Einer für Alle

-

Verbindungen an die Datenbank mit "connect through"

Jens Behring
ist-people GmbH
Frankfurt am Main

Schlüsselworte
Oracle, Proxyuser, Connect through

Einleitung

Der Umzug einer Datenbank in eine Regelbetriebsführung bringt die eine oder andere Umstellung mit sich. Neben architektonischen Vorgaben zu Tablespaces und div. Vorgaben zu Objektnamen und Programmierrichtlinien für PL/SQL - nur um hier eine kleine Auswahl zu nennen – sind auch Regeln hinsichtlich Zugriffsrechten und Kennwortkriterien einzuhalten. Speziell diesem letztgenannten Teil widmet sich dieser Vortrag.

Warum?

Die Idee zu diesem Vortrag entstand im Rahmen des Umzugs einer durch die Fachabteilung betriebsgeführten Datenbank in die Regelbetriebsführung eines IT-Dienstleisters. In diesem Zusammenhang mussten einige Vorgaben des Dienstleisters eingehalten werden. Von diesen Vorgaben sind folgend im Rahmen des Vortrages von Interesse:

- Der Zugriff auf die Datenbank erfolgt nicht mit dem Usernamen des Objekteigentümers
- Der Zugriff direkt auf die Datenbank erfolgt ausschließlich mit persönlichen Nutzern
- Es gilt die Kennwortrichtlinie des Dienstleisters. Diese sieht kryptische Kennwörter vor, die sich auch zwischen den verschiedenen Instanzen (Entwicklung, Test, Abnahme, Produktion) unterscheiden)

Vor dem Umzug gab es keine persönlichen Nutzer. Dies hatte zur Folge, dass Datenänderungen unter einem anonymen Datenbanknutzer durchgeführt wurden. In solchen Fällen ist auch die Hemmschwelle niedrig, Zugangsdaten weiterzugeben, da keinerlei persönliche Information in diesen Zugangsdaten enthalten ist. Darüber hinaus war die bis dahin verwendete Kennwortregel relativ berechenbar, so dass von den Zugangsdaten eines Nutzers relativ einfach auf die Zugangsdaten eines anderen Nutzers Rückschlüsse möglich waren. Da sich die Kennwörter zwischen den Instanzen nicht unterschieden haben, war damit einem Zugriff auf Produktionsdaten Tür und Tor geöffnet.

Da auch im produktiven Umfeld aber eine Vielzahl von SQL-Skripten existiert, die erst im Rahmen einer Konsolidierungsphase im Anschluss an den Umzug abgelöst werden sollen, bestand und besteht die Notwendigkeit, Anwendern auch im Umfeld der Regelbetriebsführung den Zugang an die Datenbank zu ermöglichen. Innerhalb dieser Skripte werden u.a. regelmäßig „Spatial Indexes“ gelöscht und neu angelegt. Dies muss zwingend unter dem Schema erfolgen, welches der Eigentümer

des Spatial Indexes ist. Hier galt es, die Anforderungen des IT-Dienstleisters mit den Anforderungen der Fachseite in Übereinstimmung zu bringen.

Die Idee

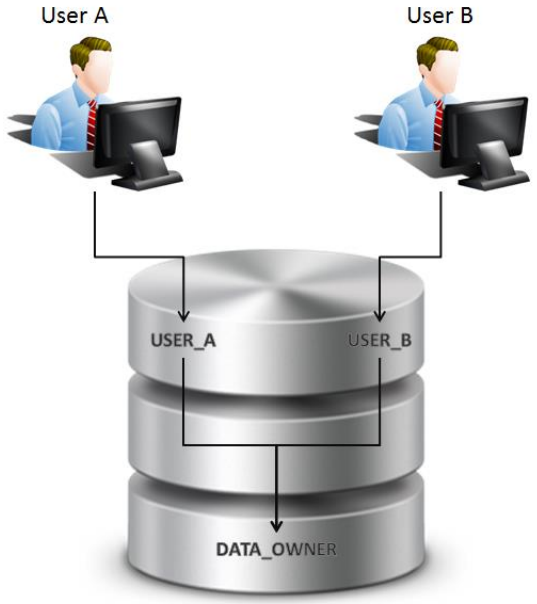
Um nun einerseits die Anforderungen des Dienstleisters erfüllen zu können, andererseits aber auch Szenarien, wie z.B. eine Post-It-Sammlung mit neuen Kennwörtern an Monitoren zu verhindern, wurden div. Szenarien untersucht. Speziell die Anforderung, dass Skripte wegen der Spatial Indexes unter dem Schema des Objekteigentümers laufen müssen, verhinderte eine Lösung, die nur mit Berechtigungen funktioniert.

In diesem Zusammenhang wurde die Möglichkeit des sog. „connect through“ mit Hilfe eines sog. Proxynutzers in Oracle Datenbanken (wieder-)entdeckt, deren Nutzung einigen Bedenken ausräumen sowie die geforderten Funktionalitäten ermöglichen konnte.

Diese Lösungsidee hat Ihren Ursprung eigentlich im Bereich der mehrschichtigen Architekturen, bei denen Nutzer evtl. sogar außerhalb der Datenbank authentifiziert wurden. In diesen Fällen wird dafür gesorgt, dass ein durch einen Application Server verwendeter Nutzername lediglich das Recht CREATE SESSION erhält und jede weitere Berechtigung über den Session Nutzer vergeben wird. Damit wird verhindert, dass ein Nutzer, der wie in obigem Beispiel für einen Application Server genutzt wird, zu viele Rechte an Daten und Funktionalitäten in einer Datenbank erhält. Die hier vorgestellte Lösung betrachtet also nur einen Teil dessen, wofür Proxynutzer eigentlich genutzt werden können.

