
ORACLE®

THE INFORMATION COMPANY

ORACLE

Eric Siglin
Principal Instructor
Oracle University

ORACLE

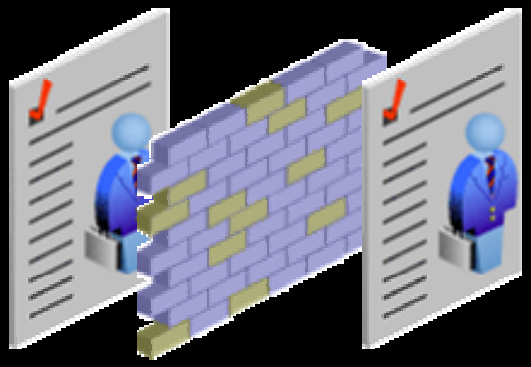
Dividing the Keys to the Kingdom

Separation of Duties with Oracle 10g Database Vault

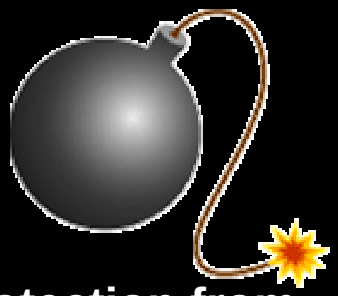
ORACLE

What Is Database Vault?

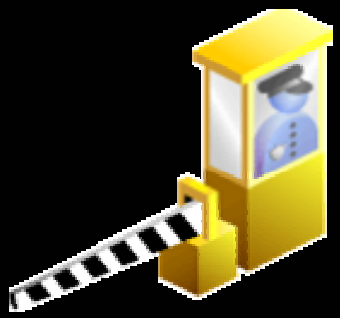
Benefits of Database Vault



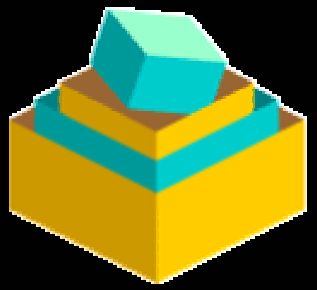
Compliant
separation of duties



Protection from
insider threat



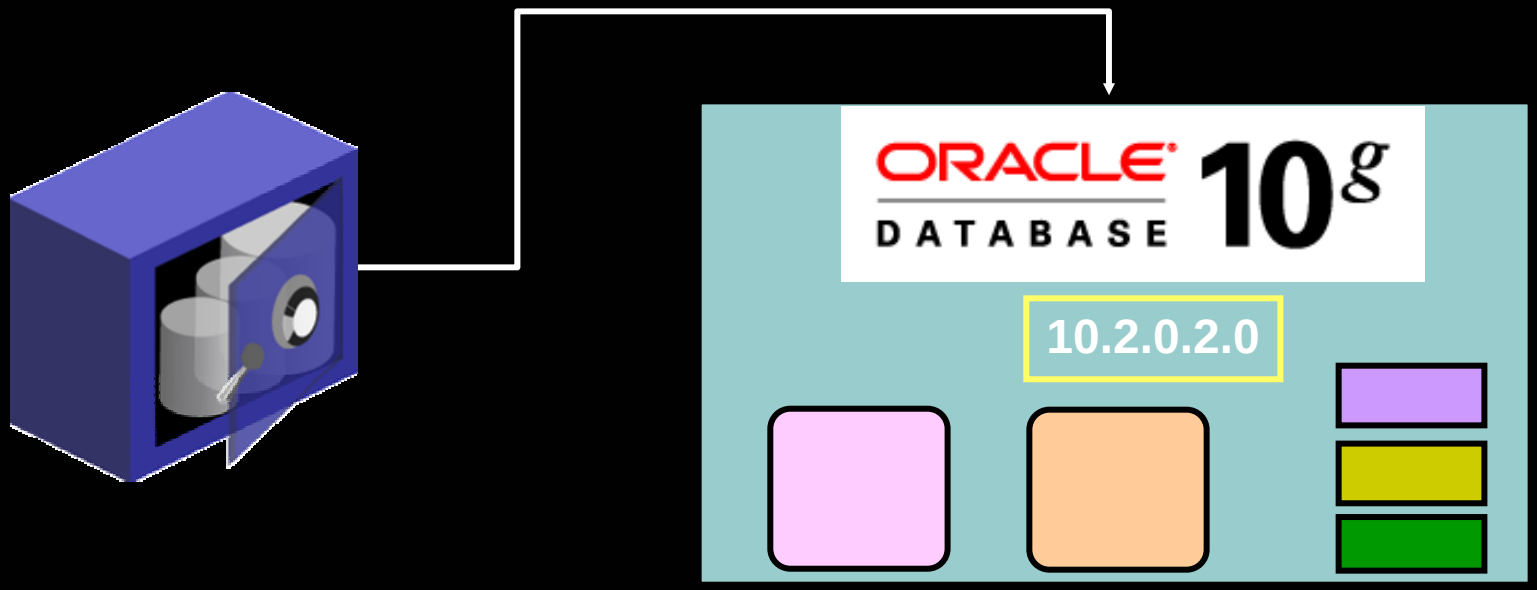
Customized control
of data access conditions



