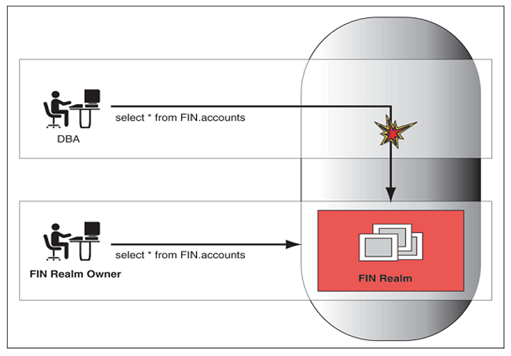
Oracle Database Vault

# Giới thiệu chung



Khái niệm:

* Oracle Database Vault là một tính năng được tích hợp thêm cho Database nhằm kiểm soát truy cập của user tới các object trong database

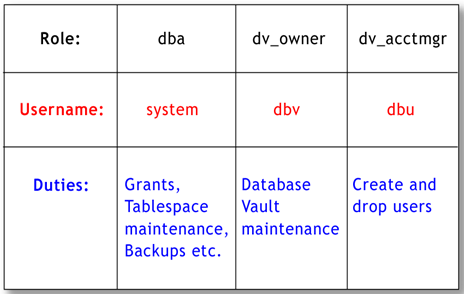
Mục đích:

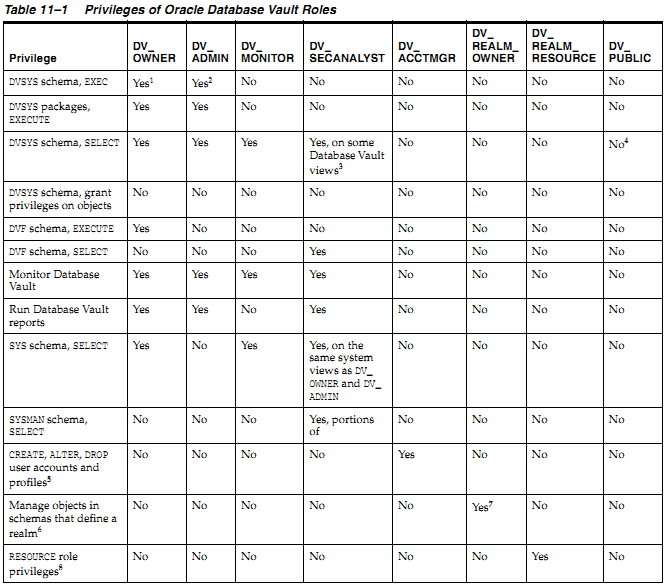
* Bảo đảm an toàn cho database từ các cuộc tấn công từ bên trong
* Bảo vệ dữ liệu khỏi DBA mà ko ảnh hưởng tới khả năng quản trị của họ

Nguyên lý hoạt động:

* Database Vault không thay thế mô hình điều khiển truy cập dữ liệu đã tồn tại trong Database mà nó hoạt động trước mô hình này
* Phân chia quyền lưc một cách rõ ràng bằng việc điều hướng truy cập người dùng (user)
* Đảm bảo rằng không ai có thể làm mọi việc ( kể cả DBA)

Các user quản trị :





Các thành phần của Oracle Database Vault:

* Oracle Database Vault Access Control Components:
  + Nhiệm vụ: Điều khiển truy câp dữ liệu trong database
  + Bao gồm các thành phần:
    - Realms: một tập hợp các thành phần như object, schema, roles cần được bảo mật
    - Command rules. Luật đặc biệt có thể được tạo ra kiểm soát cách người dùng thực hiện hầu hết các câu lệnh SQL như: SELECT, ALTER SYSTEM, DDL, DML
    - Factors: Tên của 1 biến hoặc 1 thuộc tính như: địa chỉ user, địa chỉ IP... Oracle Database Vault có thể nhận diện và đảm bảo an toàn.
    - Rule set: Một bộ quy tắc là một tập hợp của một hoặc nhiều quy tắc mà có thể kết hợp trong một lĩnh vực nào đ
    - Secure application roles: Một roles đặc biệt có thể được sử dụng dựa trên 1 tập luật ( rule set)
* Oracle Database Vault Administrator (DVA)
  + Là 1 ứng dụng java được dựng cho người quản trị có thể cấu hình các chính sách thông qua các interface của người dùng
  + Tập hợp các báo cáo thông tin cấu hình, hoạt động của hệ thống
* Oracle Database Vault Configuration Assistant (DVCA)
  + Hiện thị, hỗ trợ quá trình cài đặt DV
* Oracle Database Vault DVSYS and DVF Schemas
  + Lưu trữ nhưng object được secure bởi DV (roles, views, accounts, functions...)
  + DVF Schema chứa những fuction public và khởi động/khôi phục nó trong quá trình hoạt động
* Oracle Database Vault PL/SQL Interfaces and Packages
  + Cho phép người quản trị DV hoặc người lập trình ứng dụng có thể cấu hình các chính sách cần thiết
* Oracle Database Vault and Oracle Label Security PL/SQL APIs
  + Cho phép người quản trị DV có thể nhậm biết chính sách của label và áp dụng nó vào database
* Oracle Database Vault Reporting and Monitoring Tools
  + Tạo báo cáo định kỳ vê hoạt động của DV

