM

The database user `OPS$<SID>ADM` is created in the database. It has the `SAPDBA` role and `remote_os_authent` is set to TRUE. The `SAPDBA` role is necessary to schedule BR*Tools from SAP CCMS.

BRBACKUP, BRARCHIVE, and BRCONNECT

Since BRBACKUP has to start up and shut down the database, a special Oracle privilege like the `SYSDBA` role is necessary, that is, `<sid>adm` has to belong to the UNIX group `dba` or to the Windows local group `ORA_<SID>_DBA`. But the `SYSOPER` role with reduced authorizations can also be used. The analogous UNIX group is `oper`. On Windows, the local group is `ORA_<SID>_OPER`. BRBACKUP calls SQLPLUS with `connect / as sysoper`.

Therefore, from the point of view of BRBACKUP, the UNIX group of the `<sid>adm` could be `oper`, the Windows group `ORA_<SID>_OPER`.

Furthermore, BRBACKUP and BRARCHIVE must have full access to the SAP<SID> tables SDBAD, SDBAH, and other DBA tables. The required privileges are part of the `SAPDBA` role. Thus appropriate operating system groups and the `SAPDBA` role are sufficient for BRBACKUP and BRARCHIVE to perform backups using cpio, dd or BACKINT interface.

BRCONNECT also needs the same privileges.

BRRECOVER, BRRESTORE, and BRSPACE

BRRECOVER and BRRESTORE perform database recovery whereas BRSPACE performs, among other things, tablespace management. These tools need the `SYSDBA` privilege to perform these functions. This privilege is normally granted through the UNIX group `dba` or the Windows group `ORA_<SID>_DBA`.

Since these tools also need special file system rights to create database files, make sure that you only call them as the UNIX user `ora<sid>` or the Windows user `<SID>ADM`.

REQUIREMENTS FOR BACKUPS USING RMAN

BRBACKUP and BRARCHIVE support backups using the Oracle Recovery Manager (RMAN). To perform database backups, RMAN requires SYSDBA privilege. To enable RMAN backups (for example, incremental backups) from the transaction DBACOCKPIT or DB13 (DBA Planning Calendar), the OS users <sid>adm (UNIX) and SAPSERVICE<SID> (Windows) must be entered in the corresponding operating system groups:

UNIX

OS User	OS Group	DB Role	DB User
ora<sid>	dba oper	SYSDBA SYSOPER SAPDBA	OPS$ORA<SID>
<sid>adm	dba oper	SYSDBA SYSOPER SAPDBA	OPS$<SID>ADM

Windows

OS User	OS Group	DB Role	DB User
<SID>ADM	ORA_<SID>_DBA ORA_<SID>_OPER	SYSDBA SYSOPER SAPDBA	OPS$<SID>ADM
SAPSERVICE<SID>	ORA_<SID>_DBA ORA_<SID>_OPER	SYSDBA SYSOPER SAPDBA	OPS$SAPSERVICE<SID>

We assume that the option -u / is used (see next section).

THE OPS$ MECHANISM

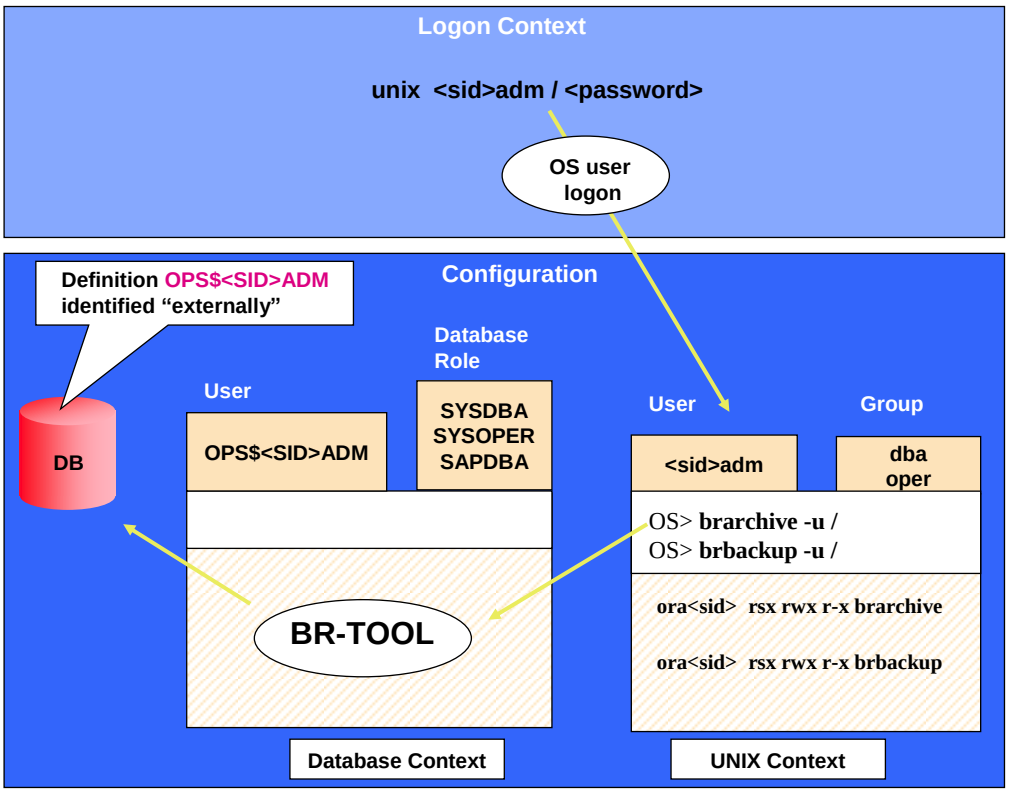
The Oracle OPS$ Mechanism moves the entire database security mechanism to the operating system level. The prerequisite is that a database user OPS$<OS_user>, corresponding to the operating system user (`OS_user`) is defined in the database, and identified externally.

