Oracle Audit Vault

presentation for:

Utah Oracle Users Group

© Puget Sound Oracle Users Group

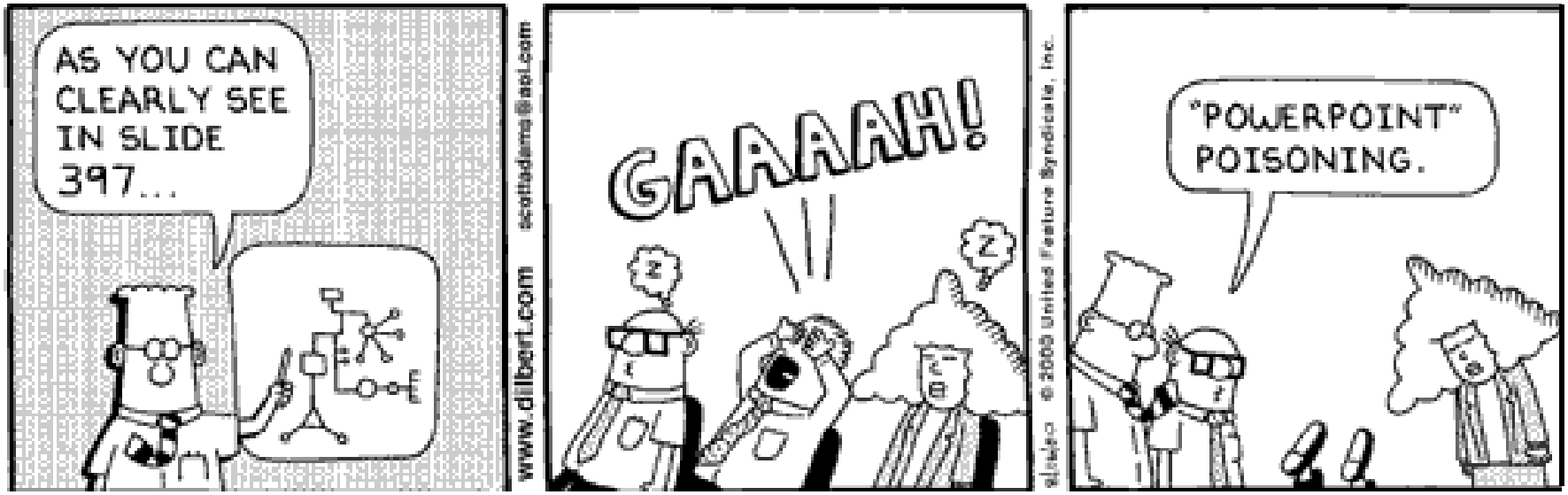
Education Is Our Passion

Who am I?

- Daniel Morgan
- Oracle Ace Director 
- University of Washington
  - Wrote UW Oracle curricula
  - Primary program instructor - 8 years
- Education Chair: PSOUG 
- Member: UKOUG
- Frequent speaker – OOW and user group events
- 10g, 11g, and TimesTen Beta tester
- Oracle since version 6
- Too many years of Fortran and COBOL
- Contact: damorgan@u.washington.edu

© Puget Sound Oracle Users Group

I will try to avoid this ...



© Puget Sound Oracle Users Group
Education Is Our Passion

What Your Management Is Hearing

© Puget Sound Oracle Users Group

Sarbanes Oxley Act (SOX, SarbOx)

- Passed by Congress on January 23rd, 2002 and signed by President Bush on July 30th, 2002
- Industrial engine manufacturing FUD

© Puget Sound Oracle Users Group
Education Is Our Passion

SOX Requirements

Sarbanes-Oxley Section 302 and 404 Internal Control Requirements

Section 302

Requires the CEO and CFO of a public company to certify quarterly and annually that they:

- Are responsible for disclosure controls,
- Have designed controls to ensure that material information is known to them,
- Have evaluated the effectiveness of controls,
- Have presented their conclusions in the filing,
- Have disclosed to the audit committee and auditors significant control deficiencies and acts of fraud,
- Have indicated in the report significant changes to controls.

Section 404

Requires the CEO and CFO to annually:

- State their responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting,
- Conduct and provide an assessment of the effectiveness of the internal controls.

Requires the external auditor to:

- Attest to management's assertion.

© Puget Sound Oracle Users Group
Education Is Our Passion

SOX Requirements

Requires the independent external Auditor to provide two opinions:

- An assessment of management's evaluation of the company's internal control over financial reporting
- Its own independent evaluation based on its review and testing of the company's internal control over financial reporting

© Puget Sound Oracle Users Group
Education Is Our Passion

HIPAA Requirements

- Give patients access to their information and ability to request change
- Restrict access to a patients information to others
- Restrict disclosure of protected information to minimum required for healthcare treatments & transitions
- Establish controls for access to records by researchers
- Assign a privacy officer that will administer the privacy policy programs and enforce compliance
- Maintain confidentiality, integrity and availability of healthcare information

© Puget Sound Oracle Users Group
Education Is Our Passion

Electronic Storage of Broker-Dealer Records

- Electronic records must be preserved exclusively in a non-rewriteable and non-erasable format
- Broker-dealers may employ a storage system that prevents alteration or erasure of the records for their required retention period.

© Puget Sound Oracle Users Group
Education Is Our Passion

FACTA Requirements (1 of 2)

- Fair Credit Reporting Act
- Required as of June 1, 2005
- FACTA provisions consumer reporting agencies and any business that uses a consumer report must adopt procedures for proper document disposal.

© Puget Sound Oracle Users Group
Education Is Our Passion

FACTA Requirements (2 of 2)

- The FTC, the federal banking agencies, and the National Credit Union Administration (NCUA) have published final regulations to implement the new FACTA Disposal Rule. The FTC's disposal rule applies to consumer reporting agencies as well as individuals and any sized business that uses consumer reports. The FTC lists the following as among those that must comply with the rule:
  - Lenders
  - Insurers
  - Employers
  - Landlords
  - Government agencies
  - Mortgage brokers
  - Automobile dealers
  - Attorneys and private investigators
  - Debt collectors

© Puget Sound Oracle Users Group
Education Is Our Passion

Gramm-Leach-Bliley Requirements (GLB)

- Establish an information security program assess and control risks to customer NPI.
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to or use of such records that could result in harm or inconvenience to any customer
- Install access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals as well as prevent employees from providing

© Puget Sound Oracle Users Group
Education Is Our Passion

PCI Requirements (1 of 2)

- Payment Card Industry Data Security Standard
- Required by September 2007 if your organization accepts credit cards
- The TJX Companies breach
  - The TJX Companies Inc. breach is the largest known data theft to date. Hackers invaded the TJX systems resulting in at least 45.7 million credit and debit card numbers stolen over an 18-month period. As well as the stolen personal data, including driver's license numbers of another 455,000 customers who returned merchandise without receipts.

© Puget Sound Oracle Users Group
Education Is Our Passion

PCI Requirements (2 of 2)

- Requirement 2.2.4 - Remove all unnecessary functionality
- Requirement 2.3 - Encrypt all non-console administrative access
- Requirement 4 - Encrypt transmission of cardholder data across open, public networks
- Requirement 6 - Develop and maintain secure systems and applications
- Requirement 6.5.1 - Unvalidated Input
- Requirement 6.5.2 - Broken Access Control
- Requirement 6.5.3 - Broken Authentication and Session Management
- Requirement 6.5.4 - Cross Site Scripting (XSS) Flaws
- Requirement 6.5.5 - Buffer Overflows
- Requirement 6.5.6 - Injection Flaws
- Requirement 6.5.7 - Improper Error Handling
- Requirement 6.5.8 - Insecure Storage
- Requirement 6.5.9 - Denial of Service
- Requirement 6.5.10 - Insecure Configuration Management

© Puget Sound Oracle Users Group
Education Is Our Passion

PIPEDA Requirements (1 of 2)

- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Office of the
Privacy Commissioner
of Canada

© Puget Sound Oracle Users Group

PIPEDA Requirements (2 of 2)

- Build and Maintain a Secure Network
  - **Install and maintain a firewall configuration to protect cardholder data**
  - **Do not use vendor-supplied defaults for system passwords and other security parameters**
- Protect Cardholder Data
  - **Protect stored cardholder data**
  - **Encrypt transmission of cardholder data across open, public networks**
- Maintain a Vulnerability Management Program
  - **Use and regularly update anti-virus software**
  - **Develop and maintain secure systems and applications**
- Implement Strong Access Control Measures
  - **Restrict access to cardholder data by business need-to-know**
  - **Assign a unique ID to each person with computer access**
  - **Restrict physical access to cardholder data**
- Regularly Monitor and Test Networks
  - **Track and monitor all access to network resources and cardholder data**
  - **Regularly test security systems and processes**
- Maintain an Information Security Policy
  - **Maintain a policy that addresses information security**

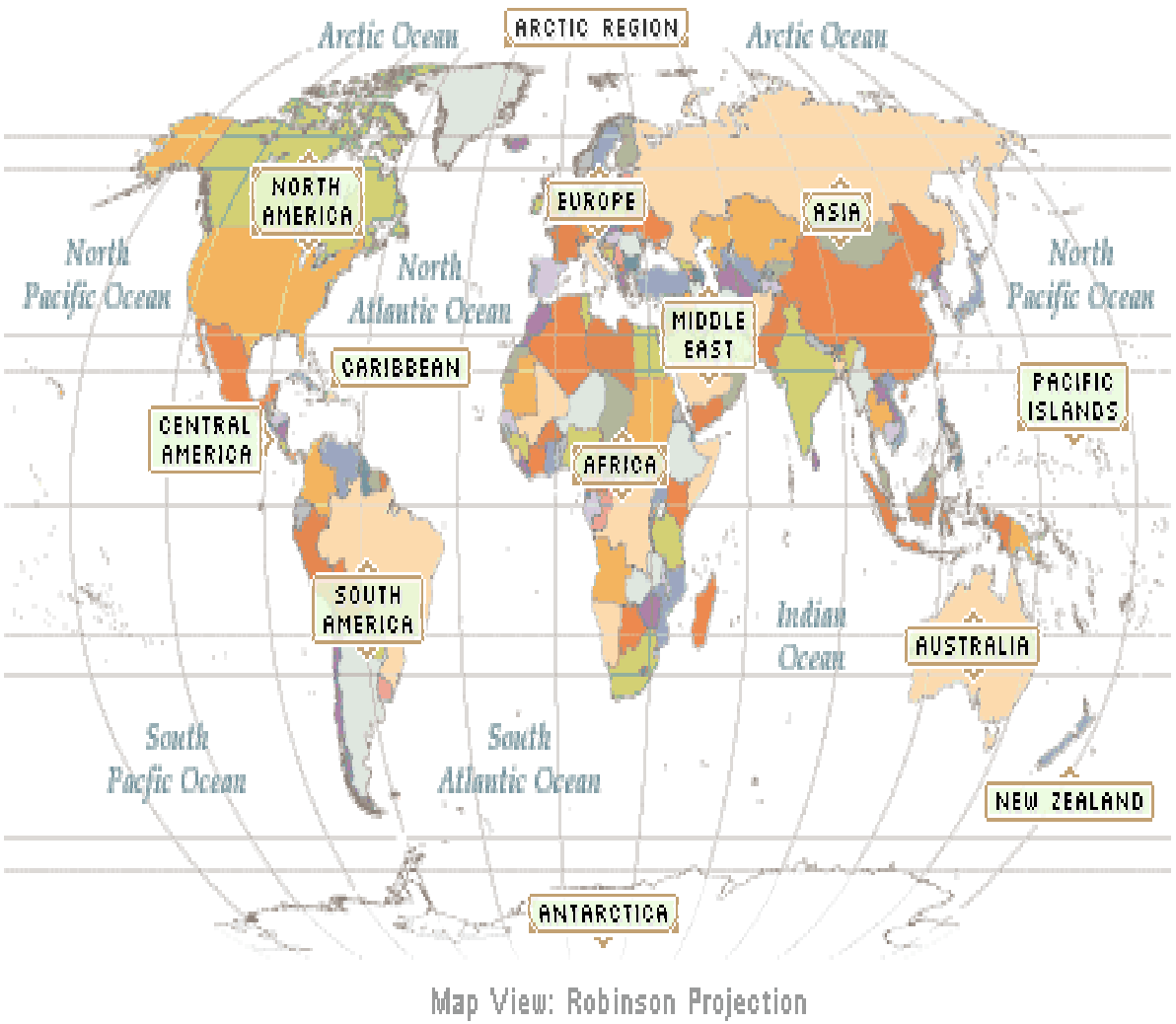
© Puget Sound Oracle Users Group
Education Is Our Passion

Basel II Requirements

- To be in compliance with Basel II, a banking institution must deliver appropriate reporting of operational risk exposures and loss data to its board of directors and senior management. These reports must:
  - Address both company-wide and line of business results.
  - Summarize operational risk exposure, loss experience, relevant business environment and internal control assessments.
  - Identify and assess the operational risk inherent in all material products, activities, processes and systems.

© Puget Sound Oracle Users Group
Education Is Our Passion

Expanding Regulatory Requirements



Map View: Robinson Projection

AMERICAS

- **HIPAA**
- **FDA CFR 21 Part 11**
- **OMB Circular A-123**
- **SEC and DoD Records Retention**
- **USA PATRIOT Act**
- **Gramm-Leach-Bliley Act**
- **Federal Sentencing Guidelines**
- **Foreign Corrupt Practices Act**
- **Market Instruments 52 (Canada)**

EMEA

- **EU Privacy Directives**
- **UK Companies Law**
- **Restriction of Hazardous Substances (ROHS/WEE)**

APAC

- **J-SOX (Japan)**
- **CLERP 9: Audit Reform and Corporate Disclosure Act (Australia)**
- **Stock Exchange of Thailand Code on Corporate Governance**

GLOBAL

- **International Accounting Standards**
- **Basel II (Global Banking)**
- **OECD Guidelines on Corporate Governance**

© Puget Sound Oracle Users Group
Education Is Our Passion

The Cost

- A study conducted by Ponemon Institute estimates an average cost of $14 million per security breach incident, with costs ranging as high as $50 million.
  - Study covered 14 separate incidents, encompassing 1.4 million compromised data records and an estimated total of $200 million in resulting losses
  - Total cost estimates include the actual cost of internal investigations, outside legal defense fees, notification and call center costs, PR and investor relations efforts, discounted services offered, lost employee productivity and the effect of lost customers.

© Puget Sound Oracle Users Group
Education Is Our Passion

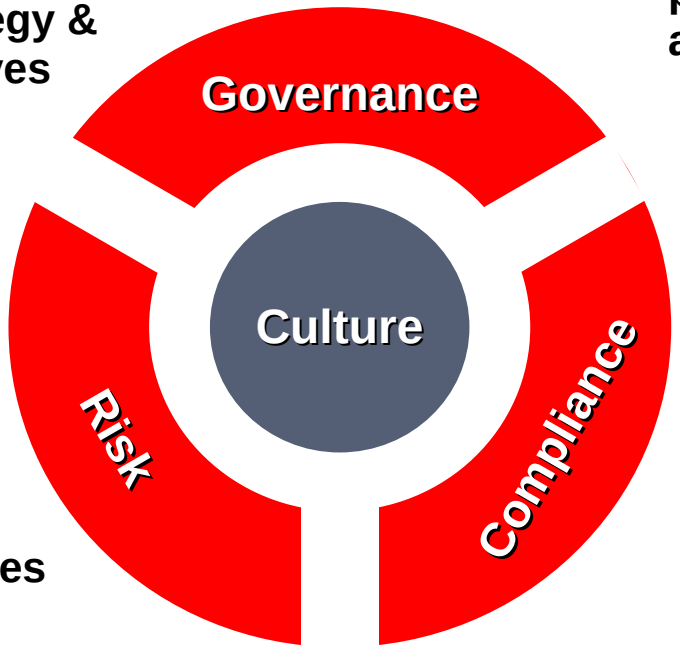
Governance, Risk, and Compliance (GRC)

Governance

- **Set and evaluate performance against objectives**
- **Authorize business strategy & model to achieve objectives**

Culture

- **Establish organizational climate and mindset that promote trust, integrity, & accountability**



Risk Management

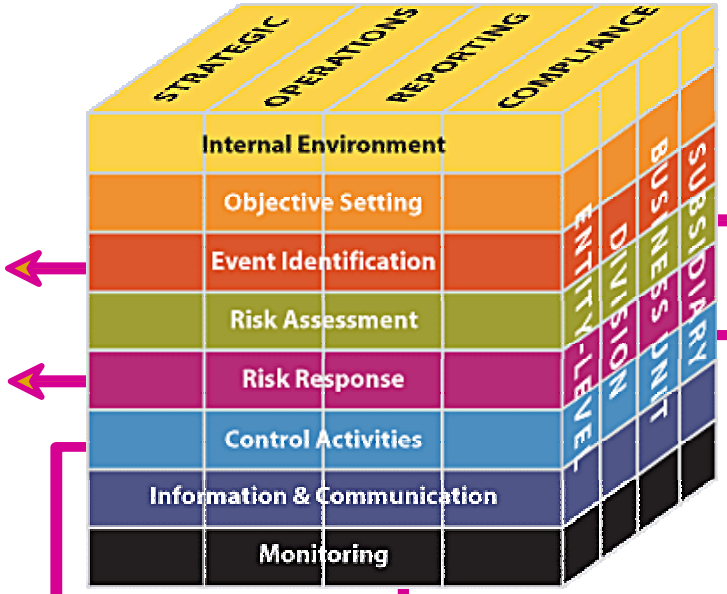
- **Identify, assess, and address potential obstacles to achieving objectives**
- **Identify / address violation of mandated and voluntary boundaries**

Compliance

- **Encourage / require compliance with established policies and boundaries**
- **Detect non-compliance and respond accordingly**

© Puget Sound Oracle Users Group
Education Is Our Passion

COSO Cube & Compliance Reference Model



Event Identification

- Exception thresholds

Risk Response

- Corrective Workflows

Information & Communication

- Approval Workflows
- Attestation Workflows
- Exception Notifications
- Delegated Administration
- Automated Provisioning
- Password Reset

Monitoring

- Continuous Exception Detection & Monitoring
- Periodic Reports and Attestations

Risk Assessment

- Model Risk assessment around resources with sensitive data – financial, ePHI, NPI
  - Electronic Transactions
  - Application, Application Server, DB, OS
- Predictive Risk Analysis

Control Activities

- Entitlement Policies: RBAC, ABAC, SoD
- Strong Authentication
- Exception Detection & Remediation
- Employee termination
- Policy Retrofits & Revocations

- Committee Of Sponsoring Organizations of the Treadway Commission
- Most accepted framework for financial controls

© Puget Sound Oracle Users Group
Education Is Our Passion

What is an Internal Control?