# Các công việc đã thực hiện

Nghiên cứu nguyên lý hoạt động của Database Vault:

* Ý tưởng chính là bảo vệ các dữ liệu nhạy cảm khỏi **sys**
* Thực hiện các tính năng bảo mật khác như:
  + Bảo vệ các schema
  + Giới hạn người/ phân mềm truy cập ...
  + ....

Thực hiện cấu hình các thành phần của Database Vault ( theo tutorial)

* Cấu hình Realm
* Cấu hình Command Rule
* Cấu hình Factor
* Cấu hình Cấu hình Secure Application Roles

Các bài lab đã thực hiện:

* Cài đặt Database Vault trên Oracle Enterprise Manager
* Cài đặt Database Vault trên Oc4j server standalone
* Tutorial: Securing a Schema from DBA Access
* Tutorial: Using a Command Rule to Control Table Creations by a User
* Tutorial: Preventing Ad Hoc Tool Access to the Database
* Tutorial: Granting Access with Database Vault Secure Application Roles

# Cài đặt Database Vault

Phiên bản áp dụng: 11gr2 ( 11.2.0.4.0 )

Sau khi cài đặt Oracle Database xong,tính năng Database Vault đã được tích hợp sẵn, nếu muốn sử dụng thì cần phải enable tính năng này lên

## Cài đặt Oracle Enterprise Manager Database Console

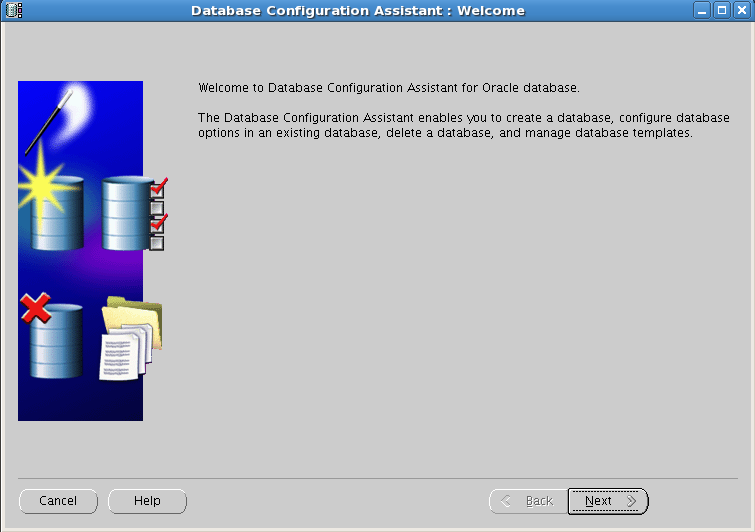
Theo mặc định thì EM đã được cài đặt cùng Database.

