Oracle Database Vault for Beginners

Heinz-Wilhelm Fabry
Oracle Deutschland B.V. & Co. KG
München

Schlüsselwörter:

Oracle Database Vault, Realm, Faktor, Regelgruppe, Regel, Befehlsregel, Sichere Anwendungsrolle, Funktionstrennung und Aufgabenverteilung

Einleitung

Dieser Beitrag versteht sich nicht als Implementierungs- oder Installationsanleitung. Vielmehr sollen die Komponenten von DV so beschrieben werden, dass zwei wichtige Aspekte nachvollziehbar werden: Warum wirkt sich DV auf Anwendungen nicht aus? Und warum wirkt DV sich auf die Datenbankadministration nur insofern aus, als dass einige Routinearbeiten aus Sicherheitsgründen etwas anders ausgeführt werden als in Datenbanken, die nicht mit DV arbeiten.

Was ist eigentlich das Problem?

Datenbanken bieten von sich aus bereits Schutz für die darin abgelegten Daten: Diese sind nur dann les- oder änderbar, wenn man sich in die Datenbank einloggen kann und zusätzlich der Zugriff auf die Daten in irgendeiner Form explizit erlaubt ist (*discretionary access control*). Für einen beträchtlichen Teil aller in Datenbanken abgelegten Daten reicht dieser Schutz aus. Aber es gibt auch unternehmens-, branchen- und gesetzesspezifische Regelwerke, die für bestimmte Daten einen stärkeren Schutz verlangen. Für ein branchenspezifisches Beispiel steht hier der Payment Card Industry Data Security Standard (PCI DSS), als gesetzespezifisches Beispiel das Bundesdatenschutzgesetz (BDSG).

Der stärkere Schutz wird in erster Linie durch technische Massnahmen implementiert: Daten werden z.B. verschlüsselt, oder der Zugriff darauf wird zusätzlich durch die Einbeziehung von Parametern aus der Umgebung der Anwender gesteuert (*mandatory access control*). In Oracle Datenbanken ist das unter anderem mit Transparent Data Encryption (TDE) und Virtual Private Database (VPD) umgesetzt. Problematisch sind in diesem Zusammenhang allerdings privilegierte Benutzer, also vor allem die Datenbankadministratoren (DBAs) und ganz besonders der Benutzer SYS. Mit ihren Privilegien können sie alle technischen Sicherheitsmaßnahmen unterlaufen.

Weil es technisch keine Möglichkeit gab, Missbrauch zu verhindern, mußten Arbeitsanweisungen oder Ergänzungen zum Arbeitsvertrag, in denen der Missbrauch untersagt und sanktioniert wurde, als eine Art Ersatz akzeptiert werden. DV bietet nun die Möglichkeit, weg von diesem Ersatz und hin zu einer technischen Einschränkung der Privilegien privilegierter Benutzer zu kommen.

Die Basis: Mehr Sicherheit durch Teamwork

DV unterstützt technisch das im Sicherheitsumfeld selbstverständliche Prinzip der Funktionstrennung und Aufgabenverteilung. Schon bei der Installation der Option werden zwei zusätzliche Rollen vergeben, die eine systemseitige erste Implementierung des Prinzips festlegen.

Die erste Rolle heißt DV_OWNER. Sie befähigt ausschließlich dazu, die Komponenten des DV zu administrieren. Ein Zugriff auf Objekte, die durch die Komponenten geschützt werden, ist mit der Rolle nicht möglich. Neben den Rechten zur Verwaltung der DV Komponenten beinhaltet die Rolle außer CREATE SESSION nur die Systemprivilegien ADMINISTER DATABASE TRIGGER, ALTER ANY TRIGGER und GRANT ANY ROLE. Die Rolle DV_OWNER macht also niemanden zum neuen Super-DBA.