- Providing reasonable assurance of:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with laws and regulations

or else…

© Puget Sound Oracle Users Group
Education Is Our Passion

What Management Wants

- You need to know who did what and when
- You need to know who accessed what data both generally and under specified conditions
- You need to protect the audit trail from tampering and be able to prove it is authentic
- Adequately guard against security threats without choking the business

© Puget Sound Oracle Users Group
Education Is Our Passion

What Auditors Want

- Separation of duties
- Reporting
- Notification
- Proven audit data integrity

© Puget Sound Oracle Users Group
Education Is Our Passion

What IT Wants

- Performance and scalability
- Minimal constraints while getting the job done
- Evenings and weekends off

© Puget Sound Oracle Users Group

Auditing

© Puget Sound Oracle Users Group
Education Is Our Passion

Traditional Auditing Methods

- Standard Auditing (since the time of the dinosaurs)
- Log Miner (since 8.1.5)
- Fine Grained Auditing (since 9.0.1)
- Triggers
  - Table Triggers (since 6.0)
  - DDL Event Triggers (since 8.1.6)
  - System Event Triggers (since 8.1.6)
- Application Auditing (hand coded into the application)
- Data Vault / Audit Vault (new)

© Puget Sound Oracle Users Group
Education Is Our Passion

Standard Auditing

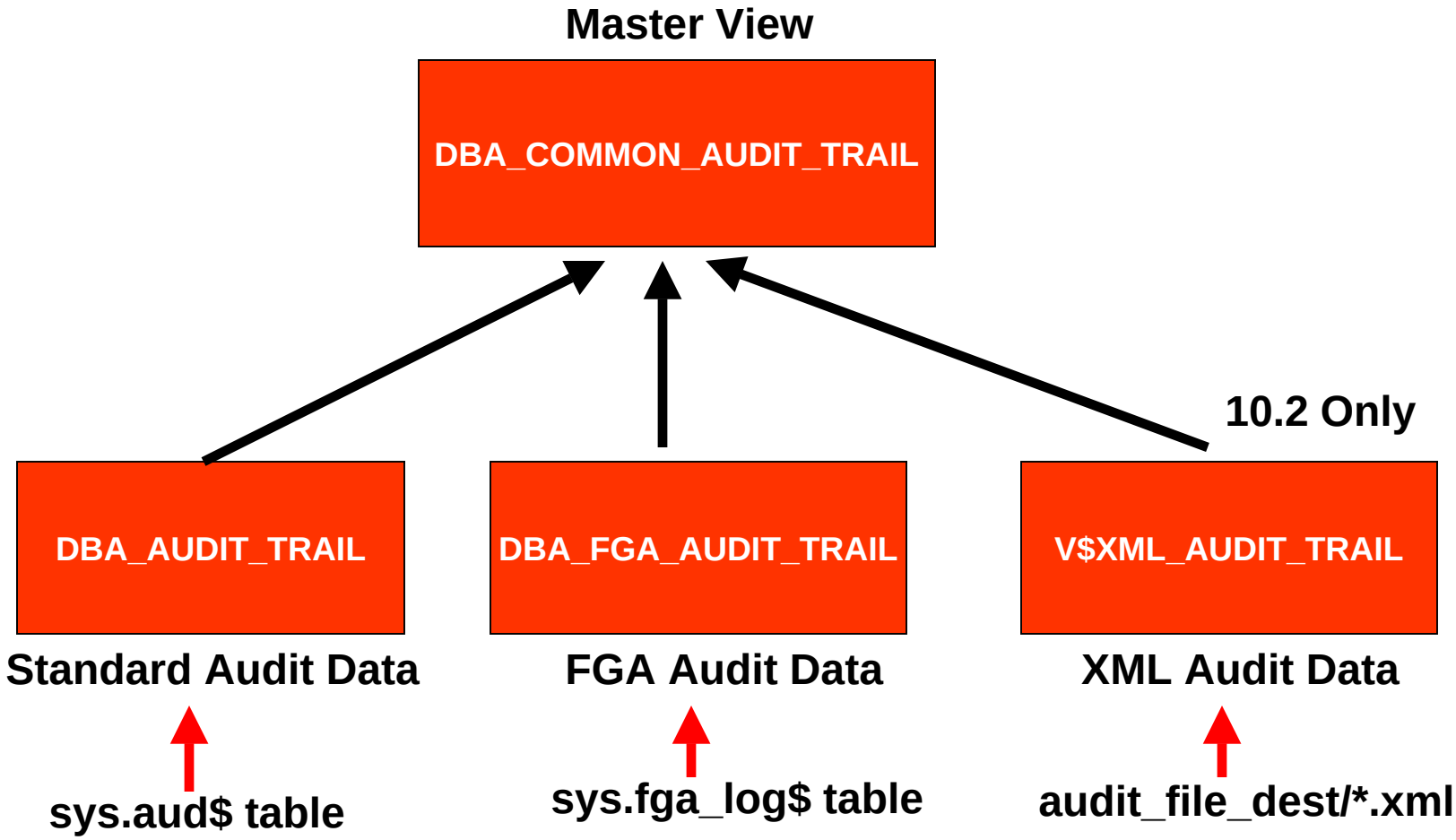
```
SQL> SELECT name, value
  2  FROM gv$parameter
  3  WHERE name LIKE '%audit%';

NAME                                 VALUE
------------------------------------ ------------------------------
audit_sys_operations                 FALSE
audit_file_dest                      C:\ORACLE\ADMIN\ORABASE\ADUMP
audit_trail                          DB

SQL>
```

© Puget Sound Oracle Users Group
Education Is Our Passion

Database Auditing



© Puget Sound Oracle Users Group
Education Is Our Passion

Standard Auditing

```
SQL> SELECT extended_timestamp, os_user, statement_type
  2  FROM dba_common_audit_trail;

EXTENDED_TIMESTAMP                        OS_USER         STATEMENT_TYPE
----------------------------------------- --------------- --------------
21-NOV-07 04.17.14.828000 PM -07:00 Daniel Morgan   LOGON
21-NOV-07 04.17.14.906000 PM -07:00 Daniel Morgan   LOGON
21-NOV-07 04.19.30.765000 PM -07:00 Daniel Morgan   LOGON
21-NOV-07 04.19.32.296000 PM -07:00 Daniel Morgan   LOGOFF
21-NOV-07 04.19.50.703000 PM -07:00 Daniel Morgan   LOGON
21-NOV-07 04.19.55.234000 PM -07:00 Daniel Morgan   LOGOFF
21-NOV-07 04.23.09.875000 PM -07:00 Daniel Morgan   LOGON
```

© Puget Sound Oracle Users Group
Education Is Our Passion

Log Miner

- DBMS_LOGMNR
  - ADD_LOGFILE
  - START_LOGMNR
  - END_LOGMNR

```
exec sys.dbms_logmnr.add_logfile('c:\temp\demo1.arc');
exec sys.dbms_logmnr.add_logfile('c:\temp\demo2.arc');
exec sys.dbms_logmnr.add_logfile('c:\temp\demo3.arc');
exec sys.dbms_logmnr.start_logmnr(7466113,7466134);

exec sys.dbms_logmnr.start_logmnr(7466113, 7466134, options=>2);

SELECT v.scn, v.commit_timestamp, v.table_name, o.object_name, v.operation
FROM sys.v_$logmnr_contents v, dba_objects o
WHERE SUBSTR(v.table_name,6) = o.object_id;

exec sys.dbms_logmnr.end_logmnr;
```

© Puget Sound Oracle Users Group
Education Is Our Passion

Fine Grained Auditing (FGA)

- Best solution for some problems
- No overhead when conditions are not met
- No overhead when policy exists on different statement types
- XML auditing performs better than DB_EXTENDED
- Still need standard auditing for coverage of areas not provided by FGA

© Puget Sound Oracle Users Group
Education Is Our Passion

Triggers

- AFTER INSERT OR UPDATE OR DELETE
- AFTER DDL
- AFTER LOGON / AFTER LOGOFF

```
CREATE OR REPLACE TRIGGER statement_level
AFTER INSERT OR UPDATE OR DELETE
ON orders;

CREATE OR REPLACE TRIGGER ddl_trig
AFTER DDL ON DATABASE

CREATE OR REPLACE TRIGGER logon_audit
AFTER LOGON ON DATABASE
```

© Puget Sound Oracle Users Group
Education Is Our Passion

Problems with In-House Auditing

- In-house auditing implementations may present the following issues:
  - Distributed audit data makes it difficult to perform analysis and issue alerts
  - Database administrator (DBA) or system administrator could potentially modify audit data
  - Large amount of audit data can burden production systems
  - Processing of audit data can affect production systems
  - Enterprise-wide audit policies are often complicated to administer

© Puget Sound Oracle Users Group
Education Is Our Passion

What Else Can We Do?

© Puget Sound Oracle Users Group

Access Control

- SQL*NET
  - Invited and Excluded Nodes
  - Encryption with seed value
- Profiles
  - Password Complexity and Expiration
- Privileges
  - Roles
  - System Privs
  - Object Privs

© Puget Sound Oracle Users Group
Education Is Our Passion

Default Passwords

```
SQL> SELECT d.username, u.account_status
  2  FROM dba_users_with_defpwd d, dba_users u
  3  WHERE d.username = u.username
  4  ORDER BY 2,1;

USERNAME                       ACCOUNT_STATUS
------------------------------ ----------------
CTXSYS                         EXPIRED & LOCKED
DIP                            EXPIRED & LOCKED
EXFSYS                         EXPIRED & LOCKED
MDDATA                         EXPIRED & LOCKED
MDSYS                          EXPIRED & LOCKED
ORDPLUGINS                     EXPIRED & LOCKED
ORDSYS                         EXPIRED & LOCKED
OUTLN                          EXPIRED & LOCKED
SI_INFORMTN_SCHEMA             EXPIRED & LOCKED
WK_TEST                        EXPIRED & LOCKED
WMSYS                          EXPIRED & LOCKED
XDB                            EXPIRED & LOCKED
HR                             OPEN
OE                             OPEN
SCOTT                          OPEN
SH                             OPEN

16 rows selected.

SQL>
```

© Puget Sound Oracle Users Group
Education Is Our Passion

Database Setup

```
SQL> show parameter audit

NAME_COL_PLUS_SHOW_PARAM TYPE        VALUE_COL_PLUS_SHOW_PARAM
------------------------ ----------- ------------------------------
audit_file_dest          string      C:\ORACLE\ADMIN\ORABASE\ADUMP
audit_sys_operations     boolean     FALSE
audit_trail              string      DB
```

© Puget Sound Oracle Users Group
Education Is Our Passion

In 11g

- Apply CPUs
- Track Blackout Periods
- Network Access Control Lists
  - DBMS_NETWORK_ACL_ADM
    - Secures UTL_HTTP, UTL_INADDR, UTL_MAIL, UTL_SMTP, UTL_TCP
- Case Sensitive Passwords
- Monitor usage of UTL_FILE and DataPump
- Encryption
  - SecureFiles
  - Transparent Data Encryption
  - DBMS_CRYPTO

But it still does not solve the underlying issue

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault:
The Marketing

© Puget Sound Oracle Users Group

Why Audit Vault?

- Comply with the law
- Protect the organization from insiders
- Proof for auditors
- Protection from lawsuits
- Mitigates many security risks

© Puget Sound Oracle Users Group
Education Is Our Passion

Compared with Competitive Solutions

- Network Traffic Monitor
  - Misses server-side code
  - Doesn't require DB restart
  - Impacts every statement not on DB server
- Database Transaction Monitoring
  - More overhead (CPU)
  - Captures all activity

© Puget Sound Oracle Users Group

Compared with Competitive Solutions

- Log Readers
  - Platform dependencies
  - Select Statements not audited
- Application Auditing
  - Non-Application Access unmonitored
  - Auditing is expressed in application transactions not database transactions

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault's History

- Built on top of Database Vault
  - Released August '06
- Leverages existing mature technologies
  - AQ
  - Streams
  - Log Miner
  - Auditing

© Puget Sound Oracle Users Group
Education Is Our Passion

Database and Audit Vault

Database Vault

- Specialized warehouse for audit data
- Leverages Database vault security to block DBA from viewing audit data
- SOD / Defined roles
- Audit vault and Compliance report
- Setup Audit Alerts

Audit Vault

- Restrict the DBA and other privileged users from accessing application data
- Protect the database and applications from unauthorized changes
- Enforce strong controls over who, when, and where application can be accessed

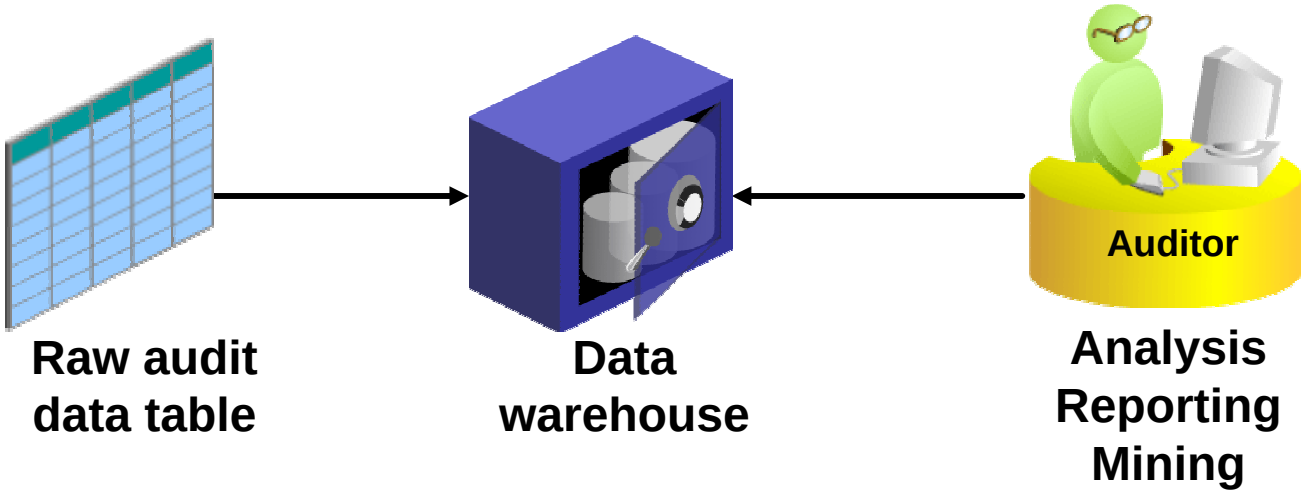
© Puget Sound Oracle Users Group
Education Is Our Passion

Built On Top Of Database Vault

- The Audit Vault Server database is protected by Oracle Database Vault features.
- Database Vault is used to:
  - Prevent access to audit data by privileged users
  - Prevent unauthorized changes to the Audit Vault Server database
  - Set access controls

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Data Warehouse: Overview



© Puget Sound Oracle Users Group
Education Is Our Passion

Only One Piece of the Puzzle

- Profiles
  - password complexity & expiration
- Roles
- System Privileges
  - Minimum required
- Object Privileges
  - Minimum required
- Database Auditing
- Fine Grained Auditing
- Fine Grained Access Control
- Identity Management

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Concepts

© Puget Sound Oracle Users Group
Education Is Our Passion

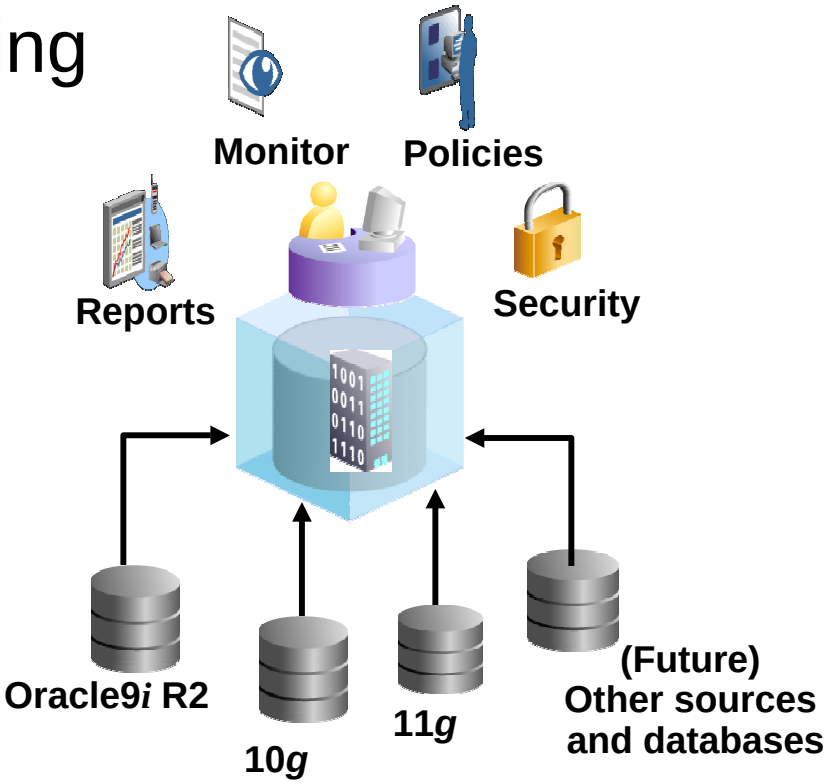
What is Audit Vault?

