

SECURITY INSIDE-OUT

Complete Protection for Your Database,
Middleware, and Applications

ORACLE®
Oracle Audit Vault
Technical Overview

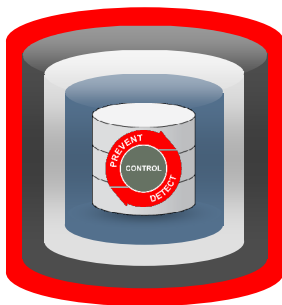
Agenda

- Oracle Database Security – Defense-in-Depth
- Business drivers and product overview
- Oracle and non-Oracle audit support
- Secure and scalable repository
- Reporting and alerts
- Applications support
- 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 Audit Vault Business Drivers

- Detective controls
 - Monitor privileged application user accounts for non-compliant activity – trust but verify
 - Audit non-application access to sensitive data (credit card, financial data, personal identifiable information, etc)
 - Verify that no one is trying to bypass the application security controls
 - PO line items are changed so it does not require more approvals
- Cost of compliance
 - Eliminate costly and complex scripts for reporting
 - Reduce reporting costs for specific compliance audits
 - SOX, PCI, HIPAA, SAS 70, STIG

ORACLE

4

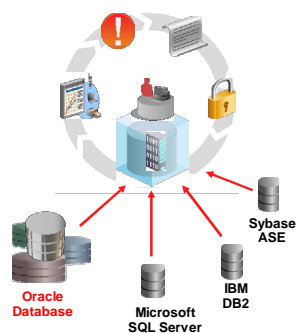
Oracle Audit Vault Trust-but-Verify

Consolidate and Secure
Audit Data

Out-of-the Box
Compliance Reports

Alert on Security
Threats

Lower IT Costs With
Entitlements & Audit Policies



ORACLE

5

Oracle Audit Vault

Oracle Database Audit Support

- Database Audit Tables
 - Collect audit data for standard and fine-grained auditing
- Oracle audit trail from OS files
 - Collect audit records written in XML or standard text file
- Operating system SYSLOG
 - Collect Oracle database audit records from SYSLOG
- Redo log
 - Extract before/after values and DDL changes to table
- Database Vault specific audit records

Audit on	Logged in
User	AUD\$
Object	FGA_LOG\$
Statement	
Privilege	OS Logs
Condition	REDO Log

ORACLE

6

Oracle Audit Vault

Heterogeneous Database Support

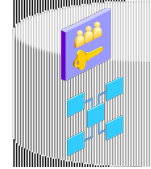
- Microsoft SQL server versions 2000, 2005, & 2008
 - Server side trace – set specific audit event
 - Windows event audit – specific audit events that are viewed by the windows event viewer
 - C2 - automatically sets all auditable events and collects them in the audit log
 - Support for 2008 audit facility targeted for CY2010
- 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

ORACLE

7

Secure & Scalable Audit Warehouse

- Audit Warehouse
 - Document Schema
 - 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

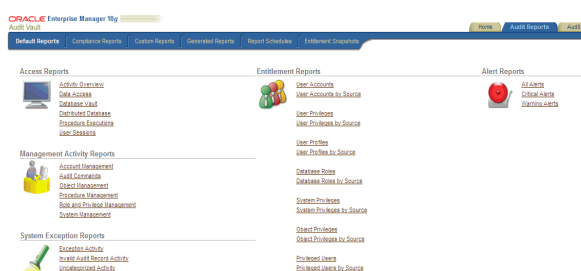


ORACLE

8

Oracle Audit Vault 10.2.3.2

Default Reports



ORACLE

9

Oracle Audit Vault

Consolidated Reports Span Enterprise Databases

Activity Overview

Rows: 15

Source	Category	Event	User	Target	Host	Event Time
HR ORACLE.VM	OBJECT MANAGEMENT	CREATE TABLE	PASSPORT	VISA	cellapp01.oracle.com	11-JUN-08 10:02:53
HR ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCAPPER	VVL_TAB	cellapp01.oracle.com	10-JUN-08 17:13:28
HR ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCAPPER	VVL_TAB	cellapp01.oracle.com	10-JUN-08 17:13:19
PAYROLL ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCAPPER	VVL_TAB	cellapp01.oracle.com	10-JUN-08 16:19:35
PAYROLL ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCAPPER	VVL_TAB	cellapp01.oracle.com	10-JUN-08 16:19:25
HR ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCAPPER	VVL_TAB1	cellapp01.oracle.com	10-JUN-08 17:13:28
HR ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCAPPER	VVL_TAB1	cellapp01.oracle.com	10-JUN-08 17:13:19
PAYROLL ORACLE.VM	OBJECT MANAGEMENT	RENAME	JSCAPPER	VVL_TAB1	cellapp01.oracle.com	10-JUN-08 16:19:35
PAYROLL ORACLE.VM	OBJECT MANAGEMENT	CREATE VIEW	JSCAPPER	VVL_TAB1	cellapp01.oracle.com	10-JUN-08 16:19:25
myqserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avacour	configurations	oracle_sa	11-JUN-08 13:22:02
myqserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avacour	ft_trace_getinfo	oracle_sa	11-JUN-08 13:22:02
myqserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avacour	ft_trace_gettable	oracle_sa	11-JUN-08 13:50:05
myqserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avacour	ft_trace_gettable	oracle_sa	11-JUN-08 13:50:02
myqserver1	OBJECT MANAGEMENT	ACCESS OBJECT	avacour	ft_trace_gettable	oracle_sa	11-JUN-08 13:50:00