Die zweite Rolle, die bei der Installation vergeben wird, heißt DV_ACCTMGR. Sie kann der Person mit der Rolle DV_OWNER zugewiesen werden oder einer anderen Person. Oracle empfiehlt, die beiden Rollen auf zwei Personen zu verteilen.

Nur ein Benutzer mit der Rolle DV_ACCTMGR kann Profile und Benutzer anlegen sowie Passwörter ändern. Damit werden gleich zwei Sicherheitslücken geschlossen. Zum einen können sich DBAs kein 'Hintertürchen' (*back door*) mehr in einer Datenbank einrichten. Zum zweiten können DBAs auch kein Passwort mehr ändern, um sich dann unter einem anderen Benutzernamen einzuloggen. DV_ACCTMGR hat neben dem Privileg CREATE SESSION nur die Privilegien CREATE / ALTER / DROP USER sowie CREATE / ALTER / DROP PROFILE. Wie im Fall der Rolle DV_OWNER macht also auch die Rolle DV_ACCTMGR niemanden zu einem neuen Super-DBA.

Damit ist die grundsätzliche Aufgabenverteilung in einer mit DV geschützten Datenbank komplett: Die Strukturen des Vault verwaltet ein Benutzer mit der Rolle DV_OWNER, die Benutzerverwaltung erfolgt gemeinsam durch Benutzer mit den Rollen DV_ACCTMGR und DBA. Alles Andere liegt nach wie vor in den Händen der DBAs und des Superuser SYS.

Es ist technisch übrigens durchaus möglich, einem DBA die DV Rollen zuzuweisen. Allerdings unterläuft man damit einen der wesentlichen Sicherheitsvorteile, den der Einsatz von DV bietet.

Ein wenig härter muß es sein

Alle Objekte, die DV benötigt oder die innerhalb von DV angelegt werden, gehören den Benutzern DVSYS und DVF. Die Benutzer werden bei der Installation von DV angelegt und gesperrt (*account lock*). Der Zugriff auf die Objekte der beiden Benutzer erfolgt entweder über Rollen oder darüber, dass in Frage kommende Objekte für den Zugriff für den Benutzer PUBLIC freigegeben werden.

Neben der Funktionstrennung und Aufgabenverteilung durch die Vergabe von Rollen werden im Rahmen der Installation Änderungen bei Privilegien und Initialisierungsparametern vorgenommen. Abbildung 1 zeigt die Veränderungen bei den Benutzern PUBLIC, SYS und SYSTEM.

PUBLIC	EXECUTE ON UTL_FILE
SYS	ALTER PROFILE ALTER USER CREATE PROFILE CREATE USER DROP PROFILE DROP USER
SYSTEM	ALTER PROFILE ALTER USER CREATE PROFILE CREATE USER DROP PROFILE DROP USER

Abb. 1: Im Rahmen der DV Installation geänderte Benutzer

Abbildung 2 zeigt, welche Privilegien welchen Rollen genommen werden.

DBA	BECOME USER SELECT ANY TRANSACTION CREATE ANY JOB CREATE EXTERNAL JOB EXECUTE ANY PROGRAM EXECUTE ANY CLASS MANAGE SCHEDULER DEQUEUE ANY QUEUE ENQUEUE ANY QUEUE MANAGE ANY QUEUE
IMP_FULL_DATABASE	BECOME USER MANAGE ANY QUEUE
EXECUTE_CATALOG_ROLE	EXECUTE ON DBMS_LOGMNR EXECUTE ON DBMS_LOGMNR_D EXECUTE ON DBMS_LOGMNR_LOGREP_DICT EXECUTE ON DBMS_LOGMNR_SESSION EXECUTE ON DBMS_FILE_TRANSFER
SCHEDULER_ADMIN	CREATE ANY JOB CREATE EXTERNAL JOB EXECUTE ANY PROGRAM EXECUTE ANY CLASS MANAGE SCHEDULER

Abb. 2: Im Rahmen der DV Installation geänderte Rollen

Wenn sie nicht bereits so gesetzt sind, wie es DV erwartet, werden fünf Initialisierungsparameter umgesetzt.