- A secure tamper-proof Oracle database
- A consolidated repository for audit logs from across the enterprise
- Protects audit data from modification and tampering
- Consolidates audit trails by mapping audit data to a common audit format
- Centralized audit policy management
- Enables analysis of audit data including timely detection of policy violations
- Report from a single repository

© Puget Sound Oracle Users Group
Education Is Our Passion

Oracle Audit Vault: "*Trust but verify*"

- Collect and consolidate audit data
  - Oracle9*i* Release 2 and higher
- Simplify compliance reporting
  - Built-in reports
  - Custom reports
- Detect and prevent insider threats
- Scale and security
  - Database Vault
  - Advanced Security
  - Partitioning
- Centrally manage and provision audit settings



© Puget Sound Oracle Users Group
Education Is Our Passion

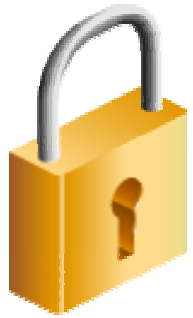
Oracle Audit Vault Reports

- User-defined reports
  - What actions did privileged users perform on the financial database?
  - What actions did user A perform across multiple databases?
  - Who accessed sensitive data?
- Custom reports
  - Oracle BI Publisher and Application Express
  - Third-party tools

© Puget Sound Oracle Users Group
Education Is Our Passion

Security

- Protected with built-in security
  - Encrypted audit data transmission
  - Separation of duty: Audit Vault Administrator and Audit Vault Auditor
- Protected using:
  - Oracle Database Vault
  - Oracle Advanced Security



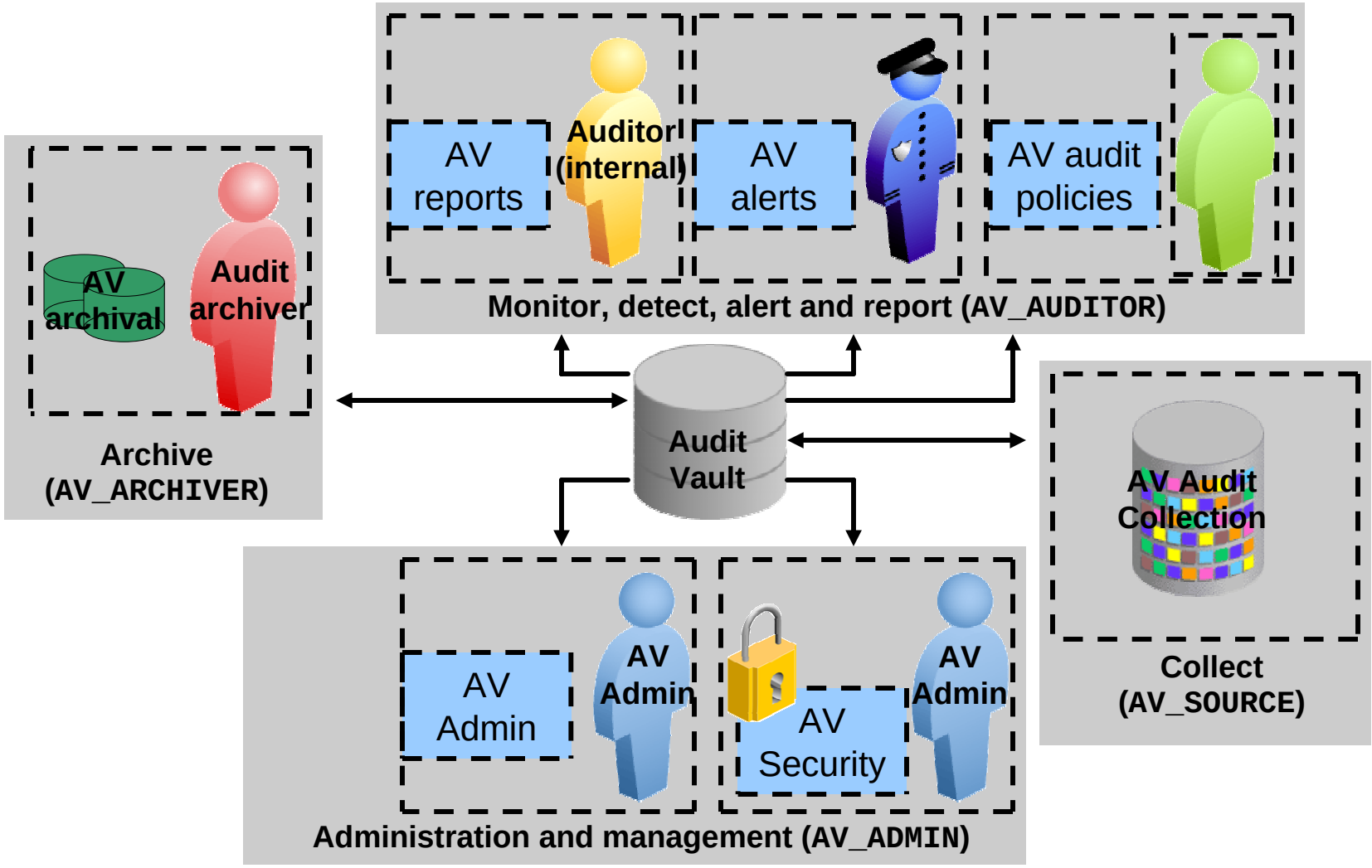
© Puget Sound Oracle Users Group
Education Is Our Passion

Separation of Duties

- Assign responsibilities to roles not people
- Manages conflict of interest policy
- Reduces chances of fraud
- Spreads critical duties across roles and in turn users
- Proposed NIST Standard for Role-Based Access Control (2001)
  - Users, roles, permissions, operations, objects
  - Core and Hierarchical RBAC
  - Separation of duties
  - Administrative functions, supportive System functions, review functions
- ANSI/INCITS 359 - 2004

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault's Separation of Duties



© Puget Sound Oracle Users Group
Education Is Our Passion

Administrator Roles

Role	When Granted	Granted To	Description
AV_ADMIN	During Server Installation	Audit Vault Administrator	Accesses Oracle Audit Vault services to administer, configure, and manage a running Oracle Audit Vault system. A user granted this role configures and manages audit sources, agents, collectors, the setup of the source with the agent, and the warehouse.
AV_AUDITOR	Server Installation	Audit Vault Auditor	Accesses Audit Vault reporting and analysis services to monitor components, detect security risks, create and evaluate alert scenarios, create detail and summary reports of events across systems, and manage the reports. A user granted this role manages central audit settings and alerts. This user also uses the data warehouse services to further analyze the audit data to assist in looking for trends, intrusions, anomalies, and other items of interest. A user is created and granted this role during the Audit Vault Server installation.
AV_AGENT	Before Agent Installation	Audit Vault Agent Owner	Manages agents and collectors by starting, stopping, and resetting them. A user is created and granted this role prior to an agent installation. A user is created and granted this role prior to an agent installation. The Audit Vault Agent software uses this role at run time to query Oracle Audit Vault for configuration information.

© Puget Sound Oracle Users Group
Education Is Our Passion

Administrator Roles

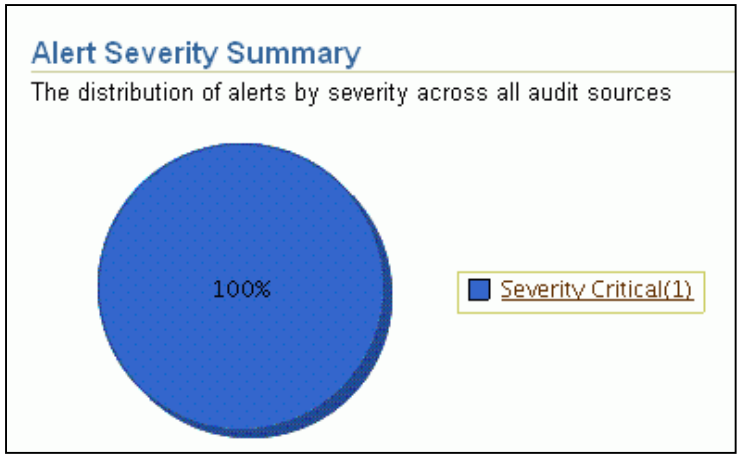
Role	When Granted	Granted To	Description
AV_SOURCE	Before Source Registration	Source User	Manages the setup of sources for audit data collection.
AV_ARCHIVER	Before archiving audit data	SYS	Archives and deletes audit data from Audit Vault and cleans up old unused metadata and alerts that have already been processed. A user granted this role can archive raw audit data.
DV_OWNER	During Server Installation	AVOWNER and DVSYS	Manages database roles and configuration.
DV_ACCTMGR	During Server Installation	AVACCTMGR and DVSYS	Manages database user accounts. Only the user granted this role can create Audit Vault administrator users.

```
SELECT *
FROM dba_role_privs
WHERE (granted_role LIKE 'AV%'
OR granted_role LIKE 'DV%')
ORDER BY 2,1;
```

© Puget Sound Oracle Users Group
Education Is Our Passion

Alerts Early Detection with Alerting

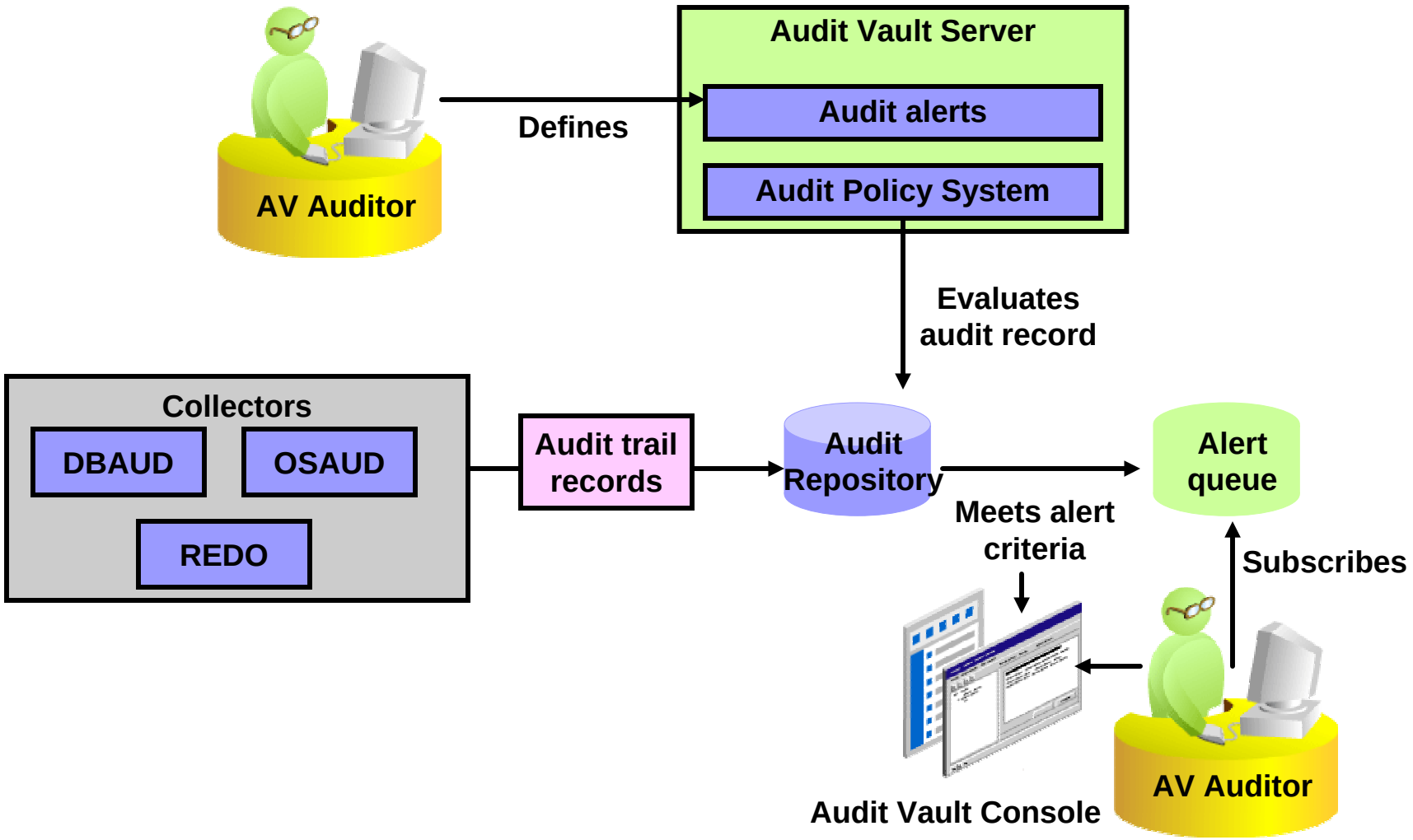
- Alerts can be defined for:
  - Viewing sensitive columns
  - Creating users
  - Granting of roles
  - DBA grants on all systems
  - Failed application logins



- Alerts are evaluated on incoming audit data
- Alert reports can be generated for suspicious activity

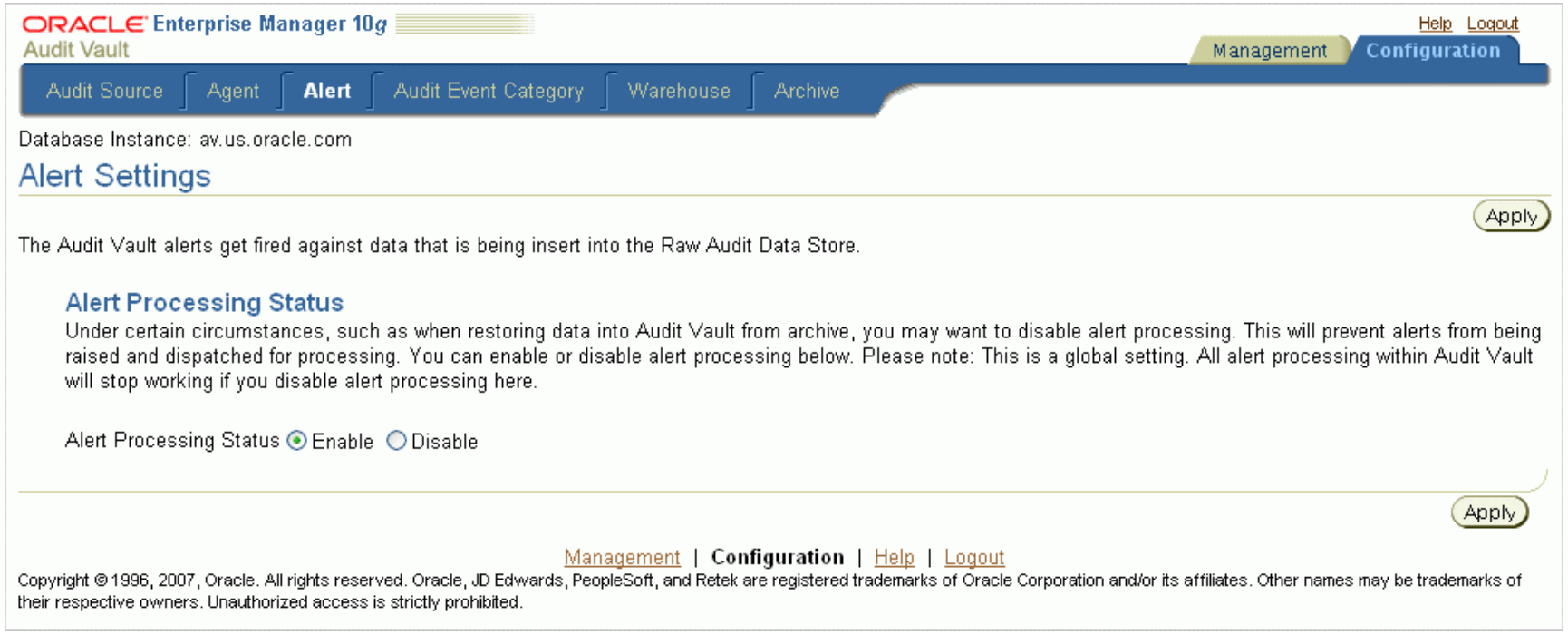
© Puget Sound Oracle Users Group
Education Is Our Passion

