

SECURITY INSIDE-OUT

Complete Protection for Your Database,
Middleware, and Applications

ORACLE®

Oracle Database Vault
Technical Overview

Agenda

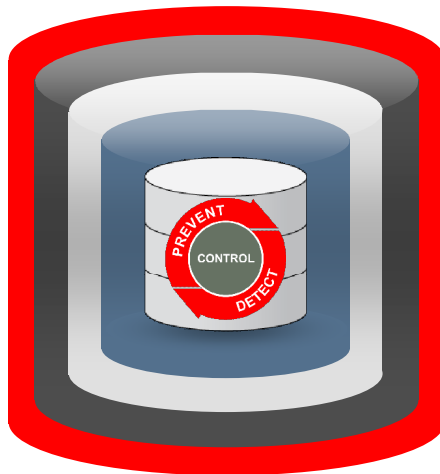
- Oracle Database Security – Defense-in-Depth
- Business drivers
- Technology introduction
- Look inside – how it works
- Demo #1 Preventive controls using Realms
- Demo #2 Trusted paths using command rules and multi-factor authorization
- Customers
- Summary
- Q&A

ORACLE

2

Oracle Database Security

Defense-in-Depth



Encryption and Masking

- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control

- Oracle Database Vault
- Oracle Label Security

Auditing and Tracking

- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

Monitoring and Blocking

- Oracle Database Firewall

ORACLE

3

Oracle Database Vault

Business Drivers

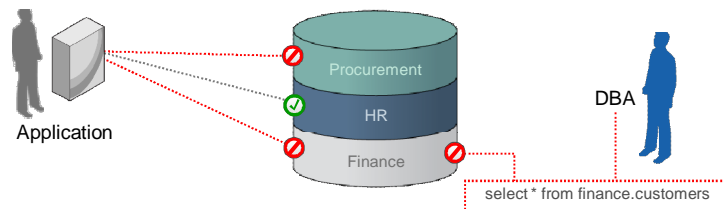
- Outsourcing / Database Consolidation
 - Reduce costs without sacrificing security
 - Enforce separation of duty controls inside the database
- Simplify Privacy and Compliance
 - Prevent audit findings
 - Prevent unauthorized database changes
 - Enforce operational controls inside the database
 - Prevent unauthorized access to sensitive application data

ORACLE

4

Oracle Database Vault

Separation of Duties & Privileged User Controls



- DBA separation of duties
- Limit powers of privileged users
- Securely consolidate application data
- No application changes required
- Works with Oracle Exadata

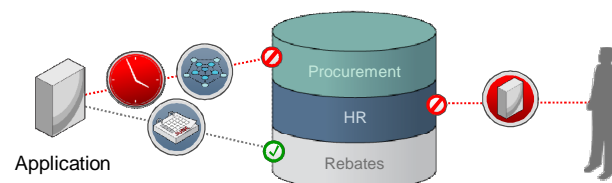


ORACLE

5

Oracle Database Vault

Multi-Factor Access Control Policy Enforcement



- Protect application data and prevent application by-pass
- Enforce who, where, when, and how using rules and factors
- Out-of-the box policies for Oracle applications, customizable

ORACLE

6

Oracle Database Vault

Built-In Factors



- User Factors
 - Name
 - Authentication type
 - Session User
 - Proxy Enterprise Identity
- Network Factors
 - Machine name
 - Client IP
 - Network Protocols
- Extensible
 - Define custom factors
- Database Factors
 - Database IP
 - Database Instance
 - Database Hostname
 - Database SID
- Runtime Factors
 - Language
 - Date
 - Time

ORACLE

7

Oracle Database Vault

Command Rules

- Alter table
- Alter trigger
- Alter package
- Alter tablespace
- Connect / login
- Create table
- Create index
- Create view
- Drop table
- Drop user
- Drop index
- Truncate table
-
-
-

ORACLE

Oracle Database Vault

Reports



- Built-in Auditing and Reporting
 - Realm violation audit report built-in shows attempts to access Realm protected data
 - Privileges reports such as who has the DBA role
- Other reports
 - 2 dozen other Database Vault and security reports
- Easy to administer
 - Web interface and API

ORACLE

9

Oracle Database Vault

Out-of-the-Box Protections For Applications

- Prevent DBA from accessing application data
- Pre-built policies include realms and command rules
- Complements application security
- Transparent to existing applications
- Customizable