When you have successfully logged on with the operating system user, you can then connect to the database with `SQL> connect /` , without entering a password. You then work there as `OPS$<OS_user>`. For example, you can start BRBACKUP in the same way:

OS> **`brbackup -u /`**

The OPS$ Mechanism is also always used when, for example, you call BRBACKUP, BRARCHIVE or BRCONNECT from the transaction DBACOCKPIT or DB13 of the SAP system.

OPS$ Mechanism for SAP



EXAMPLES OF USER CONFIGURATIONS (UNIX)

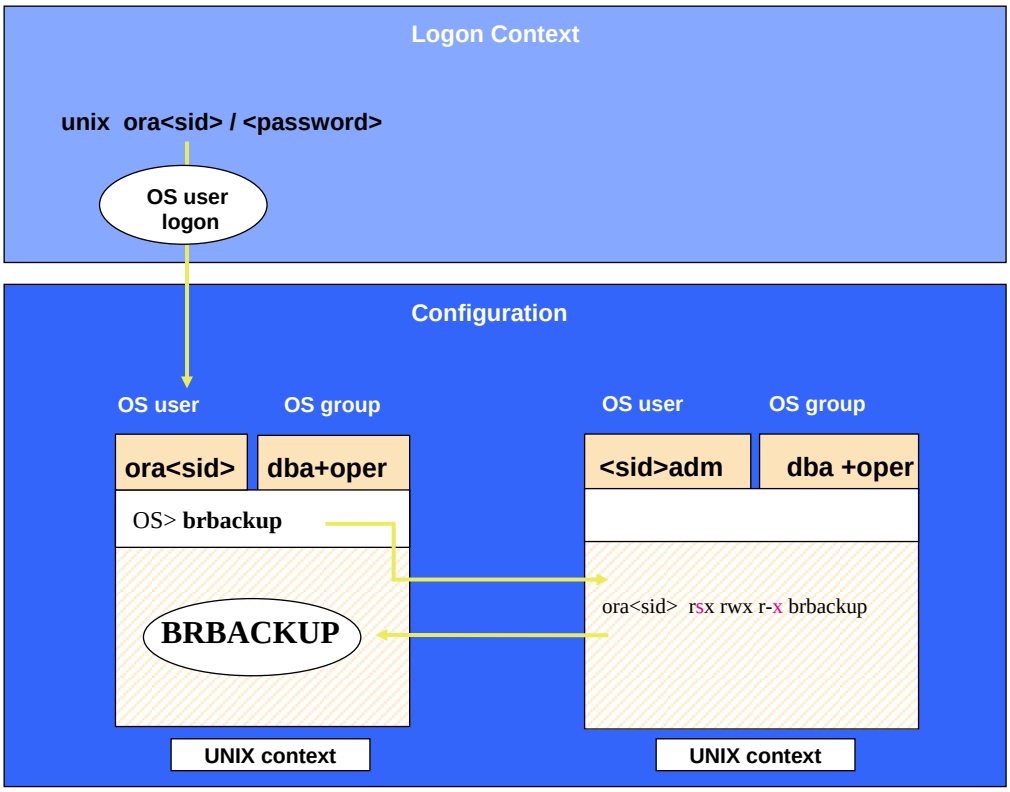
You can use different user configurations at the operating system level to meet the various security requirements in your organization.

Configuration 1: A Database Administrator with All Authorizations.

This configuration corresponds to the **SAP standard installation**. One employee has full responsibility for database administration with BR*Tools and other database tools. This employee can also execute all actions possible in this context as the UNIX user `ora<sid>`. In this case, you do not have to take any other security aspects into consideration, and the following user configuration is sensible. The database administrator knows the UNIX password of the user `ora<sid>`. When logged on under this password, the administrator has a high authorization level.

