Database Vault

Why Database Vault?

- Protecting Access to Application Data
    - “Legal says our DBA should not be able to read financial records, but the DBA needs to access the database to do her job. What do we do?”
    - “Our auditors require that we separate account creation from granting privileges to accounts.”
    - “No user should be able to by-pass our application to access information in the database directly.”
    - “New DBAs should not be able to make database changes without a senior DBA being present.”

Why Database Vault?

- Regulations such as Sarbanes-Oxley (SOX) and Graham-Leach Bliley Act (GLBA), and Basel II require **Strong Internal Controls** and **Separation of Duty**

- Internal threats are a much bigger concern today require enforcement of operational security policies - **Who, When, Where** can data be accessed?

- Database consolidation strategy requires preventive measures against access to application data by **Powerful (DBA)** users

Common Security Problems

- I have requirements around SOX and PCI, how can I prevent my DBA from looking at the application data, including Credit Cards and Personal Information?

- How can I prevent un-authorized modifications to my application and database?

Ad-Hoc Query
On Financial Data

Applications

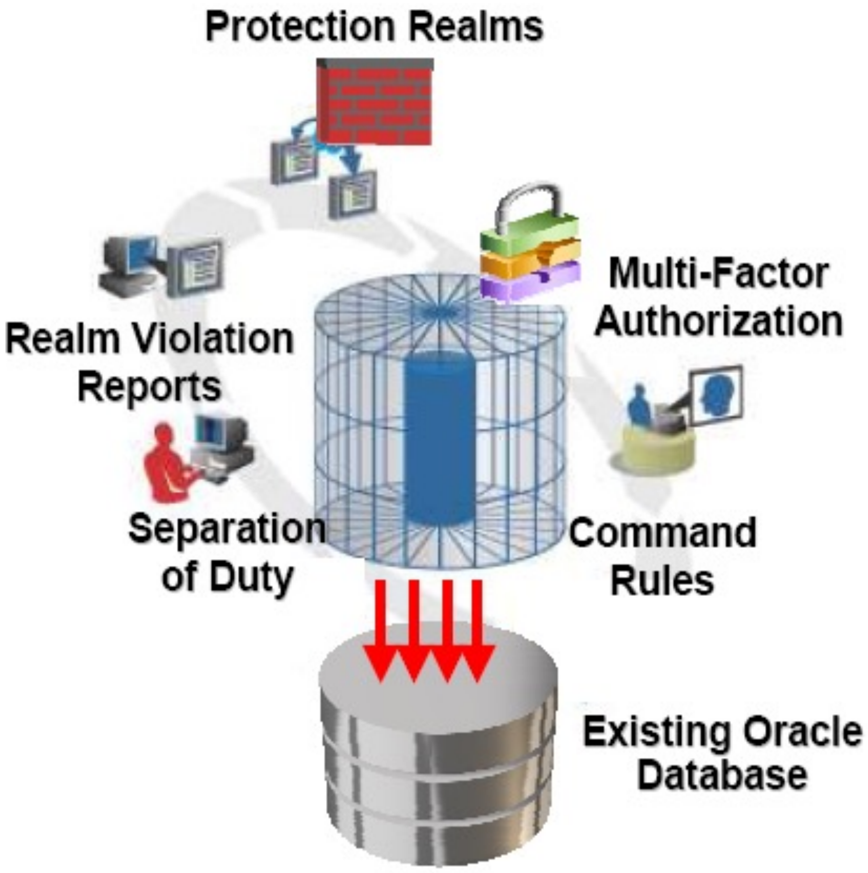
Ad-Hoc Query
Tool

Remote DBA
Services

Oracle Database Vault

Feature Overview

- Controls on privileged users
  - Restrict privileged users from accessing application data
  - Enforces separation of duty
- Real time access controls
  - Controls access based on IP address, authentication method, time of day,….
- Transparency
  - No changes to applications required



Database Vault

True “Separation of Duty”

- Protect any database object from any users *(realm)*
  - Function, job, package, synonym, trigger, view, table
  - Prevent users from viewing application data
- Prevent DBA users from creating powerful users
- Any user from executing a command *(command rule)*
  - Alter table, drop user, insert, create index, analyze
- Protect object from schema owner
  - HR user cannot modify HR objects
- Leverage sys_context *(multi-factor authorization)*
  - Only modify database structure from local IP
  - Only accept DML statement based on date or time
  - Leverage built-in or user defined factors
    - Machine, User, Domain, Language, Protocol, etc.

