SAP Note

1622837 - Secure connection of AS ABAP to Oracle via SSFS

Version 24 **Validity:** 29.08.2014 - active **Language** English

Header Data

Released On 29.08.2014 15:22:47
Release Status Released for Customer
Component BC-DB-ORA-SYS Database Interface / DBMS for Oracle
Priority Recommendations / Additional Info
Category Program error

Symptom

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 in such a way that an OPS$ connection (with the database user OPS$<SID>ADM) that was authorized by the operating system user <sid>adm was created first ("connect /@TNS"). This permitted access to the table OPS$<SID>ADM.SAPUSER, and to this table only. 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 therefore introduces 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.xx), the new method is available in all 7.xx systems (as of SAP 7.00). For security reasons, SAP recommends that you use only the new method as soon as possible.

For backward compatibility, the conventional connect method continues to be supported for all SAP systems up to 7.38 and with Oracle up to Version 11.2.
All SAP systems that use Oracle versions higher than 11g in future can be operated with the new connection method only.
As of SAP Kernel Release 7.40 (irrespective of the Oracle version), only the secure connection (secure connect) is supported via SSFS.

Other Terms

SAPUSER, ops$-User, ops$-Connect, SSFS, data protection, secure storage, Secure Connect

Reason and Prerequisites

The new connect method is supported:
- For Unicode systems: As of kernel 7.20, patch 98 with DBSL patch 102
- For non-Unicode systems: As of kernel 7.20, patch 210, download as individual patches (packages dw, R3trans, R3load, and so on) if SAPEXE/SAPEXEDB does not exist

The old connection method is invalid as of Kernel 7.40.
(See point 3.4 about the upgrade)

Solution

1: Setting up the secure storage (SSFS)

The database-independent Note 1639578 describes the individual processes of creating subdirectories and files for a secure storage with the required access authorizations, setting the profile parameters and environment variables, and entering user and password in the secure storage.

Note that the DB user name in the secure storage is case-sensitive.
(Usually, the SAP database user SAPSR3 or SAP<SID> is saved in upper case on the database.)

As an alternative to the method described in SAP Note 1639578 for entering or changing a user and password (in two steps using "sqlplus" in the database and with "rsecssfx" in secure storage), you can do this in one step using "brconnect". The following example for the user "sapsr3" with the new password "<pwd>" changes the password in the database and changes or enters the user and password in the SSFS (if the required subdirectories are set up and environment variables are set) and in the table SAPUSER (if this still exists, see 3.1):

```
> brconnect -u / -f chpass -o sapsr3 -p <pwd>
```

2: Switching to the new connection method

If all of the options listed under section 1 have been executed correctly, the system is ready for both connection methods (the standard methods with the table SAPUSER and the new methods with the secure storage).

However, the standard method is always used by default.

The actual switch to the new method occurs with the profile parameter rsdb/ssfs_connect or with the environment variable rsdb_ssfs_connect. For this, refer to the details contained in the database-independent Note 1639578.
Pay attention to lowercase/uppercase letters here: rsdb_ssfs_connect.

3: Oracle database-specific postprocessing and BR* tools

3.1: Excluding the standard SAP connect method

If you use only the new database connection method, you should delete the table SAPUSER:

```
> sqlplus
SQL> connect system/<pwd>
SQL> drop table ops$<sid>adm.sapuser;
```

Caution with the upgrade, see below: 3.4., point (3)

The Oracle user ops$<sid>adm is then no longer required for the SAP connect. However, it must not be deleted because it is still used by BR* tools for the local database connection (see 3.3).

3.2: Excluding the Oracle remote OPS$ connect

The remote OPS$ connect is deactivated by default in all Oracle versions. However, you can activate it up to Oracle 11.2, which is also required for the conventional SAP connect method. For this, the Oracle initialization parameter REMOTE_OS_AUTHENT must be set to TRUE.
If the parameter REMOTE_OS_AUTHENT is set to TRUE in Oracle 11g, the system issues the following information message when starting the database:
"ORA-32004: obsolete and/or deprecated parameter(s) specified".