The user `ora<sid>` can start BR*Tools directly at operating system level, and can also access the database directly – for example, with SQLPLUS – and manipulate database objects.

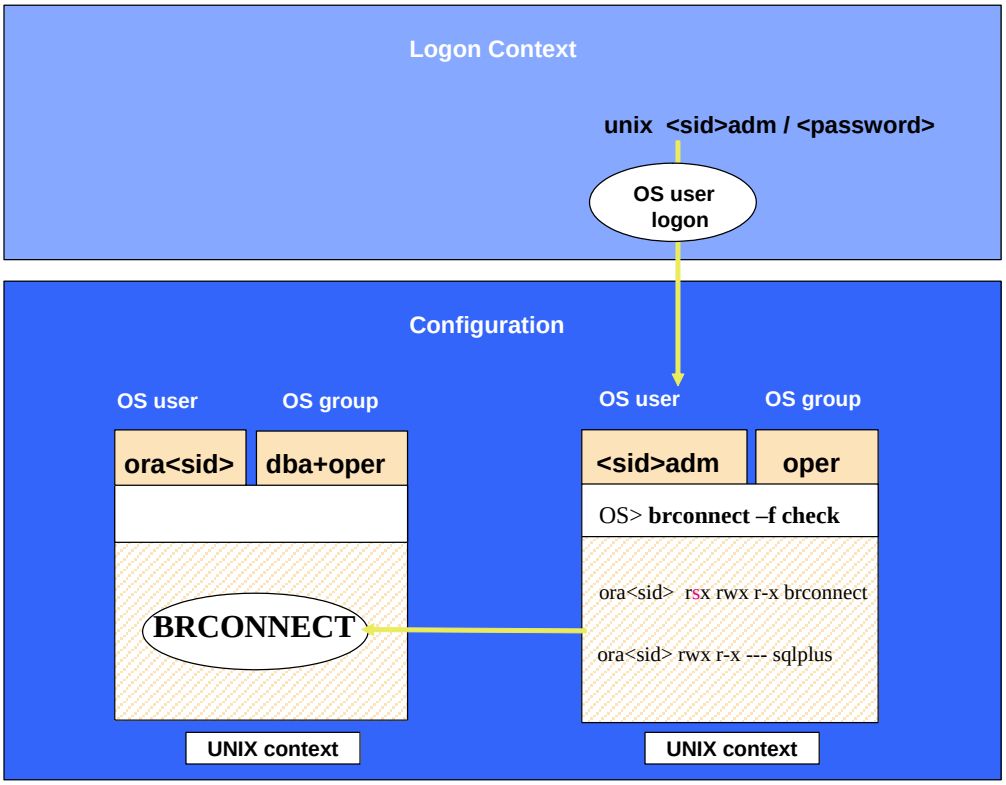
User Configuration 1



Configuration 2: An Employee with Operator Authorization

The operator is authorized to back up the database (but not with RMAN), and to call BRCONNECT with certain command options, such as `-f check`, `-f stats`, `-f cleanup`. The operator can also start up and shut down the database, but only has limited authorization to read or modify data (that is, only data that are needed to run BRBACKUP, BRARCHIVE, and BRCONNECT, but no application data). Only the administrator can restore backups.

User Configuration 2



BRCONNECT belongs to `ora<sid>`, but can be called by any user. Due to the set s-bit, BRCONNECT runs with the authorizations of the user `ora<sid>`.

The operator logs on as the user <sid>adm. This user belongs to the group oper. This allows the user to start up and shut down the database. This does not fully correspond to the standard configuration for SAP, since `<sid>adm` does not belong to the `dba` group. The user `<sid>adm` has a corresponding `OPS$` database user as standard (`OPS$<sid>adm`). This `OPS$` user is granted the `SAPDBA` role on the database and can, therefore, read the Oracle Dictionary tables and write in the DBA log tables in the database.

The OPS$ mechanism is activated automatically for the standard user `<sid>adm` during installation. You can use the OPS$ mechanism by calling BRCONNECT with the option `-u /`.

```
brconnect -u / -c -f check
brbackup -u / -c –d disk –m all –t online
```

The operator then has full administration authorization for the SAP system (but not for the database). If you want to keep privileges for the database separate from privileges for the SAP system, you must set up a separate OS user with the operator authorizations described above (see “Configuration 3” below).

If the standard password is changed from user SYSTEM and the OPS$ Mechanism is not used, then you must call BRCONNECT, BRBACKUP, and so on, with the option `-u <usr>/<password>`.

Configuration 3: An Employee Who Can Only Perform Selected Operations.

