

# Neues Benutzerkonzept für SAP NetWeaver Installationen mit Oracle Datenbank 12c unter Unix

Andreas Becker  
Oracle Deutschland B.V. & Co. KG

Oktober 2015

## Schlüsselworte

SAP NetWeaver, Oracle Datenbank 12c Release 1 (12.1), Unix/Linux, SAP BR\*Tools, SI/FS

## Benutzerkonzept mit Oracle Datenbank 12c Release 1

Der ursprüngliche Plan von SAP sah vor, das klassische Benutzerkonzept **SAP Classic** mit dem Softwareeigentümer `ora<db>sid` bei SAP Installationen auf Unix-Plattformen mit einer Oracle Single Instance Datenbank im Dateisystem (SI/FS) ab Oracle Release 12c Release 1 nicht mehr zu unterstützen. Stattdessen sollte nur noch das neue Benutzerkonzept **Oracle Standard** mit dem Softwareeigentümer `oracle`, das auch für Installationen mit RAC, ASM und für Oracle Engineered Systeme verwendet wird, erlaubt sein. Dieser Plan ist jedoch bei einigen SAP-Kunden auf Kritik und Ablehnung gestoßen.

Ein Teil der Kundenkritik bezog sich auf technische Aspekte des Benutzerkonzepts Oracle Standard, wenn mehrere SAP-Datenbanken auf einem Datenbankserver vorhanden sind. Aus diesem Grund haben sich SAP und Oracle entschlossen, das Benutzerkonzept Oracle Standard so zu erweitern und zu modifizieren, daß die Kritikpunkte beseitigt werden und darüber hinaus Anforderungen sowohl in Bezug auf die Administration als auch auf die Sicherheit erfüllt werden.

Der andere Teil der Kritik bezog sich auf den Zeitpunkt der Einführung des neuen Benutzerkonzepts und den gleichzeitigen De-Support des klassischen Benutzerkonzepts. Einige Kunden, die bis zum Ende des Premier Supports von Release 11.2 im Januar 2016 ihre Oracle Datenbanken auf Release 12.1 upgraden müssen, benötigen für die Umstellung auf ein neues Benutzerkonzept mehr Zeit.

Aus diesem Grund haben sich SAP und Oracle - entgegen der ursprünglichen Planung- entschieden, mit Oracle Datenbank 12c Release 1 neben dem Benutzerkonzept Oracle Standard auch das klassische Benutzerkonzept SAP Classic für SI/FS noch zu unterstützen (vgl. SAP Hinweise [1914631](#) und

[1915323](#)). Somit können Kunden nun beim Upgrade auf 12c Release 1 selber entscheiden, ob sie noch auf SAP Classic bleiben oder auf das neue Konzept Oracle Standard migrieren.

Mit Oracle Standard bietet SAP nun ab Oracle Release 12.1 ein über alle Oracle-Installationen einheitliches Benutzerkonzept (SI/FS, RAC, ASM und Oracle Engineered Systeme). SAP Classic ist abgekündigt und wird in einem künftigen Oracle Release von SAP möglicherweise nicht mehr unterstützt bzw. durch ein anderes Benutzerkonzept ersetzt.

Die vorgebrachte Kritik bei der Verwendung von Oracle Standard für SI/FS-Installationen hat die Entwickler von SAP und Oracle jedoch nicht ruhen lassen. Basierend auf den beiden vorhandenen Konzepten SAP Classic und Oracle Standard haben sie gemeinsam ein erweitertes, optimiertes Benutzerkonzept **Oracle Flex** entwickelt. Die angesprochenen Kritikpunkte sind in diesem Konzept eliminiert. Es ist kompatibel mit Oracle Standard und kann also sowohl für SI/FS als auch für RAC- oder ASM-Installationen verwendet werden. Es berücksichtigt einige zusätzliche Sicherheitsaspekte und bietet darüberhinaus die Möglichkeit, das Konzept sehr flexibel zu nutzen.

Dieses Dokument und der Vortrag stellt alle drei Benutzerkonzepte vor: SAP Classic, Oracle Standard und Oracle Flex.

### **Benutzerkonzept SAP Classic**

Bei SAP Classic handelt es sich, wie der Name bereits sagt, um das klassische Benutzerkonzept für SAP-NetWeaver-basierte Installationen. Ein SAP Systemadministrator administriert das SAP-System über den Betriebssystembenutzer <sapsid>adm. Für die Administration der zugehörigen Oracle-Datenbank ist der Betriebssystembenutzer ora<dbsid> vorgesehen.