Consolidation
of applications

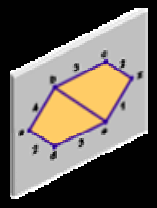
Database Vault Option

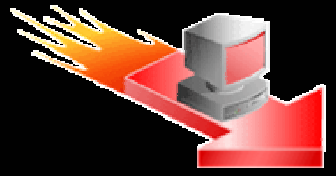
```
$ sqlplus hr/hr

SQL*Plus: Release 10.2.0.2.0 - Production on Mon May 1 14:36:16 2006
Copyright (c) 1982, 2005, Oracle.  All Rights Reserved.

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.2.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining
and Database Vault options
```



Database Vault: Effects

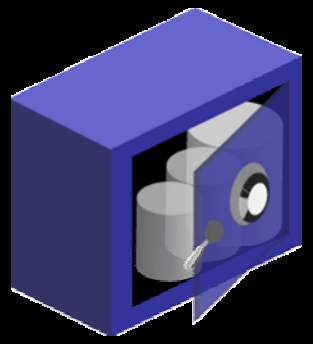
- The installation of the Database Vault option:
  - Is transparent to applications
  - Does not affect access paths for queries
  - May affect what data is accessible for a given session under certain circumstances
  - May or may not affect performance of queries, depending on the configuration of Database Vault components
  - May require more personnel to take full and proper advantage of the features






Database Vault Versus VPD and OLS

- Virtual Private Database (VPD):
  - Restricts access to certain rows for a user by modifying the `WHERE` clause
- Oracle Label Security (OLS):
  - Mediates access to a given row, based on the label on the row and the security level of the user
- VPD and OLS restrict access at the row level, whereas Database Vault restricts access at the object and command levels.

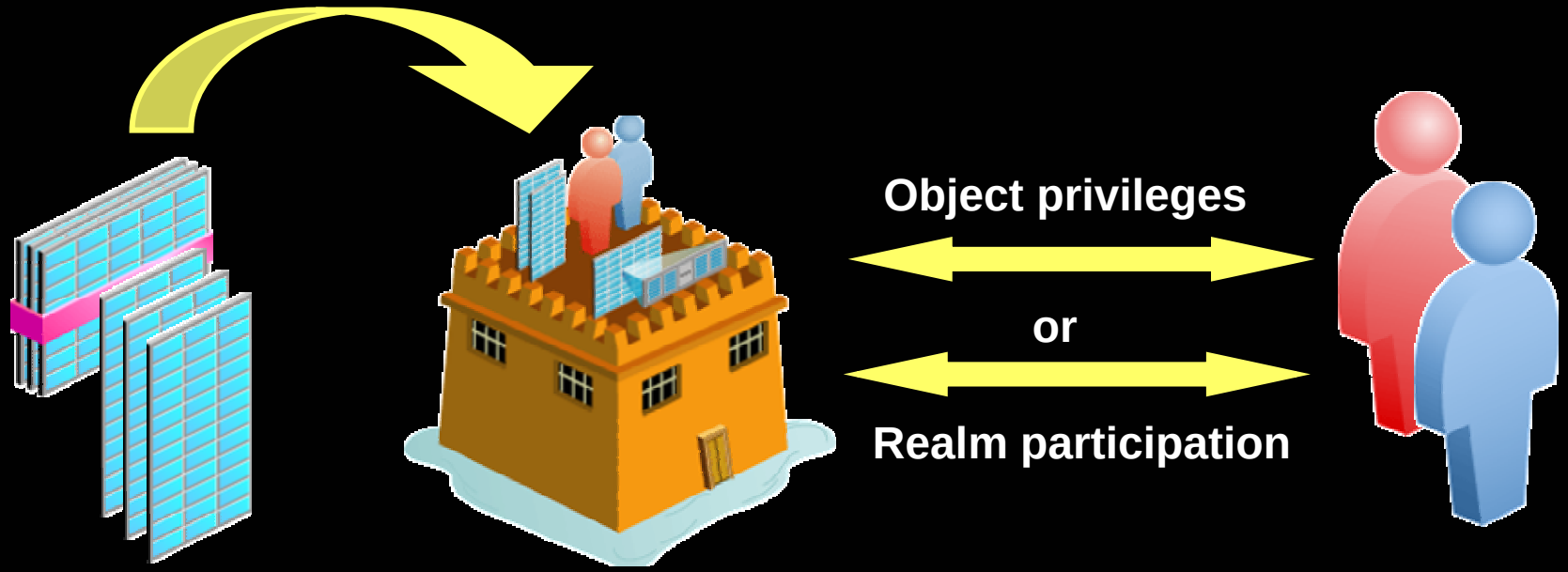


Access Control Components

- Database Vault provides the following components for securing a database:
  - Realms
  - Factors
  - Identities
  - Rule sets
  - Command rules
  - Secure application roles

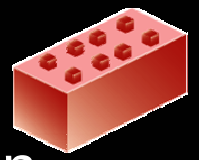
Realms: Introduction

- Realms:
  - Contain protected objects
  - Reference users who are allowed to access the objects



Factors: Introduction

- A factor:
  - Is an attribute of a database session
  - Can have a value, which can be labeled as an identity
  - Can easily be referenced in other Database Vault components to discern access
  - Can be combined with other factors to provide for multifactored authentication

