

SECURITY INSID=OUT

Complete Protection for Your Database,
Middleware, and Applications

ORACLE®

Database Activity Monitoring and Audit

Mukhi Sanjay Kumar

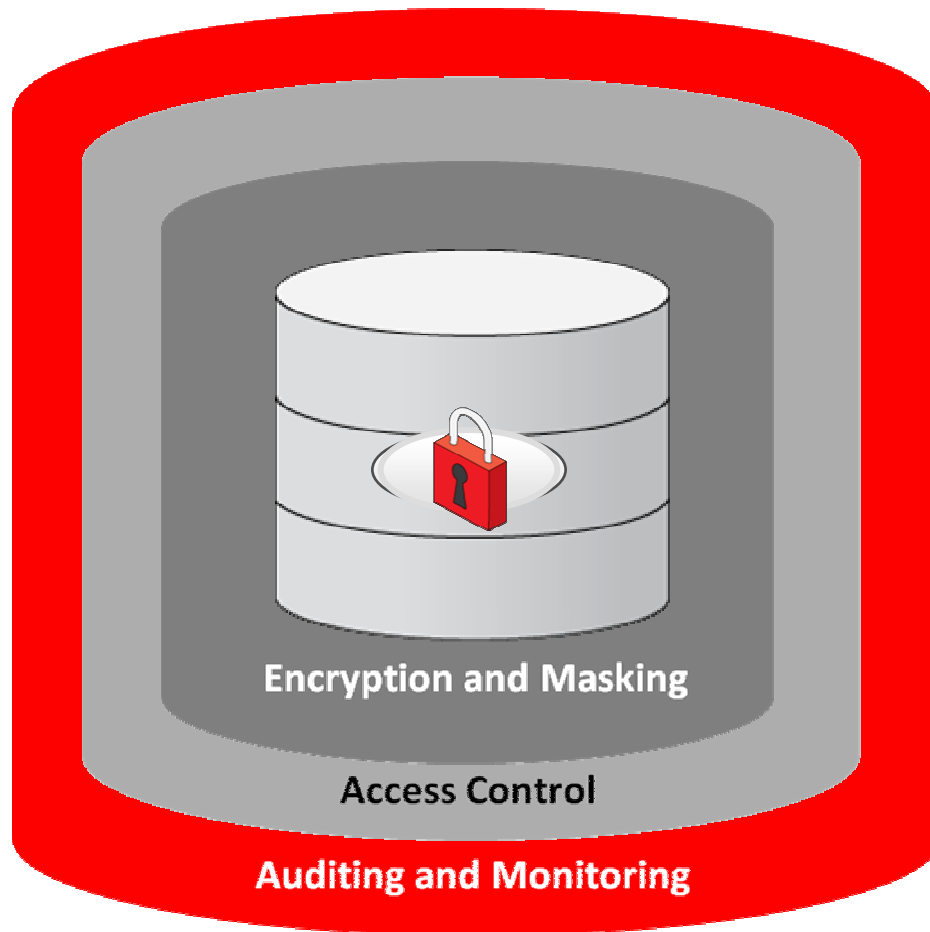
Lead Database Architect – Pakistan & SAGE



Agenda

- **Oracle Database Security – Defense-in-Depth**
- **Business drivers**
- **Solution Overview**
 - **Heterogeneous Database Support**
 - **Secure and Scalable Repository**
 - **Reporting and Alerts**
- **Applications Support**
- **Summary**
- **Q & A**

Database 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 Monitoring

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

ORACLE



Oracle Audit Vault

Business Drivers

- Detective controls
 - Monitor privileged application user accounts.
 - Audit non-application access to sensitive data (credit card, financial data, PII data etc).
 - Enforce application security controls.
- Compliance Reporting
 - Eliminate costly and complex scripts for reporting.
 - Reduce reporting costs for specific compliance audits.
 - SOX, PCI, HIPAA, SAS 70, STIG .