- AUDIT_SYS_OPERATIONS wird auf TRUE gesetzt. Damit werden alle Aktionen des nach wie vor sehr mächtigen Benutzers SYS auditiert.
- OS_ROLES wird auf FALSE gesetzt. Damit liegt die Rollenverwaltung der Benutzer auf jeden Fall in der Datenbank.
- RECYCLE_BIN wird auf OFF gesetzt. Damit kann der Zugriff auf schützenswerte Tabellen auch nach einem DROP TABLE nicht unterlaufen werden.
- SQL92_SECURITY wird auf TRUE gesetzt. Damit ist das Recht auf UPDATE und / oder DELETE nur dann durchzusetzen, wenn auch das SELECT Recht vorliegt.
- REMOTE_LOGIN_PASSWORDFILE wird auf EXCLUSIVE gesetzt. Diese Einstellung ist nötig, weil DV mit Password Dateien arbeitet.

Es ist klar, dass die Veränderungen sich auf das alltägliche Arbeiten mit der Datenbank auswirken. So ist der Import von Tabellen eines anderen Benutzers durch das nicht mehr vorhandene Privileg BECOME USER in der Rolle IMP_FULL_DATABASE nicht mehr ohne Weiteres möglich. Ein solcher Import soll aber natürlich nicht grundsätzlich unmöglich sein, sondern es soll lediglich sicher sein, dass ein Import nur noch kontrolliert stattfindet. In älteren Versionen von DV musste man dazu selbst Privilegien etc. umsetzen. In Oracle Database 11*g* Release 2 stellt das System zwei Prozeduren zur Verfügung, die alle nötigen Änderungen durchführen bzw. rückgängig machen: DBMS_MACADM.(UN)AUTHORIZE_DATAPUMP_USER. Das System stellt ähnliche Mittel zur Verfügung, um das kontrollierte Arbeiten mit dem Scheduler und Streams oder das Patchen und Monitoring zu erleichtern.

Alle Änderungen bei Privilegien und Parametern bewirken ein zusätzliches Härten der Datenbank. Diese Änderungen können bei Bedarf rückgängig gemacht werden. Allerdings sollte das nicht leichtfertig geschehen, sondern mit Blick darauf, welche Implikationen das für die Sicherheit hat. Ergänzt sei hier auch noch, dass bei einer eventuellen De-Installation von DV zwar die Privilegien der Rollen und Benutzer wieder auf ihren ursprünglichen Defaultwert zurückgesetzt werden, die Initialisierungsparameter allerdings nicht.

Auch das Auditing wird im Rahmen des Härtens ausgedehnt. Es werden deutlich mehr Statements auditiert. Allerdings ist hier der DBA gefordert, der das Auditing über den Parameter AUDIT_TRAIL so setzen muß, dass die mit dem Befehl AUDIT genannten Befehle tatsächlich auditiert werden.

DV zur Steuerung des Zugriffs auf Benutzerdaten

Abbildung 3 zeigt anhand des Eingangsbildschirms der Verwaltungskonsole des DV, dem Database Vault Administrator (*dva*), welche Features DV zur Steuerung des Zugriffs auf Benutzerdaten zur Verfügung stellt. Zugriff auf die Konsole und damit Zugriff auf die Konfiguration des DV haben ausschließlich Benutzer mit der Rolle DV_OWNER oder mit der durch DV_OWNER zu vergebenden Hilfsrolle DV_ADMIN. Die Konsole ist auch aus dem Enterprise Manager heraus direkt aufrufbar und soll zukünftig vollständig in den Enterprise Manager integriert werden. Neben dieser graphischen Oberfläche gibt es auch einen Kommandozeilenmodus für das Arbeiten mit DV.