Alert Processing



© Puget Sound Oracle Users Group
Education Is Our Passion

Enabling and Disabling Alert Processing



© Puget Sound Oracle Users Group
Education Is Our Passion

Creating an Alert Rule

Create Alert Rule

Please provide the data for all required fields

* Alert: Access_Emp_Phone

Description: Raised when a SELECT is issued for the PHONE_NUMBER column in the HR.EMPLOYEES table

* Alert Severity: Warning

Audit Source Type: ORCLDB

Audit Source: ORCL.ORACLE.COM

Audit Event Category: DATA ACCESS

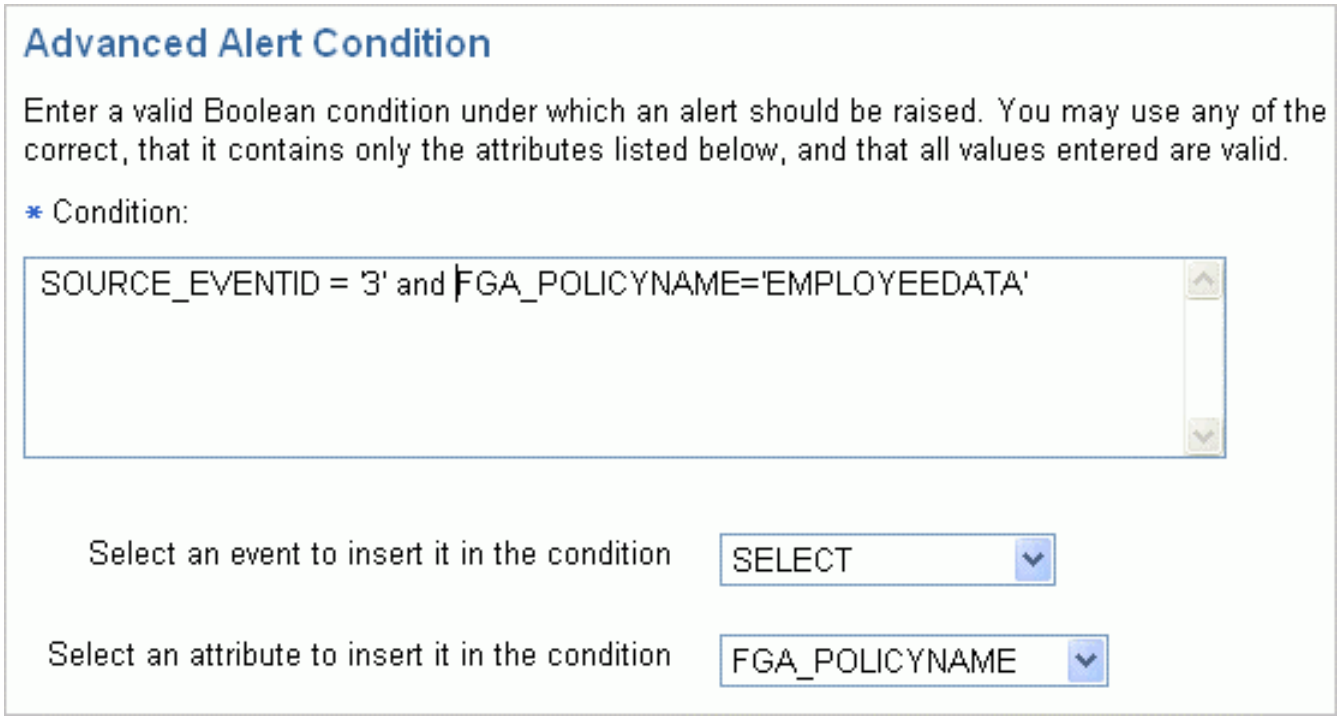
Specify additional alert conditions in: Basic / Advanced

© Puget Sound Oracle Users Group
Education Is Our Passion

Specifying the Basic Alert Condition

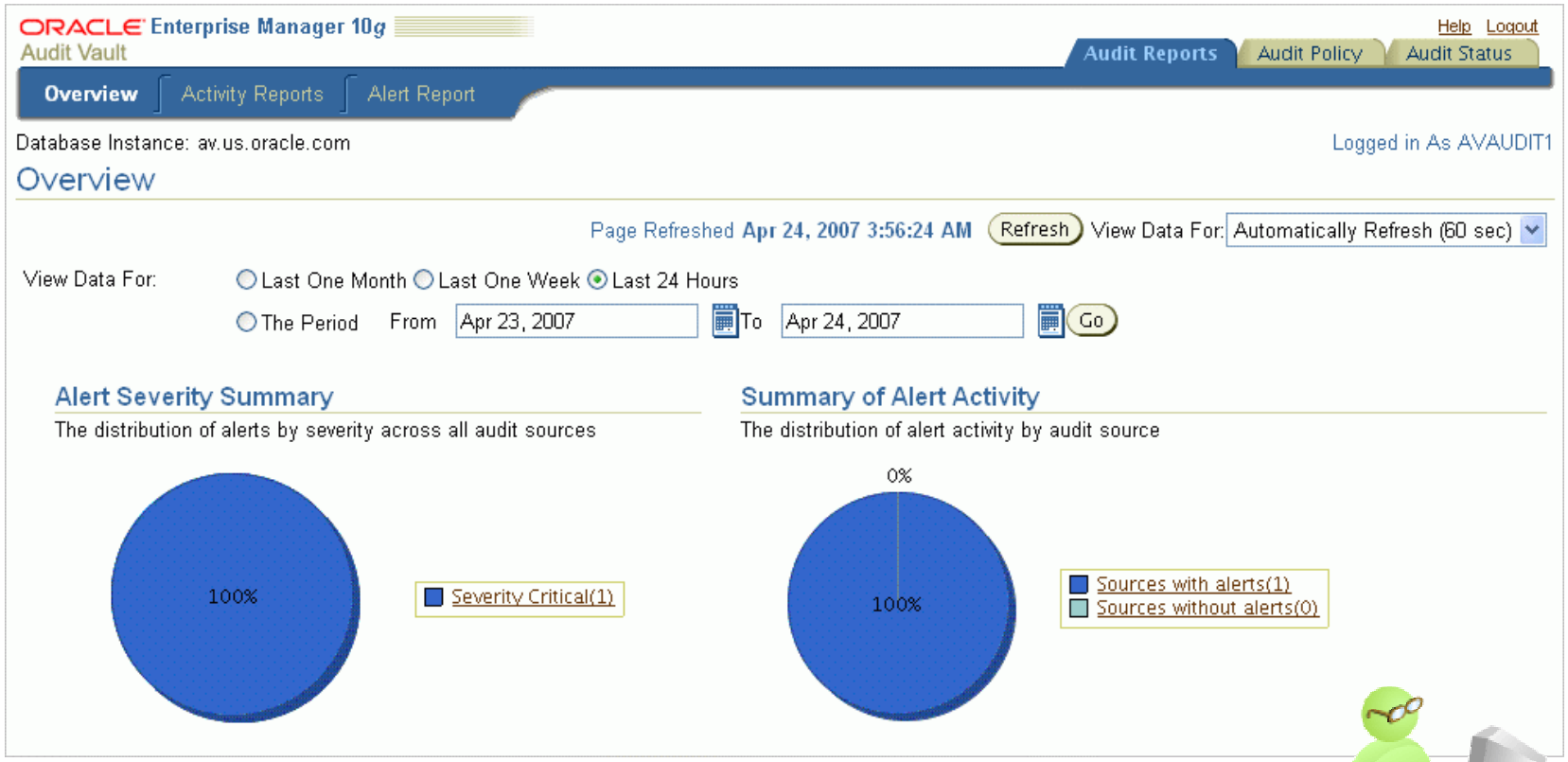
© Puget Sound Oracle Users Group
Education Is Our Passion

Specifying an Advanced Alert Condition



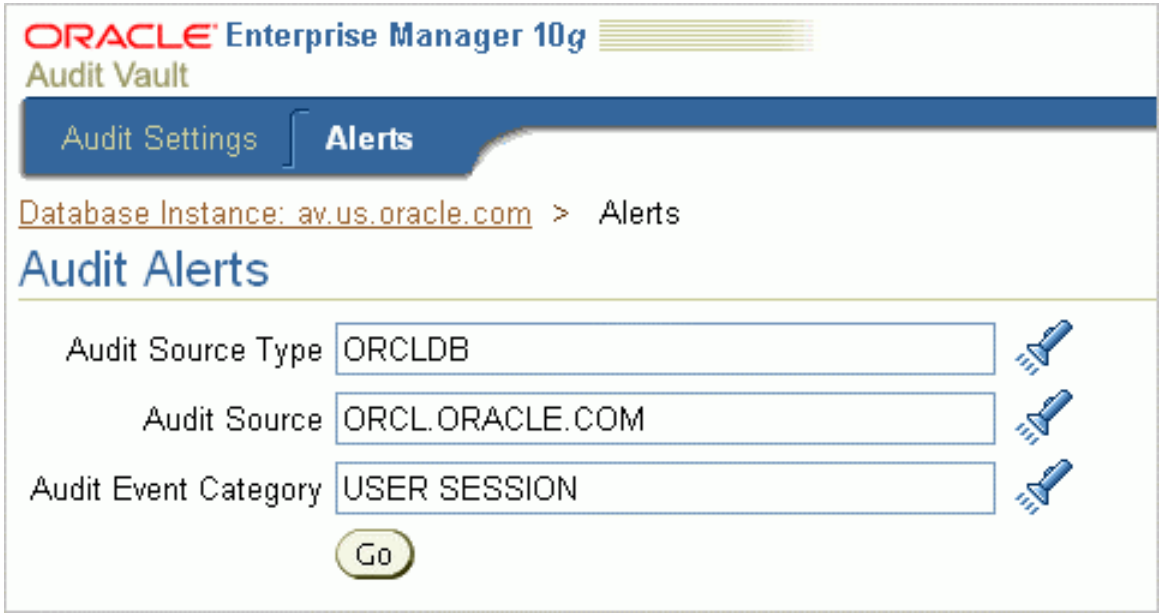
© Puget Sound Oracle Users Group
Education Is Our Passion

Viewing Alert information



© Puget Sound Oracle Users Group
Education Is Our Passion

Viewing Audit Alerts



© Puget Sound Oracle Users Group
Education Is Our Passion

Viewing Audit Alerts: Support

- AQ tables
  - When an alert is triggered, it is placed on the AVSYS.AV_ALERT_QUE
  - The AQ interface provides a number of mechanisms to send email/text messages when an alert is triggered
    - JMS : sample code
    - PL/SQL : sample code
    - DB Control : looking into integrating with the built in alert system

© Puget Sound Oracle Users Group
Education Is Our Passion

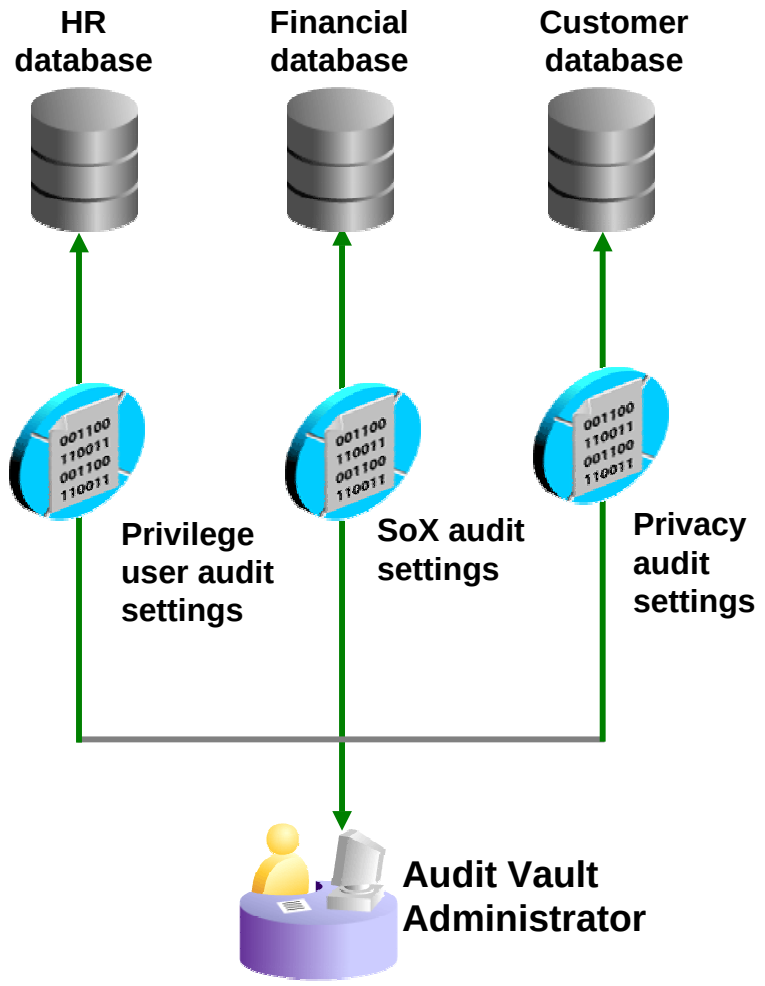
Scalable and Flexible Data Warehouse

- Audit data warehouse
  - Enables business intelligence and analysis
  - Enables reporting
- Audit data warehouse dimensions
  - Time, host, source, user, and event
  - Schema documented and published
  - Allows third-party reporting tools
- Performance and scalability
  - Built-in partitioning
  - Scales to terabytes
- Oracle RAC certified

© Puget Sound Oracle Users Group
Education Is Our Passion

Centralized Management of Audit Policies

- Collection of database audit settings
- Compare against existing audit settings on source
- Provision audit settings centrally
- Demonstrate compliance