Oracle Audit Vault

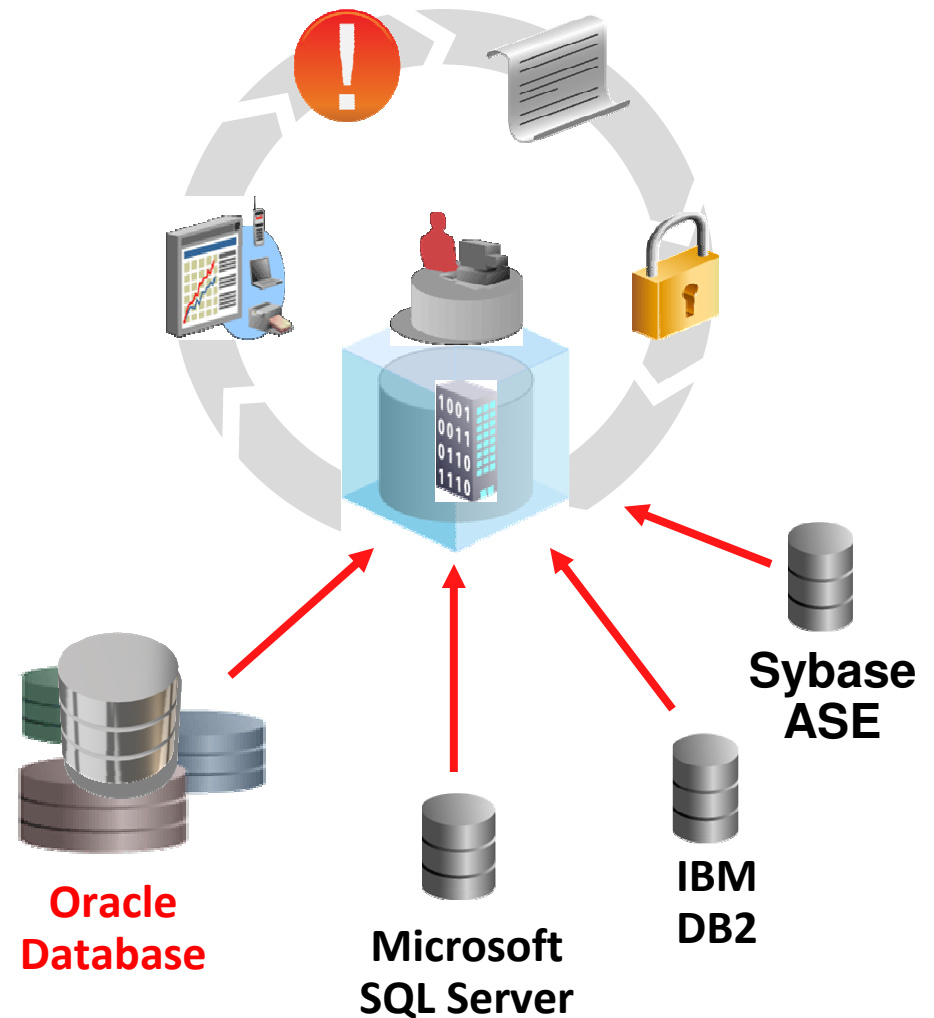
Trust-but-Verify

Consolidate and Secure
Audit Data

Out-of-the Box
Compliance Reports

Alert on
Security Threats

Lower IT Costs With
Entitlements & Audit Policies



ORACLE



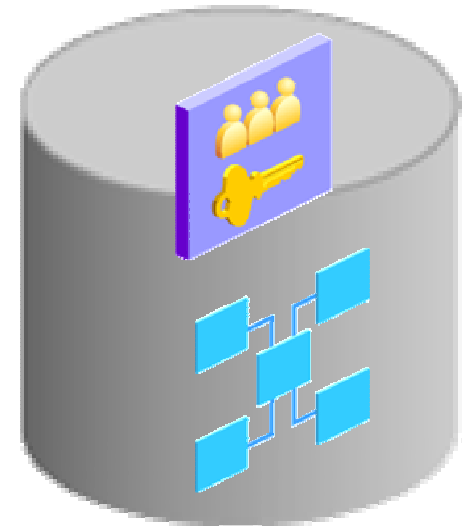
Oracle Audit Vault

Heterogeneous database Support

- Oracle Database Auditing
 - Collect audit data from Audit Tables, OS file, Syslog and redo log
- Microsoft SQL server versions 2000, 2005, & 2008
 - Collect Server Side trace, C2 auditing and Windows Event viewer audit.
- IBM DB2 8.2 - 9.5 on Linux, Unix, Windows
 - Extract binary audit files into a trace file
- Sybase ASE 12.5.4 - 15.0.x
 - Utilize the native audit tables

Secure & Scalable Audit Warehouse

- **Audit Warehouse**
 - Uses Oracle Data Warehouse Technologies
 - Enable BI and analysis
- **Performance and Scalability**
 - Built-in partitioning
 - Database compression
 - Scales to Terabytes
 - Certified with Oracle RAC
- **Protected with Built-in Security**
 - Encrypted audit data transmission
 - Separation of Duty provided by Database Vault
 - Audit Vault Administrator
 - Audit Vault Auditor



Oracle Audit Vault 10.2.3.2

Default Reports

ORACLE Enterprise Manager 10g
Audit Vault

Home Audit Reports Audit

Default Reports Compliance Reports Custom Reports Generated Reports Report Schedules Entitlement Snapshots

Access Reports



- [Activity Overview](#)
- [Data Access](#)
- [Database Vault](#)
- [Distributed Database](#)
- [Procedure Executions](#)
- [User Sessions](#)

Management Activity Reports



- [Account Management](#)
- [Audit Commands](#)
- [Object Management](#)
- [Procedure Management](#)
- [Role and Privilege Management](#)
- [System Management](#)

System Exception Reports



- [Exception Activity](#)
- [Invalid Audit Record Activity](#)
- [Uncategorized Activity](#)

Entitlement Reports



- [User Accounts](#)
- [User Accounts by Source](#)

- [User Privileges](#)
- [User Privileges by Source](#)

- [User Profiles](#)
- [User Profiles by Source](#)