Die Funktionalität

Ein Proxynutzer bietet die Möglichkeit, sich via eines dem Anwender bekannten Nutzers als ein weiterer Nutzer an der Datenbank anzumelden. Hierbei dient der Proxynutzer lediglich zur Authentifizierung. Die Möglichkeit als Proxynutzer zu dienen, muss natürlich als Berechtigung vergeben werden. Der prinzipielle Vorgang kann folgender Abbildung entnommen werden.



Hierbei muss noch einmal darauf hingewiesen werden, dass es sich beim Zugriff auf das Schema DATA_OWNER nicht um „normale“ GRANTs handelt.

Zunächst wird ein Schema benötigt, welches die Daten vorhält, die später selektiert werden:

```
create user data_owner identified by nobody_knows;
```

In diesem Schema wird nun eine Tabelle mit Daten angelegt:

```
  create table data_owner.important_data
    ( id number
    , value varchar2 (5) );
  insert into data_owner.important_data values ( 1, 'one' );
  insert into data_owner.important_data values ( 2, 'two' );
  commit;
```

Nun wird ein Nutzer benötigt, der als Proxynutzer fungieren kann:

```
  create user jens identified by secret;
  grant create session to jens;
```

Dieser bisher „normale“ Nutzer benötigt nun noch das Recht, als Proxynutzer verwendet werden zu dürfen. Dies geschieht über eine ALTER USER-Anweisung:

```
  alter user data_owner grant connect through jens_as_proxy;
```

Nun sind die Voraussetzungen für einen ersten Test erfüllt. Da das Kennwort von DATA_OWNER niemand kennt, soll die Verbindung über den Proxynutzer erfolgen. Dies geschieht mit Hilfe des folgenden Connect-Strings:

```
  connect jens[data_owner]/secret@datenbank
```

Die Eingabe von SHOW USER zeigt dann folgendes:

```
>  show user

USER ist “DATA_OWNER”
```

Damit ist klar, dass, obwohl das Kennwort von DATA_OWNER nicht bekannt ist, dem Nutzer JENS die Möglichkeit gegeben wurde, sich als DATA_OWNER an die Datenbank zu verbinden. Hier bieten sich nun alle Möglichkeiten, um als Nutzer DATA_OWNER zu arbeiten. Alle Rechte, die der sog. SESSION OWNER hat, stehen zur Verfügung. Es können Daten verändert und Funktionalitäten aufgerufen werden.

Oracle bietet natürlich die Möglichkeit, sowohl den SESSION USER als auch den PROXY USER herauszufinden. Folgende Eingabe liefert das gleiche Ergebnis, wie zuvor die Abfrage SHOW USER:

```
>  select sys_context('userenv', 'session_user') from dual;

SYS_CONTEXT('USERENV','SESSION_USER')
--------------------------------------------------------------------------------
DATA_OWNER
```

Der verwendete Proxynutzer lässt sich mit folgender Anfrage ermitteln:

```
>  select sys_context('userenv', 'proxy_user') from dual;

SYS_CONTEXT('USERENV','PROXY_USER')
--------------------------------------------------------------------------------
JENS
```

Der Data Dictionary View DBA_PROXIES können Informationen zu allen Proxy Benutzern entnommen werden.

Fazit

Auch wenn die verwendete Idee eher im Bereich mehrschichtiger Architekturen zu Hause ist –in einem reinen Datenbankumfeld gibt es durchaus Verwendungsmöglichkeiten für Proxynutzer. Ein Proxynutzer bietet die Möglichkeit, sich via eines dem Anwender bekannten Nutzers als ein weiterer Nutzer an der Datenbank anzumelden. Hierbei dient der Proxynutzer lediglich zur Authentifizierung. Mit Hilfe dieser Lösung war es im konkreten Fall möglich, die Datenbank in eine Betriebsführung beim IT-Dienstleister zu migrieren, ohne im Vorfeld bereits alle existierenden Prozesse einem regelkonformen Redesign zu unterziehen, welches den Zeitpunkt der Migration um mehrere Jahre nach hinten verschoben hätte. Durch die verwendete Lösung soll natürlich ein Redesign nicht verhindert werden – anders herum kann es aber auch nicht sein, dass ein veralteter Hardware geschuldeter Umzug nicht vollzogen werden kann, weil Vorgaben einer Betriebsführung in Ihrer Umsetzung mehrere Monate oder sogar Jahre in Anspruch nehmen.

In einem weiteren Schritt wird nun untersucht, die „WITH ROLE“-Klausel zu nutzen, die die Rollen einschränkt, die ein so verbundener Benutzer aktivieren darf. Hierzu wird es im November hoffentlich erste Ergebnisse geben, die im Rahmen der DOAG präsentiert werden.

Kontaktadresse:

Jens Behring
its-people GmbH
Lyoner Straße 44-48
D-60528 Frankfurt am Main

Telefon:	+49 (69) 247 521 00
Mobil:	+49 (172) 782 41 37
E-Mail	jens.behring@its-people.de
Internet:	www.its-people.de