Command Rule Flexibility

Alter Database
Alter Function
Alter Package Body
Alter Session
Alter Table
Password
Change Password
Create Function
Create Database Link
Create Package Body
Create Table
Noaudit
Create Tablespace
Update
Execute

Alter Database
Audit
Alter Procedure
Alter System
Alter Trigger
Alter Tablespace
Connect
Create Index
Create Procedure
Create User
Grant
Rename
Create Trigger
Insert
Select

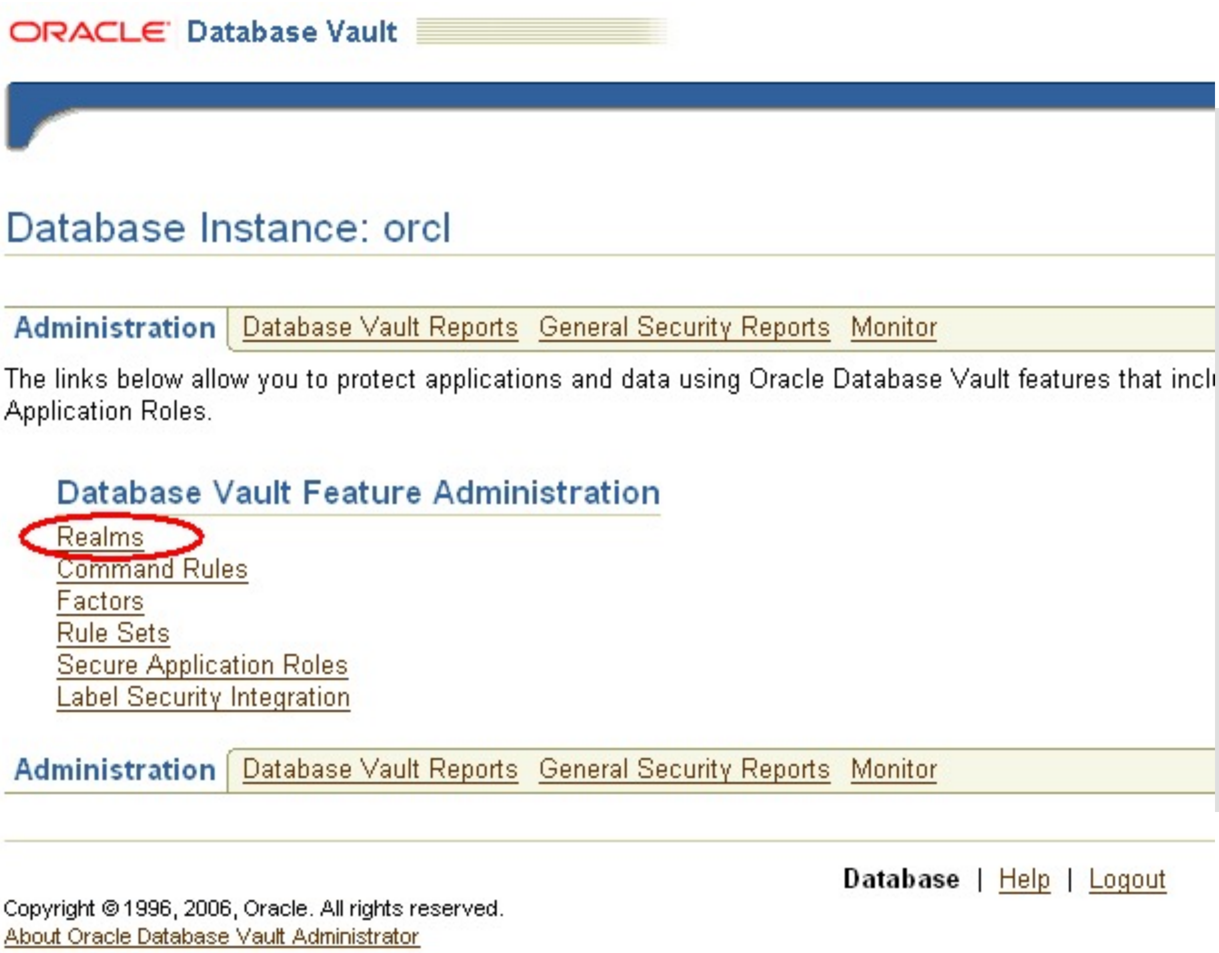
Alter Table
Alter Tablespace
Alter Profile
Alter Synonym
Alter User
Alter View
Comment
Create Package
Create Role
Create View
Insert
Lock Table
Truncate Table
Delete

