

ORACLE®

Oracle Audit Vault – Auditing Database Activity for Security and Compliance

Gary Huffman
Development Manager
Oracle OpenVMS Engineering Group



Agenda

- Overview
- What do you need to audit for compliance
- Audit Vault Deployment
- Audit Vault Reporting
- Questions and answers
- Oracle Audit Vault Demo



What we heard from customers...

- “We have Oracle database auditing turned on some of our databases but we’re not looking at the audit data.”
- “Audit data is taking up to much space on our production servers.”
- “To comply with SOX and HIPAA, we need to produce time consuming monthly reports for our auditors.”
- “We want to self-assess on a continuous basis to ensure we are in compliance before our auditors show up.”
- “We are worried about the security of our Microsoft SQL Server databases since we can’t lock down the OS.”

What Do You Need To Audit?

Database Audit Requirements	SOX	PCI DSS	HIPAA	Basel II	FISMA	GLBA
Accounts, Roles & Permissions Do you have visibility of GRANT and REVOKE activities?	•	•	•	•	•	•
Failed Logins Do you have visibility of failed logins and other exception activities?	•	•	•	•	•	•
Privileged User Activity Do you have visibility of users activities?	•	•	•	•	•	•
Access to Sensitive Data Can you have visibility into what information is being queried (SELECTs)?		•	•	•	•	•
Schema Changes Are you aware of CREATE, DROP and ALTER Commands that are occurring on identified Tables / Columns?	•	•	•	•	•	•
Data Changes Do you have visibility into Insert, Update, Merge, Delete commands?	•			•		

