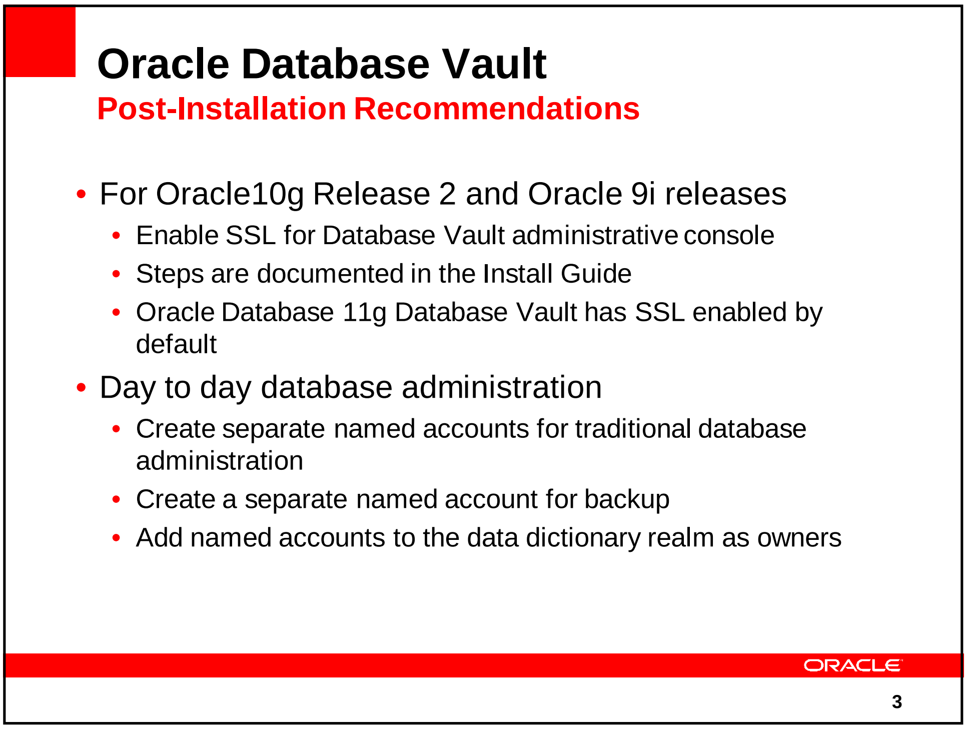
ORACLE®

Oracle Database Vault Best Practices

September 2009

Oracle Database Vault
Installation Recommendations

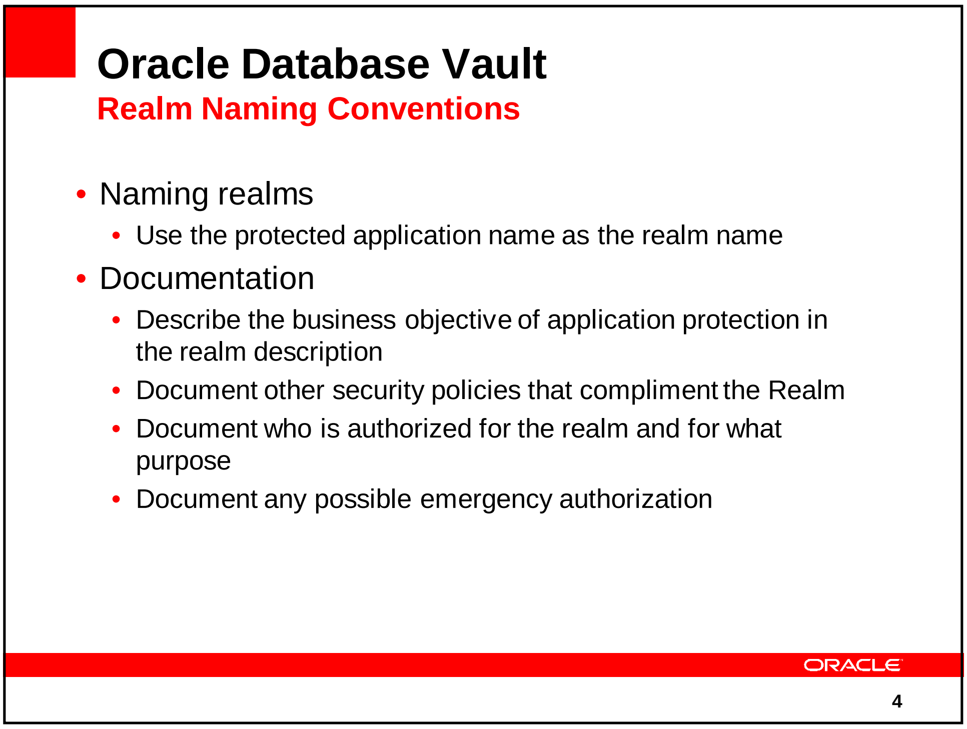
- Existing applications
  - Install applications before installation Database Vault
  - Existing application installs may violate default separation of duty
- Separation of duty
  - Create separate accounts during Database Vault installation for account management and security administration
- Choosing an ORACLE_HOME
  - You can have multiple databases running from a single Database Vault enabled ORACLE_HOME. All databases in that home must be enabled with Database Vault.
  - Use the *dvca* command line utility to enable the additional databases with Database Vault after initial installation



Oracle Database Vault

Post-Installation Recommendations

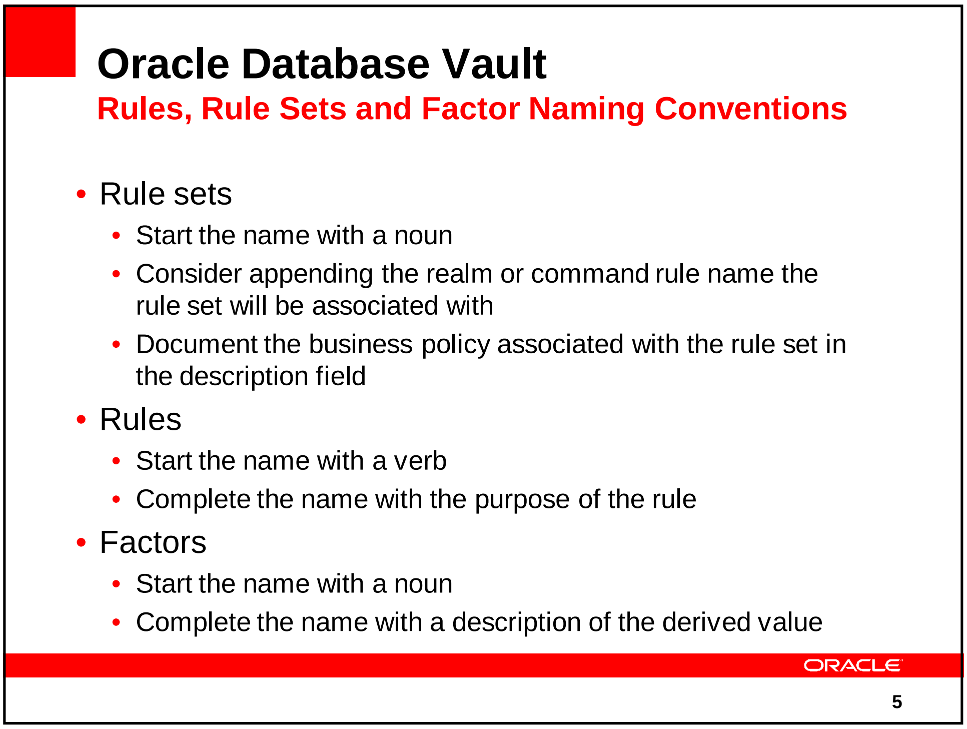
- For Oracle10g Release 2 and Oracle 9i releases
  - Enable SSL for Database Vault administrative console
  - Steps are documented in the Install Guide
  - Oracle Database 11g Database Vault has SSL enabled by default
- Day to day database administration
  - Create separate named accounts for traditional database administration
  - Create a separate named account for backup
  - Add named accounts to the data dictionary realm as owners



Oracle Database Vault

Realm Naming Conventions

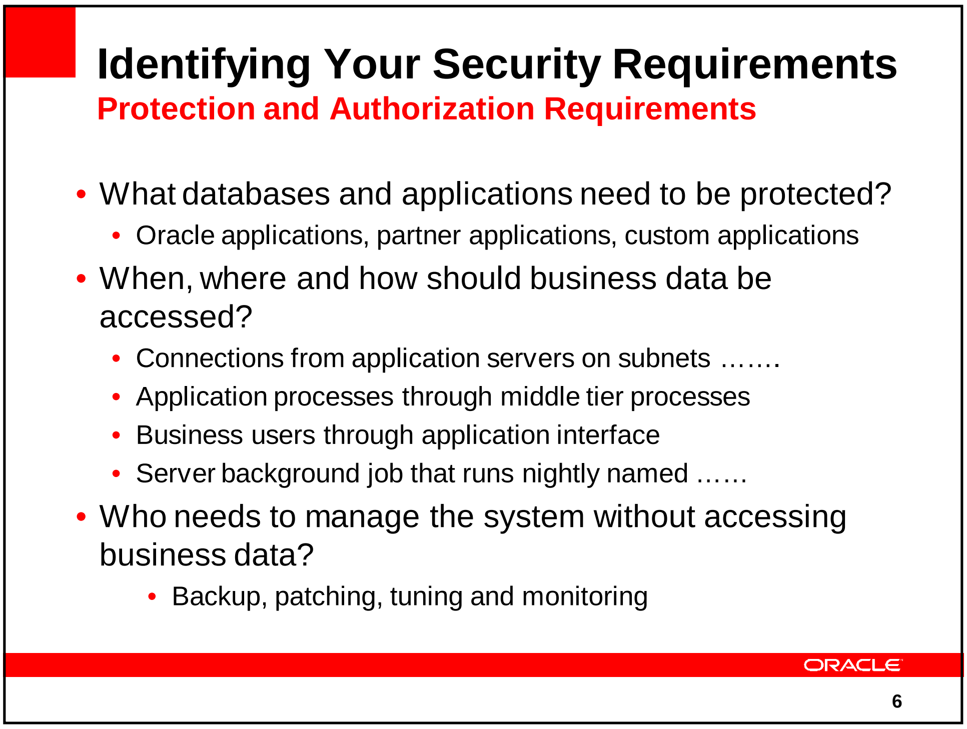
- Naming realms
  - Use the protected application name as the realm name
- Documentation
  - Describe the business objective of application protection in the realm description
  - Document other security policies that compliment the Realm
  - Document who is authorized for the realm and for what purpose
  - Document any possible emergency authorization