Oracle E-Business Suite
11i / R12



PeopleSoft Applications



Siebel, i-Flex



JD Edwards Enterprise One



SAP



Infosys Finacle

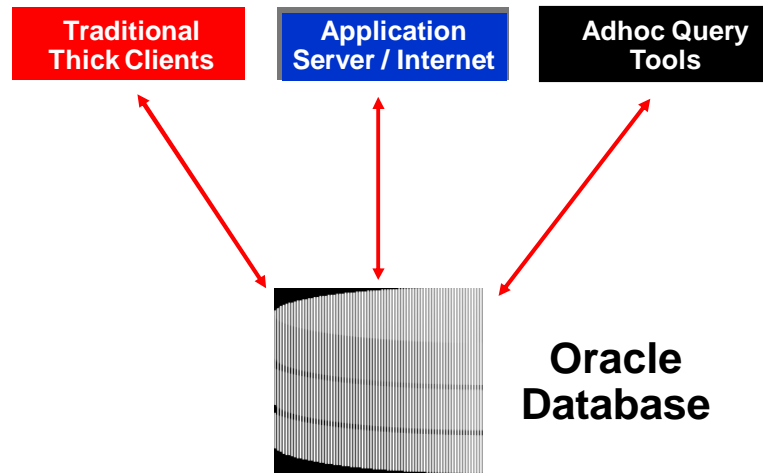


ORACLE

10

Oracle Database

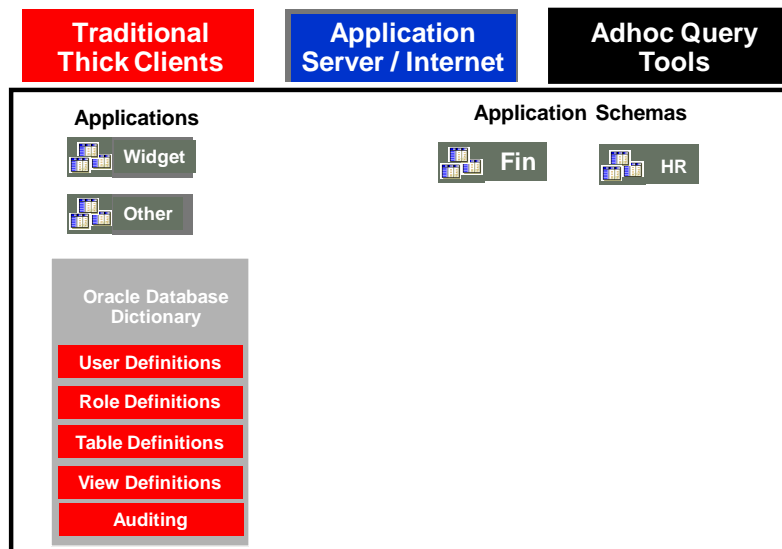
Common Data Center Architectures



ORACLE

11

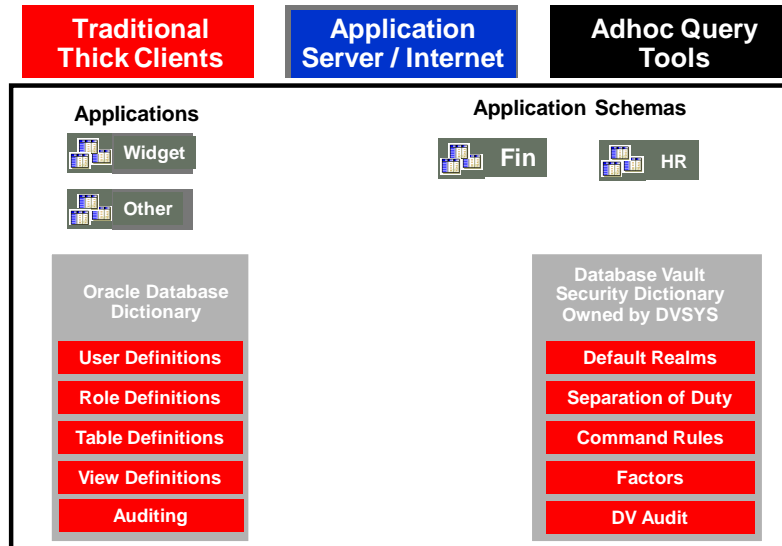
Oracle Database Without Database Vault



ORACLE

12

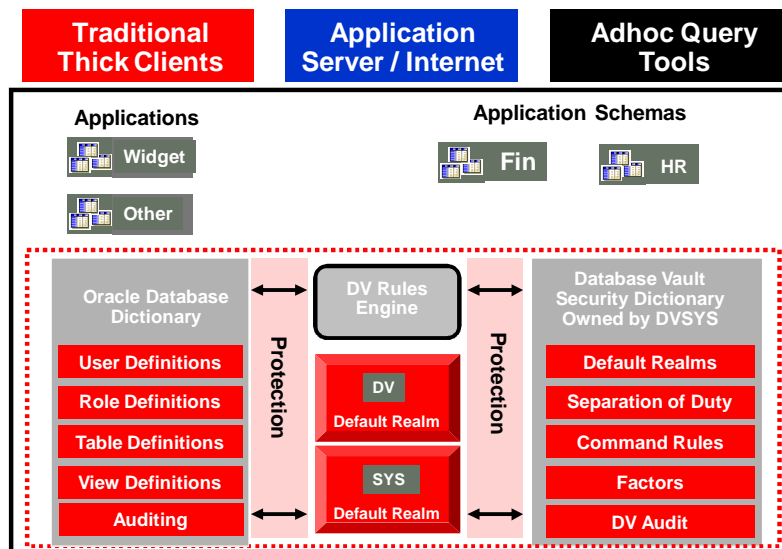
Oracle Database Vault Architecture



ORACLE

13

