Oracle Database 10g Release 2 Database Vault - Protecting the Database and 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 second 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 protect the database and applications from unauthorized changes. The business drivers for protecting the database and applications from unauthorized changes include

- Protection of company assets of business sensitive data from malicious or unauthorized changes
- Strong internal controls for regulatory compliance
- IT/DBA Outsourcing
- Online hosted applications

Protecting the Database and Applications

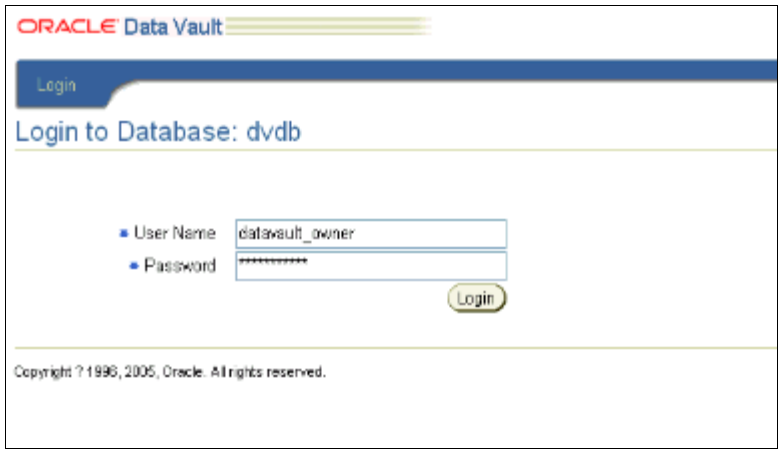
Oracle Database Vault uses the concept of a Command Rule to control the execution of most SQL commands by any user. Command Rules can control both Data Definition Language (DDL) SQL commands and Data Manipulation Language (DML) SQL commands. You can use Command Rules to protect the database and applications from malicious or unauthorized changes from any user including the owner of the application. The following steps outline the process for creating a Command Rule.

Create Command Rules:

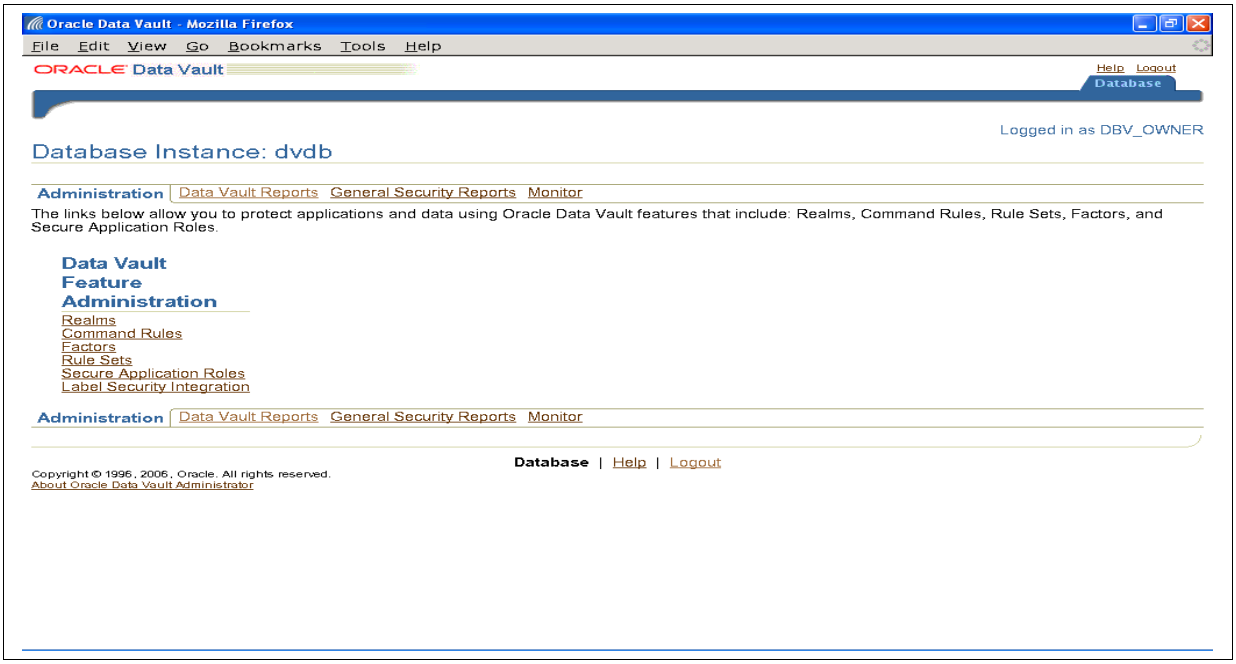
Command Rules can be created easily and quickly. You can do this using either the Database Vault Administration web interface (DVA) or the Database Vault Application Programming Interface (API).