Oracle Audit Vault

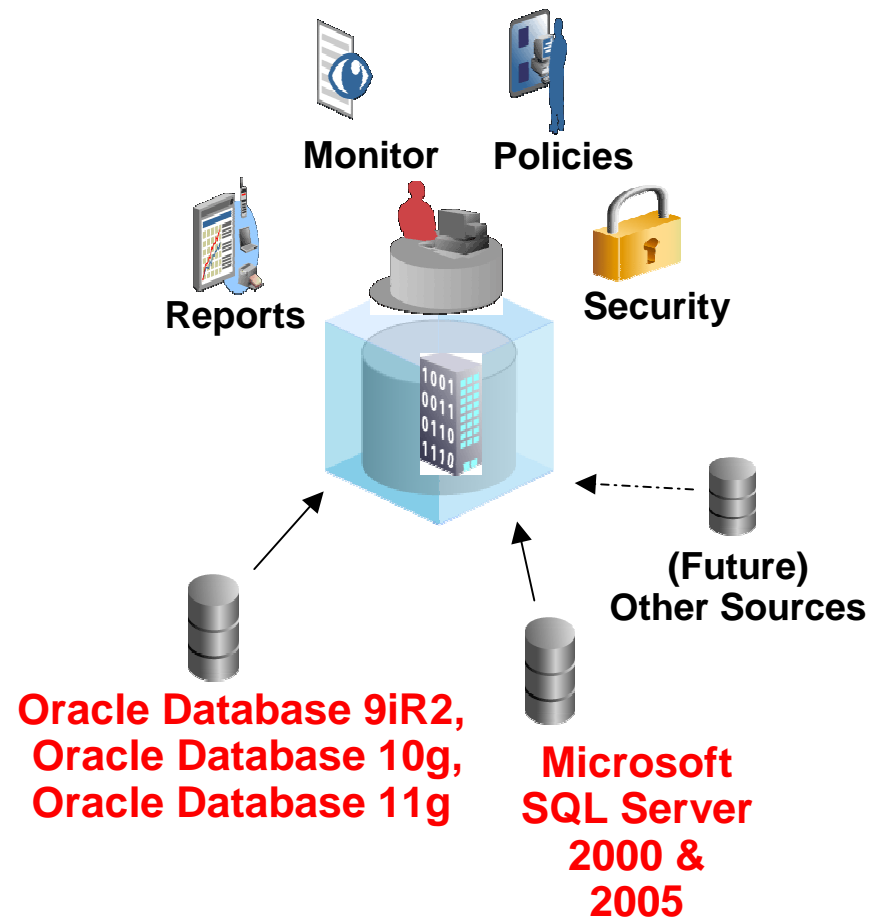
Overview

**Consolidate and Secure
Audit Data**

**Simplify Compliance
Reporting**

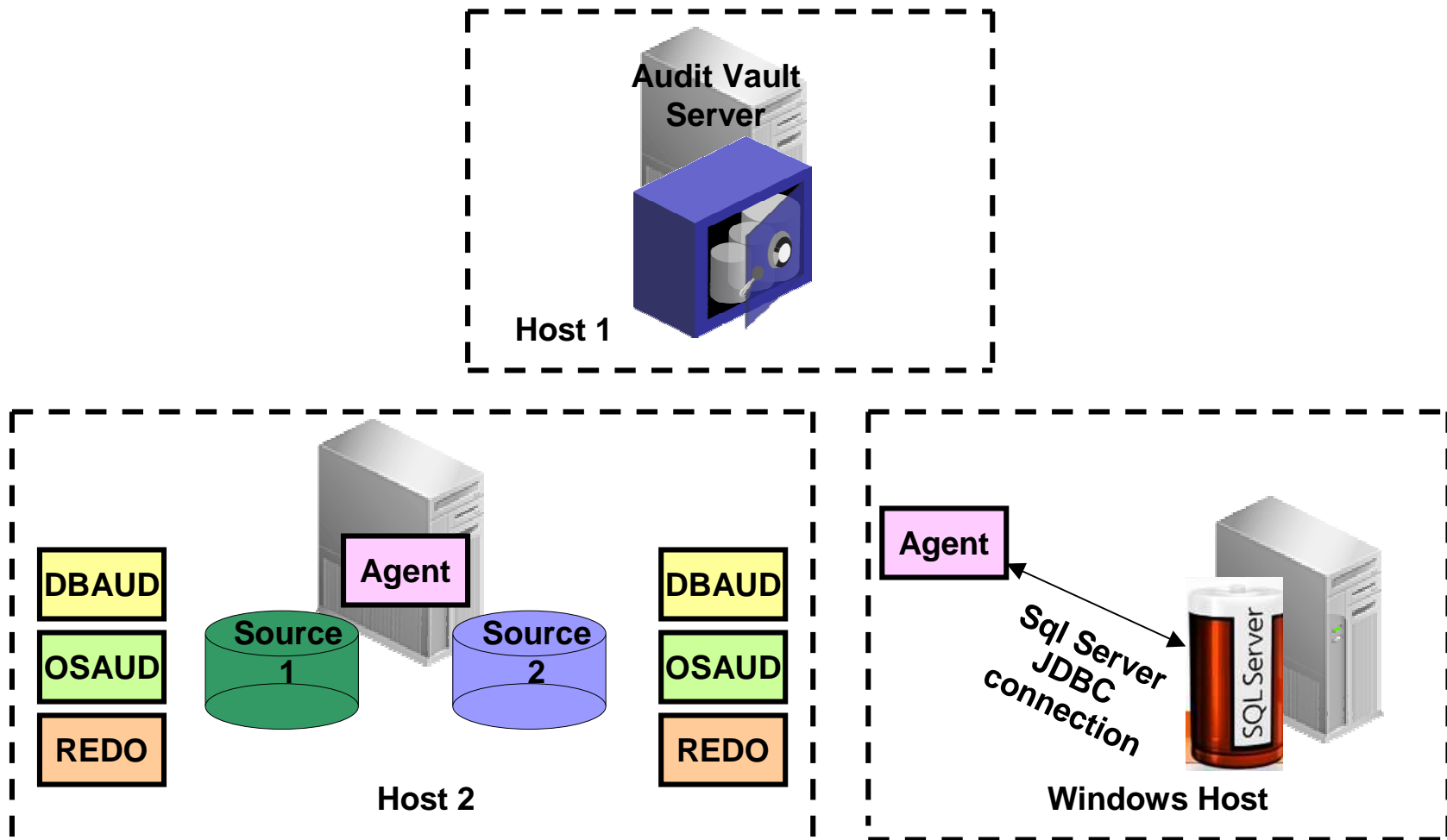
**Alert on Security
Threats**

**Lower IT Costs With
Audit Policies**



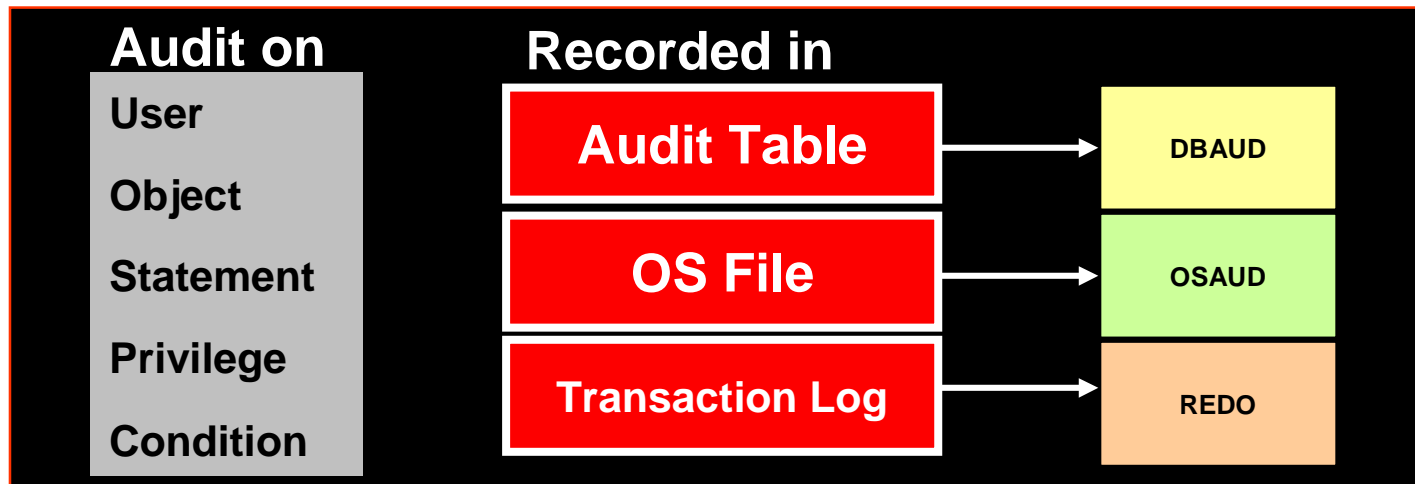
ORACLE

Deploying Audit Vault



ORACLE

Auditing in the Oracle Database & Audit Vault Collectors



- DBAUD: Retrieves audit records from database audit tables
- OSAUD: Retrieves audit records from the OS audit file
- REDO: Uses Oracle LogMiner and Streams to retrieve logical change records (LCRs) from the redo log files



Oracle Audit Vault 10.2.3

Collector's

- Microsoft SQL server
- Sybase
- DB2
- Oracle 9i, 10g, 11g
- Oracle Database on OpenVMS 10gR2
- Planned – Oracle RDB

Oracle Audit Vault Reporting

ORACLE Enterprise Manager 10g
Audit Vault

Home Audit Reports Audit Policy Audit Status

Default Reports Custom Reports

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](#)

Compliance Reports

-  [Account and Role Changes](#)
- [Account and Role Changes - Blocked](#)
- [Audit Setting Changes](#)
- [Data Changes](#)
- [Login Failures](#)
- [Login/Logoff](#)
- [Object Access](#)
- [Structure Changes](#)
- [System Events](#)



Alert Reports

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
















- Built-in customizable compliance reports
 - Privileged user activity, role grants
 - DDL activity
- User defined reports
 - What privileged users did on the financial database?
 - What user 'A' did across multiple databases?

