Oracle Database 10g Release 2 Database Vault – Controlling Access to Applications

An Oracle White Paper
August 2006

Oracle Database Vault Overview

Oracle Database Vault enables you to

- Restrict the DBA and other privileged users from accessing application data
- Protect the database and applications from unauthorized changes
- Enforce strong controls over who, when, and where application can be accessed

These features help you to address regulatory compliance, insider threats, and protection of personally identifiable information.

This paper is the third in a series of whitepapers that discuss and demonstrate real world use cases for the security provided by Oracle Database Vault. In this paper we discuss how Oracle Database Vault can be used to control access to applications. The business drivers for controlling access to applications include

- Enforce operational security policies for strong internal control
- Limit the use ad-hoc query tools to bypass the application for regulatory compliance
- Control the use of powerful commands for separation of duty and accountability
- IT/DBA Outsourcing
- Online hosted applications

Controlling Access to Applications and Databases

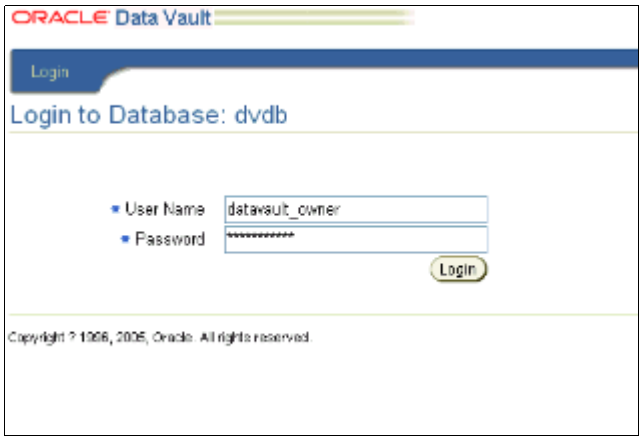
Oracle Database Vault uses the concepts of Command Rules and Factors to control access to applications. Command Rules can utilize information stored by environment variables called Factors to decide whether to allow a certain command to execute or not. Oracle Database Vault comes seeded with a number of Factors like Client IP, Database_IP, Session_User … etc. You can create your own Factors in addition to the existing ones. The following steps outline the process for creating a Command Rule and associating a Rule Set to it.

Creating a Command Rule with a Rule Set attached:

Command Rules and Rule Sets can be created easily and quickly. You can do this using either the Database Vault Administration web interface (DVA) or the Database Vault Application Programming Interface (API).

Here, we show how we can control access to the application to a specific IP address.

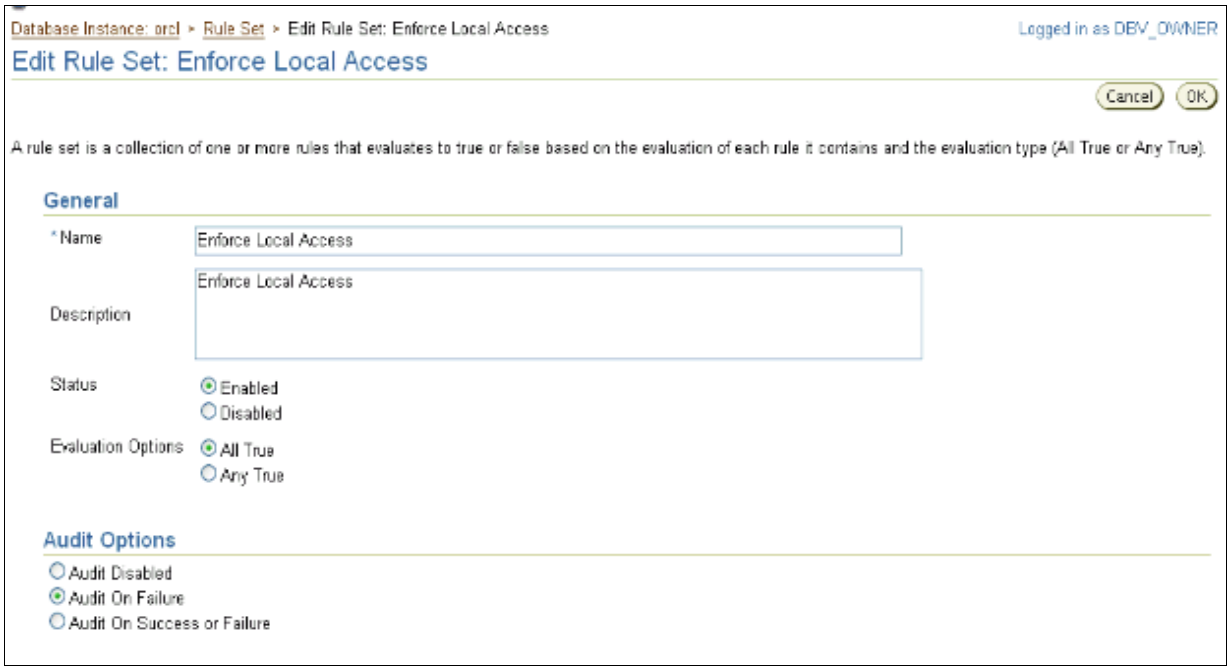
1. Point your browser to DVA URL. The URL will have the following form: http://hostname:portnumber/dva Login using the Database Vault owner account.



