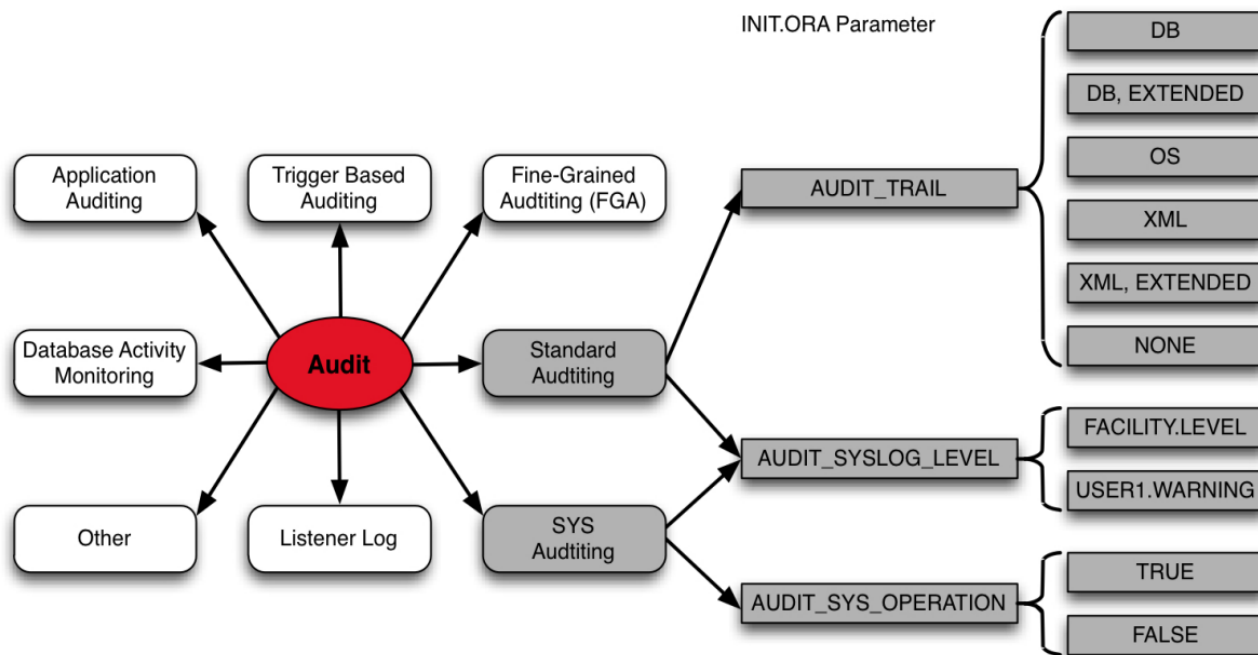


DATABASE VAULT

مقدمه

همانطور که می دانید کاربر SYS می تواند همه اطلاعات کاربران دیگر را مشاهده و نیز تغییراتی را بر روی آنها اعمال کند این مسئله به لحاظ امنیتی می تواند در برخی شرایط چالش آفرین باشد و به همین جهت ممکن است برخی از سازمانها برای حفظ اطلاعات محرمانه ای که دارند، بخواهند بر SYS هم نظارت داشته باشند برای کنترل بر این موضوع، می توان از پارامتری به نام audit_sys_operations استفاده کرد و با کمک این پارامتر، بر همه آنچه که SYS انجام می دهد، نظارت و بازرسی داشت ولی چه فایده که کاربر SYS هم می تواند خروجی را ببیند و هم می تواند آن را غیرفعال کند و صدا البته که خروجی این لاگها هم نسبتا بی کیفیت هستند و معمولا در سطح سیستم عامل قابل مشاهده می باشند. برای مدیریت کاربران غیر SYS، پارامترها و روشهای دیگری هم وجود دارند که در این نوشتار قصد پرداختن به آن را نداریم و تنها به ارائه شکل زیر بسنده می کنیم:



شایسته تاکید است که پارامتر مذکور تنها امکان نظارت بر کارهای SYS را به صورت کاملا ناقص ممکن می سازد و هیچ محدودیتی را برای کاربر SYS اعمال نمی کند و حتی کاربر SYS می تواند با یکبار راه اندازی مجدد بانک، این قابلیت را غیرفعال کند. مشابه این دغدغه، دغدغه دیگری هم وجود دارد که آن هم کنترل و محدود کردن ادمین بانک اطلاعاتی و ادمین OS در سطح سیستم عامل می باشد چون در صورتی که برای ذخیره

اطلاعات از filesystem استفاده شده باشد، ادمین سیستم عامل و یا ادمین بانک اطلاعاتی(در صورت محدود شدن در داخل بانک) ممکن است با کمک ابزارهایی، از اطلاعات فایلها با خبر شوند. اوراکل برای جلوگیری از این مسئله، ویژگی ای به نام TDE را مطرح کرد و همچنین برای رفع چالش اول که محدود سازی کاربر SYS در سطح بانک اطلاعاتی بود، database vault را ارائه کرده است.

در این نوشتار قصد بر آن است تا در مورد database vault به صورت گذرا مطالبی را عنوان کنیم و در نوشتاری دیگر، به فضل الهی به TDE خواهیم پرداخت.

مهمترین وظیفه ای که database vault بر عهده دارد: محدود کردن دسترسی کاربران به شکلی که تنها بتوانند کارهایی که بر عهده آنها است را انجام دهند و هیچ دسترسی اضافه ای نداشته باشند و با کمک این ویژگی می توان مشخص کرد که "چه کسی"، "چه وقت" و به "چه شکلی" به داده دسترسی داشته باشد و همه آنچه که در ابتدا گفته شد، یعنی محدود کردن دسترسی کاربر SYS و کنترل و نظارت بر عملکرد آن، به راحتی از طریق database vault ممکن خواهد بود.

شاید محدود شدن ورود با sysdba و مجبور کردن dba برای استفاده از sysoper به جای sysdba، مثال خوبی در این زمینه باشد که در نسخه های قبلی بلافاصله بعد از نصب DV (database vault) اتفاق می افتاد زیرا که dba می تواند عمده کارهای مدیریتی را از این طریق انجام دهد و در عین حال، می توان آن را محدود کرد تا به همه اطلاعات دسترسی نداشته باشد البته این اتفاق سبب مشکلاتی هم می شد که فرصت طرح آن در این نوشتار وجود ندارد.

در ادامه نحوه نصب database vault آورده شده و نیز در مورد مولفه های آن، مطالبی بیان خواهد شد.

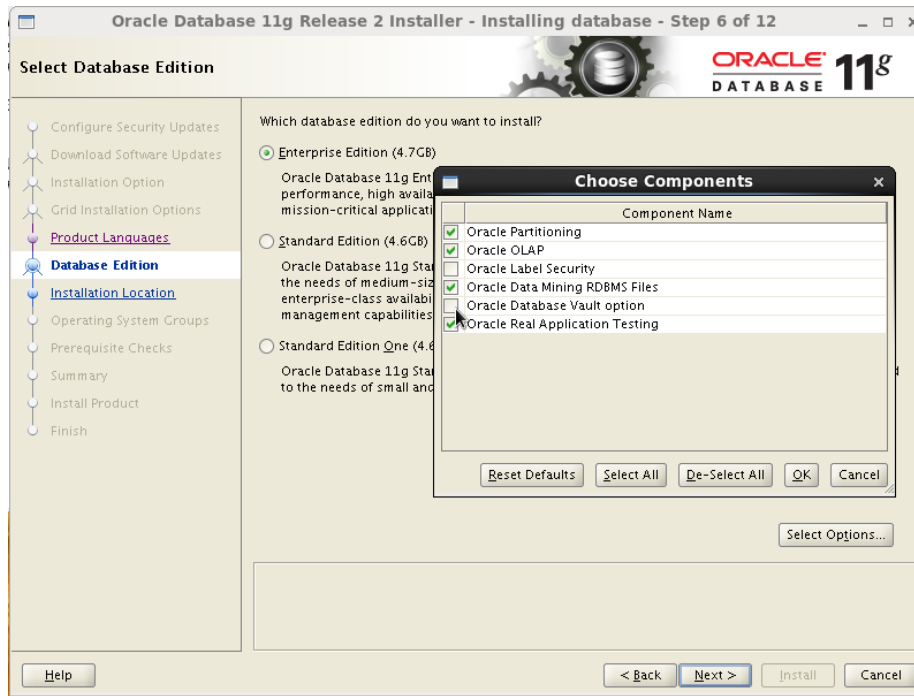
نصب database vault

database vault از نسخه 9iR2 عرضه شد که برای استفاده از آن می بایست نرم افزاری از سایت اوراکل دانلود می شد و با نصب آن نرم افزار از این ویژگی استفاده می شد ولی از اوراکل 11g این ویژگی به همراه نرم افزار اوراکل ارائه می شود و قابل نصب می باشد.