Built-In Factors

Authentication Method	Session User	Client IP	Database Name
Domain	Machine	Database Domain	Database Instance
Network Protocol	Database IP	Enterprise Identity	Proxy Enterprise Identity
Language	Database Hostname	Date	Time

*** Additional factors can be defined**

Web Based Administrative Interface



Database Instance: orcl

The links below allow you to protect applications and data using Oracle Database Vault features that incl
Application Roles.

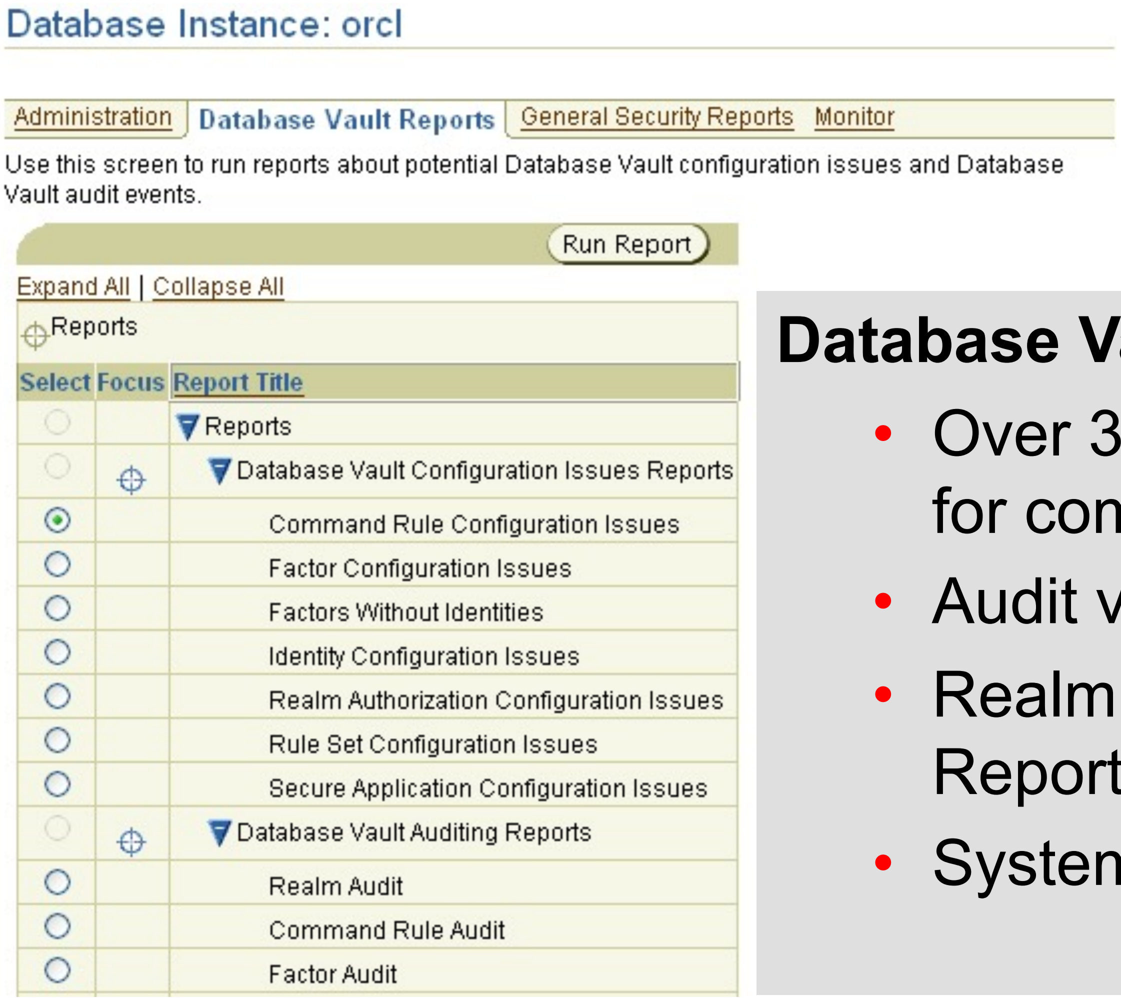
Database Vault Feature Administration

Copyright © 1996, 2006, Oracle. All rights reserved.
About Oracle Database Vault Administrator

Web Based Management

- Realms
- Rules
- Factors
- Reports
- Dashboard

Oracle Database Vault Reports



Database Instance: orcl

Use this screen to run reports about potential Database Vault configuration issues and Database Vault audit events.