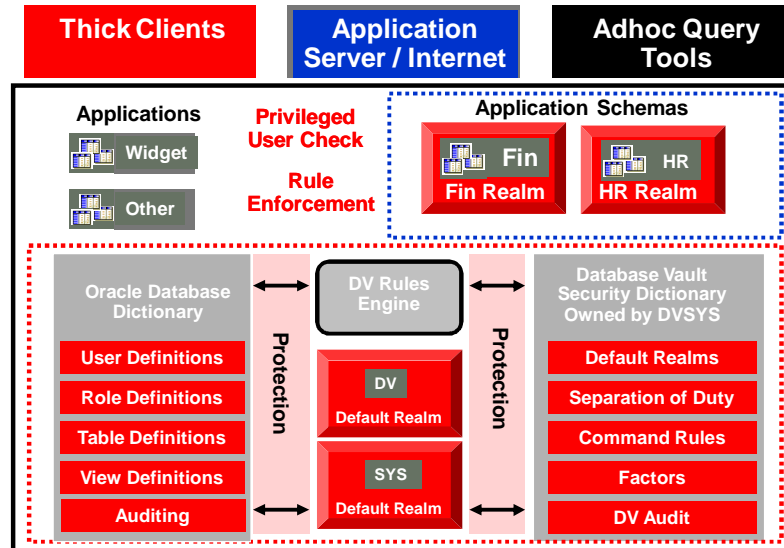
Oracle Database Vault Architecture



ORACLE

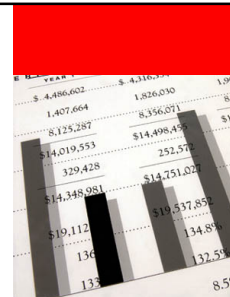
14

Oracle Database Vault Architecture



ORACLE

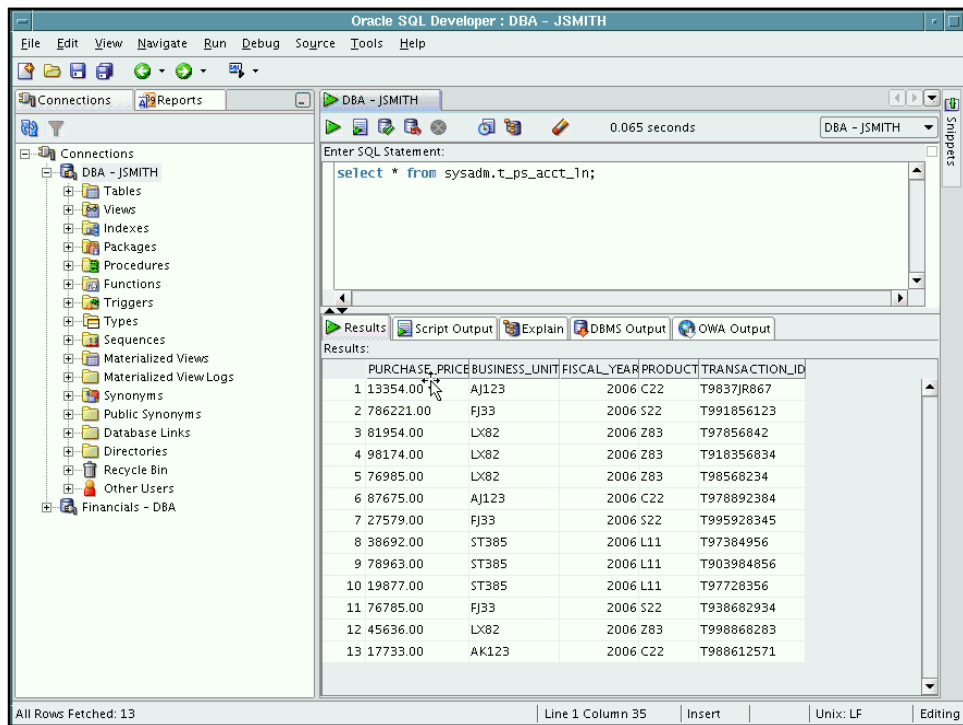
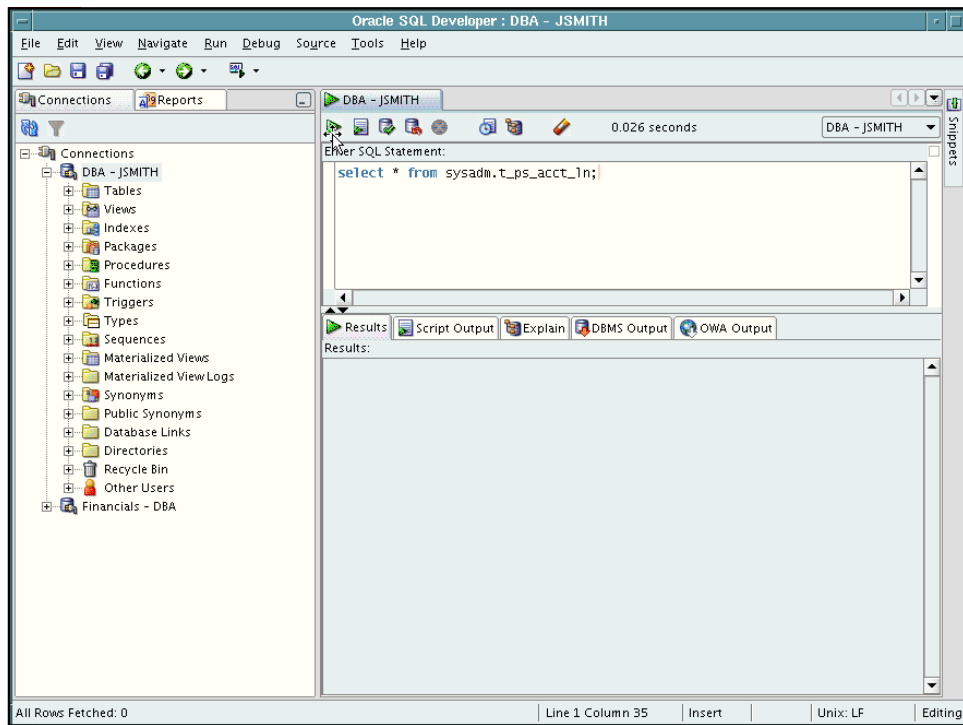
15



Demo #1:

Protecting application data from privileged users using Realms

ORACLE



Database Vault Administration Page

ORACLE Database Vault Help Logout Database

Database Instance: un102232

Logged in as DEV_OWNER

Administration [Database Vault Reports](#) [General Security Reports](#) [Monitor](#)

The links below allow you to protect applications and data using Oracle Database Vault features that include: Realms, Command Rules, Rule Sets, Factors, and Secure Application Roles.

Database Vault Feature Administration

- [Realms](#)
- [Command Rules](#)
- [Factors](#)
- [Rule Sets](#)
- [Secure Application Roles](#)
- [Label Security Integration](#)

Administration [Database Vault Reports](#) [General Security Reports](#) [Monitor](#)