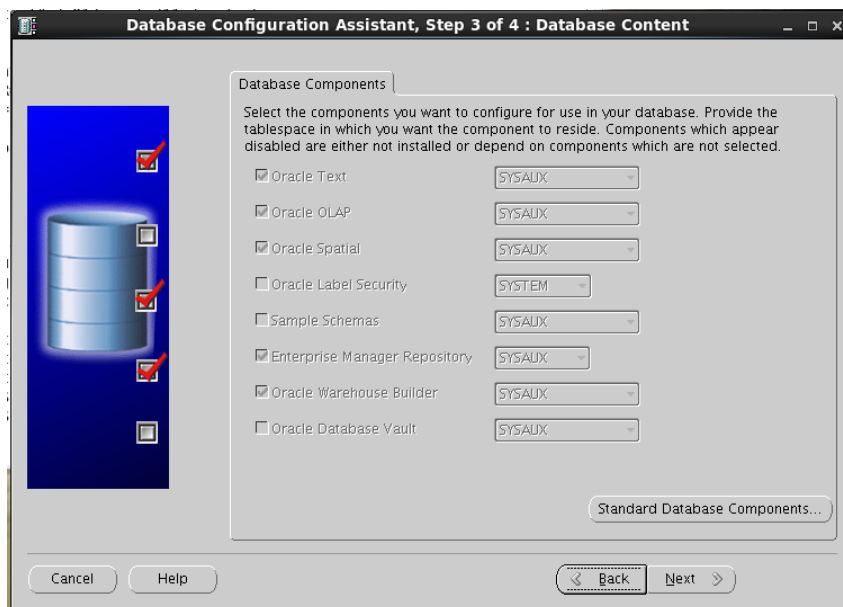
برای نصب database vault، باید در دو مرحله اقدام کرد که یکی در حین نصب نرم افزار اوراکل و دیگری در حین ساخت بانک اطلاعاتی می باشد.

–حین نصب نرم افزار

برای داشتن این ویژگی، باید در مرحله 6 از نصب نرم افزار اوراکل (نسخه 11.2.0.4)، در قسمت select options، database Vault را هم انتخاب کرد که همیشه به همراه انتخاب آن، oracle label security هم انتخاب خواهد شد.



در صورتی که بخواهیم برای بانکی که قبلا نصب شده است، این ویژگی را فعال کنیم، یا باید نصب مجدد انجام داد و یا می بایست از اسکریپت استفاده شود قبل از اجرای این اسکریپت، قابلیت نصب این ویژگی وجود ندارد:



برای فعالسازی این ویژگی، از دستور `chopt` استفاده می شود که از طریق این دستور، نه تنها این کامپوننت، بلکه می توان کامپوننتهای دیگری را هم فعال و یا غیرفعال کرد.

```
[oracle@hkm4 ~]$ chopt
```

```
chopt <enable|disable> <option>
```

options:

dm = Oracle Data Mining RDBMS Files

dv = Oracle Database Vault option

lbac = Oracle Label Security

olap = Oracle OLAP

partitioning = Oracle Partitioning

rat = Oracle Real Application Testing

e.g. `chopt enable rat`

پس برای فعالسازی `database vault` باید مراحل زیر را طی کرد:

1. ابتدا باید تمامی سرویسها متوقف شوند:

```
emctl stop dbconsole
```

```
lsnrctl stop
```

```
sqlplus "/as sysdba"
```

```
SQL> shut abort
```

2. ویژگی `Oracle Label Security` فعال شود:

```
[oracle@hkm4 ~]$ chopt enable lbac
```

```
Writing to /u01/oracle/11g/install/enable_lbac.log...
```

```
/usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk lbac_on ORACLE_HOME=/u01/oracle/11g
```

```
/usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk ioracle ORACLE_HOME=/u01/oracle/11g
```

همانطور که می بینید، خروجی دستور قبلی، شامل دو اسکریپت می باشد که باید هر دو آن را اجرا نمود:

```
[oracle@hkm4 ~]$ /usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk lbac_on
```

```
ORACLE_HOME=/u01/oracle/11g
```

```
[oracle@hkm4 ~]$ /usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk ioracle  
ORACLE_HOME=/u01/oracle/11g
```

3. ویژگی database vault را هم فعال می کنیم:

```
[oracle@hkm4 ~]$ chopt enable dv
```

```
Writing to /u01/oracle/11g/install/enable_dv.log...
```

```
/usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk dv_on ORACLE_HOME=/u01/oracle/11g
```

```
/usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk ioracle ORACLE_HOME=/u01/oracle/11g
```

برای این دستور هم اسکریپت‌ها را اجرا می کنیم:

```
[oracle@hkm4 ~]$ /usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk dv_on  
ORACLE_HOME=/u01/oracle/11g
```

```
[oracle@hkm4 ~]$ /usr/bin/ar cr /u01/oracle/11g/rdbms/lib/libknlopt.a  
/u01/oracle/11g/rdbms/lib/kzvidv.o
```

```
[oracle@hkm4 ~]$ /usr/bin/make -f /u01/oracle/11g/rdbms/lib/ins_rdbms.mk ioracle  
ORACLE_HOME=/u01/oracle/11g
```

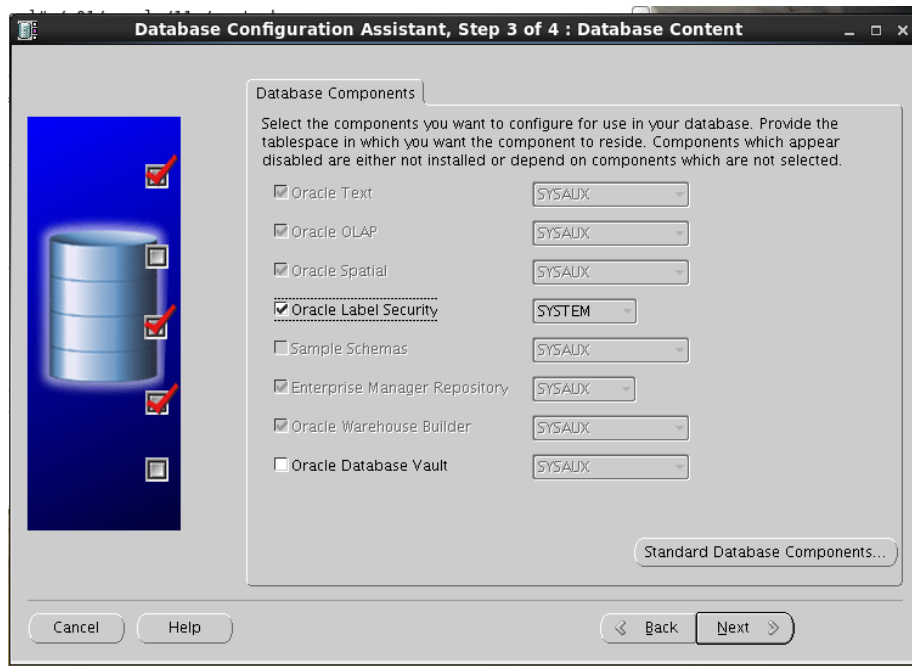
4. در نهایت بانک را راه اندازی مجدد خواهیم کرد:

```
lsnrctl start
```

```
sqlplus "/as sysdba"
```

```
startup
```