Oracle Database Vault

Rules, Rule Sets and Factor Naming Conventions

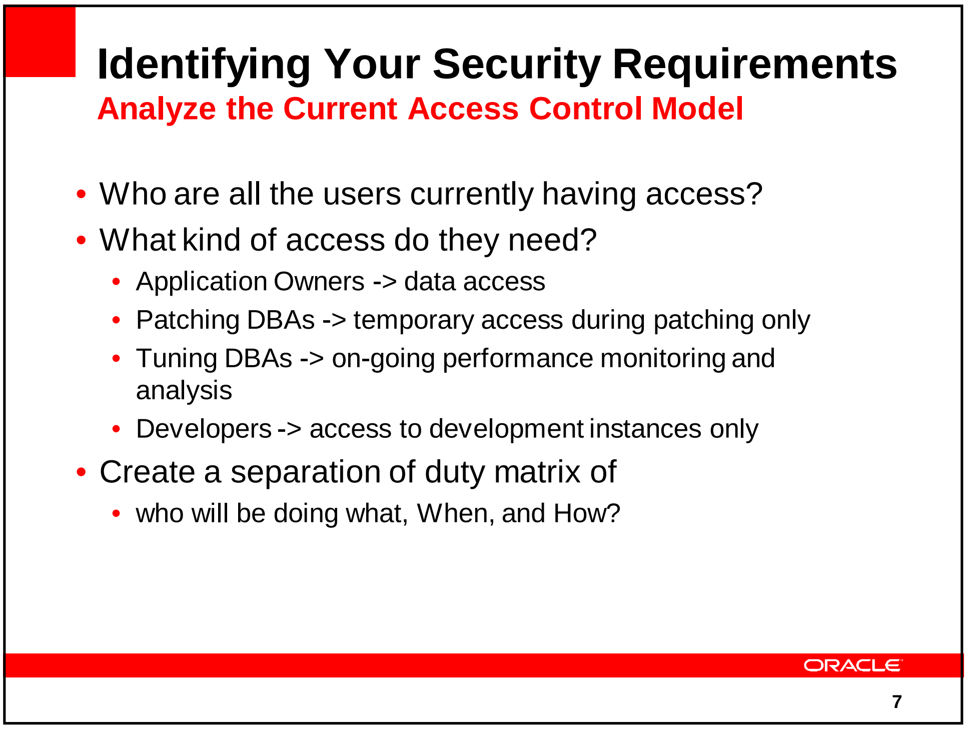
- Rule sets
  - Start the name with a noun
  - Consider appending the realm or command rule name the rule set will be associated with
  - Document the business policy associated with the rule set in the description field
- Rules
  - Start the name with a verb
  - Complete the name with the purpose of the rule
- Factors
  - Start the name with a noun
  - Complete the name with a description of the derived value



Identifying Your Security Requirements

Protection and Authorization Requirements

- What databases and applications need to be protected?
  - Oracle applications, partner applications, custom applications
- When, where and how should business data be accessed?
  - Connections from application servers on subnets …….
  - Application processes through middle tier processes
  - Business users through application interface
  - Server background job that runs nightly named ……
- Who needs to manage the system without accessing business data?
  - Backup, patching, tuning and monitoring

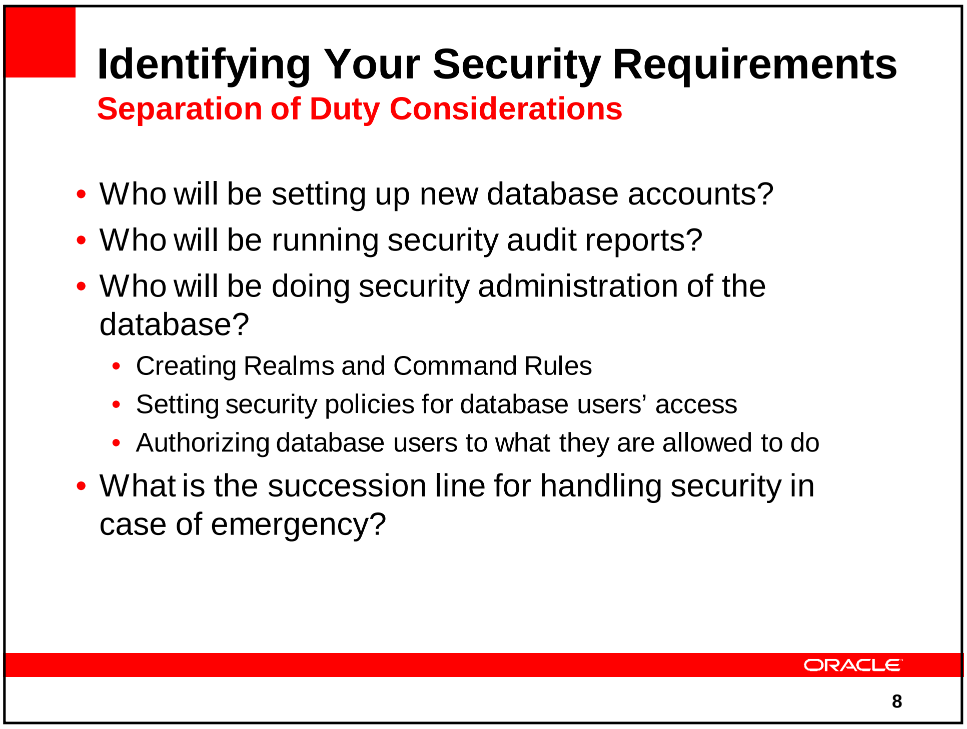


Identifying Your Security Requirements

Analyze the Current Access Control Model

- Who are all the users currently having access?
- What kind of access do they need?
  - Application Owners -> data access
  - Patching DBAs -> temporary access during patching only
  - Tuning DBAs -> on-going performance monitoring and analysis
  - Developers -> access to development instances only
- Create a separation of duty matrix of
  - who will be doing what, When, and How?

7

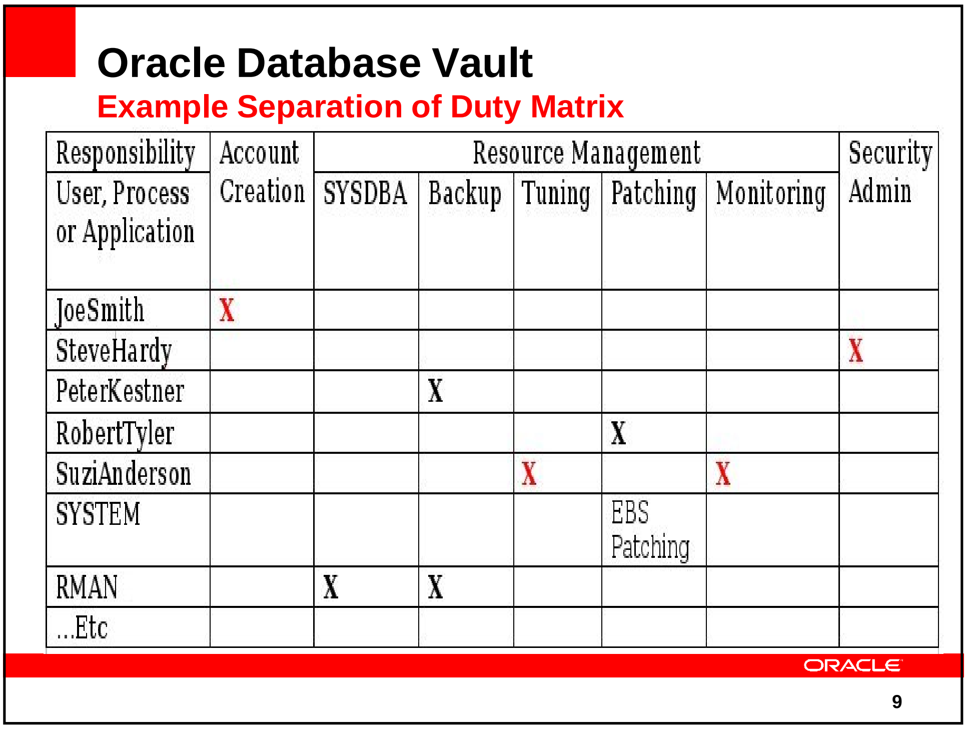


Identifying Your Security Requirements

Separation of Duty Considerations

- Who will be setting up new database accounts?
- Who will be running security audit reports?
- Who will be doing security administration of the database?
  - Creating Realms and Command Rules
  - Setting security policies for database users' access
  - Authorizing database users to what they are allowed to do
- What is the succession line for handling security in case of emergency?