Consolidated Enterprise Reporting

Activity Overview

 Rows 

+  2

	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	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 17:13:28
	HR.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 17:13:19
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 16:19:35
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 16:19:25
	HR.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 17:13:28
	HR.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 17:13:19
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 16:19:35
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	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

- Audit data normalized for consolidated reporting

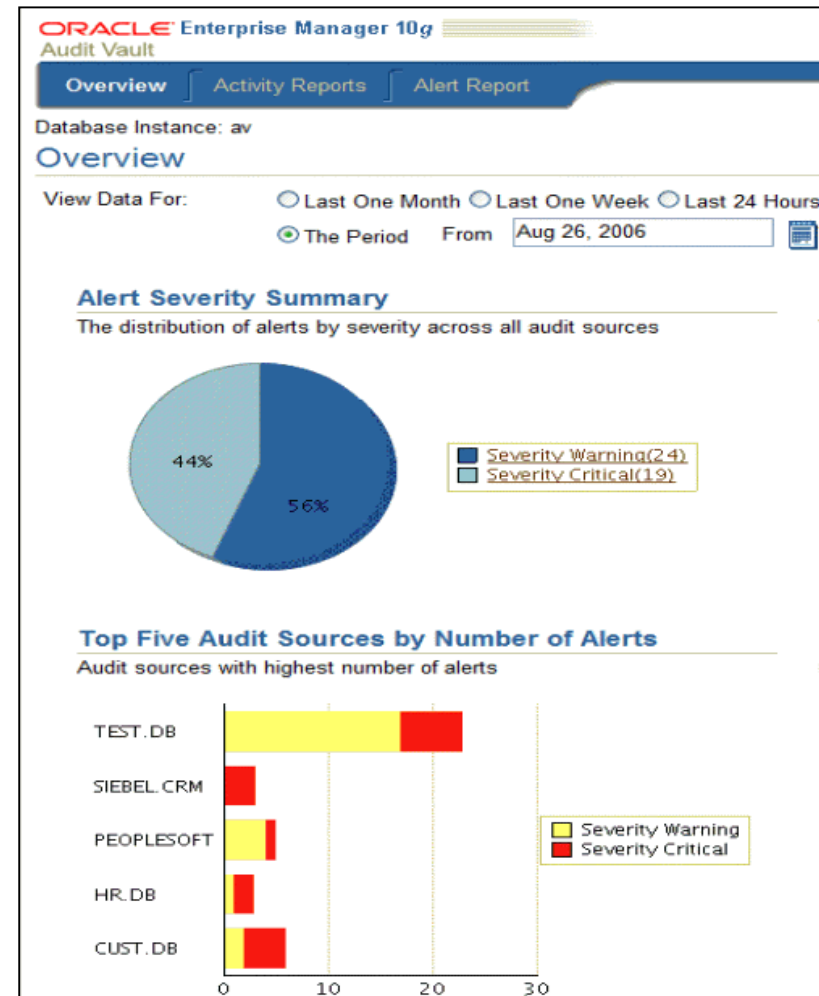
Oracle Audit Vault Report Customization

- Data filtering
- Record highlighting using condition values
- Charting with simple graphics
- Custom reports can be saved and shared

Object	Event	User	Source	Host	Event Time	SQL Text
OE.CUSTOMER_PAYMENT	SELECT	OE	PAYROLL.ORACLE.VM	oel4upd4.oracle.vm	05-FEB-08 09:48:24	select payment_card_numbr customer_payment
OE.CUSTOMER_PAYMENT	SELECT	VSHAH	PAYROLL.ORACLE.VM	oel4upd4.oracle.vm	05-FEB-08 09:48:24	select payment_code_id fro oe.customer_payment
OE.CUSTOMER_PAYMENT	SELECT	VSHAH	PAYROLL.ORACLE.VM	oel4upd4.oracle.vm	05-FEB-08 09:48:24	select payment_card_numbr oe.customer_payment
OE.CUSTOMER_PAYMENT	SELECT	VSHAH	PAYROLL.ORACLE.VM	oel4upd4.oracle.vm	05-FEB-08 09:48:24	select payment_expiration t oe.customer_payment
OE.ORDERS	UPDATE	VSHAH	PAYROLL.ORACLE.VM	oel4upd4.oracle.vm	05-FEB-08 09:48:10	
OE.ORDERS	SELECT	VSHAH	PAYROLL.ORACLE.VM	oel4upd4.oracle.vm	05-FEB-08 09:48:10	select order_total from oe.o

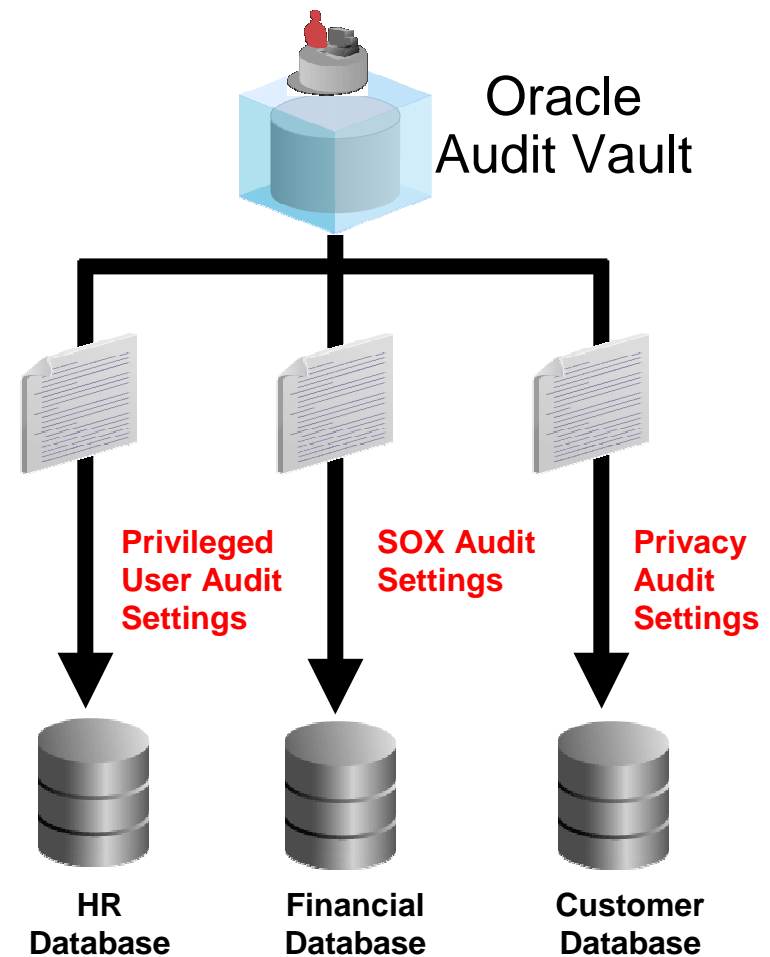
Oracle Audit Vault Alerts

- Efficient scanning
 - Inbound audit data scanning
- Alerts can be defined for
 - Direct views of sensitive columns
 - New users on sensitive systems
 - Role grants on sensitive systems
 - “DBA” grants on all systems
 - Failed logins
 - Enterprise-defined security policies