- [Database Roles](#)
- [Database Roles by Source](#)

- [System Privileges](#)
- [System Privileges by Source](#)

- [Object Privileges](#)
- [Object Privileges by Source](#)

- [Privileged Users](#)
- [Privileged Users by Source](#)

Alert Reports



- [All Alerts](#)
- [Critical Alerts](#)
- [Warning Alerts](#)

ORACLE

Oracle Audit Vault

Consolidated Reports Span Enterprise Databases

Activity Overview

Activity Overview

Search: Rows: 15 Go

	Source	Category	Event	User	Target	Host	Event Time
	HR.ORACLE.VM	OBJECT MANAGEMENT	CREATE TABLE	PASSPORT	VISA	oel4upd4.oracle.vm	11-JUN-08 10:02:53
	HR.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 17:13:28
	HR.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 17:13:19
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 16:19:35
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 16:19:25
	HR.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 17:13:28
	HR.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 17:13:19
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 16:19:35
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 16:19:26
	mysqlserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avsrcusr	configurations	oracle_ss	11-JUN-08 13:22:02
	mysqlserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avsrcusr	configurations	oracle_ss	11-JUN-08 13:22:02
	mysqlserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avsrcusr	fn_trace_getinfo	oracle_ss	11-JUN-08 13:22:02
	mysqlserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avsrcusr	fn_trace_gettable	oracle_ss	11-JUN-08 13:50:05
	mysqlserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avsrcusr	fn_trace_gettable	oracle_ss	11-JUN-08 13:50:02
	mysqlserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avsrcusr	fn_trace_gettable	oracle_ss	11-JUN-08 13:50:00



User Entitlement Reports

Oracle Databases

- Report all user accounts, roles, and privileges
- Retrieve a snapshot of user entitlement data
- Compare changes in user accounts and privileges
- View SYSDBA/SYSOPER privileges
- Searching capabilities
- Regulations: SOX, PCI, HIPAA, SAS 70, STIG

Database User Privileges Report

ORACLE Enterprise Manager 10g
Audit Vault

Default Reports Compliance Reports Custom Reports Generated Reports Report Schedules Entitlement Snapshots

User Privileges

Label **LATEST** compare

Rows **500**

User / Role = 'PJONES'

Source	Label	User / Role	Type	Privilege	Role	Owner	Target	Grantor
PAYROLL.Oracle.VM	LATEST	PJONES	USER		CONNECT			
PAYROLL.Oracle.VM	LATEST	PJONES	USER		DBA			
PAYROLL.Oracle.VM	LATEST	PJONES	USER		RESOURCE			
PAYROLL.Oracle.VM	LATEST	PJONES	USER	ALTER		SCOTT	DEPT	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	ALTER		SCOTT	EMP	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	ALTER USER				
PAYROLL.Oracle.VM	LATEST	PJONES	USER	CREATE DATABASE LINK				
PAYROLL.Oracle.VM	LATEST	PJONES	USER	CREATE SESSION				
PAYROLL.Oracle.VM	LATEST	PJONES	USER	CREATE USER				
PAYROLL.Oracle.VM	LATEST	PJONES	USER	DEBUG		SCOTT	DEPT	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	DEBUG		SCOTT	EMP	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	DELETE		SCOTT	DEPT	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	DELETE		SCOTT	EMP	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	DROP PUBLIC DATABASE LINK				
PAYROLL.Oracle.VM	LATEST	PJONES	USER	DROP USER				
PAYROLL.Oracle.VM	LATEST	PJONES	USER	FLASHBACK		SCOTT	DEPT	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	FLASHBACK		SCOTT	EMP	SCOTT
PAYROLL.Oracle.VM	LATEST	PJONES	USER	INDEX		SCOTT	DEPT	SCOTT

ORACLE

User Account Details

Account, Roles, System/Object Privileges

User HR
Label LATEST
Source PAYROLL.Oracle.VM

Account

Account Status	OPEN
Expiration Date	
Initial Lock Date	
Default Tablespace	USERS
Temporary Tablespace	TEMP
Initial Consumer Resource Group	DEFAULT_CONSUMER_GROUP
Created	11/9/2008 02:41:22 AM
Profile	DEFAULT
External Name	

Roles

Role	Admin Option	Default
RESOURCE	NO	YES

row(s) 1 - 1 of 1

System Privileges

Privilege	Admin Option	Default
ALTER SESSION	NO	
CREATE DATABASE LINK	NO	
CREATE SEQUENCE	NO	
CREATE SESSION	NO	
CREATE SYNONYM	NO	
CREATE VIEW	NO	
UNLIMITED TABLESPACE	NO	

row(s) 1 - 7 of 7

Object Privileges

Privilege	Owner	Column Name	Grantable	Table Name	Grantor
EXECUTE	SYS		NO	DBMS_STATS	SYS

row(s) 1 - 1 of 1

Out-of-the-box Compliance Reports

PCI

Widget's PCI Reports



- [Credit Card Related Data Access](#)
- [Audit Setting Changes](#)
- [Before/After Values](#)
- [Database Failed Logins](#)
- [Database Login/Logoff](#)
- [Database Logoff](#)
- [Database Logon](#)
- [Database Startup/Shutdown](#)
- [Deleted Objects](#)
- [Program Changes](#)
- [Schema Changes](#)
- [System Events](#)