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

Database Vault Reporting

- Over 3 dozen security reports for compliance
- Audit violation attempts
- Realm, Rule and Factor Reports
- System and Public Privileges

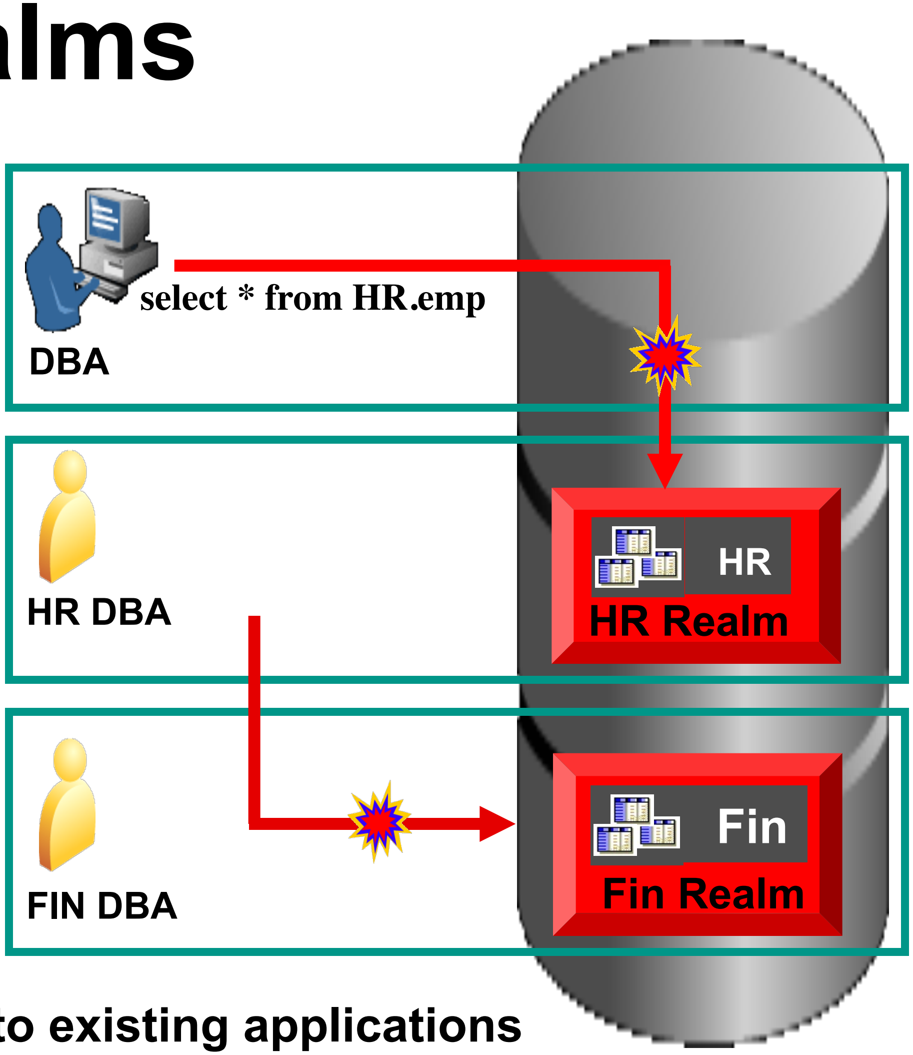
Oracle Database Vault Realms

- Database DBA views HR data

  Compliance and protection from insiders

- HR DBA views Fin. data

  Eliminates security risks from server consolidation



Realms can be easily applied to existing applications with minimal performance impact