Oracle Audit Vault Policy Management

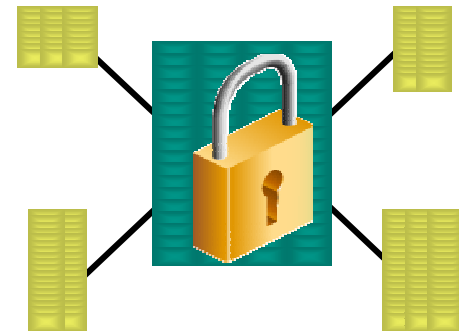
- Policy Definition
 - Named, centrally managed, collection of audit settings
 - SOX, HIPAA, PCI
 - Settings can be extracted from any database with auditing configured
- Policy Provisioning
 - Policy audit settings can be applied to databases from the central Audit Vault console
- Policy maintenance
 - Compare and contrast approved policy with current settings
 - Detect and correct policy exceptions



Oracle Audit Vault Data Warehouse

Secure, Scalable & Flexible Warehouse

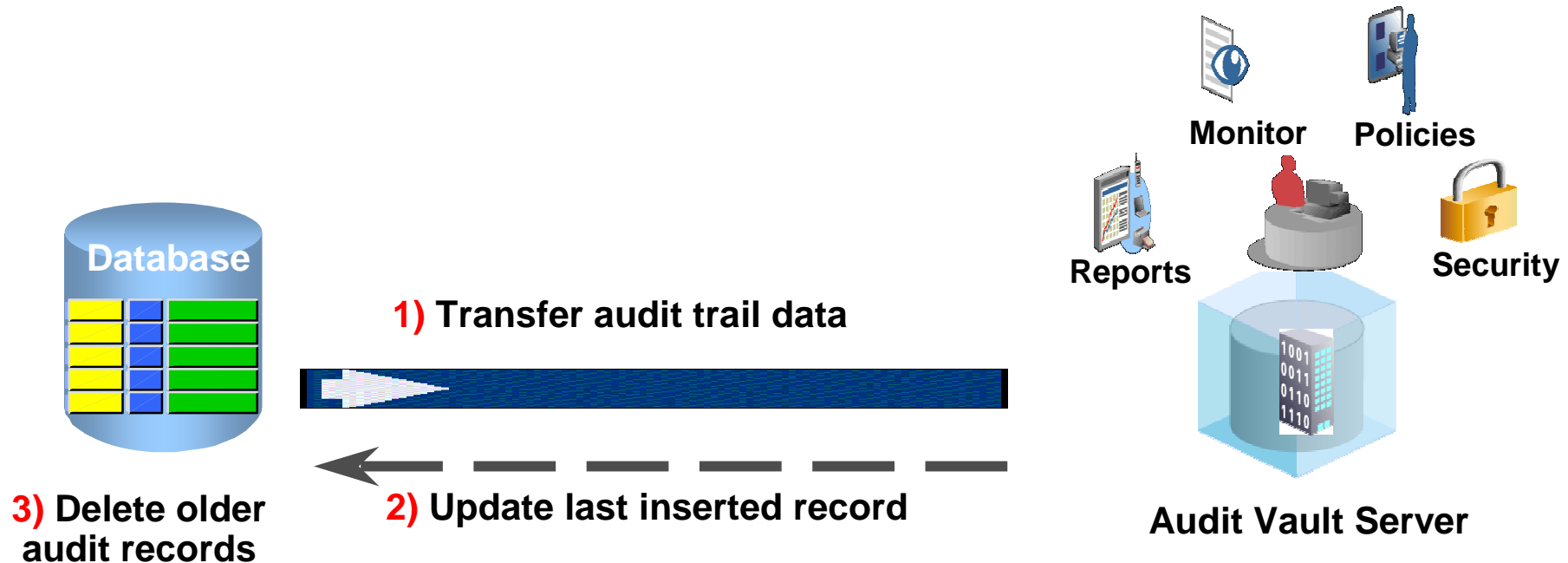
- Audit Warehouse
 - Enable business intelligence and analysis
 - Enable reporting
- Performance and Scalability
 - Built-in partitioning
 - Scales to Terabytes
 - Certified with Oracle RAC
- Protected with Built-in Security
 - Encrypted audit data transmission
 - Separation of Duty
 - Audit Vault Administrator
 - Audit Vault Auditor



Oracle Audit Vault

Audit Trail Clean-Up Integration

- Integrated with new DBMS_AUDIT_MGMT package to automatically delete audit trail records after they have been inserted into Audit Vault.



Auditing Resources

Additional CPU

- 10 audit/sec workload CPU measured 1.08%
- 100 audit/sec workload CPU measured 1.56%

	Database auditing / No Audit Vault	Audit Vault collection turned on	Database auditing / No Audit Vault	Audit Vault collection turned on
Audit Load / Audit Source	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

*Internal testing: Source: 4x32GB 3GHz Intel Xeons RHEL3.0, running 2 Oracle Database 10.2.0.3.0
© 2008 Oracle Corporation

AV Server: 2x6GB 3GHz Intel Xeons RHEL3.0, AV Server 10.2.2.0.0



Oracle Audit Vault

Strengths

Scalable repository	Leverages massive scalability features of the Oracle Database, including Oracle Partitioning. Certified with Oracle RAC. Data Guard certification planned
Reporting	Latest release uses widely popular Oracle Application Express reporting feature. Open warehouse design so any reporting tool, including Oracle BI Publisher can access
Security	Leverages Oracle's industry leading security features to protect audit data in-transit and at-rest
Heterogeneous database support	SQL Server 2000/2005 supported. SQL Server 2008 (TBD), DB2, Sybase and RDB already well underway
Easy uptake for existing customers	Customers already using native Oracle Database auditing will achieve faster results versus deploying new auditing technology
Support for other sources	Operating system specific audit data most requested enhancement after databases. OS audit support is planned for next major release



How does Audit Vault Detect Malicious Activity?