Database | Help | Logout

19

Step 1. Defining a Realm

ORACLE Database Vault Help Logout Database

Database Instance: un102232 > Realm > Create Realm

Logged in as DEV_OWNER

Create Realm Cancel OK

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

* Name

Description

Status ☒ Enabled ☐ Disabled

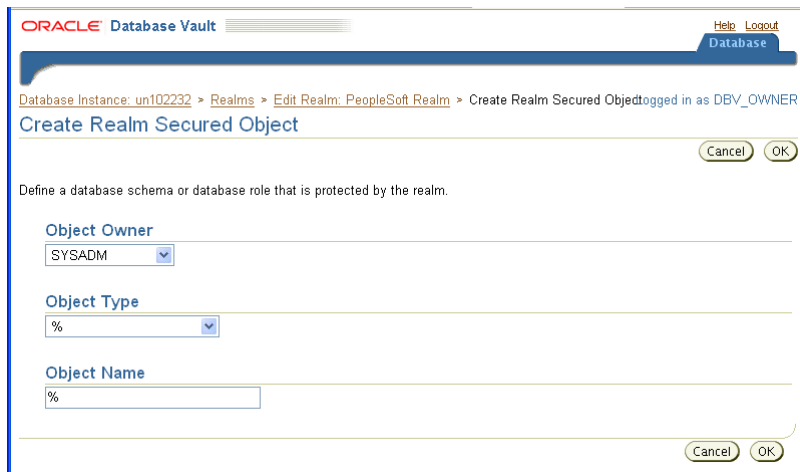
Audit Options

☐ Audit Disabled ☒ Audit On Failure ☐ Audit On Success or Failure

ORACLE

20

Step 2. Adding Protected Schema



ORACLE Database Vault Help Logout Database

Database Instance: un102232 > Realms > Edit Realm: PeopleSoft Realm > Create Realm Secured Object logged in as DBV_OWNER

Create Realm Secured Object

Cancel OK

Define a database schema or database role that is protected by the realm.