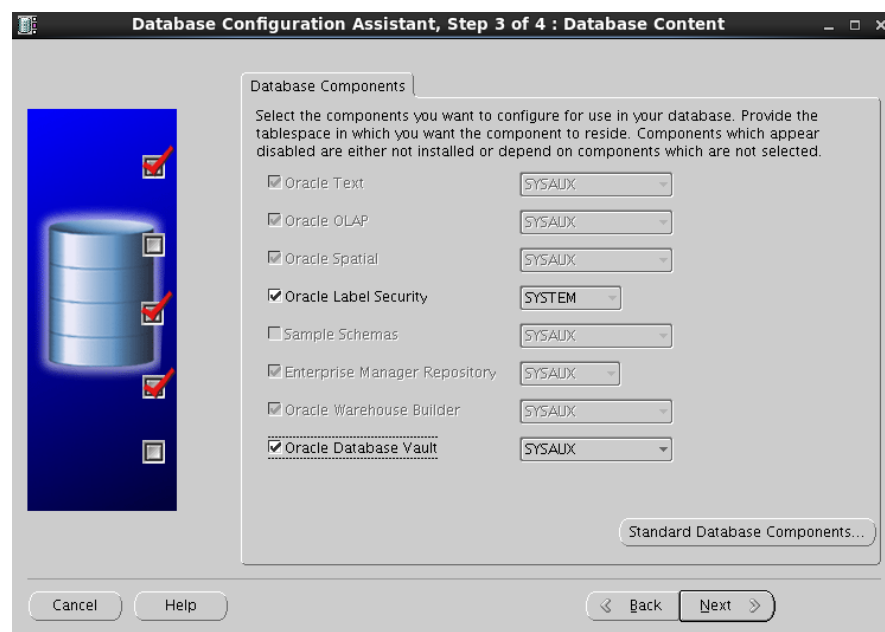
با اجرا مجدد dbca خواهیم دید که قابلیت افزودن دو کامپوننت ممکن شده است:



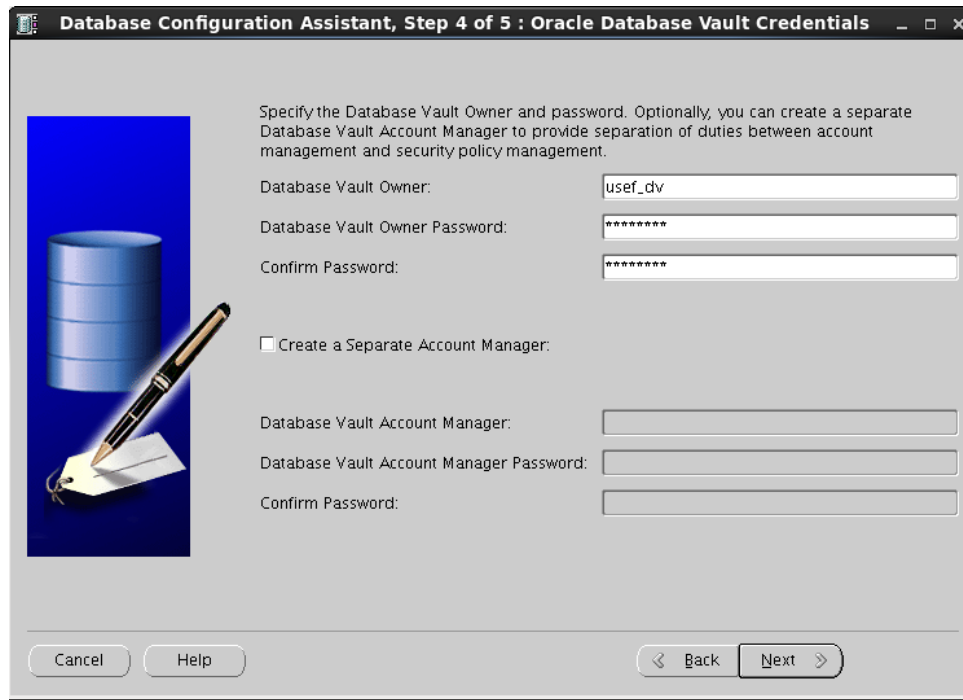
–حین dbca

در صورتی که قابلیت استفاده از این ویژگی در سطح نرم افزار ایجاد شده باشد(با یکی از دو روش مذکور) می توان از طریق dbca و یا از طریق اسکریپت، این کامپوننت را به بانک اضافه کرد که مراحل انجام آن از طریق dbca به صورت زیر می باشد:

1. گزینه های مربوط به OLS و VAULT را انتخاب می کنیم.



2. کاربری را به عنوان database vault owner معرفی می کنیم که از طریق آن می توان به کنسول مدیریتی DV متصل شد و همچنین در صورتی که می خواهیم قسمتی از مدیریت vault به کاربر دیگری تحت عنوان account manager داده شود، باید در قسمت زیرین، کاربر مورد نظر را معرفی کنیم.



Database Configuration Assistant, Step 4 of 5 : Oracle Database Vault Credentials

Specify the Database Vault Owner and password. Optionally, you can create a separate Database Vault Account Manager to provide separation of duties between account management and security policy management.

Database Vault Owner: usef_dv

Database Vault Owner Password: *****

Confirm Password: *****

Create a Separate Account Manager:

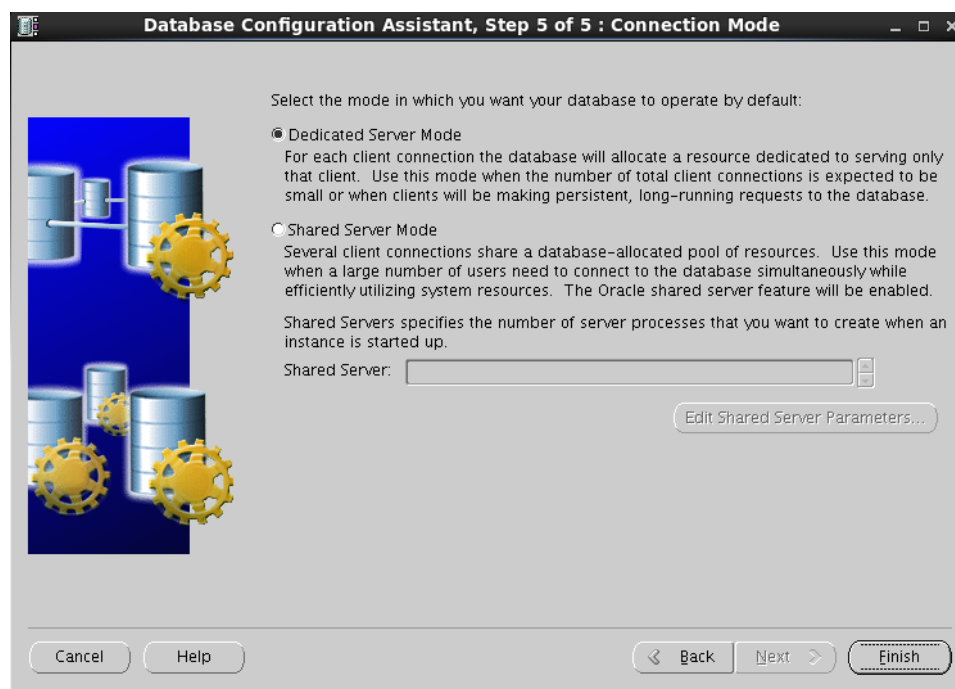
Database Vault Account Manager:

Database Vault Account Manager Password:

Confirm Password:

Cancel Help < Back Next >

3. از بین دو مدل dedicated و shared یکی را انتخاب می کنیم.