Nếu chưa cài đặt thì làm như sau:

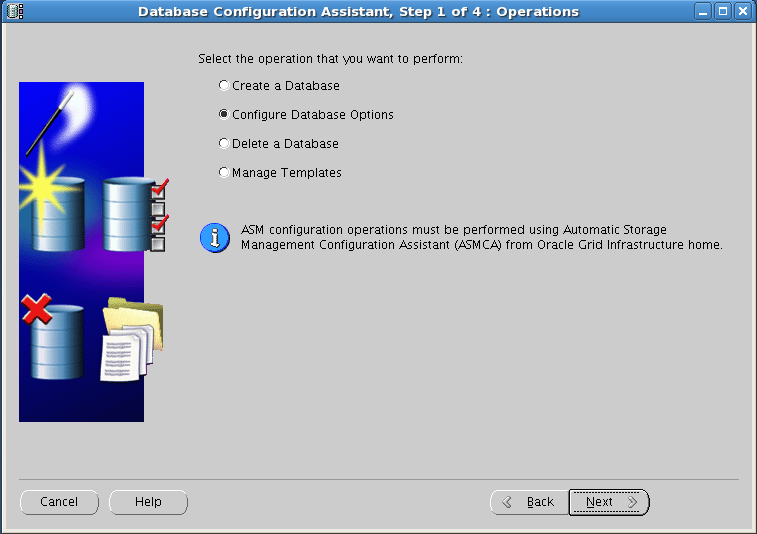
* Truy cập user oracle ( OS ):