2. Click on ***Rule Sets***.
   In the Rule Sets summary screen click on ***Create.*** Fill out the create Rule Set screen as follows:
   Name: **Enforce Local Access,** Description: **Enforce Local Access**
   Keep the default values for the rest of the attributes and click ***OK***

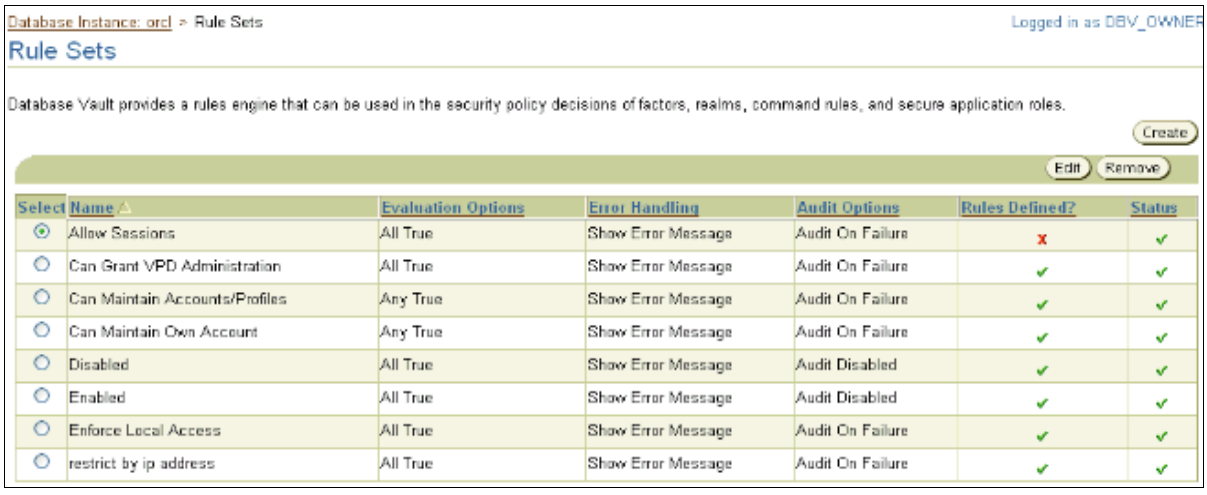
   Here we will try to prevent the DBA from executing ***alter system*** commands when not connected to the database server directly.

   This is just to show how we can use the IP address as a factor to decide whether to allow certain operations to happen or not.