Diese natürliche Aufgabenteilung sieht vor, dass der SAP-Systemadministrator auch solche datenbankspezifische Aufgaben übernehmen kann, die für den Betrieb des SAP-Systems notwendig sind. Dazu gehören beispielsweise regelmäßige Sicherungen der Datenbank und der Archive-Dateien sowie regelmäßige Datenbank-Checks und Statistikerneuerungen. Für diese Aufgaben ist der Benutzer <sapsid>adm über die Betriebssystemgruppen dba bzw. oper mit den notwendigen Systemrechten SYSDBA und SYSOPER ausgestattet und kann damit auch die BR\*Tools-Programme brarchive, brbackup und brconnect ausführen. Die Zugehörigkeit zur Gruppe dba ist nur deshalb notwendig, um Sicherungen mit RMAN durchführen zu können, wofür das SYSDBA-Recht notwendig ist. Ansonsten würde der <sapsid>adm für den Datenbankbetrieb auch ohne SYSDBA-Recht auskommen.

Der Benutzer ora<dbsid> hat im Benutzerkonzept SAP Classic die Doppelrolle des Softwareeigentümers und des Datenbankadministrators für die Datenbank <DBSID>. Als Mitglied der

Gruppen dba und oper besitzt er SYSDBA- und SYSOPER-Berechtigung. Aufgrund der Konfiguration der SAP BR\*Tools ist er auch in der Lage, alle BR\*Tools-Programme auszuführen.

Leider läßt sich dieses Benutzerkonzept nicht für Oracle-Installationen mit RAC, ASM oder auf Oracle Engineered Systemen verwenden, was in erster Linie daran liegt, dass der Softwareeigentümer ora<dbid> nicht in der Gruppe oinstall ist. Für diese Installationen musste daher Oracle Standard als neues Benutzerkonzept bei SAP-Installationen eingesetzt werden.

Ein anderer Nachteil von SAP Classic besteht darin, dass die Betriebssystemgruppen dba und oper standardmäßig für alle Oracle Homes verwendet werden. Dadurch ist aber eine sichere Trennung der Administration nicht mehr gegeben, wenn mehrere Datenbanken auf dem gleichen Datenbankserver installiert werden.

### **Benutzerkonzept Oracle Standard**

Wie oben bereits erwähnt, war das Benutzerkonzept SAP Classic in Release 11.2 nicht geeignet für SAP-Installationen mit Oracle RAC, mit Oracle ASM oder auf Oracle Engineered Systemen (Exadata, ODA, SuperCluster). Daher wurden solche Installationen mit dem neuen Benutzerkonzept Oracle Standard durchgeführt. Natürlich war auch bei diesem Konzept die Integration der SAP BR\*Tools als Standard-Werkzeuge für die Datenbankadministration zu berücksichtigen. SAP Hinweis 1598594 beschreibt die Konfiguration der BR\*Tools wie folgt:

```
-rwsrwsr-- 1 oracle oinstall 7732338 May 31 16:30 brarchive
-rwsrwsr-- 1 oracle oinstall 7908129 May 31 16:30 brbackup
-rwsrwsr-- 1 oracle oinstall 9970354 May 31 16:30 brconnect
-rwsrwsr-- 1 oracle oinstall 8376747 May 31 16:31 brrecover
-rwsrwsr-- 1 oracle oinstall 2783544 May 31 16:31 brrestore
-rwsrwsr-- 1 oracle oinstall 10479944 May 31 16:31 brspace
-rwxr-xr-x 1 <sid>adm sapsys 4103679 May 31 16:31 brtools
```

Wie man leicht erkennen kann, sind alle BR\*Tools-Programme, im Unterschied zu SAP Classic, identisch konfiguriert. Ausführungsberechtigt ist der Benutzer oracle sowie Mitglieder der Betriebssystemgruppe oinstall. Damit die für den Betrieb der Oracle-Datenbank notwendigen regelmäßigen Aufgaben (z.B. Sicherungen) auch über das SAP-System (und damit über den Benutzer <sapsid>adm) gestartet werden können, wird dieser in die Gruppe oinstall aufgenommen. Aufgrund der bei diesem Benutzerkonzept identischen Konfiguration kann der <sapsid>adm alle BR\*Tools-Programme ausführen, nicht nur brarchive, brbackup und brconnect wie bei SAP Classic. Er ist also vom Datenbank-Operator zum vollwertigen, hochprivilegierten Datenbank-Administrator