- Audit sensitive tables on source databases
- Setup Audit Vault alerts to provide near-real-time updates to policy violations
- View alert reports and optionally setup email to be sent to security team when alert is triggered
- View specific sql executed by users
- View the before/after values
- Create customized reports to highlight sensitive table access
- Take action!



D E M O N S T R A T I O N



Oracle Audit Vault

Login to Audit Vault

* User Name	<input type="text" value="avauditor"/>
* Password	<input type="password" value="*****"/>
Connect As	<input type="text" value="AV_AUDITOR"/> ▼

Login

Database Instance: av.oracle.vm

Logged in As AVAUDITOR

Overview

Page Refreshed Aug 4, 2008 3:29:32 PM UTC

Refresh

View Data For:

Automatically Refresh (60 sec)

View Data For:

☐ Last One Month ☐ Last One Week ☒ Last 24 Hours

☐ The Period

From

Aug 3, 2008

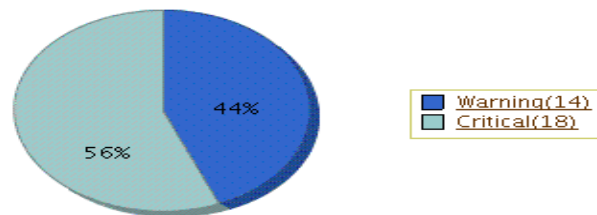
To

Aug 4, 2008

Go

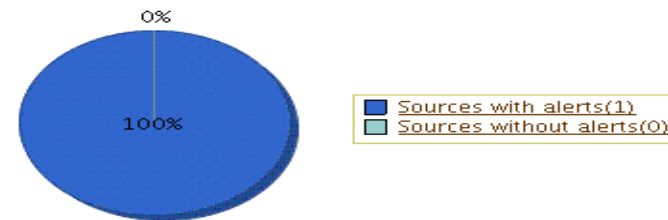
Alert Severity Summary

The distribution of alerts by severity across all audit sources



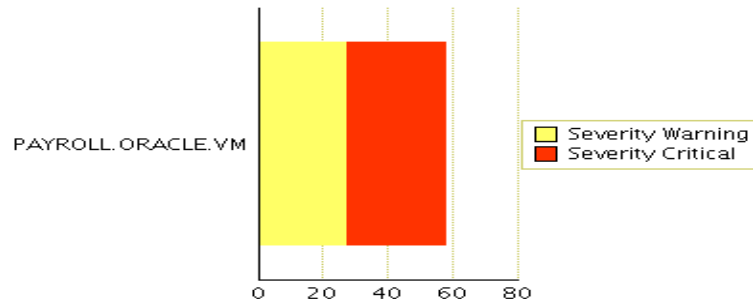
Summary of Alert Activity

The distribution of alert activity by audit source



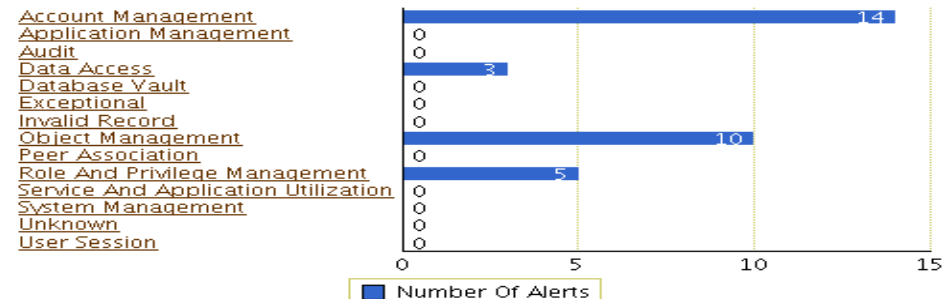
Top Five Audit Sources by Number of Alerts

Audit sources with highest number of alerts



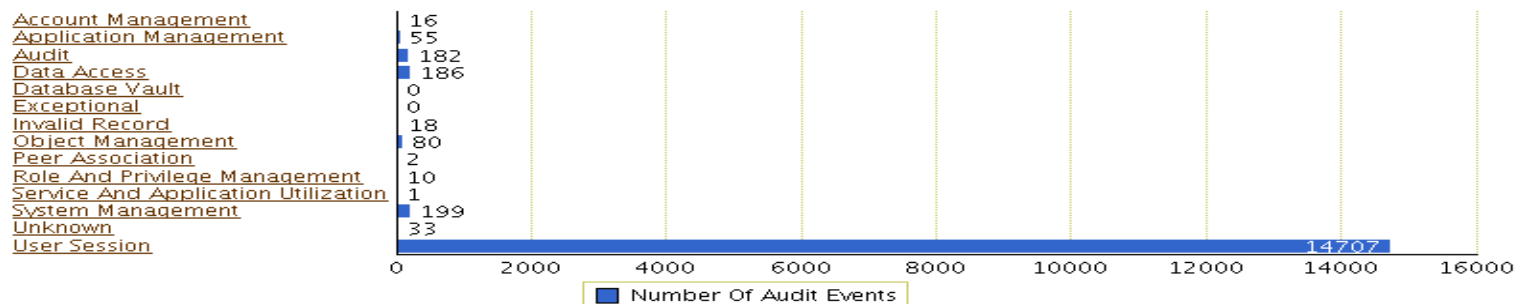
Alerts by Audit Event Category

Displays number of alerts by audit event category



Activity by Audit Event Category

Activity by audit event category



Default Reports

Custom Reports

Access Reports



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

Compliance Reports



- [Account and Role Changes](#)
- [Account and Role Changes - Blocked](#)
- [Audit Setting Changes](#)
- [Data Changes](#)
- [Login Failures](#)
- [Login/Logoff](#)
- [Object Access](#)
- [Structure Changes](#)
- [System Events](#)