Financial



- [Financial Related Data Access](#)
- [Financial Related Data Modifications](#)
- [Audit Setting Changes](#)
- [Before/After Values](#)
- [Database Failed Logins](#)
- [Database Login/Logoff](#)
- [Database Logoff](#)
- [Database Logon](#)
- [Database Startup/Shutdown](#)
- [Program Changes](#)
- [Schema Changes](#)
- [System Events](#)

Health Care



- [EPHI Related Data Access](#)
- [Audit Setting Changes](#)
- [Before/After Values](#)
- [Database Failed Logins](#)
- [Database Login/Logoff](#)
- [Database Logoff](#)
- [Database Logon](#)
- [Database Startup/Shutdown](#)
- [Deleted Objects](#)
- [Schema Changes](#)
- [System Events](#)

Reports Management

Schedule, Retention, Notification, Attestation

Create or Schedule PDF Report

Category Name: Access Reports Report Name: Activity Overview

Schedule

Run: Immediately Specify Schedule Select Schedule

Repeat: Weekly

Run Time: 12:00 AM Timezone: -07:00

Interval (Weeks): 1

Start Date:

10/5/2009

End Date:

Days of Week: Mon Tue Wed Thu Fri Sat Sun

Retention

Retention Time: 1 years 2 months

Notification

Send: Notification Attachment

Template: --No Template-- Profile: --No Profile--

To e-mail: Cc:

Add to List

Profile Name	To	Cc	Template Name	Template Type	Delete
SecurityTeam			Report Notification Template	Report Notification	

Attestation

The following auditors need to attest to this report

AVAUDITOR	LAURA
AVREPORTUSER	MARK
	TBEDNAR

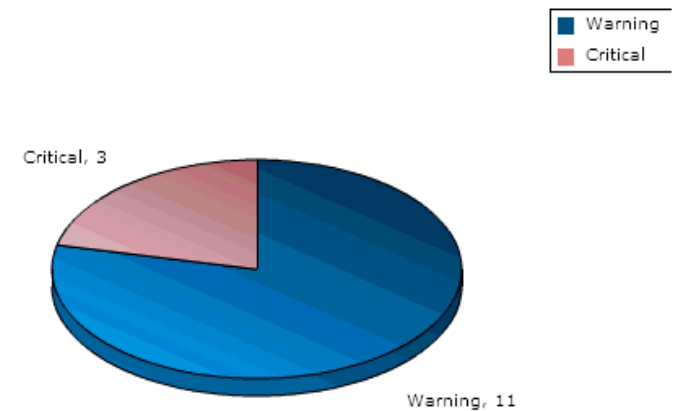
Oracle Audit Vault Alerts

Threat Detection with Custom Alerts

- Alerts can be defined for
 - Creating users on sensitive systems
 - Role grants on sensitive systems
 - “DBA” grants on all systems
 - Failed logins for application users
 - Directly viewing sensitive columns
 -
- Add workflow for alerts
- Track alerts
- Drill down from the dashboard
- Send alerts to distribution lists

Alert Severity Summary

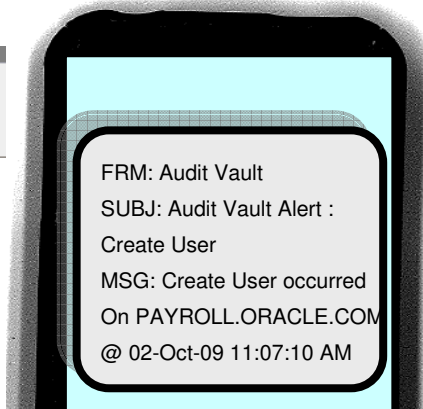
Alerts by severity, across all sources



Integration with Email / SMS / Remedy

Subject: Audit Vault Alert: Create_User2 : PAYROLL.ORACLE.VM
From: Audit Vault <noreply@oracle.com>
Date: 9:19 AM
To: tammv.bednar@oracle.com

Attribute	Value
Alert Name	Create_User2
Alert Time	02-OCT-09 04.17.09.667035 PM
Alert Status	NEW
Object	TAMMY
Alert Severity	Critical
Client Host	oel4upd4.oracle.vm
Client Host IP	
Event	CREATE USER
OS User Name	oracle
User Name	PJONES
Source Name	PAYROLL.ORACLE.VM
Description	Generate alert for create user
Trouble Ticket ID	
Trouble Ticket Time	
URL	http://oel4upd4.oracle.vm:5707/av/console/