8

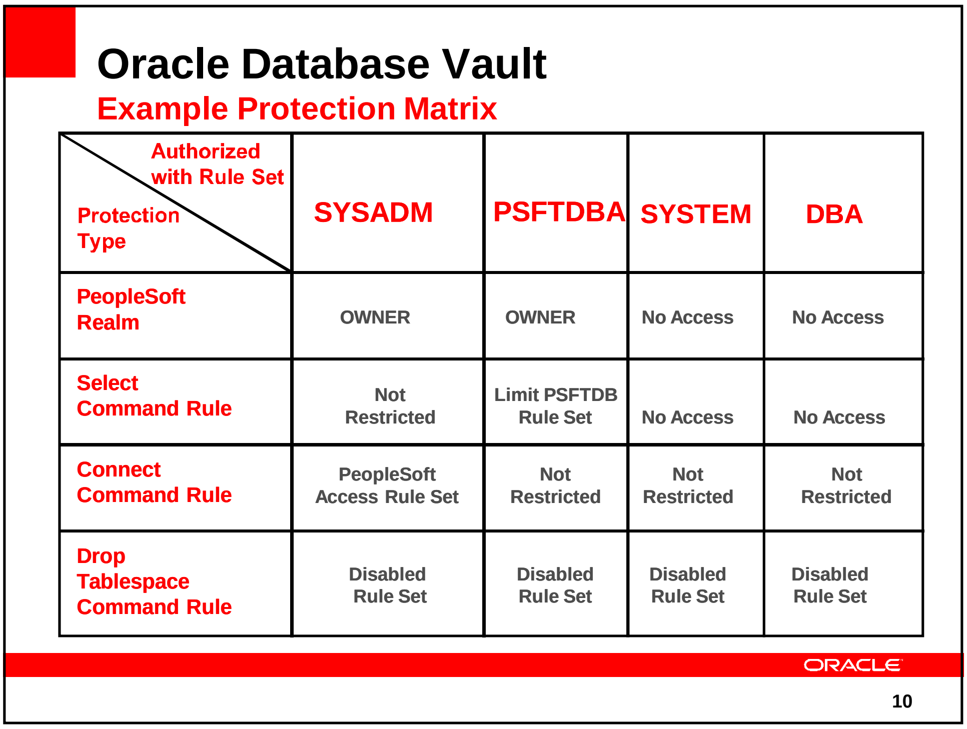


Oracle Database Vault

Example Separation of Duty Matrix

Responsibility	Account	Resource Management					Security
User, Process or Application	Creation	SYSDBA	Backup	Tuning	Patching	Monitoring	Admin
JoeSmith	X						
SteveHardy							X
PeterKestner			X				
RobertTyler					X		
SuziAnderson				X		X	
SYSTEM					EBS Patching		
RMAN		X	X				
...Etc							

ORACLE

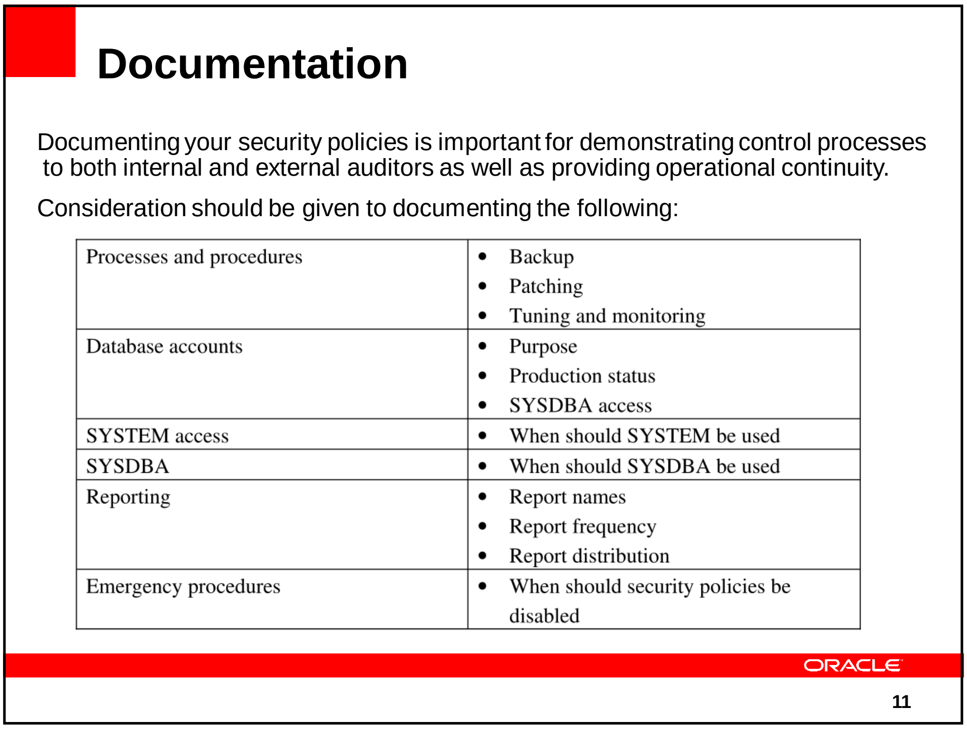


Oracle Database Vault

Example Protection Matrix

Authorized with Rule Set / Protection Type	SYSADM	PSFTDBA	SYSTEM	DBA
PeopleSoft Realm	OWNER	OWNER	No Access	No Access
Select Command Rule	Not Restricted	Limit PSFTDB Rule Set	No Access	No Access
Connect Command Rule	PeopleSoft Access Rule Set	Not Restricted	Not Restricted	Not Restricted
Drop Tablespace Command Rule	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set

ORACLE



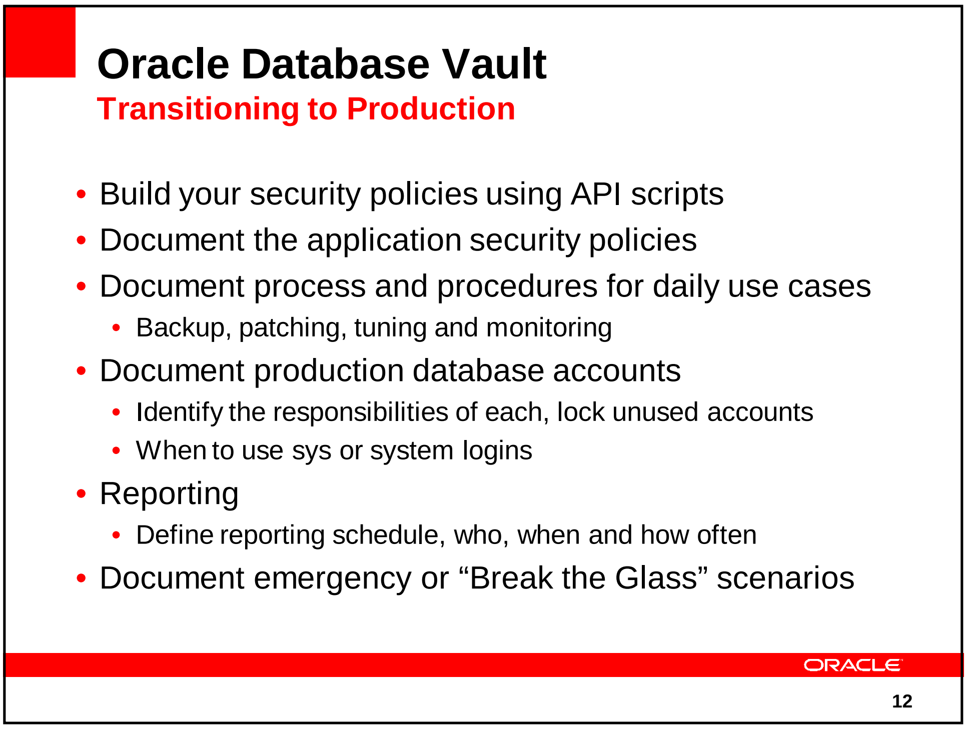
Documentation

Documenting your security policies is important for demonstrating control processes to both internal and external auditors as well as providing operational continuity.

Consideration should be given to documenting the following:

Processes and procedures	• Backup • Patching • Tuning and monitoring
Database accounts	• Purpose • Production status • SYSDBA access
SYSTEM access	• When should SYSTEM be used
SYSDBA	• When should SYSDBA be used
Reporting	• Report names • Report frequency • Report distribution
Emergency procedures	• When should security policies be disabled