After the changeover to the new SAP connect method with the secure storage, you should remove the parameter REMOTE_OS_AUTHENT. Only with this setting does the new advantage in relation to security take full effect:

```
SQL> alter system reset remote_os_authent [scope=spfile];
```
(The addition scope=spfile is required up to Oracle 10g only.)

In future Oracle versions after 11g, the remote OPS$ connect ("connect /@TNS") will no longer be possible.

3.3: Local OPS$ connect for BR* Tools

Regardless of the old or new SAP connect method described in this note, the BR* database administration tools from SAP continue to use the local OPS$ connect ("connect /") for the operating system user <sid>adm with the database user ops$<sid>adm. In UNIX systems, the same also applies to ora<sid> or ops$ora<sid>. After 3.1., these database users no longer have any data segments in the database, but they retain the authorization of the role "SAPDBA".
The local OPS$ connect is also still possible in future Oracle releases after 11g and is not influenced by the parameter REMOTE_OS_AUTHENT. This does not affect the issue of security in the SAP system.

Password changes, in particular, the encrypted entry in the table SAPUSER, were made for the old connect method using brconnect. When you use only the new method (that is, after 3.1.), the entry in the table SAPUSER is no longer required. The database password can still be changed with brconnect.

SAP Note 1764043 describes the support of the new connect method with the BR*Tools.

Important:
After the Oracle parameter REMOTE_OS_AUTHENT has been removed, you sould use transaction DB17 to change the relevant BRCONNECT check condition that monitors its setting: The check value and the check operator are deleted or removed.
In this case, an alert is triggered if the parameter REMOTE_OS_AUTHENT is specified in the Oracle Spfile.

4: Information about the upgrade

The upgrade of SAP systems that are based on Oracle databases takes place using a shadow user that you can recognize from the suffix SHD (for example, SAPSR3SHD). This user is used only for the upgrade.

The upgrade proceeds in the same way as with the previous method except that, instead of the shadow user and password being entered in the table SAPUSER, the corresponding entries are now made in the secure store.
In the standard system, the same secure store is used for this as for the default user. Accordingly, the key words read (see SAP Note 1639578):
DB_CONNECT/SHADOW_DB_USER
DB_CONNECT/SHADOW_DB_PASSWORD
DB_CONNECT/SHADOW_DB_CON_ENV

As of the following kernel patches, you can also perform the SAP upgrade with the new connect method via secure store (SSFS):
7.20: As of patch >= 318
7.21: As of patch >= 27
and as of kernel 7.38 in general. (As of 7.40, only SSFS applies (see above)).

Note the following for the upgrade:
(1)
The entire SAP Kernel 7.2x must be patched and not just the DBSL.

(2)

For the BR* tools, at least version 7.20 patch 28 is required.

(3)
The table SAPUSER can only be deleted after the completion of the full upgrade because during the upgrade the old system still connects to the DB.

(4)
The Secure Store paths are generally set in the SAP profile: Parameters rsec/ssfs_datapath and rsec/ssfs_keypath. However, these are by default defined using the variables $DIR_GLOBAL, which leads to different paths during the upgrade. As a consequence, these parameters must also be set as environment variables during the upgrade. Also the other R3 tools (R3trans,and so on), and the BR* tools require these environment variables:
RSEC_SSFS_DATAPATH = /usr/sap/<SID>/SYS/global/security/rsecssfs/data
RSEC_SSFS_KEYPATH = /usr/sap/<SID>/SYS/global/security/rsecssfs/key
rsdb_ssfs_connect = 1
(The paths in this example correspond to the standard.)