Showing 1 - 192 of 192

Incident ID*	Summary*	Status*	Priority*	Priority W.	Last Name*	First Name*	Company*	Reported Date*
INC00000000170	TEST_ALERT8 fired for Source avsource on Object AE_ROLE1.AlertSta	Assigned	High	20	Allbrook	Allen	Calbro Services	10/1/2009 11:47:37 PM
INC00000000171	TEST_ALERT8 fired for Source avsource on Object AE_ROLE1.AlertSta	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 5:51:35 AM
INC00000000172	Create_User2:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:11 AM
INC00000000173	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:14 AM
INC00000000174	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:21 AM
INC00000000175	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:34 AM
INC00000000176	CreateUser:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:35 AM
INC00000000177	Create_User2:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 8:55:40 AM
INC00000000178	Create_User2:PAYROLL.ORACLE.VM	Assigned	High	20	Allbrook	Allen	Calbro Services	10/2/2009 9:19:07 AM

Report Select All DeSelect All Delete

Quick Actions: Assign to life, Auto Assign, Broadcast Incident, Categorizations, Customer's Incidents, Incident Matching

Identification and Recording Investigation and Diagnosis Resolution and Recovery Incident Closure Closed

Incident ID*: INC00000000176
 Company*: Calbro Services
 Customer*: Allbrook, Allen
 Contact*:
 Notes: http://oel4upd4.oracle.vm:5707/av/console/??p=7700:33::NO::P33_ALERT_
 Template+:
 Summary*: CreateUser:PAYROLL.ORACLE.VM

Work Detail Relationships Date/System
 1 entries returned - 1 entries matched

Type	Summary	File	Login ID	Submit Date
Customer Comr	CreateUser:PAYROLL.ORACLE		Demo	10/2/2009 8:55:35 AM

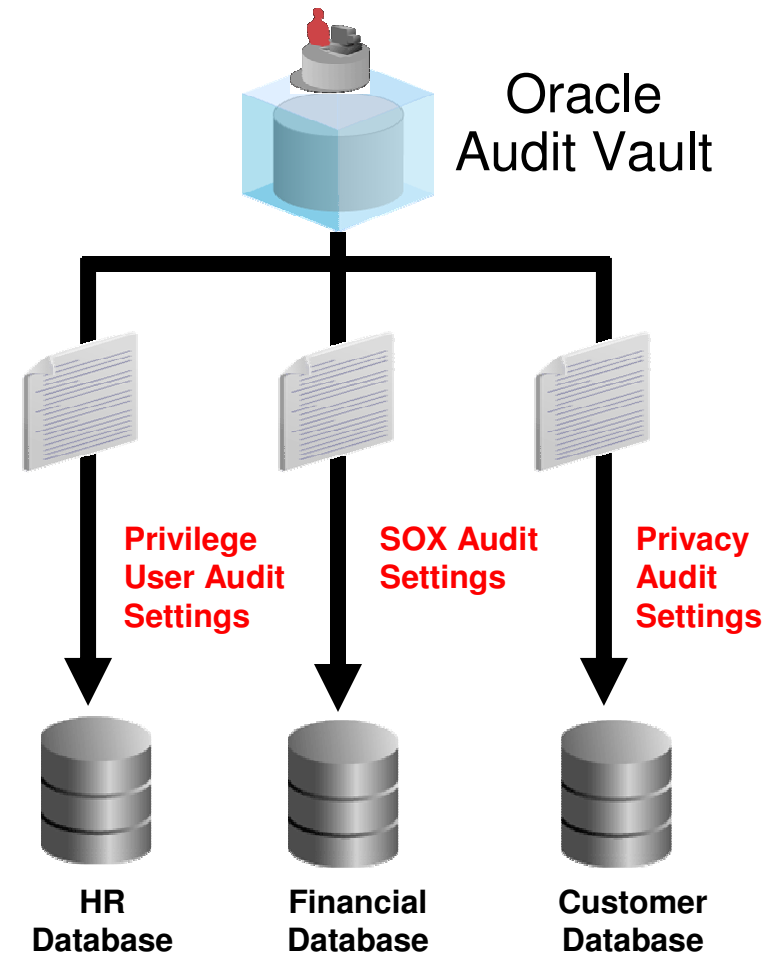
 View Create Report History

Assigned Group*: Backoffice Support
 Assignee*: Bob Baxter

Oracle Audit Vault Policies

Centralized Management of Audit Policies

- **Policy definition**
 - Named, centrally managed, collection of audit settings
- **Policy audit settings**
 - Settings can be extracted from an existing database with auditing
 - Manual entry supported
- **Policy provisioning**
 - Policies applied to databases from the Audit Vault console
- **Policy maintenance**
 - Compare and contrast approved policy with current settings