Database Configuration Assistant, Step 5 of 5 : Connection Mode

Select the mode in which you want your database to operate by default:

Dedicated Server Mode
For each client connection the database will allocate a resource dedicated to serving only that client. Use this mode when the number of total client connections is expected to be small or when clients will be making persistent, long-running requests to the database.

Shared Server Mode
Several client connections share a database-allocated pool of resources. Use this mode when a large number of users need to connect to the database simultaneously while efficiently utilizing system resources. The Oracle shared server feature will be enabled.

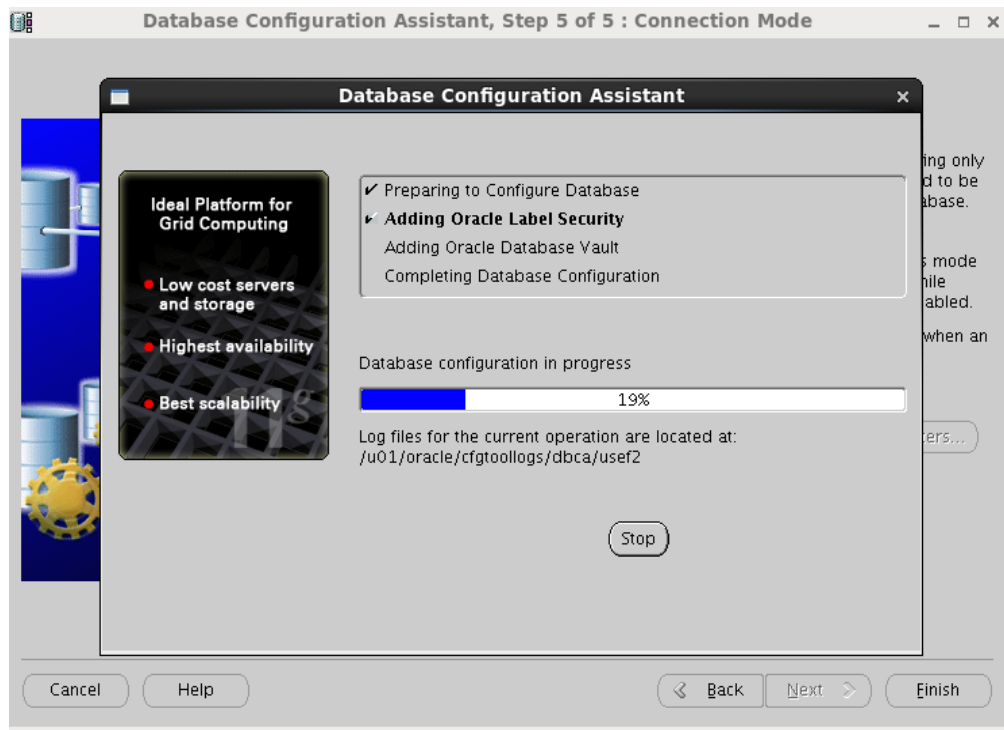
Shared Servers specifies the number of server processes that you want to create when an instance is started up.

Shared Server: []

Edit Shared Server Parameters...

Cancel Help < Back Next > Finish

4. با انتخاب finish، نصب صورت خواهد پذیرفت.



5. با پرس و جوی زیر خواهیم یافت که این دو ویژگی به بانک اضافه شده اند:

```
SQL> select PARAMETER,VALUE from v$option where PARAMETER in('Oracle Database Vault','Oracle Label Security');
```

PARAMETER	VALUE
Oracle Label Security	TRUE
Oracle Database Vault	TRUE

حال با ورود به کاربر sys، قصد داریم تا مجوز dba را به کاربر sysman اهدا کنیم:

```
sqlplus "/as sysdba"
```

```
SQL> show user
```

```
USER is "SYS"
```

```
SQL> grant dba to sysman;
```

```
ORA-47410: Realm violation for GRANT on UNLIMITED TABLESPACE
```

همانطور که می بینید، کاربر sys هم نمی تواند مجوز dba را به کسی بدهد.

به همراه نصب database vault، دو کاربر با نامهای DVSYS و DVF ایجاد می شوند که به صورت پیش فرض هر دو در حالت lock قرار دارند و معمولاً به این دو کاربر نیازی نخواهیم داشت همچنین اگر account manager به صورت جداگانه تعریف شود، کاربر دیگری هم ساخته خواهد شد.

به همراه نصب database vault، role های جدیدی هم به بانک اضافه می شوند که اسامی آنها به این شکل می باشد:

```
select role from dba_roles l where l.role like '%DV%';
```

DV_ACCTMGR

DV_ADMIN

DV_AUDIT_CLEANUP

DV_GOLDENGATE_ADMIN

DV_GOLDENGATE_REDO_ACCESS

DV_MONITOR

DV_OWNER

DV_PATCH_ADMIN

DV_PUBLIC

DV_REALM_OWNER

DV_REALM_RESOURCE

DV_SECANALYST

DV_STREAMS_ADMIN

DV_XSTREAM_ADMIN

همانطور که می بیند، این role ها در سه سطح owner، administration و monitoring قابل تقسیم می باشند.

همچنین با نصب DV، مقادیر پارامترهای زیر هم تغییر خواهد کرد:

Parameter	Default	New value
AUDIT_SYS_OPERATIONS	FALSE	TRUE
OS_AUTHENT_PREFIX	ops\$	ops\$
OS_ROLES	Not configured	FALSE
REMOTE_LOGIN_PASSWORDFILE	EXCLUSIVE	EXCLUSIVE
REMOT_OS_AUTHENT	FALSE	FALSE
REMOTE_OS_ROLES	FALSE	FALSE
SQL92_SECURITY	FALSE	TRUE

دستورات زیر با نصب DV، توسط کاربر sys و system قابل استفاده نخواهند بود(به دلیل command rule تعیین شده):

Alter user - Alter profile - Create profile - Create user - Drop profile - Drop user

از دیگر تاثیرات نصب DV، گرفتن برخی مجوزها از برخی role ها می باشد که لیست آن در جدول زیر آمده است:

Role	Privileges that will be revoked
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
PUBLIC user	EXECUTE ON UTL_FILE
SCHEDULER_ADMIN	CREATE ANY JOB
	CREATE EXTERNAL JOB
	EXECUTE ANY PROGRAM
	EXECUTE ANY CLASS
	MANAGE SCHEDULER

البته توصیه می شود تا قبل از نصب DV، از جداول مرتبط با مجوزها، کپی تهیه کنیم:

```
create table copy_dba_tab_privs as Select * from dba_tab_privs;
```

```
create table copy_dba_sys_privs as Select * from dba_sys_privs;
```

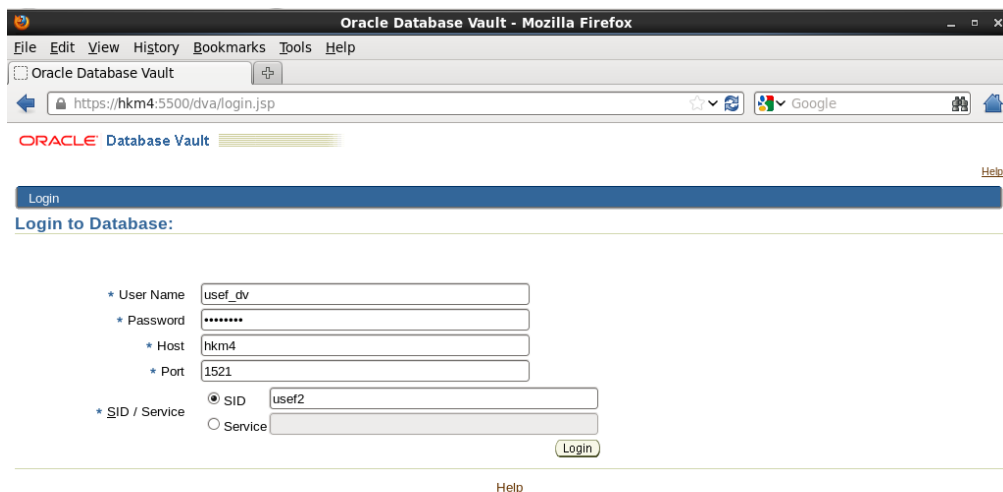
```
create table copy_dba_role_privs as Select * from dba_role_privs;
```

شایان ذکر است که در مواردی از قبیل SQL Injection و یا دسترسی غیرمجاز به دیتابیسها در لایه OS، استفاده و وجود DV موثر نخواهد بود و همچنین اگر کسی به OS دسترسی داشته باشد، می تواند این ویژگی را غیرفعال کند.