ORACLE

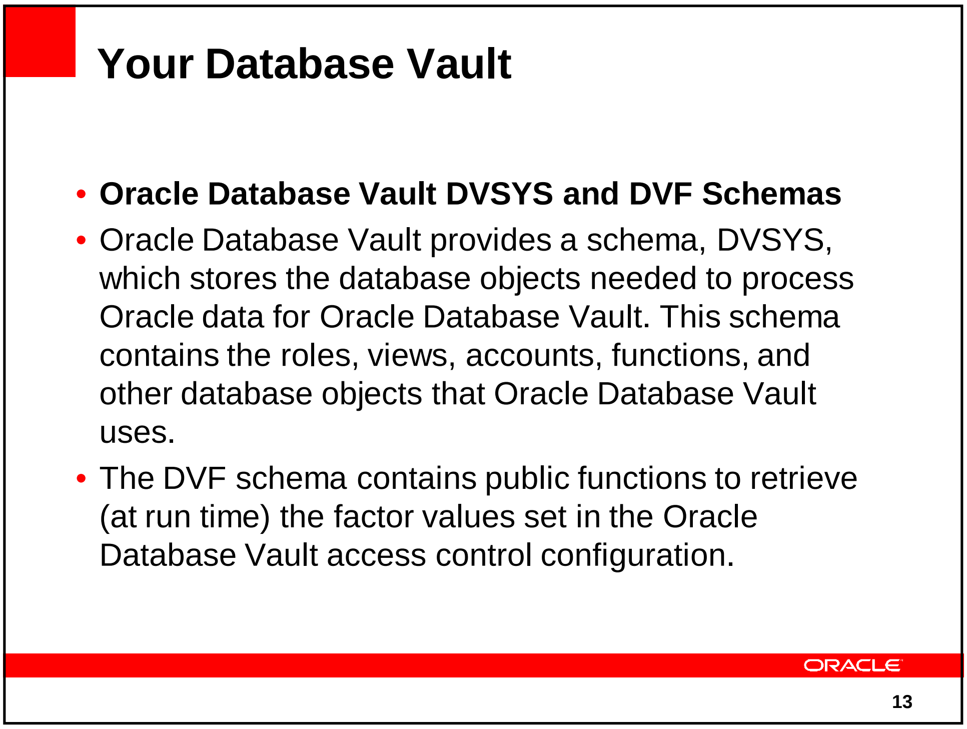


Oracle Database Vault

Transitioning to Production

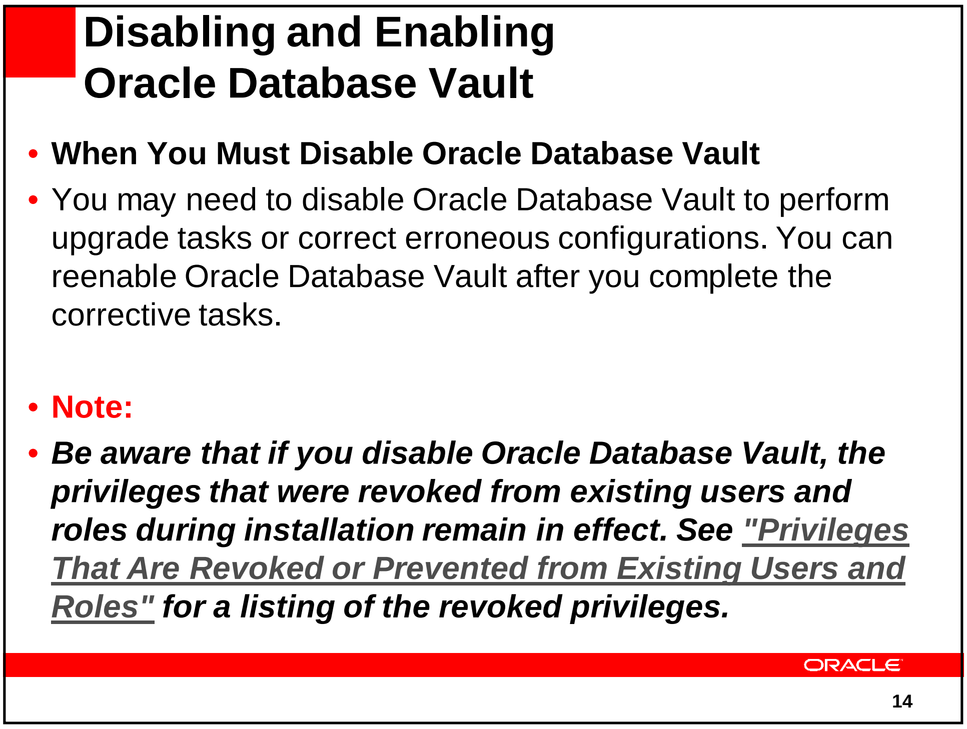
- Build your security policies using API scripts
- Document the application security policies
- Document process and procedures for daily use cases
  - Backup, patching, tuning and monitoring
- Document production database accounts
  - Identify the responsibilities of each, lock unused accounts
  - When to use sys or system logins
- Reporting
  - Define reporting schedule, who, when and how often
- Document emergency or “Break the Glass” scenarios

ORACLE



Your Database Vault

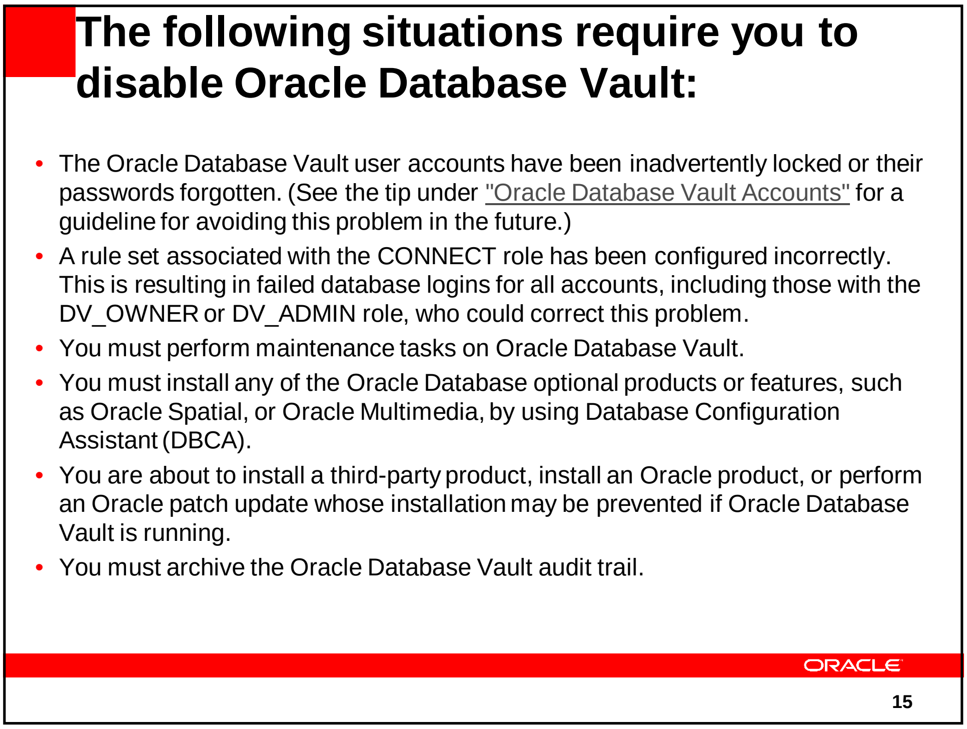
- **Oracle Database Vault DVSYS and DVF Schemas**
- Oracle Database Vault provides a schema, DVSYS, which stores the database objects needed to process Oracle data for Oracle Database Vault. This schema contains the roles, views, accounts, functions, and other database objects that Oracle Database Vault uses.
- The DVF schema contains public functions to retrieve (at run time) the factor values set in the Oracle Database Vault access control configuration.



Disabling and Enabling Oracle Database Vault

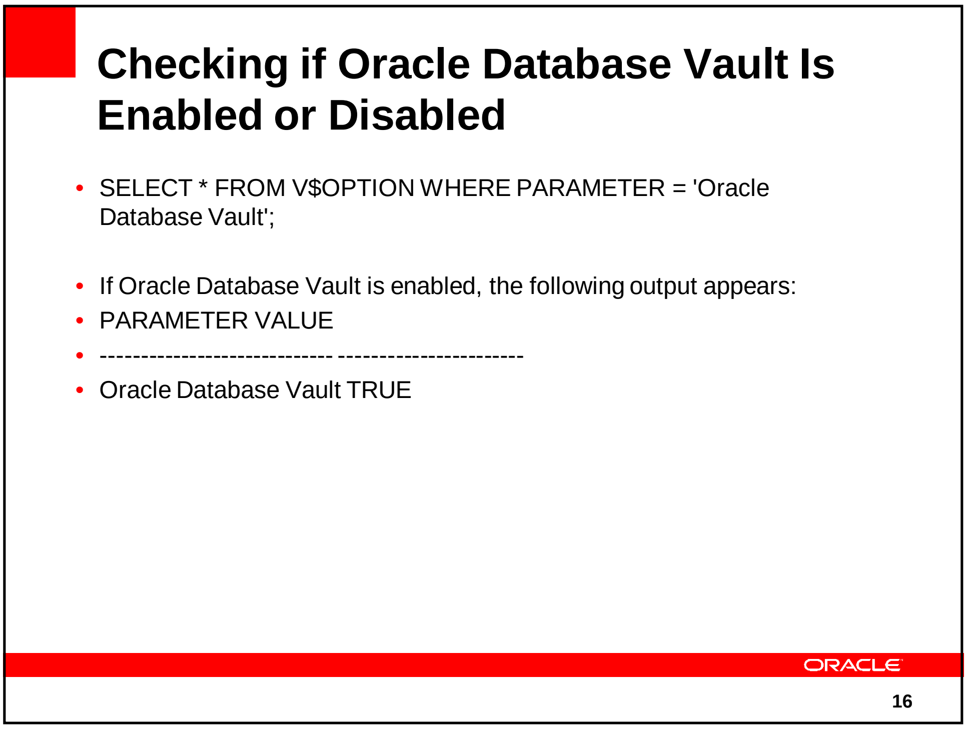
- **When You Must Disable Oracle Database Vault**
- You may need to disable Oracle Database Vault to perform upgrade tasks or correct erroneous configurations. You can reenable Oracle Database Vault after you complete the corrective tasks.