ORACLE



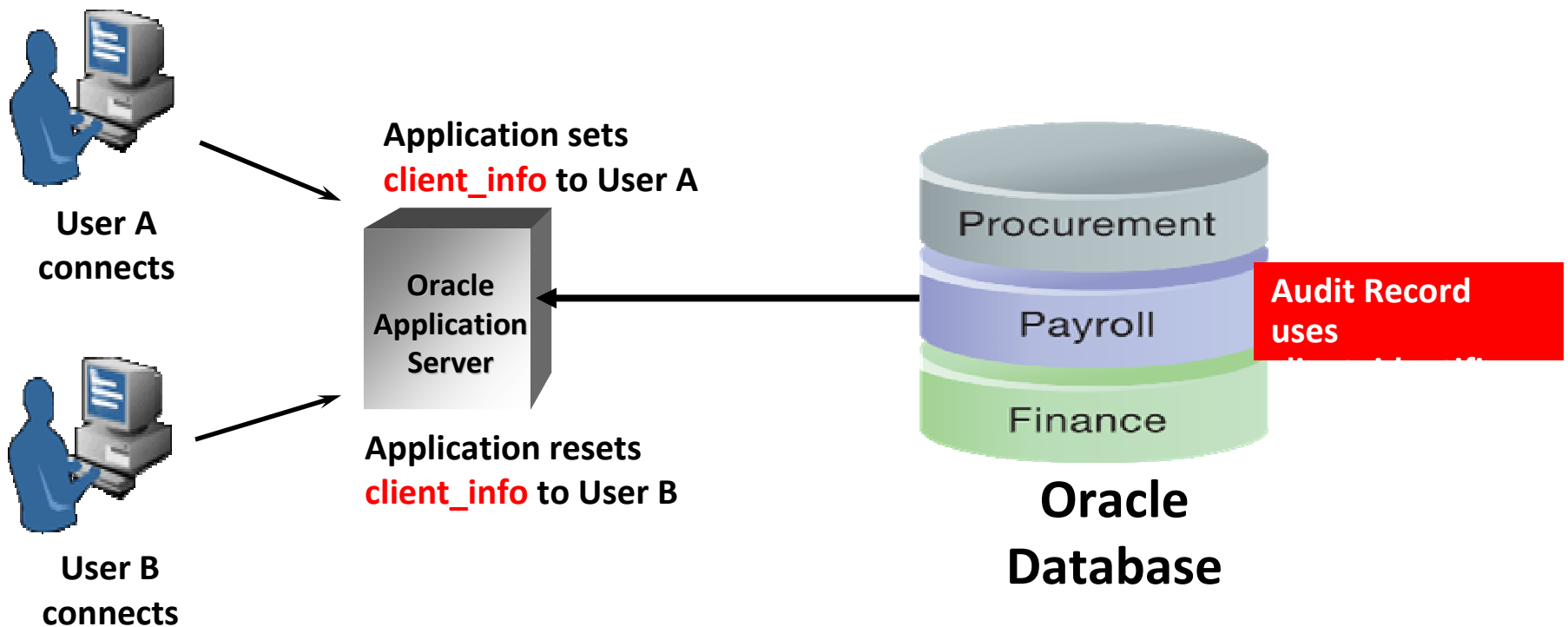
Oracle Audit Vault

Application Certification

- Applications are validated by Default
 - Database auditing is underneath the Application
- Application User Auditing
 - Application can set the database “Client Identifier” to tie application user with application shared account
- Database Auditing can be used to monitor
 - Audit base application tables and views
 - Privileged user operations in the database (logins, user/table create)

Setting Client Identifier

- Track the application user
- Any application running on Oracle database can set the client identifier





Oracle Audit Vault

Application Integration

1. Turn on database auditing
 - Set the database parameters → audit_trail, audit_trail_dest, audit_sys_operations
2. Determine the application tables to audit
 - audit *<table>* by access;
 - FGA audit policy
3. Configure Oracle Audit Vault to collect the database audit trail
4. Setup alerts in Audit Vault
5. View Reports

Oracle Audit Vault

PeopleSoft Application Integration

ORACLE Enterprise Manager 10g
Audit Vault

Default Reports | Compliance Reports | Custom Reports | Generated Reports | Report Schedules | Entitlement Snapshots

< Report View Exclude Null Values Displayed Column

Source	
Source Type	ORCLDB
Source	PSFT.US.ORACLE.COM
Host	halinux11.us.oracle.com
Version	11.1.0.7.0
IP Address	130.35.164.234
Event	
Audit Vault Time	10/12/2009 08:2:49 AM
Event Time	10/12/2009 08:2:31 AM
Event Status	0
Event	DELETE
Category	DATA ACCESS
Source Event	7
Target	
Owner	SYSADM
Target	PSROLEUSER
Client/User Information	
User	SYSADM
OS User	oracle
Host	halinux13
Client ID	PS
Statement	
SCN	35525822
Bind Variables	#1(8):HCRNZL #2(29):Training Budget Administrator
SQL Text	DELETE FROM PSROLEUSER_VW WHERE OPRID=:1 AND ROLENAME=:2
Statement ID	1339
Session	
Other	
Session ID	17520402
Transaction ID	07001500E5330000

All times are UTC-07:00

- Complete monitoring of who executed a transaction from application to database
- User is the database authenticated user
- OS User is operating system authenticated user
- Client ID is the application authenticated user that executed the command

ORACLE

Oracle Audit Vault

eBusiness Suite

ORACLE Enterprise Manager 10g
Audit Vault

Home

Default Reports Compliance Reports Custom Reports Generated Reports Report Schedules Entitlement Snapshots