aufgestiegen. Somit sind die BR\*Tools bei diesem Konzept schon vollständig integriert, ohne dass die Notwendigkeit für den Benutzer ora<dbSID> noch besteht. Bei SAP-Installationen mit Oracle Release 11.2 hat man daher auch auf den Benutzer ora<dbSID> verzichtet. Allerdings hatte man bei dieser Entscheidung zwei Aspekte übersehen: zum einen war ohne den Benutzer ora<dbSID> beim Benutzerkonzept Oracle Standard keine benutzermäßige Trennung von SAP-Administration und Oracle-Administration mehr vorgesehen, sodaß Oracle-Datenbankadministratoren den gleichen Benutzer verwenden mussten wie SAP-Systemadministratoren. Zum anderen war für den SAP Host Agent die Ermittlung existierender Datenbankinstallationen ohne ora<dbSID> nur sehr umständlich möglich. Darüber hinaus war der Benutzer ‚oracle‘ oftmals als Zugangsbenutzer für die Datenbankadministration verwendet worden, obwohl er vom Konzept her eigentlich nur als Softwareeigentümer zu sehen ist.

Ab Release 12.1 hat man eingesehen, dass es sinnvoll und notwendig ist, im Benutzerkonzept Oracle Standard neben den Benutzern <sapsid>adm und dem Softwareeigentümer oracle noch einen zusätzlichen Benutzer ora<dbSID> standardmäßig vorzusehen, der als dedizierter Benutzer für die Datenbankadministration verwendet werden kann.

### **Benutzerkonzept Oracle Flex**

Für den Einsatz mit Oracle RAC, Oracle ASM und Oracle Engineered Systemen hat sich das Benutzerkonzept Oracle Standard im SAP-Umfeld seit mehreren Jahren bereits gut bewährt. Beim Einsatz mit SAP-Standardinstallationen SI/FS jedoch hat sich gezeigt, dass das Konzept Oracle Standard in Bezug auf die getrennte Administrierbarkeit als auch auf die sichere Trennung voneinander nicht alle Erwartungen erfüllt, insb. im direkten Vergleich mit SAP Classic. Beispielsweise gehören alle Datenbankdateien verschiedener Datenbanken dem Benutzer oracle, die Instanzprozesse aller Instanzen gehören oracle, und beim Einspielen von Patches in ein Oracle Home ist nicht gewährleistet, dass nicht versehentlich ein anderes Oracle Home bearbeitet wird.

Als Antwort auf diese konzeptuellen Schwächen von Oracle Standard wurde ein erweitertes, flexibles Benutzerkonzept entwickelt, eine Kombination von SAP Classic und Oracle Standard: Oracle Flex.

Der wichtigste Unterschied liegt beim Softwareeigentümer: im Gegensatz zu Oracle Standard gibt es für jede Datenbank <DBSID> einen eigenen Softwareeigentümer orcl<dbSID>. Auf diese Weise ist sichergestellt, dass die Prozesse der Oracle-Instanz von Datenbank <DBSID> sich in der Prozessliste eindeutig zuordnen lassen. Der Benutzer orcl<dbSID> ist als Softwareeigentümer Mitglied der primären Gruppe oinstall und außerdem der sekundären Gruppen dba<dbSID> und oper<dbSID> (statt dba bzw. oper wie bei SAP Classic oder Oracle Standard). Durch die datenbankspezifischen Gruppen dba<dbSID> bzw. oper<dbSID> ist auch bei Installation mehrerer Datenbanken auf einem

Datenbankserver gewährleistet, dass über das Betriebssystem keine Authentifizierung mit SYSDBA oder SYSOPER-Rechten an eine andere Datenbank als an <DBSID> erfolgen kann. Die Zugehörigkeit zur Gruppe oinstall als primäre Gruppe kennzeichnet den Benutzer als Softwareeigentümer und macht das Benutzerkonzept kompatibel zu Oracle Standard.

Der Benutzer <sapsid>adm ist auch hier der Benutzer für die SAP-System-Administration sowie für den operativen Betrieb der Oracle Datenbank. So wie bei Oracle Standard ist dieser Benutzer auch der standardmäßige Benutzer für die Oracle-Datenbank-Administration. Mit diesem Benutzer können alle SAP BR\*Tools-Programme ausgeführt werden. Zum Ausführen der BR\*Tools ist der Benutzer Mitglied der Gruppe oinstall. Die administrativen Rechte SYSDBA bzw. SYSOPER erhält der Benutzer über die sekundären Gruppen dba<dbsid> und oper<dbsid>.