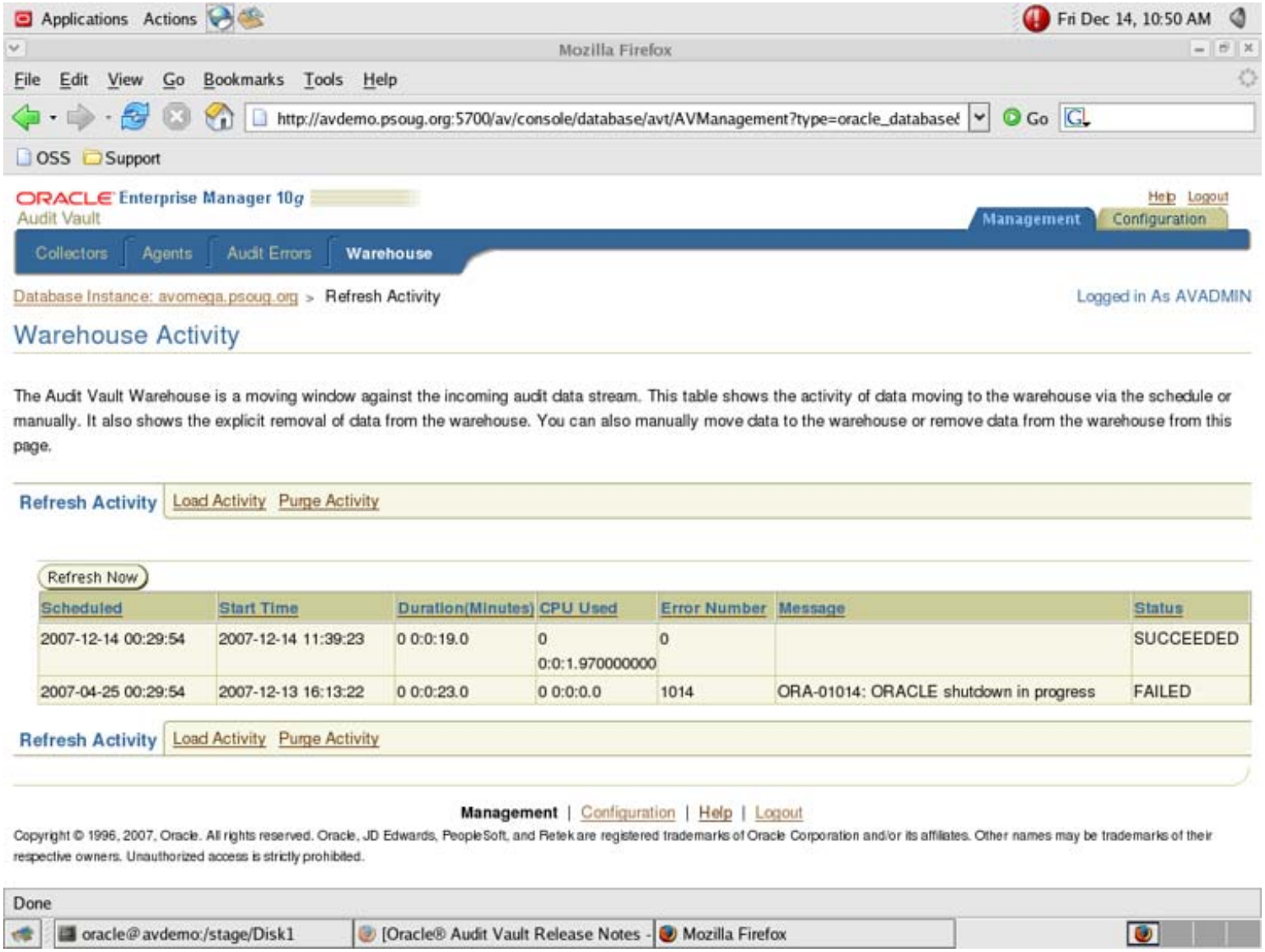
© Puget Sound Oracle Users Group
Education Is Our Passion

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault User Interface

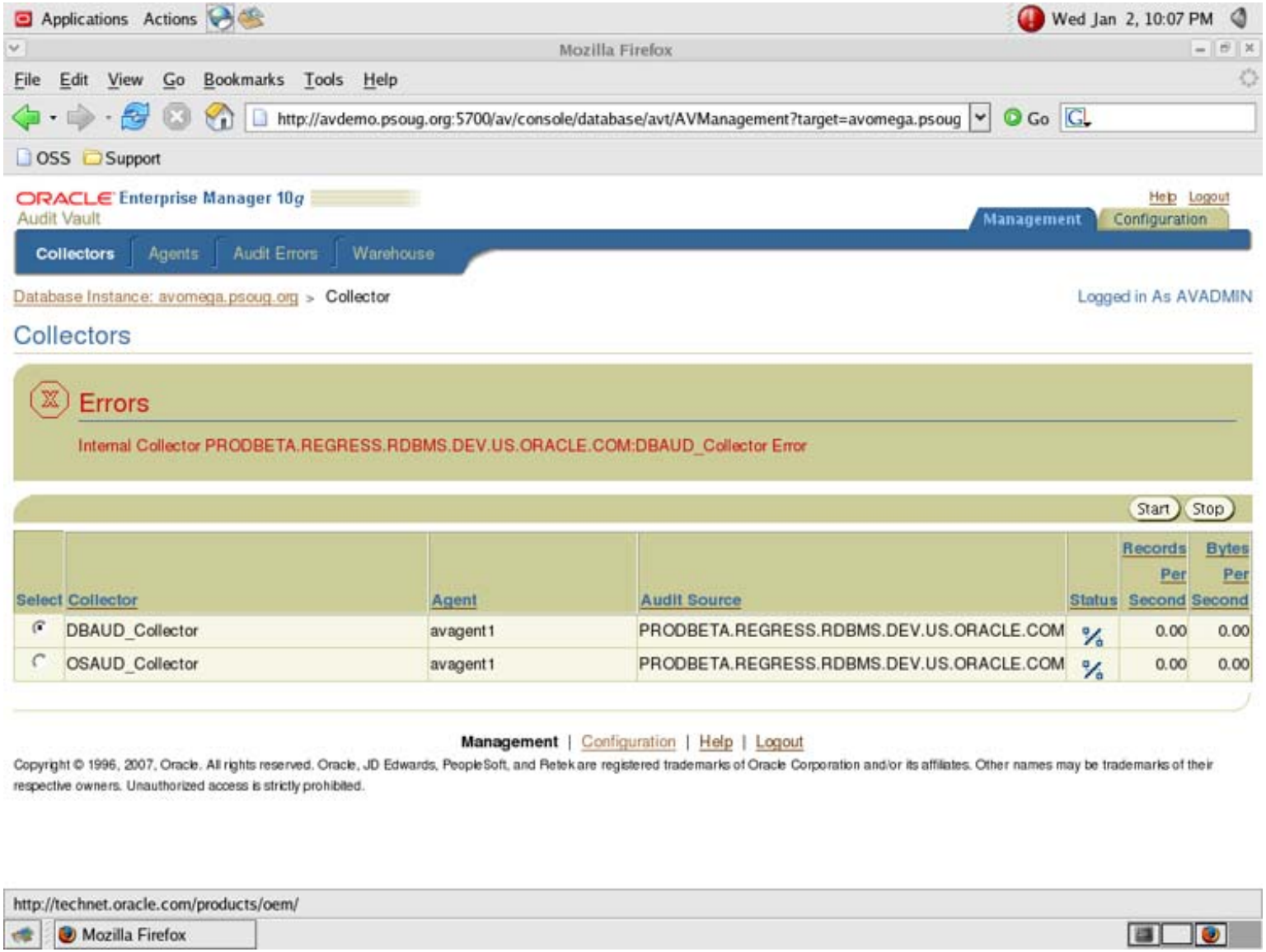
© Puget Sound Oracle Users Group

Live Demo



© Puget Sound Oracle Users Group
Education Is Our Passion

Not So Live Demo



© Puget Sound Oracle Users Group
Education Is Our Passion

Oracle Audit Vault Reports: Overview

- Out-of-the-box reports
  - Privileged user activity
  - Access to sensitive data
  - Role granting
  - DDL activity
  - Log in and log out

ORACLE Enterprise Manager 10g
Audit Vault

Overview | Activity Reports | Alert Report

Database Instance: av > Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

Privileged Users Activity - Past 24 Hours: JTAYLOR, SYSTEM, SYS

Privileged user activity over the past 24 hours: JTAYLOR, SYSTEM, SYS

Audit Source	User	Audit Event Category	Audit Event	Object	Client Host
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP2	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	ALTER TABLE	JTAYLOR.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	CREATE TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	OBJECT MANAGEMENT	DROP TABLE	SCOTT.EMP1	vipshah-lap2
VMSSRC2.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	JTAYLOR	DATA ACCESS	SELECT	SH.SALES	raclinux1.us.oracle.com
ORCL.US.ORACLE.COM	JTAYLOR	USER SESSION	LOGON		raclinux1.us.oracle.com
VMSSRC2.ORACLE.COM	SYS	USER SESSION	LOGON		vipshah-lap2
ORCL.US.ORACLE.COM	sys	USER SESSION	SUPER USER LOGON		
ORCL.US.ORACLE.COM	/	USER SESSION	SUPER USER		

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Auditing

© Puget Sound Oracle Users Group

Event Categories

Event Category Name	Description
ACCOUNT MANAGEMENT	Management of user/service accounts and profiles
APPLICATION MANAGEMENT	Management of applications or code on a system
AUDIT COMMAND	Management of Audit service
DATA ACCESS	Association with a data item or resource for its content or services
EXCEPTION	Error conditions or exceptional events
INVALID AUDIT RECORD	Collection of an invalid audit record
OBJECT MANAGEMENT	Creation and management of data items and resource elements

© Puget Sound Oracle Users Group
Education Is Our Passion

Specifying Event Categories

Event Category Name	Description
PEER ASSOCIATION	Management of association with peer systems (DBLINKs)
ROLE AND PRIVILEGE MANAGEMENT	Management of roles and privileges granted to users or services
SERVICE AND APPLICATION ACCESS	Use of services or applications
SYSTEM MANAGEMENT	Management of services that are system level
UNKNOWN	Anything that does not belong to the other categories
USER SESSION	Creation and use of user sessions on the system

© Puget Sound Oracle Users Group
Education Is Our Passion

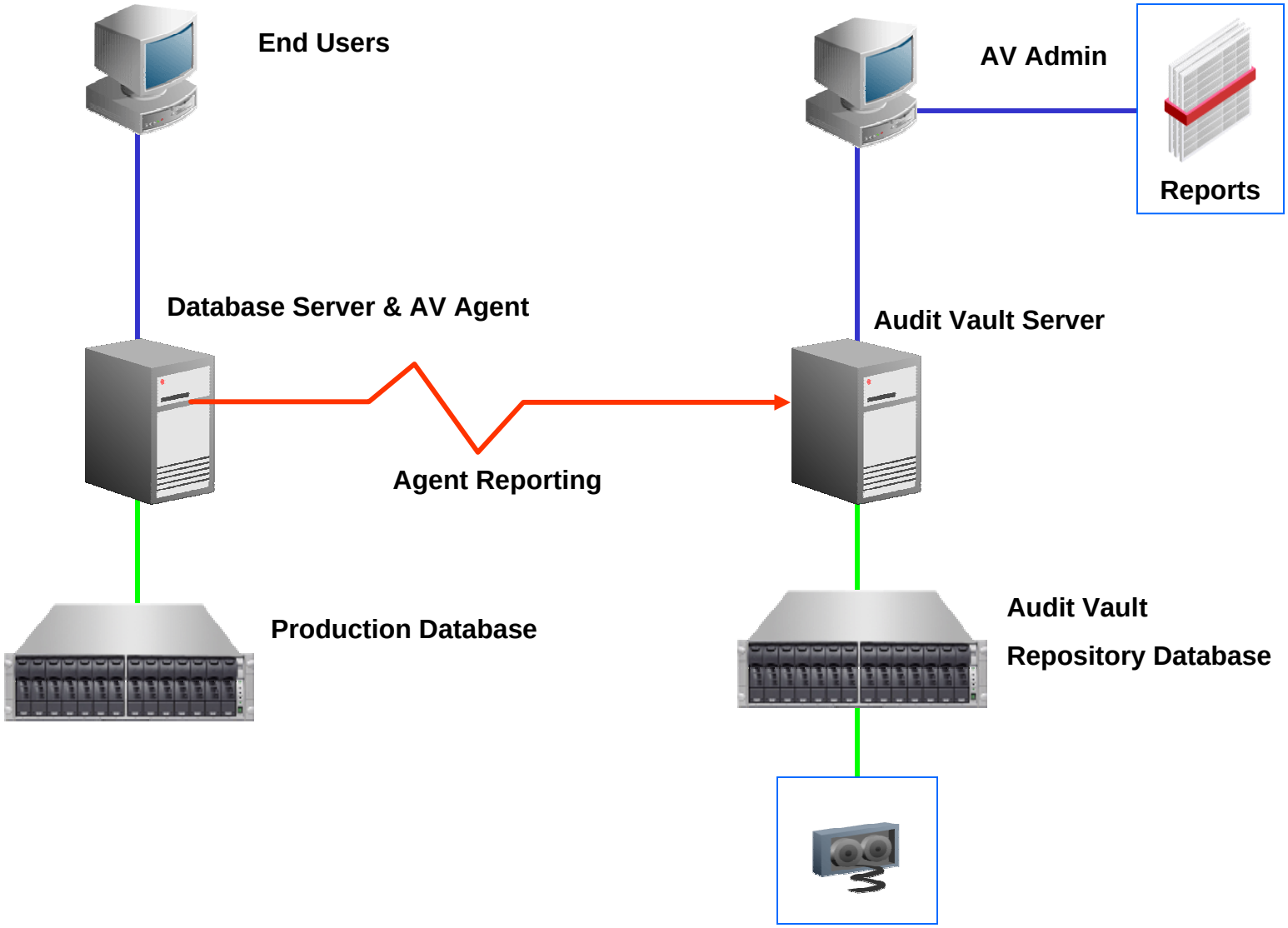
Audit Vault Live Demo
Enterprise Manager 10g

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Architecture

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Architecture (5,000 ft.)



© Puget Sound Oracle Users Group
Education Is Our Passion

Server Requirements

- Size Server Based on Insert Rate
  - 2-CPU Linux host with 4G of memory
  - 17,000 inserts/second

Available RAM	Swap Space Required
1 – 2 GB	1.5X amount of RAM
2 – 8 GB	Equal to amount of RAM
More than 8 GB	0.75X amount of RAM

© Puget Sound Oracle Users Group
Education Is Our Passion

Server Requirements

- 1.5GB disk space for Audit Vault data files
- 1.4GB disk space for Audit Vault Server software files in the Oracle base directory
- 700MB of additional disk space for the Audit Vault database files in the Oracle base directory
- 400MB disk space in /tmp
- 300 MB for every 500,000 audit trail records
- May be installed on top of ASM
- May be installed (Advanced install) on RAC

© Puget Sound Oracle Users Group
Education Is Our Passion

Agent Requirements

- Audit Vault Agent disk space requirements (platform dependent)
  - 450 MB of disk space for the Audit Vault Agent software on Linux
  - 1 GB on AIX
- If you have a target database installed you probably have sufficient resources

© Puget Sound Oracle Users Group
Education Is Our Passion

Platform Availability

- Linux x86 and Linux x64 on RedHat 3.0/4.0, RedHat EL 4.0, Suse Linux ES 9.0/10
- Sun Sparc64 on Solaris 5.9/5.10
- HP PA RISC on HPUX 11.11, 11.23
- HP UX Itanium
- IBM AIX 5L on 5.2, 5.3
- Microsoft Windows 32 bit

© Puget Sound Oracle Users Group
Education Is Our Passion

Oracle Audit Vault Components

- Oracle Audit Vault consists of:
  - Audit Vault Server
    - Oracle Database repository for audit events
    - Audit Vault Console
    - Services
  - Audit Vault Agent
    - Oracle Database client
    - Oracle Application Server Container for J2EE (OC4J)
    - Audit Vault Agent management services
    - Audit data collectors for Oracle Database

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Server

- Audit Event Repository
- Audit Vault Console
- Audit Vault Services
  - Consolidating and storing of audit data
  - Creating and managing alerts
  - Managing and monitoring collectors
  - Defining and configuring source information
  - Creating and manging reports
  - Reporting
  - Audit policy management

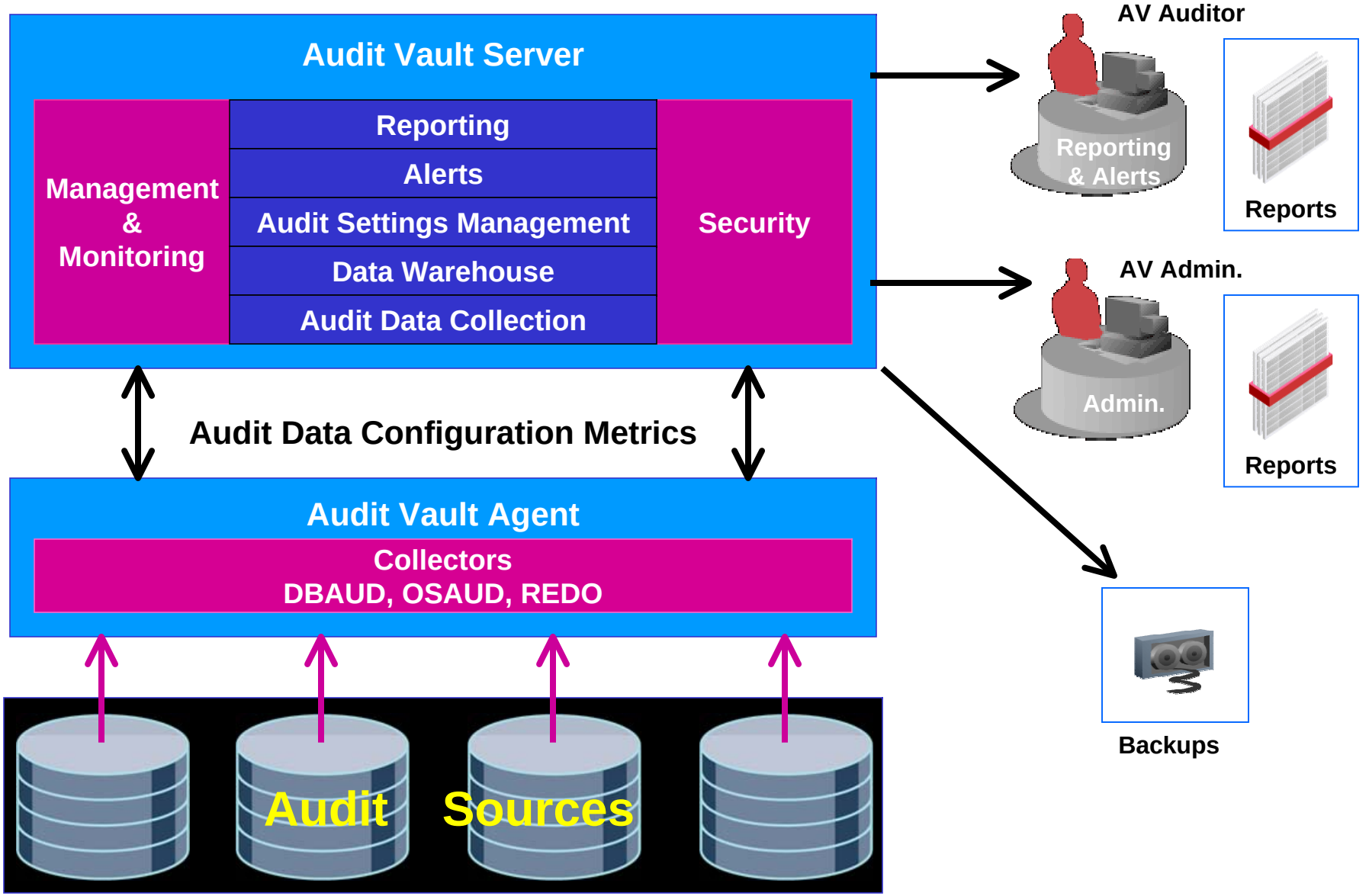
© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Agents

- Oracle Container for Java (OC4J)
- Instant Client components
- Audit Vault management services
- Audit data collectors for Oracle Database
  - Operating system audit log collection (OSAUD)
    - Requires o/s file system access
  - Database audit log collection (DBAUD)
  - Redo log collection (REDO)
- Receives configuration information using a communication channel based on OCI (AQ)
  - Can be secured with X.509 certificates

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Architecture (500 ft.)