Alert Reports



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

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](#)



All Alerts

 Rows 

















- ☐  Audit Vault Alert Time is in the last 24 hours ☒ 
-  Event Category = 'DATA ACCESS' ☒ 

	Alert Name	Object	Event	Event Category	User	Source	Alert Severity	Audit Vault Alert Time 
	Customers_table_is_accessed	CUSTOMERS	UPDATE	DATA ACCESS	JTAYLOR	PAYROLL.ORACLE.VM	Critical	04-AUG-2008 09:29:39
	Customers_table_is_accessed	CUSTOMERS	UPDATE	DATA ACCESS	JTAYLOR	PAYROLL.ORACLE.VM	Critical	04-AUG-2008 09:29:39
	Customers_table_is_accessed	CUSTOMERS	UPDATE	DATA ACCESS	JTAYLOR	PAYROLL.ORACLE.VM	Critical	04-AUG-2008 09:29:19
	Customers_table_is_accessed	CUSTOMERS	SELECT	DATA ACCESS	JTAYLOR	PAYROLL.ORACLE.VM	Critical	04-AUG-2008 09:29:03
	Customers_table_is_accessed	CUSTOMERS	SELECT	DATA ACCESS	JTAYLOR	PAYROLL.ORACLE.VM	Critical	04-AUG-2008 09:28:31



Activity Overview

 Rows 

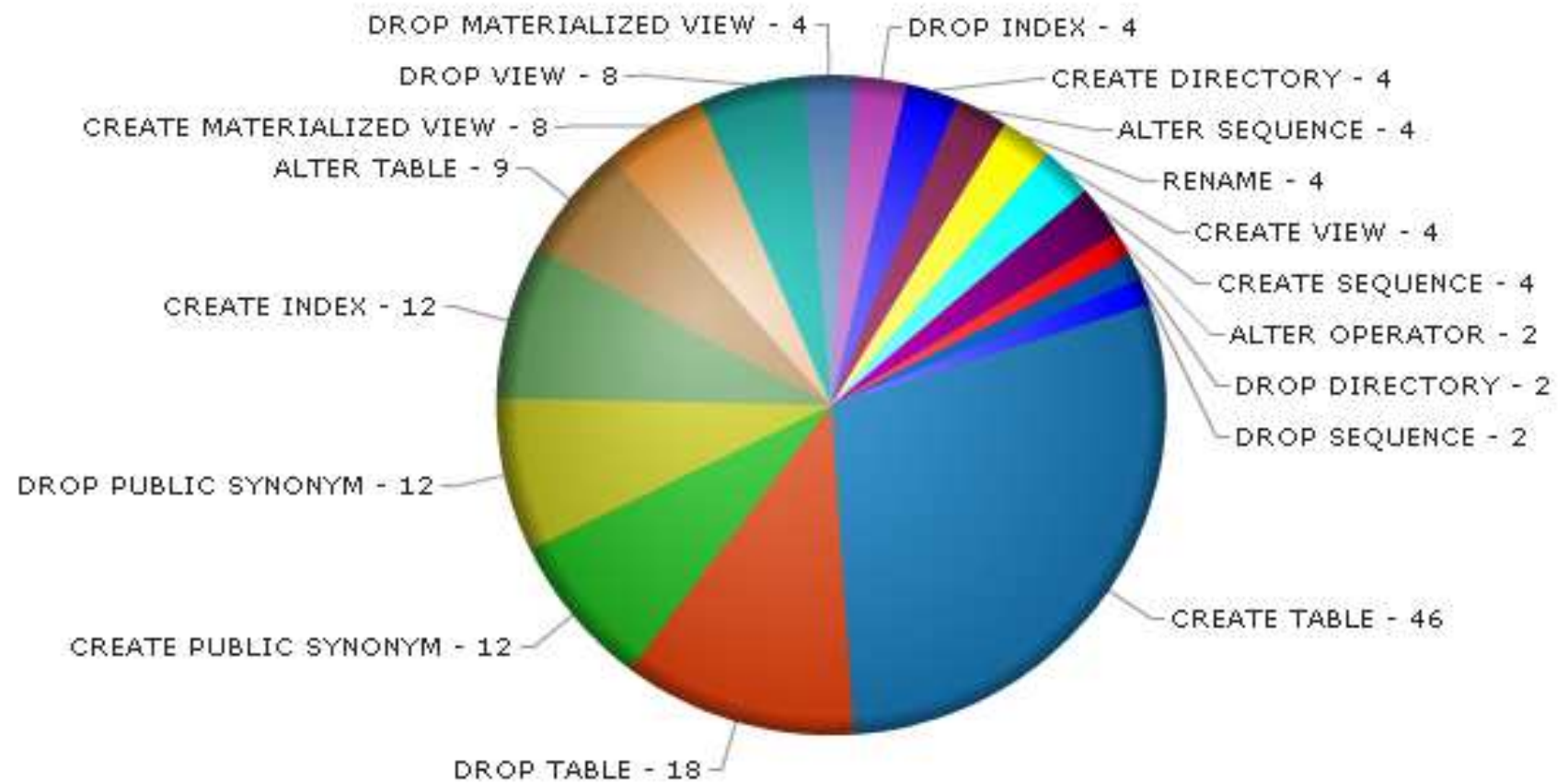
+  2

	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	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 17:13:28
	HR.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 17:13:19
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 16:19:35
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	VW_TAB	oel4upd4.oracle.vm	10-JUN-08 16:19:25
	HR.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 17:13:28
	HR.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 17:13:19
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCHAFER	VW_TAB1	oel4upd4.oracle.vm	10-JUN-08 16:19:35
	PAYROLL.ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCHAFER	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



Activity Overview



 Rows 

















 3 [Edit Chart](#) [View Report](#)