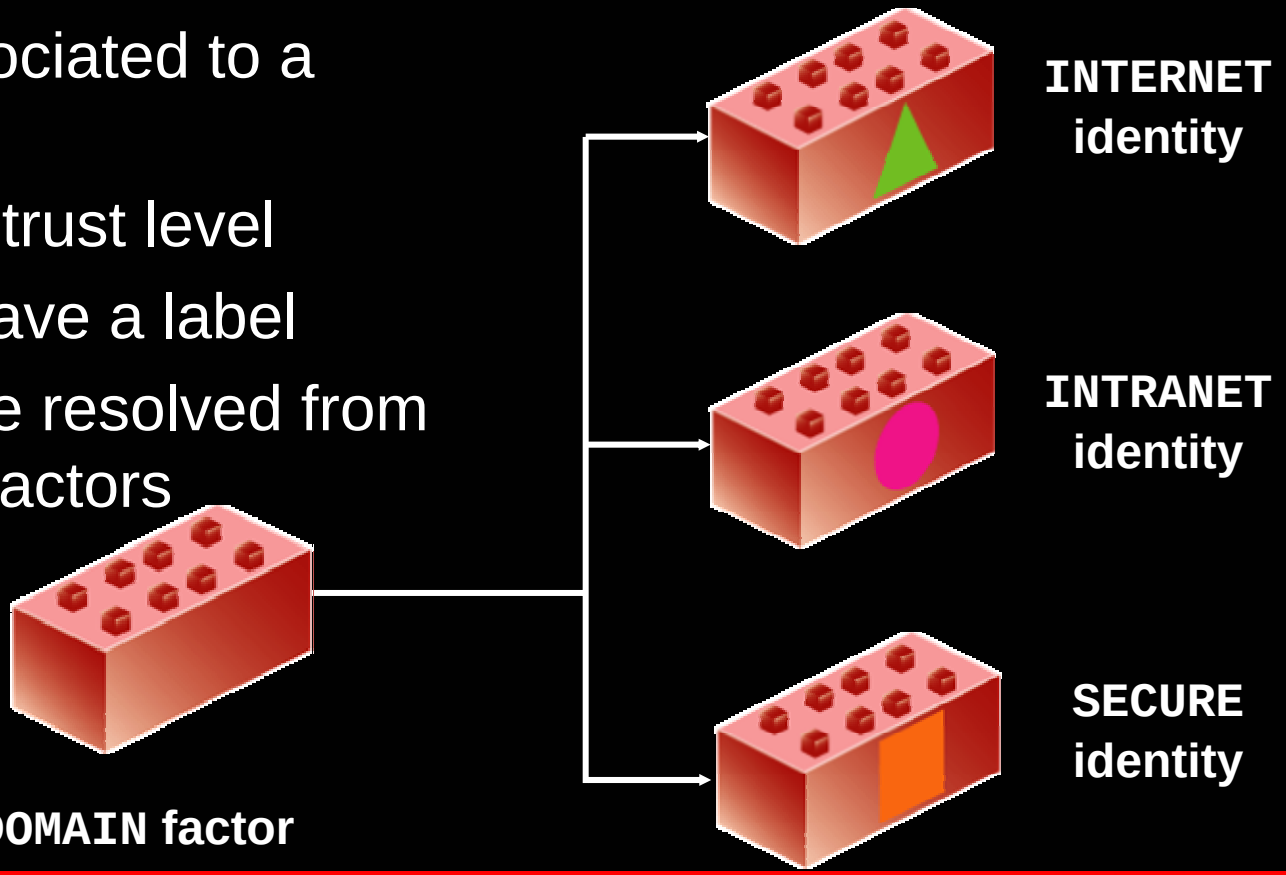


+

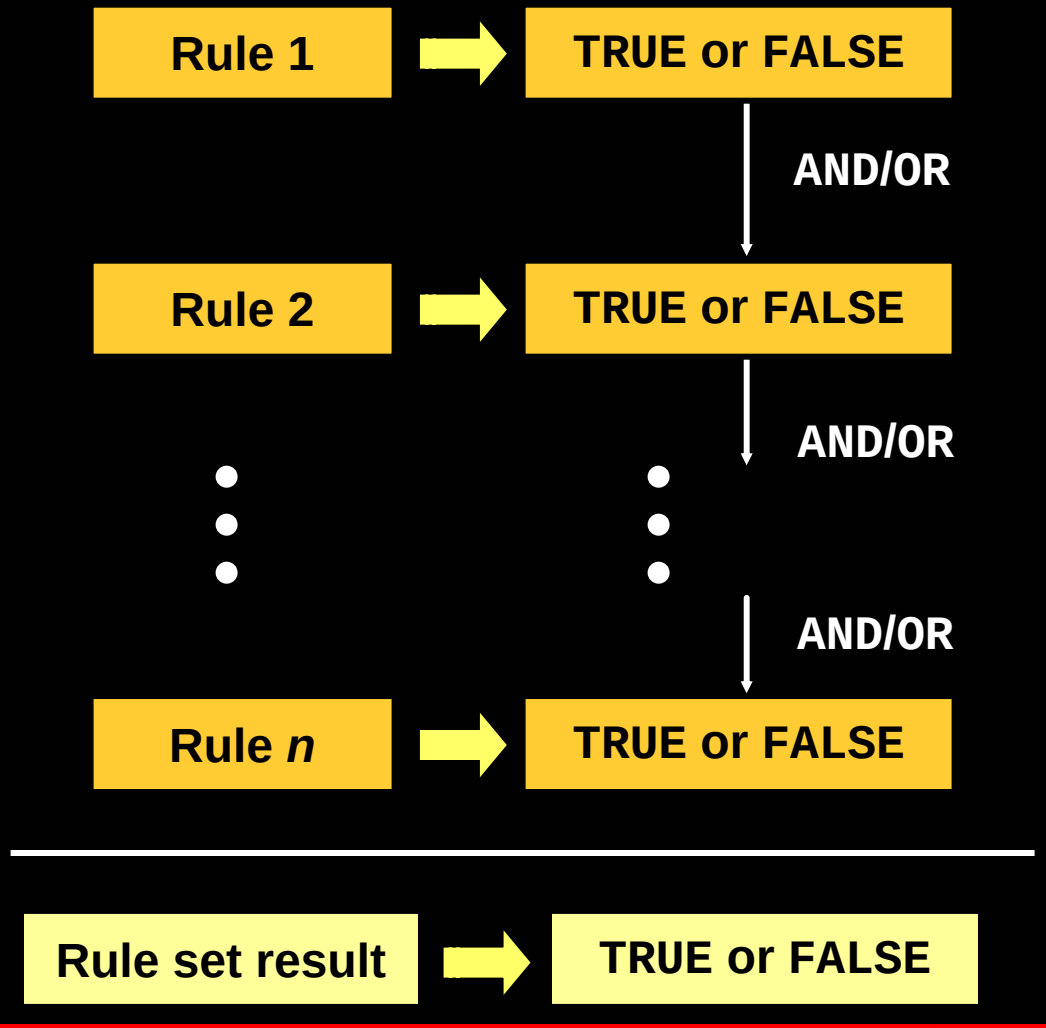
+

Identities: Introduction

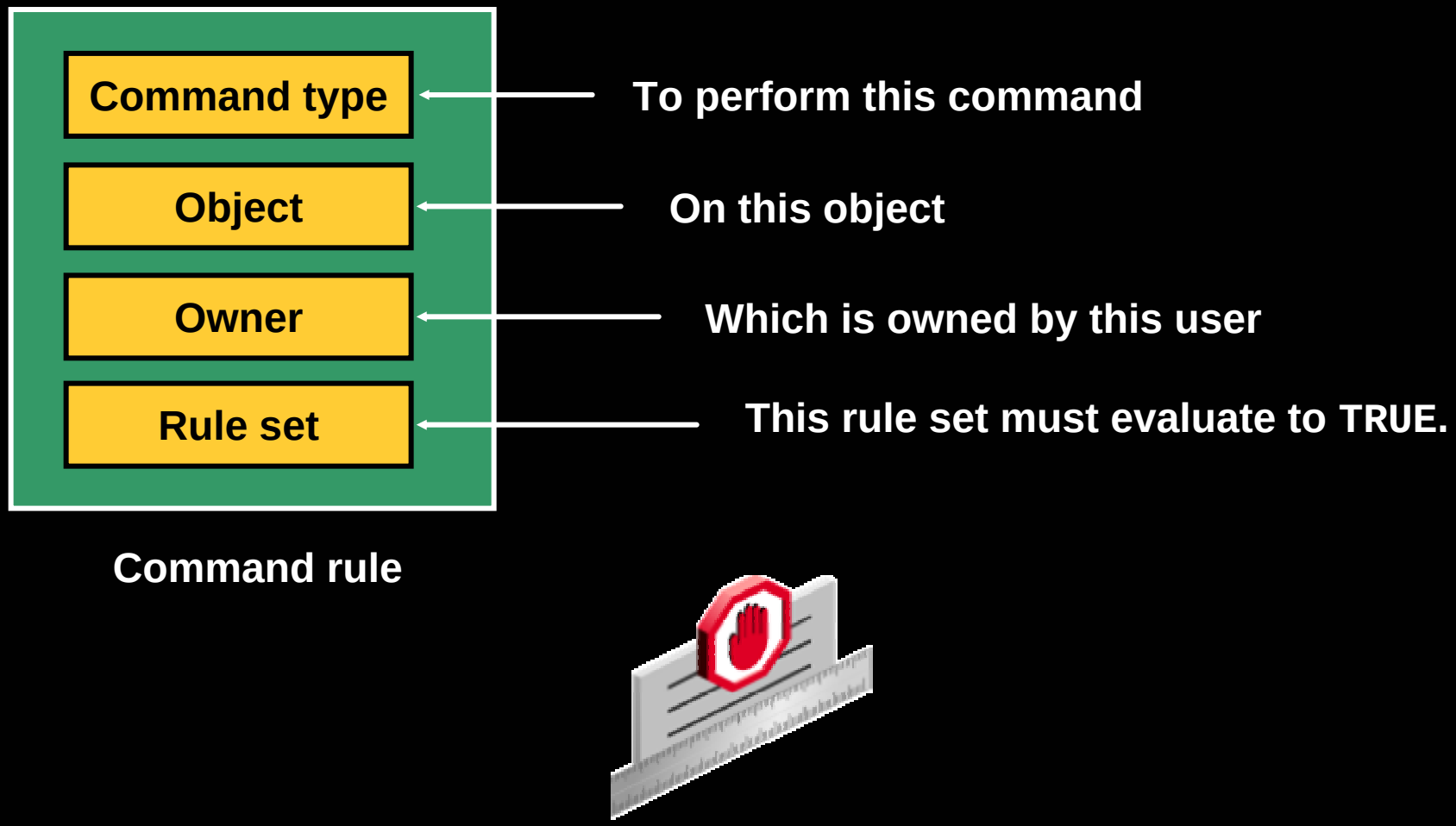
- An identity:
  - Is a value
  - Is associated to a factor
  - Has a trust level
  - Can have a label
  - Can be resolved from other factors