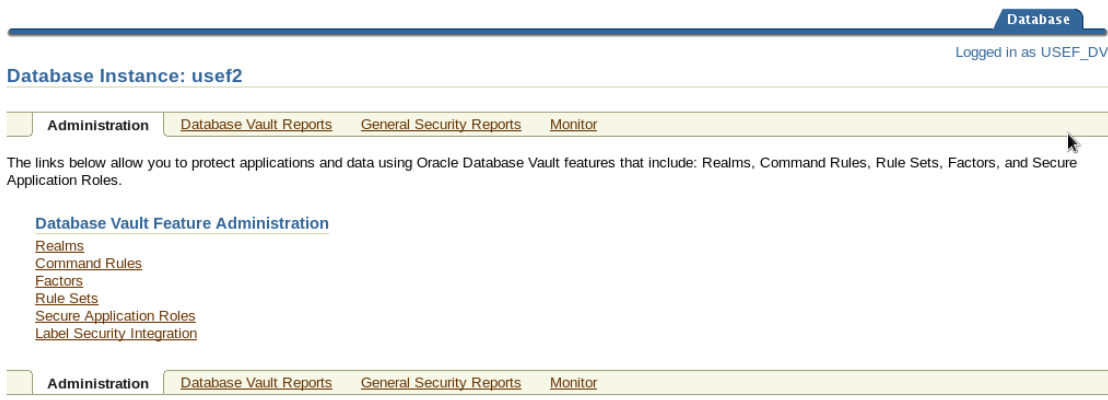
برای مدیریت vault، هم می توان از محیط گرافیکی استفاده کرد و هم می توان از پکیجهایی از قبیل DBMS_MACADM بهره گرفت که استفاده از محیط گرافیکی، به شدت کار را آسان خواهد کرد.

لینک ورود به محیط گرافیکی مربوط به database vault، همانند EM می باشد با این تفاوت که به جای عبارت em باید از dva استفاده کرد:

https://hkm4:5500/dva



بعد از ورود مشخصات کاربر و سرور، وارد صفحه اصلی مربوط به database vault خواهیم شد:



همانطور که در این صفحه می بینید، database vault شامل چند مولفه می باشد که در ابتدا در مورد این مولفه ها مطالبی را عرضه خواهیم داشت و سپس سناریوهایی را در رابطه با هر کدام، پیاده سازی خواهیم کرد.

Realm: در صورتی که قصد داشته باشیم مجموعه ای از چند اشیا را از دسترس برخی یا همه افراد دور نگه داریم و به اصلاح آنها را secure یا امنشان کنیم، می توانیم از Realm استفاده کنیم در این صورت این امکان هم وجود دارد تا تنها با چند کلیک و یا چند دستور، دسترسی به همه این اشیا تعریف شده را برای چند کاربر خاص مجاز کنیم و یا اینکه به صورت کلی، در کسری از ثانیه، همه این محدودیتها را غیرفعال کنیم.

با نصب database vault، چند realm به صورت پیش فرض ایجاد می شوند:

Select	Name ▲	Audit Options	Oracle Defined Realm?	Objects Protected?	Users Authorized?	Status
<input checked="" type="radio"/>	Database Vault Account Management	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Data Dictionary	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Database Vault	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Enterprise Manager	Audit On Failure	✓	✓	✓	✓

از مهمترین این realm ها، Oracle Data Dictionary می باشد که سبب می شود تا محدودیتهای بسیاری برای کاربران ایجاد شود. برای اینکه کاربری را از این محدودیتها مستثنی کنیم، باید نام آن کاربر را در قسمت users authorized اضافه کنیم و همچنین این امکان وجود دارد تا به لیست اشیا امن شده، اشیا دیگری را هم اضافه کنیم که برای انجام این کار، باید از قسمت object protected استفاده کرد.

برای مشاهده لیست realm ها می توان از دستور زیر هم استفاده کرد:

sqlplus usef_dv/usef_123

```
select name , enabled from dvsys.dba_dv_realm;
```

NAME	ENABLED
Database Vault Account Management	Y
Oracle Data Dictionary	Y
Oracle Database Vault	Y
Oracle Enterprise Manager	Y

همچنین برای مشاهده لیست قوانین موجود در هر کدام از realm ها، می توان از دستور زیر بهره گرفت:

```
select * from dvsys.dba_dv_realm_object where realm_name='Oracle Data Dictionary';
```

REALM_NAME	OWNER	OBJECT_NAME	OBJECT_TYPE
------------	-------	-------------	-------------

Command Rule: در صورتی که بخواهیم کاربر و یا کاربران خاصی را از زدن دستورات مشخصی منع و یا مجاز کنیم، می توانیم از Command Rule استفاده کنیم دستورات می توانند DDL ای، DML ای و ... باشند. به صورت پیش فرض، command rule های زیر در سیستم وجود دارند:

Select	Command	Object Owner	Object Name	Rule Set Name	Status
<input checked="" type="radio"/>	ALTER PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	ALTER SYSTEM	%	%	Allow Fine Grained Control of System Parameters	✓
<input type="radio"/>	ALTER USER	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CHANGE PASSWORD	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CREATE PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	CREATE USER	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP USER	%	%	Can Maintain Accounts/Profiles	✓

برای مشاهده لیست command rule ها، از ویوی dba_dv_command_rule استفاده می شود.

```
select * from dvsys.dba_dv_command_rule;
```

COMMAND	RULE_SET_NAME	OBJECT_OWNER	OBJECT_NAME	ENABLED
SELECT	ip	USEF	%	Y
DROP USER	Can Maintain Accounts/Profiles	%	%	Y

Factor: با کمک فاکتور می توان محدودیتهای دیگری را از طریق اطلاعات و خصوصیات session لحاظ کنیم از قبیل آنکه، "فردی با ip مشخص، تنها حق دسترسی به جدول مشخصی را داشته باشد"، "فردی با ماشین مشخص، نتواند از دستور x استفاده کند" و یا حتی از طریق ساعت و دیگر خصوصیات session محدودیت هایی را ایجاد کنیم. برای انجام این کار، می توان از تابع sys_context استفاده کرد. لیست فاکتورهای پیش فرض در این قسمت دیده می شود:

Select	Name ▲	Factor Type Name	Evaluation Options	Factor Identification	Assign Rule Set Name	Error Handling	Audit Options
<input checked="" type="radio"/>	Authentication_Method	Authentication Method	By Access	By Method		Show Error Message	Never
<input type="radio"/>	Client_IP	IP Address	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Database_Domain	Physical	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Database_Hostname	Hostname	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Database_Instance	Instance	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Database_IP	IP Address	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Database_Name	Instance	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Domain	Physical	For Session	By Factors		Show Error Message	Never
<input type="radio"/>	Enterprise_Identity	User	By Access	By Method		Show Error Message	Never
<input type="radio"/>	Identification_Type	Authentication Method	By Access	By Method		Show Error Message	Never
<input type="radio"/>	Lang	User	By Access	By Method		Show Error Message	Never
<input type="radio"/>	Language	User	By Access	By Method		Show Error Message	Never
<input type="radio"/>	Machine	Physical	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Network_Protocol	Authentication Method	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Proxy_Enterprise_Identity	User	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Proxy_User	User	For Session	By Method		Show Error Message	Never
<input type="radio"/>	Session_User	User	By Access	By Method		Show Error Message	Never

برای مشاهده لیست فاکتورها، می توان از ویوی DBA_DV_FACTOR استفاده کرد:

```
SELECT * FROM DVSYS.DBA_DV_FACTOR;
```

```
SELECT DVF.F$ip_factor FROM DUAL;
```

Rule Set: مجموعه ای از یک یا چند rule می باشد و در زمان استفاده از command rule و realm باید از طریق rule set مشخص کرد که دامنه محدودیتها مربوط به چه زمینه و چه محدوده ای باشد. همچنین می توان از یک rule set استفاده مکرر داشت.