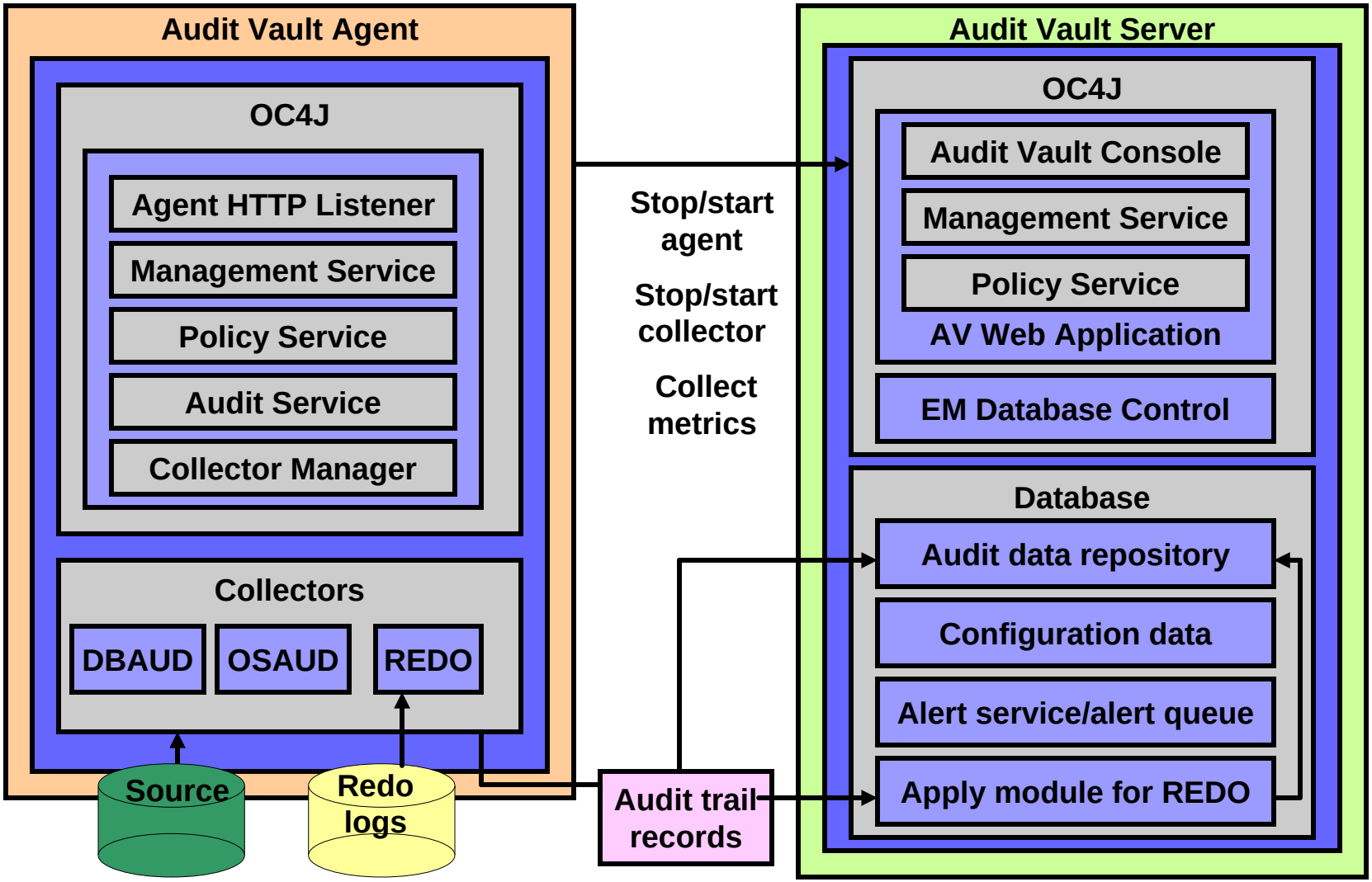
© Puget Sound Oracle Users Group
Education Is Our Passion

Services Overview

- The Audit Vault Server includes the following services:
  - Management and monitoring
  - Reporting
  - Analysis
  - Alert
  - Data warehouse
  - Audit
  - Policy
  - Configuration

© Puget Sound Oracle Users Group
Education Is Our Passion

Audit Vault Framework



© Puget Sound Oracle Users Group
Education Is Our Passion

Interfaces and Administrator Access

- Audit Vault Configuration Assistant (AVCA)
- Audit Vault Control (AVCTL)
- Audit Vault Oracle Database (AVORCLDB)

© Puget Sound Oracle Users Group
Education Is Our Passion

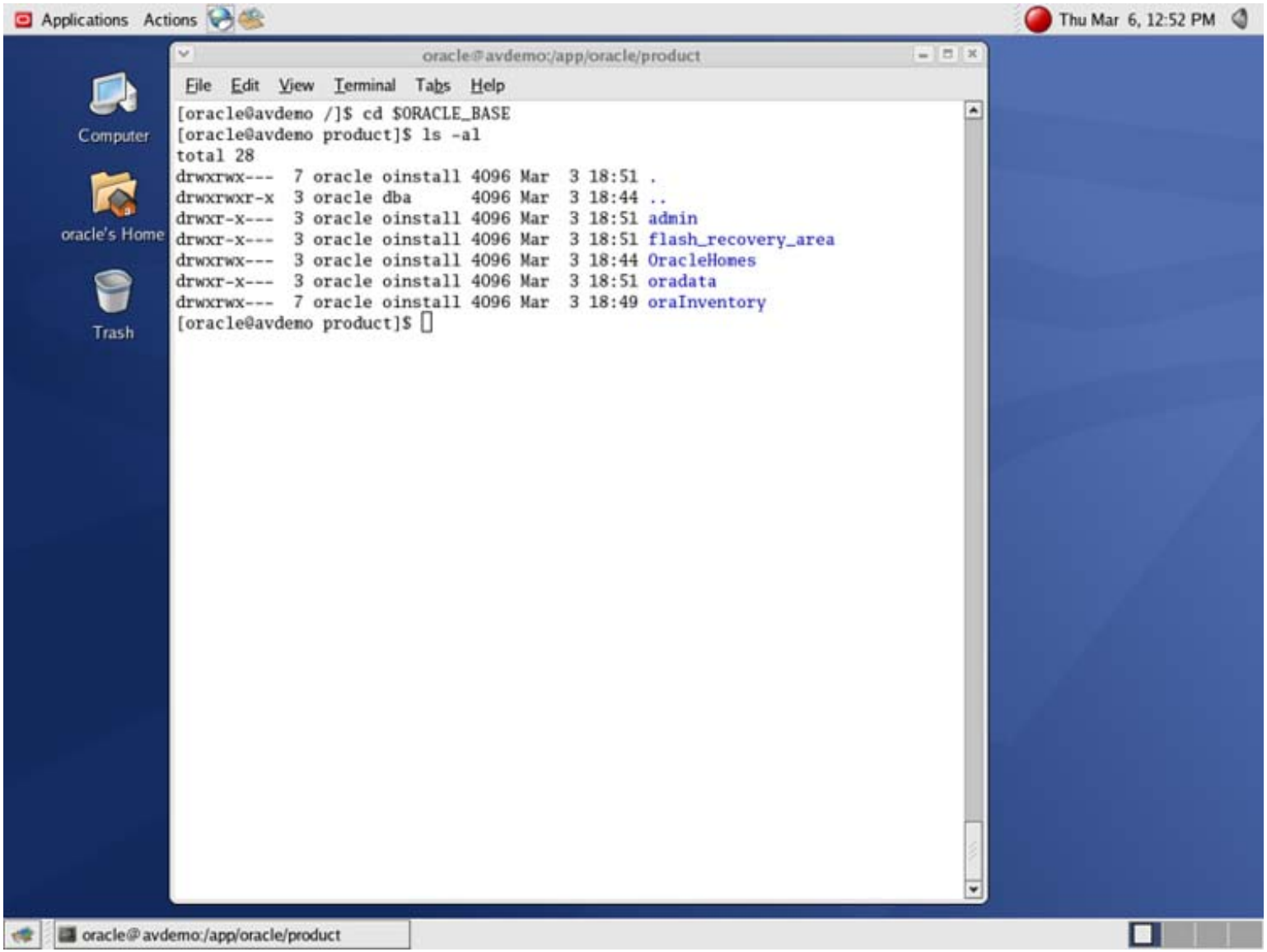
Audit Vault Walk-About

© Puget Sound Oracle Users Group
Education Is Our Passion

- cd $ORACLE_BASE
- cd $ORACLE_HOME
- cd $ORACLE_HOME/av
- cd $ORACLE_HOME/av/admin
- cd $ORACLE_HOME/av/scripts/streams/source

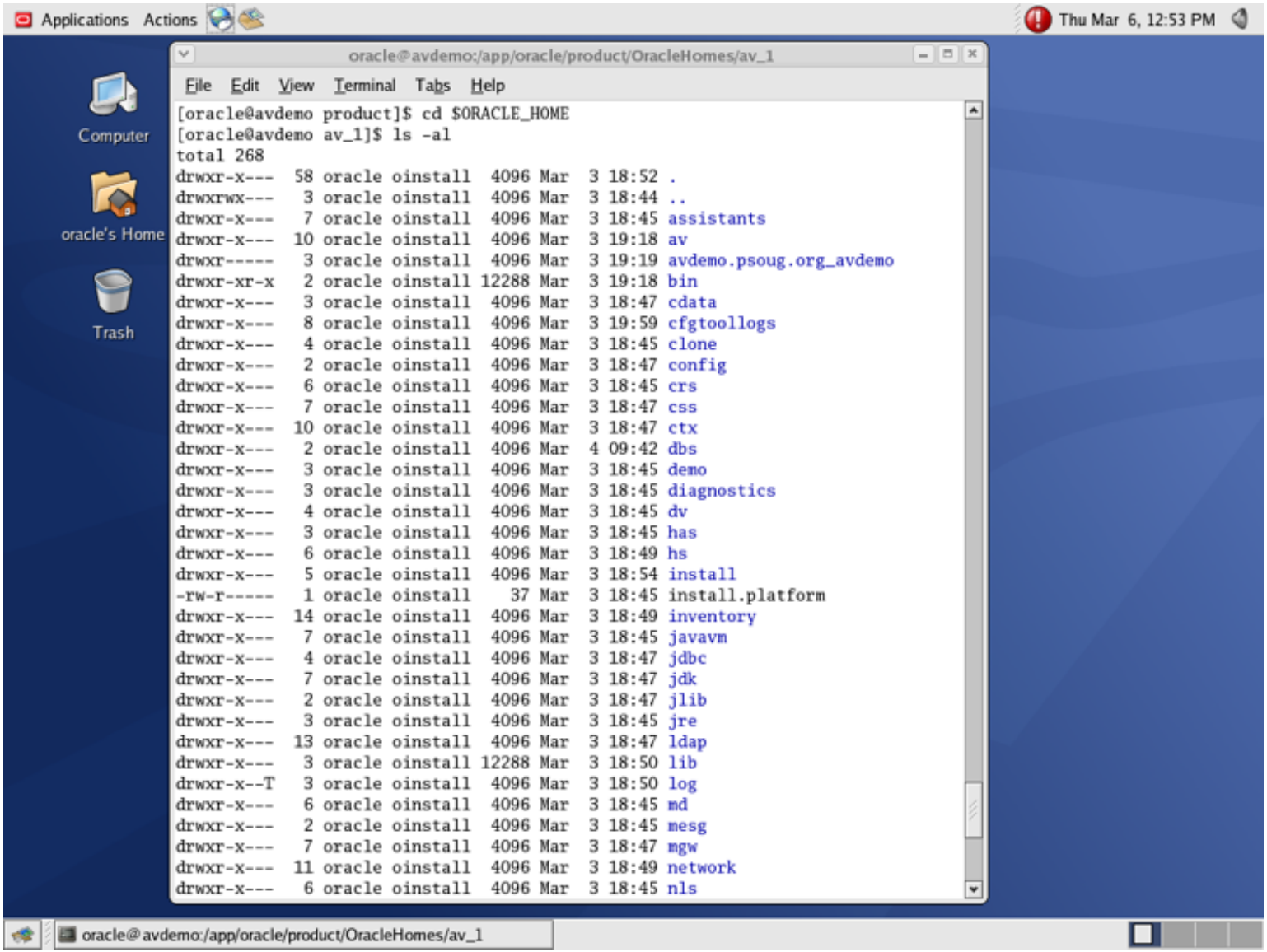
© Puget Sound Oracle Users Group
Education Is Our Passion

ORACLE_BASE



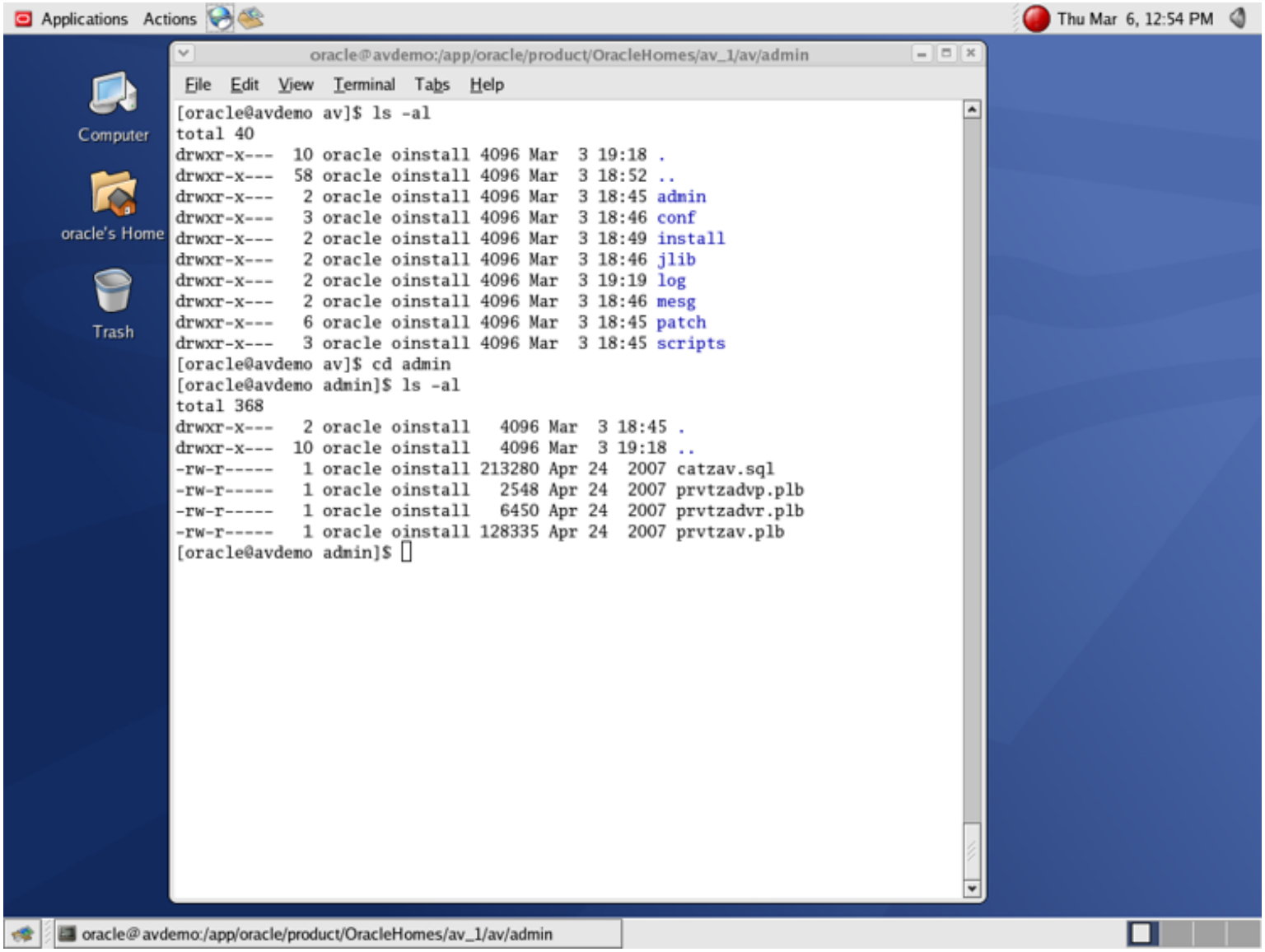
© Puget Sound Oracle Users Group
Education Is Our Passion