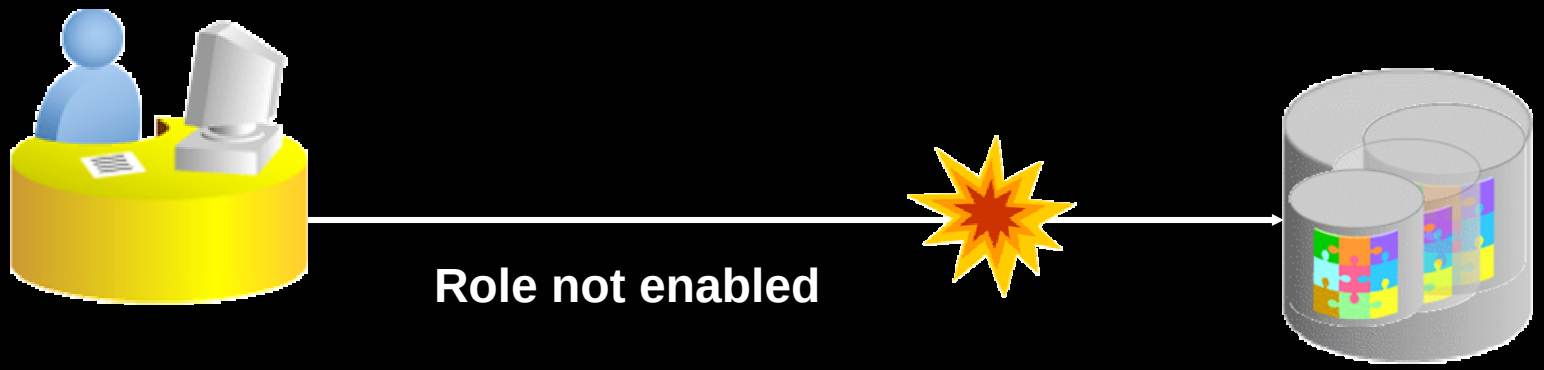
Rule Sets: Introduction



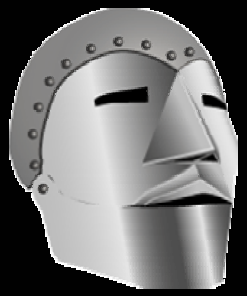
Command Rules: Introduction



Secure Application Roles: Introduction



Role enabled



Component Relationships: Static

Realm

Command rule

Secure application role

Uses

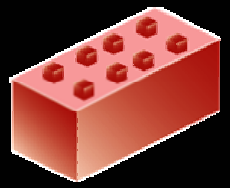
Rule set

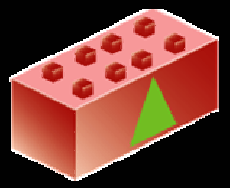
Uses

Factor

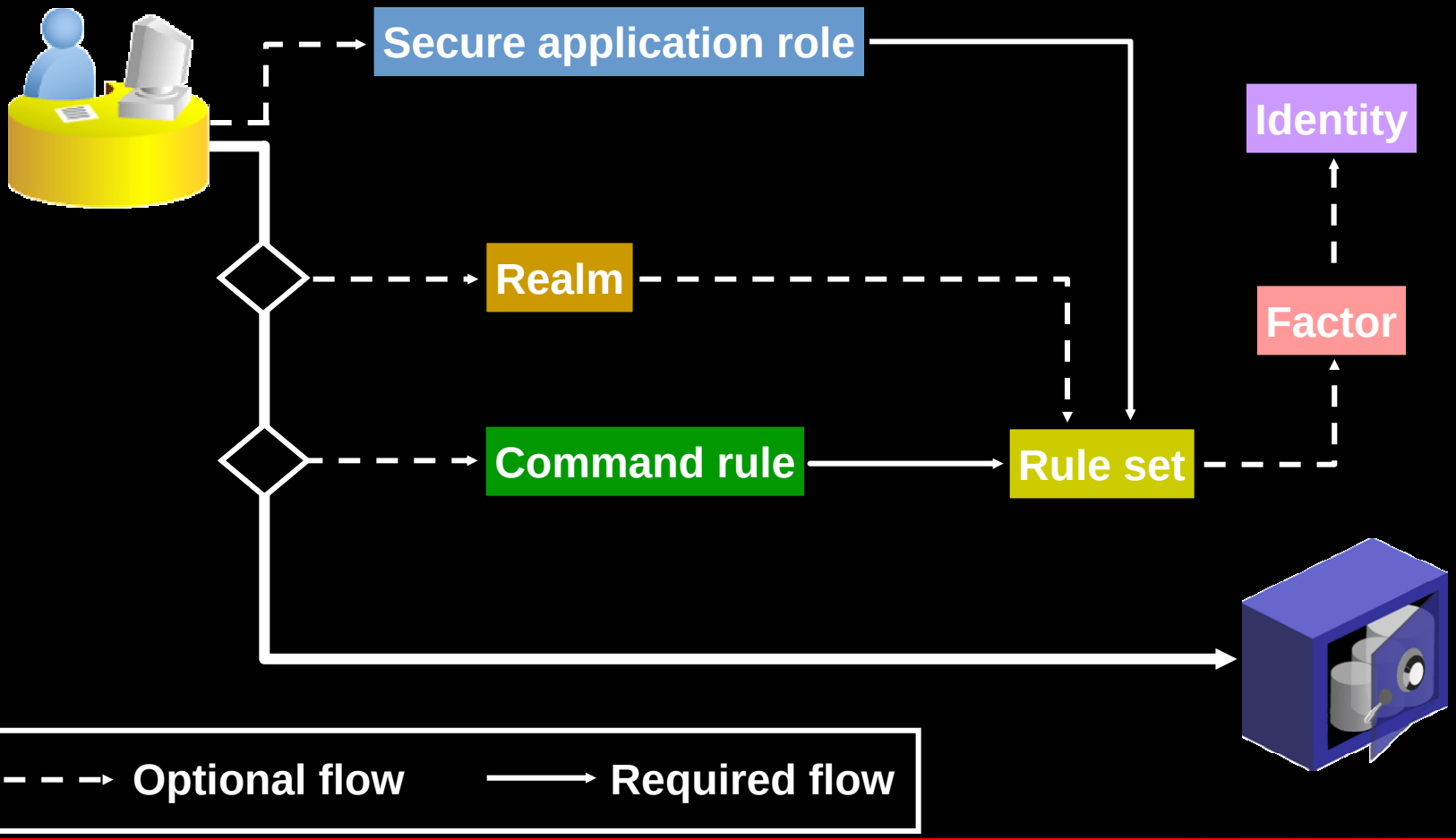