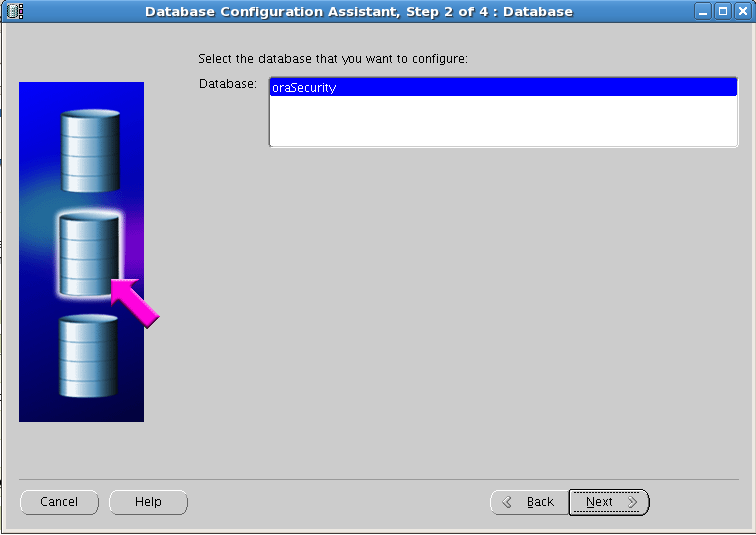
[oracle@localhost ~]$ dbca

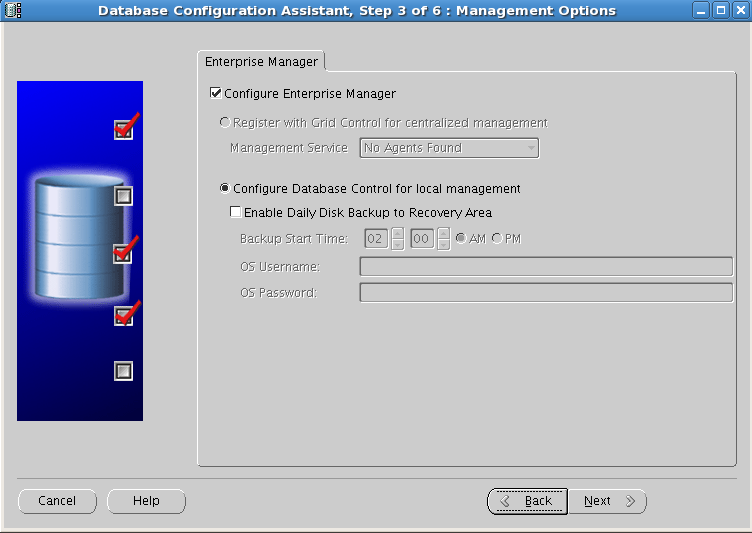
* Chọn **Next**

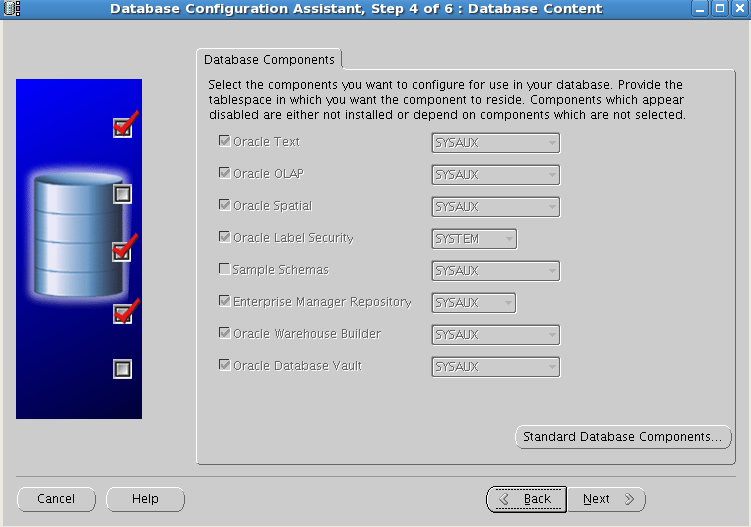


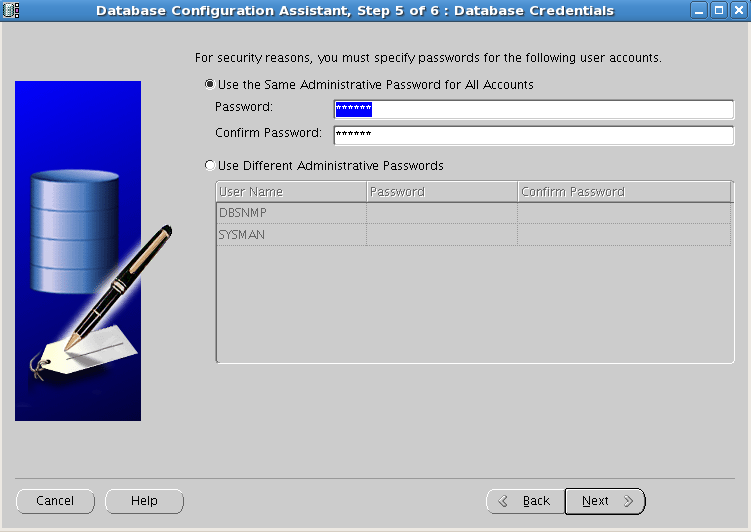
* Chọn **Configure Database Options** -> **Next**



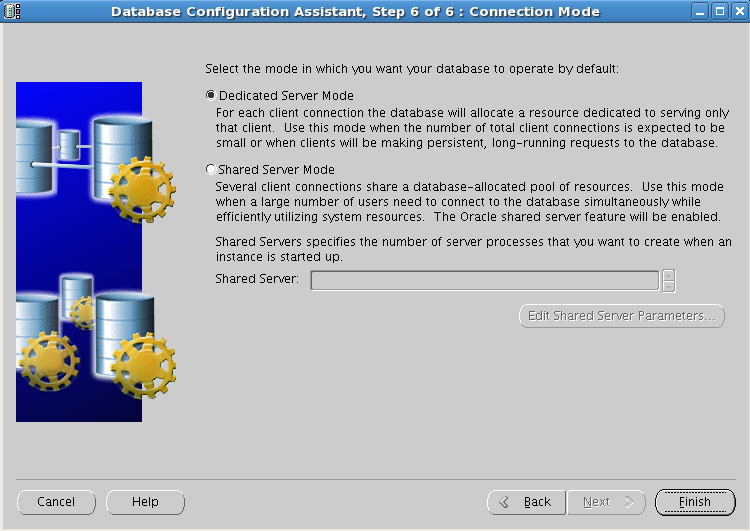
* Chọn Database muốn cài đặt EM và chọn **Next**
* Chọn Configure **Enterprise Manager** và chọn **Next**



* Chọn **Next**
* Điền mật khẩu cho các user quản trị EM và chọn **Next**



* Chọn **Finish** và chờ đợi hoàn thành quá trình cài đặt



Sau khi đã cài đặt xong, kiểm tra trạng thái của EM

[oracle@localhost ~]$ emctl status dbconsole

Oracle Enterprise Manager 11g Database Control Release 11.2.0.3.0

Copyright (c) 1996, 2011 Oracle Corporation. All rights reserved.

https://localhost.localdomain:1158/em/console/aboutApplication

Oracle Enterprise Manager 11g is running.