Here, we show how we can protect the HR database and application from the **DROP TABLE** command. We also list, at the end of this section, a number of additional commands that the HR application can be protected from.

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.

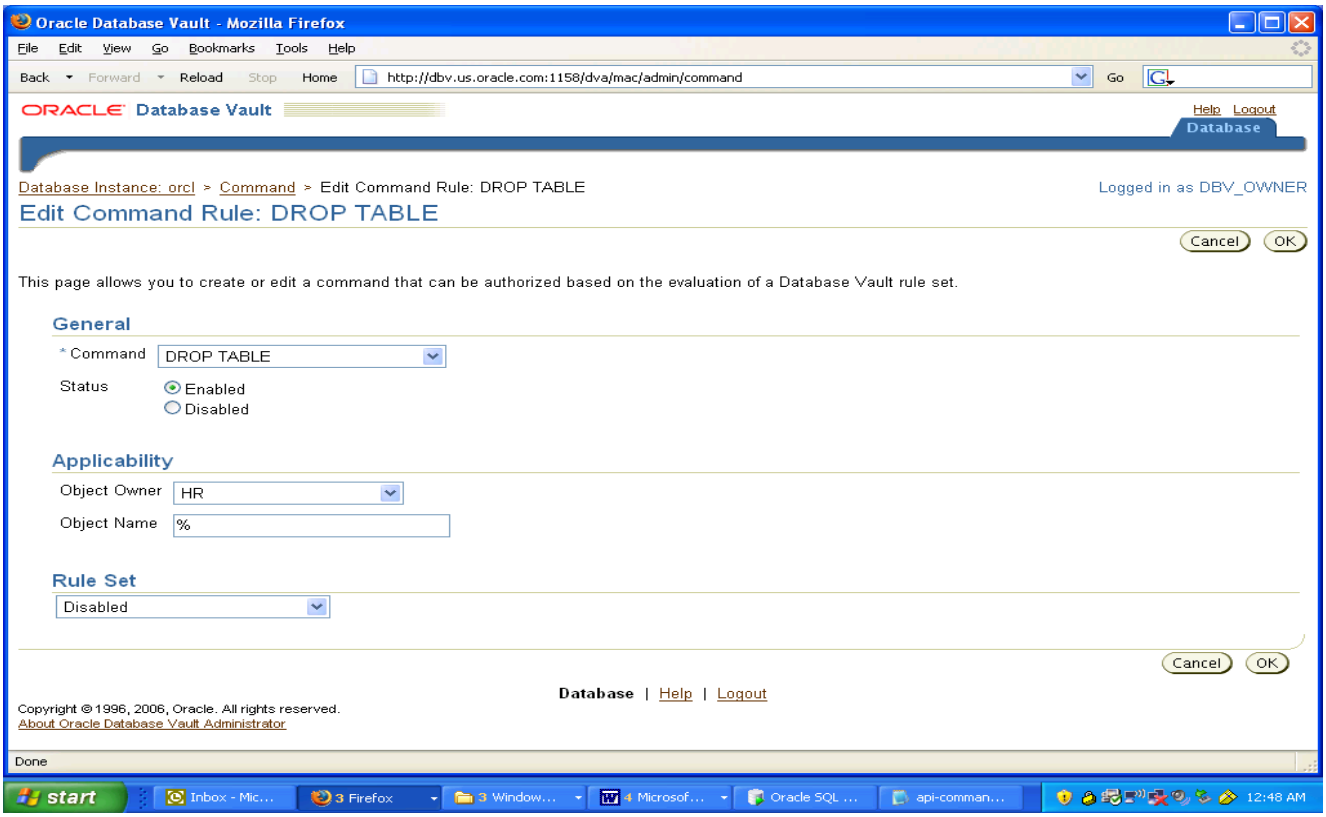


2. Click on ***Command Rules***
   In the Command Rules summary screen click on ***Create***



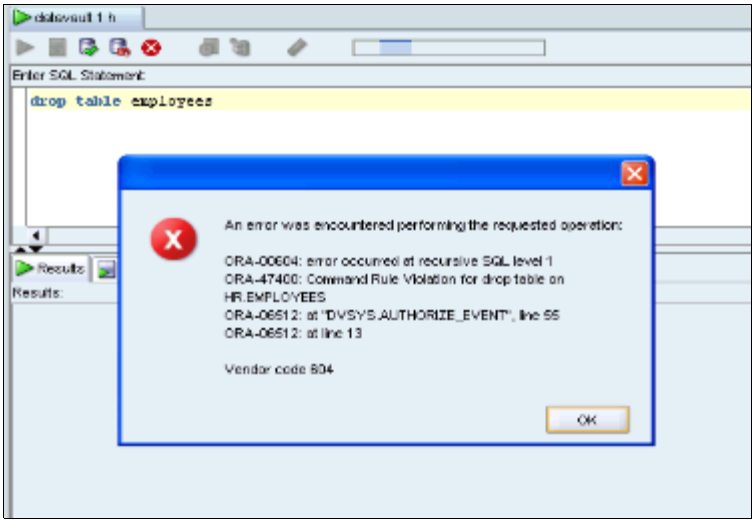
3. then fill out the attributes as follows:
   General Section: Command: **DROP TABLE,** Status: **Enabled**
   Applicability: Object Owner: **HR,** Object Name: %
   Rule Set: **Disabled.** Then click ***OK***

   This will prevent any database user, including the HR user from dropping any table in the HR application.



4. To verify login as the hr user to SQL Developer and try to drop the employees table as follows:

Drop table employees;
You will get errors. HR user is not able to drop a table in his own schema thanks to Command Rule protection.



5. The same steps can be done to protect from other SQL commands. If any of these commands need to be allowed the database vault owner account can enable it temporarily. Or it can be associated with a rule set to be enabled based on some specific conditions.
The following is a minimal list of SQL commands the customer should consider creating Command Rules for them to protect his database and application.
ALTER TABLE
CREATE TABLE
TRUNCATE TABLE
CREATE CLUSTER
DROP CLUSTER
CREATE DATABASE LINK