Uses

Identity

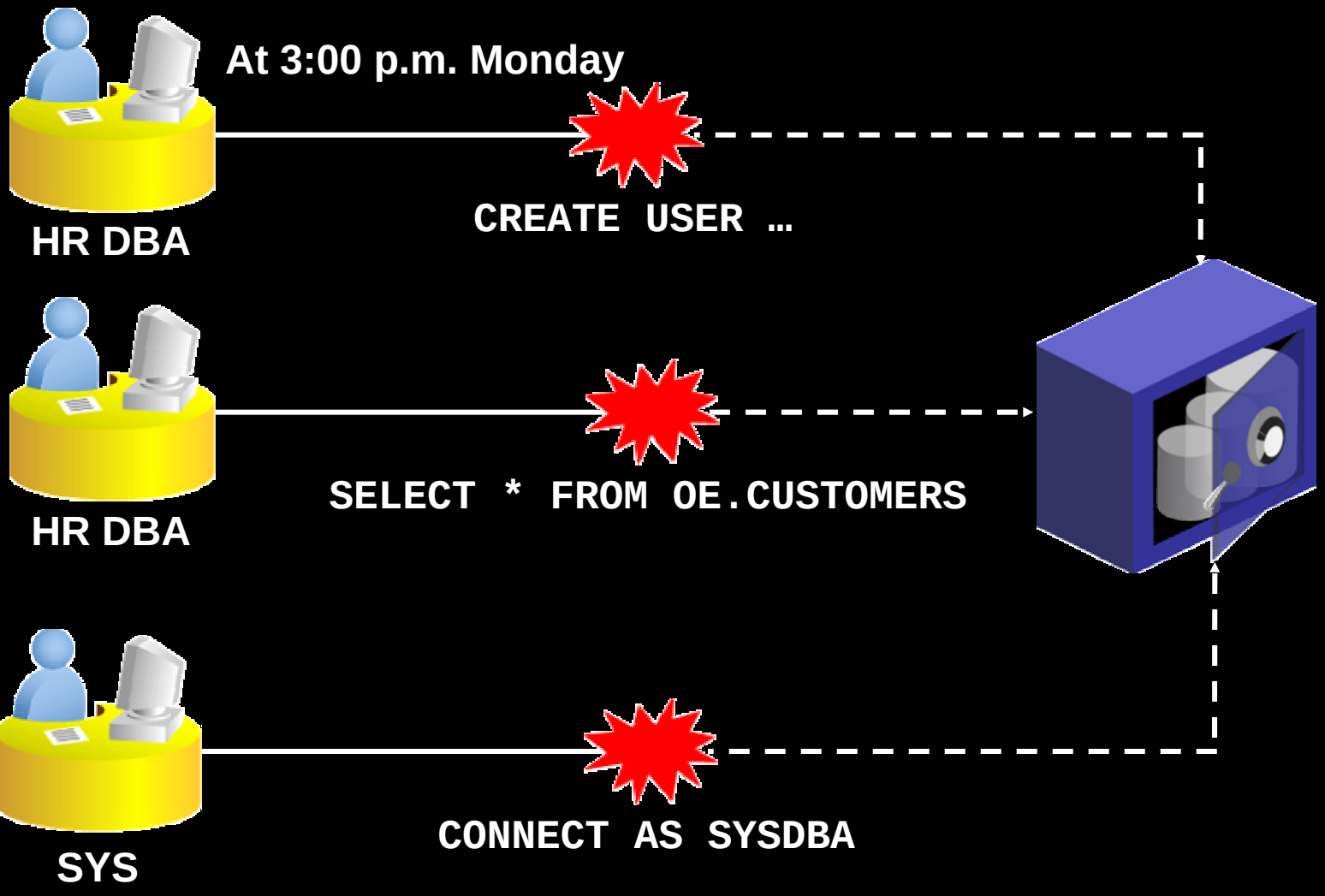




Component Relationships: Dynamic



Scenarios


At 3:00 p.m. Monday
CREATE USER …
HR DBA
SELECT * FROM OE.CUSTOMERS
HR DBA
CONNECT AS SYSDBA
SYS

Database Vault Example: Separation of Duties

1. The DBA can view the ORDERS table data.

```
SQL> SELECT order_total FROM oe.orders
  2  WHERE customer_id = 101;

ORDER_TOTAL
-----------
    78279.6
```