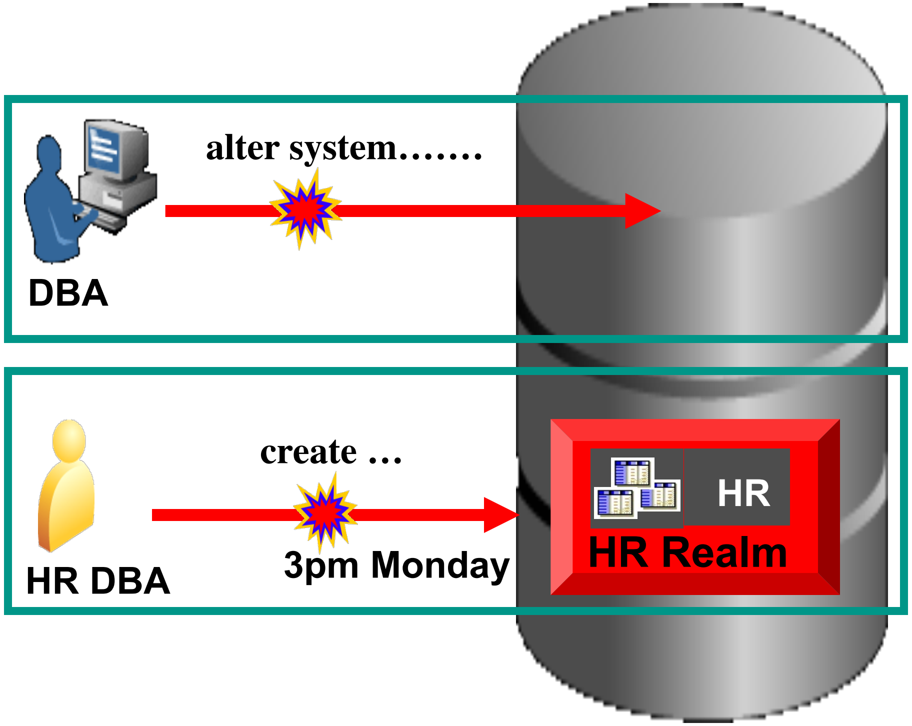
Oracle Database Vault
Rules & Multi-factor Authorization

- Database DBA attempts remote "*alter system*"

  Rule based on IP Address blocks action

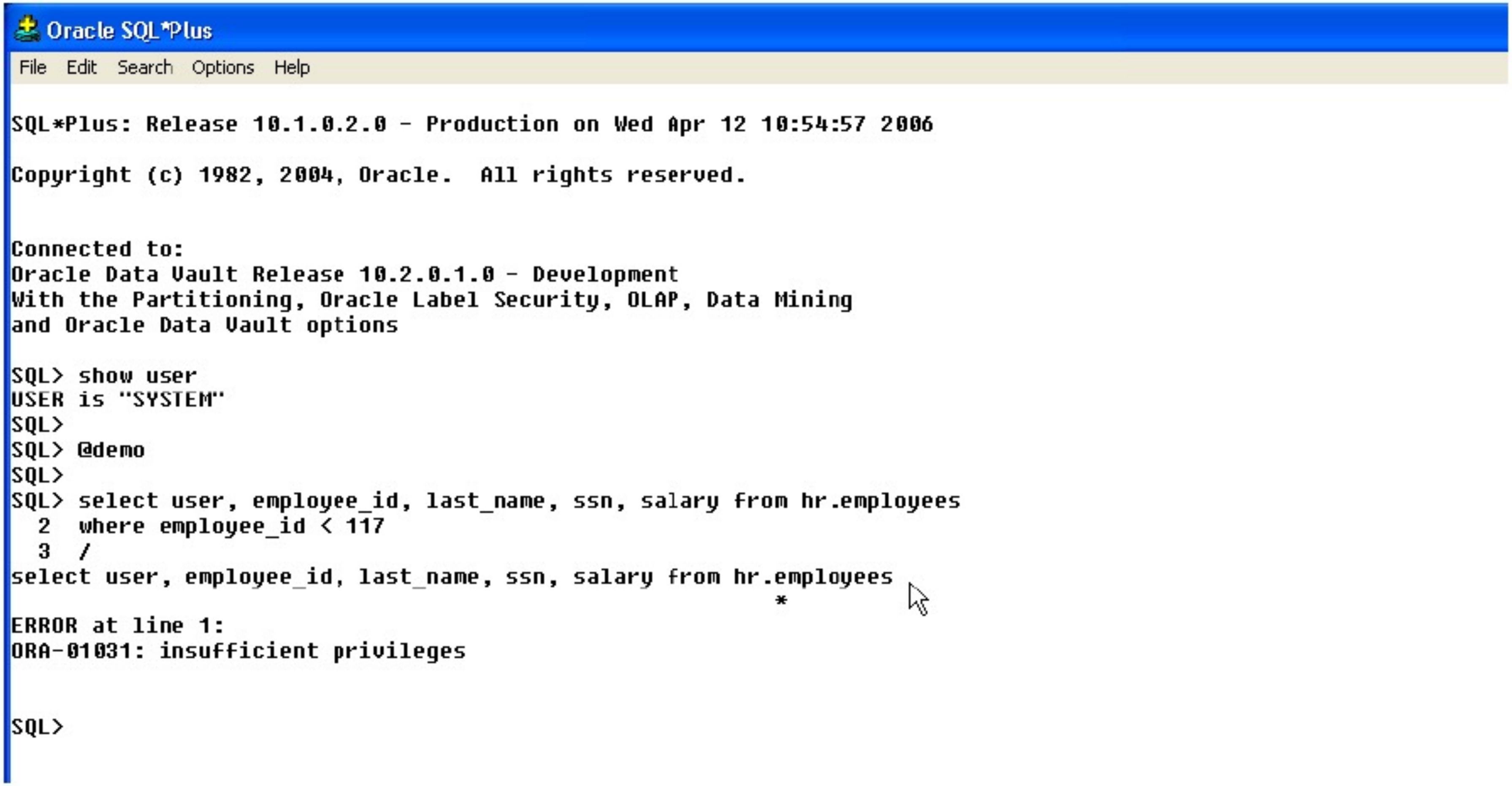
- HR DBA performs unauthorized actions during production