برای مشاهده لیست Rule Set ها، از دستور زیر استفاده می شود:

```
select rule_set_name, enabled from dvsys.dba_dv_rule_set;
```

RULE_SET_NAME	ENABLED
ip	Y
Enabled	Y
Disabled	Y
Can Maintain Accounts/Profiles	Y

در ادامه از هر یک از این مولفه ها با طرح سناریویی استفاده خواهیم کرد.

مثال اول (realm Authorization): کاربر sys از oracle data dictionary realm مستثنی شود.

ابتدا وارد قسمت realm شده و oracle data dictionary را ویرایش می کنیم:

Select	Name [△]	Audit Options	Oracle Defined Realm?	Objects Protected?	Users Authoriz	Status
<input type="radio"/>	Database Vault Account Management	Audit On Failure	✓	✓	✓	✓
<input checked="" type="radio"/>	Oracle Data Dictionary	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Database Vault	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Enterprise Manager	Audit On Failure	✓	✓	✓	✓

در قسمت realm Authorizations بر روی create کلیک می کنیم:

Realm Authorizations

Select	Grantee	Authorization Options	Authorization Rule Set Name
No Items Found			

در این قسمت، grantee را به sys تنظیم کرده و برای اینکه هیچ گونه محدودیتی در این زمینه برای کاربر sys اعمال نشود، نوع Authorizations را به owner و rule set را هم به enable تنظیم می کنیم تا این Authorizations برای کاربر sys فعال باشد.

Database Instance: usef2 > Realms > Edit Realm: Oracle Data Dictionary > Logged in as USEF_DV

Create Realm Authorization

Define a database account or database role as either a realm owner or realm participant. Realm owners and realm participants can use their system privileges against real... secured objects. Only realm owners can grant or revoke realm secured database roles.

Grantee

Authorization Type
 Participant
 Owner

Authorization Rule Set

با انجام این مراحل، خواهیم دید که کاربر sys قادر به انجام کارهایی است که بعد از نصب vault محدود شده بود(البته با این کار، قسمتی از تحریم ها برداشته شده است نه همه تحریم ها!!!).

SQL> grant dba to sysman;

Grant succeeded.

مثال دوم(Command Rule): امکان ساخت جدولی که مالک آن کاربر sys باشد، غیر فعال شود.

این کار باید از طریق command rule انجام شود به همین جهت، وارد قسمت command rule شده و rule جدیدی را ایجاد می کنیم:

allow the command to succeed based on the evaluation of a Database Vault rule set.

Select	Command ▲	Object Owner	Object Name	Rule Set Name	Status
<input checked="" type="radio"/>	ALTER PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	ALTER SYSTEM	%	%	Allow Fine Grained Control of System Parameters	✓
<input type="radio"/>	ALTER USER	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CHANGE PASSWORD	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CREATE PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	CREATE USER	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP USER	%	%	Can Maintain Accounts/Profiles	✓

سپس در قسمت create command rule، مجوز ساخت جدولی که مالک آن sys باشد را غیرفعال خواهیم کرد:

Create Command Rule

This page allows you to create or edit a command that can be authorized based on the evaluation of a Database Vault rule set.

General

* Command: CREATE TABLE

Status: Enabled Disabled

Applicability

Object Owner: SYS

Object Name: %

Rule Set

Disabled

در قسمت object_name، % به معنی همه کارکترها می باشد و همانند * در دستور sql، نقش wildcard را ایفا می کند همچنین usef% بیانگر همه اشیایی هست که با usef شروع می شوند. با بازگشت به قسمت command rule، rule جدیدی دیده خواهد شد:

<input type="radio"/>	CREATE TABLE	SYS	%	Disabled	✓
-----------------------	--------------	-----	---	----------	---

حال با کاربر sys قصد ایجاد جدول tbl را داریم که به خطای زیر برمی خوریم:

```
SQL> create table sys.tbl(id number);
```


ORA-47400: **Command Rule violation** for CREATE TABLE on SYS.TBL

نکته 1: با این rule، کاربر sys می تواند برای بقیه کاربران، جدول ایجاد کند و محدودیتی از این نظر ایجاد نشده است.

```
SQL> create table app1.u33(a number);
```

Table created.

نکته 2: در صورتی که object_name را در مثال بالا برابر با مقداری قرار دهیم، سبب می شود تا از ساختن جدولی با آن اسم ممانعت شود. برای مثال، در شکل زیر نشان داده شده که هیچ جدولی با اسم usef_tbl نمی توان ساخت.

Select	Command	Object Owner	Object Name	Rule Set Name	Status
<input checked="" type="radio"/>	ALTER PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	ALTER SYSTEM	%	%	Allow Fine Grained Control of System Parameters	✓
<input type="radio"/>	ALTER USER	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CHANGE PASSWORD	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CREATE PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP USER	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	CREATE TABLE	%	USEF_TBL	Disabled	✓

نکته 3: برای جلوگیری از ساخت جدول توسط کاربر sys باید از rule set مناسب استفاده کرد.

```
SYS_CONTEXT('USERENV','SESSION_USER') NOT IN ('SYS')
```

Database Instance: usef2 > Rule Set > Edit Rule Set: ip > Logged in as USEF_DV

Edit Rule: user [Cancel] [OK]

A rule is a SQL WHERE clause expression that evaluates to true or false.

General

* Name: user

* Rule Expression: SYS_CONTEXT('USERENV','SESSION_USER') NOT IN ('SYS')

A rule expression may be any valid SQL WHERE clause expression. The value returned by this SQL WHERE clause expression must return a boolean value (TRUE or FALSE). When using PL/SQL functions, make sure to use a fully qualified function, such as schema.function_name, and make sure to GRANT EXECUTE privilege on the function to the DVSYS account.

[Cancel] [OK]

مثال سوم (Command Rule): امکان خواندن (select) از جدول salary برای همه کاربران حتی sys غیر فعال شود.

این کار با افزودن command rule قابل انجام است.

Database Instance: usef2 > Command > Logged in as USEF_DV

Create Command Rule

This page allows you to create or edit a command that can be authorized based on the evaluation of a Database Vault rule set.

General

* Command:

Status: Enabled
 Disabled

Applicability

Object Owner:

Object Name:

Rule Set

حال از طریق کاربر sys اقدام به خواندن از جدول usef.salary می کنیم:

```
SQL> show user
```

```
USER is "SYS"
```

```
SQL> select * from usef.salary;
```

```
ORA-01031: insufficient privileges
```

مثال چهارم (Realm): دو application در بانک وجود دارند که قرار است هر کدام تنها اطلاعات خودش را ببیند و application ای حق ندارد اطلاعات دیگری را ببیند.