Data Access

 Rows 

☐  Event Time is in the last 24 hours ☒ 

	Source	Target	Event	Event Status	User	Host	Event Time 
	PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:29:15
	PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:29:15
	PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:29:15
	PAYROLL.ORACLE.VM	CUSTOMERS	SELECT	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:28:40
	PAYROLL.ORACLE.VM	CUSTOMERS	SELECT	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:28:10
	PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	0	AVSRCUSR	oel4upd4.oracle.vm	04-AUG-08 02:41:01
	PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	0	AVSRCUSR	oel4upd4.oracle.vm	04-AUG-08 02:41:00
	PAYROLL.ORACLE.VM	CUSTOMERS	UPDATE	0	AVSRCUSR	oel4upd4.oracle.vm	04-AUG-08 02:41:00
	PAYROLL.ORACLE.VM	ORDERS	UPDATE	0	OE	oel4upd4.oracle.vm	04-AUG-08 02:27:16
	PAYROLL.ORACLE.VM	ORDERS	UPDATE	0	OE	oel4upd4.oracle.vm	04-AUG-08 02:10:38
	PAYROLL.ORACLE.VM	ORDERS	UPDATE	0	OE	oel4upd4.oracle.vm	04-AUG-08 01:47:17
	PAYROLL.ORACLE.VM	LBAC\$USER	DELETE	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 01:46:59
	PAYROLL.ORACLE.VM	LBAC\$USER	DELETE	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 01:46:59
	PAYROLL.ORACLE.VM	LBAC\$POLT	DELETE	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 01:46:58
	PAYROLL.ORACLE.VM	EMP1	INSERT	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 01:46:50

1 - 15 

Default Reports

Custom Reports

< Report View

☒ Exclude Null Values ☐ Displayed Column

Source

Source Type ORCLDB
Source PAYROLL.Oracle.VM
Host oel4upd4.oracle.vm
Version 10.2.0.3.0
IP Address 192.168.203.31

Event

Audit Vault Time 04-AUG-08 09:29:39
Event Time 04-AUG-08 09:29:15
Event Status 0
Event UPDATE
Category DATA ACCESS
Source Event 6

Target

Owner OE
Target CUSTOMERS

Client/User Information

User JTAYLOR
OS User oracle
Host oel4upd4.oracle.vm
Terminal pts/3

Statement

SCN 810448
SQL Text update oe.customers set income_level = '500,000 - 750,000' where customer_id = 214
Statement ID 10



Session



Other







Session ID 30363
Transaction ID 0100080052010000
Priv Name 47



Data Changes


 Rows 


☒  Event Time is in the last 24 hours ☒ 

Source	Target	Event	Event Status	User	Host	Event Time	Data Trace Values			
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:29:15	Column	Old Value	New Value
								INCOME_LEVEL	F: 110,000 - 129,999	500,000 - 750,000
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	0	AVSRCUSR	oel4upd4.oracle.vm	04-AUG-08 02:41:01	Column	Old Value	New Value
								SSN		123456789
	PAYROLL.Oracle.VM	ORDERS	UPDATE	0	OE	oel4upd4.oracle.vm	04-AUG-08 02:27:16	Column	Old Value	New Value
								ORDER_TOTAL	264193.65	396290.48
	PAYROLL.Oracle.VM	ORDERS	UPDATE	0	OE	oel4upd4.oracle.vm	04-AUG-08 02:10:38	Column	Old Value	New Value
								ORDER_TOTAL	176129.1	264193.65
	PAYROLL.Oracle.VM	ORDERS	UPDATE	0	OE	oel4upd4.oracle.vm	04-AUG-08 01:47:17	Column	Old Value	New Value
								ORDER_TOTAL	117419.4	176129.1
	PAYROLL.Oracle.VM	EMP2	INSERT	0	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 01:48:50	Column	Old Value	New Value
								EMPNO		7902
								ENAME		FORD
								JOB		ANALYST

Default Reports

Custom Reports



 Rows 

Tasks

◇ [Manage Categories](#)

<u>Category</u>	<u>Application User</u>	<u>Report Name</u>	<u>Description</u>
-- Unassigned --	AVAUDITOR	Customers Table Highlight	Report to display data access and highlight Customer Table operations

1 - 1

Customers Table Highlight

 Rows

1 1 2

	Source	Target	Event	User	Host	Event Time	Program Name	SQL Text
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:29:15		update oe.customers set income_level = '500,000 - 750,000' where customer_id = 214
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:29:15		update oe.customers set income_level = '500,000 - 750,000' where customer_id = 214
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:29:15	sqlplus@oel4upd4.oracle.vm	
	PAYROLL.Oracle.VM	CUSTOMERS	SELECT	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:28:40		select * from oe.customers where customer_id = 214
	PAYROLL.Oracle.VM	CUSTOMERS	SELECT	JTAYLOR	oel4upd4.oracle.vm	04-AUG-08 09:28:10		select * from oe.customers
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	AVSRCUSR	oel4upd4.oracle.vm	04-AUG-08 02:41:01	sqlplus@oel4upd4.oracle.vm	
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	AVSRCUSR	oel4upd4.oracle.vm	04-AUG-08 02:41:00		update oe.customers set ssn = 123456789 where customer_id = 213
	PAYROLL.Oracle.VM	CUSTOMERS	UPDATE	AVSRCUSR	oel4upd4.oracle.vm	04-AUG-08 02:41:00		update oe.customers set ssn = 123456789 where customer_id = 213
	PAYROLL.Oracle.VM	ORDERS	UPDATE	OE	oel4upd4.oracle.vm	04-AUG-08 02:27:16	sqlplus@oel4upd4.oracle.vm	

04-AUG-08

Database Instance: [av.oracle.vm](#) > [Audit Settings](#)

Logged in As AVAUDITOR

Audit Settings

Audit Source



Go

[Retrieve from Source](#)

Select	Audit Source	In Use	Needed	Problem	Audit Trail	Audit Sys	Last Retrieved	Last Provisioned
	PAYROLL.Oracle.VM	2202	2203	15	DB, EXTENDED	TRUE	Aug 4, 2008 3:42:41 PM UTC	Aug 4, 2008 8:13:21 AM UTC

[Home](#) | [Audit Reports](#) | [Audit Policy](#) | [Audit Status](#) | [Help](#) | [Logout](#)

Copyright © 1996, 2008, Oracle. All rights reserved. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Unauthorized access is strictly prohibited.