ORACLE_HOME



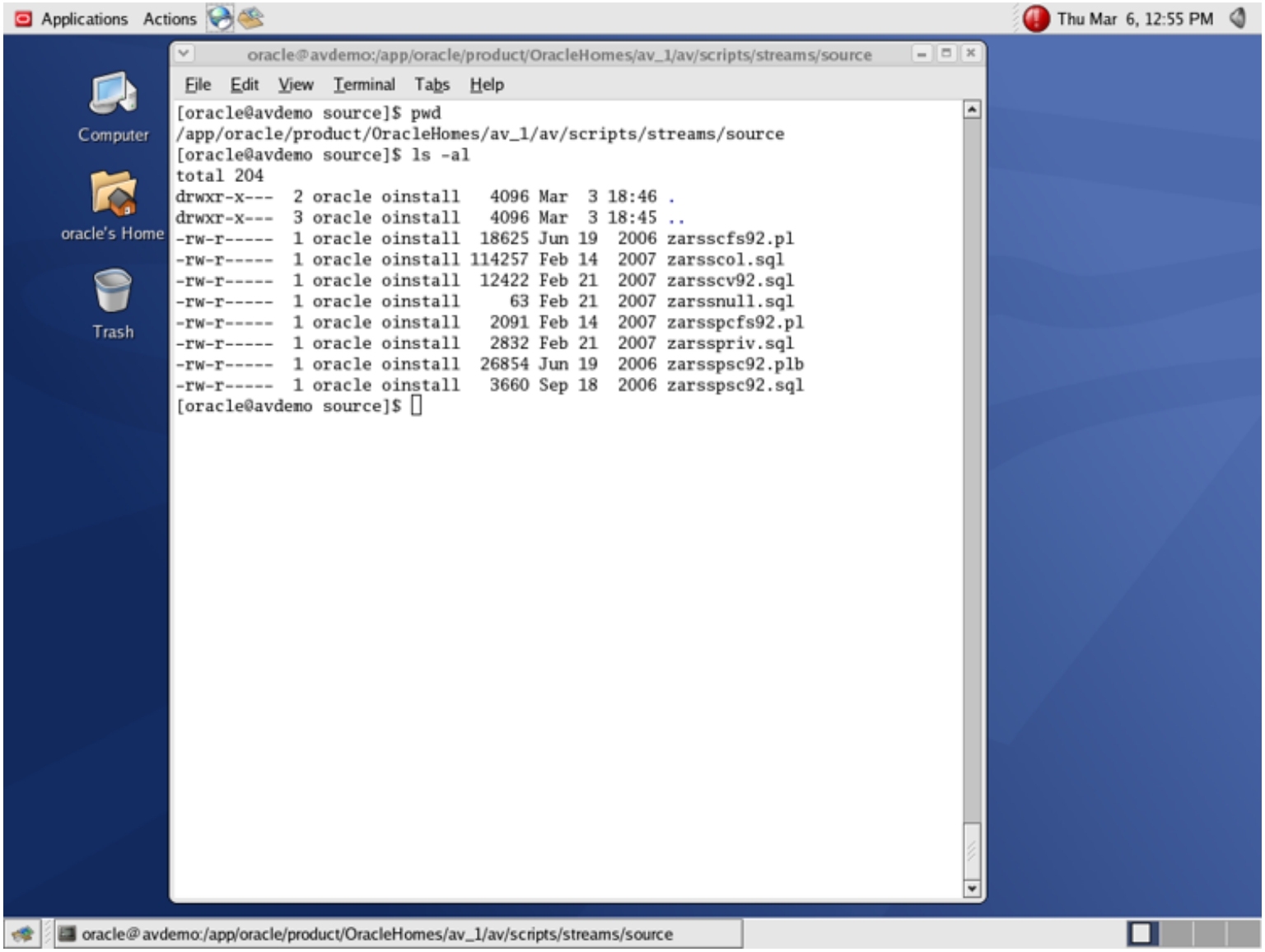
© Puget Sound Oracle Users Group
Education Is Our Passion

ORACLE_HOME/av



© Puget Sound Oracle Users Group
Education Is Our Passion

/scripts/streams/source



© Puget Sound Oracle Users Group

Audit Vault Collectors

© Puget Sound Oracle Users Group
Education Is Our Passion

Which Audit Source is Best for You?

Characteristic	OSAUD	DBAUD	REDO
Select	✓	✓	
DML	✓	✓	✓
DDL	✓	✓	✓
Before and After Values			✓
Success and Failure	✓	✓	
SQL Text	✓*	✓	
SYS Auditing	✓		✓
Other considerations	Separation of Duties	FGA data	Supplemental logging may be required for values

***SQL text is only written for sys operations**

© Puget Sound Oracle Users Group
Education Is Our Passion

Oracle Database Collectors

- DBAUD: Retrieves audit records from:
  - Database audit trail stored in `SYS.AUD$`
  - Fine-grained audit trails stored in `SYS.FGA_LOG$`
- 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

© Puget Sound Oracle Users Group
Education Is Our Passion

Protecting the Audit Trail

- Database – aud$, fga_log$
  - The DBAUD collector can extract up to 2200 records/second
  - Put a Oracle Database Vault Realm around the tables
- Oracle audit trail written to OS files
  - As a best practice the DBA should not be connecting to the host as 'oracle'
  - The OSAUD collector can extract up to 6500 records/second
- Online Logs
  - Use best practices today to protect the online logs
  - The REDO collector can extract up to 2100 records/second

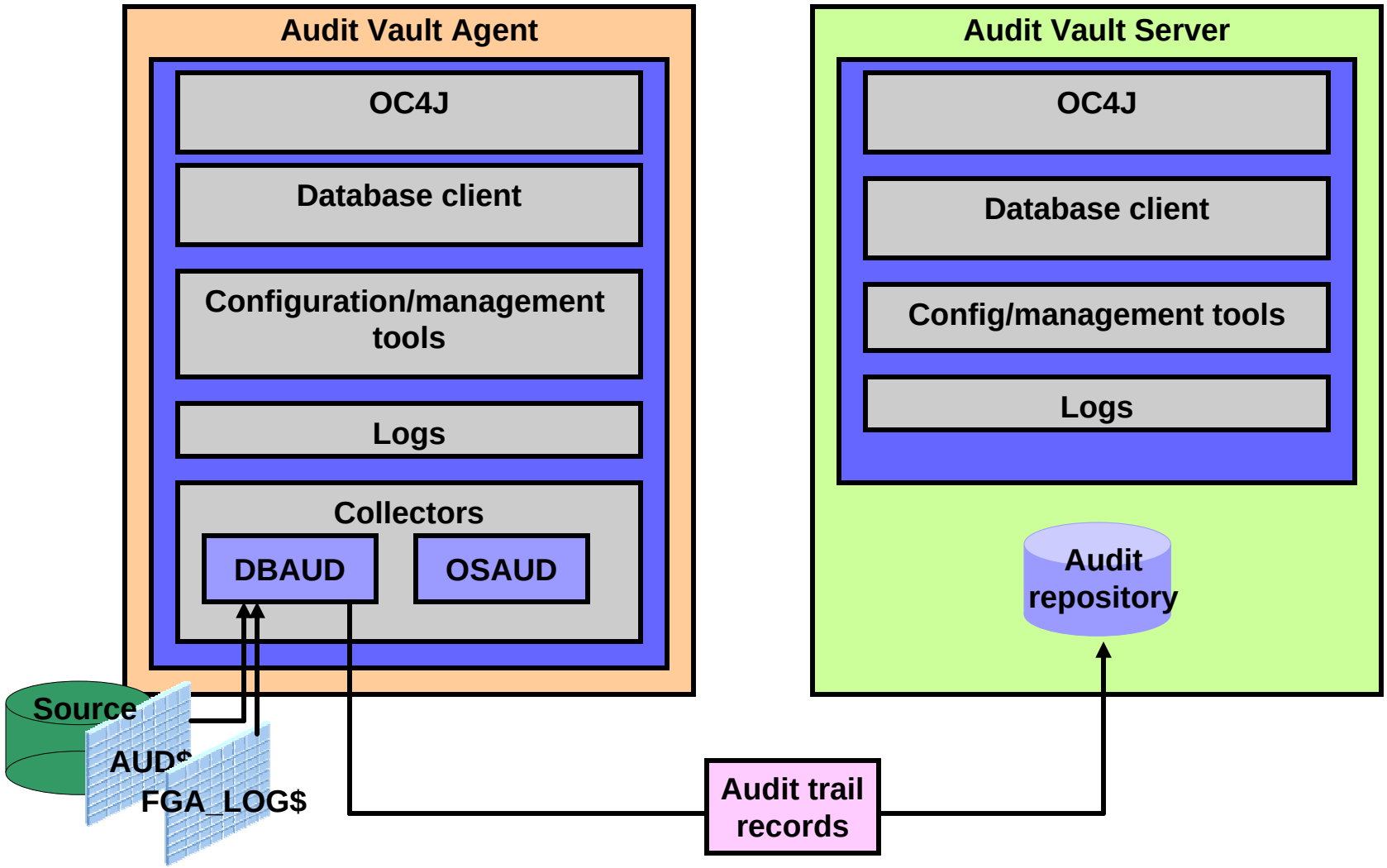
© Puget Sound Oracle Users Group
Education Is Our Passion

DBAUD Collector

- Collects audit records from the audit trail when `AUDIT_TRAIL` is set to `DB,EXTENDED`
- Collects data from the `SYS.AUD$` and `SYS.FGA_LOG$` tables
- Collects:
  - DDL and DML statements
  - SQL text
  - Successes and/or failures as specified in audit settings
- Can be remote from the source database and the Audit Vault Server
- Requires 9.2 or above

© Puget Sound Oracle Users Group
Education Is Our Passion

Oracle Database Collectors: DBAUD



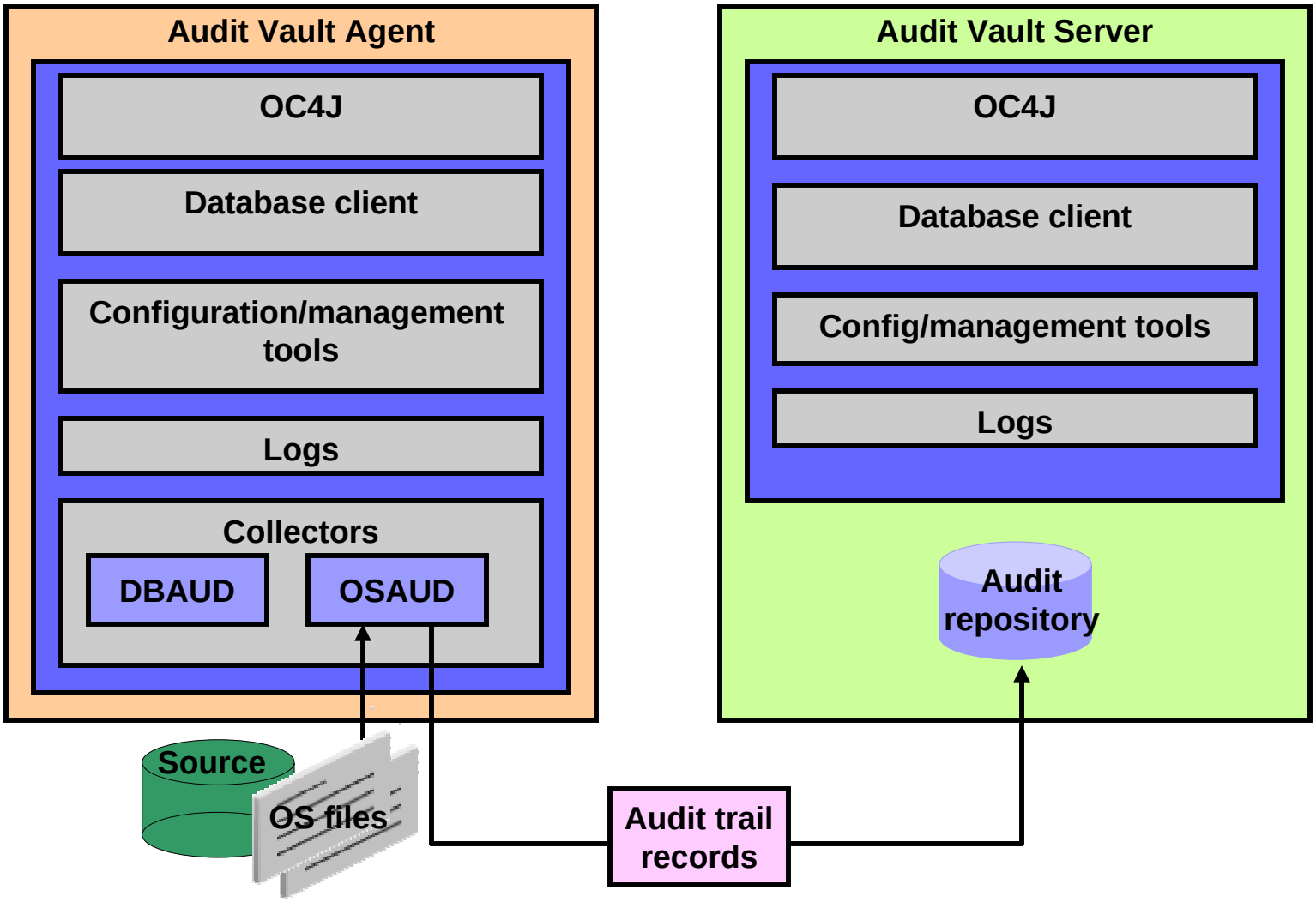
© Puget Sound Oracle Users Group
Education Is Our Passion

OSAUD Collector

- Collects audit records from the audit trail when `AUDIT_TRAIL` is set to `AUDIT_TRAIL = OS`
- Collects mandatory audit records from the operating system audit trail
- Collects:
  - DDL and DML statements
  - SYS privilege usage
  - Successes and/or failures as specified in audit settings
- Independent process running on source host
- Requires 9.2 or above