Der Benutzer ora<dbsid> ist analog zu <sapsid>adm Mitglied der Gruppen dba<dbsid>, oper<dbsid> und oinstall, besitzt also betriebssystemseitig die notwendigen Gruppen, um die Datenbank als SYSDBA zu administrieren und die BR\*Tools-Programme zu verwenden.

Genauso wie beim Benutzerkonzept Oracle Standard haben sowohl <sapsid>adm also auch ora<dbsid> jeweils die notwendigen Umgebungsvariable für die Oracle Datenbank <DBSID> und die SAP BR\*Tools bereits standardmäßig vorkonfiguriert (ORACLE\_BASE, ORACLE\_HOME, ORACLE\_SID, DB\_SID, SAPDATA\_HOME). Im Unterschied zu Oracle Standard hat aber auch der Softwareeigentümer orcl<dbsid> diese Umgebungsvariable gesetzt. Dadurch wird gewährleistet, dass ein Patch nicht versehentlich in das falsche Oracle Home eingespielt wird.

Die folgende Tabelle zeigt die einzelnen Benutzer und deren Konfiguration im Überblick:

<b>&lt;sapsid&gt;adm</b>	<b>orcl&lt;dbsid&gt;</b>	<b>ora&lt;dbsid&gt;</b>
SAP Administrator Oracle Database Administrator	Oracle Software Eigentümer Oracle Database Administrator	Oracle Database Administrator User für SAP Host Agent
Primäre Gruppe: sapsys	Primäre Gruppe: oinstall	Primäre Gruppe: dba<dbsid>
Gruppen: dba<dbsid>, oper<dbsid>	Gruppen: dba<dbsid>, oper<dbsid>	Gruppen: oper<dbsid>
Env: ORACLE_SID, ORACLE_HOME, ORACLE_BASE, SAPDATA_HOME, DB_SID	Env: ORACLE_SID, ORACLE_HOME, ORACLE_BASE, SAPDATA_HOME, DB_SID	Env: ORACLE_SID, ORACLE_HOME, ORACLE_BASE, SAPDATA_HOME, DB_SID
BR*Tools : ja	BR*Tools : ja	BR*Tools : ja

Wie aus der Beschreibung bereits hervorgeht, sind die Nachteile von Oracle Standard beim Einsatz mit SI/FS bei Oracle Flex nicht mehr vorhanden. Wenn mehrere Datenbanken auf demselben Datenbankserver installiert sind, lassen sie sich jederzeit sicher voneinander getrennt administrieren und identifizieren.

Das Konzept läßt viele Verwendungsmöglichkeiten zu: die Datenbankadministration kann über den Benutzer <sapsid>adm erfolgen, der Benutzer ora<dbid> muss nicht zwingend verwendet werden. Wenn jedoch eine Trennung zwischen SAP- und Oracle-Administration gefordert ist, dann ist das möglich. Durch die beiden Benutzer ora<dbid> und orcl<dbid> ist es möglich, Softwareinstallation und Datenbankadministration als separate Aufgaben auch über getrennte Benutzer zu separieren. Als weitere Option ist es möglich, mit dem Benutzer orcl<dbid> - wie bei SAP Classic- sowohl die Software zu installieren als auch die Datenbank zu administrieren.

## Referenzen

SAP Hinweise
1914631 - Zentralhinweis mit technischen Informationen zu Oracle Database 12c Release 1 (12.1)
1915317 - Migration des Software-Eigentümers zu 'oracle'
1915323 - OS User Concept for Oracle Database 12c and higher
1915324 - How to find the ORACLE_HOME of a running Oracle Database Instance
1930298 - Zugriff auf Softwareeigentümer "oracle" einschränken
1598594 - BR*Tools-Konfiguration für Oracle-Installationen unter "oracle"-User
1554661 – Konfiguration der Umgebung für den Benutzer ‚oracle‘
1710997 - Using Personalized Database Administrator Accounts
1755636 - Database Administrators Segregation
135772 - Konfiguration von BR-Programmen in ORACLE-Umfeld

### Kontaktadresse:

Andreas Becker  
Oracle Deutschland B.V. & Co. KG  
Riesstr. 25  
D-80992 München  
E-Mail [andreas.becker@oracle.com](mailto:andreas.becker@oracle.com)  
Internet: [www.oracle.com/sap](http://www.oracle.com/sap)