Data Access

Rows

Event Time is in the last 24 hours

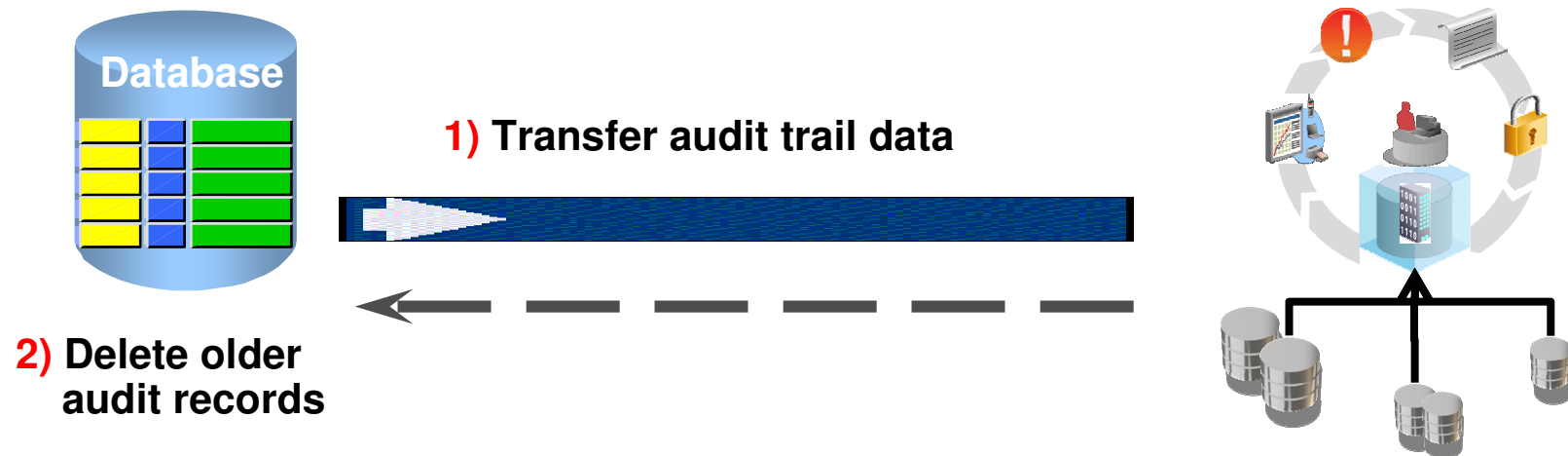
Source	Target	Event	Event Status	User	Client ID	
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	UPDATE	0	APPS	SYSADMIN	
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	UPDATE	0	APPS	SYSADMIN	
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	UPDATE	0	APPS	SYSADMIN	
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	INSERT	0	APPS	SYSADMIN	10/11/2009 11:8:38 PM
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	UPDATE	0	APPS	SYSADMIN	cosdev16.us.oracle.com 10/11/2009 10:59:59 PM
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	UPDATE	0	APPS	SYSADMIN	cosdev16.us.oracle.com 10/11/2009 10:59:36 PM
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	UPDATE	0	APPS	SYSADMIN	cosdev16.us.oracle.com 10/11/2009 10:55:54 PM
VIS1211.US.ORACLE.COM	WF_LOCAL_USER_ROLES	UPDATE	0	APPS	SYSADMIN	cosdev16.us.oracle.com 10/11/2009 10:55:52 PM
PAYROLL.ORACLE.VM	INVENTORIES	SELECT	0	APPS		oel4upd4.oracle.vm 10/11/2009 10:52:17 PM
PAYROLL.ORACLE.VM	INVENTORIES	SELECT	0	APPS	Paul Jones	oel4upd4.oracle.vm 10/11/2009 10:52:17 PM
PAYROLL.ORACLE.VM	CUSTOMERS	DELETE	UNKNOWN:FGA	OE		oel4upd4.oracle.vm 10/11/2009 10:52:17 PM
PAYROLL.ORACLE.VM	CUSTOMERS	INSERT	UNKNOWN:FGA	OE		oel4upd4.oracle.vm 10/11/2009 10:52:17 PM
PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	UNKNOWN:FGA	OE		oel4upd4.oracle.vm 10/11/2009 10:52:17 PM
PAYROLL.ORACLE.VM	ORDERS	UPDATE	UNKNOWN:FGA	OE		oel4upd4.oracle.vm 10/11/2009 10:52:17 PM
PAYROLL.ORACLE.VM	SALES	SELECT	UNKNOWN:FGA	PJONES		oel4upd4.oracle.vm 10/11/2009 10:52:9 PM

- Client ID is the application authenticated user that executed the command
- If client id is null, need to investigate that this is a connection directly to the database, not through application

Oracle Audit Vault

Audit Trail Clean-Up: DBMS_AUDIT_MGMT

- Automatically deletes audit trails from target after they are securely inserted into Audit Vault
- Reduces DBA manageability challenges with audit trails
- Supports audit trail cleanup for all databases



ORACLE®

What Do You Need To Audit?