## Dừng Database, Database Control console và listener.

* Dừng Database: ( đối với Rac thì cần dừng Database ở tất cả các node)

[oracle@localhost ~]$ sqlplus

SQL> CONNECT sys as sysoper

Enter password: password

SQL> SHUTDOWN IMMEDIATE

SQL> EXIT

* Dừng Database Control console

[oracle@localhost ~]$ emctl stop dbconsole

* Dừng Listener

[oracle@localhost ~]$ lsnrctl stop

## Bật tính năng Oracle Database Vault

Phải bật tính năng **Oracle Label Security** trước khi sử dụng Oracle Database Vault

[oracle@localhost ~]$ cd $ORACLE\_HOME/rdbms/lib

[oracle@localhost ~]$ make -f ins\_rdbms.mk dv\_on lbac\_on ioracle

## Khởi động lại Database và Listener

* Khởi động Database: ( đối với Rac thì cần khởi động lại ở tất cả các node)

[oracle@localhost ~]$ sqlplus

SQL> CONNECT sys as sysoper

Enter password: password

SQL> startup

SQL> exit

* Khởi động Listener

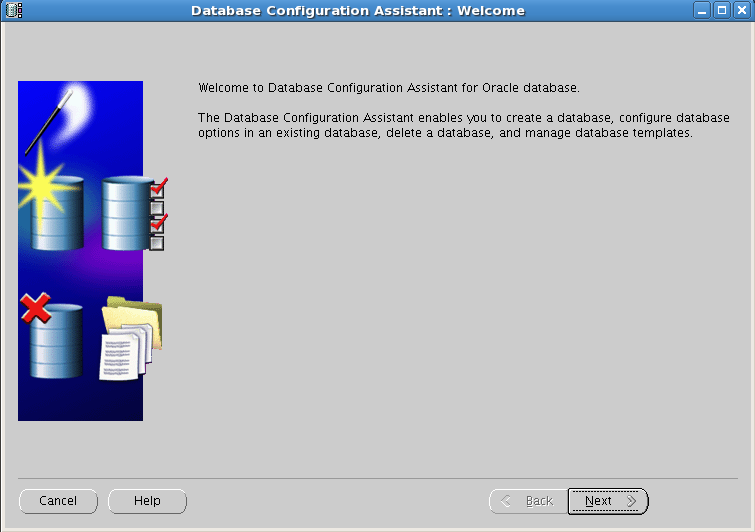
[oracle@localhost ~]$ lsnrctl start

## Áp dụng Database Vault vào Database

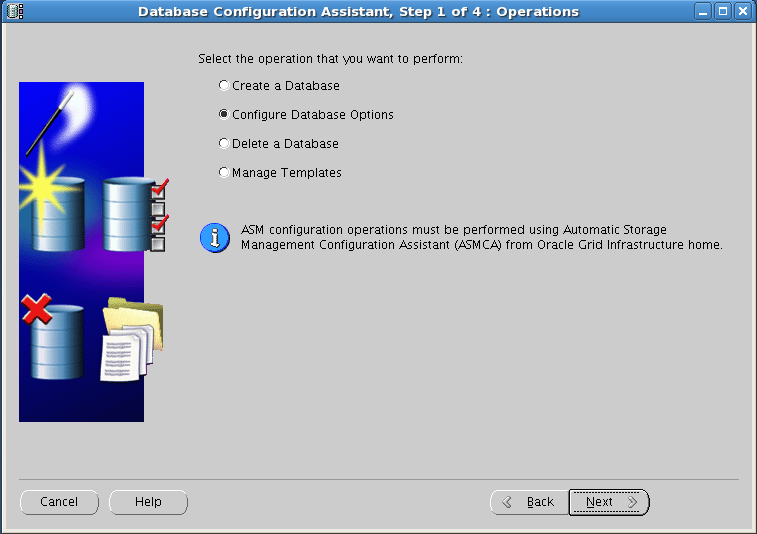
* Truy cập user oracle ( OS ):