Object Owner
SYSADM

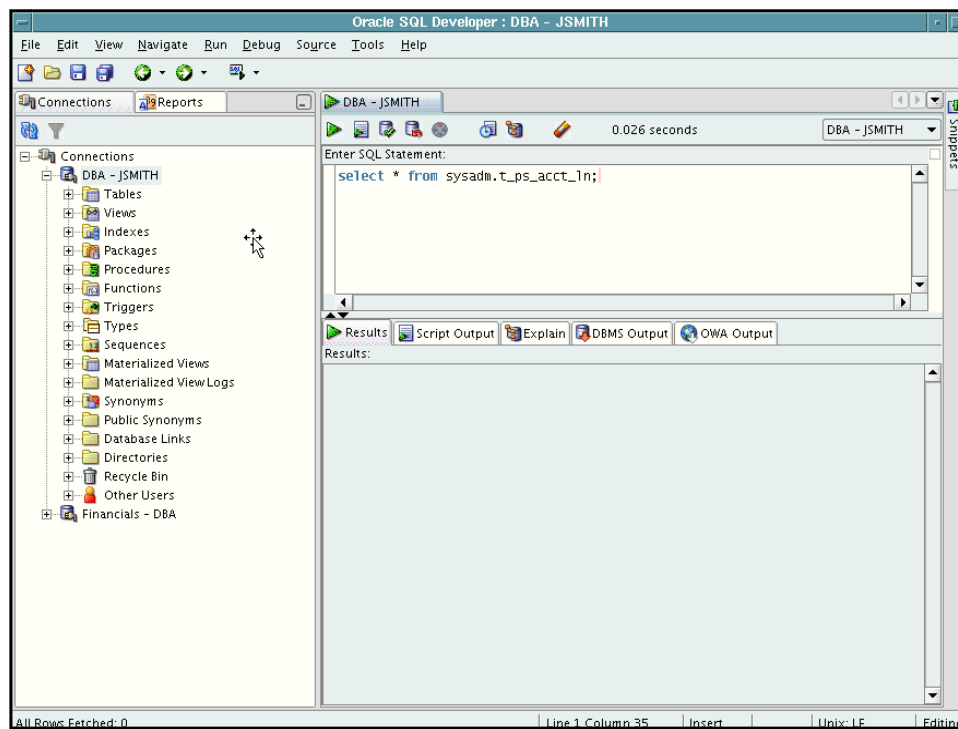
Object Type
%

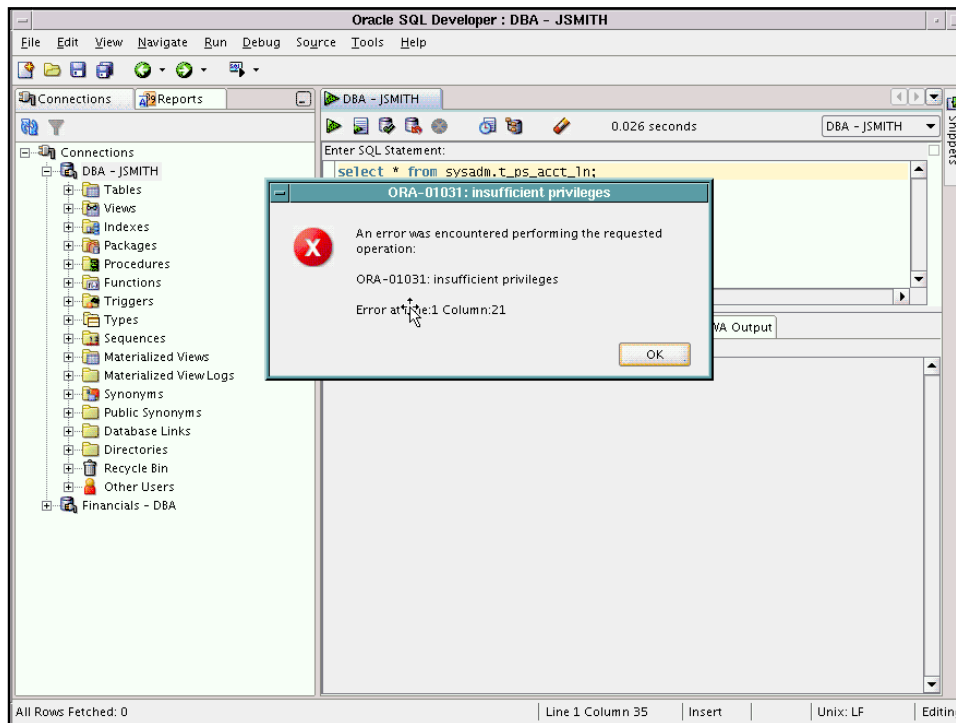
Object Name
%

Cancel OK

ORACLE

21





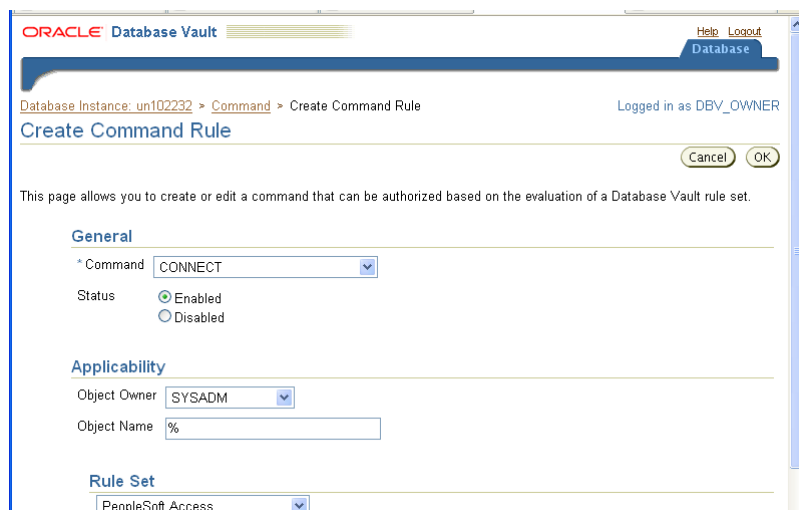
Demo #2:

Creating a Trusted Path - Limiting connection from non-application server IP addresses using Command Rules

ORACLE

Limit Access to Specific IP Addresses

Creating a Command Rule



ORACLE Database Vault Help Logout Database

Database Instance: un102232 > Command > Create Command Rule Logged in as DBV_OWNER

Create Command Rule

Cancel OK

This page allows you to create or edit a command that can be authorized based on the evaluation of a Database Vault rule set.

General

* Command:

Status: ☒ Enabled ☐ Disabled

Applicability

Object Owner:

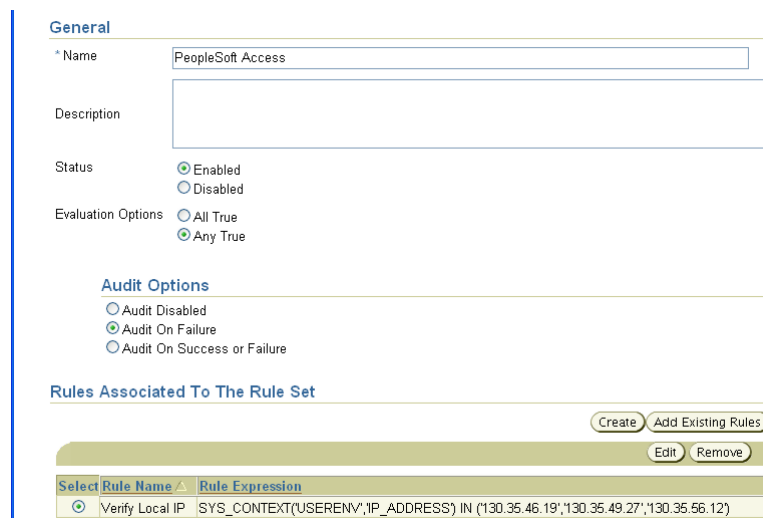
Object Name:

Rule Set

ORACLE

25

List of Allowed IP Addresses



General

* Name:

Description:

Status: ☒ Enabled ☐ Disabled

Evaluation Options: ☐ All True ☒ Any True

Audit Options

☐ Audit Disabled ☒ Audit On Failure ☐ Audit On Success or Failure

Rules Associated To The Rule Set

Create Add Existing Rules

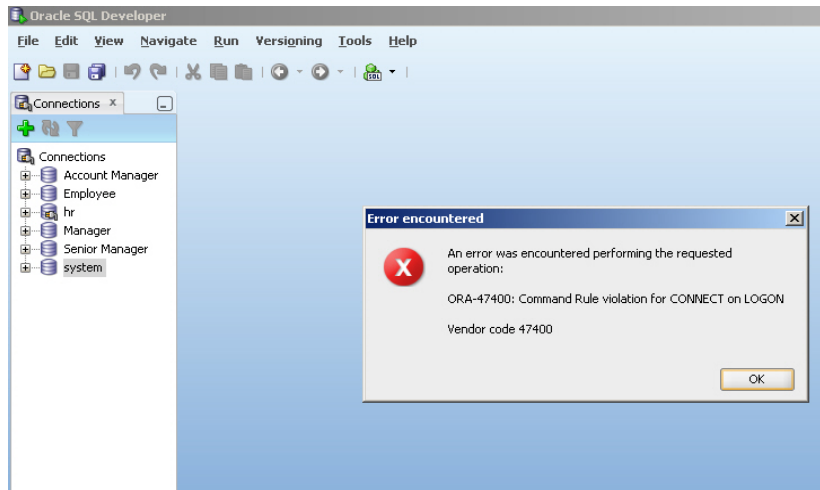
Edit Remove

Select	Rule Name	Rule Expression
<input checked="" type="radio"/>	Verify Local IP	SYS_CONTEXT('USERENV','IP_ADDRESS') IN ('130.35.46.19','130.35.49.27','130.35.56.12')

ORACLE

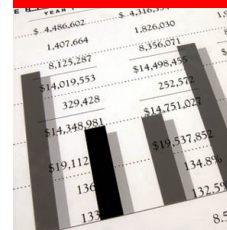
26

Connection Blocked from Other IP Addresses



ORACLE

27



Oracle Database Vault Customers

ORACLE

Absa Group Limited

http://www.itweb.co.za/index.php?option=com_content&view=article&id=29021&Itemid=1&lang=en

Latest Headlines

Oracle Manufacturing

ORACLE
oracle.com/goto/industry
or call 1.800.ORACLE.1

FREE NEWSLETTERS IT DIRECTORY NEWS ALERTS RSS NEWS TIP-OFFS ADD TO FAVOURITES

Web INDUSTRYSOLUTIONS

HOME COLUMNISTS IN DEPTH INDUSTRY VIEWS SURVEYS JOBS EVENTS SERVICES PUBLICATION

COLUMNISTS HOME BOOTH'S BITES DOUBLE TAKE IT HAPPENS IT'S ALL GEEK TO ME OFF THE HOOK THE SPIKE

VIRTUAL PRESS OFFICES™ By company By industry sector (011) 807 3294 itnews

You are here > Home > IndustrySolutions

Absa steps up compliance with Oracle

Oracle
Press release issued by Emerging Media Communications
5 Jan 2010

VISIT OUR PRESS OFFICE POST YOUR COMMENT

Read in this story A need for compliance A solid audit trail Consistent configuration throughout Absa The road ahead

One of South Africa's largest financial services groups, the Absa Group Limited (Absa), has been a prominent innovator in the financial services industry and offers a complete range of banking, bank assurance and wealth management products and services.

Premlin Pillay, Head of Group Information Services at Absa:
"Oracle Database Vault provides a security solution inside the Oracle Database, which enables our existing applications to comply with these and possibly future regulations without much customisation,
..."

ORACLE

29



Financial Customer



Customer Profile

- Annual revenue €39.283 Billion
- Over 2000 employees
- Located in Dusseldorf, Germany

Challenge

- Meet internal and external compliance requirements
- Streamline data management, consolidate applications
- Protect the privacy and security of very sensitive data

Solution

- **Oracle Database Vault**
 - Separation of Duties
 - Realms and Command Rules to restrict DBAs access to data
 - Consolidate multiple applications into one DB

Results

"With this new solution provided by Oracle our highly sensitive personal data is now protected against unauthorized access. We therefore were able, to integrate our hr applications into our centralized IT and save cost."
Detlev Althaus, Deutsche Apotheker

ORACLE

30



CMC Markets

Financials Customer



Customer Profile

- Annual revenue \$312 million
- Over 1000 employees
- Located in London, United Kingdom

Challenge

- Meet internal and external compliance requirements
- Streamline data management, consolidate applications
- Protect the privacy and security of very sensitive data

Solution

- **Oracle Database Vault**
 - Separation of Duties
 - Realms and Command Rules to restrict DBAs access to data
 - Consolidate multiple applications into one DB

Results

"Our aim is to have the most secure database systems in our industry which protect our client data and our business from internal and external threats. The Oracle security components underpinning our standard Oracle security configuration bring a new level of assurance to our senior management and audit teams."