DROP DATABASE LINK
DROP INDEX
DROP SEQUENCE
DROP TABLESPACE
CREATE VIEW
DROP VIEW
CREATE SYNONYM
DROP SYNONYM

API Steps:

1. Create command rule for DROP TABLE command:

```
begin
 dvsys.dbms_macadm.CREATE_COMMAND_RULE(
  command => 'CREATE TABLE'
 ,rule_set_name => 'Disabled'
 ,object_owner => 'HR'
 ,object_name => '%'
 ,enabled => 'Y');
end;
/
commit;
```

2. Create command rule for CREATE TABLE command:

```
begin
 dvsys.dbms_macadm.CREATE_COMMAND_RULE(
  command => 'DROP TABLE'
 ,rule_set_name => 'Disabled'
 ,object_owner => 'HR'
 ,object_name => '%'
 ,enabled => 'Y');
end;
/
commit;
```

3. Create command rule for ALTER TABLE command:

```
begin
 dvsys.dbms_macadm.CREATE_COMMAND_RULE(
  command => 'ALTER TABLE'
 ,rule_set_name => 'Disabled'
 ,object_owner => 'HR'
 ,object_name => '%'
 ,enabled => 'Y');
end;
/
commit;
```

4. Create command rule for TRUNCATE TABLE command:

```
begin
 dvsys.dbms_macadm.CREATE_COMMAND_RULE(
  command => 'TRUNCATE TABLE'
 ,rule_set_name => 'Disabled'
 ,object_owner => 'HR'
 ,object_name => '%'
 ,enabled => 'Y');
end;
/
commit;
```

Oracle Database 10g Release 2 - Database Vault
August 2006
Author: Kamal Tbeileh, 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

Copyright © 2006, Oracle. All rights reserved.
This document is provided for information purposes only and the contents hereof are subject to change without notice.
This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.
Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.