  Rule based on Date and Time blocks action



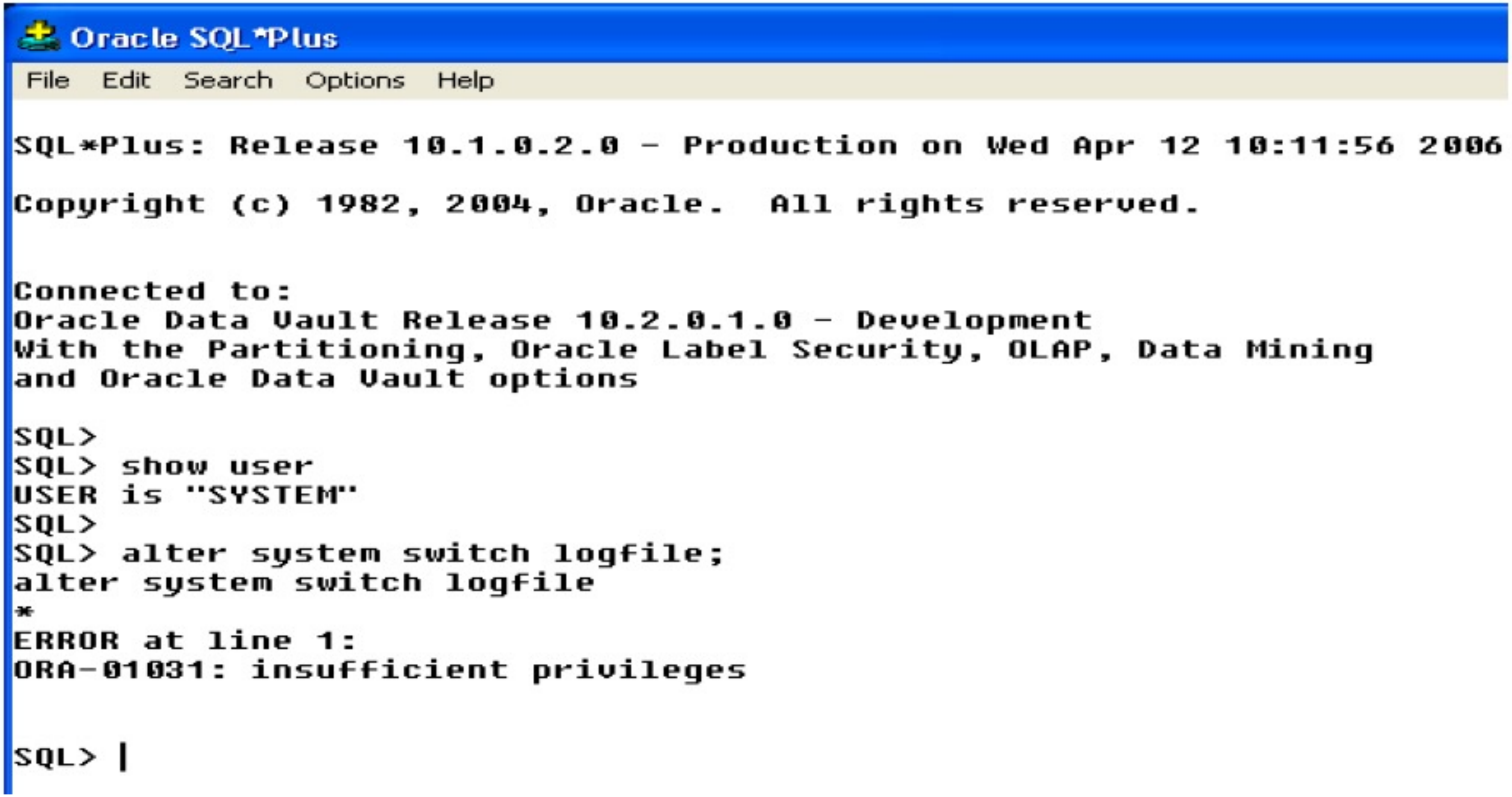
Factors and Command Rules provide flexible and adaptable security controls