(5)
for the upgrade to 7.40

5.1 start release < 7.00:

The upgrade (SUM) stops during the extraction phase with a DB connect error. Install SSFS with the 7.40 kernel that is already unpacked at this time. Then continue the upgrade, that is, terminate the SUM process and restart with the new environment variables (log on as OS user if necessary).

5.2 source release = 7.0x and 7.1x as well as older 7.2x patches (see above):

There are two options:
a)
Kernel exchange (replace the old 7.xx Kernel with the current, backward compatible Kernel 7.2x), implement SSFS, carry out the upgrade.
b)
Start the upgrade (SUM) with the old 7.xx Kernel. It will stop with a DB connect error during the extraction phase. Install SSFS with the 7.40 kernel that is already unpacked at this time. Then continue the upgrade, that is, terminate the SUM process and restart with the new environment variables (log on as OS user if necessary).

5.3 source release >= 7.2x (SSFS-compatible patch, see above prerequisites):

First set up Secure Store if you have not yet done this.
Then, perform the upgrade.

Validity

Software Component	From Rel.	To Rel.	And Subsequent
KRNL32NUC	7.20	7.20	☐
	7.20EXT	7.20EXT	☐
	7.21	7.21	☐
	7.21EXT	7.21EXT	☐
KRNL32UC	7.20	7.20	☐
	7.20EXT	7.20EXT	☐
	7.21	7.21	☐
	7.21EXT	7.21EXT	☐
KRNL64NUC	7.20	7.20	☐
	7.20EXT	7.20EXT	☐
	7.21	7.21	☐
	7.21EXT	7.21EXT	☐
KRNL64UC	7.20	7.20	☐
	7.20EXT	7.20EXT	☐
	7.21	7.21	☐
	7.21EXT	7.21EXT	☐
KERNEL	7.20	7.21	☐

Support Packages & Patches

Support Package Patches		
Software Component	Support Package	Patch Level
SAP KERNEL 7.20 32-BIT	SP000	000318
SAP KERNEL 7.20 32-BIT UNICODE	SP000	000318
SAP KERNEL 7.20 64-BIT	SP000	000318
SAP KERNEL 7.20 64-BIT UNICODE	SP000	000318
SAP KERNEL 7.21 32-BIT	SP000	000027
	SP027	000027

SAP KERNEL 7.21 32-BIT UNICODE	SP000	000027
	SP027	000027
SAP KERNEL 7.21 64-BIT	SP000	000027
	SP027	000027
SAP KERNEL 7.21 64-BIT UNICODE	SP000	000027
	SP027	000027
SAP KERNEL 7.21 EXT 32-BIT	SP000	000027
	SP027	000027
SAP KERNEL 7.21 EXT 32-BIT UC	SP000	000027
	SP027	000027
SAP KERNEL 7.21 EXT 64-BIT	SP000	000027
	SP027	000027
SAP KERNEL 7.21 EXT 64-BIT UC	SP000	000027
	SP027	000027

References

This document refers to:

SAP Notes

1868094	Overview: Oracle Security SAP Notes
1764043	Support for secure storage in BR*Tools
1678336	RSecSSFs: UTF8 conversion failed with returncode 1
1639578	SSFS as password store for primary database connect
1611877	Support for ABAP SSFS during database connect
1431798	Oracle 11.2.0: Database Parameter Settings
830576	Parameter recommendations for Oracle 10g
700548	FAQ: Oracle authorizations
157499	OPS$ connect and security aspects

This document is referenced by:

SAP Notes (9)

1611877	Support for ABAP SSFS during database connect
1678336	RSecSSFs: UTF8 conversion failed with returncode 1
1431798	Oracle 11.2.0: Database Parameter Settings
830576	Parameter recommendations for Oracle 10g
1868094	Overview: Oracle Security SAP Notes
1639578	SSFS as password store for primary database connect
1764043	Support for secure storage in BR*Tools
700548	FAQ: Oracle authorizations
157499	OPS$ connect and security aspects