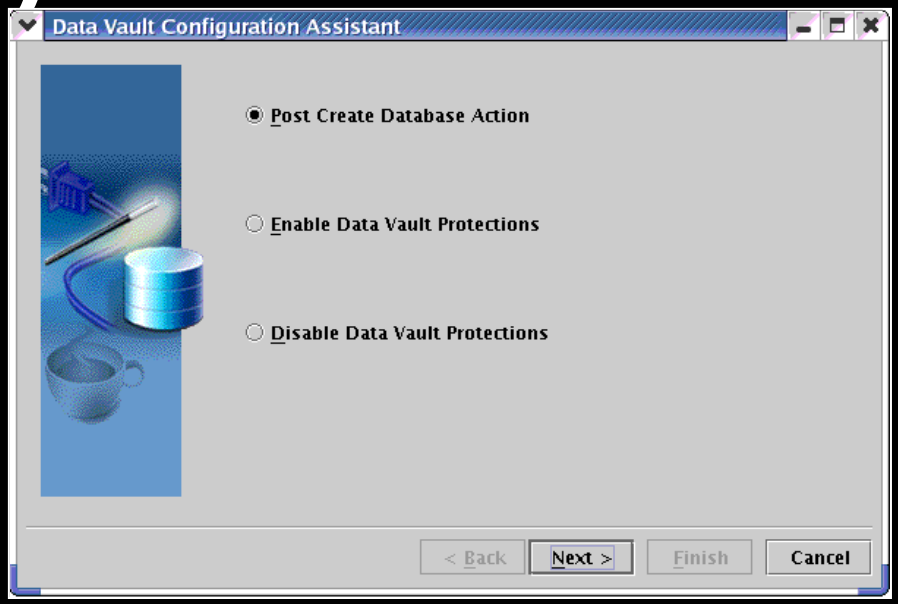
2. The security manager protects the OE.ORDERS table with a realm.

3. The DBA can no longer view the ORDERS table data.

```
SQL> SELECT order_total FROM oe.orders
  2  WHERE customer_id = 101;
ERROR at line 1:
ORA-01031: insufficient privileges
```

Database Vault Administrator (DVA)

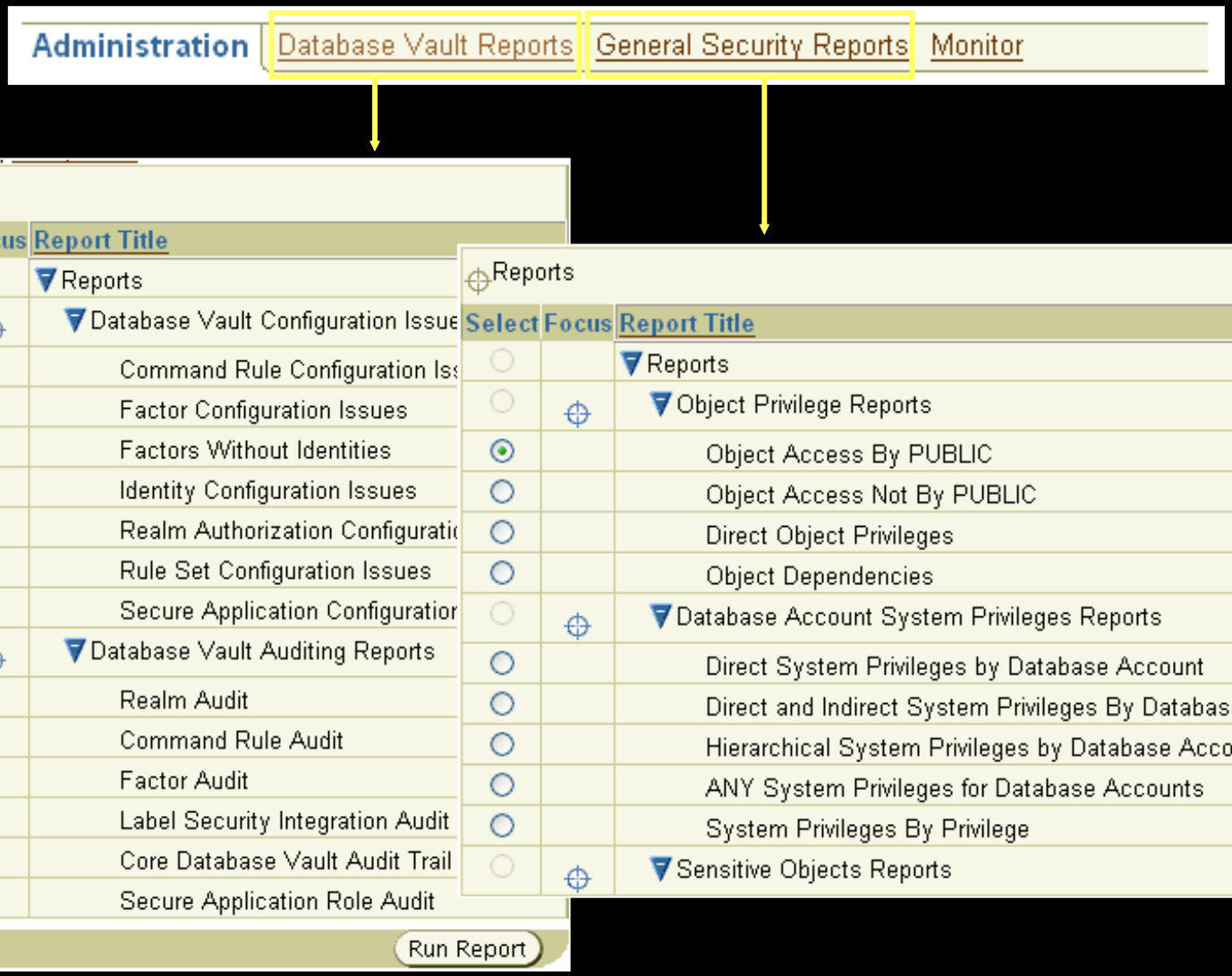
Database Vault Configuration Assistant (DVCA)