3. In the Rule Sets summary screen select ***Enforce Local Access*** and click ***Edit*** then scroll down the page.

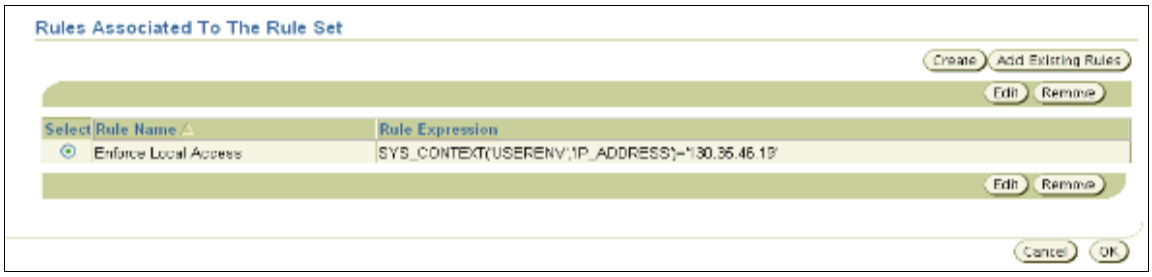
   Now that we created the Rule Set "Enforce Local Access" we need to create a rule for it



Select	Name	Evaluation Options	Error Handling	Audit Options	Rules Defined?	Status
◉	Allow Sessions	All True	Show Error Message	Audit On Failure	x	✓
○	Can Grant VPD Administration	All True	Show Error Message	Audit On Failure	✓	✓
○	Can Maintain Accounts/Profiles	Any True	Show Error Message	Audit On Failure	✓	✓
○	Can Maintain Own Account	Any True	Show Error Message	Audit On Failure	✓	✓
○	Disabled	All True	Show Error Message	Audit Disabled	✓	✓
○	Enabled	All True	Show Error Message	Audit Disabled	✓	✓
○	Enforce Local Access	All True	Show Error Message	Audit On Failure	✓	✓
○	restrict by ip address	All True	Show Error Message	Audit On Failure	✓	✓

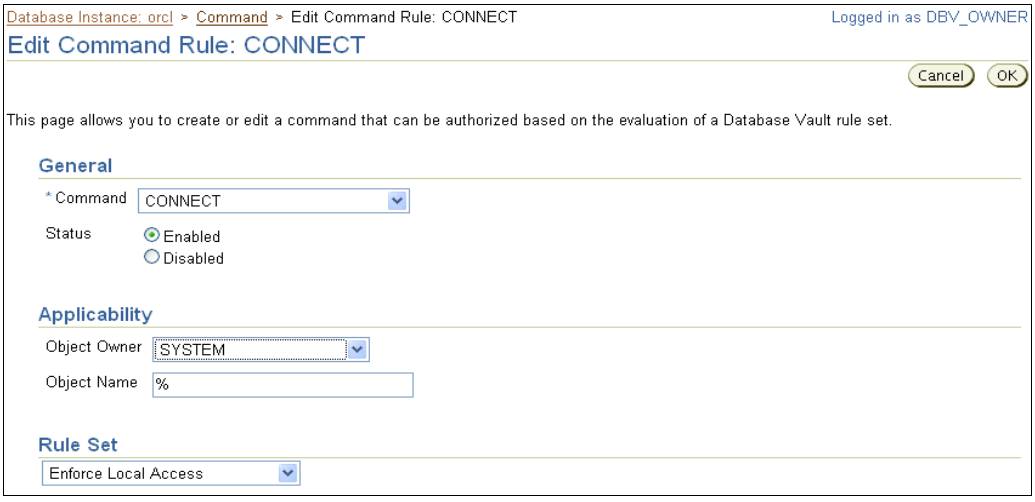
4. Scroll down and under the section "Rules Associated to the Rule Set" Click on ***Add Existing Rules***.
   Under Available Rules, select ***Enforce Local Access*** and click on ***Move.*** Then click ***OK***
   In the Rule Set Edit screen, click ***OK*** again

   Here we create a rule and attach it to the rule set. The rule set says: Disallow DBA on a non-local IP from executing *alter system* commands.