Akash Gharu, Global Database Services Manager

ORACLE

31

대우증권



DAEWOO
SECURITIES

Financial Customer



Customer Profile

- Investment banking and brokerage service
- Over 3000 employees
- Located in Seoul, Korea

Challenge

- Meet internal and external compliance requirements
- Prevent privileged user access to sensitive data
- Enhance security without rebuilding the application code

Solution

- **Oracle Database Vault and Oracle Advanced Security**
 - Separation of Duties
 - Realms and Command Rules to restrict DBAs access to data
 - Use Transparent Data Encryption for encryption

Results

"We used Oracle's database security solutions to resolve internal security issues, a common challenge for financial institutions. Oracle Database Vault offers internal controls that help secure human resources data, while Oracle Advanced Security has automated encryption functions that further protects sensitive information." – Jung HakSoo, Deputy Manager, Infrastructure Development Department, Daewoo Securities

ORACLE

32

SAP Utility Customer – Hydro One

hydroOne

“Oracle Database Vault is helping Hydro One to further address regulatory compliance,” said Norman Crook, Director IT Service Delivery, Hydro One Networks Inc. “With Oracle Database Vault, Hydro One is positioned to complete the final stages of the SAP security roadmap, further strengthening the security policies safeguarding our data.”

Challenge

- Meet internal and external compliance requirements - NERC
- Protect the privacy and security of SAP sensitive data
- Prevent any tampering of data by privileged users

Solution

- **Oracle Database Vault**
 - Apply Database Vault Protections for SAP
 - Realms and Command Rules to restrict DBAs access to sensitive data
 - Multi-Factor authorization to further enhance data security

Results

- Ensure compliance with regulations – NERC Regulations
- Reduce the risk of data breaches and impropriety
- Enhance SAP Application Availability by gaining confidence that no user can change database objects without the Security Administrator's approval

ORACLE

33

Oracle Database Vault (DBV)

Regulatory Legislation	Regulation Requirement	Does DBV Mitigate This Risk?
Sarbanes-Oxley Section 302	Unauthorized changes to data	Yes
Sarbanes-Oxley Section 404	Modification to data, Unauthorized access	Yes
Sarbanes-Oxley Section 409	Denial of service, Unauthorized access	Yes
Gramm-Leach-Bliley	Unauthorized access, modification and/or disclosure	Yes
HIPAA 164.306	Unauthorized access to data	Yes
HIPAA 164.312	Unauthorized access to data	Yes
Basel II – Internal Risk Management	Unauthorized access to data	Yes
CFR Part 11	Unauthorized access to data	Yes
Japan Privacy Law	Unauthorized access to data	Yes
PCI – Requirement 7	Restrict access to cardholder data by business need-to-know	Yes
PCI – Requirement 8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed	Yes
PCI – Compensating Controls for Requirement 3.4	Provide ability to restrict access to cardholder data or databases based on the following criteria: <ul style="list-style-type: none"> • IP address/Mac address • Application/service • User accounts/groups 	Yes
PCI - Requirement A.1: Hosting providers protect cardholder data environment	Ensure that each entity only has access to own cardholder data environment	Yes

ORACLE

34

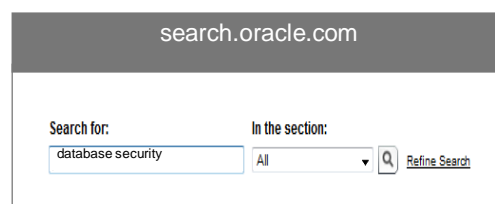
Summary

- Restrict full access of privileged users
 - Restrict access to application data stored in the database
 - Enforce Separation of duty controls
- Easily implement environment based access control
 - User parameters
 - Network parameters
 - Database parameters
- Applying on existing applications
 - Highly transparent
- Minimal performance impact
 - Less than 5%

ORACLE

35

For More Information



The screenshot shows the search.oracle.com search bar. It has a search input field containing 'database security' and a dropdown menu set to 'All'. There is a search button with a magnifying glass icon and a 'Refine Search' link.

oracle.com/database/security

ORACLE

36



Q&A

ORACLE

37



ORACLE IS THE **INFORMATION** COMPANY

ORACLE

38

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.