- The Database Vault Configuration Assistant (DVCA) is run as part of the installation steps to:
  - Create the Database Vault specific accounts
  - Disable Database Vault security for installing other database options
  - Enable Database Vault security after installing database options

```
$ dvca
```

Reporting

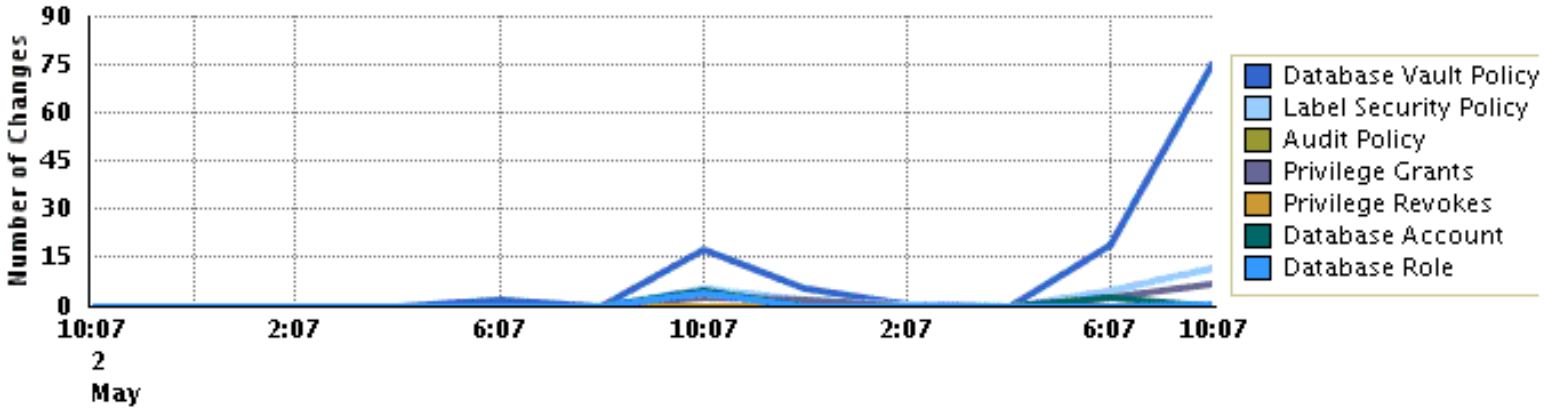

Administration
Database Vault Reports
General Security Reports
Monitor
Reports
Select
Focus
Report Title
Reports
Database Vault Configuration Issue
Command Rule Configuration Iss
Factor Configuration Issues
Factors Without Identities
Identity Configuration Issues
Realm Authorization Configurati
Rule Set Configuration Issues
Secure Application Configuratior
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
Reports
Select
Focus
Report Title
Reports
Object Privilege Reports
Object Access By PUBLIC
Object Access Not By PUBLIC
Direct Object Privileges
Object Dependencies
Database Account System Privileges Reports
Direct System Privileges by Database Account
Direct and Indirect System Privileges By Database Account
Hierarchical System Privileges by Database Account
ANY System Privileges for Database Accounts
System Privileges By Privilege
Sensitive Objects Reports

Monitoring

Show Records For Past 24 Hours Go

Security Policy Changes By Category

May 2, 2006 10:08:52 PM - May 3, 2006 10:08:52 PM



▶Security Policy Changes Detail

▶Security Violation Attempts

▶Database Configuration and Structural Changes

Database Vault API

- The Database Vault application program interface (API) provides the following functionalities:
  - Create, modify, and delete Database Vault components
  - Allow a session to define its security environment
  - Query the state and values of components
  - Administer and configure systemwide Database Vault parameters


QUESTIONS
&
ANSWERS
ORACLE


ORACLE®