- **Note:**
- ***Be aware that if you disable Oracle Database Vault, the privileges that were revoked from existing users and roles during installation remain in effect. See "Privileges That Are Revoked or Prevented from Existing Users and Roles" for a listing of the revoked privileges.***



The following situations require you to disable Oracle Database Vault:

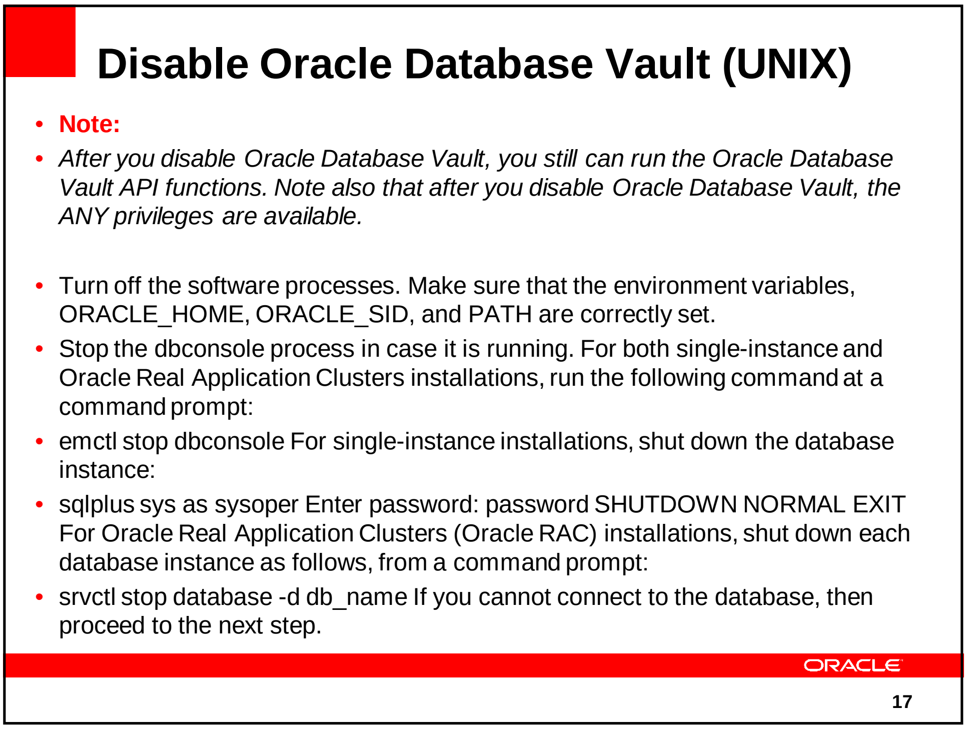
- The Oracle Database Vault user accounts have been inadvertently locked or their passwords forgotten. (See the tip under "Oracle Database Vault Accounts" for a guideline for avoiding this problem in the future.)
- A rule set associated with the CONNECT role has been configured incorrectly. This is resulting in failed database logins for all accounts, including those with the DV_OWNER or DV_ADMIN role, who could correct this problem.
- You must perform maintenance tasks on Oracle Database Vault.
- You must install any of the Oracle Database optional products or features, such as Oracle Spatial, or Oracle Multimedia, by using Database Configuration Assistant (DBCA).
- You are about to install a third-party product, install an Oracle product, or perform an Oracle patch update whose installation may be prevented if Oracle Database Vault is running.
- You must archive the Oracle Database Vault audit trail.



Checking if Oracle Database Vault Is Enabled or Disabled

- SELECT * FROM V$OPTION WHERE PARAMETER = 'Oracle Database Vault';

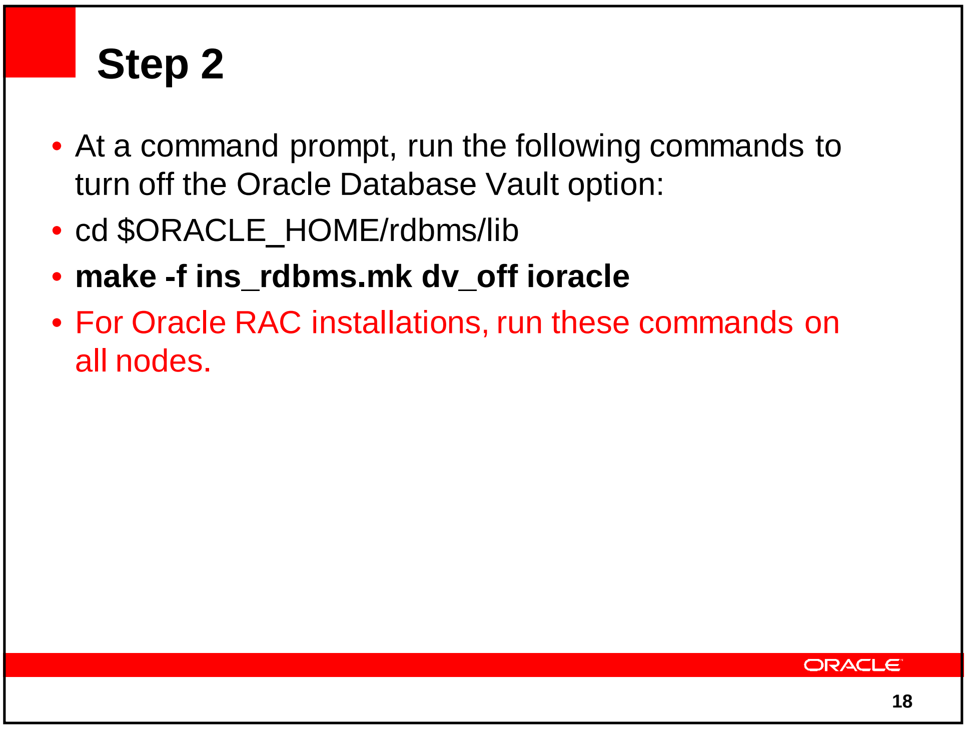
- If Oracle Database Vault is enabled, the following output appears:
- PARAMETER VALUE
- ----------------------------- -----------------------
- Oracle Database Vault TRUE



Disable Oracle Database Vault (UNIX)

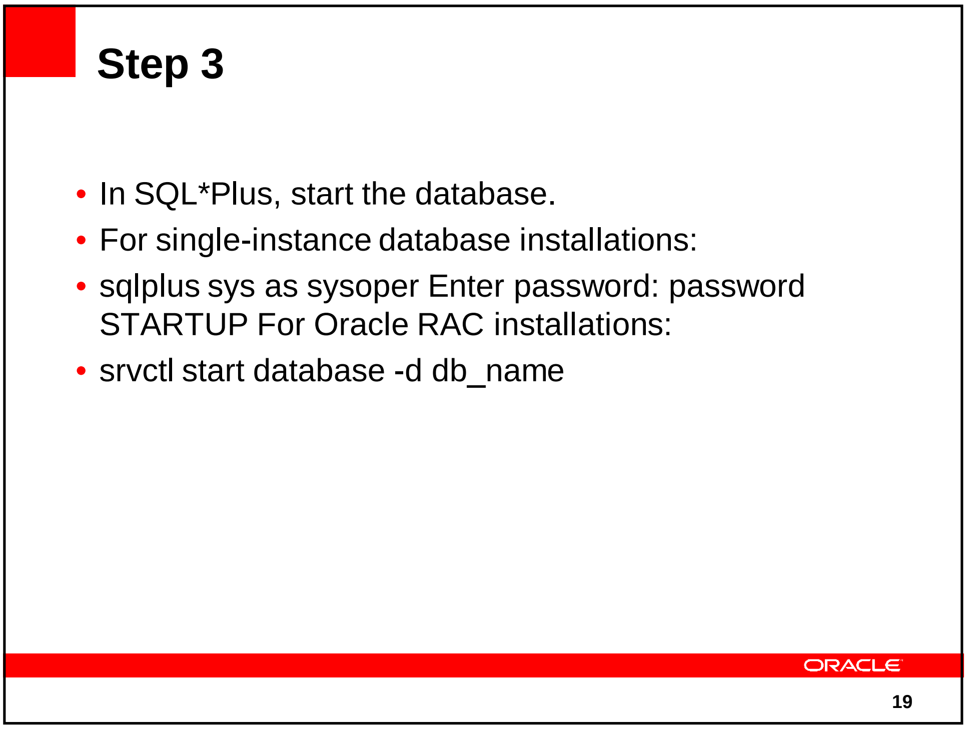
- **Note:**
- *After you disable Oracle Database Vault, you still can run the Oracle Database Vault API functions. Note also that after you disable Oracle Database Vault, the ANY privileges are available.*

- Turn off the software processes. Make sure that the environment variables, ORACLE_HOME, ORACLE_SID, and PATH are correctly set.
- Stop the dbconsole process in case it is running. For both single-instance and Oracle Real Application Clusters installations, run the following command at a command prompt:
- emctl stop dbconsole For single-instance installations, shut down the database instance:
- sqlplus sys as sysoper Enter password: password SHUTDOWN NORMAL EXIT For Oracle Real Application Clusters (Oracle RAC) installations, shut down each database instance as follows, from a command prompt:
- srvctl stop database -d db_name If you cannot connect to the database, then proceed to the next step.



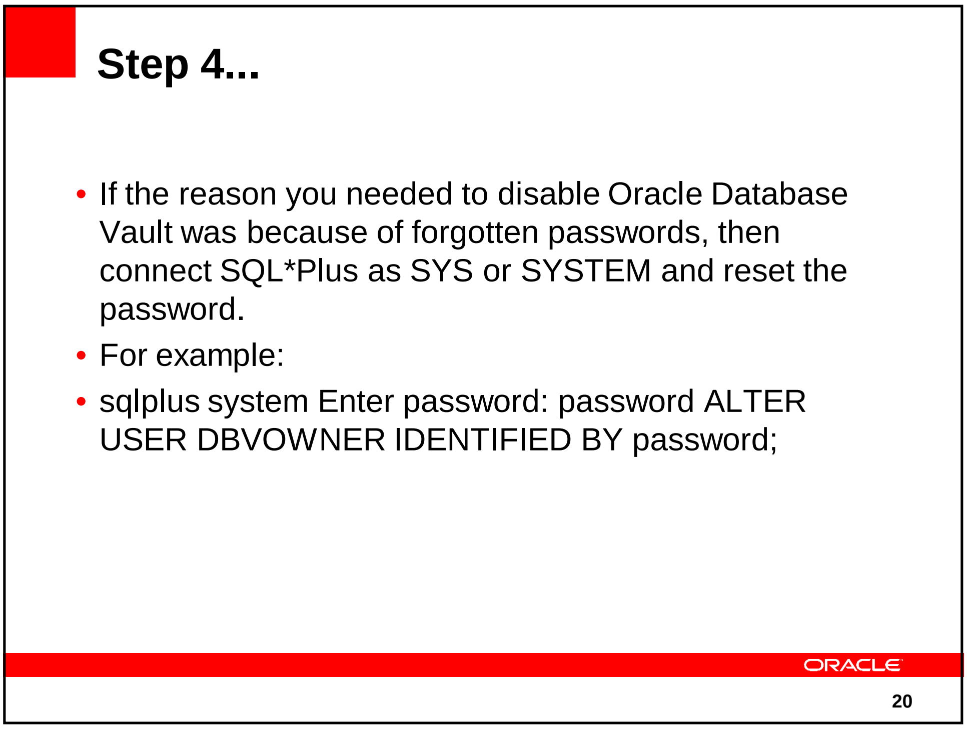
Step 2

- At a command prompt, run the following commands to turn off the Oracle Database Vault option:
- cd $ORACLE_HOME/rdbms/lib
- **make -f ins_rdbms.mk dv_off ioracle**
- For Oracle RAC installations, run these commands on all nodes.