Abb. 3: Database Vault Administrator (dva)

Um das Verständnis zu erleichtern und das Zusammenspiel der unterschiedliche Features deutlicher zu machen, folgt die Beschäftigung mit den einzelnen Features nicht der Reihenfolge in der Liste des *dva*. Ausserdem konzentriert sich die Beschäftigung auf die für DV insgesamt sicher wichtigeren Bereiche Realms, Faktoren, Regelgruppen und Befehlsregeln und behandelt die Bereiche Label Security Integration, Sichere Anwendungsrollen und Berichte nur sehr knapp.

Realms

Ein Realm ist ein logischer Container für Datenbankobjekte wie Schemas, Tabellen, Packages und Rollen. Das Anlegen eines Realms und die Zuweisung von Objekten zu einem Realm erfolgen deklarativ und können ausschließlich durch Benutzer mit der Rolle DV_OWNER oder DV_ADMIN erfolgen. Der Zugriff auf Realm-geschützte Objekte ist nur für den Eigentümer der Objekte möglich oder wenn explizite GRANTs dazu ermächtigen. Jeder Versuch, mit einem ANY Privileg auf ein Realm-geschütztes Objekt zuzugreifen, führt zur Fehlermeldung *ORA-01031: insufficient privileges*.

Weil sie standardmäßig über ANY Privilegien auf Objekte zugreifen, wird so Personen mit der Rolle DBA und auch dem Benutzer SYS der Zugriff auf Objekte eines Realms grundsätzlich verwehrt. Auf der anderen Seite müssen Anwendungen, die auf diese Objekte über explizite GRANTs zugreifen, NICHT geändert werden. Das erklärt auch, warum z.B. die Content Database und auch die großen Anwendungspakete von Oracle - Siebel, Peoplesoft, E-Business Suite, JD Edwards EnterpriseOne, iFlex - sowie SAP sehr zügig für die Verwendung mit DV zertifiziert werden konnten.

Zur Standardinstallation von DV gehören 4 Realms: Data Dictionary, Enterprise Manager, Database Vault und Database Vault Account Management. Diese Realms sichern die zentralen Objekte der Datenbank. Für jedes Realm gibt es einen sogenannten *Owner*, der vollen Zugriff auf alle Objekte des Realms hat - sofern er zusätzlich die notwendigen Objektprivilegien in irgendeiner Form hat - explizit durch GRANT oder im Rahmen eines ANY Privilegs. Im Fall des Realms Data Dictionary ist der *Owner* SYS, *Owner* von Enterprise Manager sind SYSMAN, DBSNMP und SYSTEM, von Database Vault unter anderem DV_OWNER und von Database Vault Account Management DV_ACCTMGR.

Die mitgelieferten Realms können Auswirkungen auf administrative Routinetätigkeiten haben. Denn wer etwa gewohnt ist, als SYSTEM mit Data Pump zu arbeiten, wird zunächst auf einen Fehler laufen, selbst wenn SYSTEM mit der o.g. Prozedur authorisiert wurde, einen Export durchzuführen. Das liegt daran, dass Data Pump die *Master Table* für den Export im Default Tablespace desjenigen Benutzers anlegt, der den Export anstößt. Für SYSTEM wird also versucht, die *Master Table* im Tablespace System anzulegen. Da aber das Tablespace System zum Realm Data Dictionary gehört, hat SYSTEM darauf zunächst keinerlei Zugriffsrechte. Will man nicht mit einem anderen Benutzer arbeiten, dessen Default Tablespace nicht System ist - das ist eigentlich die empfohlene Vorgehensweise - könnte man entweder SYSTEM dem Realm Data Dictionary als weiteren *Owner* hinzufügen oder man nutzt die andere verfügbare Berechtigung für das Arbeiten innerhalb eines Realms, man fügt SYSTEM als *Participant* dem Realm hinzu. Während ein *Owner* im Rahmen seiner Objektprivilegien vollen Zugriff auf die Objekte eines Realms hat, kann ein *Participant* zwar alle seine Objektprivilegien in einem Realm verwenden, allerdings kann ein *Participant* keine GRANTs auf die Objekte im Realm vergeben.