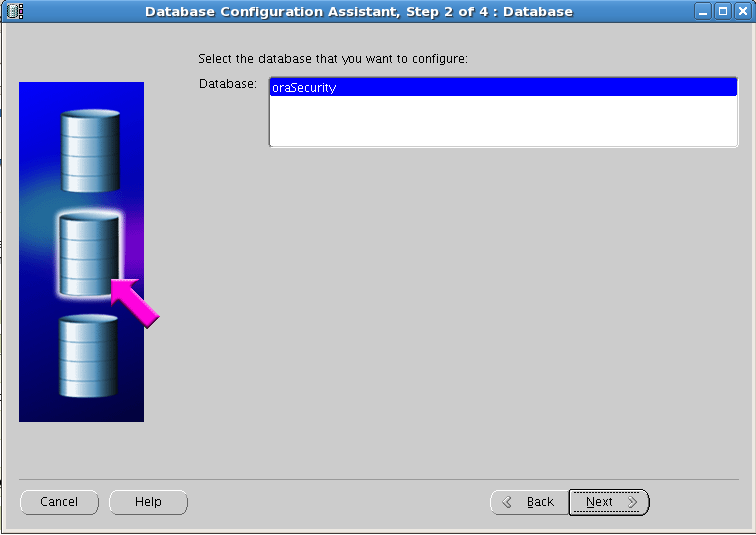
[oracle@localhost ~]$ dbca

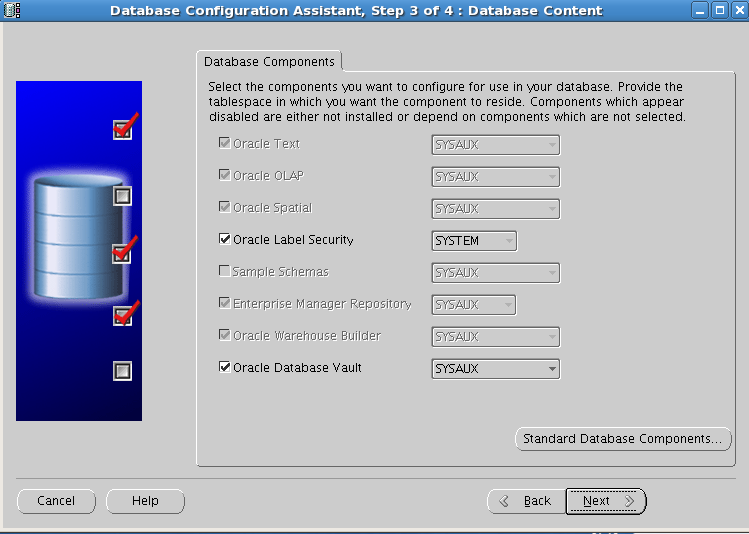
* Chọn **Next**



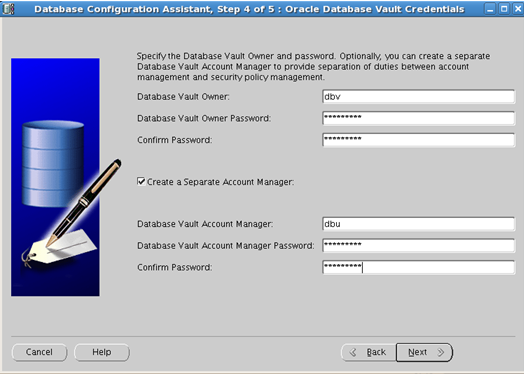
* Chọn **Configure Database Options** -> **Next**



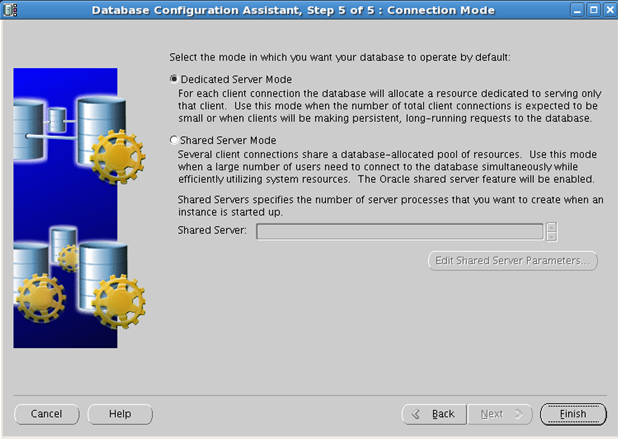
* Chọn Database muốn cài áp dụng Database Vault và chọn **Next**
* Tích vào **Oracle Label Security** và **Oracle Database Vault** và chọn **Next**



* Điền thông tin **user quản trị** ( username, password ) và chọn **Next**
  + **Database Vault Owner:** User quản trị chính sách
  + **Database Vault Account Manager:** User quản trị các user khác