Oracle System User Blocked



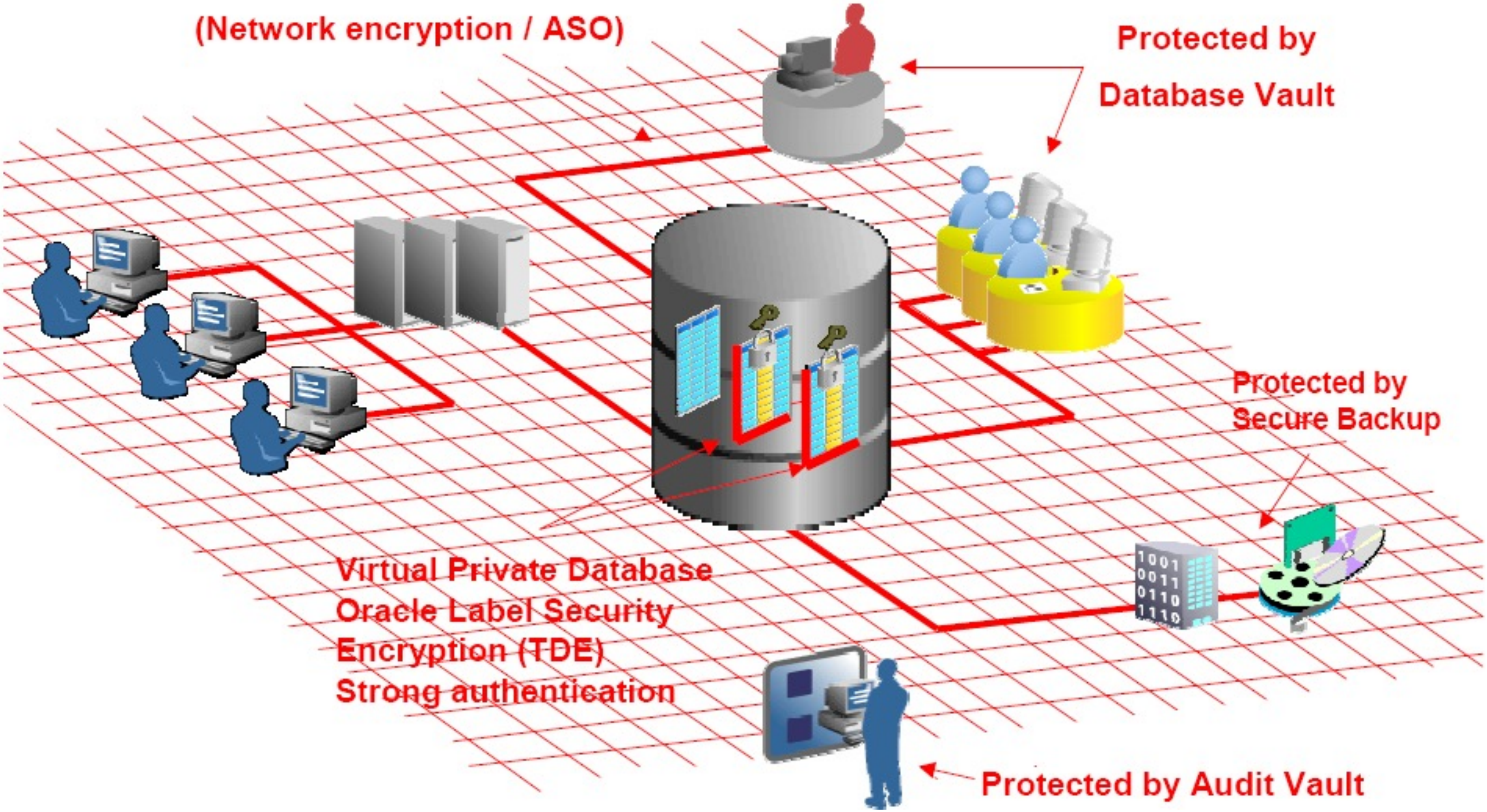
```
SQL*Plus: Release 10.1.0.2.0 - Production on Wed Apr 12 10:54:57 2006

Copyright (c) 1982, 2004, Oracle.  All rights reserved.


Connected to:
Oracle Data Vault Release 10.2.0.1.0 - Development
With the Partitioning, Oracle Label Security, OLAP, Data Mining
and Oracle Data Vault options

SQL> show user
USER is "SYSTEM"
SQL>
SQL> @demo
SQL>
SQL> select user, employee_id, last_name, ssn, salary from hr.employees
  2  where employee_id < 117
  3  /
select user, employee_id, last_name, ssn, salary from hr.employees
                                                       *
ERROR at line 1:
ORA-01031: insufficient privileges


SQL>
```