برای پیاده سازی این مسئله، نیاز است از realm استفاده شود. برای پیاده سازی این سناریو، ابتدا دو کاربر با نامهای App1 و App2 می سازیم و با کمک realm، هر یک را تنها به دیدن اطلاعات خودشان محدود می کنیم.

```
SQL> create user app1 identified by app1;
```

```
SQL> grant dba to app1;
```

```
SQL> create user app2 identified by app2;
```

```
SQL> grant dba to app2;
```

```
SQL> conn app1/app1
```

```
SQL> create table tbl_app1 as select * from v$tablespace;
```

```
SQL> conn app2/app2
```

```
SQL> create table tbl_app2 as select * from v$tablespace;
```

As sysdba:

SQL> select * from app2.tbl_app2;

TS#	NAME	INC	BIG	FLA	ENC
0	SYSTEM	YES	NO	YES	
1	SYSAUX	YES	NO	YES	
2	UNDOTBS1	YES	NO	YES	
4	USERS	YES	NO	YES	
3	TEMP	NO	NO	YES	

حال با کمک realm، سناریوی مورد نظر را انجام می دهیم ابتدا realm ای برای app1 ایجاد می کنیم:

Create Realm

Cancel OK

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

OK

General

* Name

Description

Status Enabled
 Disabled

Audit Options

Audit Disabled
 Audit On Failure
 Audit On Success or Failure

Cancel OK

با ویرایش این realm، اشیایی که قرار است امن بمانند را مشخص می کنیم:

Cancel OK

enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

* Name

Description

Status Enabled
 Disabled

Audit Options

Audit Disabled
 Audit On Failure
 Audit On Success or Failure

Realm Secured Objects

Create

Select Owner	Object Type	Object Name	Create
No Items Found			

Database Instance: usef2 > Realms > Edit Realm: app1 >

Logged in as USEF_DV

Create Realm Secured Object

Cancel OK

Define a database schema or database role that is protected by the realm.

Object Owner

Object Type

Object Name

Cancel OK

همانطور که می بینیم، قرار است همه اشیاهای مختص به کاربر App1، از دسترسی همگان خارج شوند. حال تستی را انجام می دهیم که ایا کاربر sys و یا App2 می توانند به اطلاعات App1 دسترسی داشته باشند یا نه؟ App1 چگونه؟

As sysdba:

```
SQL> select * from app1.tbl_app1;
```

ORA-01031: insufficient privileges

```
SQL> conn app2/app2
```

```
SQL> select * from app1.tbl_app1;
```

ORA-01031: insufficient privileges

SQL> conn app1/app1

SQL> select * from app1.tbl_app1;

TS#	NAME	INC	BIG	FLA	ENC
0	SYSTEM	YES	NO	YES	
1	SYS_AUX	YES	NO	YES	
2	UNDOTBS1	YES	NO	YES	
4	USERS	YES	NO	YES	
3	TEMP	NO	NO	YES	

حال می توانیم همین سناریو را برای App2 انجام دهیم.

مثال پنجم (Rule Set - Factor): تنها فردی بتواند از اطلاعات کاربر usef بخواند (select) که از ip ای با

شماره 10.47.52.21 وارد بانک شده باشد.

این کار از طریق فاکتور به همراه Rule set و یا Rule set به تنهایی قابل انجام است به همین جهت rule set جدیدی را با نام ip ایجاد می کنیم:

Database Instance: usef2 > Rule Set > Logged in as USEF_DV

Create Rule Set Cancel OK

A rule set is a collection of one or more rules that evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True). OK

General

* Name:

Description:

Status: Enabled Disabled

Evaluation Options: All True Any True

Audit Options

Audit Disabled

Audit On Failure

Audit On Success or Failure

سپس Rule set مورد نظر را ویرایش می کنیم:

Rule Sets

Database Vault provides a rules engine that can be used in the security policy decisions of factors, realms, command rules, and secure application roles.

Create

Edit Remove

Select	Name	Evaluation Options	Error Handling	Audit Options	Rules Defined?	Status
<input type="radio"/>	Allow Fine Grained Control of System Parameters	All True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Allow Sessions	All True	Show Error Message	Audit On Failure	✗	✓
<input type="radio"/>	Allow System Parameters	All True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Can Grant VPD Administration	All True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Can Maintain Accounts/Profiles	All True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Can Maintain Own Account	Any True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Disabled	All True	Show Error Message	Audit Disabled	✓	✓
<input type="radio"/>	Enabled	All True	Show Error Message	Audit Disabled	✓	✓
<input checked="" type="radio"/>	ip	All True	Show Error Message	Audit On Failure	✗	✓

Edit Remove

Edit

در قسمت rule associated، می توانیم فاکتوری را اضافه کنیم و یا rule جدیدی را تعریف کنیم که به همین جهت، create را انتخاب می کنیم:

Rules Associated To The Rule Set

Create Add Existing Rules

Select Rule Name	Rule Expression
No Items Found	

Create

Cancel OK

در قسمت create rule، با کمک application context پیش فرض بانک که USERENV می باشد، شرط مورد نظر را قرار می دهیم.

`SYS_CONTEXT('USERENV','IP_ADDRESS') IN ('10.47.52.21')`

Create Rule

Cancel OK

A rule is a SQL WHERE clause expression that evaluates to true or false.

OK

General

* Name

* Rule Expression

A rule expression may be any valid SQL WHERE clause expression. The value returned by this SQL WHERE clause expression must return a boolean value (TRUE or FALSE). When using PL/SQL functions, make sure to use a fully qualified function, such as schema.function_name, and make sure to GRANT EXECUTE privilege on the function to the DVSYS account.

در نهایت به طریقی که قبلا آورده شد، command rule جدیدی را ایجاد می کنیم و در آن، rule set را به ip تنظیم می کنیم تا تنها ip مورد نظر بتواند اطلاعات کاربر usef را بخواند.

Database Instance: usef2 > Command > Logged in as USEF_DV

Create Command Rule

This page allows you to create or edit a command that can be authorized based on the evaluation of a Database Vault rule set.

General

* Command: SELECT

Status: Enabled Disabled

Applicability

Object Owner: USEF

Object Name: %

Rule Set

ip

Cancel OK

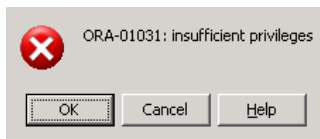
تست زیر نشان می دهد که اطلاعات کاربر usef به کاربرانی که از ip غیر مجاز وارد شده اند، نشان داده نمی شود:

Conn usef/usef

```
select get_factor('client_ip') from dual;
```

10.43.136.34

```
select * from usef.salary;
```



همچنین در صورتی که بخواهیم این کار با کمک Factor انجام شود، باید ابتدا یک فاکتور ایجاد کنیم:

Create Factor

Cancel OK

A Database Vault factor is a configuration item that contributes to the database application security policy for rule sets, command rules and realms.

OK

General

* Name

Description

* Factor Type

Factor Identification

- By Method
- By Constant
- By Factors
- By Context

Evaluation

- For Session
- By Access
- On Startup

Factor Labeling

- By Self
- By Factors

Retrieval Method

UPPER(SYS_CONTEXT('USERENV','IP_ADDRESS'))

The retrieval method returns a factor's identity and may be any valid PL/SQL expression, package function or standalone function. The value returned must be a VARCHAR2 data type or otherwise convertible to one. When using PL/SQL functions, make sure to use a fully qualified function, such as schema.function_name, and make sure to GRANT EXECUTE privilege on the function to the user who will be using the factor.

که در این صورت یک تابع با F\$ip_factor برای کاربر DVF ساخته می شود که با اجرای آن، عبارت قید شده در قسمت Retrieval Method برخواهد گشت.

```
SELECT DVF.F$ip_factor FROM DUAL;
10.47.52.21
```

حال می توانیم با کمک این فاکتور، شرط مورد نظر را اعمال کنیم:

Edit Rule: new_rule

Cancel OK

A rule is a SQL WHERE clause expression that evaluates to true or false.

General

* Name

* Rule Expression

DVF.F\$IP_FACTOR IN ('10.47.52.21','10.33.136.34')

A rule expression may be any valid SQL WHERE clause expression. The value returned by this SQL WHERE clause expression must return a boolean value (TRUE or FALSE). When using PL/SQL functions, make sure to use a fully qualified function, such as schema.function_name, and make sure to GRANT EXECUTE privilege on the function to the DVSYS account.

Cancel OK

و در نهایت از این Rule Set در Command Rule مورد نظر استفاده کنیم.

DATABASE VAULT REPORT

از دیگر ویژگی های مفید database vault، قابلیت مانیتورینگ آن می باشد که می توان از طریق آن، مشاهده کرد که "چه کسی" با کمک "چه مولفه ای" موفق به انجام "چه کاری" شده است.