Faktoren

Die Bezeichnung Faktoren ist etwas irreführend. Es handelt sich bei Faktoren um Datenstrukturen, die man zum besseren Verständnis eher als Variablen bezeichnen kann. Dabei handelt es sich zunächst um die in Abbildung 4 gezeigten mitgelieferten Umgebungsvariablen.

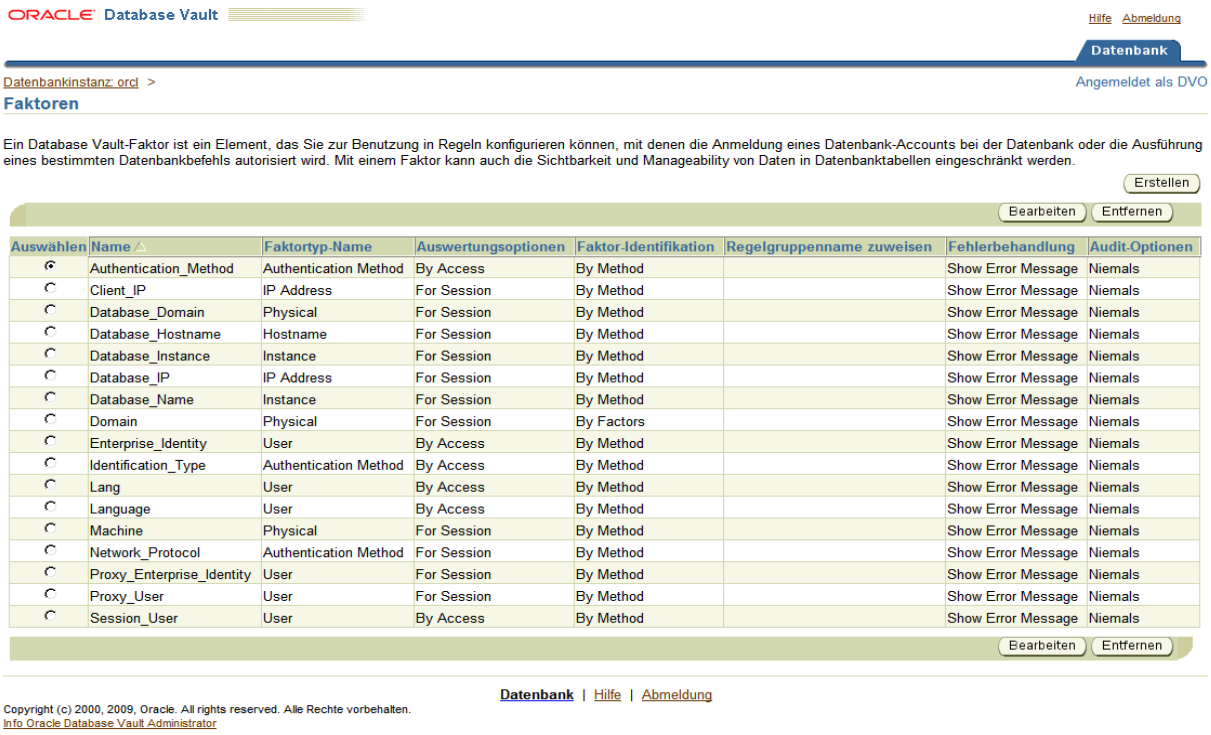

Abb. 4: DV Faktoren

Die mitgelieferten Umgebungsvariablen können auch zu neuen Variablen zusammengesetzt werden. Aber es können sogar völlig eigene Variablen definiert werden, deren Wert berechnet oder über eine Konstante festgesetzt wird. Alle Variablen können zusätzlich über sogenannte Trust-Ebenen gewichtet werden. Die Variablen können durch Anwendungen gesetzt und abgefragt werden, so dass über die Variablen der Zugriff auf Objekte der Datenbank und auf Objekte von DV gesteuert werden kann. Der Vorteil der mitgelieferten Variablen gegenüber den aus VPD bekannten *application contexts* ist, dass sie alle durch DV vor Manipulationen durch privilegierte Benutzer geschützt sind.