Database Vault Rules and Factors Block(Remote Intranet Connection)



```
SQL*Plus: Release 10.1.0.2.0 - Production on Wed Apr 12 10:11:56 2006

Copyright (c) 1982, 2004, Oracle.  All rights reserved.


Connected to:
Oracle Data Vault Release 10.2.0.1.0 - Development
With the Partitioning, Oracle Label Security, OLAP, Data Mining
and Oracle Data Vault options

SQL>
SQL> show user
USER is "SYSTEM"
SQL>
SQL> alter system switch logfile;
alter system switch logfile
*
ERROR at line 1:
ORA-01031: insufficient privileges


SQL> |
```

Oracle secured DB environment



(Network encryption / ASO)

Protected by

Database Vault

Protected by
Secure Backup

Virtual Private Database
Oracle Label Security
Encryption (TDE)
Strong authentication

Protected by Audit Vault

Hands-on Resources

- **Oracle Database Vault:**

http://www.oracle.com/technetwork/database/options/database-vault/index.html

- **Oracle Security Overview:** http://www.oracle.com/technology/deploy/security/database-security/index.html
- Lab3-1: Protect Application Data from DBA and Privileged Users (no submission)

http://st-curriculum.oracle.com/obe/db/11g/r1/prod/security/datavault/datavault.htm

- Lab3-2: Restrict DBA commands based on IP address (no submission)

http://st-curriculum.oracle.com/obe/db/11g/r1/prod/security/datavault/datavault2.htm

Oracle Database Vault Secured Installation

- Disallows connections with SYSDBA
  - Will affect
    - Oracle Data Guard and Data Guard Broker command line utilities
    - Oracle Recovery Manager command line utility
    - Oracle Real Application Clusters svrctl utility
    - Oracle ASM command line utilities
    - Custom DBA scripts
  - Can be re-enabled with the orapwd utility
- Enables password file and Turns off OS authentication
  - (e.g. sqlplus “/” as SYSDBA)

Oracle Database Vault Secured Installation

- Requires Oracle Label Security version 10.2.0.2
- Requires one of the following:
  - Enterprise Manager 10.2.0.2
  - 10g Application Server Containers for J2EE (OC4J)
- Cannot be installed into an Oracle home that contains an ASM instance
- Best practice is to create a database vault owner and database vault manager
- Requires 270 MB of disk space for DB Vault software
- Requires 400 MB of /tmp disk space
- OS authentication is turned off for all databases in the Oracle home
- Database vault can be enabled for each database in the Oracle home (optional)