ORACLE

10

User Entitlement Reports For 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
- Filter data based on users or privileges
- Regulations: SOX, PCI, HIPAA, SAS 70, STIG

ORACLE

11

Database User Privileges Report

ORACLE Enterprise Manager 10g

Audit Vault

Default Reports

User Privileges

Label: LATEST

Rows: 500

Create PDF

Source	Label	User / Role	Type	Privileges	Roles	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	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

12

User Account Details

Account, Roles, System/Object Privileges

User: HR
Last Login: 11/9/2008 02:41:22 AM
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

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	

Object Privileges

Privilege	Grantor	Grantee	Table Name	Grantee
EXECUTE	SYS	HR	HR.EMP	HR

ORACLE

13

Out-of-the-box Compliance Reports

PCI

Financial

Health Care

Violations

Financial

Health Care

ORACLE

14

Reports Management

Schedule, Retention, Notification, Attestation

Reports Management

Schedule

Retention

Notification

Attestation

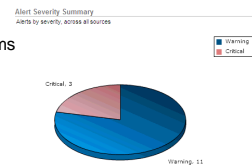
ORACLE

15

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



ORACLE

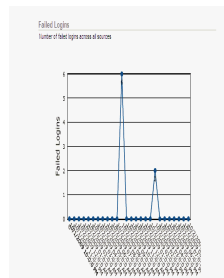
16

Alerts Dashboard Snippets

Recent Alerts

Alert Name	Alert Severity	Source	Object	Alert Time
OverFlow	Critical	PAYROLL.Oracle.VM	NEW_ROLE	10/2/2009 08:42:12 AM
DropTable	Critical	PAYROLL.Oracle.VM	TEST_BASIC_TYPE	10/2/2009 08:41:42 AM
DropTable	Critical	PAYROLL.Oracle.VM	EMP	10/2/2009 08:41:42 AM
CreateUser	Warning	PAYROLL.Oracle.VM	RUTUSER	10/2/2009 08:41:42 AM
UserUpdate	Warning	PAYROLL.Oracle.VM	RUTUSER	10/2/2009 08:41:42 AM

Recent Alerts



Monitor failed logins

ORACLE

17

Integration with Email / SMS / Remedy

Integration with Email / SMS / Remedy

Alerts

Value

Alerts

Value

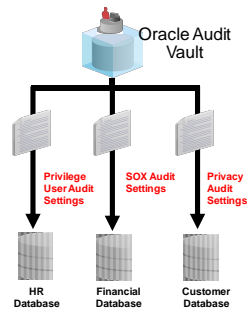
ORACLE

18

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

19

Oracle Audit Vault

Application Certification

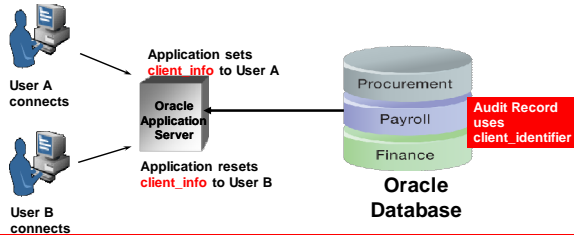
- Applications are validated by Default
 - Database auditing is underneath the Application
- Application User Auditing
 - Application can set the database "Client Identifier" to tie application user with application shared account
- Database Auditing can be used to monitor
 - Audit base application tables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

ORACLE

20

Setting Client Identifier

- Track the application user
- Any application running on Oracle database can set the client identifier
- PSFT Tools 8.50 sets the client_identifier
- eBusiness can update the code manually today – bug 8386700



