SECURITY [INSIDE OUT]

Complete Protection for Your Database, Middleware, and Applications

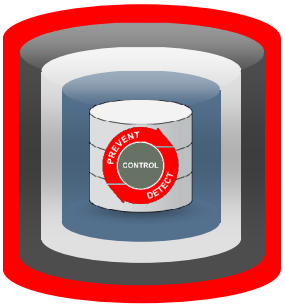
ORACLE

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 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 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

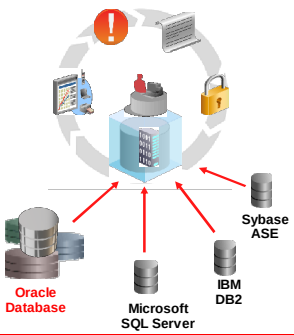
Oracle Audit Vault
Trust-but-Verify

Consolidate and Secure Audit Data

Out-of-the Box Compliance Reports

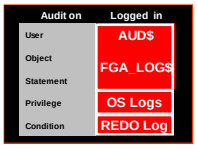
Alert on Security Threats

Lower IT Costs With Entitlements & Audit Policies



Oracle 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

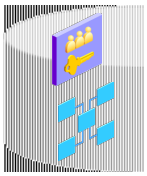


Oracle Audit Vault
Heterogeneous Database Support

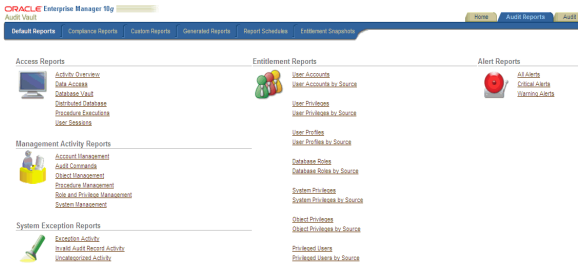
- Microsoft SQL server versions 2000, 2005, & 2008
  - Server side trace – set specific audit event
  - Windows event audit – specific audit events that are viewed by the windows event viewer
  - C2 - automatically sets all auditable events and collects them in the audit log
  - Support for 2008 audit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

Secure & Scalable Audit Warehouse

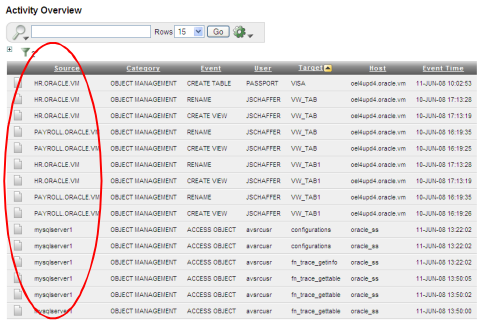
- Audit Warehouse
  - Document Schema
  - Enable BI and analysis
- Performance and Scalability
  - Built-in partitioning
  - Database compression
  - Scales to Terabytes
  - Certified with Oracle RAC
- Protected with Built-in Security
  - Encrypted audit data transmission
  - Separation of Duty provided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



Oracle Audit Vault 10.2.3.2
Default Reports



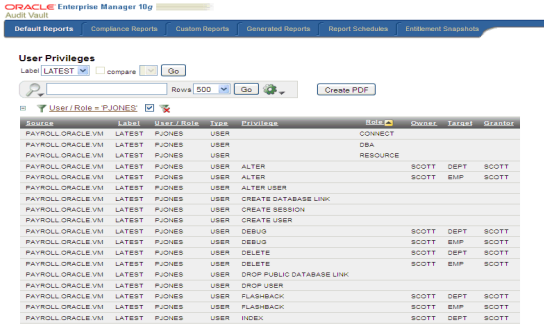
Oracle Audit Vault
Consolidated Reports Span Enterprise Databases



User Entitlement Reports For
Oracle Databases

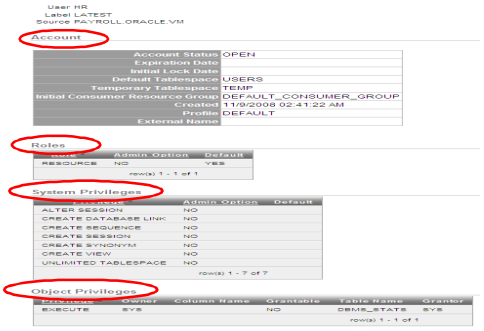
- Report all user accounts, roles, and privileges
- Retrieve a snapshot of user entitlement data
- Compare changes in user accounts and privileges
- View SYSDBA/SYSOPER privileges
- Filter data based on users or privileges
- Regulations: SOX, PCI, HIPAA, SAS 70, STIG