Die Variablen / Faktoren werden in Regeln ausgewertet, die der Einfachheit halber in sogenannten Regelgruppen gespeichert sind.

Regelgruppen

Regelgruppen bieten die Möglichkeit, Regeln anzulegen, die für die Aktionen in einer DV gesicherten Datenbank ausgewertet werden. Eine Regel ist eine WHERE-Klausel, die entweder zu TRUE oder FALSE ausgewertet werden kann. Ist für eine Aktion die Auswertung einer Regelgruppe vorgesehen, wird die Aktion nur dann ausgeführt, wenn die Auswertung einer Regel oder aller Regeln der Regelgruppe den Wert TRUE ergibt (*all / any true*). Eine Aktion kann verhindert werden, wenn auch nur eine Regel mit dem Ergebnis FALSE ausgewertet wird. Abbildung 5 zeigt als Beispiel die einzige Regel, die zur mitgelieferten Regelgruppe *Disabled* gehört. Die mögliche Komplexität einer solchen Regel und das mögliche Zusammenspiel unterschiedlicher Regeln in einer Regelgruppe ist nur begrenzt durch die SQL Kenntnisse desjenigen, der die Regeln schreibt.

Bei der Installation von DV werden neben den Regelgruppen *Disabled* und *Enabled* eine Reihe weiterer Gruppen angelegt, die DV auch intern verwendet. Diese Regelgruppen können zwar auch für Benutzerzwecke verwendet und verändert werden, allerdings sollte dabei größte Umsicht walten.

Abb. 5:Regel False *der Regelgruppe* Disabled

Befehlsregeln

DV erlaubt, die Ausführung von beliebigen SQL Befehlen vom Ergebnis einer Auswertung von Regelgruppen abhängig zu machen. So können Befehle für die gesamte Datenbank, für ein bestimmtes Schema oder für ein bestimmtes Objekt kontrolliert werden - und diese Kontrolle gilt ausnahmslos auch für alle privilegierten Benutzer. Ein ganz einfaches Beispiel zeigt Abbildung 6. Nachdem die Regelgruppe *Disabled* und ihre Regel *False* mit dem Befehl DROP TABLE für das Schema SCOTT verknüpft wird, ist dieser Befehl in dem Schema von niemandem mehr auszuführen.