Database Audit Requirements	SOX	PCI DSS	HIPAA/HITECH	Basel II	FISMA	GLBA
Accounts, Roles & GRANT changes	●	●	●	●	●	●
Failed Logins and other Exceptions	●	●	●	●	●	●
Privileged User Activity	●	●	●	●	●	●
Access to Sensitive Data (SELECTs...)		●	●	●	●	●
Data Changes (INSERT, UPDATE, ...)	●			●		
Schema Changes (DROP, ALTER...)	●	●	●	●	●	●

Auditing Resources

Impact on CPU performance

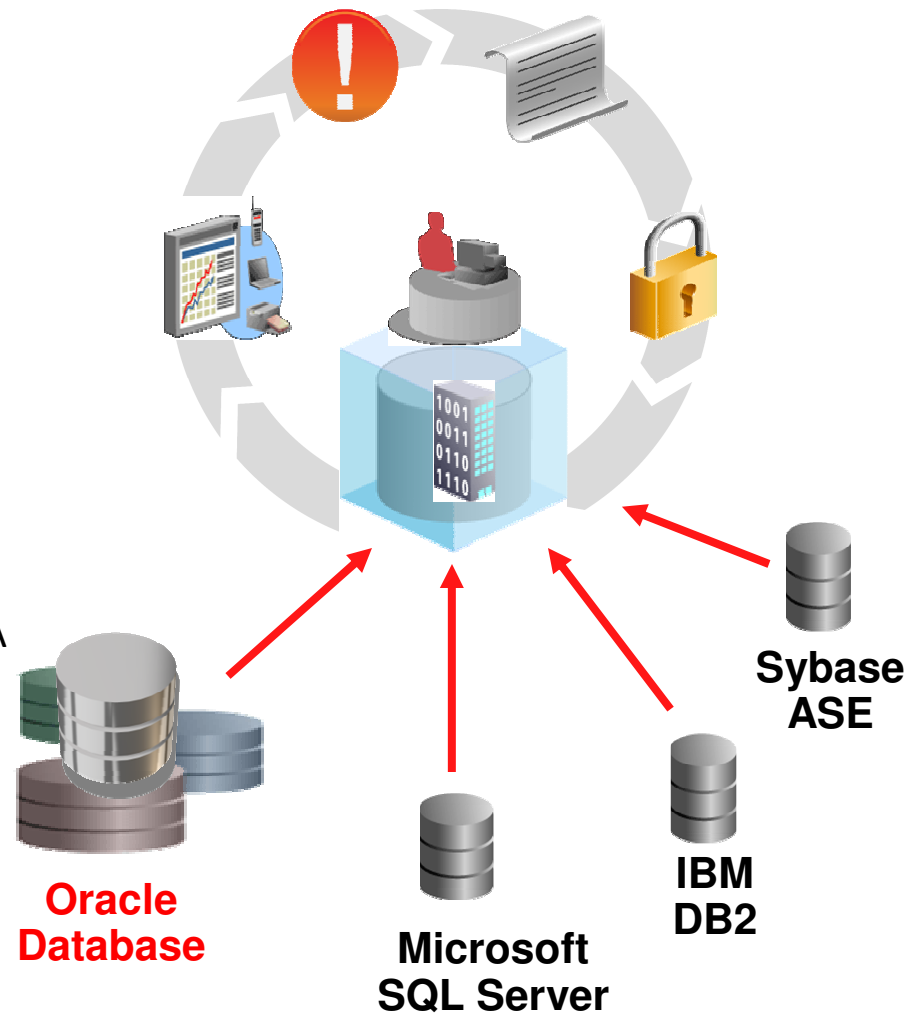
- Original workload CPU 1.08% for 10 audit/sec case
- Original workload CPU 1.56% for 100 audit/sec case

Audit Source	Database auditing / No Audit Vault	Audit Vault collection turned on	Database auditing / No Audit Vault	Audit Vault collection turned on
Audit Load	10 records / second	10 records / second	100 records / second	100 records / second
OS Log	0.08%	0.7%	0.15%	2.7%
DB Audit	0.13%	0.5%	1.6%	3.4%
Redo	0%	3.7%	0%	8.2%

Oracle Audit Vault 10.2.3.2

Summary

- **Consolidate and secure audit data**
 - Oracle 9i Release 2 and higher
 - SQL Server 2000, 2005, & 2008
 - IBM DB2 UDB 8.5 - 9.2
 - Sybase ASE 12.5.4 - 15.0.x
 - Secure and scalable
 - Cleanup of source Oracle audit data
- **Centralized reporting**
 - Compliance reports for PCI, SOX, & HIPAA
 - Entitlement Reports
 - PDF, Scheduling, & Attestation
- **Alert on security threats**
 - Integration with email & Remedy



ORACLE



For More Information

search.oracle.com

Search for: In the section: [Refine Search](#)

oracle.com/database/security



Q&A



ORACLE IS THE INFORMATION COMPANY