Step 3

- In SQL*Plus, start the database.
- For single-instance database installations:
- sqlplus sys as sysoper Enter password: password STARTUP For Oracle RAC installations:
- srvctl start database -d db_name



Step 4...

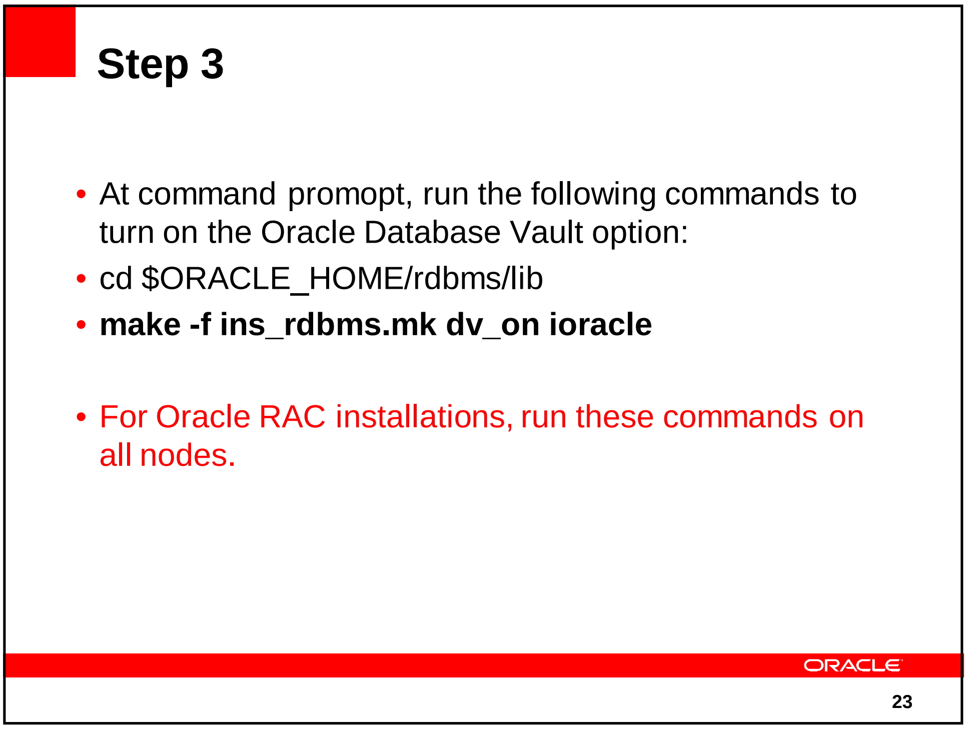
- If the reason you needed to disable Oracle Database Vault was because of forgotten passwords, then connect SQL*Plus as SYS or SYSTEM and reset the password.
- For example:
- sqlplus system Enter password: password ALTER USER DBVOWNER IDENTIFIED BY password;

Enabling Database Vault (UNIX)

- Step 1
- Turn off the software processes. Ensure that the environment variables, ORACLE_HOME, ORACLE_SID, and PATH are correctly set.
- Stop the dbconsole process in case it is running. For both single-instance and Oracle RAC installations, use the following command:
- emctl stop dbconsole

Step 2

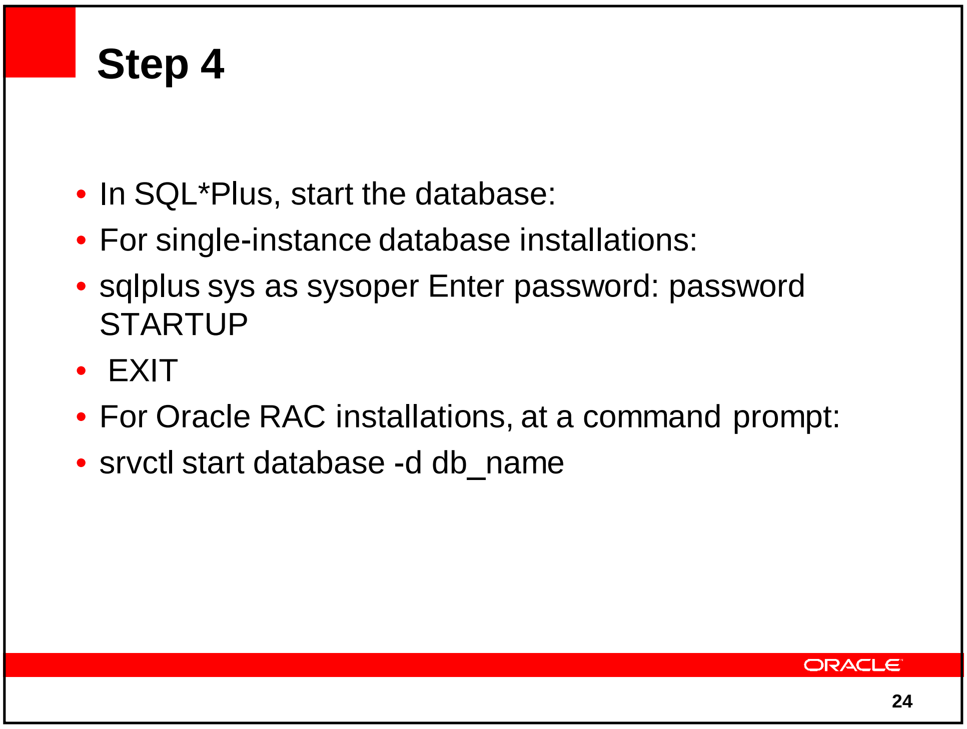
- Shut down the database instance.
- For single-instance installations:
- sqlplus sys as sysoper Enter password: password SHUTDOWN NORMAL EXIT For Oracle RAC installations:
- srvctl stop database -d db_name



Step 3

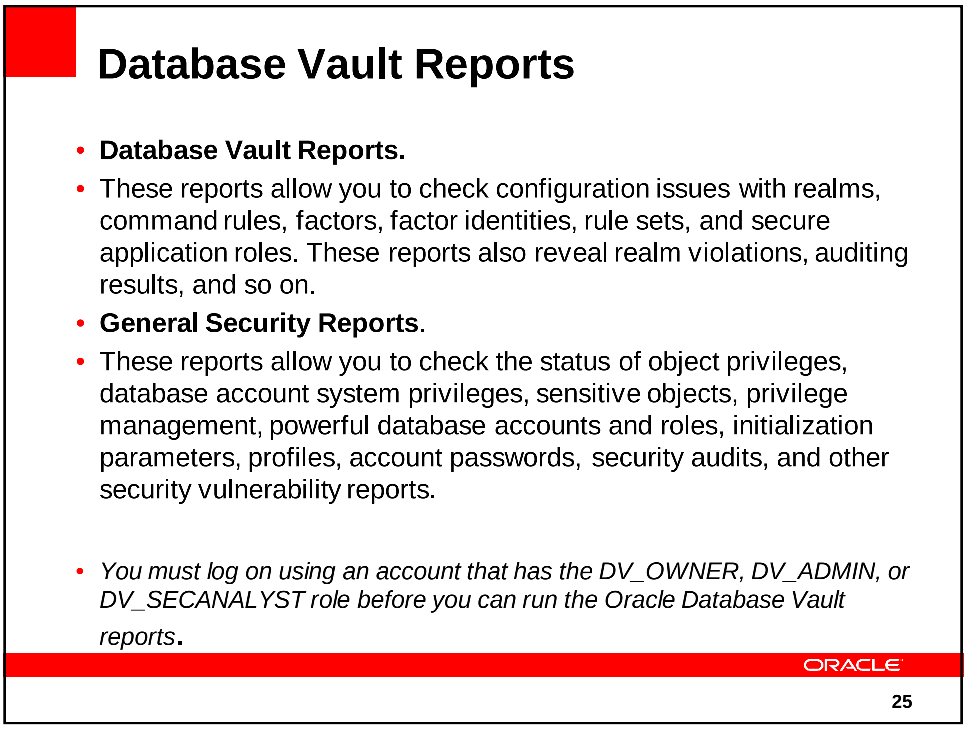
- At command promopt, run the following commands to turn on the Oracle Database Vault option:
- cd $ORACLE_HOME/rdbms/lib
- **make -f ins_rdbms.mk dv_on ioracle**

- For Oracle RAC installations, run these commands on all nodes.