5. In the Rule Sets summary screen, click on the ***Database Instance:*** link which will take you to the main Administration screen. Click on ***Command Rules***
   In the Command Rules summary screen click on ***Create*** then fill out the attributes as follows:
   Command: **CONNECT,** Status: **Enabled,** Object Owner: SYS**,** Object Name: %
   Rule Set: **Enforce Local Access.** Then click ***OK***

   We associate the rule set created in the previous steps to Command Rule "CONNECT" we have just created.

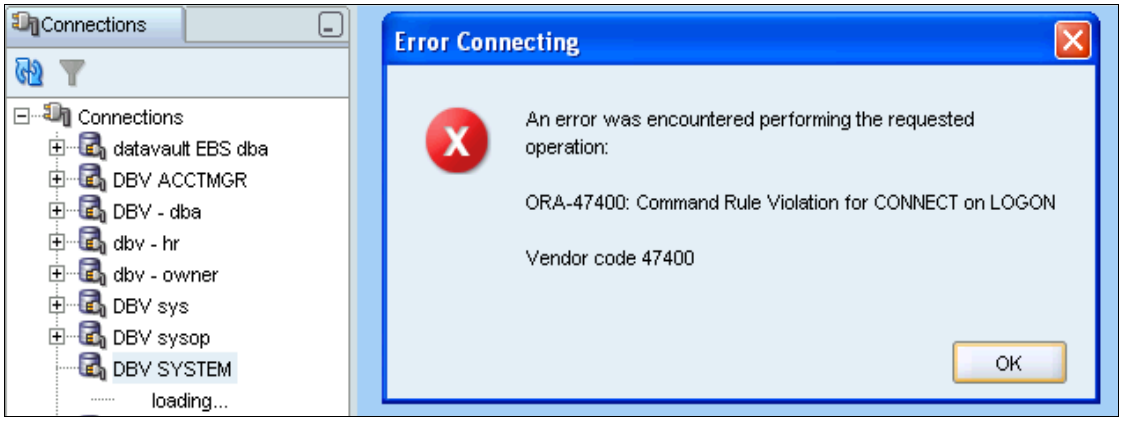


6. Start SQL Developer and try to login as a user SYSTEM. You will get an error.

   Here the DBA tries to login as the user SYSTEM from a client machine. Since the IP address of the DBA client machine does not match the local IP address of the database server, DBA gets an error (ora-01031: insufficient privileges).

   This is an example of how an IP address can be used as a factor in deciding whether to allow connecting to the database or not in Oracle Database Vault environment.

   Customers can use other factors that come with Oracle Database Vault or create their own and utilize them to implement their own security requirements.



API Steps:

1. Create rule set Enforce Local Access:

```
begin
  dvsys.dbms_macadm.CREATE_RULE_SET(
   rule_set_name => 'Enforce Local Access'
  ,description => 'Enforce Local Access'
  ,enabled => 'Y'
  ,eval_options => 1
  ,audit_options => 1
  ,fail_options => 1
  ,fail_message => ''
  ,fail_code => 0
  ,handler_options => 0
  ,handler => NULL);
end;
/
commit;
```

2. Create rule Enforce Local Access. The rule here has the same name as the rule set. This is OK since these are different objects.

```
begin
  dvsys.dbms_macadm.CREATE_RULE(
   rule_name => 'Enforce Local Access'
  ,rule_expr =>
'SYS_CONTEXT('USERENV','IP_ADDRESS')='130.35.46.19'');
end;
/
commit;
```

3. Add rule Enforce Local Access to rule set Enforce Local Access:

```
begin
  dvsys.dbms_macadm.ADD_RULE_TO_RULE_SET(
   rule_set_name => 'Enforce Local Access'
  ,rule_name => 'Enforce Local Access');
end;
/
commit;
```

4. Create command rule for ALTER SYSTEM command:

```
begin
  dvsys.dbms_macadm.CREATE_COMMAND_RULE(
   command => 'CONNECT'
  ,rule_set_name => 'Enforce Local Access'
  ,object_owner => 'SYS'
  ,object_name => '%'
  ,enabled => 'Y');
end;
/
commit;
```

Oracle Database 10g Release 2 - Database Vault
August 2006
Author: Kamal Tbeileh and Paul Needham

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com