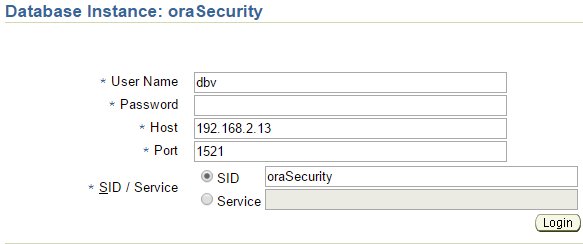
* Tích vào **Delicated Server Mode** và chọn **Finish**



## Đăng nhập vào Enterprise Manager quản lý Database Vault

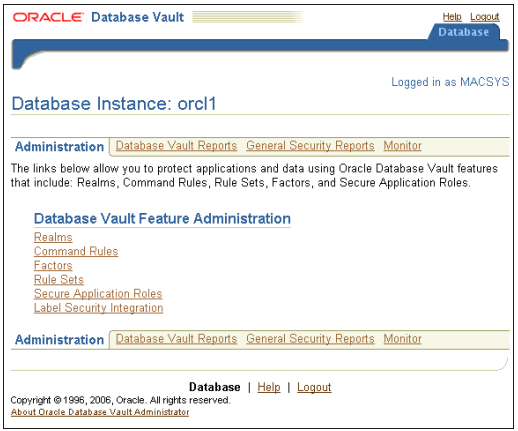
Đăng nhập vào địa chỉ:

[*https://host\_name:port/dva*](https://host_name:port/dva)



* User Name: user có roles như dv\_owner hoặc dv\_acctmgr
* Password: mật khẩu
* Host: địa chỉ của DB
* Port: port sử dụng của DB ( mặc định là 1521)
* SID/Service: định danh cho DB

Đăng nhập thành công:



# Cấu hình Realm

Khái niệm:

* Realm là 1 tập hợp các đối tượng được gom nhóm để được bảo vệ khỏi các truy cập trái phép

Ví dụ: Schema ( table, view, package), role

* Realm ko ảnh hướng tới các quyền được gán trước khi Database Vault được enable . Việc này đảm bảo các ứng dụng vẫn hoạt động bình thường trước và sau khi Database Vault được enable

Các thành phần của Realm:

* **Name :** định danh của Realm
* **Audit Options:** Chế độ theo dõi ( nên để theo default)
* **Realm Secured Objects:** nhóm được bảo vệ ( schema, role....)
* **Realm Authorizations:** đối tượng được truy cập:
  + **Owner:** User được phép gán quyền truy cập cho user khác
  + **Participant**: User chỉ được phép truy cập xem dữ liệu

Ví dụ: Tạo 1 Realm bảo vệ schema của user duong

* User sys ko còn truy cập vào các object của user duong nữa
* Owner của Realm là duong có quyền gán các quyền cho các user khác

# Cấu hình Command Rule

Khái niệm:

* Command rule là các luật được đề ra để bảo vệ các câu lệnh SQL ( DDL và DML).
* Ví dụ: alter , create, drop ....

Các thành phần của Command rule:

* **General :**
  + Command : Câu lệnh được bảo vệ
  + Status: Trạng thái của Command rule
* **Applicability:** 
  + Object Owner : user sở hữu đối tượng sẽ bảo vệ
  + Object Name : Tên chính xác của đối tương sẽ bảo vệ
* **Rule Set:** Cập nhật vào nhóm các câu lệnh
  + **Enable:** cho phép xảy ra
  + **Disable:** không cho phép xảy ra

# Cấu hình Rule Set

Khái niệm:

* Command rule là các luật được đề ra để bảo vệ các câu lệnh SQL ( DDL và DML).
* Ví dụ: alter , create, drop ....

Các thành phần của Command rule:

* **General :**
  + Command : Câu lệnh được bảo vệ
  + Status: Trạng thái của Command rule
* **Applicability:** 
  + Object Owner : user sở hữu đối tượng sẽ bảo vệ
  + Object Name : Tên chính xác của đối tương sẽ bảo vệ
* **Rule Set:** Cập nhật vào nhóm các câu lệnh
  + **Enable:** cho phép xảy ra
  + **Disable:** không cho phép xảy ra

# Cấu hình Factors

# Cấu hình Secure Application Roles

# Tích hợp Database Vault với các sản phẩm khác

# Các hoạt động quản trị trên Database Vault