Step 4

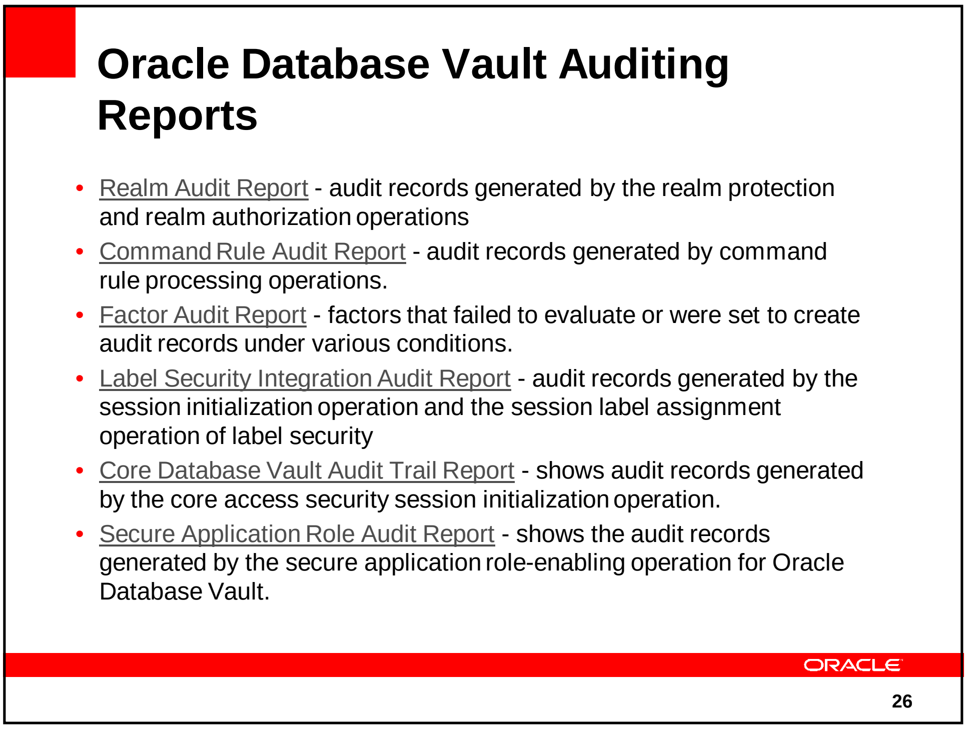
- In SQL*Plus, start the database:
- For single-instance database installations:
- sqlplus sys as sysoper Enter password: password STARTUP
- EXIT
- For Oracle RAC installations, at a command prompt:
- srvctl start database -d db_name



Database Vault Reports

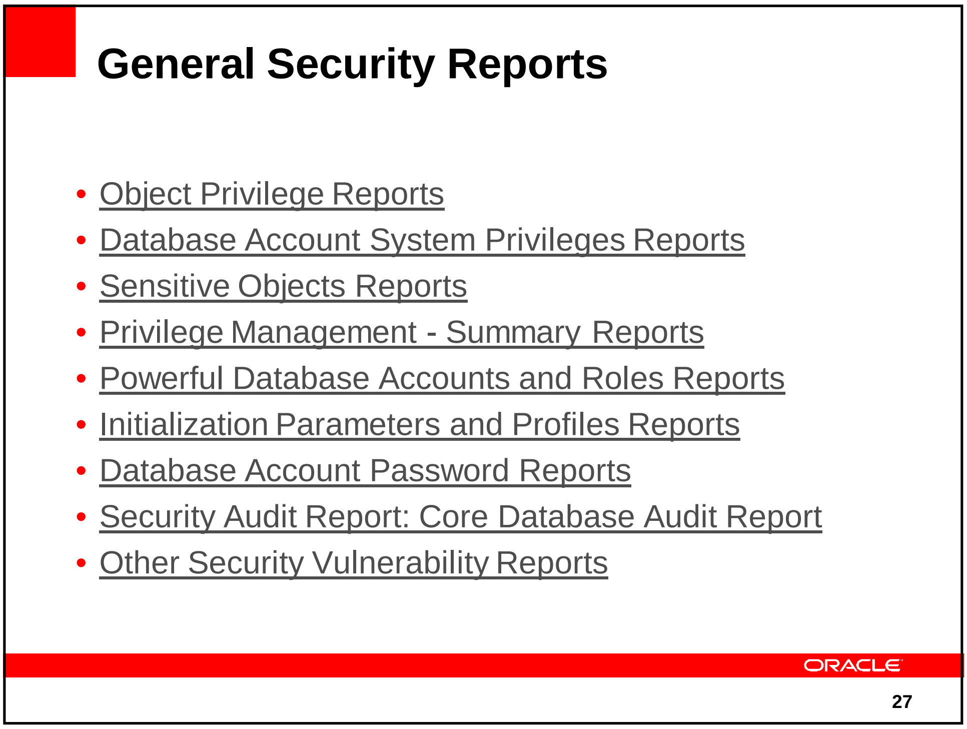
- **Database Vault Reports.**
- These reports allow you to check configuration issues with realms, command rules, factors, factor identities, rule sets, and secure application roles. These reports also reveal realm violations, auditing results, and so on.
- **General Security Reports**.
- These reports allow you to check the status of object privileges, database account system privileges, sensitive objects, privilege management, powerful database accounts and roles, initialization parameters, profiles, account passwords, security audits, and other security vulnerability reports.

- *You must log on using an account that has the DV_OWNER, DV_ADMIN, or DV_SECANALYST role before you can run the Oracle Database Vault reports*.



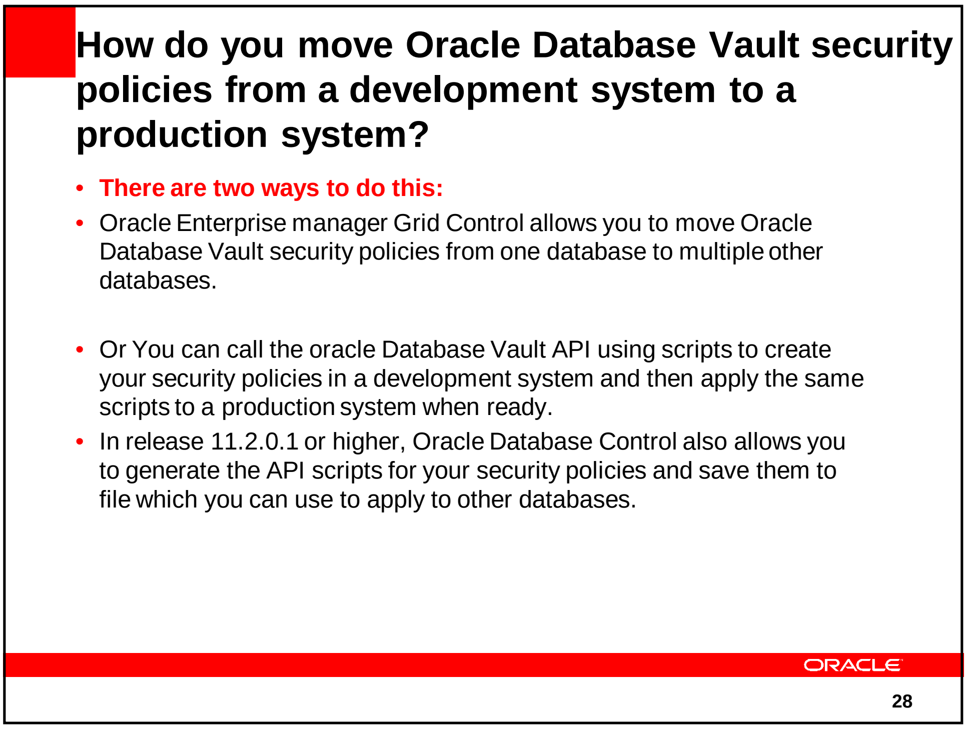
Oracle Database Vault Auditing Reports

- Realm Audit Report - audit records generated by the realm protection and realm authorization operations
- Command Rule Audit Report - audit records generated by command rule processing operations.
- Factor Audit Report - factors that failed to evaluate or were set to create audit records under various conditions.
- Label Security Integration Audit Report - audit records generated by the session initialization operation and the session label assignment operation of label security
- Core Database Vault Audit Trail Report - shows audit records generated by the core access security session initialization operation.
- Secure Application Role Audit Report - shows the audit records generated by the secure application role-enabling operation for Oracle Database Vault.



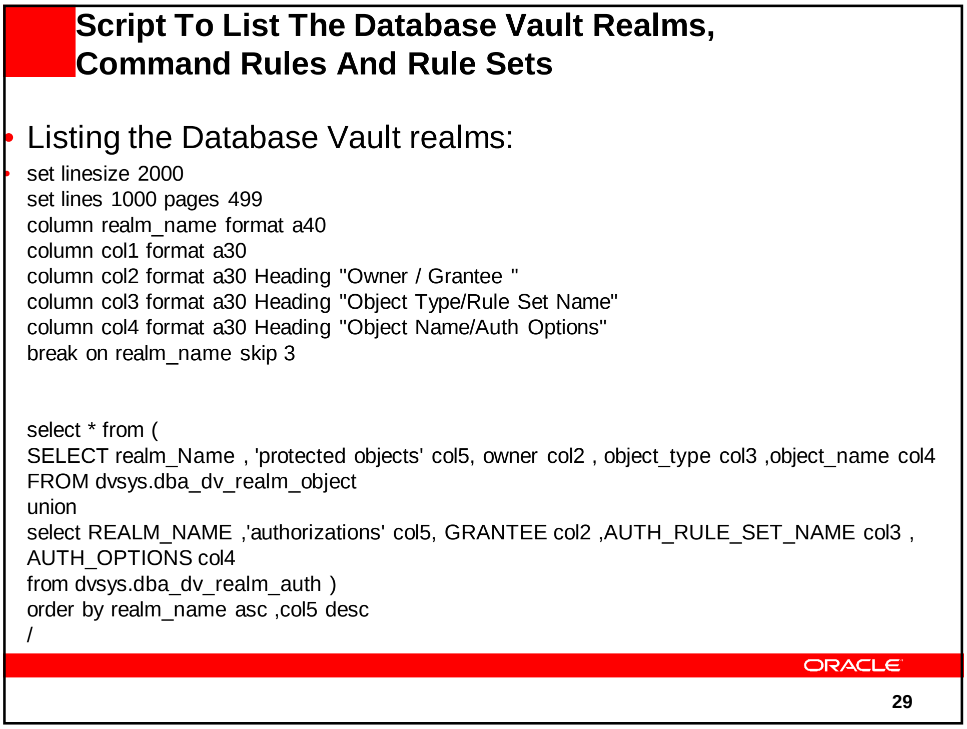
General Security Reports

- Object Privilege Reports
- Database Account System Privileges Reports
- Sensitive Objects Reports
- Privilege Management - Summary Reports
- Powerful Database Accounts and Roles Reports
- Initialization Parameters and Profiles Reports
- Database Account Password Reports
- Security Audit Report: Core Database Audit Report
- Other Security Vulnerability Reports



How do you move Oracle Database Vault security policies from a development system to a production system?