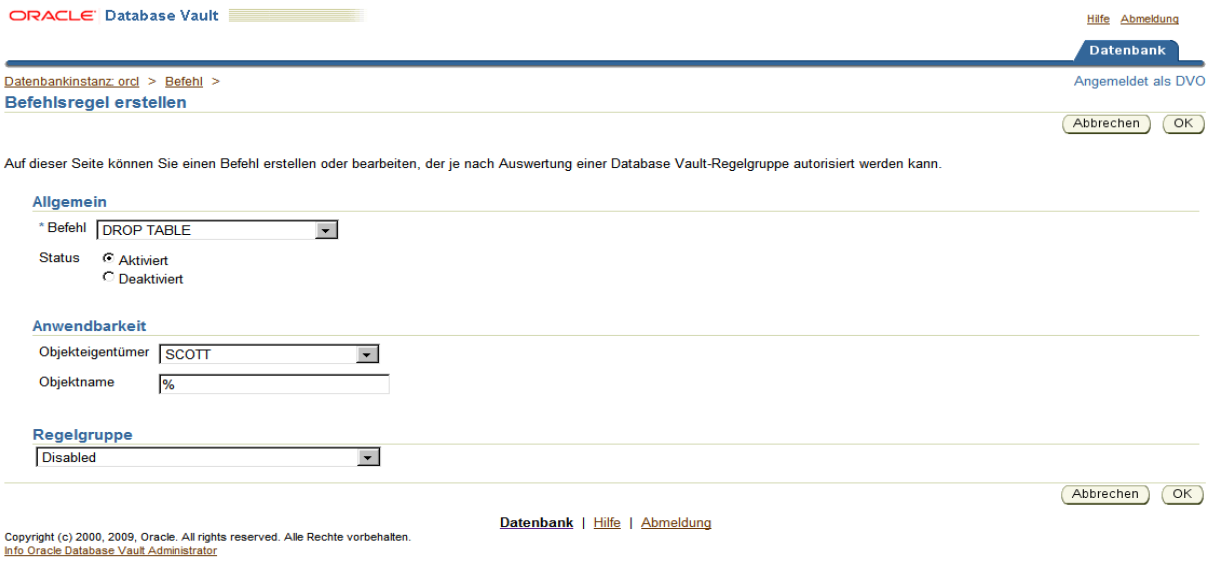

Abb. 6: Befehlsregel für DROP TABLE *im Schema von* SCOTT

Bei der Installation von DV werden einige Befehlsregeln angelegt, die DV intern verwendet. So werden die Befehle CREATE USER und CREATE PROFILE, die ja auschließlich von Benutzern mit der Rolle DV_ACCTMGR ausgeführt werden dürfen, über vorkonfigurierte Befehlsregeln kontrolliert. Diese Befehlsregeln können - ebenso wie die Regelgruppen - zwar auch für Benutzerzwecke verwendet und verändert werden, allerdings sollte auch hier größte Umsicht walten.

Integration Label Security / Sichere Anwendungsrollen

Abschließend soll kurz auf die Oracle Label Security (OLS) Integration und auf die sicheren Anwendungsrollen eingegangen werden. OLS kann verwendet werden, um Faktoren zusätzlich Labels zuzuweisen. Damit ist der Zugriff auf diese Faktoren in einer Datenbank, die OLS einsetzt, noch differenzierter zu steuern. Bei der Installation von DV werden keine Labels angelegt.

Es werden auch keine sicheren Anwendungsrollen angelegt. Solche Rollen müssen bei Bedarf durch den DV_OWNER bzw. DV_ADMIN deklariert werden. Sie sind durch DV geschützt, denn sie können nicht durch das bekannte DBMS_SESSION.SET_ROLE aktiviert werden wie die bereits seit längerem bekannten Secure Application Roles ausserhalb von DV. Vielmehr werden sie durch den Aufruf der DV spezifischen Prozedur DBMS_MACSEC_ROLES.SET_ROLE aktiviert. Dieses SET_ROLE führt zur Auswertung einer für diese Rolle zuvor zu definierenden Regelgruppe. Nur wenn die Auswertung zum Wert TRUE führt, wird die Rolle tatsächlich aktiviert. Wichtig ist auch hier die Zusammenarbeit mit DBAs oder Objekteigentümern, denn die Privilegien einer DV Rolle werden von ihnen und nicht vom DV_OWNER oder DV_ADMIN festgelegt.

Berichte

Im Lieferumfang sind eine ganze Reihe von Berichten enthalten, die das Monitoring einer mit DV abgesicherten Datenbank erleichtern. Sie erlauben die Kontrolle der Konfiguration der in DV angelegten Objekte und die Auswertung der DV spezifischen Audit Einträge. Schließlich sind auch eine ganze Reihe von Berichten über allgemeine sicherheitsrelevante Themen verfügbar, z.B. der in Abbildung 7 gezeigte Bericht über Personen und Rollen mit bestimmten Systemprivilegien.

Abb. 7: Beispielbericht

Kontaktadresse:

Heinz-Wilhelm Fabry
Oracle Deutschland B.V. & Co. KG
Riesstr. 25
D-80992 München

Telefon: +49 (0) 89-1430 1534
E-Mail heinz-wilhelm.fabry@oracle.com
Internet: www.oracle.com/de