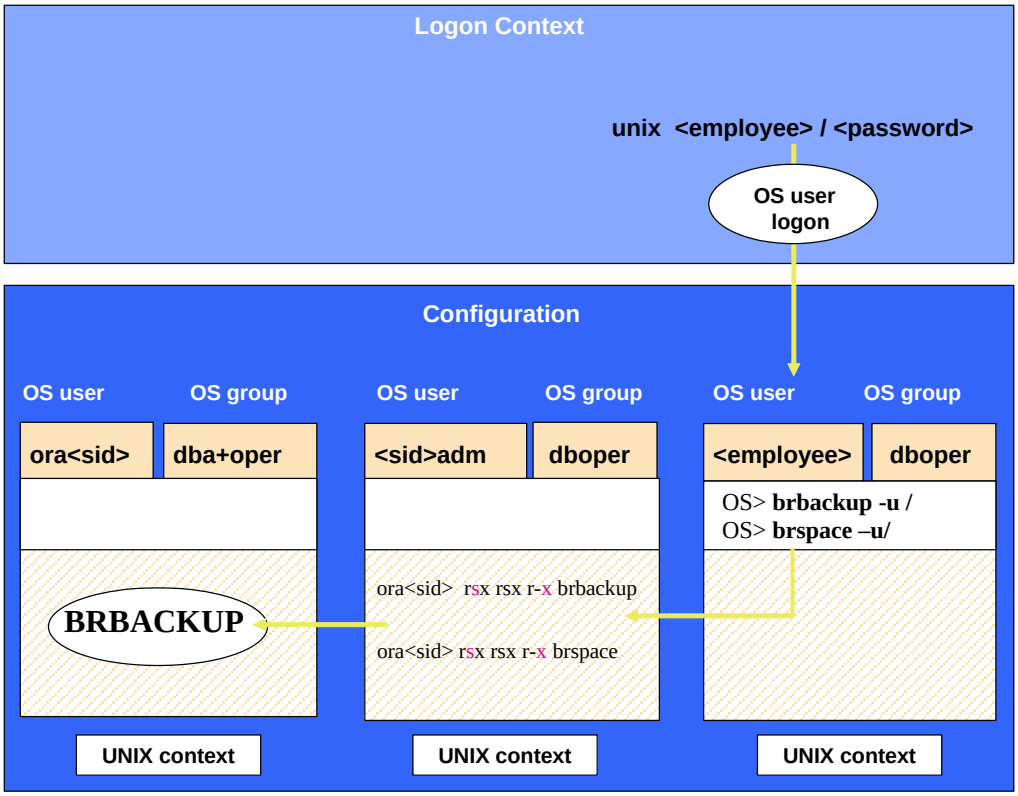
This configuration is for when you require a security mechanism for BR*Tools on UNIX with the following features:

- Only authorized DBA operators are allowed to execute BR*Tools operations. Such users have no other database access rights.
- Authorized DBA operators must **not** know the password of `ora<sid>` or `<sid>adm` and must **not** belong to the `dba` or `oper` groups.
- BR*Tools operations are logged continuously, including the ID of the person executing the operation. This person must **not** be able to manipulate these logs.

To achieve this level of security, BR*Tools executables are placed in a separate directory and given special rights. The new UNIX group required for the authorized DBA operators is `dboper`, which must contain all such users. If BR*Tools are also called under the user `<sapsid>adm` (for example, using transaction DBACOCKPIT or DB13, the DBA Planning Calendar), this user must also belong to the group `dboper`.

For more information, see **SAP Note** 832662.

User Configuration 3



BRBACKUP belongs to `ora<sid>`, but can be called by any user `<employee>`. Due to the set bit, BRBACKUP runs with the authorizations of the user `ora<sid>`.

You can start BRBACKUP with `brbackup -u /`, and therefore work with the user `OPS$ora<sid>`, to perform backups. To use this mechanism, the user `OPS$ora<sid>` with the `SAPDBA` role granted has to be defined in the database.

ADDITIONAL INFORMATION

SAP Library

You can find more information on Oracle database administration and the contents of this document in the SAP Library as follows:

All paths refer to SAP NetWeaver 7.3.

1. Call up the SAP Help Portal at help.sap.com/nw73 → *Application Help* → *SAP Library: English*.
2. Choose one of the following:
   - *SAP NetWeaver Library: Function-Oriented View* → *Database Administration* → *Database Administration for Oracle* → *SAP Database Guide: Oracle*
   - *SAP NetWeaver Security Guide* → *Security Guides for the Operating System and Database Platforms* → *Oracle Under UNIX or Oracle on Windows*

You can also find these plus selected extracts from the SAP Library at:

www.sdn.sap.com/irj/sdn/ora → *SAP on Oracle Knowledge Center* → *SAP Documentation in Help Portal*

SAP Notes

You can find SAP Notes at:

service.sap.com/notes