ORACLE

21

Oracle Audit Vault

Application Integration

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

ORACLE

22

Oracle Audit Vault

PeopleSoft Application Integration

- 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

23

Oracle Audit Vault

eBusiness Suite

Oracle Audit Vault eBusiness Suite

Source	Source Type: ORCLDB Source: VBS211.US.Oracle.com Host: c095v12.us.oracle.com Version: 11.1.2.3.0 IP Address: 10.25.54.180
Event	Audit Vault Time: 10/11/2009 11:53:38 PM Event Time: 10/11/2009 11:53:38 PM Event Status: 0 Event: 0000 Category: CATCH_ACCESS Source Event: 2
Target	Owner: APPLSYS Target: IMP_LOCAL_USER_ROLES
Client/User Information	User: apts OS User: apts Host: 10.25.54.180 Terminal: j05014 Client ID: 51340203
Statement	SQL Text SCN: 1013214088312 Bind Variables VARIABLES SQL Text Statement ID: 848 Session Session ID: 10201801

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



26

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...)	●	●	●	●	●	●

ORACLE

27

Script to run on Oracle to start auditing

\$SAV_HOME/demo/secconf.sql

- AUDIT SYSTEM
- CREATE SESSION
- ALTER SYSTEM
- ALTER DATABASE
- ALTER ANY PROCEDURE
- CREATE ANY PROCEDURE
- DROP ANY PROCEDURE
- CREATE ANY JOB
- CREATE EXTERNAL JOB
- ALTER ANY TABLE
- CREATE ANY TABLE
- DROP ANY TABLE
- CREATE ANY LIBRARY
- ALTER PROFILE
- DROP PROFILE
- ALTER USER
- CREATE USER
- DROP USER
- EXEMPT ACCESS POLICY
- AUDIT ROLE BY ACCESS
- GRANT ANY ROLE
- GRANT ANY OBJECT PRIVILEGE
- GRANT ANY PRIVILEGE
- CREATE PUBLIC DATABASE LINK

ORACLE

28

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%

Internal testing: Source: 4x32GB 3GHz Intel Xeon RHEL3.0, running 2 Oracle Database 10.2.0.3.0
AV Server: 2x6GB 3GHz Intel Xeon RHEL3.0, AV Server 10.2.2.0.0

ORACLE

29

Oracle Audit Vault Customers



ORACLE

CMC Markets Baking in Security

"...The Oracle security components underpinning our standard Oracle security configuration bring a new level of assurance to our senior management and audit teams."

Business Challenges	<ul style="list-style-type: none"> Simplify complex audit cycles by providing a standard security platform for 6 Oracle databases using RAC and running Oracle eBusiness Suite Automate security monitoring and alerting to free up administrator resources for other infrastructure projects Sustain strong brand reputation for rigorous protection and security of customer data
Solution	<ul style="list-style-type: none"> Oracle Audit Vault consolidated reporting on audit data
Business Results	<ul style="list-style-type: none"> Reduced administrative audit cycle duties by 50% Increased security awareness among administrative staff, without adversely impacting their essential functions Tightened security processes for data protection by increasing checkpoints and audit points for data access

ORACLE

31

JPMC Payment Tech Stronger Controls

Business Challenges	<ul style="list-style-type: none"> Audit credit card transactions 20+ production Oracle databases with native auditing already turned on Need for reports but without any resource or budget to create and review them
Solution	<ul style="list-style-type: none"> Oracle Audit Vault for audit data collection and secure centralized storage Monitors privileged user access violations, failed database logins, and generate forensic data
Business Results	<ul style="list-style-type: none"> Passed internal audits Automated reporting on credit card transactions Secure consolidation of audit data Detected policy violations of database activity

ORACLE

32

Large Online Retailer Address Insider Threats

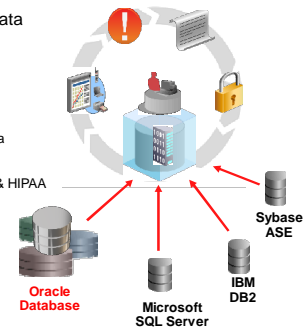
Business Challenges	<ul style="list-style-type: none"> Internal audit led to requirement for increased db security controls, fraud prevention system, and monitoring Allow for correlation of audit records Alert on configured suspicious activity
Solution	<ul style="list-style-type: none"> Automated solution to monitoring with Audit Vault Out of the box compliance reporting Scalable solution – large DB population Flexibility to build complete custom reports from warehouse
Business Results	<ul style="list-style-type: none"> Oracle skills plentiful at customer, no need to retrain Flexibility in reporting Scale to terabytes of audit data Performance – Audit Vault and Native DB Auditing is negligible with a transaction rate of 90,000 / 5 minutes

ORACLE

33

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

34

For More Information

search.oracle.com

Search for: In the section:

oracle.com/database/security

ORACLE

35



ORACLE

36



ORACLE IS THE **INFORMATION** COMPANY

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.