DV به دو شیوه امکان نظارت و مانیتورینگ را فراهم می کند:

1. database Vault reports: در این بخش اطلاعاتی را مورد مولفه های مختلف اعم از realm، factor و ... را مشاهده خواهیم کرد. برای مثال میتوان با مراجعه به این قسمت مشاهده کرد که realmها مانع از انجام چه کاری شده اند:

Administration Database Vault Reports General Sec

Use this screen to run reports about potential Database Vault confi

Run Report

Expand All | Collapse All

Select Focus Report Title

- Reports
- Database Vault Configuration Issues Reports
 - Command Rule Configuration Issues
 - Factor Configuration Issues
 - Factors Without Identities
 - Identity Configuration Issues
 - Realm Authorization Configuration Issues
 - Rule Set Configuration Issues
 - Secure Application Configuration Issues
- Database Vault Auditing Reports
 - Realm Audit**
 - Command Rule Audit
 - Factor Audit
 - Label Security Integration Audit
 - Core Database Vault Audit Trail
 - Secure Application Role Audit

Run Report

https://hkr Run Report /mac/report#

Database Instance: usef2 >

Logged in as USEF_DV

Report Results: Realm Audit

Page Refreshed Sep 3, 2017 5:30:35 PM

Violation Attempt	Timestamp	Return Code	Account	User Host	Instance Number	Realm Name	Rule Set	Command
Realm Violation Audit	03-SEP-17 03:56:01 PM	1031	APP2	hkm40		app1		SELECT * FROM APP1.TBL_APP1
Realm Violation Audit	03-SEP-17 03:55:14 PM	1031	SYS	hkm40		app1		SELECT * FROM APP1.TBL_APP1

همانطور که در خروجی می بینید، کاربر app2 و sys قصد اجرای دستوری را داشته اند که به خاطر وجود realmی به نام app1، موفق به دسترسی آن اطلاعات نشده اند.

General Security reports.2: در این بخش گزارشی در مورد مسائل امنیتی عمومی از قبیل system privilege و object privilegeها ارائه می شود. برای مثال، شکل زیر نشان می دهد که کاربر usef دو مجوز create any table و drop any table را دریافت کرده است.

Administration Database Vault Reports **General Security Reports** Monitor

Use this screen to run reports about potential security issues with the existing privilege model, database roles.

Run Report

Expand All Collapse All

Run Report

Select	Focus	Report Title
<input type="radio"/>		▼ Reports
<input type="radio"/>	<input checked="" type="radio"/>	▼ Object Privilege Reports
<input type="radio"/>		Object Access By PUBLIC
<input type="radio"/>		Object Access Not By PUBLIC
<input type="radio"/>		Direct Object Privileges
<input type="radio"/>		Object Dependencies
<input type="radio"/>	<input checked="" type="radio"/>	▼ Database Account System Privileges Reports
<input type="radio"/>		Direct System Privileges by Database Account
<input type="radio"/>		Direct and Indirect System Privileges By Database Account
<input type="radio"/>		Hierarchical System Privileges by Database Account
<input checked="" type="radio"/>		ANY System Privileges for Database Accounts
<input type="radio"/>		System Privileges By Privilege
<input type="radio"/>	<input checked="" type="radio"/>	▼ Sensitive Objects Reports
<input type="radio"/>		Execute Privileges to Strong SYS Packages
<input type="radio"/>		Access to Sensitive Objects
<input type="radio"/>		Public Execute Privilege To SYS PL/SQL Procedures

https://hk4-5500/dva/mac/nrntect# SDBA/SYSOPER Privilege

Database Instance: usef2 > Logged in as USEF_DV

Report Parameters: ANY System Privileges for Database Accounts

Account: USEF

Result Set Size: 100 250 500 1000 All

Run Report


Run Report

Run Report

Report Results: ANY System Privileges for Database Accounts

Page Refreshed Sep 4, 2017 1:40:25 PM

Return To Reports Menu

Privilege 	Grantee	Return To Reports Menu
CREATE ANY TABLE	USEF	
DROP ANY TABLE	USEF	

Return To Reports Menu

حذف database vault

برای حذف database vault می توان مراحل زیر را طی نمود:

1. ابتدا همه سرویسها را متوقف می کنیم:

```
sqlplus "/as sysdba"
```

```
shut abort
```

2. با دستور chopt، این ویژگی را غیرفعال می کنیم:

```
[oracle@hkm6 ~]$ chopt disable dv
```

```
Writing to /u01/oracle/11g44/install/disable_dv.log...
```

```
/usr/bin/make -f /u01/oracle/11g44/rdbms/lib/ins_rdbms.mk dv_off ORACLE_HOME=/u01/oracle/11g44
```

```
/usr/bin/make -f /u01/oracle/11g44/rdbms/lib/ins_rdbms.mk ioracle ORACLE_HOME=/u01/oracle/11g44
```

اجرای اسکریپت ایجاد شده:

```
[oracle@hkm6 ~]$ /usr/bin/make -f /u01/oracle/11g44/rdbms/lib/ins_rdbms.mk dv_off
ORACLE_HOME=/u01/oracle/11g44
```

```
/usr/bin/ar cr /u01/oracle/11g44/rdbms/lib/libknopt.a /u01/oracle/11g44/rdbms/lib/kzvndv.o
```

```
[oracle@hkm6 ~]$ /usr/bin/ar cr /u01/oracle/11g44/rdbms/lib/libknopt.a /u01/oracle/11g44/rdbms/lib/kzvndv.o
```

```
[oracle@hkm6 ~]$ /usr/bin/make -f /u01/oracle/11g44/rdbms/lib/ins_rdbms.mk ioracle
ORACLE_HOME=/u01/oracle/11g44
```

3. حال با راه اندازی مجدد بانک اطلاعاتی، تمامی اطلاعات مرتبط با DV را پاک می کنیم و تنظیمات بانک را

به قبل از راه اندازی DV بر می گردانیم:

```
@?/rdbms/admin/dvremov.sql
```

```
drop user dbvowner cascade;
```

```
drop user dbvacctmgr cascade;
```

```
grant BECOME USER to DBA;

grant SELECT ANY TRANSACTION to DBA;

grant CREATE ANY JOB to DBA;

grant CREATE EXTERNAL JOB to DBA;

grant EXECUTE ANY PROGRAM to DBA;

grant EXECUTE ANY CLASS to DBA;

grant MANAGE SCHEDULER to DBA;

grant DEQUEUE ANY QUEUE to DBA;

grant ENQUEUE ANY QUEUE to DBA;

grant MANAGE ANY QUEUE to DBA;

grant BECOME USER to IMP_FULL_DATABASE;

grant MANAGE ANY QUEUE to IMP_FULL_DATABASE;

grant DBA to INFA_ADMIN;

grant EXECUTE ON DBMS_LOGMNR to EXECUTE_CATALOG_ROLE;

grant EXECUTE ON DBMS_LOGMNR_D to EXECUTE_CATALOG_ROLE;

grant EXECUTE ON DBMS_LOGMNR_LOGREP_DICT to EXECUTE_CATALOG_ROLE;

grant EXECUTE ON DBMS_LOGMNR_SESSION to EXECUTE_CATALOG_ROLE;

grant EXECUTE ON DBMS_FILE_TRANSFER to EXECUTE_CATALOG_ROLE;

grant EXECUTE ON UTL_FILE to PUBLIC;

grant CREATE ANY JOB to SCHEDULER_ADMIN;

grant CREATE EXTERNAL JOB to SCHEDULER_ADMIN;

grant EXECUTE ANY PROGRAM to SCHEDULER_ADMIN;

grant EXECUTE ANY CLASS to SCHEDULER_ADMIN;

grant MANAGE SCHEDULER to SCHEDULER_ADMIN;

ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=FALSE SCOPE=SPFILE sid='*';

ALTER SYSTEM SET RECYCLEBIN='ON' SCOPE=SPFILE sid='*';

ALTER SYSTEM SET SQL92_SECURITY=FALSE SCOPE=SPFILE sid='*';
```