© Puget Sound Oracle Users Group
Education Is Our Passion

Oracle Database Collectors: OSAUD



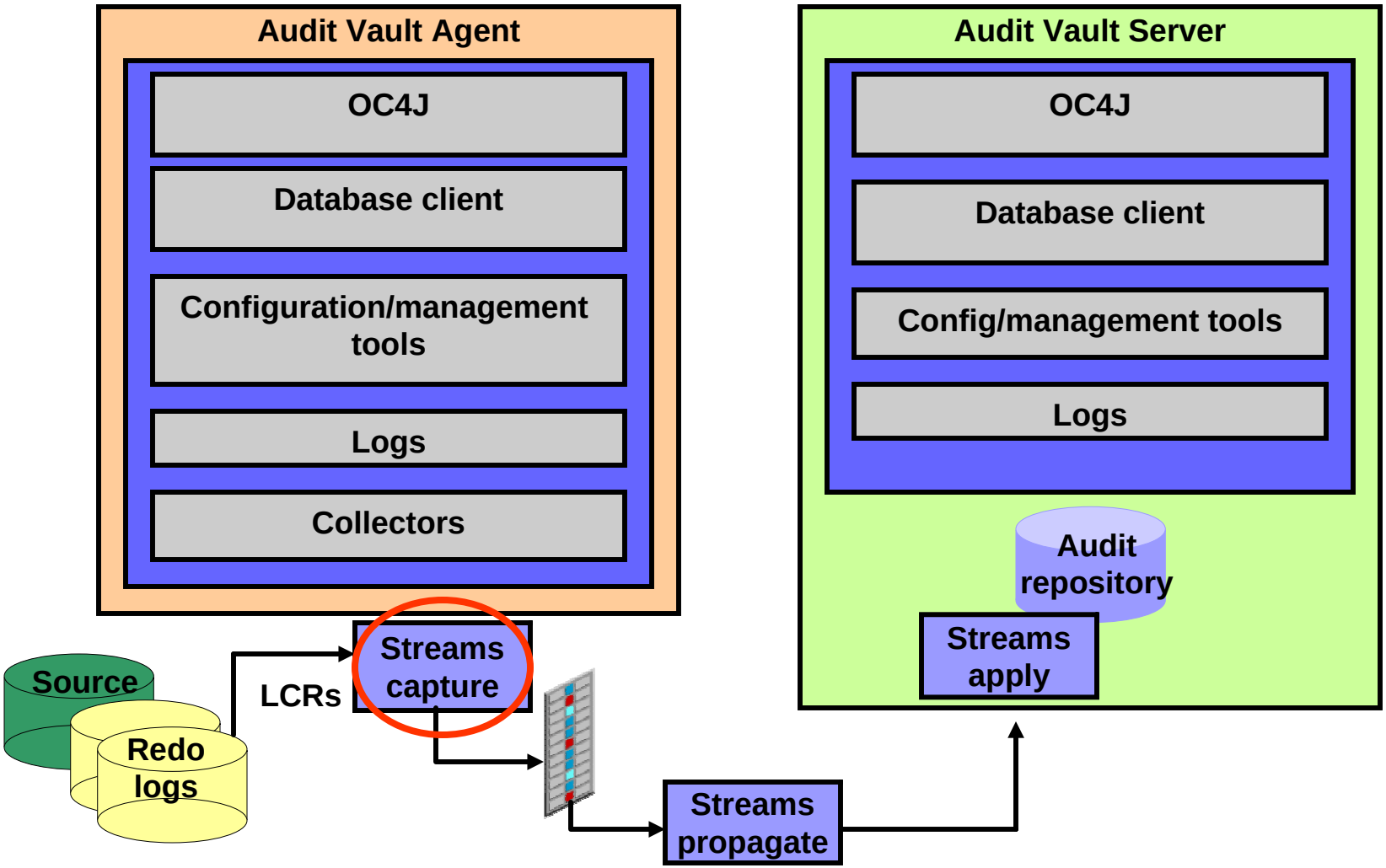
© Puget Sound Oracle Users Group
Education Is Our Passion

REDO Collector

- Uses Streams technology to retrieve logical change records (LCRs) from the redo log files
- Collects:
  - Committed DDL and DML statements
  - SYS privilege usage
  - Before-and-after values (successes only)
- Requires 10.2.0.3 or above

© Puget Sound Oracle Users Group
Education Is Our Passion

Oracle Database Collectors: REDO



© Puget Sound Oracle Users Group
Education Is Our Passion

Initialization Parameters for REDO Collectors

Parameter	Recommended Value
_SPIN_COUNT	5000
_JOB_QUEUE_INTERVAL	4 - ANY_VALUE
JOB_QUEUE_PROCESSES	4 - ANY_VALUE
SGA_MAX_SIZE	209715200 - ANY_VALUE
SGA_TARGET	209715200 - ANY_VALUE
UNDO_RETENTION	3600 - ANY_VALUE
GLOBAL_NAMES	TRUE

© Puget Sound Oracle Users Group
Education Is Our Passion

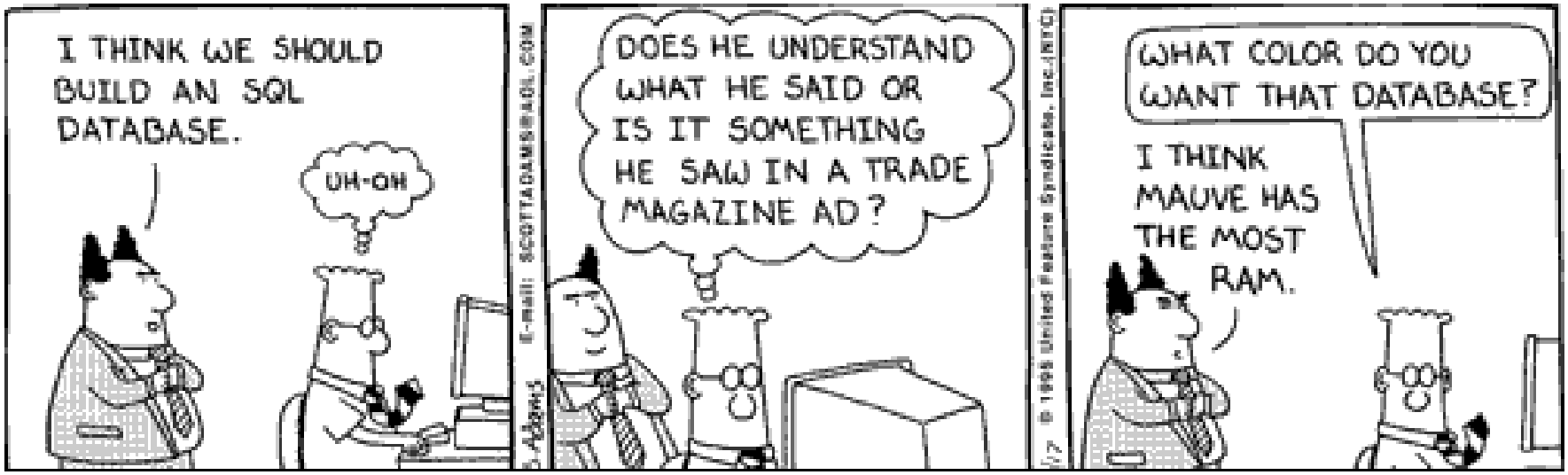
CPU Overhead (Nothing Is Free)

	10 audit/sec		100 audit/sec		1000 audit/sec	
	Create;	Collect	Create;	Collect	Create;	Collect
OS Log	0.08%	0.70%	0.15%	2.70%	1.4%	10.80%
DB Audit	0.13%	0.50%	1.60%	3.40%	21.3%	22.93%
Redo	0.00%	3.70%	0.00%	8.20%	0.0	20.40%

© Puget Sound Oracle Users Group
Education Is Our Passion

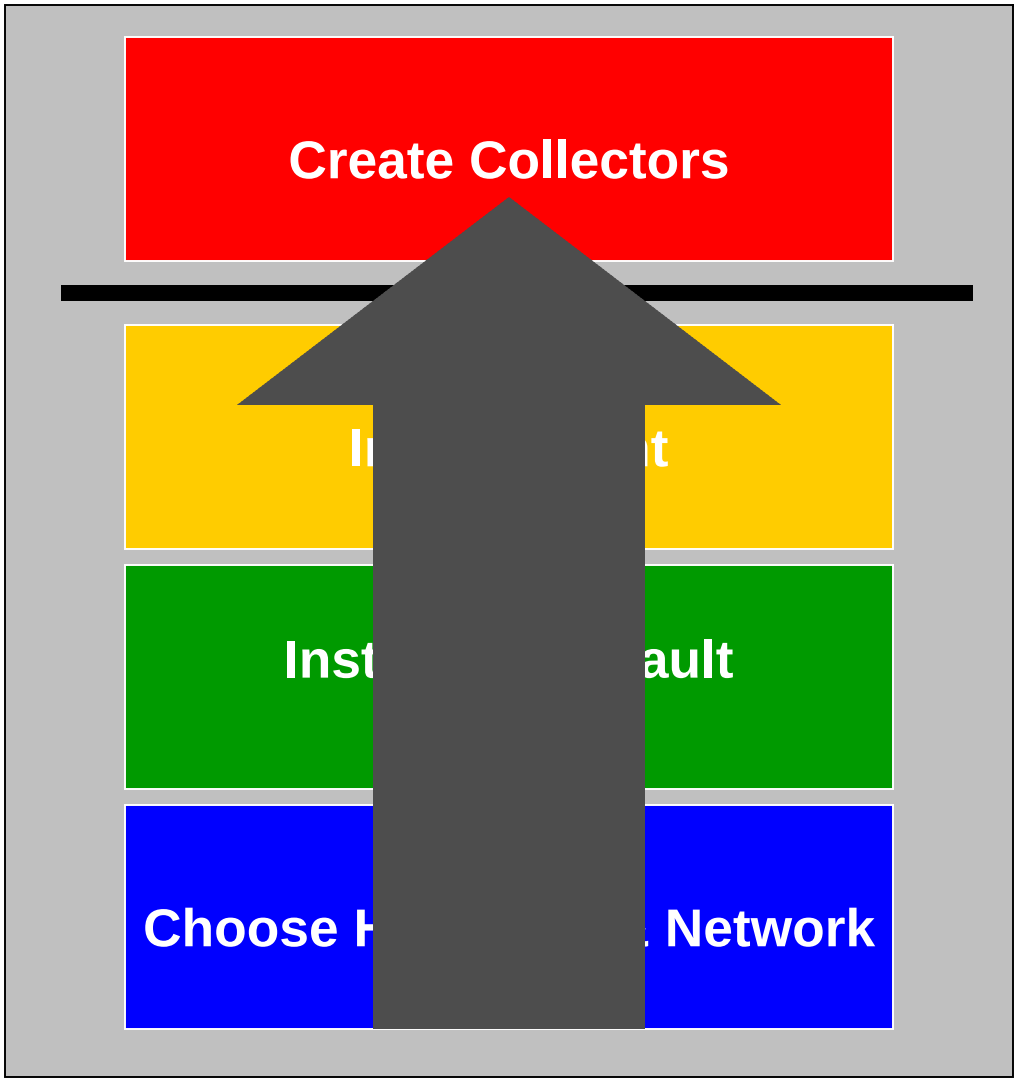
Audit Vault Installation

© Puget Sound Oracle Users Group
Education Is Our Passion



© Puget Sound Oracle Users Group
Education Is Our Passion

The “Black Line”



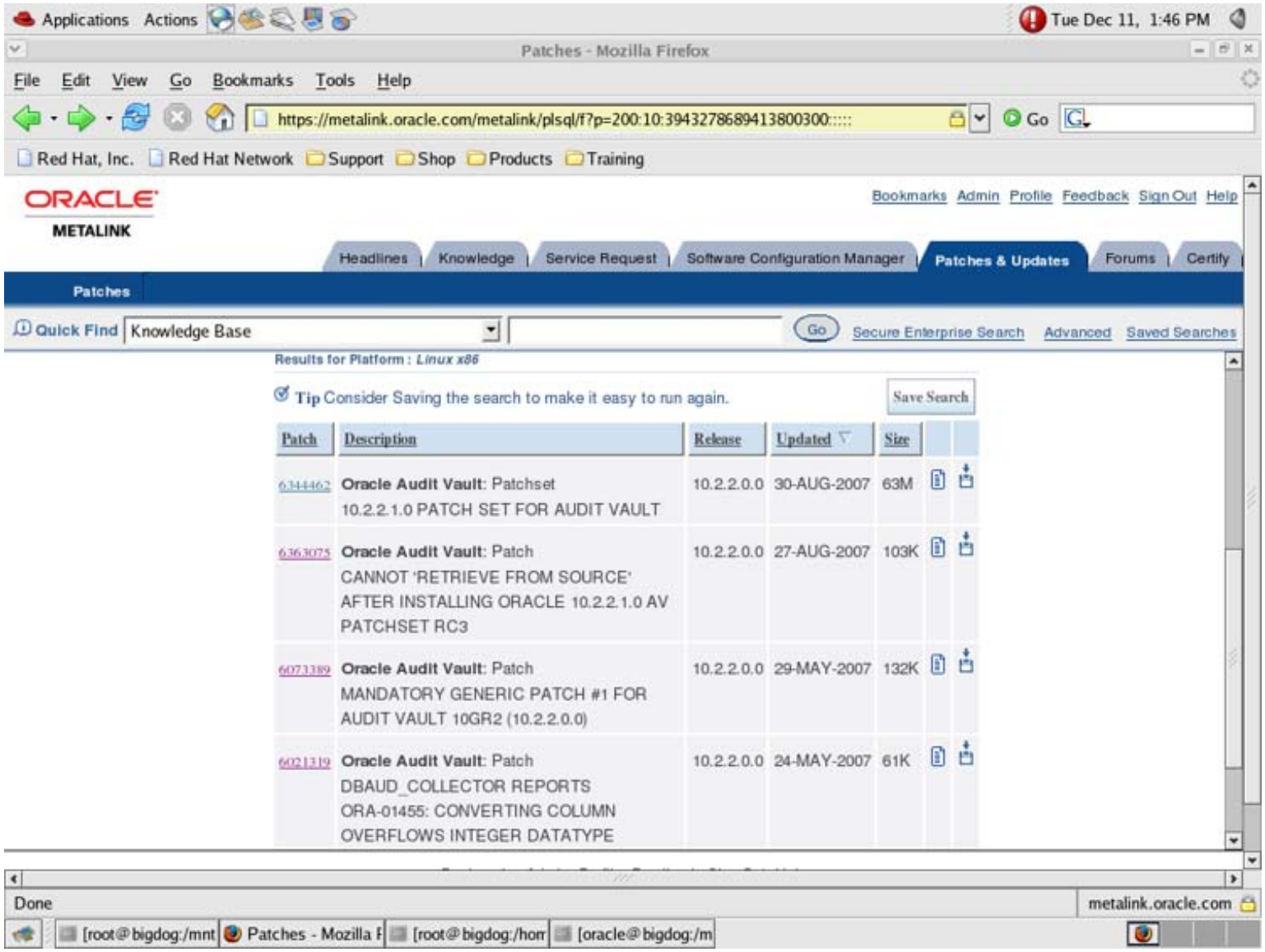
© Puget Sound Oracle Users Group
Education Is Our Passion

Steps

- Audit Vault Server
  - Operating System Installation & Configuration
  - Audit Vault Server Installation
  - Apply Patch (10.2.2.0 to 10.2.2.1)
  - Create Agent Consumer
- Audit Vault Source (Target)
  - Install Oracle Database
  - Set Up Auditing
  - Install Agent
  - Patch Agent
- Create Collectors
- Set Up Auditing & Reports

© Puget Sound Oracle Users Group
Education Is Our Passion

Patches



© Puget Sound Oracle Users Group
Education Is Our Passion

SQLNET.ORA

```
# begining of Audit Vault configuration

SQLNET.AUTHENTICATION_SERVICES= (BEQ, TCPS)
SSL_VERSION = 0
SSL_CLIENT_AUTHENTICATION = TRUE
SQLNET.WALLET_OVERRIDE = TRUE
WALLET_LOCATION =
  (SOURCE = (METHOD = FILE)
  (METHOD_DATA = (DIRECTORY = /apps/oracle/product/10.2.2/av_1/network/admin/avwallet)))

# end of Audit Vault configuration
```

© Puget Sound Oracle Users Group
Education Is Our Passion

Enabling SYSDBA Privilege Connections

- The password file is created with SYS granted only the SYSOPER privilege and not the SYSDBA privilege.
- NOSYSDBA flag is set in the password file.
- Use the orapwd utility to create a new password file to enable SYSDBA connections.

```
orapwd file=orapwav password=oracle entries=5 force=y nosysdba=n
```

SYSDBA Live Demo

© Puget Sound Oracle Users Group
Education Is Our Passion

© Puget Sound Oracle Users Group

Recommended Resources

- Oracle Technology Network
  - http://otn.oracle.com (Audit Vault forum)
  - www.oracle.com/database/audit-vault.html
  - www.oracle.com/technology/products/audit-vault
- Tahiti
  - http://tahiti.oracle.com
- Metalink
  - http://metalink.oracle.com
- Morgan's Library
  - www.psoug.org (Audit Vault)
- Product Manager: tammy.bednar@oracle.com

© Puget Sound Oracle Users Group
Education Is Our Passion

ORA-03113

End-of-file on communication channel

© Puget Sound Oracle Users Group
Education Is Our Passion

Pricing and Packaging

- Oracle Audit Vault Server is priced at $50K per Processor,
  - Includes Restricted Use Licenses for
    - Oracle Database Enterprise Edition
    - Database Vault
    - Advanced Security
    - Partitioning
- Audit Vault Collection Agent
  - $3K per processor of the system from where audit data is being collected.
  - Supports Oracle 9iR2, 10g, and 11g databases
    - OS Audit File
    - AUD$, FGA$
    - Transaction Log (9.2.0.8, 10.2.0.3+, 11.1.0.6+)

© Puget Sound Oracle Users Group
Education Is Our Passion