Database User Privileges Report



User Account Details

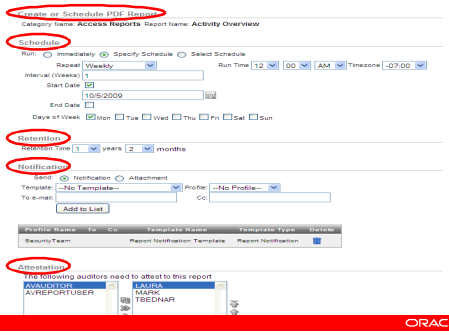
Account, Roles, System/Object Privileges



Out-of-the-box Compliance Reports

Reports Management

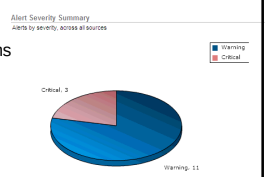
Schedule, Retention, Notification, Attestation



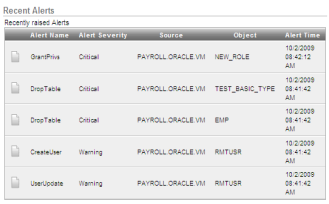
Oracle Audit Vault Alerts

Threat Detection with Custom Alerts

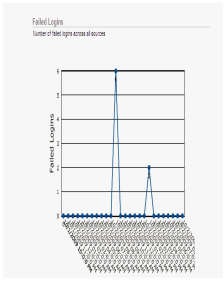
- Alerts can be defined for
  - Creating users on sensitive systems
  - Role grants on sensitive systems
  - "DBA" grants on all systems
  - Failed logins for application users
  - Directly viewing sensitive columns
  - ….
- Add workflow for alerts
- Track alerts
- Drill down from the dashboard
- Send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



Alerts Dashboard Snippets

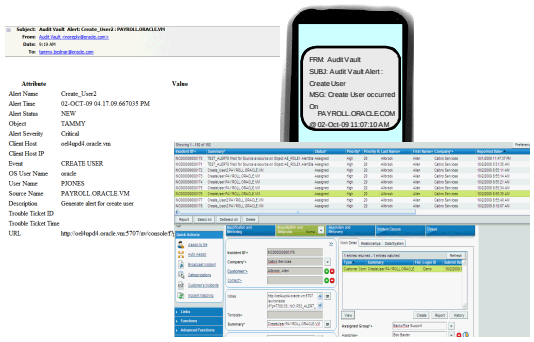


Recent Alerts



Monitor failed logins

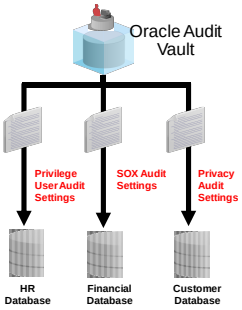
Integration with Email / SMS / Remedy



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



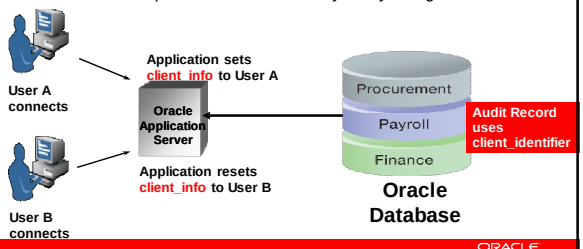
Oracle Audit Vault

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
- PSFT Tools 8.50 sets the client_identifier
- eBusiness can update the code manually today – bug 8386700