- **There are two ways to do this:**
- Oracle Enterprise manager Grid Control allows you to move Oracle Database Vault security policies from one database to multiple other databases.
- Or You can call the oracle Database Vault API using scripts to create your security policies in a development system and then apply the same scripts to a production system when ready.
- In release 11.2.0.1 or higher, Oracle Database Control also allows you to generate the API scripts for your security policies and save them to file which you can use to apply to other databases.

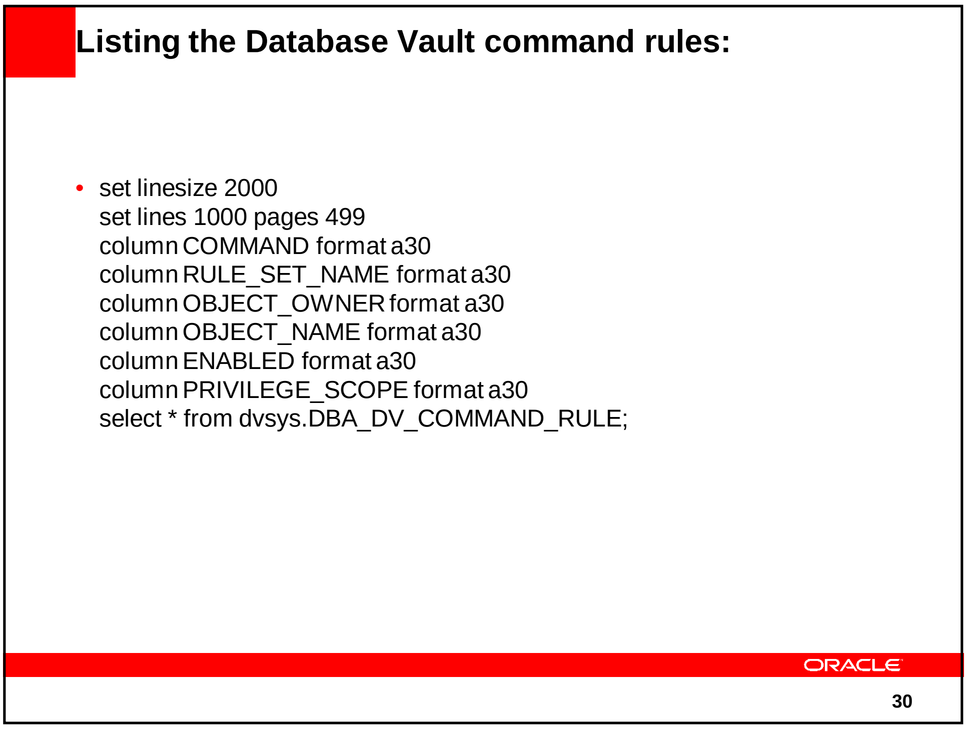


Script To List The Database Vault Realms, Command Rules And Rule Sets

- Listing the Database Vault realms:

```
set linesize 2000
set lines 1000 pages 499
column realm_name format a40
column col1 format a30
column col2 format a30 Heading "Owner / Grantee "
column col3 format a30 Heading "Object Type/Rule Set Name"
column col4 format a30 Heading "Object Name/Auth Options"
break on realm_name skip 3


select * from (
SELECT realm_Name , 'protected objects' col5, owner col2 , object_type col3 ,object_name col4
FROM dvsys.dba_dv_realm_object
union
select REALM_NAME ,'authorizations' col5, GRANTEE col2 ,AUTH_RULE_SET_NAME col3 ,
AUTH_OPTIONS col4
from dvsys.dba_dv_realm_auth )
order by realm_name asc ,col5 desc
/
```



Listing the Database Vault command rules:

```
set linesize 2000
set lines 1000 pages 499
column COMMAND format a30
column RULE_SET_NAME format a30
column OBJECT_OWNER format a30
column OBJECT_NAME format a30
column ENABLED format a30
column PRIVILEGE_SCOPE format a30
select * from dvsys.DBA_DV_COMMAND_RULE;
```

Listing the Database Vault rules and rule sets:

```
column RULE_SET_NAME format a30
column RULE_NAME format a50
column RULE_EXPR format a60
column ENABLED format a8
column RULE_ORDER format 9999
break on RULE_SET_NAME skip 3

select * from dvsys.DBA_DV_RULE_SET_RULE;
```

Learn More

http://search.oracle.com

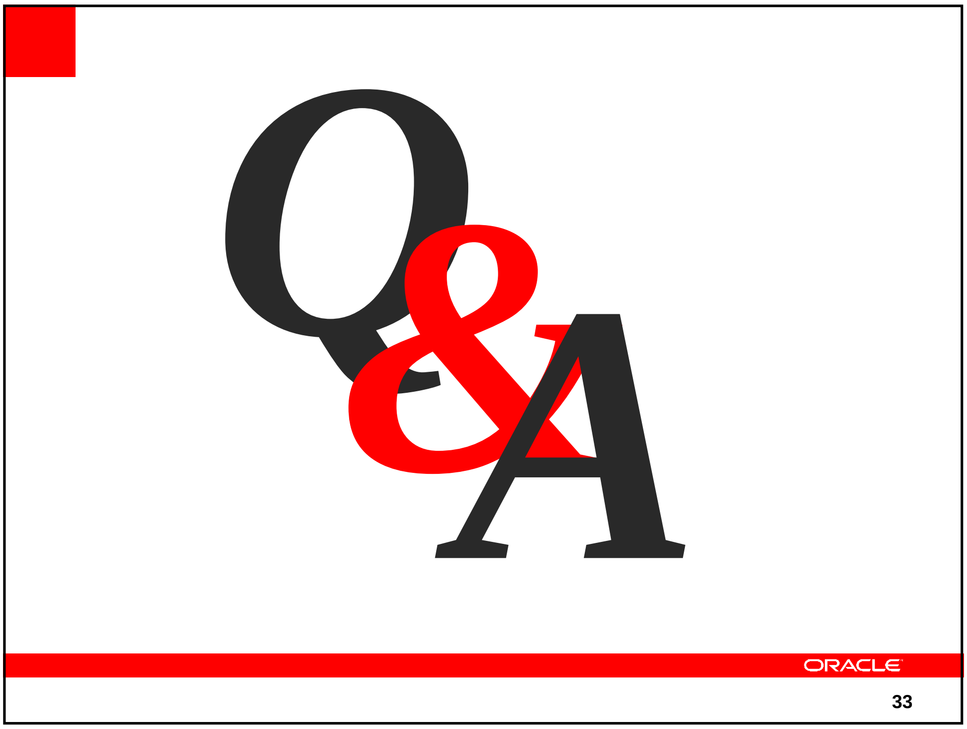
database security 🔍

Technology Overview

- Visit: oracle.com/database/security
  - View Whitepapers and webinars

Technical Information, Demos, Software

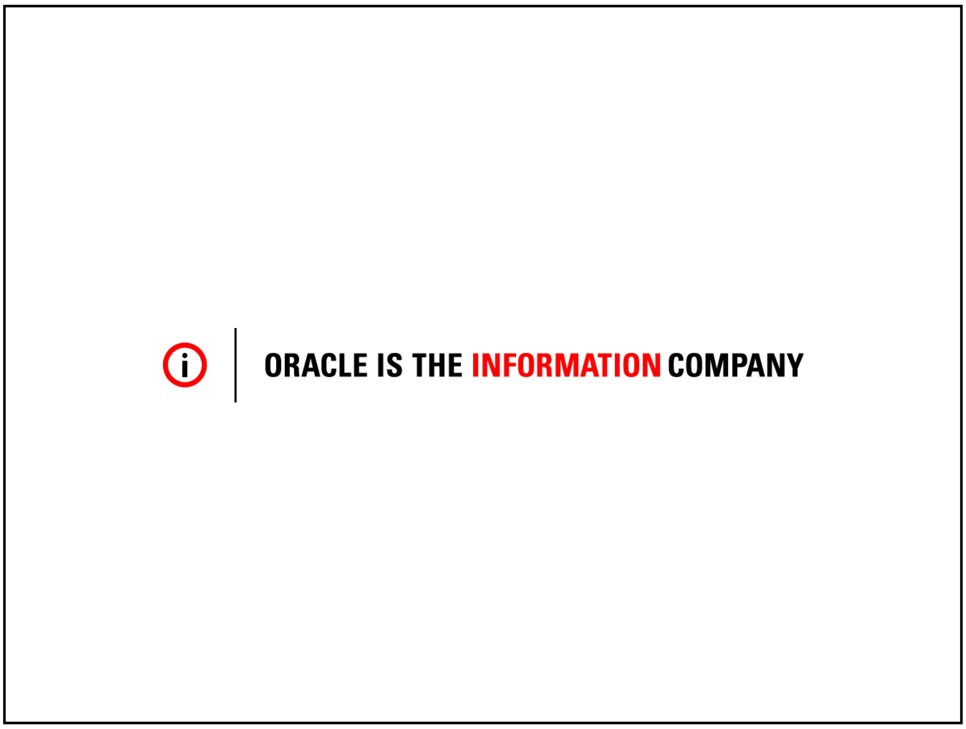
- Visit OTN: otn.oracle.com -> products -> database -> security and compliance



Q&A

ORACLE

33



ORACLE IS THE INFORMATION COMPANY