Database Instance: [av.oracle.vm](#) > [Audit Settings](#) > PAYROLL.Oracle.VM

Logged in As AVAUDITOR

PAYROLL.Oracle.VM

Overview [Statement](#) [Object](#) [Privilege](#) [FGA](#) [Capture Rule](#)

Save Audit Settings

You can save your work by clicking on the Save All Audit Settings button below. Please note, saving your work does not automatically apply these settings to the source database

[Save All Audit Settings](#)

Apply Audit Settings

You can verify that the audit settings can be successfully applied to a given source by clicking on Verify. If the DBA for the source has provided you an account on the source, you can directly apply the audit settings you need using the Provision button. If you do not have such an account, you can export your changes to a SQL script that you can give the DBA, who can then apply the settings for you.

[Select All](#) | [Select None](#)

Select	Audit Settings Type	In Use	Needed	Problem
<input checked="" type="checkbox"/>	Statement	104	104	0
<input checked="" type="checkbox"/>	Object	1834	1832	2
<input checked="" type="checkbox"/>	Privilege	251	257	6
<input checked="" type="checkbox"/>	FGA	5	4	1
<input checked="" type="checkbox"/>	Capture Rule	8	6	0

[Verify](#)

[Export as SQL](#)

* Audit Source User Name

* Audit Source Password

[Provision](#)

Copy Audit Settings from Another Source

You can quickly replicate audit settings from one database to the source database to seed it with common audit settings. You either can use settings that are already in use in the database or settings that you have created in Audit Vault but not yet applied to that database.

Copy ☐ Actual (In Use) ☒ Needed (Not Yet In Use) Audit Settings

From [Load](#)

Overview [Statement](#) [Object](#) [Privilege](#) [FGA](#) [Capture Rule](#)

Database Instance: av.oracle.vm > [Audit Settings](#) > PAYROLL.Oracle.VM

Logged in As AVAUDITOR

PAYROLL.Oracle.VM

[Overview](#) [Statement](#) **[Object](#)** [Privilege](#) [FGA](#) [Capture Rule](#)

Mark All as Needed

Create

Previous 1-25 of 1836 Next 25

	Statement	Schema ▾	Object	Execution Condition	Audit granularity	In Use	Needed	
	ALTER	SCOTT	EMP	Both	BY ACCESS	↑	✓	
	UPDATE	OE	CUSTOMERS	Both	BY ACCESS	↑	✓	
	SELECT	OE	CUSTOMERS	Both	BY ACCESS	↑	✓	
	INSERT	OE	CUSTOMERS	Both	BY ACCESS	↑	✓	
	DELETE	OE	CUSTOMERS	Both	BY ACCESS	↑	✓	
	AUDIT	LBACSYS	LBAC_LABEL	Both	BY ACCESS	↑	✓	
	ALTER	LBACSYS	LBAC_LABEL	Both	BY ACCESS	↑	✓	
	GRANT	LBACSYS	LBAC_LABEL	Both	BY ACCESS	↑	✓	
	EXECUTE	LBACSYS	LBAC_LABEL	WHENEVER NOT SUCCESSFUL	BY ACCESS	↑	✓	
	AUDIT	LBACSYS	LBAC_BIN_LABEL	Both	BY ACCESS	↑	✓	
	ALTER	LBACSYS	LBAC_BIN_LABEL	Both	BY ACCESS	↑	✓	
	GRANT	LBACSYS	LBAC_BIN_LABEL	Both	BY ACCESS	↑	✓	
	EXECUTE	LBACSYS	LBAC_BIN_LABEL	WHENEVER NOT SUCCESSFUL	BY ACCESS	↑	✓	

Database Instance: av.oracle.vm > [Audit Settings](#) > PAYROLL.Oracle.VM

Logged in As AVAUDITOR

PAYROLL.Oracle.VM

[Overview](#) [Statement](#) [Object](#) [Privilege](#) [FGA](#) [Capture Rule](#)

Mark All as Needed

Create

	Rule Type	Schema	Table	DDL	DML	In Use	Needed	
	Schema	SCOTT		Yes	No	↑	✓	
	Schema	SCOTT		No	Yes	↑	✓	
	Table	SH	SALES	Yes	No	↑	✓	
	Table	OE	ORDERS	No	Yes	↑	✓	
	Table	OE	ORDERS	Yes	No	↑	✓	
	Table	SH	SALES	No	Yes	↑	✓	
	Table	OE	CUSTOMERS	No	Yes	↑	✓	
	Table	OE	CUSTOMERS	Yes	No	↑	✓	

[Overview](#) [Statement](#) [Object](#) [Privilege](#) [FGA](#) [Capture Rule](#)

Database Instance: [av.oracle.vm](#) > Alerts

Logged in As AVAUDITOR

Audit Alerts

Audit Source Type



Audit Source



Audit Event Category

[Go](#)[Create](#)

Alert Name	Description	Audit Source	Audit Source Type	Audit Event Category	Remove
ACCESSSS EMP PHONE	Raised when a SELECT is issued for the PHONE_NUMBER column in HR.EMPLOYEES table		ORCLDB	DATA ACCESS	
CreateUser	Alert that is raised when a user is created		ORCLDB	ACCOUNT MANAGEMENT	
CustomerSSN	Raised when a SSN is selected		ORCLDB	DATA ACCESS	
Customers table is accessed	Raise alert when oe.customers tables is accessed		ORCLDB	DATA ACCESS	
DropTable	Alert if a drop table operation is issue.		ORCLDB	OBJECT MANAGEMENT	
GrantPrivs	Alert if a privilege is granted.		ORCLDB	ROLE AND PRIVILEGE MANAGEMENT	
NonAppOrder	Alert if a user other than APPs updates the Order table.		ORCLDB	DATA ACCESS	
Select on Employees	Alert if a select on employees table occurs		ORCLDB	DATA ACCESS	
UserUpdate	Alert if a user is created or dropped		ORCLDB	ACCOUNT MANAGEMENT	




For More Information

<http://search.oracle.com>

database security



oracle.com/database/security



The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



ORACLE IS THE INFORMATION COMPANY