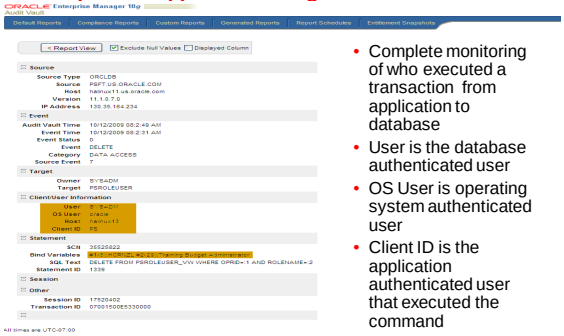
Oracle Audit Vault

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

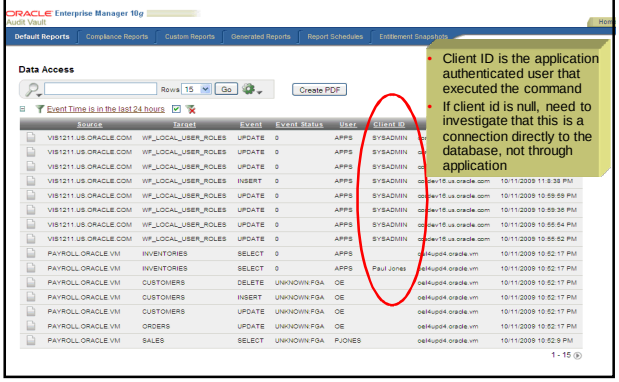
PeopleSoft Application Integration



- 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

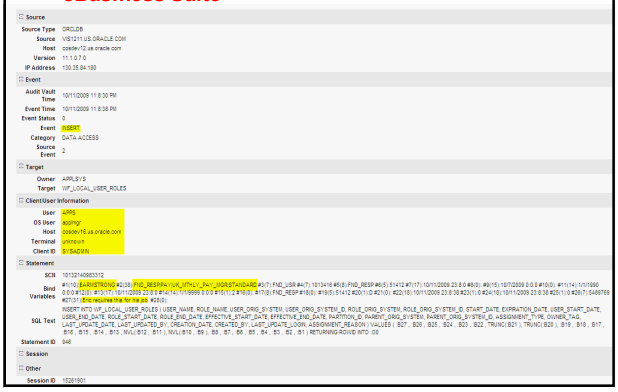
Oracle Audit Vault

eBusiness Suite



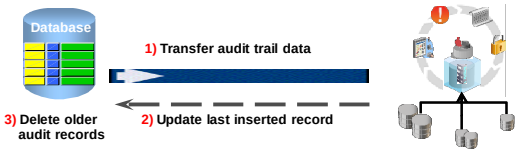
- Client ID is the application authenticated user that executed the command
- If client id is null, need to investigate that this is a connection directly to the database, not through application

Oracle Audit Vault
eBusiness Suite



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



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…)	●	●	●	●	●	●

Script to run on Oracle to start auditing
$AV_HOME/demo/secconf.sql

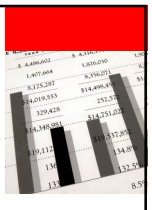
- AUDIT SYSTEM
- CREATE SESSION
- ALTER SYSTEM
- ALTER DATABASE
- ALTER ANY PROCEDURE
- CREATE ANY PROCEDURE
- DROP ANY PROCEDURE
- CREATE ANY JOB
- CREATE EXTERNAL JOB
- ALTER ANY TABLE
- CREATE ANY TABLE
- DROP ANY TABLE
- CREATE ANY LIBRARY
- ALTER PROFILE
- DROP PROFILE
- ALTER USER
- CREATE USER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

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 Xeons RHEL3.0, running 2 Oracle Database 10.2.0.3.0
AV Server: 2x6GB 3GHz Intel Xeons RHEL3.0, AV Server 10.2.2.0.0



Oracle Audit Vault Customers

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	• 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	• Oracle Audit Vault consolidated reporting on audit data
Business Results	• 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

JPMC Payment Tech
Stronger Controls

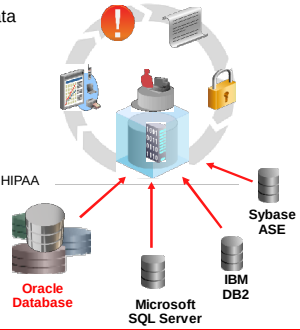
Business Challenges	• Audit credit card transactions • 20+ production Oracle databases with native auditing already turned on • Need for reports but without any resource or budget to create and review them
Solution	• Oracle Audit Vault for audit data collection and secure centralized storage • Monitors privileged user access violations, failed database logins, and generate forensic data
Business Results	• Passed internal audits • Automated reporting on credit card transactions • Secure consolidation of audit data • Detected policy violations of database activity

Large Online Retailer
Address Insider Threats

Business Challenges	• 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	• 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	• 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

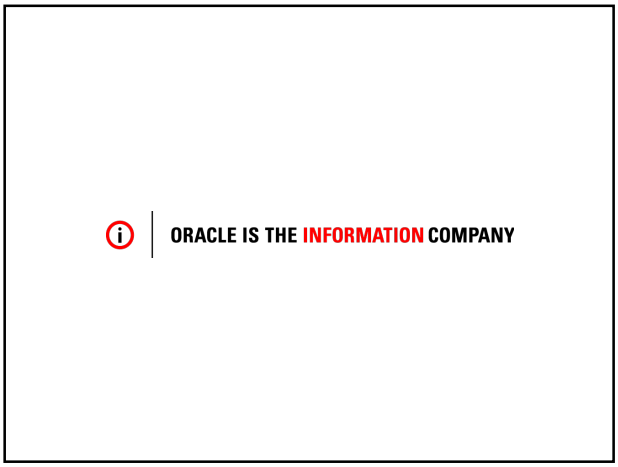
Oracle Audit Vault 10.2.3.2
Summary

- 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



For More Information

oracle.com/database/security


ORACLE IS THE INFORMATION COMPANY